BINOD BANIYA
5th SEMESTER

Computer Networks

Chapter - 2
Reference Model

2.1 **Protocol:**

→ It is a set of rules which governs the format and meaning of frames, packets or messages that are being exchanged between the peer entities.

→ The entities use protocols so as to implement their services.

Services:

→ It is defined as a set of operations that a layer can provide to the layer above it.

→ A service defines the state of operations that a layer is ready to perform but doesnot specify anything about implementation of these operations.

Interfaces And Services:

Interfaces:

It is defined as a bridge between two layers for the successful exchange of information between them in layer structu

Some important Terms

Entities and Peer Entities:

An entity is defined as the active element in each layer.
An entity can be either a software entity or hardware entity
Entity on same layer but on different machines are called pe
entity.

Service Provider And Service User

-> The entities at layer 'n' provides services for the layer (n+1) which is above nth layer.

-> Hence, layer 'n' which provides services is called service provider and layer 'n+1' which utilizes this service is called service user.

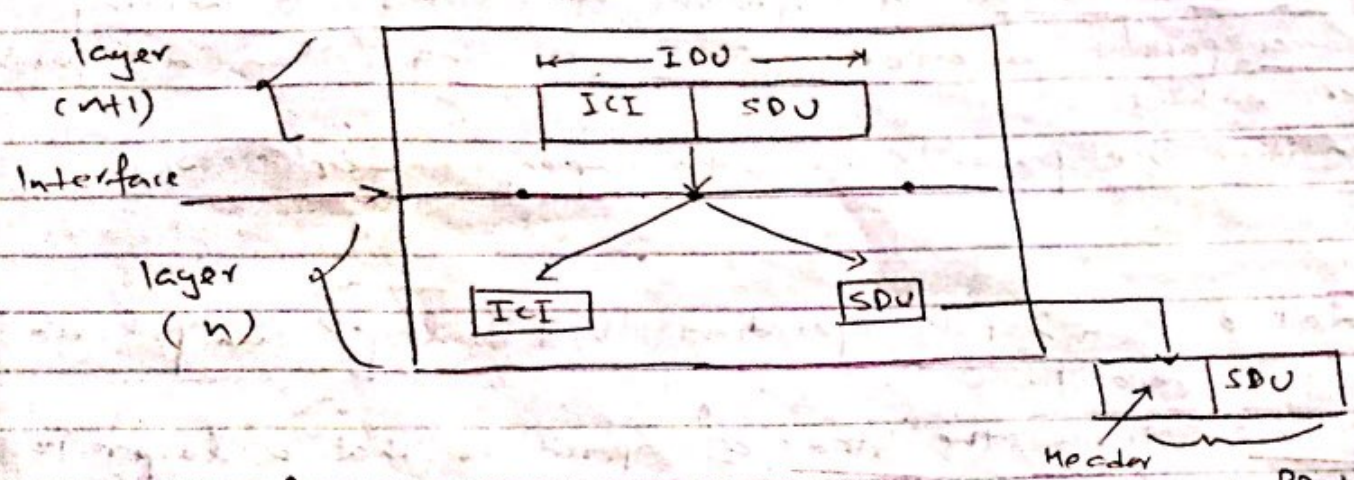


fig: Relation between layer at an Interface.

Service Access Points (SAPs)

-> They are available at interface of (n) and (n+1) layer.

-> Layer (n+1) can access services being offered by the layer (n) at the SAPs of layer n.

-> Each SAP has a unique address for its identification.

Interface Data Unit (IDU)

An IDU consists of two parts namely.

- SDU (Service Data Unit)
- ICI (Interface Control Information)

As shown in above figure, the layer (n+1) entity passes an IDU to the layer n entity through the SAP

IDU = | ICI | SDU |

Interface Control Information (ICI)

-> ICI contains the control information which is necessary to help the lower layer (n) to do the necessary job.

Services Data Unit (SDU)

-> SDU is the information passed across the network to the peer entity and then upto layer (n+1).

Protocol Data Unit (PDU)

-> In order to transfer the SDU, the layer n entity has to divide it into many smaller pieces.
-> Each piece is given a header and sent as a separate PDU.
-> Some PDU contain data while other contain control information.
-> The PDU headers will identify different types of PDUs.

Connection Oriented And Connectionless Services:

Layers can offer two types of services to the layers above them.

1) Connection Oriented Service:

- It is similar to the telephone system.
- The service users of connection oriented service undergo the following sequence of operation.
  i) Establish a connection.
  ii) Use the connection.
  iii) Release the connection
- The connection acts like a tube. The sender pushes bits from one end of the tube and the receiver takes them out from the other end.

-> The order in which the bits are sent is same as the order in which they are received.
-> Sometimes after establishing a connection, the sender and receiver can negotiate about quality of service message size and some other issues

0, Connectionless services
- It is similar to the postal service.
- Each message carries the full address of the destination.
- Each message is routed independently from source to destination through the system.
- It is possible that the order in which the message are sent and the order in which they are received may be different.

Quality of services (QoS)
- Each service can be judged by its quality of services. services can be of two types:
  i) Reliable
  ii) Unreliable

-> Reliable services are those which never lose data.
- Generally reliable services are implemented with receiver sending acknowledgements of the received messages.
- But acknowledgements introduce overheads and delays which are sometimes undesirable. for example: voice transmission. But electronic mail application is desirable for reliable service.

-> Unreliable services require high reliability of message arrival but no guarantee of arrival.
- The reliable service is more costly, complex as well as it causes more overhead than unreliable service.

Service Primitives

-> Primitives means operation.
-> A service is satisfied by a set of primitives specified
-> Primitives of connection oriented service are different from those of connection less service.
-> The primitives of client server environment are as follows:

Name	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection.
RECEIVE	Block waits for a message
SEND	Send the message
DISCONNECT	Terminate the connection

Reference Models (Network Architecture)

1.3 OSI Layers:

OSI Reference Model:

- The OSI reference is designed to deal with open systems.
- This model is based on a proposal developed by the International Standards Organization (ISO).
- It has seven layers:

Layer 7	Application Layer
Layer 6	Presentation Layer
Layer 5	Session Layer
Layer 4	Transport Layer
Layer 3	Network Layer
Layer 2	Data Link Layer
Layer 1	Physical Layer
Layer 0	Transmission media

fig: A seven layer of ISO-OSI reference model.

OSI is a layered framework for the design of n/w system that allows communications across all types of computer system.

Functions of different layers:

Physical layer:

i) To activate, maintain and deactivate physical connection
ii) To define voltages and data rates needed for transmission.
iii) To convert the digital bits into electrical signals.
iv) To decide whether the transmission is simplex, half duplex or full duplex.

Data Link layer:

i) Synchronization and error control of information which is to be transmitted over the physical layer.
ii) To enable the error detection, it adds error detection bits to the data which are to be transmitted.
iii) The encoded data are then passed to the physical layer.
iv) On other side, these error detection bits are used by data link layer to detect and correct the errors.
v) The outgoing messages are assembled into frames and the system waits for acknowledgements to be received after every frames is transmitted.

Network layer:

-> To route the signal through various channels to the other end.
-> To act as network controller by deciding which route data should take.
-> The outgoing messages are divided into packets & The incoming packets are assembled into message.

Transport layer

-> To decide whether transmission should be parallel or single path
-> To perform functions such as multiplexing, splitting or segmenting the data.
-> To guarantee transmission of data from one end to the other.
-> To break the data groups into smaller units so they can be handled more efficiently by the network layer.

Session layer

-> To manage and synchronize conversations between two different applications.
-> To control logging on and off, user identification.
-> To control billing and session management.
-> To avoid data loss.

Presentation layer:

-> To ensure that the information is delivered in such a way that the receiving system will understand and use it.
-> The form and syntax of a communication system can be different. In such conditions, the presentation layer provides the translations.

Application layer:

-> Manipulation of information in various ways.
-> To carry out the functions such as login, password checking etc.

Merits of OSI reference Model:

-> Services, Interfaces and Protocols are clearly distinguished.
-> The protocol in OSI model are better hidden. So, they can be easily replaced by new protocols as the technology changes.

-> It supports both connection oriented as well as connection less services.
-> It is a general protocol.

Demerits of OSI model:
-> Sessions and presentation layers are not used mostly.
-> In real life, there is a problem of fitting protocol into a model
-> This model was devised before the protocols were invented.

TCP/IP Reference Model:
-> It is a set of protocols that allow communication across multiple diverse network.
-> ARPA originally created TCP/IP to connect military network together, but later this protocol was given to government agencies and universities free of cost.
-> With the development of the HTTP for sharing HTML documents freely on the internet. www was born and soon TCP/IP came into much use.
-> TCP/IP are two protocols: Transmission control protocol and Internet Protocol. These two protocol describes the movement of data from Host computer to Internet.

Application
Transport
Internet layer
Host to Network

fig: layers of TCP/IP reference Model

Host-to-Network layer:

-> This is the lowest layer in TCP/IP reference model.
-> It helps to connect host to the network using some protocol so that the host can send the IP packet over internet.
-> This protocol varies from host to host and network to network.

Internet layer:

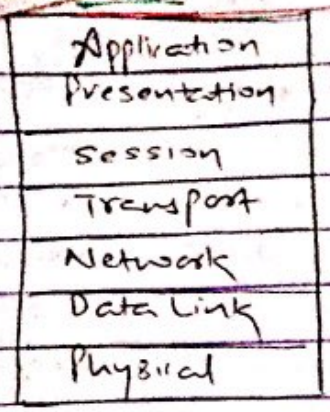
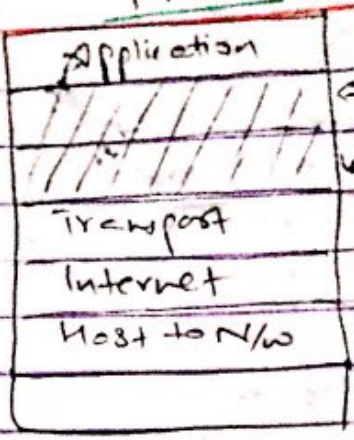
-> To allow the host to insert packets into any network and then make them travel independently to the destination.
-> To define a packet format and protocol called internet protocol.
-> It emphasize on routing of packets and congestion control.

Transport layer:

-> It allows peer entities of the source and destination machines to converse with each other.
-> Here, the protocols used are TCP and UDP.
* TCP is a reliable connection oriented protocol.
* UDP (User Datagram Protocol) is an unreliable connectionless protocol which is used for those applications which donot require flow control or sequencing.
* UDP is also preferred over TCP in those applications in which prompt delivery is more important than accurate delivery.

Application layer:

TCP/IP model doesnot have session and presentation layers because they are of little importance in most applications.
It is above Transport layer.
The protocols related to this layers are high level protocols such as HTTP, TELENET, FTP, SMTP etc.

OSI	TCP/IP
	
-> Has 7 layers.	-> Has 4 layers
-> Horizontal approach.	-> Vertical approach
-> Separate session layer.	-> No separate session layer, characteristics provided by transport layer.
-> separate presentation layer.	-> No presentation layer, characteristics are provided by application layer.
-> Transport layer guarantee delivery of packets.	-> Transport layer doesn't guarantee delivery of packets.
-> Network layer provides both connectionless & connection oriented service	-> Network layer provides only connection less services
-> It defines the service, interface and protocols clearly and makes a clear distinction between them.	-> It doesnot clearly distinguish between service interfaces and protocols.
-> The protocols are better hidden and can be easily replaced as the technology changes.	-> It is not easy to replace protocols
-> OSI is truely general model.	-> TCP/IP cannot be used for any other application.
-> It has a problem of protocol fitting.	-> This protocol don't fit any other protocol stack.

Demerits of TCP/IP model:

-> It doesnot clearly distinguish between service, interface and protocols.

-> It is not a general model and cannot be used for any other application.

-> It doesn't fit any other protocol stack.

-> The host to layer network layer is not a layer in normal sense. It is simply an interface.

-> TCP/IP model doesnot even mention physical and data link layer. A proper model should include both as separate layer.

Network hardware components

1) NIC (Network Interface Cards)
2) Hub
3) Repeater
4) Switches
5) Bridge
6) Router

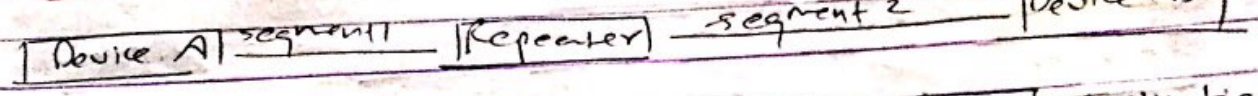
1) NIC (Network Interface Card)

- NIC is housed inside the computer on the motherboard.
- It provides the physical connection between the network and the computer station.
- The NIC is responsible for operations taking place in the physical layer of OSI reference model
- It is only concerned with sending and receiving 0's and 1's
- All the NICs are manufactured with a unique 48 bit MAC address
- There are following three common types of NICs.
  - i) Ethernet cards
  - ii) Local talk connections
  - iii) Token ring cards

2) Repeater:

- A repeater is a device which operates only in the physical layer.
- We know that all transmission media weaken the electromagnetic waves that travel through them.
- Devices that amplifies signals to ensure data transmission are called repeaters.

- A repeater receives a signal and before it becomes too weak or corrupted, regenerates the original bit pattern. Hence a repeater can extend the physical length of the LAN as shown



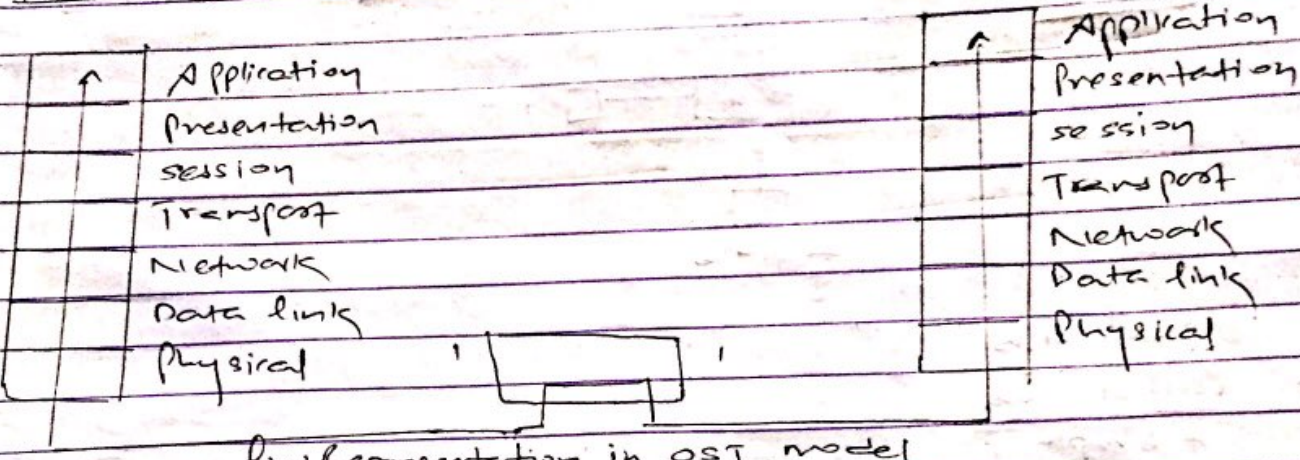
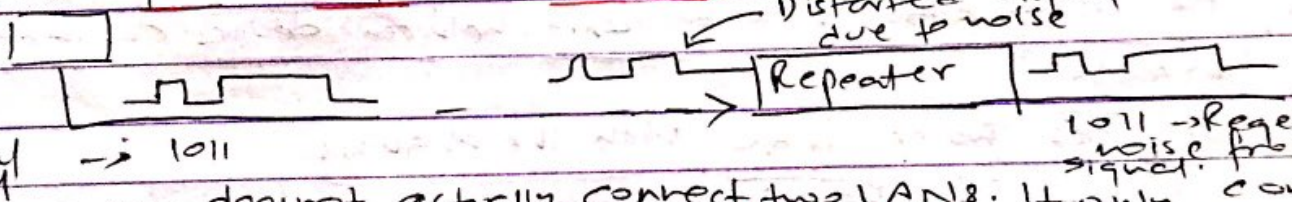


fig: Representation in OSI model

→ Repeater is not an amplifier because amplifier simply amplify the entire incoming signal along with noise however repeaters create an exact duplicate of incoming data by identifying it from the noise, reconstructing it and retransmitting only the desired information.

- In repeater, original signal ~~strength~~ is duplicated, boosted to its original signal strength and sent as shown in figure



- A repeater doesn't actually connect two LANs. It only connect two segments of the same LANs.
- A repeater cannot connect two LANs of a different proto
- A repeater forwards every frames, it has no filtering capabi
- A repeater must be placed at a precise point on the link su that the signal reaches it before the noise has induced an error in any of the transmitted bit.

3) Hubs

- Usually, the word Hub can refer to any connecting devices however, its specific meaning is multiport repeater.
- Basically used in star topology.
- Hub organizes cable and relays signal to other media segment

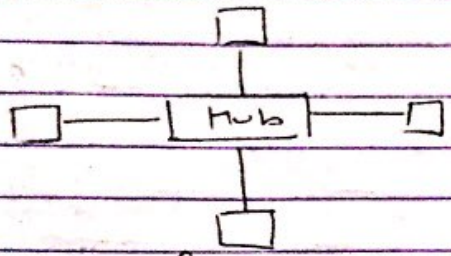


fig: Hub

Types of Hub

i) Passive Hub

- It simply combines the signals of a network segments.
- There is no signal processing or regeneration.
- Passive hub reduced the cabling distance by half because it doesnot boost the signals but infact absorbs some of the signal.

ii) Active Hub

-> They are like passive hub but have electronic components for regeneration and amplification of signals.

-> By using active hub, distance between devices can be increased.

-> It amplifies noise along with the signals

-> much expensive than passive hubs

iii) Intelligent Hubs.

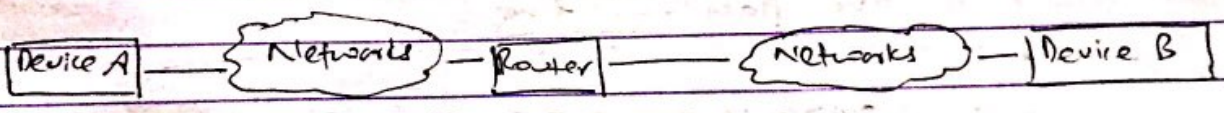
-> In addition to signal regeneration, intelligent hubs performs some network management and intelligent path selection.

4) Bridges
- It can operate in physical as well as in the data-link layer.
- In physical layer it can regenerate the signal that it receives.
- In data link layer, it can check the physical (MAC) address of source and destination contained in the frame

- The major difference between bridge and repeater is that the bridge has a filtering capacity i.e it can check the destination address of a frame and decide if the frame must be forwarded or drop.

- If the frame is to be forwarded then the bridge must specify the port over which it must be forwarded.
- The bridge about change the physical address contained in the frame
- Two types
  i) Transparent Bridge and Routing bridge

5) Routers



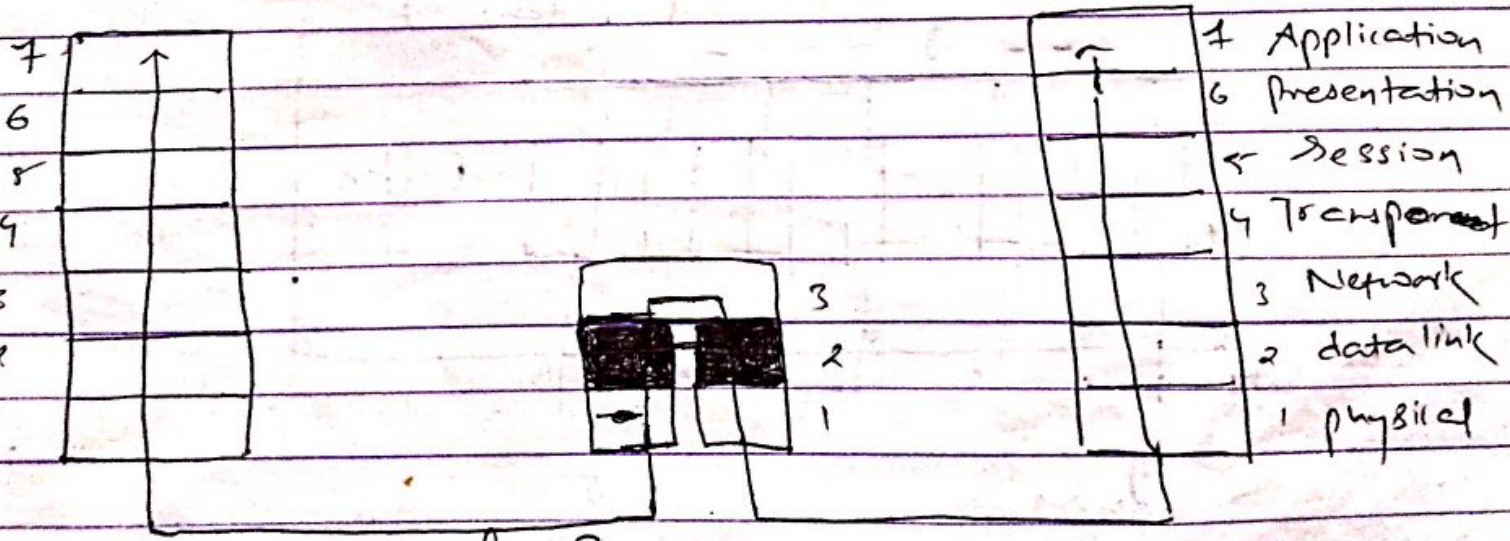


fig: Router in OSI model

- Routers are devices that connect two or more networks.
- They consists of a combination of hardware and software.
- hardware : It can be network server, a separate computer or a special device
- software : It includes OS and routing protocol. Management software can also be used.
- Routers use logical and physical addressing to connect two or more logically separate networks

c) Switch :
- A switch is a device which provides bridging functionality with greater effeciency.
- A switch acts as a multiport bridge to connect devices or segments in a LAN.
- The switch has a buffer for each link to which it is connected
→ when it receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link. If outgoing link is free, the switch sends the frame to the particular link.

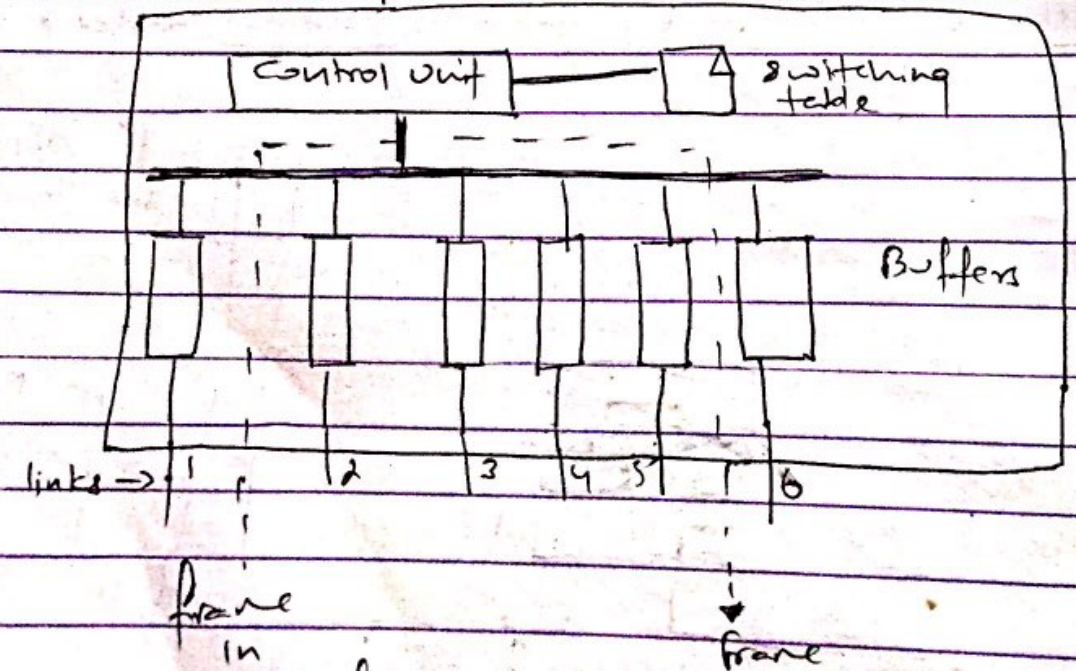


fig: Illustration of a switch

Two types

1) Store-and-forward switch: It stores the frame in the input buffer until the whole packet had arrived.

2) Cut-through switch: It forwards the packet to the output buffer as soon as the destination address is received.

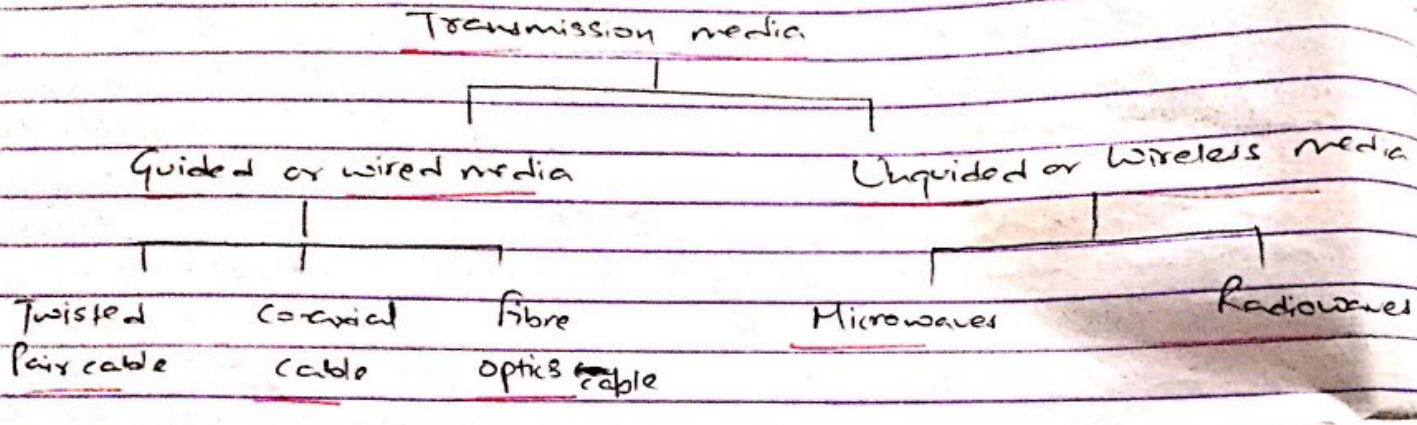
Hub	Switch
1) It is a broadcast device.	1) It is a point-to-point device
2) It operates at physical layer.	2) It operates at data link layer
3) It is not an intelligent device	3) It is an intelligent device.
4) It simply broadcast the incoming packets.	4) It uses switching table to find the correct destination.
5) It cannot be used as repeater.	5) It can be used as repeater.
6) Not a complex device	6) It is a complex device.
7) Not very costly	7) Costly.

Chapter 3

Transmission Medium:

-> It is defined as anything that can carry information from source to destination

Classification



Wired Media

-> The signal energy is contained and guided with a solid medium.

-> Twisted pair cables, coaxial cable, optical fibre cables are the examples of wired media.

-> It leads to discrete network topologies.

It is used for point-to-point communication.

Installation is costly, time consuming and complicated.

Wireless Media

-> The signal energy propagates in the form of unguided electromagnetic waves.

-> Radio and Infrared light are the examples of wireless media.

-> It leads to continuous network topologies.

-> It is used for radio broadcasting in all.

-> Installation needs less time and money.

Wired Media	Wireless Media
- Attenuation depends exponentially on the distance.	- Attenuation is proportional to the square of the distance.
- Bandwidth can be increased by adding more wires.	- It is not possible to increase bandwidth.

Advantages of wireless Media over wired Media

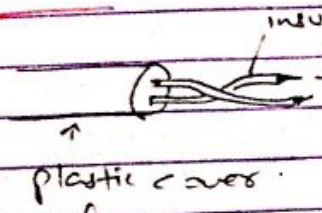
* Using wireless medium, we can access the server anywhere (i.e mobility)
* It helps to enable the Bring Your Own Device (BYOD) phenomenon so that the employees can bring their own devices in the workplace and access the server.
* With the help of wireless medium, the employee can collaborate where and when they need which helps to increase the efficiency and speed of operation that results in increased productivity.
* The Public Wi-Fi hotspots enables people to get onto the internet when they are away from office and home.
* It is more convinient to add new users to a wireless network than wired network.
* It is cheaper to make international calls using wireless media. (voice over internet protocol) VoIP.
* Using wireless media over wired media is more cost effective for developing large area network.
* As there is no physical wires involved in wireless media, there is no potential risk of accident, which ensures health and safety.

Twisted Pair cable:

Types:
- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)

UTP

Construction



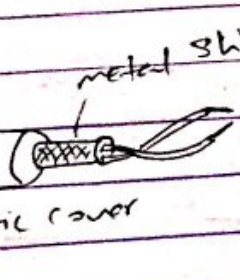
It consists of two insulated conductors twisted together in a spiral form as shown in figure.

Advantages:
- It is cheap & easy to install.

Disadvantages:
- It is easily affected by noise.

STP

construction



- It consists of two insulated conductors twisted together in a spiral form.
- However, it has a metalshield to cover each pair of insulating conductor to reduce the interference of noise.

Advantages:
- It has relatively less interference of noise than UTP.
- It has higher bandwidth (relatively) than UTP

Disadvantages:
- It is bulky than UTP
- It is expensive than UTP.

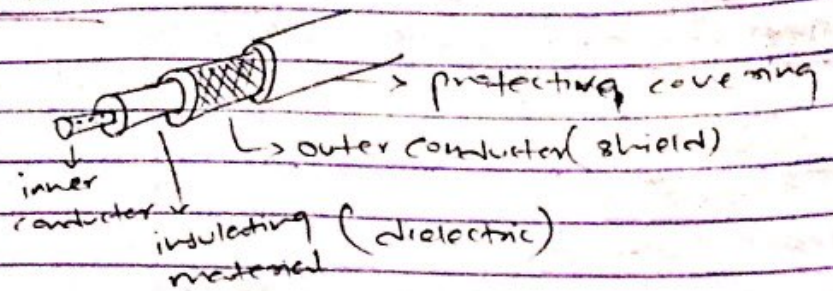
Why to twist the wires?
-> Twisting of wires will reduce the effect of noise or external interference.
-> Number of twists per unit length determines the quality of cable
-> More twists means better quality.

Applications of Twisted pair cable:
(i) In telephone lines to carry voice and date channels.
(ii) In DSL line (ADSL)
(iii) In LAN such as 10 BaseT and 100 BaseT
(iv) In ISDN

Connectors for Twisted pair cable:
(i) RJ45 (Registered Jack)

d. Co-axial cable:

Construction:



-> It consists of concentric conductors separated by a insulating material. The external conductor is used for shielding purpose which is a metallic braid and inner conducter is used for to transmit
-> The tough plastic jacket forms the cover of the cable providing insulation and protection.

Advantages:

-> It has relatively less noise interference than twisted pair.
-> It has greater bandwidth and low attunation than twisted pair cable.
-> It is easy to install.
-> cheaper than fibre optics.

Disadvantages:

① Expensive than twisted pair.
② High attunation than fibre optics cable.
③ Low bandwidth than fibre optics cable.

Applications of co-axial cables

1) Analog telephone networks
2) Digital telephone networks
3) Cable TV

iv) Traditional Ethernet LANs
v) Thick and thin Ethernet
vi) Digital Tearymission.

Imp

Broadband Co-axial cable
-> It is used for analog signaling.
-> They are capable of transmitting many signals simultaneously.
-> It is capable of transmitting data, voice and video.
-> It can cover greater distance.
-> They are not pupular.
-> They are more expensive.
-> They are difficult to maintain and install.

Baseband Coaxial cable
-> It is used for digital signaling.
-> They are capable of transmitting one signal at a time.
-> It is capable of transmitting only data and voice.
-> It cover less distance.
-> They are popular.
-> They are less expensive.
-> They are easy to maintain and install.

connecter for Co-axial cable:
* BNC connecter
* BNC-T "
* BNC terminater.

Inf

Optical fibre cables:

Construction:

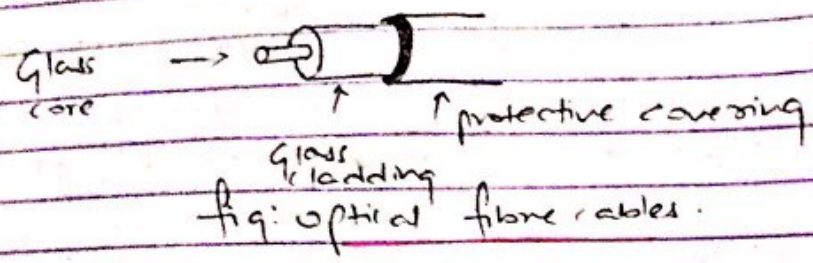


fig: optical fibre cables.

-> It consists of an inner glass core surrounded by a glass cladding which has a lower refractive index.

Working Principle:

-> for data transmission to take place, the sending device must be capable of inducing digital bits / signal (0 & 1) into the light signal with the help of light source such as LED or laser.

-> when the light enters into a glass fibre from one end then the light stays inside the fibre and doesnot escape through the walls because of the total internal reflection taking place inside the fiber.

> At the receiving end, the light that travels from the sender is captured by using a photo detector.

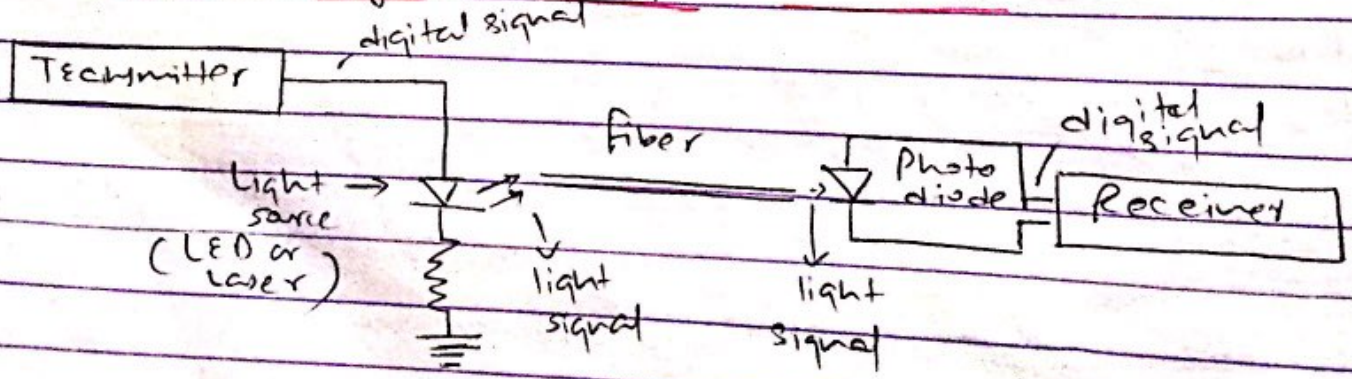


fig: Working Principle of Optical fibre.

Advantages:

-> Higher bandwidth for data transmission.
-> Lower attenuation
-> can carry signal to longer distances without using amplifiers and repeater in between.
-> arent affected by EMI effects and can be used in those areas where high voltages are passing.
-> It is of small size & light weight.
-> The material used for the manufacturing of optical fibre is silica glass. The material is easily available. So, the optical fibres cost lower than the cables with metallic conductors.

Drawbacks:

1) Sophisticated plants are required for manufacturing optical fibres.
2) The initial cost is high.
3) Joining the optical fiber is difficult task.
4) The cost of fibre optic cable is more compared to twisted pair and co-axial
5) The installation of fiber optics cable is tedious.

Copper wire	Optical fibre.
-> Low bandwidths	-> High bandwidths.
-> Higher attenuation.	-> Lower attenuation.
-> Are affected by EMI effects	-> are not affected by EMI effe
-> It is large size & heavy in weight.	-> It is small in size & light in weight.
-> Joining the copper wire is easy.	-> Joining optical fiber is difficult

Copper wire

-> cheaper installation cost.
-> Easy to maintain
-> Requires less handle with care.

Optical fibre

-> Expensive installation cost
-> Difficult to maintain.
-> It requires more handle with care.

Unguided (Wireless)

-> It doesnot use an electrical or optical conductor.
-> In most cases the earth atmosphere is the physical path for the data.

Wireless transmission:

-> Radio wave
-> Microwave
-> Infrared

1. Radiowave:

-> Radiowave have frequencies between 10 kHz to 1 gigahertz.
-> The electromagnetic spectrum between 10kHz and 1 GHz is called radio frequency (RF).

Types of radio wave:

-> Short wave is used in AM radio
-> Very High frequency (VHF) used in FM radio and TV
-> Ultra High frequency (UHF) used in TV.

Applications:
i) Cellular communication
ii) Wireless LAN
iii) Radio System
iv) Satellite communication

2) Microwave transmission: (1 - 300 GHz)
-> It is lower GHz frequency of electromagnetic frequency spectrum.
-> They have higher frequency than RF.
-> They produce better throughput and performance.
-> They are unidirectional.

Two types:
i) Terrestrial Microwave System.
ii) Satellite
-> It requires line of sight for data transmission.

Applications:
i) In cellular phones
ii) wireless LANs
iii) Satellite Networks

3) Infrared:
-> The electromagnetic waves having the frequencies from 300 GHz to .400 THz are known as infrared waves
* They use line of sight propagation.
-> It cannot penetrate walls. This means that it can be easily contained within a room.
-> It can be used in different rooms for same frequency.

-> It has greater bandwidth.

Disadvantages:

-> Sun generates the infrared radiation which cause a lot of interference for infrared communication.

Applications:

- TV remote
- Keyboard
- Mouse
- transmission of data with very high data rate.
- Printer

Satellite Communication:

-> A geostationary satellite is basically a relay station in space. It receives signal from one earth station, amplifies it, improves it and radiates it back to other earth station.

-> Such a communication system allows us to communicate with any corner of the world.

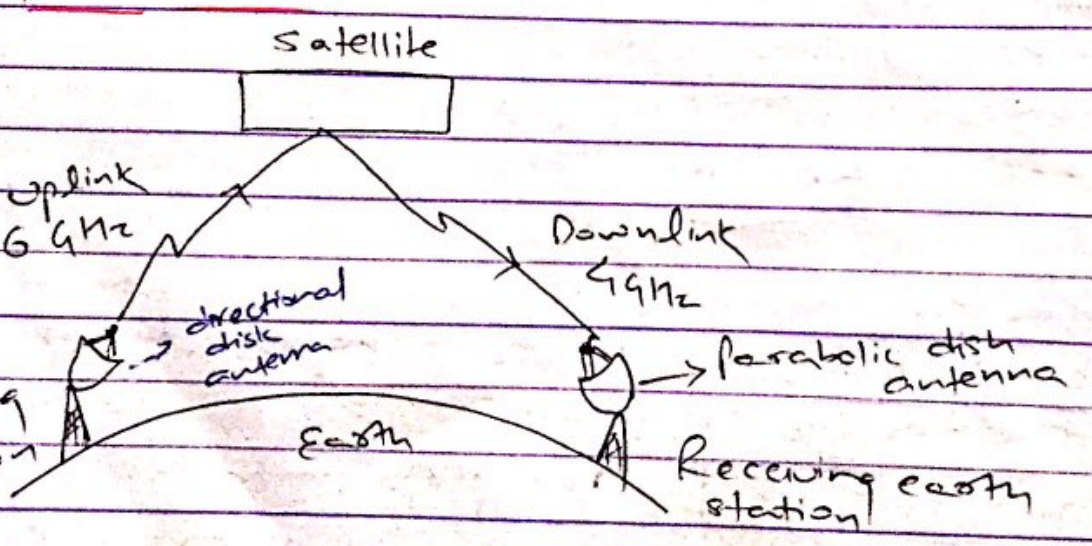


fig: Basic operation of satellite communication system.

-> An earth station transmits information signal to the satellite using directional dish antenna.
-> The satellites receives this signal, processes it and transmits it back at a reduced frequency.
-> The receiving earth stations receive this signal using parabolic dish antennas pointed towards the satellite.
-> The signal which is being transmitted upwards to the satellite is called as the up-link and is normally at a frequency of 6GHz.
-> The signal which is transmitted back to the receiving earth station is called as the down link and is normally at a frequency of 4GHz.

Features of Satellite System:

1) Due to long distance, delay is introduces.
2) Satellite is a broadcast media. Hence it is useful for a broadcast applications.
3) The cost of transmitting a message doesnot depend on the distance to be travelled
4) It is useless when privacy is needed as it is broadcast media.
5) have low error rates.

Satellite Communication	Optical Communication
-> Communication takes place via Satellite.	-> communication takes place via optical fibrer.
-> Communication takes place by means of em. waves.	-> communication takes place by means of light rays.
-> useful for long distance communication.	-> useful for short distance communication.
-> useful for broadcast communication.	-> useful for point to point communication.
-> Special type of antennas are required.	-> Antennas are not required.
-> cost of installation is high.	-> cost of installation is low.
-> difficult to setup.	-> easy to setup.

-> It allows multiple digital signals to operate on single easily through the same regular phone wiring used for analog lines, but ISDN transmits a digital signal rather than analog.
-> Latency is much lower on ISDN.

ISDN (Integrated Services Digital Network)

-> It is a wide area network that provides end-to-end digital connectivity to support voice and data services.

Types:

① Narrowband ISDN
② Broadband ISDN

Narrowband ISDN	Broadband ISDN
-> first generation of ISDN	-> Second generation of ISDN
has smaller bandwidth.	-> has larger bandwidth.
-> provides poor service	-> provide better service.
-> has circuit switching orientation.	-> has message switching orientation.

Services provided by ISDN

1) FAX
2) Videotext services
3) Teletext services
4) Voice applications
5) Data applications

ISDN Architecture

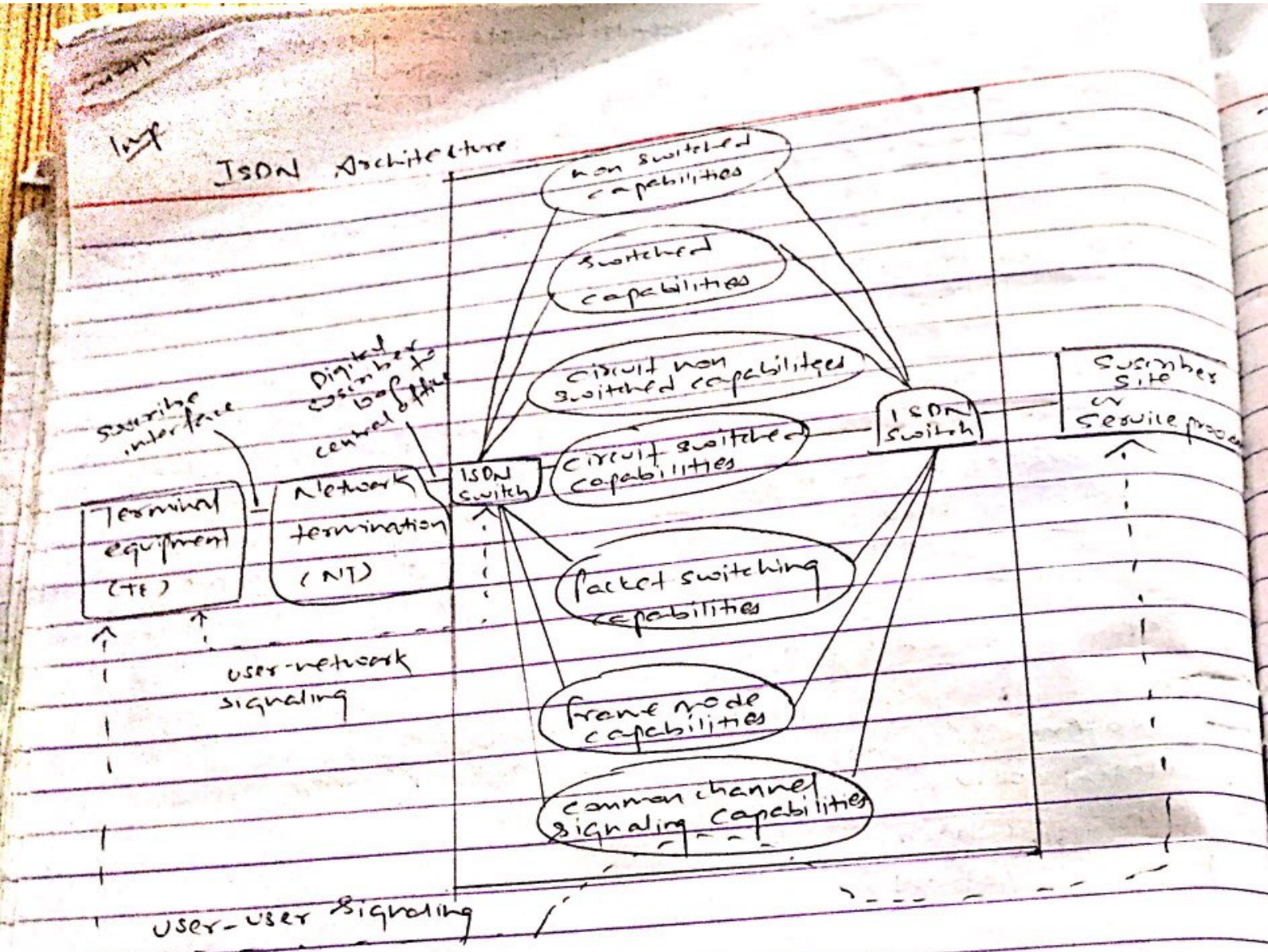


fig: ISDN Architecture

-> The architecture of ISDN is as shown in figure
-> A physical connector called 'Digital Subscriber loop' is supported by ISDN.
-> The Digital Subscriber loop is the link between the end user and the central or end office.
-> It provides common physical interface.
-> The central information between user device and network is exchanged using protocols.

-> The subscriber loop belonging to the telephone network is one or two twisted pair to provide communication link to connect subscriber to office.

Advantages of using ISDN
-> Cost saving and flexibility.

Network Performance Measures:
1. Bandwidth
2. Throughput
3. Latency
4. Bandwidth-delay product
5. Jitter

Bandwidth:
-> In Analog communication, the total capacity of the communication channel is measured in hertz (Hz). The difference between highest and lowest frequencies capable of being transmitted is called bandwidth.
-> In Digital communication, total number of bits transferred in unit time is called bandwidth. It is expressed in bits per second (bps) and known as data rates.

Throughput:
-> It is realistic measure of the amount of data transmitted between two nodes in a given time period.
-> Compared to bandwidth, throughput is what the channel really achieves, whereas bandwidth is what is theoritically possible.
-> function of hardware/software, speed, CPU power etc.

Latency:

- The amount of delay a network device introduces when data frames pass through it.
- In other words, it is the amount of time a frame spends inside a network device.

Jitter:

-> An irregular variation in the shape of signal. will vary over time.

-> Also, it is the variation in the timing between a sender's and receiver's respective clocks

* Sliding window Protocol
- A protocol that allows several data units to be in transition before receiving an acknowledgement. It is used in TCP for error control and flow control.
- Send window
  * Maintain by the sender
  * A set of sequence number
  * Represents a range of valid sequence number for transmitted but not yet acknowledged frame.
  * As the protocol operates, the window slides forward over the sequence number space.
- receive window:
  * Maintain by the receiver
  * A set of sequence number
  * Represents a range of frames it is permited to accept.
  * As the protocol operates, the window slides forward over the sequence number space.

Chapter: 4

Data link layers and protocols

- This layer deals with frame formats, flow control, error control, addressing and link management.
- It received from data layer and provides service to the network.
- It transfer data from the network layer of the sending machine to the network layer of the receiving machine.

4.3 Framing:

- Breaking the bit stream into frames is called as framing
- During transmission;
  - The bits to be transmitted is broken into discrete frames at data link layer.
  - Checksum of each frame is computed.
  - when a frame is received, checksum is recomputed
  - If it is different from the checksum present in the frame then, there is error.
  - the bad frame is discarded and request for transmission is sent

Framing Methods:

i) Character count (used practically with combination of other)
ii) Starting and ending characters, character stuffing
iii) starting and ending flags with bit stuffing
iv) Physical layer coding violations.

i) Character count:

A field in the header is used to specify the number of characters in the frame.

ii) Starting and ending characters with character stuffing
Here starting character is used before the starting of each frame and ending frame is used at the end of each frame.

iii) Starting and ending flags:
Here, specific bit pattern is used before and after the frame.

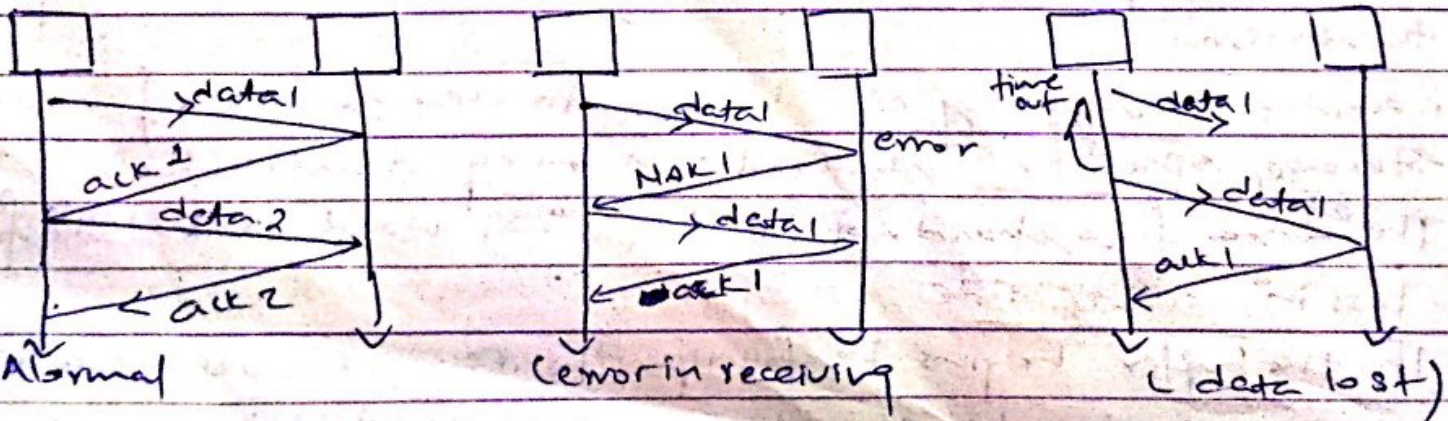
iv) Physical layer coding violations:
- 1 is encoded as 10 pair
- 0 is encoded as 01 pair.

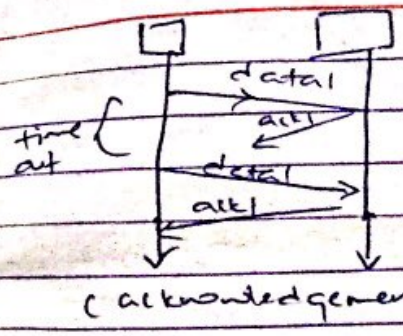
4.4 Flow control:
- Flow control is the mechanism to control the rate of frame transmission from sender to a value which can be handled by the receiver.
- The receiver will keep loosing some of the frames simply because they are arriving too quickly, so flow control is used.
- Problems in modern communication:
* The rate of processing is generally slower than the rate of transmission
* Receiving device may also have a limited amount of memory storage space for storing the incoming data (buffer).
* The rate of data flow should not be high, that would result the frame loss in receiver side.
* If the buffer begins to fill up, the receiver must be able to tell the sender to stop transmission until it is once again able to receive.
Eg: Youtube Buffer

ARQ - (Automatic Repeat Request)
The sender waits for a positive acknowledgement before advancing to the next data item.

Methods of flow control:
1. Stop-and-wait
2. Go-back-N
3. selective-repeat-request
4. Piggy backing

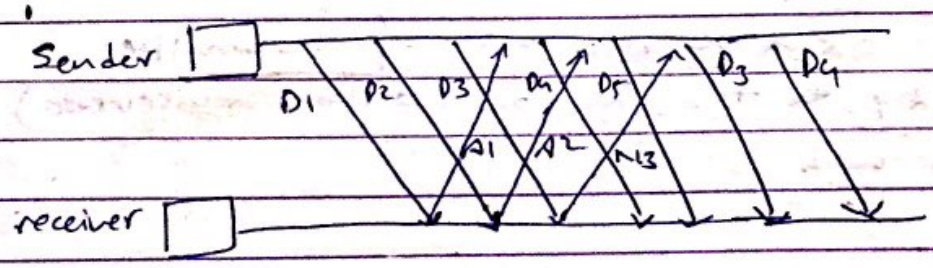
① Stop and wait ARQ:
- The sender sends one frame and waits to gets its acknowledgement. Only after receiving the ack, it transmits the next frame.
- The sender sends one frame of data and waits for an acknowledgement from the receiver. If it receives a positive acknowledgement (ack) it transmits the next frame. If it receives a negative acknowledgement (nak) it retransmits the same frame. If neither is received for specified time the last frame is retransmitted.





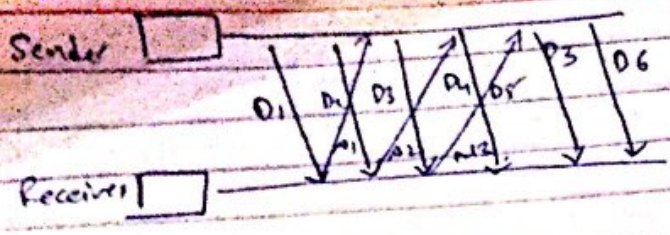
② Go-back-N

- In this method, Sender is allowed to ~~transmit~~ continue sending enough frames so that channel is kept busy while waiting for the acknowledgement signal from the receiver
- If one frame is damaged or lost all frames since the last acknowledged frame is retransmitted.
- The major difference between Go-back-N and stop-and-wait is that the sender doesn't wait for ~~acceptance~~ 'Ack' signal for the transmission of next frame. It transmits the frame continuously as long as it doesn't receive the 'NAK' signal.



③ Selective-Repeat-Request ARQ:

- In this method, Sender is allowed to continue sending enough frames so that channel is kept busy while waiting for the acknowledgement signal from the receiver..
- If one frame is damaged or lost only that specific frame is retransmitted.



(4) Piggy Backing:

- In this method, when a data frame arrives, the receiver does not immediately send the acknowledgement signal.
- The acknowledgement signal is sent back to the receiver along with the data that is being transferred from receiver to sender
- This technique of delaying acknowlegement is "Piggy Backing".
- Advantage is better use of bandwidth.
- Drawback is additional system complexity.

4.5 Error Control Mechanism:

4.5.1 Error Detection:

- Error occurs when one or more number of transmitted bit will be reversed during transmission. (0 to 1 or viceversa)
- Error Detection Methods:

1) Parity check
2) Checksum Error detection
3) Cyclic Redundancy check.

1) Parity check:

- Add an extra bit known as parity bit to each word being transmitted.
- It can be odd or even parity.
- Two-dimensional parity check can find the exact bit.

② checksum error detection:
- when a word is being transmitted, it is added to the previously send word and the sum is retained known as checksum
- checksum is calculated in receiving end also, If checksum sender = checksum receiver. Then no error. otherwise there is error.

3) Cyclic Redundancy check (CRC)
- CRC is based on binary division.
- Define are divisor.
- Divide the word being transmitted and receive the remainder.
- Append the remainder at the end of data unit.
- The resulting data unit becomes exactly divisible by the same divisor.
- The resulting data unit is called 'codeword'
- At the receiver divide the received codeword by the divisor. If no remainder than no error if remainder then error exists

4.5.2. Error Correction:

Techniques:

① Linear Block Codes

② Hamming Codes:

① Linear Block Codes:

- At the end of k-bits of message, 'N-k' bits of parity is added to form n-bit code word.

(2) Hamming code: is defined by the following eqn.
If n be the block length, n be the number of parity bits and k be the number of message bits then

Block length (n) = $2^m - 1$
No. of msg bits (k) = $2^m - 1 - m$
No. of parity bits (m) = $n - k$

The code word pattern for 7-bit hamming code is.

D_7	D_6	D_5	P_4	D_3	P_2	P_1

where D bits are data bits, P bits are parity bits.

Selection of P_1: P_1 is adjusted to 0 or 1. So, as to establish even parity over bits 1, 3, 5, 7
ie P_1, D_3, P_5, P_7

Selection of P_2: P_2 is adjusted to 0 or 1, so, as to establish even parity over bits 2, 3, 6, 7
ie P_2, D_3, D_6, D_7

Selection of P_4: P_4 is adjusted to 0 or 1, so as to establish even parity over bits 4, 5, 6 & 7
ie P_4, P_5, D_6 & D_7

Hamming code is obtained and transmitted:

At the receiver, the received hamming code is decoded to get the data back. The bits (1,3,5,7), (2,3,6,7) and (4,5,6,7) are checked for even parity. If all 4 bits ~~detect contain error then~~ groups posses even parity then the received code word is correct. If not there is error. Error can be located by forming a 3-bit number out of the 3 parity checks.

Message: 1011

P_7	P_6	P_5	P_4	P_3	P_2	P_1
1	0	1	1	1		

For, P_1 even parity check (1, 3, 5, 7)
So, P_1 will be 1
So P_2 - P_2 will be 0
And for, P_4 it will be 0
So, code word = 1010101
Suppose ~~transmitte~~ received word was 1000101

even
Check parity:
bits 1, 3, 5, 7 are in ~~are in~~ odd parity
bits 2, 3, 6, 7 are in even parity
bits 4, 5, 6 7 are in odd parity.

So, error bit will be.

P_4	P_2	P_1	
1	0	1	→ 5th bit

i.e P_5

So, correct code word is 1010101

Flow control

-> Flow control observes the proper flow of the data from sender to the receiver.
-> Flow control adjust and confirm data flow rate for successful transmission.
-> It is done by:
i) Stop-and-wait
ii) Go-back-N
iii) Selective-repeate-request.
iv) Piggy Backing

Error control

-> Error control observes that the data delivered to the receiver is error free and reliable.
-> Error control is a way to recover corrupted data.
-> It is done by:
Error detect by Parity check
Checksum, CRC
Error control by Hamming code.
Linear Block code

HDLC frame format:

- HDLC (High-level Data Link control) is a group of protocols for transmitting data (packets) between nodes (point-to-point).
- In HDLC, data is organized into a frame.
- HDLC protocol resides with Layer 2 of the OSI model the data link layer.
- HDLC uses zero insertion/deletion process (bit stuffing)

HDLC ~~frame~~ frame format

Flag	Address	Control	Information	FCS	Flag
8 bits	8 or more bits	8 or 16 bits	n x 8	16 or 32	8 bits

Flag:

- It is present at start and end.
- It helps in frame-level synchronization

Address:
- It is used for addressing in multi-point links

control field:
- It is used for flow control and error control

Information field:
- It is used for link management data.
- It is used to store user data bits
- It is completely transparent

FCS (Frame check sequence):
- It is used for error detection.

Types of HDLC frame format:
i) The I-frame or information frame
ii) The S-frame or Supervisory frame
iii) The U-frame or unnumbered frame

(Logical Link control)
LLC and MAC Sublayers:
(Medium Access Control)

LLC
* Handles communication between upper and lower layers
* Takes the network protocol data and adds control information to help deliver the packet to the destination.

MAC:
* Constitutes the lower sublayer of the data link layer
* Implemented by hardware, typically in the computer NIC
* Two primary responsibilities: i) Data encapsulation
ii) Media Access control

Channel Access:

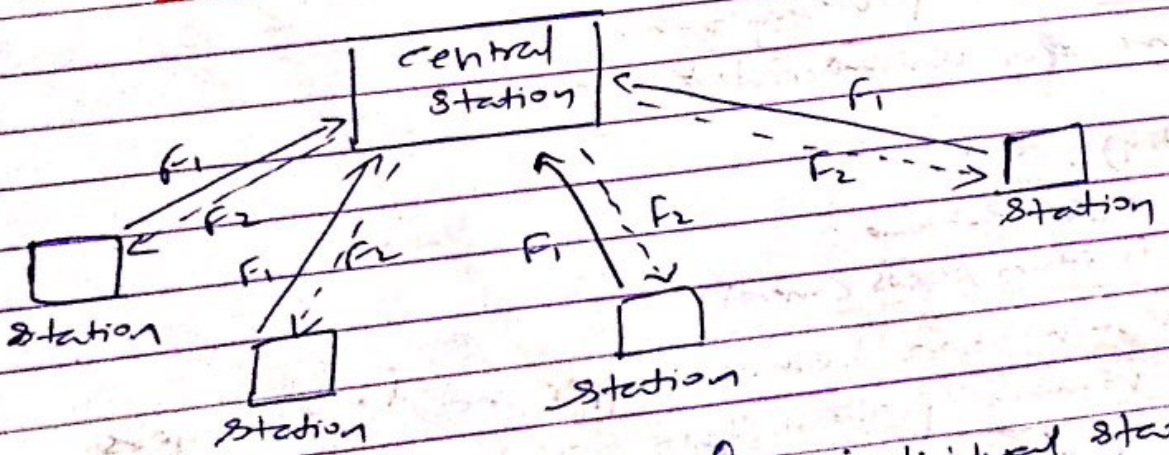
4.6.1 ALOHA System:

- System in which multiple users share a common control in a way that can lead to conflicts are widely known as contention systems
- The ALOHA system is a contention protocol.
- Two types: Pure and slotted ALOHA

1) Pure ALOHA:

- It allows any station to broadcast at 'anytime'. If two signals collide, each station simply waits a random time and tries again

- collisions are easily detected



F_1 - broadcast frequency from individual station.

F_1 - " " from the central station.

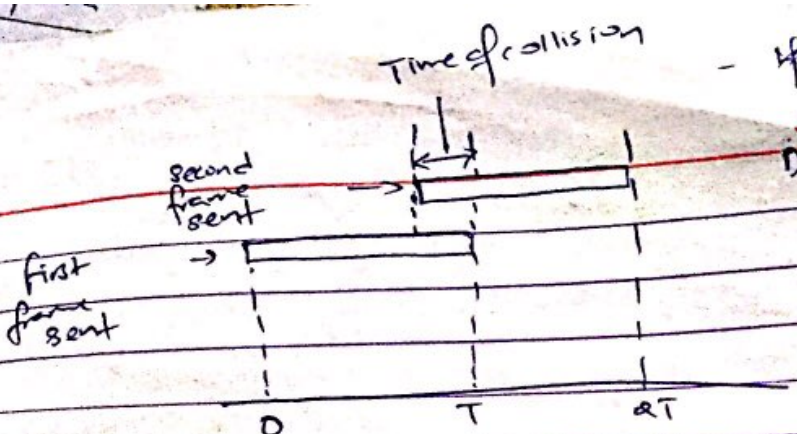


fig: Transmission using Pure ALOHA.

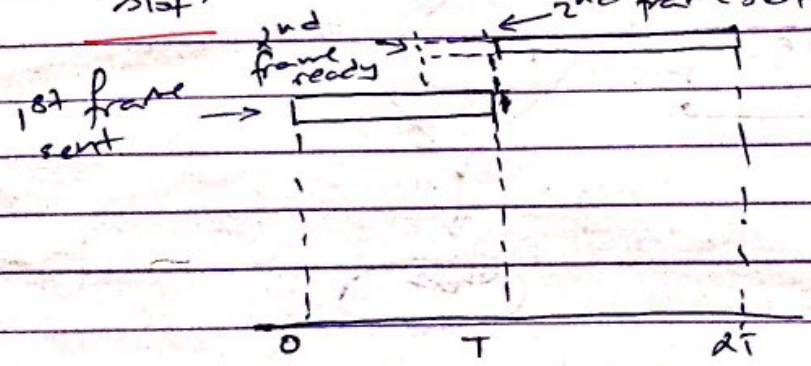
- If ... station

Advantage: ... plo

Disadvantages: Performance is worst when traffic increases.

2. Slotted ALOHA:

- Here, time is divided into discrete intervals, each interval corresponds to one frame.
- ~~Frames~~ frames can be sent only at starting of each time slot.



Transmission using Slotted ALOHA.

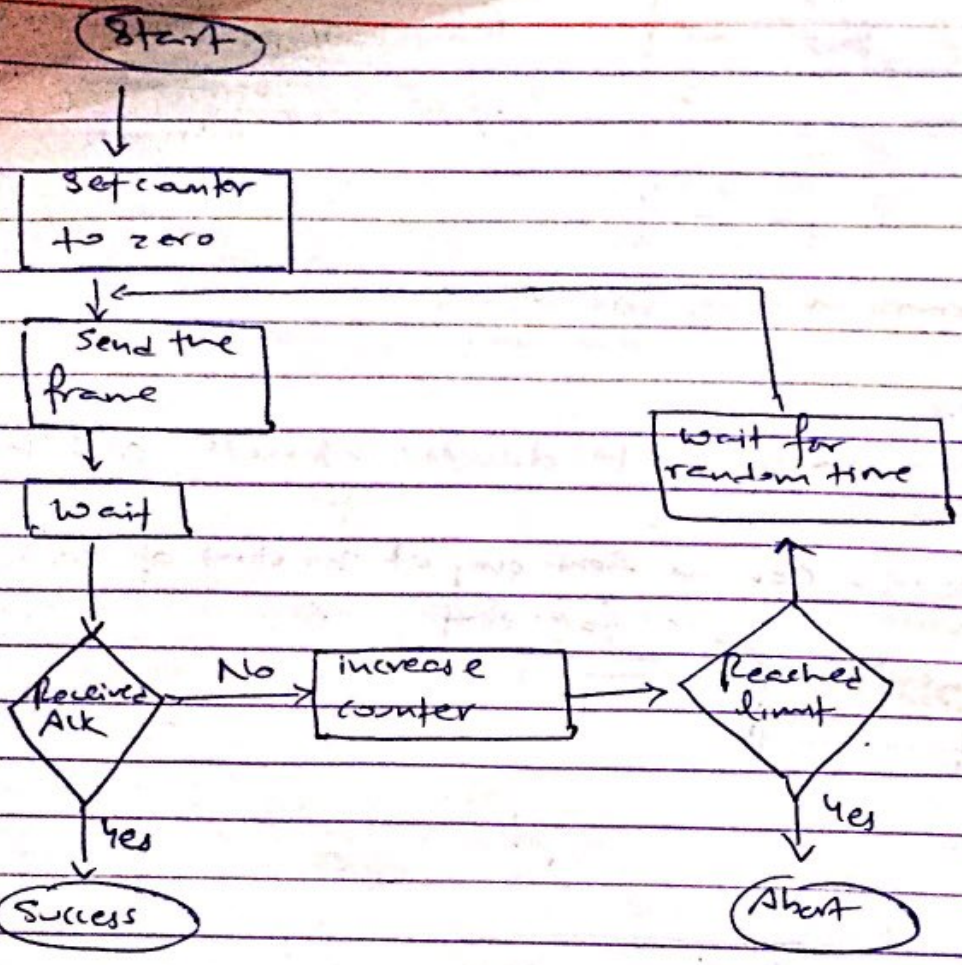


fig: flowchart of ALOHA

4.6.2 CSMA, CSMA/CD

Carrier Sense Multiple Access/collision Detect

- CSMA is a protocol that operates on carrier sensing i.e a station listenes to see the presence of transmission on the cable and decides accordingly.

Types:

① Non-Persistent CSMA:
- wait fixed time if channel is busy.
- check after the fixed interval of time
- send if free.

ⓐ 1- persistent CSMA
- check continuously if channel is busy.

ⓑ P- persistent CSMA.
- The waiting stations cannot send immediately when channel is free.
- If P = 1/6 and if 6 stations are waiting then on average only one station can transmit while others will wait.

In CSMA, transmitting station continues to transmit its frame even though a collision occurs.

CSMA/CD

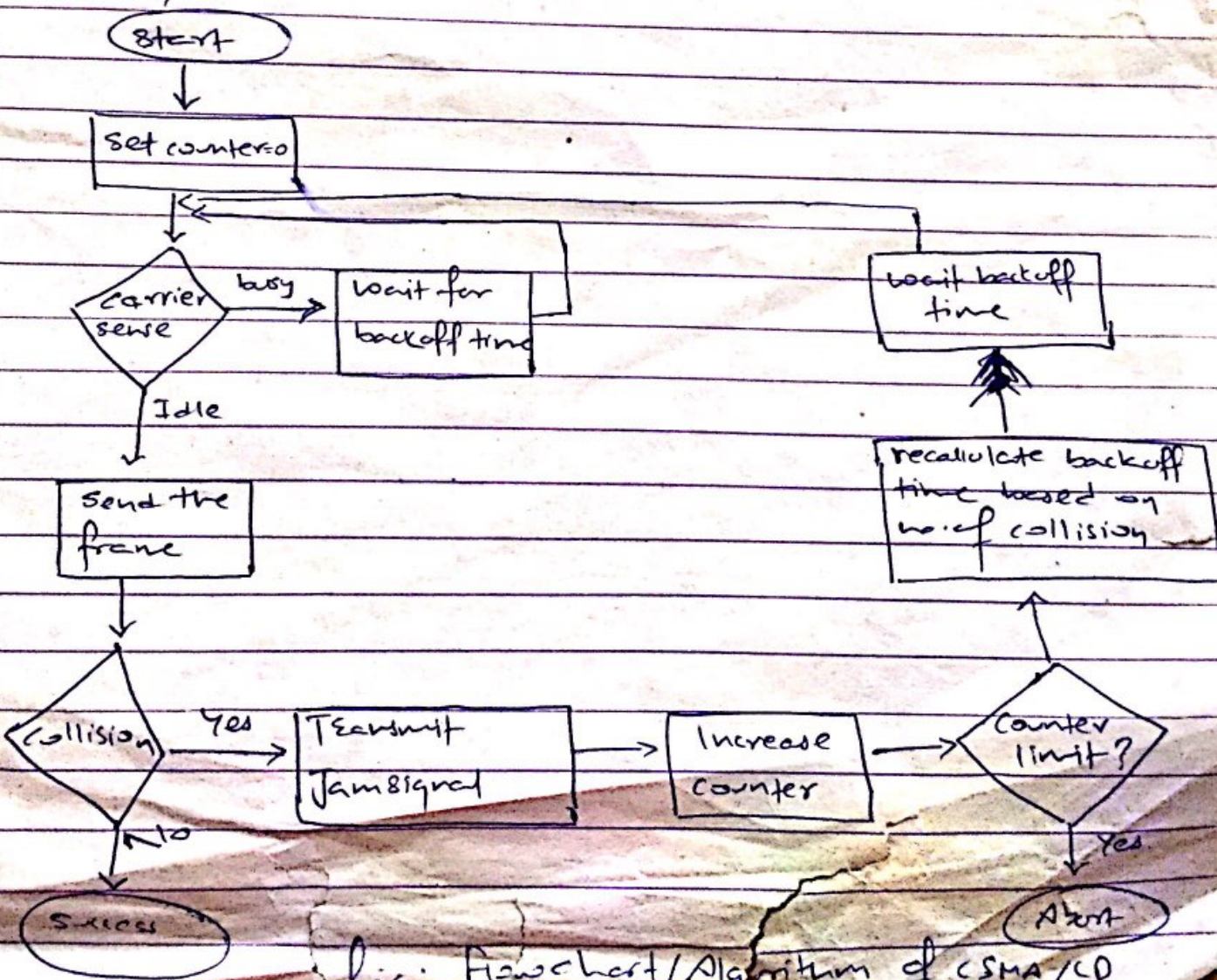


fig: Flowchart/Algorithm of CSMA/CD

when collision occurs the transmitting station releases a jam signal. this will alert other stations to not transmit the data.

- Ethernet is most widely installed local Area Network (LAN) technology. Ethernet is a link layer protocol in TCP/IP stack, describing how network devices can format for transmission to other network devices on the same network segment and how to put that data out on the network connection.
- It touches both layer 1 (the physical) and layer 2 (the data link layer) on the OSI network protocol model.
- Ethernet defines two units of transmission packet and frame.

Fast Ethernet:

- Fast Ethernet is the protocol designed to work upto 100 Mbps. Traditional Ethernet can operate only upto 10Mbps.

GigaBit Ethernet:

It is a protocol that has been designed in order to support the data rates upto 1000 Mbps.

Frame Relay:

Virtual Circuit Switching:

- Virtual circuit switching is a packet switching methodology where a path is established between the sare and the final destination through which all the packets will be routed during a call.
- The path is virtual circuit because to the user the connection appears to be a dedicated physical circuit.
- It is connection oriented.

Advantages of virtual Switching

1) Packets are delivered in order, since they all take the same route.
2) The overhead in packet is smaller since it doesnot need to contain full address.
3) The connection is more reliable.
4) Billing is easier. Since, billing records need only be generated per call and not per packet.

Disadvantages:

1) The switching equipment should be more powerful.
2) Resileience to the loss of trunk is more difficult.

Examples: X.25 and Frame Relay.

Frame Relay:

- Frame Relay is a packet switching methodology that is designed in the late 1980s and developed in 1990s.
- It uses virtual circuits that can be set up for each session or set up permanently.
- Frame Relay is designed for fiber optic cables with a very low bit error rate.
- It is packet-switching telecommunication service designed for cost-efficient data transmission for LANs and WANs
- It has no error recovery and no flow control.
- Whenever a frame Relay switch detects an error in a packet, it just discard the data.

X.25

- X.25 is a packet-switching protocol standard that is developed in 1970's. It is used to carry large amounts of data over public data networks.
- Subscribers are usually connected to this data network with a leased line.
- X.25 uses a virtual connection. A path from source to destination is set up before the data transfer begins.
- An X.25 WAN consists of packet switching exchange nodes as the networking hardware, and leased lines plain old telephone service connections or ISDN connections as physical links.
- At present X.25 protocol has been replaced by less complex protocol, especially the Internet Protocol (I the service is still in use.

ATM

- The ATM data packet is a cell composed of 53 bytes (5 bytes of header and 48 bytes of payload).
- ATM ~~eliminates~~ eliminates the varying delay times associated with different-sized packets.
- ATM can handle real time transmission.
- In ATM, connection between two endpoints is accomplished through transmission paths (TPs), virtual paths (VPs) and virtual circuit (VCs).
- In ATM, a combination of a virtual path identifier (VPI) and virtual circuit identifier identifies a virtual connection.
- The ATM standard defines three layers.
  * Application Adaptation layer
  * ATM layer
  * Physical Layer.

Chapter 9:

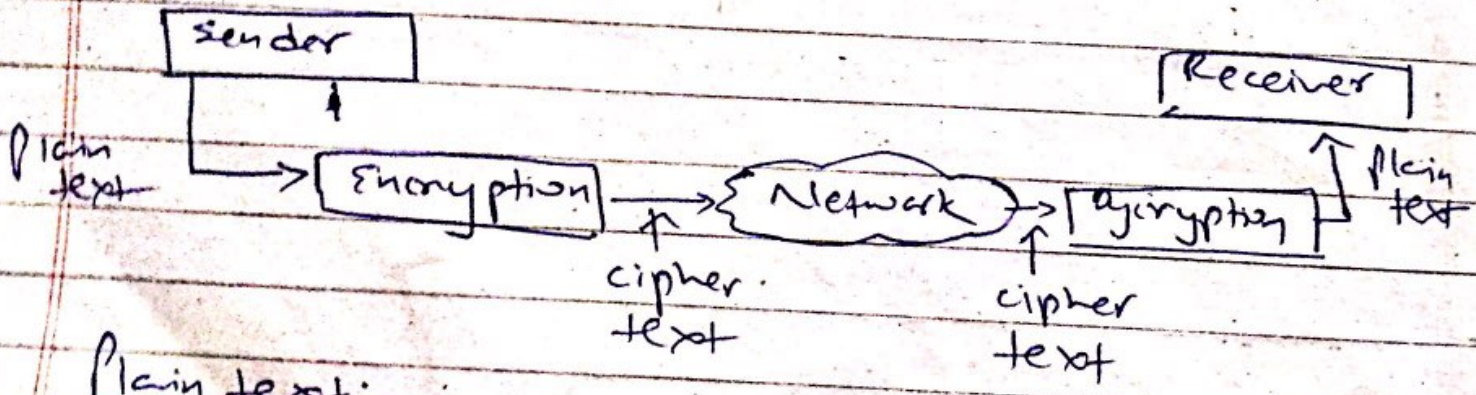
Network Management And Security:

Cryptography:

The study of various ways to disguise messages in order to avoid the interception from an unauthorized interceptor is known as cryptography.

Encipher And Encrypt correspond to the message transformation performed at the sender in order to disguise the message.

Decipher and Decrypt correspond to the inverse transformation performed at the receiver in order to recover the original message back.



Plain text:

The original message produced by the sender

Cipher text:

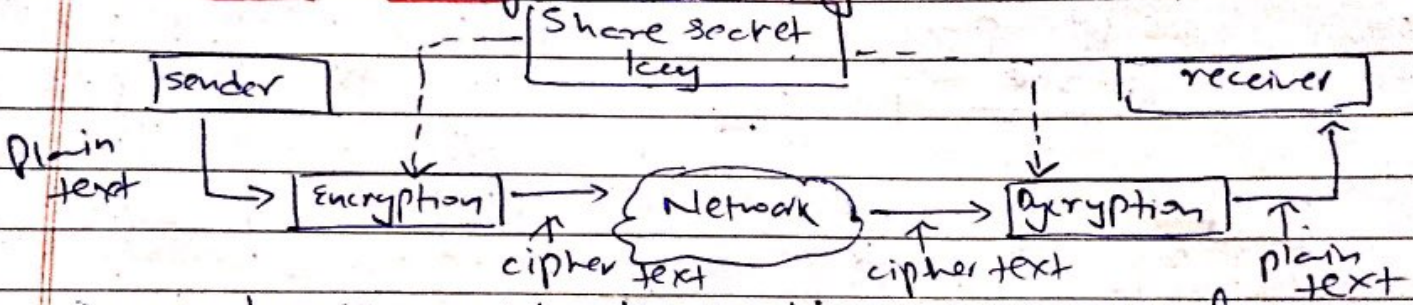
Encryption program converts the plain text

into cipher text which has no meaning.

Dycryption:
Process which is exactly opposite to encryption.

Ciphers:
The encryption and dycryption algorithm together are referred to as ciphers.

Symmetric key Cryptography:
- a.k.a secret key cryptography.

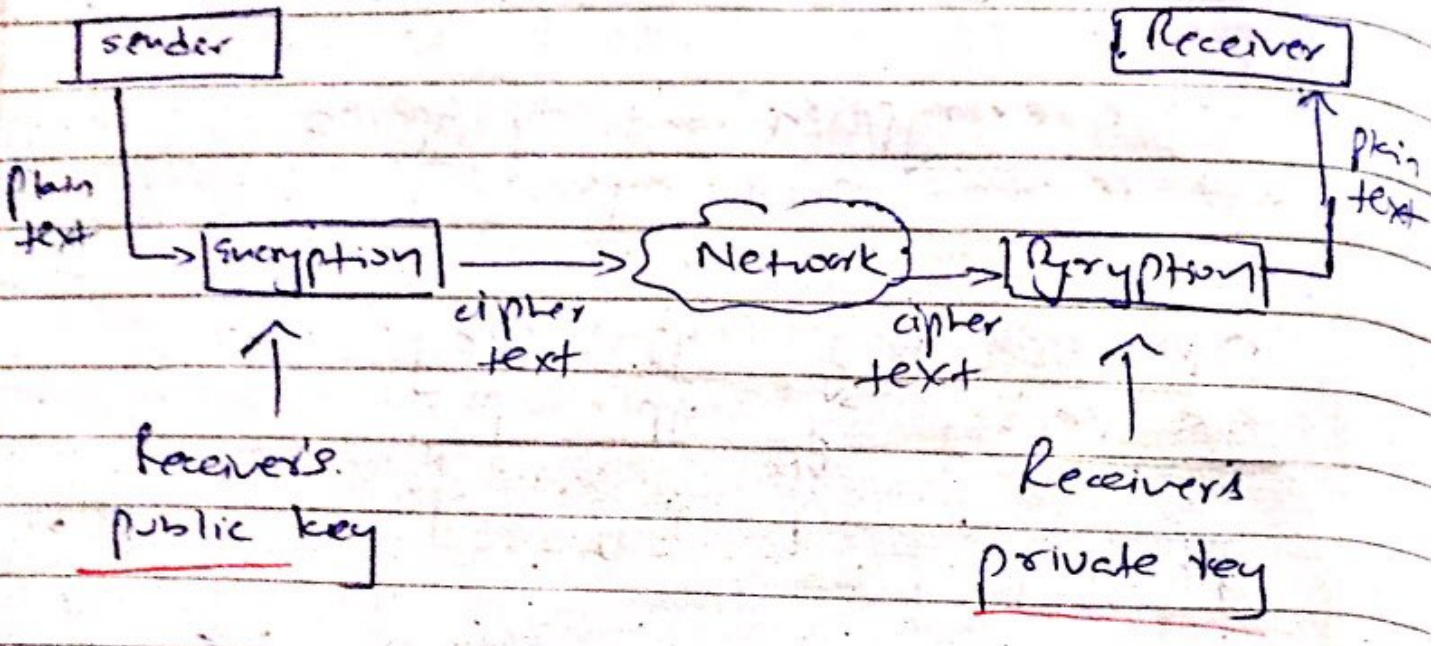


-> Same key is used by the sender and receiver. for encryption and dycryption respectively.

Advantage
- More effective than the Assymetric key cryptography.
- Faster encryption and dycryption.

Drawbacks:
- Sender and receiver both should have a unique Symmetric key. Therefore a large number of key is required when the number of user increases.
- Distribution of keys between two users in different location can be difficult.

Asymmetric key cryptography
- aka. public key cryptography



- public key is known to everyone but private key is known to only the receiver.
- The sender uses the public key to encrypt the message ~~to send the message~~.
- At the receiver, this message is decrypted with the help of receivers private key.
- Private and public key are different

Advantages:
- Number of keys required is largely reduced.

Disadvantages:
- Algorithms used are complex
- long time to calculate cipher text from plain text

RSA Algorithm

- Most widely used public key Algorithm

Steps-1

1. take 2 very large prime numbers A and B. find their product N

$$N = a \times b$$

2. Subtract 1 from both A and B and take the product T

$$T = a(A-1) \times (B-1)$$

3. Choose the public key 'E' such that it has no common factor with T.

4. Obtain the private key 'D' as

$$D = E^{-1} \bmod T$$

5. If 'M' is plain text and 'c' is cipher text then

$$C = M^e \bmod N$$

This gives cipher text

6. At receiver, 'C' is dycrypted to get 'M'.

$$M = C^D \bmod N$$

Key-Exchange protocols

Deffie-Hellman key exchange.

- It is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first publick-key protocols.
- It is also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific power
- Traditionally, secure encrypted communication between two parties, requires that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted carrier.
- used in number of commercial product.

Advantages: * communication can take place through an insecure channel.

* Secret keys are created only when needed
* Exchange requires no pre-existing infrastructures
* Sharing of secret key is safe.

Disadvantages

* no authentication of participants.
* computationally intensive
* vulnerable to replay attacks (more later).

Virtual Private Network:

A VPN extends a private network across a public network, such as the internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private Network.

- It secures the private network as these system use encryption and other security mechanisms to ensure that only authorized users can access the network and the data can't be intercepted.
- A VPN is designed to provide a secure, encrypted tunnel in which to transmit the data between the remote user and the company network.
- The first step to security is usually a firewall.
- There are three main network protocols for use with VPN tunnels.
  1) IPsec
  2) PPTP (Point to Point Tunneling Protocol
  3) L2TP (Layer-2 (two) Tunneling Protocol.
- A VPN service is especially useful when accessing public Wi-Fi hotspots because the public wireless service might not be secure.
- It also provides consumers with uncensored internet access and can help prevent data theft and unblock websites.
- Companies and organizations will typically use a VPN to communicate confidentially over a public network and to send voice, video or data.

- It is also useful to share data in private manner between remote workers and organizations with global offices.
- Type :- Virtual private dial-up Network (VPDN)
  - Site-to-Site VPN.

. IPSec :

-> IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication.

-> IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private network.

-> A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

-> IPsec provides two choices of security service:
  i) Authentication Header (AH):
     It essentially allows authentication of the sender of data.

ii) Encapsulating Security Payload (ESP):
It supports both authentication of the sender and encryption of a data as well.

- The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header.

- IPsec can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

- In transport mode, only the payload of the IP packet is usually encrypted or authenticated.
- In tunnel mode, the entire IP packet is encrypted and authenticated.

Firewall And its types:
- A firewall is a hardware or software system that prevents unauthorized access to or from a network.
- It can be implemented in both hardware and software or both.
- It was first term as 'firewall' to describe the process of filtering out unwanted network traffic.
- Firewalls are frequently used to prevent unauthorized internet users from accessing private networks connected to the internet.

- All the data entering and leaving the Intranet pass through the firewall, which examines each packet and block those that do not meet the specified security criteria.
- They prevent interactive logins from the outside world.
- This helps prevent hackers from logging into machines on your network.

Types:

1) Packet-filtering firewalls: (Network layer)
operate at the router and compare each packet received to a set of established criteria (such as allowed IP addresses, packet type, port number) etc

~~2) Circuit-level gateways:~~
~~monitor the TCP handshaking going on between the local and remote hosts.~~

2) Application layer firewalls:
They are hosts that run on proxy servers, which permit no traffic directly between network, and they perform elaborate logging and examination of traffic passing through them.

3) Proxy firewalls:
- offer more security than other types of firewalls, but at the expense of speed and functionality, as they can limit which applications the network

supports.

Network Management:

- It is defined as monitoring, testing, configuring, and troubleshooting network components to meet a set of requirements defined by an organization. These requirements include the smooth, efficient operation of the network that provides the predefined quality of services to users.
- To accomplish a task a network manager system uses hardware, software and humans.

Functions:

1) configuration Management
2) fault management
3) Performance management
4) Security "
5) Accounting "

Chapter: 7

Congestion Control & quality of Service

- When too many packets are present in a part of a subnet, the performance degrades. This situation is known as congestion.
- This is an important issue in a packet switching network
- occurs when rate of transmission is fast.
- It is not possible to completely avoid the congestion but it is necessary to control it.

Causes of congestion:

i) In a router, stream of packets starts coming on three or four input lines which all need the same output line.
ii) Slow links
iii) Slow processors.

Congestion control

- Open loop soln
- Closed loop soln

Open loop solutions try to solve the problems by excellent design to prevent the congestion from happening. It uses the concepts like deciding when to accept the new packets, when to discard the packets, which packets

to be discarded etc.

Closed loop soln try to solve the problem by excellent design to prevent the congestion from happening.

Closed loop soln uses some kind of feedback. It is based on following steps.

① Detect the congestion and locate it
② Transfer the info about congestion to places
③ Adjust the system operations to correct the congestion.

Open	closed
→ Doesn't need feedback system	→ Need feedback system
→ faster	→ slower (by the time the source gets feedback and reacts to it, many data is lost)

1.2) Traffic Shaping:

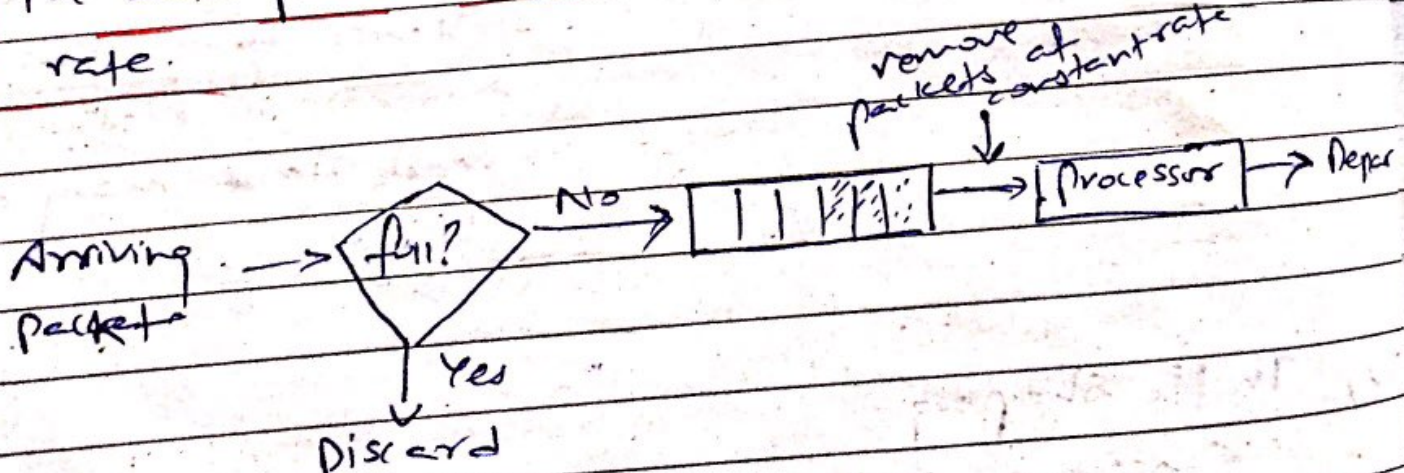
- Congestion occurs due to bursty nature of the traffic
- if the traffic has a uniform data rate then congestion could be less.
- Traffic shaping is an open loop control where traffic shaping regulates the average rate of the data transmission

- Two traffic shaping techniques :

1) Leaky Bucket Algorithm

Leaky Bucket is a bucket with a hole at Bottom. The flow of the water from the bucket is of a constant rate independent of water entering the bucket. If the bucket is full, any additional water entering in the bucket is thrown out.

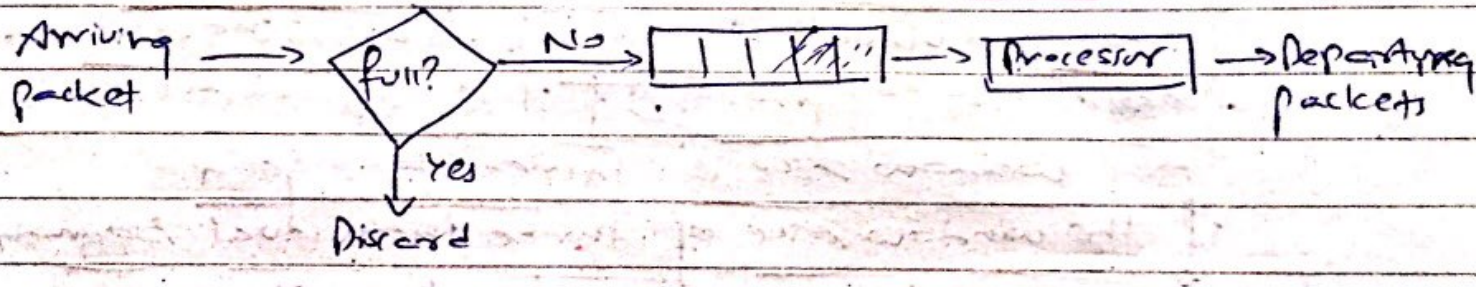
- Same mechanism is used in network.
- Every host in a network has buffer with finite queue length.
- Packets which are put in the buffer after the buffer is full are thrown away...
- The data passes through the buffer at the same rate.



ii) Token Bucket:

- This is useful when large burst of traffic arrives.
- Similar to leaky Bucket but allows varying output rates
- A token bucket is used to manage the queue regulator that controls the rate of packet flow into the network.
- A token generator constantly generates token at the rate of 'R' tokens per second and places them into a token bucket with a depth of D tokens.
- If the bucket is full, newly generated token are discarded.

one token is removed an discarded per cell transmitted



TCP congestion control:

Here, we assume that congestion occurs due to two reasons.

i) Buffer capacity of receiver
ii) internal carrying capacity of the network.

To deal with these two problem sender maintains two windows:

① The window to adjust the transmission rate to match the capacity of receiver buffer.
② The window to adjust the network capacity.
③ The number of bytes that may be send by the sender is the minimum of the two windows.

A) Slow-start Algorithm:
After establishing a connection, the sender initalize the congestion window to the size of one individual segment, it they sends the segment. If the segment is acknowledged they it increases the size of window to two individual segements. The sender they sends two segments. If it is again acknowledged the window size is increased again.
If the window size of three individual segment is not acknowledged they the window size is decreased to two segment size and rest of the communication is done in the window of two segment size.

B) Internet Congestion Control Algorithm

Chapter 6

Transport layer and Protocol

Services of Transport layer:

1. Connection oriented communication
2. Same order delivery of packets
3. Reliability (packets may be lost but error is detected and retransmitted)
4. Flow control
5. Congestion Avoidence
6. Multiplexing.

Multiplexing & Demultiplexing:

Multiplexing is sending multiple packets of information on a carrier at the same time in the form of a single complex signal.

Demultiplexing is recovering the separate packets from the signal, complex signal at the receiving end.

In analog transmission signals are commonly multiplexed using frequency division multiplexing (FDM) in which the carrier bandwidth is divided into sub channels of different frequency widths, each carrying a signal at the same time in parallel.

In digital transmission signals are commonly multiplexed using time division multiplexing (TDM) in which the multiple signals are carried over the same channel in alternating time slots.

Imp

Port is a 16-bit number used to identify each address and protocol in the internet. (a.k.a port number).

Specific port number are often used to identify specific services.
TCP & UDP uses ports.
25 is used for simple mail transfer protocol (SMTP)
80 is used for HTTP.

Ans

UDP	TCP
- Simple, high speed, low functionality protocol.	- Full featured, high functionality protocol.
- Connectionless data transmission.	- Connection-oriented data transmission.
- Message based data is sent.	- Stream-based data is sent.
- Unreliable delivery of message. : no acknowledgement.	- Reliable delivery of message, all data is acknowledged.
- No retransmission of lost data.	- Lost data is retransmitted automatically.
- No flow control and congestion control	- Flow control using sliding window and congestion avoidence algorithm.
- very low overhead.	- Higher overhead than UDP
- very high transmission speed.	- High, but not as high as UDP

UDP

- Suitable for small to moderate amount of data.
- Applications where data delivery speed matters more than completeness.

TCP

- Suitable for small to large amount of data.
- Applications where data delivery completeness matters more than speed.

imp

User Datagram Protocol

UDP header format

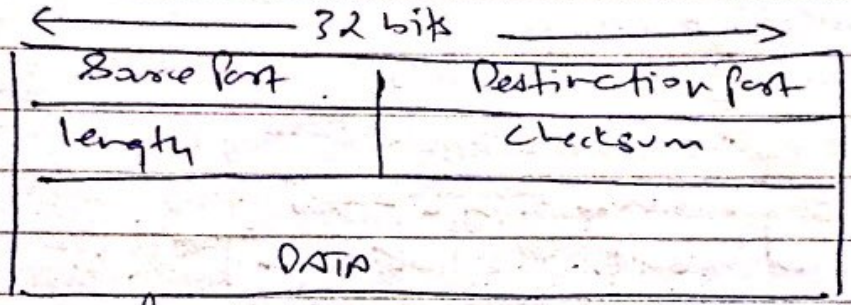


fig: UDP datagram including header and data segment.

UDP header consists of 4 fields, each of which is 2 bytes (16 bits).

① Source Port number:

It indicates the port of the sending process and may be assumed to be the port of reply to if needed. If not used then it will be zero.

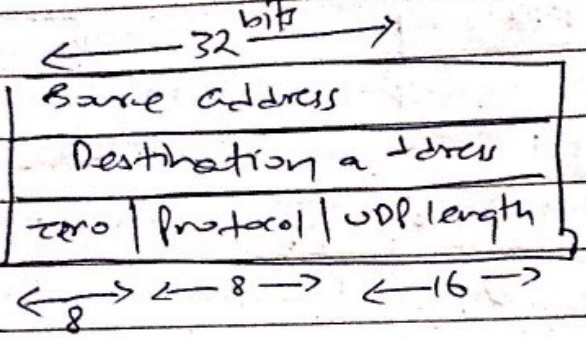
② Destination Port number:

- It indicates the receivers port number and is compulsory.

③ length:
This is the size in bytes of the UDP packet including the header and data.

④ UDP checksum:
Used for error-checking of the header and data.

UDP pseudo header



- used to verify that the UDP packet has reached its correct destination.

Socket Programming:
Socket are the combination of IP address plus corresponding TCP/UDP port number.

Two forms of sockets:

① Active Socket:
The socket that is connected to a remote active socket via an open data connection

② Passive Socket:

The socket that is not connected, but rather awaits an incoming connection.

- Socket is not a port.
- A port can have multiple active sockets and a passive socket.

Socket() - create a socket
bind() - Associate a socket with a network address
connect() - Connect a socket to a remote network address.
listen() - wait for incoming connection attempts
accept() - accept incoming connection attempts
close() - connection is terminated.

3 types of Socket:

① The stream socket: for connection oriented protocol such as TCP

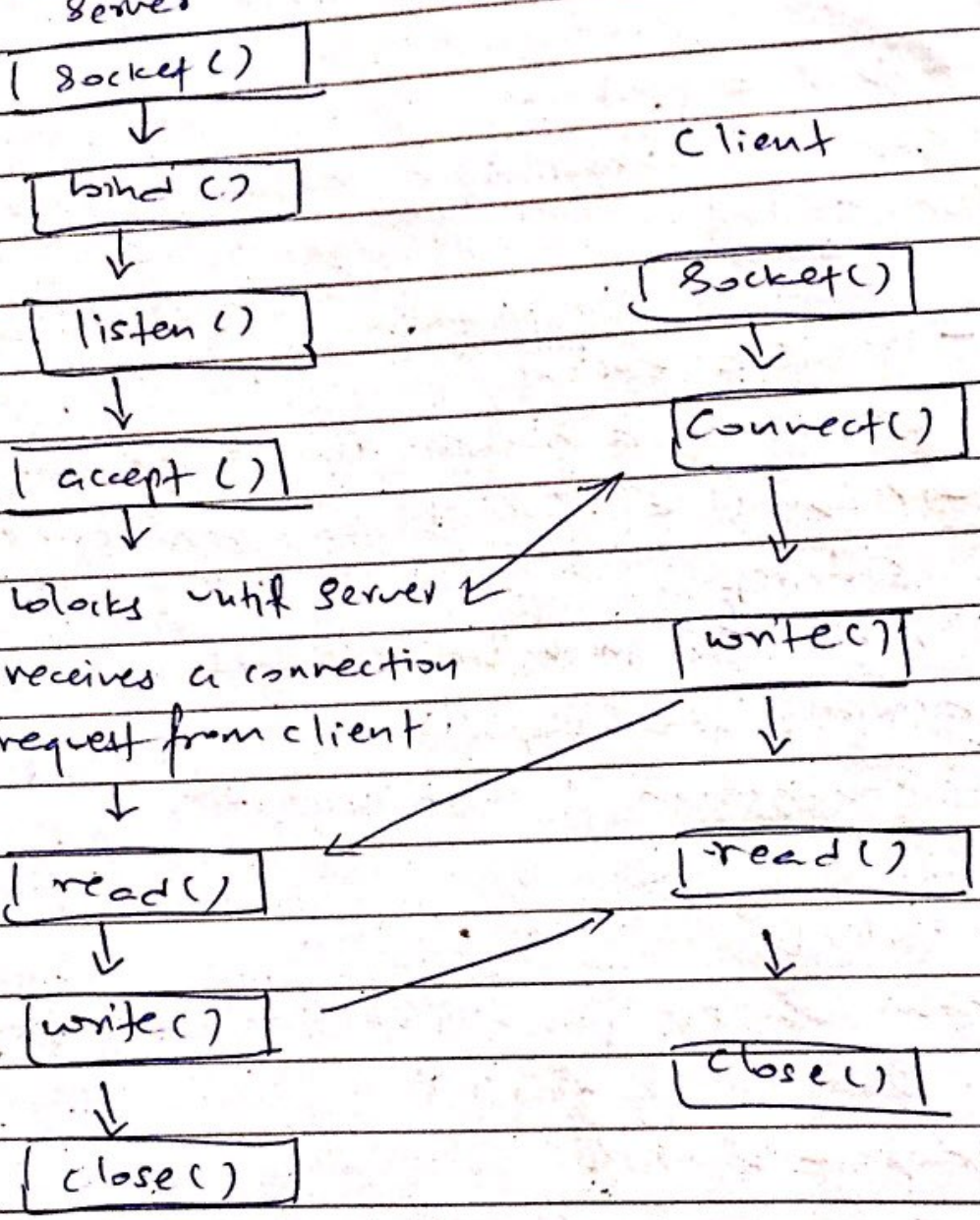
② The datagram socket:

for connection less protocol such as UDP.

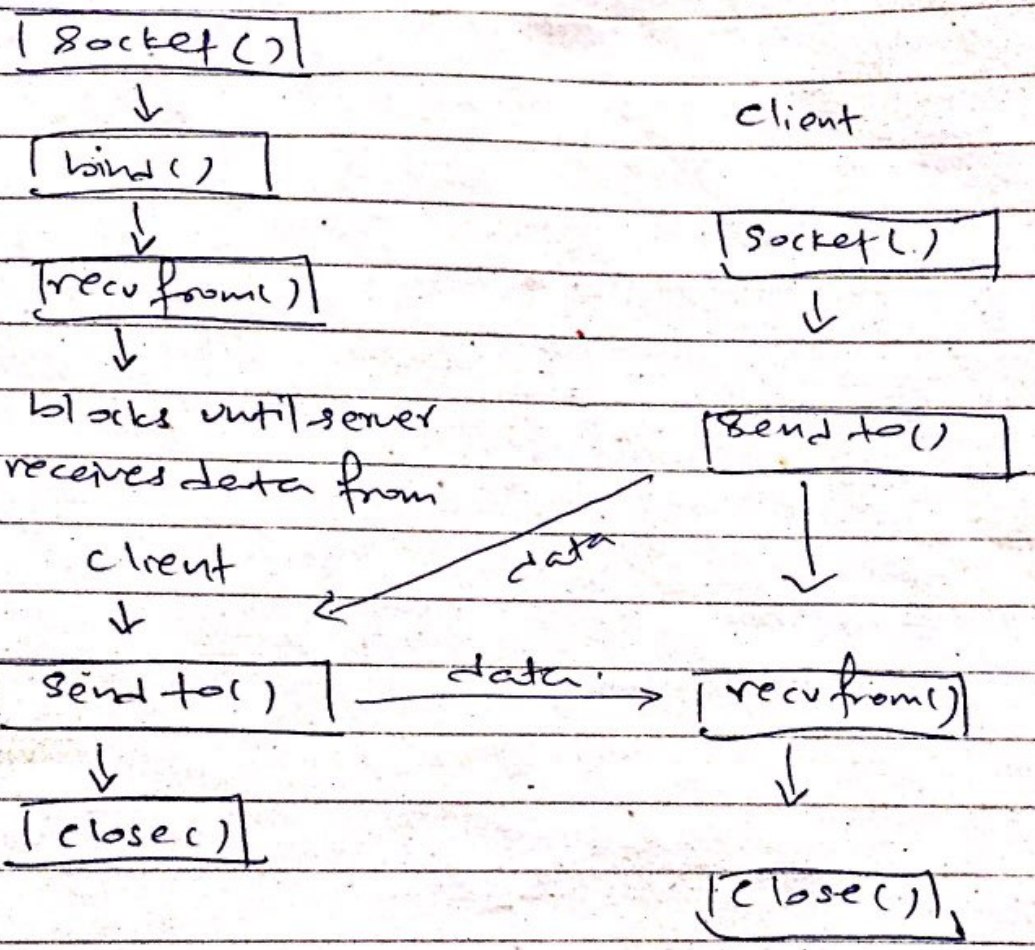
③ Raw Socket:

for other protocols that do not use either stream or datagram socket.

TCP Socket calls.



UDP Socket call



SMPT

- Email is supported by TCP/IP protocol SMPT
- It provides system for sending message to other comp.
provide a mail exchange between users

SMPT supports:

i) Sending a message to one or more recepients.
ii) Sending message that includes texts, video or graphics
iii) Sending message to users on the network outside the internet (viber or call).

Mail Transfer:

- Email is submitted by mail client to a mail server using SMPTP on port 25
- Mail Server delivers the mail to its mail transfer agent
- SMPTP is used to transfer the message over the internet internally with each host transferring mail to next host (done by MTA)
- The boundy MTA has to locate the target host.
- It uses the domain name system DNS to lookup for receipents domain. (i.e the part of the address on the right of '@')
- Than the MTA can know the IP address of the receipient
- The mail now reaches to mail delivery Agent (MDA)
- MDA ~~Send message~~ may deliver message directly to storage or forward them over a network using SMTP.
- One the mail is delivered to the local mail server the mail is stored for [illegible] mail clients.

- Mail is retrieved by Mail client using either Internet Message Access Protocol (IMAP) or Post office protocol (POP)

(change aybhane thapauma, same topology ma sajilo)

non-adaptive routing

Static → Shortest k ko adhar ma
- distance
- kati ota hub bata pass garne

→ Flooding → najik ko router sabaima pathaune

→ flowbased → bg bixa bhane arko bata pathaunche jati lamo bhayeni; topology/pad condition paile define garne

~~dynamic~~ dynamic - change aka tha hunxa bigger topology lai use hunxa

ADaptive routing → distance vector / link state

Distance Vector Routing:

→ uses hop count as metric
→ vector table update garxa
→ info of source, path and destination
→ destination sma ko overall path tha huna, neighbouring matra tha hunxa. (koi bigrexa bhane tesko neighbour lai matra tha huxa
→ jun path satso parxa (metric) tyo choose garxa.

Computer Networks

1) Introduction to Computer Networks

- A computer is a telecommunication network which allows computers to exchange data with each other using a data link
- The best known computer network is Internet.
- Computer network supports a large number of applications and services such as access to world wide web (www) digital audio, digital video, shared use of application and storage services etc.

Merits And Demerits of Computer Network

Merits:

-> communication is made efficient and easy via various means email, instant messaging, chat rooms video telephone calls and video conferencing.
-> used for shared storage.
-> Allows sharing of files, data and other type of information.
-> share resources such as printers in the network.
-> Saves money and time.

Demerits:

-> computer crackers can deploy computer viruses or computer worms on devices connected to the network
-> Data being transferred over the computer network may be accessed by some random user.
-> A network may also mean loss of privacy as some especially your boss, with more rights over the network may be in a position to read your private email.

1.2 Network Models:

1.2.1 Local Area Network (LAN)

- It is a network which is designed to operate over a small physical area such as an office, factory or a group of buildings
- LANs are easy to design and troubleshoot.
- LAN may use various topologies such as Bus, Ring, Star, Tree etc
- LAN is usually privately owned.
- LAN usually use only one type of transmission medium.
- LAN is capable of operation at hundreds of Mbits/sec

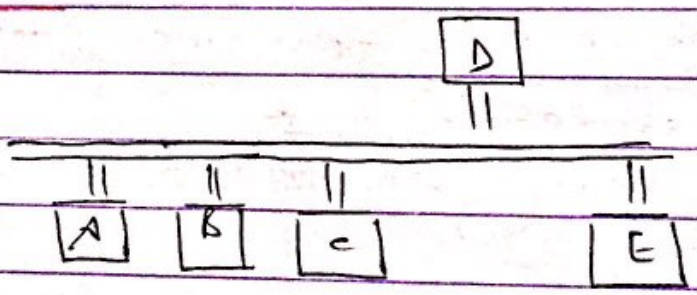


fig: Illustration of LAN in Bus topology

Campus Area Network (CAN) → part of LAN
Country Area Network ((AN*) → part of WAN.
Geographical Area Network (GAN) → part of MAN

Metropolitan Area Network (MAN)

- Bigger version of LAN usually extended over an entire city.
- It can be single network such as a cable TV network, or it may be a means of connecting a number of LANs into a large network.
- MAN may be owned and operated by a private company or it may be a service provided by a public company.

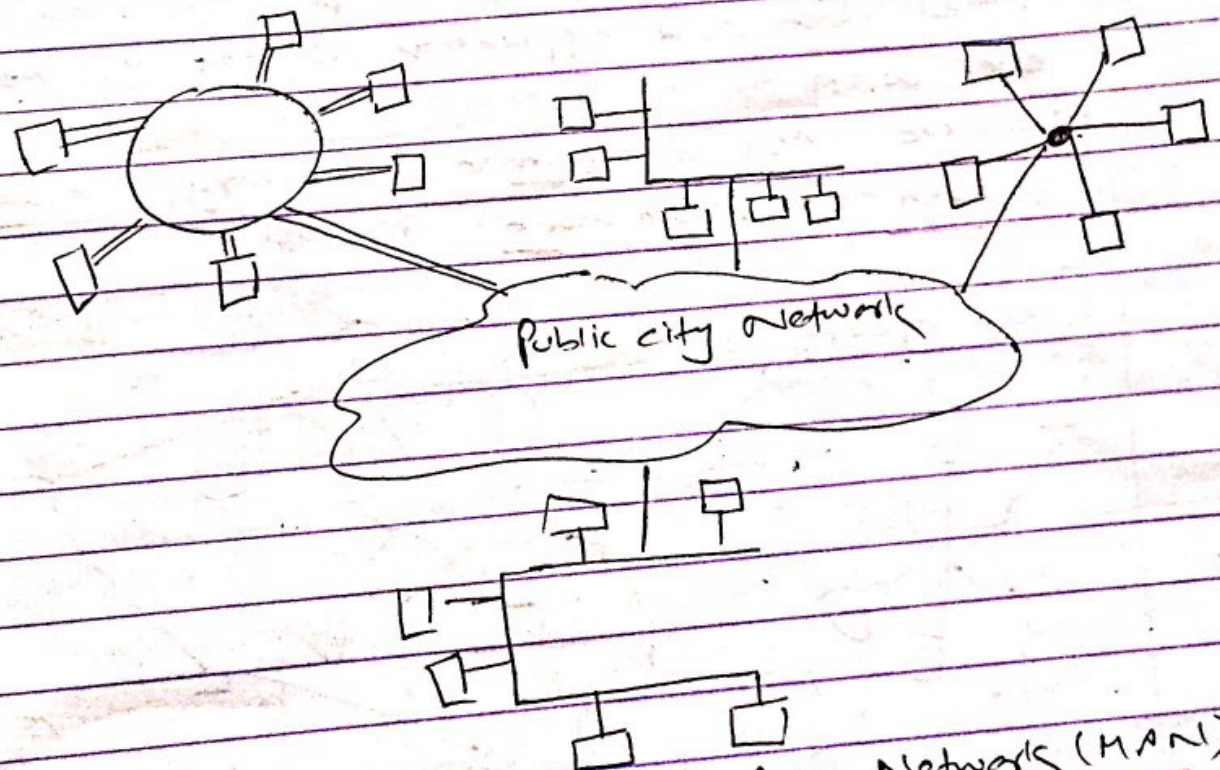


fig: Metropolitan Area Network (MAN)

Wide Area Network (WAN)

- It is a network which is designed to connect computers which are widely separated such that LAN and MAN cannot connect them.
- Leased telephone line or satellite links are used to establish the connection.
- Because of large distances involved in the wide area networks, the propagation delays and variable signal travel times are major problems. So, time critical data and application is not preferred over WAN.
- The area may compromise a country, a continent or even the whole world.

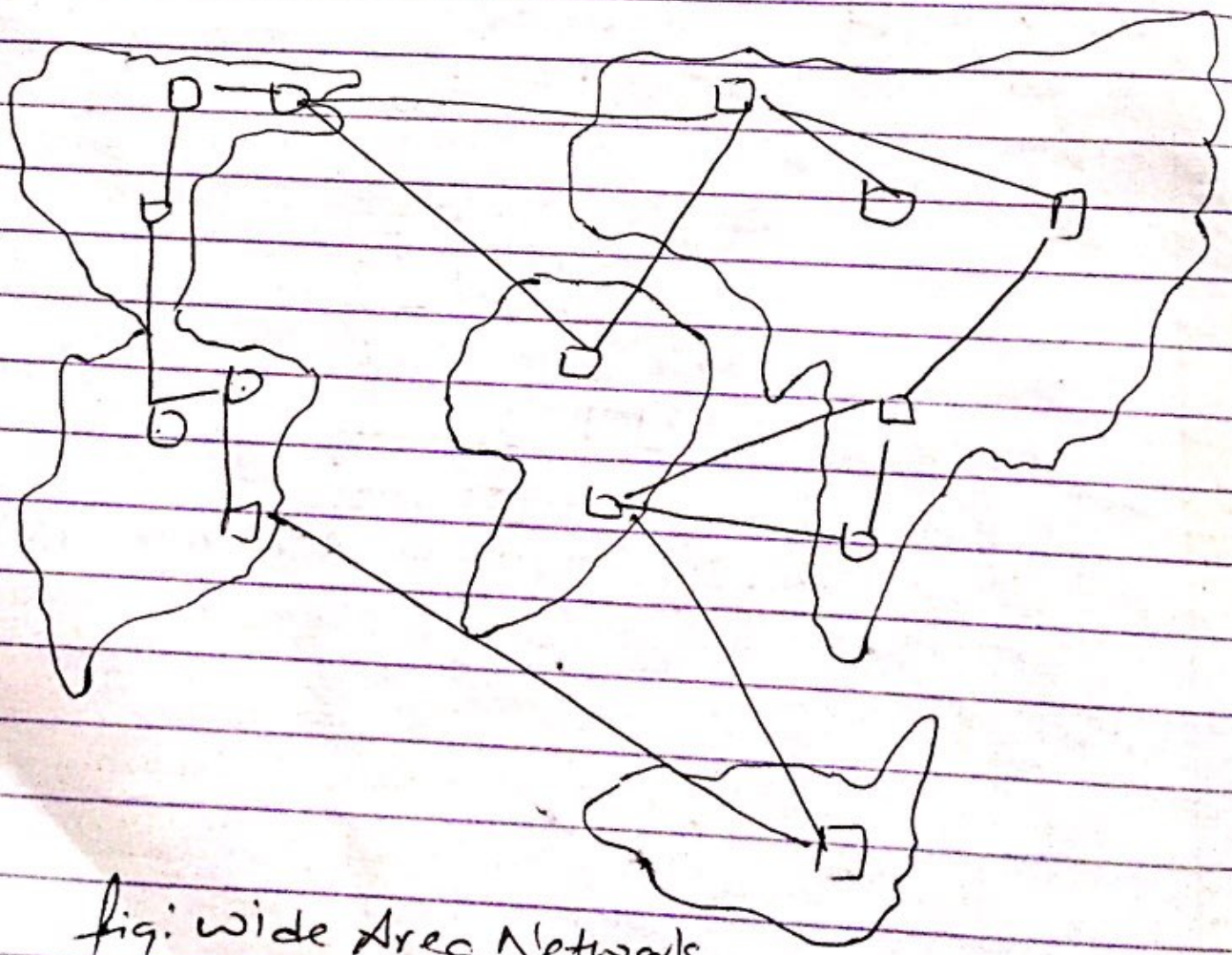


fig: Wide Area Network

Topological Models

Star topology

- All the cables run from the computers to a central location where they are connected by a device called a hub.
- End points are directly reachable from central location
- Each computer on a star network communicates with a central hub that resends the message either to all the computers (in a broadcast star network) or only to the destination computer (in switched star network)
- Several types of cable can be used to implement a star network

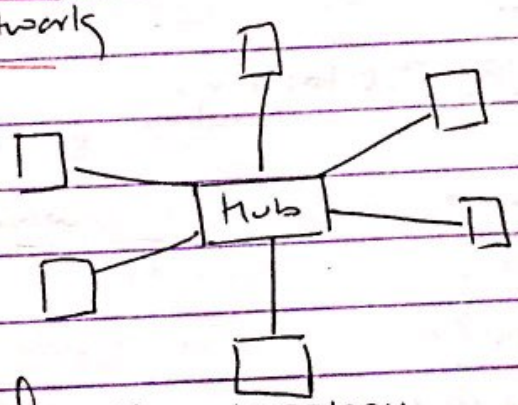


fig: Star topology

Advantage:

→ Easy to increase no. of users

→ Star network can be expanded by placing another star hub as shown in figure

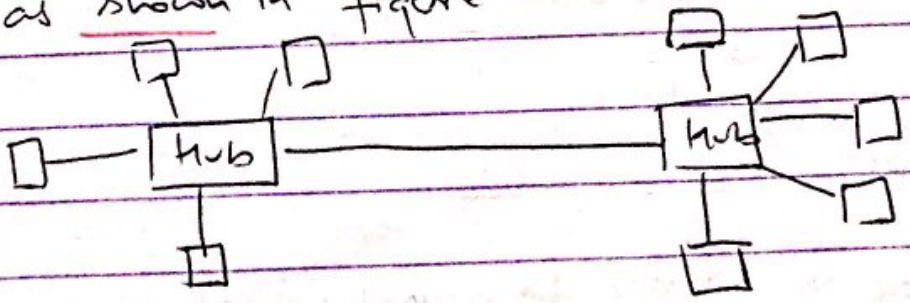


fig: Hybrid Star Network

Disadvantages:

-> If the central hub fails, the whole network fails to operate.

-> Cabling cost is more.

Bus topology:

In bus topology all the computers are connected to a single cable as shown in figure below

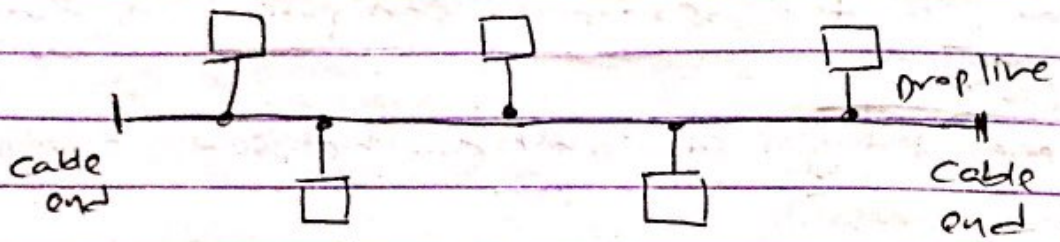


fig: Bus topology

- Used in simple or temporary network
- Cheap.
- Usually no amplifier is used.
- When one computer sends a signal up to the cable, all the computers on the network receive the information, but the one with the address that matches the one encoded in the message accepts the information while all the others reject the message.
- only one computer can send a message at a time.
- Require proper termination at both ends of the cable.

Advantages:

- Easy to understand, install and use for small network
- Cabeling cost is less.
- Easy to expand.
- Signals can be boosted by using repeaters during expansion.

Disadvantages:

- Heavy network traffic can slow down the communication speed since only one computer can send a data at one time
- If the main cable is broken the entire network will fail to communicate

Distributed Bus topology:

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two end points that are created by adding branches to the main section of the transmission media as shown in figure.

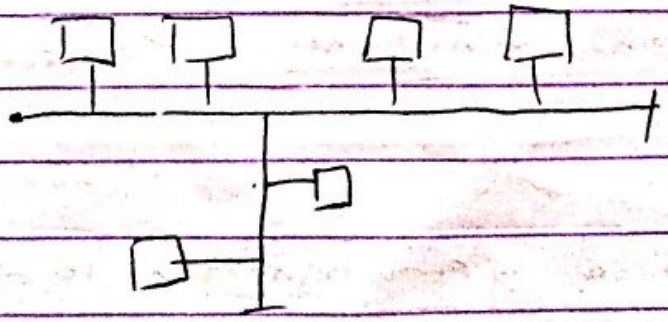
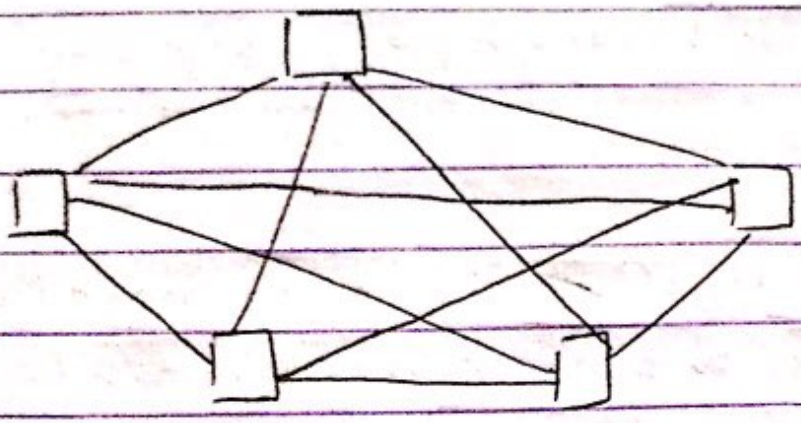


fig: Distributed Bus Topology.

Mesh Topology

Every device has a dedicated point-to-point link to every other device as shown in figure



A fully connected mesh network therefore has $n(n-1)/2$ physical channels to link n devices.
Every device must have $n-1$ input/output ports

Advantages:

- Eliminate traffic problem
- failure of single computer does not bring down the entire network.
- Provide security and privacy because every message sent travels along a dedicated line.
- point-to-point links make fault diagnose easy.

Drawbacks:

- Installation & reconfiguration is difficult.
- Cabling cost is high.

Tree Topology:

- Variation of star topology
- As in a star, nodes in a tree are linked to a central hub that controls the traffic of the network however, not every computer plugs into the central hub, Majority of them are connected to a secondary hub which in turn is connected to the central hub.

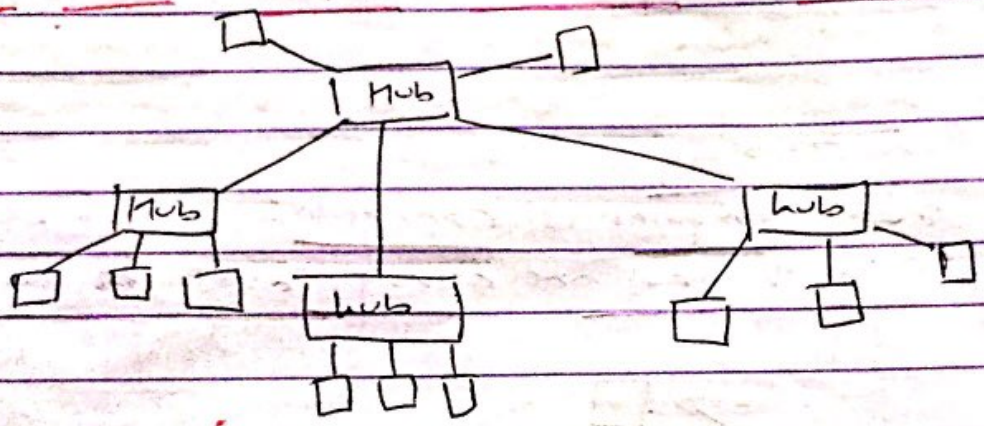


fig: Tree Topology

- Repeaters are used to amplify signal and increase the distance a signal can travel.

Advantages:

- Allows more device to be connected to the main hub
- Allows to isolate and priorities communication from different computers.
- Suitable for multistoried company.

Drawbacks:

- If the central hub fails, the system breaks down
- Cabling cost is more.

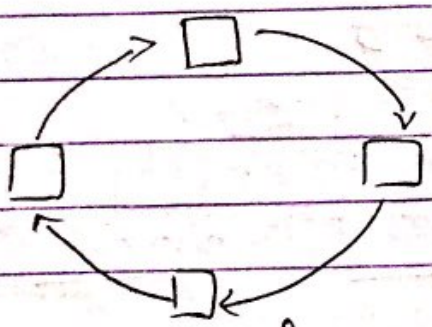
Page:
Date:

Hybrid Topology

- It combines two or more topologies in such a way that the resulting network doesn't exhibit one of the standard topologies. (bus, star, ring etc)
- Example: Tree Topology is a hybrid topology. ~~in which~~ Snowflake topology is a star network of star networks.

Ring Topology :

- Each computer is connected to the next computer, with the last one connected to the first one



- Used in high performance network where large bandwidth is essential.
- The message flows around the ring in one direction.
- Tokens are used to keep track of message passing

Advantages:

- Every computer is given equal access to the token.
- When user increase, the network maybe slow but won't fail.

Disadvantages:

- If a link breaks or a computer fails the entire network will be disabled.
- Difficult to troubleshoot.
- Adding or removing the computers disturbs the network activity.

~~Client/Server Model~~

	LAN	WAN
1	The LAN is owned by a person, college, factory etc It is privately owned network.	1, WAN can be private or it can be public leased type network.
2	Designed to operate over a small physical area.	2, Designed to operate over a large distance such as spanning states, countries etc
3,	LAN is easy to design and maintain.	3 WAN is not so easy to design and maintain.
4,	Communication medium used for interconnection is a simple co-axial cable.	4, Communication medium used can be PSTN or satellite links due to longer distance.
5,	No propagation delay.	5) Propagation delay occurs.
6,	Preferred for time critical applications.	6, Not preferred for time critical applications.
7	It can operate on very high data rates.	7) It operates on low data rates.

Page:
Date:

Client / Server Network:

- In client server network each computer is assigned a defined role ie either client or server
- The client makes a request and the server respond to the request.
- The client have access to resource available on file server.
- client/server model provides convinient way to interconnect program that are distributed across different stations.

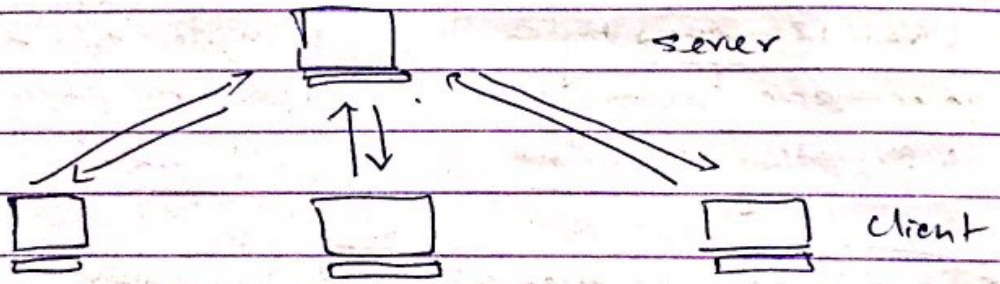


fig: client/ Server model

Advantage

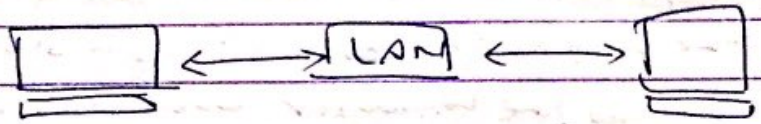
- centralized
- Scalability (add/remove)
- flexibility (change)
- Accessibility

Disadvantages

- Initial cost is high
- Management cost is high
- When Sever goes down entire network goes down (dependency)

Peer-to-peer Network.

- In peer to peer network all the computers are considered equal.
- All the computer have equal ability to use resources available in the Network
- It is designed for small to medium LAN



Advantages

- Less initial expense
- No need of dedicated Server

Disadvantages

- Decentralized (no central repository for files and applications)
- Does not provide security available in client/server

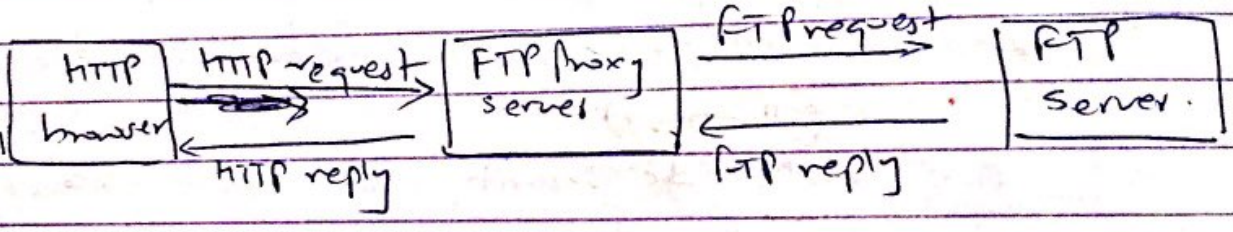
Active Network Model

It is a network model in which the nodes are programmed to perform custom operations on the message that pass through the node.

This approach is specially important in mobile network.

3) Anonymous proxy server:
- Secure the user's personal information by hiding the IP address.

Proxy Server:
- All servers cannot speak HTTP. Some of them may speak FTP and other protocols.
- A large information is available on FTP and other servers, hence, it must be made available to web users.
- One solution can be to have a browser which can use the http as well as FTP and other protocols. But this makes the browser unnecessarily large.
- Other solution is to use 'proxy server'. Proxy server can be a program running on the same machine or can be a free standing machine.
- Proxy server is basically a gateway which speaks http to the browser but FTP and other protocols to the server.



- Proxy server may have the feature of caching.
- A caching proxy server collects and stores all the pages which pass through it
- Proxy server can also be ~~used~~ put inside a ~~firewall~~

Types:

i) ~~Transparent proxies: Also known as~~ forced proxy ~~involves a combination of proxy server with NAT (server that sit between~~

ii) Reverse proxies: handles the request on behalf of the main web server

Transparent proxy: aka forced proxy which sits between your computer and the internet and redirects your request and responses without modifying them.

IPV4	IPV6
- There are only 2^{32} possible ways to represent the address	-> There are 2^{128} possible ways to represent the address.
- Address is written by dotted decimal notation. eg: 121.82.8.12	-> Address is written in hexadecimal and consists of 8 groups containing 4 hexadecimal digits. eg: FABC:ACAA:7834:2222:FACB:AB58:5432:9567
-> IPV4 header can be 20 bytes to 60 bytes in length.	-> IPV6 header can be is always 40 bytes in length.
- IPV4 header has checksum	-> IPV6 header don't have checksum
- less secure	-> more secure
- Must be configured either manually or through DHCP.	-> doesn't require manual configuration or DHCP

IP Address:

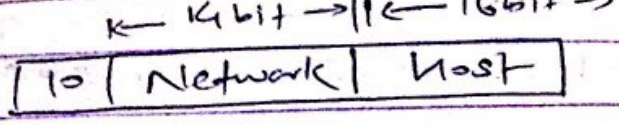
- Every host and router on the internet has a unique address known as IP address.
- 32 bit long.

(i) Class A address: 1 ← 8bit → | 1 ← 24 bit →

0	Network	host

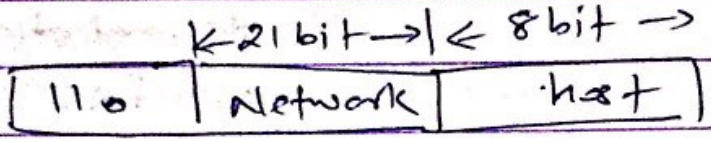
- host number range: 0.0.0.0 to 127.255.255.255

(2) Class (B) address



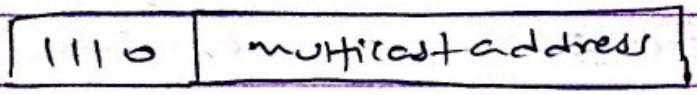
Range: 128.0.0.0 to 191.255.255.255

(3) class c address

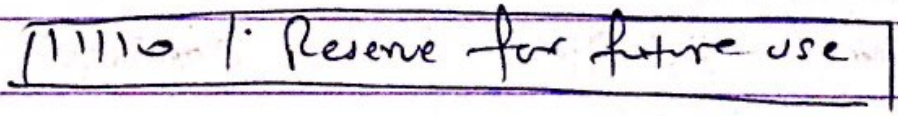


range: 192.0.0.0 to 223.255.255.255

(4) class D address:



(5) Class E address



classful Routing Protocol	classless Routing Protocol
- Do not carry subnet mask information within the routing updates.	- carry subnet masks info within the routing updates
- Exchange routing updates at the regular time intervals.	- Exchange routing tables only when the change occurs in the network topology
- use periodic updates	- use triggered updates
- Do not use hello message	- Use hello message to check the status of neighbours routers.
- consume MR network bandwidth.	- consume less network bandwidth
~~- Do not support CIDR~~	
- Address have three parts: network, subnet and host.	- Address have two parts: subnet or prefix and host.
- Does not support VLSM	- Support VLSM.
- Discontiguous subnets are not visible to each other.	- Discontiguous subnets are visible to each other.
- Example: RIP	- Example: IS-IS

HTTP

- System for transmitting and receiving information over internet.

HTTPS

- HTTPS need arose to address exchange of confidential information over insecure internet.
- Secure HTTP (HTTPS) is used for accessing or posting web server information.

HTTP	HTTPS
- HTTP URL begins with "http://"	- HTTPS URLs begin with "https://"
- It uses port 80 by default	- It uses port 443 by default
- It is unsecured (man-in-the-middle) attack.	- It is more secured.
- used in Blogs, Entertainment and articles	- Used for financial and other confidential information.
- SSL certificates not used for communication (Secure Socket layer)	- uses SSL certificates for communication
- invented by Sir. Timothy doh.n.	- Netscape corporation invented.
- Data not encrypted.	- Data is encrypted.
- faster than HTTPS.	- HTTPS is slower than HTTP
- No, encryption, computational overhead.	- Add computational overhead

Existing Network: 192.168.1.0/24

default subnet mask: 11111111.11111111.11111111.00000000

Total Number of subnets to be designed = 3

So, number of bits required to design 3 subnet = 2

So Subnet Mask for this network will be

11111111.11111111.11111111.11000000

= 255.255.255.192

Host per Network = $2^{32-26} - 2 = 62$

Block size = 256 - 192 = 64

Subnet	Subnet Address	1st Host add	last host add	Broadcast address
1	192.168.1.0	192.168.1.1	192.168.1.20	192.168.1.63
2	192.168.1.64	192.168.1.65	192.168.1.88	192.168.1.127
3	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.191

1st Subnet Address - sweet ko deko

2nd bhane - black sne add garne

1st host add - Subnet + 1

Broadcast - take 2nd of subnet and subtract 1

last Host - Normally, Broadcast - 1

but no. of computer dekha bhane 1st host add ma jodne and sab 1.