Q you are given 10 bits $B = 4$ Mbps & $v = 2 * 10^8$ m/s

10 bits $B = 4$ Mbps

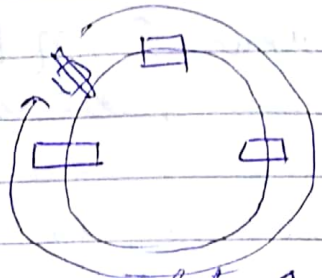
$sec = \frac{1}{4 \times 10^{6}}$ sec $= 0.25 \times 10^{-6}$ sec

Ans $0.25 \times 10^{-6} \times 2 * 10^{8}$

500 m

THT

- Delay token reinsertion
- Early token reinsertion



Ring latency → Time taken to complete 1 circumference of ring.

$$RL = \underbrace{\frac{d}{v}}_{\text{secs}} + \underbrace{N * b}_{\text{bits}}$$

N → no of station
b → bit delay

(X)

sec $RL = \frac{d}{v} + \frac{1}{N * b}$

bits $RL = \frac{d}{v} * N * b + N * b$

$= N * b \left(\frac{d}{v} + 1\right)$

sec $RL = \frac{d}{v} + \frac{N * b}{B}$ secs

bits $RL = \left(\left(\frac{d}{v}\right) B + Nb\right)$ bits

Network Layer

Address Resolution Protocol Logical to physical

RARP – Physical to logical

classless

classful

A — 0 0 - 127
B — 10 128 - 135
C — 110 136 - 169
D — 1110 170 - 191
E — 1111 192 - [illegible]

Page No.
Date

Next Level Numericals

In IPV4 packet value of HLEN is 1000 in Binary. how many bytes of options are being carried by this packet.

$(1000)_2 \longrightarrow (8)_{10}$

$8 \times 4 = 32$ bytes

IPV4 → 32 bits → 2^{32} address space

→ Binary notation
→ Dotted decimal notation (127.47.

Ques change from Binary

① 1000 0001 00001011 00001011
1110 1111
129. 11. 11. 139

classless Addressing
x.y.z.t / (n) → no. of masks

Q. address →
205.16.37.39/28.
↓
Binary

11001101 00010000 00100101 00100111
first address = 32 − 28 = 4 bits.
→ last 4 bits 0000

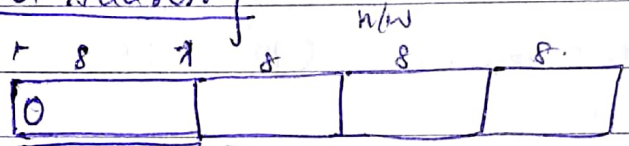
00100000
32

205.16.37.32 → first address
last address → last 4 bits 1111
00101111
205.16.37.47

$(=2^4)$ → 16 addresses

classless Addressing

classful Addressing.



0-127	class A	0	2^{24}
128-191	class B	10	2^{16}
192-223	C	110	2^8
224-239	D	1110	multicast 2^{28}
240-255	E	1111	Reserved 2^{28}

0.10.12.27

↓

class A

225.197.0.127

10.

IPV4 HLEN - 4 bit

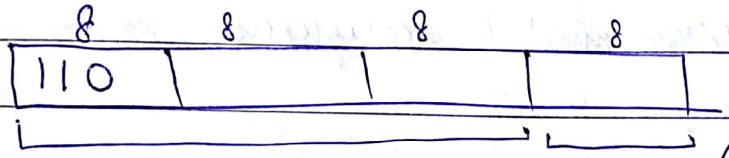
$\frac{20B}{4}$ = 5 words = $(0101)_2$

Date

60/8

Q. In IPV4 Addressing, the no. of n/w allowed under class C address is _____?

Ans class C = 255.255.255.0



NW = ID
R.B = 3
21

21 networks

2^{21} networks

Q. In IPV addressing no. of network allowed under class B address is _____?

NID = 16
R.B 2
14

2^{14} → networks

class A NID = 8
RB 1
7

2^7

2 | 144
2 | 72
2 | 36

200. 10. 11. 144/27
first address 32 - 27 = 5 bits
00100000
Last address
10011111
10000000
= [128 159]

CIDR Notation
x.y.z.t/n
address
no of masks.

[Network ID is called Block ID

Page No.
Date

Q 20.10.50.100/20

BID = 20

∴ HID = 32 − 20

= 12

BID	HID
20	12

2^{12} → host IDs

Rules CIDR Block

(1) All the IP address must be contiguous

x.y.2.0
x.y.2.1
⋮
x.y.2.7
x.y.2.10

} → 8 = 2^3

(2) Block size must be the power of 2.

(3) First IP address in block should be divisible by size of block.

Q. Find whether the following is CIDR Block.

(1) 150.20.10.64
150.20.10.127

64
0100 0000

2^6

120.130.20.32
⋮
63

→ 32 = 2^5

00100

Q. 20.10.50.75
100

26 = NO 2 ki power

Divide kiya hua hoga

2^9 →

Address Mapping

ARP → MAC Address, identify physical addr

RARP

Bootstrap Protocol

- ARP → queries are broadcast
  reply unique cast
- RARP → Reverse address resolution protocol

Page No. _____
Date

Logical Address
Bootstrap protocol → is used to provide physical to logical address mapping

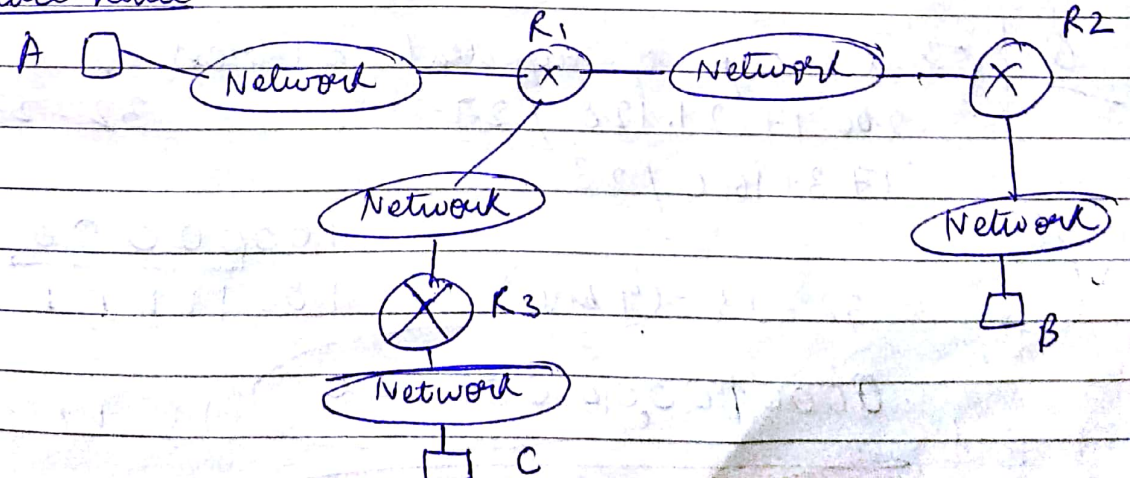
- ICMP - Internet control Message protocol
  - ① Error reporting msg
  - ② Query msg

→ Destination unreachable (3) (Type)
  Type
  → Source quench (4)
  Time exceeded (11)
  Parameter problems (12)
  Redirection (5)

→ Echo request & reply
  Time stamp request & reply
  Address Mask request & reply
  Router solicitation and advertisment

{ We use PIN to find whether host is alive and responding
  Echo request / reply query message is used.

Trace route



A → B message
TDL → (1)

→ Then R1 rejects and sends time exceeded message to A.

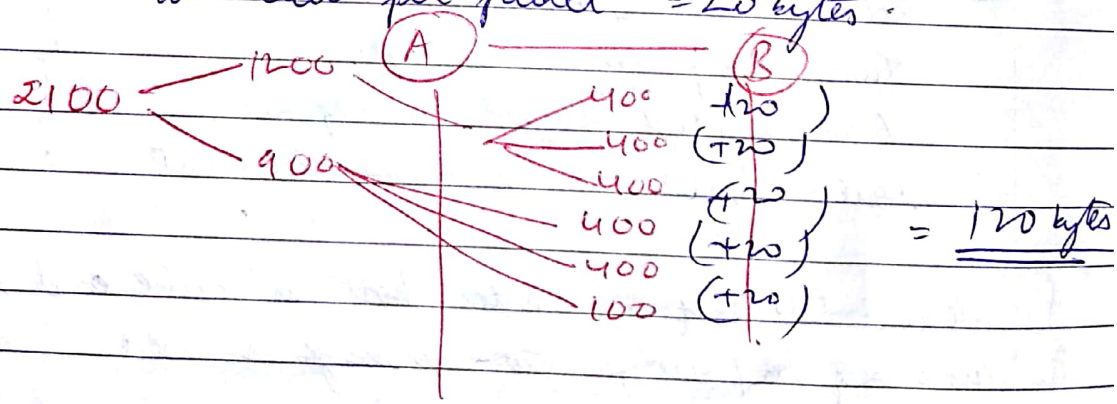
→ If TDL is said to 2 then R2 discards the time exceed message to A

→ If TDL is said to 3 then B doesn't discard but since it is a query message. B sends the destination unreachable message to source A as it doesn't know whether to receive the message.

9 April '18

8. A TCP msg consisting of 2100 bytes is passed to IP layer for delivery across 2 networks. First network can carry a max payload of 1200 per frame. Second network can carry 400 per frame excluding network overhead. Assume that IP overhead per packet is 20 bytes. What is the total IP overhead in second network?

IP overhead per packet = 20 bytes.



9. Find range of different address

200.17.21.128 / 27

32 - 27 = 5

17.34.16.0 / 23

32 - 23 = 9 bits

10000000
10011111 128 159

00000000.000000

11111

Transport Layer

Page No. _____
Date | | | |

Port no. are 16-bit addresses

1. well known ports. - Ports from 0 to 1023 are assigned as well known ports by IANA (Internet Assigned Number Authority)

2. Registered Ports - 1024 - 40151

3. Dynamic Ports - 40152 - 65535

Socket address = IP address + Port address is socket address

⇒ **UDP** connection less service (User Data Protocol)

- Reliable
- performs very limited error checking

Header - 8 bytes

Diagram is imp.

Source Ports No. 16-bits	Destination Port No. 16 bits
Total length 16 bits	checksum 16 bits

- suitable for process that requires simple req. response communication with little concern for flow & error control
- No error control except for the checksum
- Suitable for multicasting.
- suitable for some routing updating protocols like RIP.
- If there is any error encountered by UDP protocol then they sent ICMP.

TCP

Transmission control Protocol
- connection oriented & reliable
- Process-to-Process communication FTP (20-21)

FTP Port (20, 21)
data control

daytime	13
TELNET	23
SMTP	25
DNS	53
HTTP	80

→ Stream delivery service - TCP allows the sending process to delivery data as stream of bytes and allows a receiving process to retrive or obtain data as stream of bytes
→ sending and receiving buffers for each direction (req sending or reply receiving)

→ Segments → transport layer groups a no of byte together into a packet called as segment and TCP adds the header to each segment
→ connection oriented services
1. 2 TCP's establish a comm. b/w them
2. Data are exchanged in both direction
3. connection is terminated.

TCP example, Telephone, skype, ATM,

TCP Header

TCP Header

Header = 20B – 60B

Source Port Address 16	Destination Port Address 16
32 Sequence No.	
32 Acknowledgment No.	

HLEN 4	Reserved 6	URG	ACK	PSH	RST	SYN	FIN	WINDOW SIZE 16
checksum 16								urgent pointer 16
options								

Page
Date

Q Header length = 40B

HLEN = 40B

↳ HLEN (actual) = $\frac{40}{4}$ = 10 words.

URG value of urgent point field is valid.

ACK value of acknowledgment field is valid

PSH Push the data

RST Reset the connection

SYN - Synchronise sequence no. during connection

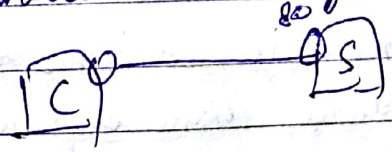
FIN - Terminate connection.

Max window size ⓪ - 65536

Lab

Small chat system

(i) Port no. - end point of the device through which it is connected to the system.



C

C

(2nd) → Header files

Header files - ① server
② client

↳ some for both

+ streaming data

Port no. Protocol UDP - TCP

Some functions

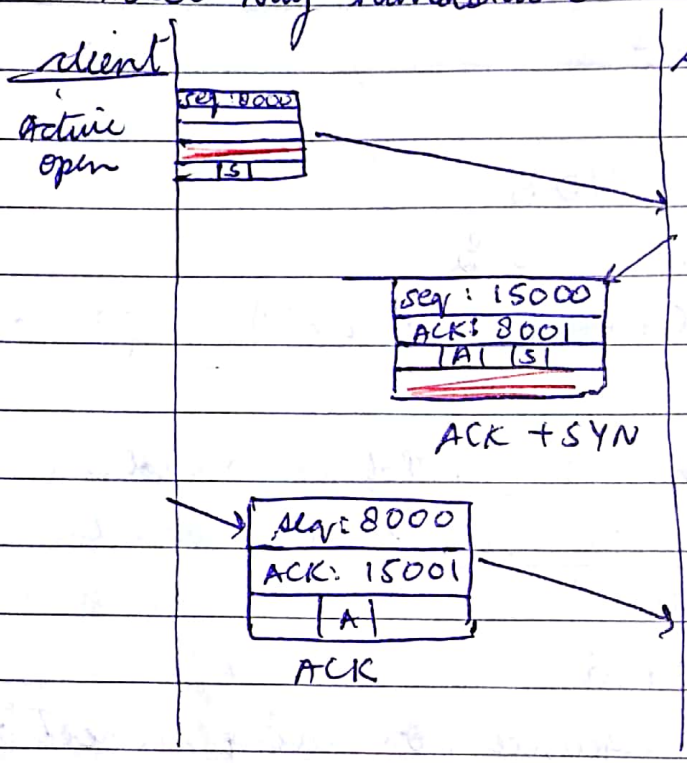
sum (x, y) - client server

remote method invocation

April 2018 connection establishment

- nothing

- Three way handshake

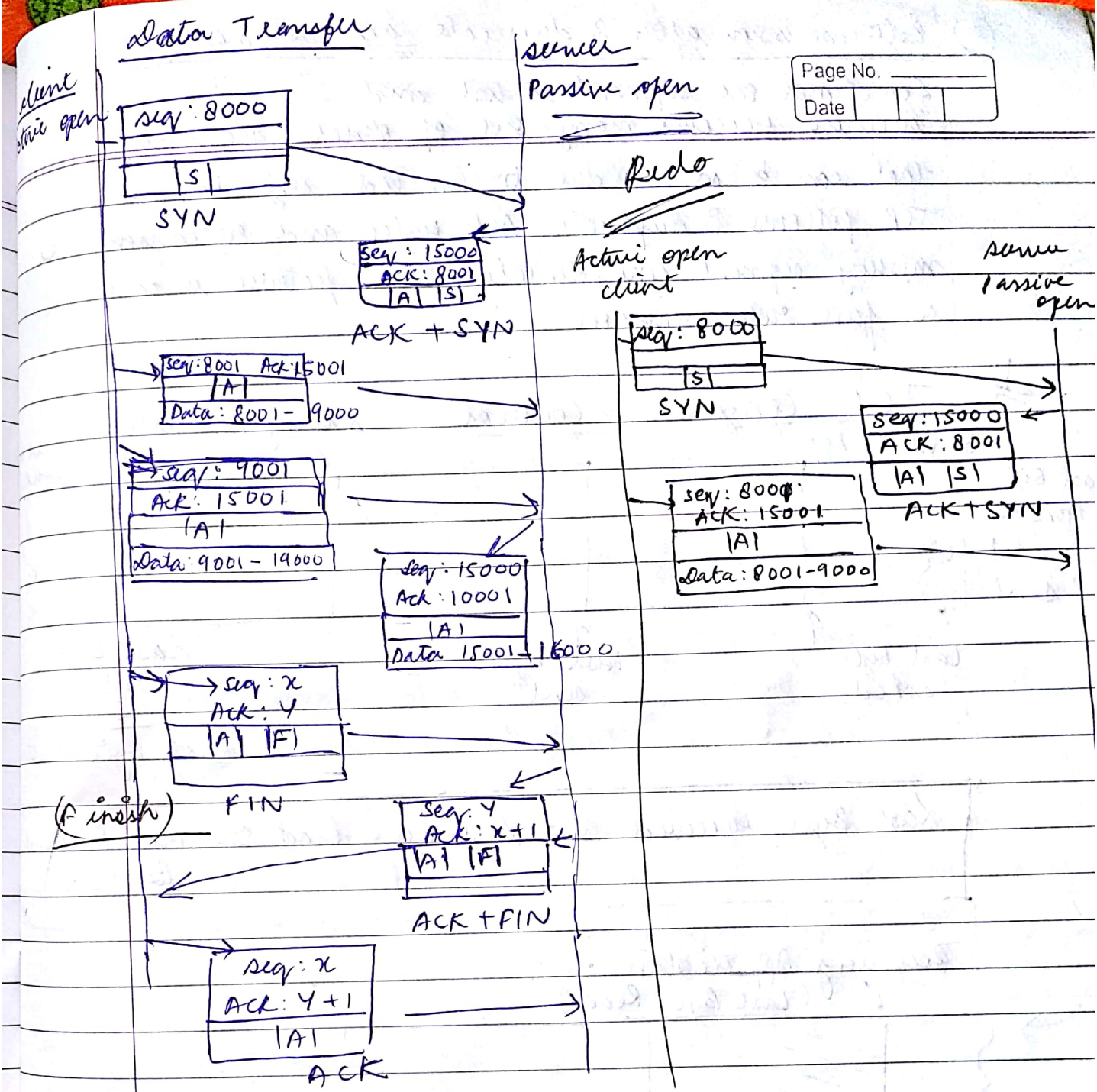


① Ack - acknowledgment packet does not consume sequence no.

② syn - synchronise msg

- A SYN seg. cannot carry data but consumes 1 seq. no.
- ACK + SYN - Cannot carry data but consumes 1 seq no
- ACK segment if carrying no data consumes no seq. no. and if it is carrying a data then sequence no is incremented.

Data Transfer



- The FIN + ACK segment consumes 1 sequence no. if they are not carrying data

Error control in TCP

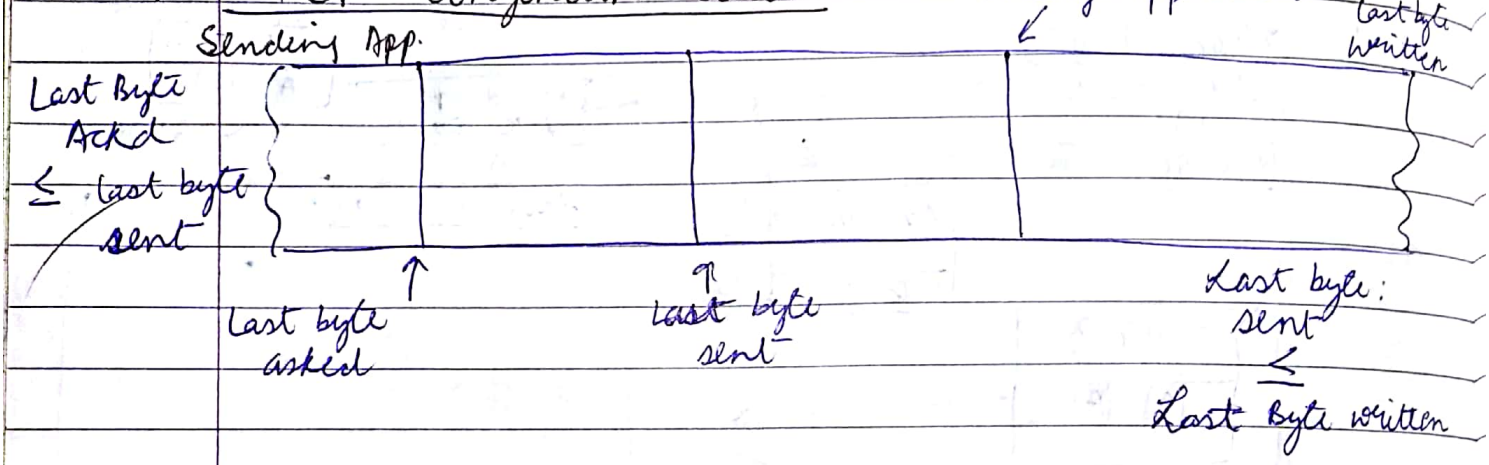
1. Retransmission after RTO (retransmission Time out) TCP maintains 1 ~~(actions FO)~~ RTO timer for all outstanding segments
   Value of RTO is dynamic and updated based on the round - trip time

(2) Retransmission after 3 duplicate ack segment

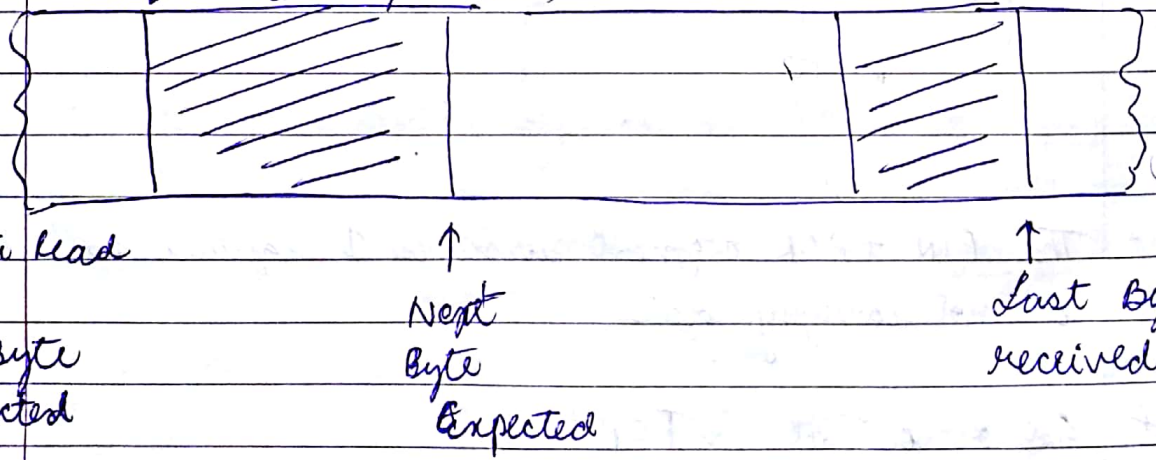
Page No. _____
Date

Sometimes one segment is lost and receiver receives many out of order segments that can be saved due to limited size buffer thus TCP follows 3 duplicate ACK rules and retransmit the missing segment immediately. This feature is called as fast retransmission

TCP Congestion Control



Last Byte received − Last Byte Read ≤ Max Received Buffer



Next Byte expected ≤ Last Byte Received + 1

Advertised window = Max. Received Byte Buffer − [(Next Byte expected − 1) − Last Byte Read]

For sending Application

Advertised window $\geq$ Last Byte sent $-$ Last Byte Acknowledged

~~effective~~

For sending Application

Effective window = Advertised window $-$ (Last Byte sent $-$ Last Byte Ackd)

Last Byte written $-$ Last Byte Ackd $\leq$ Max sending Buffer

= Min (cwnd, rwnd) $-$ (Last Byte sent $-$ Last Byte Ackd).

Q. On a TCP connection current congestion window size is 4K window advertised by receiver is 6KB. Last byte sent by sender is 10240 and last Byte acknowledged by receiver is 8192. Current window size of the sender.?

a) 2048
b) 6144
c) 8192
d) 4096

Topologies

① → Gateway, Router, Repeater, switch, hub — Passive / Active.] — Application: → Topology

Bridge ← Transparent

② LAN, MAN, WAN — Range / Application.

③ IP Address ← classless / classful

④ Subnetting — Last Address / First Address. / No. of N/W / No of Host.

Hamming ← even / odd] — — — 14 M.

16 April 2018

Routing

Adaptive Routing — Non-adaptive

DV = [Dv(y) : y ∈ N] Routing

Centralized — Isolated — Distributed

Intra domain Routing (IGP: Interior Gateway Protocol)

Inter domain Routing (EGP: Exterior Gateway Protocol)

IGP

Distance vector [RIP] Bellman Ford

link-state [OSPF]. (Dijkstra Algo)

192.168.27.41 /13

32 - 13 = 19.

192.168.27.00101001

192.168.00011011.00100100

0.00000000

1.11111111

2	41	— 1
2	20	— 0
2	10	— 0
2	5	— 1
2	2	— 0
	1	

2	27	— 1
2	13	— 1
2	6	— 0
2	3	— 1
	1	

192.168.26.0 — first

192.168.27.127 — last

~~192.168.0.1~~

~~192.~~

192.168.0.0

192.175.255.255

No. of N/w = $2^{19} - 1$

$2^{32-n} - 1$

Page No.
Date

* Routing Type
① Adaptive → ② Non adaptive

Adaptive: Centralised | Distributive | Isolated

Distributive: Intra domain routing (IGP) — Interior Gateway Protocol | Inter domain EGP (Exterior Gateway)

IGP: Distance vector | Link state

Distance vector	Link state
eg RIP	OSPF protocol
AODB	Dijkstra's Algo
DSDB etc	
Bellman Ford	

Function

- Measurement of pertinent network data
- Forwarding the info to where the routing computation will be done
- compute routing tables
- convert the routing table info into a routing decision & then dispatch the data packet

Distance to itself = 0
Dist. to other node = ∞
} Initially

① The router transmits its distance vector to each of its neighbors in the routing packet

② Each router receives and saves the most recently received dist. vector for each of its neighbours.

③ A router recalculates its dist vector when :-

(a) It receives a distance vector from a neighbor containing different info than before

(b) It discovers that a link to the neighbor has gone down

(4) The dist. vector calculation is based upon minimising the cost of each destination.

Page No. _____
Date | | |

$$d_x(y) = \min_v \{ c(x,v) + d_v(y) \}$$

where min is taken over all neighbours $v(x)$.

$d_x(y)$ = Estimate of least cost from x to y.

$c(x,y)$ → Node x knows cost to each neighbour.

Node x also maintains its neighbouring dist^ vector for each neighbour v, x. maintains $DV = [D_v(y) : y \in N]$

RIP - Routing Info Protocol

DSDB - Destination Sequenced Dist vector routing

OSPF - Open shortest path First

CSMA - Carrier sense multiple access

TDMA - Time division ————

SDMA - Space ————

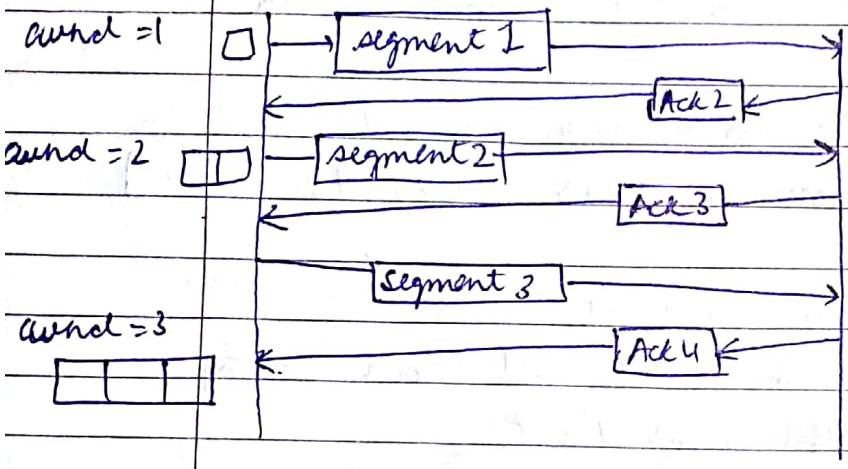
ICMP - Internet control ————

IGMP - Internet Group Multiple Access

Congestion Avoidance

Additive ↑ in congestion is same

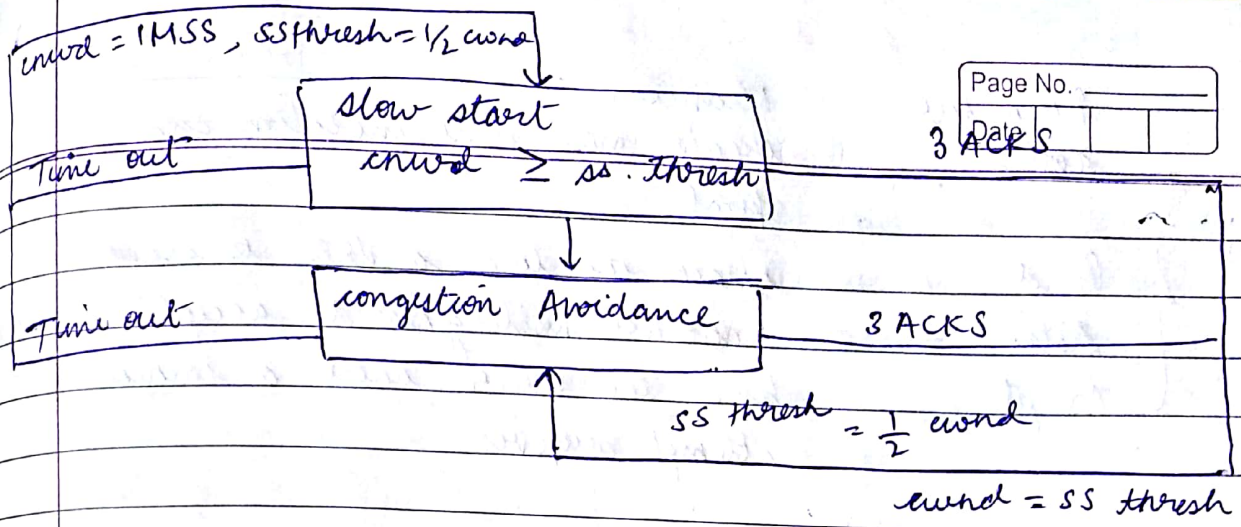
To avoid congestion before it happens one must slow down this exponential growth each time the whole window of segments is acknowledged. The size of segment window is ↑ by 1



Congestion Detection (Multiplicative ↓)

- If time out occurs there is a strong possibility of congestion
  - sets the value of threshold to ½ of current window size
  - sets the congestion window to size of one segment
  - starts the slow start phase again

- If 3 acknowledgements are received there are weaker possibility of congestion. This is called fast transmission & fast recovery
  - sets value of threshold to ½ of current window size
  - sets congestion window to value of threshold
  - starts congestion avoidance phase again.



Page No.
Date

3 ACKS

Let assume max window size is 32 segments and initial threshhold is 16 segments

Threshhold is set to 10, because in first round, window size was 20 when it was time out

Threshhold = ½ window size

When 3 acknowledgement is encountered, then window size was 12, Threshold = 6 = $\frac{1}{2}$(12)

Q — Consider TCP connection in state where there are no outstanding acknowledgement. Sender sends 2 segments back to back, sequence no. of first and 2nd segments are 290, 290. first seg was lost. but second was received correctly by receiver. Let x be amount of data carried in first segment. 'y' acknowledgement no. send by receiver. 'x', 'y' values

(a) 60, 290

(b) 60, 230

* Berkley sockets

Primitive	Meaning

	Primitive	Meaning
server side	Socket	creates new communication end point
	Bind	attach the local address to socket
	Listen	announce willingness to accept connection
	Accept	block the caller until a connection attempt arrives
client side	connect	actively attempt to establish a connection
	send	send some data over the connection
	receive	receive some data
	close	release the connections

	State	Description
(1)	closed	No connection is active or pending
(2)	Listen	Server is waiting for an incoming call
(3)	synchronize / receive	connection request has arrived, wait for acknowledgement.
(4)	syns / sent	application has started to open a connection
(5)	establish	normal data transfer state
(6)	fin wait 1	application has finished, it has se
(7)	fin wait 2	other side has agreed to release
(8)	time wait	wait for all packets to die of
(9)	close	both sides have tried to close simultane
(10)	close wait	other side has initiated a release
(11)	last ack	wait for all packets to die of

Cryptography

encryption Decryption

Page No.
Date

metric (Private key) Asymmetric (public key) → Different keys are use and decryption key cannot be derived from encryption key

→ Same key is used for encryption and description

DES AES — (128 bit)

(64 bit)

Diffie-Hellman Algo — (Numerical, words algo)

steps

1. Alice and Bob agree on prime no. 'p' and a base 'g'
2. Alice chooses a secret no. 'a' and sends bob $g^a \bmod p$.
3. Bob ——— 'b' ——— Alice $g^b \bmod p$.
4. Alice will compute $(g^b \bmod p)^a \bmod p$.
   Bob ——— $(g^a \bmod p)^b \bmod p$.

$p = 23 \quad g = 5 \quad a = 6 \quad b = 15.$

$$\text{Alice} = [5^6 \bmod (23)]^{15} \bmod (23)$$

$$\text{Bob} = [5^{15} \bmod (23)]^6 \bmod (23)$$

$$= [15625 \bmod 23]^{15} \bmod 23.$$

$$\text{Alice} = 5^6 \bmod (23) = 8 \qquad \text{Bob} = 5^{15} \bmod (23) = 19.$$

$$\text{Bob} = (19)^6 \bmod (23) = 2$$

$$\text{Alice} = (8)^{15} \bmod (23) = 2$$

∴ secret key is 2.

Suppose 2 parties A & B wish to set up a common secret key b/w themselves using deffie-Hellman key exchange.

Page No. _____
Date

They agree on (7) as modulus '3' as primitive root party 'a' choose 2 and party 'b' choose 5 as their respective secrets where deffie-Hellman key is _____

$p = 7 \quad g = 3 \quad a = 2 \quad b = 5$

$A = 3^2 \bmod 7 = 2$

$B = 3^5 \bmod 7 = 5$

$K1 = (5)^2 \bmod 7 = 4$

$K2 = (2)^5 \bmod 7 = 0$

$K = 3^{2 \times 5} \bmod 7$

$= 2$

↳ shared key

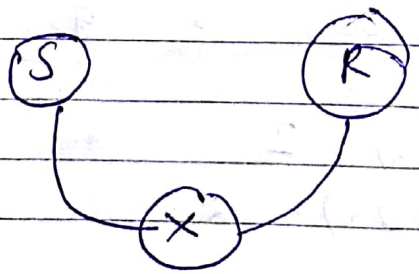
$K = g^{ab} \bmod p$

Middle man attack

$K_1 = g^a \bmod p \quad K_2 = g^b \bmod p \quad K_3 = g^c \bmod p$

$R_2 \quad R_1 \quad R_3 \quad R_2$

middle man attack



RSA Reverse shammer

choose very large prime nos. p & q

compute $n = p \times q$

compute $\phi(n) = (p-1) \times (q-1)$

choose random no. e such that.

$e \times d = 1 \bmod \phi n$

'e' and 'n' are made public keys 'd' & $\phi(n)$ 'are secret keys.

$$C = (M)^e \bmod n$$

$$M = (C)^d \bmod n$$

crypto - RSA, Deffie

Symmetric / Asymmetric ka difference

Cipher text, (Plain text original)

Application layer PROTOCOL - short note

Routing techniques - Diff b/w Link state & Dist vector

Diff b/w additive ↑, multiplicative ⊗ &.

Authentication, Security, Intrusion, Ethical Hacking,

Persistent vs Non persistent connection.

~~wireless~~ socket

Berkley