Jai Hoo Satnaryan

CSI. (PART-A)

Date 22/8/23

Page 1

CHAPTER-1.

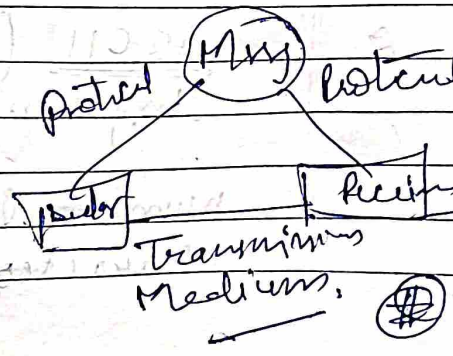
DATA COMMUNICATION COMPONENTS.

Syllabus: Representation of data and data flow, various network topologies, protocols and standards, LAN: wired LAN, wireless LAN, Connecting LAN and virtual LAN, Techniques for Bandwidth utilization: Multiplexing, frequency division, Time division and wave division, concepts on spread spectrum, OSI model, TCP/IP reference model and their comparision

friend 01/09/23

Data: Comp of Data Comp.

1. Message
2. Sender
3. Receiver
4. Transmission Medium
5. Set of rules



Jai Hoo Satnaryan ॐ 01/09/2023

Date | Page | 2

Representation of data and data flow

Representation of data:

Data representation involve Converting of data from its original form into a format that can be easily processed, stored, and transmitted by Computer system.

Different type of data, such as text, numbers, images and multimedia, require specific encoding method to represent them effectively.

Here some Common key encoding method:

1. Binary encoding:- Data is represented using only two symbols typically 0 and 1. Computer use binary code to represent all form of data internally.

2. ASCII (American Standard Code for Information Interchange): ASCII assign a Unique numerical value (8 bits / 1 byte) to each characters and symbol in the English

alphabet, numbers and special characters.

3. Unicode: Unicode is a character encoding standard that aims to represent all character from all language. It provide a Unique code point for each character, allowing international character sets to be used uniformely.

Data flow: It refers to the Moment of data from one device to another within a network.

This process involved several stages:

1. Sender: The Sender (Source device) generate data to be transmitted.

2. Encoding: The data is encoded into a format suitable for transmission. This coding involve Converting text to binary or encoding multimedia data.

3. Transmission: The encoded data is sent over the network medium, such as cables, wireless signals, or optical fibers.

4. Reception: The receiving device capture the transmitted data.

5. Decoding: The received data is decoded back into its original formats.

6. Recipient: The recipient (destination device) processes the data as needed.

Various Network Topologies:

1. Bus Topology: In bus topology, all devices are connected to a single central cable, often called the "bus" or "backbone". Data is transmitted in both directions along the cable.

Advantages:

1. Simple to set up
2. Cost effective
3. Works well for small networks with few devices.

#

Disadvantages

1. If main cable fails, the entire network can be affected.
2. Performance can degrade as more devices are added.

Uses

Commonly used in small office or home networks where simplicity and cost effectiveness are key.

2. Star topology: Each device is connected directly to a central hub or switch. All communication are passes through the central hub.

Advantages

1. Easy to manage, scalable, and if one of the cable fails, doesn't affect the rest of the network.

Disadvantage

1. More expansive Due to central hub.
2. Network performance can be limited by hub capacity.

Uses: Ideal for medium sized network or where centralized managment is imp, like in business setup.

Date
Page

3. Ring Topogy: In a ring topology, devices are connected in a circular or ring-like fashion. Data travel in one direction around the ring.

Advantages

1. Simple to build.
2. If one part fail data can still flow in the opposite Direction

Disadvantage

1. A break in the ring can distrubt the entire network until it's repaired.
2. Adding and removing devices can be challenging.

Uses

Less common today but can be found in specific application where fault tolerance is crucial.

4. Mesh Topogy: In Mesh topology, every device is connected to every other device. There are full mesh and partial

mess configuration.

Advantages

1. It is highly fault tolerant.
2. It offers robustness and redundancy.

Disadvantages

1. It can be expensive and complex due to large no. of connections, especially in full mess setups.

Uses:

Used in critical application such as large data centers and telecommunication networks.

5. Hybrid Topology: A hybrid topology combines two or more different topologies into a single network.

Eg: Combination of star and bus topology.

Advantages

1. It allows for flexibility and customization to meet specific network requirement.

Date
Page

Disadvantages

1. More complex to design and manage them in single topology.

Uses Help to reduce the cost of the overall system.
Use to easily running the systems.

Local Area Networks (LAN):

1. Lalized LAN (Local Area Network) (1) : A new lan is like a network of devices in one place, such as computer in office.

(2) Ethernet Technology: This is the cable that connect devices and lets them chat with each other.

(3) MAC address: Each device has special name (MAC address) so they can recognize each other.

(4) Switches and hubs: They help send data between devices, like traffic signal on the road.

A network that is designed for a limited area such as building or campus.

2. Wireless LANs: It is like a network that talks without any cables, like wifi at home.

(a) wifi Standards (802.11a|b|g|n|ac|ax): These are like different version of wifi that get faster and better.

(b) Security Mechanism: They're like locks on your wifi to keep it safe from strangers.

(c) Frequency Bands: wifi uses radio waves, like different channels on radio.

Connecting and Virtual LAN (VLAN):

Imagine you have two offices in different building. Connecting Connecty LANs means making them offices Communicate like they are in the Same building.

Virtual LAN (VLCAN): Think of VLAN's as invisible walls in your network, separating different parts to keep them Organized and secure.

Date
Page

In easy terms

* Wired lans use cables.
* Wireless lans use wifi
* Connecting lans make different places talk
* VLANs are like secret dividers for your network.

Bandwidth utilization Techniques:

Imagine a highway. and many cars (data signal) want to use it to reach their destinations (other devices).

Dai Hoo Satnaryan 08/09/2025

Bandwidth: The Maximum amount of data transmitted over an internet connection in a given amount of time.

Bandwidth Utilization Techniques

Multiplexing :→ Multiplexing is a crucial techniques in networking and telecommunications

Jai Hoo Satnaryan

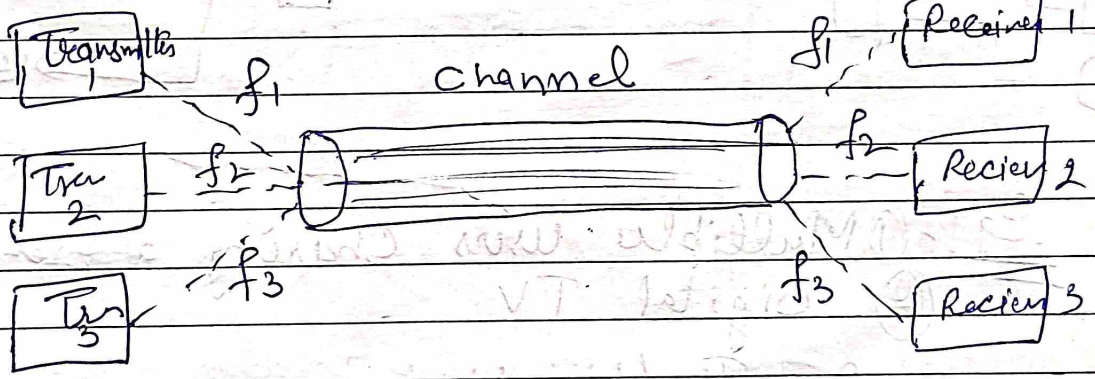
Date 09/09/2023
Page 4

that allow multiple signal or data streams to share a common communication channel. This technique optimizes the utilization of

There are Types of Multiplexing

1. Frequency Division Multiplexing: FDM divides the communication channel into multiple frequency bands or subchannels, each allocated to a specific signal or data stream.

Eg:- broadcast radio, television, Cable television etc.



Advantages:

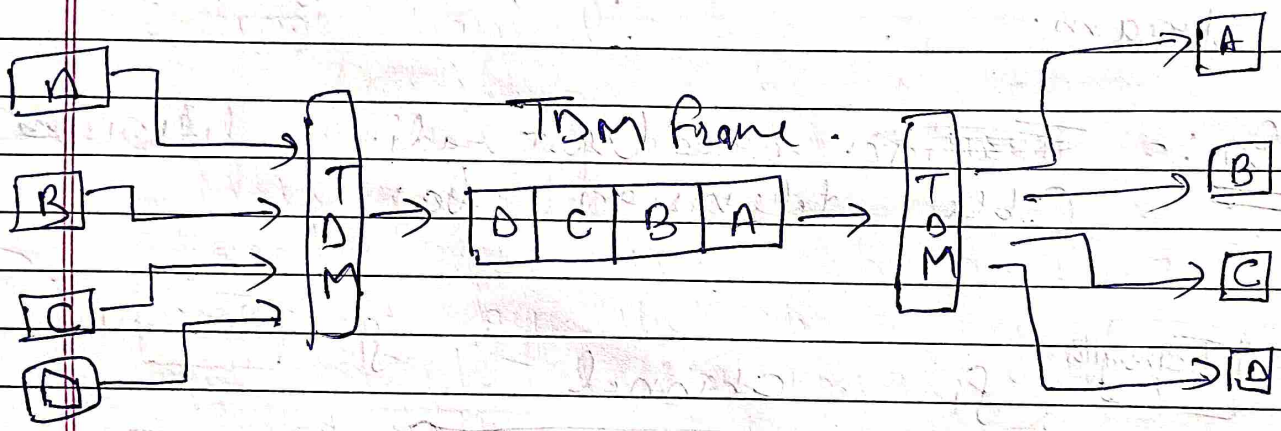
1. Provide dedicated frequency band to each signal.
2. Suitable for analog signal. or Continuous data stream.

Date
Page

Disadv.

1. Efficient when signal have varying data rates.

2. Time Division Multiplexing (TDM) : A Multiplexing technique by which multiple data signals can be transmitted over a common communication channel in different time slots is known as time division multiplexing (TDM).



Eg:- (1) Multiple users sharing a printer
(2) Digital TV.
(3) In Traffic lights.

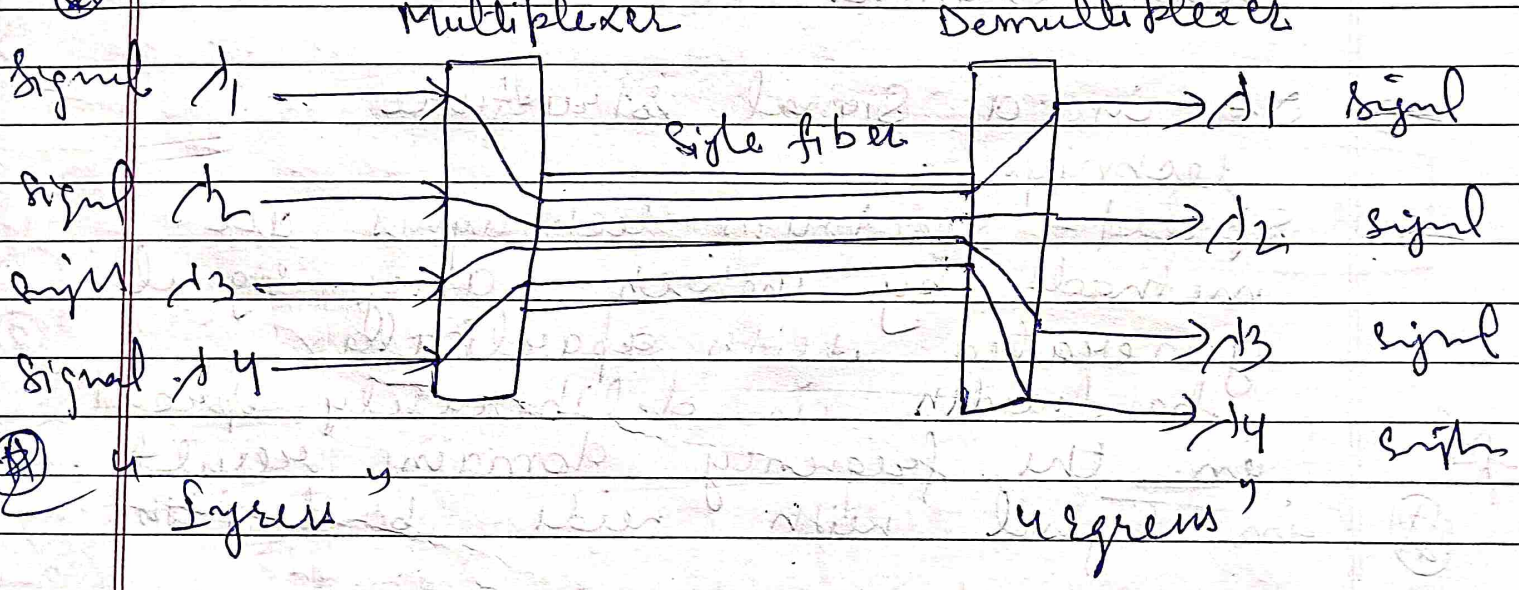
Adv

1. Equal access time for each slots
2. Efficient for digital data streams with fixed data rates.

Disadv.

1. Inflexible for signal with varying data rates
2. Limited scalability for a large no of signals.

3. Wave Division Multiplexing (WDM): It is primarily used in optical communication system, where it combines multiple optical signal with different wavelength (colors of light) into a single optical fiber.



Eg: In high speed optical network, such as for - distance fiber-optics cables and Undersea Cables.

Advs.

1. It increases the bandwidth capacity of optical fibres
2. Enables high capacity data transmission.

Date
Page

Disadv

(1) Require high expensive equipment for bandwidth control.

Concept of spread spectrum

It is a fascinating techniques used in wireless communication channel.

→ It is a signal structure technique.

→ Spread-spectrum techniques are methods by which any signal generated with aparticular bandwidth is deliberately spread in the frequency domain, result in signal with wide bandwidth.

Here, signal may be electrical, electromagnetic or any other signal.

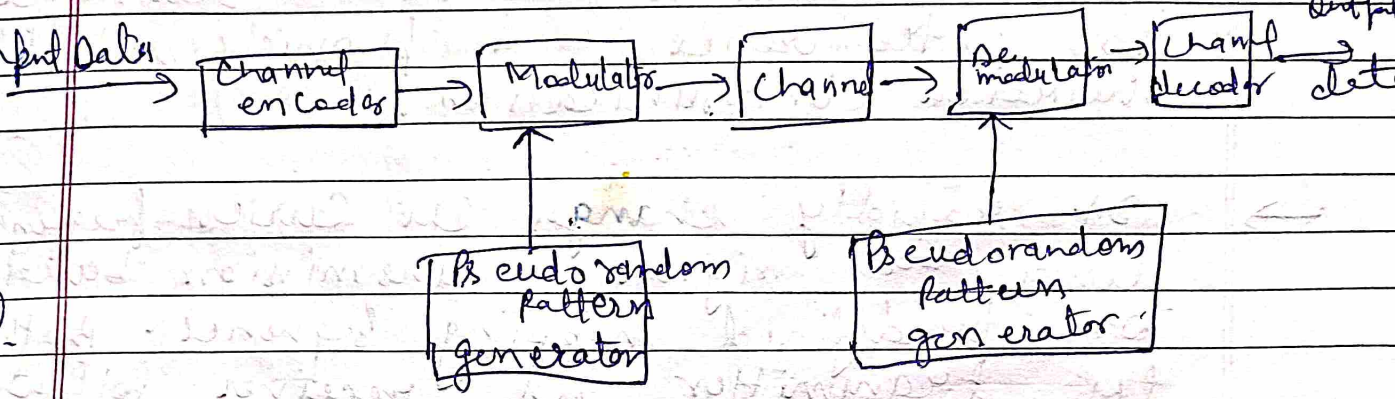
Achieve

A telecommunication signal is transmitted on a bandwidth considerably larger than the frequency content of the original information.

into larger bandwidth.

Types

1) Frequency hopping spread spectrum (FHSS)
2) Direct sequence spread spectrum (DSSS)



Block diagram of spread spectrum

Use

1) Establishment of secure communication.
2) To prevent detection.
3) To prevent noise
4) To limit power flux density.

Frequency Hopping spread spectrum (FHSS)

It is a wireless communication technique that spread a signal over a range of frequencies in a specific sequence. This method is primarily used to enhance resistance to interference and provide reliable wireless communication.

→ It rapidly changes the carrier frequency used for signal transmission based on predefined hopping sequence. Both the transmitter and receiver follow the same hopping sequence to maintain communication. This sequence is determined by a hopping pattern or algorithm.

Apl.

1. Bluetooth, Military comm.
2. wireless lan.

Adv

1. Resistance to interference
2. Effective in noisy
3. offers degree of security

Dis.

1. It require extra hardware complexity.

Date
Page

Direct Sequence spread spectrum (DSSS)

It is a spread spectrum modulation technique which is used to reduce overall signal interference.

→ It is responsible for the spreading of the bandwidth.

→ The user signal is multiplied by a Pin Cod sequence of high bandwidth.

Note: It is highly resistance to interference because it spread the signal over a wide bandwidth.

Apl

① neifi ed GPS system

OSI model

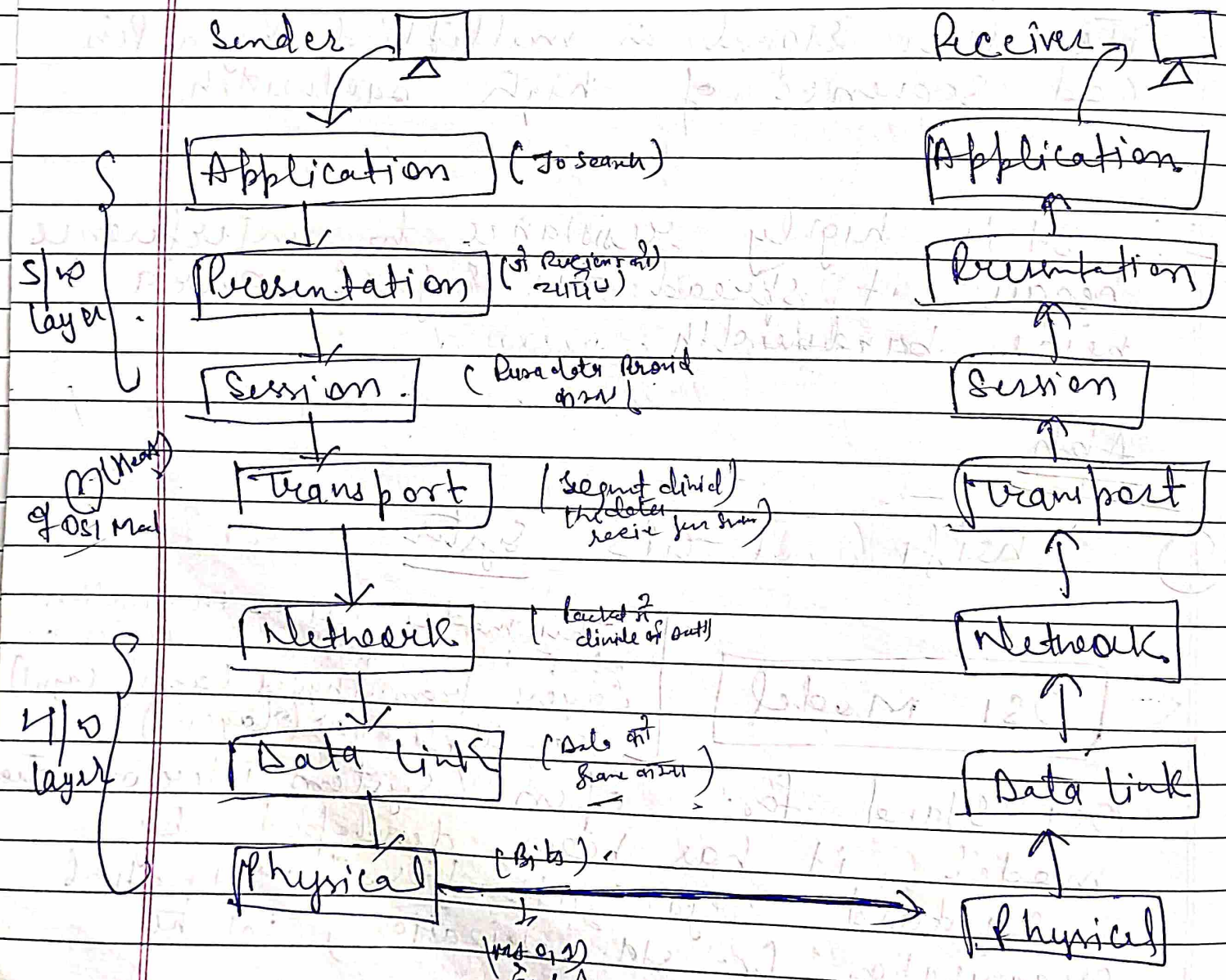
This model tell us the function of a telecommunication into seven layers from Physical layer, Lay to Application (Layer7).

OSI stand for open systems interconnect model, it has been developed by standard organization (Iso) international organisation for standerization) in the year 1984.

Date
Page

Note: ① It is a 7 - layer architecture where each layer having specific functionality -

② All these 7 layers work collaboratively to transmit the data from one n/w to another n/w across the globe.



Jai Hoo Satnaryan

Date 18/9/23
Page 1

OSI Model :→ Stand for open systems interconnection.

Developed by ISO, in 1984. It is a seven layer architecture the function of each layer to transmit the data from one person to another across the Globe.

Seven layers

1. Physical layer
2. Data link layer
3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer.

Physical layer: The lowest layer of OSI Model is called physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the forms of bits. It is responsible for transmitting individual bits from one node to the next.

Functions

1. Bit rate control: It defines the transmission rate. i.e no. of bits per second

Date
Page

(2) Physical topology : It specifies how different devices are arranged in a network ie bus, star or mesh topology.

2. Data Link layer (DLL) :- The data link layer is responsible for node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.

Functions

1. Error control : It provide the mechanism of error control.
2. Framing : It is a function of the data link layer.

3. Network layer :- Network layer works for the transmission of data from one host to the other located in different networks. The sender and receiver IP addresses are placed in the header by the network layer.

Function

(1) Routing :- The network layer protocol determine which route is suitable from source to destination. This function of network layer is called Routing.

Date
Page

4. Transport layer :- The transport layer provide service to the application layer and take service from the network layer. The data in the transport layer is referred as segments. At the sender side: Transport layer receives the format data from the upper layers, performs segmentation. and also implement flow and error control to ensure proper data transmission.

Functions

(#). Segmentation: This layer take the message from session layer, and break the mssg into smaller Units.

5. Session layer: This layer is responsible for the establishment of connection, maintaines of sessions, and also ensure security.

(##) Functions

(1). Session establishmnt: The layer allow the two process to establish, use and terminate the connection.

(2). Dialog Controller: The session layer allow two systems to start communication with each other in half-duplex or full duplex.

6. Presentation layer: It is also called the Translation layer. The data from application layer is extracted here and manipulated as per the required format to transmit over the network.

Function

1. Compression: Reduces the no. of bits that need to be transmitted on the network.
2. Translation: Eg: ASCII to EBCDIC.

7. Application layer: At the very top of the OSI Reference model stack of layers, we find the Appli. Layer which is implemented by the network applications. These application produces data, which has to be transferred over the network.

Function

1. Mail Servies: Provide email service.
2. FTAM — File transfer access and Managment.

Date
Page 04

Network Protocol: Protocol is a "set of rules" which are used in digital communication. to connect network devices and exchange information between them.

Types

1. TCP/IP
2. HTTP
3. SMTP — Simple Mail Type Protocol.
4. POP → Post office protocol.
5. IMAP →
6. UDP →
7. PPP →
8. FTP → File Type Protocol.

TCP/IP Model → Transmission control protocol / Internet protocol.

It is developed before OSI Model.

→ contain four layers but now 5 layers before.

Layer 1 →	Application	Now Application
2 →	Transport	Transport
3 →	Internet	Network
4 →	Internet network interface	Data link
5 →		Physical

TCP/IP is used to design and understand of the internet. It consist of four layers.

Date
Page

1. Application → Access to network resources
(Appli, Present, Sessin) (OSI) (Present, data to the user, encoding and session control)
2. Transport → Process to process message and error free delivery (Transport)
3. Internt → source to destination delivery
(Internet) (Determine the path of delivery)
4. Network → transmission b/w two devices in a network.
Access (Data link, Physical)

→ OSI Model (reference model) Virtual network herein multiple computer networks are interconnected

→ It was designed and developed by Department of defence (DoD) 1960s.

→ More reliable

→ TCP is used to transfer the data over the internet, it divides the data into small packets and sends it to the destination through network while IP is used for addressing through which data reached the final destination

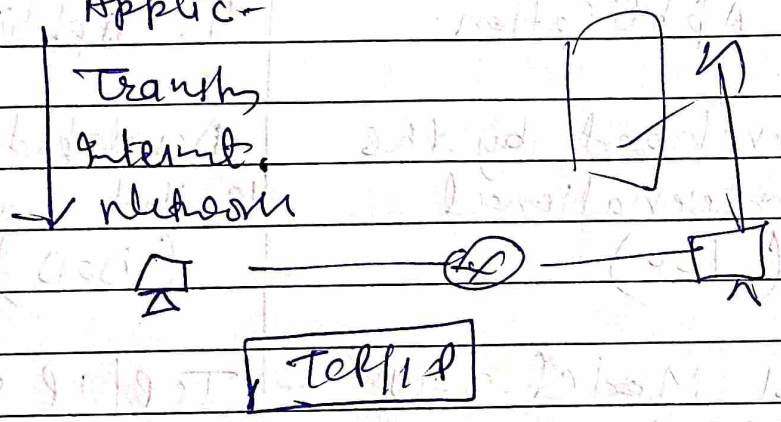
Date |
Page | 39

Comparison between OSI Model and TCP/IP Model

Aspect	OSI Model	TCP/IP Model
No. of layers.	Seven layers 1. Physical 2. Data Link : 7. Application	Four layers. 1. Link / Network Interface : 4. Application
Development origin.	Developed by the International (ISO)	Developed by the United states. (DOD)
Protocol.	OSI Model does not prescribe specific protocol.	TCP/IP specifies the use of specific protocol at each layer. - Link layer: Ethernet - Internet layer: IP - Transport layer: TCP, UDP - Application layer: HTTP, FTP, SMTP and others.
Complexity.	More complex due to its seven layer structure.	Simple with actual Internet implementations due to its four layer str.

Date
Page

	OSI	TCP/IP
Layer separation	OSI Model has a separate presentation layer and session layer	TCP/IP does not have a separate presentation layer or session layer.



Unit- 1st

Data Communication Compont is Completed

Jai Hoo Satnaryan ✪

Date | 09/09/23
Page |

UNIT-2.

PHYSICAL LAYER

Syllabus: Concept of analog and digital system, Transmission Media, Transmission impairements and data rate limits — Nyquist formula, Shannon formula, Switching — Circuit, Message and packet switching.

Physical layer: The physical layer is the first and the lowest layer of the OSI (Open system Interconnection) model. It deals with the actual physical transmission of data. bits over a physical medium.

16/9/23

The physical layer is like the "messages" of computer networks. It's responsible for sending and receiving individual Os and 1s (bits) over wires (cables) or wireless signal.

Date
Page

Concept of Analog and Digital System

Analog System: In a analog system, information is represented using continuous signals. For eg: in analog audio.

Analog signal can have an infinite no. of value within a range, which can led to signal degradation over long distance.

Features of Analog System:

1. **Uses continuous Signal:** Analog system use continuous signal to represent information, such as electrical signal or sound wave.

2. **Real world representation:** It is better suited for representing real world phenomenon such as sound and light, which are continuous in nature.

3. **Smooth transitions:** It provide smooth and continuous transition between different value.

4. **Complexity:** Analog system can be more complex than digital system.

Digital System: In digital system, information is represented using discrete signal, typically in binary form (0s and 1s).

Features:

1. **Using binary codes:** It uses binary codes, which is a combination of zeros and ones, to represent information.

2. **Accuracy:** They are more accurate than analog system. because the information is represented in consistent manner.

3. **Processing speed:** They are capable of processing large amount of data quickly and accurately.

4. **Noise immunity:** They are immune to noise which means that the transmitted information is less likely to be corrupted.

Date
Page

	Analog System	Digital System
Signal	They represents physical measurement.	They are discrete and generated by digital modulation
Means	Sine means	Square means
Representation	Continuous means are use to represent	Use discrete value to represent
Data Transmission	Affected by noise during transmission.	Noise-immune during transmission
Response to Noise	More likely to get affected.	less likely to get affected
Flexibility	Hardware is not flexible	Hardware is flexible.
Memory	Store data in the form of mean signal	Store data in the form of binary bit
Cost	Cost is low	Cost is high
Example:	Human voice in air,	Computer, CDs, DVDs

17/4/24

Calculate missing value when its mean is 115.86

$\bar{x} = 115.86$

Wages	f	Σfx
110	25	2750
112	17	1904
113	13	1469
117	15	1755
a	14	14a
125	8	1000
128	6	768
130	2	260

$\Sigma f = 100$

$\Sigma fx = 9906 + 14a$

$\bar{x} = \frac{\Sigma fx}{\Sigma f}$

$115.86 = \frac{9906 + 14a}{100}$

$11586 = 9906 + 14a$

$14a = 11586 - 9906$

$14a = 1680$

$a = \frac{1680}{14}$

$a = 120$

Q- Sum of deviations of certain no. of items measured from 2.5 is 50 & from 3.5 is -50. Find N & $\bar{X}$

$$\bar{X} = A + \frac{\Sigma d}{N}$$

$$\bar{X} = 2.5 + \frac{50}{N} \quad \text{— (1)}$$

$$\bar{X} = 3.5 - \frac{50}{N} \quad \text{— (2)}$$

$$2.5 + \frac{50}{N} = 3.5 - \frac{50}{N}$$

$$\frac{50}{N} + \frac{50}{N} = 3.5 - 2.5$$

$$\frac{100}{N} = 1$$

$$N = 100$$

$$\bar{X} = 2.5 + \frac{50}{2}$$

$$\bar{X} = 2.5 + 0.5 = 3$$

Evergreen
Page No.
Date : / /20

⇒ Correcting incorrect values of mean

H.W

Q The mean of 100 item is 80. By mistake 1 item is misread as 92 instead of 29

→ Combined Arithmatic Mean

$$\bar{X} = \frac{N_1\bar{X}_1 + N_2\bar{X}_2}{N_1 + N_2}$$

Q Mean height of 25 male worker is 61 cm.
& " " " 35 female " " 58 cm.
Find combined mean height of 60 worker

$$\bar{X} = \frac{(25 \times 61) + (35 \times 58)}{60}$$

$$= \frac{1525 + 2030}{60}$$

$$= \frac{3555}{60}$$

$$\bar{X} = 59.25$$

2 Ques H.W.

Evergreen
Page No.
Date : / /20

⇒ Mathematical properties of AM

1. Sum of deviation of items from mean is always zero

$$\Sigma(x - \bar{x}) = 0$$

2.

TM

Guided → Twisted, Coaxial, Fiber

Unguided → Radio, Microwave, Satellite

Date | Page |

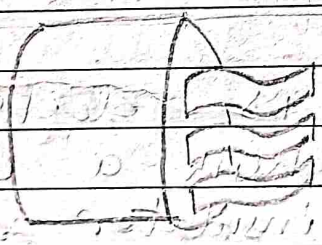
Transmission Media: Media are the physical pathways that enable data to travel from one device to another in a network. Common transmission Media include:-

1. **Twisted pair Cable:** Most common type:-

They consist pair of copper wire twisted together. These cables are widely used for telephone line and Ethernet connection in LANs.

Types

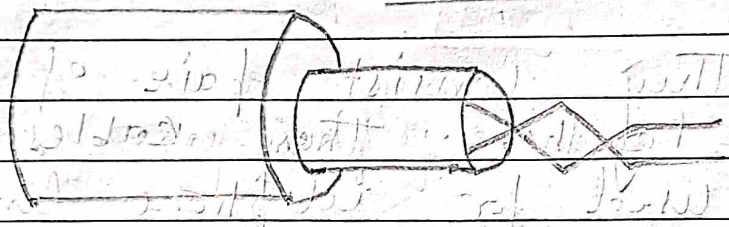
(A) **Unshielded Twisted pair (UTP):** UTP consist of two insulated copper wires twisted around together. It is used for telephonic communication.



Adv	Dis
1. least expensive	1. Short distance Capacity due to attenuation
2. Easy to install	2. lower capacity
3. High speed capacity	

Date |
Page |

(B) Shielded Twisted pair (STP): It consist of a special jacket (a copper braid covering or a foil shield) to block external interference. Used in fast-data-rate ethernet.



Adv

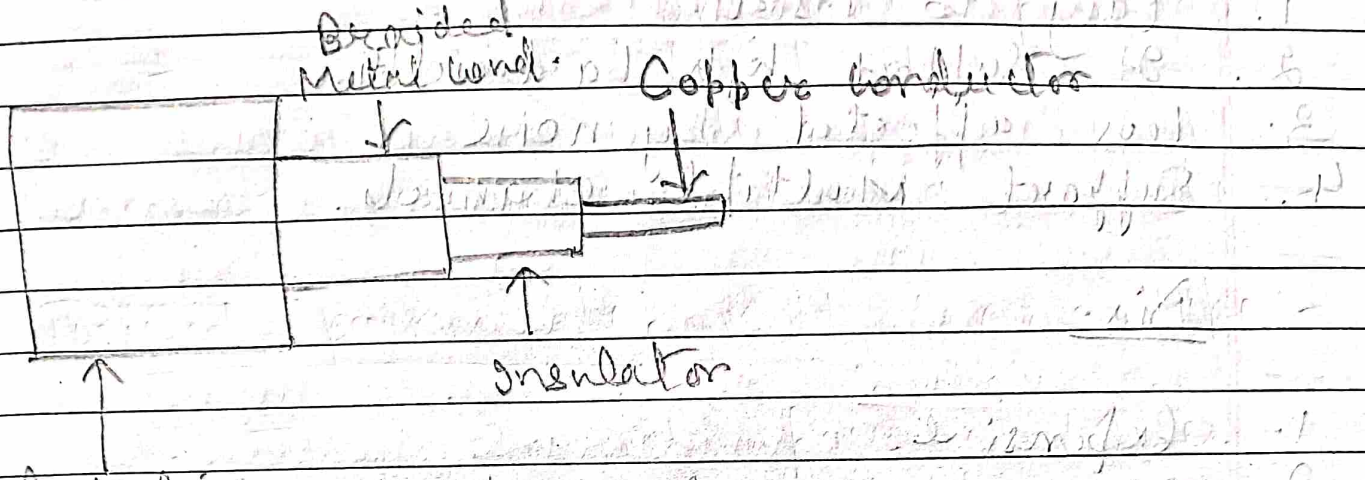
1. Better performance as compared to UTP.
2. Comparatively faster.

Dis

1. Most expensive.
2. Bulky.

2. Coaxial Cable: It is electrical Cable with a copper conductor and an insulator shielding around it and a braided metal mesh that prevent signal interference and cross talk. Coaxial Cable is also known as Coax.

Structure



- Copper conductor is used for transmission of signal
- Insulator is used to provide the insulation of the copper conductor.
- Braided Metal conductor is surrounded above insulator which help to prent the interference of electrical signal and prent cross talk.
- Protecting plastic layer is surrounded above the entire setup to provide extra safety to the cable.

Application

1. Used for Television, Carry internet signal, in CCTV System, Video Transmission.

Date |
Page |

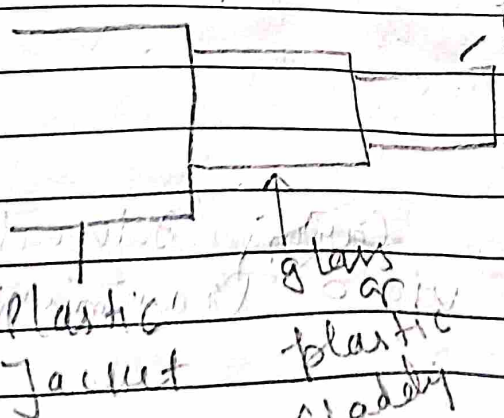
Adv

1. Easy to install
2. It support high bandwidth.
3. Less affected by noise
4. Support multiple channels.

Dis.

1. Expensive
2. It is very bulky due to its multiple layer

3. Fiber-optic cable : The transfer data at travel hundreds of miles faster than those used in electrical cable.
   - New transmission media
   - Long distance line
   - Used by private communication in implementing local data communication.
   - Require a light source with injection laser diode (ILD) & light emitting diode (LED)



(20) 1200 (8).

(#).

Date |
Page | 30

1. Multimode Step Inde fiber :- The reflecti wall of the fiber more the light forces to the receiver.

2. Multimode graded Inde fiber :- dect to refract the ligh toward the centre of the fibre by variation in Dnsity.

3. Sigle Mode fiber :- The ligh is guided down the cater of an extremely narrow role.

Adv

1. greater Capacity (2Gbps)
2. Smaller Size & lighter weight.
3. lower attenuation.
4. Immunity to Environmt
5. highly secure.

Disadv

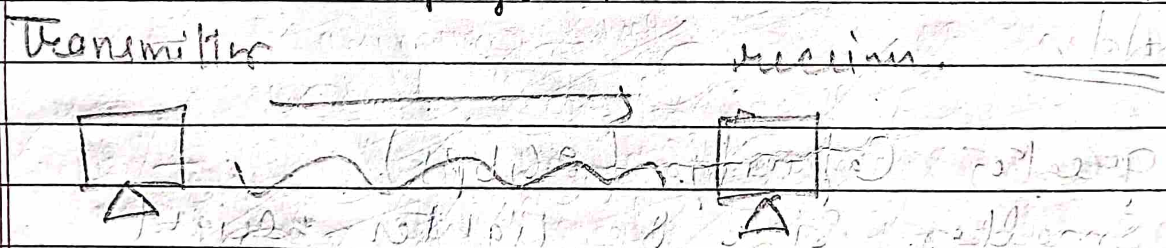
1. Expensive over short distance
2. Repire high Skills.

4. <u>Wireless Communication</u> :-

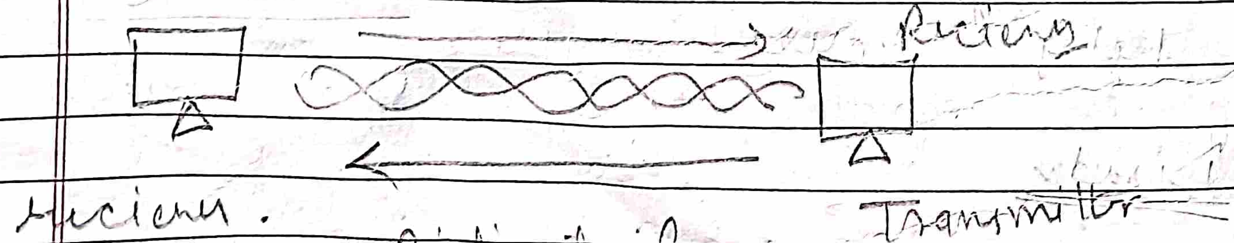
- It uses invisible radio waves
- Devices has transmitter and receiver
- Transmitter send out signal and receiver catch them.
- <u>Modulation</u>: Information is turned into radio wave pattern.
- Radio waves is affected by obstacles

<u>Example:-</u> wifi, and cell phones are wireless communication.

In this devices can communicate without physical wire or cables.



Unidirectional communication



Bi directional

~~Interference from other devices~~

Transmission impairements: are the factors that degrades the quality of a signal during transmission. Common impairments include :-

1. **Attenuation:** Signal loss over distance due to the Natural resistance of the medium, which absorb the signal energy.

2. **Noise:** It is an unwanted interference that mix with the original signal during transmission.
   Due to external factors like Electromagnetic interference (EMI), RFI.

3. **Delay:** It is the time it take for a signal to travel from the sender to the receiver.
   It includes
   - Propagation delay
   - Transmission delay.

4. **Jitter:** It refers to the variability of signal delay.

Date |
Page |

Data Rate limits → Nyquist and Shannon formula:

There are two theorems for the evaluation of the data rate:-

1. Nyquist formula:

Formula: $R = 2B \log_2(M)$

Purpose: It is used to calculate the maximum data rate (R) achievable in a noiseless channel.

Components:

R → Maximum data rate in bits per second (bps).

B → Bandwidth of the channel in Hertz (Hz)

M → No. of signal levels.

Explanation: (1) It is based on the idea that in a noiseless channel you can transmit information by varying amplitude (signal level) of a carrier wave. Greater the no. of signal (M), more information you can convey.

(2) It tell us that to increase the data rate you can either increase the bandwidth (B)

100

Date
Page 34

are the number of signal levels (M).

Example:- Suppose a comm. channel has a bandwidth (B) of 5000Hz, and you want to transmit digital information using different signal level (M). Let M=64.

Sol: $R = 2B \log_2(M)$

$= 2 \times 5000 \log_2 \log_2(64)$

$= 10000 \times \log_2(2^6)$

$= 10000 \times 6 = 60,000$ bps | bits per second

2. Shannon formula:

Formula: $R = B \times \log_2(1 + SNR)$

Purpose: Used to calculate the theoretical maximum data rate (R) in a channel that has noise (Signal to Noise Ratio, SNR) while taking into account the channel Bandwidth (B).

Components: SNR → Signal to noise Ratio.

It is usually expressed in decibals (dB)

34

Date |
Page |

Explanation

① It extends Nyquist's model to real world scenarios where noise is present. It accounts for the quality of the signal by considering the SNR.

② It tells us that the maximum data rate depends on both the channel bandwidth (B) and the quality of the signal (SNR).

③ As SNR increase (Means Signal is stronger compared to noise), the data rate can approach the channel's theoretical limit.

Example: Imagine a Bandwidth (B) of 10,000 Hz. In this channel, the Signal-to-Noise Ratio (SNR) is 20 dB. Now you calculate the maximum data rate (R).

Solution: First convert SNR to decibals.

$$SNR = 10^{\left(\frac{SNR_{dB}}{10}\right)}$$

$$= 10^{\left(\frac{20}{10}\right)} = 10^{2} = 100$$

Date |
Page | A7

Acc. to Shannon formula.

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

$= 10000 \times \log_2 (1+100)$

$= 10000 Hz \times \log_2 (101)$

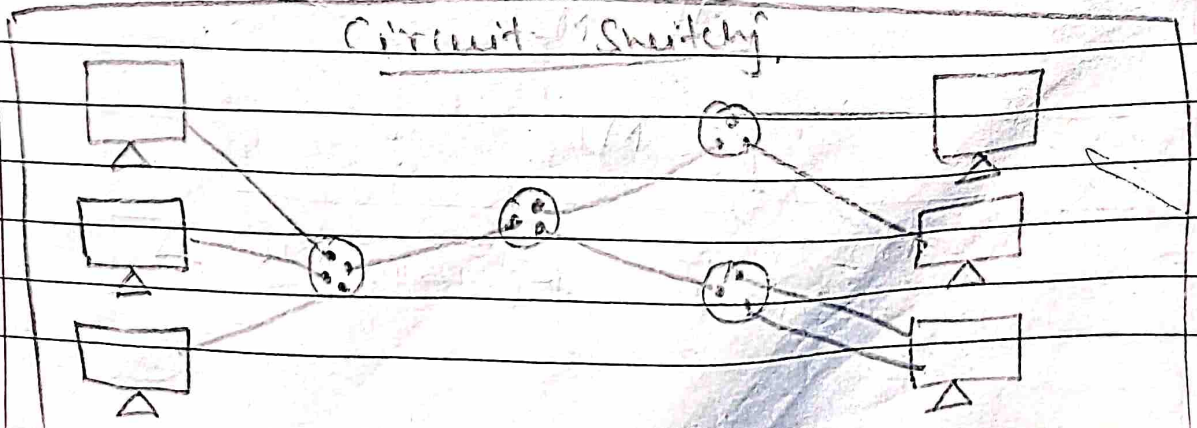
$[\log(101) = 6.67]$

$R = 10000 \times 6.67$

$R = 66700 bps$ (bits per second)

Switching — Circuit, Message and Packet Switching

Circuit Switching: It is a type of switching in which we set a physical connection between sender and receiver. The connection is set up when the call is made from transmitter to receiver telephone.



Date |
Page |

Adv.

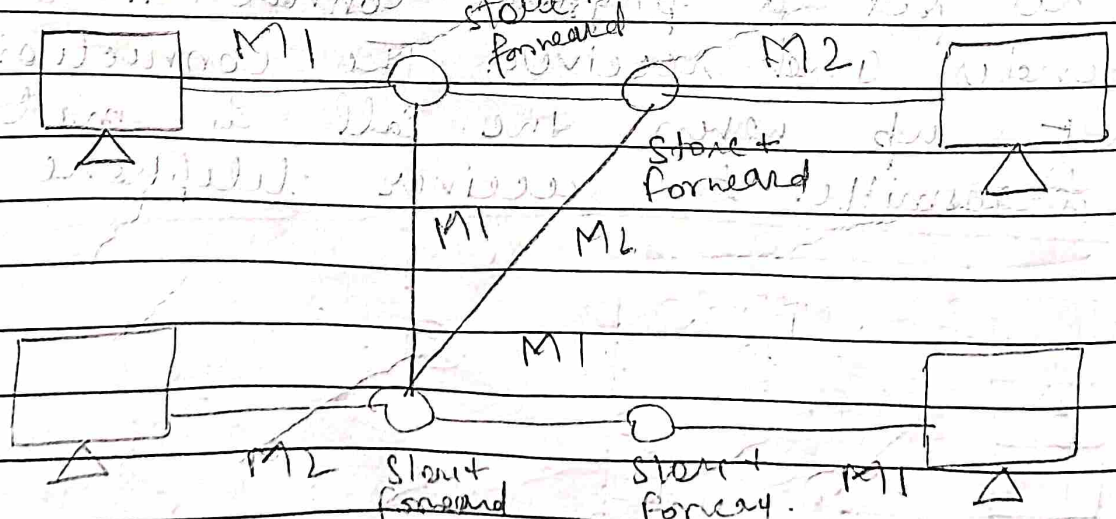
1. It provide a Guaranted data rate.
2. No delay in data flow

Dis

1. Require More bandwidth
2. Take time to establish connection.
3. Not Suitable for high traffic

2. **Message Switching** : In this the complete message is transferred from one end to another through nodes. There is no physical connection or link b/w sender & receiver.

Each node store the message and then forward it to the next node shown in below diagram.



Date
Page 03

Adv

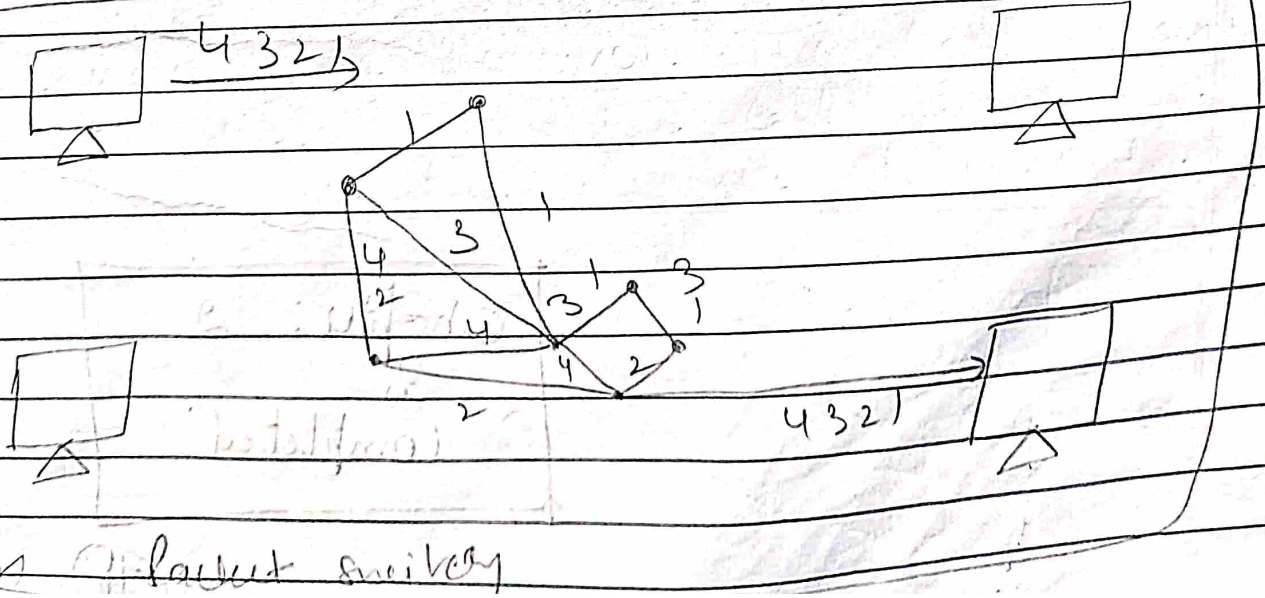
1. Reduce Network traffic
2. Network devices share the channel

Dis:

It does not establish a dedicated path b/w two communication paths.

3. Packet Switching :→ In this, Message is broken into packets for transmission. Each packet has the source, destination and intermediate node address information.

The entire message is divided into smaller pieces, called packets. Each packets travel independently. Their packets travel through the shortest path in Communication network.



Date |
Page |

Two Types

1. Datagram Packet switching
2. virtual Circuit Packet switching.

Advantages

1. Bandwidth is reduced.
2. If one like goes down, the remaining packets can be sent through another route.

Chapter: 2
is
completed

Jai Hoo Satnaryan

Date / Page / 10/9/2023

UNIT: 03

DATA LINK LAYER AND MEDIUM ACCES SUB LAYER.

Syllabus :- Errore detection and errore correction - Fundamentals, Block coding, Hamming Distance, CRC, Flow control and Errore Control protocols - stop and wait, Go back - N ARQ, Selective Repeat ARQ, Sliding neindow, Piggybacking, Random Access, Multiple Acces protocol- Pure ALOHA, slotted ALOHA, CSMA/CD, CDMA/CA.

Jai Shri Satnarayan

Date 16/10/2021
Page 1

Introduction

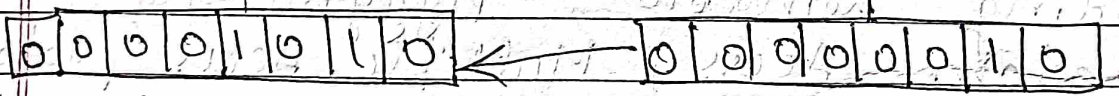
- Data can be corrupted during transmission. For reliable communication errors must be detected and corrected.
- Error detection and correction are implemented either at data link layer or the transport layer of the OSI Model.

Types of Errors

1. Single bit error :-

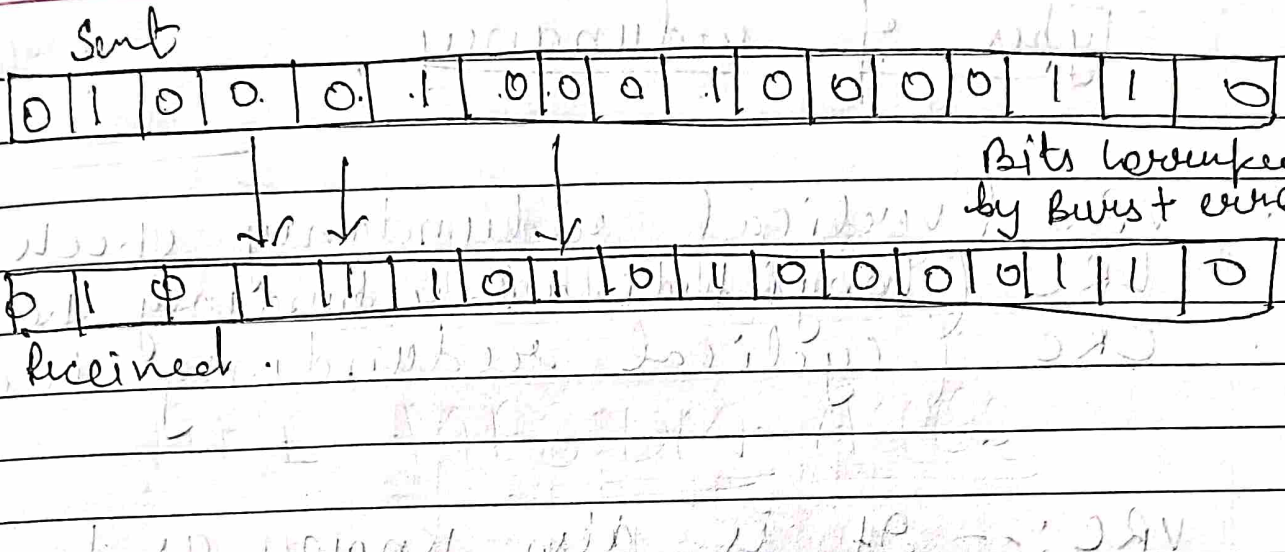
— only one bit in the data unit has changed.

0 changed to 1 .



2. Burst Error :-

It means that two or more bits in the data unit has changed.



Error detection :→ It is a mechanism to find out whether there is an error or not. It does not necessarily mean that it knows exact location of error. It may or may not the exact location depends on the detection mechanism.

→ Adding some extra bits to detect occurance of ~~or~~ error.

— It uses the concept of redundancy, which means adding extra bits for detecting error at the destination.

— **Redundancy**: Instead of repeating the entire data stream, a shorter group of bits may be appended to ~~the~~ end of each unit. This technique is called redundancy.

Date
Page

Types of redunancy,

1. VRC (vertical redundancy check)
2. LRC (longitudinal redundancy check)
3. CRC (cyclical redundancy check).

1. **VRC**:- It is also known as parity check.
   - It is least expensive mechanism for error detection.

Example

1110110 1101111 1110010

If even → 0
If odd → 1

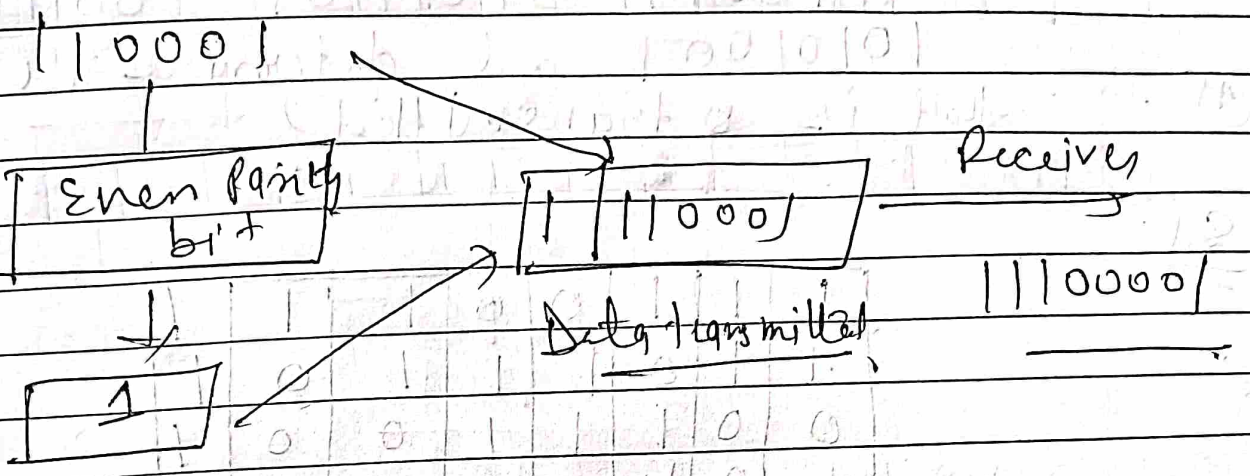
- After adding the parity bit

11101101 11011110 11100100

2. **LRC**:- In this a block of bits is organized in tables (rows and colours).

Date
Page 6

VRC



— It detect only single bit errors.
— It detect burst error only if the no. of errors is odd.
odd.
[Means accept only even no. of odd]

Eg
Sender → Transmission error 1010000
1110001 ↗
↓
Receiver reject

Sender: 1110000 → " 1010010 — Receiver accept

LRC:- Its known as Two Dimensional Parity

→ The parity bit is Calculated for each columns and sent along with the data.

— It block of parity.

Date
Page

Eg: Find the LRC for the data blocks 11100111 11011101 00111001 10100011 and determine the data that is transmitted?

Sol-

	1	1	1	0	0	1	1	1
	1	1	0	1	1	1	0	1
	0	0	1	1	1	0	0	1
	1	0	1	0	1	0	0	1
LRC →	1	0	1	0	1	0	1	0

odd no. 1's
even no. 1's

Direction of Mount

10101010	10100011	00111001	11011101	11100111
LRC		Data		

Performance

- Increase the likelihood of detecting burst error.

Polynomial
$x^7 + x$

Date
Page 83

3. CRC :-

Q Find the CRC for the data block 100100 with the divisor 1101 ?

Sol :-

CRC Generation at sender side

1. Find length of the divisor 'L'.
2. Append 'L-1' bits to the original message
3. Perform binary division operation
4. Remainder of the division = CRC

Note:

CRC must be of L-1 bits.

Divisor → 1101

```
        1111 Q
1101 | 100100000
       1101
       01000
        1101
        0101 0
         1101
         0110
          1101
          0011 0
           0000
           0110
           1101
           0011  ← Remainder
```

Apply XOR op.

Here L=4, 3 0's are appended to the message

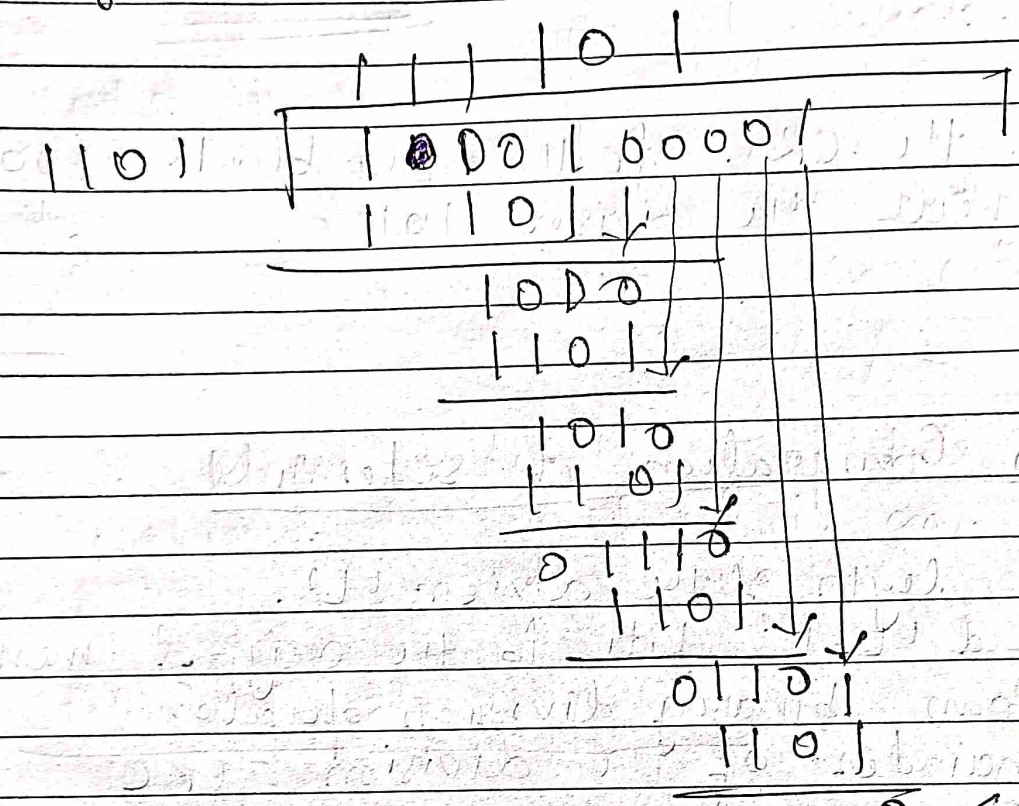
Data transmitted

Data: 100100 | 011 ← CRC

CRC

Date |
Page |

- Now how we check the given data is error free.

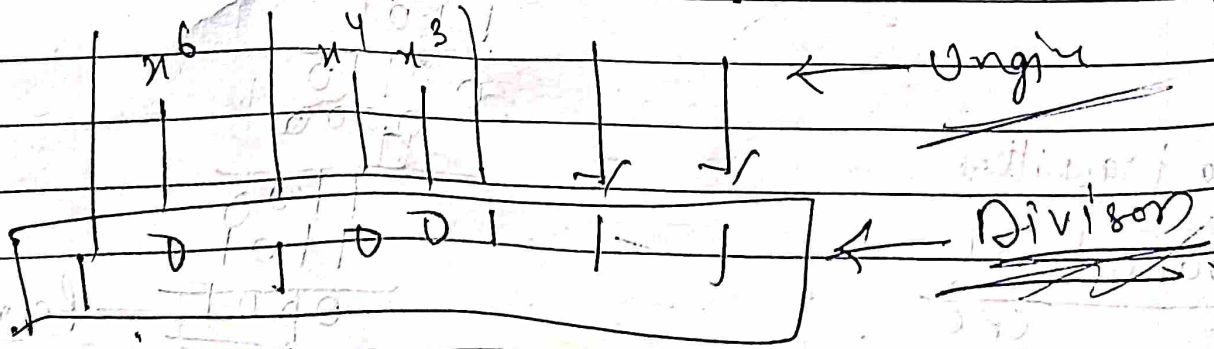


Means data are error free.

Data Accepted →

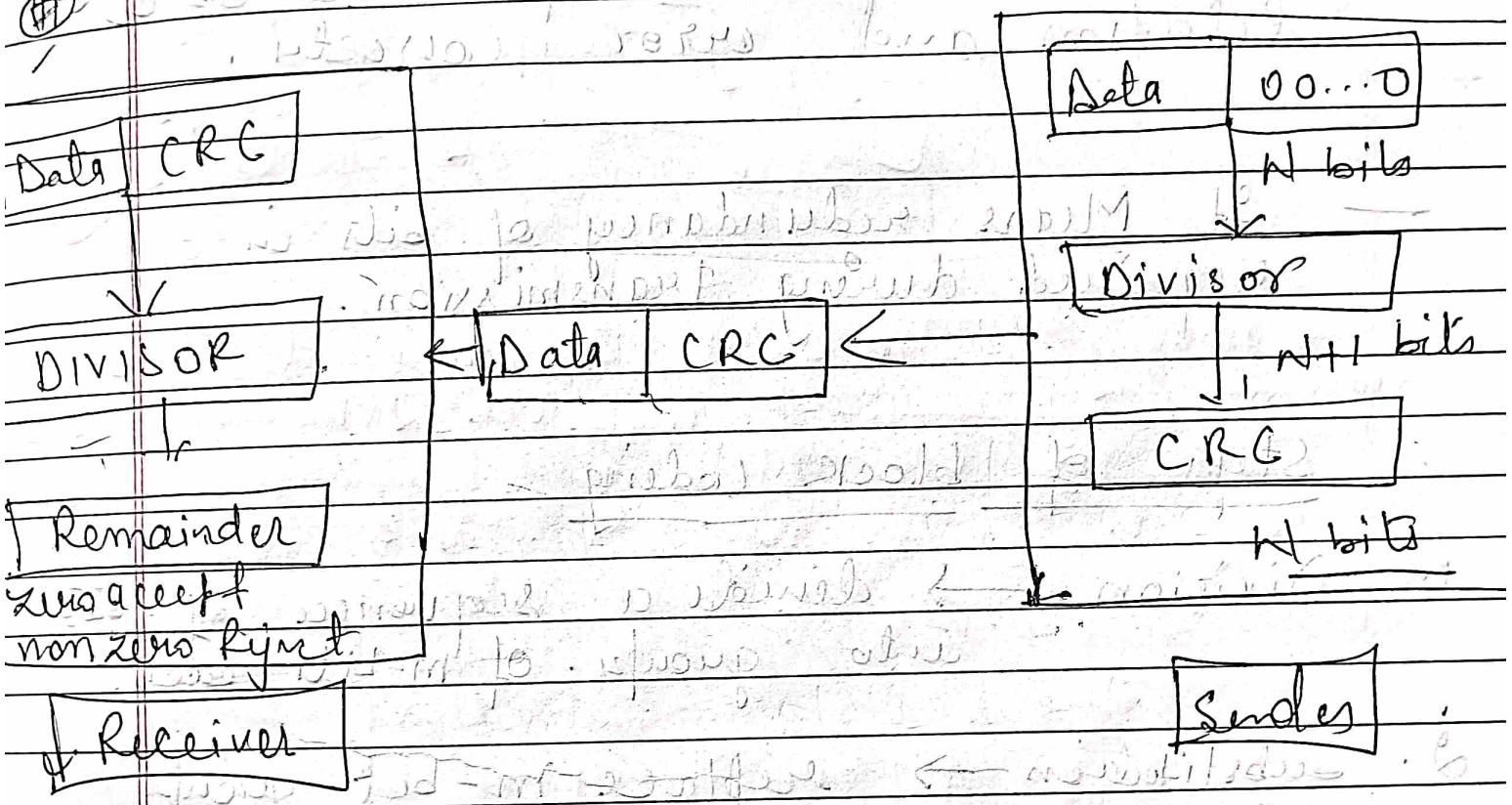
Q If data in polynomial.

→ $x^7 + x^5 + x^2 + x + 1$ — Given



~~Block coding~~

CRC generator and checker



- CRC is a method for error detection. It involves appending a checksum to the data, which is calculated using polynomial division. The receiver can check if the received data has been corrupted by performing the same calculation.

Jai Maa Saraswati

Mind Your Exam channel.

Date | 16/10/18
Page |

Block coding: Block codes are a type of error-correcting code that divide data into fixed-size blocks and adds redundancy to each block to facilitate error detection and error correction.

— It Means redundancy of bits in required during Transmission.

Steps of block coding

1. Division ⟶ divide a sequence of bits into groups of m-bits each.

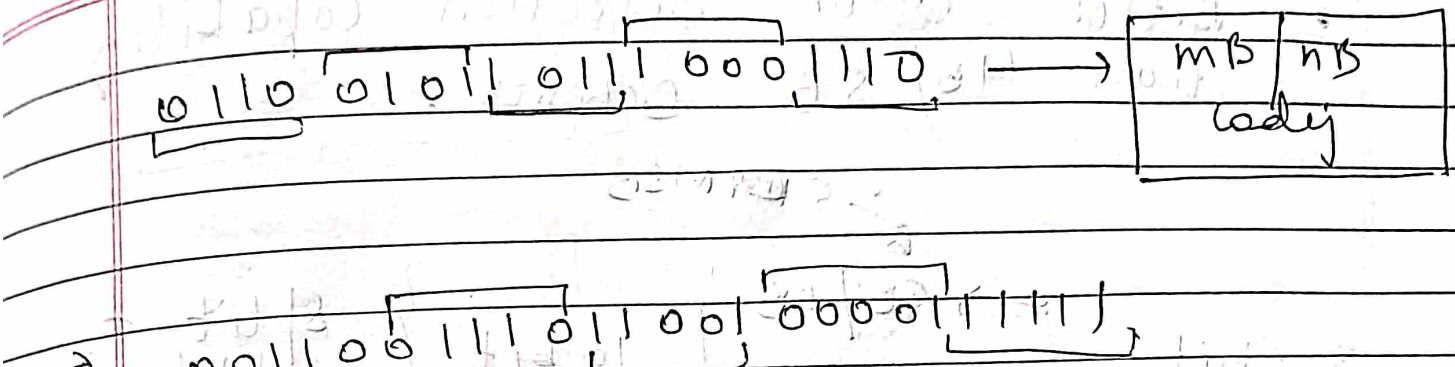
2. Substitution ⟶ replace m-bit group with an n bit group.

3. Combination ⟶ n-bit groups are Combined to form a stream. more bits than original.

Block coding is represented by:

mB/nB coding :- Changes a block of m bit to a block of n bits.
(B = bits)

where n > m.



Types of Block codij

1. **4B/5B**
   - Divide the original bit sequence into group of 4 bits each.
   - Substitute each 4 bits group with 5 bit group.
   - Combine all the 5 bits groups into a single data stream.

$2^4 = 16$ Combination

$2^5 = 32$ Combinations.

UNUSED COMBINATIONS → Control purpose, error detection, synchronisation

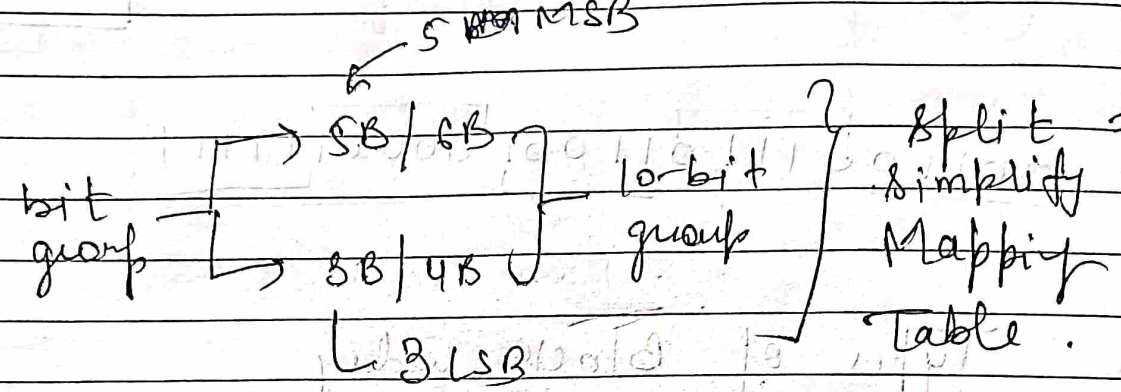
2. **8B/10B**
   - 8 bits group substituted by 10-bit groups.

$2^{10} - 2^9 = 768$ — redundant group

(11).

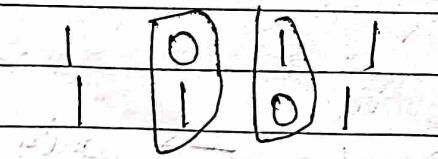
Date
Page

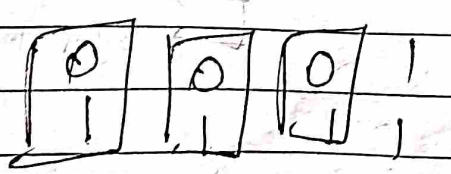
- Better error detection capability than 4B/5B scheme.



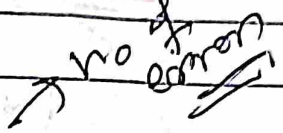
Hamming Distance :→ Hamming distance measure the difference between two binary string of equal length. In error correction, it's used to identify and correct error.

— No. of bit positions at which the two codes differs.





d bits for error detection



Minimum Hamming distance $d_{min} = d+1$

d bits for error correction

Minimum Hamming distance $d_{min} = 2d+1$

Example:- $d_{min} = 4$? what is error Detection and error correction Cabability ?

Sol:- $d_{min} = 8\ d+1$

$4 = d+1$

$\boxed{d=3}$ → No. of error to detect

$d_{min} = 2d+1$

$4 = 2(d)+1$

$2d = 3$ $\quad d = 3/2 = 1.5$

$\boxed{d=1.5}$ or $t = 1.5 \sim 1$

$\boxed{t=1}$

Jai Hoo

Date 12/10/2022
Page 1

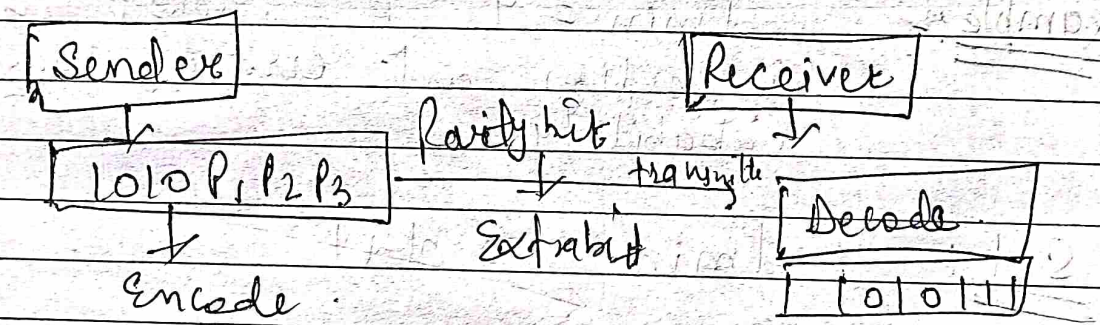
⇒ If dmin = even.

then Capability of Error correction is nearest.

If dmin = odd.

then it is good.

Hamming code:



Flow control and Error control protocol:

1. Stop and wait :- The stop and wait protocol is a simple flow control and error control mechanism used in data communication. It is often implimited in the Data link

layer to ensure that data is transmitted reliably between a sender and a receiver.

- The idea of stop and wait protocol is straightforward.

Primitives of STOP and WAIT Protocol

Sender side :

Rule 1 :- Send one data packet at a time.

Rule 2 :- Send the next packet only after receiving ACK for the previous.

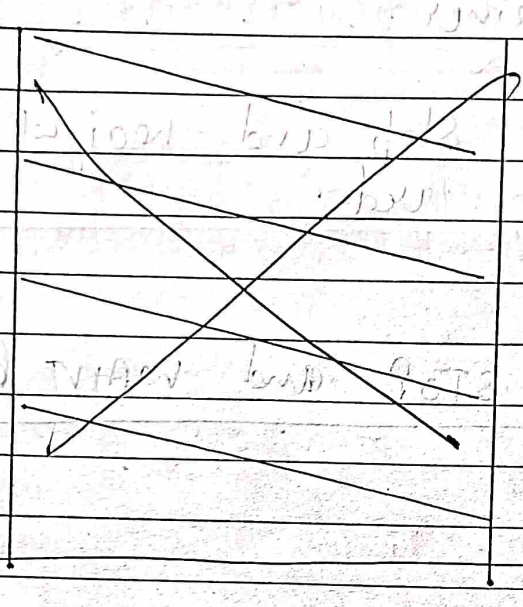
Receiver side :

Rule 1 : Receive and consume data packet

Rule 2 : After consuming packet ACK need to be send (Flow Control).

Date |
Page |

Working of stop and wait protocol



Protocols

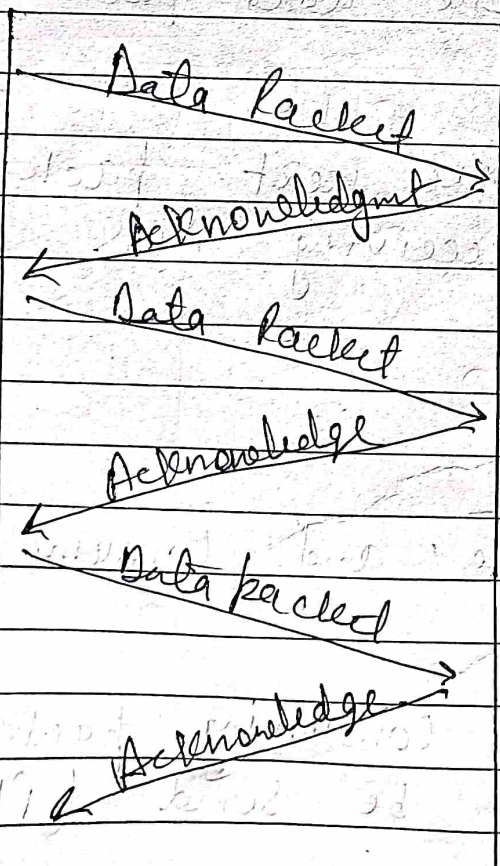
Noiseless channel

Simplest stop + wait

Noisy channel + stop + wait Go back N ARQ Selective Repeat

Sender

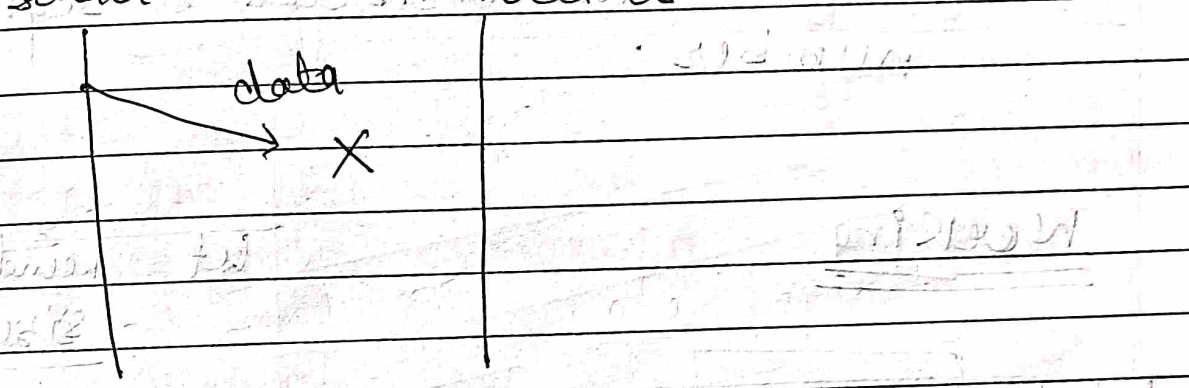
Receiver



Problems of stop and wait protocol

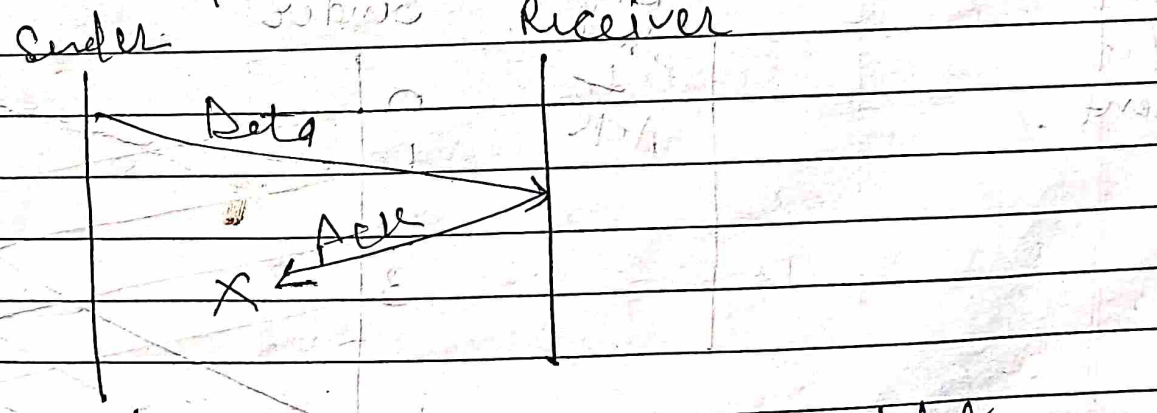
1. Problem due to lost data.

* Sender waits for ack an infinite amount of time.
* Receiver waits for data an infinite amount of time.

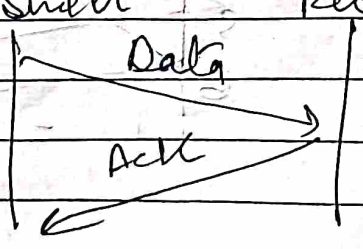


2. Problem due to lost ack.

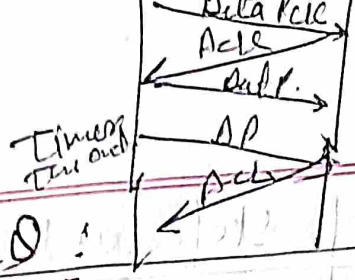
* Sender waits for an infinite amount of time for ack.



3. Problem due to delayed ACK | data.



Stop & Wait ARQ



Date
Page

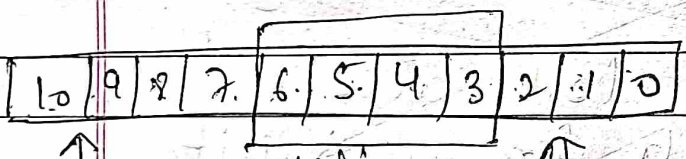
2. Go back N ARQ :

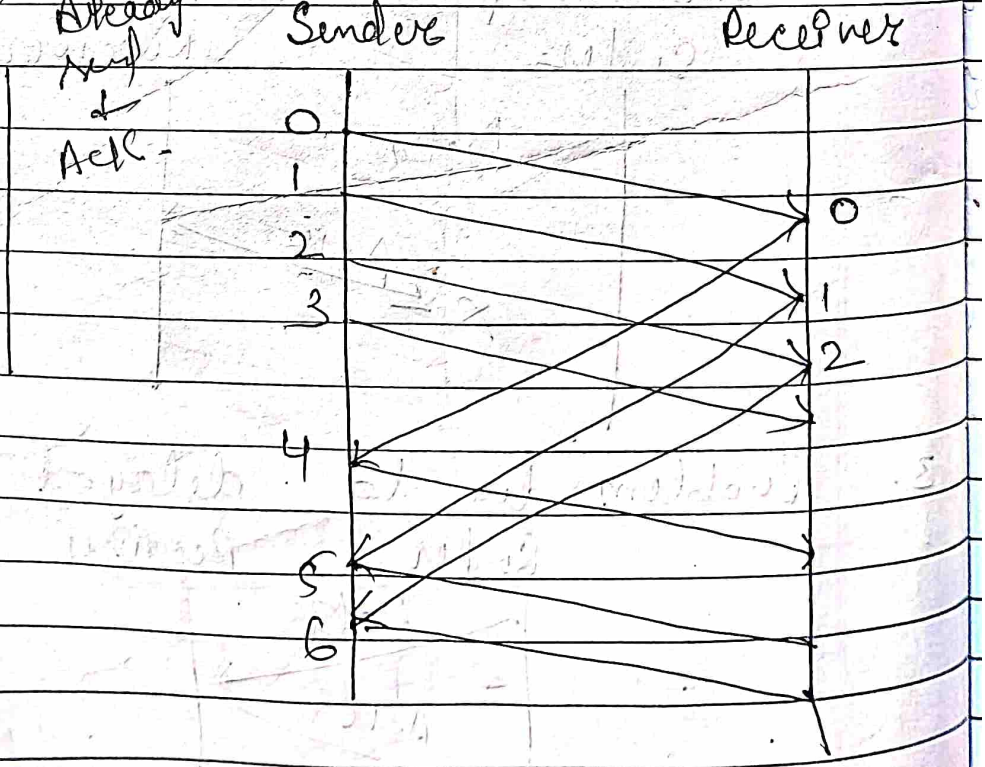
2. Sliding window protocol → Go back N ARQ / Selective Repeat ARQ

- Send multiple frame at a time
- no. of frames to be send is based on window size
- Each frame is numbered → Sequence number.

working

let window size : 4





3. Go back - N ARQ :→

N → is the Sender window size.

→ It uses the concept of protol pipelining ie. the Sender can send multiple frames before receiving the acknowledgement for the first time.

— There are finite no. of frame and the frames are numbered in a sequential manner.

— The no. of frame that can sent depend upon the window size of the sender.

— If the ack of a frame is not received with an agreed upon time period, all frame in the current window are transmitted.

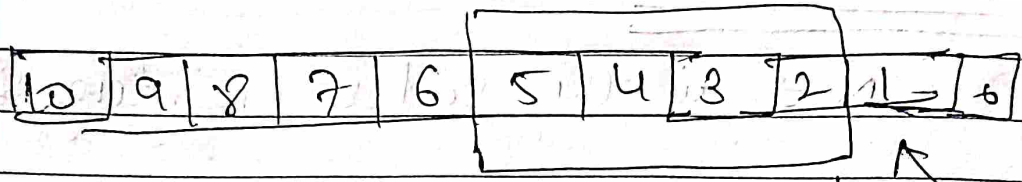
N - Sender window is size.

— Eg :- if Sending window size is 4 (2^2).
then the sequence no. will be
0, 1, 2, 3, 0, 1, 2, 3, 0, 1 and so on.

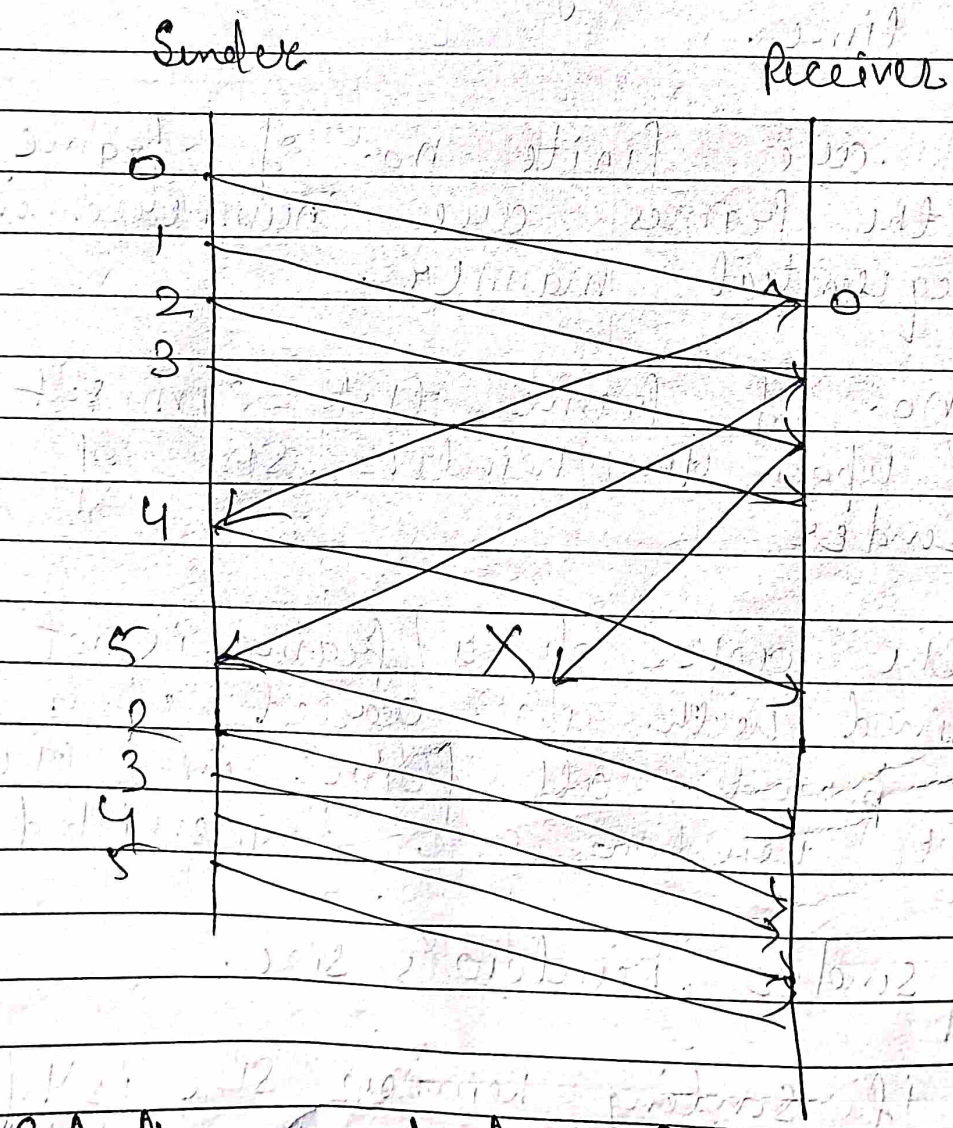
— The no. of bits in the sequence no. is 2 to generate the binary no. is
00, 01, 10, 11.

Date |
Page |

Working of Go back protocol



Let window size 4



3. Selective repeat ARQ :

In Selective repeat ARQ, only the erroneous or lost frames are

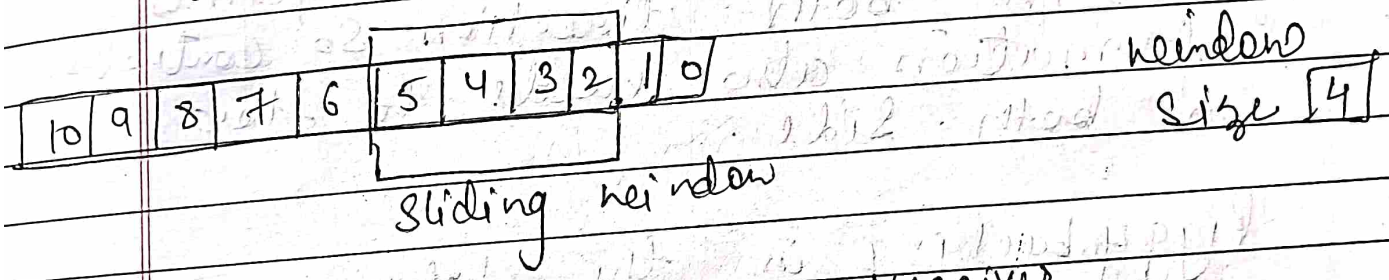
Jai Hoo Saiswaroop

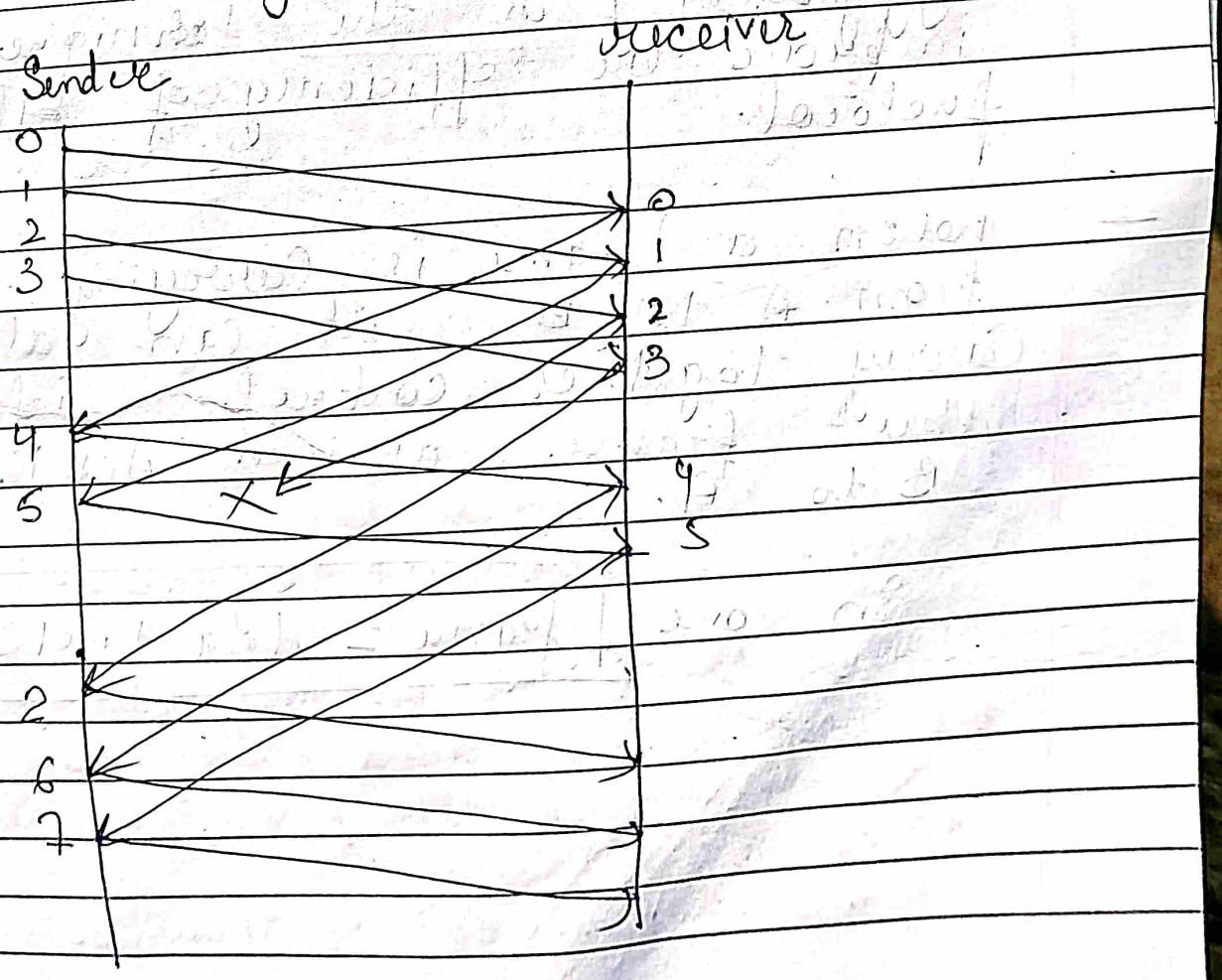
13/10/2023
Page 58

retransmitted, while correct frames are received and buffered.

(b) The Sender will send / retransmit packet for Negative acknowledgement (NACK) is received.

Jacking





★ ★ (11)

Date
Page

4. Piggybacking :-

— Protocol of noisy and noiseless channel are unidirectional.

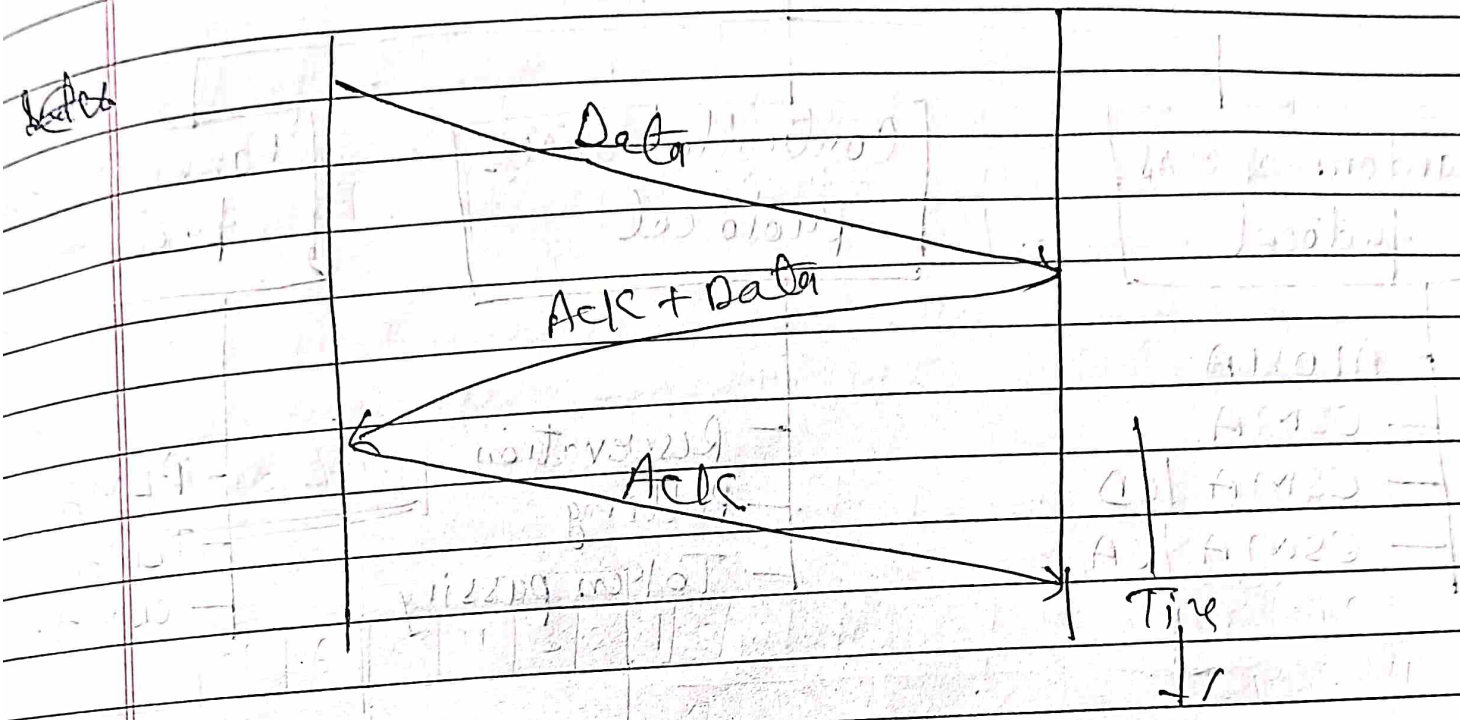
— The data frames in one direction and ACK in other direction.

— In many scenario data frames flow in both direction so control information also needs to flow in both side.

★ Piggybacking is the technique used to improve the efficiency of bidirectional protocol.

— When a frame is carrying data from A to B, it can also carry together control information about frame arrived (ACK) from A. B to A.

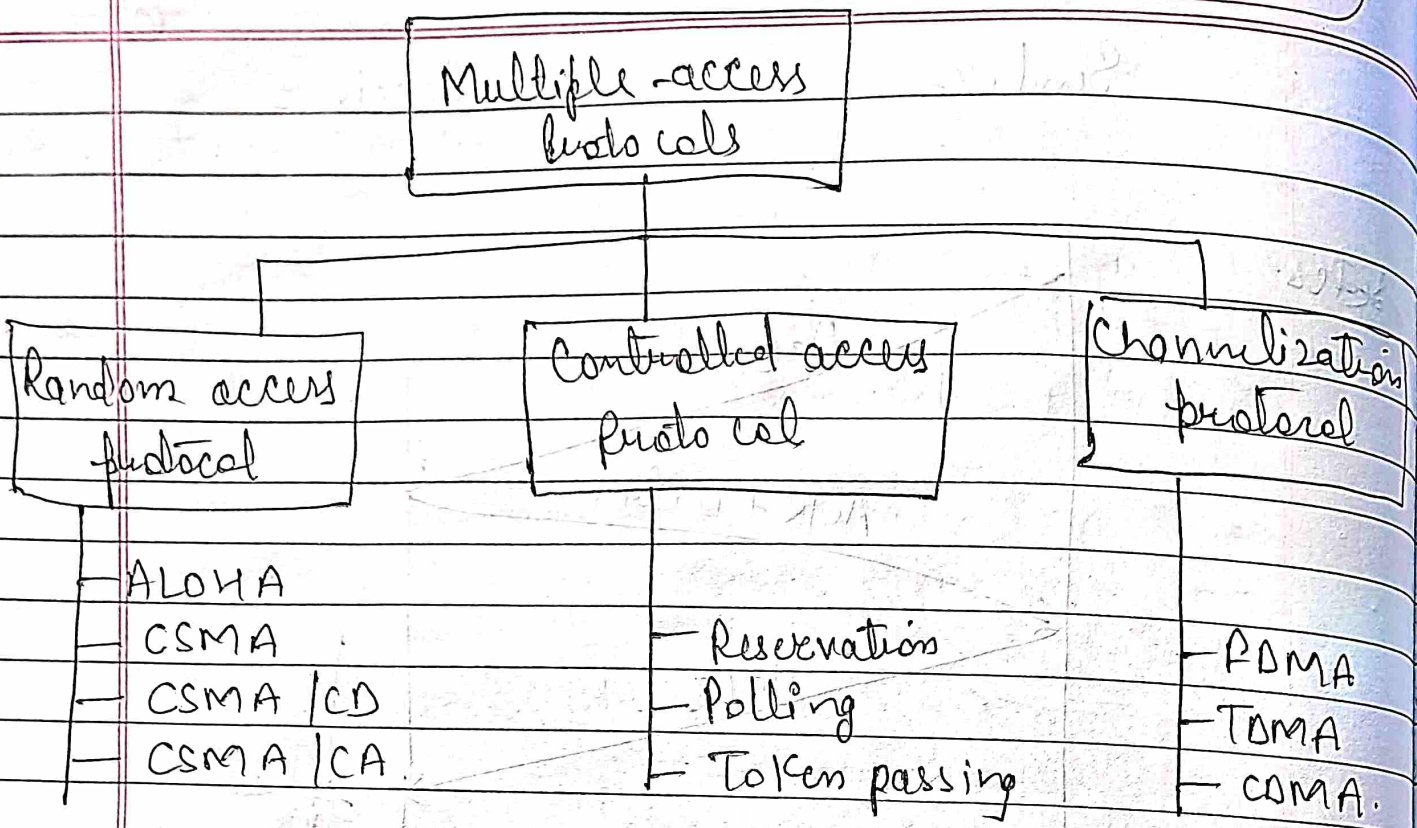
In one frame = data + ACK



Multiple Access protocols

Why

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple station can access the channel simultaneously. Hence MAP are required to decrease collision and avoid crosstalk.



Random access protocol – It means any station can send data at any time but there is a chances of collision.

- In this all station have same priority that is no station has more priority than another station. Any station can send data depending on Medium's state (idle or busy).
- In this each station has the right to the medium without being controlled by other station.
- If more than one station tries to send

there is an access conflict (collision) and the frames will be either destroyed or modified.

To avoid conflict, each station follow a procedure.

1. when can the station access the medium?
2. what can the station do if the medium is busy?
3. How can the station determine the sucess or failure of the transmission?
4. what can the station do if there is an access conflict.

Control access protocol:

- In this, the stations consult one another to find which station has the right to send.
- A station cannot send unless it has been authorized by other stations.

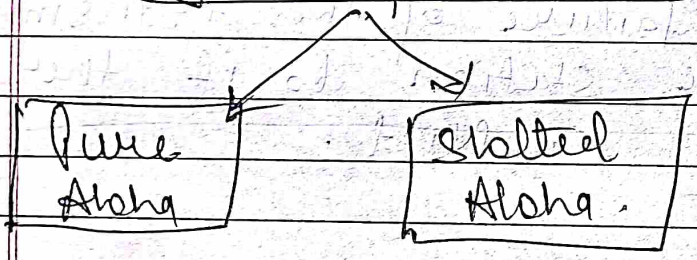
Channelization protocol: is a multiple access method in which the available bandwidth of a link is shared in time, frequency or through code between different stations.

Date
Page

1. Pure ALOHA :-

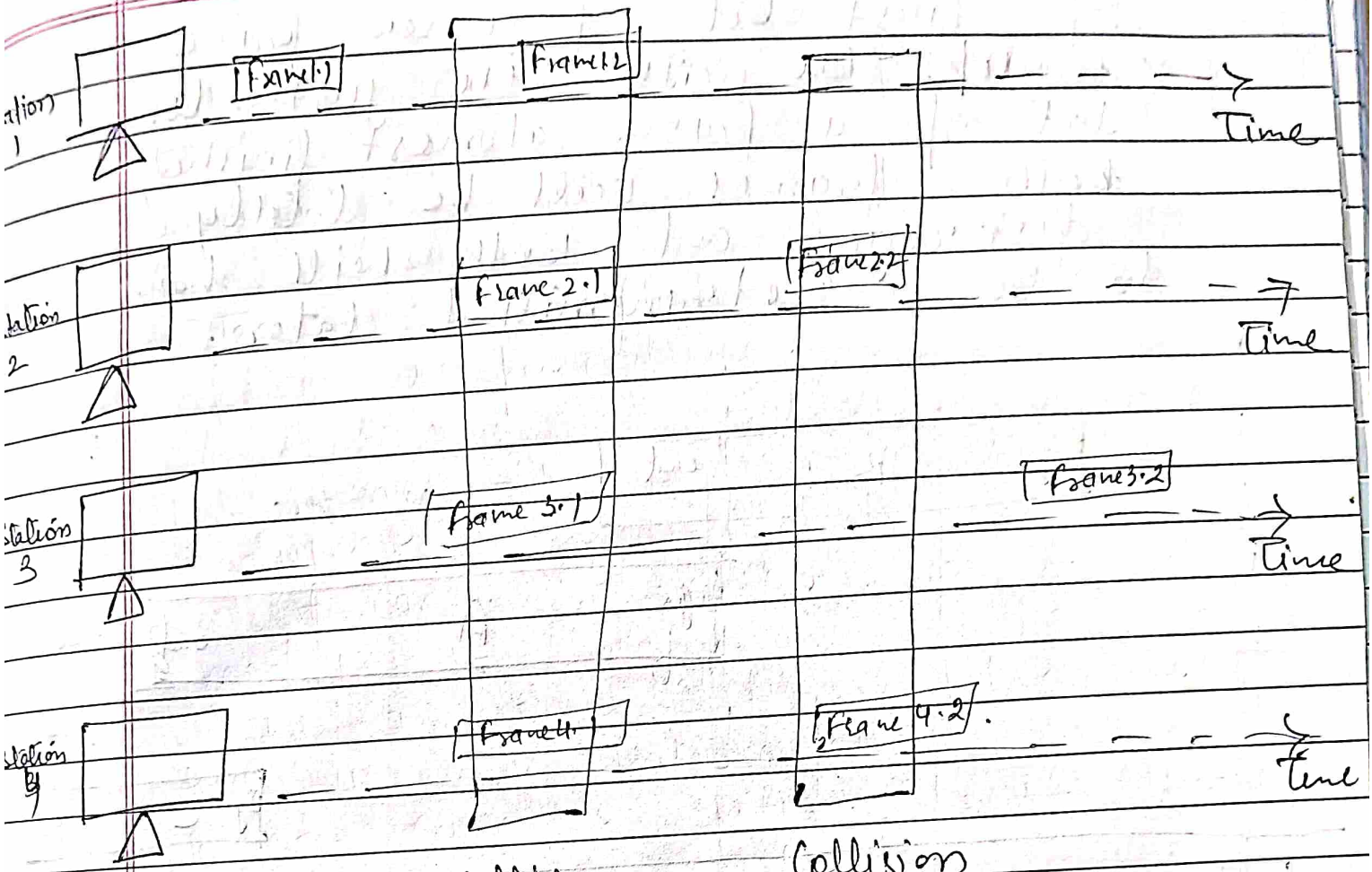
- Aloha is a random access protocol.
- It was actually designed for WLAN but it is also applicable for shared medium.
- In this, multiple station can transmit data at the same time and can hence lead to collision and data being garbled.

Types of Aloha



Pure Aloha :

- Pure aloha allows station to transmit whenever they have data to be sent.
- When a station sends data it waits for an acknowledge.
- If the ack doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-send the data.
- Since different station wait for



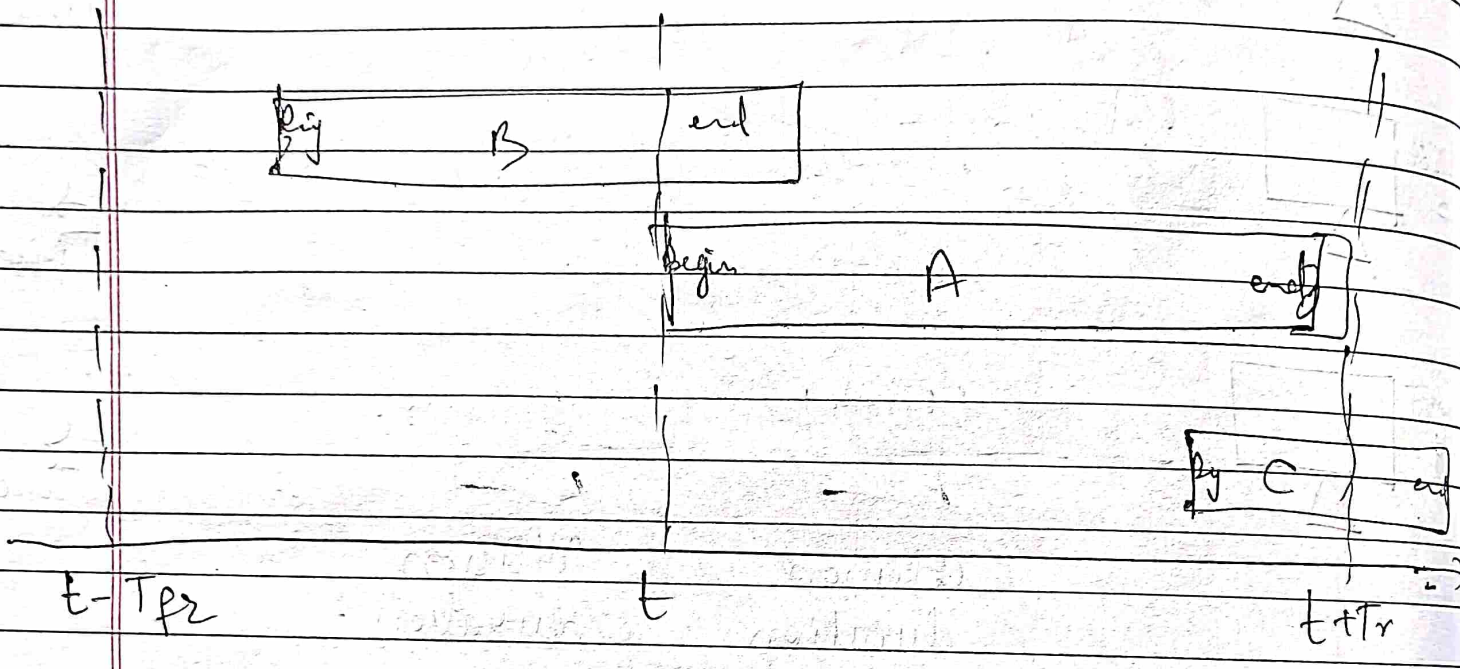
different amount of time and the probability of further collision decrease.

— The throughput of pure aloha is maximized when frames are of uniform length.

Mark

— whenever two frames try to occupy the channel at the same time, there will be a 'collision and both will be garbled.

- If first bit of a new frame overlaps the near the just last bit of a frame almost finished, both frames will be totally destroyed and both will have do be retransmitted later.



← Vulnerable time = 2 × T_{fr} →

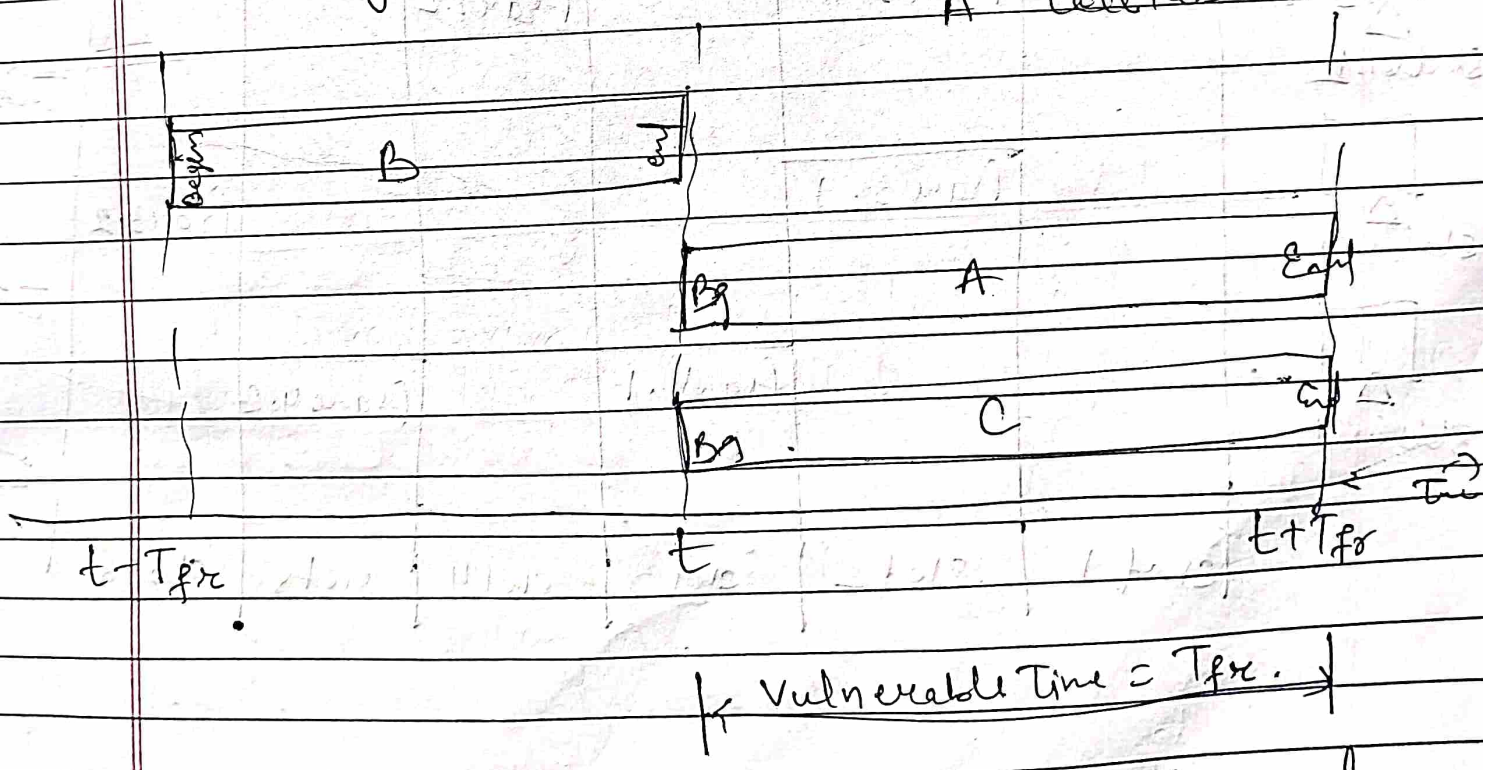
↑ frame Transmission time

- Vulnerable time = 2 * T_{fr}.
- Throughput = $G \times e^{-2G}$, G → no. of station with to transmit at same time.

Maximum throughput = 0.184 for $G = 1/2$.
= 18.4

2. Slotted Aloha:

- Developed just to improve the efficiency of pure aloha as the chances of collision in pure aloha are high.
- The time of the shared channel is divided into discrete time interval called slots.
- The entry of data is allowed only at the beginning of these slots.

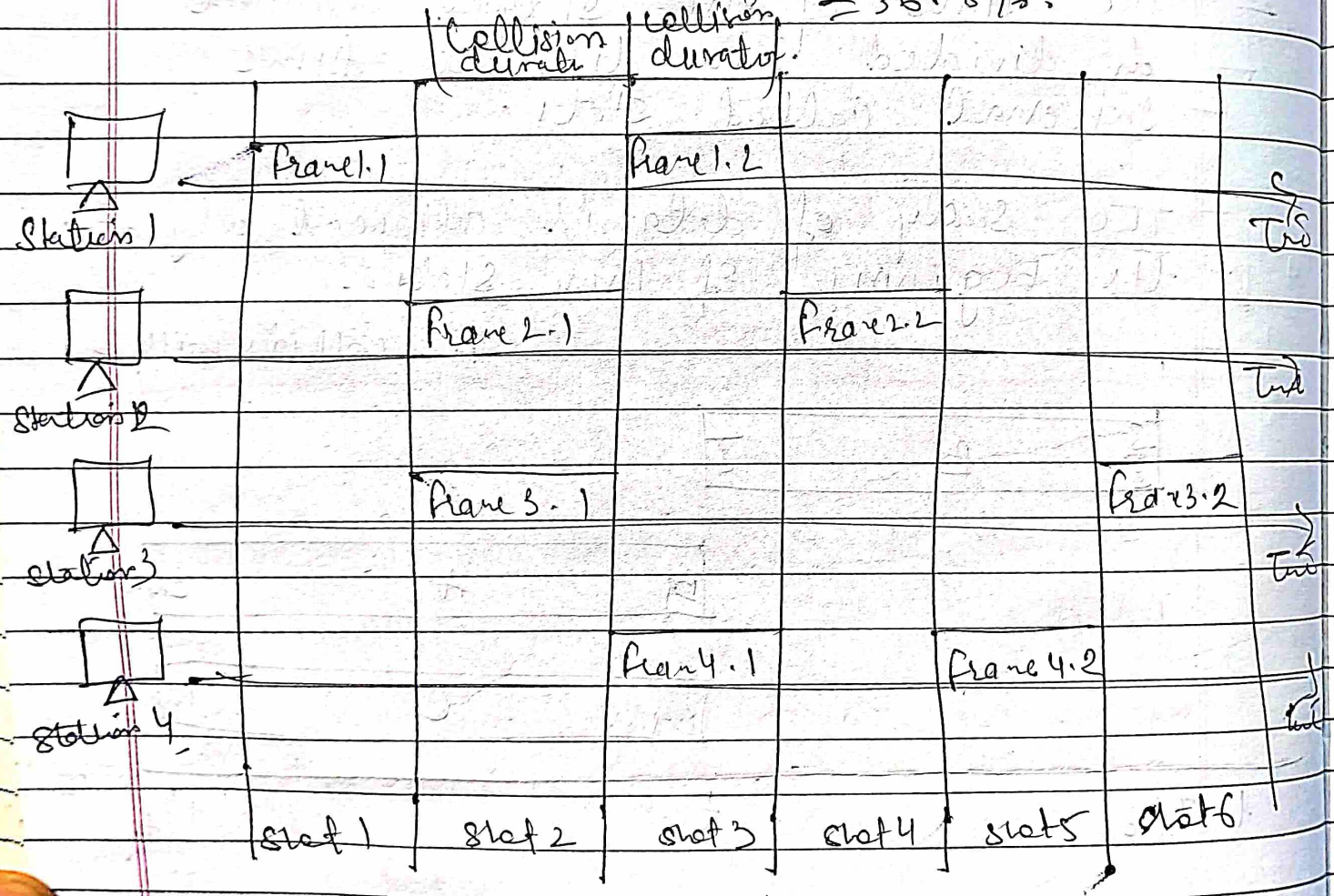


→ If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

Vulnerable Time = Frame Transmission Time (T_{fr})

Throughput = $G \times e^{-G}$, where G → no. of stations ready to transmit in the same time.

Maximum throughput = 0.368 for G = 1
= 36.8%.



Carrier Sense multiple Access.

Date
Page 77

CSMA Protocol

CSMA stand for Carrier Sense protocol

- To Minimise the chance of collision and therefore, increase the performance, the CSMA method

Principle of CSMA: "Sense before transmit" or "listen before talk".

Carrier busy — Transmission is taking place
Carrier idle — No transmission currently taking place.

Types of CSMA

1. 1-Persistent CSMA
2. P- Persistent CSMA
3. Non- Persistent CSMA
4. O- Persistent CSMA.

Modified form

CSMA/CD — (CSMA with collision detection)

CSMA/CA (CSMA with Collision Avoidance).

Date
Page

(1) CSMA/CD (Very easy)

↳ CSMA with collision detection.

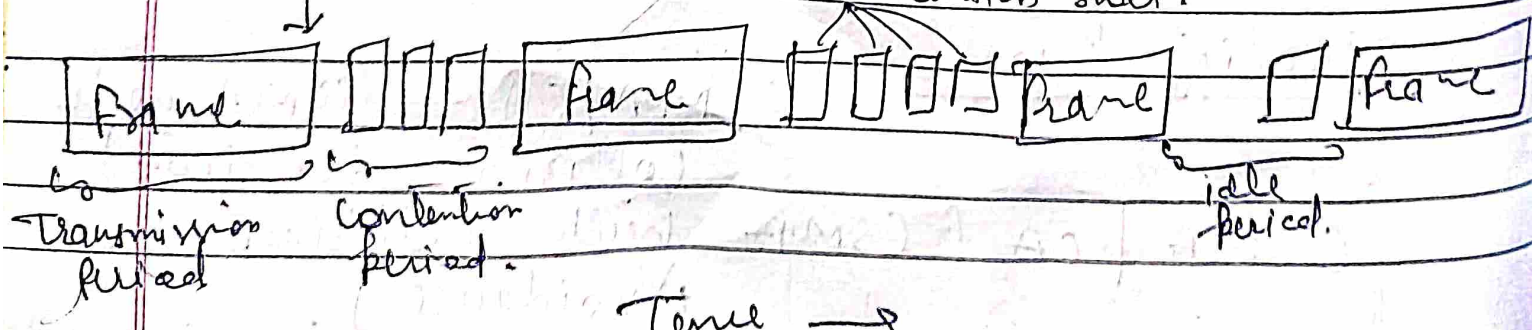
— If two stations sense the channel to be idle and begin transmitting simultaneously they will both detect the collision almost immediately.

— Rather than finish transmitting their frames, which are irretrievably garbled anyway, they should abruptly stop transmitting as soon as the collision is detected.

— Quickly terminating damaged frames saves time and bandwidth.

— This protocol known as CSMA/CD is widely used on LANs in the MAC sublayer.

— Access method used by Ethernet: CSMA/CD.



to :- a station has finished transmitting its frame.

- Collision can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.

After a station detect a collision, it aborts its transmission, waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime.

For BATE

$$\text{Efficiency} = \frac{1}{1+6.44 \times a}$$

$$a = \frac{Tp}{Tt}$$

Note :- If length of packets is bigger, the efficiency of CSMA also increase, but maximum limit for length is 1500 Byte.

need for wireless

Date
Page

(2) CSMA/CA

↳ CSMA with collision avoidance

— Carrier-Sense multiple access with collision avoidence (CSMA/CA) is a network multiple access in which Carrier sensing is used, but nodes attempt to avoid collision by begning transmission only after the channel is sensed to be "idle".

— It is particularly important for wireless networks, where the collision detection is not of the alternate CSMA/CD is not possible, due to wireless transmitters desensing their receivers during packets transmission.

CSMA/CA is unreliable

Due to

hidden node

exposed-terminal problem.

solution

RTS/CTS exchage.

- CSMA/CA is a protocol that operates in the Data link (layer 2) of the OSI Model.

- The Access method used by IEEE 802.11 hei-fi is CSMA/CA.

Unit-3 is finished.

(PART-B).

UNIT: 4

NETWORK LAYER.

Syllabus :→ Logical addressing - IPV4, IPV6, Addressing mapping - ARP, RARP, BOOTP and DHCP - Delivery, Routing algorithms, Congestion Control policies, Leaky bucket and token bucket algorithms.

Q.

IP adress :- IP stands for "Internet protocol adress". An IP adress is a unique number provided to each an every devices.

It is in the form of integric number which is separated by dot (.).

Example : 192.168.10.26.

Date
Page

Addressing

- IP (logical)
- MAC (Physical)

IP address

IPV4

- length 32 bits
- octet 4 (each of 8)
- Orange (0 to 255)
- 4 billion (2^{32}) Maximum
- 192.168.10.26
- → Broadcasty

IPV6

- length 128 bits
- octet 8 (each of 16).
- 0 to FFFF (65535)
- → 340 trillion (2^{128})
- → 3FBB:1806:4545:2:100:LYFF:F821:9X
- Unicasty not broadcasty.

Uses of IP :→ 1). Private IP
2) Public IP.

Class of IP address (IVPv) :

Class A → 0 to 126 (125.225.23.17)

Class B → 128 to 191 (191.23.28.144)

Class C → 192 to 223 (192.204.18.114)

Class D → 224 to 239 (Used for Multicasting)

Class E → 240 to 255 (Used for research)

IP address parts

- Network ID (1)
- Host ID (0)

Class A | N | H | H | H |

Class B | N | N | H | H |

Class C | N | N | N | H |

Date |
Page |

IPV4	IPV6
1. The length of IPv4 is 32 bits	1. The length of IPv6 is 128 bit.
2. In IPv4, around 4 billion unique IP adress are generate (2^{32})	2. In IPv6, around 340 trillion unique IP adress are generated (2^{128}).
3. The range of IPv4 is 0 to 225.	3. The range of IPv6 is 0 to FFFF (65535)
Eg:- 192.225.108.255	Eg.
4. It consist 4 octets, each has 8 bits	4. It consist 8 octets, each has 16 bits.
5. IPv4 is a numeric address seperated by (.)	5. It is a alpha-numeric seperated by colon (:)
6. IPv4 has total five classes	6. It doesn't have any class.

MAC adress: Stand for "Media access control" adress. It is also known as physical adress or hardware adress.

MAC adress is a Unique and permanent adress of all electronic and networking devices.

Format of MAC adress (Total 48 bits)

(I) MM:MM:MM:SS:SS:SS

(II) MM-MM-MM-SS-SS-SS

(III) MMM.MMM.SSS.SSS

Example:- 3C:D9:2B:6F:2b:9C

- 48 bits.
- 12 HDM.
- without nic cannot access any internet.

Uses: 1) Device tracking
2) To connect devices each other.
3) To block unknown person.

Date
Page

IPv4

Header format

4	8	16	32
VER	HLEN	Type of Service	Total Length (16 bits)
Identification (16 bits)		Flags (3 bits)	Fragmentation offset (13 bits)
Time to Live (8 bits)	Protocol (8 bits)	Header Checksum (16 bits)	
Source IP address			
Destination IP address			
Option + Padding			

IP stands for Internet protocol and V4 stand for Version four (IPV4).

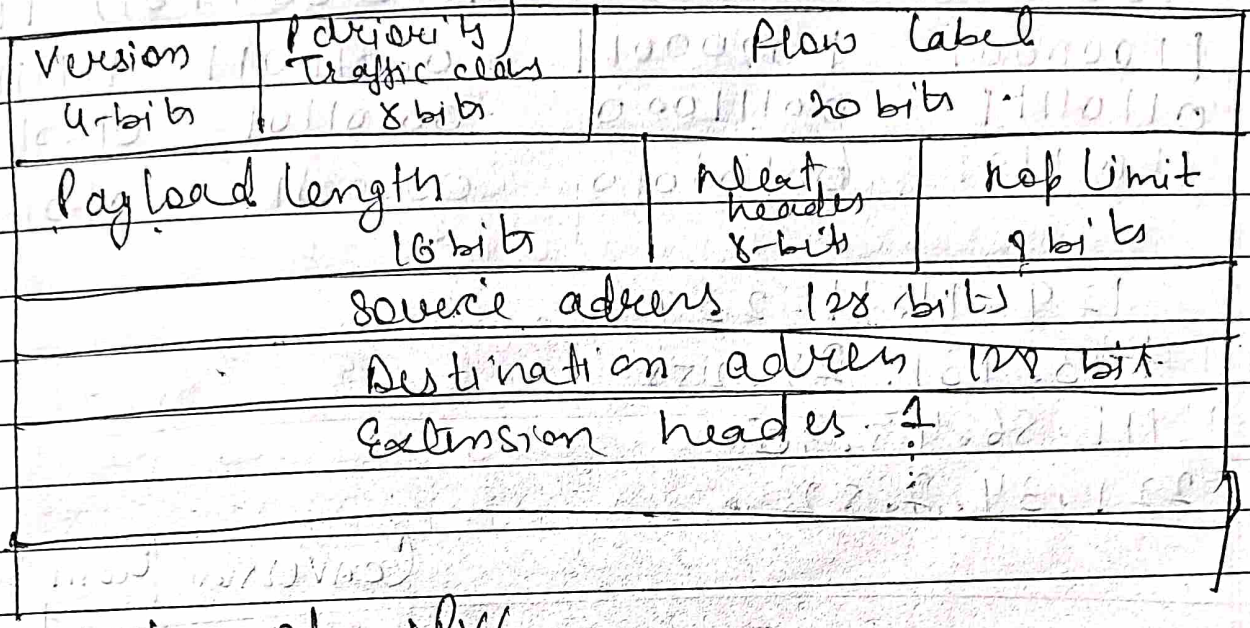
IPv4 support VLSM (Virtual Length Subnet Mask)

Parts

Network part	Host part	Subnet no.
defines the category of network it's assigned.	uniquely identifies the machine on your network	

IPv6

Headers format



Types of IPv6

1) Unicast → refer a single sender and a single receiver. and identifies a unique node on a network.
2) Multicast address: - represent a group of IP ~~address~~ devices.
3) Anycast address: - it is assigned to a set of interface that typically belongs to different nodes.

Date
Page

Question: Convert the following IPv4 adress from binary notation to dotted-decimal notation.

(a) 10000001 00001011 00001011 11101111
(b) 11000001 10000011 00011011 11111111
(c) 01101111 00111000 00101101 01001110
(d) 11011101 00100010 00000111 01010010

Sol (a) 129.11.11.239
(b) 193.131.27.255
(c) 111.56.45.78
(d) 221.34.7.82

Conversion from binary to decimal

Explained

(a) ~~128~~ 64 ~~32~~ ~~16~~ 4 2 1 →

1 2 3 4 5 6 7 8
128 64 32 16 8 4 2 1

64 32 16 4 2 1
1 0 0 0 0 0 0 1

128 64 32 16 8 4 2 1
1 0 0 0 0 0 0 0

If 1 — then

128 64 32 16 8 4 2 1
1 0 0 0 0 0 0 1

128+1 = 129

128 64 32 16 8 4 2 1
0 0 0 0 1 0 1 1 → 8+1+1+1

128 64 32 16 8 4 2 1
0 0 0 0 1 0 1 1 → 8+2+1 = 11

128 64 32 16 8 4 2 1
1 1 1 0 1 1 1 → 239

Now Converting fins decimal to binary.

(b) 111.56.45.25

2	111	1
2	55	1
2	27	1
2	13	1
2	6	0
2	3	1
	1	

1101111

2	56	0
2	28	0
2	14	0
2	7	1
2	3	1
	1	

00111000

Similarly

Date
Page

Classfull addressing.

- IPV4 used the concept of classes. This architecture is known as classfull addressing.
- In classfull addressing, there are 5 classes in which the address space is divided : A, B, C, D and E.
- Each class occupied same fraction of the adress space

But there is a problem with the classfull addressing that is " each class is divided into a fixed no. of blocks with each block having fixed size ".

Class A

- This class is designed for large organisation to manage a large no. of attached hosts or routers
- In a class A, the first bit of first octet is always "0". range from 0.0.0.0 to 127.255.255.255

The first 8 bits or the first octet denote the network portion and the rest 24 bits or 3 octet belong to the host portion.

in the range 0 to 24.

Example: 10.1.1.1

Class B

designed for midsize organisation, to manage tens of thousands of attached hosts or router.

In class B, the first octet always starts with '10'.

Range 128.0.0.0 to 191.255.255.255

The first two octet denote the network portion and remain 2 octet belong to host potion.

Example: 172.16.1.1.

Date
Page

Class C

- Small no. of nodes — intended for a small organization.
- First 3 three octet denote the network portion and rest one octet belong to host portion.
- In class C, the first octet would always starts with '110'.

Range from 192.0.0.0 to 223.255.255.255

Example: 192.168.1.1

Class D and E

Class D is reserved for Multicasting. In Multicasting data is not destinated for a particular host, that why there is no need to extract host address from the IP address, and class D does not have any subnet mask.

- E class is reserved for future

use and experimental purpose only for R+D or study.

- This type of adressig is known as class full addressig and resulted in very wasted IP address allocation.

Classless adressig

- Classfull adressig leads to address depletion. That's the big issue for this scheme and that's why it's not used nowadays.

- To overcome this problem the classless adressig is designed and implemented In this scheme of classless adressig, there is no class, but the addresses are still granted in blocks.

- In this, when an entity, machines which needs to connected to the Internet, it is granted a block (range) of adress. The size of the block (no. of adress) varies based on the nature, type and need of the entity.

Jai Hoo Sathariyan

Date 18/10/2023
Page 1

Adressing Mapping :

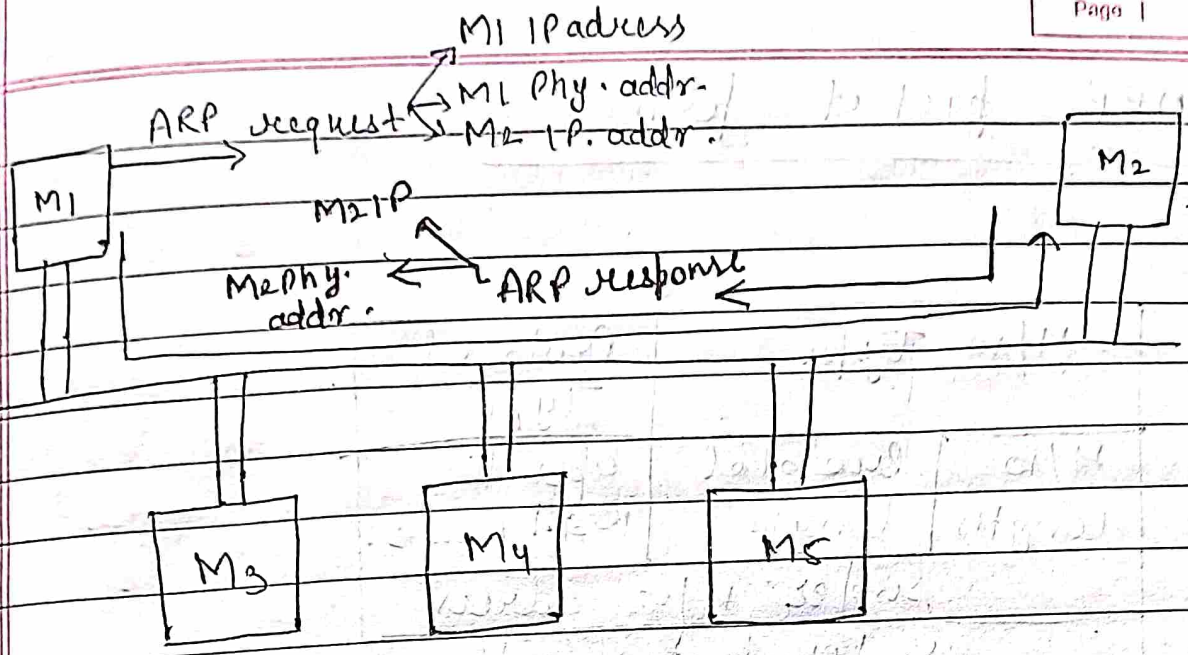
1. ARP (Adress Resolution Protocol) : ARP associate an IP address with the physical adress.

Logical adress $\xrightarrow[(ARP)]{\text{Mapping}}$ Physical adress

Imp As 'IP' uses the service of Data link layer, it needs to know the physical adress of the next hop $\Rightarrow$ ARP.

Working of ARP protocol

ARP accepts a logical adress from the IP protocal, maps the adress to the corresponding physical address and pass it to the data link layer.



ARP request ⟶ Broadcast
ARP response ⟶ Unicast

Anytime a Host or a Router needs to find a physical address of another Host or Router on its network (N/w), it sends an ARP Query packet. The packet include the physical and IP adress of the sender and the IP adress of the receiver. Query is broadcasted to the network, when the intended recipient recognize its IP adress, it sends back an ARP response packet which contain both IP and physical address.

Date |
Page |

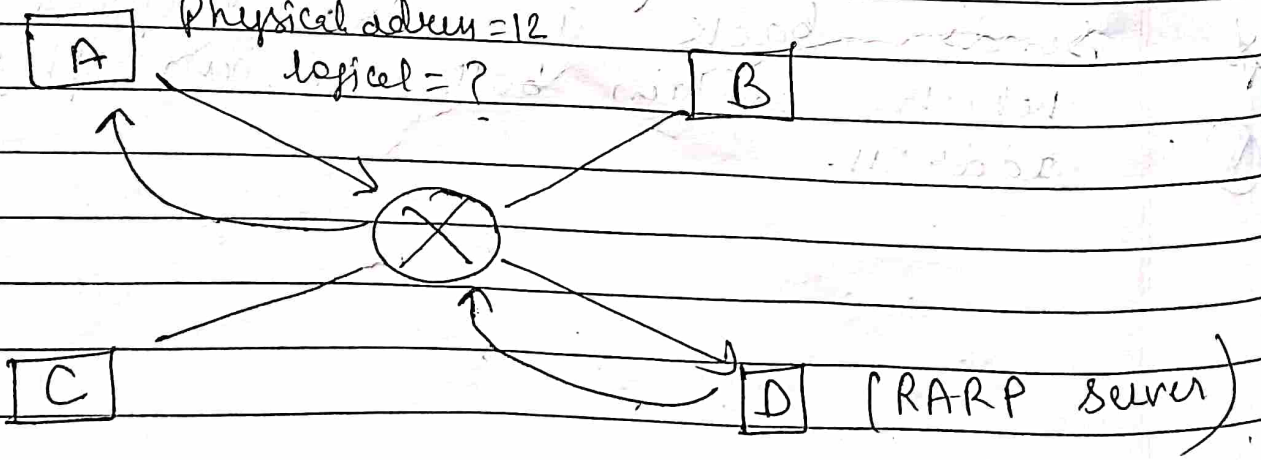
ARP packet format

H/w Type		Protocol Type
H/w Length	Protocol Length	operation Req. 1, Reply 2.
Sender H/w adress		
Sender protocol adress		
Target H/w adress (not filled)		
Target protocol adress		

2. RARP (Reverse address Resolution protocol)

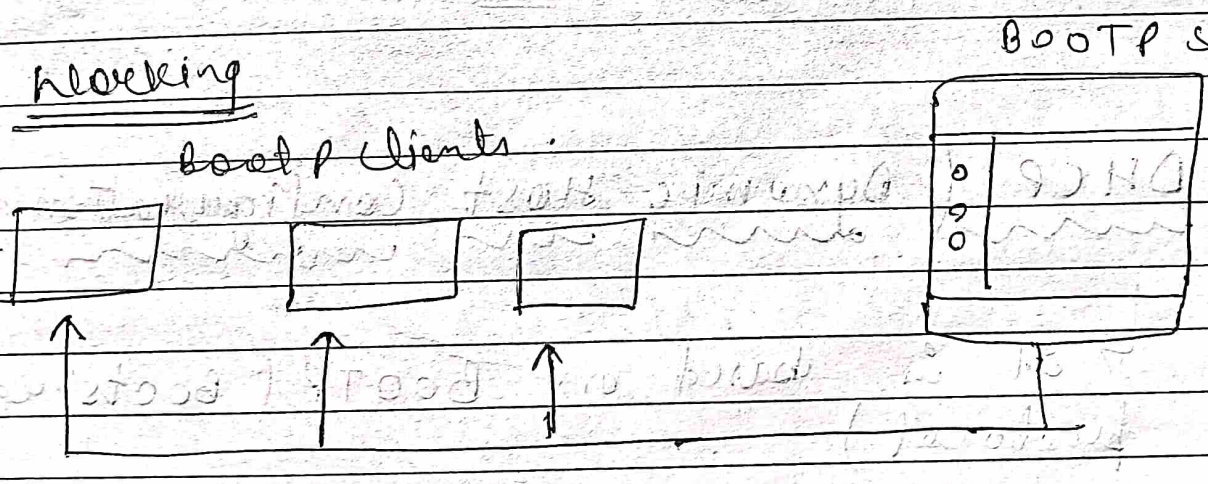
RARP Maps a physical adress to a logical adress.

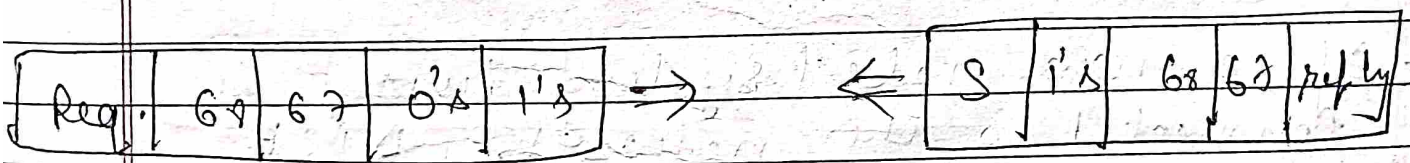
Physical adress —Mapping→ logical/IP adress



— RARP performs the reverse of ARP. It is used to map a known MAC address to an IP address. This is mainly used in older diskless workstations

3. BOOTP (Bootstrap protocol) :- It is a network protocol used to assign IP address to a network device from a configuration server.





— BOOTP help devices that don't have their addresses yet, like brand new phones, to get set up on a network.

Date
Page

Uses

1. BOOTP is mainly used in a diskless environment.
2. BOOTP is the transfer of a data between a client and a server to send and receive request and corresponding responses by the networking server.
3. It is primarily required to check the system or a network the first time you start from your computer.

4. DHCP (Dynamic Host Configuration protocol)
   - ↳ It is based on BOOTP (Bootstrap protocol)
   - If a new node (system/ device) is connected to the network, DHCP provide it with :-
     - (i) DNS server.
     - (ii) Subnet Mask
     - (iii) Domain Name
     - (iv) IP adress.

DHCP client & server works together to handle the roaming status and to assign the IP address on a new n/w efficiency.

- DHCP server allocates an IP addresses from Pool of IP addres to client.
- ~~Dynamically allots them~~

Importance of DHCP in Mobile Computing

It provide temporary IP address whenever a host moves from n/w to another n/w.

Note:- DHCP is like an automatic addressing. It hands out IP addresses to devices when they connect to a network, so they don't have to do it themselves.

Delivery:- This is like the postal service for computer. The network layer decide how to send data from one computer to another through routers and switches.

Date
Page

Routing Algorithms

Refer link in notebook

Conjuction Control: A state occuring in network layer when the message traffic is so heavy that it slows down network response time.

Cause

1. Many input lines demanding the same output lines.
2. Slow receiver fast sender
3. Low bandwidth lines can also cause congestion.
4. Congestion itself (duplicacy).
5. Traffic is busy.

Leaky bucket Algorithm

Imagine a bucket with a small hole in the bottom as depicted in figure, no matter at what rate enter the bucket, the outflow is at a constant rate, when there is any water in bucket and zero when the bucket is

empty. Also once the bucket is full, any additional water entering it spills over the sides and is lost.

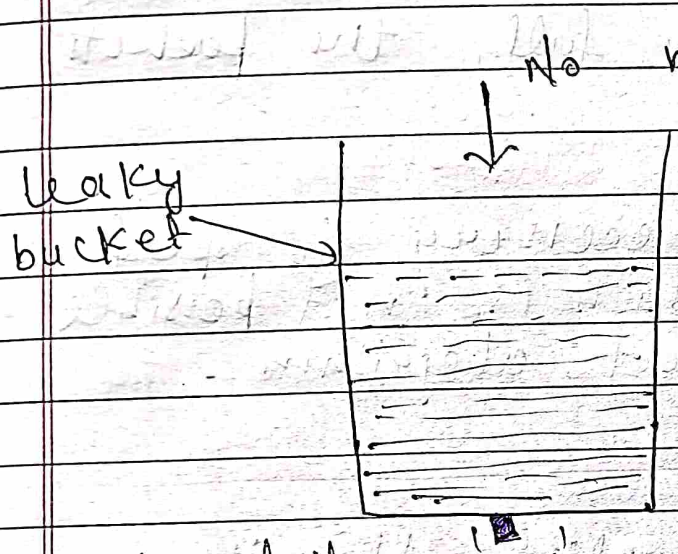
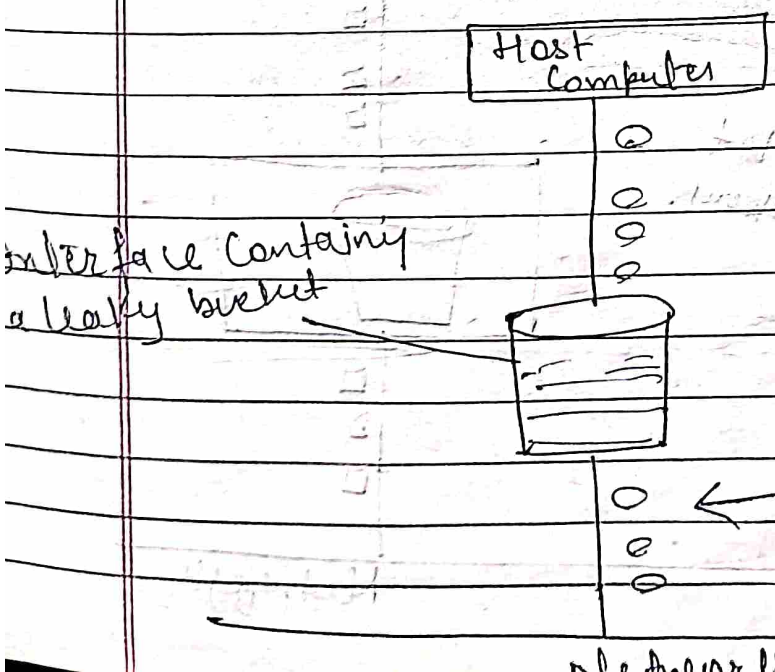


Fig. Normal leaky bucket.



Date
Page

Advantages

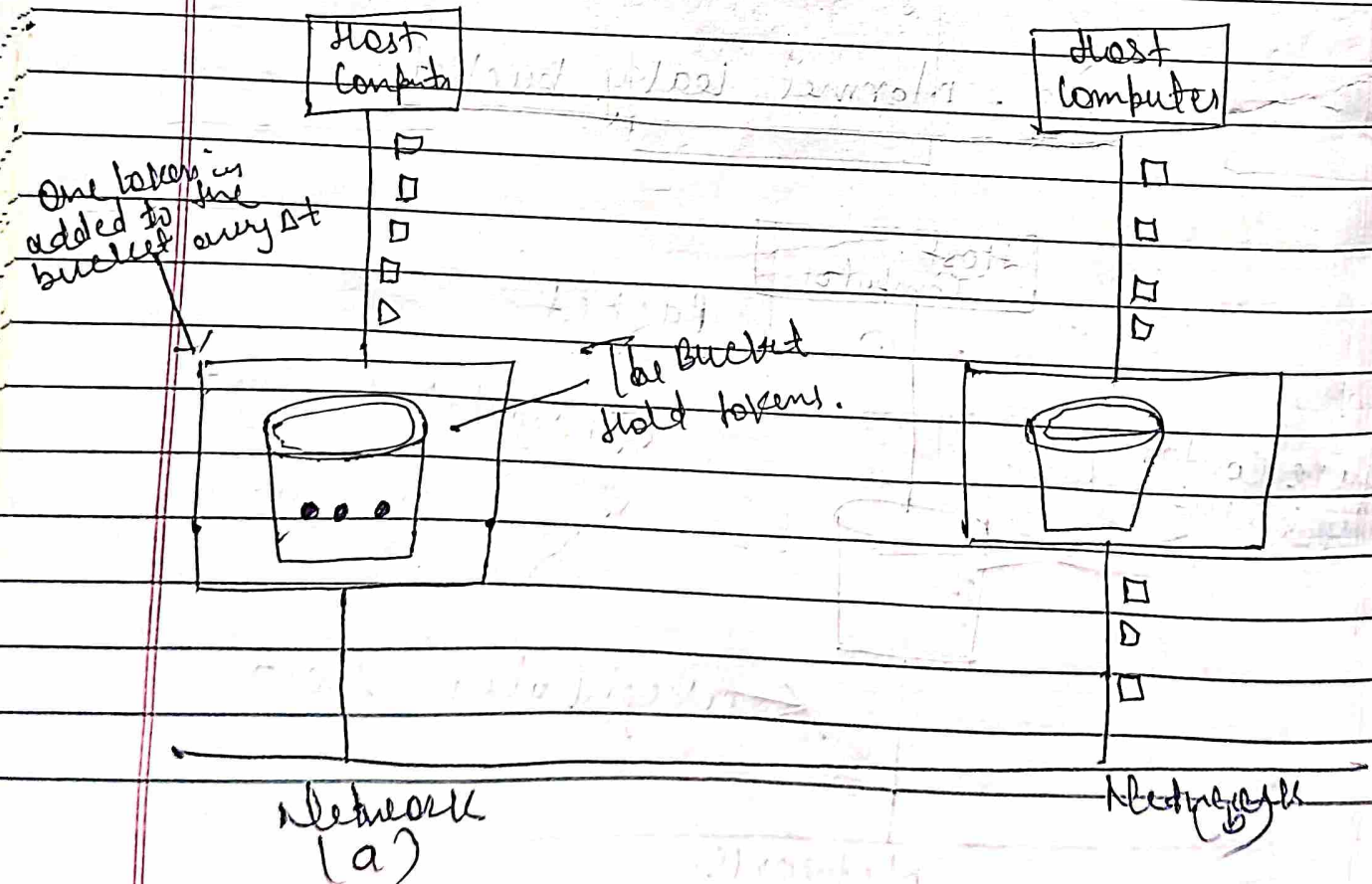
Reduces the chances of congestion

Disadvantages

1. When the queue is full, the packets are discarded.
2. Sometime it is necessary to speed up the output which is not possible in leaky bucket algorithm.

Token bucket Algorithm

Hold 'token' generated by a clock at the rate of one token every ΔT sec.



A token bucket algorithm throws away token when the buckets fills up but never discards packets.

Steps of this algorithm.

1. In regular interval tokens are thrown into the buckets.
2. The bucket has maximum capacity.
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.

Formula = $M * S = C + P * S$.

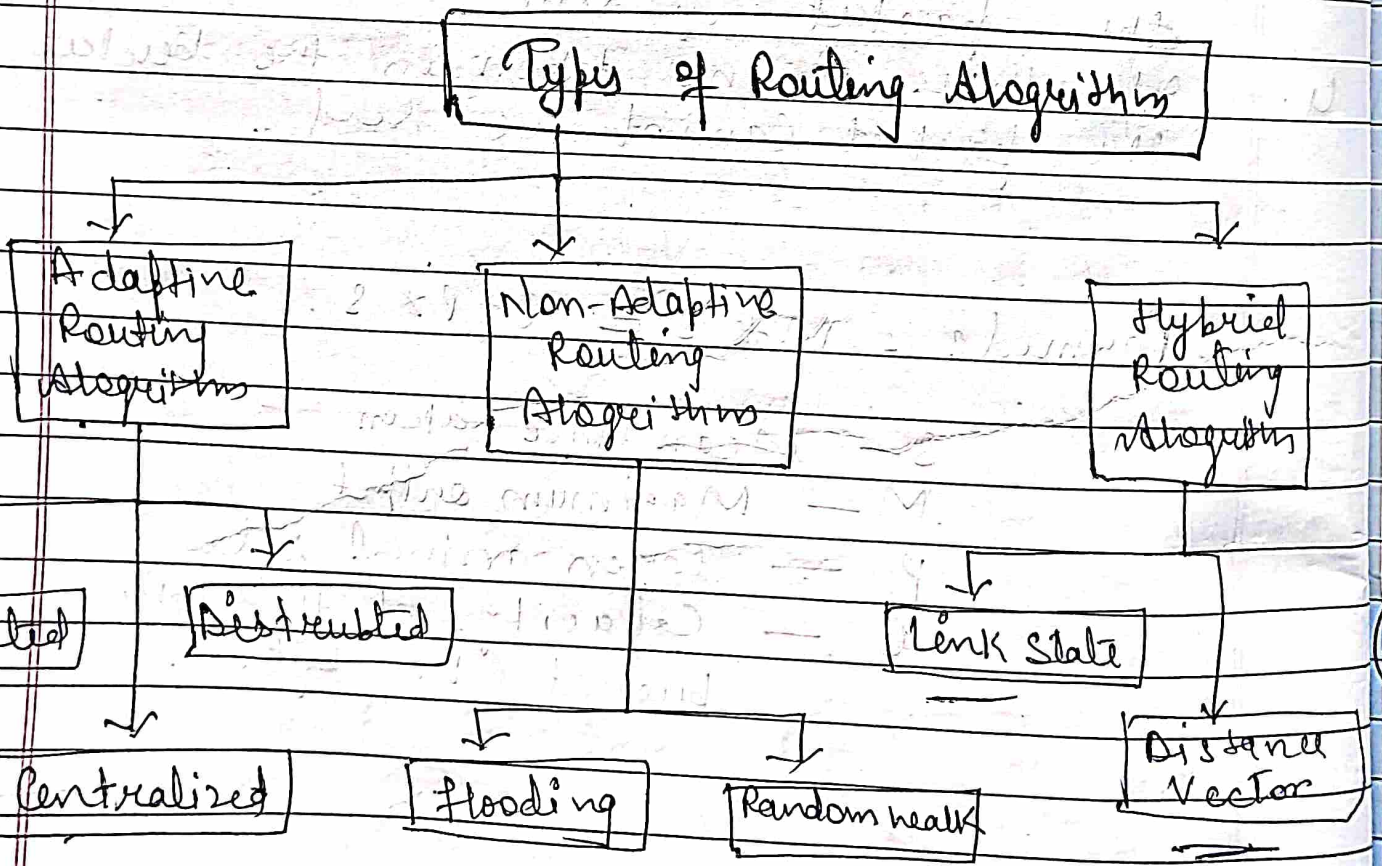
S — Mean time taken
M — Maximum output
P — Token arrival rate
C — Capacity of the token bucket in byte.

Date
Page

Routing Algorithms

Routing is the process of establishing the routes that data packets must follow to reach the destination.

Routing algorithm are like GPS for the internet. They help decide the best path for data to travel from your computer to its destination.

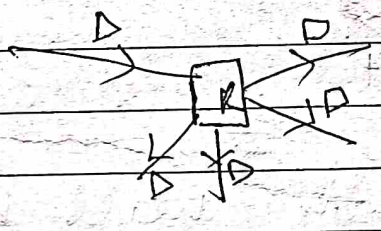


1. Non-Adaptive Algorithm:

- Also known as static Routing
- Routing process will designed in advance
- All the routing process will be stored in routers when the booty complete.
- It doesn't effect with change in network topology and traffic.

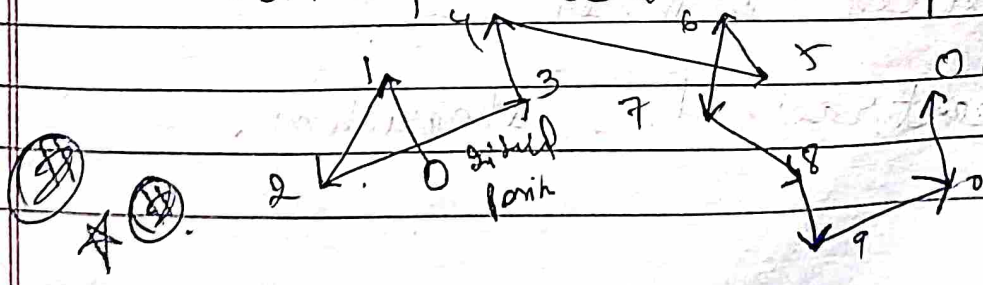
Types

- Flooding
  - All incomig will be transmitted to all outgoig links



  - Multiple copies of packet

- Random walk
  - Incomig packets will be transmitted to neighbours links randomly.
  - Best for alternative path.



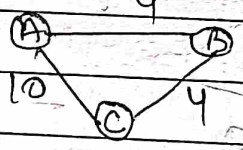
Date
Page

2. Adaptive Routing algorithm

- Dynamic Routing algorithm.
- Routing will change dynamically based on change in in topology and traffic
- Parameters - Hop count
  Distance
  Transmit Time

Classifications

1. **Centralized**: also called Global routing algorithm.
   - Compute least cost path based on global information.



2. **Isolation**: Routing will be decided based on local information rather than global.

3. **Distributed**: Compute least cost path based on iterative and distributed manner.
   - Decentralized algorithm.

Date
Page

3. Hybrid Algorithms: these algorithms are a combination of both adaptive and non-adaptive algorithm. In this network is divided into small region, and each region uses a different algorithm.

1. Link state: In this, each router create a detailed and complete map of the network which is then shared with all other routers.

2. Distance vector: In this, each router maintain a table that contain information about the distance and direction to every other node in the network.

Count to infinity: problem is that if A tells B that it has a path somewhere, there is no way for B to know if the path has B as a part of it.

To see this problem:

Imagine a subnet connection like A-B-C-D-E-F, and let the Metric between the routers be 4 no. of jumps.

Chapter-4 is completed.

Date |
Page |

Link State	Distance Vector
1. Routers shared a detailed map of the entire network with each other.	1. Routers only tell their neighbours about the routes they know.
2. Routers talk to each other only when something in the network changes.	2. Routers chat with their neighbours regularly, even when nothing is changing
3. Router have a full picture of the entire network.	3. Router just knows the distance and direction to reach destination.
4. Eg OSPF	Eg RIP.
5. Wide bandwidth is available	5 bandwidth is less

Jai Hoo Satmeyan

Date 17/10/22
Page 1 (1)

UNIT: 05

TRANSPORT LAYER.

Syllabus :→ Design issues, Elements of transport protocols — Connection establishment and release, process to process communication, User datagram protocol (UDP), Transmission control protocol (TCP), flow control.

Elements of transport protocol :→

(i) Addressing
(ii) Connection Establishment.
(iii) Connecting release
(iv) Error control and flow control.
(v) Multiplexing.
(vi) Crash recovery

Date
Page

1. **Connection establishment :→** With packet lifetime bounded, it is possible to devise a foolproof way to establish connections safely.

Packet lifetime can be bounded to known maximum using one of following techniques:

→ Restricted subnet design.
→ Putting a hop counter in each packet.
→ Time stamping in each packet.

Using a 3-way handshake, a connection can be established. This establishment protocol doesn't require both sides to begin sending with same sequence no.

2. **Connection release :→** A connection is released using either asymmetric or symmetric variant. But, the improved protocol for releasing a connection is a 3-way handshake protocol.

There are 2 styles of terminating a connection:

(i) Asymmetric release.
(ii) Symmetric release.

Asymmetric release is the way the telephone system works: when one party hang up, the connection is broken.

Symmetric release treats the connection as two separate unidirectional connections and requires each one to be released separately.

In short

Connection establishment involves a series of step to set up a connection, including handshaking and negotation.

Connection release involves terminating an establishment connections, typically with a graceful termination process.

Process to process communication: The transport layer enables communication b/w processes or applications running on different devices. It must identify these processes through port numbers or identifiers.

Date
Page

User Datagram protocol (UDP) :

UDP is one of the core transport layer protocol in the Internet protocol (IP) suite. It is connectionless, lightweighted protocol that is designed for efficiency and speed. Unlike Transmission control protocol (TCP), which is connection-oriented and provides reliable data delivery, UDP does not establish a connection, does not provide error ~~correction~~ checking, and does not guarantee the order of delivery. Instead, UDP is often used where speed is low overhead are more more important than reliability, and it is well-suited for applications that can tolerate some data loss.

Header format of UDP

The UDP header is simple and consist of four fields, each 16 bits (2 bytes) in length.

Then field include:

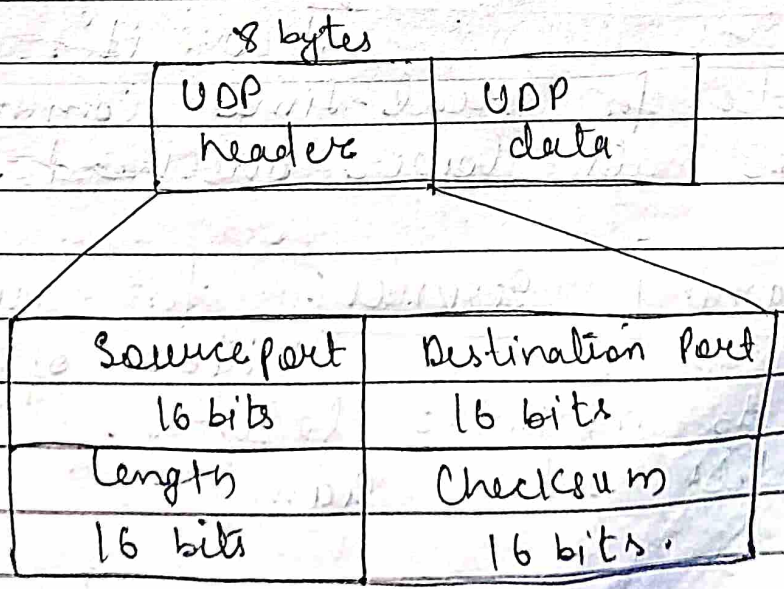
1. Source Port (16 bits): This field specifies the source port number, which is used to

identify the application or process on the sending host.

2. Destination port (16 bits): This field specifies the destination port number, which identifies the application or process on the receiving host.

3. Length (16 bits): This field specifies the length of the UDP header and the data in bytes. The minimum length is 8 bytes (the size of the header itself).

4. Checksum (16 bits): This field is optional and is used for error checking. If the checksum field is set to all zeros, it means that no checksum is used.



Date
Page

Protocols that can be used with UDP:

1. **DNS (Domain Name System):** DNS uses UDP for quick lookups and queries. When the response data is too large for a single UDP packet, it may switch to TCP.

2. **DHCP (Dynamic Host Configuration Protocol):** DHCP uses UDP to lease and manage IP addresses for network devices.

3. **TFTP (Trivial File Transfer Protocol):** TFTP is a simple file transfer protocol that uses UDP for transferring files.

4. **VoIP (Voice over IP):** It uses UDP because it's more suitable for real-time communication due to its lower overhead.

5. **Streaming Services:** For audio and video often use UDP to minimize latency. Example online Gamy

6. SNMP (Simple Network Managment Protocol):

SNMP can use UDP for certain operations, and it may switches to TCP for more extensive data exchange.

7. Network time protocol:- NTP used synchronise time across networked devices, UDP to

8. BootP (Bootstrap Protocol): Similar to DHCP, BootP uses UDP for obtaining IP addresses during bootstrapping.

UDP are chooses when speed and efficiency are more critical than guaranted delivery and error recovery.

Jai Hoo Satnarayan

Date 22/10/2024
Page 1

Transmission control protocol (TCP)

TCP is a fundamental transport layer protocol in the Internet protocol (IP) suite. It provides reliable, connection-oriented, and error-checked data communication between devices on a network.

TCP ensure the ordered delivery of the data, flow control, congestion control, and error detection and correction, making it suitable for application where data integrity is critical.

Header format of TCP-

The TCP header is more complex than UDP due to the additional functionality it provides.

The TCP consist of the following fields:-

1. Source Port (16 bits) — specifies the source port no which identify the send application or process.

2. Destination port (16 bits) — " " destination " " " the receiving application or process.

3. Sequence Number (32 bits) — Used for reliable data transfer.

4. Acknowledgement no. (32 bits) — this field contain the Sequence no. that the sender is expecting to receive next.

5. Data offset (4 bits) — Indicate the length of TCP header in 32-bit words.

6. Reserved (6 bits) — These bits are reserved for future use and must be set to zero.

7. flags (6 bits) — To manage the connect and data transfer.
   - URG (1 bit) - Urgent point field significant
   - ACK (1 bit) - Acknowledge field significant
   - PSH (1 bit) - Push function
   - RST (1 bit) — Reset the connection
   - SYN (1 bit) — Synchronize Sequence no. for a new connection
   - FIN (1 bit) — no more data from the sender.

8. Window size (16 bits) — Specifies the size of receiver window. This help with flow control.

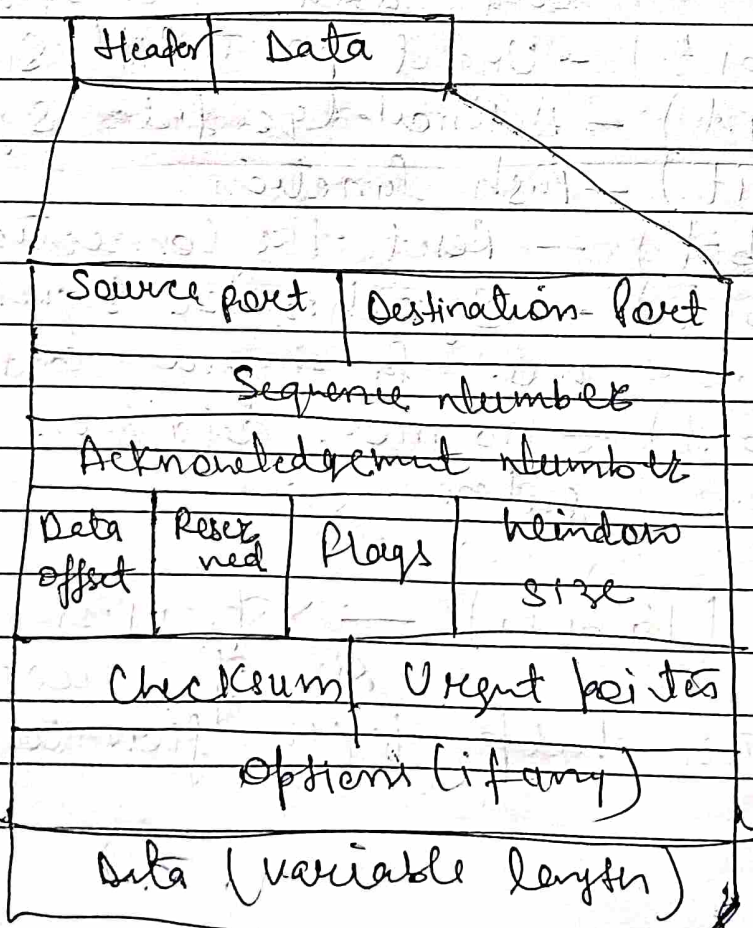
9. Checksum (16 bits) — Used for error checking, ensuring data integrity.

10. Urgent pointer (16 bits) — Shereby the last urgent data byte.

11. Option (variable length) — options such as maximum size (MSS), timestamp, window scale factor etc. can be included here.

12. Data (variable length) — The actual application data being transmitted.

TCP header —



Protocols that can operate over TCP:

TCP widely used for applications that require connection-oriented communication.

1. HTTP (Hypertext transfer protocol) :- Used for serving and accessing web pages on the world wide web.
2. FTP (File Transfer protocol) — Design for transferring file b/w hosts.
3. SMTP (Simple Mail Transfer Protocol) — Used for sending email messages.
4. Pop3 (Post office protocol, version 3) — Used by email clients to retrieve message from a mail server.
5. IMAP (Internet message Access protocol) -
6. HTTPS (HTTP secure) — A Secure version of HTTP Used for secure web browsing.
7. SSH (secure shell) — protocol for secure remote login and command execution.

8. SQL (Structural Query language) — Used for communication b/w database and applications.

9. DNS (Domain name system) — DNS can use both UDP and TCP for various tasks, with TCP often used for larger data transfer.

10. SMTPS (SMTP Secure).

11. XMPP (Extensible Messaging and presence protocol): Used for instant messaging and presence information.

Connection Oriented Services (TCP):

1. Connection Establishment:- In this phase, the two host, often refered to as the client and the server, engage a process known as "three way handshaking" to establish a connection.

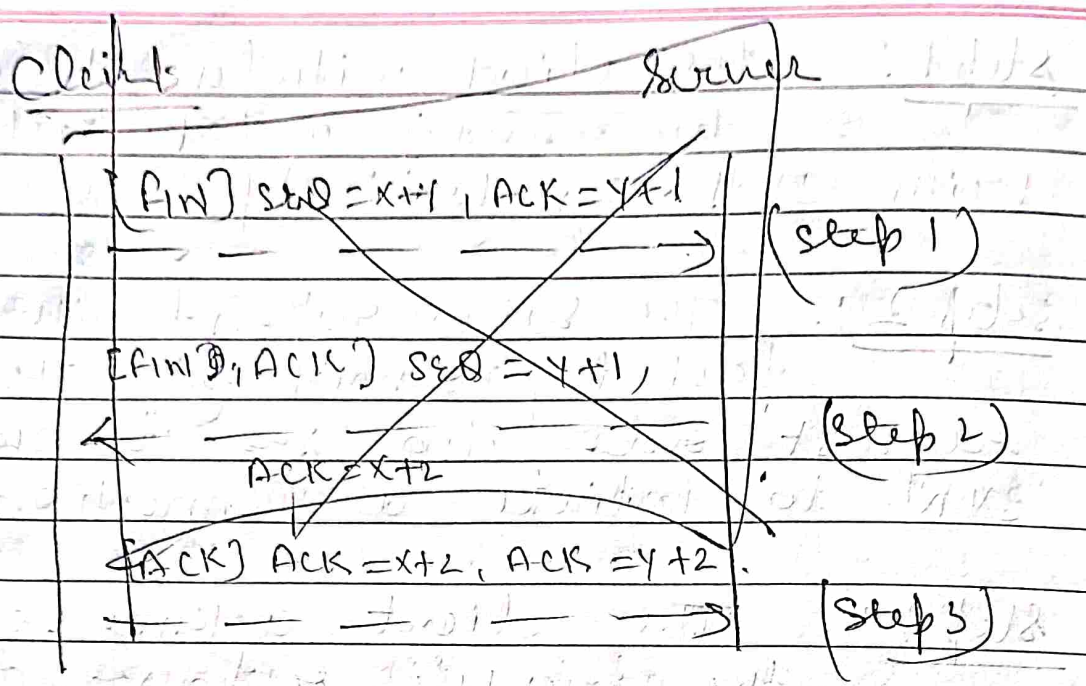
Step 1: the Client initiates the Connection by sending a TCP packet with SYN (Synchronize) flag set.

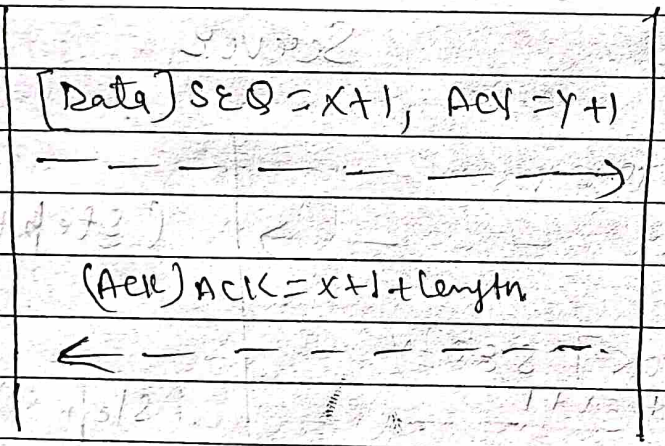
Step 2: The server responds with a TCP packet acknowledging the client's request and also send its own SYN to initiate a Connection.

Step 3: The client acknowledges the server's response, and the Connection is established.

Client		Server
(SYN) SEQ = X	——→	(Step 1)
[SYN, ACK] SEQ = Y ACK = X+1	←——	(Step 2)
(ACK) ACK = Y+1	——→	(Step 3)

2. Data transfer:- During this phase, data is exchanged b/w the client and server in segment. Each segment is assigned a sequence no. to maintain order and is acknowledge by the receiving party.





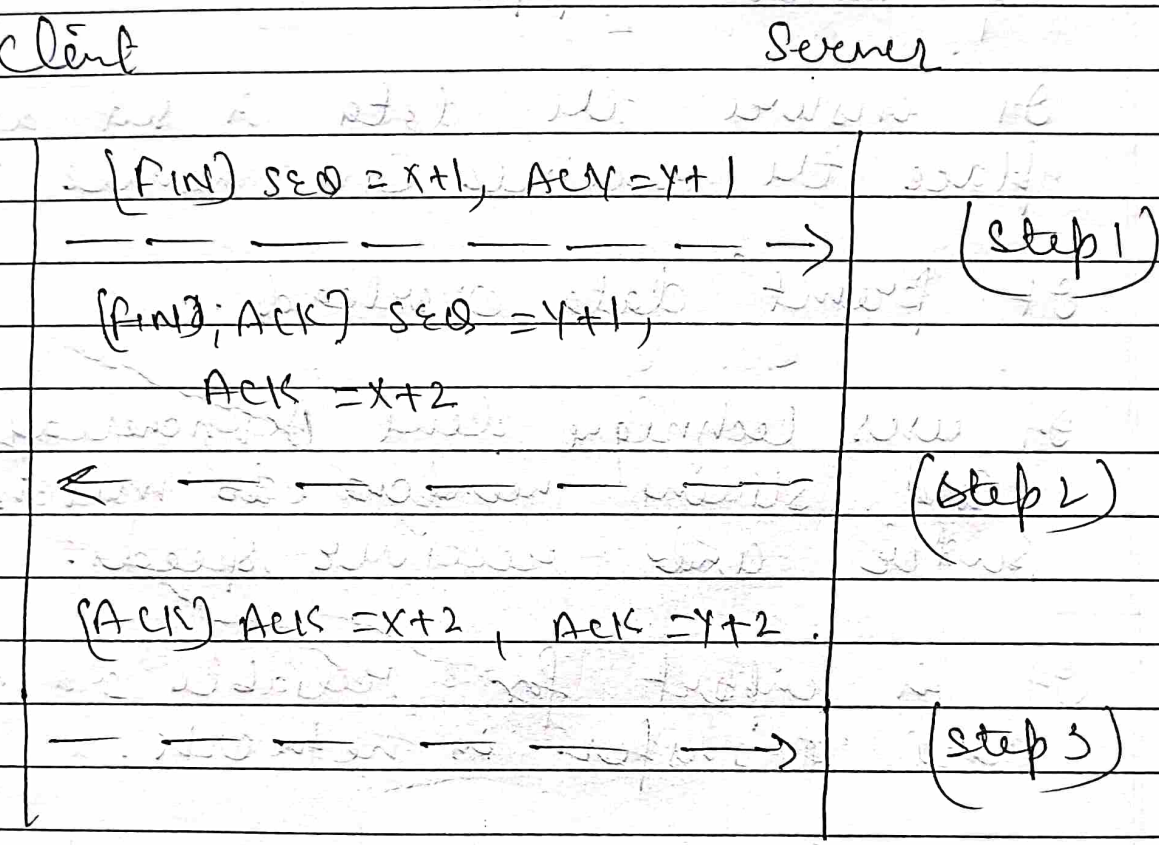
3. Connection release (three way handshaking):-

On this phase, the client and server perform a three way handshake to gracefully release the TCP connection.

1. The client initiate the termination by sending a TCP packet with FIN (finish) flag;

2. The server acknowledge the client's request and send its own FIN to indicate its willingness to terminate.

5. The client acknowledge the server's FIN request.



Then three phase ensure the orderly and reliable establishment, data transfer, and release of a TCP connection.

Date
Page

Flow control: This mechanism is designed to manage the rate at which data is transmitted from the sender to the receiver.

1. It is just like regulating the flow of water in pipe.
2. It ensure the data is sent at a place the receiver can handle it.
3. It prent data overload.
4. It uses technique like Acknowledgent (ACK) and sliding window to match sender and receiver speed.
5. It is cipart for reliable and efficint data transfer in network.
6. It's is like a "traffic cop" for data, makig sure everything flow smoothly and does n't get stuck.

Design issues: Renin graf Rafter 22/10/21.

Unit-5 is complied

Date | 24/10/25
Page | 15

UNIT: 06

SESSION, PRESENTATION AND APPLICATION LAYER

Syllabus :→ Session layer — Design issues, remote procedure call, presentation layer — Design issue, Data Compression techniques, Application layer — Domain Name space (DNS), DDNS, TELNET, EMAIL, File Transfer protocol (FTP), WWW, HTTP, SNMP.

Session layer :→

Design Issue :- One of the issue in session layer is managing and maintaining communications

Session b/w two devices. This involves establishing, maintaining and termination sessions. For example, when a user connects to a remote sensor, there should be mechanism for session initiation, security and error recovery.

Remote procedure Call (RPC) :- RPC is a protocol that allow a program to call a procedure (subroutine) to execute on another address space (commonly on a remote server). One design issue related to RPC is ensuring the reliability and security of these remote procedure calls, including handling errors and handling concurrent request.

Presentation layer :-

Design issue - group

Data compression techniques - group.

Application layer :-

1. DNS (Domain name system) :- It is a naming system that is used to identify devices across the network. It is an application layer protocol and is used to map the domain names to the IP address.

why needed

It is very difficult to remember IP address for every website that we check out. For example, if we want to do online shopping, we search for some online shopping website i.e. name. It will be really difficult for us to visit a website if we have to remember IP address for every website instead of their name.

DNS makes this task very easy for us as it maps the domain name with IP address and we don't need to remember IP address and we don't need to remember IP address. We just search for the domain name of the website and DNS provide the IP address for that website.

Date |
Page |

Types of Domain

1. Generic domain — It define the category of domain

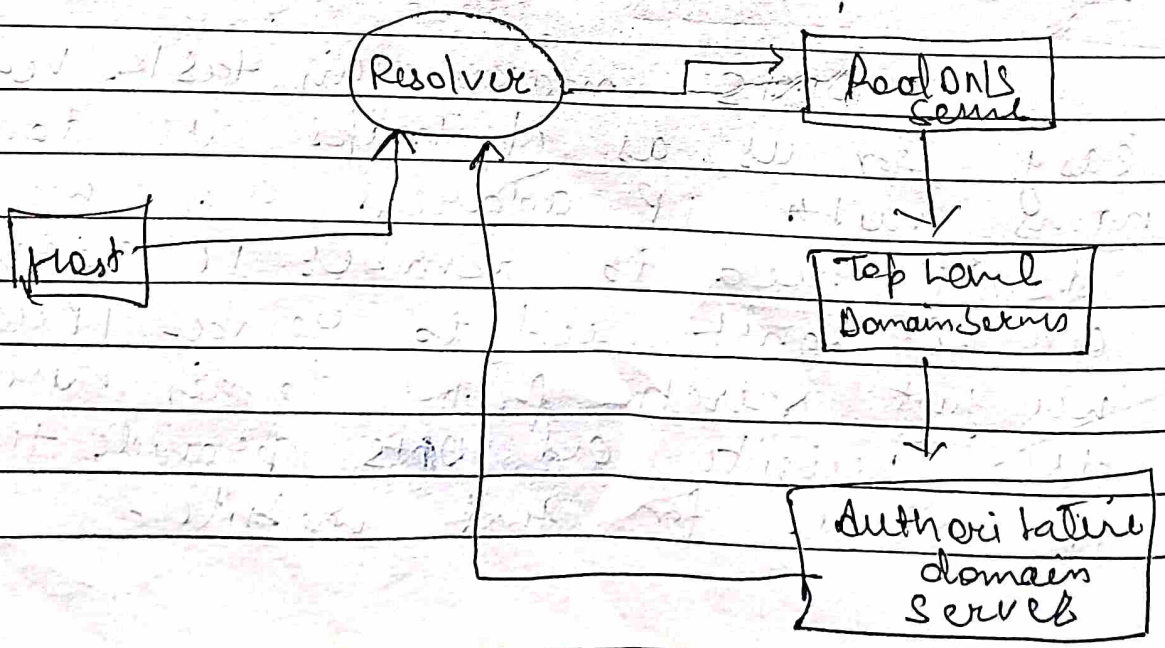
Eg (.com — commerical)
(.org — non-profit organization)
(.edu — educational),

2. Country domain — It categories acc. to country.

Eg. (.in — India), (.UK — United Kingdom)

3. Inverse Domain — used for mapping an address to a name.

Working



1. The client request for the IP adress of a particular domain name to the DNS resolver.
2. The resolver request to the root DNS server.
3. The root DNS Server than forwards the query to the Top-Level DNS server
4. The Top level domain Server has all the information about the authoritative DNS Server
5. The authoritative server than returns the IP adress corresponding to the requested domain name to the resolver.
6. The resolver than return the IP address to the host.

2. Dynamic DNS (DDNS) :- DDNS is an extension of DNS that allow dynamic IP adress to be updated in real-time. This is particularly useful when you have a device with dynamic IP adress, which can change frequently, and you wants to ensure that it's always accessible via its hostname or domain name.

Next page

Date |
Page |

3. Telnet :- TErminal NETwork.
— Group.

4. EMAIL

5. File Transfer protocol (FTP).

6. www.

7. HTTP, | HTTPS

8. SNMP

Unit-6 This is completed

Jai Shri Satnarayan Ji.

Date | 18/11/2023
Page |

Previous Year Questions

Qno1:-

Aspect	Hop to Hop delivery	Host to Host delivery
Def.	Transmission of data b/w consecutive network node hops.	End to end transmission of data b/w source and destination hosts.
Characteristics (*)	Passing data from one network device to the next until it reaches its destination	focus on delivering data directly from the source host to the destination host.
Examples (*)	routers, switches etc	Eg :- Computers, servers.

(*)

2 Ans:- header length in IPv defines the size of the header in 32 bit words.
— Multiply 4.

3 Ans Yes,
ARP help a Computer find the physical address (MAC address) of another Computer on the same network when it knows the target computer's IP address by asking all devices on the network who has that IP address.

Date
Page

Q4 :- Fragmentation occurs when large packets are split into smaller fragments to fit with in the Maximum transmission Unit (MTU) size of the network.

Ans: ARP Query Broadcast

Because the sender need to find the mac address associated with specific IP address. Broadcasts allows the query to reach all devices on the network, and the devices with the matching IP address respond.

- ARP response are Unicast bcoz one device on the local network recognise its own IP address in the ARP query, it response directly to the sender.

Q6: Properties of routing algorithm

1. Easy to Understand, implent
2. It adapts to failure, topology changes to maintain network connectivity.
3. Adjust to diverse network conditions.
4. Considers security measures to prevent malicious attacks.

Q7: C.S one P.S include low latency, guaranteed bandwidth, suitability for constant bit rate application, and minimal packet loss during transmission.

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

$= 2MHz \cdot \log_2(1+60)$

$C = 2MHz \cdot 5.934$

$C = 11.868$ Mbps

Q9. Yes, a host can use a Telnet client to connect to other client-server like FTTP or HTTP by manually issuing commands to their respective ports. However its not a practical or common method due to lack of user friendly interface and automation.

Q10. — 0 0 0 1 1 0 1 0 1

Manchester

Bit stream: 0 0 0 1 1 0 1 0 1

Manchester: 01, 01, 01, 10, 10, 10, 01, 10, 01, 10

— 0 — high to low. } transition
— 1 — low to high }

Differential Manchester

Bit stream: 0 0 0 1 1 0 1 0 1

diff-man: 10, 10, 10, 01, 01, 01, 10, 01, 10, 01

A transition represent — 0
No transition represent by — 1

Date
Page

Q11: Congestion Control policies

1. Open loop Congestion Control:

- It adjust the sending rate without feedback from the network
Eg TCP slow start

2. Closed-loop Congestion Control:

- It adjust the sending rate based on feedback from the network.
Eg TCP Congestion avoidance

~~3. Explicit Congestion Notification (ECN)~~

Quality of service (QoS) Mechanisms:

1. Integrated services (IntServ)
2. Differentiated services (DiffServ)
3. Queue Management
4. Resource Reservation protocol (RSVP).

Q12: Given B = 1600 Kbps,

(I) SNR → 0

C = 1600 Kbps log2 (1+0) = 0 bps

(II) C = 1600 Kbps log2 (1+20) = 1600 Kbps log2 (21)

= 1600 Kbps × 4.392 = 7027.2 bps

Q13: ~~802~~ IEEE 802.4 (Token Bus) and 802.5 (Token Ring) both use token passing access methods but differ in topology, with 802.4 using a bus and 802.5 using a ring, and frame formats.

Q14 Dynamic web documents

Generated on the Server side in real time based on user request

Eg: Python etc.

Static web documents

Predefined and fixed, created and stored in advance, not change dynamically

Eg: Basic HTML Pages, images etc.

→ Remote login

Computer Network
Last syllabus
is
completed

SN
13/11/2025

Jai Hoo Satnarayan

28/11/2022

Date |
Page |

Q: Why MAC and IP are required in same network.

Ans: Both plays crucial role in network MAC and IP direct comm. in local network.

IP address enable comm. across diff net

Q: Fast ethernet :- Most popular than gigabit ether

100BaseTx

100BaseFx

100BaseT4

Perfor reliabli security

Fast ethernet gigabit

Repeaters, Routers, Gateways

Q SNR = Signal Power / Noise power

$SNR_{dB} = 10 \log_{10}(SNR)$

$SNR = \frac{200 \times 10^{-3}}{10(2 \times 10^{-6})} = 100,000$

$SNR_{dB} = 10 \log_{10}\left(\frac{200 \times 10^{-3}}{100 \times 2 \times 10^{-6}}\right)$

$= 10 \times \log_{10}(10,000)$

$= 50\ dB$

Q MSE-3. We need to send 265 Kbps over a noiseless channel with a bandwidth of 20 KHz. How many signal level do we need.

Q. Q. Bandwidth = 4 KHz

Sig = 20V

Noise = 6 mV

Data rate :-

Shannon Capacity = $B \log_2(1+SNR)$

$= 4 \times 10^3 \log_2(1+SNR)$

$SNR = \frac{\text{Signal}}{\text{Noise}} = \frac{20}{6 \times 10^{-3}} = \frac{20 \times 10^3}{6} = 3300$

$\Rightarrow 4 \times 10^3 \log_2(3301)$

$4000 \log(3301)^3$

Bandwidth = No. of channel × channel bandwidth + (no. of ch − 1) × guard band

$12 \times 40 \times 10^3 + (11) \times 500$

$= 485500$

8 1101

$2^r \geq r+p+1$

r = redundancy bit, p = no of data bit

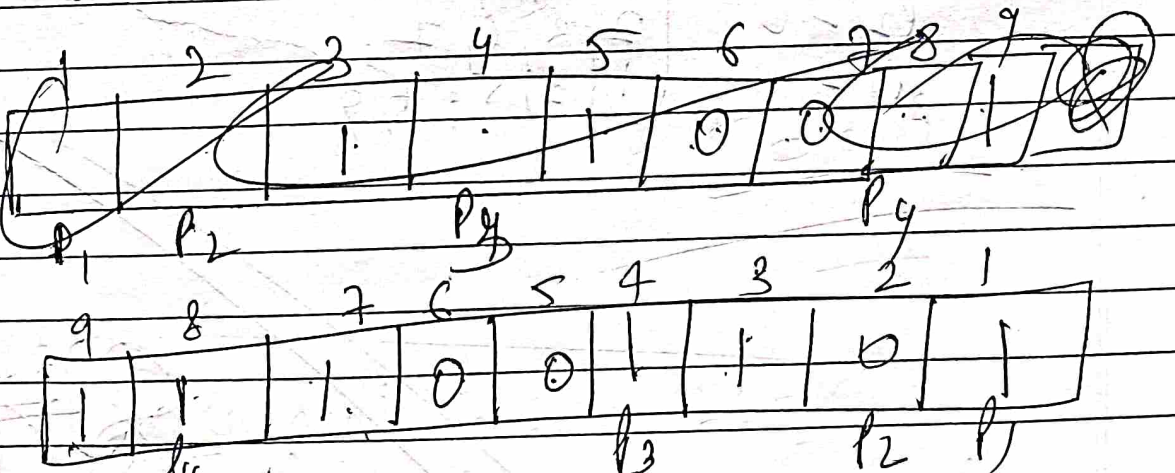
$p = 8$

$2^r \geq 8 + r$

$r = 4$

$16 \geq 13$

Total bits are = 5+4 = 9



$2^r \geq r + p + 1$

r no. of

	C_4	C_3	C_2	C_1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
	1	0	1	0
	1	0	1	1

P_4 – 8, 9

P_3 – 4, 5, 6, 7

P_2 – 2, 3, 6, 7

P_1 – 1, 3, 5, 7, 9

Date | 8/12/2024
Page |

Subject: Computer network lab

LAN:
Hub
Switch
Router

Subnet mask:- a number that distinguished the network address and the host address within an IP address.

Subnet: A network inside a network

Subnetting:- divide a network into two or more networks.

e.g. In IPV4 address — 32 bits
(1 octet = 8 bit)
Each octet (4 octet) → convert decimal

dynamic IP address → A temporary address for devices connected to a network that continuously change over time.