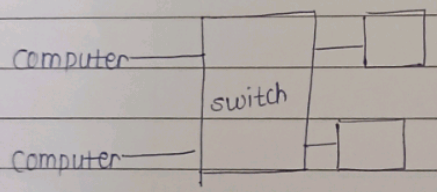
Page No.
Data

Host address - 32 bits
→ IPV4 address
→ IPV6 address (128 bit)
→ MAC Address
↓ 48 bits.

Ethernet Address
↓
NIC → LAN Case 1.

IP - add
— — — —
8 bit 8 8 8
↓
decimal conversion.



gateway

gateway to pass the message through switch
Subnet wall mask (is used to create) the network.

255.255.255.00000000.
↓
Host bit.

8 bits - 2^8 → Address can be created.
$2^8 - 2 = \boxed{254}$ → maximum no. of computer can be connected.

256 - 2 ip's are reserved.
1st is network id
2nd is Broadcast address.
} ip's.

witch - To connect number of Host to send packet within same N/w.

Page No.
Date

- How to assign the address ?

↓

two methods

Static Dynamic

↓

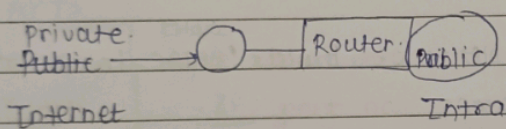
1) Assign IP address
2) Subnet mall mask
3) Gateway
4) DN switch

inside network

outside network.

MAC is by defaut

* Router is used to connect the Nlw from LAN to LAN.



Dynamic. DHCP server → Assign IP address immediately.

↓

IP Address. - - - - Dynamic.

lease address

Static → comp

class c

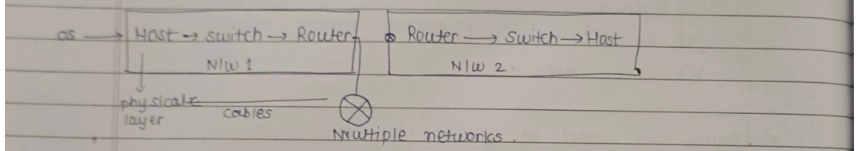
192168.0.1

Static IP address is assign to server

Dynamic IP address is assign to LAN.

Optical fiber

- Multimode
  - OM1
  - OM2
  - OM3
  - 400 m only.
- Single mode
  - Use in large distance.



Switch → Datalink & Network. Builds tables (MAC table of ARP table) to forward frames.

Books → Computer Nlw up to down
(Kurose)
Data Communication (Frozen)

Q. Can client and server is Host ?
client → source
server → host

Page No.
Date 19 07

TCP/IP Model

↓

Google.com

Appl^n layer | message | pdu

↓

Transport layer | TH | message

↑ 3040

segment | Dest^n port | source port | Message

↓ 80 ↓ Telnet

Resolving DNS get Destination IP.

Service < HTTP, FTP, Telnet, SSH } Well known port:
80 port no.
443.

At source - tempory port assign. Always
Destination - well known port
i.e 80.

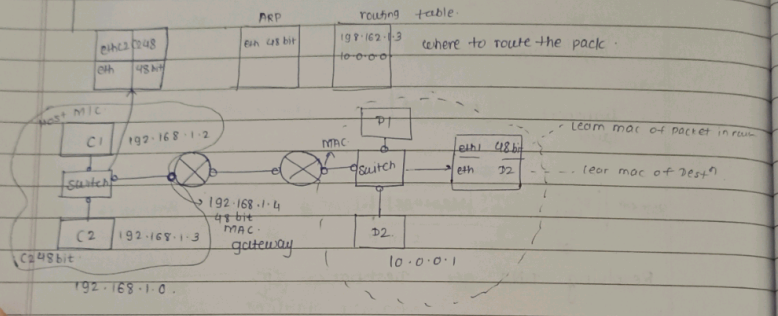
Appl^n layer | Message | pdu

Transport | TH | Message | segment

Network | NW Host | Segment | packet | Dst IP | Sorce IP | Dest port | Source port | Message

DLL | DLL Head | packet | frame | DLL Head → Header → MAC Add S/D | Taller

- To get destination o mac computer sent ARP request to gateway (Router)
- Router also has it's own ARP table and routing table.
- Mode of the switch is to learn the MAC and bit the table & forward



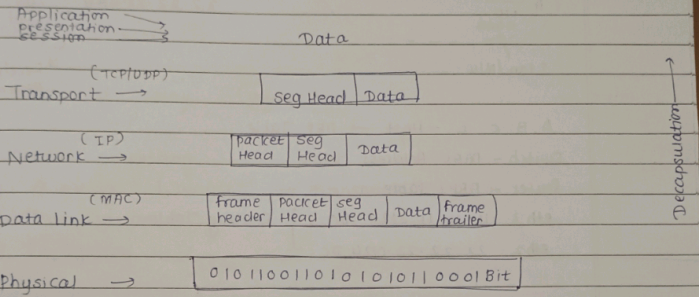
- Every device communicate with each other through mac address.
- Router doesn't touch · packet, message · but touch N/w & MAC.
- Router only known N/w IP.
- Router is used to Route and take decision of routing interface
- ARP Request happen at DLL.

1st chapter – Read Internet, Network Edge, Access network, Core encapsulation & Decapsulation, Host.

Page No.
Date 22/07

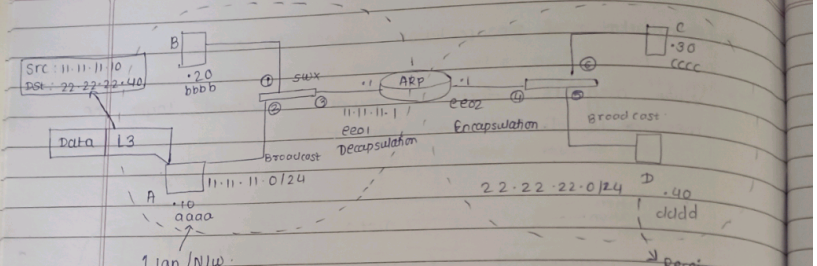
- Encapsulation & Decapsulation in OSI Model

When msg is forward toward transport layer the message is divided into segment.



Q. What is the Dest^n MAC from the given Dest^n IP, Source IP, Source MAC.

- 255.255.255.255 → Broadcast Address.
- Size of MAC Address – 48 bit.
- 6 octats are used for Broadcast Address → FF:FFFF:FF:FF
- /24 → 254 Computer can connect to network.
  /25 → 126.
  11.11.11.0/24
  N/w Add Host



Lan / NIW.

Receive - Decapsulation
Response - Encapsulation

A, B, C, D - Host → ARP Table

Switch - MAC Address table

Router - ARP Table

eth 1 11.11.11.0/24 DC } Routing Table

eth 2 22.22.22.0/24 DC

Q. What are the distributed application in your device that is connected to internet ?

Q. Who produces (RFC's)

private n/w → intranet.

public n/w → internet.

Q. What is connection oriented services and connectionless oriented service.

Q Where TCP / UDP use ? Why the application used TCP.

Q Can host is client or server ? → both.

Page No.
Date 23 07

Q What are the codes used in application layer protocol ?

Q How many imgs are send by web browser?

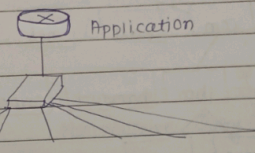
. FTP - client server architecture.

Q Delay. Calculate ?

- Types of Delay (4marks) 24/07

1. Nodal processing
2. Queueing (waiting for transmission)
3. Transmission
4. Propagation

- Application layer - OSI and TCP/IP Models. Chapter 2



DNS Telnet Email DHCP Webserver FTP

DNS - Resolve internet name to IP address
Telnet - Access to server and network devices
SMTP - Transfer of mail messages and
DHCP - Assigns IP address & other parameter to host
Client & server { HTTP - Transfer file to create web pages.
FTP - Transfer file between system.

Page No.
Date

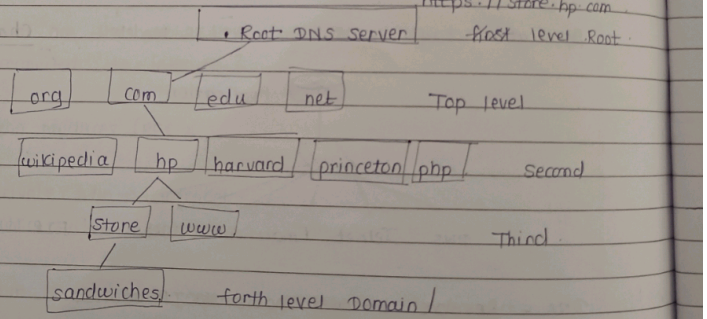
Communication

Peer-to-Peer | Client & Server

Q. What is port of ....

- Commonly used protocols in Application layer
  1. Domain Name system -
  2. Hypertext Transfer -
  3. Simple MTP
  4.

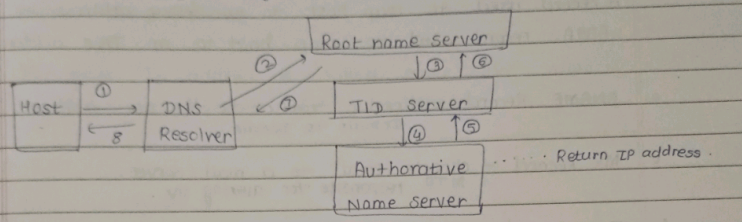
- DNS - Domain Name System.
  To translate a host name into an IP address.
  13 root server in DNS.



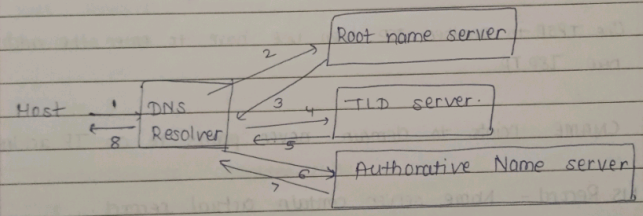
Q. URL given tell the levels.

Page No.
Date

Q Explain Recursive Query.



• Iterative Query



Two types of queries : Recursive ① and Iterative ②.
Nonrecursive Query ③

What is the port used by DNS.
What server hirearchical.
What are the quenes used by DNS to get webpage.
How many Root Server are there.

Page No.
Date 29 07 24

- A and AAAA Records -
  A record used to map host to an IPV4 address
  AAAA record used to map host to an IPV6 address

- CNAME Record - directs traffic to the new address
  Domain to Domain.

- Mx Record - directs email to a mail server.
  MTA responsible for quering mx.

- TXT Record - Resource type

Q. What is the uses of these records? what are other Records

One ISP to another ISP then we have to enter the address of new ISP IP

CNAME points to domain never points to an IP address.

- NS Record - Name server contain actual record.

- - Class type field - Internet
  - Record type field - SOA
  - zone file is always created on Mster server.
  - Name server that server IP server field use to map IP address
  - The refrest time field.
  - The refresh time field.
  - The negative cache
  - SOA is par of the

Page No.
Date

Q ~~For given IP address & subnet mask, find ntw id & broadcast address for given device.~~

Q For given Ip address & subnet mask, find ntw & broadcast address for given device.

DNS: Chapter 2.

1) Explain concept of DNS
2) Types of DNS server → Explain (Resolver, Root, TLD, Authoratiy)
3) DNS Queries (3)
4) DNS Records Resource
(AAAA, A, NS, CNAME, TXT, SOA, PTR.

Chapter 1.

Introduction to Computer N/W
ISP
Internet
IP address public & private
What are the devices used in CN → Switch, router, hub,
~~How~~ Host, end system, distributed applications running on host
client server, p2p
median → wired, wireless
TCP/IP layer and OSI layer difference.
layer architecture
ARP → How mac is obtained.
Which device is used at which layer.

Page No.
Date 30 7 24

- HTTP

Q. What is RFC ? → Request for comment.

Q. private IP has no cost → free.
public IP address has to pay cost because it is provided by ISP.

DHCP contains
↓
Ip address
gateway
DNS

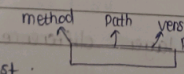
Where is DNS entry ?

Q. Which underline protocol used by HTTP? → Tcp.

HTTP Method - GET, POST, PUT, DELETE. used for request
HTTP status codes - used for response by server.

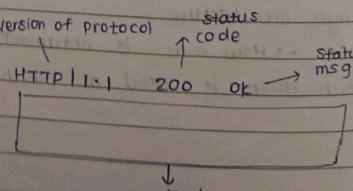
1xx : informational
2xx : success
3xx : redirect
4xx : client error
5xx : server error

200 - ok
201 - ok created
301 - Not modified (cached version)
400 - Bad request
401 - unauthorised.
404 - Not found
500 - Internal



HTTP Request.

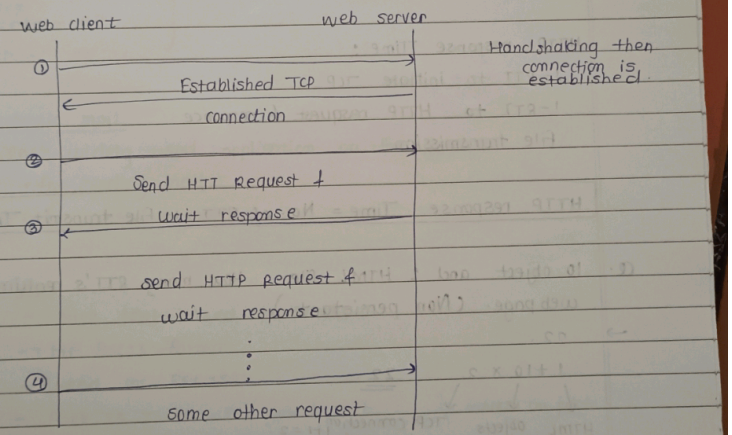
HTTP Respons



Request - [Request Type] — [URL] — [HTTP version]

Response - [HTTP version] — [status code] — [status Phrase]

Q. Status code → can be asked for match the pairs.



Socket → combination of [IP + Port]

Client IP + port → client socket

Server IP + port → HTT / server

Page No.
Date

Internet connection
Reliable data transfer → All this is done by TCP.
Reording of data

Two methods (Types) of HTTP connection → persistant → with pipelining / without pipeling.
Non persistant.

- RTT [round-trip time] — A time for small packet to travel from client to server and server to client.

HTTP response Time :
1-RTT to initiate TCP
1-RTT to HTTP resquest & responce
file transmission

HTTP response Time = No. of RTT + file transmit Time

Q. 10 object and 1 HTML file. How many RTT's required to get web page (Non persistant).

→ 22.

1 + 10 × 2 = 22.

↓ HTML file
↓ objects
↓ TCP connection and resquest HTML. 1+1 = 2.

Page No.
Date

1 TCP + 22 Images 23x2 = 46 RTT NP

23*1 24 RTT P

31/07

Port

- DNS - 53
  HTTP - 80
  SMTP - 25
  POP3 - 110
  Telnet - 23
  DHCP
  ~~Telnet~~ - 67
  FTP - 20, 21

} Commonly used protocols.

- Electronic mail

  Most widely used application on the internet.
  - for sending mail
  - for receiving mail.

1) SMTP
   - pure ~~text~~ based protocol
   - 7 bit ASCII format.
   - Based on RFC 2821.
   - Port 25 - non-encrypted port
     Port 465 - send message securly

   } works on port.

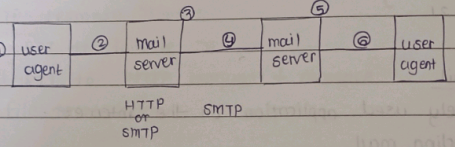
   - Push protocol

Working of SMTP.

220 - service ready
221 - closing trans
250 - Requested action ok
354 - end with <endl> <crlf>

- Internet - mail system
Three major components - user agent, mail server & SMTP protocol

Transfer the email message from user to mail server and other mail server. to another mail server. → main use of SMTP.



HELO	code / command from client	101
EHLO		211
MAIL		214
FROM		220
RCPT TO		221
SIZE DATA		235
QUIT		250
VRFY		354
EXPN		500
HELP		510

code from server

- Email Sever Processes : MTA & MDA.
. Mail Transfer Agent - used to forward email
Receives msg from MUA or another MTA

- Mail Delivery Agent - 1) Accept mail from MTA.
  2) Place it into appropriate mail box

- MUA - mail user agent.

2) POP3 - Post office Protocol (POP3) version 3
   - Pull protocol
   - Uses TCP 110.
   - Download-&-delete mood → retriver server - store locally - Delete server,
   - Download-&-keep mood.
   - works on two port → 110 - Normal.
     995 - secure

3) IMAP - Internet Message Access Protocol.
   - Email is not download, but can retained
   - Any received email is associated with users INBOX
   - Users can create message
   - two port → 143 - Normal
     993 - secure.
   - Web based email - HTTP is used to → Pull (client to server)
     Push
   - Pull protocol.

- Proprietary protocol -
  1) IBM lotus Notes
  2) Novell Groupwise
  2) Microsot Exchange

  Web based -
  1) Hot mail
  2) Gmail

→ Email server process MUA, MTA.
Other internet email format.

Q. What is SMTP, POP3, IMAP → Draw diagram, gives senario and show where it is used.

Page No.
Date 05 08 24

Ports

- Port - A 16 bit number that identifies the application process that receives an incoming message. $2^{16} = 65536$ port
- Reserved port or well known ports (0 to 1023)
  Client can't use this ports. These are standard ports.
  telnet, http, ftp
- Ephemeral port ~~(1024 - 49,151)~~ (49,152 to 65,535)

IANA Ranges
- well know ports - 0 to 1023
- Registered port - 1024 - 49,151
- Dynamic (or private) - 49,152 to 65,535

command - netsh int ipv4 show dynamicport tcp.

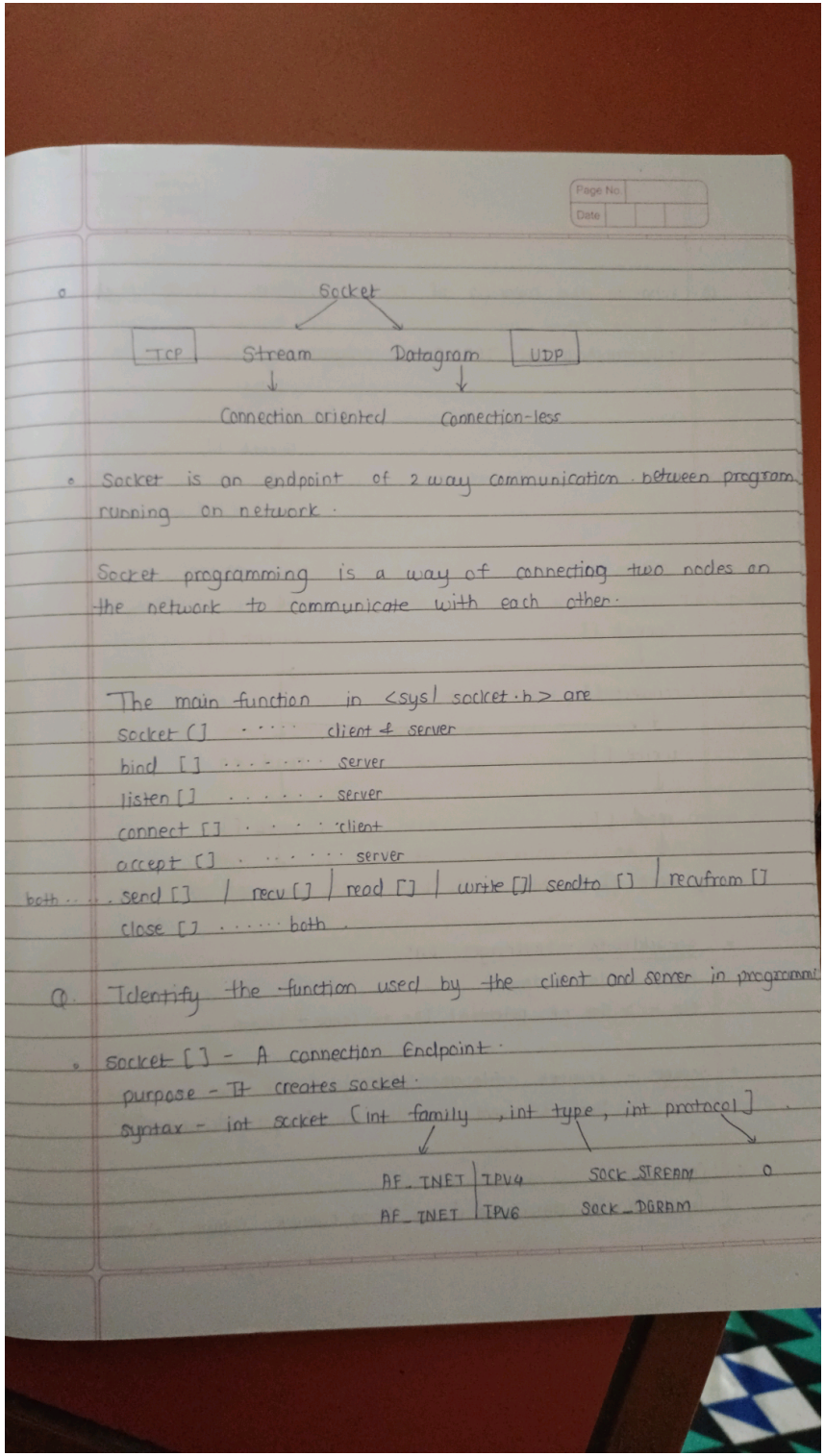
What is the range of ~~1~~ Register Dynamic port ?

- Socket is combination of an 32 bit Ip address and 16 bit port number

Use of socket
1) as an endpoint for communication.
2) A socket is identify by an IP address concatenated with a port.

Q. what is the use of socket ?
Q. Differentiate between socket and port ?

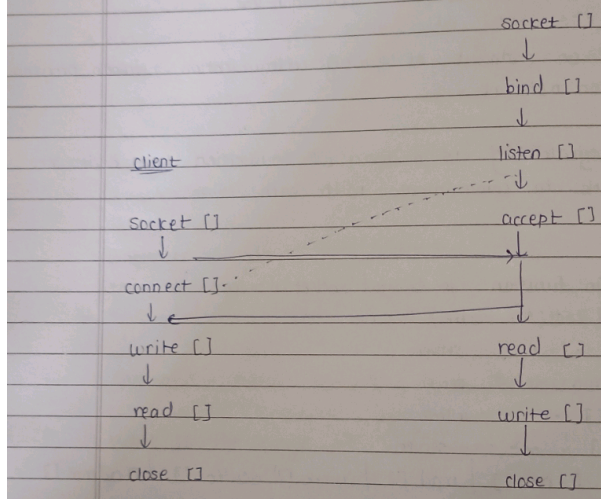
- Socket is interface between Application layer & transport layer.


Page No.
Date
Socket
TCP
Stream
Datagram
UDP
Connection oriented
Connection-less
Socket is an endpoint of 2 way communication between program running on network.
Socket programming is a way of connecting two nodes on the network to communicate with each other.
The main function in <sys/ socket.h> are
socket [] ..... client & server
bind [] ..... server
listen [] ..... server
connect [] ..... client
accept [] ..... server
both ..... send [] / recv [] / read [] / write [] / sendto [] / recvfrom []
close [] ..... both
Q. Identify the function used by the client and server in programmi
Socket [] - A connection Endpoint.
purpose - It creates socket.
syntax - int socket [int family , int type , int protocol]
AF_INET | IPV4 SOCK_STREAM 0
AF_INET | IPV6 SOCK_DGRAM

Page No.
Date

Q. What is the meaning of socket primitive TCP socket.

- Understanding of TCP socket programming.



- getaddrinfo - Leverages DNS.
  ilp - a dns hostname
  olp - a list of potential IPs to connect / listen.

- Socket - creates a file descriptor, just like open.
  Doesn't event use the olp of getaddrinfo

- Connect -
  Given a file descriptor & an IP to connect, create a connection.

- send & recv
  Given a connected file descriptor, submit bytes to the OS for delivery bytes

- close
  Given ~~|~~ ~~-|~~ ~~|~~, tell kernal that it can terminate this connection.

- bind
  ~~—|—~~, tell the kernal to associate with given IP:port.

- listen
  ~~—|—~~ that has been binded to IP|port, tell the OS that you wish to start receiving connections.

- accept
  ~~—|—~~ that has already been activated via listen, create a new FD that can be used to communicate with individual client. By default this call block until client show up.

```
#
import socket

#
server_socket = socket.socket(socket
```

198 - 2 | 198 | 0
2 | 99 | 1
2 | 49 | 1
0 0 1 1 0 0

110 00 110
class C

Page No.
Date 06 08 24

- ~~Transport Layer~~

17 N/w bits — class A 2^7 — N/w (8 bits) — Network N/w — 0NNNNNNN — Host host host — 1-126 — /8

class B 2^6 — 10NNNNNN — N/w — host — host — 128-191 — /16

class C 2^5 — 110NNNNN — N/w — N/w — host — 192-223 — /30

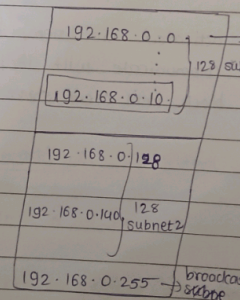
class D — 1110 MMMM — multicast group — — — 224-239

class E — Research.

Q. Binary 1st octact is given find out the class.

- ~~Subnet Size~~ — /24 to /30.

class C subnet mask /24.



and 192.168.0.10
255.255.255.0 → sub netmask
192.168.0.0 → N/w id.

192.168.0.10
Or
255.255.255.0
192.168.0.255 → Broadcast address

/25 ⇒ Bit by bit and operation.

255.255.255.0000 0000
2800

192.168.0.20
and 255.255.255.128
192.168.0.0

0.0.0.127 inversion of 255.255.255.128

or 192.168.0.20

255.255.255.128

192.168.0.127 → Broadcast Address.

192.168.0.140 ← 2nd subnet

255.168.0.128

192.168.0.128 → start address of subnet 2.

Subnet /28

255.255.255.240

No. of subnet -16

Host per subnet - 2^4-2 =14.

8 8 8 4 ubit $2^4=16$

255 255 255 0 000

128 64 12 16 8421

192.168.0.250.

255.255.255.240

192.168.0.240 → Nw id.

0.0.0.239 } 16 bit

192.168.0.250

192.168.0.255 → Bn id.

If subnet is /30 2 computer can be connected.

class A 10.0.0.10 /25 → 2^{17}/128 (subnet bit per subnet address) 255.0.0.0. 8+8+1=17

Class B 172.16.0.10 /25 → 2^9/128

class C 192.168.0.10 /25 → 2^1/128.

Page No.
Date 07 08 24

Transport Layer

TP Layer Process to process communication
Nw Layer Host to Host communi
DLL Node to Node communi

- Transport layer is responsible.
  1. Service point and addressing.

- Process level addressing
- Multiplexing & Demultiplexing
  Q where multiplexing & Demultiplexing occurs.
- Segmentation, Packaging & Reassembly → host.
- Connection Establishment & Management and Termination
- Acknowledgment
- flow control

- Network layer, Transport layer

- Process to process achieve through client-server paradigm.
  process on the local host - client,
  need services from a process on remote host - server.
  for communication we must define.
  1) local host - IP
  2) local process - port
  3) Remote host - IP
  4) Remote process - port
     0-65536. (16 bit).

MSS - Maximum segment size - TPL
MTU - maximum Tranfer unit - NL

Page No.
Date

Provide -
- aggregate data from different applications into a single Stream - Multiplexing.
- distributing that data to different application - Demultiplexing.

Segmentation - host , fragmentation - every node.

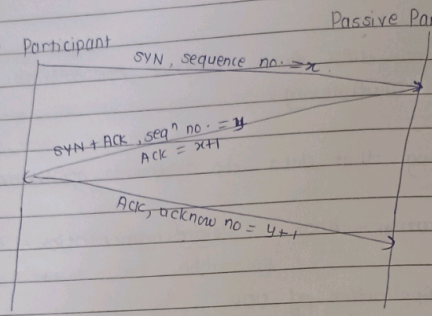
- Popular Application of UDP.
  1) Multimedia Streaming.

Q What are the applications supported by UDP
→ DNS TFTP RTP.
SNMP NFS
BOOTP NTP

Q Difference between TCP & UDP.

* Connection (Establishing) between sender & receiver → connection oriented.

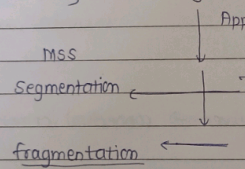
- UDP data Reassembly.
- TCP Protocal → Provide a reliable, in-order, byte stream abstract
  - flow and ~~cegne~~ congestion control.
- TCP Segment Reassembly
- Connection creation.
  - Active participant (Client)
  - Passive participant (Server).



three-way handshaking

Q. If seqⁿ x what is the acknowment no ? → y+1.

- Three-way handshaking.

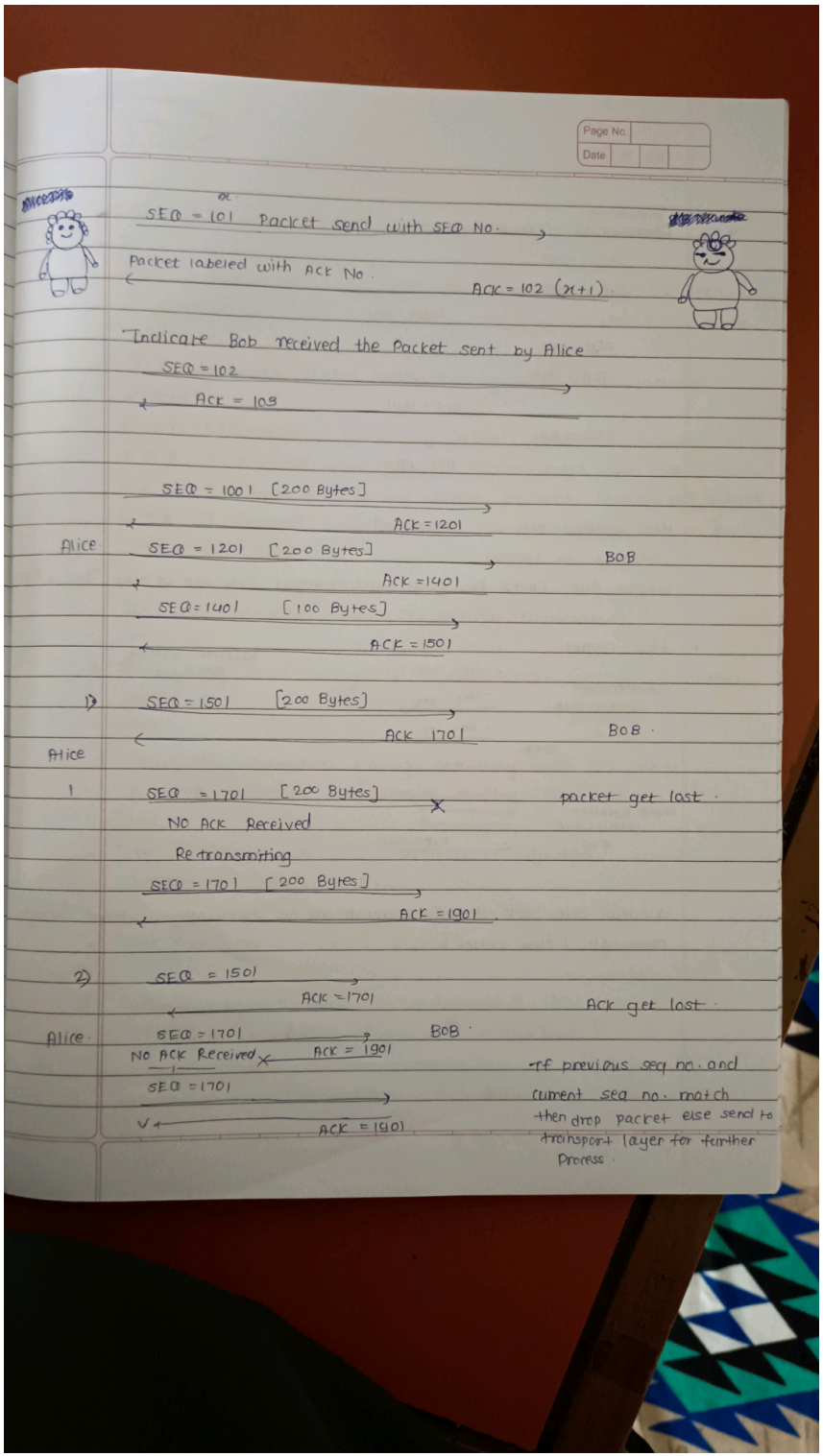


Q. Why segmentation is done at transport layer & why fragmentation is done at Ntw layer?

Maximum Transport unit (MTU) 1500 bytes.

→ In between node at router fragmentation is done.
Host perform segmentation.

If DF = 1 at router → Drop packet from router to router.
If DF = 1 at receiver → fragment is received by receiver (do not fragm DF | Do not fragmenent)



SEQ = 101 Packet send with SEQ No. →

Packet labeled with ACK No.

← ACK = 102 (x+1)

Indicate Bob received the Packet sent by Alice

SEQ = 102 →

← ACK = 103

SEQ = 1001 [200 Bytes] →

← ACK = 1201

Alice SEQ = 1201 [200 Bytes] → Bob

← ACK = 1401

SEQ = 1401 [100 Bytes] →

← ACK = 1501

1) SEQ = 1501 [200 Bytes] →

← ACK 1701 Bob.

Alice

1 SEQ = 1701 [200 Bytes] → X packet get lost.

No ACK Received

Retransmitting

SEQ = 1701 [200 Bytes] →

← ACK = 1901.

2) SEQ = 1501 →

← ACK = 1701

ACK get lost.

Alice. SEQ = 1701 → Bob.

No ACK Received ← X ACK = 1901

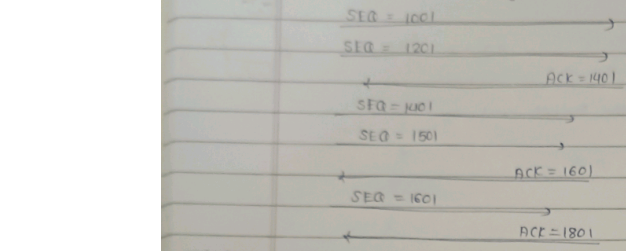
SEQ = 1701 →

← ACK = 1901

If previous seq no. and current seq no. match then drop packet else send to transport layer for further Process.

Page No.
Date

- Cumulative Acknowledgement:



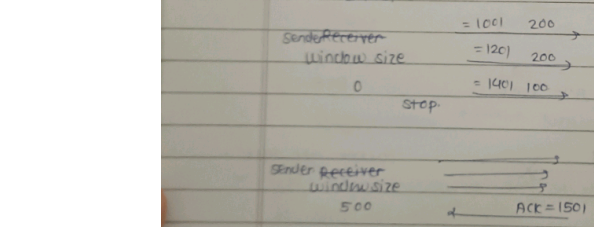
Window Size

Q How window size is determined.

Depends on receiver.

Window size limits how much unacknowledged data can be sent. "byte in flight"

- Flow control



Window size sent in each segment can be dynamically updated through connection (flow control).

Page No.
Date 13 08

Initial Sequence Number

TCP is bidirectional - both peers can send data. Both the peer have SEQ to track bytes send. Both peer have an Ack # to track

+ TCP connection starts with 3-way handshaking, includes 4 events:

A → B SYNchronize with my initial sequence Number of X.
A ← B I received your SYN, I Acknowledge that I am ready [X+1]
A ← B SYNchronize with my initial sequence Number of Y
A → B I received your SYN, I Acknowledge that I am ready for [Y+1]

Q. TCP Connection setup. Three way handshaking?

+ four-way handshaking with FIN flags. Graceful connection closing

+ Ungraceful connection closing one-way with RST flags
A ⟷ B something went wrong sending RESET flag.

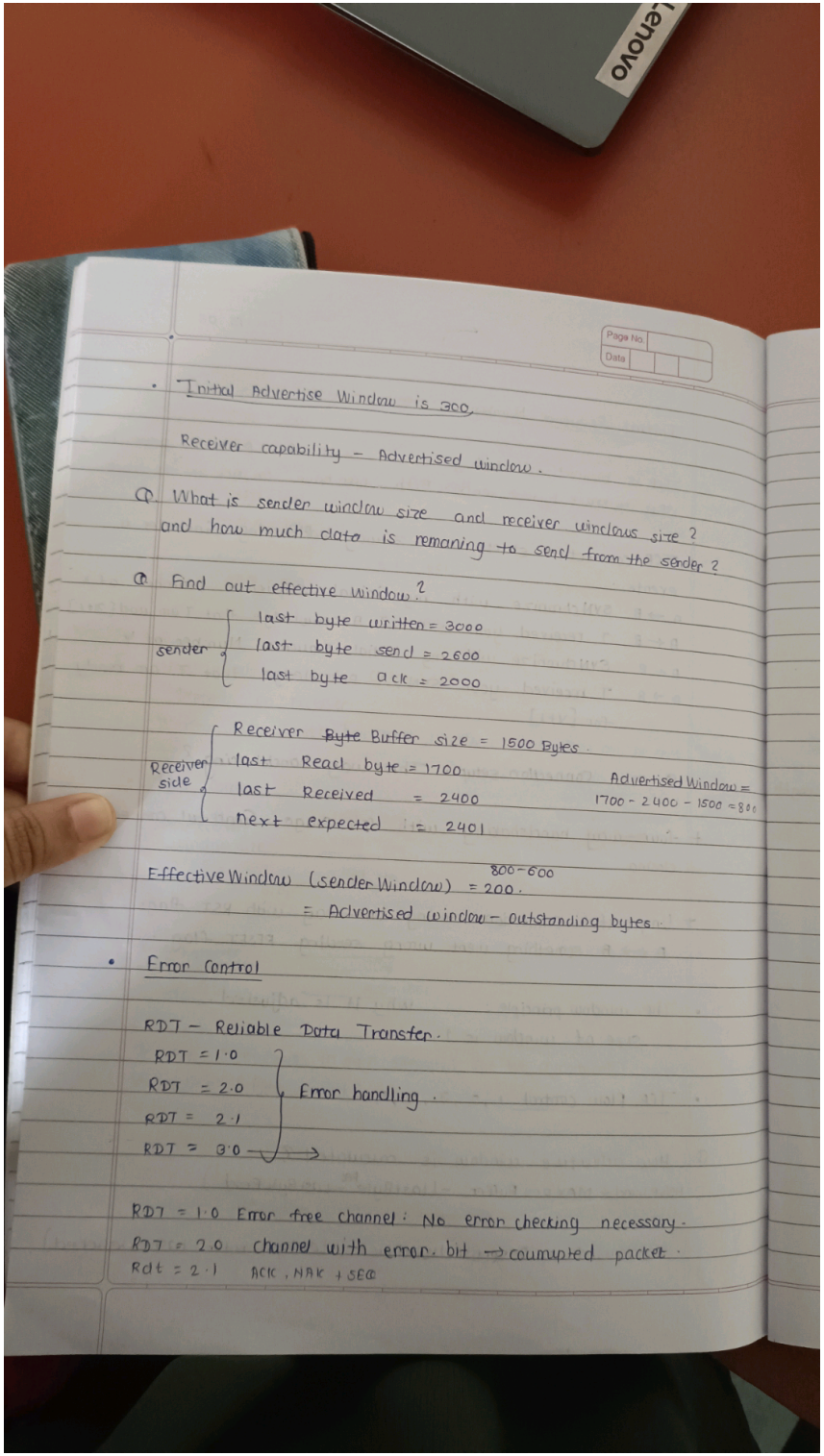
- The window principle: why it is adjusted.
size of window is 1.

- TCP flow control 1, 2, 3, 4, 5, 6

Q. How advertise window is calculated?

AdvWind = MAX RcvBuffer - (LastByte^{Rec} - LastByteRead)

SenderWindow = AdvertisedWindow - (LastByteSent - LastByteAcked)



- Initial Advertise Window is 300,

  Receiver capability - Advertised window.

Q. What is sender window size and receiver windows size ? and how much data is remaning to send from the sender ?

Q. Find out effective window ?

sender:
- last byte written = 3000
- last byte send = 2600
- last byte ack = 2000

Receiver side:
- Receiver ~~Byte~~ Buffer size = 1500 Bytes
- last Read byte = 1700
- last Received = 2400
- next expected = 2401

Advertised Window = 1700 - 2400 - 1500 = 800

Effective Window (sender Window) = 200. (800 - 600)

= Advertised window - outstanding bytes.

- Error Control

RDT - Reliable Data Transfer.

RDT = 1.0
RDT = 2.0
RDT = 2.1
RDT = 3.0 → Error handling.

RDT = 1.0 Error free channel : No error checking necessary.

RDT = 2.0 channel with error. bit → coumupted packet.

Rdt = 2.1 ACK, NAK + SEQ

- Handling Bit Errors:
  Error detection

- Corrupt Ack / NAK packet
  option 1
  Sender interrupts corrupt ACK / NAK = Act.
  Receives misses data packet.
  option 2. RDT 2.0 without sequence number.
  sender interrupts corrupt ACK / NAK.

Bug fix - with seq^n no.
Pack to mode = 0
Pack to mode 1
Pack to mode = 0
} seq^n number.

Version 2.1 . with seq^n no. SEQ + ACK + NAK.
2.2 with SEQ + ACK without NAK. → corrupted packet

- Lost Packets
  Packet lost , Handling lost packets → packet lost
  Versim 3.0 with SEQ + ACK + Timeout.

- Performance Problem with stop-and-wait (wait too long).
  T_T = transmission Delay $\approx \frac{64\,KB \times 8bits/B}{10\,Mbps} = 5ms$

$$\frac{T_T}{T_T + nlw\ entity} = \frac{T_T}{T_T + RTT}$$

19/08

- Piplined protocol - error handling method ?
  Go Back N (GBN)
  Why seq no. is small in selective ~~and~~ repeat protocol.

- TCP connection setup.
  Three way handshake.
  TCP SEQ + ACK.
  Q what is ACK & SEQ ?

- Selective Acknowledgement Option (SACK)

20/08

- TCP Header & UDP Header
  Q Find out sequence number.
  Source port, destination port, seq^n number, Ack number, Header length
  Reserved bits, URG Bit, ACK bit, PSH bit, RST bit.
  Header length (4 bits)
  Q what is the size of TCP header.
  0101 → 5 (5d)
  1010 → A (10d)
  1111 → F (15d)

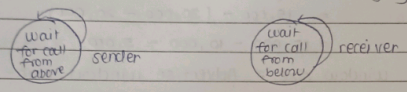
- Concept of scaling factor -

  Q Hex value will be given. using Hex 1 bit, 2 bit ..... find IP, Port, flag set, length.

- UDP Header contains four fields :-

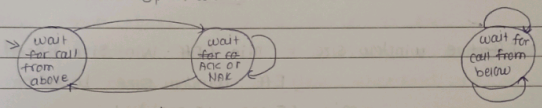
  Cheksum calculation → find sum and negate the sum.

- Underlying channel perfectly reliable
  1. No bit errors
  2. No loss of packets.
- Seperate FSMs for sender, receiver:
  1. Sender sends data into underlying channel
  2. Reciver read data from underlying channel.



- RDT 2.0: FSM Specification.

12 marks



sender

Q. What is difference between RDT 2.1 & RDT 2.0 → (seq^ no. is decoded)

RDT 3.0: Sender (Timer is introduced)

Lab → Implement Rdt 2.2 and 3.0.

21-08-24

- Congestion Control

2m / 3m Q Sample Question - Flow control ang ~~cogne~~ Congestion Control)

. Consider the status of a TCP connection at the source and destination as shown in the figure and table below. let the congestion window size be 15,000 bytes.

Notation	Description	Byte SEQ No.
a	last byte Ack	20,000
b	last byte sent	30,000
c	last byte read	15,000
d	last byte Received	20,000

Page No.
Date

a) only congestion control b) only flow control c) Both fc & cc

b) 1. Calculate Advertise window.

MAX Rev Buffer − (lastByteRevd − last Byte Read) = 25,000

~~30,000 − (15,000 − 20,000) = 15,000 − 10,000 = 5~~

a) 2. Minimum of congestion window.

= MAX Recei Buffer − (Last Byte Received − last Byte Read

Effective window size = Congestion window − (last byte sent − LB Ack)

= 15,000 − (30,000 − 20,000)

= 15,000 − 10,000 = 5,000

b) 1.1. Effective window size = Advertise window size − (LB.sent − LBA)

= 25,000 − (30,000 − 20,000)

= 15,000

c) 3. Effective window size = Min (Eff. Win. Size based on flow control, Eff window size based on cong. control)

= min (5,000 , 15,000) bytes

= 5000 bytes.

- Congestion Control in TCP

cw = 1 it gets Ack then cw=2. when both get Ack cw=4.

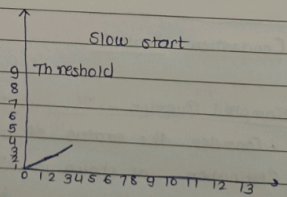
$2^0 = 1$

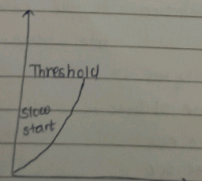
$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

exponential Increase





when it reaches to threshold it chang the state. and increases by only one.

- Two states.
  1) TCP has two state: slow start and cognetion Avoidance.
  2) A window size threshold governs the state transition.

- AIMD (Additive increase & Multiplicative Decrease).
  1 to 20, packet loss, 20 to 10, 10 to 30, packet loss, 30 to 15, 15 to 20, packet loss, 20 to 10, 10, to 16 packet loss. 16 to 8, 8 . . .

1. Slow Start.
   Initial cw is 1
   slow start phase : 1, 2, 4, 8, 16, 32, 64
   When it is about to reach 64? window size reduces to 1
   First time reach threshold, New threshold is set to half of previous : 40/2 = 20.

2. Fast Recovery (No threshold).
   when packet lost it will go to half of previous window size.
   slow start + AIMD. is used here.

slow start - Exponential increas until congestion window reaches congestion threeshold or Advertised window.

Ex. 30 packets are send, if 15 packet is loss, 22nd and 27 packet is lost, 5th packet lost. By using AIMD how many RTT's are required to send 30 packets.

RTT	Seq no. packet
①	1
②	2, 3
③	4, ⑤, 6
④	5

RTT	Seq no. of packet.
5	6, 7
6	8, 9, 10
7	11, 12, 13, 14
8	(15), 16, 17, 18, 19
9	15, 16
10	17, 18, 19
11	20, 21, (22), 23
12	22, 23
13	24, 25, 26
14	(27), 28, 29, 30
15	27, 28
16	29, 30,

- It takes 16 RTTs to send 30 packets.

throughput = (30 packet * 1kB) / (16 RTT * 100 ms / RTT)

= 153600 bit/sec.

Q. Slow start + congestion avoidance.

packet lost : 5, 15, 22, 27

→

RTT	Seq No. of packet
1	1
2	2, 3
3	4, (5), 6, 7
4	5 cong. Threshold = 2 (Threshold = cw = 2)
5	6, 7
6	8, 9, 10
7	11, 12, 13, 14
8	(15), 16, 17, 18, 19 cong. Threshold = 2 (Threshold = cw = 2)
9	15
10	16, 17
11	18, 19, 20
12	21, (22), 23, 24 cong. Threshold = 2
13	22
14	23, 24
15	25, 26, (27) cong. Threshold = 1 (Threshold = (cw)/2 = 1

16	27
17	28, 29
18	30

It takes 18 RTT to send 30 packets.

The throughput = $\frac{(30 \text{ packet} * 1 \text{ KB/packet})}{(18 \text{ RTTs} * 100 \text{ ms/RTT})}$ = 136533 bit/sec

27-08

- Fast Recovery

Q. Solve same problem using fast Recovery 5, 15, 22, 27. How many RTTs will be required to sent 30 packets.

1	1
2	2, 3
3	4, (5), 6, 7
4	5, 6
5	7, 8, 9
RTT=15 6	10, 11, 12, 13
7	14, (15), 16, 17, 18
8	15, 16
9	17, 18, 19
10	20, 21, (22), 23
11	22, 23
12	24, 25, 26
13	(27), 28, 29, 30
14	27, 28
15	29, 30

$w = 4/2 = 2$

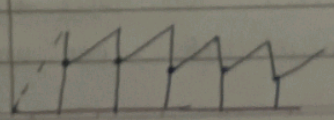
$w = 5/2 = 2$

$w = 4/2 = 2$

$w = 4/2 = 2$.

1st Exponential increase

2nd Additive increase.



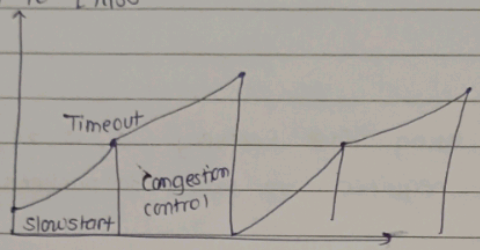
Imp • TCP Tahoe (4-6 marks)

Slow start and congestion avoidance

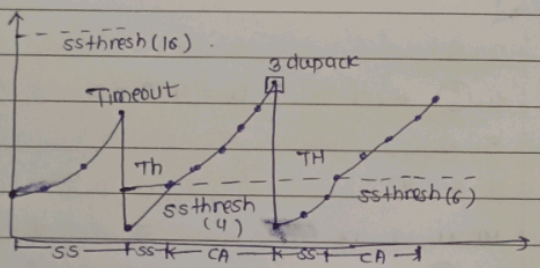
TCP Tahoe treats the two signs used for congestion detection,

time-out three duplicate ~~segmen~~ ack.

cwd to 1 MSS



(16 marks)



Packet lost, Ack loss, Delay Ack } timeout

- TCP Reno

two signals of ~~cogne~~ congestion

time-out the arrival of three duplicate Acks

It behaves like the slow start, in which cwd grows exponentially cwd start with the value ssthresh plus 3 MSS (instead of 1)

Q. Same problem → Difference between TCP Tahoe & Reno?

Q. What is the threashold value in TCP Tahoe and Reno?

"TCP Tahoe : SS + AI + Fast Retransmit"

Step 1 - Assume that the cwd = 8 and sender has sent segments 31-38, and 31 is lost.

Step 2 - Receiver will reply with 7 duplicate ACKs of segment 30 (indicating the it is waiting for 31).

Step 3 - On receiving 3 duplicate ACKs, ~~would~~ cwnd is set to 1 & 31 is retransmitted, and SS phase is started.

Step 4 - Restart in slow start by sending segment 39.

EX. TCP Tahoe (1/2), (2/2)

- TCP state Transition Diagram (do it own)

  Connection establishment and connection reestablishment. (do it own)

- Web caching and DNS caching - chapter 2.
- CDN
- Bit torent in p-to-p architecture.

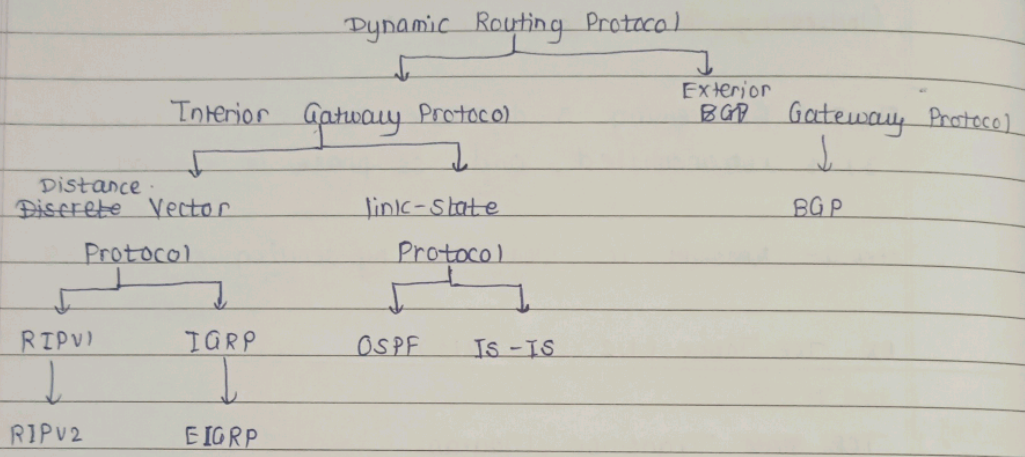
Page No.
Data

Chapter # 4

- Static Vs Dynamic Routes.

- Routing Protocol

Q. Diagram is given where BGP and IGP used ?



1) Distance Vector Routing Protocols:

Provides two characteristics → Distance → how far destination is.
Vector → Direction of the next-hop

R_1 and R_2 should be in one subnet.

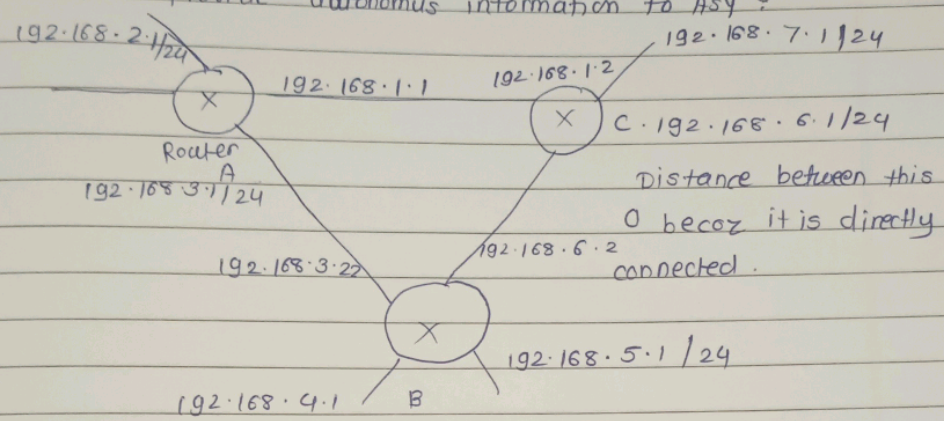
2) Link State Routing Protocol.

3) Interior Gateway Protocols

4) Exterior gateway protocol is used to do this:
ASx and ASy

Page No.
Date

Q. How Asx provide autonomus information to Asy?



Distance between this is 0 becoz it is directly connected.

- Metrics - is a variable assigned to routes as a means of wrost or from most preferred to least pereferred.
- Hop Count -
- Bandwidth
- Load
- Autonomous System (AS)
  - collecting of routers whose prefixes & routing policies are under common administrative protocol.

Dynamic IGP :- Protocol used to distribute routing information within an AS.

Dynamic. EGP :- [Exterior Gateway Protocol]

- Switching via bus
  - datagram from i/p port memory to o/p port memory via shared bus
  - bus connection : switching speed limited by bus bandwidth
  - 32 tbps

- Switching via interconnection network or Crossbar
  - mutistage switch
  - exploiting

* Input port Queuing
  - queuing delay or loss due to input buffer overflow
  - Head-of-the-Line (HOL) blocking : (2 marks)

* Output port Queuing
  - queuing and loss due to o/p buffer overflow !

04-09

- Buffer Management
  1. drop < tail / proprity
  2. marking
  3. Random

- Packet Scheduling : FCFS
  - first come, first serve
  - priority
  - round robin
  - weighted failure queue

- FIFO

- Queue Operation
  1. Packets are served in the order they arrive
  2. After the transmission of packet

- prioritized Traffic

  prioritized Queuing
  Operation prioritized Queue with Two priority classes - 1) high priority 2) low priority
  packet arrival and Transmission

- Packet Classification
  1) High priority 2) low priority class
  pckt 1 pckt 2
  pckt 3 pckt 5
  pckt 4
  pckt 6

- Scheduling Policies: Round Robin Discipline
  - packets are sorted into classes similar to ~~pkt~~ priority queuing
  - Basic operations
  - Operation of Two-classes Round Robin Queuing
  - class 1
    class 2
  - packets: class 1: pckt 1, pckt 2, pckt 4
    Class 2: pckt 3 pckt 5

- Weighted Fair Queuing
  Scheduling Mechanism

- Sidebar: Network Neutrality
  What is network neutrality?
  - technical: how an ISP should share / allocation its resources → packet scheduling, buffer management etc. and mechanism
  - social, economic principles
    - protecting free speech
    - encouraging innovation, competition
  - enforced legal rules and policies
  Different countries have different "takes" on network neutrality.

- IPV4 Header format.
  IPV4 checksum is applied to only header not for entire segment.
  Version -
  Header length - min 20 byte max 60 bytes.

Q. calculate, version, header length, IP address, source and destination address. find ?

Q. When an IP datagram fragmented ?

- DF Bit -
  DF = 1 no fragmentation
  DF = 0 allow for fragmentation.

- MF Bit
  MF = 0 - last fragment
  MF = 1 - given permission for paise fragmentation on process begin.

- Fragment Offset - 13 bit field
  Q - Size of datagram is given what is the no of fragmentation can be done ?

- Time to live

- Concept of scaling factor
  fragment offset value field = fragment offset | 8.

Time to live value is decremented by 1 when packet moving from one hop to another.

If the value of TTL becomes 0 befor reaching the destination, the datagram discard.

- Protocol field
  - protocol number of ICMP is 1, IGMP is 2, TCP is found 6 and UDP is 17

- Header checksum
  Computation of header ~~contains~~ checksum includes IP header only
  At each intermediate device checksum is checked.

Source IP

Destination

Options - This field is used for several purpose.
1. Routing
2.