

DCEN

Data Communication &
Computer Network

Syllabus

Unit-1: Networks & Protocol

✓ 1.1 Data Communication

✓ 1.2 Networks

✓ 1.3 Protocol & Architecture, Standards,
OSI, TCP/IP

Unit-2: Data Transmission & Media

✓ 2.1 Data Transmission Concepts & Terminology

✓ 2.2 Analog & Digital Data Transmission

✓ 2.3 Transmission impairments, Channel Capacity

✓ 2.4 Transmission Media, Guided Transmission, Wireless Transmission

Unit-3: Data Encoding

✓ 3.1 Data Encoding

✓ 3.2 Digital Data to digital signals

✓ 3.3 Digital data to analog signals

✓ 3.4 Analog data to digital signals

✓ 3.5 Analog data to analog signals

Unit-4: Data Communication & Data Link Control

✓ 4.1 Asynchronous & Synchronous Transmission

✓ 4.2 Error Detection

✓ 4.3 Line Configuration

✓ 4.4 Flow Control

✓ 4.5 Error Control

✓ 4.6 Multiplexing

✓ 4.7 FDM, synchronous TDM

✓ 4.8 Statistical TDM

✓ Unit 5: Switching & Routing

- 5.1 Circuit Switching networks
- 5.2 Packet Switching principles
- 5.3 X.25
- 5.4 Routing in Packet switching
- 5.5 Congestion
- 5.6 Effect of congestion, congestion control
- 5.7 Traffic Management
- 5.8 Congestion Control in Packet Switching Network

Unit 6: LAN Technology

- ✓ 6.1 Topology & Transmission Media
- ✓ 6.2 LAN protocol architecture
- ✓ 6.3 Medium Access Control
- ✓ 6.4 Bridges, Hub, Switch
- ✓ 6.5 Ethernet (CSMA/CD), File Channel
- ✓ 6.6 Wireless LAN Technology

✓ Unit 7: TCP/IP

- ✓ 7.1 TCP/IP Protocol Suite
- ✓ 7.2 Basic protocol functions
- ✓ 7.3 Principles of Internetworking
- ✓ 7.4 Internet protocol operation
- ✓ 7.5 Internet protocol

Unit-1

1.1 Introduction to Networks of Data Communications

→ In data communications, data generally are defined as information that is stored in digital form.

→ Data Communications is the process of transferring digital information b/w two or more points.

→ Information is defined as the knowledge or intelligence.

Data communications can be summarised as the transmission, reception, and processing of digital information.

→ For data communication to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

→ The effective of data communication system depends on four fundamental characteristics i.e. delivery, accuracy, timeliness and jitter.

A data communication system has five components :-

(i) Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

(ii) Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, television etc.

(iii) Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television etc.

(iv) Transmission Medium: The transmission medium is the physical path by which a message travels from sender to receiver.

Ex- twisted-pair wire, coaxial cable, fibre-optic cable, radio waves etc.

(v) Protocol: A protocol is a set of rules that govern data communications. It represents an agreement b/w the communicating devices.

2.4 Guided Media

1. Twisted-pair wire

→ A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

→ One of the wires is used to carry signals to the receiver and other is used only as a ground reference.

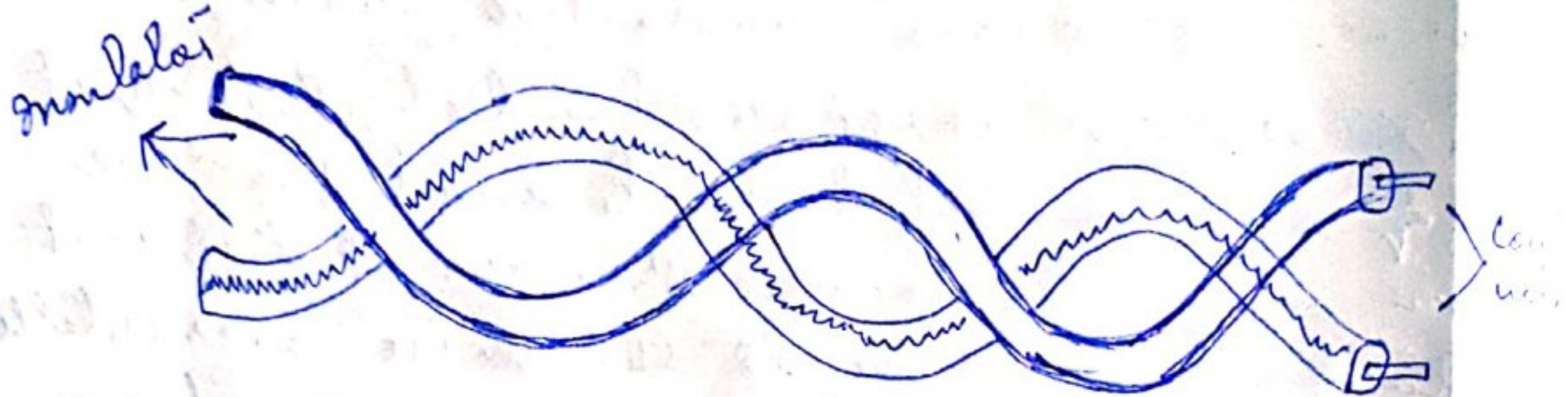
- The receiver uses the difference of the two.
- In addition to the signals sent by the sender on one of the wires, interference (noise) and cross talk may affect both wires and create unwanted signals.
- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or cross talk sources (ex- one is closer and the other is farther) & in the next twist the reverse is true).
- ~~twisted~~ Twisting makes it probable that both wires are equally affected by external influences (noise or cross talk). This means the receiver, which calculates the difference of the two, receives no unwanted signals. The unwanted signals are mostly canceled out.
- The number of twists per unit length (i.e. inch) has some effect on the quality of the cable.

Applications

- Used in telephone lines to provide voice & data channels. The local loop - the line that connects subscribers to the central telephone office - commonly consists of unshielded twisted pair cables.
- The DSL lines that are used by telephone companies to provide high data rate connections

also use the high-bandwidth capability of unshielded twisted pair cables.

→ Local area nets such as 10Base-T & 100Base-T also use twisted pair cables.



2. Coaxial Cable

→ Coaxial cable (or coax) carries signals of higher frequency ranges than those of in twisted pair cable, in part because the two media are constructed quite differently.

→ Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which in turn, is enclosed in an outer conductor of metal foil, braid or a combination of two.

→ The outer metallic wrapping serves both as a shield against noise & as the second conductor, which completes the circuit.

→ This outer conductor is also enclosed in an insulating sheath and the whole cable is protected by a plastic cover.

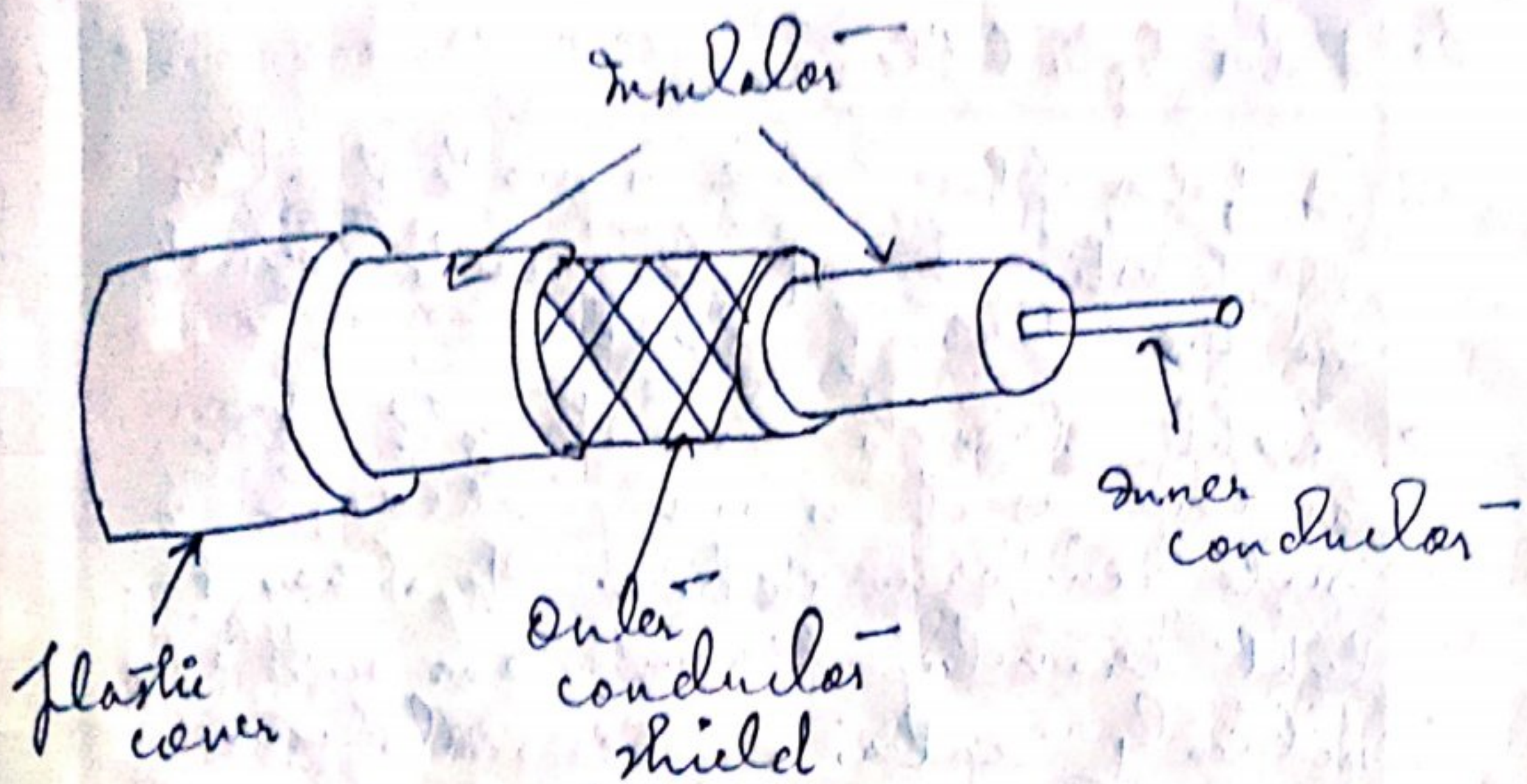


fig: Coaxial cable

Applications

- Coaxial cable was widely used in analog telephone networks where a single coaxial cable could carry 10,000 voice signals.
- Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps.
- However, coaxial cable in telephone networks has largely been replaced today with fibre-optic cable.
- Cable TV networks also use coaxial cables.
- Cable TV uses RG-59 coaxial cable.
- Also used in Ethernet LANs. ~~See~~ because of its high bandwidth & consequently high data rate.

3. Fiber Optic Cable ;

- A fiber optic cable is made of glass or plastic & can transmit signals in the form of light.
- Light travels in a straight line as long as it is moving through a single uniform medium. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes its direction.

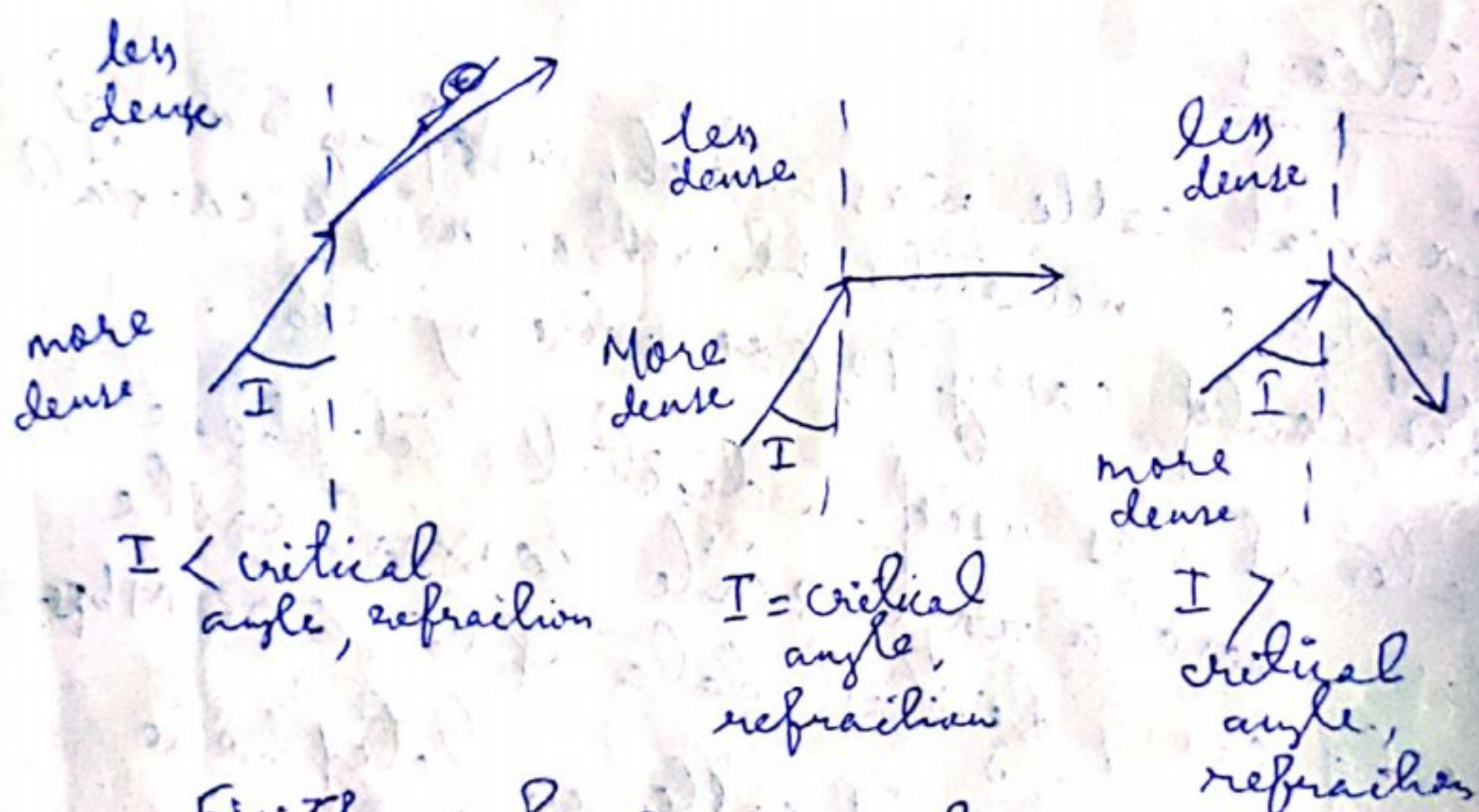
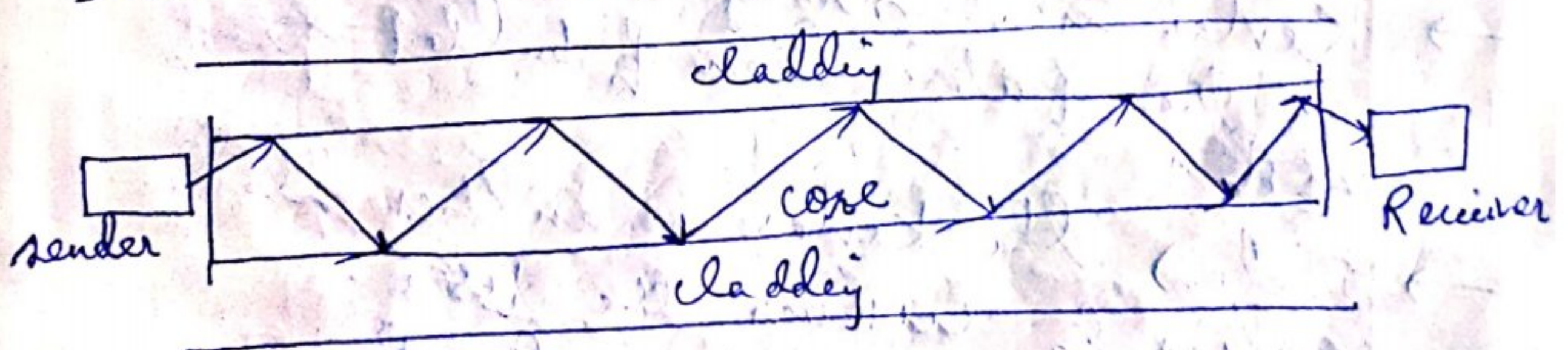


Fig: Shows how a ray of light changes direction when going from more dense to a less dense substance.

- If the angle of incidence I (the angle the ray makes with the line perpendicular to the interface of the two substances) is less than the critical angle, the ray refracts and moves closer to the surface.

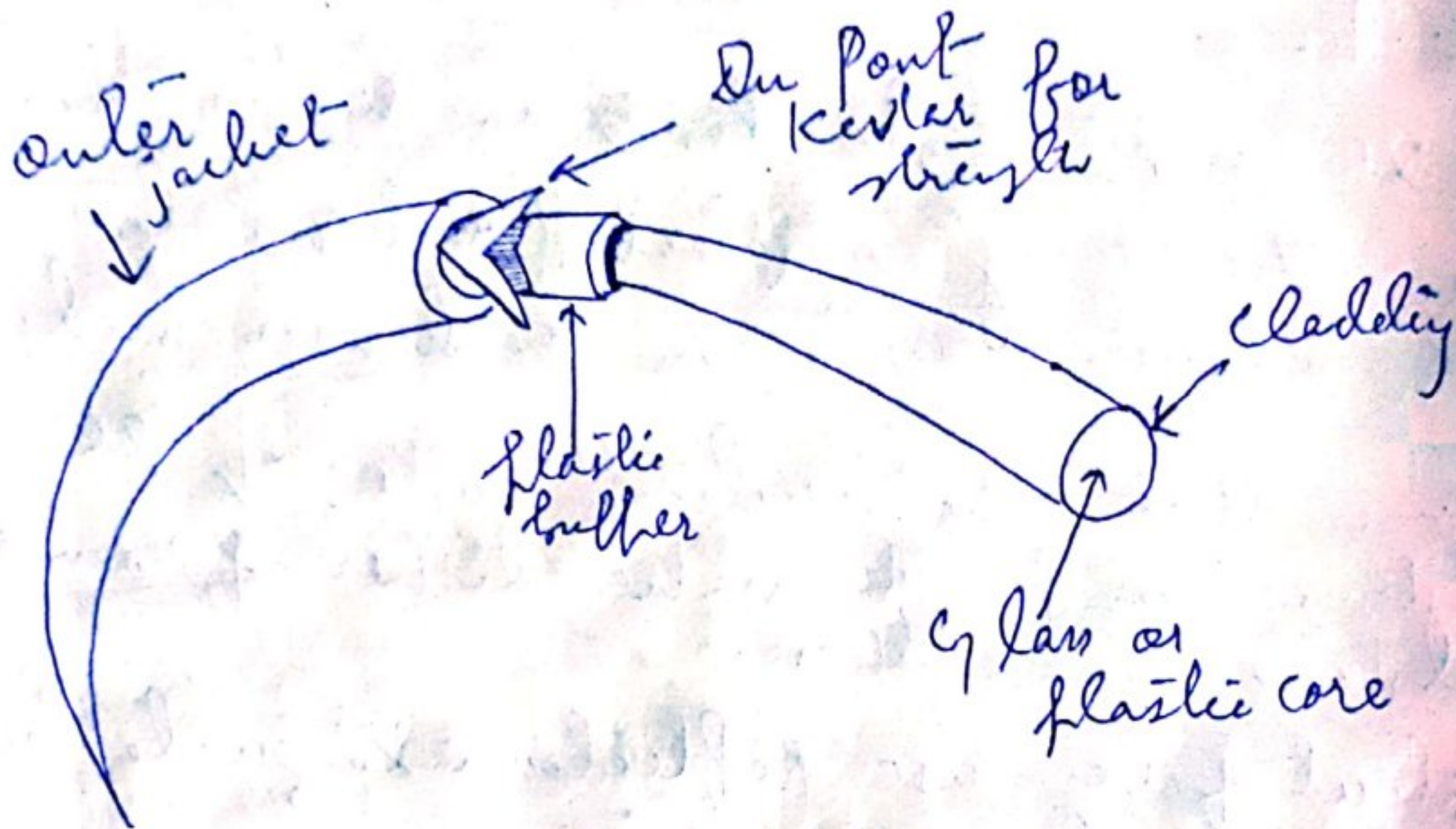
- If the angle of incidence is equal to the critical angle, the light travels along the interface.
- If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser medium.
- Note that the critical angle, of the substance, and its value differ from one substance to another.
- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



by: optical fiber

~~Fiber~~

Fiber Construction



→ The above fig. shows the construction of a typical fiber-optic cable.

→ The outer jacket is made of either PVC or Teflon.

→ Inside the jacket are Kevlar strands to strengthen the cable.

→ Kevlar is a strong material used in the fabrication of bullet-proof vests.

→ Below the Kevlar is another plastic coating to cushion the fiber.

→ The fiber is at the center of the cable, and it consists of cladding and core.

Advantages

(or ~~explanation~~) Fiber optic cable has several advantages over metallic cable (twisted pair or coaxial).

(a) Higher bandwidth: Fiber optic cable can support dramatically higher bandwidths and hence high data rates than either twisted pair or coaxial cable.

→ ~~By~~ Currently data rates and $\therefore$ utilisation over fiber optic cable are limited by the signal generation & reception technology available.

(b) Less signal attenuation: Fiber optic transmission distance is significantly greater than that of other guided media. A signal can run 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted pair cable.

(c) Immunity to electromagnetic interference: electromagnetic noise cannot affect fiber optic cables.

(d) Resistance to corrosive materials: Glass is more resistant to corrosive material than copper.

(e) Light weight: Fiber optic cables are much lighter than copper cables.

(f) Greater immunity to tapping:-

Fiber optic cables are more immune to tapping than copper cables. Copper cables antenna effects can easily be tapped.

Disadvantages

(a) Installation & maintenance:-

Fiber optic cable is relatively new technology, its installation & maintenance require expertise that is not yet available everywhere.

(b) Unidirectional light propagation

Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

(c) Cost: the cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

Applications

- Today with wavelength-division multiplexing (WDM), we can transfer data at a rate of 160 Gbps. The SONET n/w provides such a backbone. (synchronous optical n/w)
- Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid n/w.
- Local area n/w such as 100Base-FX n/w (Fast Ethernet) or 100Base-X also use fiber optic cable.

electrical signal is converted to optical signal through the help of optical transmitter. (used at both sender and receiver for n/w), which encodes the information to be transmitted on the light that is generated.

Types of transmitter $\left\{ \begin{array}{l} \text{LEDs (light emitting diodes)} \\ \text{Laser diodes} \end{array} \right.$

Unguided Media: Wireless

- Unguided media transport electromagnetic waves without using a physical conductor.
- This type of communication is often referred to as wireless communication.
- Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

→ Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, line of sight propagation as shown in fig below: -



Ground propagation
(below 2 MHz)
(AM radio)



Sky propagation
(2-30 MHz)



line of sight
propagation
(above 30 MHz)

→ In ground propagation, radio waves travel through the lowest portion of the atmosphere hugging the earth.

→ These low-frequency emanate in all directions from the transmitting antenna and follow the curvature of the planet.

→ Distance depends on the amount of power in the signal. The greater the power, the greater the distance.

→ In sky propagation, higher frequency radio waves radiate upward into the ionosphere where they are reflected back to earth. This type of transmission allows for greater distances with lower output power.

- In line of sight propagation, very high frequency signals are transmitted in straight lines directly from antenna to antenna.
- Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth.
- Line of sight propagation is tricky because radio transmissions cannot be completely focused.

Radio Waves :-

- Waves ranging in frequencies of 3 KHz and 1 GHz are called radio waves.
- Radio waves, for the most part, are omnidirectional.
- When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned.
- A sending antenna sends waves that can be received by any receiving antennas.
- The omnidirectional property has a disadvantage too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.
- Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves

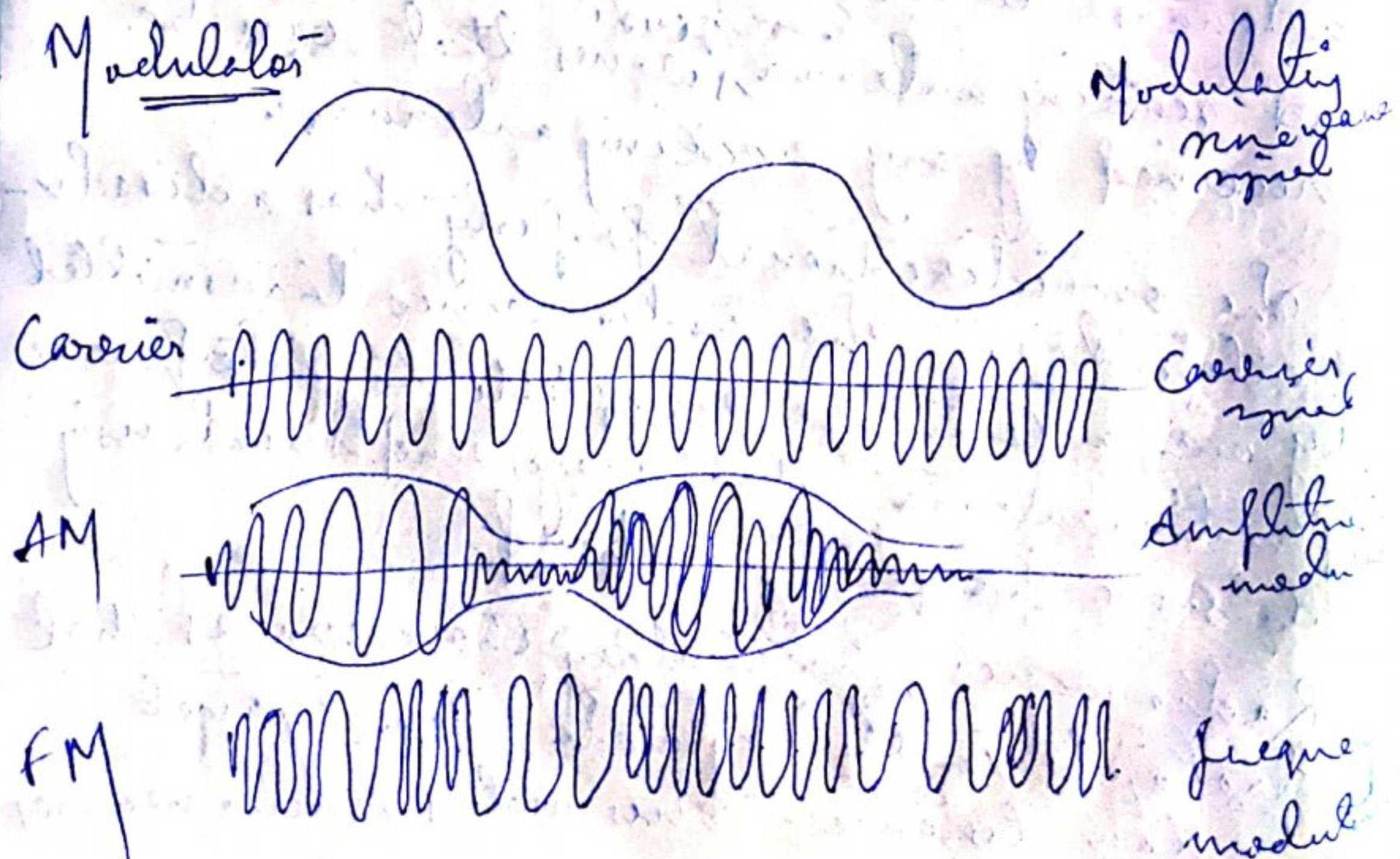
a good candidate for long-distance broadcasting such as AM radio.

→ Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both advantage and disadvantage.

→ It is an advantage because, for example, an AM radio can receive signals inside a building.

It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

→ The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into sub bands, the sub bands are also narrow, leading to a low data rate for digital communications.



The The difference is in how the carrier wave is modulated, or altered. With AM radio, the amplitude, or overall strength, of the signal is varied, to incorporate the sound information.

With FM, the frequency (the number of times each second that the current changes direction) of the carrier signal is varied.

→ FM is less prone to interference than AM. However, FM signals are impeded by physical barriers.

→ FM has better sound quality due to higher bandwidth.

→ In AM radio broadcasting, the modulating signal has bandwidth of 15 KHz and hence the bandwidth of an amplitude-modulated signal is 30 KHz.

AM → varies amplitude with frequency constant.

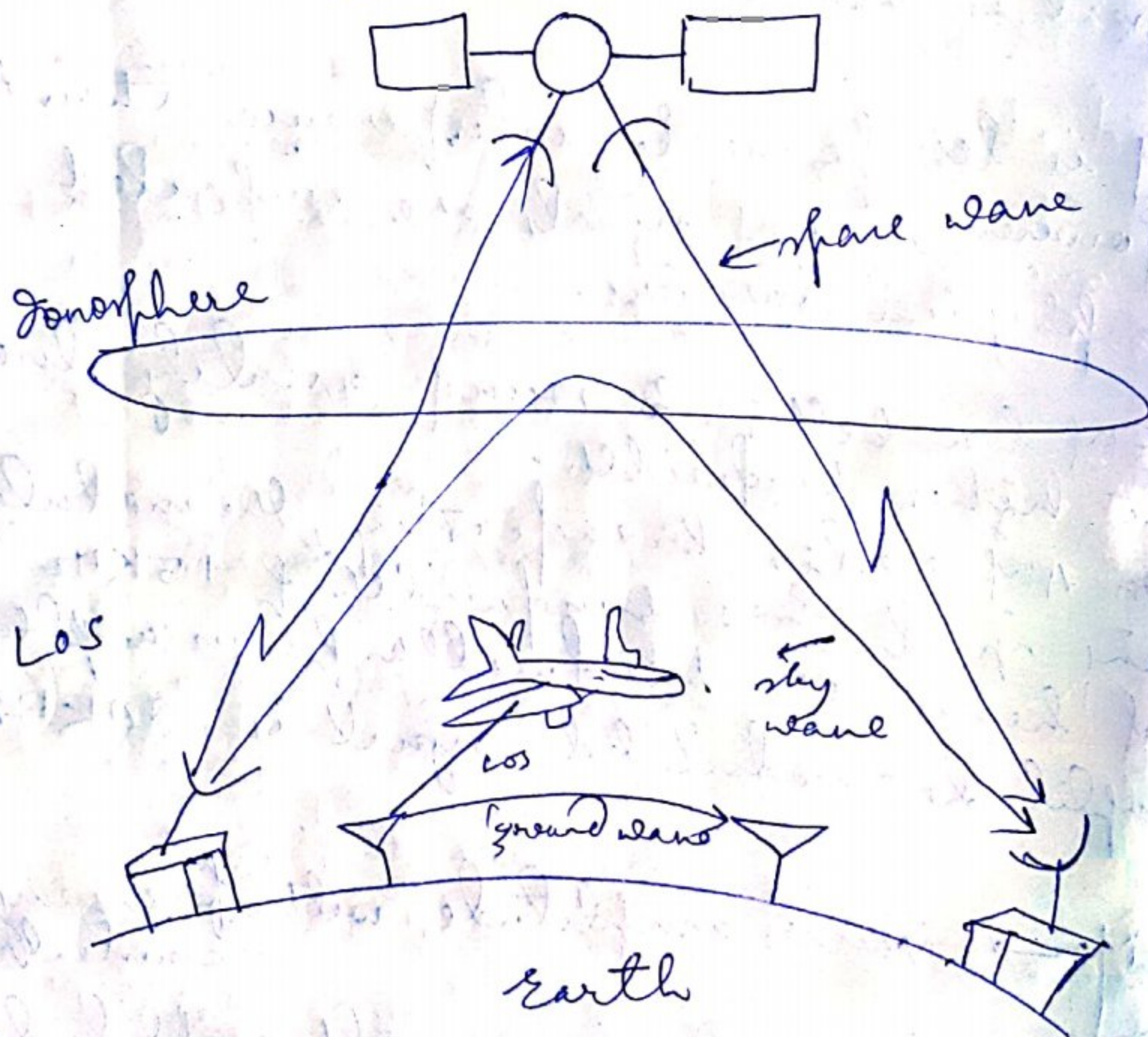
FM → varies frequency with amplitude constant.

Which travel farther AM or FM?

Low frequencies travel farther mostly because they propagate along the surface of the earth. High frequency FM signals are

basically line of sight. Under the right conditions, any signals will bounce off the ionosphere and can travel around the globe. This is not possible with high frequency signals.

Communication satellite-



Note Line of sight propagation is a characteristic electromagnetic radiation or acoustic wave propagation which means waves travel a ~~direct~~ direct path from the source to the receiver.

→ It can transmit and receive data only where each other transmit & receive data are in view of each other without any sort of obstacle b/w them.

1.2 Networks

* A Network is defined as a group of two or more computer systems linked together.

→ There are many types of computer networks such as :-

- Local-area n/w (LANs) → the computers are geographically close together (i.e. in the same building).
- Wide-area n/w (WANs) → the computers are farther apart and are connected by telephone lines or radio waves.
- Campus-area n/w (CANs) → the computers are within a limited geographic area, such as a campus or military base.
- Metropolitan-area n/w (MANs) → A data n/w is designed for a town or city.
- Home-area n/w (HANs) → A n/w contained within a user's home that connects a person's digital devices.

Network Criteria

1. Performance (No. of users, medium, hardware, software)
2. Reliability
3. Security (Virus, unauthorised access)

Advantages of Computer n/w

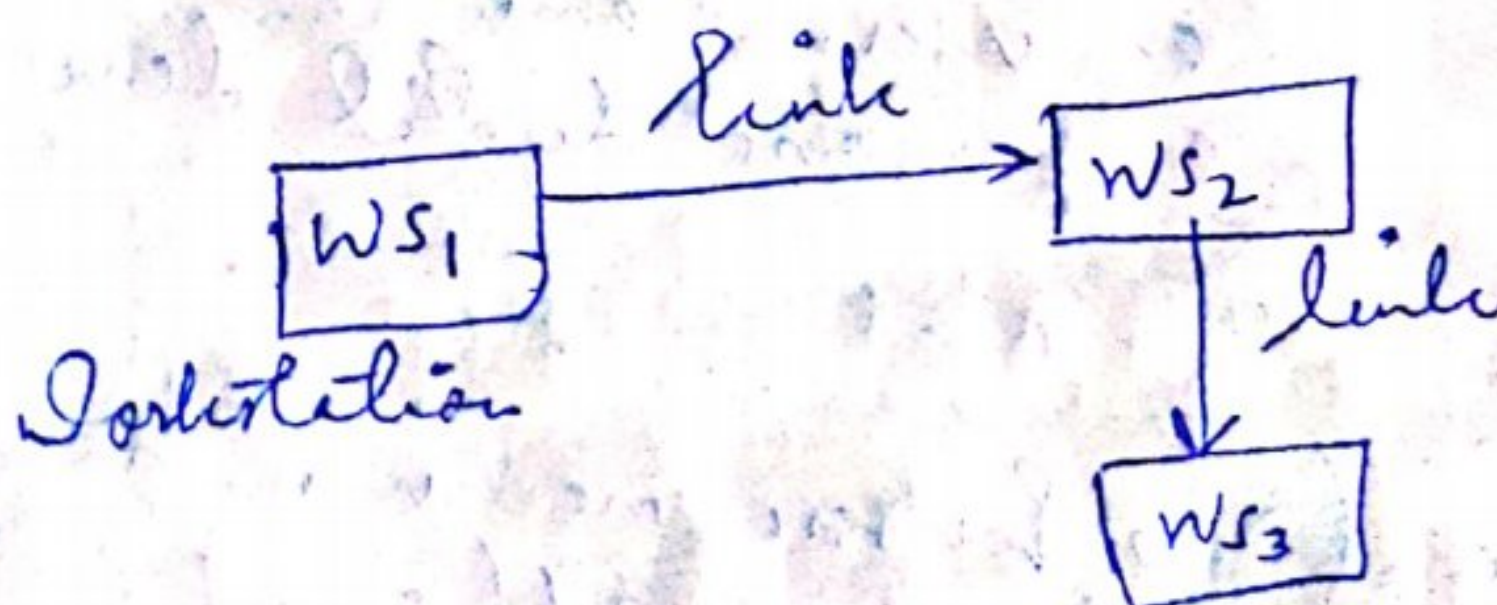
- sharing of information
- sharing of hardware resource
- sharing of software resource
- presenting the information
- Communication.

Applications

- Business
- Financial
- Reservation / Ticket Booking
- Mail services
- Online registration
- Industries
- Mobile app
- Video conferencing

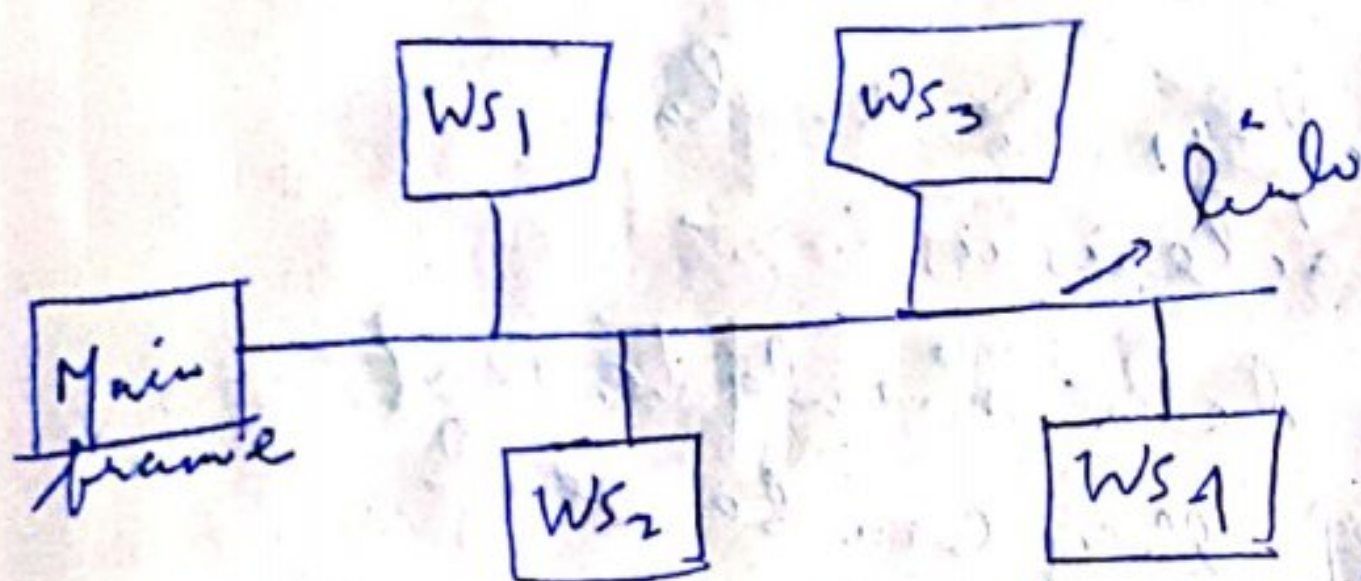
4 Architecture of n/w Physical structure of the Network

1. Peer-to-peer connection
(point to point connection)



→ It refers to a ^{communicating} connection b/w endpoints or nodes directly without any host or any other intermediary in b/w.

2. Multipoint connection



→ A multipoint connection is a link b/w three or more devices. It is also known as multidrop configuration.

→ The networks having multipoint configuration are called as broadcast n/w.

→ In this n/w, a message or packet sent by any machine is received by all other machines in a n/w.

1.3 Protocols

→ Protocol is a set of rules and regulations which govern the data communication.

→ The protocol defines what is communicated, how it is communicated & when it is communicated.

→ The key elements of the protocols are:-

- Syntax
- Semantic
- Timing

Syntax : It refers to structure or format of the data i.e., the order in which they are represented.

Semantic : It refers to the meaning of each section of the bit.

Timing : It refers to the two characteristics : —

- (i) when the data should be sent
- (ii) how fast they can be sent

N/D Architecture

N/D architecture refers to how computers are organised in a system and how tasks are allocated to these computers.

Standards

→ A standard provides a model for development that makes it possible for a product to work regardless of the individual manufacturer.

→ The data communication standards fall into two categories : —

- (i) De facto → by fact or by convention
- (ii) De Jure → by law or by resolution.

→ The standard organisations are :-

1. ISO → International Standard Organisation

2. ANSI → American National Standard
organisation

or
American Nations Organisation for
standardisation.

3. IEEE → Institute of Electrical
Engineering

4. EIA → Electronic Industry Association

5. CCITT → Consulting Committee for
International Telegraphy and
Telephony

6. ITU-T → International Telecommunication
Union - Telecommunication Standard
Sector.

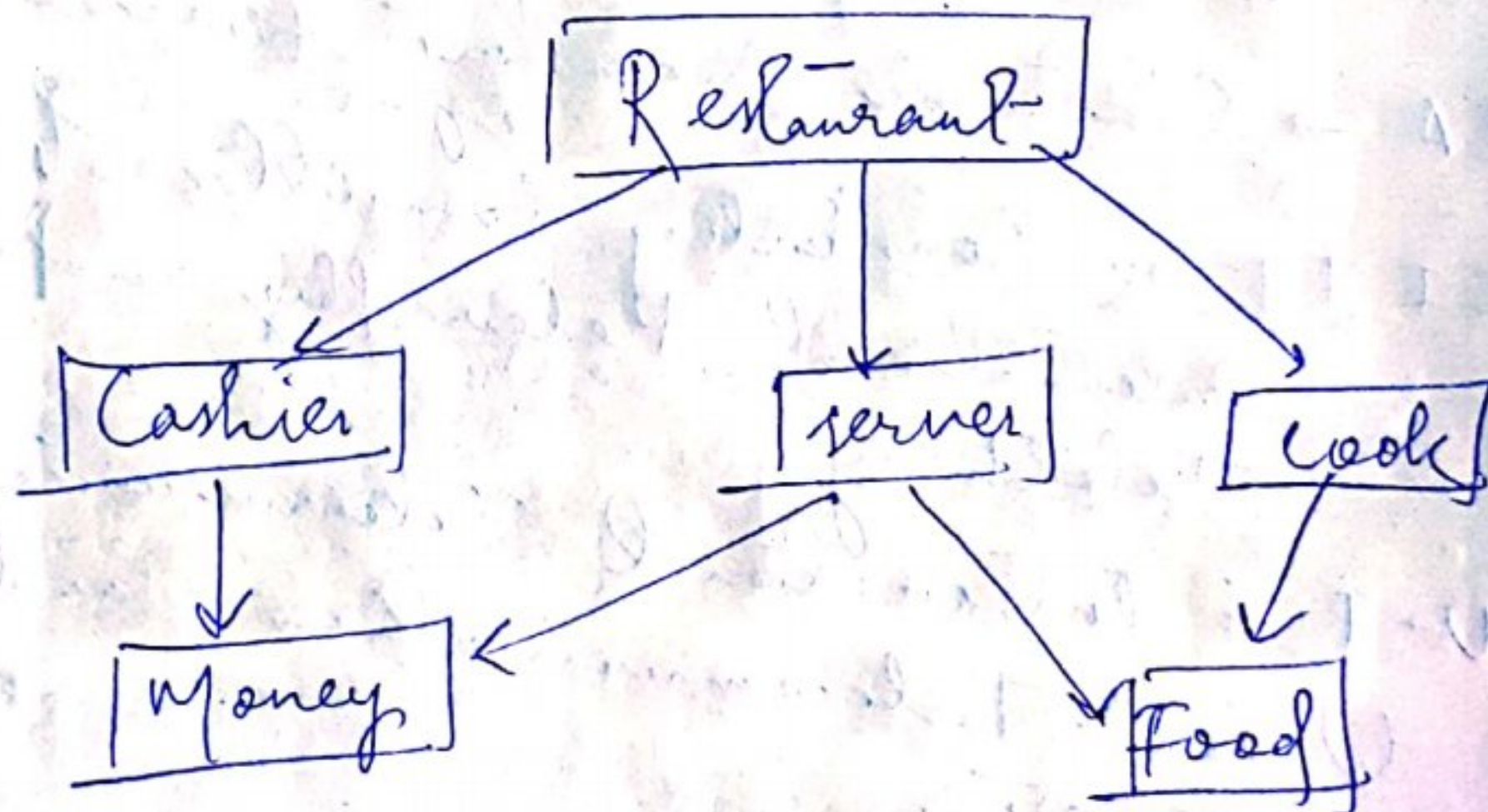
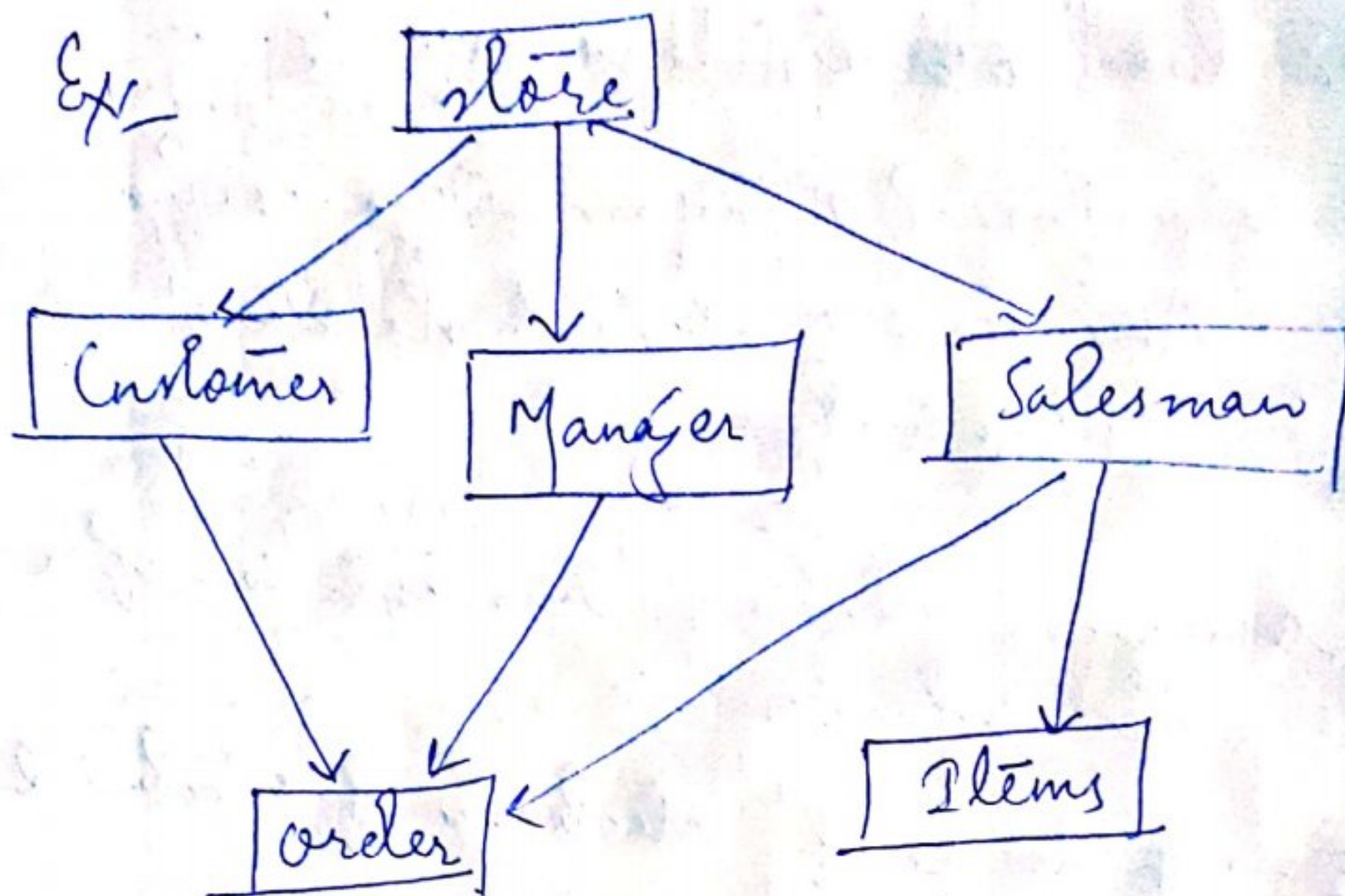
Network Model

1. OSI (Open System Interconnection) Model
(7 layer Protocol)

2. Internet Model (TCP/IP) (4 layer protocol)

→ Network model is a database model that shows
the relationships among the objects.

→ It is viewed as a graph with nodes or
ends connected through links.



OSI Model

→ It stands for ~~Open Systems Interconnect~~ Model that characterises and standardises the communication functions of a telecommunication or computing system without regard to its underlying inter structure and technology.

→ The OSI reference model was first introduced in the late 1970.

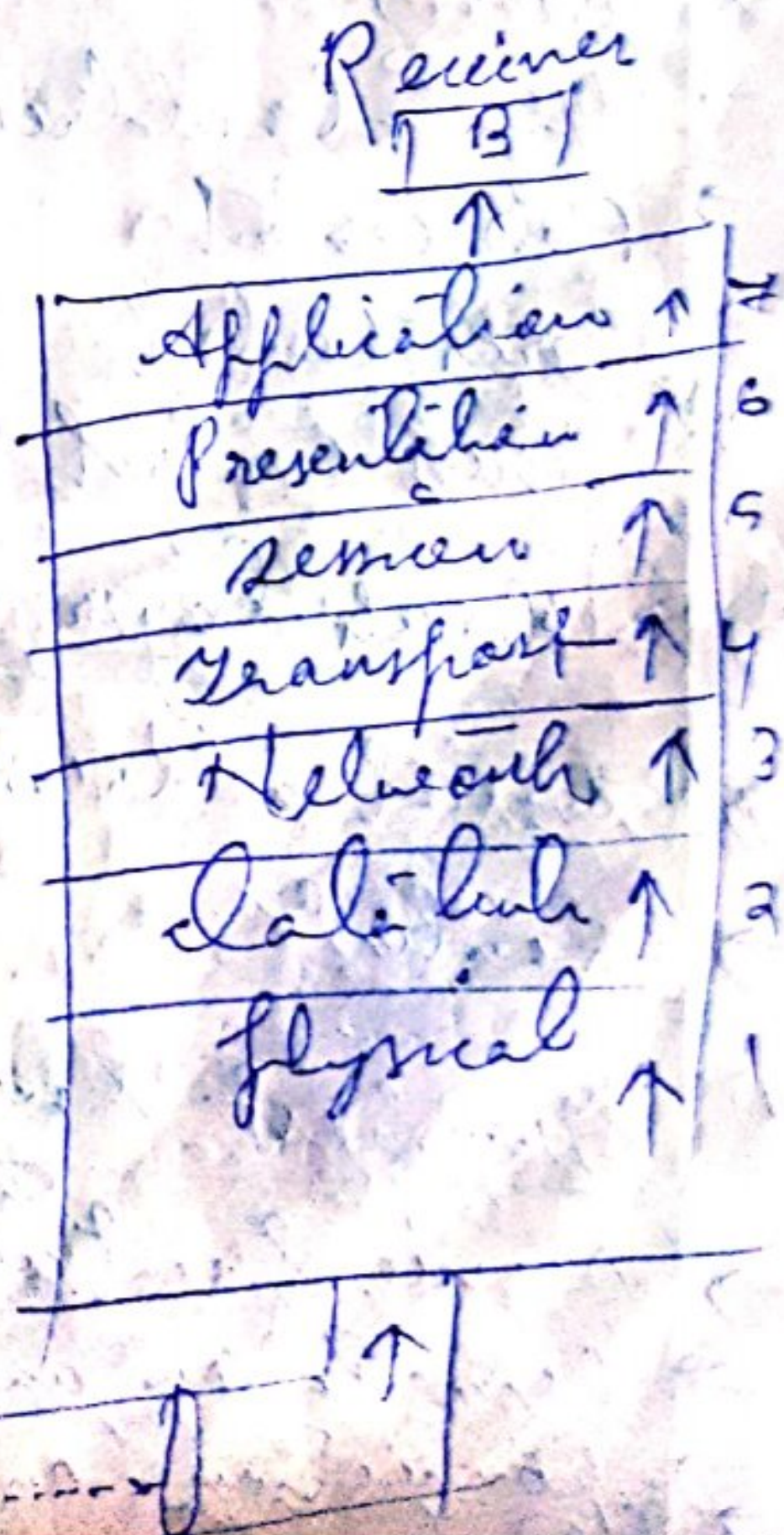
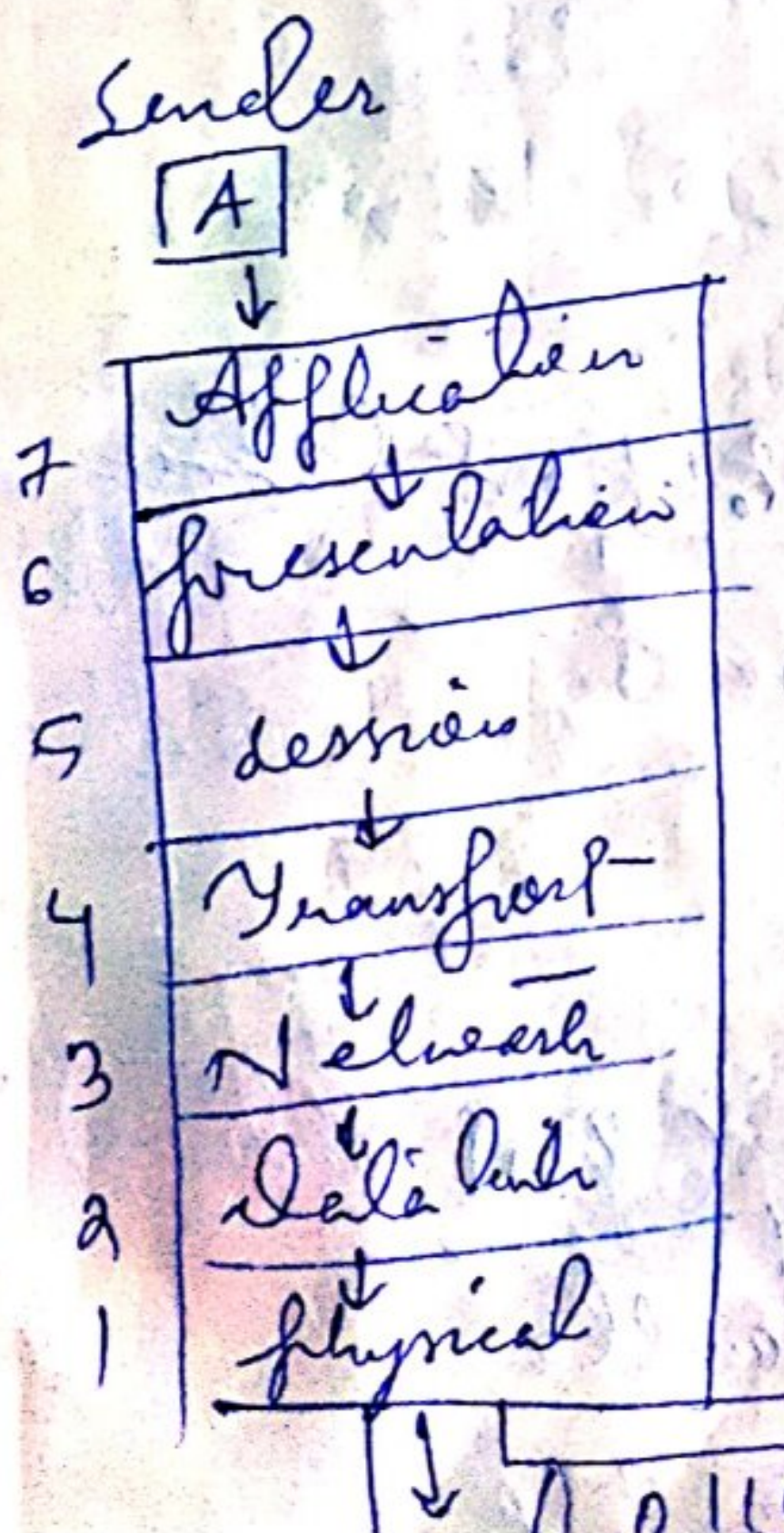
→ An open system is a set of protocols that allows any two different systems to

communicate regardless of their underlying architecture.

→ the OSI model is not a protocol, it is a model for understanding and designing the network architecture i.e. flexible, robust and interoperable.

→ the ~~ISO~~ OSI Model consists of 7 layers named as :-

- (i) Physical layer
- (ii) Data-link "
- (iii) N/w "
- (iv) Transport "
- (v) Session "
- (vi) Presentation "
- (vii) Application



Functions of Different Layers of OSI Model

(i) Physical Layer

- physical characteristics of interface and medium.
- Representation of bits
- Data transmission rate
- Signal sequence synchronization of bits
- Line configuration.
- Physical topology
- Transmission mode

(ii) Data Link Layer

- Framing
- Physical Addressing
- Flow control
- Error control
- Access control

(iii) Network Layer (Host-to-Host Delivery)

- logical addressing
- Routing

(iv) Transport Layer

- service point addressing (port address)
- Segmentation and Reassembly
- Connection control
- Flow control → Error control

(v) Session Layer

- Dialogue control
- Synchronisation

(vi) Presentation Layer

- Translation
- Encryption
- Compression

(vii) Application Layer

- Network virtual terminal
- File transfer, access and management
- Mail services
- Directory services

TCP/IP

→ The Internet Protocol suite is the conceptual model and set of communication protocols used in the Internet and similar computer networks.

→ It is commonly known as TCP/IP because the foundational protocols in the suite are the Transmission Control Protocol and Internet Protocol.

→ This is a set of networking protocols that allows two or more computers to communicate.

→ The Defense Data N/w, part of the Department of Defense, developed TCP/IP and it has been widely adopted as a networking standard.

→ In basic terms, TCP/IP allows one computer to talk to another computer via the internet through compiling packets of data and sending them to right location.

→ It specifies how data is exchanged on the internet by providing end-to-end communications that identify how it should be broken into packets, addresses transmitted, routed and received at the destination.

→ An IP address is a numerical label assigned to each device connected to a computer network that uses the internet protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.

→ The difference b/w TCP/IP is that TCP is responsible for the data delivery of a packet and IP is responsible for the logical addressing.

In other words, IP claims the address & TCP guarantees delivery of data to that address.

Similarities b/w OSI & TCP/IP

→ Both OSI and TCP/IP model use a set of independent protocols for enabling communication b/w the users.

→ In both models, upper layer focus on application such as Web browser and the lower layer focus on end-to-end delivery of data.

OSI Reference Model

(i) 7 layer architecture

7. Application
6. presentation
5. session

4. Transport (CO)
3. Network (COSI)

2. Data link
1. Physical

(ii) It is unable to connect Radio & satellite n/w.

(iii) It supports only connection-oriented communication in transport layer while both connection-oriented & connectionless communication in n/w layer.

(iv) It clearly distinguish services, interfaces & protocols.

(v) It was defined before the invention of Internet.

(vi) The model was developed before the corresponding protocol came into existence.

TCP/IP Protocol Model

(i) 4 layer architecture

4. presentation (specific address)

3. Transport (CO) (port address)

2. Network (CI) (logical address)

1. Network Access (host-to-host) deals with physical address

(ii) It has the ability to connect Radio & satellite n/w.

(iii) It supports both connection-oriented and connectionless communication protocol in transport layer while only connectionless communication in Network layer.

(iv) It doesn't clearly distinguish services, interfaces & protocols.

(v) It was defined after the invention of Internet.

(vi) The model was developed after the protocol came into existence.

(2.1)

Data Transmission Concepts & Terminology

Transmission Terminology

→ Transmission from transmitter to receiver goes over some transmission medium using electromagnetic waves.

- Guided media → Waves are guided along a physical path: twisted pair, fiber, coaxial cable.

- Unguided media → Waves are not guided: air, radio waves.

- Direct link → Signal goes from transmitter to receiver with no intermediate devices other than amplifiers and repeaters.

- Point to point link → Guided media with direct link b/w two devices, with those two devices being the only ones sharing the medium.

- Multipoint guided configuration → More than two devices can share the same medium.

→ Simplex, half duplex & full duplex transmission.

Frequency, Spectrum & Bandwidth

→ Signal is generated by a transmitter & transmitted over a medium.

→ Signal is a function of time or frequency (components of different frequency).

→ Time domain concept:-

Continuous signal → Signal intensity varies in a smooth fashion over time; no breaks or discontinuities in signal.

Discrete signal → Signal intensity can take one of two pre-specified values for any amount of time.

Periodic signal → Same signal pattern repeats over time; signal is said to be periodic

$$\text{if } s(t+T) = s(t) \quad - \infty < t < \infty$$

T is the period of the signal; sine wave.

Aperiodic signal → Signal that is not periodic

Peak Amplitude → Maximum signal intensity over time; typically measured in volts

Frequency (f) → Rate at which signal repeats; measured in cycles per second or Hz.

Period (T) → Amount of time required for one repetition of signal.

Phase → Measure of relative position in time within a single period of a signal.

for a periodic signal $s(t)$, phase is fractional part $\frac{t}{T}$ of the period T through which t has advanced relative to an arbitrary origin.

ex- $s(t) = A \sin(2\pi f t + \phi)$

Wavelength (λ) $\rightarrow$ Distance occupied by a single cycle:—

$\rightarrow$ Consider a signal traveling at velocity v
 $\rightarrow$ Wavelength is related to period as

$$\lambda = vT$$

$$\rightarrow \text{Also } \lambda f = v$$

Fundamental frequency $\rightarrow$ The base frequency i.e. the frequency of all components can be expressed as its integer multiples.

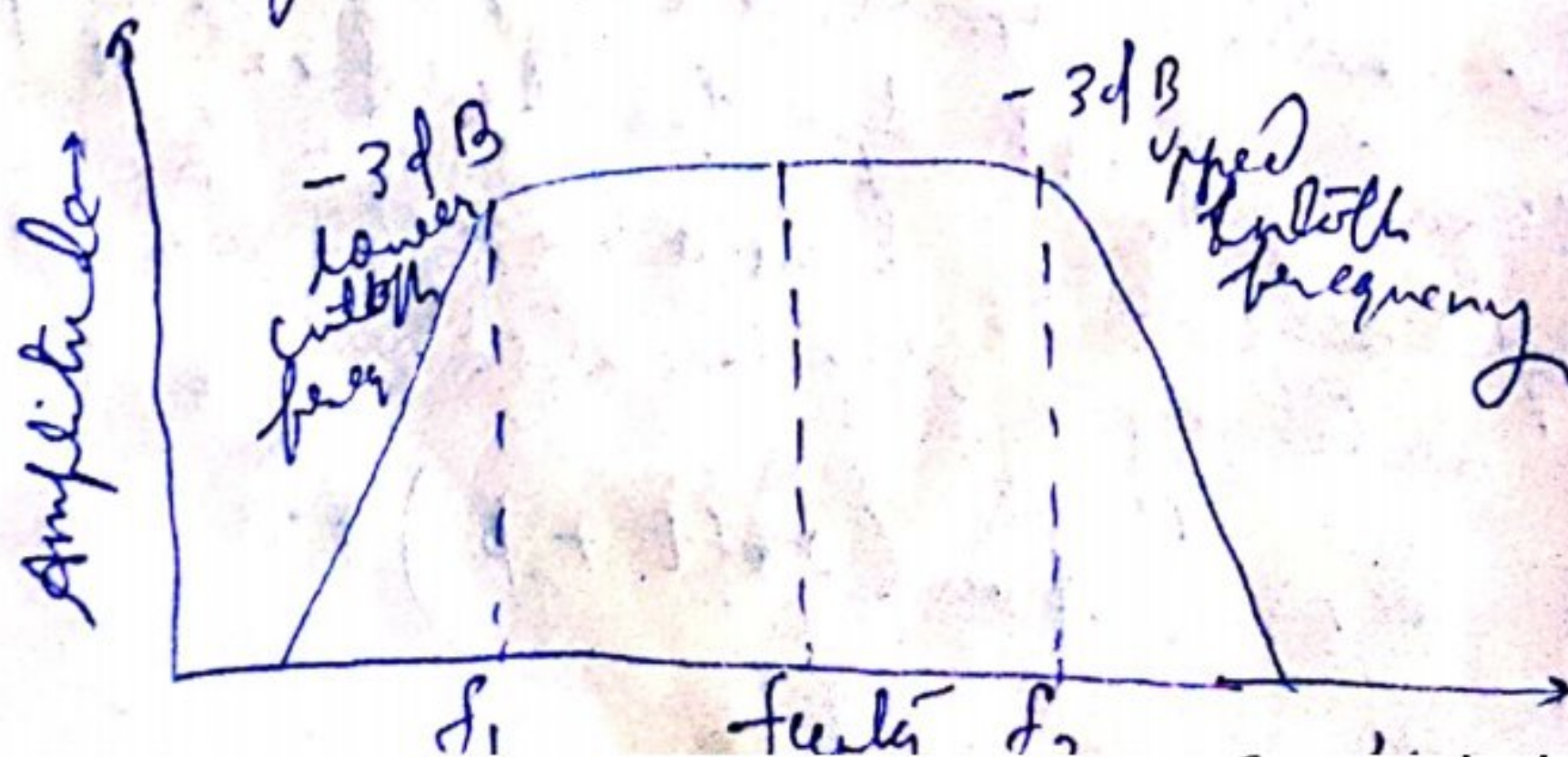
The period of the aggregate signal is the same as the period of fundamental frequency.

Spectrum $\rightarrow$ Range of frequencies contained in the signal.

Absolute bandwidth $\rightarrow$ Width of the spectrum

Effective bandwidth $\rightarrow$ Narrow band of frequency containing most of the energy of the signal.

Center frequency $\rightarrow$ Point where bandwidth of a signal is centered. Higher the center frequency, higher the potential bandwidth.



2.2 Analog & Digital Data Transmission

Data: The data refers to an entity that expresses some meaning based on some rule which are agreed upon by the sender and receiver.

It can be available in various forms such as text, graphics, audio, video etc.

Signal: Signal refers to the representation of data in a suitable form for transmission over a transmission medium.

There are two types of Data: —

1. Analog Data
2. Digital Data

1. Analog Data

→ Analog Data is defined as the data having continuous state or continuous value in some intervals.

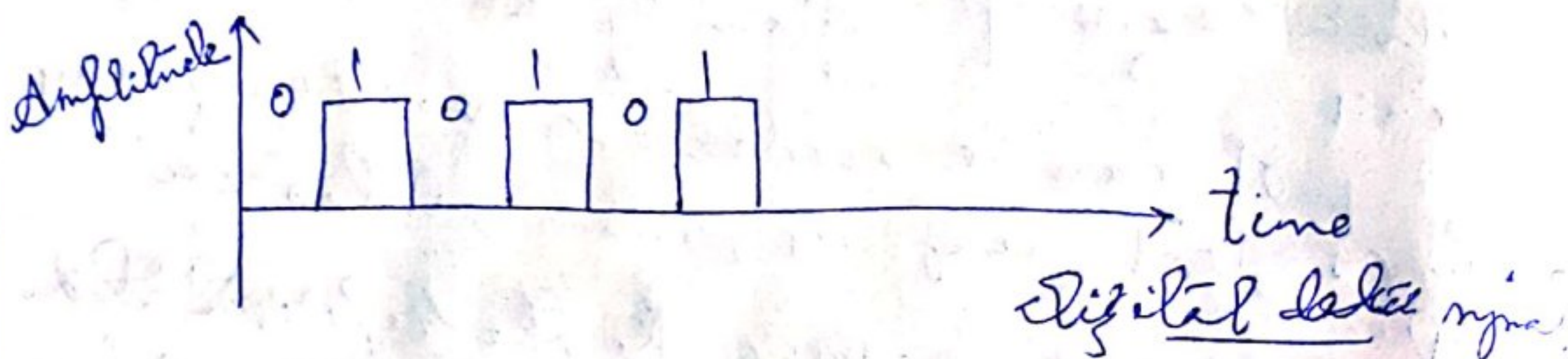
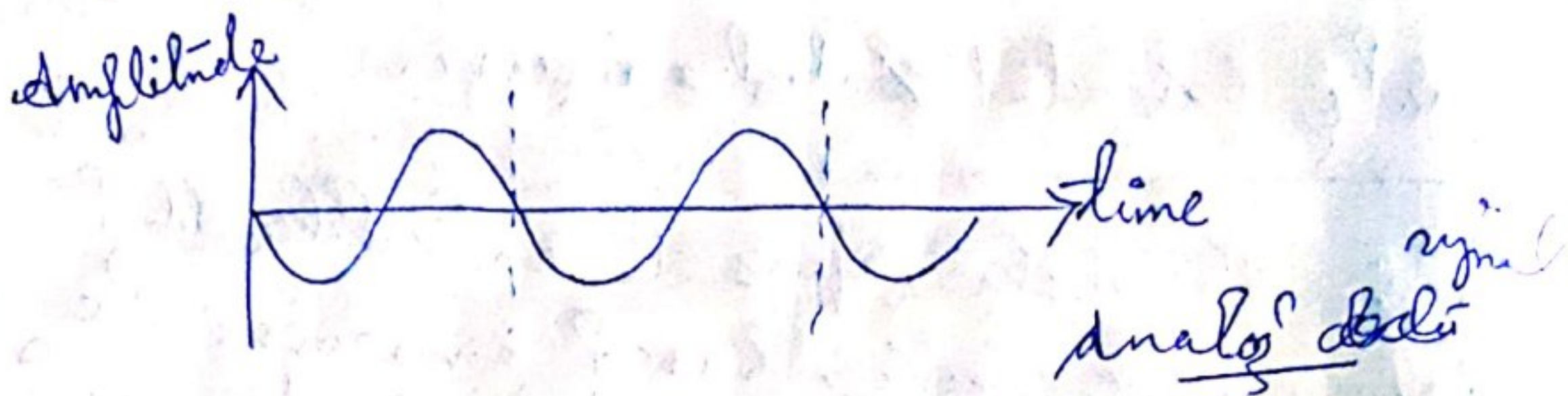
→ For example, voice, video, temperature etc.

2. Digital Data

→ It is defined as the data having continuous state or continuous value in some intervals.

→ It is defined as the data having discrete state or discrete value.

→ For example, Data represented in computer memory in form of 0 or 1.



Signals :-

the signals are again classified into two types :-

- (a) Analog signal
- (b) Digital signal

Analog signal → A signal that passes through and includes a wide range of varying values of intensity over a period of time is referred to as analog signal.

Digital signal → A signal that has only a finite range of value generally 0 & 1 is referred to as a digital signal.

Bit Interval :-

It is the time required to transmit one bit. (time/bit)

Bit rate -

The number of bit transmitted per second is called bit rate. (No. of bits/sec)

Bit length -

The distance occupied by a single bit while transmission on a transmission medium.

Bit rate

1
2
3
⋮
n

Bit Interval

1
 $\frac{1}{2}$
 $\frac{1}{3}$
⋮
 $\frac{1}{n}$

Bit rate & Bit Interval

→ Different bandwidths are used to transmit the signals from the sender to the receiver end.

→ Generally, both Base Band & Broad Band transmissions are used for transmitting the digital signal.

Base Band

Broad Band

(i) The digital signal is sent over a channel without converting it into an analog signal.

(ii) The entire bandwidth of the cable or channel is consumed by the single signal.

(i) The digital signal is first converted into analog signal and then sent into channel.

(ii) The signals are sent in multiple frequency and it allows the multiple signals to be sent simultaneously.

(iii) It requires a low pass channel, i.e. a channel whose bandwidth starts from 0.

(iv) It requires a band pass channel i.e. a channel whose bandwidth doesn't start from 0.

(2.3)

Transmission Impairments

1. Attenuation

→ To reduce the amplitude of an electrical signal with little or no distortion.

→ Logarithmic in nature for guided media: expressed as a constant number of decibels per unit distance.

→ For unguided media, complex function of distance and atmospheric condition.

→ Three considerations for transmission engineer:-

(i) Received signal must have sufficient strength to enable detection.

(ii) Signal must maintain a level sufficiently higher than noise to be received without error.

(iii) Attenuation is an increasing function of frequency.

→ Signal strength must be strong but not too strong & overload the capacity of transmitter or receiver, which will cause distortion.

2. Delay distortion

3. Noise

4. Intermodulation noise
→ Crosstalk
→ Impulse noise

5. Channel Capacity -

Max rate at which data can be transmitted over a communication path or channel.

Data rate - in bps

Bandwidth - Hz, cycles per second.

Noise - Avg noise level over channel

Error rate - percentage of time which bits are flipped

- BW is $\propto$ to cost

Nyquist BW(C)

Shannon Capacity formula

* BW = B, highest frequency signal

Rate = $2B$

$$C = 2B \log_2 M$$

3/11/2020

2. Intermodulation noise

- signals at different frequencies share the same transmission medium.
- May result in signals that are sum or difference or multiples of original frequencies.
- Occurs when there is some nonlinearity in the transmitter, receiver, or intervening transmission system.
- Non linearity may be caused by component malfunction or excessive signal strength.

3. Crosstalk

- Unwanted coupling b/w signal paths.
- Occurs due to electric coupling b/w nearby ~~to~~ twisted pairs, multiple signals on a coaxial cable, or unwanted signals picked up by microwave antennas.
- Typically same order of magnitude or less than thermal noise.

4. Impulse noise

- Noncontinuous noise, consisting of irregular pulses or noise spikes of short duration and high amplitudes.
- May be caused by lightning, or flaws in communications system.
- Not a major problem for analog data but can be significant for digital data.

→ A spike of 0.01 sec will not destroy any voice data but will destroy 560 bits being transmitted at 56 Kbps.

5. Channel Capacity

→ Maximum rate at which data can be transmitted over a communication path or channel.

→ Depends on four factors:-

(i) Data rate - in bps

(ii) Bandwidth - constrained by transmitter and nature of transmission medium, expressed in cycles per second or Hz.

(iii) Noise - Average noise level over channel

(iv) Error rate - percentage of times when bits are flipped.

→ Bandwidth is proportional to cost i.e. for digital data, we will like to get as high a data rate as possible within a limit of error rate for a given bandwidth.

→ Nyquist bandwidth:-

- limitation on data rate for a noise free channel; equals that of channel bandwidth.

- If the rate of signal transmission is $2B$ then a signal with frequency no greater than B is sufficient to carry the signal rate.

- Given a bandwidth B , the highest possible signal rate is $2B$.

The above is true for signals with two voltage levels.

- With multilevel signaling, Nyquist formulation is

$$C = 2B \log_2 M$$

- For a given bandwidth, data rate can be increased by increasing the number of different signal elements.
- Value of M is practically limited by noise & other impairments on transmission line.

→ Shannon Capacity formula

- Nyquist formula gives the relationship b/w bandwidth and data rate.
- Noise can corrupt bits of data.
 - shorter bits imply that more bits get corrupted by a given noise pattern.
- ~~Signal-to-noise (SNR) ratio~~
Higher data rate means higher errors & rate.
- higher signal strength can lead to better discrimination of signals in the presence of noise.
- Signal-to-noise (SNR) ratio.
 - ratio of power in signal to the power in noise present at a particular point in the noise

- Typically measure of at the receiver to process the signal & eliminate unwanted noise.
- often measured in decibels

$$(SNR)_{dB} = 10 \log_{10} \frac{\text{signal power}}{\text{noise power}}$$

- SNR expresses the amount by which the intended signal exceeds the noise level.
- High SNR implies a high quality signal while low SNR indicates the need for repeaters.
- SNR sets the upper bound on achievable data rate.
- Maximum channel capacity C , in bps is given by

$$C = B \log_2 (1 + SNR)$$

where B is the bandwidth of the channel in Hz.

- Shannon formula gives the maximum possible capacity assuming only white noise; it does not take into account the impulse noise, delay distortion, and attenuation.

The data encoding technique is divided into the following types, depending upon the type of data conversion:—

- Analog data to analog signals
- Analog data to digital signals
- Digital data to analog signals
- Digital data to digital signals.

Unit-3 (Data Encoding)

3.1 Data Encoding

→ Encoding is the process of converting the data or a given sequence of characters, symbols, alphabets etc, into a specified format, for the secured transmission of data.

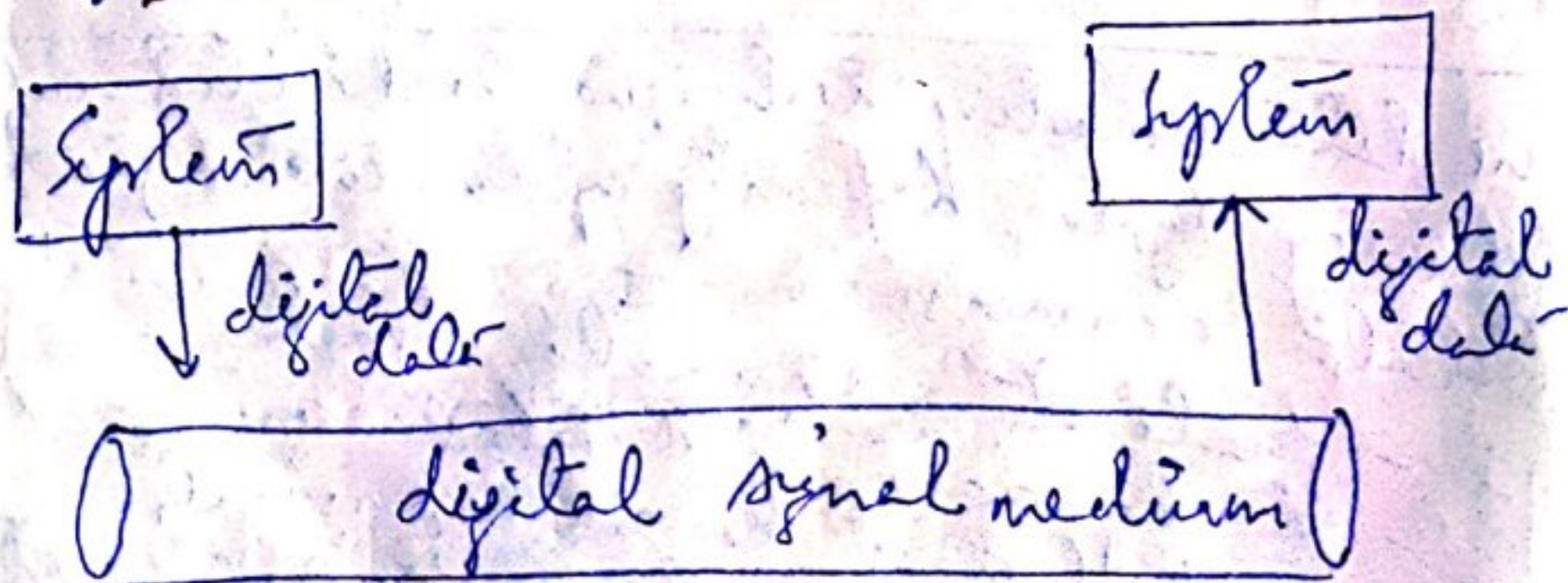
Decoding is the reverse process of ~~encod~~ encoding which is to extract the information from the converted format.

→ It uses various patterns of voltage or current levels to represent 1s and 0s of the digital signals on the transmission link.

→ The common types of line encoding are Unipolar, polar, Bipolar and Manchester.

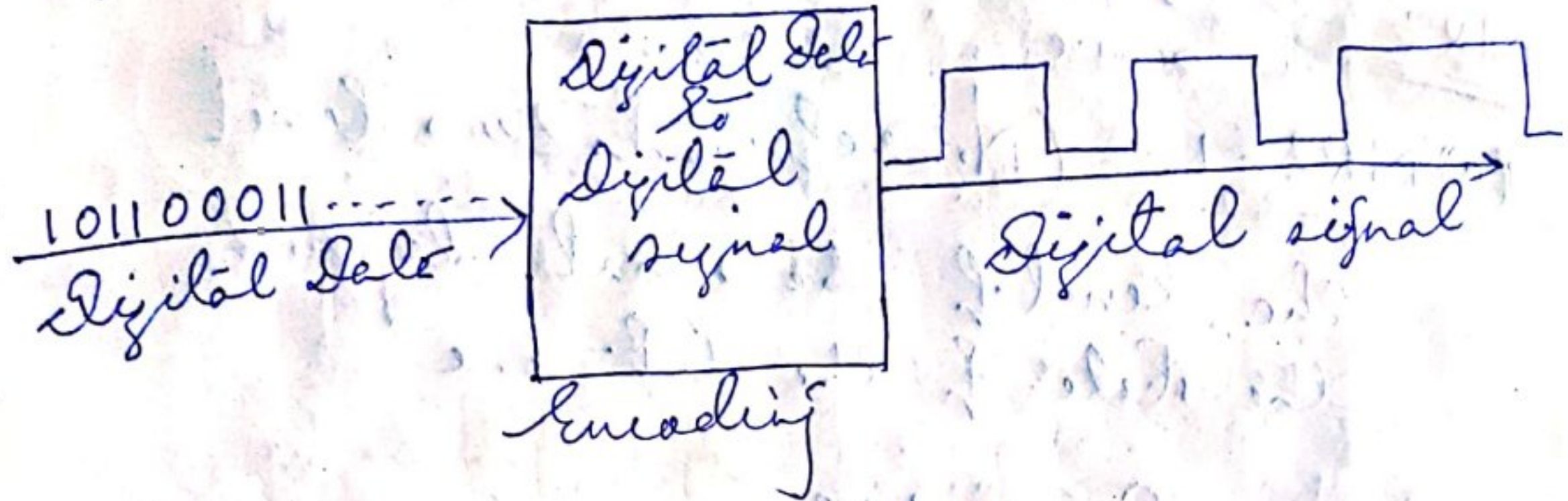
3.2 Digital Data to Digital Signal

Digital data to Digital signal conversion

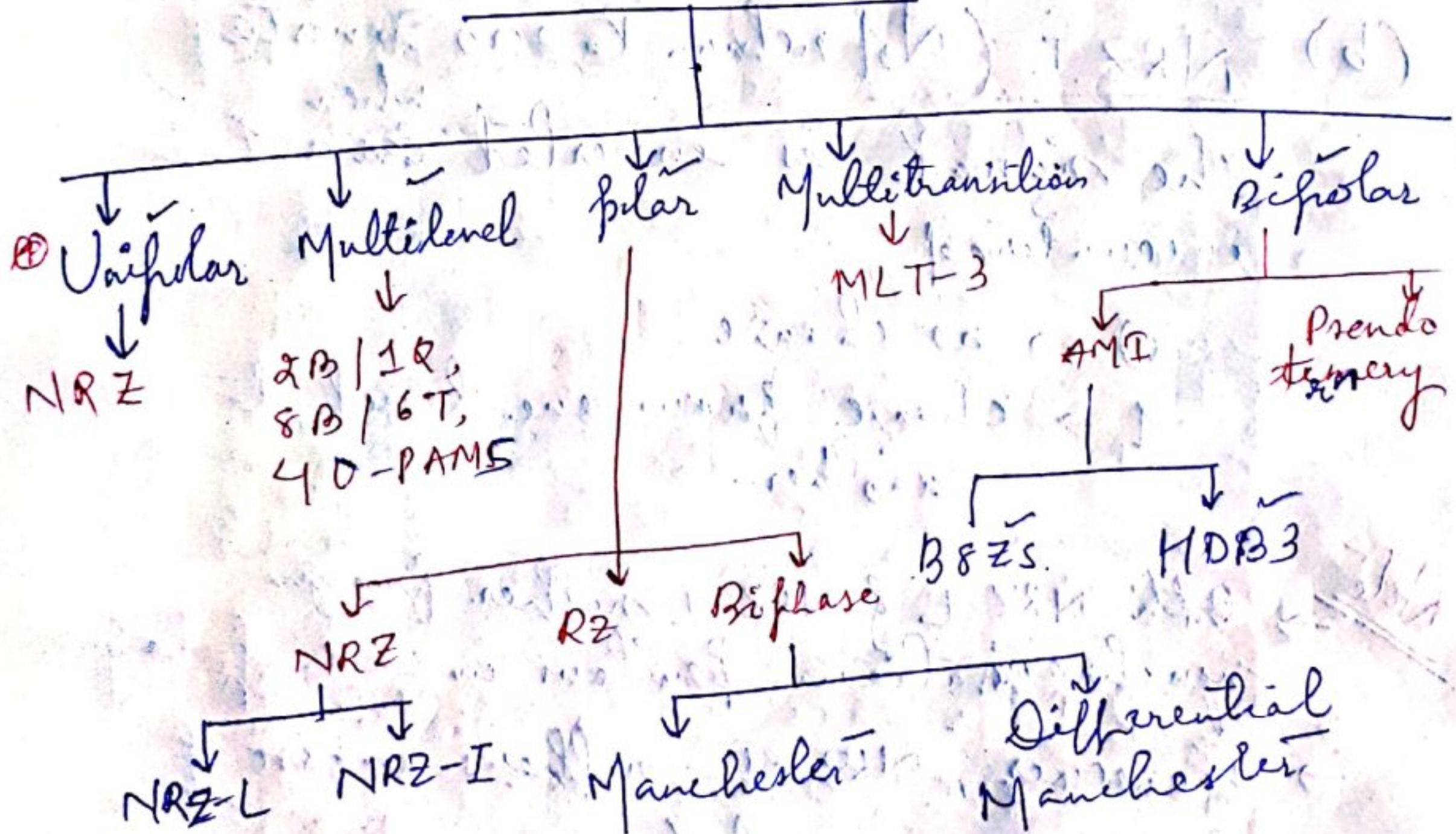


Line coding

→ The line coding is defined as a process of converting the digital data as a sequence of bits to the form of digital signal.



Line coding



① Unipolar

→ Traditionally, a unipolar scheme was designed as a non-return to zero as a NRZ.

→ '1' was defined as positive voltage and '0' was defined as zero voltage.

0 → +ve
1 → -ve

② Polar

→ In polar, it will use two voltage level one is positive & another is negative.

NRZ $0 \rightarrow +ve$
 $1 \rightarrow -ve$

(a) NRZ-L (Not return to zero level)

The level of the signal depends upon the state of the bit i.e.

$0 \rightarrow +ve$

$1 \rightarrow -ve$

(b) NRZ-I (Not return to zero inverted)

The signal is inverted ^{when} a 1 is encountered.

$0 \rightarrow$ no change

$1 \rightarrow$ change from one level to another.

Note

→ Both NRZ-L & NRZ-I suffer from synchronisation problem in case of long 0.

→ However, NRZ-I suffers in case of long sequence of 1.

→ In addition, both NRZ-L & NRZ-I have DC component problem.

RZ (Return to zero)

→ This scheme solves the synchronisation problem of NRZ scheme.

→ It uses 3 values of voltage i.e. +ve, 0 & -ve.

- There is no DC component problem in RZ encoding scheme.
- In this scheme, '1' bit could be represented by the positive to 0 transition through mid-way.
- '0' bit could be represented by the negative to 0 transition through mid-way.

1 → +ve to 0 through mid-way



0 → -ve to 0 through mid-way




Biphase

- It combines the idea of RZ and NRZ-L scheme.

- The transition is always in the middle of interval.

(a) Manchester

- In Manchester, this is a biphase scheme that contains the idea of RZ & NRZ-L scheme.

- In this scheme, the level of voltage changes at the middle of the bit to provide the synchronization.
- The low-to-high transition in the middle of bit indicates 1.



→ The high-to-low transition encoding '0' and this scheme overcomes the disadvantages of NRZ-L.

(b) Differential Manchester

→ This is also a biphasic scheme, it combines the idea of RZ and NRZ-L scheme.

→ It is similar to Manchester scheme, i.e. it changes during the middle of the bit but only the difference is that the bit values are determined at starting of the bit.

→ The transition and beginning of the interval occurs, when the next bit is 0 otherwise there is no transition at the beginning of the interval.

(3) Bipolar

→ In Bipolar encoding, we use 3 levels i.e., +ve, 0 and -ve.

→ This is similar to RZ coding i.e. having 3 voltage levels, the only difference is that 0-bit is represented by 0 level and 1 bit is represented by either +ve or -ve level of voltage.

(a) AMI (Alternative Mark Inversion) :-

0 $\rightarrow$ neutral, 0 voltage

1 $\rightarrow$ +ve, -ve alternately

(b) Pseudo Ternary :-

1 $\rightarrow$ 0 voltage

0 $\rightarrow$ +ve/-ve alternately

Scrambling

$\rightarrow$ In the bipolar scheme, that are suitable for dedicated links & in a LAN, it is not suitable for long distance communication because of their wide bandwidth requirements.

$\rightarrow$ So we are looking for a solution that substitute long zero level pulses with a combination of other level to provide synchronisation and the solution is called scrambling.

$\rightarrow$ The two common scrambling techniques are :-

1. B8ZS

2. HDB3

1. B8ZS

$\rightarrow$ Binary 8 zero substitution.

Bipolar 8 zero substitution.

$\rightarrow$ Whenever 8 consecutive zeros are transmitted into a signal, it inserts two successive ones of the same voltage

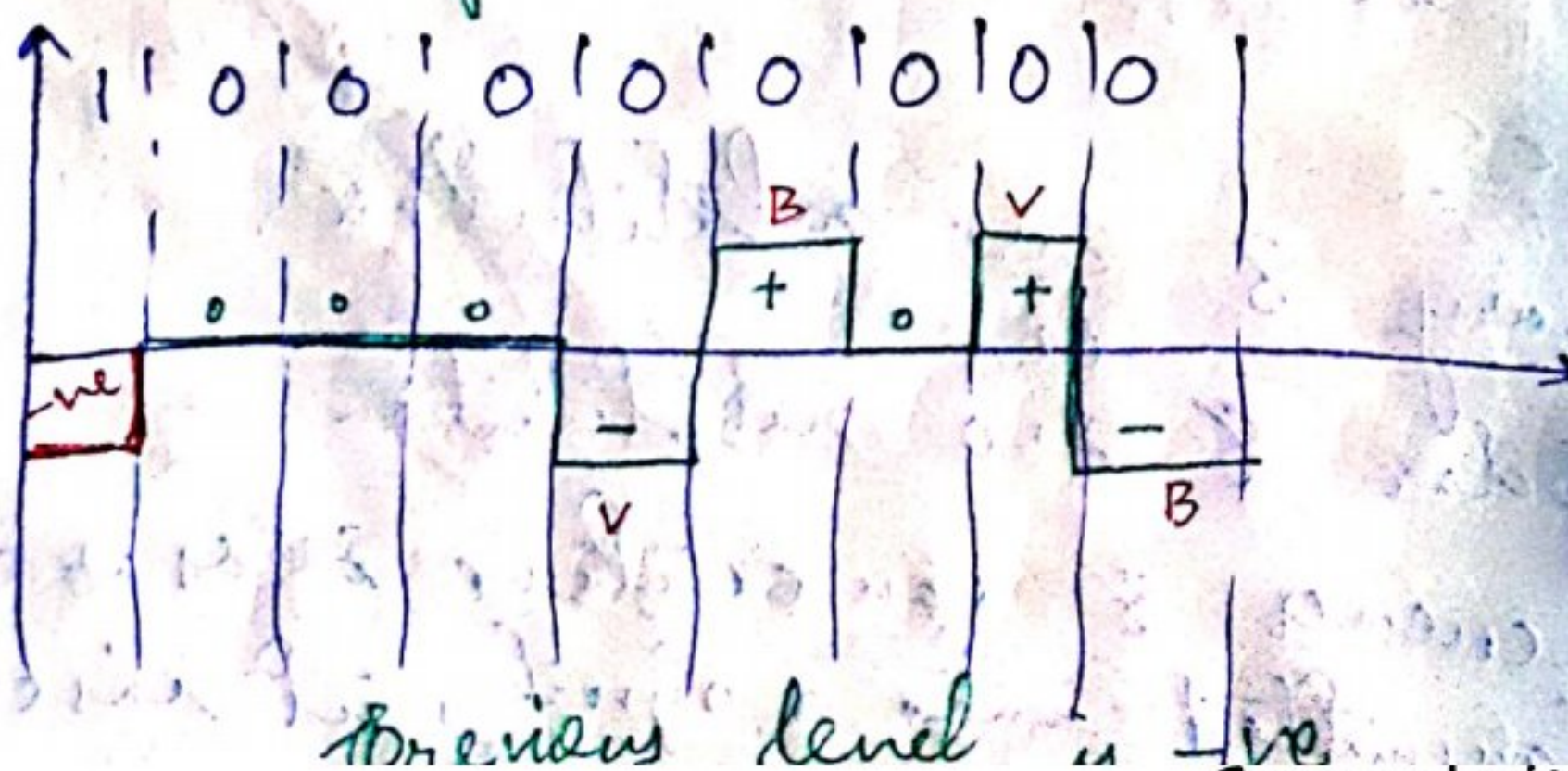
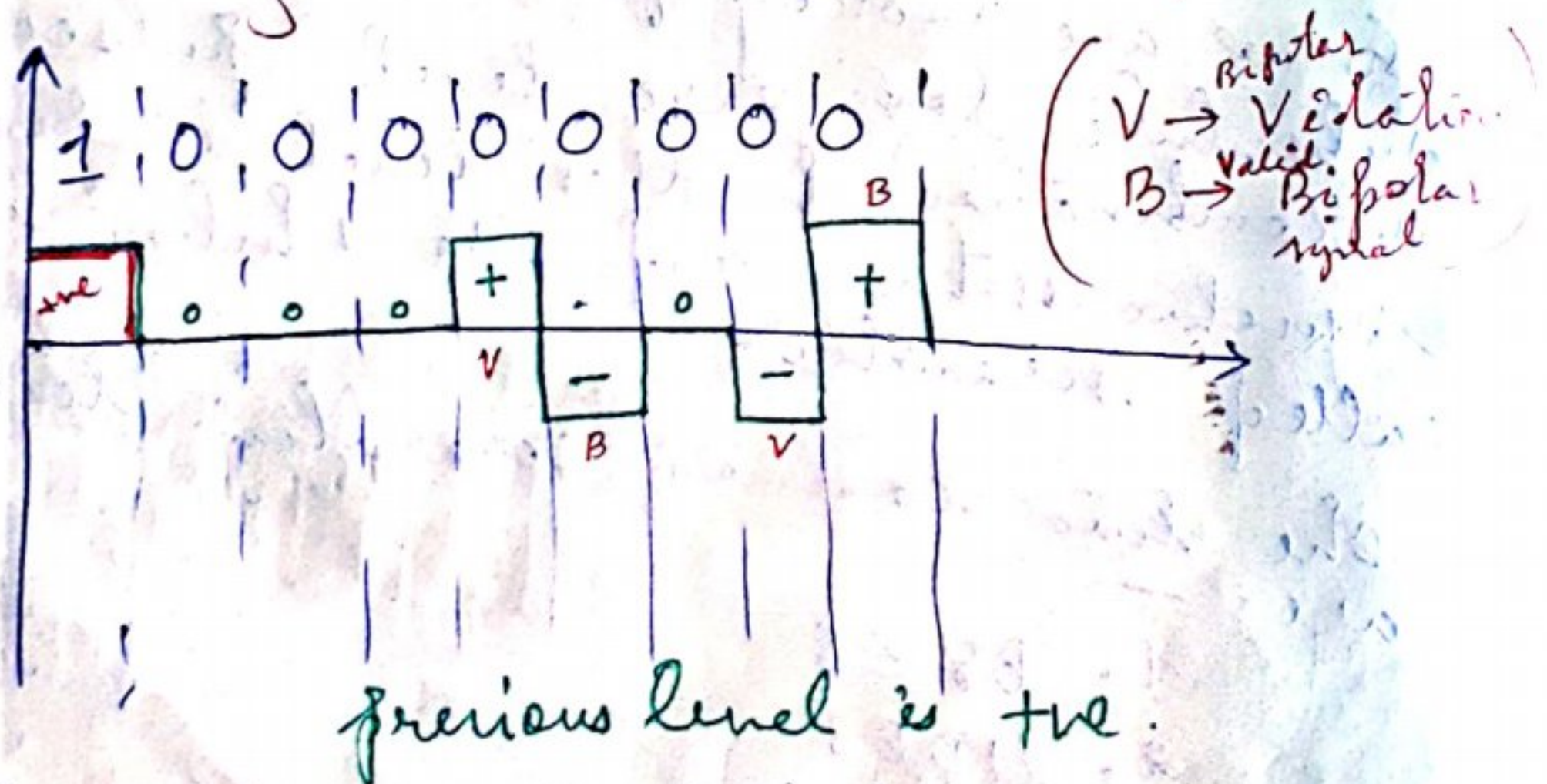
referred to as a bipolar violation.

Run Encoding rule

(i) A sequence of eight 0's are replaced by $000 + - 0 - +$ if the previous pulse is positive.

(ii) A sequence of eight 0's is replaced by $000 - + 0 + -$ if the previous pulse is negative.

Note → such bit pattern is known to both transmitting & receiving multiplexers. The receiving multiplexer can restore the original 00000000 bit pattern.



2. HDB3

- High Density Binary 3 zeros.
- It introduces changes into the bipolar AMI pattern every time 4 consecutive 0s are encountered.
- It is based on the polarity of the previous 1 bit. It also looks at the number of 1s that have occurred in the bit stream since the last substitution.

Encoding rule

(i)

+	0	0	0	0
---	---	---	---	---



+	0	0	0	+
---	---	---	---	---

-	0	0	0	0
---	---	---	---	---



-	0	0	0	-
---	---	---	---	---

- If the number of 1s since the last substitution is odd.

(ii) If the number of 1s since the last substitution is even.

+	0	0	0	0
---	---	---	---	---



+	-	0	0	-
---	---	---	---	---

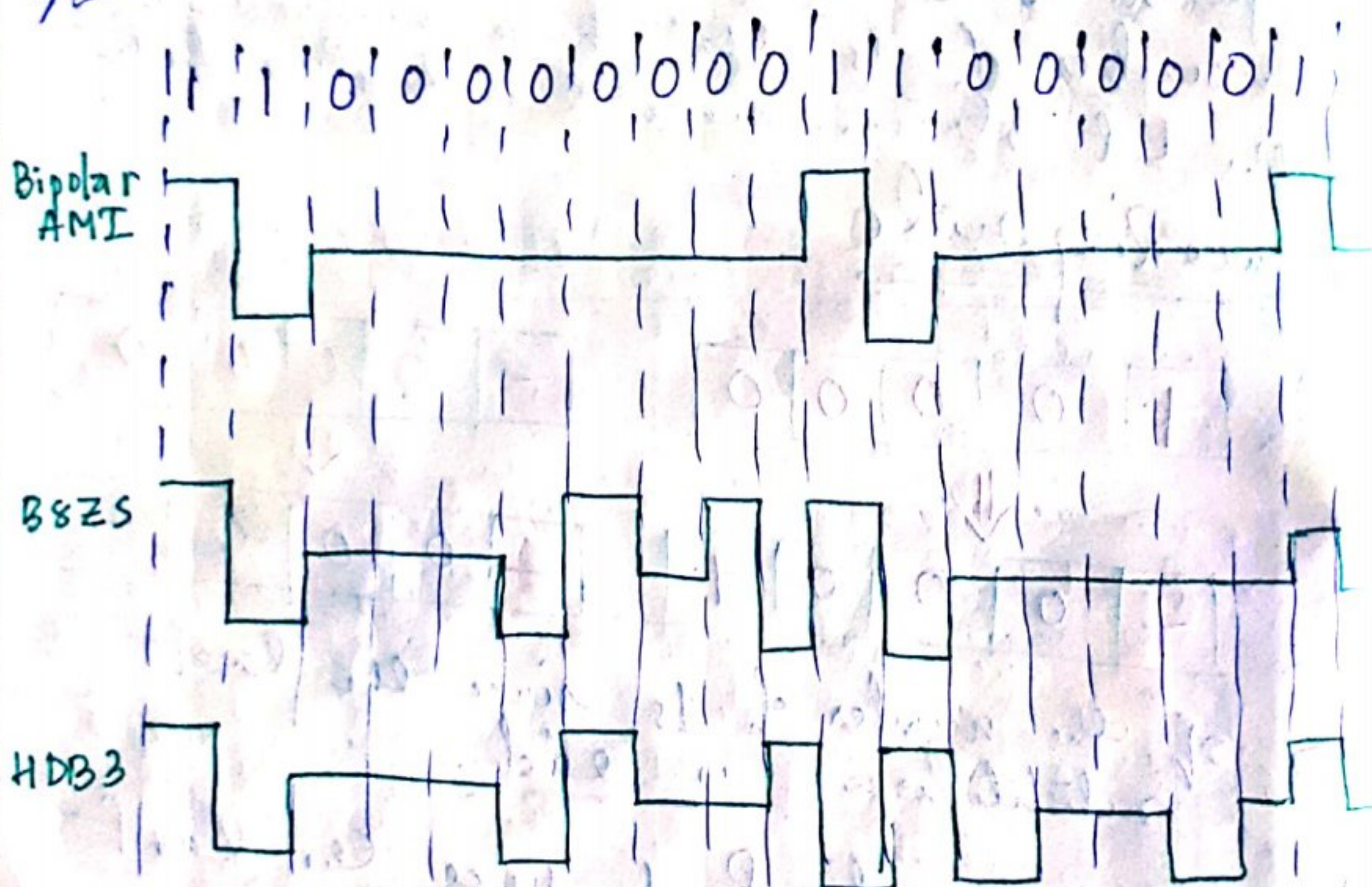
-	0	0	0	0
---	---	---	---	---



-	+	0	0	+
---	---	---	---	---

	<u>ODD 1's</u>	<u>EVEN 1's</u>
+ve -ve	000-	+ 00 +
+ve	000+	- 00 -

Ex

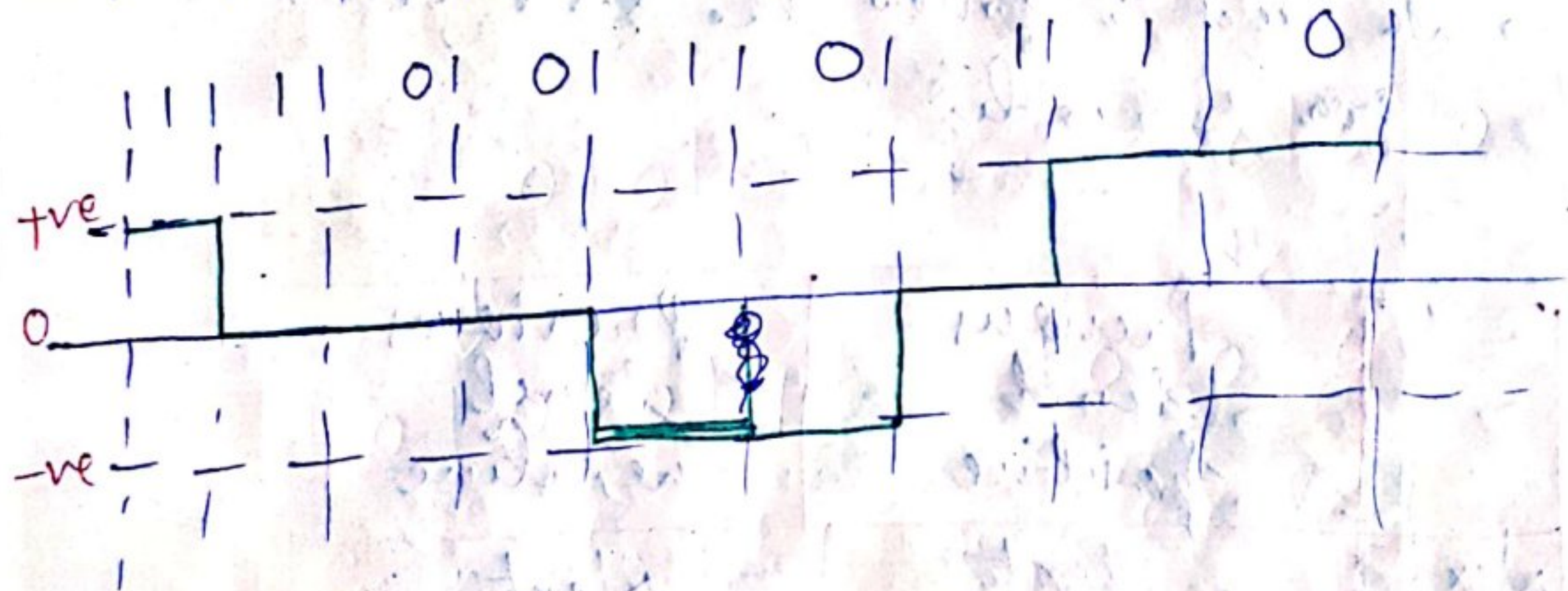


(4) Multilevel MLT-3

- It uses 3 levels of voltages +ve, 0 & -ve.
- For the 1st bit, 0 will be represented by 0
1 will be represented by 1
- Then the voltage level of 0 depends on 1
- 1st '1' should be +ve.
- 2nd '1' " " neutral.

→ And again '1' will become -ve and this process will reverse after 3 steps if '1' are encountered and will continue.

Ex-1



Ex-3

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

hint For 1st most bit '0' → 0 voltage
 " " " " '1' → +ve voltage
 " " " " '1' → +ve voltage
 Then other zero values '0' → depends on the level.
 " " " " '1' values will continue as
 + 0 - 0 + 0 - ...
 so on

2B/1Q (~~2B~~ Two-Binary,
One-quaternary)

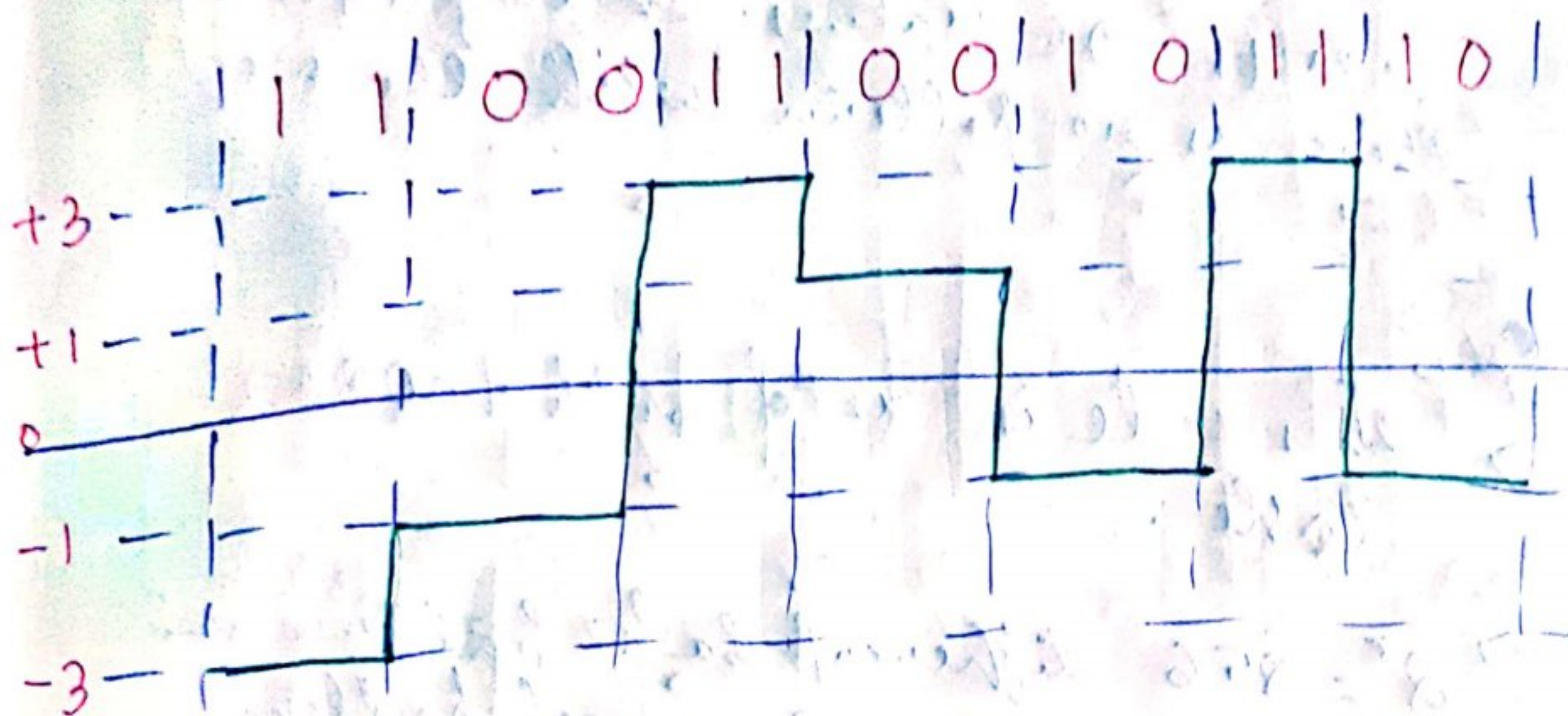
→ In this line coding scheme, a block of two binary bits can represent four different values: 00, 01, 10, 11

→ These four values are mapped to one quaternary value which is encoded using four different voltages i.e. (+3, +1, -1, -3)

→ We need to follow the table given below for encoding:-

	Previous level positive	Previous level negative
Next bit-	Next level	Next level
00	+1	-1
01	+3	-3
10	-1	+1
11	-3	+3

Ex- data $\rightarrow$ 11001100101110



Ex- data $\rightarrow$ 1001100



8B/6T (Eight Binary, Six ternary)

$\rightarrow$ The idea is to encode a pattern of 8 bits (ex. 00010001) as a pattern of 6 signals, where the signal has three levels (-1, 0, +1).

Ques → Each signal pattern has a weight of 0 or +1 DC values. It implies that there is no pattern with the weight -1.

Ans → This code is used with 100BASE-4T cable.

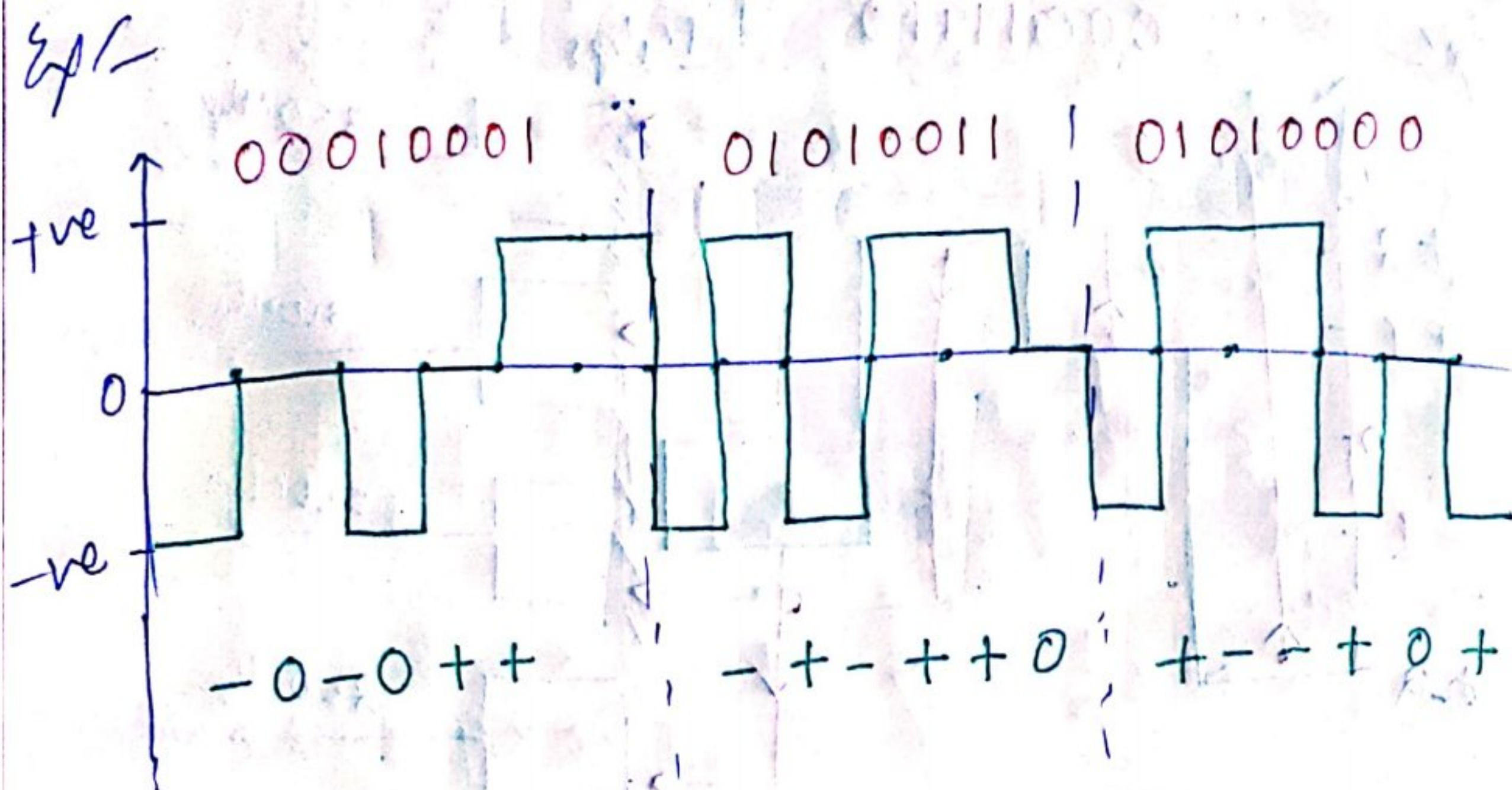
→ $2^8 = 256$ different data patterns and $3^6 = 478$ different signal patterns.

→ there are $478 - 256 = 222$ redundant signal elements that provide synchronisation & error detection.

→ $\begin{matrix} + & \rightarrow & \text{positive signal} \\ - & \rightarrow & \text{negative signal} \\ 0 & \rightarrow & \text{lack of signal} \end{matrix} \left. \vphantom{\begin{matrix} + \\ - \\ 0 \end{matrix}} \right\} \text{notations.}$

→ To make whole stream DC-balanced, the sender keeps track of the weight of two groups of weight '1' are encountered one after another, the first one is sent as it is, while the next one is totally inverted to give a weight of -1.

→ For each 8 bit pattern, the signal code is fixed already.



4D-PAM5

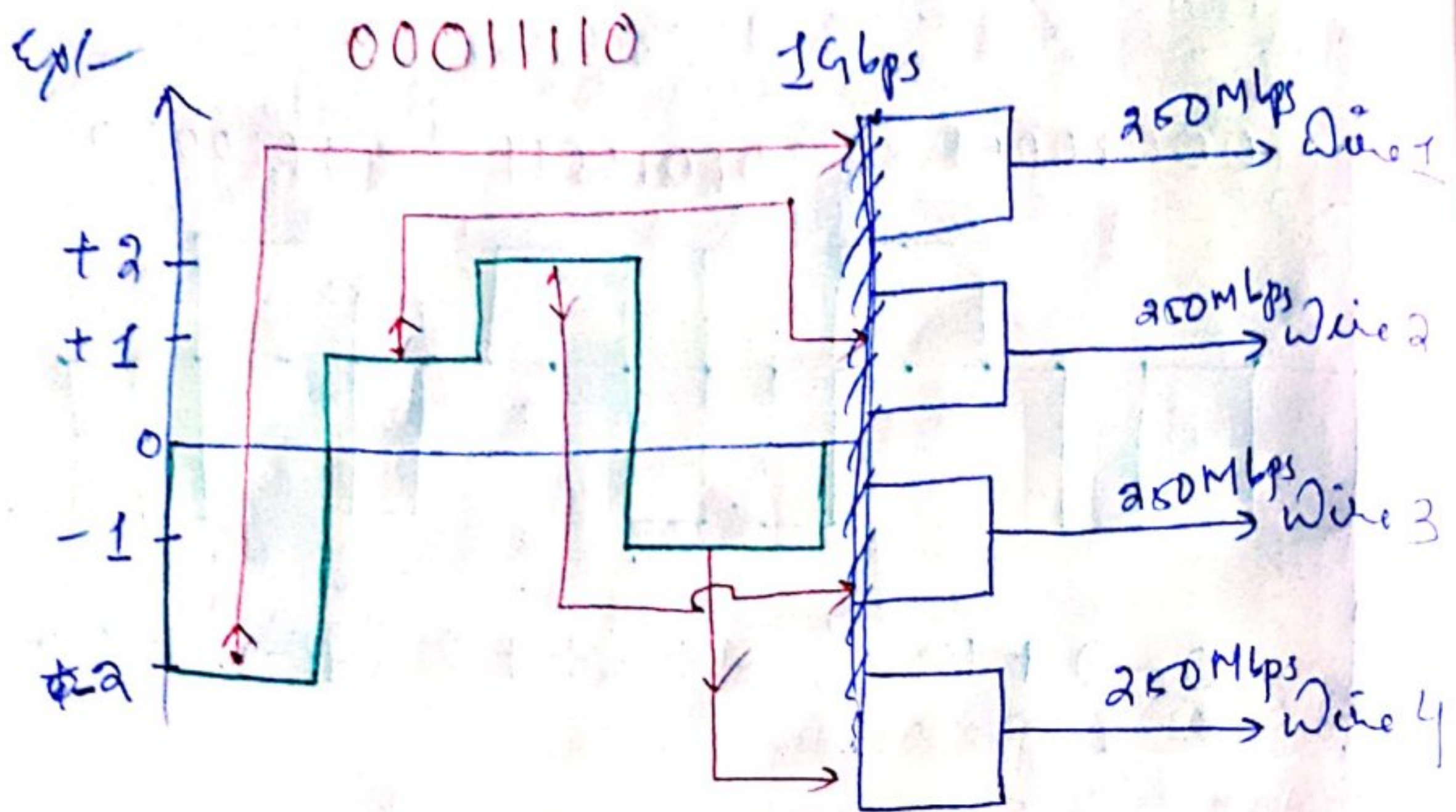
(Four Dimensional Five-Level Pulse Amplitude Modulation)

→ It uses five voltages such as -2, -1, 0, 1, 2.

→ 4D means that the data is transmitted over four channels at the same time.

→ All bits can be applied into a channel simultaneously and sent by using one signal element.

→ Gigabit LANs use this technology to send 1 Gbps over copper wires.



→ Voltage '0' is not used here. If it is used for forward error correction,

3.3 Digital Data Analog Signal

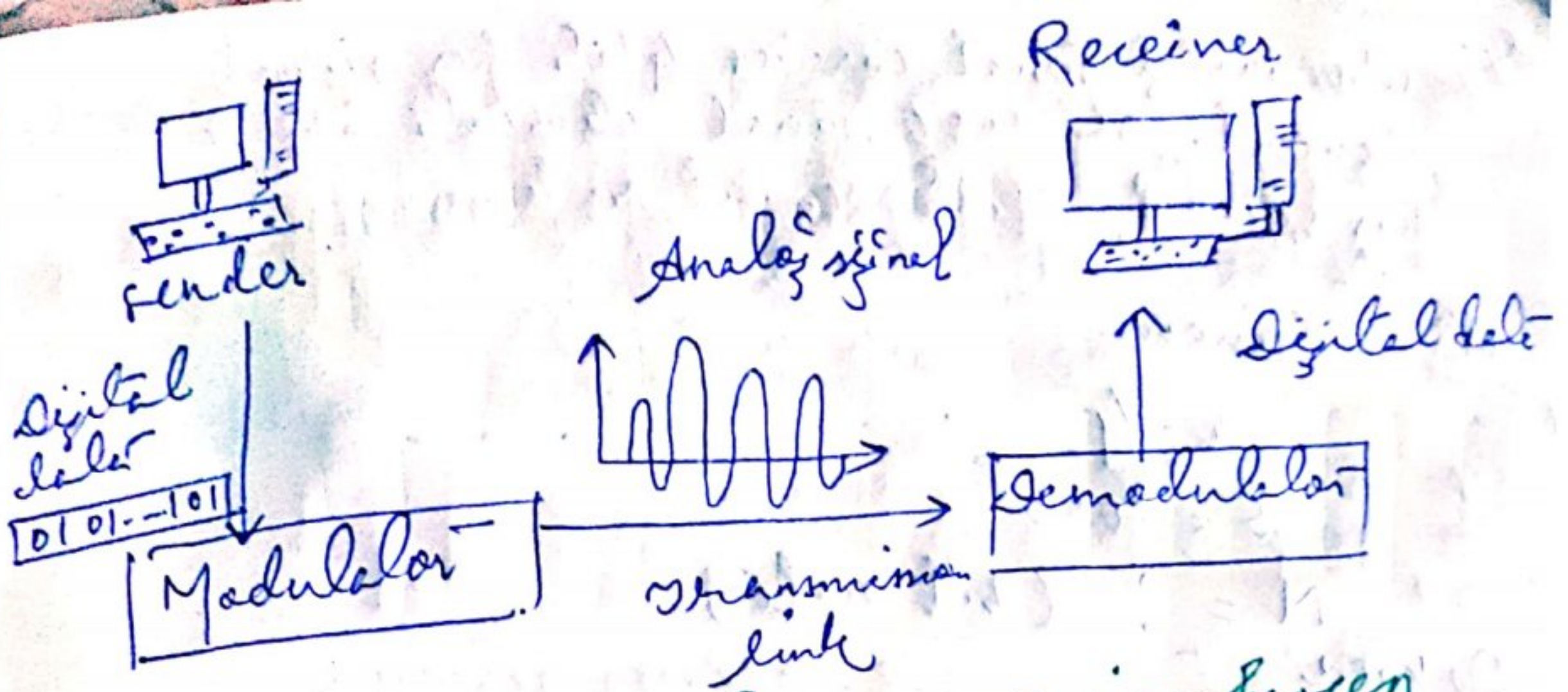
Digital to Analog Conversion : -

It is the process of changing one of the characteristic of an analog signal based on the information in digital data.

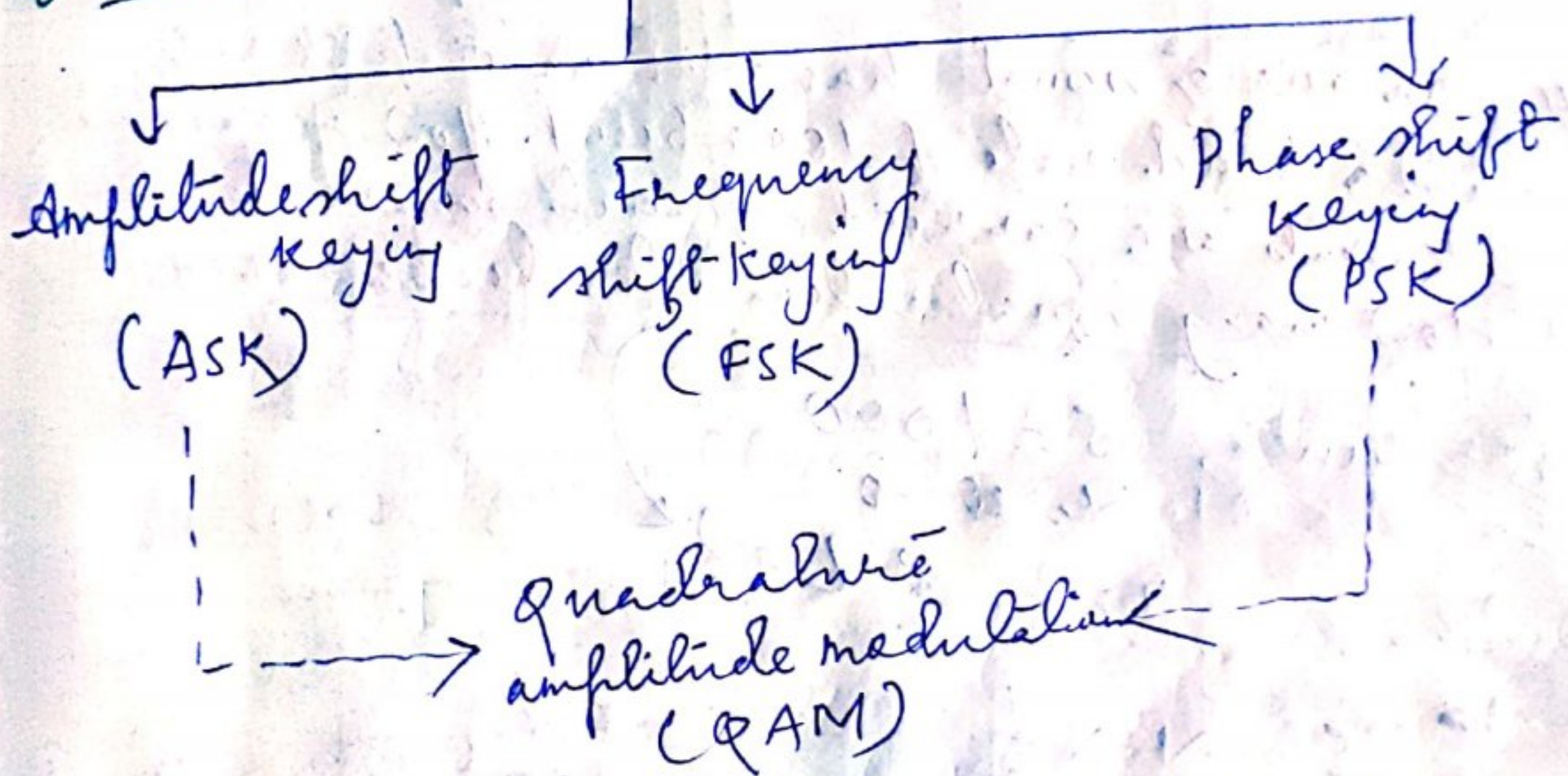
→ Here digital data needs to be carried on an analog ~~data~~ signal.

→ A carrier signal frequency (f_c) performs the function of transporting the digital data in an analog waveform.

→ The analog carrier signal is manipulated to uniquely identify the digital data being carried.



Types of digital to analog conversion process



Note

• $N \rightarrow$ Bit rate - i.e. the number of bits per second (bps).

Band rate is the number of signal elements per second. (bands).

• In the analog transmission of digital data, the signal or band rate is less than or equal to the bit rate.

$$S = N \times 1/r \text{ bands}$$

where 'r' is the number of data bits per signal element.

Ex. An analog signal carries 4 bits per signal element. If 1000 signal elements are sent per second, find the bit rate.

Soln

Given,

$$r = 4$$

$$S = 1000$$

$$N = ? \text{ (bit rate)}$$

We know,

$$S = N \times \frac{1}{r}$$

$$\Rightarrow N = S \times r = 1000 \times 4 = 4000 \text{ bps}$$

Ex. An analog signal has a bit rate of 8000 bps and a band rate of 1000 baud. How many data elements are carried by each signal element? How many signal elements do we need?

Soln

Given, $S = 1000$

$$N = 8000$$

$$r = ? \text{ and } L = ?$$

$$S = N \times \frac{1}{r}$$

$$\Rightarrow r = \frac{N}{S} = \frac{8000}{1000} = 8 \text{ bits/ baud}$$

$$L = 2^r = 2^8 = 256$$

$$\Rightarrow r = \log_2 L$$

Amplitude shift Keying (ASK)

- ASK is implemented by changing the amplitude of a carrier signal to reflect amplitude levels in the digital signal.
- For example: a digital '1' could not affect the signal whereas a digital '0' would, by making it zero.
- The line coding will determine the values of the analog waveform to reflect the digital data being carried.

Bandwidth of ASK

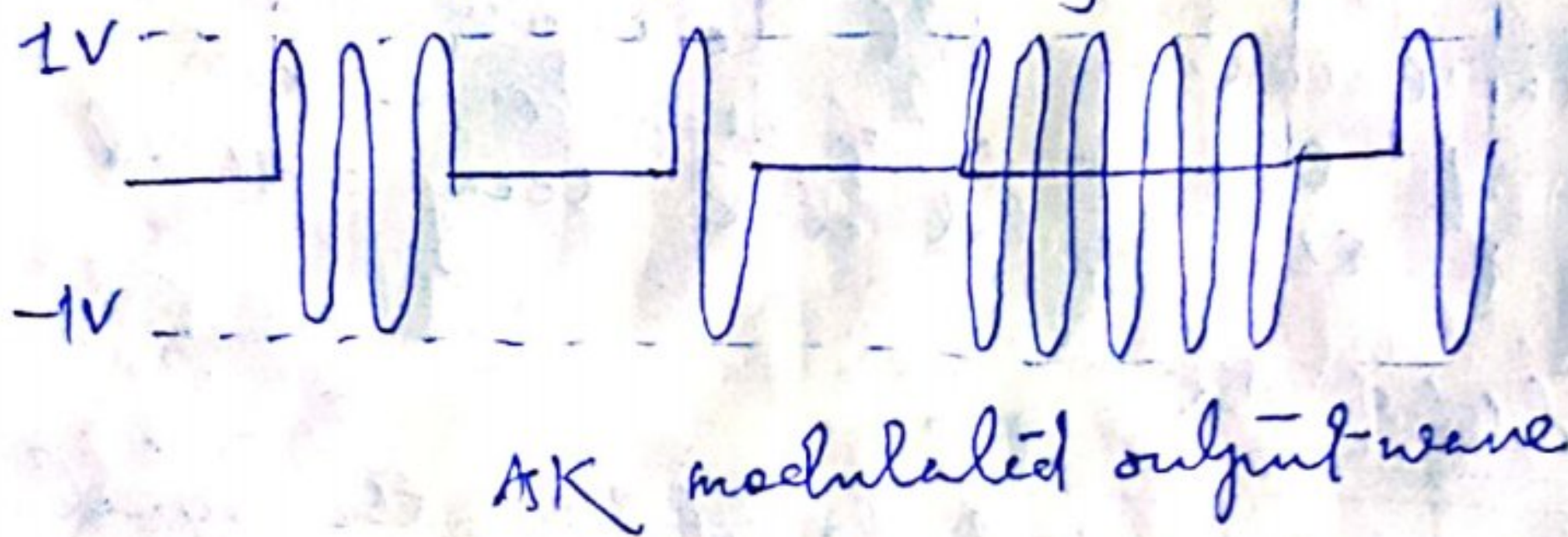
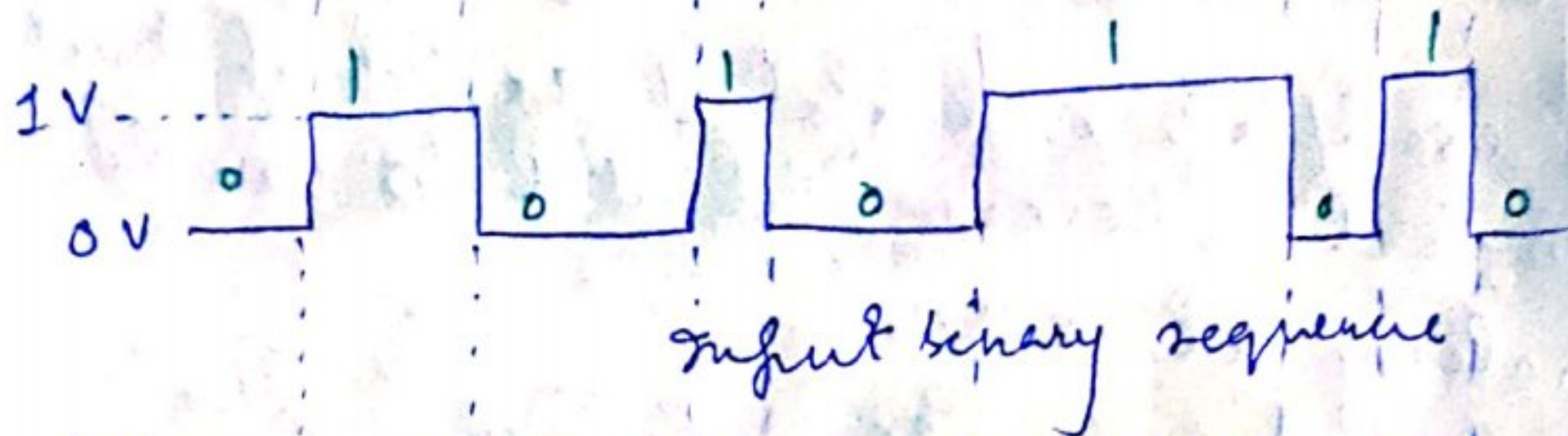
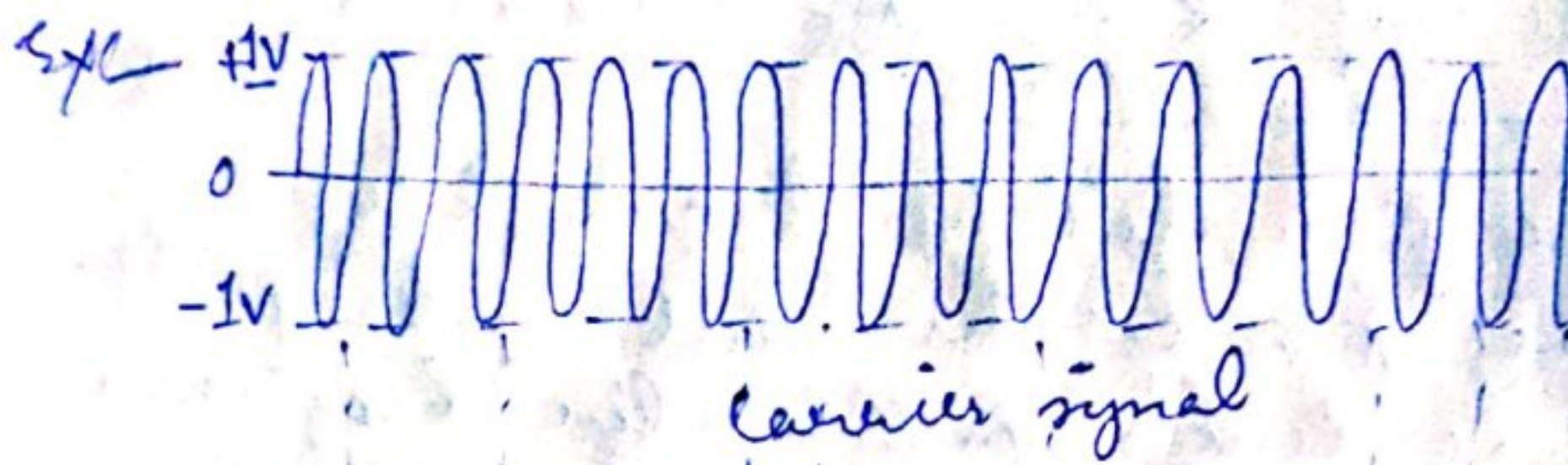
- BW of ASK is proportional to the signal rate S .

$$BW = (1+d)S$$

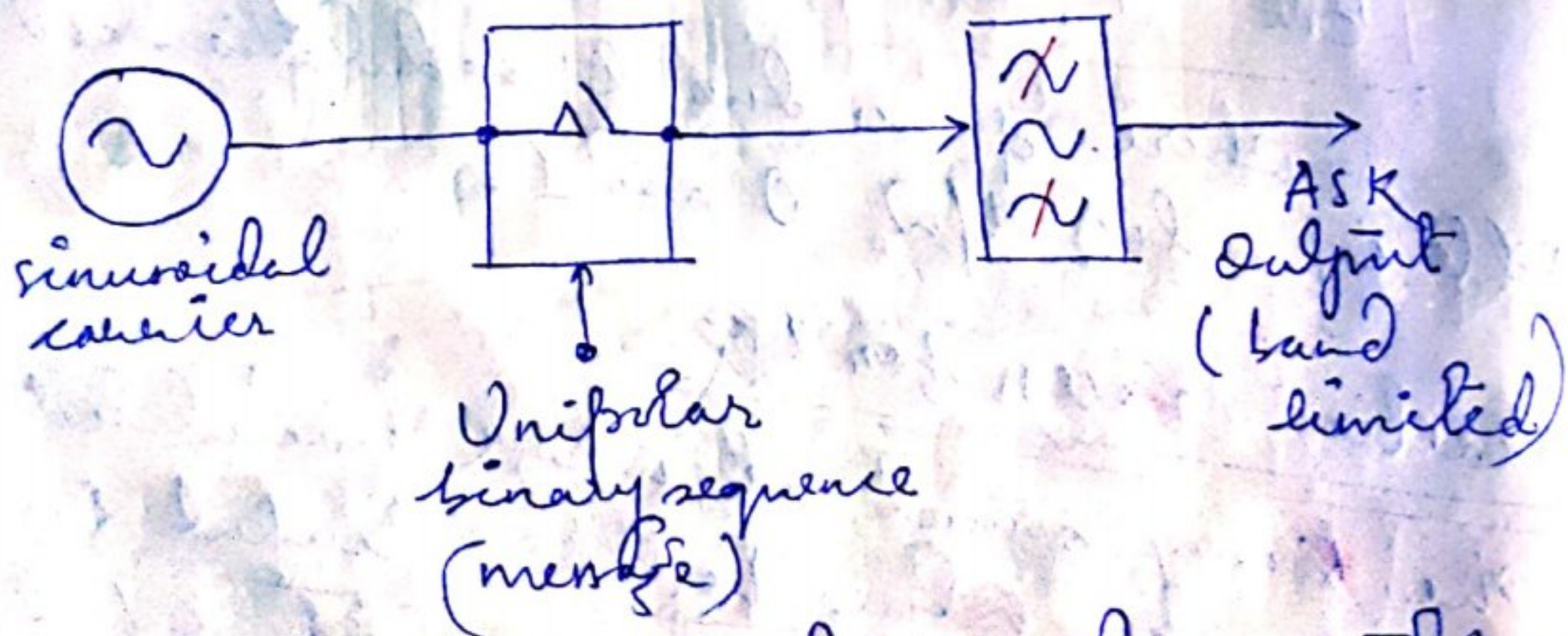
where 'd' is due to modulation and filtering, lies b/w 0 and 1.

Encoding Process for ASK

- The binary signal when ASK modulated gives a zero value for low input & gives carrier output for high input.
- 1st carrier signal
then digital data
then ASK signal is the modulated signal.



Ex 2 ASK Modulator



- The carrier generator, sends a continuous high frequency carrier. The binary sequence from the message signal takes the unipolar output either High or Low.
- The high signal closes the switch, allowing a carrier wave.

Hence, the output will be the carrier signal at high input.

→ when there is low input, the switch opens, allowing no voltage to appear. Hence the output will be low.

ex
We have an available bandwidth of 100 KHz which spans from 200 to 300 KHz. What are the carrier frequency and the bit rate if we modulated our data by using ASK with $d=1$?

sol Given, $f_c = 250 \text{ KHz}$

$$d=1, r=1$$

$$B = (1+d)S = 2 \times N \times \frac{1}{r} = 2 \times N = 100 \text{ KHz}$$

$$\Rightarrow N = 50 \text{ Kbps}$$

Frequency Shift Keying (FSK)

→ The digital data stream changes the frequency of the carrier signal, f_c .

→ Ex: '1' could be represented by $f_1 = f_c + \Delta f$ and a '0' could be represented by

$$f_2 = f_c - \Delta f.$$

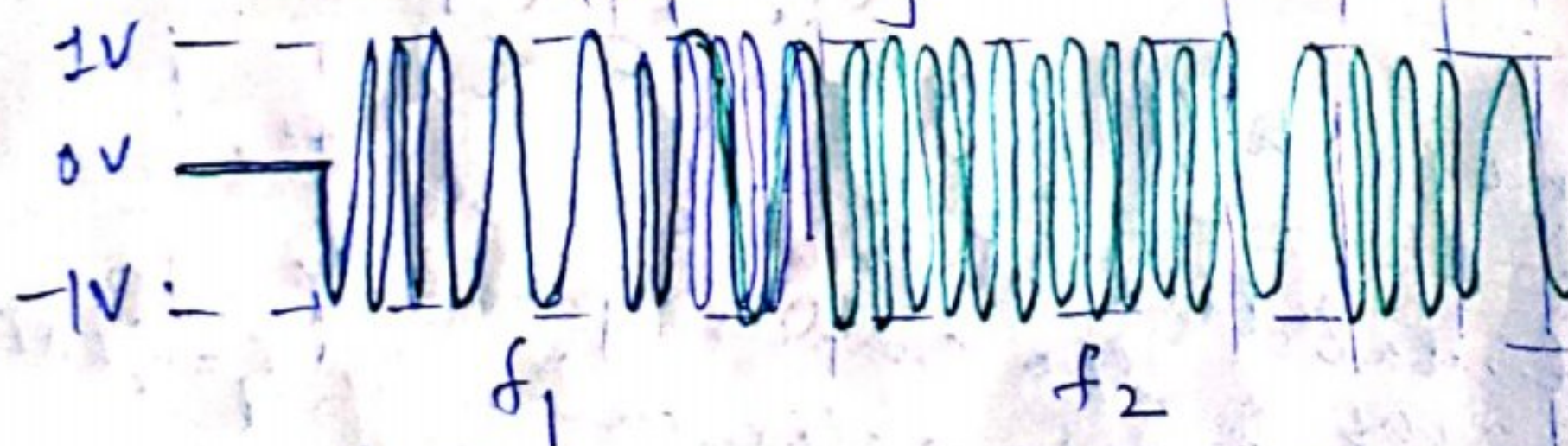
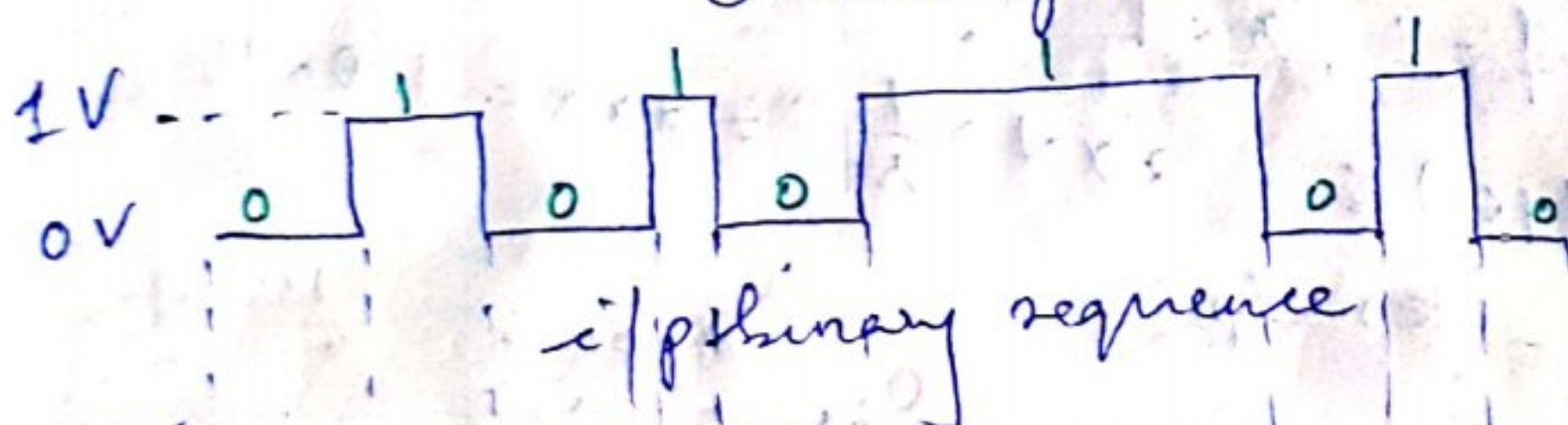
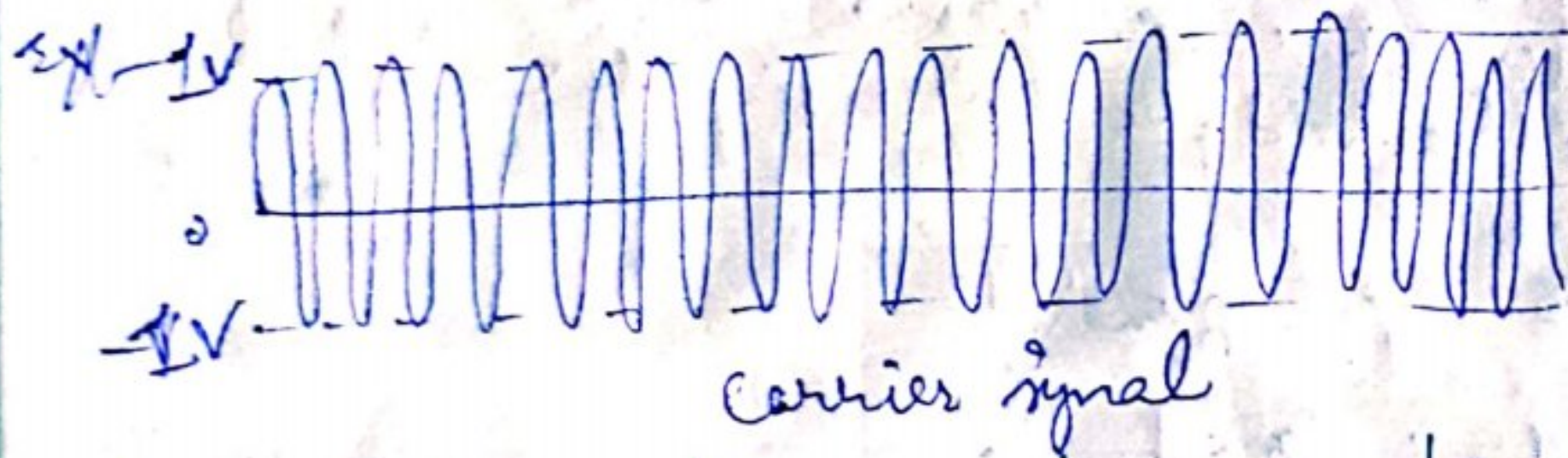
Bandwidth of FSK

→ If the difference b/w the two frequencies (f_1 & f_2) is $2\Delta f$, then the required BW B will be:

$$BW = (1+d)S + 2\Delta f$$

→ Encoding process

- The freq of a FSK modulated wave is high in frequency for a binary High i/p and is low in frequency for a binary low i/p.
- The binary 1s and 0s are called mark & space frequencies.



FSK modulated i/p wave.

Q) We have an available BW of 100 kHz which spans from 200 to 300 kHz. What should be the carrier frequency and the bit rate if we modulated our data by using FSK with $d=1$?

Ans) Midpoint of the band is at 250 kHz.

→ We choose $2\Delta f$ to be 50 kHz.

$$\rightarrow B = (1+d)S + 2\Delta f = 100$$

$$2S = 50 \text{ kHz}$$

$$\rightarrow S = 25 \text{ Kband} \Rightarrow N = 25 \text{ Kbps}$$

$f_1 = 200$
$f_2 = 300 \text{ K}$
$f_c = 250$
$2\Delta f = 50 \text{ K}$

Phase shift keying (PSK)

→ Here we vary the phase shift of the carrier signal to represent digital data.

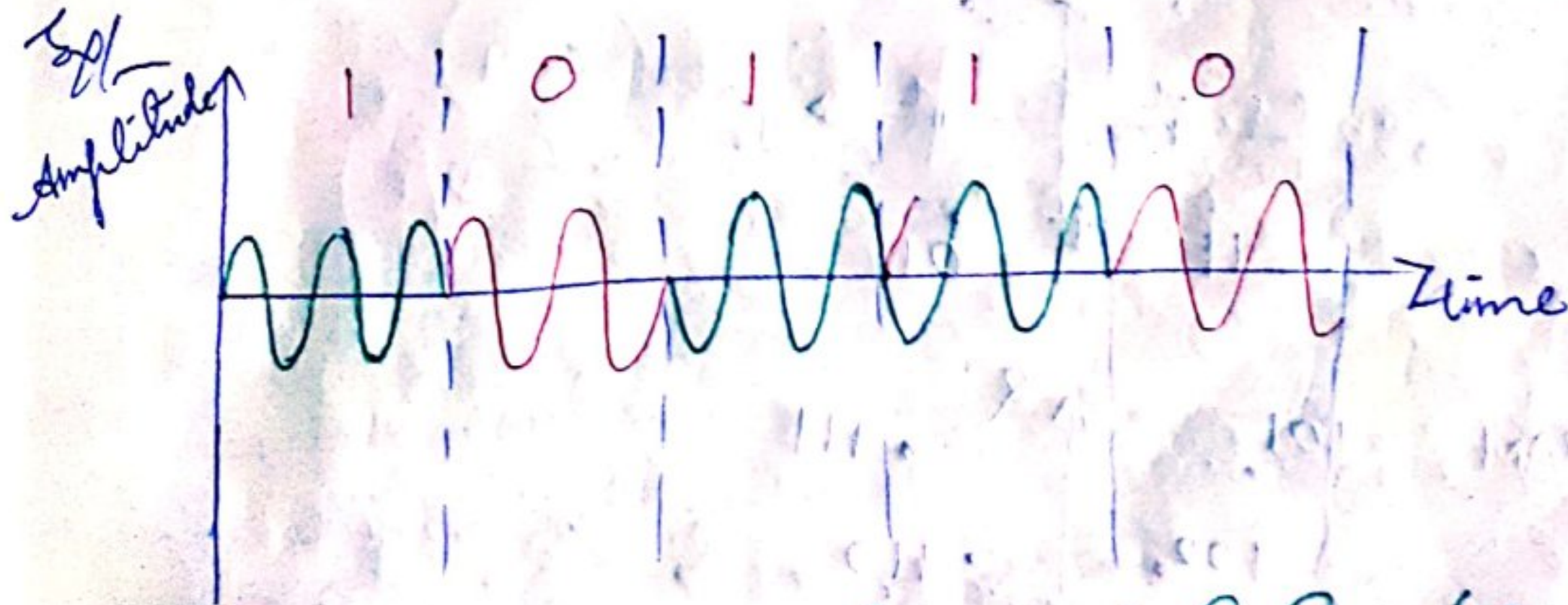
→ $B = (1+d) \times S$
↓
Bandwidth requirement

→ PSK is much more robust than ASK as it is not that vulnerable to noise, which changes amplitude of the signal.

Encoding process

→ For 1 → No change in carrier signal
(both are same)

For 0 → phase changes.



Quadrature Amplitude Modulation (QAM)

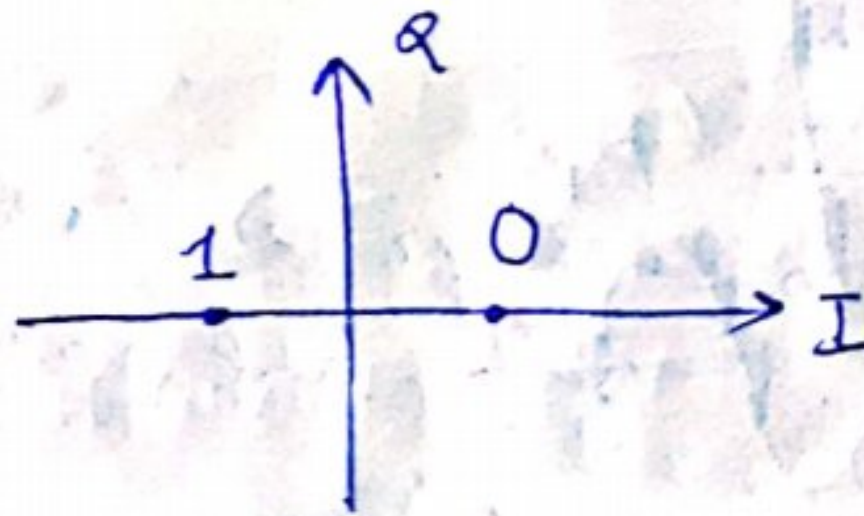
→ Quadrature Amplitude Modulation combines amplitude & phase changes to give additional capacity & is widely used for data communications.

→ QAM is a signal in which two carriers shifted in phase by 90° are modulated and the resultant sp consists of both amplitude & phase variations.

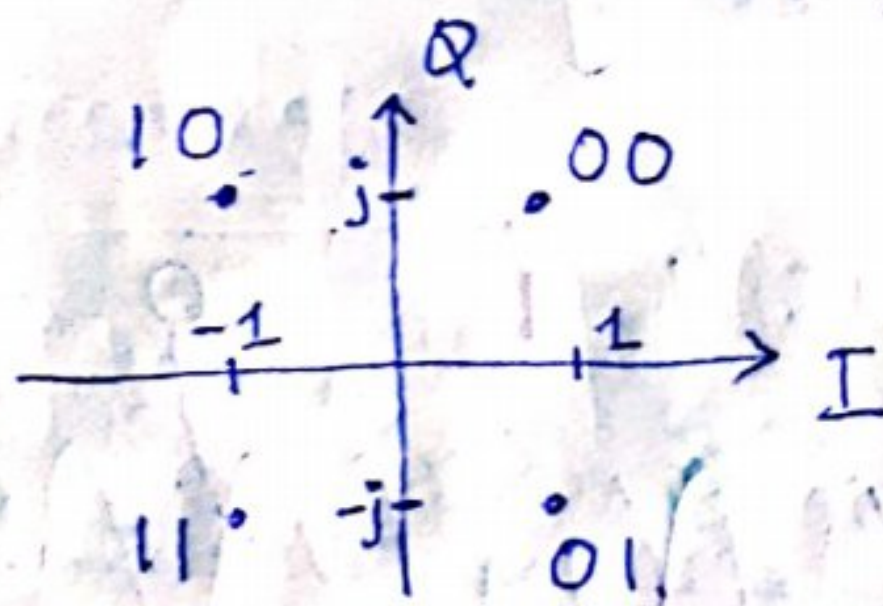
→ ~~QAM is a combination of both~~

Constellation Diagram for QAM

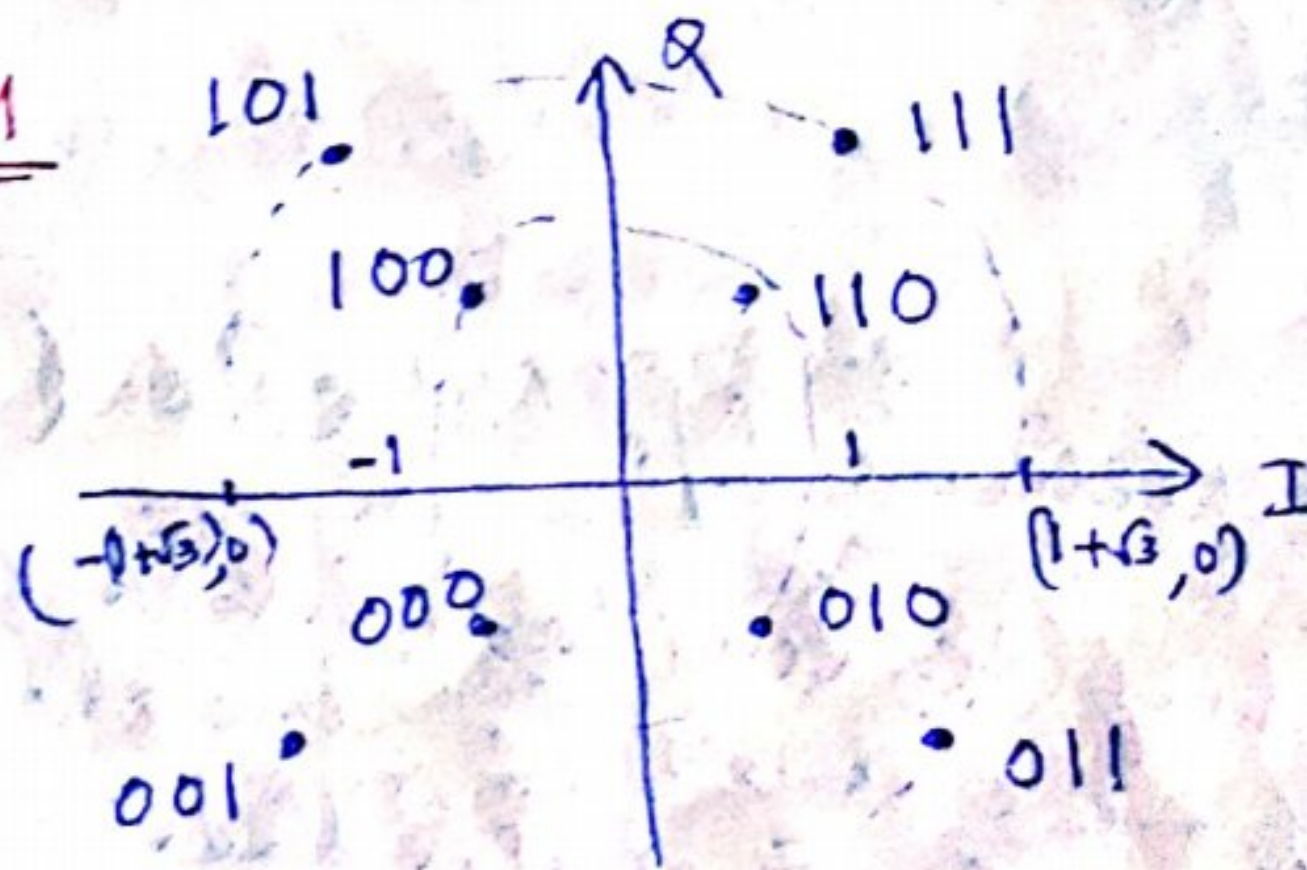
2-QAM



4-QAM

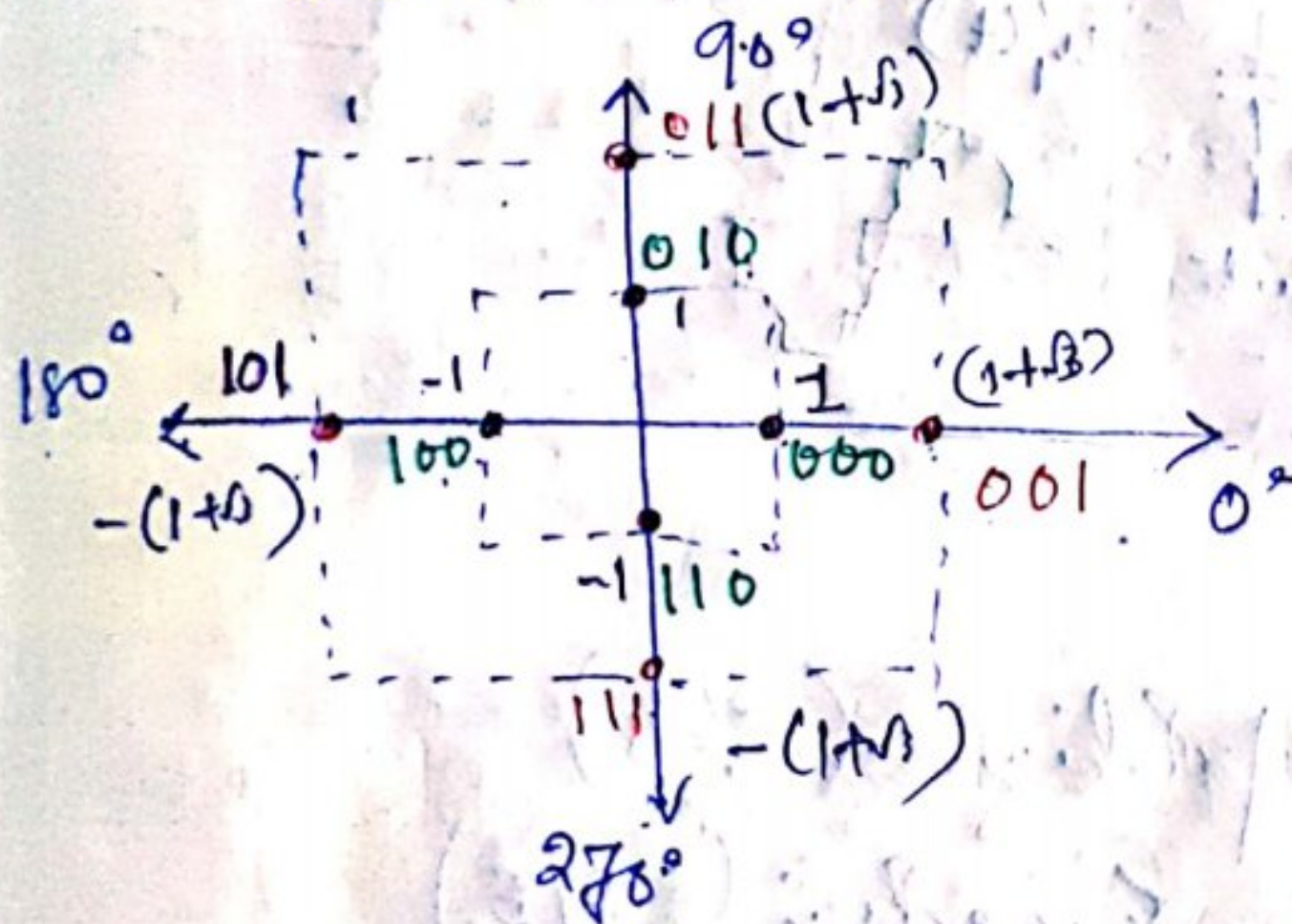


8-QAM





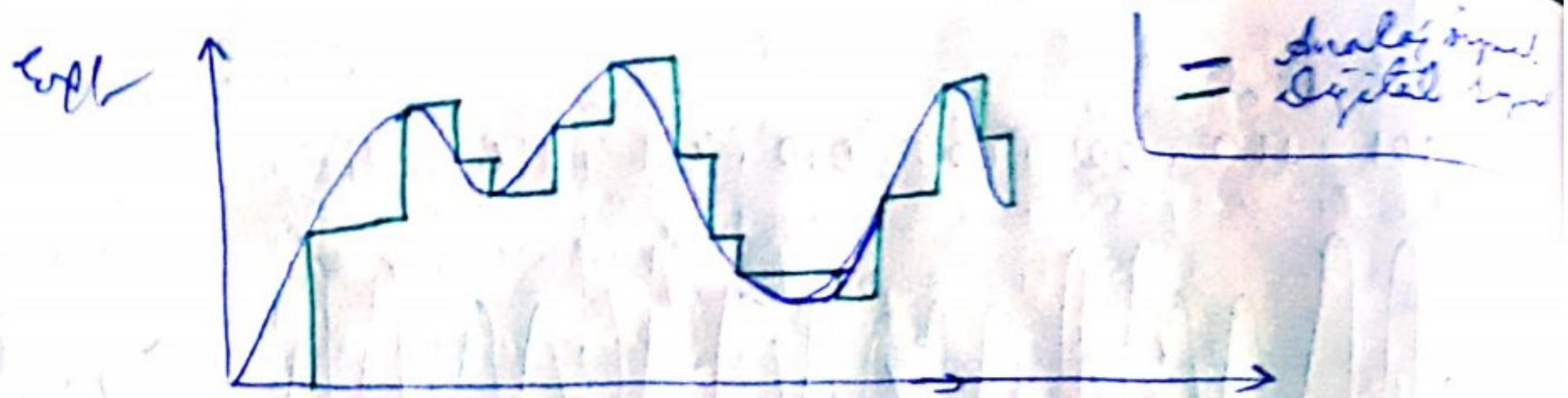
Total $\rightarrow$ Bit rate = 24 bps
 Band rate = 8 bands



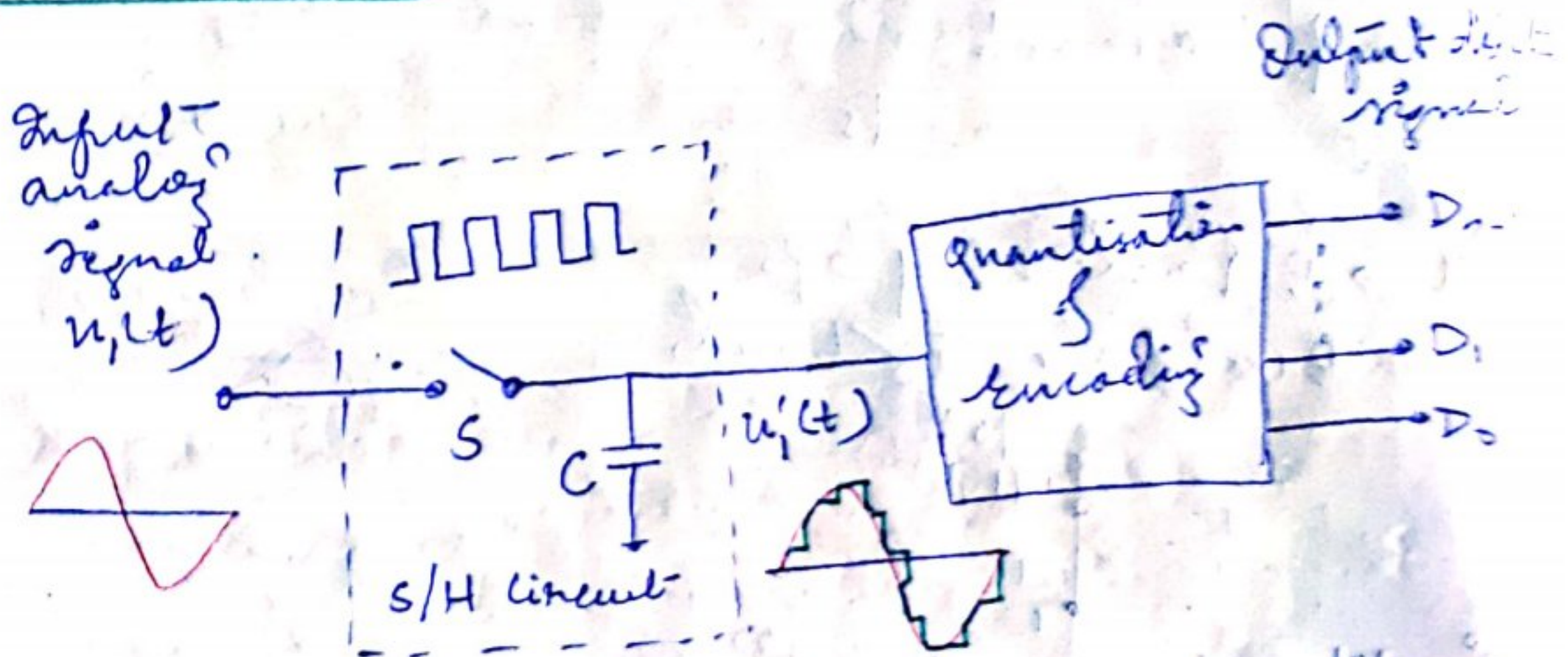
3.4) Analog data digital signal

$\rightarrow$ An analog signal is a continuous signal that contains time-varying quantities such as temperature or speed, with infinite possible values in between.

$\rightarrow$ Even in digital devices, there is typically some analog component that is used to take in information from the external world, which will then get translated into digital form.
 (using an analog-to-digital converter)



ADC Process

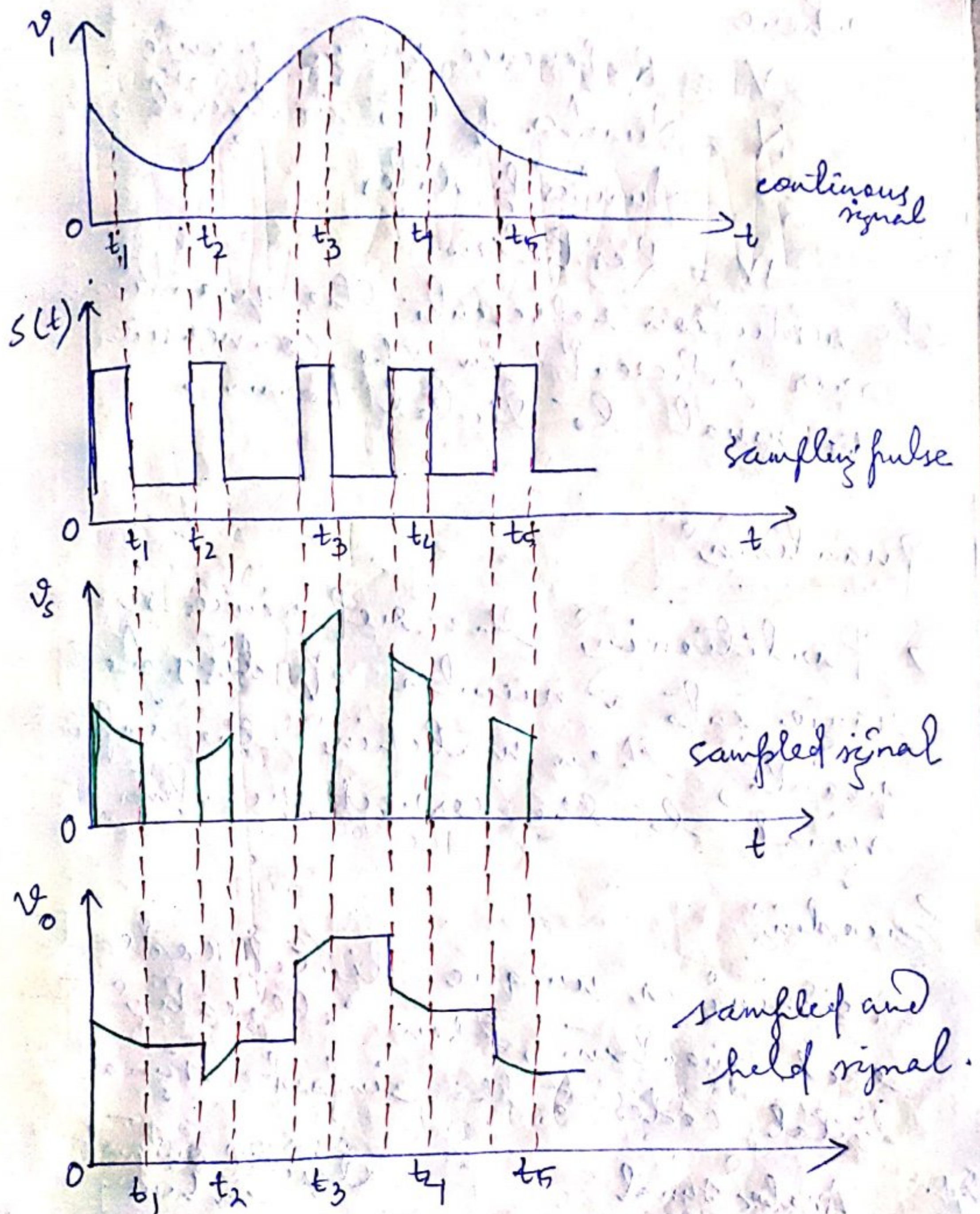


Two process steps

- (i) Sampling & Holding (S/H)
- (ii) Quantisation & Encoding (Q/E)

(i) Sampling & Holding

- Holding signal benefits the accuracy of the A/D conversion.
- Minimum sampling rate should be at least twice the highest data frequency of the analog signal.



(ii) Quantising & Encoding

Resolution: the smallest change in analog signal that will result in a change in the digital output.

$$\Delta V = \frac{V_r}{2^N}$$

where

V = Reference voltage range

N = Number of bits in digital output

2^N = Number of states

ΔV = Resolution

The resolution represents the quantisation error inherent in the conversion of the signal to digital form.

Quantising

→ Partitioning the reference signal range into a number of discrete levels, then matching the input signal to the correct quantum.

Encoding

Assigning a unique digital code to each quantum, then allocating the digital code to the input signal.

Ex

Analog signal

Digital output in binary

7.5	7	7V	111
6.5	6	6V	110
5.5	5	5V	101
4.5	4	4V	100
3.5	3	3V	011
2.5	2	2V	010
1.5	1	1V	001
0.5	0	0V	000

here
 $n = 3$
no. of bits
= 3
4A

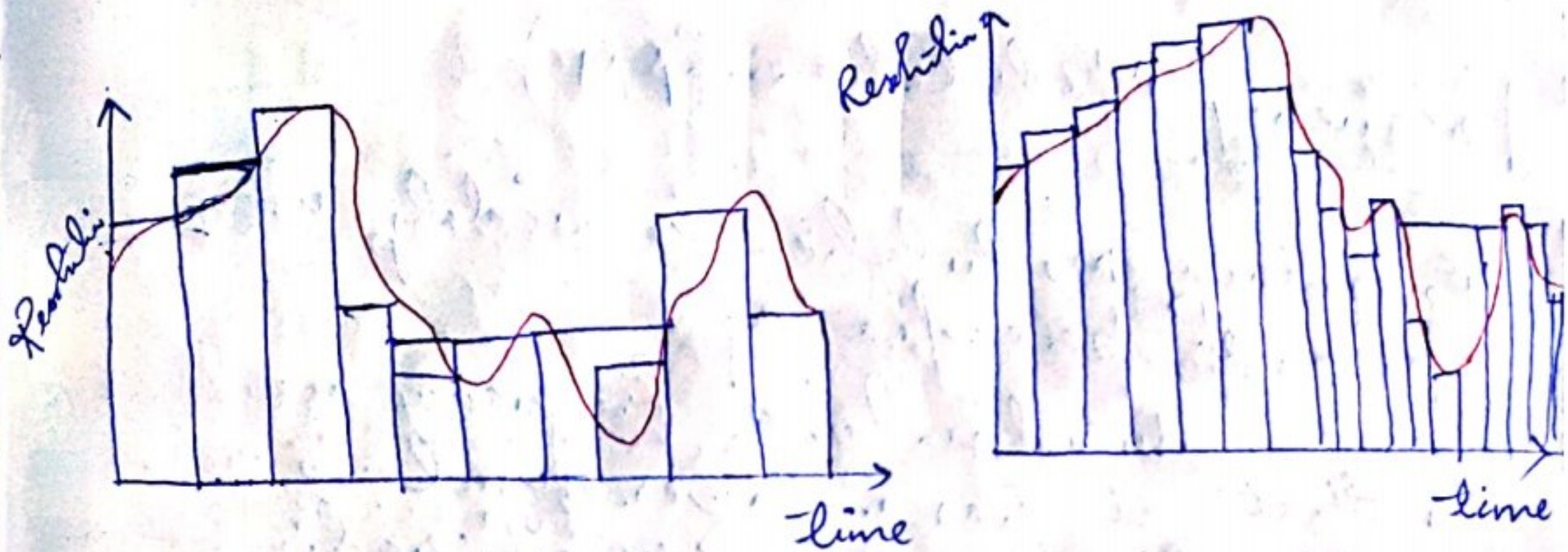
here $\Delta V = 1V$

→ Maximum quantisation error = $\pm \frac{\Delta V}{2} = \pm 0.5V$

Accuracy of A/D Conversion

• Low Accuracy

• High (improved) Accuracy



3.5 Analog Data - Analog signal

- Analog to analog conversion or modulation, is the representation of analog information by an analog signal.
- It is a process by virtue of which a characteristic of carrier wave is varied according to the instantaneous amplitude of the modulating signal.

Need of Modulation

- Modulation allows us to send a signal over a bandpass frequency range. If every signal gets its own frequency range, then we can transmit multiple signals simultaneously over a single channel, all using different frequency ranges.
- Another reason is that it allows the use of a smaller antenna.

Modulation : Modulation is the process of converting data into radio waves by adding information to an electronic or optical carrier signal. Information can be added to the carrier by varying its amplitude, frequency, phase, polarisation.

Frequency Modulation (FM)

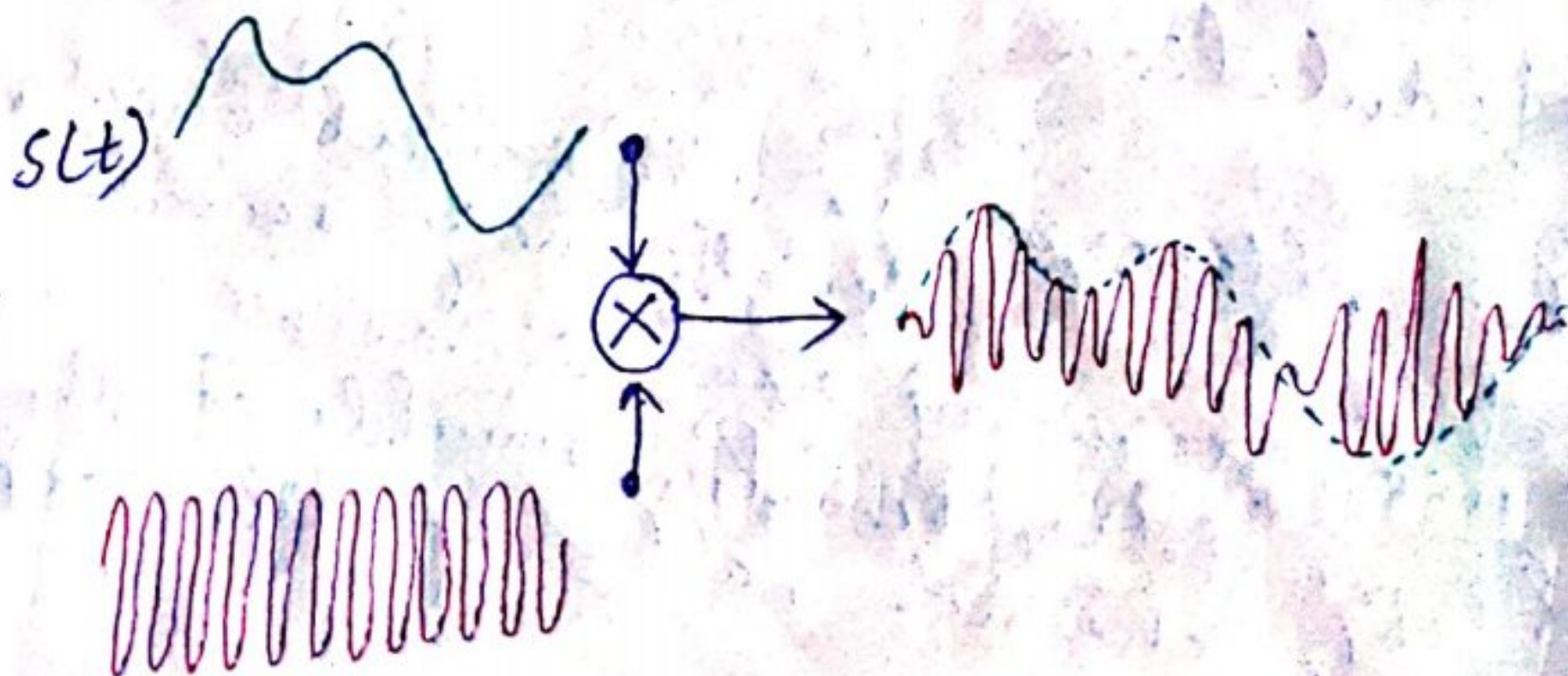
Frequency Modulation is widely used for FM radio broadcasting.

An advantage of frequency modulation is that it has a larger signal-to-noise ratio and therefore rejects radio frequency interference better than an equal power amplitude modulation (AM) signal.

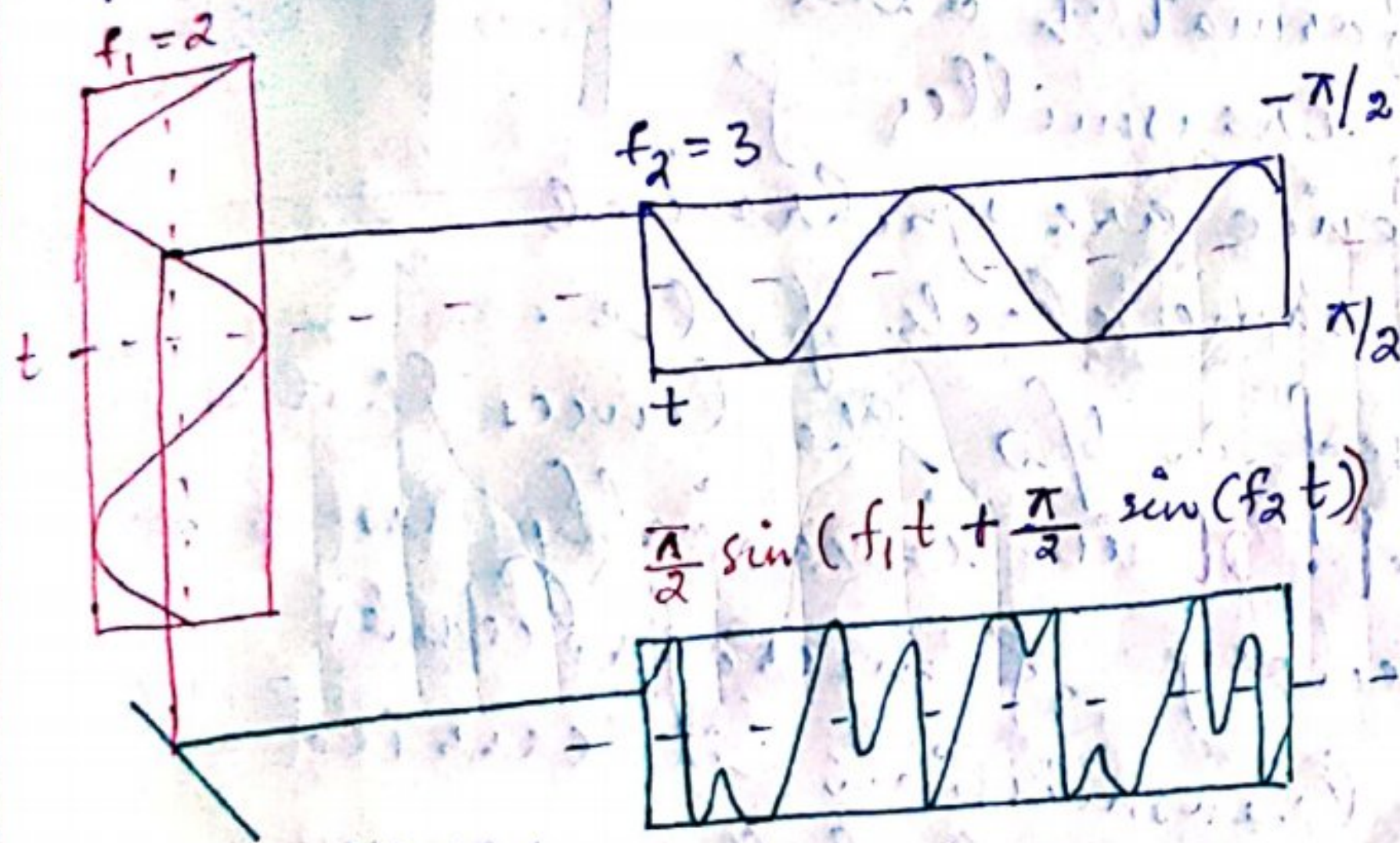
Amplitude Modulation (AM)

The modulation in which the amplitude of the base signal changes or modulates by superimposing it with a carrier signal of a different amplitude of same frequency as the base signal.

Amplitude Modulation



Phase Modulation : The modulation in which the phase of the carrier signal modifies by superimposing it with a carrier signal is phase Modulation.



4.1 Asynchronous & Synchronous Transmission

Need of Synchronisation

- Whenever an electronic device transmits digital (and sometimes analogue) data to another electronic device, there must be a certain rhythm established between two devices i.e. the receiving device must have some way of knowing, within the context of the fluctuating signal that it is receiving.
- It should know that where each unit of data begins & where it ends.
- There are two types of synchronisation processes : — (i) Asynchronous (ii) Synchronous.

(i) Synchronous

→ Synchronous means "at the same time".

→ In this format of data transfer, transmitter & receiver device are synchronised with the same clock pulse.

→ It is used in $\forall$ the devices that match in speed. It is invariably used in $\forall$ memory & microprocessors.

→ Data transmission is carried out under the control of a common master clock.

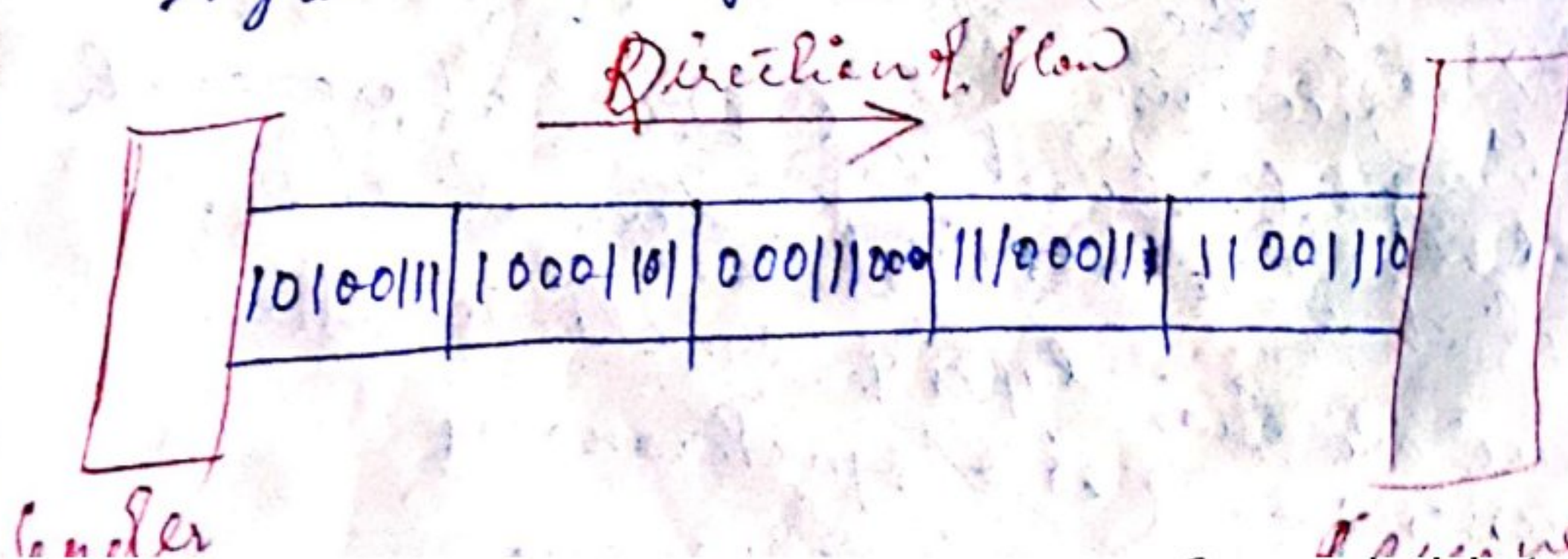
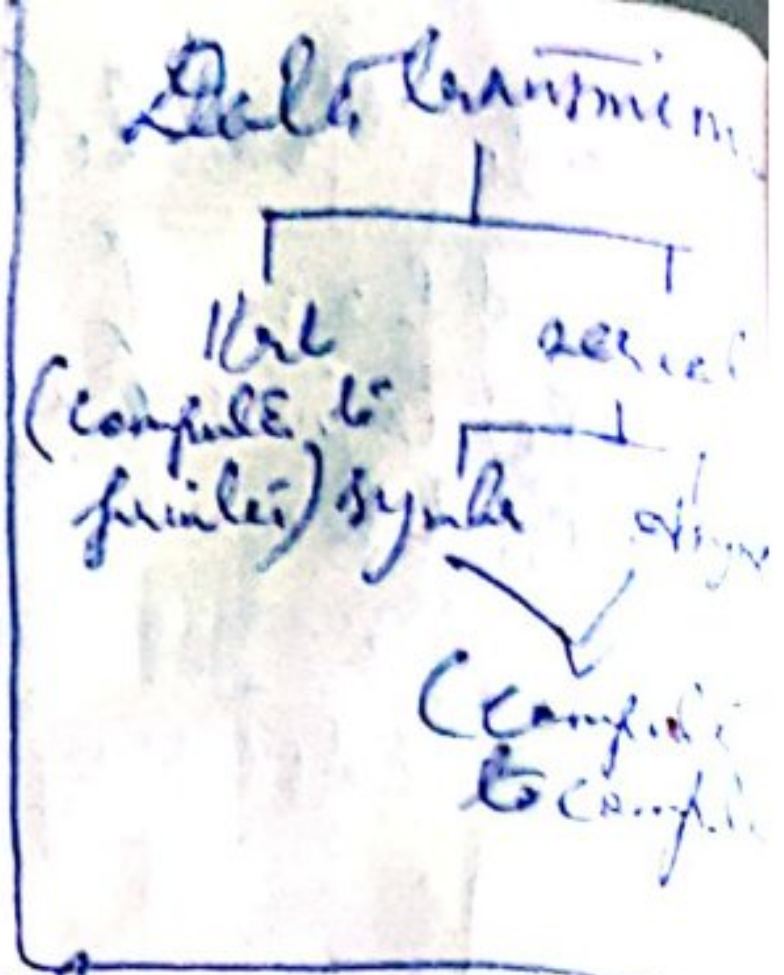
→ Bytes are transmitted as a stream in a continuous stream of bits.

→ Transmitter & Receiver operate at synchronised clock frequencies.

→ No 'start' & 'stop' bits are used.

→ No need of idle time $\forall$ data bytes.

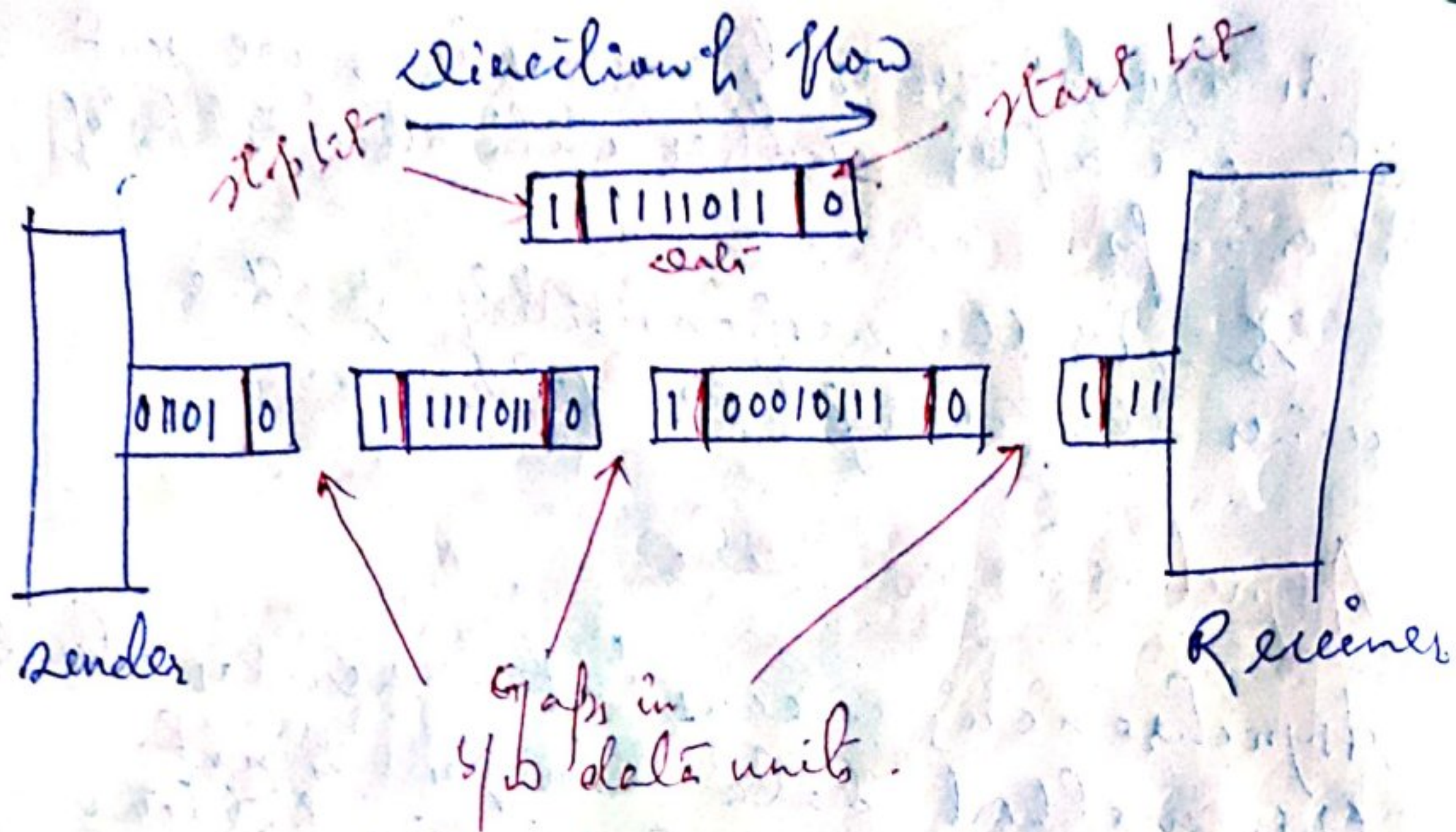
→ In this transmission type, timing of signal is important.



Note In synchronous transmission, we send bits one after another without start/stop bits or gaps.
So it's the responsibility of the receiver to group the bits.

(ii) Asynchronous Data

- Asynchronous means 'at a regular interval'. In this method data transfer is not based on predetermined timing pattern in this technique the status of the I/O device is checked by the MP before the data is transferred.
- It is used in b/w the devices that are not match in speed.
- Ex: MP & I/O devices.
- In this transmission, the transmitter transmits data bytes at any instant of time.
- Only one byte is sent at a time. There is ideal time b/w data bytes.
- To help receiver start & stop bits are used along with data in middle.
- Ideal time b/w bytes is not constant. They are also known as gaps.
- Here timing to signal is not important.



Note We mainly send one start bit (0) at the beginning and one stop bit (1) at the end of each byte. There may be a gap b/w each byte.

1.2 Error Detection

- In networking, error detection refers to the ~~deliberate~~ techniques used to detect noise or other impairments introduced into data while it is transmitted from source to destination.
- Error detection ensures reliable delivery of data across networks.
- Because of attenuation, distortion, noise and interferences, errors during transmission are unavoidable, leading to corruption transmitted bits.

→ The lower the frame size, the higher the probability of single bit errors & the lower is the probability of receiving a frame without errors.

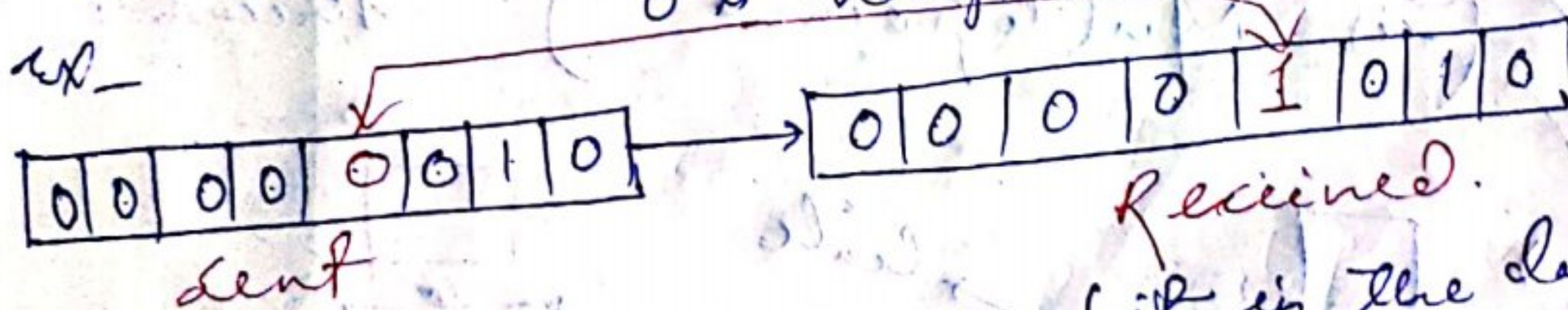
types of error

- Single-bit error
- Multiple-bit error
- Burst error

Error detection popular techniques:-

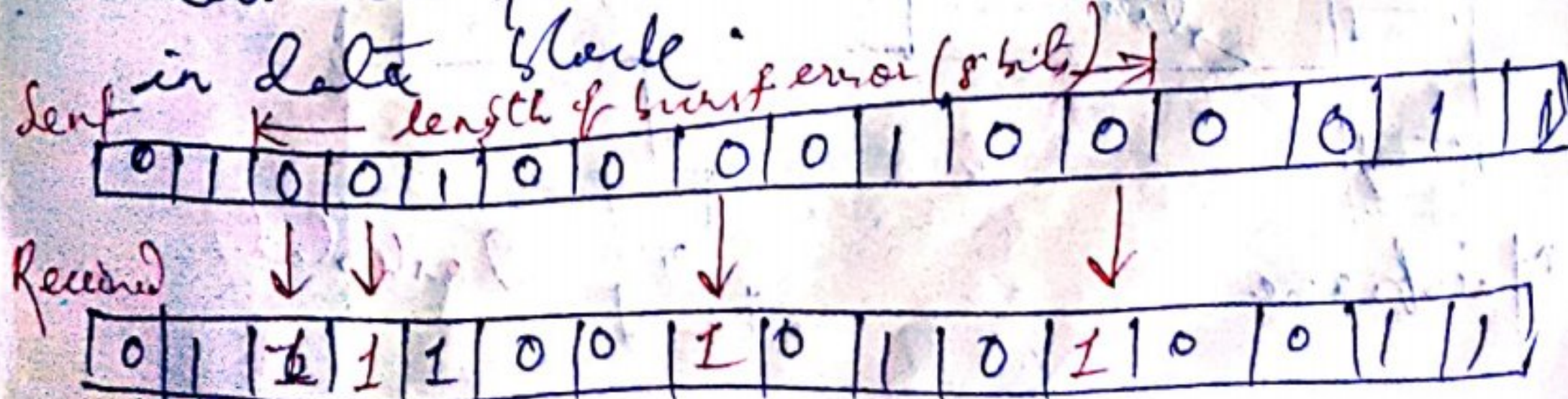
1. Simple parity check
2. Two-dimensional parity check
3. Cyclic redundancy check
4. Checksum

→ Single bit error :- Only one bit in the data unit is changed.
0 is changed to 1



Burst Error :- Two or more bits in the data unit get changed. The length of the burst is measured from the first corrupted bit to the last corrupted bit.

Distance b/w the first and last errors in data block.



4.3 Line Configuration

Line configuration refers to the way two or more communication devices are attached to a link.

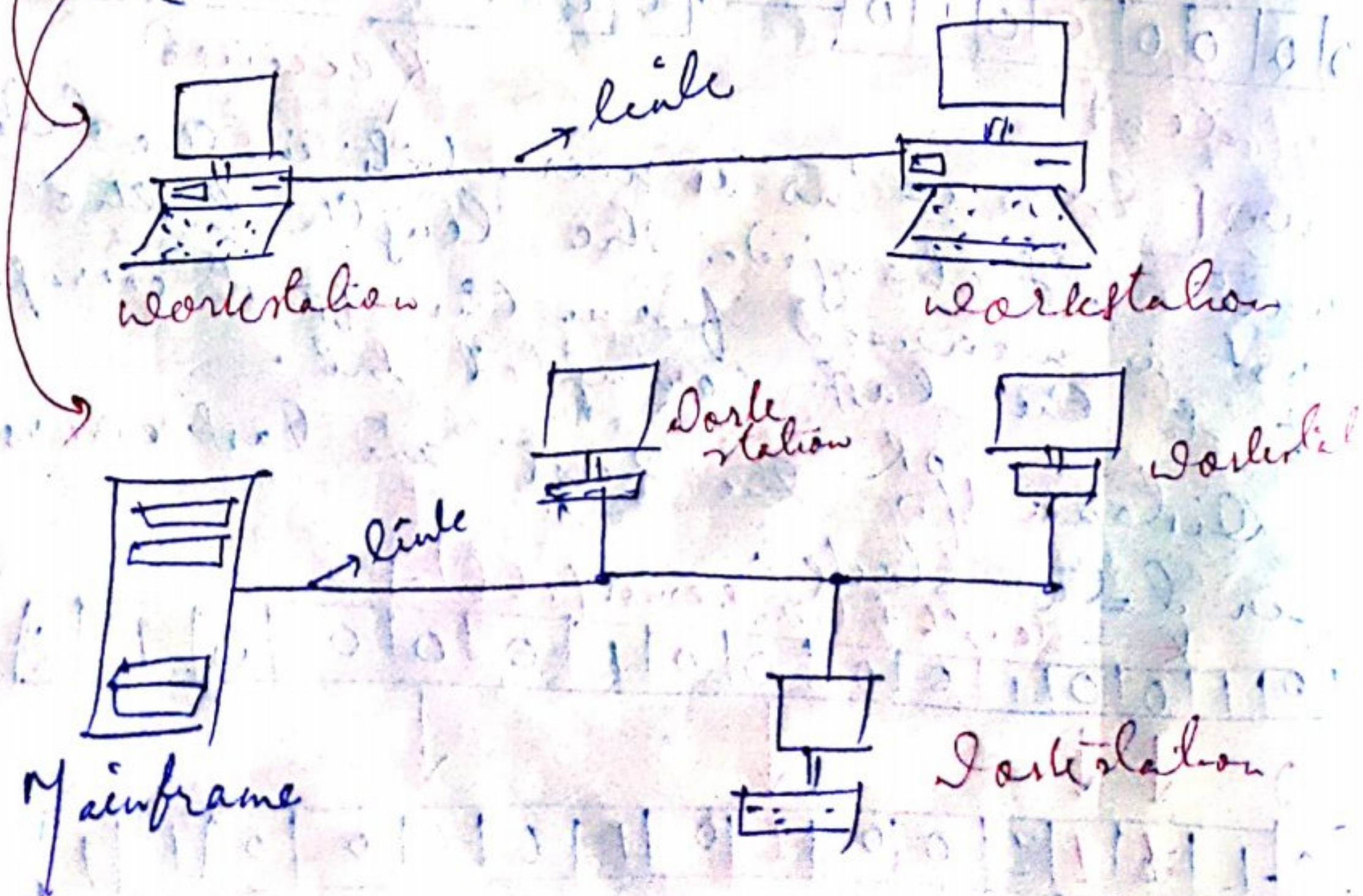
A link is the physical communication pathway that transfers data from one device to another.

For communication to occur, two devices must be connected in the same way to the same link at the same time.

Types

There are three possible line configurations such as:-

- (i) Point-to-point
 - (ii) Multipoint
- } Notes on phone screenshot.



4.4 Flow Control

→ Flow control is the management of data flow b/w computers or devices or b/w nodes in a network so that the data can be handled at an efficient pace.

Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be ~~be~~ retransmitted.

→ Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver.

→ Network layer provides flow control b/w routers by TCP.

Types

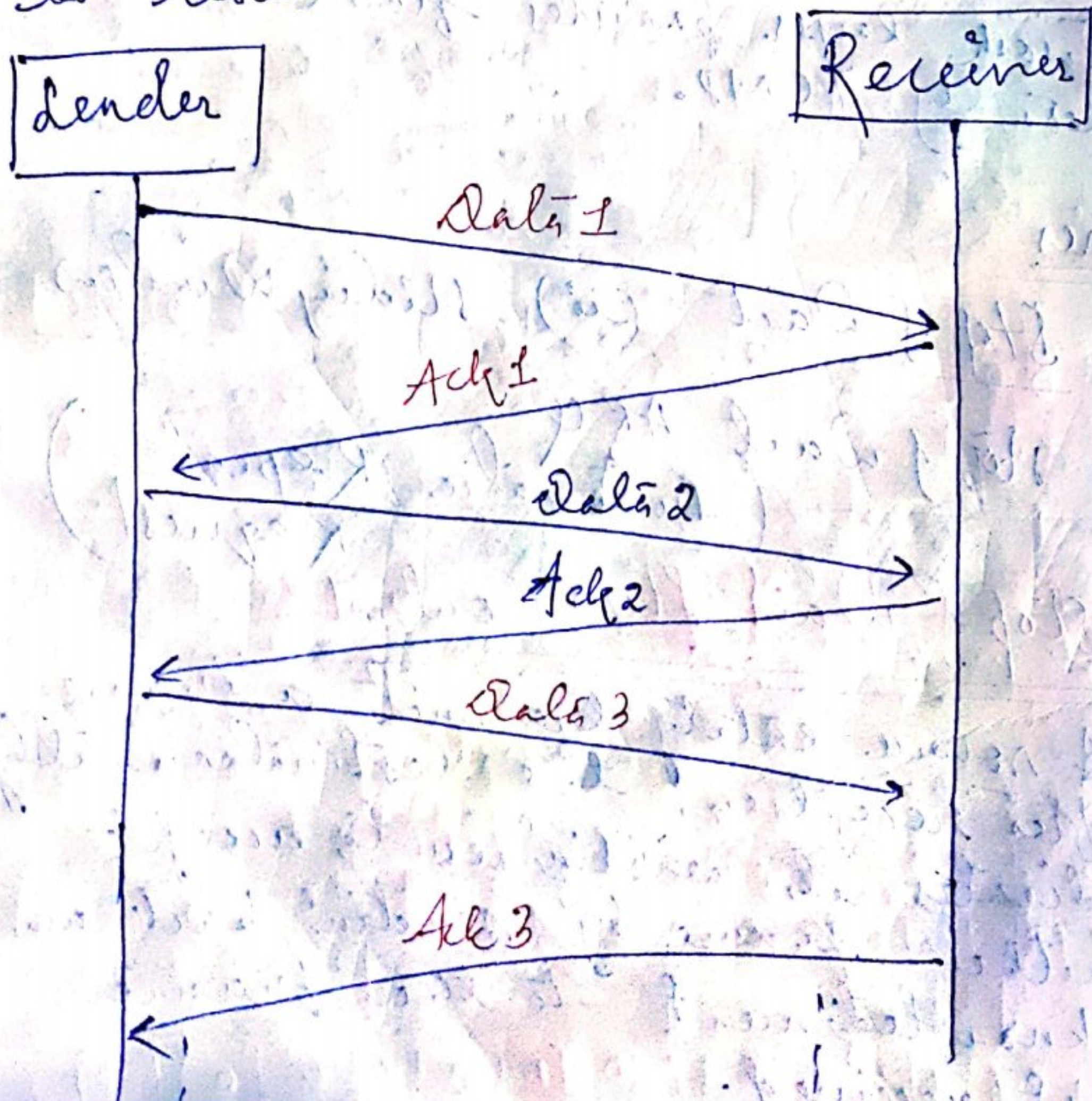
(i) Stop & Wait (ii) Sliding Window

(iii) Stop & Wait ARQ (Automatic Repeat Request)

(i) Stop & Wait flow Control

→ A source entity transmits a frame. After reception, the destination entity indicates its willingness to accept another frame by sending back an acknowledgment to the frame just received.

- The source must wait until it receives the acknowledgment before sending the next frame.
- The destination can thus stop the flow of data by simply withholding its acknowledgment.
- With the use of multiple frames for a single message, the stop-and-wait procedure may be inadequate.
- The essence of the problem is that only one frame at a time can be in transit.
- For ~~over~~ very high data rates, or for very long distances b/w sender & receiver, stop-and-wait flow control provides inefficient result.

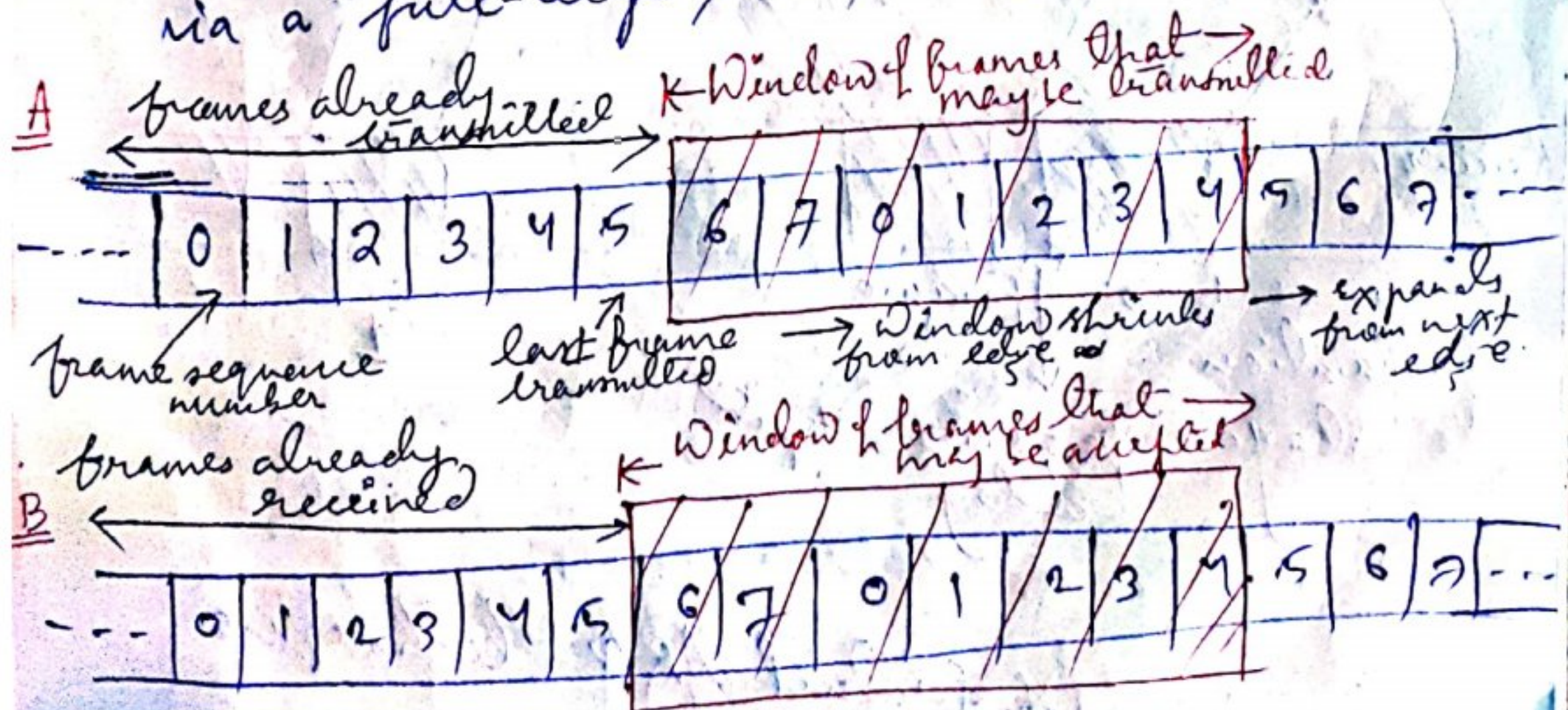


(ii) Sliding Window Flow Control :-

- Major drawback of stop-&-wait flow control is only one frame can be transmitted at a time; this leads to inefficiency if propagation delay is much larger than transmission delay.
- Sliding window flow control allows the transmission of multiple frame.
- It assigns each frame a 'k'-bit-sequence number and the range of sequence no. is $[0 \text{ to } 2^k - 1]$.

Ex/ - if no. of bit k is 2, then the range of sequence will be from 0 to $2^2 - 1$ i.e. 0 to 3 i.e. 0, 1, 2, 3.

Ex/ - Let us assume two stations A & B connected via a full-duplex link - transmitter → receiver.

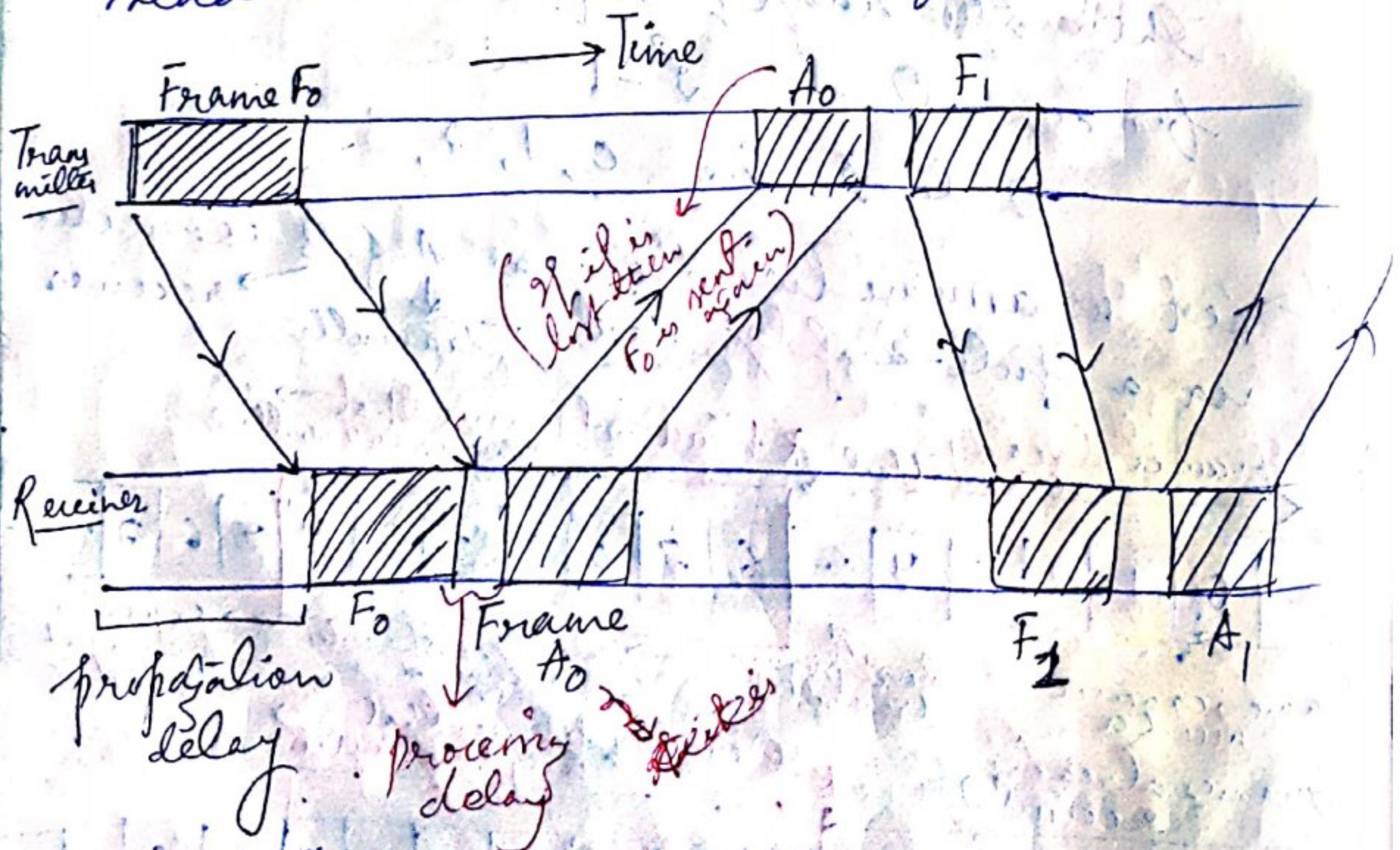


A → Transmitter's perspective
B → Receiver's perspective

(iii) Stop & Wait ARQ (Automatic Repeat Request)

↓ Also an error control technique

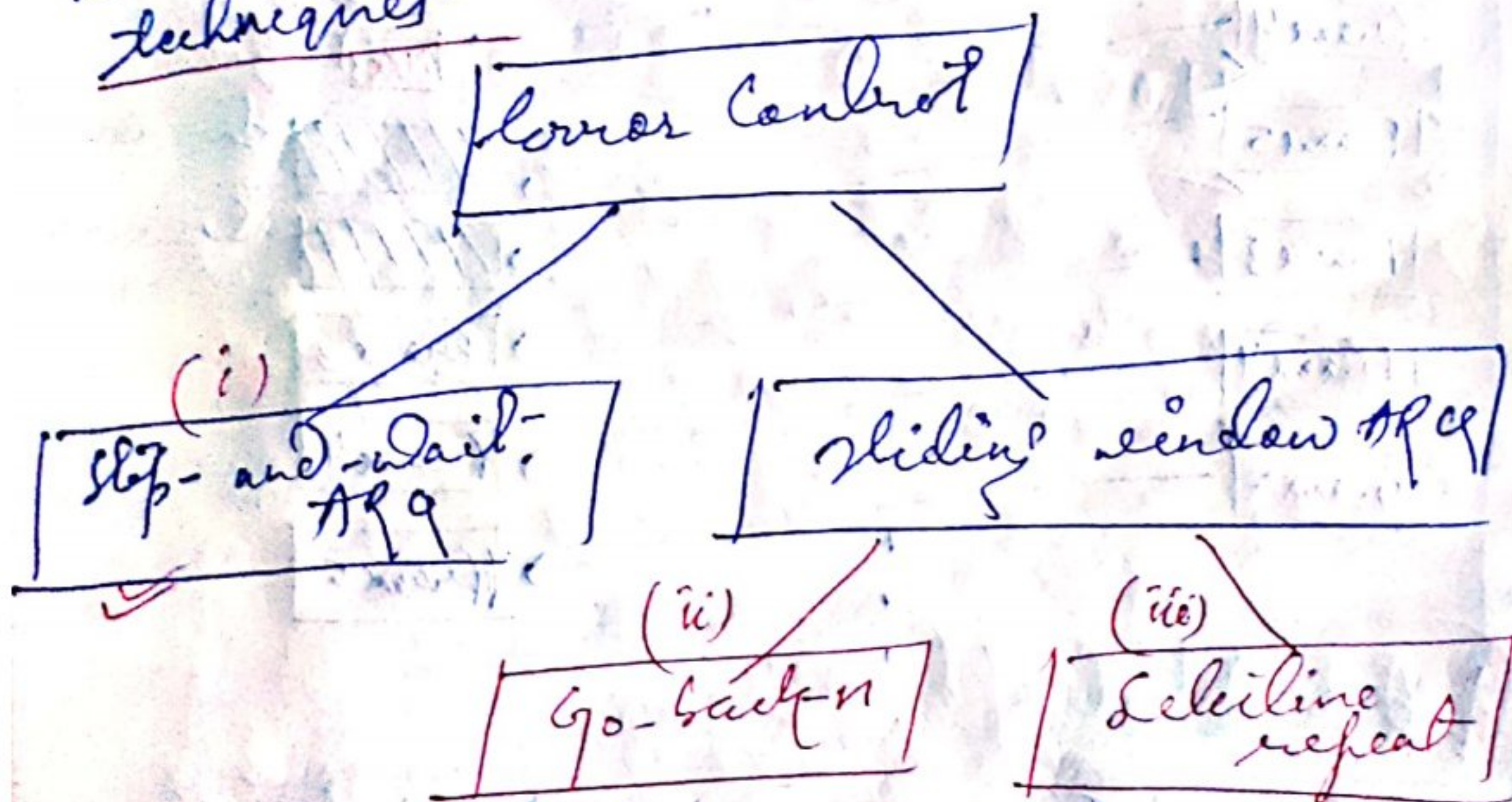
- Here, the sender transmits a frame and then waits till it receives positive ^(ACK) acknowledgment or negative ^(NACK) acknowledgment from the receiver.
- The receiver sends an ACK if the frame is received correctly otherwise it sends NACK.
- Transmitter sends a new frame after receiving ACK otherwise retransmits the old frame, if it receives a NACK.
- To tackle the problem of a lost or damaged frame, the sender is equipped with a timer. In case of a lost ACK, the sender transmits the old frame again.



stop & wait ARQ technique

4.6 Error Control

- When an error is detected in a message, the receiver sends a request to the transmitter to retransmit the packet.
- The most popular retransmission scheme is known as Automatic Repeat Request (ARQ).
- Such schemes where receiver asks transmitter to re-transmit if it detects an error, are known as reverse error correction techniques.



(ii) Go-back-n

- Here the sender sends the frames continuously without waiting for any acknowledgement. That is why it is also called as continuous ARQ.

- As the receiver receives the frame, it keeps on sending ACK, or a NACK, in case a frame is incorrectly received.
- When the sender receives a NACK, it retransmits the frame in error plus all

the succeeding frames as it shows in figure below:-

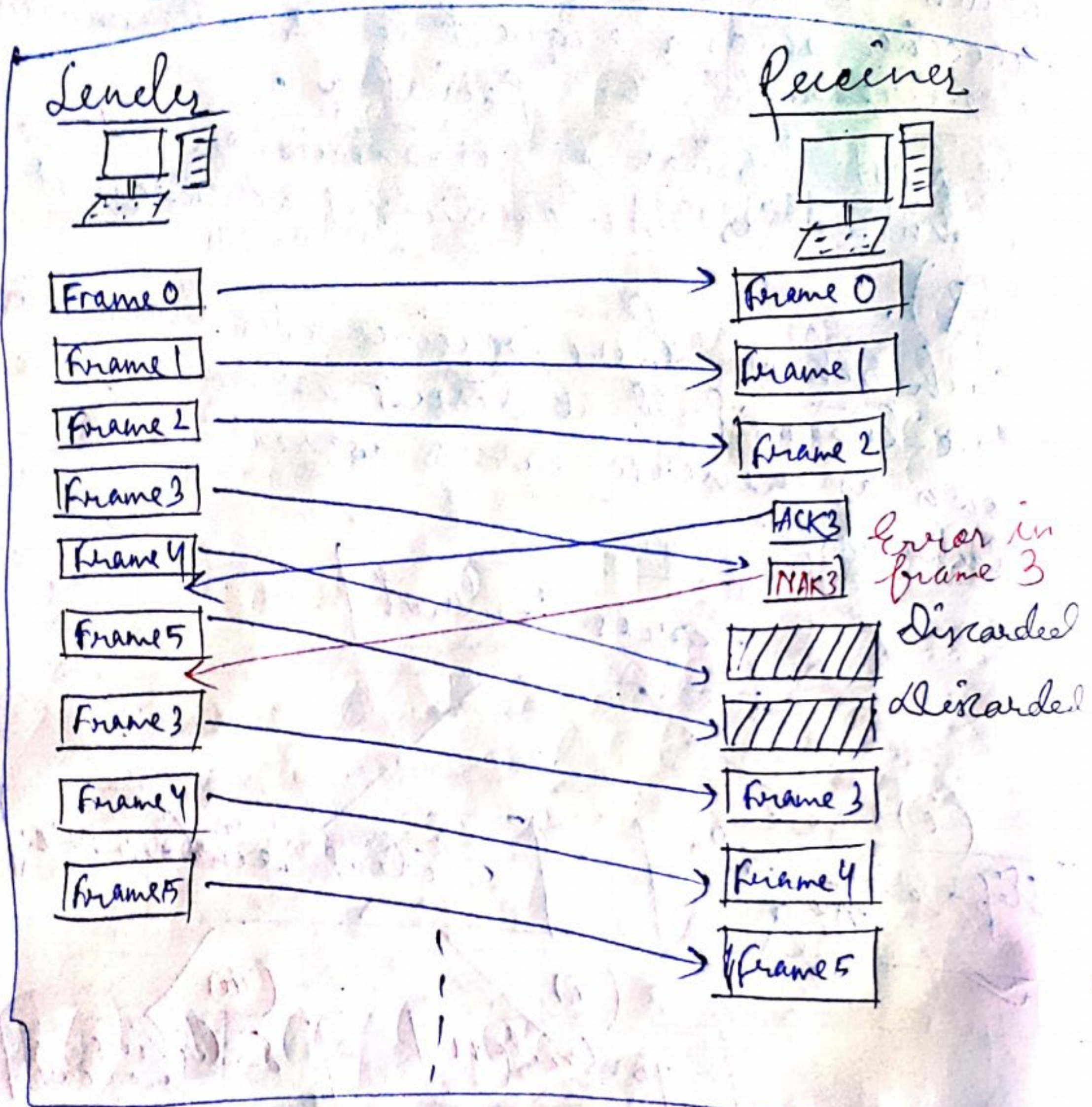
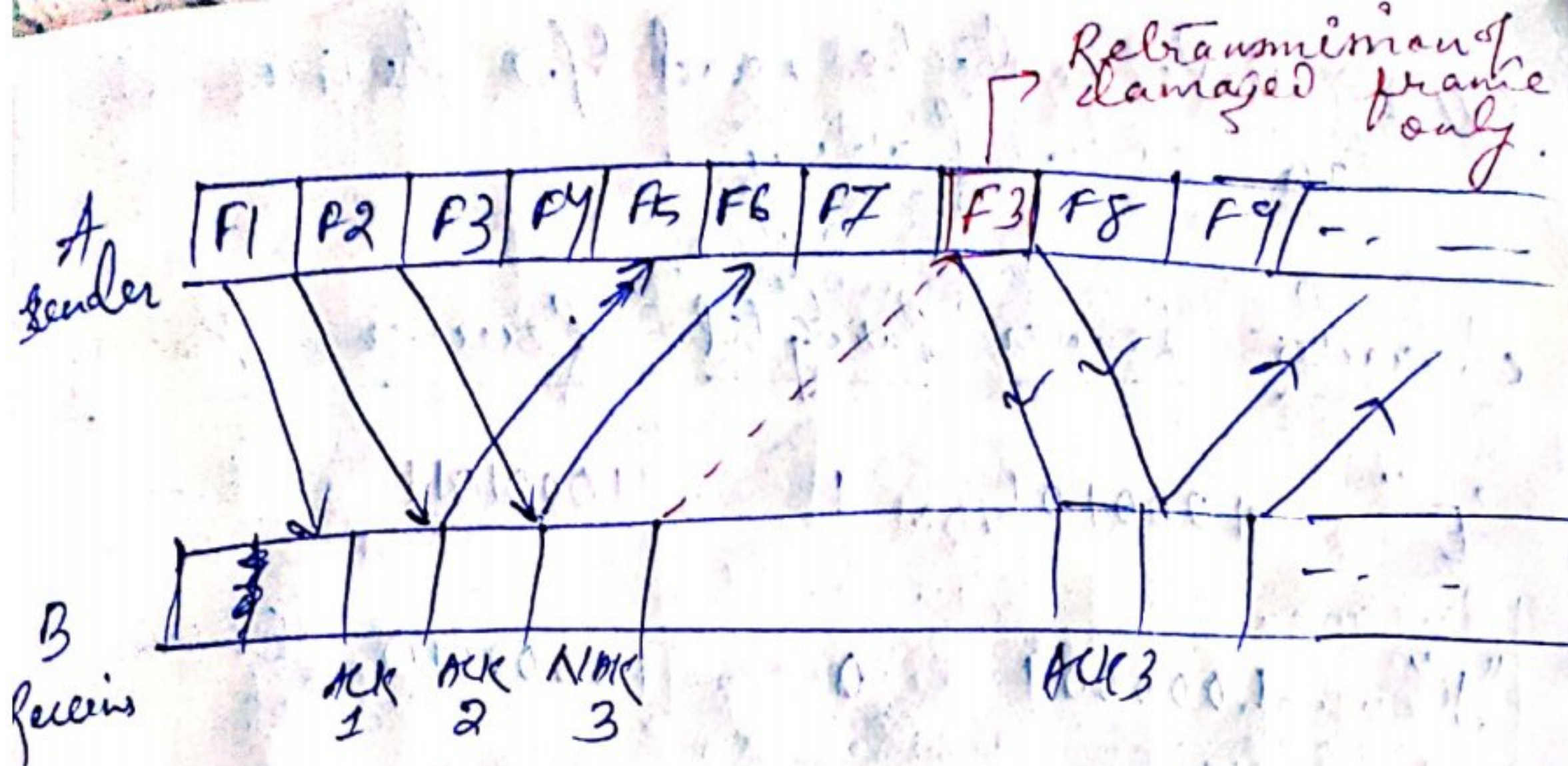


Fig: Frames in error in go-back-N-ARQ.

→ Hence, the name of the protocol is go-back-N ARQ.

(ii) Selective-Repeat ARQ

→ This scheme retransmits only those for which NAKs are received or for which timer has expired.



Error Detection :- Parity Check (single)

→ A parity check is the process that ensures accurate data transmission b/w nodes during communication.

A parity bit is appended to the original data bits to create an even or odd bit number; the number of bits with value one.

→ Mostly it is used in ASCII where characters are represented by seven bits and the eighth bit is a parity bit.

→ Single bit parity check codes can detect all single-bit errors. It can also detect multiple errors only if the total number of errors in a data unit is odd.

Drawback

- Only can detect single bit errors.
- Can not detect errors, if 2 bits are interchanged.

Ex Data is to be sent b/w devices using an even parity.

<u>character</u>	<u>Sender</u>	<u>Parity bit</u>	<u>Receiver</u>	<u>Parity</u>
"E"	1000101	1	10001011	Even
"A"	1000001	0	10000010	Even
"C"	1000011	1	11100111	Even
"q"	1110001	0	11100000	Odd Error

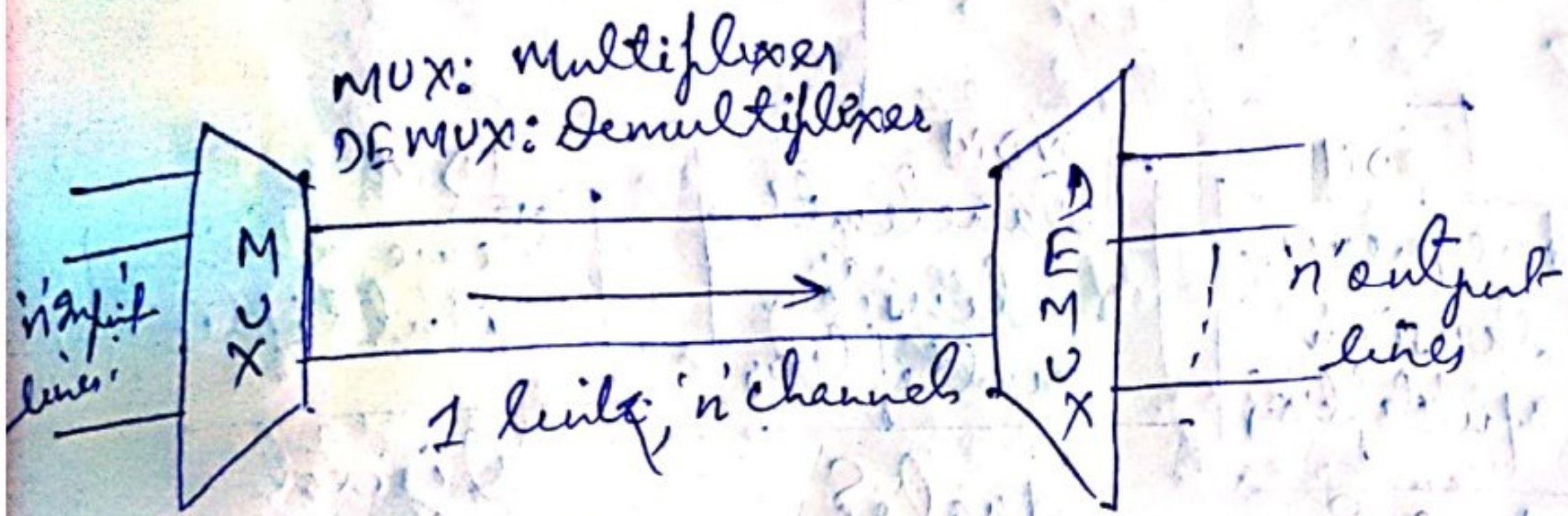
* Errors will not be detected if there are even number of bit swaps, which maintains the agreed parity (even or odd).

Q-6 Multiplexing

→ It is the set of techniques that allow the simultaneous transmission of multiple signals across a single data link.

→ Multiplexing is done using a device called Multiplexer (MUX) that combine 'n' input lines to generate one output line i.e. (many to one).

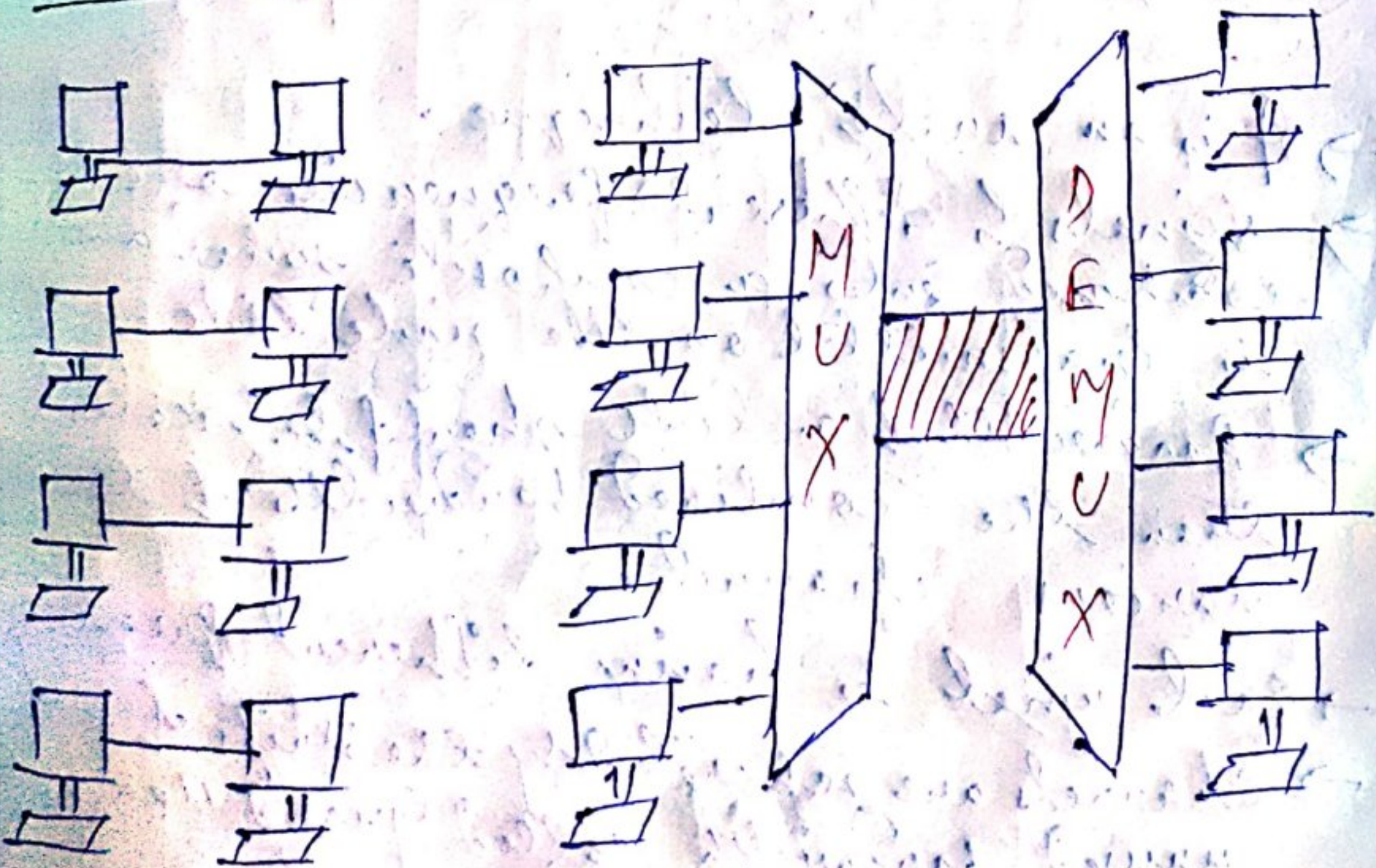
→ At the receiving end a device called demultiplexer (DEMUX) is used that separates signal into its component signals i.e. one input and several outputs (one to many).



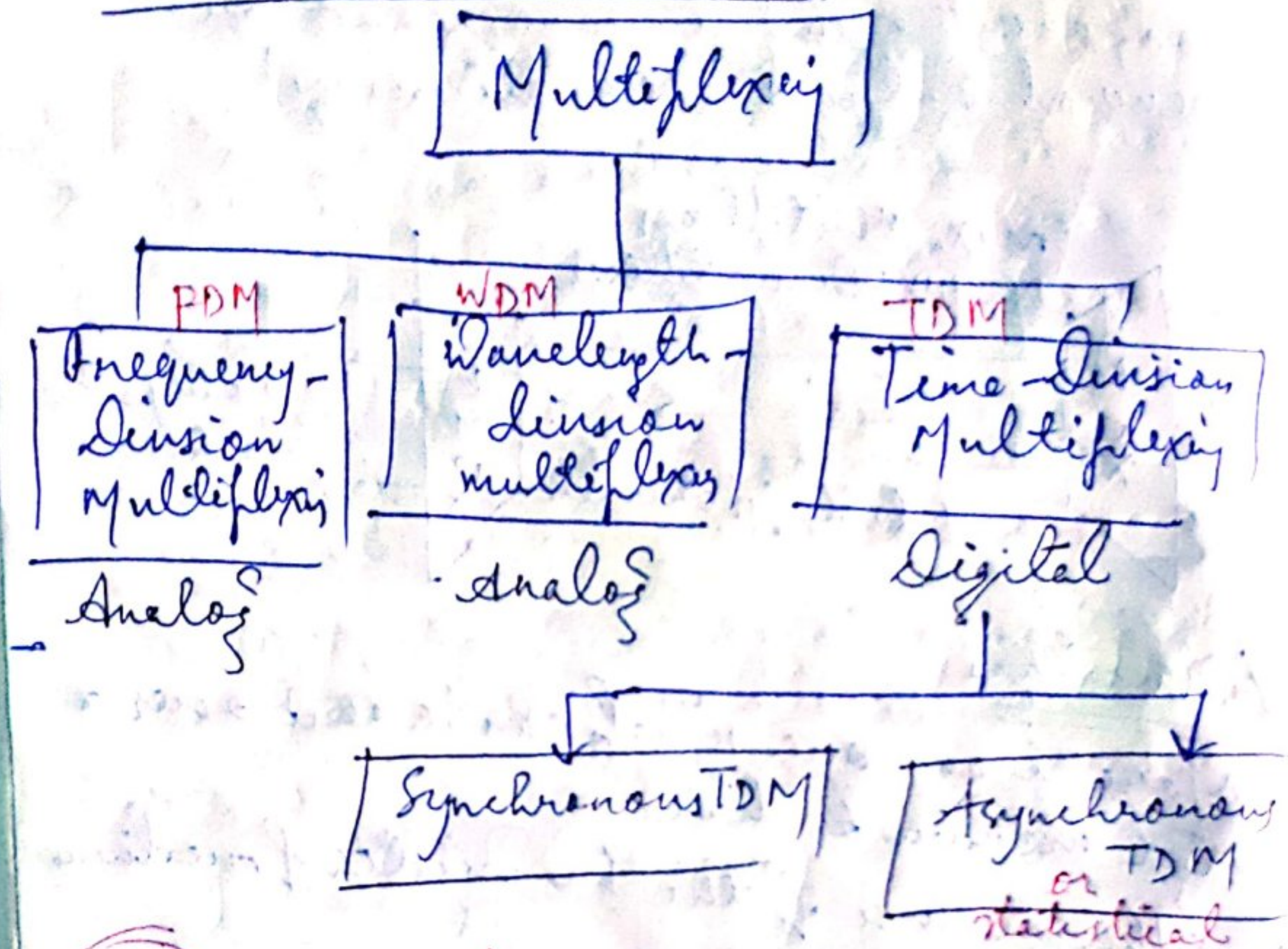
Advantages

- More than one signals can be sent over a single medium or link.
- Efficient use of the bandwidth of medium.

Multiplexing Vs. No Multiplexing

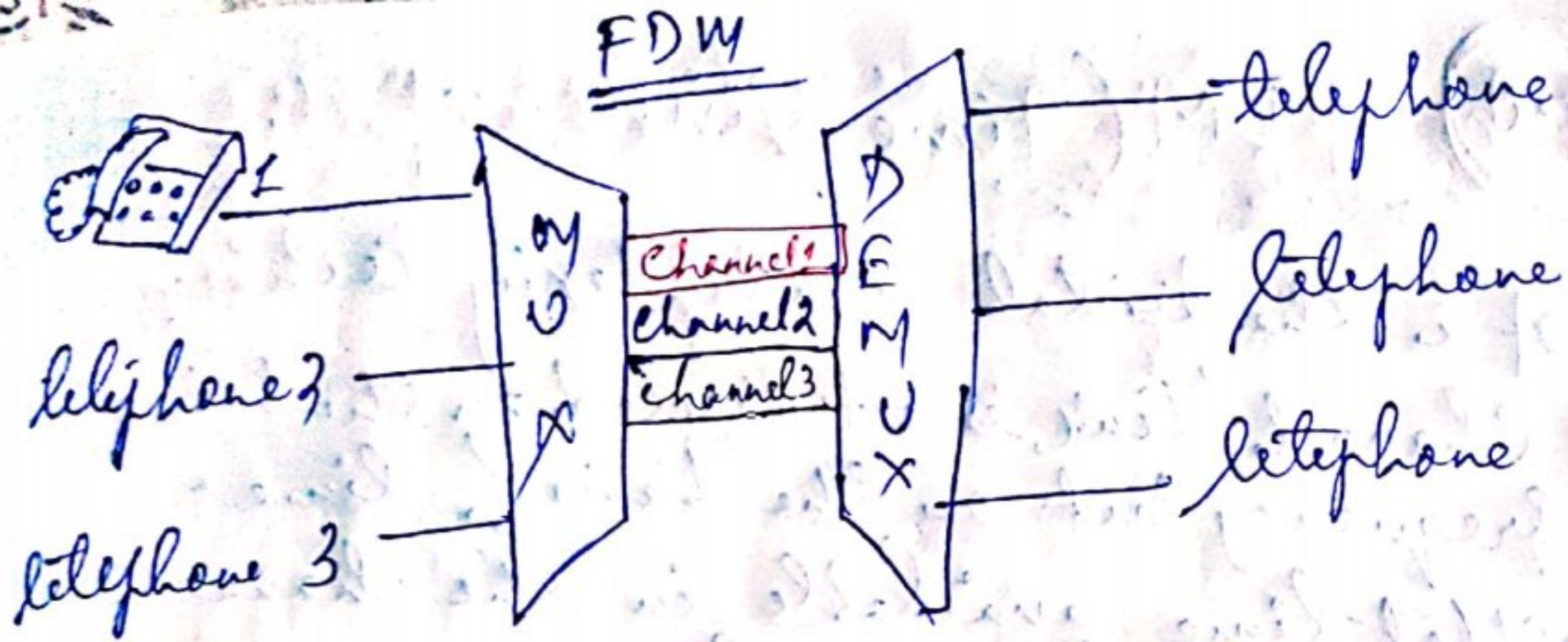


Types of Multiplexing



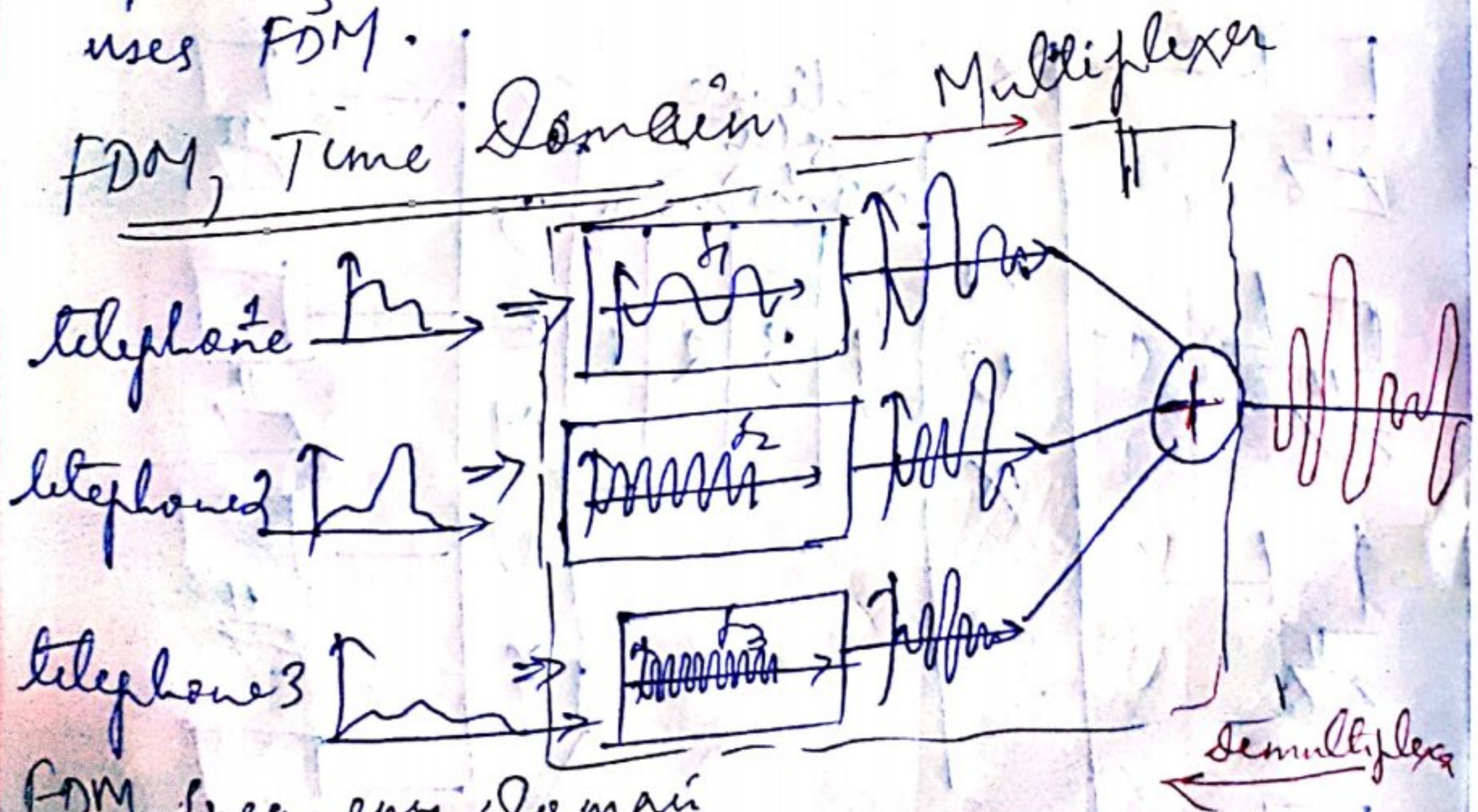
Q.7 FDM (Frequency Division Multiplexing)

- It is an analog technique.
- Signals of different frequencies are combined into a composite signal and is transmitted on the single line.
- Bandwidth of a link should be greater than the combined bandwidth of the various channels.
- Each signal is having different frequency.
- Channels are separated by the strips of unused bandwidth called Guard Bands (to avoid overlapping).



Applications

- Used for FM & AM radio broadcasting
- AM frequency = 530 to 1700 KHz
- FM " = 88 to 108 MHz
- FDM is used in television broadcasting
- First generation cellular telephone also uses FDM.

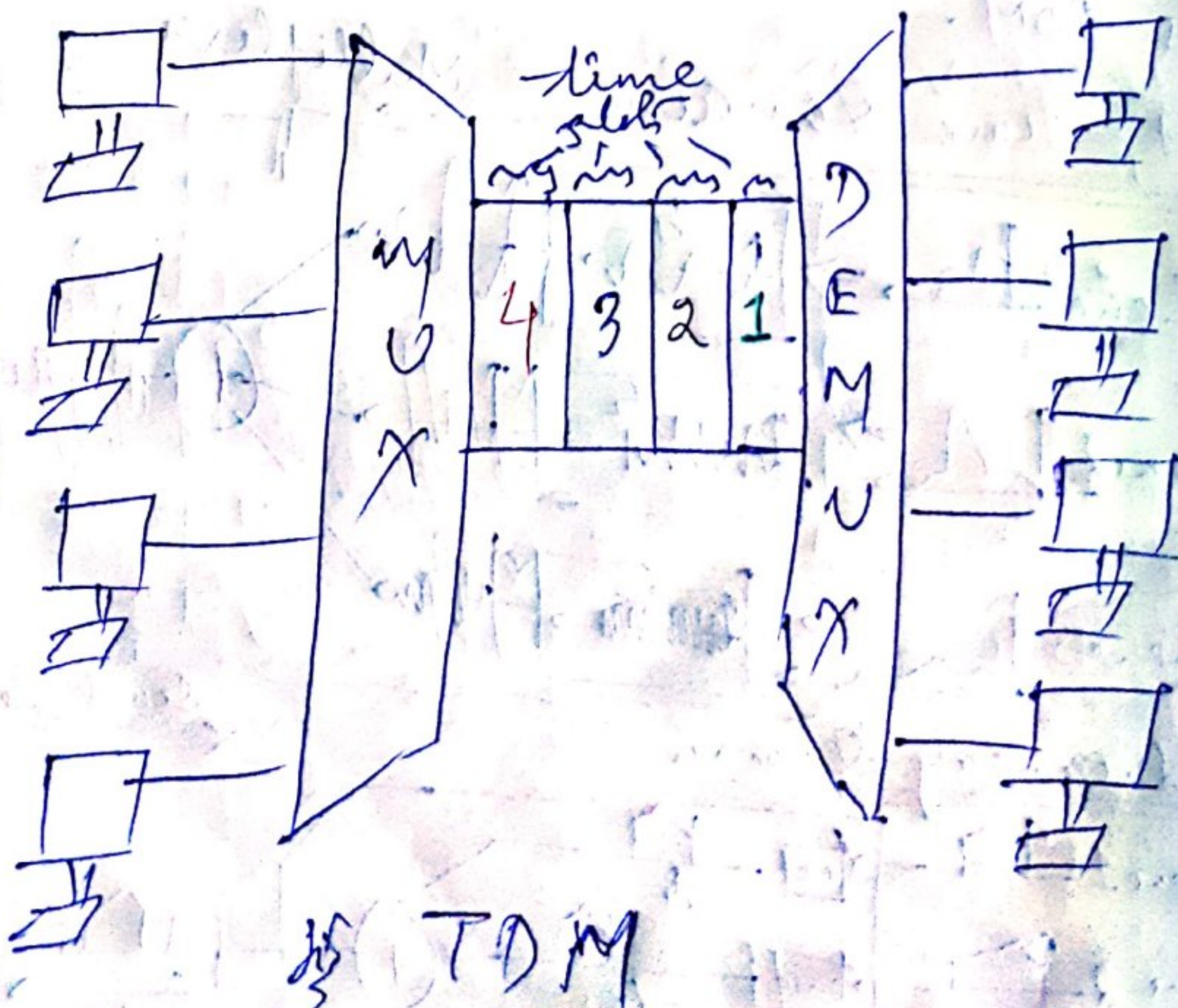


FDM, Frequency Domain



4.8 TDM (Time Division Multiplexing)

- It is the digital multiplexing technique.
- Channel/Link is not divided on the basis of frequency but on the basis of time.
- Total time available in the channel is divided among several users.
- Each user is allotted a particular time interval called time slot or slice.
- In TDM, the data rate capacity of the transmission medium should be greater than the data rate required by sending or receiving devices.



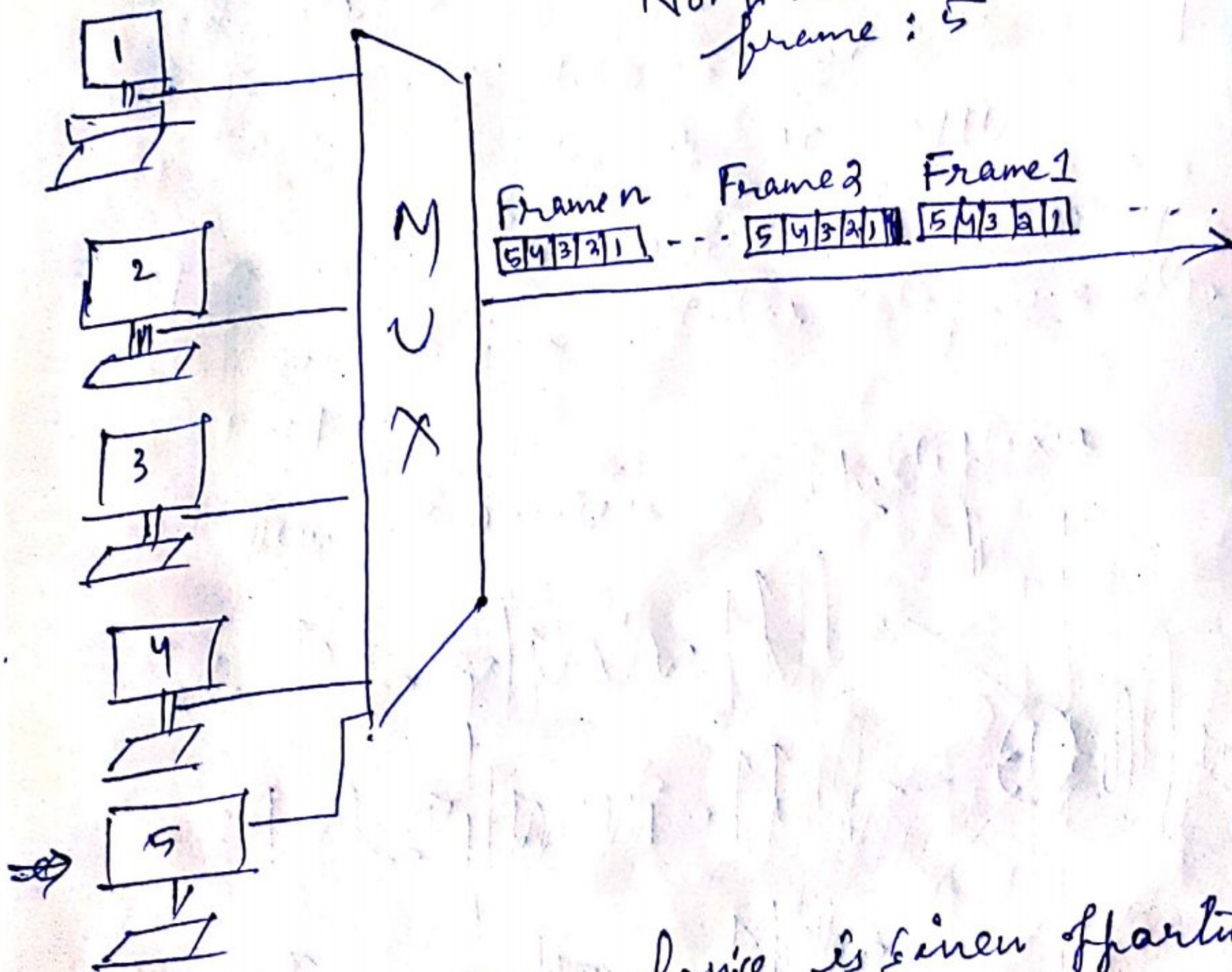
Types of TDM

synchronous
TDM

Asynchronous TDM

Synchronous TDM

No. of inputs: 5
No. of slots in each
frame: 5



- In S TDM every device is given a part of the data to transmit a specific amount of data into the link.
- Each device places its data into the link when its Time slot arrives, each device is given the possession of the line turn by turn.

Q. What is a switch?

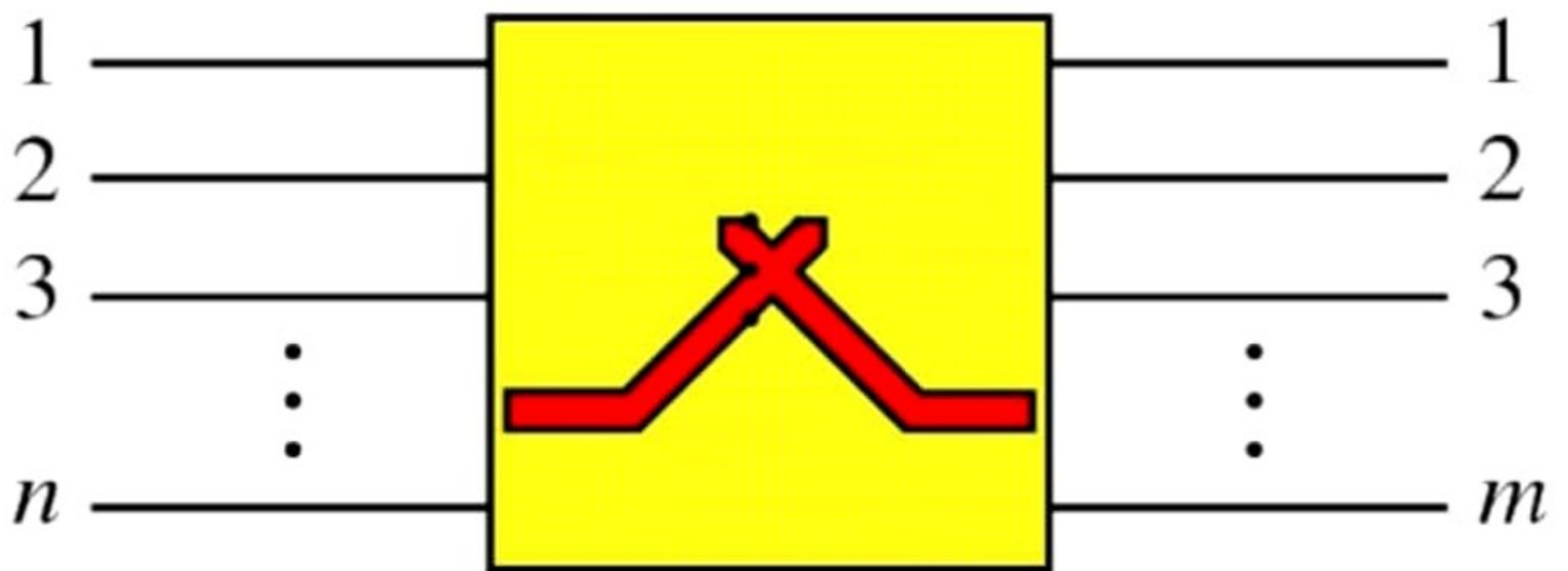
Q. What is switching?

Q. What is switched network?

Switch

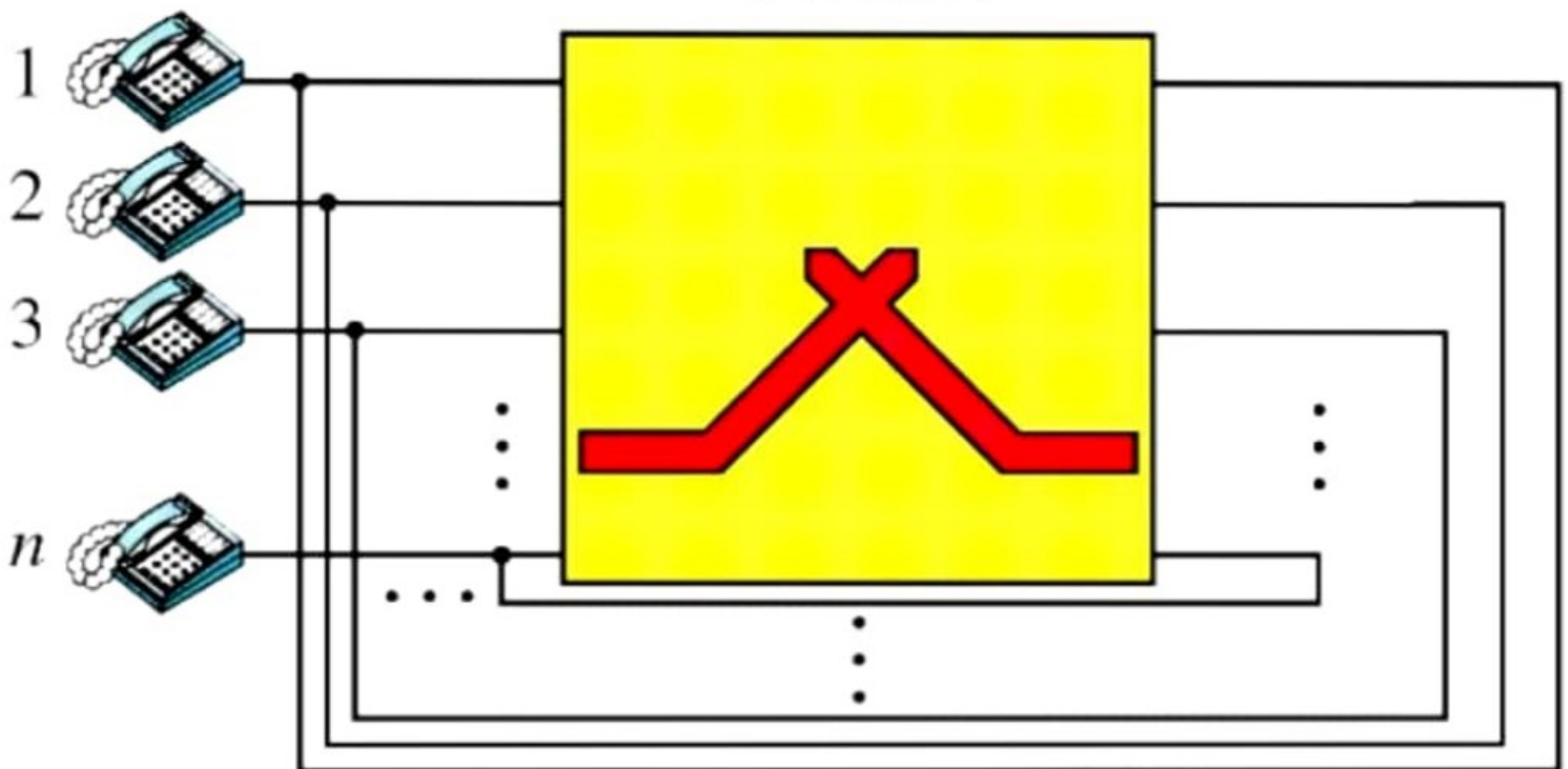
Switches are the hardware or software devices capable of creating temporary connections between two or more devices linked to the switch but not to each other. It is a device which connects multiple communication lines together.

Switch



Folded Switch

Switch



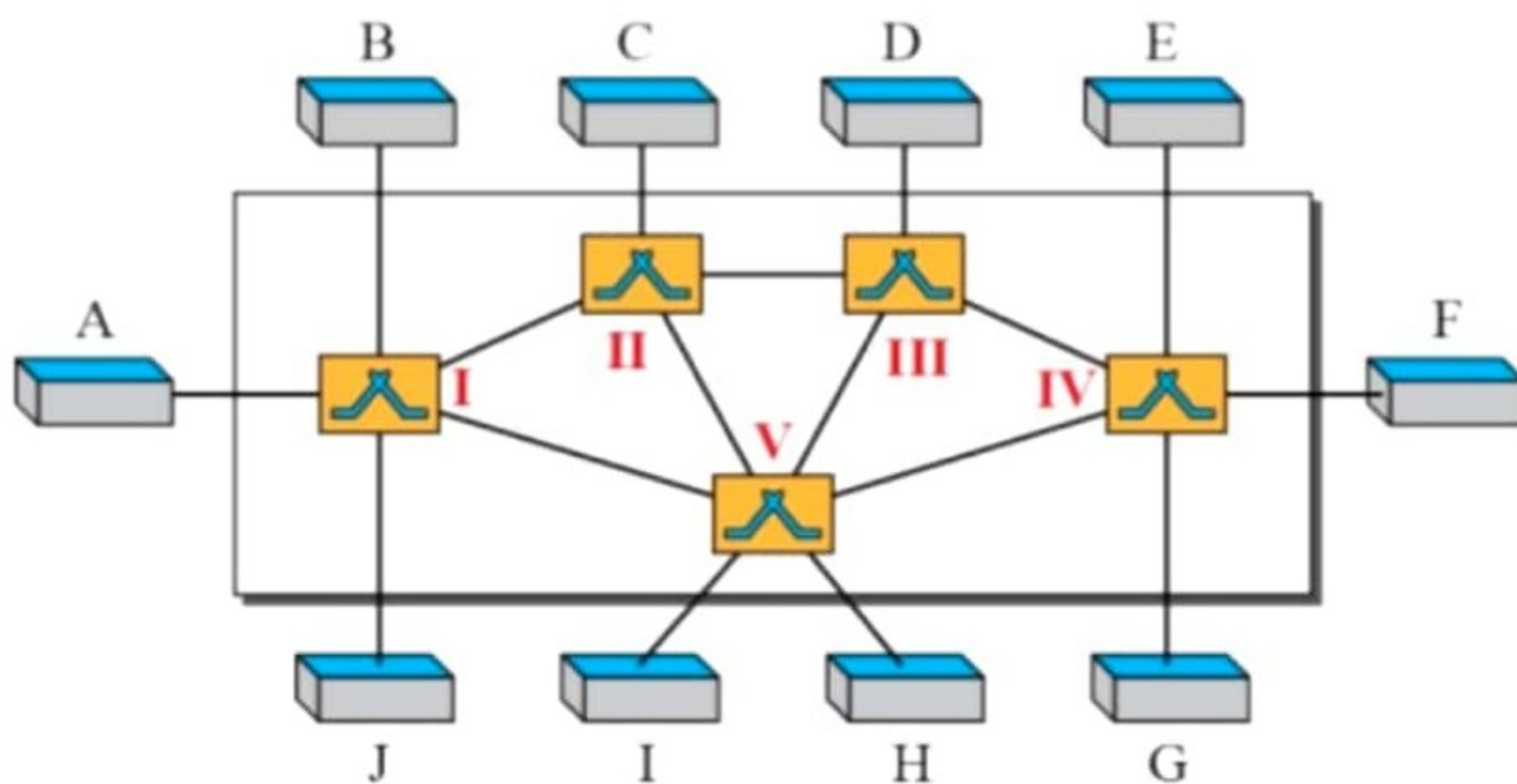
Switching

- A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible.
- The solution is switching.
- A switched network consists of a series of interlinked nodes, called switches.

Switched Network

- A Computer network in which connectivity is provided by using numbers of switches.
- A fully switched network uses only switches for connecting all devices used in that network.

Switched network (Networking using Switches)



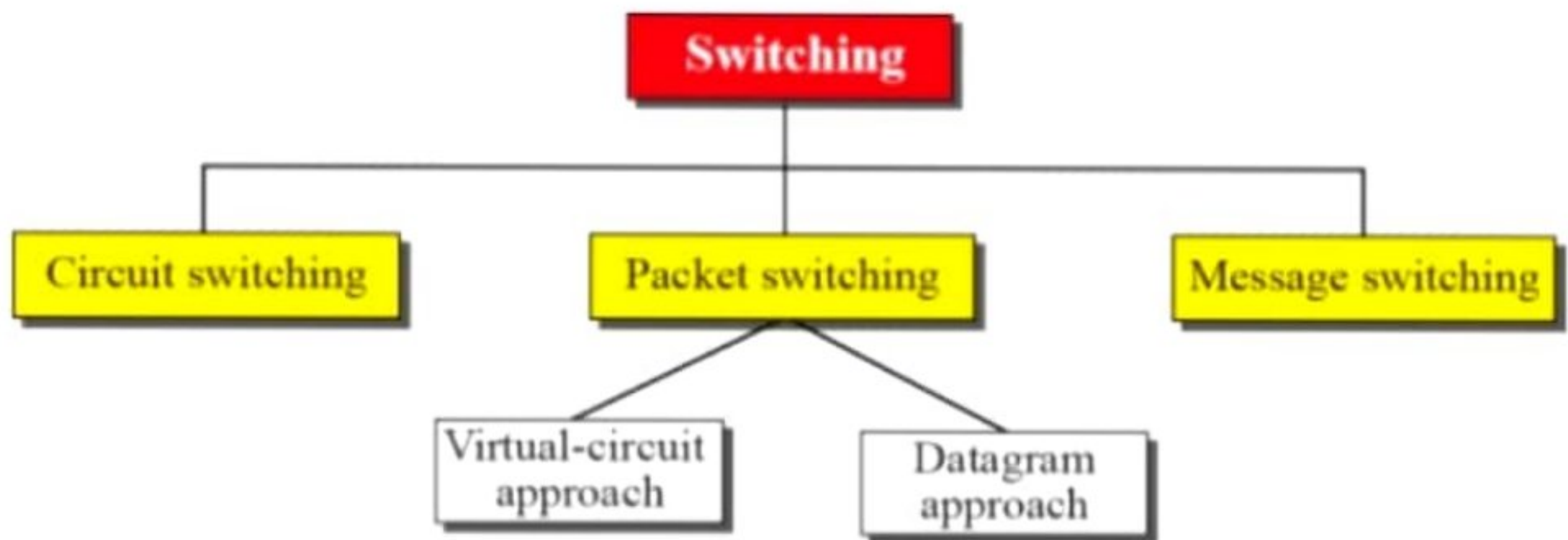
- ✓ Computers are denoted by A,B,C upto L
- ✓ Switches are denoted by I,II,III upto VIII

Traditionally, three methods of switching have been discussed:

- 1.circuit switching,
- 2.packet switching
 - i. Virtual circuit
 - ii. Data gram
- 3.message switching.

- The first two are commonly used today.
- The third has been phased out in general communications but still has applications.

Taxonomy of switched networks





Switching and TCP/IP Layers

Switching takes place at several layers of the TCP/IP protocol suite:

1. at the physical layer it is **circuit switching**. There is no exchange of packets at PL. The switches at PL allow signals to move in one path or another.

2. at the data-link layer we can have **packet switching**. However, the packet can mean frame or cells here. Packet switching is done normally using Virtual Circuit Approach.

3. at the network layer we can have packet switching. Here, either a virtual circuit or datagram approach can be used. Internet uses datagram approach.

4. Switching at [Application Layer](#) : we can have only message switching at AL. It is done by exchanging messages like email etc. So such communication can be called as message switched communication. As such there is no concept of message switched Network.

Circuit switching

- Circuit switching is used in public telephone network but it is used for data transmission also along with voice communication
- Voice communication is efficient but data communication is not that efficient
- In this method a dedicated path is established between two computer using one or more switch

- The transfer mode of a network involves setting up a dedicated end to end connection. This path is maintained till the end of communication.
- Link is released after communication is over
- Circuit switching takes place at physical layer
- Data transfer may use FDM or TDM

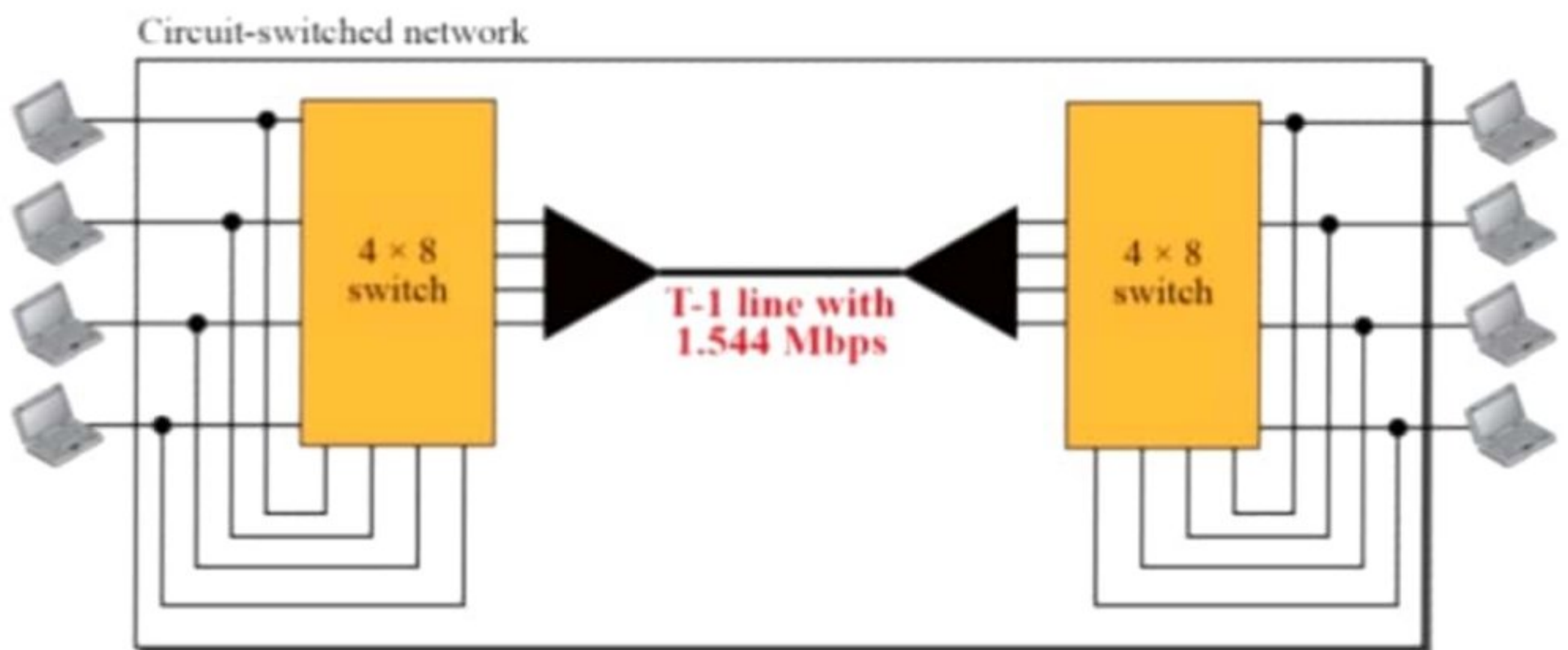


Three Phases of Circuit Switching

The actual communication in a circuit-switched network requires three phases:

- 1. connection setup,*
- 2. data transfer, and*
- 3. connection teardown.*

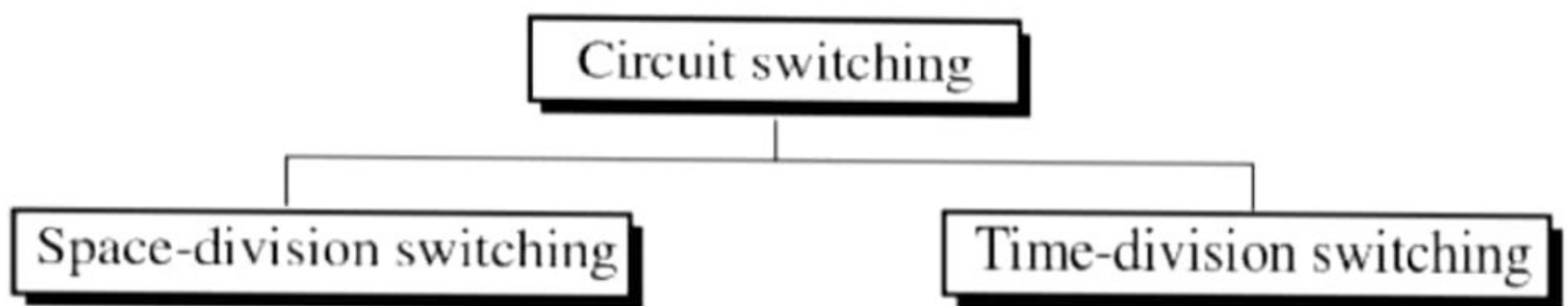
Circuit-switched network used in Example



Certain issues in circuit switching

- **Efficiency** – low, because of resources remain dedicated through out the connection
- **Delay** – despite low efficiency there is very low delay in transmission.
 - Since connection is dedicate so only time taken in connection is the only delay in transmission

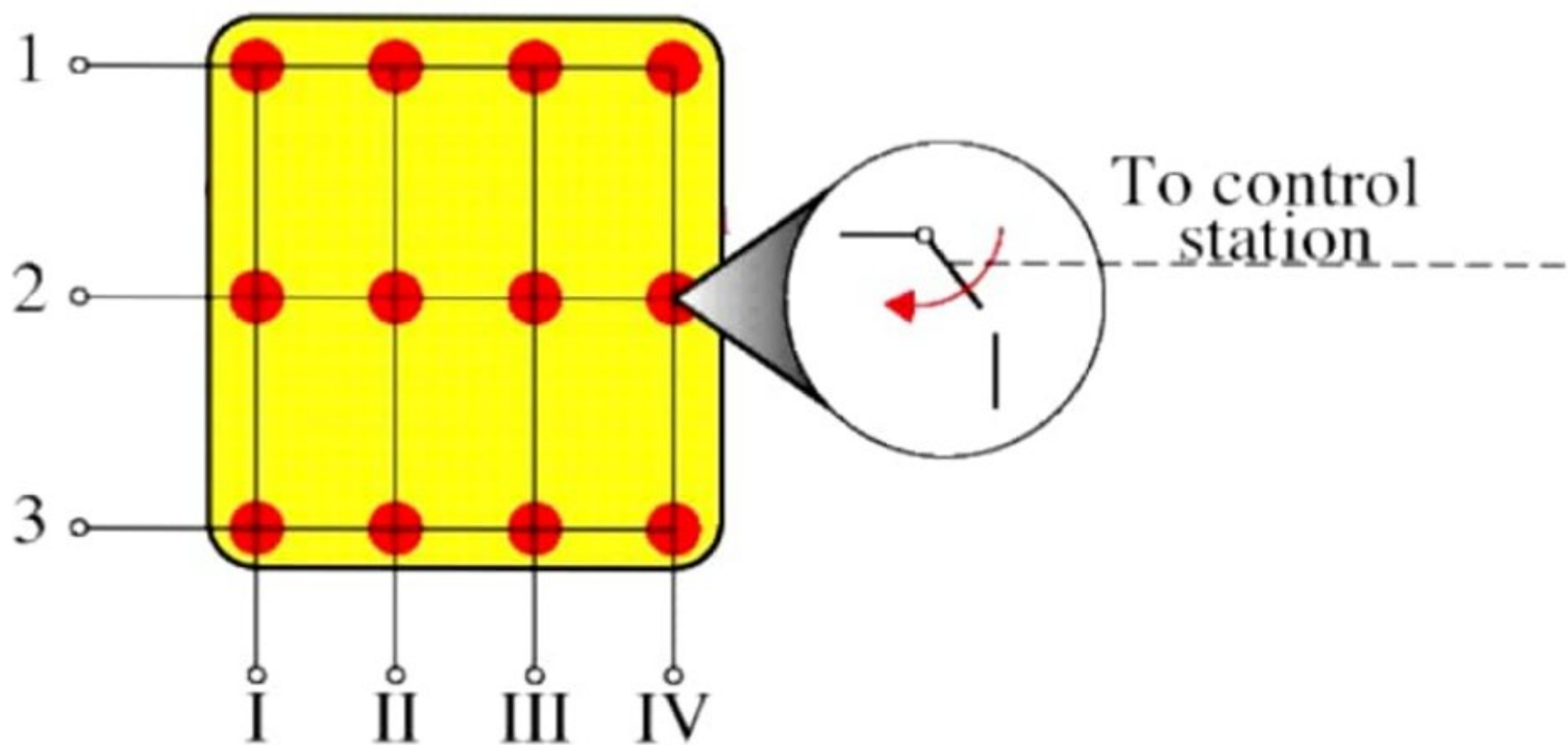
- Advantages –
 - Dedicated transmission
 - No delay in transmission
- Disadvantages
 - Because of dedicated connection other devices waste time in waiting
 - Dedicated connection will consume all bandwidth
 - Sometimes it may take long time to establish a connection
- Applications – Public Switched Telephone Network (PSTN)



Space Division Switching

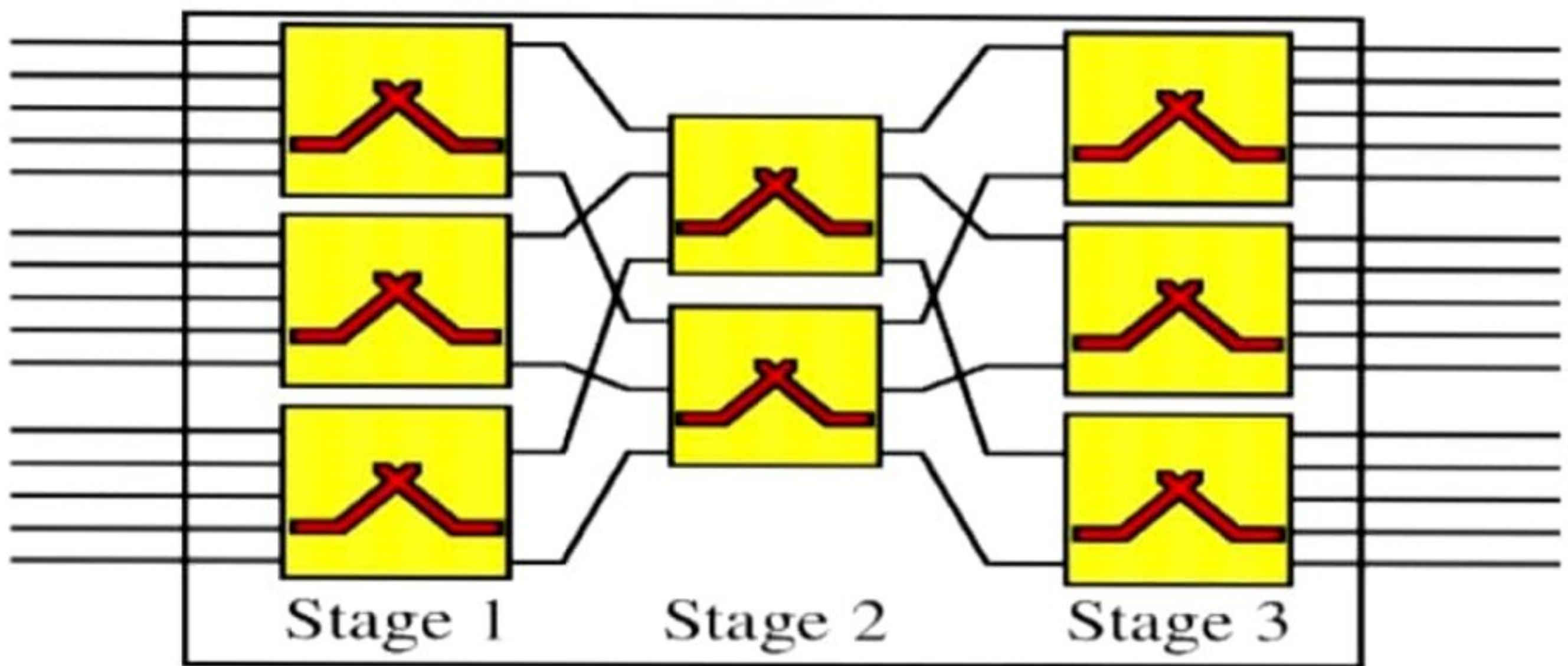
- In space division switching, the paths in the circuit are separated from each other spatially. This technology is used in both analog & digital networks. It uses following switches for connection:
 - Cross bar switch
 - Multistage switch

Crossbar Switch



A cross bar switch connects n input lines to m output lines in a grid using micro switches (transistor) at each cross point.

Multistage Switch



- ☐ The limitations of crossbar switch is removed by multistage switch. In fact it combines cross bar switches in several stages.
- ☐ In multistage switching, devices are linked to switches that, in turn are linked to a hierarchy of other switches.

Time-division multiplexed switch

- Time slot interchange reads bits from incoming slots in each frame and writes these into a register. Call setup would have created a permutation table for how the contents are read out.
- These switches are only used in voice calling.

Examples of Circuit Switched Network

- Public switched telephone network (PSTN)
- ISDN B-channel
- Circuit Switched Data (CSD) and High-Speed Circuit-Switched Data (HSCSD) service in cellular systems such as GSM
- Datakit
- X.21 (Used in the German DATEX-L and Scandinavian DATEX circuit switched data network)
- Optical mesh network

X.25

- *X.25 (ITU-it)* is protocol standard for WAN communications
- It defines how connections between user devices and network devices are established and maintained.
- X.25 is designed to operate effectively regardless of the type of systems connected to the network.
- It is typically used in the packet-switched networks (PSNs) of common carriers, such as the telephone companies
- Subscribers are charged based on their use of the network.

X.25

- The development of the X.25 standard was initiated by the common carriers in the 1970s.
- At that time, there was a need for WAN protocols capable of providing connectivity across public data networks (PDNs)
- X.25 is now administered as an international standard by the ITU-T.

X.25 Devices and Protocol Operation

X.25 network devices fall into three general categories:

1. Data Terminal Equipment (DTE),
2. Data Circuit-terminating Equipment (DCE),
3. Packet-switching Exchange (PSE)

Data Terminal Equipment (DTE),

Data terminal equipment devices are end systems that communicate across the X.25 network.

They are usually

terminals,
personal computers, or network hosts,
and are located on the premises of individual
subscribers.

Data Circuit-terminating Equipment (DCE),

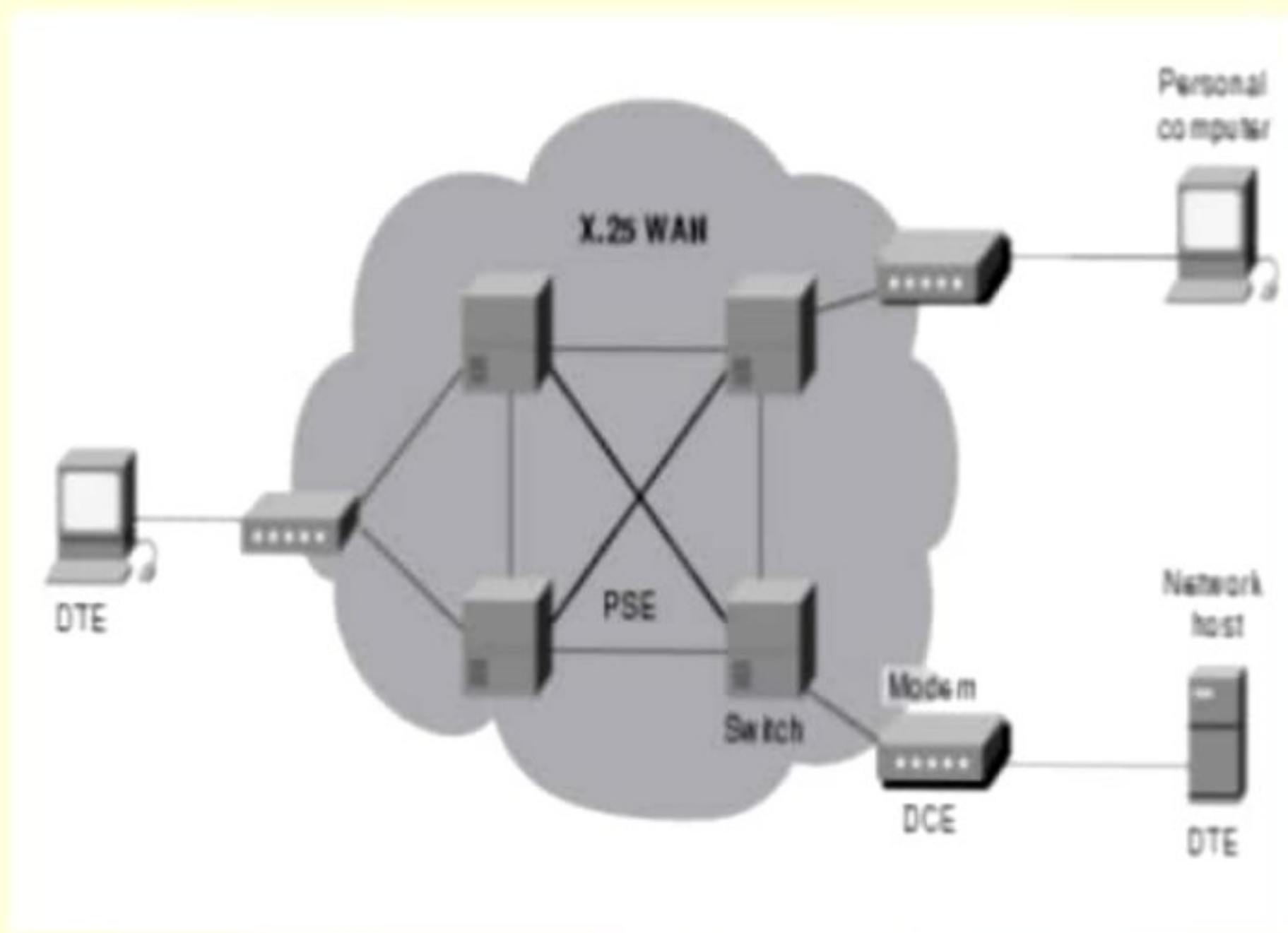
DCE devices are communications devices, such as modems and packet switches, that provide the interface between DTE devices and a PSE, and are generally located in the carrier's facilities.

PSEs are switches that compose the bulk of the carrier's network. They transfer data from one DTE device to another through the X.25 PSN.

Packet-switching Exchange (PSE)

- PSEs are switches that compose the bulk of the carrier's network. They transfer data from one DTE device to another through the X.25 PSN

DTEs, DCEs, and PSEs Make Up an X.25 Network



Two types of X.25 virtual circuits exist: switched and permanent.

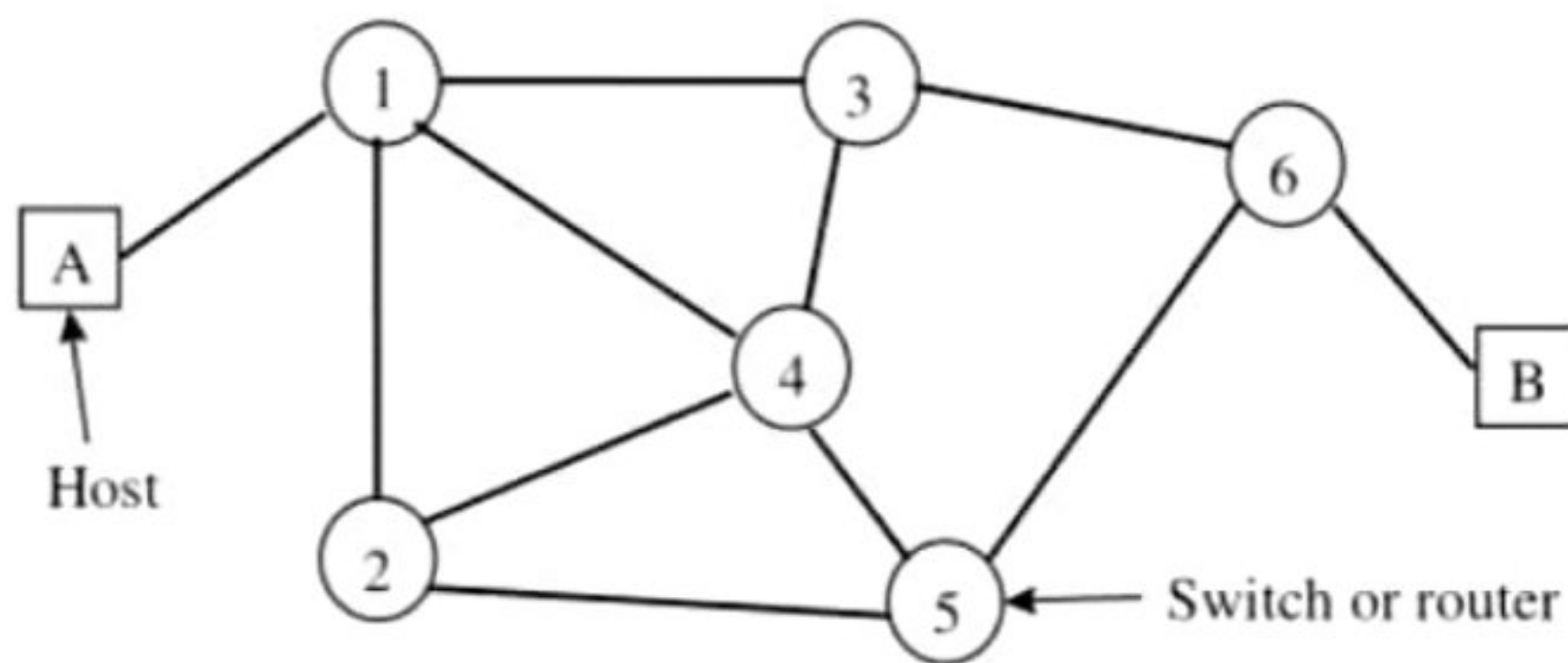
Switched virtual circuits (SVCs) are temporary connections used for irregular data transfers. They require that two DTE devices establish, maintain, and terminate a session each time the devices need to communicate.

Permanent virtual circuits (PVCs) are permanently established connections used for frequent and consistent data transfers. PVCs do not require that sessions be established and terminated. Therefore, DTEs can begin transferring data whenever necessary because the session is always active

Routing in packet switching networks

- Routing is a key function: determine a (best) path from any source to any destination
- There exist multiple paths
- Which path is best?
- Depend on objective:
 - Minimize number of hops
 - Minimize end-to-end delay
 - Maximize available bandwidth
- Must have global knowledge about network state to perform this task

An example of a packet-switch network



Paths: 1-3-6, 1-4-3-6, 1-2-5-6, ...

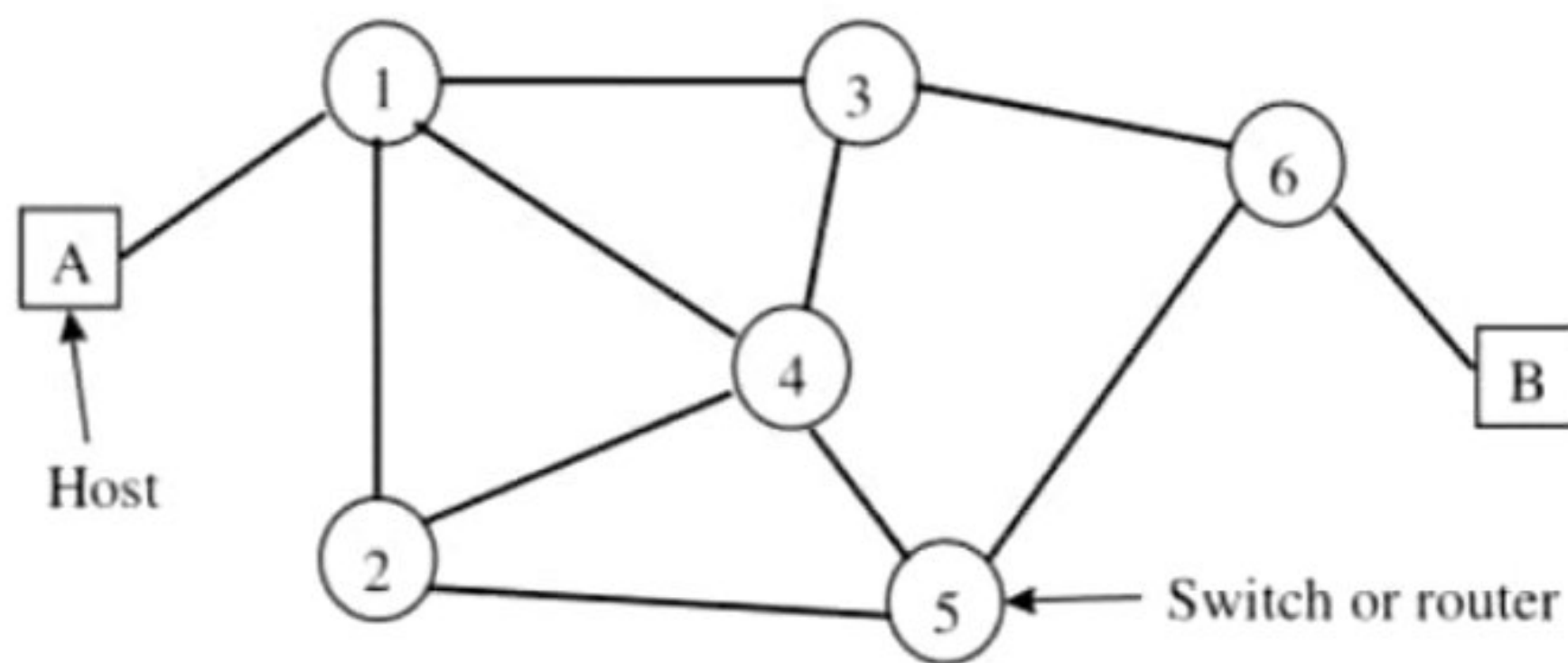
Criteria for a good routing algorithm

1. Correctness: correct route and accurate delivery of packets
2. robustness: adaptive to changes of network topology and varying traffic load
3. Cleverness: ability to detour congestion links and determine the connectivity of the network.
4. Efficiency: rapid finding of the route and minimization of control messages.

Classification of routing algorithms

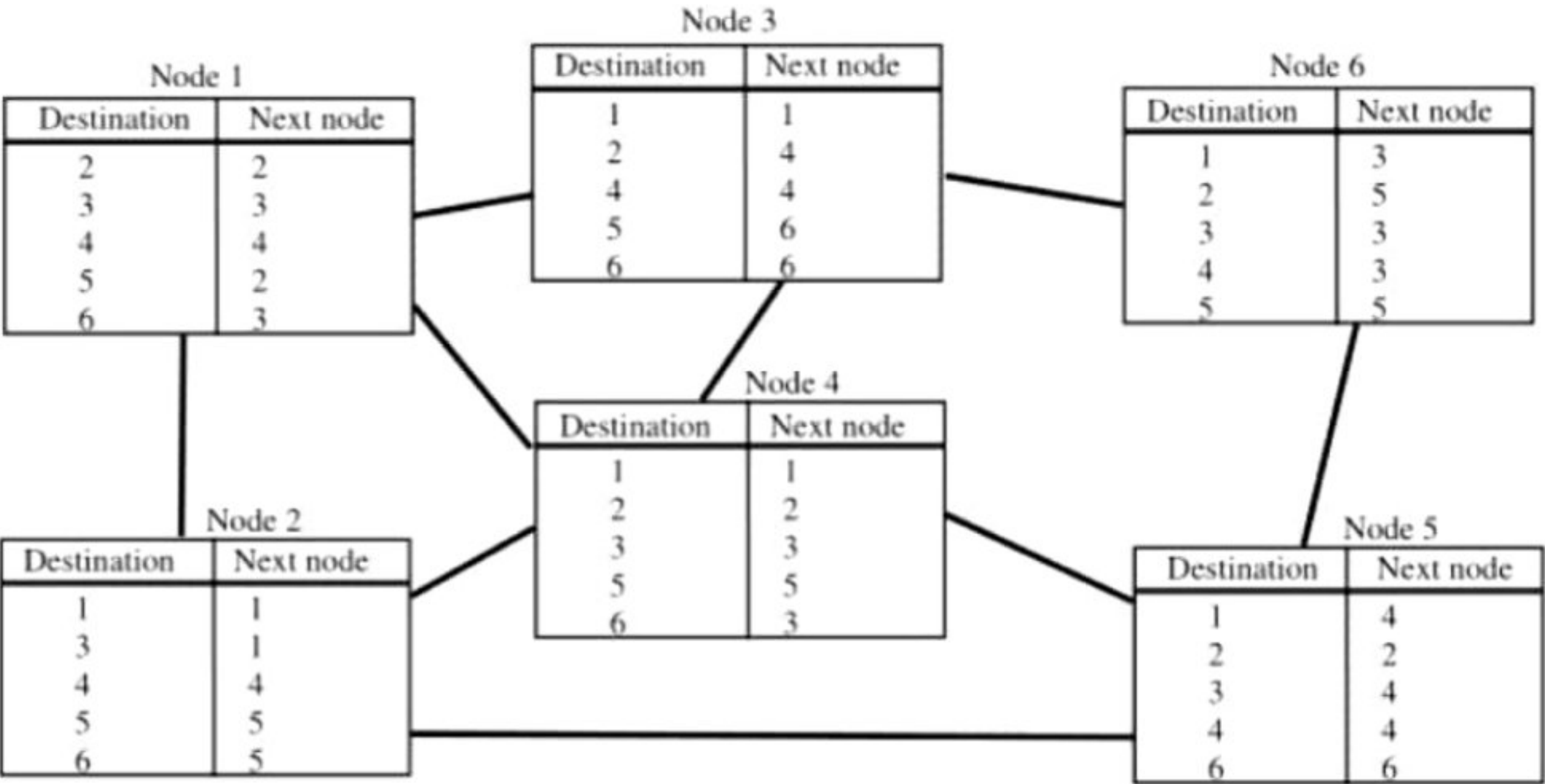
- Static vs. dynamic:
 - Static: manually compute routes, simple, but not scalable and dynamic
 - Dynamic: automatic route computation, adaptive to dynamics of network but complicated
- Centralized vs. distributed
 - Centralized: a center entity computes all routes and load the routes into all routers, but not scalable
 - Distributed: routers exchange topology information and perform own computation of routes, but inconsistent and loop routes.
- In datagram, routing is based on packet by packet but in VC, routing is executed during setup

An example of a datagram packet-switch network



Paths: 1-3-6, 1-4-3-6, 1-2-5-6, ...

Routing table for datagram packet switching network



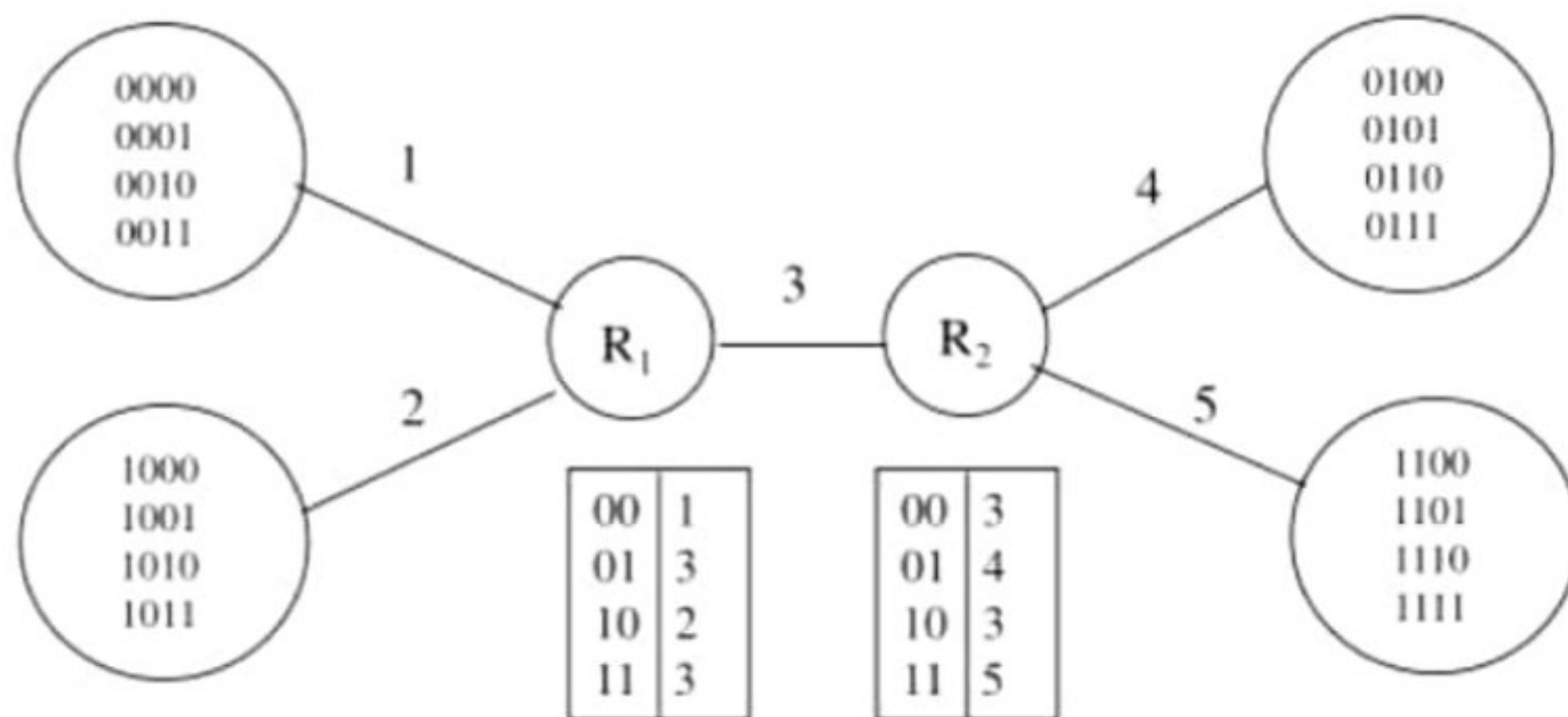
9
Figure 7.26

Hierarchical routing

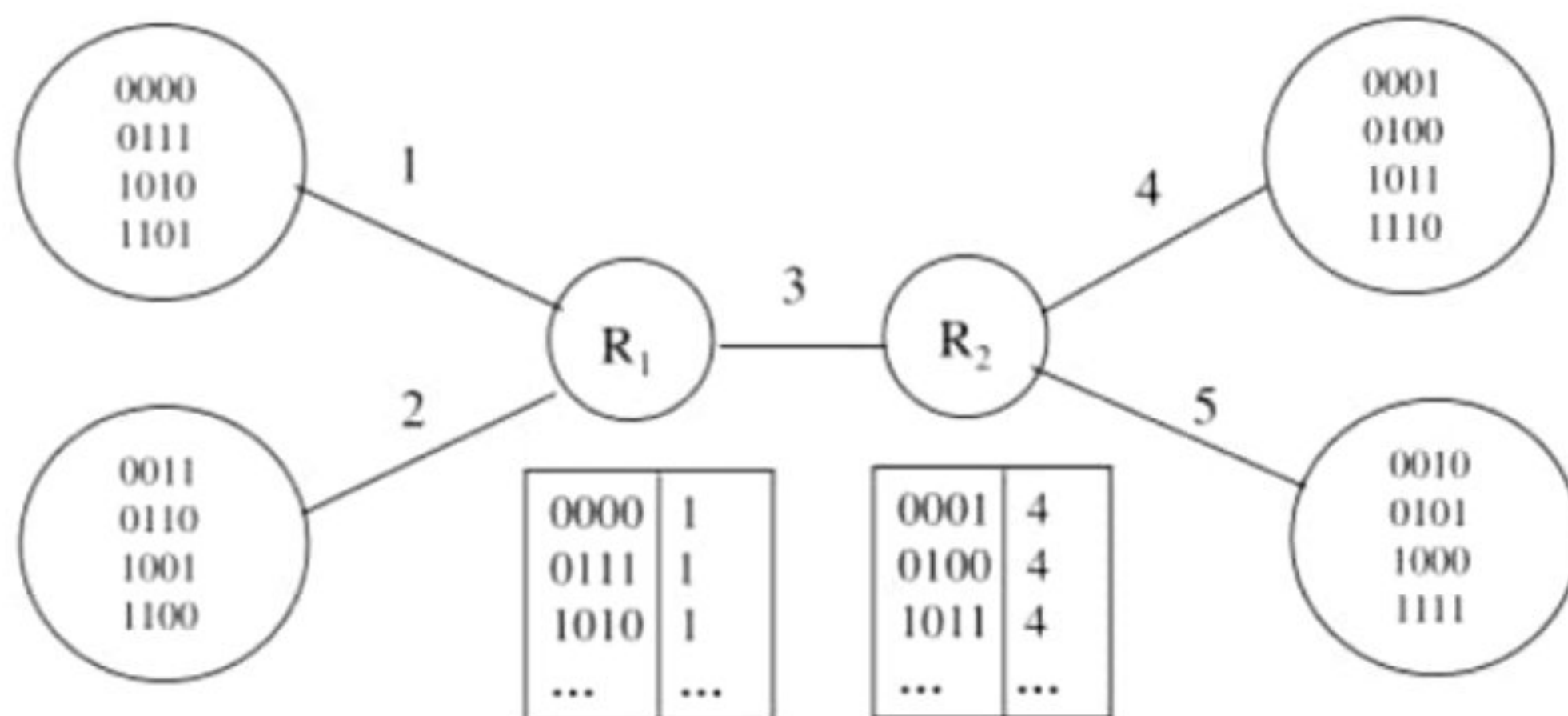
- Size of routing tables will become extremely large when network increases
- Solution is: the hosts close to each other are assigned network addresses with the same prefixes. In a remote routing table, all these hosts are treated as one address, just one entry in the routing table. (only in the local routing table, these hosts are treated separately).
- All packets towards to these hosts are forwarded to this area from remote area based on remote routing table and further forwards to the specific host based on local routing table.
- Therefore hierarchical addressing.

Hierarchical routing table

(a)



(b)

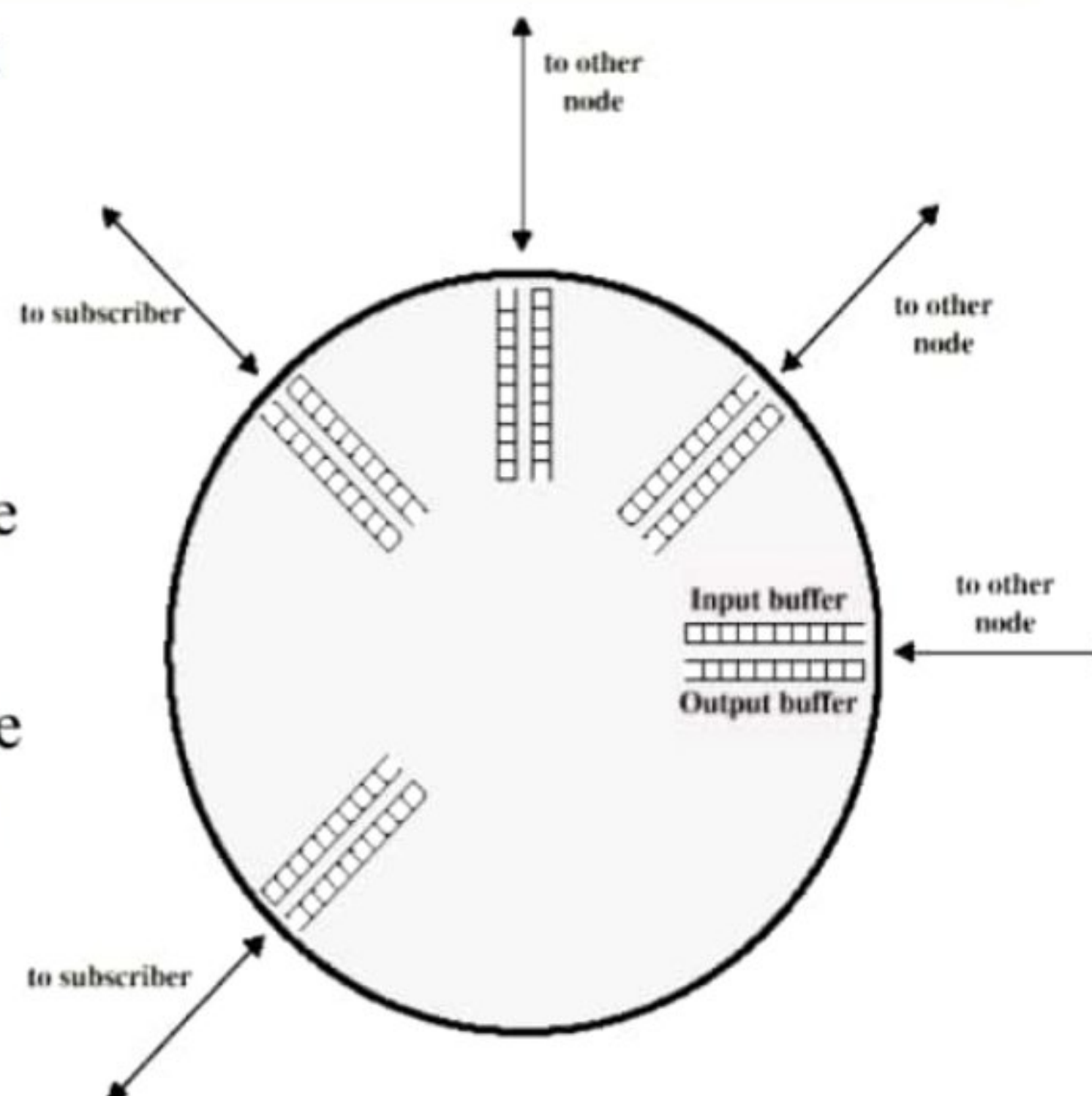


What Is Congestion?

- Congestion occurs when the number of packets being transmitted through the network approaches the packet handling capacity of the network
- Congestion control aims to keep number of packets below level at which performance falls off dramatically
- Data network is a network of queues
 - Can congestion occur at Circuit Switching network?
- Generally 80% utilization is critical
- Finite queues mean data may be lost

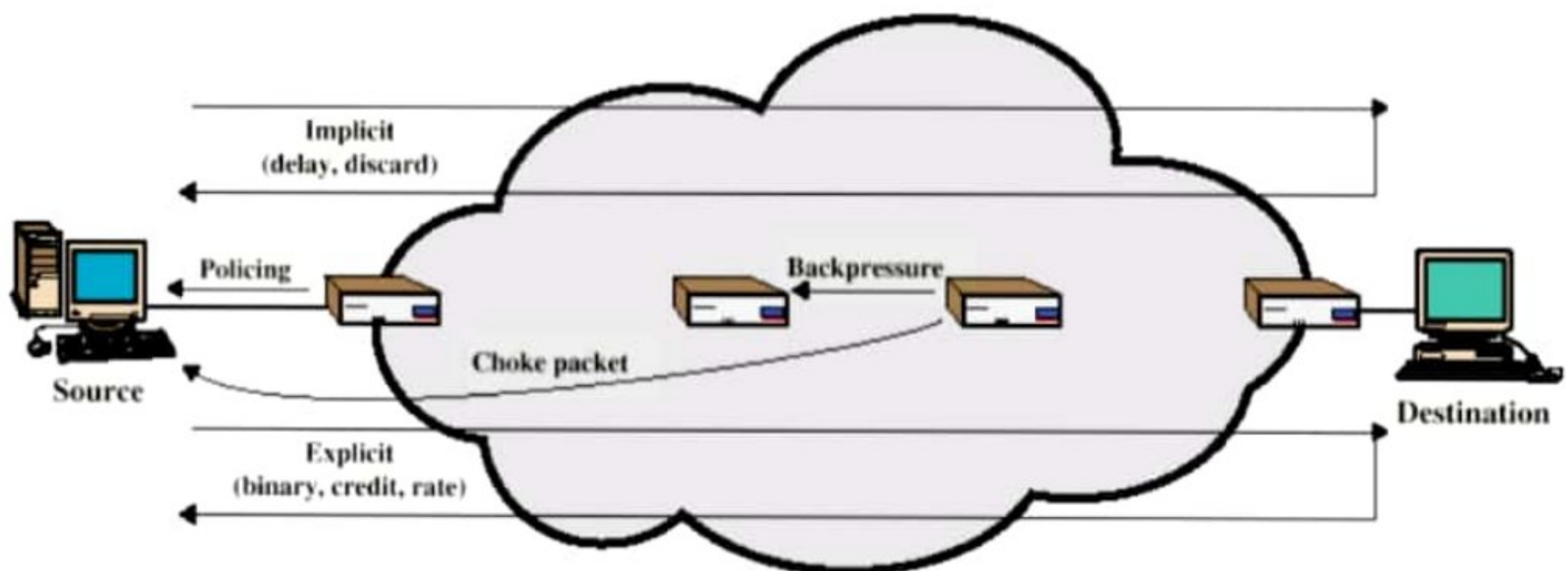
Effects of Congestion

- Packets arriving are stored at input buffers -> Routing decision made -> Packet moves to output buffer
- Packets **queued** for output transmitted as fast as possible
 - Statistical TDM
- If packets arrive **too fast** to be routed/output, buffers fill up
 - Discard packets
 - Flow control



Mechanisms for Congestion Control

- Backpressure (connection oriented hop-by-hop net flow control) : **X.25**
- Choke Packet (a control packet from congested node) : crude
- Implicit Congestion Signaling
- Explicit Congestion Signaling



Backpressure

- If node becomes congested it can **slow down or halt** flow of packets from other nodes
- May mean that other nodes have to apply **control** on incoming packet rates
- Propagates back to **source**
- Can **restrict** to logical connections generating most traffic
- Used in **connection oriented** that allow hop-by-hop congestion control (e.g. X.25)
- Not used in ATM nor frame relay
- Only recently developed for IP

Choke Packet

- Control packet
 - Generated at congested node
 - Sent to source node
 - e.g. ICMP source quench
 - From router or destination
 - Source cuts back until no more source quench message
 - Sent for every discarded packet, or anticipated
- Rather crude mechanism

Implicit Congestion Signaling

- Transmission delay may increase with congestion
- Packet may be discarded
- Source can detect these as implicit indications of congestion -> responsibility of end systems
- Useful on connectionless (datagram) networks
 - e.g. IP based
 - (TCP includes congestion and flow control - see chapter 17)

Explicit Congestion Signaling

- Network alerts end systems of increasing congestion
- End systems take steps to reduce offered load
- Typically used in connection-oriented network
 - Backwards
 - Congestion avoidance in opposite direction to packet required
 - Forwards
 - Congestion avoidance in same direction as packet required ??
- Categories of Explicit Signaling
 - Binary: A bit set in a packet indicates congestion
 - Credit based
 - Indicates how many packets source may send
 - Common for end-to-end flow control
 - Rate based
 - Supply explicit data rate limit
 - e.g. ATM

Congestion Control in Packet Switched Networks

- Send **control packet** to some or all source nodes
 - Requires **additional traffic** during congestion
- Rely on **routing information**
 - May vary too rapidly
- End-to-end **probe** packets
 - Adds to overhead
- Add **congestion info** to packets as they cross nodes
 - Either backwards or forwards

Traffic management and QoS

- Purpose of traffic management is to provide QoS.
- Mechanisms:
 - Control load on links and switches
 - Set priority and scheduling at routers/multiplexers to provide differentiated treatments to different packets.
 - Perform policing and shaping (admission control)
 - Congestion control.
- For a packet, we are interested in
 - End-to-end delay, also jitter (variation of delay)
 - Packet loss

Approaches to traffic management

- Queue strategies (control sharing of bandwidth among users):
 - FIFO (First In First Out):
 - all arriving packets are put in a common queue and sent in the order of arrival.
 - Packets are discarded when queue (i.e., buffer) is full at the time of arrival
 - Packet length, queue size, and interarrival time affect the performance
 - *A high rate user will deprive other users of transmitting packets.*
 - FIFO with discard priority
 - Packets are classified as different types, only discard low priority packets.
 - Fair Queues
 - Every user flow has a logical queue, all the queues shares bandwidth equally.
 - Weighted Fair Queue
 - Every user flow has a logical queue, but each queue has a specific weight, queues shares bandwidth based on their weights.
 - The weights may be based on types of traffic, or how much payment.

Random Early Detection (RED)

- Problem with fair queue: in core network, too many flows at the same time and tracking the states of all flows is difficult.
- One solution is having a limited number of logical queues with each for a given class of flows. But the bad sender may hog the buffer resource.
- So RED: randomly drop packets before buffer overflows.
 - A higher rate source would suffer higher dropped packets.
 - Two thresholds: min_{th} and max_{th} ,
 - Below min_{th} , no drop,
 - From $min_{th} \rightarrow max_{th}$, randomly drop arriving packets with increasing probability
 - Above max_{th} , drop all arriving packets.

ATM Traffic Management

- High speed, small cell size, limited overhead bits
- Requirements & Challenges
 - Majority of traffic not responsive to flow control (e.g. voice, video)
 - Feedback slow due to small transmission time compared with propagation delay
 - Wide range of application demands
 - Different traffic patterns
 - Different network services
 - High speed switching and transmission increases volatility
 - Fluctuation in routing policy and flow control

Traffic & Congestion Control Framework

- ATM layer traffic and congestion control should support QoS classes for **all** foreseeable network **services**
- Should not rely on AAL protocols that are network specific, nor higher level application specific protocols -> **more general**
- Should **minimize** network and end-to-end system **complexity**
- **Determine** whether a given new connection can be accommodated
- **Agree** performance parameters with subscriber -> **contract**

Traffic Management & Congestion Control Techniques

- Resource management using virtual paths
- Connection admission control
- Usage parameter control (UPC)
- Selective cell discard
- Traffic shaping

Congestion control in packet switching networks

- When more incoming packets than out-going capacity, buffer is needed
- If the situation lasts too long, buffer will be full, packets be discarded, congestion occurs.
- Retransmission of lost/discard packets worsen congestion
- As a result, the throughput will be very low.
- Some ways are needed to control and solve congestion

Congestion control in packet switching networks

Question: is it OK to increase buffer size?

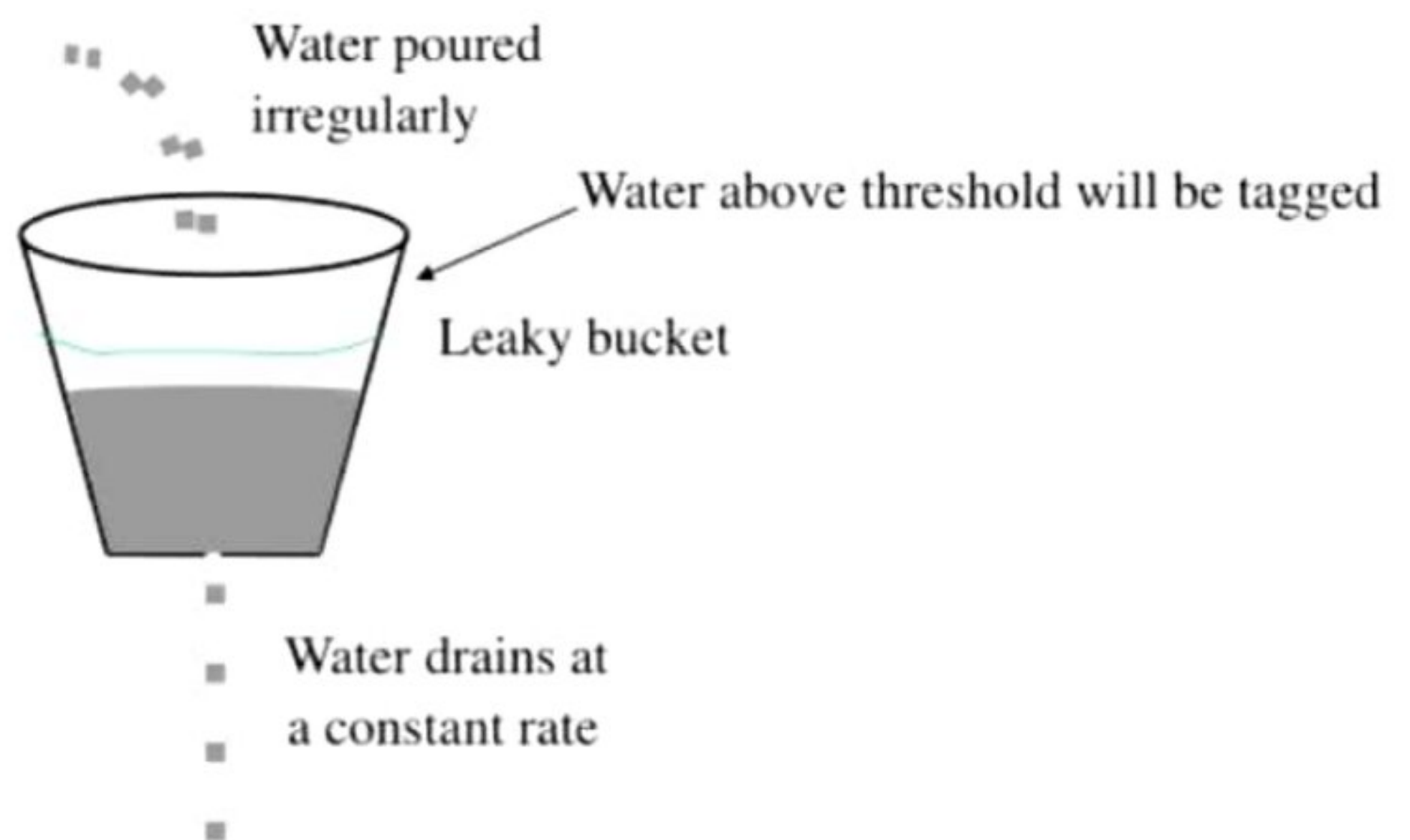
Not OK.

1. Buffer is larger, then waiting time is longer. It will cause time out and retransmit packets, thus more congestion. If buffer size is infinite, then packet can delay forever.

Congestion control is a very hard problem.

Approaches to congestion control

- Open-loop (preventive approaches):
 - If a traffic flow will degrade the network performance and QoS can not be guaranteed, then reject the traffic flow from the beginning. Called admission control.
 - *Leaky bucket* traffic policing:
 - An admitted bad user may violate initial contract and pour too much traffic into network
 - There is a *bucket* which controls a *constant rate* flowing into network.
 - The user packets are first poured into the bucket, instead of to network.
 - Once amount of packets into bucket exceeds certain level, the further packets will be tagged. If the bucket is full, the extra packets will be discarded. [leaky bucket](#)
 - Whenever congestion occurs, the tagged packets will be discarded
- Close-loop (after fact approaches):
 - After congestion occurred, eliminate or reduce congestion.



Close-loop control—TCP congestion control

- TCP uses sliding-window for flow control
 - *Advertised window* to tell sender how many bytes to send and guarantee the receiver window never overflow
 - However *advertised window* does not prevent buffers in routers overflow, I.e., congestion.
- Another window: *congestion window* used by sender
 - Sender sends $\min\{\text{advertised window}, \text{congestion window}\}$
 - At beginning, the *congestion window* is set to one maximum size segment.
 - Whenever receiving a ACK, sender increases *congestion window* (double, then linearly)
 - Whenever time-out or a duplicate ACK is received, sender will reduce *congestion window* (half, then linearly).

Bridges

Bridges are used to divide larger networks into smaller sections. They do this by sitting between two physical network segments and managing the flow of data between the two. By looking at the MAC address of the devices connected to each segment, bridges can elect to forward the data (if they believe that the destination address is on another interface), or block it from crossing (if they can verify that it is on the interface from which it came). Figure 3.4 shows how a bridge can be used to segregate a network.



Bridges can also be used to connect two physical LANs into a larger logical LAN.

When bridges were introduced, the MAC addresses of the devices on the connected networks had to be entered manually, a time-consuming process that had plenty of opportunity for error. Today, almost all bridges can build a list of the MAC addresses on an interface by watching the traffic on the network. Such devices are called *learning bridges* because of this functionality.

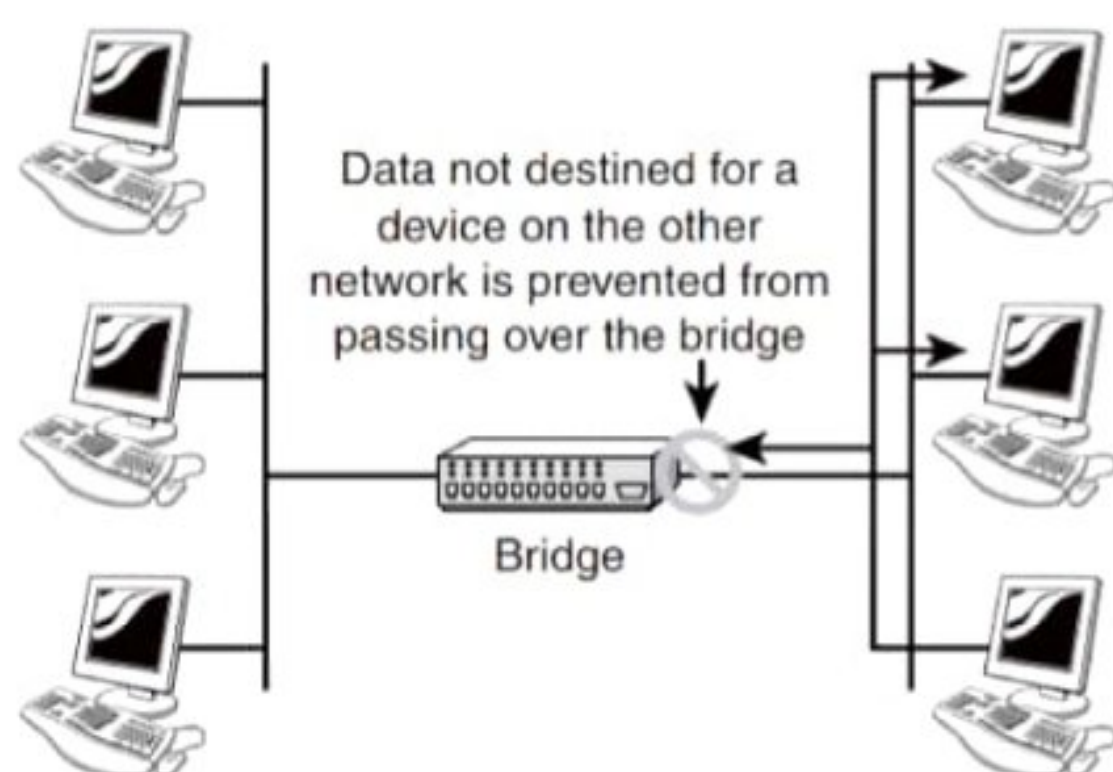


Figure 3.4 How a bridge is used to segregate networks.

Bridge Placement and Bridging Loops

There are two issues that you must consider when using bridges. The first is the bridge placement, and the other is the elimination of bridging loops:

- **Placement**—Bridges should be positioned in the network using the 80/20 rule. This rule dictates that 80% of the data should be local and that the other 20% should be destined for devices on the other side of the bridge.
- **Bridging loops**—Bridging loops can occur when more than one bridge is implemented on the network. In this scenario, the bridges can confuse each other by leading one another to believe that a device is located on a certain segment when it is not. To combat the bridging loop problem, the IEEE 802.1d Spanning Tree protocol enables bridge interfaces to be assigned a value that is then used to control the bridge-learning process.

Types of Bridges

Three types of bridges are used in networks:

- **Transparent bridge**—Derives its name from the fact that the devices on the network are unaware of its existence. A transparent bridge does nothing except block or forward data based on the MAC address.
- **Source route bridge**—Used in Token Ring networks. The source route bridge derives its name from the fact that the entire path that the packet is to take through the network is embedded within the packet.
- **Translational bridge**—Used to convert one networking data format to another; for example, from Token Ring to Ethernet and vice versa.

Today, bridges are slowly but surely falling out of favor. Ethernet switches offer similar functionality; they can provide logical divisions, or segments, in the network. In fact, switches are sometimes referred to as multiport bridges because of the way they operate.

Hubs

At the bottom of the networking food chain, so to speak, are hubs. Hubs are used in networks that use twisted-pair cabling to connect devices. Hubs can also be joined together to create larger networks. *Hubs* are simple devices that direct data packets to all devices connected to the hub, regardless of whether the data package is destined for the device. This makes them inefficient devices and can create a performance bottleneck on busy networks.

In its most basic form, a hub does nothing except provide a pathway for the electrical signals to travel along. Such a device is called a *passive* hub. Far more common nowadays is an *active* hub, which, as well as providing a path for the data signals, regenerates the signal before it forwards it to all of the connected devices. A hub does not perform any processing on the data that it forwards, nor does it perform any error checking.

Hubs come in a variety of shapes and sizes. Small hubs with five or eight connection ports are commonly referred to as *workgroup hubs*. Others can accommodate larger numbers of devices (normally up to 32). These are referred to as *high-density devices*. Because hubs don't perform any processing, they do little except enable communication between connected devices. For today's high-demand network applications, something with a little more intelligence is required. That's where switches come in.

Switches

Like hubs, *switches* are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device. The difference between hubs and switches is in how the devices deal with the data that they receive. Whereas a hub forwards the data it receives to all of the ports on the device, a switch forwards it only to the port that connects to the destination device. It does this by *learning* the MAC address of the devices attached to it, and then by matching the destination MAC address in the data it receives. Figure 3.1 shows how a switch works.

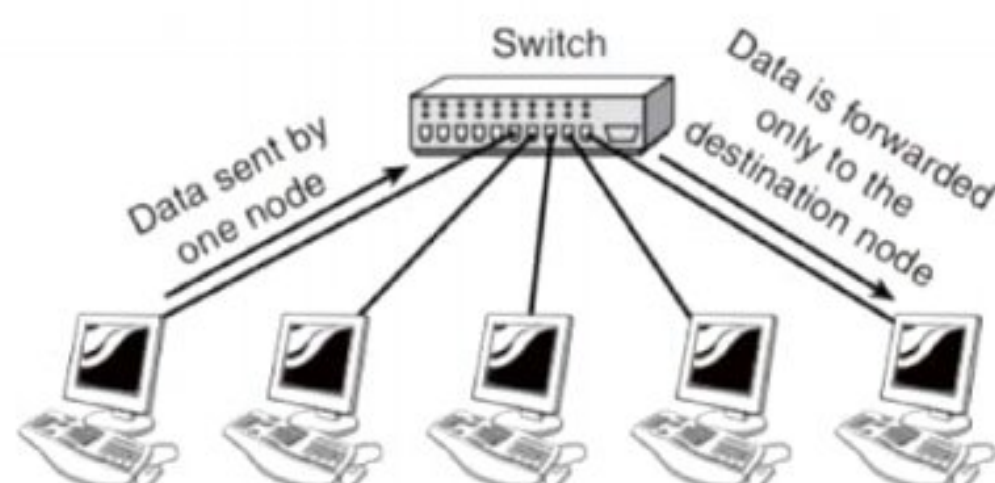


Figure 3.1 How a switch works.

By forwarding data only to the connection that should receive it, the switch can improve network performance in two ways. First, by creating a direct path between two devices and controlling their communication, it can greatly reduce the number of collisions on the network. As you might recall, collisions occur on Ethernet networks when two devices attempt to transmit at exactly the same time. In addition, the lack of collisions enables switches to

communicate with devices in full-duplex mode. In a full-duplex configuration, devices can send and receive data from the switch at the same time. Contrast this with half-duplex communication, in which communication can occur in only one direction at a time. Full-duplex transmission speeds are double that of a standard, half-duplex, connection. So, a 10Mbps connection becomes 20Mbps, and a 100Mbps connection becomes 200Mbps.

The net result of these measures is that switches can offer significant performance improvements over hub-based networks, particularly when network use is high.

Irrespective of whether a connection is at full or half duplex, the method of switching dictates how the switch deals with the data it receives. The following is a brief explanation of each method:

- **Cut-through**—In a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is very fast, but creates the possibility of errors being propagated through the network, as there is no error checking.

- **Store-and-forward**—Unlike cut-through, in a store-and-forward switching environment, the entire packet is received and error checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error checking process takes a relatively long time, and store-and-forward switching is considerably slower as a result.
- **FragmentFree**—To take advantage of the error checking of store-and-forward switching, but still offer performance levels nearing that of cut-through switching, FragmentFree switching can be used. In a FragmentFree-switching environment, enough of the packet is read so that the switch can determine whether the packet has been involved in a collision. As soon as the collision status has been determined, the packet is forwarded.

LAN PROTOCOL ARCHITECTURE

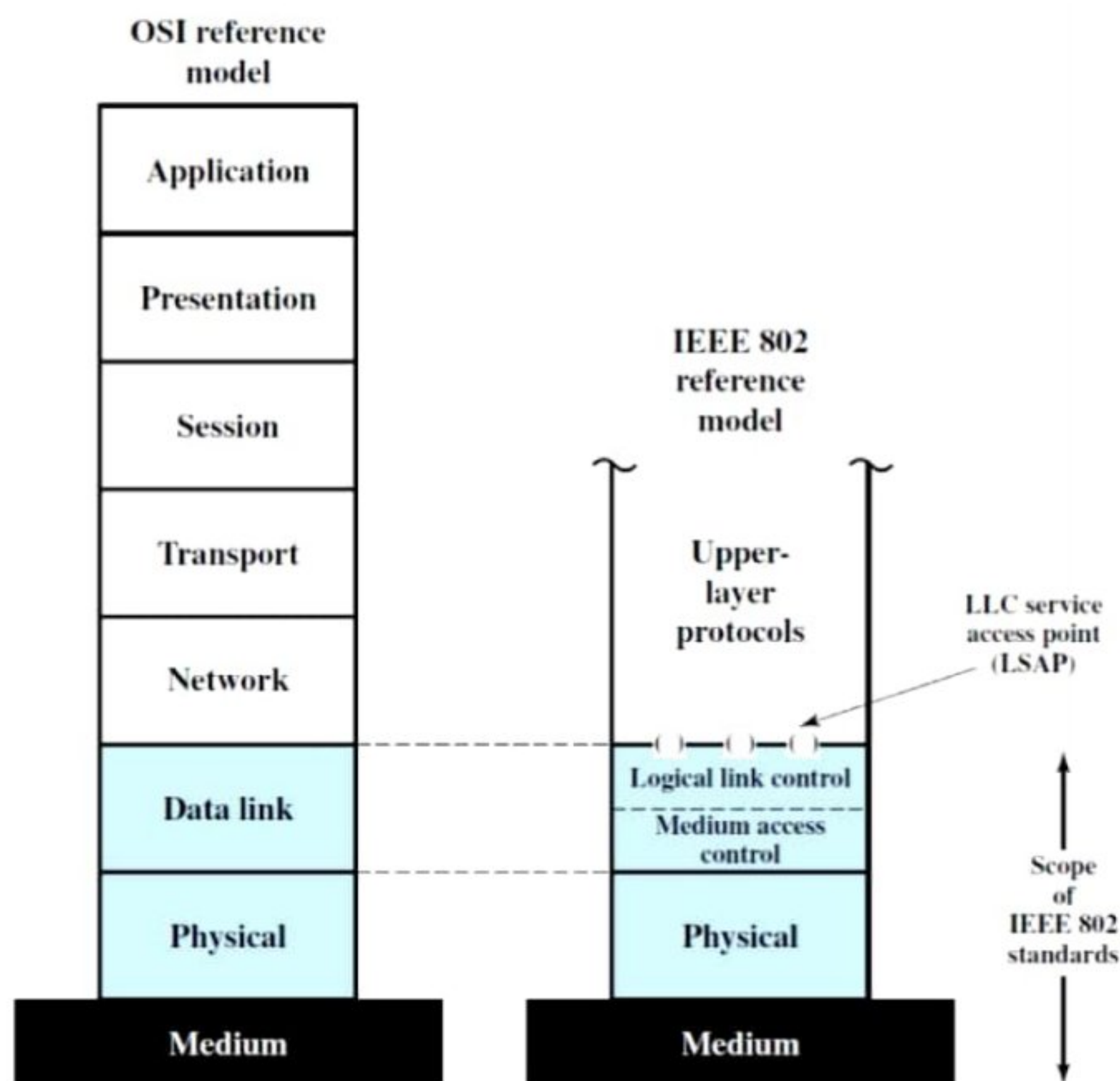
- The basic functions of a LAN is organized by set of layering protocols.
- **IEEE 802 Reference Model**
Protocols defined specifically for LAN and MAN transmission address issues relating to the transmission of blocks of data over the network
- In **OSI** (Open System Interconnection), higher layer protocols (layer 3 or 4 and above) are independent of network architecture and are applicable to LANs , MANs, and WANs .

LAN PROTOCOL ARCHITECTURE

- A discussion of LAN protocols is concerned principally with lower layers of the OSI model.
- This architecture was developed by the IEEE 802 LAN standards committee
- It is generally referred to as the IEEE 802 reference model.

LAN PROTOCOL ARCHITECTURE

- Working from the bottom up, the lowest layer of the IEEE 802 reference model corresponds to the **physical layer** of the OSI model and includes such functions as :
 - Encoding / decoding of signals
 - Preamble generation/removal
 - Bit transmission / reception
- In addition, the physical layer of the 802 model includes a specification of the transmission medium and the topology.



IEEE 802 Protocol Layers Compared to OSI Model

LAN PROTOCOL ARCHITECTURE

- Above the physical layer are the functions associated with providing service to LAN users. These include the following:
 1. **On transmission**, assemble data into a frame with address and error-detection fields.
 2. **On reception**, disassemble frame and perform address recognition and error detection.
 3. Govern access to the LAN transmission medium .
 4. Provide an interface to higher layers and perform flow and error control .
 - These are functions typically associated with OSI layer 2 (Data Link Layer) .
-

LAN PROTOCOL ARCHITECTURE

- The set of functions in the last point are grouped into a **logical link control (LLC) layer**.
- The functions in the first three points are treated as a separate layer, called **medium access control (MAC)**.
- **The separation** is done for the following reasons:
 1. The logic required to manage access to a shared access medium is not found in traditional layer 2 data link layer .
 2. For the same LLC, several MAC options may be provided .

LAN PROTOCOL ARCHITECTURE

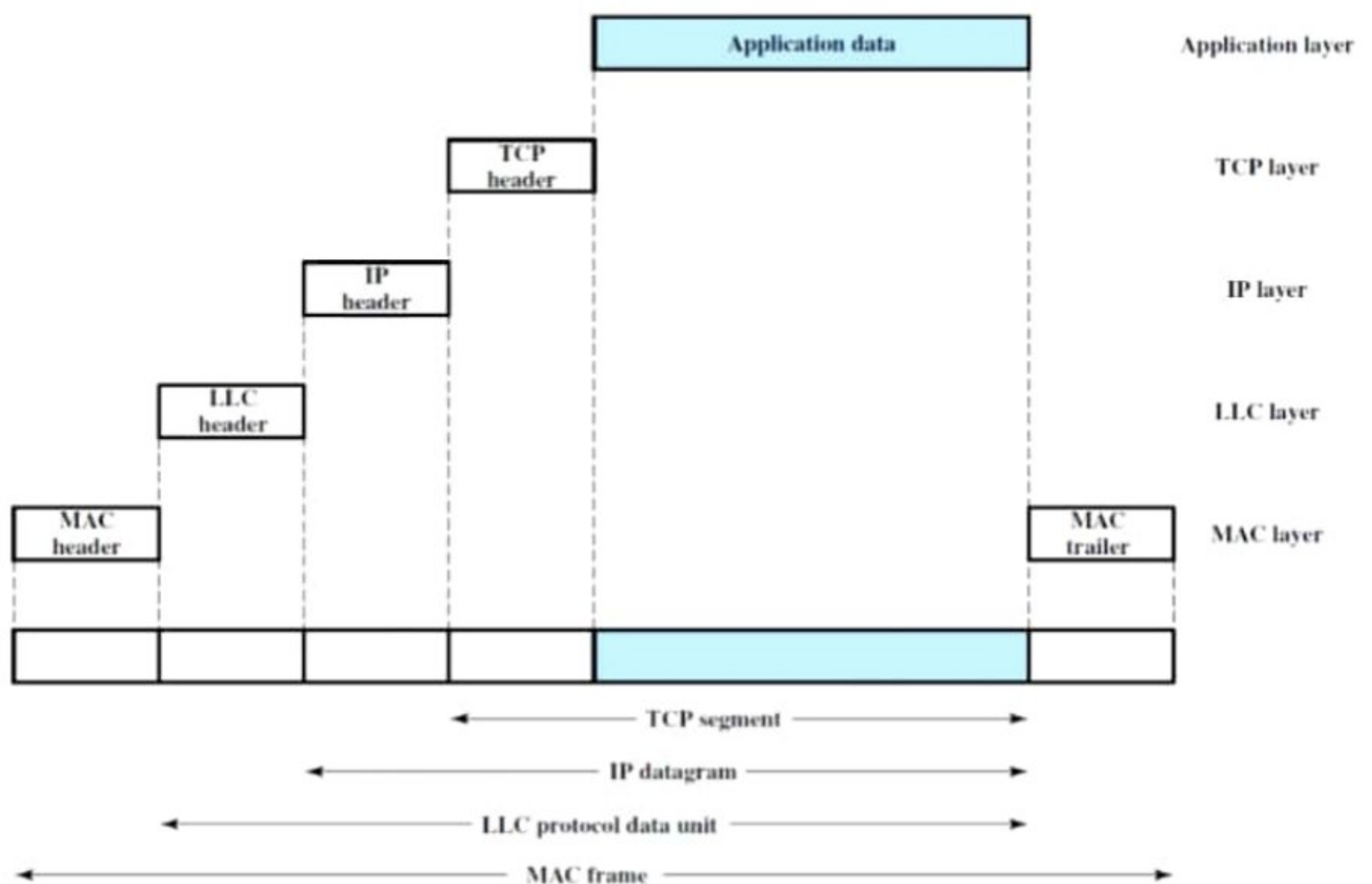


Figure illustrates the relationship between the levels of the architecture

3.3 Network Principles

- Packet Transmission

- Packet transmission superseded telephone/telegraph switched network
- Messages are packetized and packets are queued, buffered (in local storage), and transmitted when lines are available using asynchronous transmission protocol

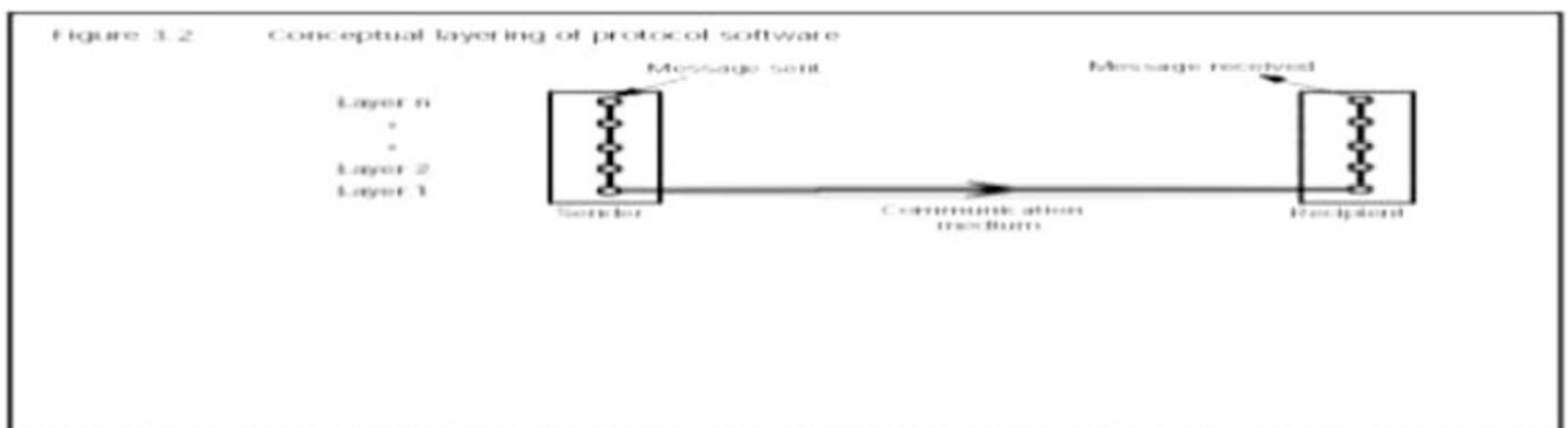
- Data Streaming

- Multimedia data can't be packetized due to unpredicted delays. AV data are streamed at higher frequency and bandwidth at continuous flow rate
- Delivery of multimedia data to its destination is time-critical / low latency – requiring end-to-end predefined route
- E.g. networks: ATM, IPv6 (next generation – will separate 'steamed' IP packets at network layer; and use RSVP (resource reserv. protocol) resource/bandwidth prealloc and RTP play-time/time-reqs (real-time transp protocol) at layers 3 & 1, respectively) to work

- **Switching Schemes – 4 Kinds of switching methods typically used**
 - **Broadcast** – no switching logic, all nodes 'see' signals on circuits/cells (e.g., Ethernet, wireless networks)
 - **Circuit Switching** – Interconnected segments of circuits via switches/exchange boxes, e.g., POTS (Plain Old Telephone System)
 - **Packet Switching** – Developed as computing tech advanced with processors and storage spaces using store-and-forward algorithms and computers as switches. Packets are not sent instantaneously, routed on different links, reordered, may be lost, high latency (few μ sec – msec). Extension to switch audio/video data brought integration of 'digitized' data for computer comm., telephone services, TV, and radio broadcasting, teleconferencing
 - **Frame Relay** – PS (not instantaneous, just an illusion!), but FR, which integrates CS and PS techniques, streams smaller packets (53 byte-cells called frames) as bits at processing nodes. E.g., ATM

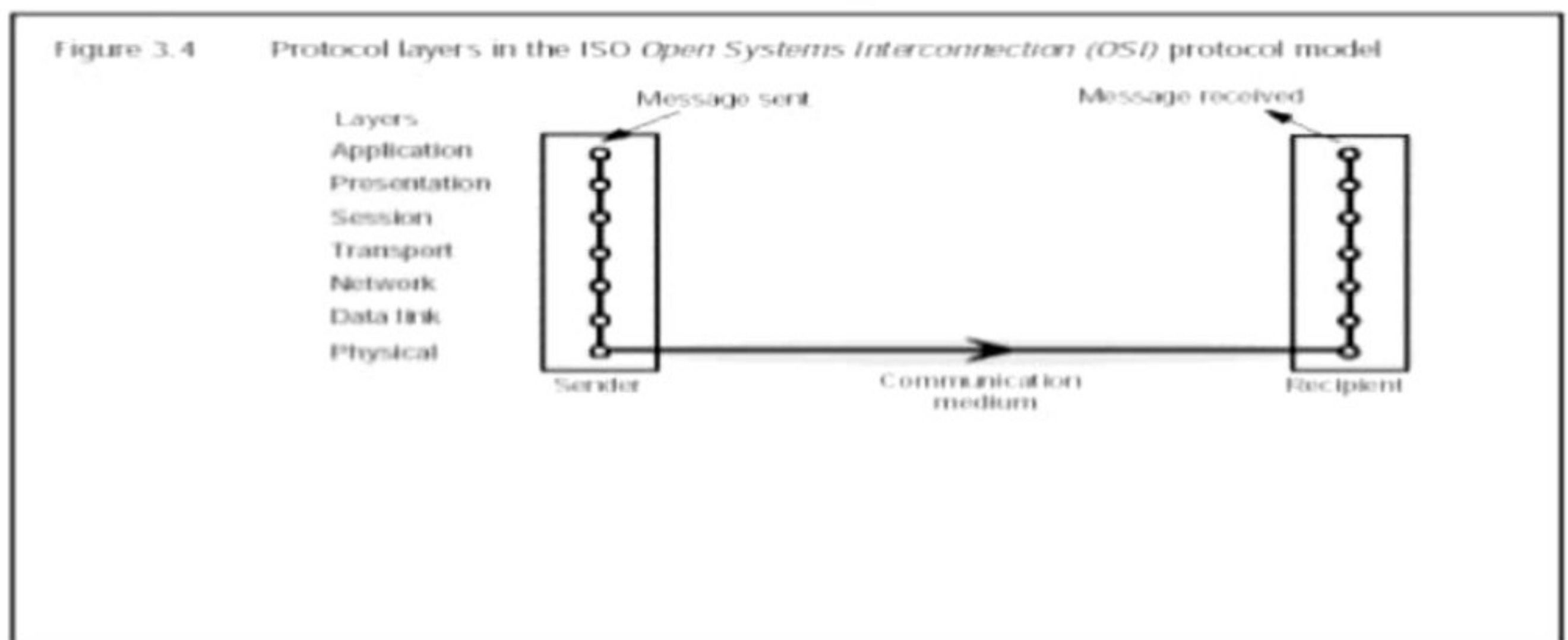
• **Protocols –**

- Protocols – implemented as pairs of software modules in send/receive nodes,
 - Specify the sequence of messages for transmission
 - Specify the format of the data in the messages
- Protocols Layers – layered architecture, following the OSI suite
 - packets are communicated as peer-to-peer transmission but effected vertically across layers by encapsulation method over a physical medium



Protocols Suites – The 7-layered architecture of the ISO-OSI

- Each layer provides service to the layer above it and extends the service provided by the layer below it
 - A complete set of protocol layers constitute a suite or stack
 - Layering simplifies and generalizes the software interface definitions, but costly overhead due to encapsulations and protocol conversions



• Protocols

Addressing:

Transport layer addressing scheme, composed of network address (of host), i.e., the IP address, and the port number. The combined address is typically called a socket or transport address of the Transport Layer. Each host may have several port #s for different kinds of protocols (e.g., for HTTP, FTP) or services. Hosts send port numbers to clients to establish, e.g., TCP, connection. Finding port # on server hosts in DS for arbitrary services requires RMI/RPC type of schemes

• Packet Delivery (at network layer):

- Datagram – one-at-a-time, hop-by-hop transmission of packets with no storing of copies at switches, no setup of paths, unreliable and failures are handled by hosts, each packet contains full network address of source-to-destination, e.g., Internet IP datagram in network layer and some wireless networks
- Virtual circuits – set up of end-to-end path/address held in switch tables, no network address in packets except VC #, switching at intermediate nodes, more reliable, latency depends on time to use the links/path segments, unlike POTS voice-links VC links can be shared and used/entered in multiple tables, e.g., ATM
[Note: At transport layer, connection-oriented TCP is like virtual circuits, and connection-less UDP is like datagram]

• Internetworking

- Network technologies (or subnets):
 - LANs: Ethernet, ATM networks using different physical, data link, and network layers
 - WANs: Internet, using analog and digital POTS switched technologies, satellite links and wide-area ATM networks, and relying on underlying LANs and MANs
- Internetworking:
 - Integrated network of subnets using
 - 1) unified internetworking addressing scheme for communication between host and any subnet
 - 2) PDU (protocol data unit) format and conversion/handling protocols
 - 3) standards/protocols and devices/switches for interconnecting and addressing component subnets and hosts
 - Network (hardware) components: routers, bridges, hubs, switches
 - Tunneling: Internetworking protocol, e.g., IPv6, for bridging a variety of physical subnets using 'packet encapsulation' techniques. E.g., IPv6 protocol packets encapsulated inside IPv4, IP, ATM PDU's and transported across a sea of IPv4, IP, ATM networks. Another, e.g., MobileIP transmits IP packets to other mobiles by encapsulating IP packets over other networks, Another, e.g., PPP for transmitting IP packets.

• Internet Protocols

- History: 1970's research results. TCP – Transport control protocol, IP – Internet protocol
- Forms a single 'internetworking' protocol (using IP datagram 'encapsulation' methods)
- Many existing application-specific/layer protocols are based on / using TCP/IP i.e., built on top of TCP/IP – (e.g., Web (HTTP), SMTP, POP, FTP, Telnet)
- When TCP is not enough additional higher-level protocol, e.g., SSL (secure socket protocol) for security, can be built atop TCP
- Internet protocols were initially developed for simple ftp and e-mails
- Exceptional networks not using TCP/IP – WAP and protocols for multimedia
- Internet protocols usually layered over existing 'physical' networks, e.g., over Ethernets and over telephone serial lines via PPP for modem connection

INTERNET PROTOCOL OPERATION

8

IP provides a connectionless, or datagram, service between end systems. There are a number of advantages to this approach:

- A connectionless internet facility is flexible. It can deal with a variety of networks, some of which are themselves connectionless. In essence, IP requires very little from the constituent networks.
- A connectionless internet service can be made highly robust. This is basically the same argument made for a datagram network service versus a virtual circuit service.
- A connectionless internet service is best for connectionless transport protocols, because it does not impose unnecessary overhead.