Steganography - hides the msg

port 20 & 21

Page No.
Date

Network layer
→ to add logical address
IP addr for source to destination
→ Router / level 3 switch / Routing algo.

Transport layer
→ responsible for process-to-process delivery of data. (use of socket adr)
→ Perform Segmentation Not
↳ segment (msg.)

Process is identified using port No.

System ⟹ FTP → port - 20 & 21
Data Transfer & Control

No.s are for process comm^n
Name & for humans.

Port addr ⟹ Socket address
↙ IP add ↘ PN

Physical, logical, Socket address

segment → datagrams / Packets

Stream Control Transfer Protocol
SCTP → UDP
↘ TCP

$[D_1 - D_2 - D_3 - D_4]$
segment

Page No.
Date

segments of
(collection of datagrams)
→ Reassembly of msg.

Circuit switching → Linear Comm^
(wired)
Packet switching → Wireless

→ Connection control
→ Delivering to the system
→ error control → flow control
Conn^ Oriented Service (Ack req.)
- Establish
- Transfer
- Terminate

Conn^ less service (No ack.)

Session layer
→ Dialog Control
→ Checkpoints

Presentation layer
→ syntax, semantics } Translation
→ Compression
→ Encryption. (pro jumble data)

Application layer
→ All processes related to different appl^

IP addr → Physical addr → PA → IP addr

Page No.
Date

Encapsulation - adding Headers & Trailers to data
- senders side

Headers → source addr
→ destination addr

Trailer

decapsulation - removing Header & Trailer
- Receivers side

—— x o x ——

link - Network used to connect computers & connecting devices (Ex - Routers)

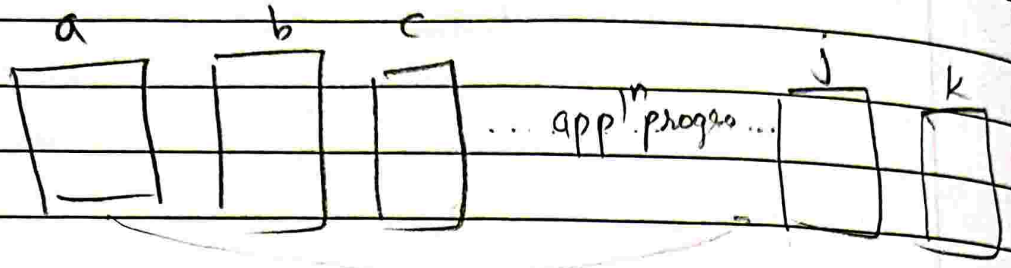
Physical layer → Node (hop-by-hop to Node delivery)
→ stream of bits are being moved.

Data link layer → type of delivery (hop by hop)
→ frames [D] [Header]
→ Router connects two networks

TTL - Time to Live
128 hops

Page No.
Date

Port No :- address of an appl" Program



Sender → Receiver

Data

Port No :- | a | j | Data |

| A | P | a | j | Data |

Physical Address

H2

Internet

Port No ⇒ Port Address ⇒ Transport layer

TL → Socket Addr

IP P. No.

Datalink layer → Physical Addr.

Page No.
Date

Application Specific Address
→ works at Appl^n layer
→ Uses format of URL.
Name of protocol : // address of file locater
from www followed by
domain name
Ex : https : // www . gmail . com
→ Can also be in format of email
. . < > @ — . com

Q1. Match the following to one or more layers of the OSI and TCP/IP Model

(1) Reliable process to
Process msg delivery

OSI : Layer Name : ~~Transport~~
TCP : layer Name Transport

(2)

(3) Defines frames DLL

(4) Provides user services such as email & File Transfer Appl^n

(5) Mechanical, Electrical & Functional Physical interface

(6) Transmission of bit stream across physical medium Physical

(7) Error correction & Retransmission DLL as trailer bits

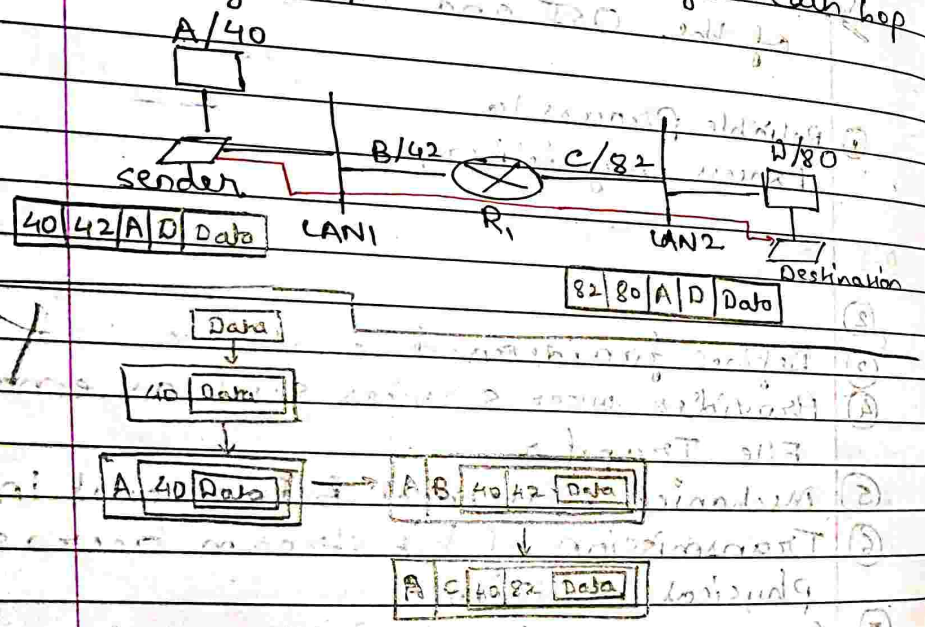
(8) Format & Code Conversion services Presentation

(9) Establishes, manages & terminates session session

(10) Provides independence from differences in Data representation — Presentation

(11) Login / Logout procedures — Session

Q2 As shown in the following fig computer A sends a msg to computer B via Lan1, Router R, & Lan2. Show the content of the packet and frames at the network and DLL for each hop interface.



Q3 Using the above fig assume that, the comm^n is bet^n a process running at comp. A with Port Address i and a process running at comp. D with Port Address j. Show the content of packets and frames at Network, Datalink and Transport layer for each hop.

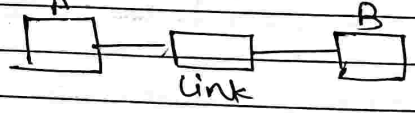
40	42	A	D	i	j	Data

82	80	A	D	i	j	Data

Q4 Suppose a comp. sends a frame to another computer on a bus topology LAN. The physical destination addr. of the frame is corrupted during the transmission. What happens to the frame? How can the sender be informed about the situation

frame gets discard & inform source to retransfer

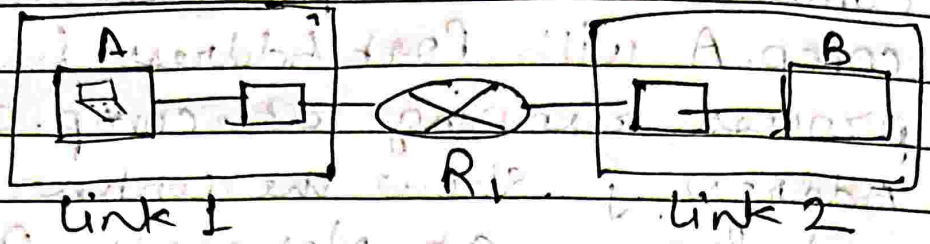
Q6 Show the communication at the appl^n layer for the simple private internet in fig



Q 8 Comp. betⁿ TCP/IP and OSI Model

Page No.
Date

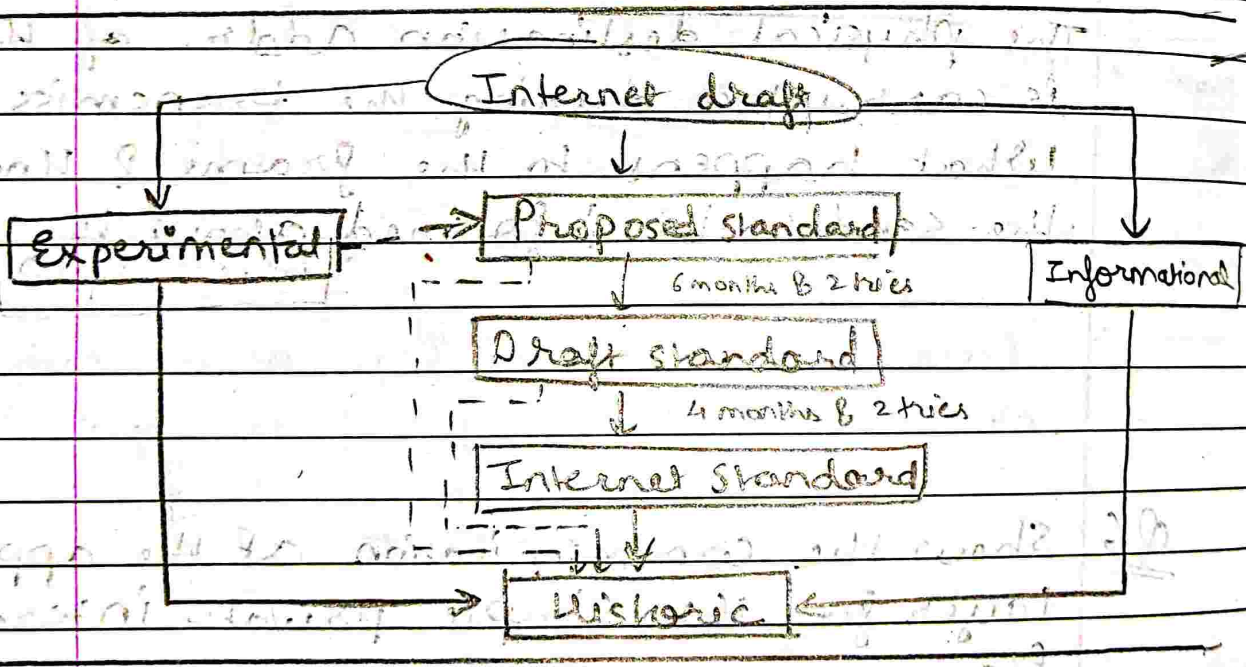
Q 7 Show the commⁿ arr



Internet Standard (document) ~~Internet draft~~

→ defined as a specification used by users to use the internet

→ known as RFC (Request for comment)



Maturity levels of RFC

Proposed → demonstrate successful tries

Historic → keeps info for general use.

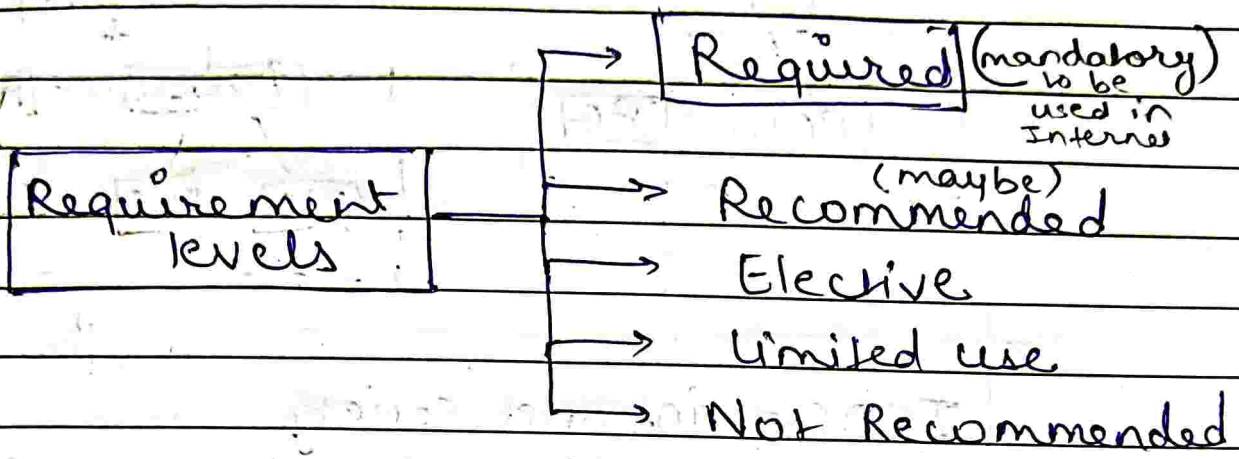
Informational → Manual kinda

Page No.
Date 6 | 2 | 23

following fig shows the various majority levels of an RFC.

→

~~Internet~~ RFC is classified into 5 Requirement level (RFC Tags)

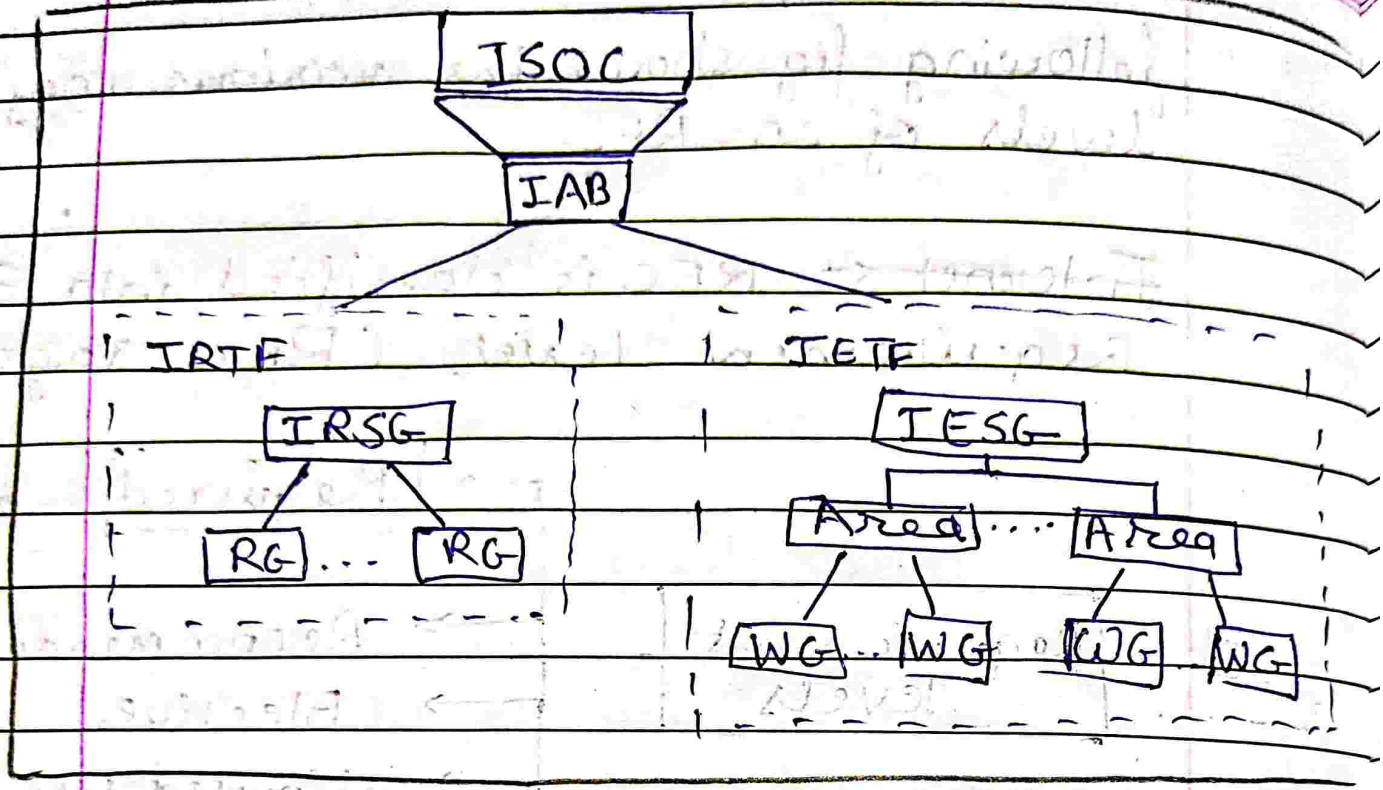


Required → IP & ICMP Protocol
Internet control Management
Recommended → FTP & TELNET
Elective → Not req. not recommended System uses it
Limited use → experimental RFCs
Not Recommended → Historic RFC.

Internet Administration

following fig. shows dig of Int Adm

- Various Grps. that coordinate internet issues and growth & development.



ISOC - internet society
IAB - Internet Architecture Board
IETF - Internet Engineering Task Force
IRTF - -11- Research Task Force
IESG - Int. Eng. Steering Group.
IRSG - -11- Research -11-
RG - Research Grp
WG - Working grp

LAN Standards.

- IEEE → Wired
- FDDI
- ATM LAN
- Wireless LAN

DLL PL → DLL & PL underlying technologies

Mux - many to one
Demux - vice versa

Page No.
Date

IEEE 802 Std.
- Intercomm^n bet^n the equipments manufactured by diff. Manufacturers

Underlying Techno. under Wired LAN
→ IEEE 802.3 std. (Ethernet Std.)

DLL PL → LLC (logical link control sublayer)
→ MAC (Media access control)
- Performs task of mux / Demux
- Adds frame no.
- Adds checksum bit

Ethernet LAN → Ethernet Frame (IEEE 802.3 EF structure)

Preamble	SFD	Destination addr	Source addr	Length or Type	Data & Padding	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes		4 bytes
physical layer header		Header				Trailer

Preamble: 56 bits of alternating 1s & 0s → synchronize the I/p timing to the receiver (receiver ko bahana frame aa rhi hai)

SFD: Start Frame delimiter, flag (10101011) 8 bits

In IEEE, the bit stream is converted using Manchester Encoding signal (101010....10) to signal for receiver.

FRAME → DLL → Physical Addr.

Page No.
Date

- Preamble alert krti hai
- SFD (frame pohoch chuki hai) kaise ?? bit stream k end-11 wale pattern se.

MAC addr structure

OR

- Destination Addr (6 bytes) — Physical addr
  12 Hexadecimal = 48 bits

Format : $d_1d_2 : d_3d_4 : d_5d_6 : d_7d_8 : d_9d_{10} : d_{11}d_{12}$

4 bit + 4 bit
1 byte.

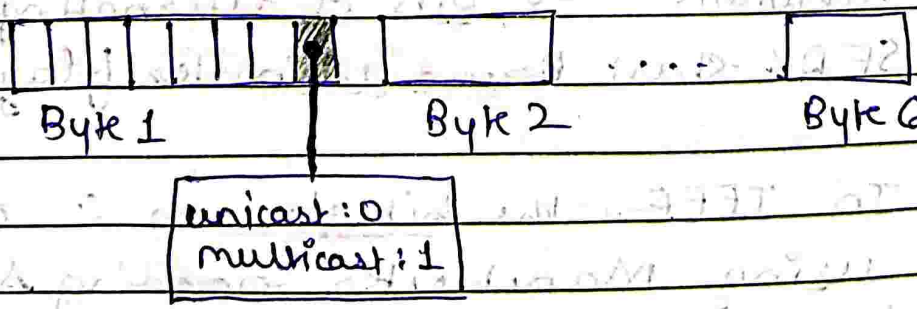
3 bytes = 24 bits
ID no. of the manufacturer (Manuf. kon hai)

3 bytes = 24 bits
Addr provided by the manufacturer (Device ka addr.)

MAC addr → NIC (Network Interface card)

Unicast / Multicast / Broadcast MAC addr.

Unicast → last bit 0. (LSB = 0)
multicast → last bit 1 (LSB = 1)



when all 48 bits are 1s or Fs then it is broadcast Addr.

Page No.
Date

Q. Identify the type of the given Destination Mac Addr.

① 4A : 30 : 10 : 21 : 10 : 1A

4A → 0100 1010
4 bits 4 bits

LSB = 0, Thus Unicast

② 47 : 20 : 10 : 3F : 2E : EE

47 → 0100 0111

LSB = 1, Thus Multicast

③ FF : FF : FF : FF : FF : FF

Broadcast :

Q. Solve Show how the address 47:20:1B:2E:08:EE is sent out of line

Soln The address is sent left to right, byte by byte; for each byte, it is sent right-to-left, bit by bit as shown below

47 → 01000111

Sent R to L matlab mirror image

11100010

Page No.
Date

Ans: 11100010 00000100 11011000 01110100 00010000 01110111

* Length or Type

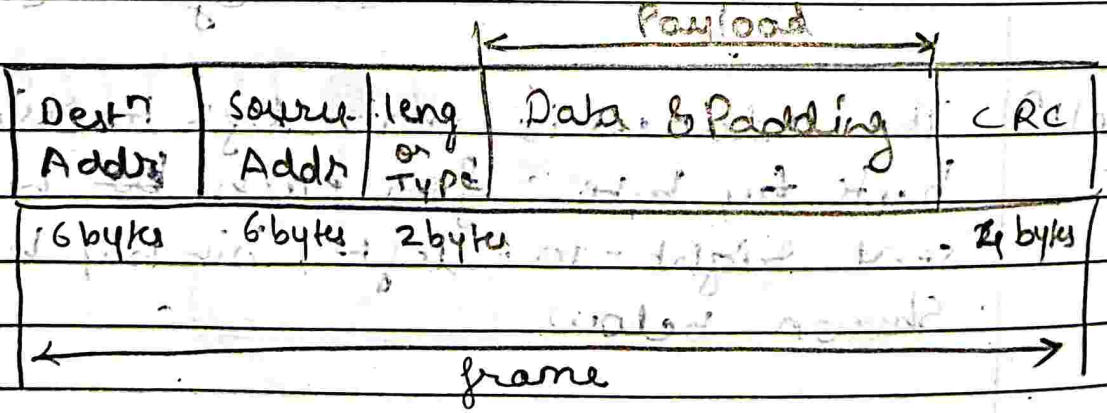
In this field, it represents how many (no. of byts) byts of data present in the frame.

* Data & Padding

Minimum payload lenth : 46 byts
Max payload length : 1500 byts

Minimum frame length : 512 bits or 64 byte
Max —11— : 12144 bits or 1518 byts

If: Data 10 byte + 36 byte Padding



Headers + Trailers = 18 bytes

Page No.
Date

64 frame = 46 payload + 18 HBT

Assignment

Q. An Ethernet MAC sublayer receives 42 bytes of data from the LLC sublayer. How many bytes of padding must be added to the data.

Network → LLC

Q An ethernet MAC sublayer receives 1510 byte of data from the LLC layer can the data be encapsulated in 1 frame? If not how many frames need to be sent? What is the size of data in each frame?

No, 2 frames, 1 - 1500 byte

2 - 10 byte data + 36 byte Padding

As the max. payload length of a frame is 1500 bytes

Thus, we cannot send a data of 1510 bytes using single frame

We would require 2 frames

1st frame contain payload length of 1500 byte of data

2nd frame contain payload length of 46 bytes of 10 byte data & 36 bytes padding.

+ figures.

Ethernet Evolution

- Standard Ethernet — 10 Mbps
- Fast Ethernet — 100 Mbps (FDDI Protocol)
- Gigabit Ethernet — 1 Gbps
- Ten-Gigabit Ethernet — 10 Gbps

CSMA - Carrier sense Multiple Access protocol

- Ethernet
- supports bus & star topology
- wherever transmission medium is shared

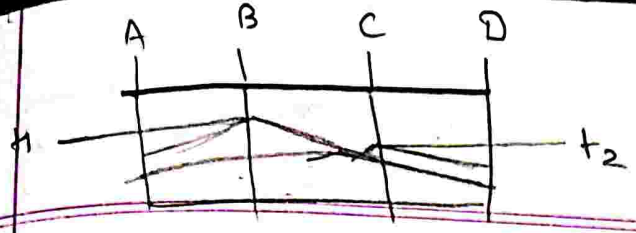
Carrier → Transmission medium for frames (Ethernet use kare vo is liye)

- Ex :- People using single Road.

Abort signal due to collision ← CSMA/CD → wired LAN

CSMA/CA → wireless LAN

Propagation → time req. to send single bit



B starts at time t_1
C starts at time t_2

Page No.
Date

t_1 pe B ka laga carrier idle hai kyuki uske pass koi bit nhi aarhi hai.

CSMA/CD

- JAM signal should be sent by system who 1st senses the collision

Persistent

Non-persistent

p-persistent

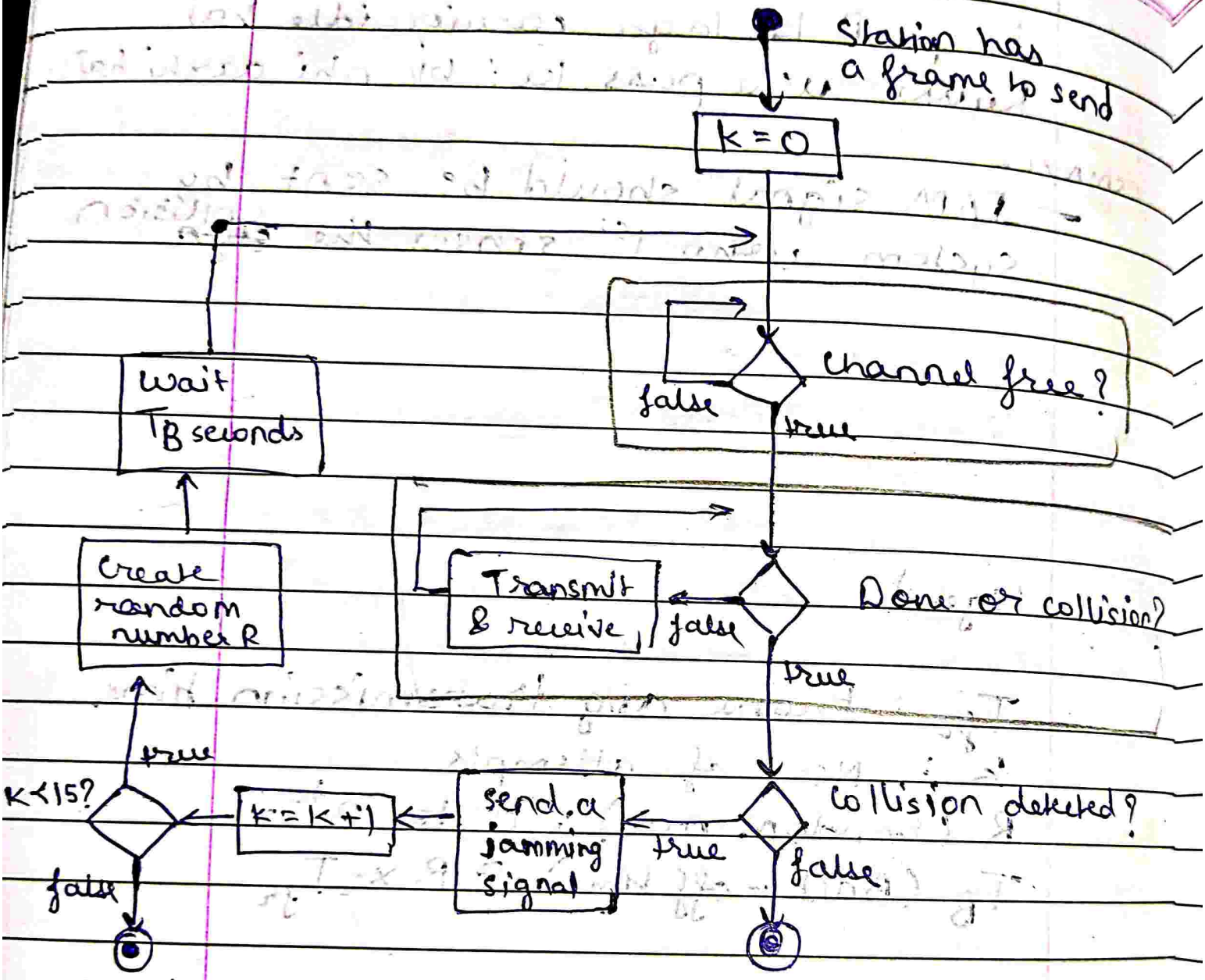
Legend

T_{fr} : Frame avg transmission time.

k : No. of attempts

R (random no.) : 0 to $2^k - 1$

T_B (Back-off time) = $R \times T_{fr}$



Q In the standard Ethernet, if the maximum propagation time is 25.6 μsec, what is the min size of the frame

Page No.
Date

Q The datarate of 10 Base 5 is 10 Mbps. How long does it take to create the smallest frame? Show your calculation.

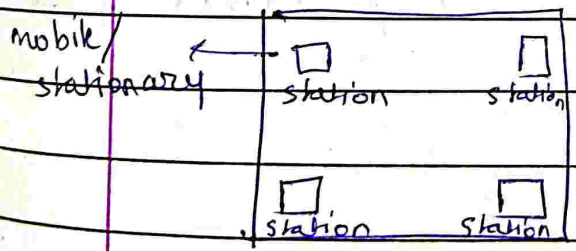
Q Compare and Contrast CSMA/CD and CSMA/CA

Standard Ethernet (10 Mbps) — data rate supported

Characteristic	10Base5	10Base2	10Base-T	10Base-F
Medium				
Max length	500m	185m	100m	2000m

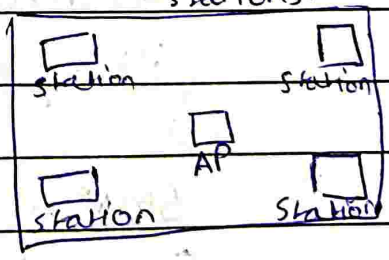
① IEEE 802.11 (Wireless LAN)
② Bluetooth

BSS: Basic service Set



Adhoc Network
(BSS without An AP)

AP: Access point
- Provides permission to stations.



Infrastructure
(BSS with an AP)

Page No.
Date

frame to frame

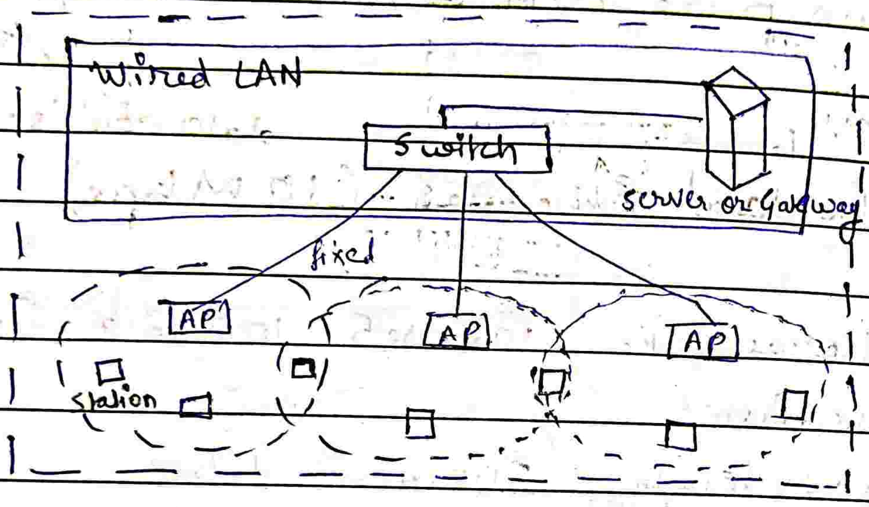
differnce ...

does'nt have an AP	Has An AP

Extended service set

ESS

distributed system



- Extension of BSS of infrastructure
- 2 types of station - fixed & mobile
- AP connected to wired
- If the station betn different BSS want to communicate it is through wired system using APs

Station Types

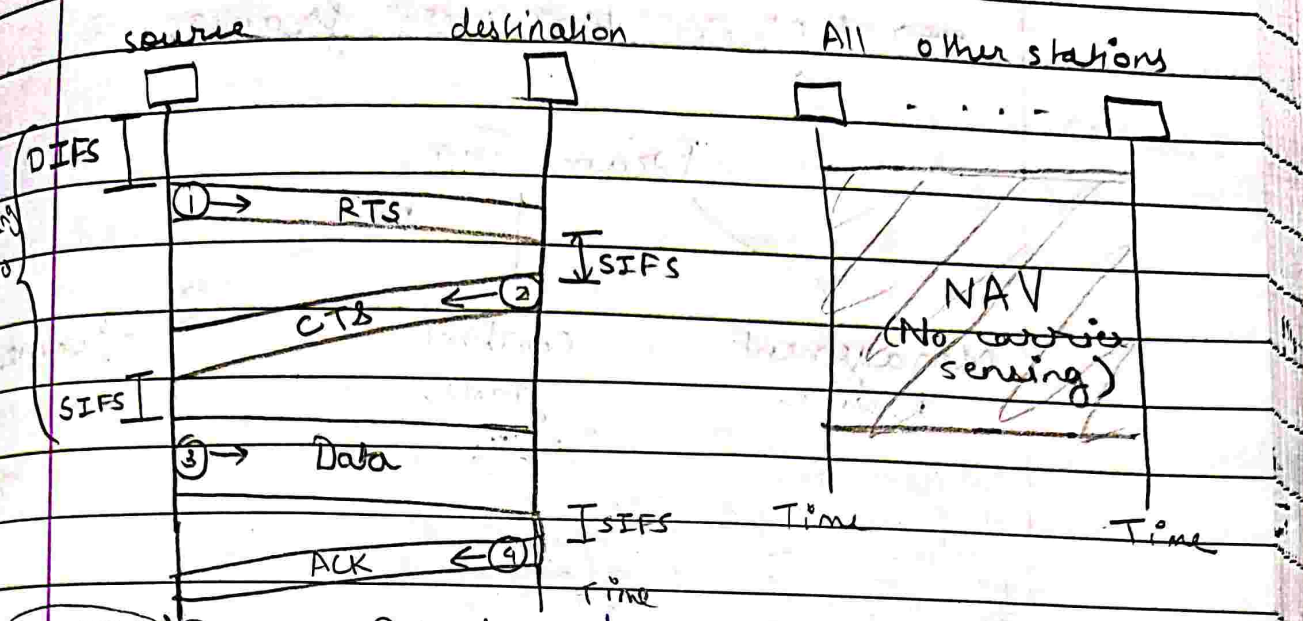
① No. transition — Either stationary or move inside a single BSS

② BSS Transition — move from one BSS to another but within a single ESS

③ ESS - transition mobility — station within 2 different ESS are communicating

* communication bet^n stations in IEEE 802.11 using CSMA/CA

CSMA/CA and NAV



DIFS - Distributed Interframe space

RTS - Request to send frame

SIFS - Short Interframe Space

CTS - clear to send

NAV - Network Allocation vector

following fig shows ~~IEEE 802~~ IEEE 802.11 frame structure

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 byte	6 bytes	0 to 2312 bytes	4 bytes
FC	D	Addr1	Addr2	Addr3	SC	Addr4	Frame body	FCS

Protocol Version	Type	subType	To DS	from DS	More flag	Retry	PWR mgt	More data	WEP	Rsvd
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

For control frames the value of type field is 01;

subtype	Meaning
1011	RTS
1100	CTS
1101	ACK

Values of subfields in control frames

Page No.
Date

Frame Control

→ defines type of frame.

Frame Types

Management Frame
- Collision avoid
- used for initial comm^n bet^n stations and the APs

control frame
- RTS & CTS, ACK
- used for accessing the channel and ack frames

Data frame
- carrying data and control info

CSMA/CA & NAV

→ IEEE 802.11

→ RTS

→ CTS

→ Data

→ Ack

↳ Duration / Time

Control frame Structures

RTS

2 bytes	2 bytes	6 bytes	6 bytes	4 bytes
FC	D	Addr 1	Addr 2	FCS

CTS & ACK

2 bytes	2 bytes	6 bytes	4 bytes
FC	D	Addr 1	FCS

Page No.
Date

Subfields in FC field

Field	Meaning
Version	→ Current version is 0
Type	→ Type of info: management (00) control (01) or data (10)
Subtype	of each type (control frames)
To DS	→ defined later (Destination source)
From DS	→ defined later
More flag	→ when set to 1, means more fragments
Retry	→ When set to 1, means (collision k liye) retransmitted frame
Pwr mgt	→ when set to 1, means station is in power management mode
More data	→ when set to 1, means station has more data to send
WEP	→ Wired Equivalent privacy (encryption implemented)
Rsvd	→ Reserved.

Addresses

Addr 1 → addr of next device
Addr 2 → addr of previous device
Addr 3 → addr of final destination station
Addr 4 → addr of original source station

To DS	From DS	Adr 1	Addr 2	Addr 3	Addr 4
0	0	dest	Source	BSS ID	N/A
0	1	dest	sending AP	Source	N/A
1	1	Receiving AP	source	Destination	N/A
1	1	Receiving AP	sending AP	Destination	Source

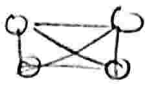
D → Duration → to be mentioned in RTS or CTS
- duration of transmission that is used to set the value of NAV
- defines ID... of frame
- used by control frames

Sequence control
- the seq. no. of the frame to be used in flow control

FC body
- contains actual

FCS
- Error correction code

15/2/24

Mesh → WAN
Pt to Pt.  no. of connections $^nC_2$ __/__/__

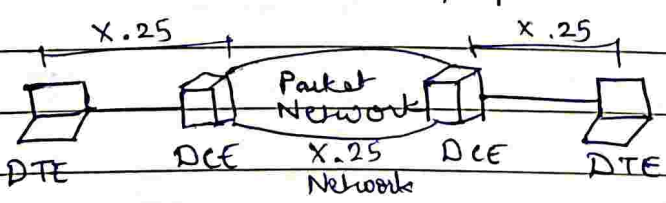
Q8 Use table to compare and contrast fields in IEEE 802.3 and 802.11

Fields	Field size IEEE 802.3	Field size IEEE 802.11
Destination Addr	6	-
Source Addr	6	-
Address 1	-	6
Address 2	-	6
Address 3	-	6
Address 4	-	6
FC	-	2
D/ID	-	2
SC	-	2
PDU length	-	-
Data & Padding	64 bit padding 46 to 1500	-
Frame body		0 to 2312
FCS (CRC)	4	4

X.25 SWITCHED WAN

- WAN K Routers are level 3 switches
- Pt to Pt → unicast → switch
- WAN - internet → Network layer → packets ↓
- Packet switched Network ← Packet switching
- Pt. to Pt services — connection oriented services (keyek pt. to pt.)

Data communication Equipment (DCE) → X.25 ka switch
DTE → Data terminal equipment (systems)



__/__/__

X.25 layer Mapping with OSI Model

OSI		X.25
Appl^n		
presentation		
session		
Transport		
Network	⟷	Packet (PLP)
DataLink	⟷	frame (LAPB)
Physical	⟷	Physical X.21 → ANSI Standard
		X.25

3 layers

Physical → bits to transmit krna
→ sequence me
→ maintain synchronization using X.21

LAPB → Link Access Procedure Balance Protocol
→ part of Bit oriented type of protocol
→ Part of HDLC protocol (High level Datalink control)

PLP → Packet level protocol for packet transfering

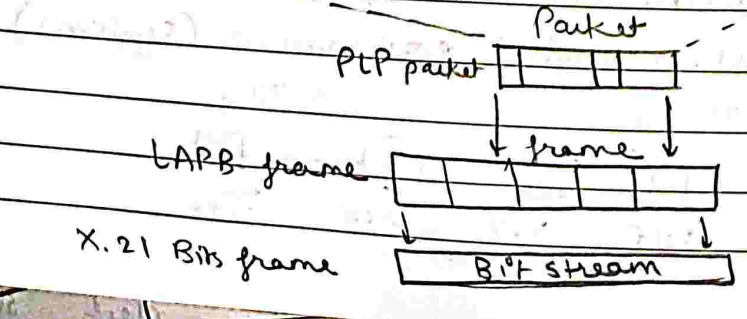
X.25 supports flow control and error control mechanism

X.25 frame structure

Field length in bits

8	8	8	Varies	16	8
Flag	Address	control	Data	FCS	Flag
7E					7E

0X7E
01111110



- from the above fig, the user data of variable size is used to form a packet by PLP layer
- In this packet format the flag field at the start and end of packet indicates the start and position of the packet. the value is 7E
- The next field is an Address field of 8 bits that defines the type of frame. In this field it consist of two binary values used for communication between DCE and DTE following shows the table.

Binary Values	Command	Response (Ack)
0000 0001	DTE → DCE	DCE → DTE
0000 0011	DCE → DTE	DTE → DCE

- The next field is the control field that represents command and response frame as mentioned in the address field. It also indicates the type of frame used such as I - frame (info frame or data fr
S - frame (supervisory frame / Response frame)
U - frame (unnumbered frame) (comand / control fram

- FCS → frame control sequence (checksum bit)

X.25 ⇒ Packet switched N/w
- COS → Estab
- Data
- Terminate
- uses concept of virtual circuit.

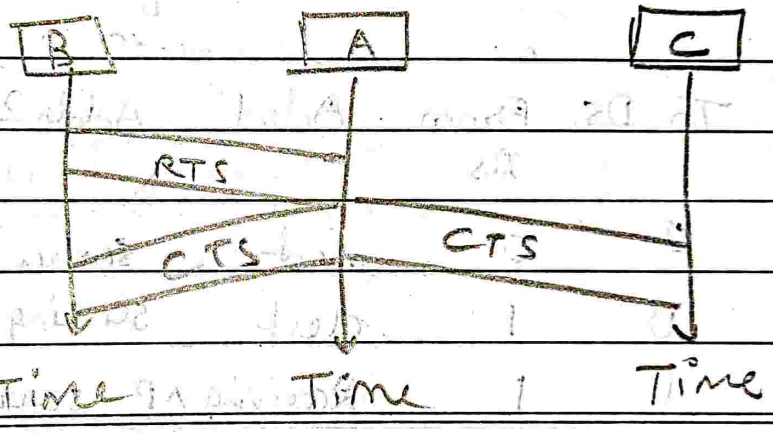
Adv. & Drawbacks of X.25.

Hidden and Exposed Station Problem

↳ solve collision problem

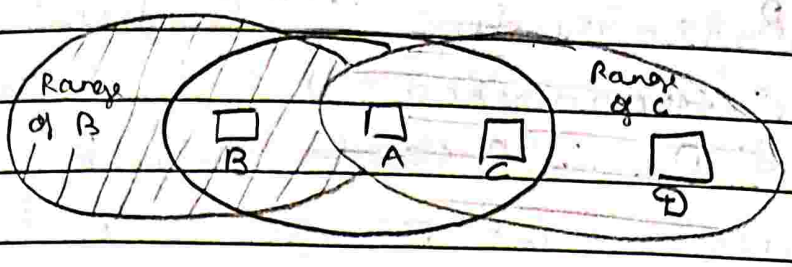
— The CTS frame in CSMA/CA handshake can prevent collision for from a hidden station.

Use of handshaking to prevent hidden station problem:



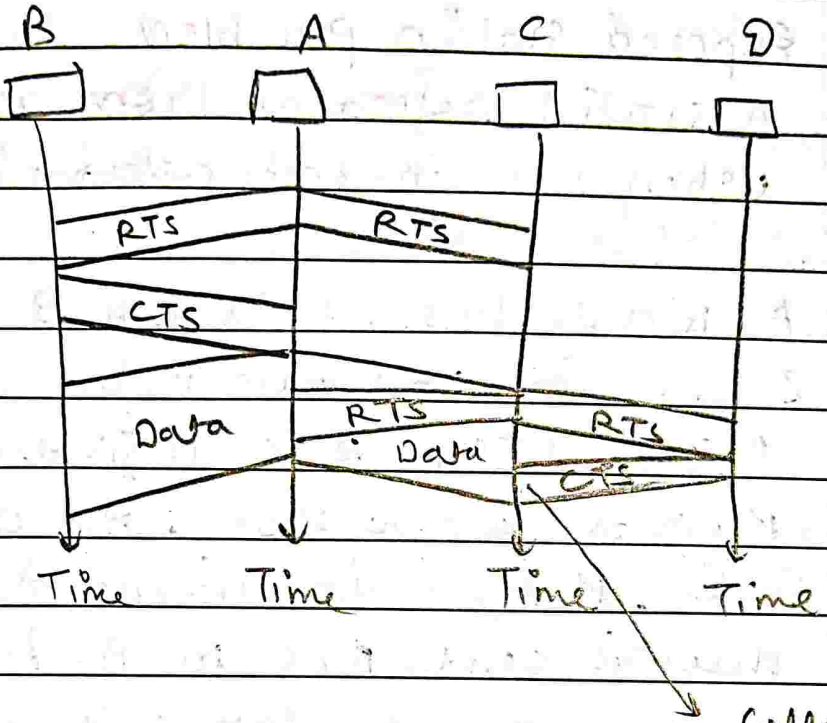
Page No.
Date

Exposed station problem



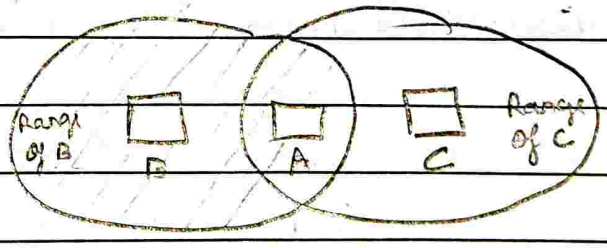
C is exposed to transmission from A to B

Use of handshaking in exposed station problem



Following fig shows the hidden station problem

B & C are hidden from each other w.r.t A



Left oval represents Range of B, stations within that range can listen only signals of B
A is in b/w range of B & C, ∴ it can hear what B & C says. Thus collision may happen.
To reduce the collision in CSMA/CA is used.

B is sending RTS frame
C cannot hear it as it is out of range of B. ∴ A sends CTS to B & C as it lies within range of B & C ....

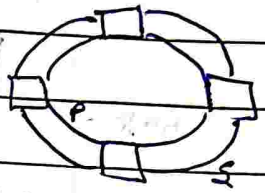
Exposed station problem
- A station refrains from using a channel when it is in fact available.

A wants to send data to B
& C wants send data to D
A sends RTS to B, C it finds channel empty
B sends clear to send, A sends Data to B & C, But C doesn't need that does mean it sends RTS to A & D & as D is unaware of data sending of A it send CTS to C and that CTS send by D and data being sent by A to C collides thus occuring collision in exposi...

27/7/24

Page No.
Date

Fibre distributed data interface (FDDI)
- aka Token Ring N/w
- Ring N/w is made using fibre optical cable
- Multimode fibre optic cable
- Consist of 2 Rings
  - (1) Primary Ring
  - (2) secondary Ring



- either clockwise / anticlockwise
- both rings travel in opposite dir^
- costly
- used as backbone N/w
- supports 1000 station at a time
- covers 200 km approx
- Stations connected in FDDI called as MAU → media auess unit
- If stations connected to using only PR
  - single attachment station (SAS)
- If 2 Rings - Dual attachment station (DAS)
- To solve the problem of ~~sin~~ Ring Topology (ek cable cut gya toh N/w shutdown)
- Supports IEEE 802.5 frame structure →

2 parts ① Token frame 3 byte

SFD	AC	ED
1	1	1

bytes →

② Data frame

SFD	AC	FC	DA	SA	Data	CRC	ED	FS
1	1	1	6	6	>=0	1	1	1

bytes →

Token frame keeps revolving in N/w

SFD Start frame delimiter

ED End frame delimiter

initially AC in Token frame is 0

when Token is captured by any MAU AC becomes 1

Token stays with a station for 10 millisec

AC - Access ~~capture~~ control field

when AC = 1

FC frame control status field

This field is used to identify data frame/ control frame

DA - SA Dest Addr & source Addr

FS Frame Status → A avail dest

→ C copy the frame

consist → Data

→ destination Addr

Page No.
Date

ITMU

If A=0, C=0
destination is not available, No frames to copy

If A=1, C=1
dest is available, copy frames to dest.

If A=0, C=1
Desti Nhi hai, But frames hai

If A=1, C=0
Station hai, But no frames to copy

Page No.
Date

UNIT 2

TCP → Process → Transport layer → Port No. Socket Addr

- Connection oriented Protocol
- creates a virtual connection betn two tcp's to send data.
- TCP uses flow & error control mechanisms at transport level

TCP services

① Process to Process Communication

Ports used by TCP

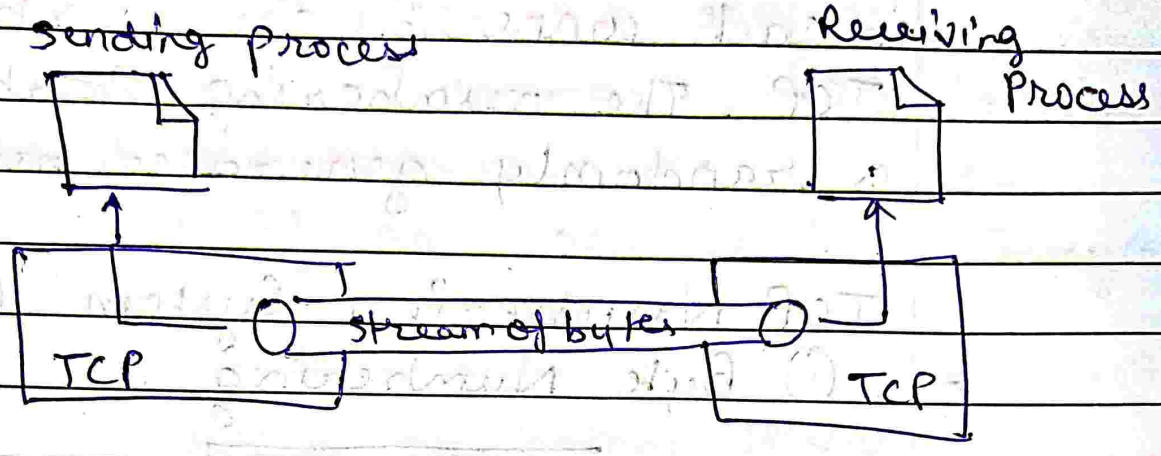
Port	Protocol	Description
7	Echo	
9	Discard	
11	Users	
13	Daytime	
17	Quote	
19	chargen	
20	FTP, Data	
21	FTP, Control	
23	TELNET	
25	SMTP	
53	DNS	Domain Name service
67	BOOTP	Bootstrap Program
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure call

but waiting for ack ← Red - Not sent
grey - sent
white - empty

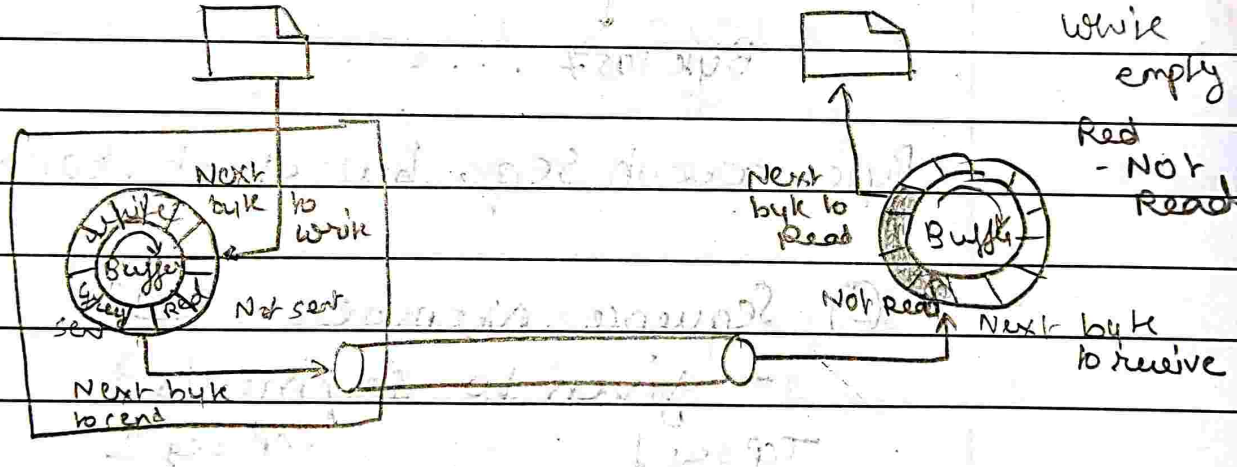
Byk oriented protocol
- aka TCP

Page No.
Date

(2) Stream delivery
↳ ek k piche ek



—— xox ——



Buffer - circular array
- 10000s of locations

(3) sending & Receiving Buffers

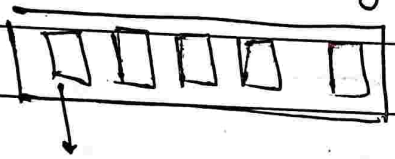
—— xox ——

(4) TCP Segment - grouping of bytes along with Header
- Size of ~~Segment~~ may variable

The bytes of data being transferred in each connection are numbered by TCP. The numbering starts with a randomly generated number.

TCP Numbering System (0 to 2^{32-1})

— ① Byte Numbering



Bytes are in seq. but start random hota hai

— ② Sequence Number
— given to segments.

Bytes within a seg should be synchronized as compared to the seg no.

— Byte no. within a segment aligned hona irrespective of seg. no

— seg. no. change ho skta hai send krne pe.
aka initial sequence Number (isn)

TCP - connection oriented protocol
Stream byte oriented protocol

Page No.
Date

Q. Suppose a TCP connection is transferring a file of 5000 bytes. The 1st byte is numbered as ~~10000~~ 10,001. Write down the sequence no. for each segment if data are sent in 5 segment each carrying 1000 bytes.

1000 bytes

Seg 1 → Seq. No: (10001) (Range: 10001 to 11000)
Seg 2 → Seq. No: 11001 (Range: 11001 to 12000)
Seg 3 → Seq No: 12001 (Range: 12001 to 13000)
Seg 4 → Seq NO: 13001 (Range: 13001 to 14000)
Seg 5 → Seq NO: 14001 (Range: 14001 to 15000)

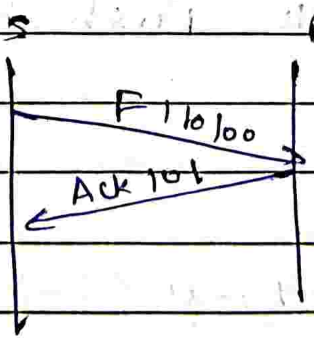
byk no.

③ Acknowledgement Number

Ack No. → Control Packet

→ Piggybacking (2 info previous frame received & Reciver waiting for next frames onwards)

If Ack = x, the Receiver will send x+1



Suppose

2 parts
① 1 to 100 frames received
② 101 se fir hai

Piggy backing

NAk → Not acknowledge
Koi frame corrupt hogya hai
Ex - NAK 89

Ek pkg data se saath bhejna

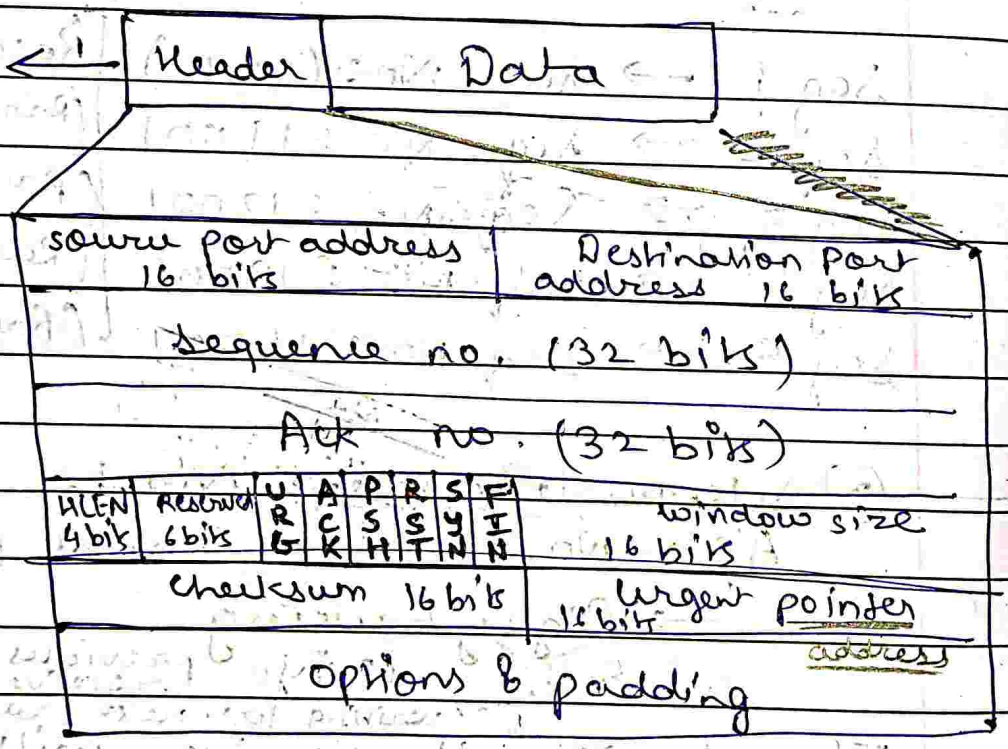
Port identifies Appl^n Process of a Machine

circular Array

+ TCP segment Format

Link list

TCP header minimum 20 bytes
to 60 bytes



Header length

flags → urgent, Ack, Push, Reset, Syn, Finish

Out of order segment → URG = 1. Segment urgent hai
URG pointer → message ka address

MSS segment → PSS

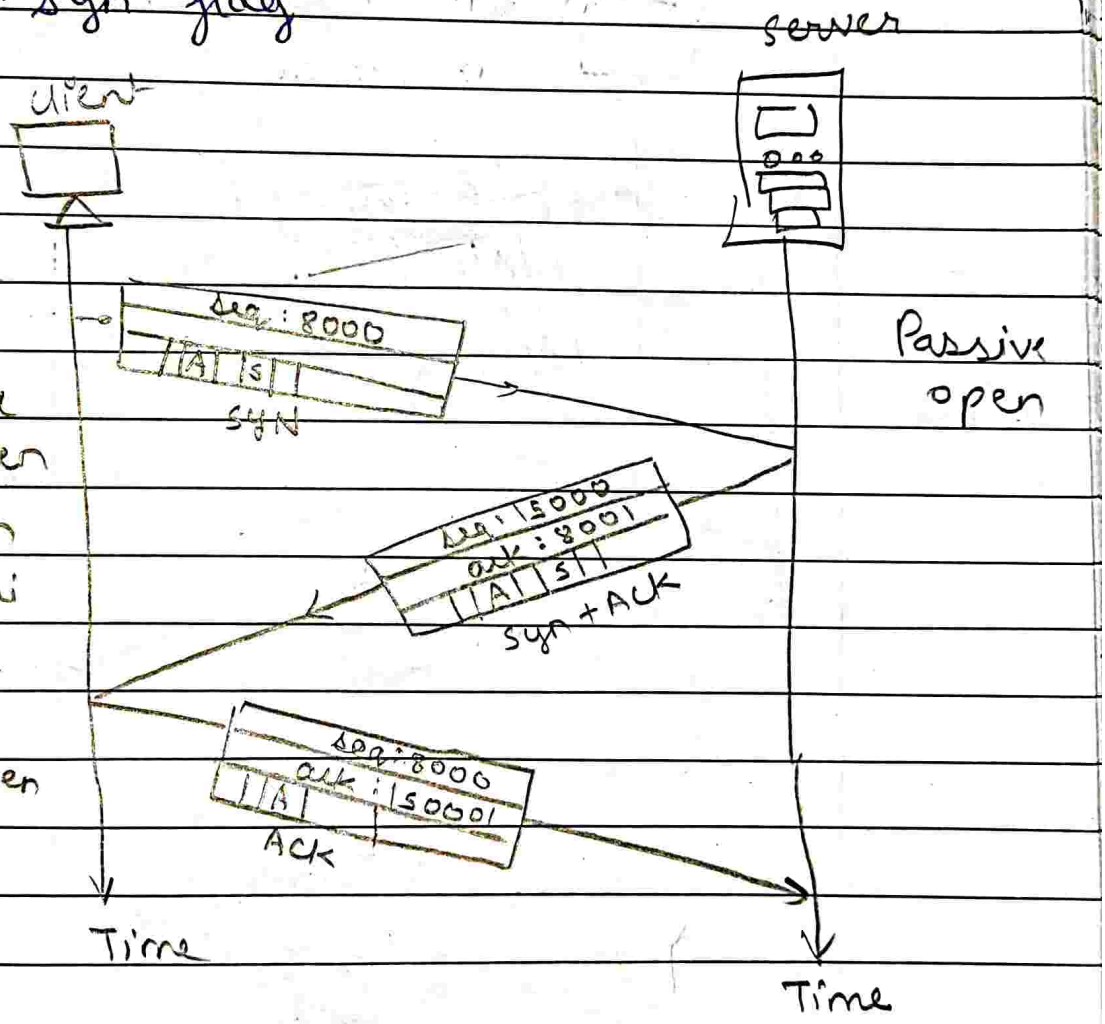
TCP → establishment
data transfer
termination

Page No.
Date

24/7 open
passive
open

Connection establishment using three - way handshaking

A: ACK flag
S: Syn flag



(1) Seq : 8000

(2) Syn + Ack : Seq : 15000 pe store krrega
ack = 8000 Tak data hai 8001 se next ~~save kr start~~

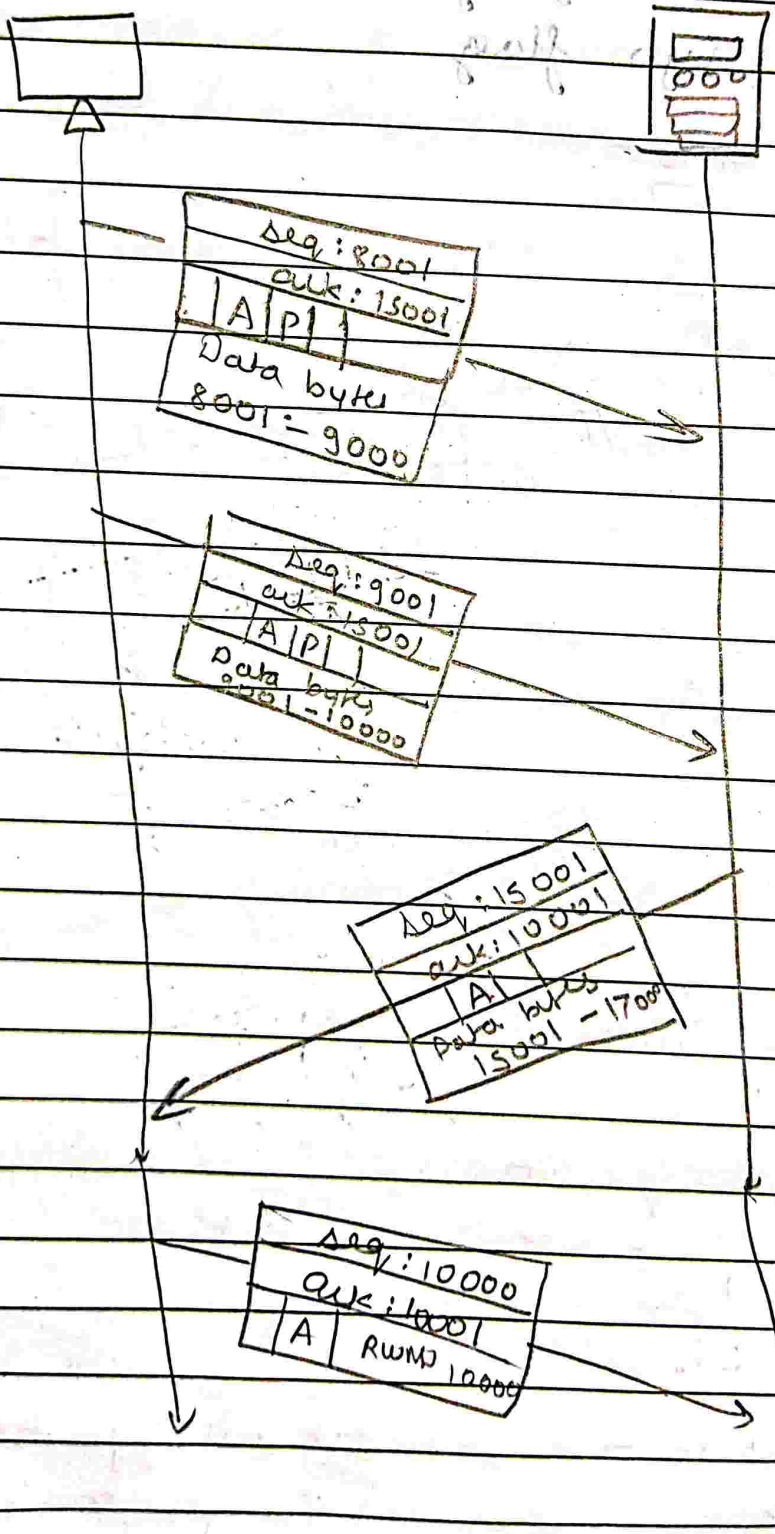
(3) Ack - Aapka ack mil gya hai
aapke sequence no. pe maine ack diya hai aap store krlo 15000 1 se

Ack 10001
is the packet which bits
message has I'm
waiting for
10001

Page No.
Date

Data transfer

A : Ack flag
P : PSH flag



Page No.
Date

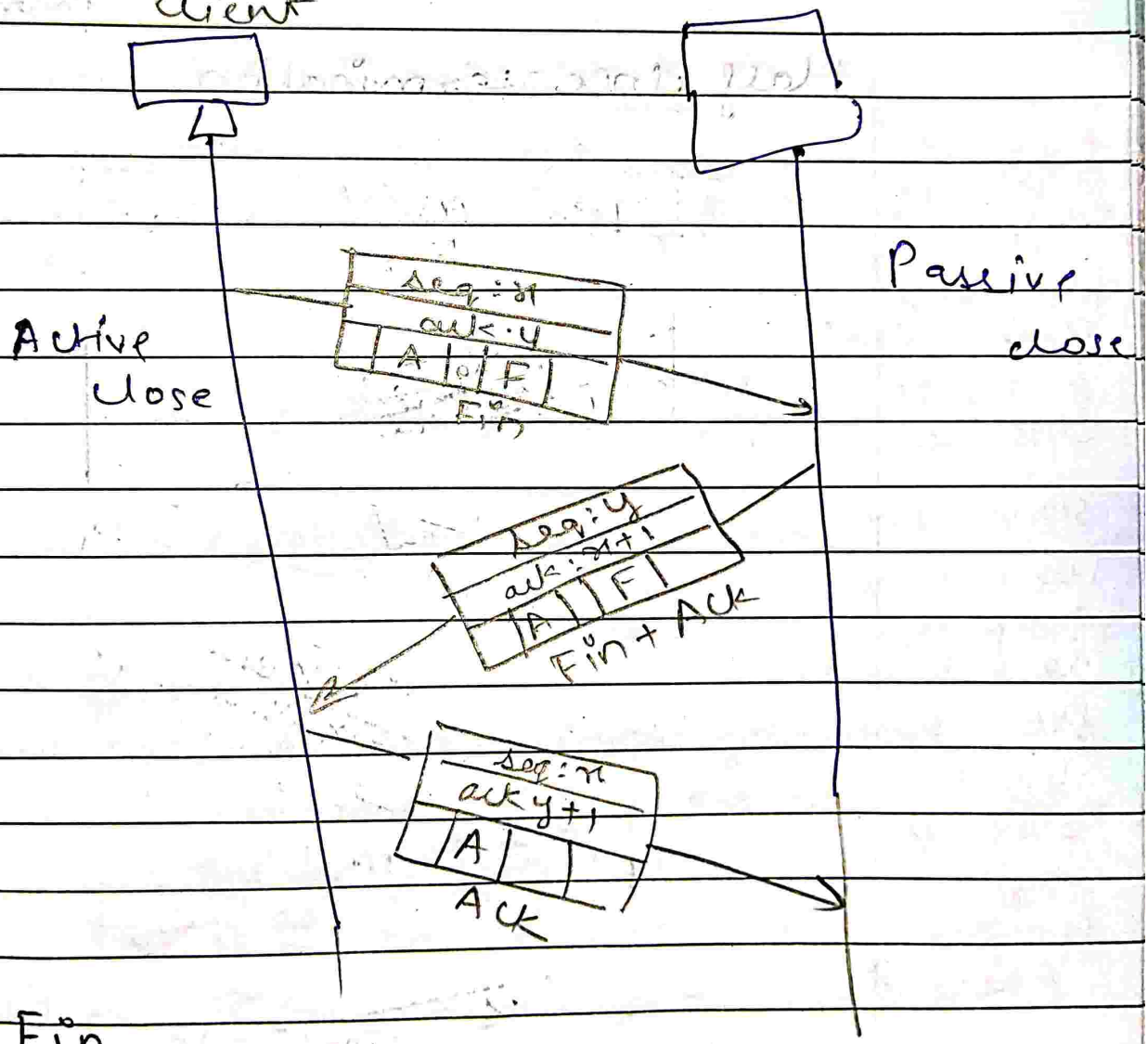
RWND

Reciver Window size

Connection termination using 3 way handshake

A : Ack flag

F : Fin flag.



Fin

Fin+Ack

Ack

TCP seg 536 bytes

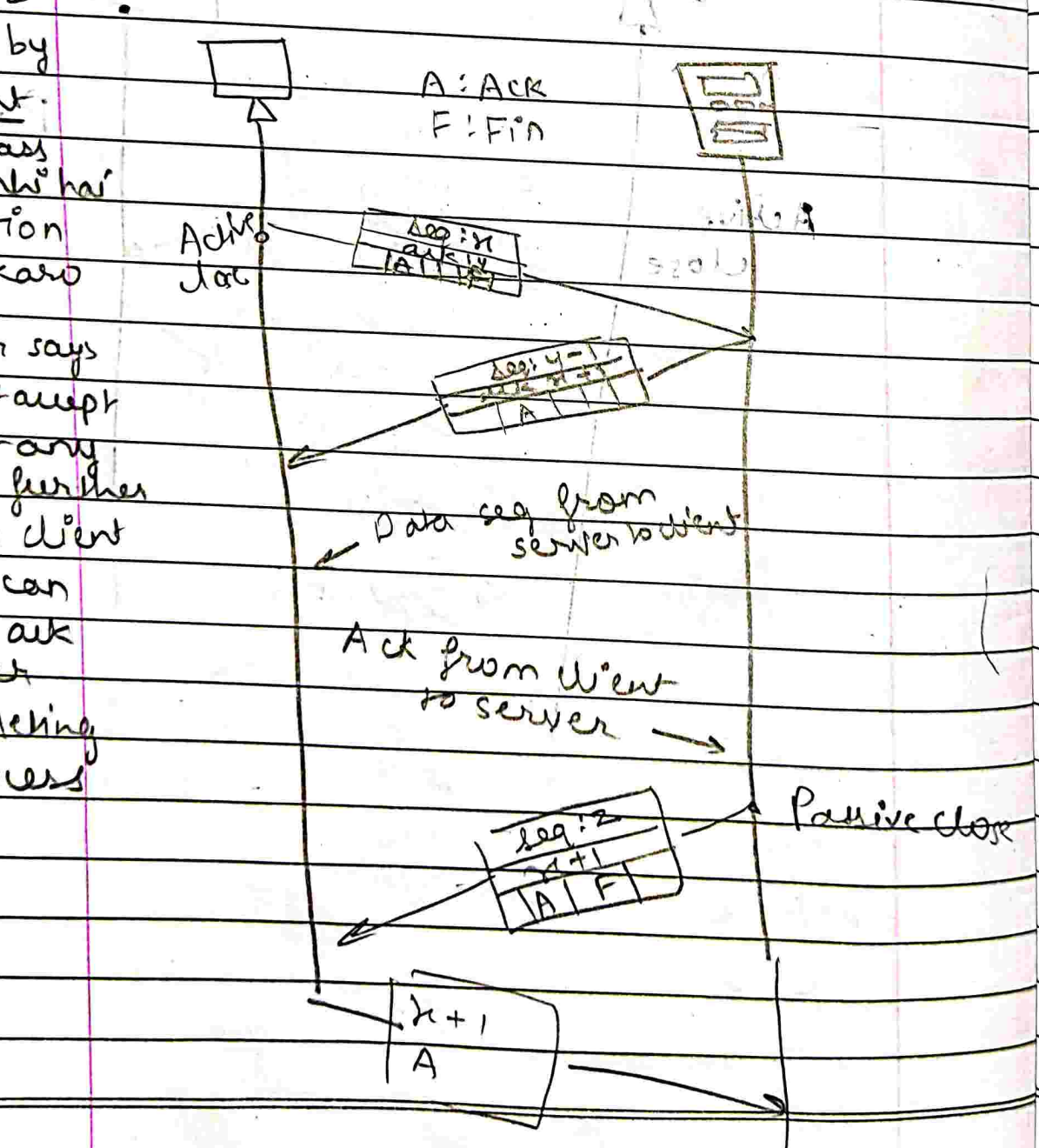
Page No.
Date

Assumed

TCP has a MSS (1024 byte)
maximum segment size
The TCP segment cannot be transferred until it reaches its MSS

- JAB MSS sekam ka data transfer krna hai tab use use PSH flag
immediate data

Half close termination



urgent pointer is valid
Acknowledgement is valid
Request for PUSH
Reset the connection

synchronize sequence numbers
Terminate the conn^n

Page No.
Date

c) What can you say about the TCP segment in which the value of the control field is one of the following
① 000001 ② 000000
③ 010001

URG	ACK	PSH	RST	SYN	FIN

① from the given TCP seg control field the Fin flag is set. Fin flag is set during connection termination

② No control flags are set i.e no TCP segment is being generated.

③ ACK + Fin → termination

d) The following is a dump of a TCP header in Hexadecimal format
05320017 00000001 00000000 500207FF 00000000
Answer the following ques. (in bytes)
a) What is the source port no.
b) dest port no.
c) seq no.
d) ack no.
e) length of header
f) Type of seg
g) Window size

0x0532 → hexadecimal format

ex hai

Page No.
Date

Hexadecimal → each value of 4 bit

0532-0017

0 → 0000
5 → 0110

0x0532
↳ bytes

0532 = $0\times16^3 + 5\times16^2 + 3\times16^1 + 2\times16$
= 0 + 256 + 48 + 2
= 316 bytes → bytes me convert karo

Source port Address =

Sliding window byte oriented

Window size = minimum (rwnd, cwnd)

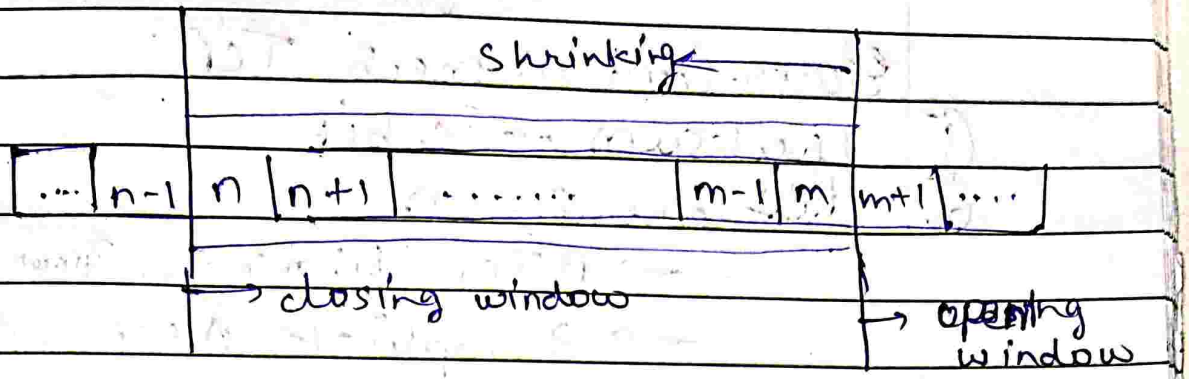
rwnd → size advertised by opposite end
→ reciver tells that this is the size of window I'm maintaining

cwnd → congestion window
→ set by admin

shrinking → to control the flow

wi

Page No.
Date



Q What is the value of receiver window (rwnd) for host A if the receiver, host B has a buffer size of 5000 bytes and 1000 bytes of received and unprocessed data

jiska ack nhi bheja hai that is called unprocessed data

Rwnd
= 5000
- 1000
= 4000

B
Buffer = 5000 bytes
Empty white ←
Grey ← 1000 bytes unprocessed data
unprocessed
jiska Ack nhi bheja hai B ne

What is the size of window for host A is the value of rwnd is 3000 bytes & value of cwnd is 3500 bytes

window size = min (rwnd, cwnd)
= min (3000, 3500)
= 3000

Page No.
Date

Error Control mech TCP

(1) Checksum → 16 bit

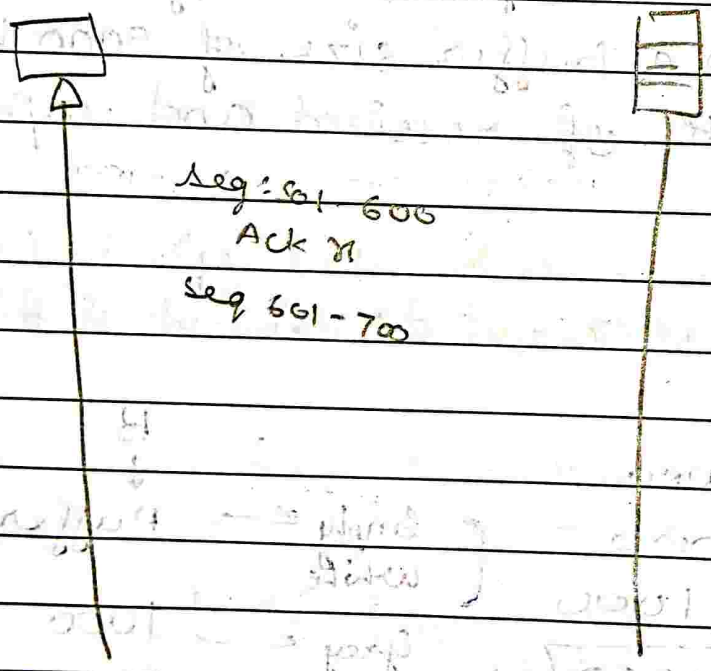
(2) Retransmission

→ RTO (Retransmission Timer out time)

→ 3 Duplicate Ack

faster than RTO

Lost segment



RTO → gives Round trip time.

if 128 hop pe time aa rha

RTO is 128 sec.

MSL → Message segment Lifetime

Page No.
Date

States for TCP (Transition)

Closed : No connection exists

server port — Listen : Passive server open received; waiting for SYN

client — SYN-sent : Syn sent; waiting for ACK

server — SYN - RCVD : SYN + Ack sent; waiting for Ack

Established : Connection established; data transfer in progress

client active close — FIN-Wait-1 : first Fin sent; waiting for ACK (connection still exist, data khtm hogya)

server Passive close — FIN-wait-2 : Ack to first FIN received; waiting for second FIN

server — Close-Wait : First Fin received, Ack sent; waiting for application to close

client — Time-wait : Second Fin received, Ack sent; waiting for 2MSL time-out

server — LAST ACK : second Fin sent; waiting for ACK

Closing : Both sides decided to close simultaneously.

Page No.
Date

closed

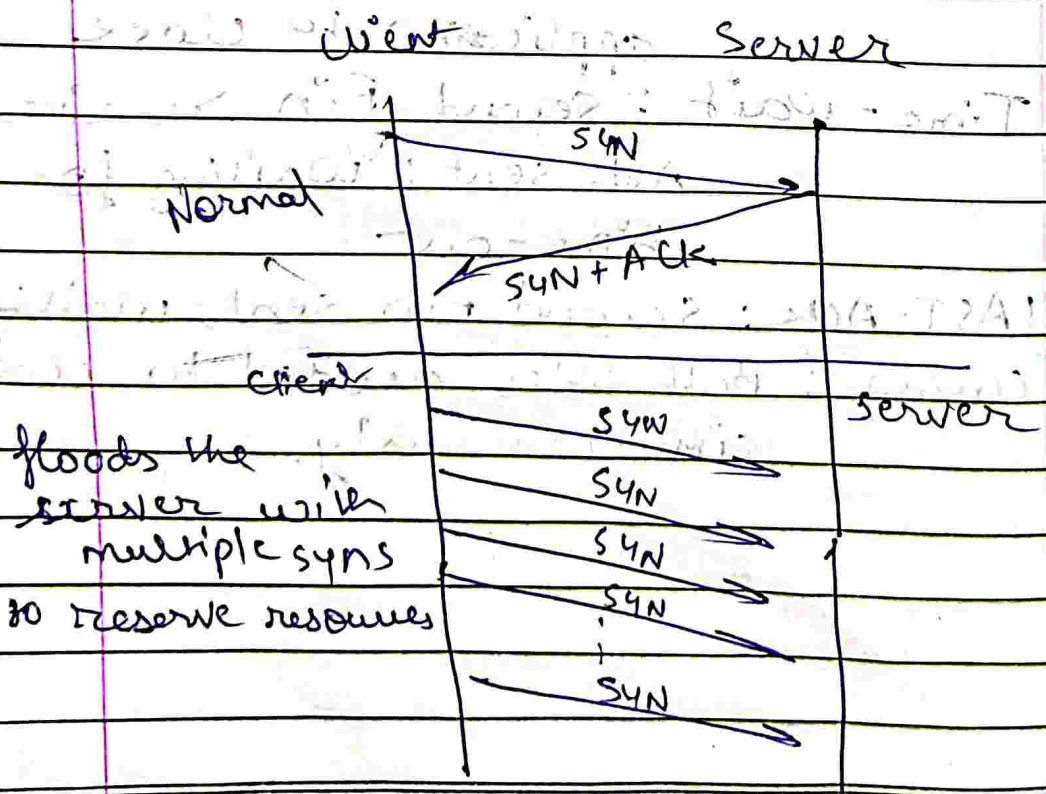
listen

SYN.

Denial of serving attack

SYN flooding attack - (DOS)
server ko crash krna

SYN: Resources need to be reserved (server)
If Resources hai : SYN + ACK → mere liye resources reserved hai (client)



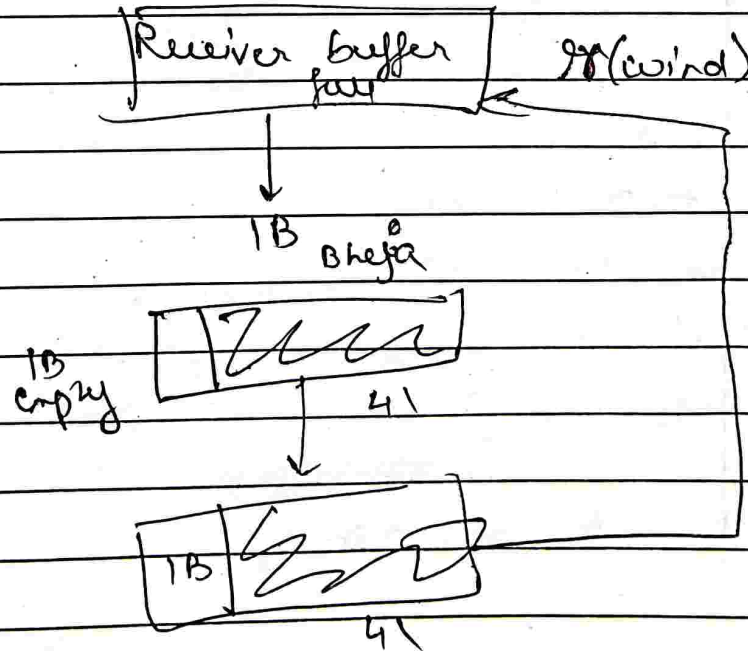
Page No.
Date

To stop SFA delay laga skte hai ki ek time tak agar client se Ack nhi aa rha toh we can free those resource.

Silly Window syndrome at sender side
sending data byte by byte even if MSS is larger

→ solved by Nagle's Algo

silly window syndrome at receiver's



→ solved by Clark's solution.
window size = 0 jab tak
apple jagah nhi hai

→ solved by delayed Ack not greater than 500 ms.