COMPUTER NETWORK

Page No.
Date / /

Unit-1 ONESHOT + 3 PYQ Solutions

Topics

- Basics of Computer Network
- Categories of Networks.
- Internet Service providers
- Network Structure and Architecture.
- OSI Reference Model - 2018-19, 2022-23
- TSP/IP Protocol Suite
- Network Devices and Components - 2022-23

Physical Layer

- Network Topology - 2018-19, 21-22, 22-23
- Types of Connection
- Transmission Media.
- Signal Transmission and Encoding - 2018-19
- Network performance
- Switching Techniques and Multiplexing.

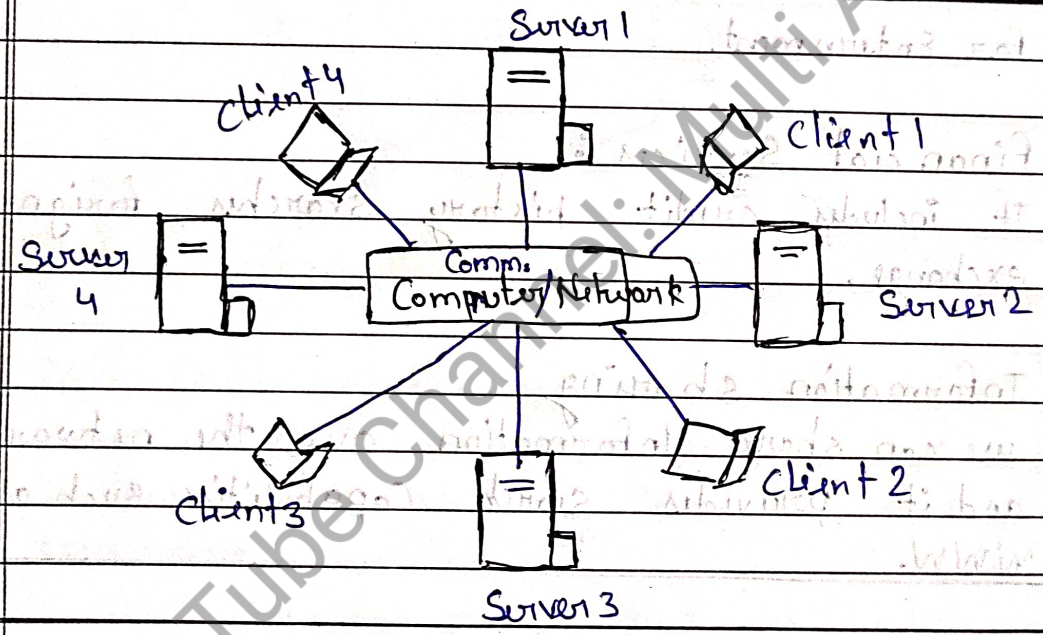
Subscribe + Join Telegram

Page No.:
Date : / /

What is Computer Network?

→ Computer Network is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.

→ The aim of the computer Network is the sharing of resources among various divices.



Goals of Computer Network

→ Cost Reduction → by sharing hardware & softwar Resources.
→ High Reliability → by having multiple supply.
→ High Flexibility
→ powerful Communication Medium.
→ Data Access is fast
→ Reliability and Redundancy → ~~Fund~~ Redundant system in case of failure.

Page No.
Date / /

→ Applications of Computer Network :-

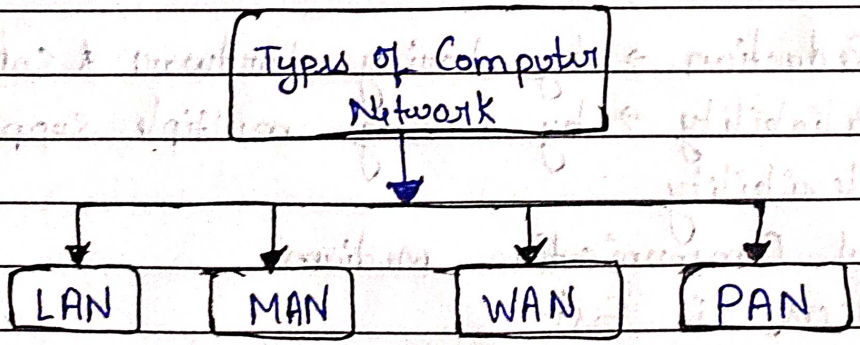
① Business Applications :
→ Resource sharing
→ providing communication medium
→ doing business electronically [E-commerce]

② Home Network Applications :
→ Access to Remote information
→ Person to Person Communication
→ for Enternment.

③ Financial Services :
→ It includes credit history searchs, foreign exchange.

④ Information sharing
→ we can share information over the network and it provides search capabilities such as WWW.

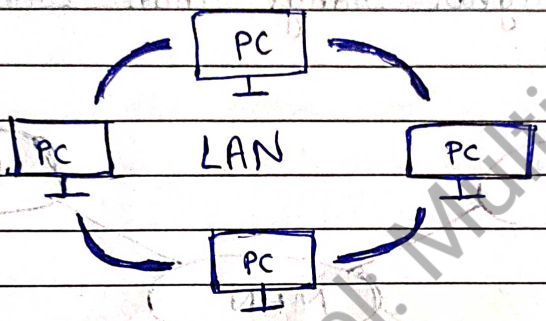
→ Categories of networks.



Page No.:
Date : / /

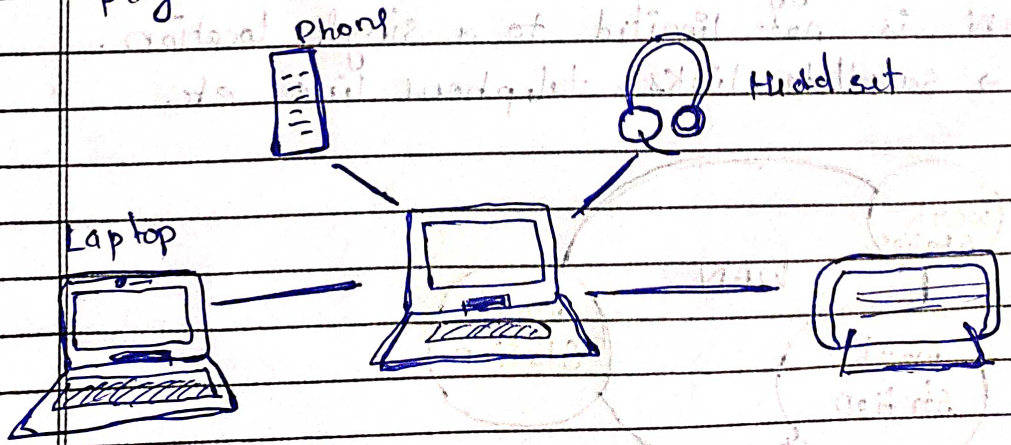
LAN (Local Area Network)

→ LAN is a group of computers connected to each other in a small area such as building, office.
→ Connecting two or more personal computers
→ less costly and data transmission extremely faster.
→ LAN provides higher security.



PAN (Personal Area Network)

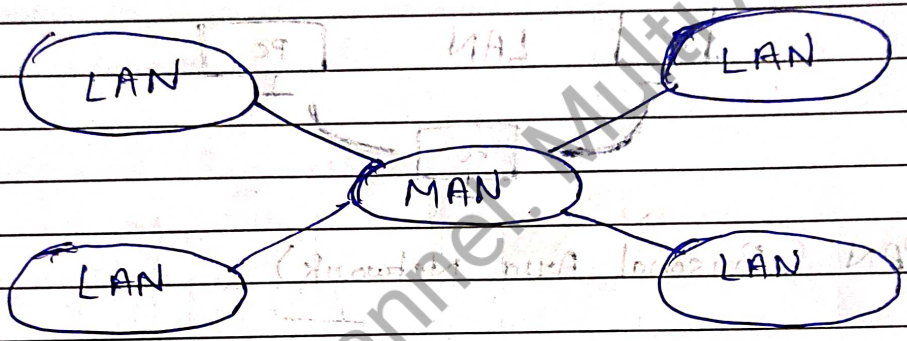
→ PAN is a network arranged within an individual person, typically within a range of 10 meters.
→ Thomas Zimmerman who bring PAN first time.
→ ~~PAN that~~
→ Personal computer devices that are used to develop the PAN are the laptop, mobile, media player and play station.



Page No.
Date / /

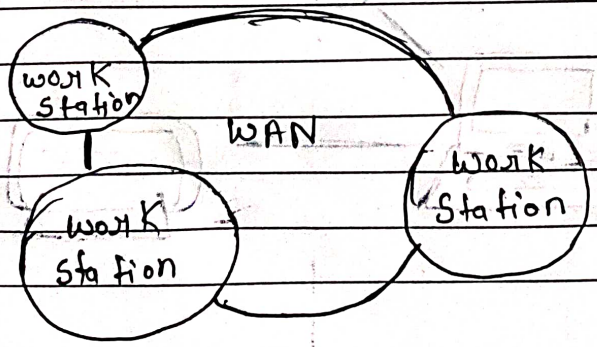
MAN (Metropolitan Area Network)

→ A MAN is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
→ Government agencies use MAN to connect to the citizens and private industries.
→ It has a higher range than Local Area Networks (LAN).



WAN → (Wide Area Network)

→ A wide Area Network is a network that extends over a large geographical area such as states or countries.
→ WAN is bigger than the LAN
→ WAN is not limited to a single location.
→ e.g → satellite links, telephone line etc.



Page No.:
Date: / /

Organization of Internet

→ Internet is hierarchy structure of networks that allows connection over of two internet connected devices, both being at diff. geographical locations.

→ Every computer that is connected to internet has a unique address (IP address → IP → Internet protocol)

→ address is in the form of nnn.nnn.nnn.nnn where nnn can be any number in the range from 0 to 225.

ISP (Internet Service Provider)

→ An ISP make it possible for customers to access the Internet while also provide additional services such as email, web hosting etc.

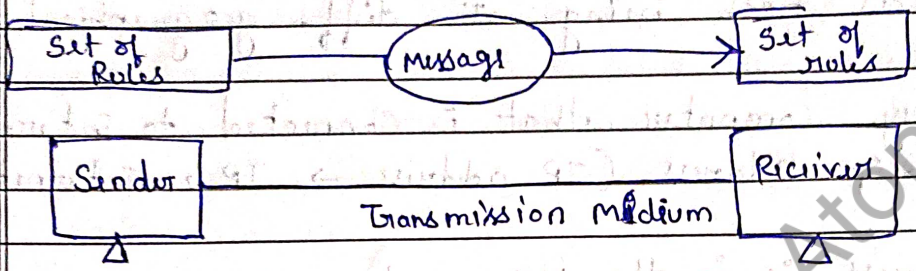
→ internet connection types such as, cables and fibers

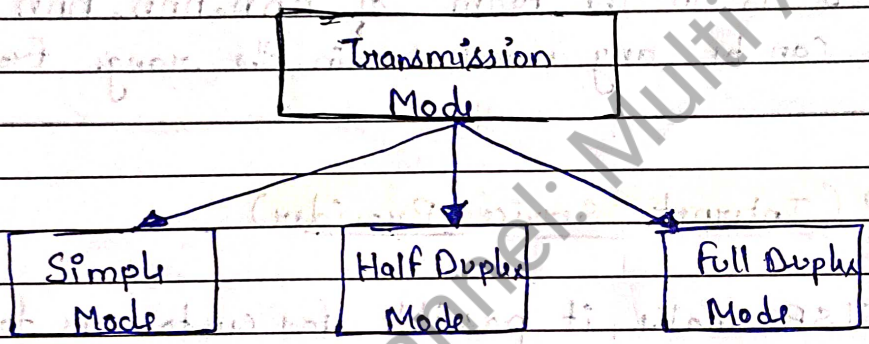
ISPs are grouped into the following three tiers:

1. Tier 1 ISPs :
   - Global reach, extensive infrastructure
   - Negotiate with other Tier 1s, sell to Tier 2s.
2. Tier 2 ISPs :
   - Regional / national operation.
   - Connect Tier 1s and Tier 3s
3. Tier 3 ISPs :
   - focus on local markets, lease from higher tiers.

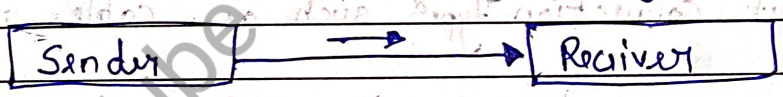
Page No.
Date: / /

Data Communication ⇒ A process of exchanging data or info in case of computer networks. this exchange is done b/w two devices over a transmission medium.



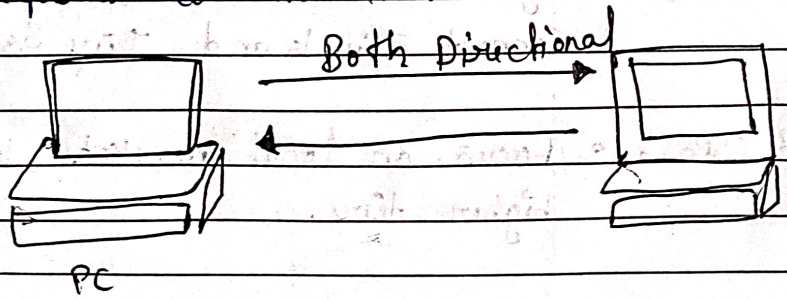


1. Simple Mode : Unidirectional e.g → Loudspeaker.



2. Half Duplex Mode : Bidirectional flow of data but in one direction at a time. e.g → Walkie-talkie.

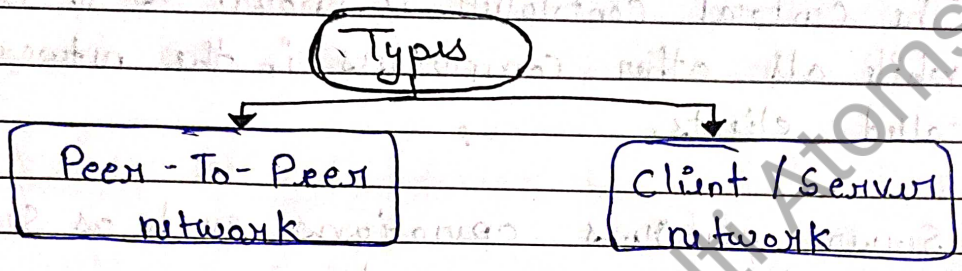
3. Full Duplex Mode : Communication in both directions is required all the time.



Page No.:
Date : / /

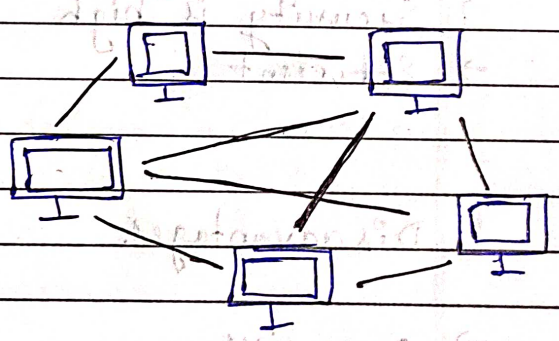
Network Structure and Architecture

→ Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols and media of the transmission of data.
→ how computers are organized.



1. Peer - To - Peer network

→ It is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
→ useful for small environments (10 computers)
→ No dedicated server.



Advantages :

→ less costly.
→ If one system stop other system don't ~~don~~ stop.
→ easy to set-up

Disadvantages

→ not contain the centralized system.
→ Cannot backup and data is in diffrent locations
→ Security issue.

Date / /

Client / Server Network

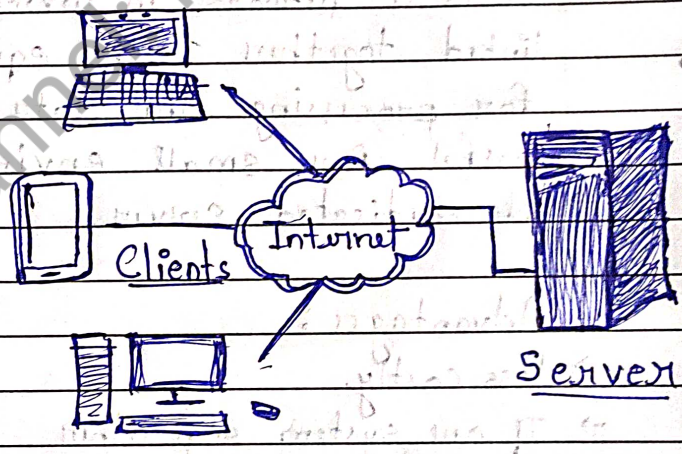
→ It is a network model designed for the end users called clients, to access resources such as songs, video, etc. from Server (central computer).

→ The central controller is known as a Server while all other computers in the network are called clients.

→ Server performs operations such as security and network management.

Advantages :

→ centralized system.
→ backup easily.
→ Security is high
→ Efficient



Disadvantages.

→ expensive
→ required a dedicated network administrator.

Layering

→ Layering means decomposing the problem into more manageable components (layers).

Page No.:
Date : / /

Layering Principles

① The first principle dictates that if we want bidirectional Comm^n, each layer should be able to perform two opposite tasks, one in each direction.

② The second principle is that the two objects under each layer at both sites should be identical.

Services offered by Layers.

① Connection - oriented service :
(telephone System)
→ Establish a connection
→ Use the connection
→ Release the connection

② Connection less Service :

→ There is no guarantee to follow the same path of Sender - Receiver and Receiver to Sender.

Services Primitives (operations)

Connection Oriented → ① LISTEN
② CONNECT
③ RECEIVE
④ SEND
⑤ DISCONNECT

Connection less → UNIDATA
→ FACILITY / REPORT.

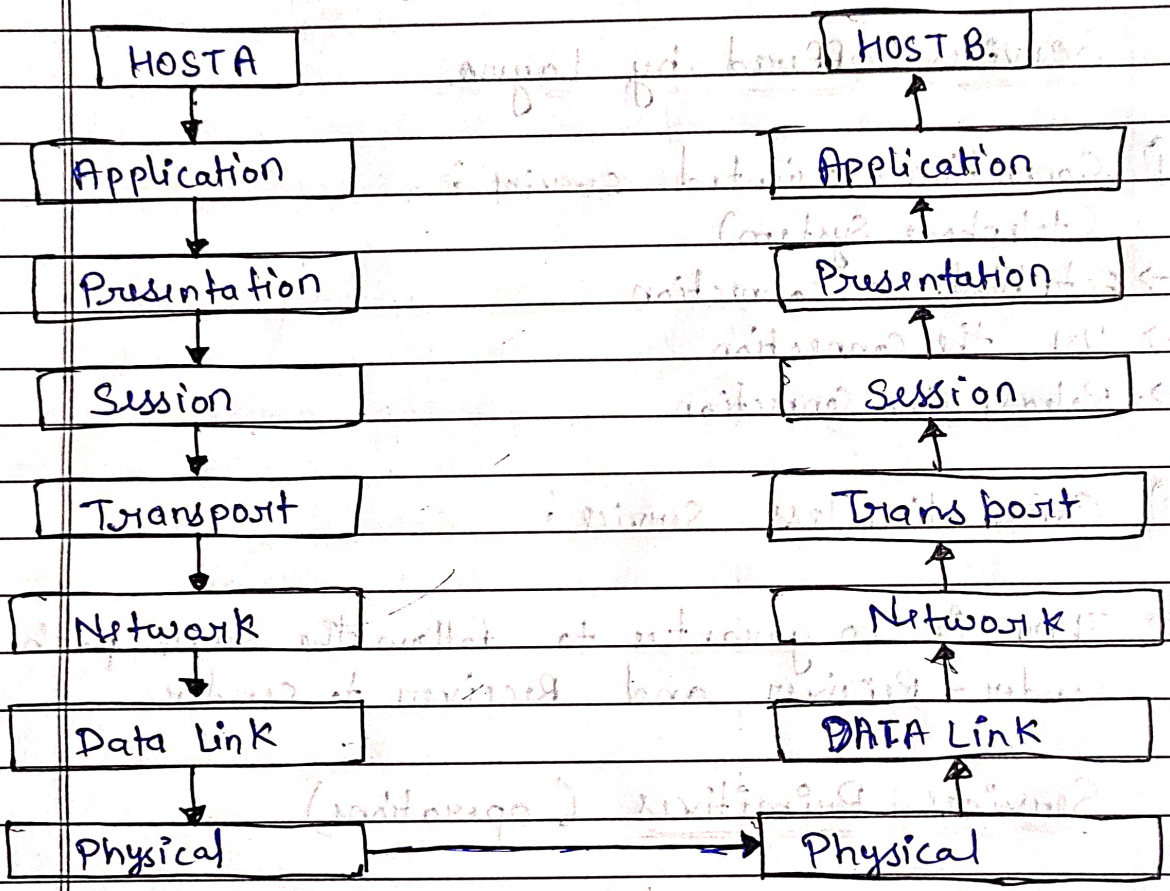
Page No.
Date: / /

AKTU- 2022-23, 2018-19

The OSI Reference Model

→ OSI reference model is a seven layer architecture which defines seven levels in a complete communication system.

→ It is designed to deal with open systems i.e the systems which are open for communication with other systems.



① Application layer :

→ Provides services directly to end-user application

→ E.g → HTTP, FTP, SMTP etc.

Page No.:
Date: / /

2. Presentation layer:
→ prepares data for the application layer.
→ Handles data encoding, encryption and compression.

3. Session Layer:
→ Establishes, manages and terminates connections (sessions) between applications.
→ manages checkpoints for data recovery.

4. Transport Layer:
→ Segments and reassembles data into smaller packets.
→ Ensures error-free, in-sequence delivery of data.

5. Network layer:
→ Handles routing and forwarding of data packets b/w different networks.
→ Determines the best path for data transmission using logical addressing.

6. Data Link Layer:
→ Ensures reliable transmission of data frames b/w directly connected nodes.
→ Provides error detection and correction.

7. Physical Layer:
→ Deals with the physical connection between devices
→ Defines hardware specifications for transmitting data over a medium.

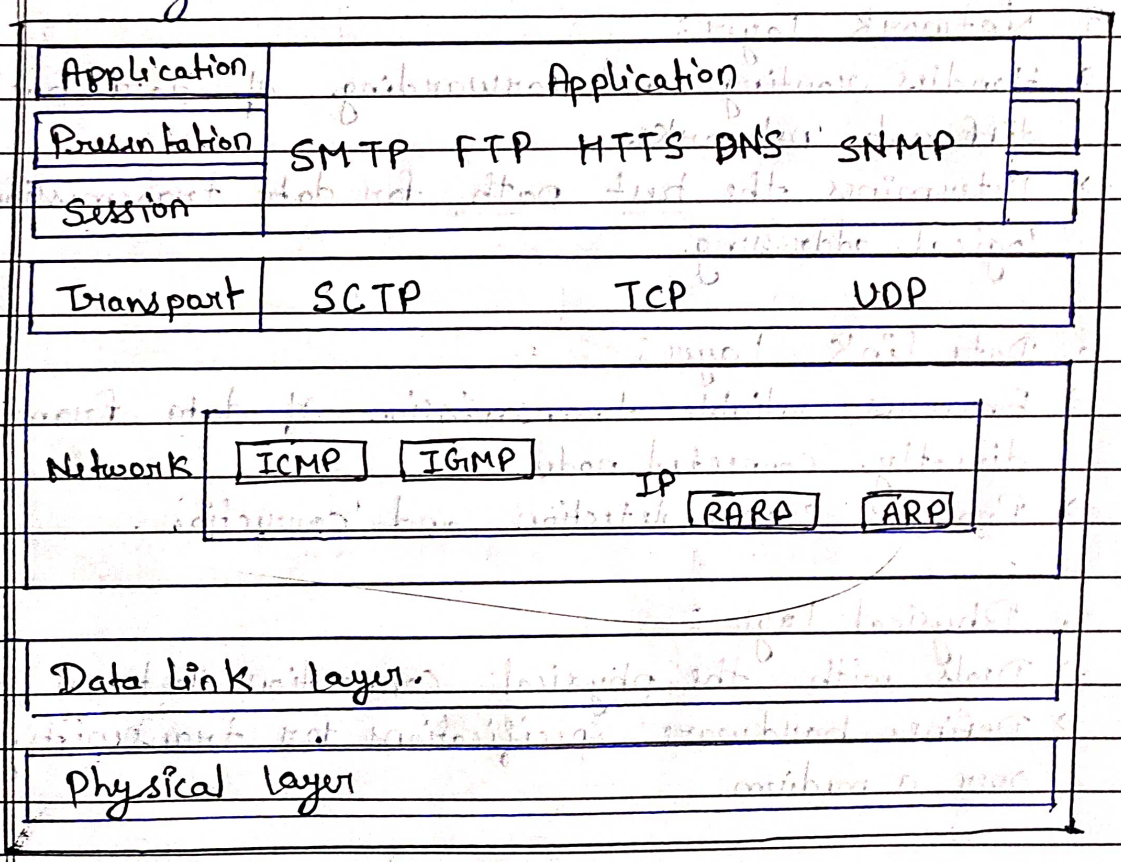
Page No.
Date / /

TCP/IP Protocol Suite

→ The TCP/IP protocol suite consists of five layers : physical, data link, network, transport and application.

→ The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI MODEL.

→ The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer as shown in figure.



Page No.:
Date: / /

1. Physical and Data Link layers:

→ At these layers, TCP/IP does not define any specific protocol.
→ It supports all of the standard and proprietity protoco

2. Internet / Network layer:

→ It defines the protocols which are responsible for the logical transmission of data over the entire network.
- IP = Internet Protocol responsible for delivering packets.
- ICMP = Internet Control Message Protocol encapsulate datag
- ARP = Address Resolution Protocol → find the hardware address of a host from a known IP Address.

3. Transport Layer:

→ These protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error

a. UDP (User Datagram Protocol) → adds only port addresses, checksum error control, and length information to the data from the upper layer
b. TCP (Transmission Control Protocol) → provides full transport layer services to application.

c. Stream Control Transmission Protocol (SCTP): It provides support for newer applications such as voice over the internet.

4. Application Layer :
→ Many protocols like Simple mail Transfer Protocol, File Transfer Protocol, HTTP, DNS, SNMP, etc are defined at application layer.

AKTU - 2022-23

Network Devices and Components.

1. HUB :
→ It is the simplest of these devices.
→ Hubs cannot filter data.
→ do not have intelligence to find out best path.
→ used on small networks.

2. Bridge :
→ It is more complex than hub. ↑ physical address.
→ It maintains MAC address table for both LAN segments.
→ It has a single incoming and outgoing port.
→ looks at the destination

3. Switch :
→ It has multiple ports.
→ can perform error checking before forwarding data.
→ very efficient
→ large networks use switches.

④ Router :

→ like a switch forwards packets based on address.
→ Supports diffirent WAN technologies but switches do not.
→ Wireless Routers have Access Point built in.
→ shared board band internet Connection.

⑤ WAP

→ wireless Access point bridges wireless and wired traffic.
→ allows computers to Connect to LAN in a wireless design
→ wired and wireless devices work to communicate with each other.

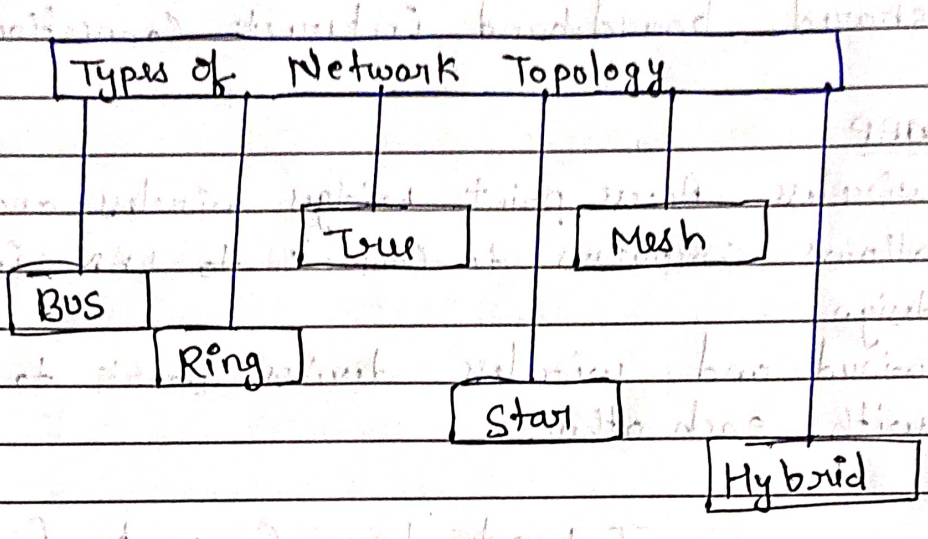
Introductory Concepts finish.

physical layer :

→ Network Topology, Types of Connection — 2018-19, 2021-22, 2022-23
→ Transmission Media.
→ Signal Transmission and Encoding — 2018-19
→ Network Performance and Transmission Impairment
→ Switching Techniques and Multiplexing.

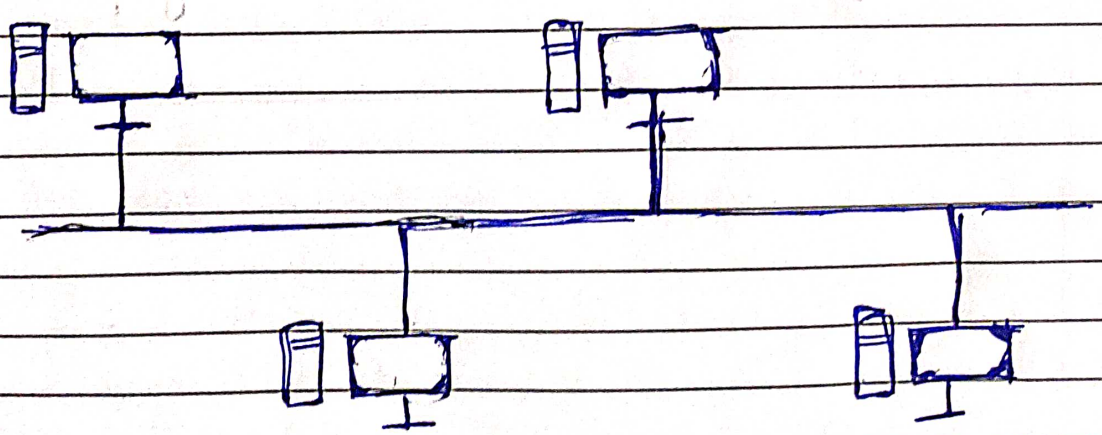
Page No.
Date: / /

Network Topology :- The physical arrangement of the computer system, which is connected to each other via communication medium is called topology.



① Bus Topology

It is a type of network topology in which all devices are connected to a single cable called a "bus". This cable serves as a shared communication medium, allowing all devices on the network to receive the same signal simultaneously.



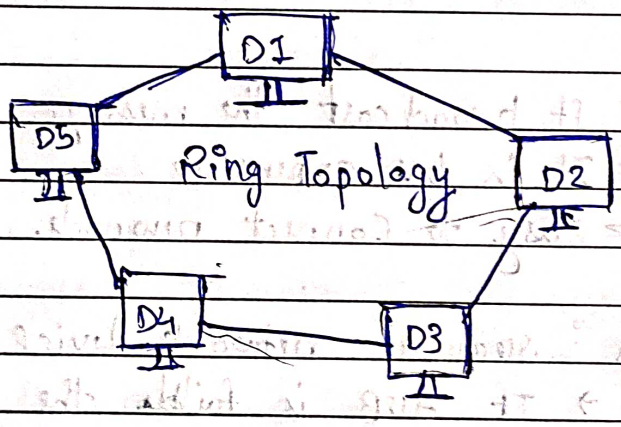
Page No.:
Date : / /

Advantages → 1. Easy to add / remote nodes in network
2. It is less Expensive.

Disadvantages → If the cable is fail then the entire network will be failed.
→ message can not send private.

2. Ring Topology

→ In this devici connections create a closed circular data path. devices in a ring topology are called a ring network.



Advantages. 1. form a strong lans network.
2. Each and every node can share data with another node.

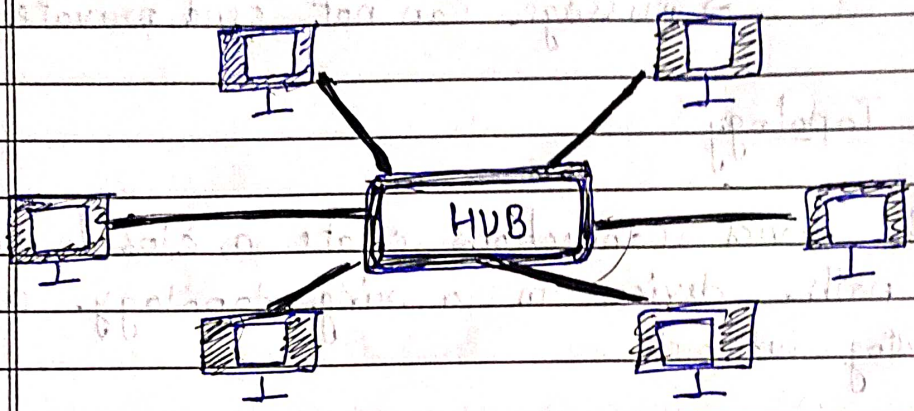
Disadvantage. 1. It is difficult task to add some new node.

→ If we want to send data from a sender to destination machine then data will un necessary passed to all nodes.

Page No.
Date: / /

③ Star Topology

Each network component is physically connected to a central node such as router, hub or Switch.

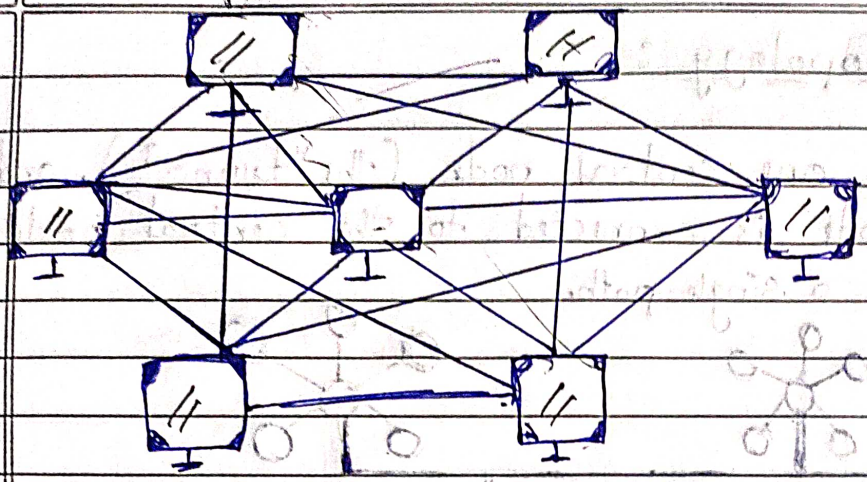


Advantage = It broadcast the message
= It is less expensive
= Easy to connect new node.

Disadvantage : require network device
→ If HUB is failed the entire network will be failed.

④ Mesh Topology

→ every computer is directly connected with eachother, so we can directly send the data to the destination machine without going to intermediate machine.

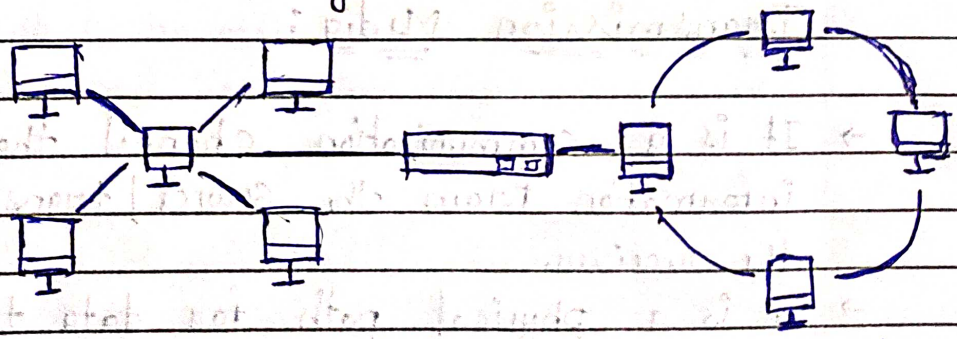


Advantages ⇒ In this ~~prdu~~ private message is send.
⇒ It provide point to point connection.

Disadvantage ⇒ It is very difficult to add some new node.

⑤ Hybrid Topology

→ It is a type of network topology that combines two or more network topologies, including ring, bus and mesh topologies.



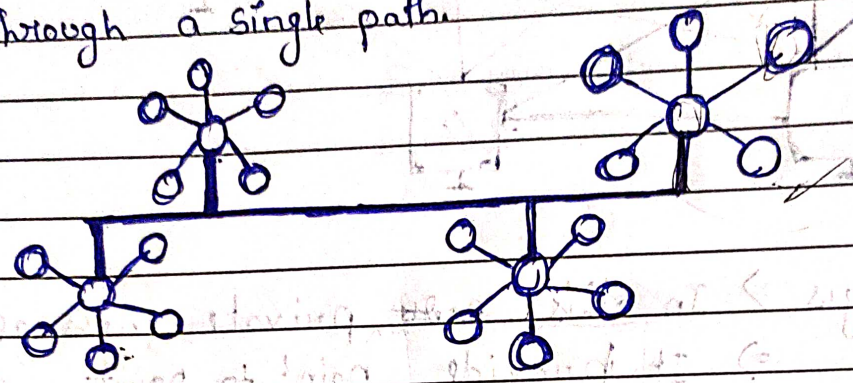
Advantage : Can be modified as per requirement
It is extremely flexible.

Disadvantage : → It is a type of network. Expensive.
→ design is very complex.

Date: / /

⑥ Tree Topology :-

→ In this one central node (the "trunk"), and each node is connected to the central node through a single path.

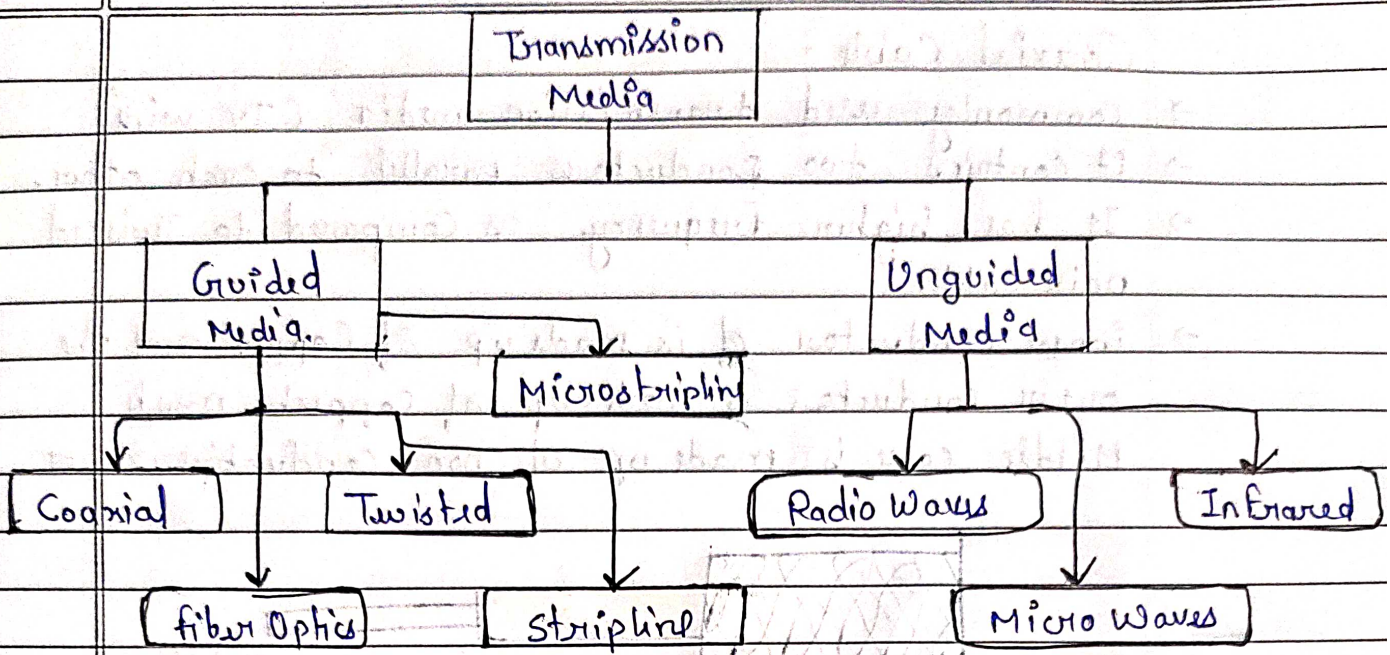


Advantage → It can support a large number of nodes
→ It can be easily expanded.

Disadvantage → it hard to identify where the issue is located.
→ If one node goes down, it can affect the entire network.

Transmission Media :

→ It is a communication channel that transmits information from the source / transmitter to the receiver.
→ It is a physical path for data transfer through electromagnetic signals.



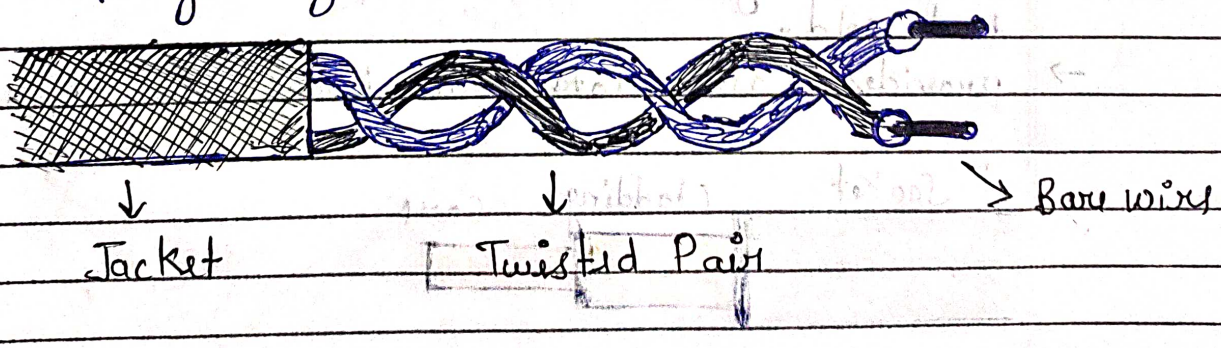
1. Guided Media : It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

- High Speed
- Secure

Twisted Pair : It is a physical media made up of a pair of cables twisted with each other.

→ It is cheap and lightweight cable.

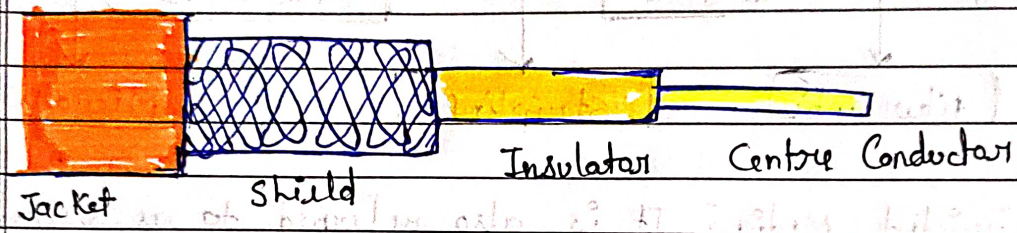
→ Frequency rang 0 to 3.5KHz.



Page No.
Date / /

Coaxial Cable:

→ Commonly used transmission media (TV wire)
→ it contains two conductors parallel to each other.
→ It has higher frequency as compared to Twisted pair cable.
→ inner conductor of is made up of Copper and the outer conductor is made-up of Copper mesh Middle core is made up of non-conductive cover.



Advantages ⇒ Speed is high and higher bandwidth.
Disadvantages ⇒ more expensive then twisted pair.

Fibre Optic Cable:

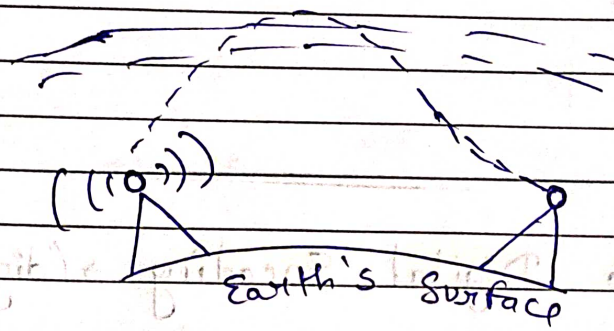
→ It is a cable that uses electrical signals for Comm".
→ It holds the optical fibres coated in plastic that are used to send the data by pulses of light.
→ plastic coating protects the optical fibres from heat, cold.
→ provides faster data transmission than Copper Wires.

Page No.:
Date : / /

2. Unguided Transmission : It transmits the electromagnetic waves without using any physical medium. Therefore it is also known as wireless transmission.

Radio waves :

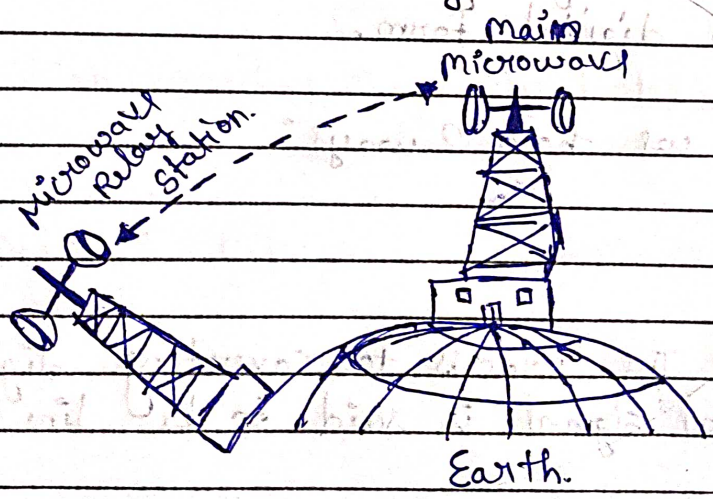
→ Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
→ The range in frequencies of 3Khz to 1Ghz.
→ e.g → FM radio.



→ Used for WAN
→ Higher transmission Rate.

Microwaves : Sending and receiving information using a microwave is known as microwave transmission.

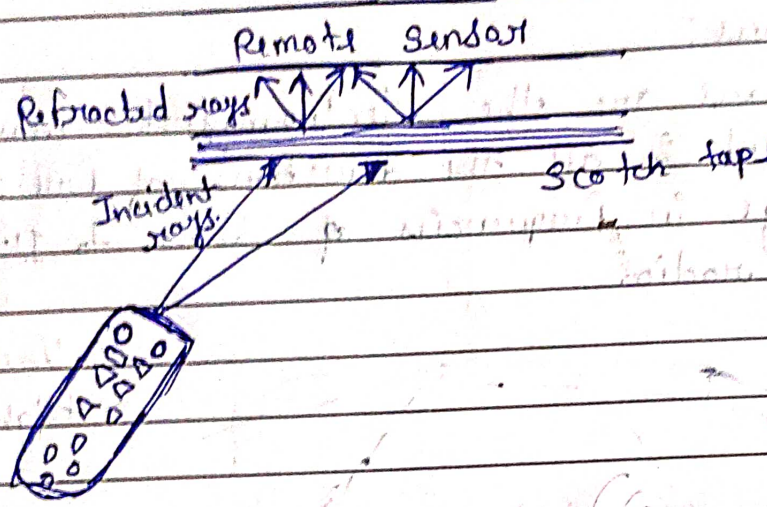
→ widely used for point-to-point communications.
→ cheaper than using cables



Page No.
Date: / /

8 Infrared:

→ used for communication over short ranges, such as two cell phones, TV remote, etc.



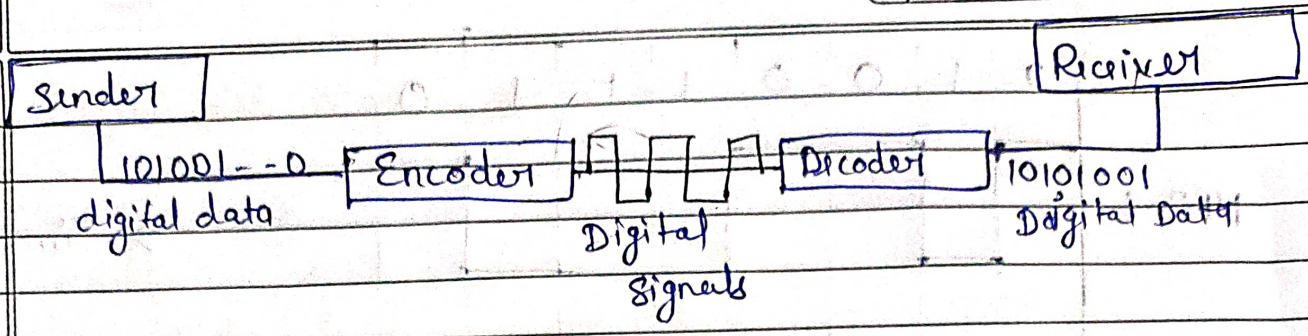
Digital to Digital Encoding → (digital data into digital signal)

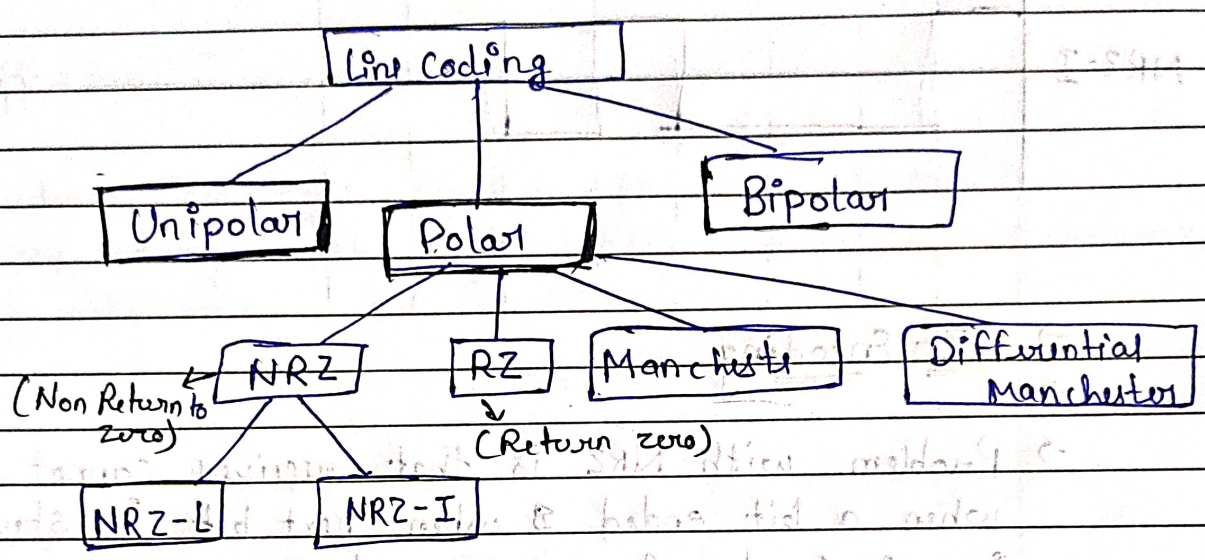
→ Data & information can be stored in 2 ways Analog and Digital.

→ To transmit data digitally, it needs to be first converted to digital form.

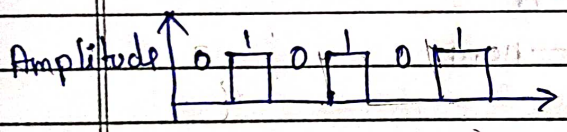
→ for conversion we have 2 ways:
* Line Coding
* Block Coding.

Line Coding ⇒ The process for converting digital data into digital signal is said to be line coding.





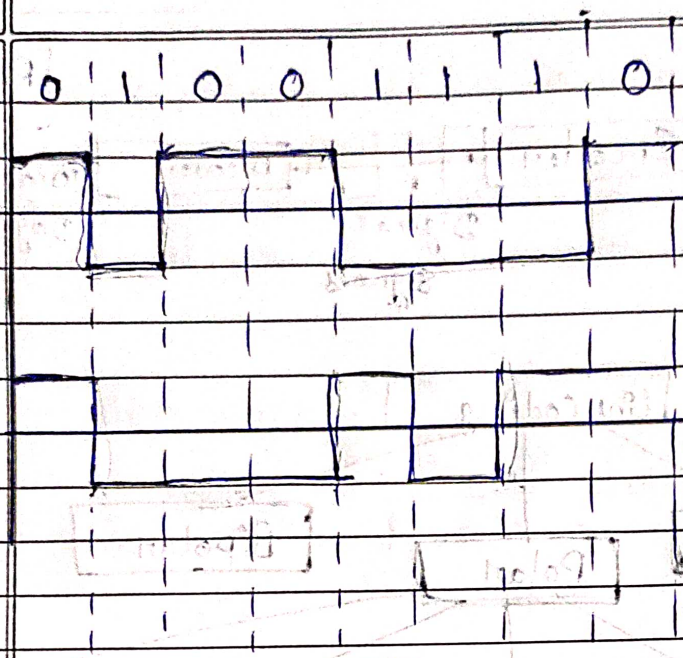
① Unipolar Encoding → Use Single voltage level to represent data
1 → high voltage and 0 → no voltage.



② Polar Encoding → uses multiple voltage levels to represent binary values.

→ NRZ → It uses 2 different voltage levels.

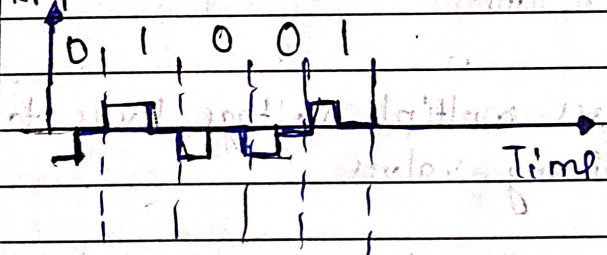
It has 2 variants:
→ NRZ-L (Levels Signals)
→ NRZ-I (Signals gets inverted)



→ RZ- Encoding

→ Problem with NRZ is that receiver cannot conclude when a bit ended & when next bit is started, in case Sender & receiver clock are not Synchro-nized.

+voltage — 1
-voltage — 0
Zero voltage — none.



→ Manchester :-

This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided in two halves.

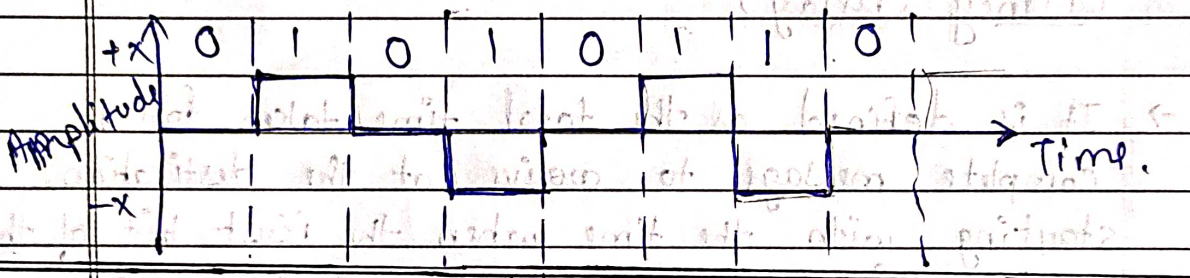
→ It transits in the middle of the bit & changes phase when a different bit is Encountered.

→ Differential Manchester :-

This Encoding Scheme is a combination of RZ and NRZ-I. It also transits at the middle of the bit but change phase only 1 is encountered.

③ Bipolar Encoding :-

It uses 3 voltage levels, +ve, -ve & zero.
Zero voltage represents binary 0 & bit 1 is represented by alternating +ve & -ve voltages.



Network Performance

→ To estimate the performance of the network, we should consider following 4 terminologies :-

- Bandwidth.
- Throughout.
- Latency (Delay).
- Bandwidth * Delay Product.

Bandwidth ⇒ In networking, we use the term bandwidth in two contexts :

- The first, bandwidth in hertz, (no. of vibration per second) refers to the range of frequencies in a composite signal.

Page No.
Date: / /

- The second, bandwidth in bits per second, refers to the speed of bit transmission in a channel or link.

Throughout:

→ It is the number of messages successfully transmitted per unit time.
→ bits per second, Kilobytes per second, megabytes per second and gigabytes per second.

Latency (Delay)

→ It is defined as the total time taken for a complete message to arrive at the destination, starting with the time when the first bit of the message is sent out from the source and ending with the time when the last bit of the message is delivered at the destination
→ measured in milliseconds (ms).

Latency = Propagation Time + Transmission Time + Queuing Time + Processing Delay.

① P.T = $\frac{\text{Distance}}{\text{Propagation Speed}}$, ② T.T = $\frac{\text{Message Size}}{\text{Bandwidth}}$

Page No.:
Date: / /

Bandwidth - delay product

It is a measurement of how many bits can fill up a network link. It gives the maximum amount of data that can be transmitted by the Sender at a given time before waiting for acknowledgment.

Transmission Impairment

When a signal transmit from one medium to other, the signal that is received may differ from the signal that is transmitted due to various impairments.

1) Attenuation :- "It refers to lose of Energy by a Signal time"
   → for compensat we can use amplifire

2) Distortion :- "means signal changes its form or shape".

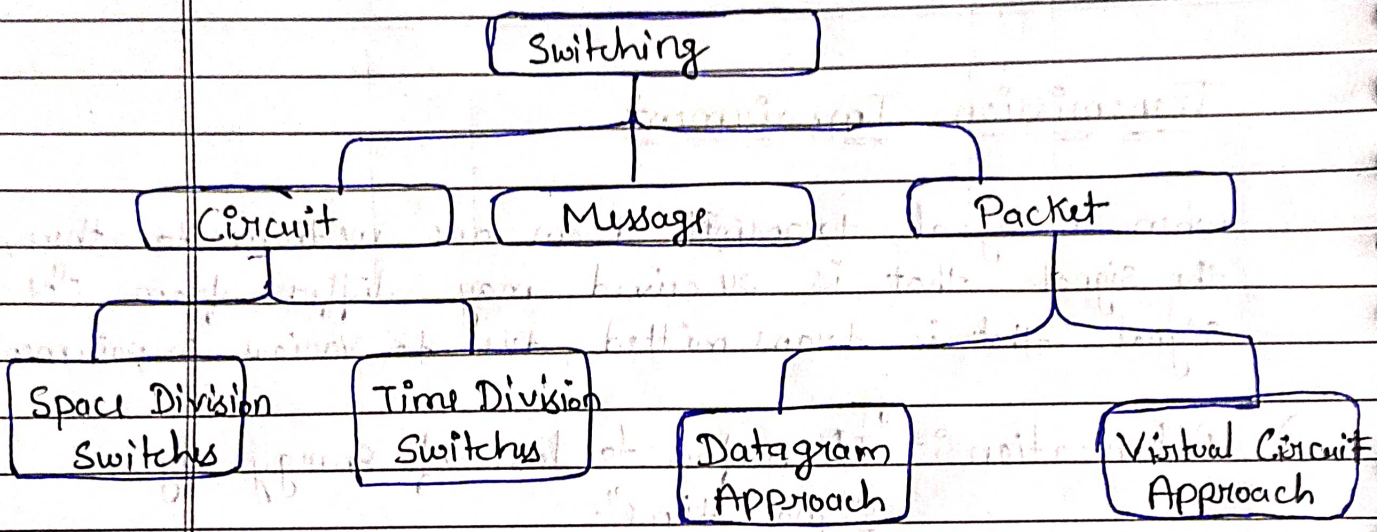
3) Noise :- The random or unwanted signal that mixes up with the original signal is called noise.

   → There are Several types of noise such as induced, thermal, cross talk and implust noise which may corrupt the signal.

Page No.
Date / /

Switching Techniques

→ It is the process of transferring data packets from one device to another in a network, or from one network to another, using specific devices called switches

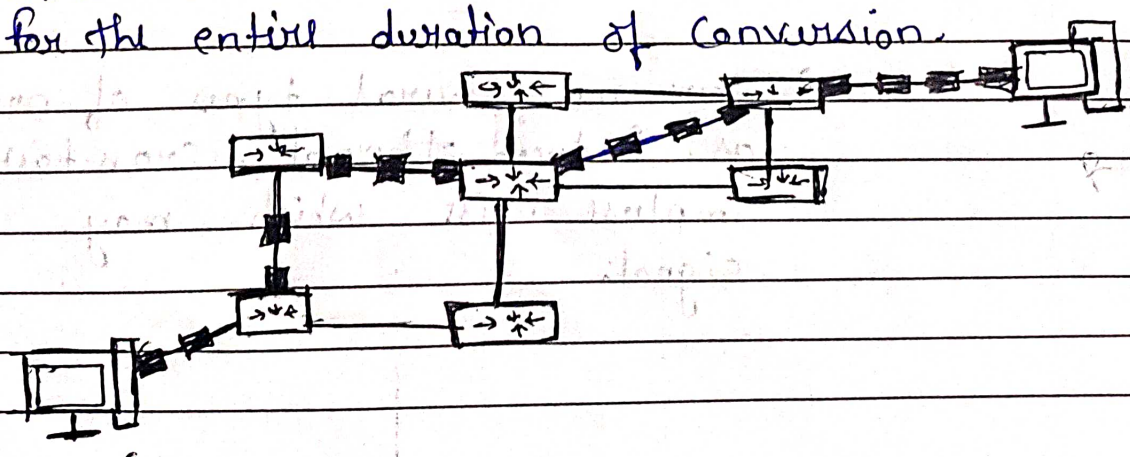


① Circuit Switching

→ When two nodes communicate with eachother over a dedicated communication path, it is called circuit switching.

→ A dedicated path is established between the Sender and the receiver which is maintained for the entire duration of conversion.

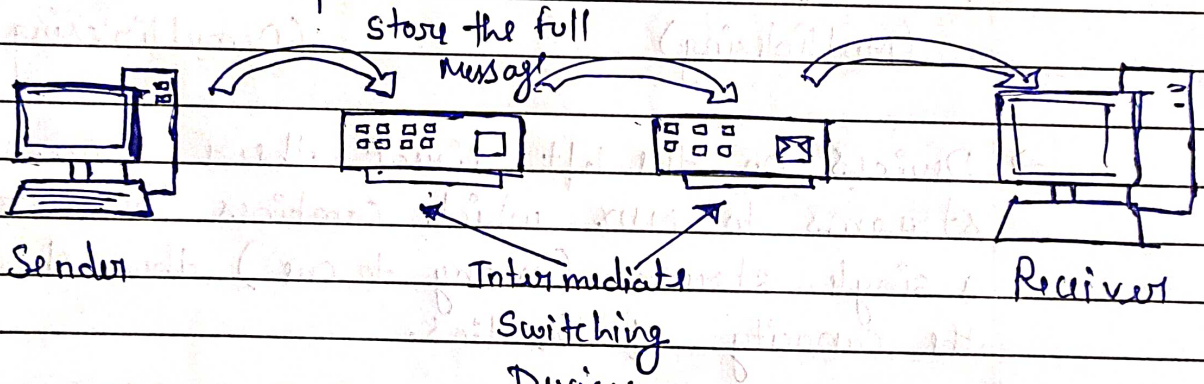
→



→ Circuit switching was designed for voice applicatio
→ e.g → Telephone.

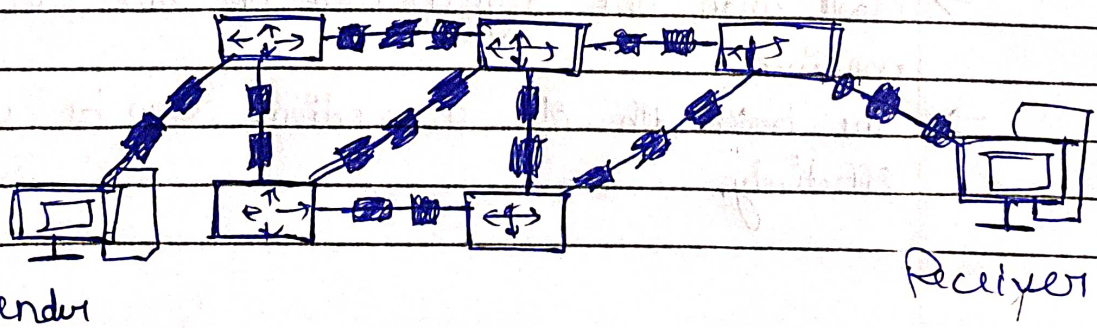
2. Message Switching :

→ This technique was somewhere in middle of circuit switching and packet switching..
→ the whole message is treated as a data unit and transferred in its entirety.
→ first receives the whole message and buffers it until there are resources available to transfer it to the next hop.



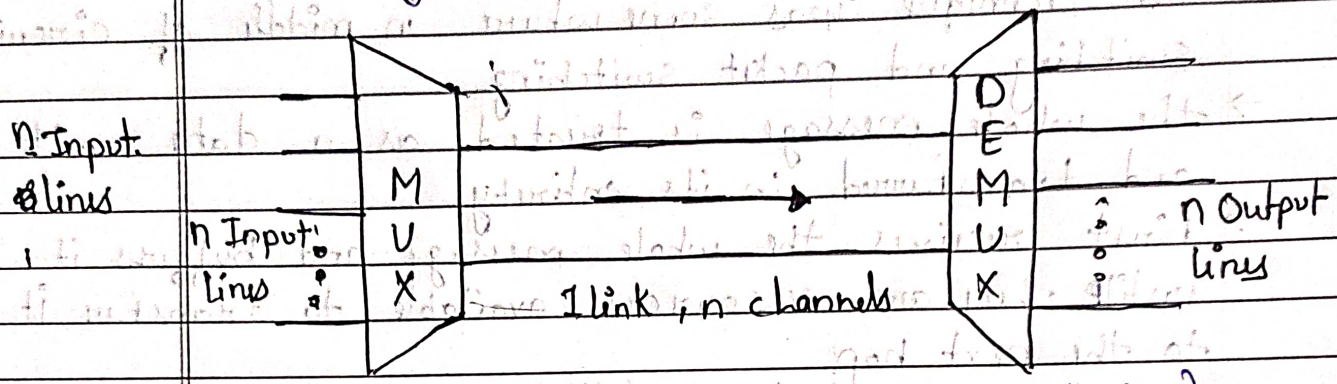
3. Packet Switching

→ The entire message is broken into small chunks called packets. The switching info. is added in the header of each packet and transmitted independently.
→ packets are stored and forwarded according to their priority to provide quality of service.



Multiplexing

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



(Multiplexing) (Demultiplexing)

→ Devices on the left direct their transmission streams to MUX which combines them into a single stream (many to one) thus sharing the capacity of the link.

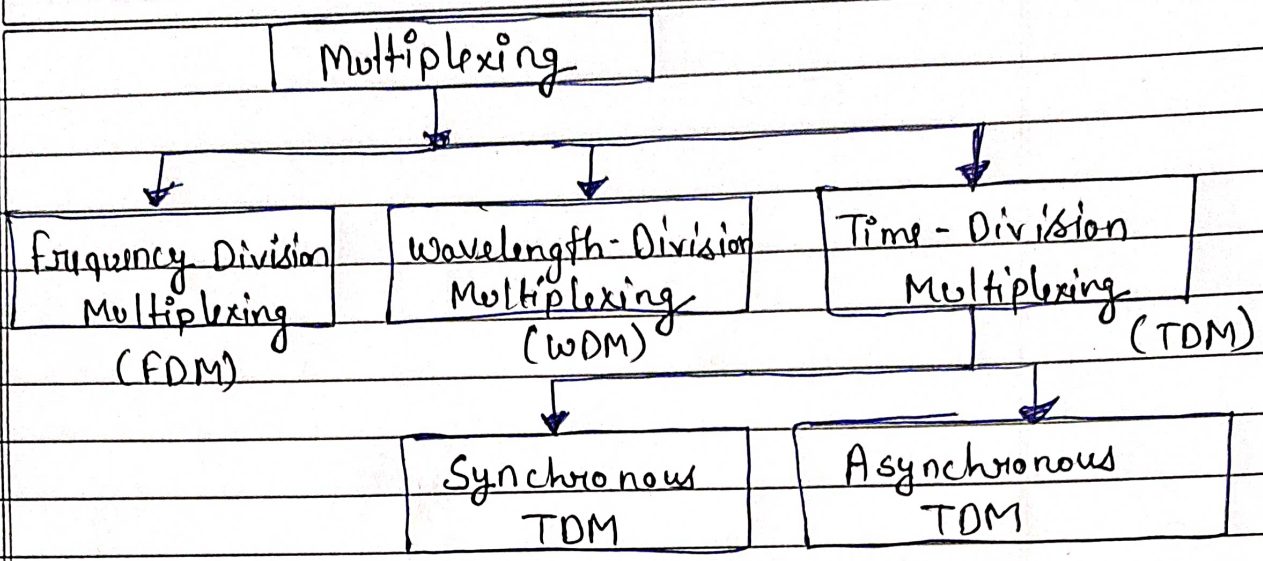
→ Receiving end, demultiplexer separates the single stream back into its component transmissions (one to many) & directs them to their intended Receiving Devices.

Advantages

→ More than one signal can be sent over a single medium.

→ The bandwidth of a medium can be utilized effectively.

Page No.:
Date : / /



Completed Unit-1

Subscribe MULTI ATOMS

Join Telegram for Notes

COMPUTER NETWORK

Page No.
Date: / /

Unit-2

ONE SHOT + 3 PYQ SOLUTIONS

Topics :-

→ Data Link layer → Services
→ Framing and its type
→ Error Detection & Correction.
→ Error Detection method — 2022-23
→ FLOW CONTROL
→ STOP N WAIT → 10 marks (2021-22, 18-19)
→ Slinging window protocol.
→ Channel Allocation.
→ Multiple Access protocols. → (2021-22, 22-23)
→ LAN Standards.
→ Bridging & Spanning Tree Algo.

Page No.:
Date: / /

Data Link Layer

→ It is second layer of OSI Layered Model.
→ Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware.

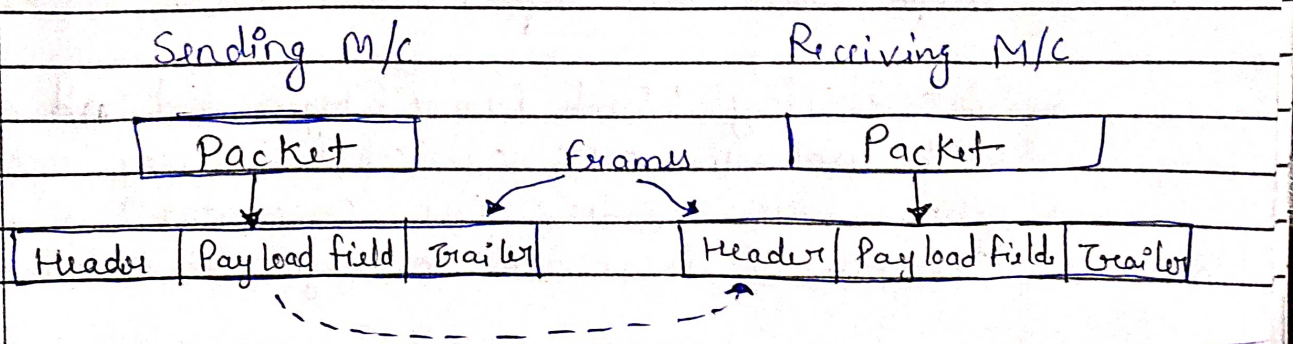
Services of Data Link Layer

→ framing & Link access
→ Reliable Delivery
→ Flow Control
→ Error Detection
→ Error Correction
→ Half - Duplex & Full - Duplex

Framing

→ Data link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames.

→ Smaller sized frames makes flow control and error control more efficient. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.



Page No.
Date: / /

Parts of a Frame:

- Frame Header : It contains the source and the destination addresses of the frame.
- Payload field : It contains the message to be delivered.
- Trailer : It contains the error detection & error correction bits.
- Flag - It marks the beginning and end of the frame.

Flag	Header	Payload field	Trailer	Flag

- **Types of framing**

1. Fixed size
2. Variable size → Length fixed ✓
   → End Delimeter ✓
   - Character Oriented Framing (Byte) (8 bit)
   - Bit Oriented Framing. (1 bit).

A. Byte stuffing ⇒ Sender's DLL Insert Special escape (ESC) Just before 'Accidential data. (Byte).

B. Bit Stuffing ⇒ Each frame begin and end with pattern (01111110) that is flag byte.
→ when even Sender's DLL encounter's five Consecutive is in the message it automatically

Page No.:
Date: / /

Stuff '0' bit into outgoing bit stream.

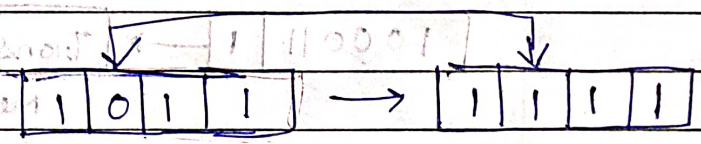
Error Detection and Correction [2022-23] - 10 marks

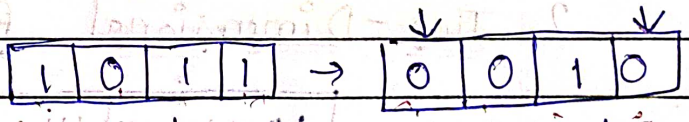
Errors are introducted into binary data transmitted from the sender to the receiver due to noise during transmission.

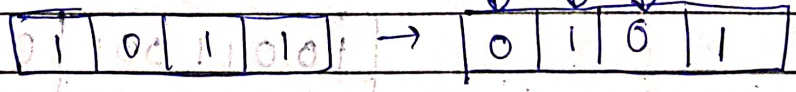
Error Detection : methods are used to check whether the receiver has received correct data or corrupted data.

Error Correction : It is used to correct the detected errors during the transmission of data from sender to receiver.

Types of Errors.

1. Single bit Error ⇒ 

2. Multiple bit Error ⇒ 

3. Burst Error ⇒ 

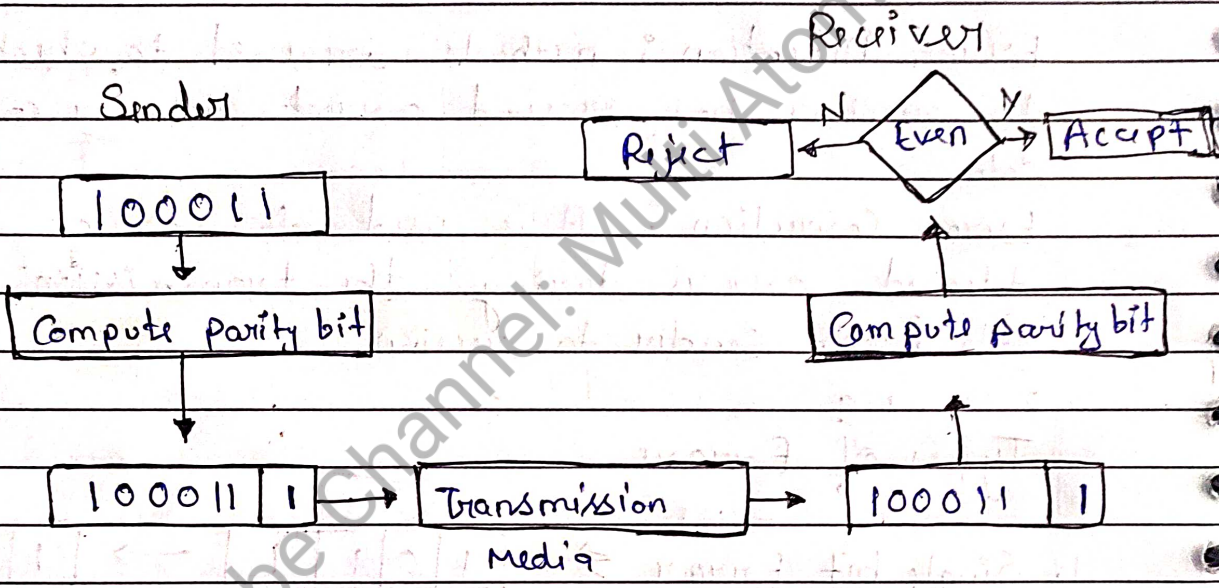
Error Detection Method	Error Correction
simple	Type ↓
→ ~~Single~~ Parity Check	→ Backward EC
→ 2-Dimensional parity check	→ Forward EC
→ Checksum	Techniques ↓
→ Cyclic Redundancy check	1. Hamming Code ✓
	2. Determing Parity bit

Page No.
Date / /

* Even parity → 1011 → 10111
  → 1010 → 10100

* Odd Parity → 1011 → 10110
  → 1010 → 10101

1. Simple Parity Check.



2. Two-Dimensional Parity Check

Data = | 10011001 | 11100010 | 00100100 | 10000100 |

10011001	0 ← row
11100010	0
00100100	0
10000100	0
11011011	0

↓ column

→ | 100110010 | 111000100 | 001001000 | 100001000 | 110110110 |

Page No.:
Date: / /

3. Checksum

10011001	11100010	00100100	10000100
1	2	3	4

Sender

1→ 10011001

2→ 11100010

10111101 1

→ 1

01111100

3→ 00100100

10100000

4→ 10000100

10010001 00

→ 1

Sum: 00100101

checksum: 11011010

Receiver

Same as Sender

Sum: 00100101

checksum: 11011010

11111111

Complement = 00000000

Conclusion: Accept Data.

4. Cyclic Redundancy Check (CRC):

→ eqn → $x^3 + x^2 + 1 = 1101$ $\quad x^4\ x^3\ x^2\ x^1\ x^0$

$x^4 + x^2 + x^0 = 10101$

→ Frame = 101 0000

→ Generator = $x^3 + 1$ → 1001 4 bit.

→ if CRC generator is of n bit, then append (n−1) Zeross in the end of original message.

Page No.
Date: / /

X → XOR

Sender

```
1001 | 101 0000 000
     X 1001
     -------
      0011 0000000
        X 1001
        ---------
        01010000
          X 1001
          ------
          0011000
            X 1001
            ------
            01010
              X 1001
              ------
              0011   <- Remainder
```

→ Message to be transmitted. => 1010000 000
+ 011
1010000011

Reciver

```
1001 | 1010000011
     X 1001
     -----------
     0011000011
       X 1001
       ---------
       01010011
         X 1001
         ------
         0011011
           X 1001
           ------
           01001
             X 1001
             ------
             0000   <- Zero means data is accepted.
```

✓

AKTU - 2022-23 [10 marks]

Page No.:
Date: / /

Q. A bit stream 10011101 is transmitted using x^3+1 generator polynomial. Generate the CRC code word for this message.

→

```
1001 | 10011101000
     x 1001
       00011010000
         x1001
           0100000
           x1001
            000100  ← Remainder.
            x1001
```

→ CRC code = 10011101100

Page No.
Date: / /

Hamming Code

→ It is a set of error-correction codes that can be used to detect and correct bit errors that can occur when computer data is moved or stored.

→ It use parity bit.

→ Using more than one parity bit, an error-correction code ~~is the use of extra~~ not only identify a single bit error in the data unit, but also its location in the data unit.

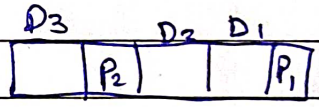
① → It can be applied to data units of any length.

② → no. of parity bit is decided by

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

r = No. of parity.

m = message bits.



e.g ⇒ m = 4 [1010]

$2^3 \geq 4 + 3 + 1$

$8 \geq 8$ ✓

③ → This parity bits are positional parity bit :

m = 4 bit

r = 3 bit

4 + 3 = 7 bit.

P1	P2	P3
2^0	2^1	2^2

7	6	5	4	3	2	1
D_4	D_3	D_2	P_3	D_1	P_2	P_1
			2^2		2^1	2^0

Page No.:
Date: / /

E.g A bit word 1011 is to be transmitted construct the even parity seven bit Hamming code for this data.

→ Even parity = No. of 1s will Even. ✓

Sol m = 4 bit
r = 3 bit

→ $2^r \geq m+r+1$ ✓

step 1 ⇒ r = 0 $[2^0 \geq 4+0+1]$ ×
$[2^1 \geq 4+1+1]$ ×
$[2^2 \geq 4+2+1]$ ×
$[2^3 \geq 4+3+1]$ ✓

r = 3

P_1 P_2 P_3
2^0 2^1 2^2

→

7	6	5	4	3	2	1
D_4	D_3	D_2	P_3	D_1	P_2	P_1

→

7	6	5	4	3	2	1
1	0	1	P_3	1	P_2	P_1

111 110 101 100 011 010 001 ✓

⇒

1	0	1	0	1	0	1

P=3 Data
P_1 – (3, 5, 7) → (1, 1, 1) = 1
P_2 – (3, 6, 7) → (1, 0, 1) = 0
P_3 – (5, 6, 7) → (1, 0, 1) = 0

Page No.
Date: / /

AKTU - 2022 - 23 [2 marks]

Q. If a 7-bit hamming code received as 1110101, show that the code word has error. Also, rectify error in this code.

7	6	5	4	3	2	1
1	1	1	0	1	0	1

111 110 101 P_3 011 P_2 P_1

100 010 001

P_1 = 1, 3, 5, 7 = (1, 1, 1, 1) = 0

P_2 = 2, 3, 6, 7 = (0, 1, 1, 1) = 1

P_3 = 4, 5, 6, 7 = (0, 1, 1, 1) = 1

1 1 0 = 6

7	6	5	4	3	2	1
1	0	1	0	1	0	1

↑

Flow Control

- Feedback based
  - Sender gets ack. from the user
- Rate Based
  - check the rate of flow without ack.

Protocols

- for Noiseless Channels
  - Simplex protocol
  - Stop & wait protocol
- for Noisy channels
  - Stop & wait ARQ
  - Go-Back-N ARQ
  - Selective Repeat ARQ

Page No.:
Date: / /

① ~~Elem~~ AKTU - 2022-23 [10 marks]

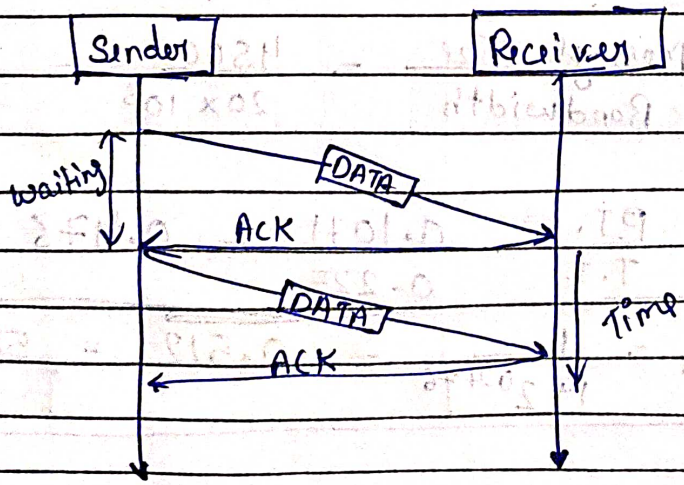
Q. Explain error control ~~control~~ mechanism in Data Link layer and giving example of each method

Ans ① Elementary Data Link Protocol → Simplex & stop and wait

② Sliding Window Protocols → Go-Back-N ARQ
→ Selective Repeat ARQ

① Simplex Protocol
→ As the name suggests, is the most basic Data Link protocol.
→ data can only be sent in a single direction.
→ the Sender/receiver can generate an infinite amount of data.
→ e.g → Keyboard transmitting keystrokes to a Computer

② Stop and wait Protocol
→ It is a fundamental data link protocol where the sender transmits a frame and waits for an ack. from the receiver before sending the next frame.
→



Page No.
Date / /

AKTU - 2018-19 [10 marks]

Q. A channel has a bit rate of 20 Kbps. The stop and wait protocol with frame size 4500 bit is used. The delay for error detection and sending ACK by the receiver in 0.25 seconds because of a fault. Find the maximum efficiency of the channel if distination is 30000 km away and the speed of the propagation of the signal is 2.8×10^8 m/s. Find the decrease in efficiency due to the fault.

Sol Bandwidth = 20×10^3 bps — delay because of fault = 0.25 sec.
Size = 4500 bit
distance = $30,000 \times 10^3$ m
propagation speed = 2.8×10^8 m/s

decrease in efficiency = ? & Max efficiency = ?

→ $\eta_{max} = \frac{1}{1+2a}$ $\quad a = \frac{\text{Propagation Time}}{\text{Transmission Time}}$

→ $P.T = \frac{\text{Distance}}{\text{Propagation Speed}} = \frac{30,000 \times 10^3}{2.8 \times 10^8 \text{ m/s}} = 0.1071$

$T.T = \frac{\text{Message Size}}{\text{Bandwidth}} = \frac{4500}{20 \times 10^3} = 0.225$

$a = \frac{P.T.}{T.T.} = \frac{0.1071}{0.225} = 0.476$

$\eta_{max} = \frac{1}{1+2*0.476} = 0.512 = 51.2\%$

$$\eta_{fault} = \frac{1}{1 + 2a + \frac{0.25}{T.T.}} = \frac{1}{1 + 2 \times 0.476 \times \frac{0.25}{0.225}}$$

$$\eta_{fault} = 0.326 = 32.6\%$$

→ decrease in η (%) $= \frac{\eta_{max} - \eta_{fault}}{\eta_{max}} \times 100$

$= \frac{0.512 - 0.326}{0.512} \times 100$

$= 36.3\%$

AKTU- 2021-22 [10 marks]

Q. Define the relationship b/w Transmission delay & Propagation delay, if the efficiency is at least 50% in STOP n wait protocol.

→ $\eta = \frac{1}{1 + 2a}$, $a = \frac{P.T.}{T.T.}$, $\eta = 0.50 = \frac{1}{2}$

$= \frac{1}{2} = \frac{1}{1 + 2 \times \frac{P.T}{T.T}}$

$= 1 + 2\frac{P.T}{T.T} = 2$

$= 2 \times \frac{P.T}{T.T} = 1$

2 Propagation Time = Transmission Time.

Page No.
Date: / /

→ Sliding window Protocol

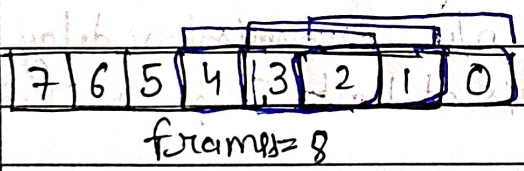
* It is a technique for controlling transmitted multiple data packets b/w two network computers.

* Each data packet includes a unique consecutive Sequence number which is used by Receiver
* to place data in the correct order.
→ avoid duplicate data & to request missing data.

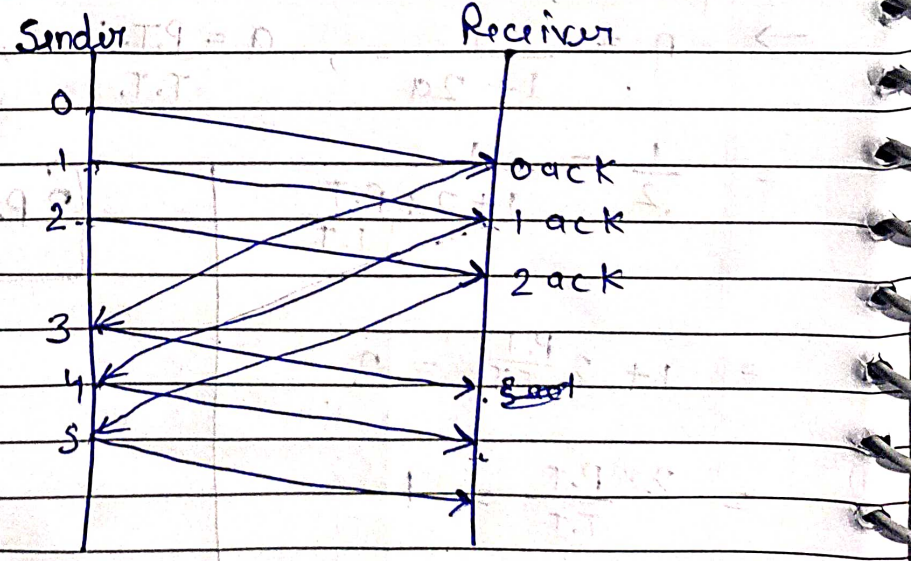
→ It uses the concept of piggy backing - Instead of sending ack frame on its own, if there is an outgoing data frame in the next short interval, attach the ack to it (using "ack" field in header).

AKTU - 2022-23 [2 mark] - (piggy backing.)

e.g



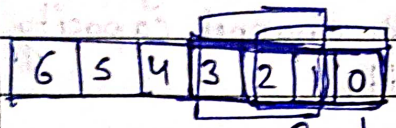
window size = 3



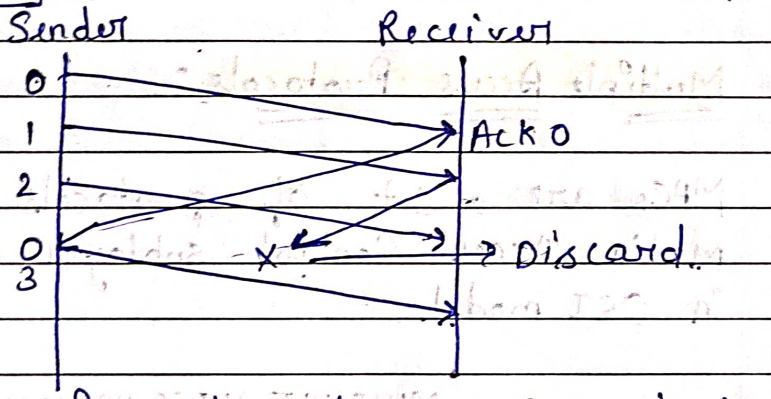
Page No.:
Date : / /

① GO - BACK - N ARQ (Automatic Repeat Request)

→ If one frame is corrupted then all frames have to be sent again. (as respect window size)
→ Number of frames sent depends on window size.
→ The size of the sender window is N and the receiver window size is always 1.

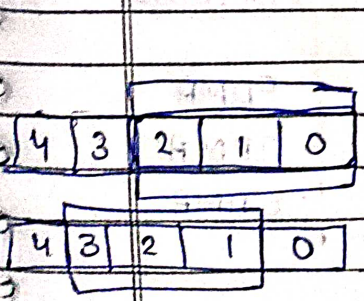


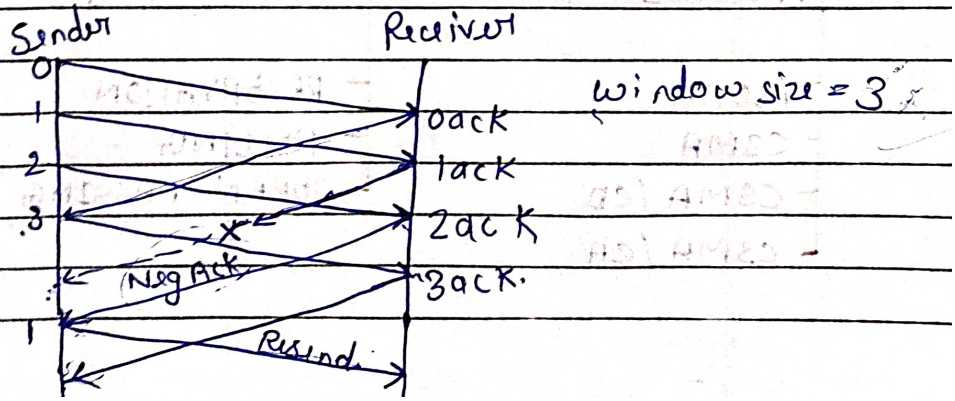
window size = 3



→ Now, Sender have to sent 1, 2, 3 again to Receiver.

② SELECTIVE REPEAT ARQ [Automatic Repeat Request].
→ In this only the frame is sent again, which is lost.
→ Size of Sender window = Size of Receiver window.
→ Size of the sliding window is always greater than 1.
→ when receiver receives corrupt frame. It sends a Neg ACK.





Page No.
Date: / /

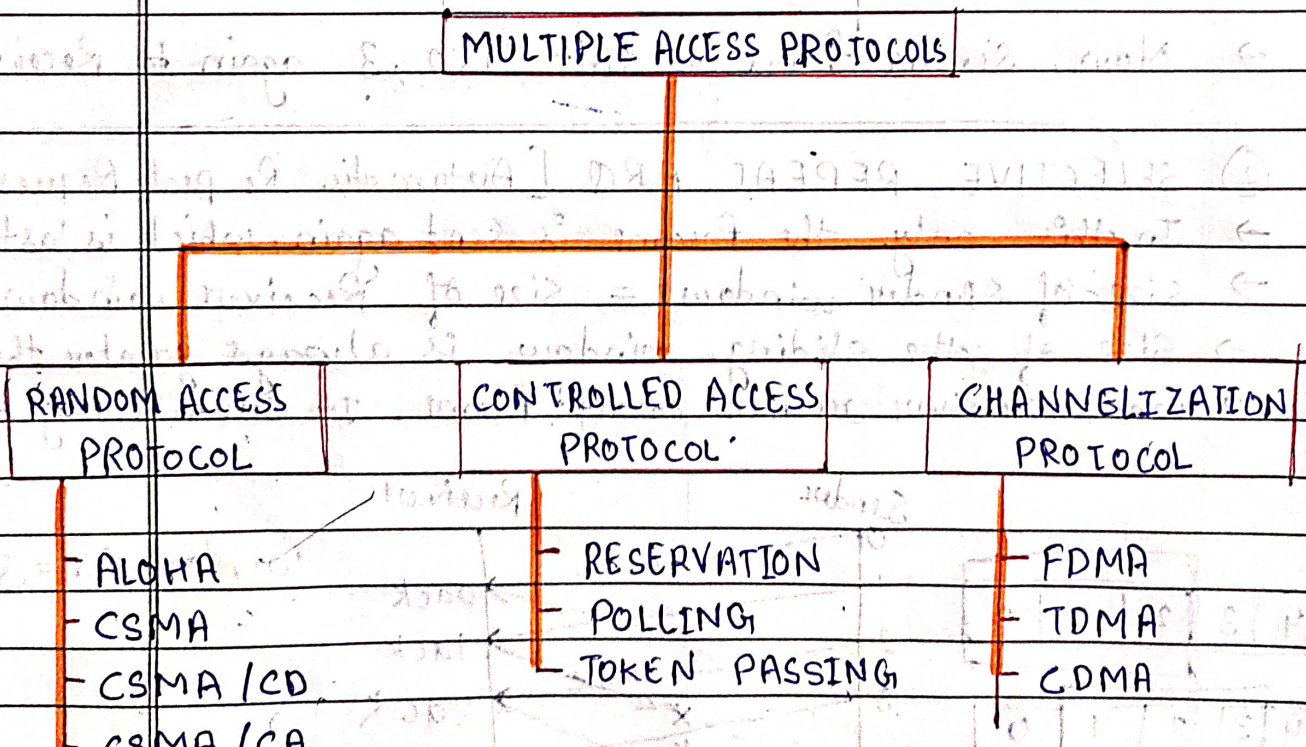
Channel Allocation

→ It is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks.

polling → A central controller interrogates each host and allocates channel capacity to those who need it.

Multiple Access Protocols :

MACs are a set of protocols operating in the Media Access Control sublayer of Data Link Layer in OSI model.



Page No.:
Date : / /

1. **Random Access Protocols** → Assign uniform priority to all connected nodes.

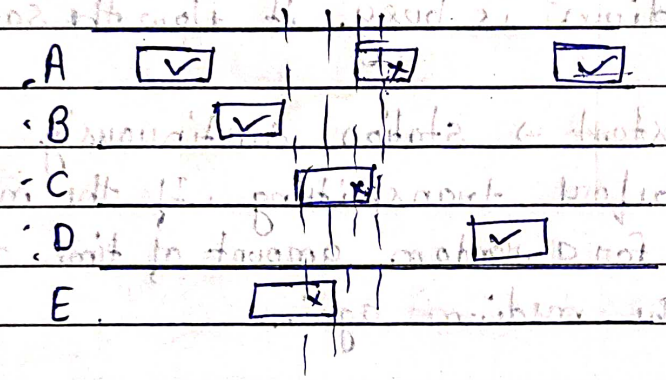
→ ALOHA

- Pure ALOHA
- Slotted ALOHA.

1. PURE ALOHA ⇒ Devices transmit data whenever they have it, without checking if the channel is busy. Collisions are detected through ack. messages or by the sender if no ack. is received after a certain time.

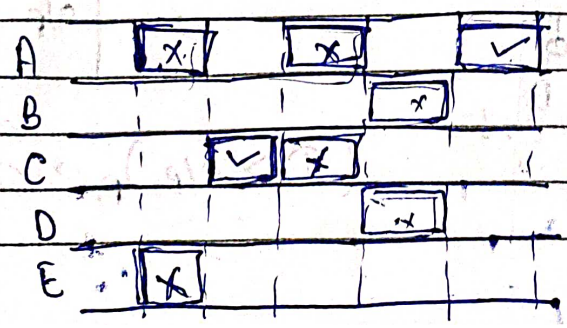
→ The total vulnerable time of pure ALOHA is $2 * T_{fr}$

→ effective maximum channel utilization is 18.4%



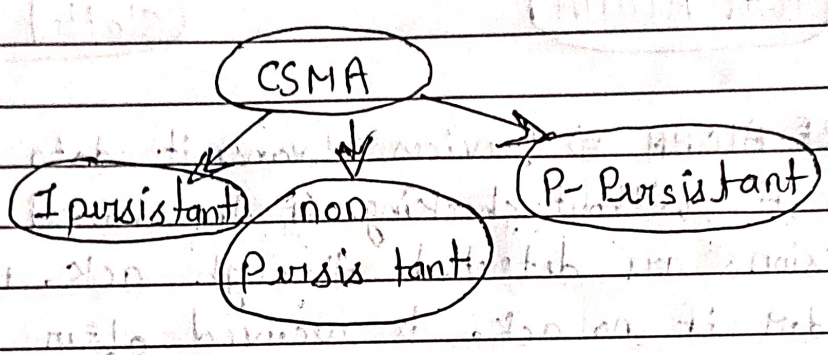
2. Slotted ALOHA ⇒ This variant divides time into discrete slots, and devices are only allowed to transmits at the biggining of each slot. reduces the probability of collisions compared to pure ALOHA. However, collisions can still occur.

→ vulnerable time period is T_{fr} & effective max. utilizat. → 36.8%



Page No.:
Date: / /

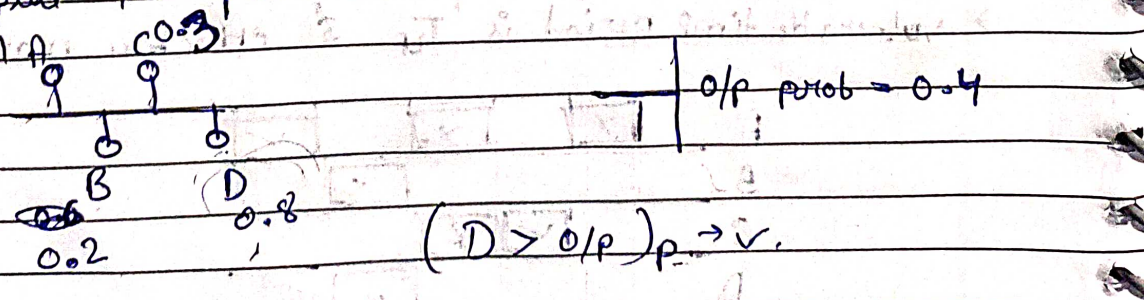
→ CSMA (Carrier Sense Multiple Access).
→ devices listen to the communication channel before transmitting. If the channel is Idle, the device can proceed with transmission. and if the channel is busy the device will wait.



1. 1-persistant → Continuously Senses the medium. If the medium is Idle, it immediately begins transmission if the medium is busy, it flow the same process.

2. Non-persistant → station continuously Sinsus the medium buford transmitting. If the medium is busy it waits for a random amount of time and then checks the medium again

3. p- persistant → when a station wants to transmit data, it sinsus the medium. If the medium is Idle, It check (if device probability > output prob.) it transfer otherwise wait for a slot. and repeat the process.



Page No.:
Date : / /

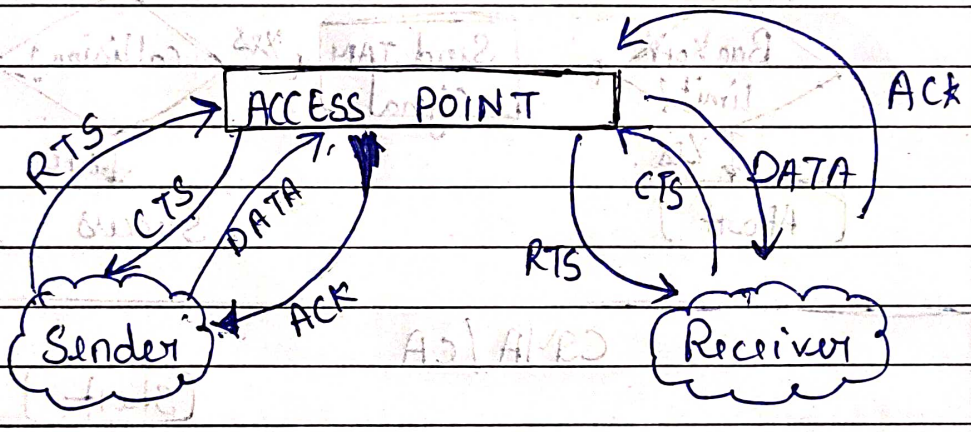
AKTU- 2021-22 + Flowchart:

→ CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

* Commonly used in Ethernet networks, not only listens to the channel before transmitting but also detects collision while transmitting. If a collision is detected, the node stop transmission and send JAM signal to all other nodes and waits for a random backoff time.

→ CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

* Used in wireless networks like WiFi.

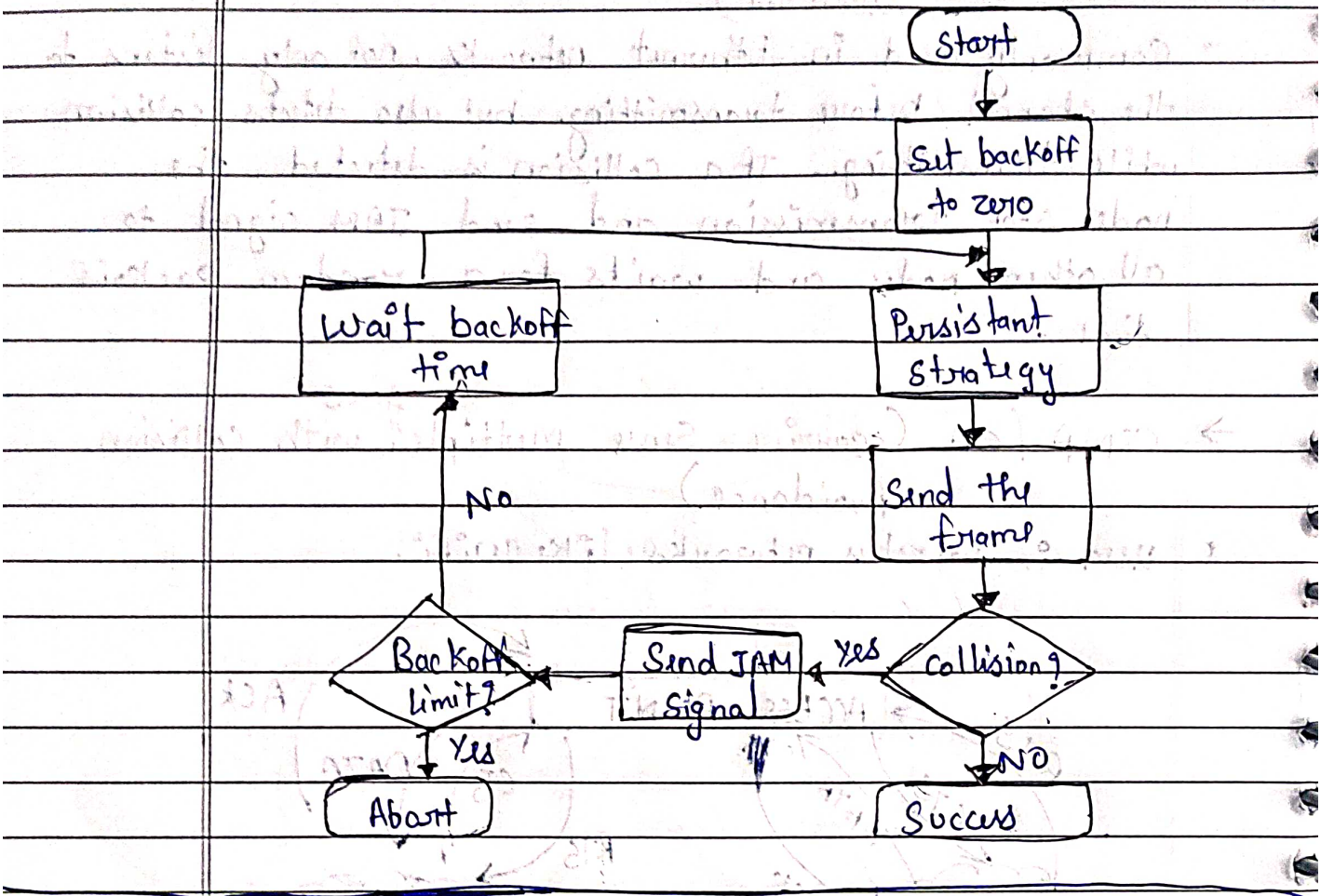


RTS → Request to send
CTS → clear to send.

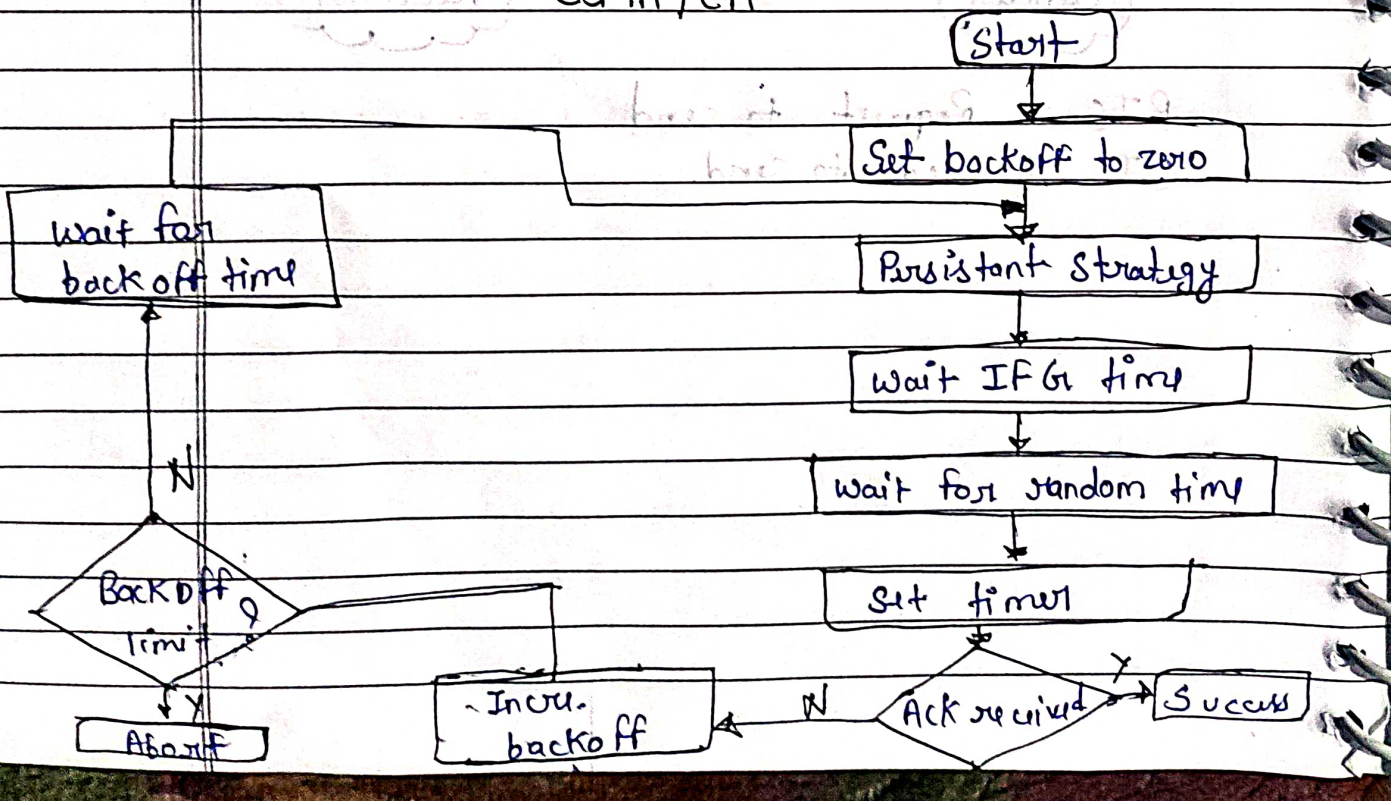
Page No.
Date / /

AKTU - 2022-23 (10 marks)

CSMA/CD



CSMA/CA



Page No.:
Date : / /

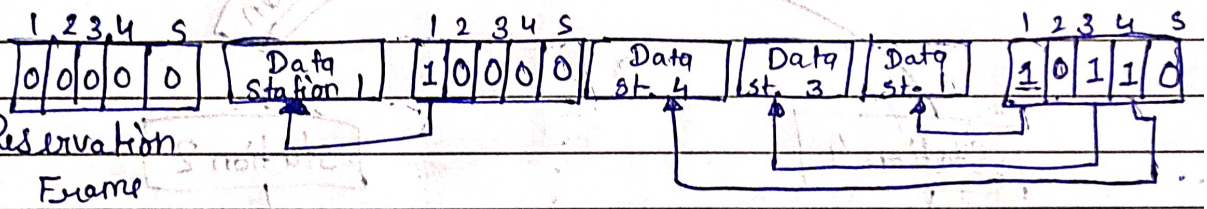
2. Controlled Access Protocol

→ It allows only one node to send at a time, to avoid collision of messages on shared medium.

A Reservation

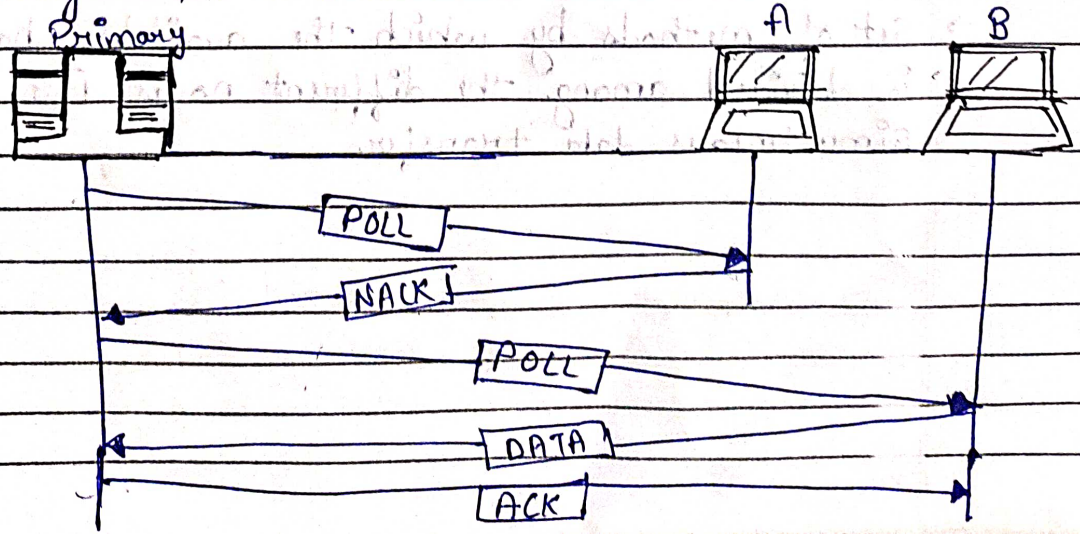
→ A station needs to make a reservation before sending the data.

→ whenever a station needs to sends the data frame, then the station makes a reservation in its own minislot.



B. Polling

→ In this, one acts as a controller and the others are secondary stations. All data exchanges must be made through the controller.

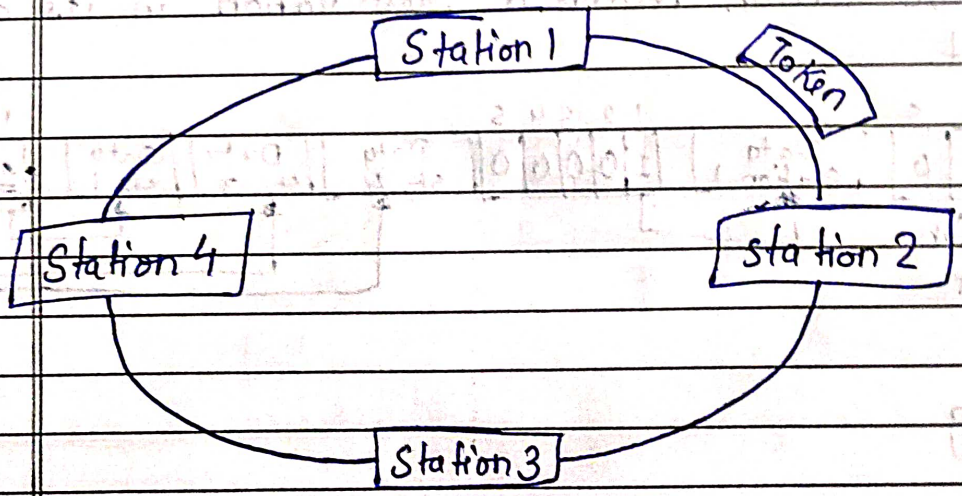


Page No.
Date / /

c. Token Passing

→ the stations are connected logically to each other in form of ring and access to stations is governed by tokens. (short message)

→ drawbacks are duplication of token or token is lost or insertion of new station, removal of a station.



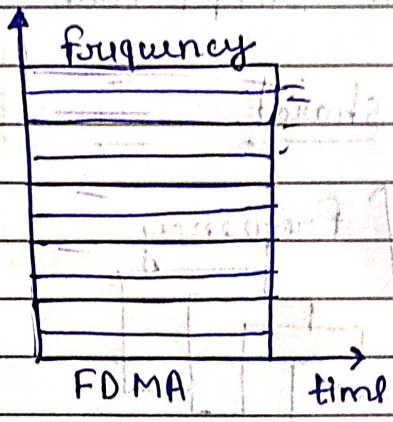
3. Channelization Protocol

→ Set of methods by which the available bandwidth is divided among the different nodes for simultaneous data transfer.

Page No.:
Date: / /

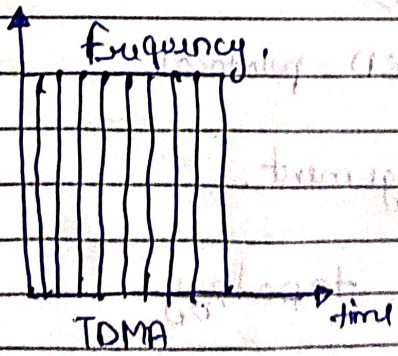
A FDMA (Frequency Division Multiple Access)

→ In this bandwidth is divided into various frequency bands. Each station is allocated with band to send data and that band is reserved for particular station for all the time, which is as follows:



B. Time Division Multiple Access (TDMA)

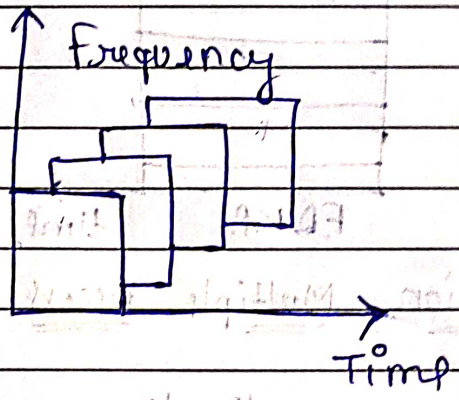
→ TDMA is the channelization protocol in which bandwidth of channel is divided into various stations on the time basis. There is a time slot given to each station, that station can transmit data during that time slot only which is as follows:



3. Code Division Multiple Access (CDMA):

→ all the stations can transmit data simultaneously. It allows each station to transmit data over the entire frequency all the time. & they are separated by unique code sequence. Each user is assigned with a unique code sequence.

Data + Code → shared.



LAN Standards

* 802.3 frame format.

→ used by LAN ✓
→ use CSMA/CD protocol ✓
→ No. acknowledgment. ✓
→ Bus and star topology.

Page No.:
Date: / /

46 to 1500

7 byte	1 byte	6 byte	6 byte	2 byte	↑ byte	4 byte
Preamble	Start Frame Delimeter	Destination Address	Source Address	length	Data	Frame check Sequence

1. Preamble → 56 bit pattern of 1s or 0s used for synchronization and timing recovering by the receiving device.
2. SFD → indicating the start of the frame.
3. D.A → indicating the MAC Address of the receiver device.
4. S.A → indicating the MAC Address of the Sinder device.
5. Length → indicating the type of protocol (e.g IPv4, ARP (length of data
6. Data → Data.
7. FCS → for error detection.

→ Data link layer Max Data length → 1518 byte. (→ from 2 marks AKTU)

(2) 802.5 Format

→ LAN

→ Use for Ring Topology

→ Access Control Method for token passing.

→ Piggy backing (Data + Ack.)

→ Use Differential Manchester encoding.

Page No.
Date: / /

[802.5] frame format.

Fiber Distributed Data Interface (FDDI): frame format.

Start Delimiter	Access Control	Frame Control	Dest Add.	Src Add.	Data	FCS	End Deli.	Frame Status
1 byte	1	1	6	6	>=0	4	1	1

max 4500 byte

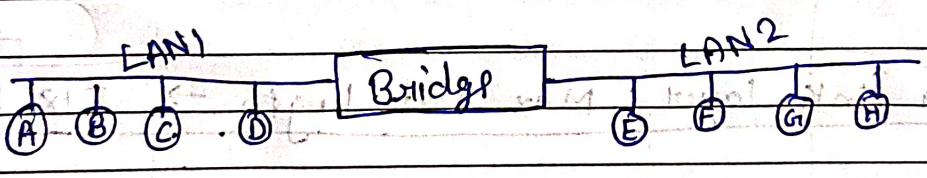
Start Deli.	Access Control	End Deli
1	1	1

← token format

→ Switching in unit-I ✓

→ **Bridging Concept**

Bridge is used to connect two different LAN's



Bridge works at 'physical layer' as well as at "DLL"

Mapping table for bridge.

MAC	A	B	C	D	E	F	G	H
PORT	P1	P1	P1	P1	P2	P2	P2	P2

Page No.:
Date : / /

① Static Bridge : Do ~~mapping~~ Manually Mapping.

② Dynamic / learning / Transparent Bridge :

They will automate learning the entries.

Capabilities of a Bridge :

① Filtering : (S.MAC & D.MAC are on same LAN)

② Forwarding : (S.MAC & D.MAC are on diff. LAN)

③ Flooding : (If any new station will be added)

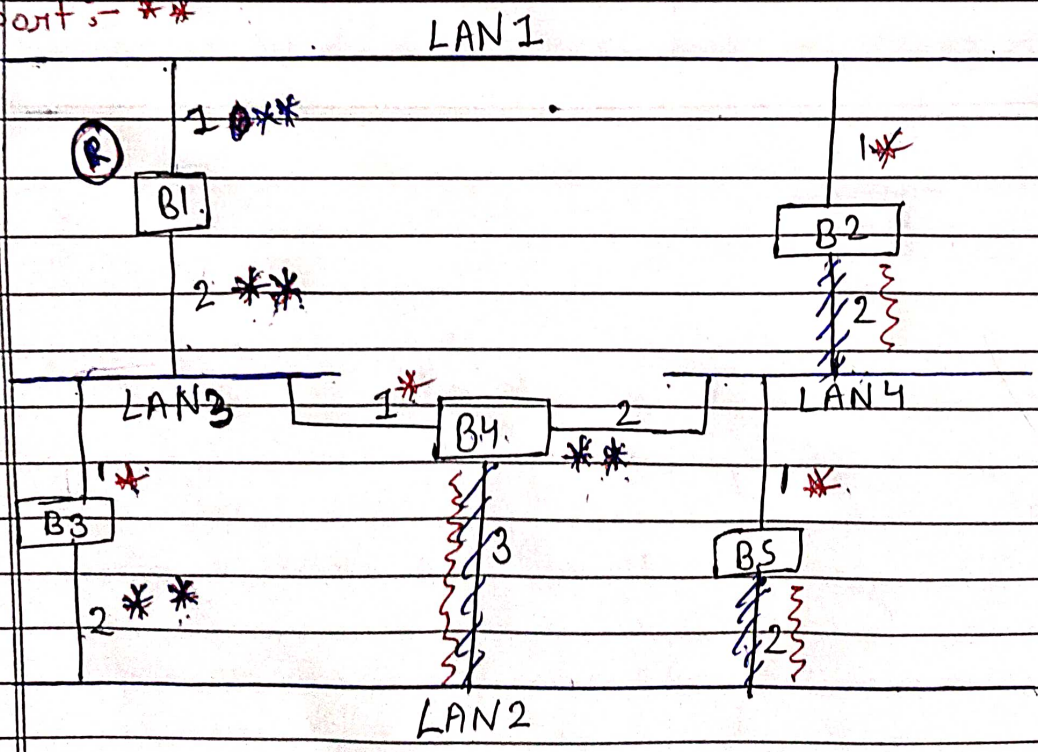
④ Store & forward : (No collision will occur)

Page No.
Date: / /

Spanning Tree Algorithm for Bridging

1. Every Bridge is having a built in ID. The one with smallest ID is taken as root bridge.
2. Mark one port of each bridge which is closest to the root bridge as a root port.
3. ~~LAN~~ Every LAN choose a bridge closest to it as a designated bridge for that LAN & mark that corresponding port as a designated port.
4. Mark the root port and designated port as forwarding port & block the remaining * port.

Root Port :- *
Designated Port :- **



Page No.:

Date : / /

Unit-2 is Completed

Subscribe

MULTI ATOMS

Join

TELEGRAM

COMPUTER NETWORKS

Page No.
Date / /

Unit-3 Network Layer

One Shot + 3 PYQ Solutions

Topics :-

1. Network layer functions
2. Point to Point Network & logical Addressing
3. Basic Internetworking [IP, CIDR, ARP, DHCP, ICMP]
→ 4. Subnetting + 2021-22 10 marks numerical.
+ 2022-23 - 18-19 10 marks numerical.
5. IP Adressing and its class classification.
→ 6. IPv4 & IPV6
7. IPv6 advantages over IPv4 - 2018-19 [10 marks].
→ 8. IPV6 Vs IPv4 - 2022-23 [10 marks]
→ 9. ICMP - 2021-22 - [10 marks]
→ 10. Routing [Static & Dynamic]
11. Forwarding & Delivery.
→ 12. Routing Algorithms [Imp - DVR] 2021-22
→ 13. Congestion Control - [2017-18]
→ 14. QoS [Quality of Service] - [2018-19]
15. Congestion Control Algorithms.

Page No.:
Date: / /

Network Layer

- The Network Layer is the third layer of the OSI Model.
- It handles the service requests from the transport layer and further forwards the service requests from the transport layer and for to the data link layer.
- The network layer translates the logical addresses into the physical addresses.
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

Main functions performed by the network layer

1. Routing
2. Logical Addressing
3. Internetworking
4. Fragmentation.

Page No.
Date: / /

Point to Point Network

→ A point to point network is a permanent link between two end points.
→ A point to point connection provides a dedicated link between two devices.
→ link can be wire, microwave or satellite link.
→ The entire capacity of the link is reserved for transmission between two devices.
→ Uses different types of topology (mesh or star) to connect two internet nodes.

AKTU-[2021-22] 2marks

Q. Discuss the role logical addressing

→ For different level of communication, we need a global addressing scheme known as logical addressing.
→ An IP address is used globally to refer to the logical address in the network layer of the TCP/IP protocol.
→ An IPV4 address is a 32 bit address that uniquely and universally defines the connection of a device to the Internet.

Page No.:
Date:

* Basic Internetworking [IP, CIDR, ARP, DHCP, ICMP]

→ Internetworking is the process of connecting different networks by using intermediary devices such as routers or gateway devices.

→ It ensures data communication among networks owned & operated by different entities using a common data communication and the Internet Routing Protocol.

→ Internetworking is only possible when all the connected networks use the same protocol stack.

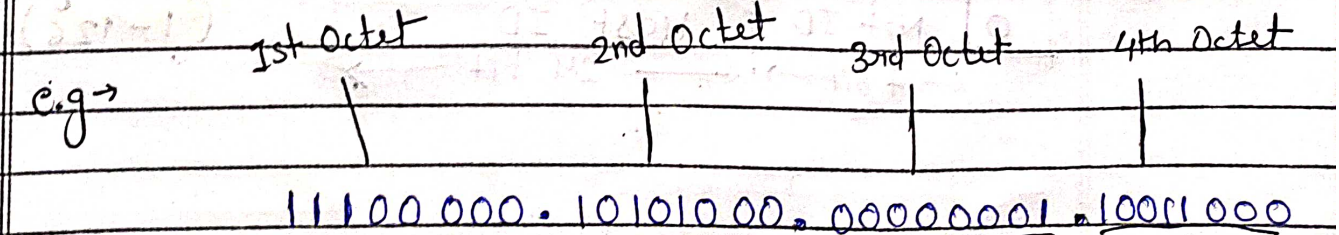
* IP Addressing

→ It is the process of finding unique IP address. A unique IP address is required for each host and network component that communicates using TCP/IP.

→ It is a network layer address and has no dependence on the data link layer address.

IP Address Classes:

→ The 32-bit IP address contains information about the host and its network.



Page No.
Date: / /

- Routers use Subnet Mask, which is as long as the size of the network address in the IP address. (32 bit)
- IP address (Binary) AND with its Subnet Mask result will Networks Address.

for example ⇒

IP Address : 192.168.1.152
Subnet Mask : 255.255.255.0 then :

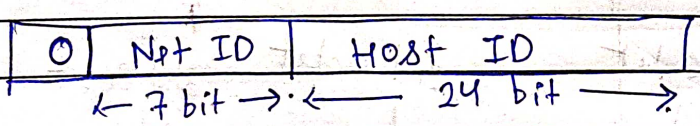
IP	11000000	10101000	00000001	10011000
Mask	11111111	11111111	11111111	00000000
Network	11000000	10101000	00000001	00000000

IP Address = no. of Networks + no. of hosts

No. of networks = $2^{\text{network\_bits}}$
No. of Hosts = $2^{\text{host-bits}} - 2$

1. Class A

The first bit always set to 0.

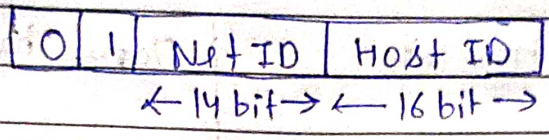


1st Octet (1-126)

Page No.:
Date:

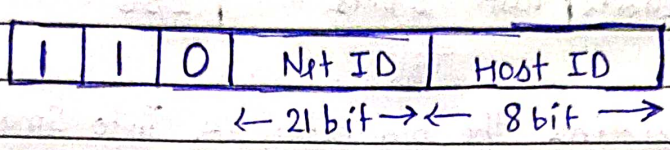
2. Class B

1st Octet
(128 - 191)



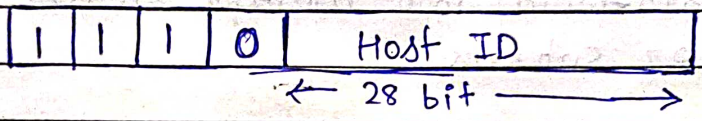
3. Class C

1st Octet
(192 - 223)



4. Class D

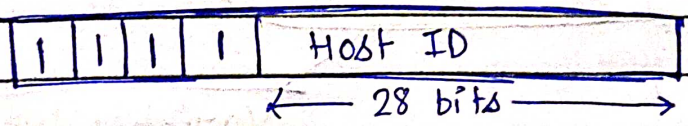
1st Octet
(224 - 239)



In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first Octet is always set to 1110, and the remaining bits determines the host ID in any network.

5. Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting.



* Classful Network Architecture

Class	Higher bits	Network address bits	Host address bits	No. of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 125.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	224.0.0.0 to 239.255.255.255
E	1111	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	240.0.0.0 to 255.255.255.255

Page No.
Date: / /

Default Subnet Mask

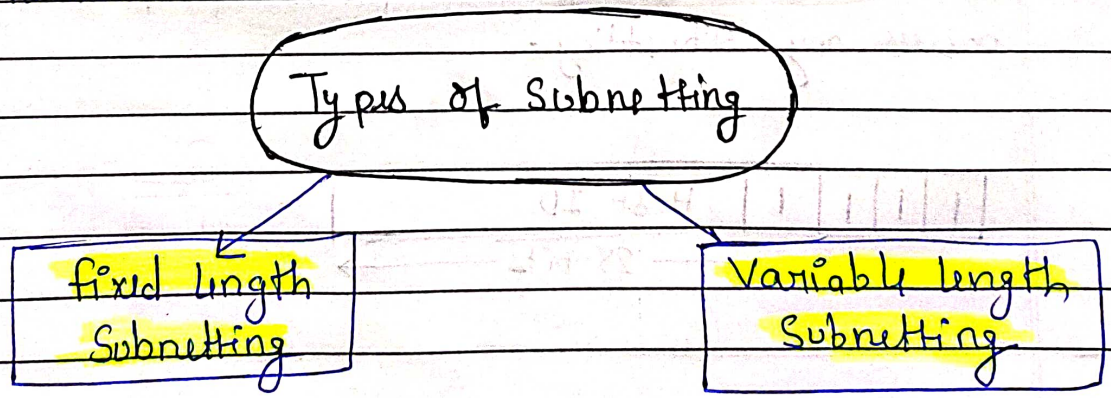
IP Class	Default Subnet	Network bits	Host bits	Total hosts
A	255.0.0.0	first 8 bits	last 24 bits	16,777,216
B	255.255.0.0	first 16 bits	last 16 bits	65,536
C	255.255.255.0	first 24 bits	last 8 bits	256

* **Subnetting** (Dividing the big network into small network)

It is a technique in which a single physical network is logically partitioned into multiple smaller subnetworks or subnets

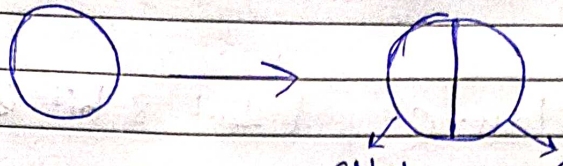
Advantages
- It improves the security
- The maintenance and administration of subnet is easy.

Disadvantages
- Identification of a station is difficult.
- Not possible to directed broadcast from outside network.



Page No.:
Date: / /

Q. Consider the network having IP Address 200.1.2.0. Divide this network into two Subnets.



200.1.2.0 0 0 0 0 0 0 0 ← 25 →

200.1.2.1 0 0 0 0 0 0 0 ← 25 →

(127) 0 1 1 1 1 1 1 1

(128) (255) 1 1 1 1 1 1 1 1

1st Subnet	2nd Subnet
• IP Address of the Subnet = 200.1.2.0 (Reserved)	• IP Address of the Subnet = 200.1.2.128 (Reserved)
• Direct Broadcast Address = 200.1.2.127 (Reserved)	• Direct Broadcast Address = 200.1.2.255 (Reserved)
• Total number of IP Addresses = $2^7 = 128$	• Total number of IP Addresses = $2^7 = 128$
• Range = [200.1.2.0, 200.1.2.127]	• Range = [200.1.2.128, 200.1.2.255]
• Total no. of host = 128 - 2 = 126	• Total no. of host = 128 - 2 = 126
• Range of Allocated IP Addresses = [200.1.2.1, 200.1.2.126]	• Range of Allocated IP Addresses = [200.1.2.129, 200.1.2.254]

Page No.
Date / /

AKTU- 2021-22 [10 marks]

Q. Divide the network with IP address 200.1.2.0 into 5 subnets.

Ans 200.1.2.0 → class-C [last 8 bit is host]

00 000000
00 111111

200.1.2.0 - 200.1.2.63
1st subnet

01 000000
01 111111

200.1.2.64 - 200.1.2.127
2nd subnet

10 000000
10 111111

200.1.2.128 - 200.1.2.191
3rd subnet

110 00000
110 11111

200.1.2.192 - 200.1.2.223
4th subnet

111 00000
111 11111

200.1.2.224 - 200.1.2.255
5th subnet

→ 00
→ 01
→ 10
→ 11 → 110, 111

Page No.:
Date: / /

AKTU - [2022-23, 2018-19] [10 marks]

Q. The IP network 200.198.160.0 is using subnet mask 255.255.255.224. Draw the subnets.

Ans. Step 1st = IP – Binary = 200.198.160.0
= 11001000.11000110.10100000.00000000

2. Step 2nd = Inverse Subnet mask = 255.255.255.224 = 0.0.0.31

3. Step 3rd Broad cast Address = (IP) logical OR (Inverse Subnet)

(IP) = 11001000.11000110.10100000.00000000
OR (Inverse) 00000000.00000000.00000000.00011111
= 11001000.11000110.10100000.00011111

4. Broad cast Address = 200.198.160.31.

5. Range of Subnet Mask = 0 – 31

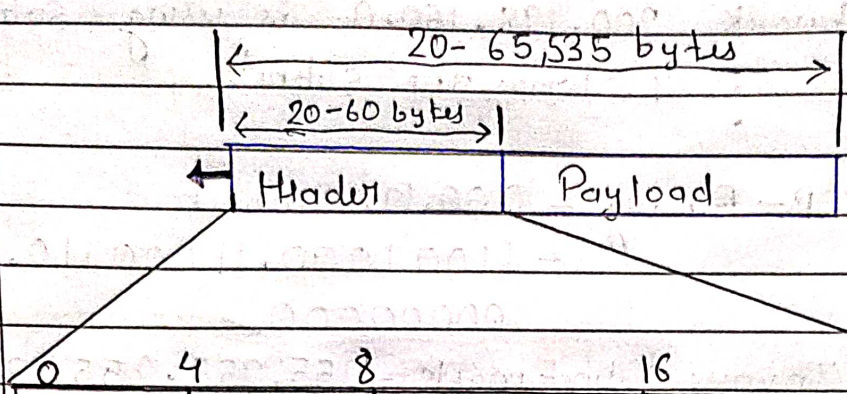
6. Draw Subnets.

1st Subnet =	200.198.160. 0	—	200.198.160. 31	.
2nd Subnet =	"	.32 –	"	.63 .
3rd Subnet =	"	.64 –	"	.95
4th Subnet =	"	.96 –	"	.127
5th Subnet =	"	.128 –	"	.159
6th Subnet =	"	.160 –	"	.191
7th Subnet =	"	.192 –	"	.223
8th Subnet =	"	.224 –	"	.255

Total = 8 Subnet

Page No.
Date / /

IPv4



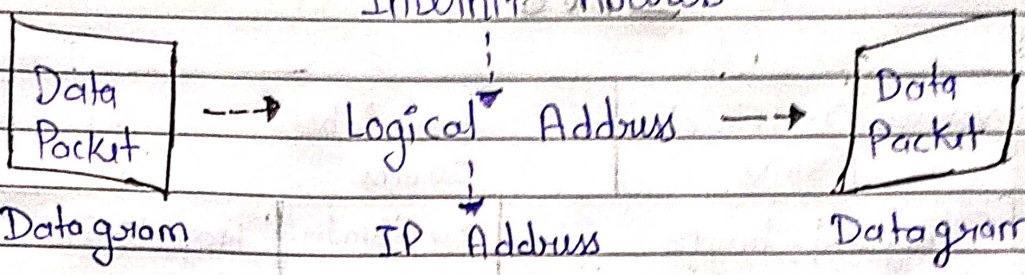
0	4	8	16	31
VER (4 bits)	HLEN (4 bits)	Service type (8 bits)	Total length (16 bits)	
Identification (16 bits)			Flags (3 bits)	Fragmentation offset (13 bits)
Time-to-live (8 bits)		Protocol (8 bits)	Header checksum (16 bits)	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + Padding (0 to 40 bytes)				

→ An IPv4 datagram consist of a header section and data section.
→ IPv4 header contains 13 fields of which 12 always requested, but 13th is optional.
→ fields in the header are packed in left to right and top to down fashion with MSB comes first.

① **Version** = which version of IP (4/6)

② **Header** = because header length is variable.

Page No.:
Date:



IPv4 address --> 32 bit ---> 2^{32} addresses
IPv6 address --> 128 bit ---> 2^{128} addresses

③ **Services** : used to define priority and special demands like delay throughput, reliability, cost etc.

④ **Total length** = total datagram = header + data.

⑤ **Identification** : used to identify a datagram uniquely.

⑥ **Flags** : Do not fragment, More fragments.

⑦ **Fragmentation offset** : used in case of fragmentation, how many bits before current packet.

⑧ **Time to live** : maximum hops after which packet will be discarded.

⑨ **Protocol** : the protocol for which it is carrying the payload.

⑩ **Header checksum** : for user check but confined to header only.

⑪ **Source Address** : Sets the source IP Address.

⑫ **Destination Address** : An indicating the receiver of the packet.

Page No.
Date: / /

IPv6

Version 4bits	Traffic class 8bits	Flow label 20 bits	
Payload length 16bits		Next header 8 bits	Hop limit 8 bits
Source address 128 bits			
Destination address 128 bits			

→ IPv6 is the most recent version of the Internet Protocol, designed to succeed IPv4.

→ IPv6 was developed to address the exhaustion of available IPv4 addresses and to provide additional features and improvements over IPv4.

- **Version** (4bits): It represents the IP version number.
- **Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of service to let the Router known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).

Page No.:
Date : / /

- **Flow Label (20 bits):**
→ An identifier of a flow of packets between a source & destination.
→ The label 0 means the packet does not belong to any flow.

- **payload length (16 bits):**
→ The size of the payload in octets, including any extension headers.

- **Next header (8 bits):** It specifies the type of the next header.

- **Hop limit (8 bits):** It replaces the Time To Live field in IPv4.

AKTU- 2018-19 [10 marks]

Q. Write advantages of Next-generation IPv6 over IPv4.

1. Larger Address Space = IPv6's 128 bit addresses offer an immense pool of unique addresses.

2. Efficient Routing = IPv6's simplified header improves routing efficiency and network management.

3. Built-in Security = Enhancing security without additional layers.

4. Enhanced Mobility = IPv6 supports mobile devices better.

5. Future-Proofing = designed to accommodate the continued growth of the Internet.

Page No.
Date / /

AKTU - 2022-23 [10 marks]

Q. Illustrate the difference between IPv4 and IPv6.

IPv6	IPv4
→ IPv6 has 128-bit address length	→ IPv4 has 32-bit address length.
→ It supports Auto and renumbering address configuration	→ It supports Manual and DHCP address configuration.
→ 3.4×10^{38} Address space	→ 4.29×10^{9} address space
→ Address Representation is in Hexadecimal (:)	→ Address Representation is in decimal. (.)
→ Checksum field is not available	→ checksum field is available.
→ IPv6 has a header of 40 bytes fixed.	→ IPv4 has a header of 20-60 bytes.
→ It does not support VLSM	→ It support VLSM (variable length subnet mask).

Page No.:
Date: / /

[IP, CIDR, ARP, RARP, DHCP, ICMP]

- **IP** → stands for Internet Protocol. It's set of rules governing the format of data sent over the Internet. IP addresses are unique identifiers assigned to each device on a network. e.g → 192.255.255.255.

- **CIDR** → stands for Classless Inter-Domain Routing. It's method for allocating IP addresses and routing IP packets more efficiently. CIDR notation is used to specify a range of IP addresses by combining the IP address with its Subnet mask. e.g ⇒ 192.255.255.255/12. ↑ N/w id

- **ARP** → stands for Address Resolution Protocol. used to find the MAC address of the destination. The purpose of ARP is to resolve an IPv4 address to the corresponding physical Address. IP ⟶ MAC

- **RARP** → stands for Reverse Address Resolution Protocol. we find IP address using RARP. RARP is a TCP/IP protocol that is responsible for the translation of MAC address to be translated into an IP address. MAC ⟶ IP

- **DHCP** → stands for Dynamic Host Configuration Protocol. The DHCP is controlled by a DHCP server that dynamically distributes network configuration parameters for interfaces and services. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.

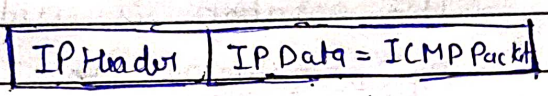
Page No.
Date / /

HRTU 2021-22 [6th sem]

- ICMP - Internet Control Message Protocol.

→ IP is an unreliable service, Here we don't forward an ack. for confirmation of frame reception.

→ ICMP is a Network layer protocol, that operates on Internet Protocol.
→ It is used for error reporting and diagnostic purposes



IP Packet.

→ ICMP is not a mandatory protocol in computer network
→ mainly used for reporting errors and management queries.

* Error Reporting : ✓

1. Source quench message:
→ when sender resends the packet at a higher rate and the router is not able to handle.
→ then router sends a SQM to sender to send the packet at a lower rate.

2. Time excided message:
→ when time-to-live value to Zero. then router discards a datagram and sends the TEM message to the original source.

Page No.:
Date: / /

3. Parameter Problem:
→ Incase of mismatch of calculated header checksum, packet will be dropped by the router and informs to the source by sending a PPM.

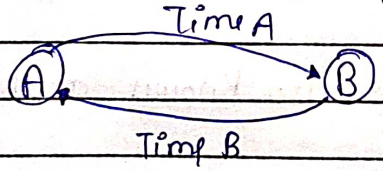
4. Destination un-reachable:
→ DU is generated by the host to inform the client that the destination is unreachable for some reason.

5. Redirection Message:
→ Redirect requests data packets are sent on an alternate route. The message informs a host to update its routing information.

* Query Management:

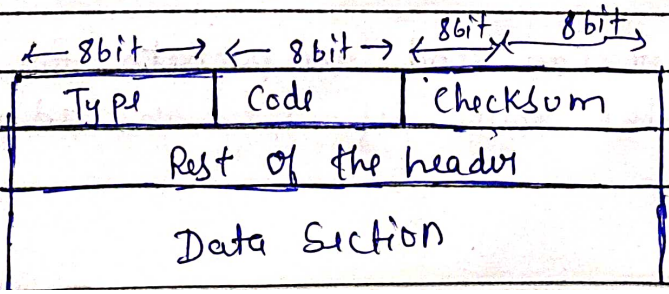
1. Echo Request & Reply:
→ It is used for diagnostic purpose whether two hosts can communicate with each other.

2. Timestamp Request and Reply:
→ used to calculated Round Trip Time.



$$\frac{\text{Time A} + \text{Time B}}{2} = \text{Timestamp}$$

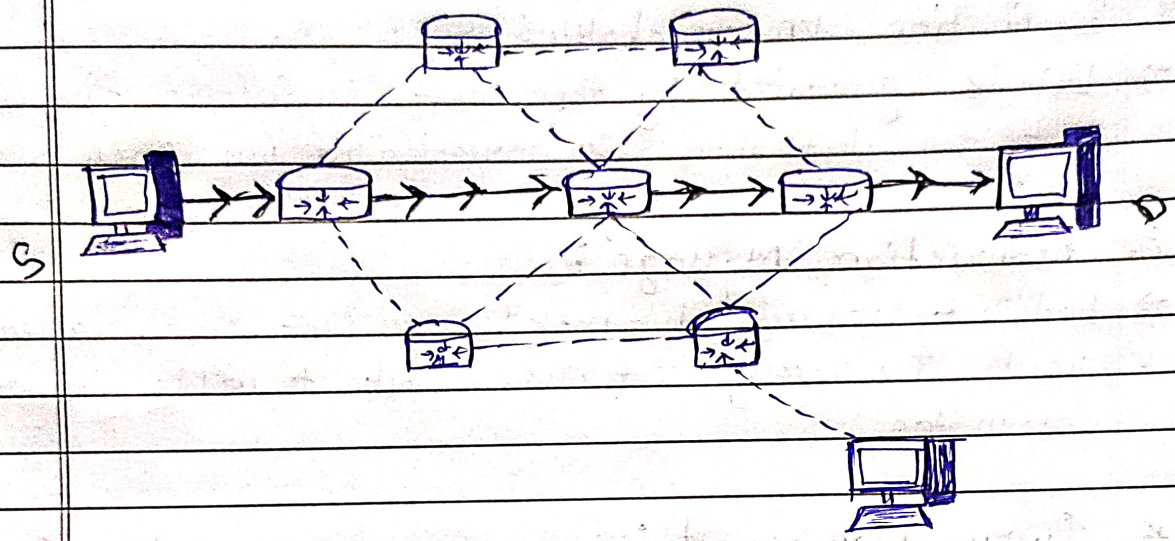
Format of ICMP



Page No.
Date / /

Routing

→ It is a process of selecting path along which the data can be transferred from source to destination



→ Routing is performed by a special device known as a router.

→ The routing algorithms are used for routing the packets. The routing algo. responsible for choosing the optimal path.

Static Routing

→ Static Routing is also known as Non-adaptive Routing.

→ It is a technique in which the administrator manually adds the routes in a routing table.

→ A Router can send the packets for the destination along the route defined by the administrator.

Page No.:
Date : / /

Adv ⇒ The cheaper router can be used to obtain static routing.
⇒ It provide security as the system administrator is allowed only to have control.

Disadv ⇒ Very difficult for large network.
⇒ The system administrator should have a good knowledge of a topology.

⇒ **Dynamic Routing**

→ It is also known as Adaptive Routing.

→ It is a technique in which a router adds a new route in the routing table for each packet in the condition of the network.

→ In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.

Adv ⇒ It is easy to configure.
It is effective in selecting the best route.

Disadv ⇒ It is less secure.
⇒ It is more expensive.

Page No.
Date: / /

Forwarding

→ It is simply defined as the action applied by each router when a packet arrives at one of its interfaces. When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network.

1. Next hop Method:

→ One technique to simplify the routing table is called the Next-hop method.

→ Routing table holds only address of the next hop.

2. Network-Specific Method:

→ This technique helps to reduce the routing table and simplify the searching process.

→ Here, we have only one entry that defines the address of the distination network itself

3. Default Method:

→ Another technique to simplify routing is called the default method.

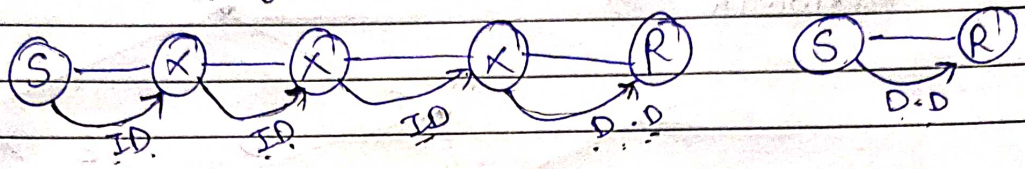
→ In this technique instead of listing all networks in the entire Internet, host just has one entry called the default.

→ It is normally defined as network address 0.0.0.0

Page No.:
Date: / /

Delivery

→ Delivery refers to the way a packet is handled by the network layer.
→ The network layer supervises the handling of the packets by the underlying physical networks.



1. Direct Delivery

→ Packet reaches final destination
→ via router or Sender itself

2. InDirect Delivery

→ Packet reaches intermediate node & not final destination
→ via router or Sender itself.

Routing Algorithms

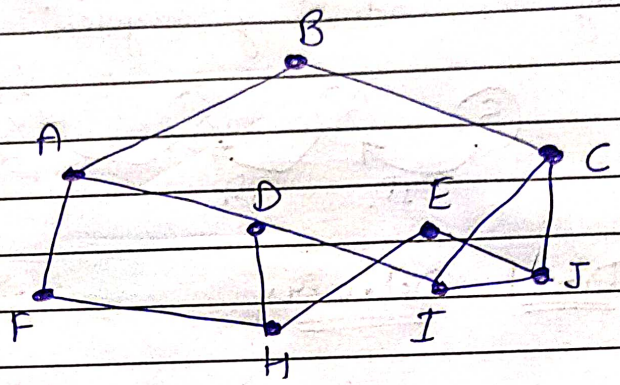
Static	Dynamic
→ Shortest path Routing	→ Distance Vector Routing
→ Flooding	→ Link State Routing
→ Flow Base Routing	

Page No.
Date / /

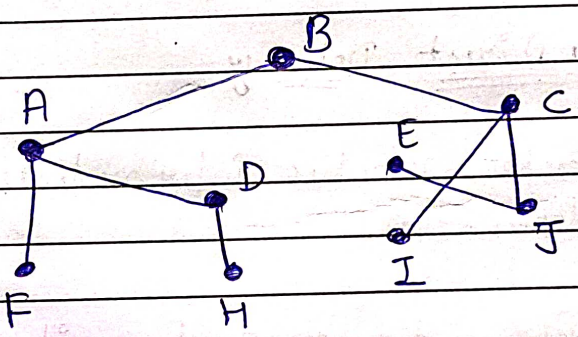
1. The Optimality Principle:

Each portion of a best path is also a best path; the union of them to a router is a tree called the sink tree.

Network ⇒



Sink tree of best paths to router B ⇒



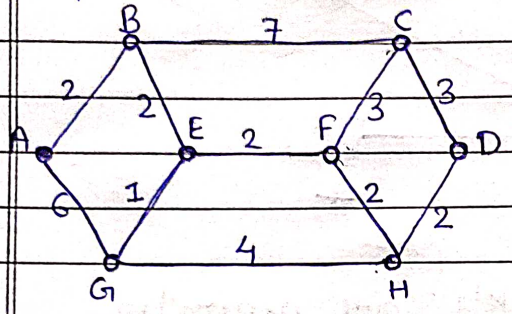
2. Shortest Path Algorithm

a) Dijkstra's algorithm computes a sink tree on the graph.
b) Each link is assigned a non-negative weight / distance.

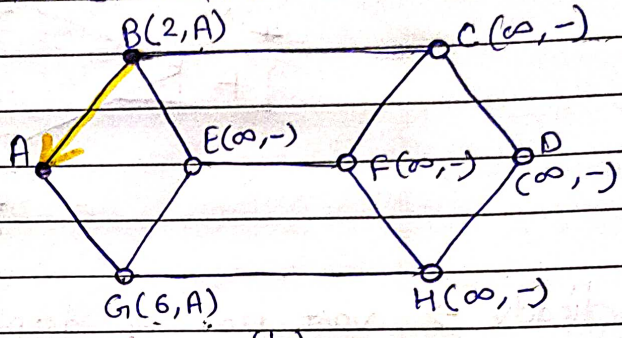
Page No.:
Date:

Algo:

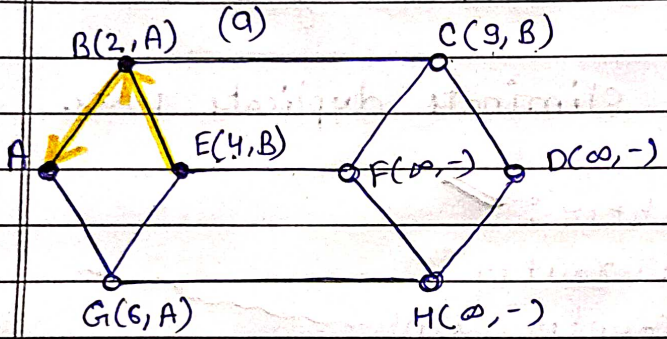
a) Start with sink, set distance at other nodes to infinity.
b) Relax distance to adjacent nodes
c) Pick the lowest adjacent distance node, add it to sink tree.
d) Repeat untill all nodes are in the sink tree.



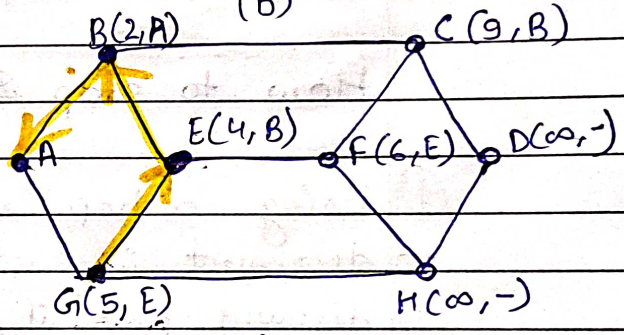
(a)



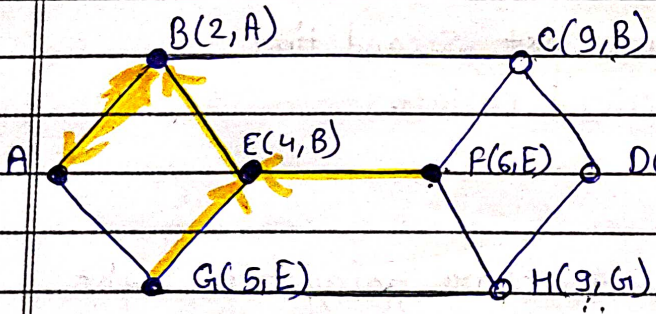
(b)



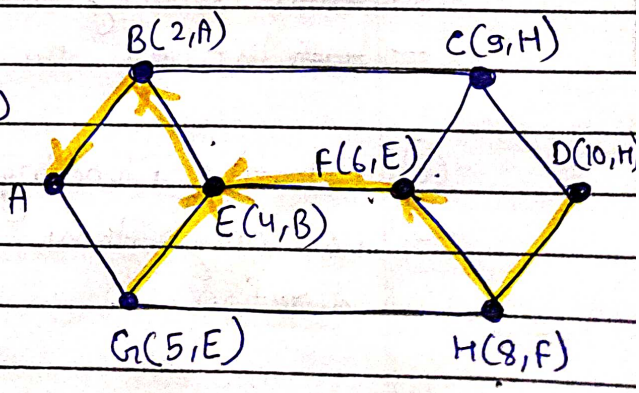
(c)



(d)



(e)

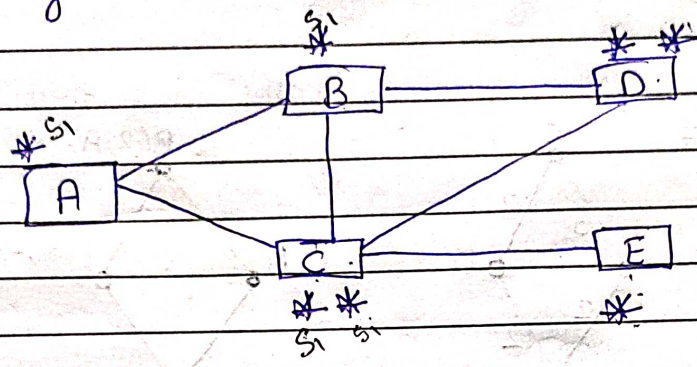


(f)

Page No.
Date: /

3. Flooding

→ A simple local technique is Flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on.



disadv → vast no. of duplicate pkts are generated.

How to stop & Eliminate duplicate pkts.

① Using a hop counter:
- decrement in each router
- discard pkt if counter is '0'

② Sequence no. in pkt:
- avoid sending the same pkt second time
- ~~lists~~ list all the received packets.

③ Selective Flooding:
- use only those lines that are going in right direction.

Page No.:
Date:

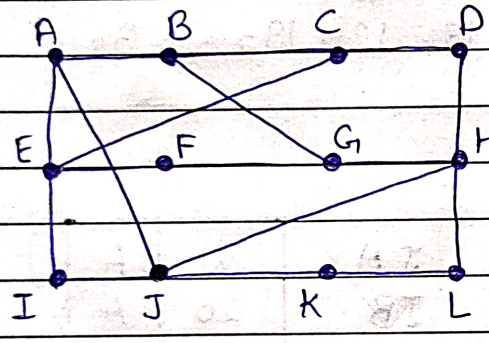
AKTU - 2021-22 [10 marks].

4. Distance Vector Routing

→ It is an Unicast Routing Protocol.
→ DVR uses the Bellman-Ford algorithm.

Algo:-
a) Each node knows distance of links to its neighbours.
b) Each node advertises vector of lowest known distances to all neighbours
c) Each node uses received vectors to update its own.
d) Repeat periodically.

e.g.→



To	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	06	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9
	JA	JI	JH	JK
	delay	delay	delay	delay
	8	10	12	6

→ We have to find New estimated delay from J.

Page No.
Date / /

→ JA → min (JA + AA, JI + IA, JH + HA, JK + KA)

min (8 + 0, 10 + 24, 12 + 20, 6 + 21)
(8, A)

→ JB → min (JA + AB, JI + IB, JH + HB, JK + KB)

min (8 + 12, 10 + 36, 12 + 31, 6 + 28)
(20, A).

→ JC → min (JA + AC, JI + IC, JH + HC, JK + KC).

min (8 + 25, 10 + 18, 12 + 19, 6 + 36).
(28, I).

JA	8	A
JB	20	A
JC	28	I
JD	20	H
⇒ JE	17	I
J	30	I
'	18	H
'	12	H
'	10	I
'	0	-
	6	K
JL	15	K

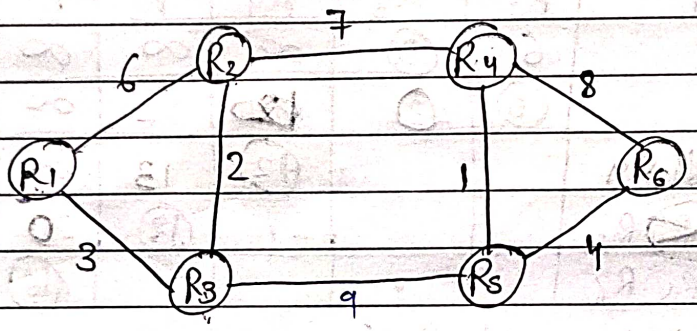
New vector for J

Page No.:
Date: / /

5. Link State Routing

→ It is an Unicast Routing Protocol.
→ Discover its neighbours and learn their network addresses.
→ Set the distance metrics to each of its neighbours.
→ Construct a packet telling all it has just learned.
→ Computs the shortest path to every other router.
→ Using this packet (send this packet to and receive packets from all other routers).

Eg⇒



Table

1st ⇒

R1	
Seq. No.	
111	
R2	6
R3	3

R2	
R1	6
R3	2
R4	7

R3	
R1	3
R2	2
R5	9

R4	
R2	7
R5	1
R6	8

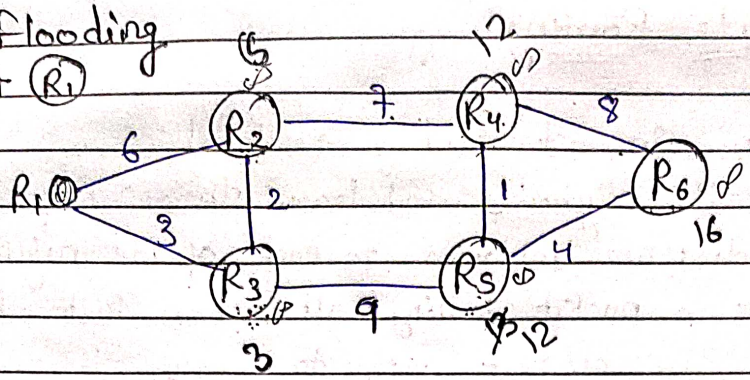
R5	
R3	9
R4	1
R6	4

R6	
R5	4
R4	8

Step 1

Page No.
Date / /

2nd Flooding at R_1



3rd Dijkastra.

R_1	R_2	R_3	R_4	R_5	R_6
$R_1 R_3$	6	(3)	∞	∞	∞
$R_1 R_3 R_2$	(5)	(3)	~~∞~~	12	∞
$R_1 R_3 R_2$ ~~R_4~~ R_4			(12)	13	∞
$R_1 R_3$ ~~$(R_2 \; R_4)$~~ R_5				(13)	20
$R_1 R_3 R_5$ R_6					(16)

4th Routing Table of R_1

		Via
R_1	0	R_1
R_2	5	R_3
R_3	3	R_1
R_4	12	$R_3 R_2$
R_5	12	R_3
R_6	16	$R_3 R_5$

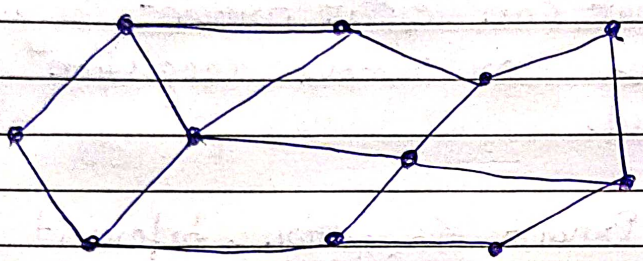
AKTU - 2018-19 Q→ Unicast Routing Protocols.
1. – DVR
2. – Link state Routing

Page No.:
Date : / /

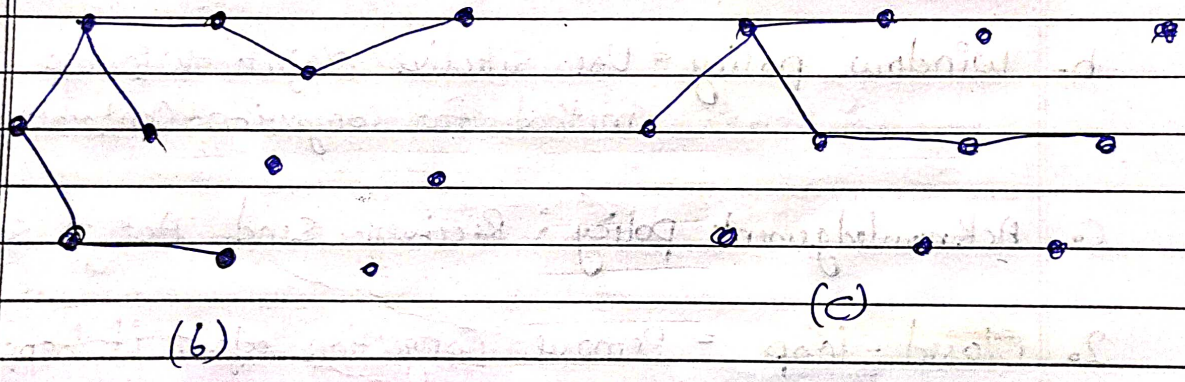
6. Multicast Routing

→ Sending a massage to a group is called multicasting. Multicasting requires group management need to create & destroy groups. For multicast routing each router computes a spanning tree covering all other routers.

e.g.



(a) network.



(b) (c)

7. Broadcast Routing

→ Sending a packet to all destinations simultaneously is called broad casting.

1. Multi destination Routing.
2. Flooding
3. Sink tree.

Page No.
Date: / /

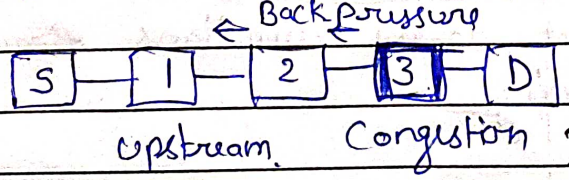
DKTU 2017-18 [10 marks]

Congestion

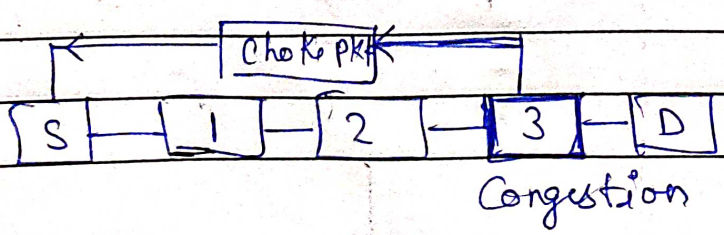
→ Congestion in a network may occur if the load on the network is greater than capacity of network.

Congestion Control : It refers to techniques and mechanisms that can either prevent congestion, before it happens or remove congestion, after it has happened.

1. **Open Loop** = Prevent Congestion, before it happens)
   a. Retransmission policy = pkt can be retransmitted
   b. Window policy = Use Selective reject window method for Congestion Control
   c. Acknowledgement policy : Reciver send Ack to Sender
2. **Closed - loop** = Remove Congestion after it happens.
   a. Back pressure = In this congested node stops receiving data from the immediate upstream nodes.



   b. Choke packet =



Page No.:
Date:

c. Implicit signaling = there is no communication b/w congested node or node and the source.

→ Source guesses there is a congestion in network. when it does not receive any ack.

d. Explicit signaling = sending direct signal to source or destination.

Quality of Service (QoS) AKTU-2018-19 [10 marks]

→ QoS is an overall performance measure of computer Network.

(1) Reliability ⇒ lack of Reliability means loosing Packet or Acknowledgement, which result Retransmission.
e.g → Email, File Transfer, Internet Access (More Reliability Need)

(2) Delay ⇒ It is time taken to transmit Packet from source to Destination in flow.

(3) Jitter ⇒ Jitter is variation in Packet Delay.

(4) Bandwidth ⇒ It is number of bit send.

Page No.
Date: / /

QoS Table

Application	Bandwidth	Delay	Jitter	Loss
Email	Low	Low	Low	Medium
File sharing	High	Low	Low	Medium
Web access	Medium	Medium	Low	Medium
Remote login	Low	Medium	Medium	Medium
Audio	Low	Low	High	Low
Video	High	Low	High	Low
Telephony	Low	High	High	Low
Video conferencing	High	High	High	Low

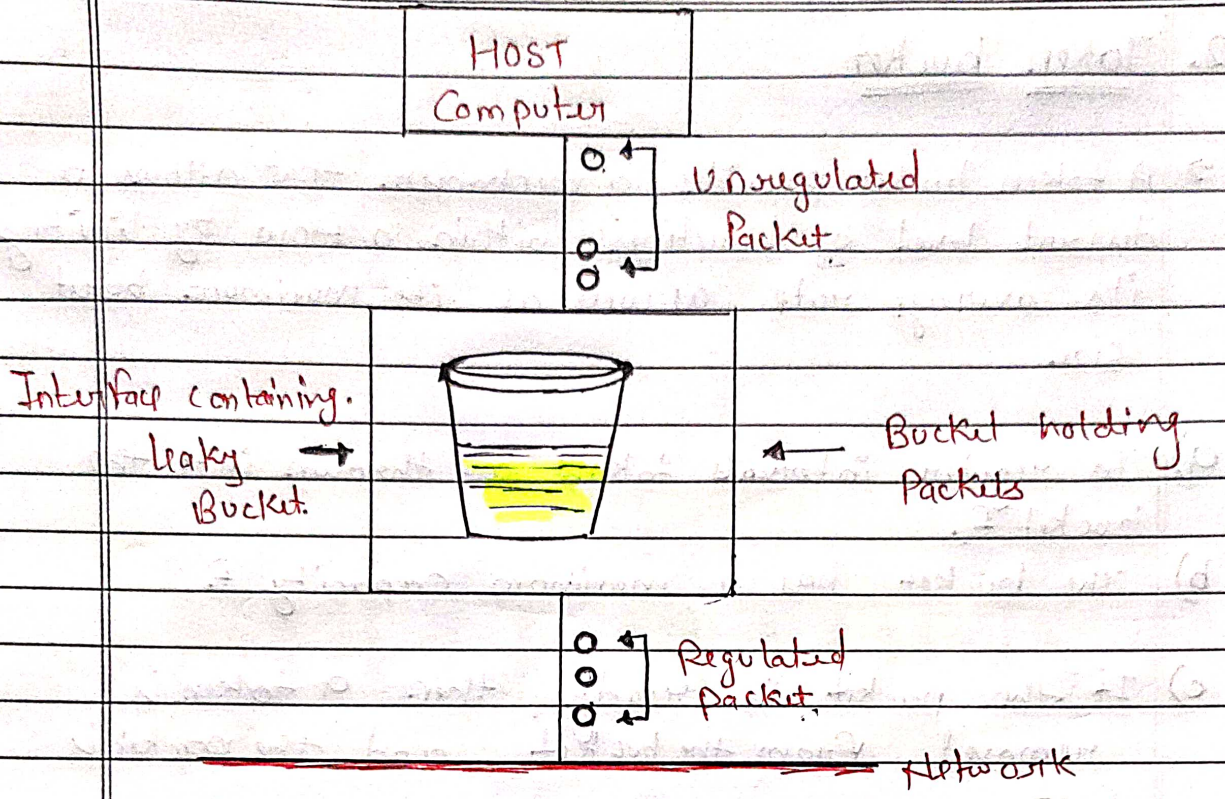
Congestion Control Algorithms:

1. Leaky Bucket

The Leaky Bucket Algorithm is a method of congestion control where multiple packets are stored temporarily. These packets are sent to the network at a constant rate. This algo is used to implement congestion control through traffic shaping in data networks.

→ a bit overdone and also packet can get lost (bucket is full)

Page No.:
Date:



Step1 ⇒ Initialize buffer size & leak rate.

Step2 ⇒ At clock tick, Initialize n as the leak rate.

Step3 ⇒ If n > size of packet (Send the packet into N/w)
(n − size of Pa)

Step4 ⇒ Decrement n by the size of the packet

Step5 ⇒ Repeat step 3 and step 4 untill n < size of pkt
No other packet can be transmitted till the next clock tick

Step6 ⇒ ~~Go~~ Go to Step2.

Page No.
Date / /

2. Token bucket

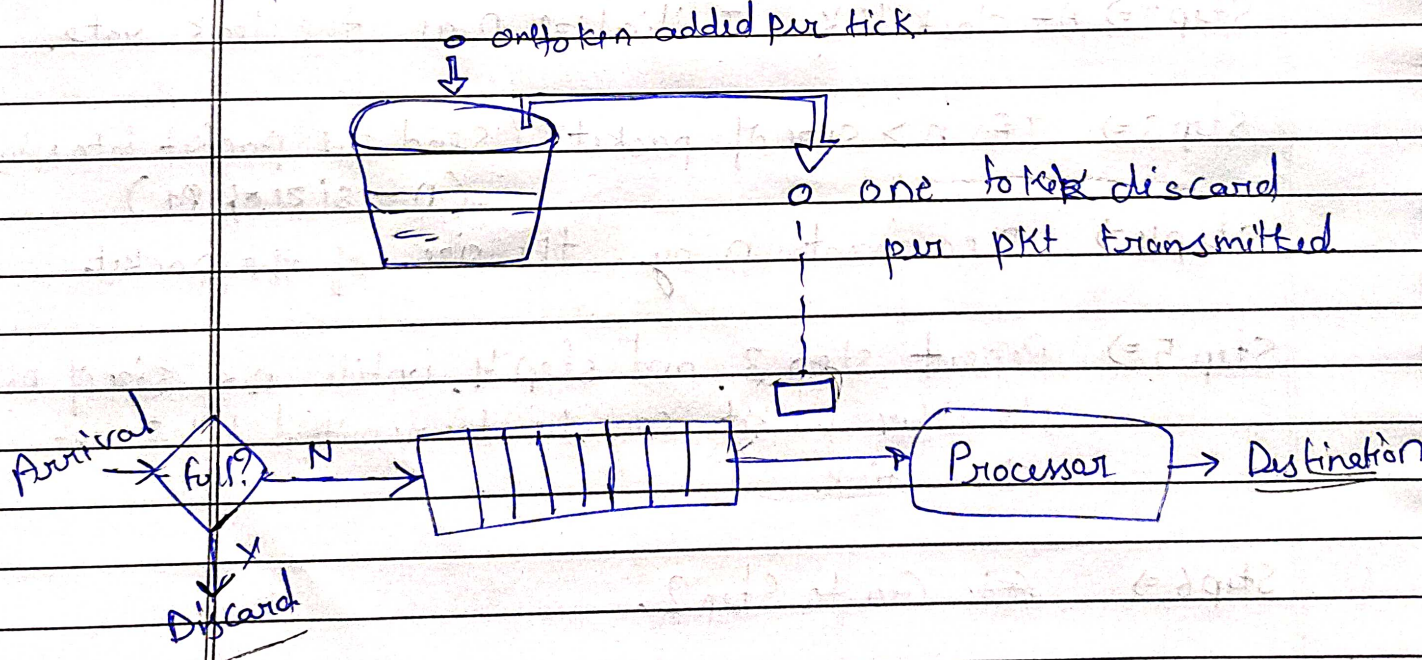
⇒ A token bucket provides a mechanism that allows a desired level of burstiness within a flow by limiting its average rate as well as its maximum burst size.

a) In regular intervals tokens are thrown into the bucket f.

b) The bucket has a maximum capacity f.

c) If the packet is ready, then a token is removed from the bucket, and the packet is sent

d) Suppose, if there is no token in the bucket, the packet cannot be sent.



Page No.:
Date:

Unit-3 Completed

COMPUTER NETWORK

Page No.
Date : /

Transport Layer Unit-4

ONE SHOT + 3PYQ Solutions

Topics :-

→ Transport layer & its functions
→ Process to Process delivery.

* → TCP and UDP [Header format] [2022-23, 2021-22]
* → TCP Vs UDP

* → TCP numerical [2018-19]
* → Three-way Handshake.

→ TCP window management System.
→ Flow Control & Retransmission.

→ Multiplexing & Demultiplexing.

→ QoS & its techniques to improve it.

* → TCP Congestion Control.

Subscribe + Join Telegram

Page No.:
Date: / /

Transport Layer

It is the second layer in the TCP/IP model and the fourth layer in the OSI model. It is an end to end layer used to deliver messages to a host.

Working of Transport layer

The transport layer takes services from the Application layer and provides services to the Network layer.

At the sender's side: It receives data from Application layer and then performs Segmentation, divides the actual message into segments, adds to source and destination's port numbers into the header of the Segment, and transfer the message to the Network layer.

At the receiver's side: It receives data from the Network layer, reassembles the segmented data, reads its header, identifies the number, and forwards the message to the appropriate port in the Application layer.

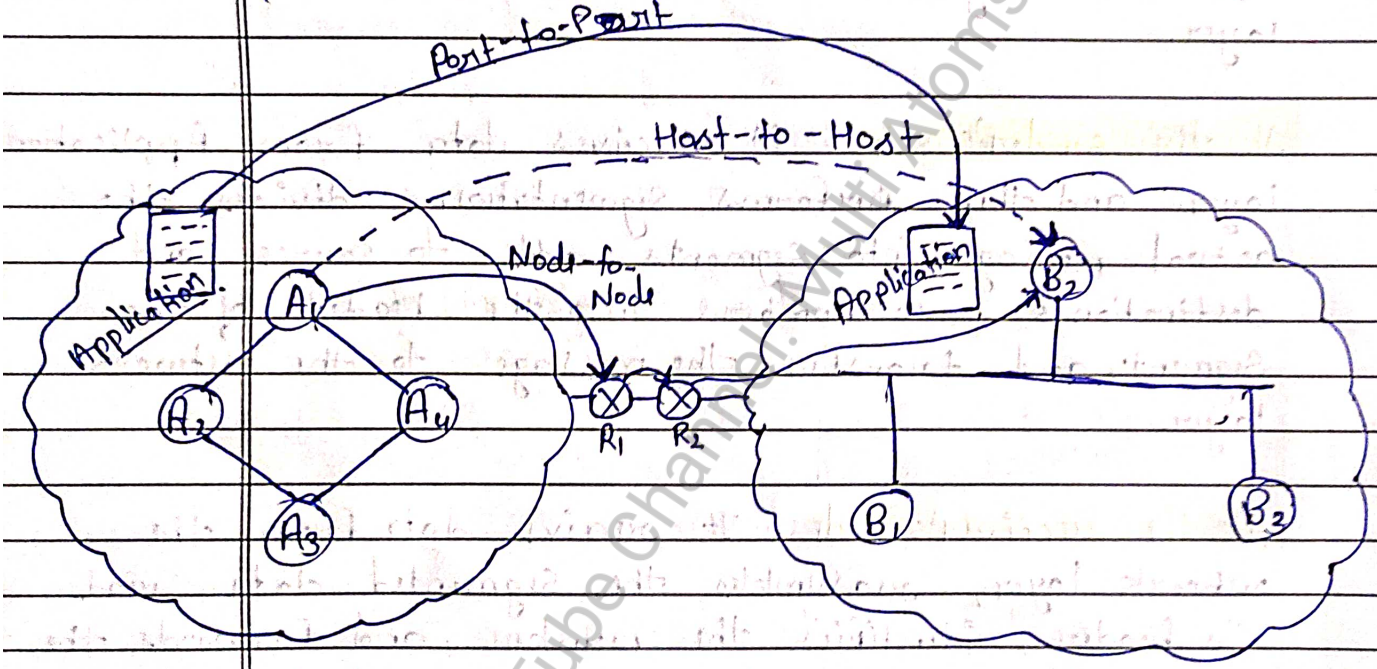
Functions of Transport layer:

1. Process to Process Delivery
2. Multiplexing & Demultiplexing
3. Congestion Control
4. Data Integrity & Error Correction
5. Flow Control.

Page No.
Date / /

Process-to-Process delivery / Port to port / Node to Node

→ A process is an application program running on a host.
→ The data link layer performs a node-to-node delivery.
→ The network layer performs host-to-host delivery.
→ The transport layer is responsible for the delivery of a packet, part of a message, from one process to another.



→ Transport Layer Protocols

① TCP [Transmission Control Protocol]

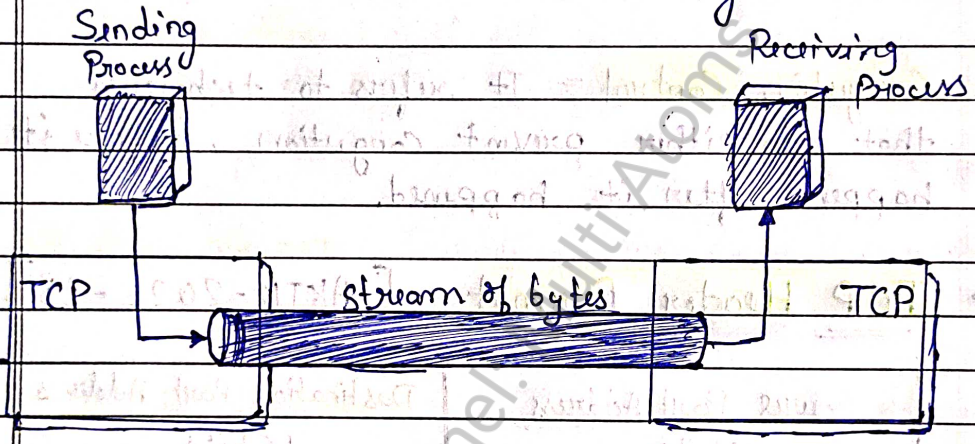
② UDP [User Datagram Protocol]

Page No.:
Date : / /

Transmission Control Protocol

→ TCP is Connection-oriented protocol.

Services TCP provides
- → Byte streaming
- → Connection Oriented
- → Full Duplex
- → Piggy backing
- → Error Control
- → Flow Control
- → Congestion Control



* **Byte Streaming** = TCP sends data as a continous, ordered stream of bytes, simplifying data handling by hiding packet details from application.

* **Connection Oriented** = It establishes a connection before data transfer begins and maintains it until the transfer is complete.

* **Full-Duplex** = TCP processes can send & receive both at the same time.

Page No.
Date / /

* **Piggybacking** :- means sending an acknowledgment along with data in the same packet to save time & resources.

* **Error Control** = TCP ensures data is sent and received accurately by detecting errors, requesting retransmission, and confirming successful delivery.

* **Flow Control** = manages the rate of data transmission between sender and receiver to prevent overwhelm & ensure smooth communication.

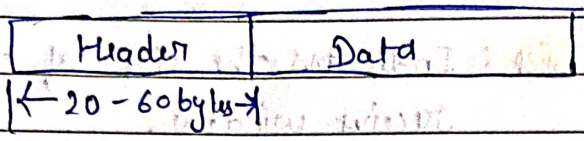
* **Congestion Control** = It refers to techniques that can either prevent congestion, before it happens, after it happened.

→ **TCP Header Format** [AKTU-2022-23]

Source Port Address 16 bits								Destination Port Address 16 bits
Sequence number 32 bits								
Acknowledgment number 32 bits								
HLEN 4 bits	Reserved 6 bits	U R G	A C K	P S H	R S T	S Y N	F I N	Window size 16 bits
Checksum 16 bits								Urgent pointer 16 bits
Options & Padding								

Page No.:
Date:

→ The Segment consists of a 20- to 60- byte header, followed by data + header.



Segment

1. **Source Port** : A 16-bit number identifying the application that TCP segment originated from within the sending host.
2. **Destination Port** : A 16-bit number identifying the application that TCP segment is destined for on a receiving host.
3. **Sequence number** : Identifying the current position of the first data byte. main the sequence of data.
4. **ACKnowledgement no.** : Identifying the next data byte that the Sender expects from the receiver.
5. **HLEN** : length of the header. (multiply by 4)
6. **Reserved** : Reserved for future use. Must be '0'.
7. **Control bit** or **Flags** : one or more of these bits can set at a time.
   i) **URG** : The value of urgent pointer field is valid.
   ii) **ACK** : The value of acknowledgement field is valid.
   iii) **PSH** : Push the data
   iv) **RST** : Reset the data.

Page No.
Date / /

(v) SYN: Synchronize sequence numbers.
(vi) FIN: No more data from sender.

8) Window Size: Indicates the size of the sender's receive window.

9) Checksum: Used for error-checking / control the header and data.

10) Urgent Pointer: If the URG flag is set, this field points to the sequence number of the urgent data.

11) Options: There can be upto 40 bytes of optional information in the TCP header [Maximum Segment Size, Timstamp, etc.].

AKTU - 2018-19

Q. The following is the dump of a TCP header in hexa decimal format:
05320017 00000001 00000000 500207ff 0000000

(I) what is the Sequence number?
(II) what is the destination port number?
(III) what is the acknowledgement number?
(IV) what is the window size?

Hexadecimal no. represent in 4bits.

Page No.:
Date: / /

* Sequence Number (32 bits)

Hexadecimal value = 00000001 = 1×16^0
Decimal Value = 1

* Destination Port number (16 bits) =

Hexadecimal value = 0017 = $(1 \times 16^1 + 7 \times 16^0)$
Decimal Value = 23

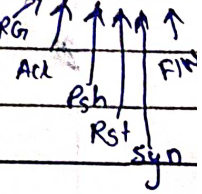
* Acknowledgement number (32 bits)

Hexadecimal Value = 00000000
Decimal Value = 0

* Window Size (16 bits)

Hexadecimal value = 07ff = $(7 \times 16^2 + 15 \times 16^1 + 15 \times 16^0)$
Decimal value = 2047

* Source Port no. = ? [1330]
* HLEN = ? [5 x 4] = 20
* Reserved/Flags = ? / Type of Segment = [SYN] 000010
* Checksum = ? [0]
* Urgent pointer = ? = [0]

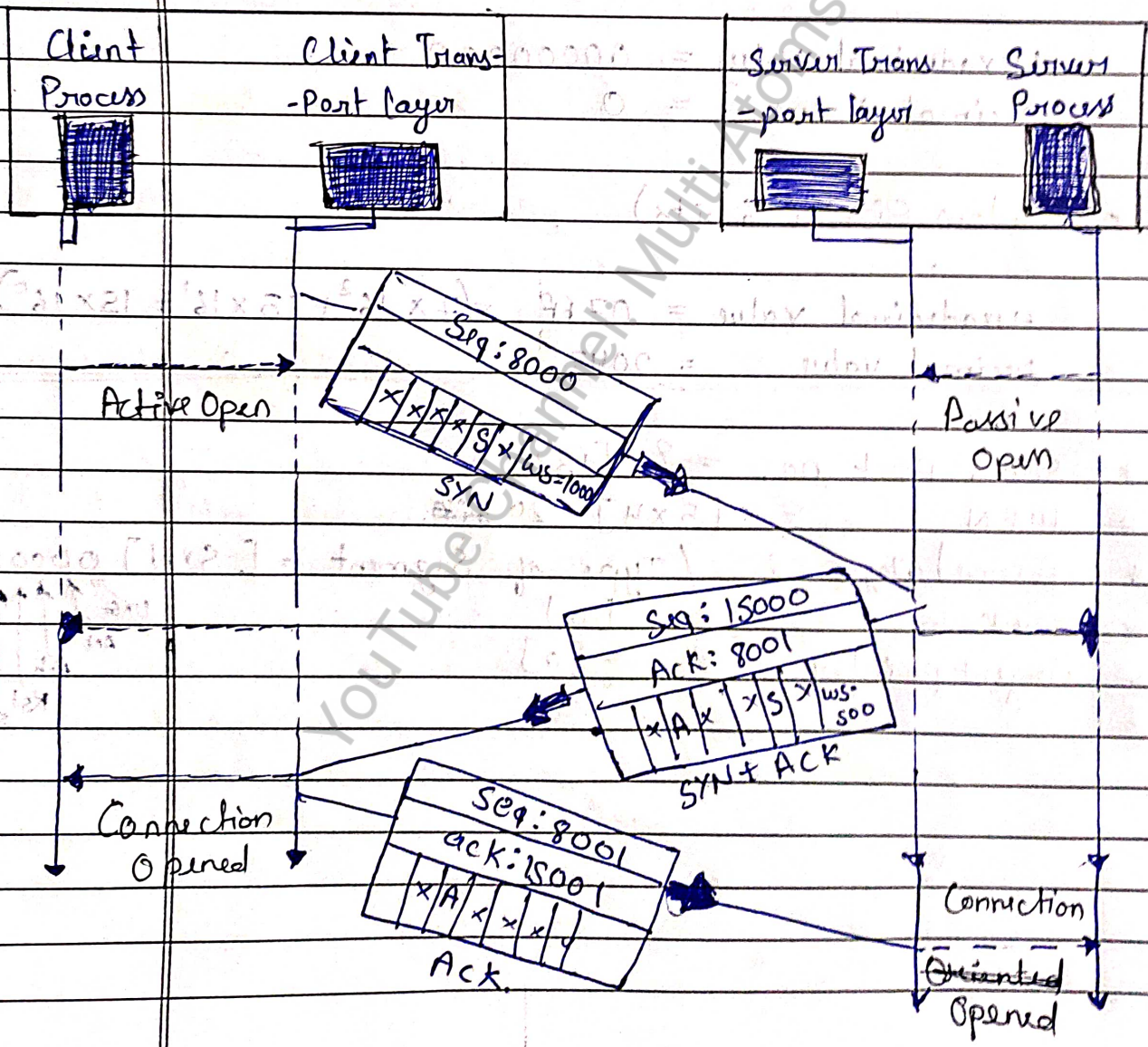


Page No.
Date / /

A TCP Connection

→ The connection establishment in TCP is called three-way handshaking.

→ The client program issues a request for an active open. A client that wishes to connect to an open server tells its TCP to connect to a particular server. TCP can now start the three-way handshaking process.



Page No.:
Date : / /

* User Datagram Protocol

→ The User Data protocol is a Connectionless, unreliable transport protocol.

→ It does not add anything to the services of IP except for providing process to process communication instead of host to host communication.

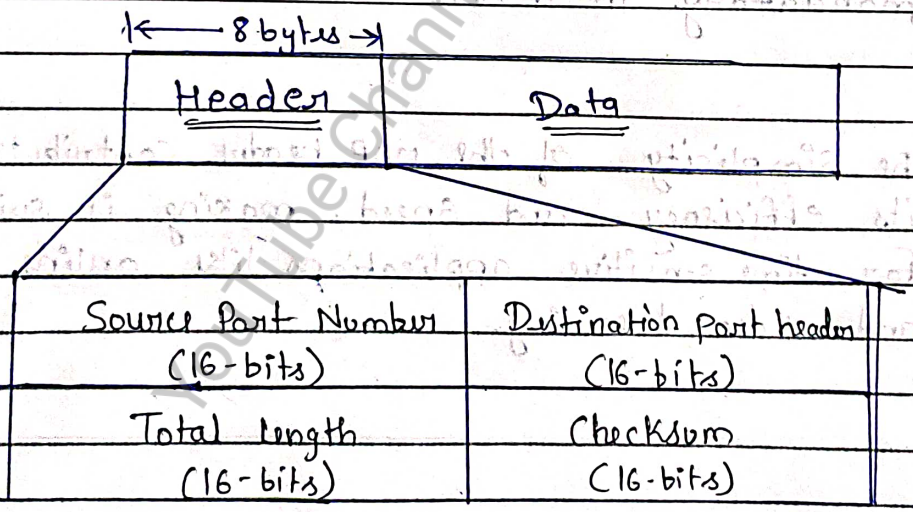
Why to use UDP

→ Low Latency - for real time application. [online Games]

→ Broadcast and Multicast.

→ Data loss is acceptable & Suitable for small packet Exchanges.

* UDP Header [AKTU-2022-23]



Page No.
Date: / /

→ The UDP header is divided into the following four 16-bit fields:

1. Source port: The port number of the sender. This is optional in some cases, but when used it, it helps to receiver to send a reply.

2. Destination Port: The port number of the receiver. This field is essential for directing the packet to the correct application on the destination machine.

3. Length: The length of the entire UDP datagram, including the header + data. mini (8 bytes) to max (65,535 bytes).

4. Checksum: Used for error-checking the header and data. The field is optional in IPV4 but mandatory in IPV6.

→ The simplicity of the UDP header contributes to its efficiency and speed, making it suitable for time sensitive applications like online gaming and video streaming.

Page No.:
Date : / /

[AKTU - 2022-23, 2021-22]

Q. Diff. b/w TCP and UDP

Feature	TCP	UDP
Connection Type	Connection - oriented	Connection - less
Reliability	Reliable (Acknowledge, Retransmission)	Unreliable (no guarantee of delivery)
Flow Control	Yes	No
Congestion Control	Yes	No.
Header Size	Minimum 20 bytes	8 bytes
Error checking	Extensive	Basic
Data Order	Ensures Order	No order guarantee
Connection Establishment	Three - way handshake	None
Use Cases	HTTP / HTTPS, FTP, SMTP, SSH	DNS, VOIP, online gaming, live streaming.

Page No.
Date

* TCP window management System

⇒ Window Management in the context of TCP refers to the process of controlling the flow of data between sender and receiver to ensure efficient and reliable data transmission.

→ It involves managing the amount of data that can be sent before receiving an acknowledgement.

→ This mechanism helps in optimizing network performance & preventing congestion.

→ During the TCP three-way handshake, both the Sender and receiver.
→ The receiver advertises it window size.

Example Scenario:

1. Initial state:
- Receiver advertises a window size of 5000 bytes.
- Sender can send up to 5000 bytes of data without waiting for an acknowledgement.

2. Data Transmission
- Sender sends 5000 bytes.
- Receiver processes data and sends an acknowledgement, updating the window size (3000 bytes).

3. Sliding the Window:

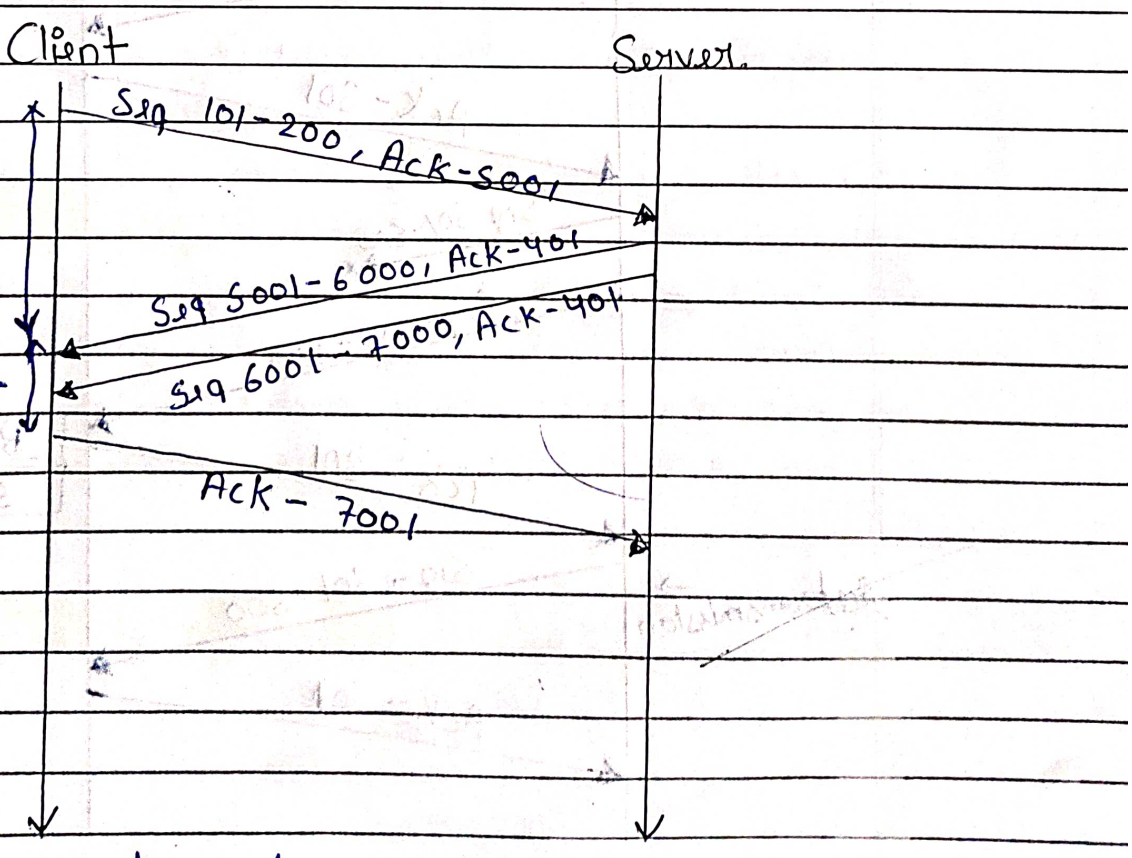
→ Upon receiving the acknowledgement, the sender slides the window forward and sends the next segment of data.

4. Congestion Event:

→ If congestion is detected, the sender reduces the Congestion window size, limiting the data rate until the network stabilizes.

* Flow Control & Retransmission

→ Flow Control is a technique used to prevent the Sender from overwhelming the receiver with too much data quickly & match the rate at which the Sender transmits data which the receiver can process & buffer it.



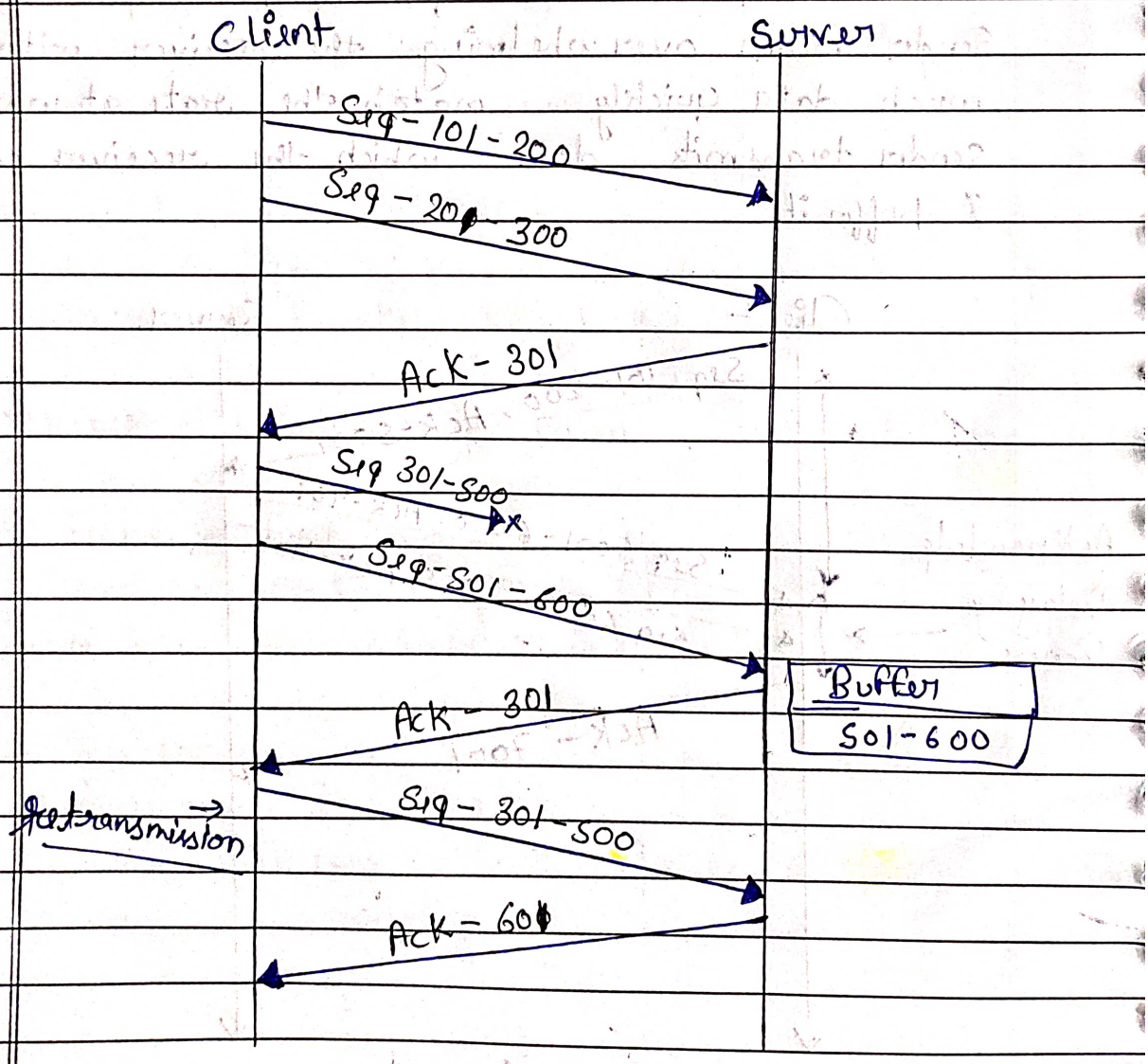
Normal

Page No.
Date: / /

Retransmission is a mechanism to ensure that lost or corrupted packets are resent, maintaining the reliability of TCP connections.

→ If the sender does not receive an ack. for a packet within a specified time, it assumes the segment is lost and retransmit it.

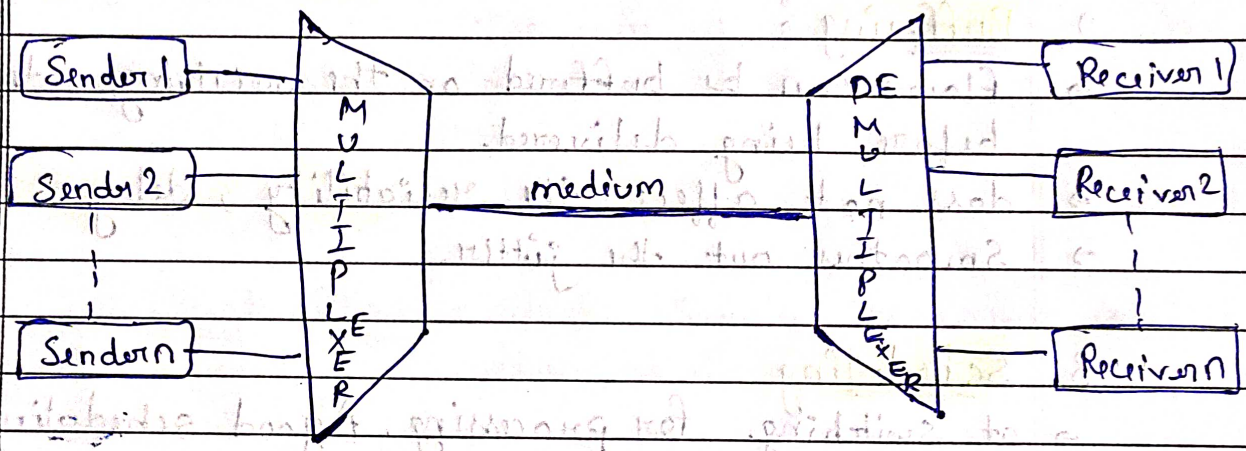
→ Use buffer for storing segments after the same segment lost.



Page No.:
Date: / /

Checkout Unit-1

* **Multiplexing** : It is the process of collecting data from different application processes running on the Sender's end and then gathered data with the header and then transmitting the whole to the receiver. The main purpose of multiplexing is to choose one of the n input lines and transmit it to the output.



Multiplexer Demultiplexer

* **Demultiplexing** : Working of Demultiplexing is just the reverse of the multiplexing process and demultiplexing delivers the segment received from the received from the receiver to the correct process of the application layer.

→ **QoS** → **Quality of Services** → Reliability, Delay, Jitter, Bandwidth.

→ Unit-3

Techniques for improving QoS:

1. **Over Provisioning:**
   - → Increase the capacity of router, Buffer space and bandwidth

2. **Buffering:**
   - → Flows can be buffered on the receiving side before being delivered.
   - → does not affect the reliability, delay
   - → Smoothes out the jitter.

3. **Scheduling**
   - → at switching for processing. A good scheduling technique treats the diff. flows in a fair and appropriate manner.
   - → FIFO and Priority Queuing.

4. **Traffic Shaping**
   - → It is a mechanism to control the amount and the rate of the traffic sent to the network.

   i) Leaky bucket
   ii) Token bucket

Page No.:
Date:

* TCP Congestion Control

→ Congestion occurs if the load offered to any network is more than its capacity.

→ TCP uses a congestion window & a congestion policy that avoid congestion.

Congestion Window - If the network cannot delivery the data as fast as sent by the Sender, it inform to sender to Slow down.

Congestion policy

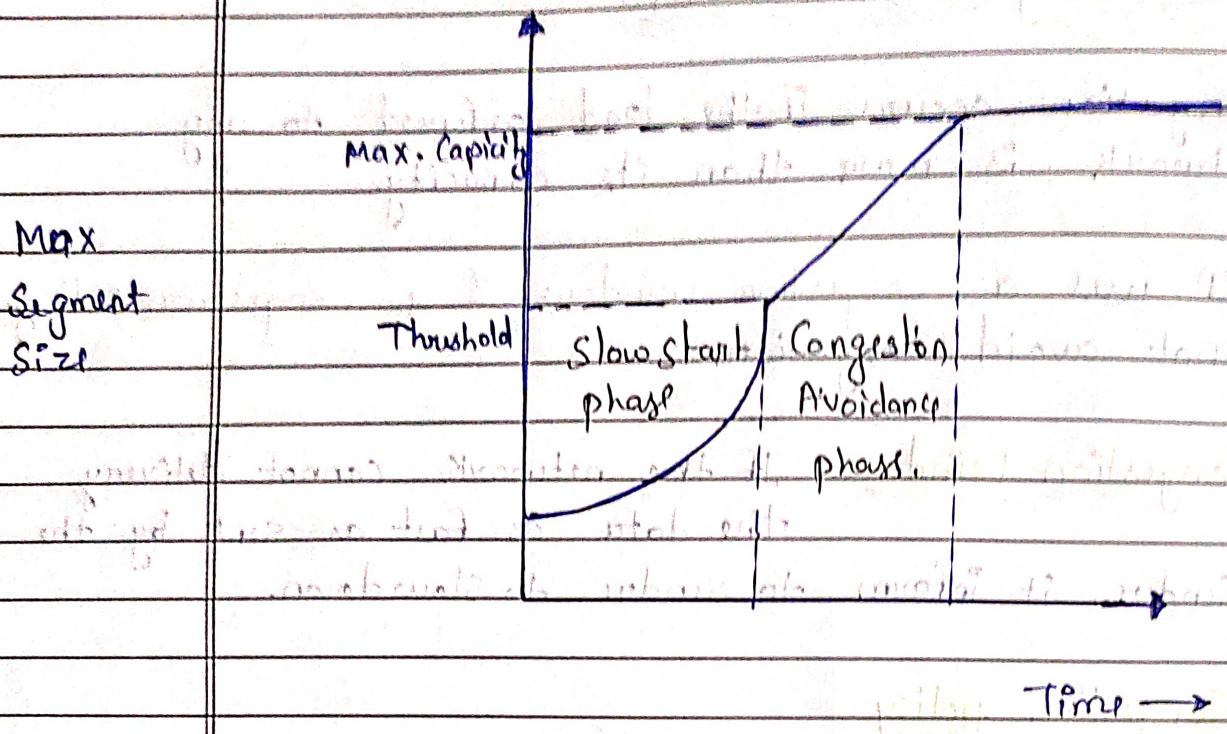
1. Slow Start Phase - Starts slowly increment is exponential to threshold.

2. Cogestion Avoidance phase - After reaching the threshold, increment is by '1'.

3. Congestion Detection phase - Sender goes back to Slow start phase or Congestion avoidance phase.

Case 1 : Retransmission due to Timeout - goes back to Slow start phase.

Case 2 : Retransmission due to 3 Duplicate Acknowledgement - goes back to Congestion avoidance phase.



Unit-4 Completed

COMPUTER NETWORK

Page No.
Date

Unit-5 Application Layer

ONE SHOT + 3 PYQ SOLUTIONS

Topics :-

1. Application layer & its functions.
2. WWW
3. * DNS [2021-22, 22-23, 18-19]
4. HTTP [2018-19]
5. * FTP [2021-22, 22-23]
6. Remote Login Protocol
   TELNET & SSH [2018-19]
7. * Network Management [SNMP] - [2022-23, 18-19]
8. * EMAIL protocol [SNMP, POP3, IMAP]
   → [2021-22, 18-19, 22-23]
9. Data Compression & its Types
10. Cryptography & its Types

* → RSA Algo. with example - [2022-23]

Page No.:
Date:

[AKTU- 2021-22]

* Application Layer

→ It is the top most layer in both the the OSI and TCP/IP models.
→ It provides the interface b/w the application software on a device and the underlying network protocols.
→ It delivers the standard interface that applications can use transmit and obtain info. to communicate with each other over the network.

Functions

→ It determines the comm^n patner to whom data will be transmitted.
→ Spefiy the availability of resources.
→ Interface b/w user applications and the network.
→ This layer provides email services.
→ provides file transfer access and management.

Protocols of the Application layer in OSI model:

1. SMTP - Simple Mail Transfer Protocol
2. HTTP - Hypertext Transfer Protocol
3. FTP - File Transfer Protocol
4. DNS - Domain Name System
5. SNMP - Simple Network management Protocol.
6. TELNET - Telecommunication network.

Multi Atoms

Page No.
Date / /

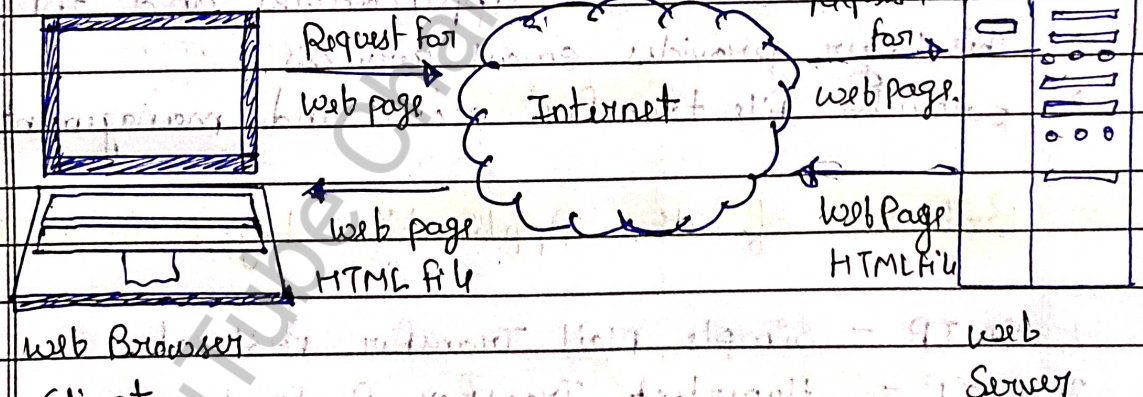
* World Wide Web

→ www, often simply referred to as "the web" is a vast information system, where documents and other web resources are identified by URL (Uniform Resource Locators) and can be accessed via the Internet.

→ invented by Sir Tim Berners-lee in 1989.

Key Components of the www:

1. (Web Pages) 2. (Web Browser) 3. (web Servers)
4. (URL) 5. (HTTP / HTTPS)



Page No.:
Date:

[AKTU-2021-22, 2022-23, 2018-19]

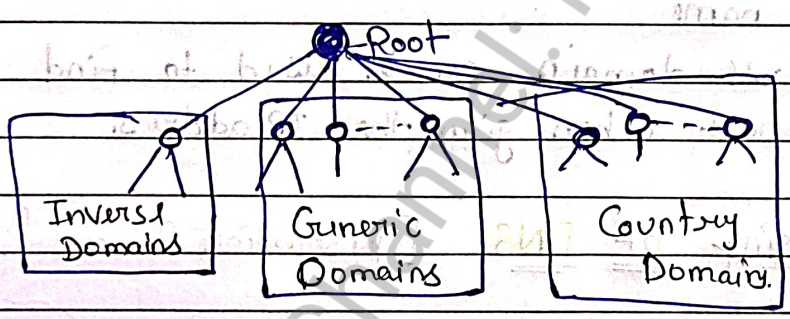
* Domain Name System [DNS]

→ As we know human beings are not comfortable in remembering numbers so to remember IP address of a website or mail account in Internet is difficult.

→ Domain Name System solve this problem. DNS can map a name to an address and conversely an address to a name.

→ However, for a person it is convenient to use names instead of addresses.

→ In the Internet, the domain name space is divided into three sections.



A. Generic Domains

→ In generic domain the registered hosts are define according to their generic behaviours. They are not restricted by country or region.

1) aero - Airlines
2) biz - business
3) com - Commercial
4) coop - Cooperative
5) edu - Education
6) gov - Government
7) info → Info. service
8) int - International org.
9) mil - Military
10) museum - Museums
11) name - personal names
12) net - Network Centers
13) org - Non profit Org.
14) pro - professional org.

Multi Atoms

Page No.
Date: / /

B. Country domains :

→ Country domains are two letters designated for specific country or territory, based on country code.

ex = .us - united state
.in - india. (academic institutes in india use .ac.in - gkte.ac.in)

C. Inverse domains

→ The inverse domain is used for mapping an address to a name

→ inverse domain can be used to find the name of a host when given the IP address.

Working of DNS [Resolution Process]

→ To map an address to a name or a name to an address we use a DNS client known as resolver.

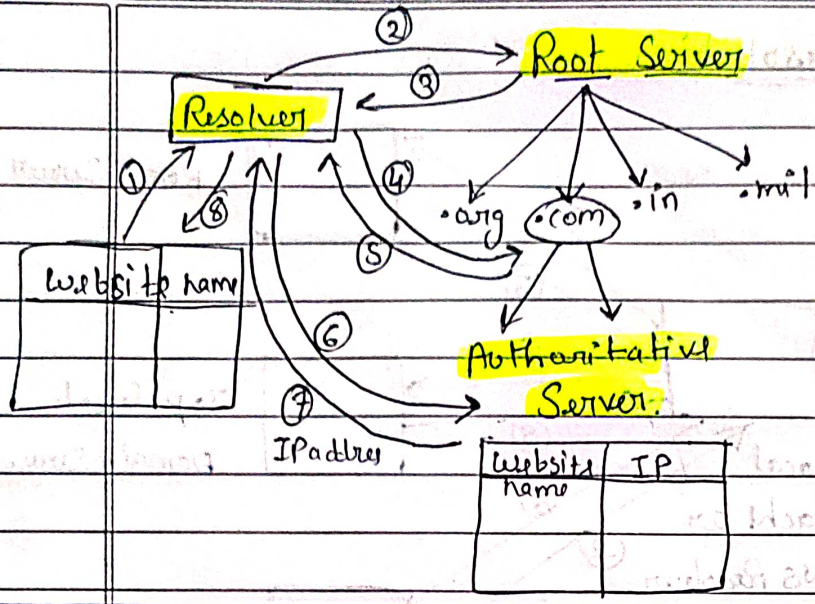
→ The resolver approaches the nearest DNS server with a mapping request.

→ If the server has the info. it provides the resolver with the info.

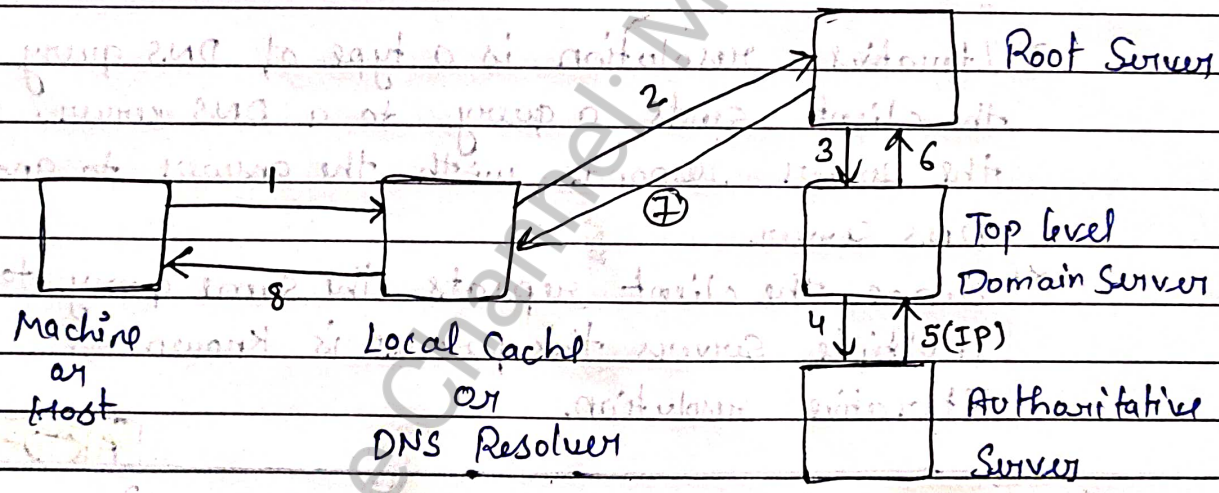
→ After the resolver receives the mapping it interprets the response and delivers the result to the process that requested it.

→ Resolution can be either recursive or iterative.

Page No.:
Date:



A). Recursive Resolution



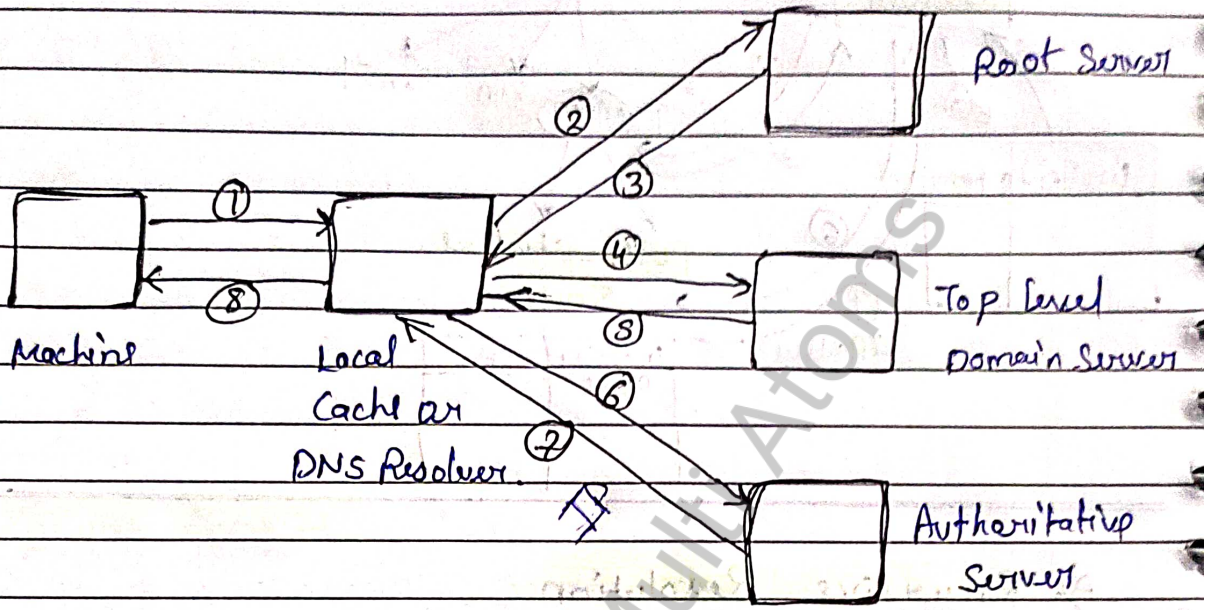
→ First Host check the IP address into Local cache if there is IP found then it responds otherwise it move to root Server.

→ It send query to Top level server and Authoritative Server send IP address to Root Server.

→ Now, query is finally resolved, the response travel back to the requesting client.

Page No.
Date / /

B. **Iterative Resolution**



→ Iterative resolution is a type of DNS query where the client sends a query to a DNS server, and the server responds with the answer to another DNS server.

→ Since the client repeats the same query to multiple servers this process is known as Iterative resolution.

AKTU-2018-19

* **HTTP** (Hyper Text Transfer Protocol)

→ It is a protocol used to access the data on the world wide web (www).

→ Port No. 80.

→ Uses TCP to achieve reliability.

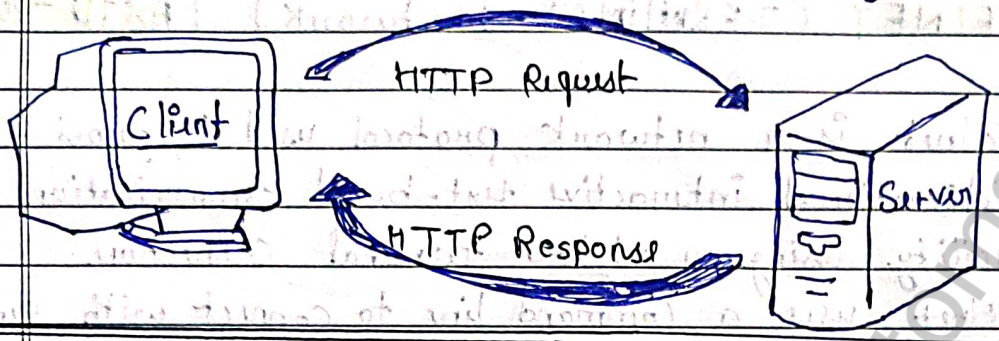
→ Stateless ⇒ It is a stateless protocol. Client & Server know each other only during the current request.

→ Inband Protocol ⇒ generates commands & data from same port.

Multi Atoms

Page No.:
Date:

→ Http 1.0 - non-persistant connection (multiple connection)
→ Http 1.1 - persistant connection (single connection).

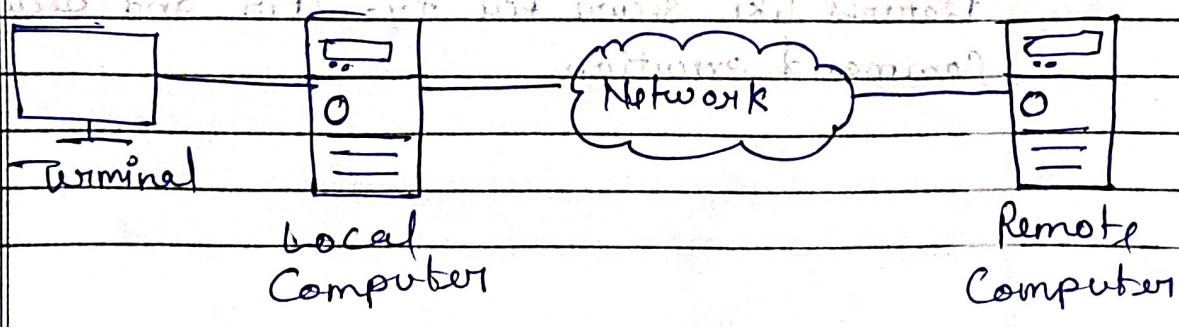


AKTU - 2021-22, 22-23

* **FTP** (File Transfer Protocol)
It is a standard network protocol used for transferring files between a client and a server on a computer network.
→ Reliable Protocol
→ Not Inband : (port no 20) for data and (21) for control commands like user identification, password.
→ Data connection is non-persistent.
→ Control connection is persistent.
→ Stateful (info about data) store.

* Remote Login Protocol

→ Remote Login Protocol, allowing users to access to a remote host/machine and use their terminals connected to the networks.



Multi Atoms

Page No.
Date / /

→ There are two protocols. (① TELNET ② SSH).

1. TELNET (TERMINAL Network) [AKTU - 2018-19]

→ Telnet is a network protocol used to provide a bidirectional interactive text-based communication facility using a virtual terminal connection.
→ Telnet uses a command line to connect with remote computer.
→ Client enters their username and password to access the remote computer.
→ It is not secure protocol because it is unencrypted.
→ Telnet transmits data, including usernames & passwords, in plaintext. This makes it highly vulnerable.
→ Due to its lack security features, Telnet has largely been replaced by more secure protocols for remote access like (SSH.)

2. SSH (Secure Shell).

→ Similar to telnet but it's provides encrypted communication over the network, offering a secure alternative to Telnet.
→ SSH uses port 22 by default and includes features like secure file transfer and secure command execution.

Multi Atoms

Page No.:
Date:

* Network Management

→ It means applications, tools and processes used to ensuring that network operates smoothly, securely and efficiently.

→ Main functions → operate, maintain, administer and secure network infrastructure.

1. SNMP [AKTU - 2022-23] [2018-19]

→ Simple Network Management Protocol is a widely used protocol for managing and monitoring devices on a network.

There are 3 components of SNMP:

i. SNMP Manager: A software system that collects and processes info. from network devices and monitor the network. → also known as Network Management Station (NMS)

2. SNMP agent: A software component that runs on network devices (such as routers, switches) and reports info. to the SNMP manager.

3. Management Information Base (MIB): A database or collection of info. that describes the structure of the network device data.
This info. is organized and stored hierarchically.

Page No.
Date / /

Email Protocols

→ Email protocols are rules and standards that governs the exchange of emails over the Internet.

→ They ensure that emails are sent, received and accessed efficiently and securely.

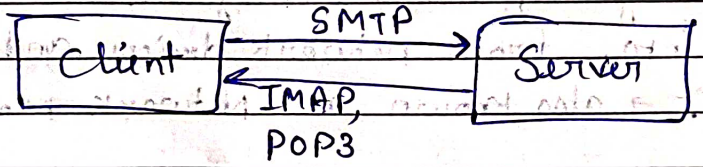
→ The primary email protocols are SMTP, IMAP & POP3.

3PYD [AKTU-2021-22]

1. **SMTP** (Simple Mail Transfer Protocol)

→ SMTP is used to send emails from client to a server or between server.

→ Companies use their SMTP server for marketing, password change and promotional emails



- Port 25 - Default (unencrypted port)
- Port 465 - Encrypted port.
- port 2525 - open at server side.

2. **MIME** (Multipurpose Internet Mail Extension)

→ It is able to send multiple attachments with a single message

→ Images, audio, video files etc.

Page No.:
Date:

→ MIME defines extensions to SMTP to support binary attachments.
→ Unlimited message length.

→ MIME Header → (MIME version, Content Type, Content-Type encoding, Content Id, Content discription).

2. Post Office Protocol 3 (POP3) Version 3.

→ POP3 is used to retrive emails from a server (single client).
→ It downloads emails from the server to the client divice.
→ Once downloaded, emails can be accessed offline.
→ Port 110 : Un-encrypted port.
→ Port 995 : encrypted port.

3. IMAP (Internet Passage Access Protocol).

→ IMAP versions (IMAP, IMAP2, IMAP3, IMAP4 etc).
→ retrive emails from multiple client.
→ have search option
→ It allows to access email without dowanloading them.
→ It allow multiple operations (create, delete, manpolate).
→ port 143 - Unencrypted port.
→ port 993 - Encrypted port.

Multi Atoms

Page No.
Date: / /

[AKTU - 2018-19]

Q. How is TFTP different from FTP?

→ Trivial file Transfer Protocol (TFTP) and file Transfer protocol (FTP) are both protocols used for transferring files b/w devices over a network but they have several key differences in terms of functionality and complexity.

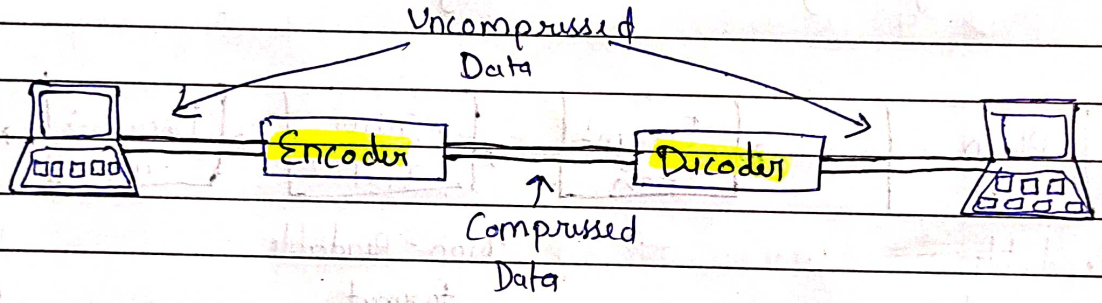
Feature	FTP	TFTP
protocol Type	TCP	UDP
Port no.	20, 21	69
Complexity	High	Low
Security	Basic	None
Authentication	Yes	No
Use Cases	Complex file management, websites.	Simple file transfers, read and write.
performance	Handles large files less fast.	fast, Handles simple file.

Multi Atoms

Page No.:
Date:

* Data Compression

→ It is the way of downloading the compressed form of text, audio and video data using the computer.
→ It is essential for efficient storage and transmission of different type of data.
→ A data compression system consists of an encoder & a decoder.
→ The encoder performs compression of the incoming data and decoder is used for decompression and reconstruction.



Types of compression :

1. **Lossless** Compression

→ In lossless comparession, the redundant information contained in the data is removed.
→ There is no loss of information.
→ has lower comparision ratio.

2. **Lossy** Compression

→ there is a loss of Information in a controlled manner.
→ not completely reversible
→ but has higher comparission.

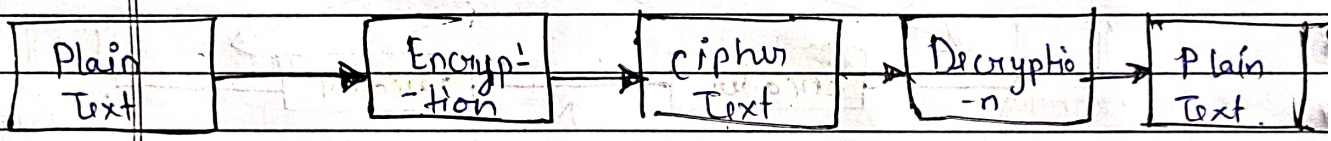
Multi Atoms

Page No.
Date / /

* Cryptography

→ It is a technique of securing communication by converting plain text into ciphertext. It involves various algorithms and protocols to ensure data confidentiality, integrity, authentication and non-repudiation.

→ "Crypt" means "hidden"
→ "graphy" means "writing"



Types of Cryptography

1. Symmetrical Encryption

→ This is the simplest kind of encryption that involves only one secret key to cipher and decipher information.

→ It uses a secret key that can either be a number, a word or a string of random letters. It is a blended with the plain text of a message to change the content in a particular way.

→ The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages.

Page No.:
Date:

→ The most popular Symmetric key cryptography systems are Data Encryption System (DES) and Advanced Encryption System (AES)

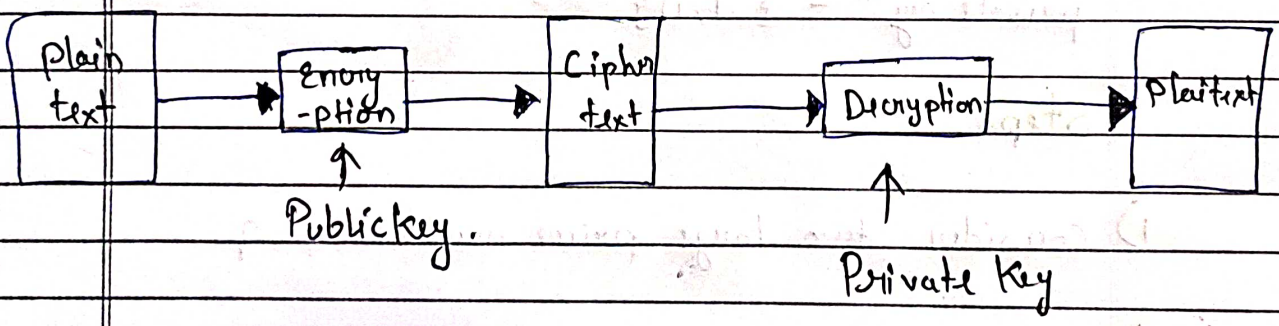
2. Asymmetric key Cryptography

→ A pair of keys is used to encrypt and decrypt info.

→ A receiver's public key is used for encryption and a receiver's private key is used for decryption.

→ You publish your public key to the world while keeping your private key secret.

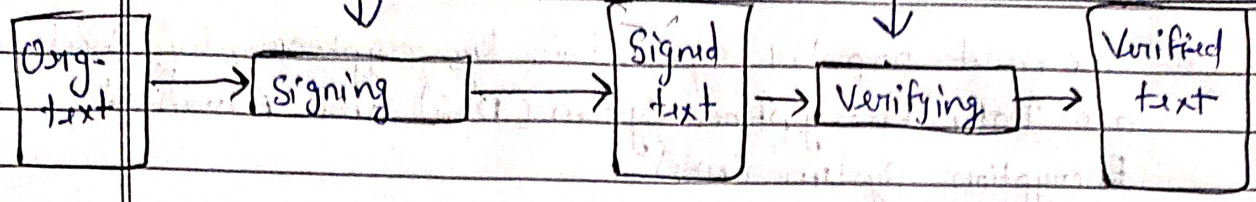
→ The most popular asymmetric key cryptography algorithm is the RSA algorithm. (Rivest - Shamir - Adleman)



3. Digital Signature

→ The signature is encrypted using the private key and decrypted with the public key.

→ More secure than handwritten signature.



[AKTU-2022-23]

* RSA Algorithm

→ RSA (Rivest - Shamir - Adleman) is an algorithm used to encrypt & decrypt messages.

⇒ It is an asymmetric cryptography algo.

Encryption – $C = P^e \bmod n$

Decryption – $P = C^d \bmod n$

public key = $\{e, n\}$
private key = $\{d, n\}$

Steps.

1) Consider two large prime numbers p, q.
2) Calculate $n = p \times q$
3) $\phi(n) = (p-1)(q-1)$ — $\phi(n)$ → Euler's function
4) choose a small number e, co-prime to $\phi(n)$
   $\gcd(e, \phi(n)) = 1$ & $1 < e < \phi(n)$
5) Find d, such that $d \times e \bmod \phi(n) = 1$

Page No.:
Date:

Example =

1) Two prime numbers $p = 3$, $q = 5$

2) $n = p \times q = 3 \times 5 = 15$ $\boxed{n = 15}$

3) $\phi(n) = (p-1)(q-1) = (3-1)(5-1) = 8$ $\boxed{\phi(n) = 8}$

4) Assume e such that $\gcd(e, \phi(n)) = 1$ &

$1 < e < \phi(n)$

$\boxed{e = 3}$

5) find d $\quad d \times e \bmod \phi(n) = 1$

$d \times 3 \bmod 8 = 1$

Let $d = 3$

$3 \times 3 \bmod 8 = 1$

$9 \bmod 8 = 1$

$\boxed{1 = 1}$

$\boxed{d = 3}$

1) public key = $\{e, n\} = \{3, 15\}$
2) private key = $\{d, n\} = \{3, 15\}$

Let Data (P) = 8 = plain text.

Encryption $C = P^e \bmod n = 8^3 \bmod 15 = 2$ $\boxed{C = 2}$

$(512 \bmod 15)$

Decryption $P = C^d \bmod n = 2^3 \bmod 15 = 8$ $\boxed{P = 8}$

$(8 \bmod 15)$