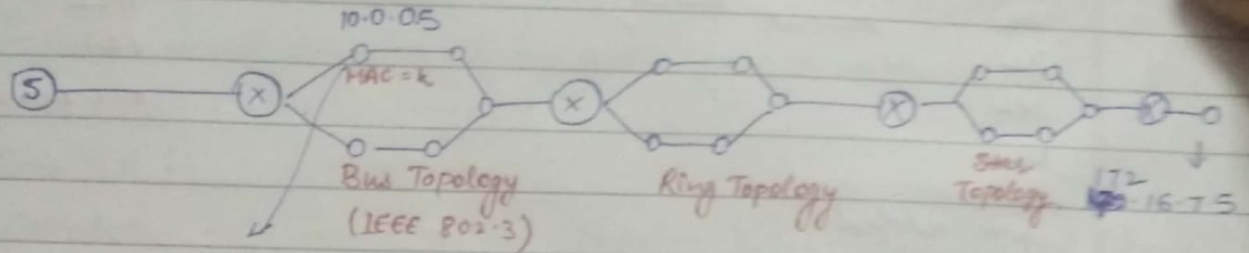
Date: 02/06/18
Page No.

(If in a website, there is some window with cricket score, It is considered as urgent ∴ early reply)

02/06/18

→ Transfer of data in a WAN Network / Internet :



C:\> ping -t 172.16.7.5 ↵

SIP	DIP
10.0.0.5	172.16.7.5

frame

↓ converted to ARP packet

S.MAC	D.MAC	SIP	DIP
k	?	10.0.0.5	172.16.7.5

ARP Packet

This packet will be broadcasted on the LAN network. (bus topology) but there will be no response bcz DIP does not belong to this network.

Then this packet will reach the next router, here the ARP packet is removed and only encapsulated frame reaches the router.

At the right side junction of router, this frame is again encapsulated in the packet of new LAN network.

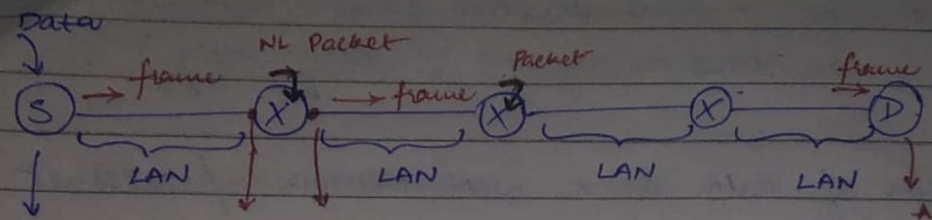
This shedding & encapsulation keeps on happening till we reach destination system in WAN network.

So actually only frames are transmitted over the WAN.

Scanned by CamScanner

Date : / /
Page No.

→



DATA
AL
TL
NL
DLL
PL
are added.

DLL PL removed

DLL PL added

AL TL NL DLL PL are removed.

PH	DH	NH	TH	AH	Data

Now this whole will be forwarded

∴ we can say bits are transmitted or frames is transmitted.

When the frame passes through a network & reaches the exit point of a router, then PH & DH are removed ∵ 2 layers are touched & | NH | TH | AH | Data | is forwarded. This is a packet.

When this packet reaches the entry point of next network, DH & PH of next network will be added. Now this frame will be forwarded over the network.

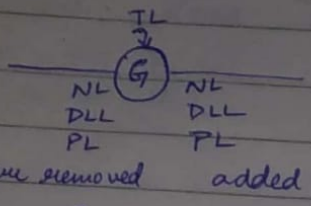
Router touches three layers → ~~DLL~~ NL, DLL, PL

∴ It is called a three layer switch.

Scanned by CamScanner

Date : / /
Page No.

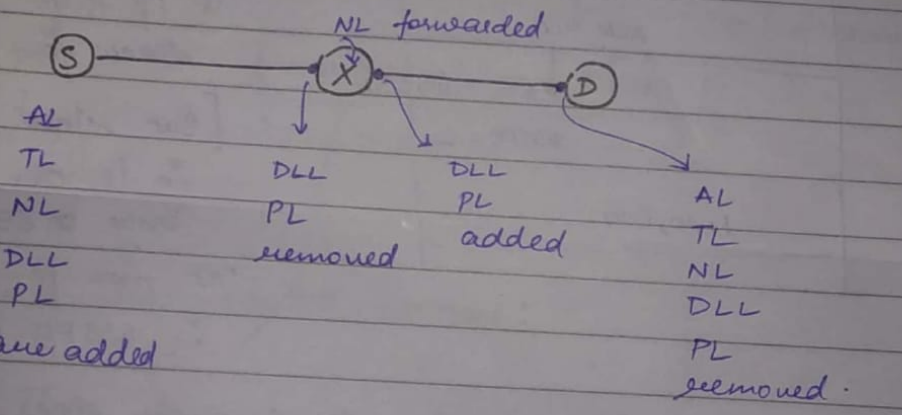
→ Gateway is an all layer switch. as it touches all layers.



- Gateway is costlier
- It is used at the entry gates of a country.

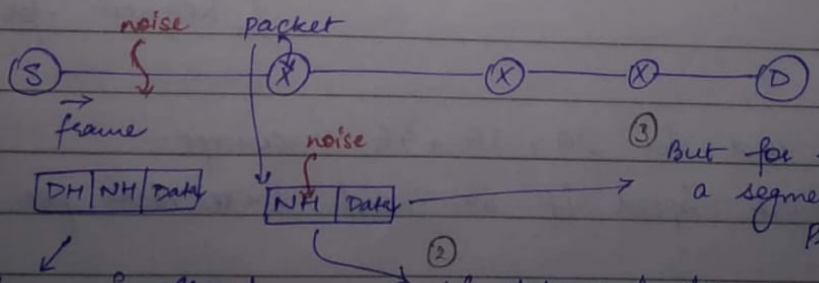
EXAMPLE :

Calculate how many times N.L. , D.L.L. are visited from S to D ?



∴ DLL is visited 4 times
& NL is visited 3 times.

TCP protocol provides checksum to protect segment from potential errors inside a router.



① If frame is altered by noise, CRC is present to detect

② If Network header is altered, IP protocol provides header checksum

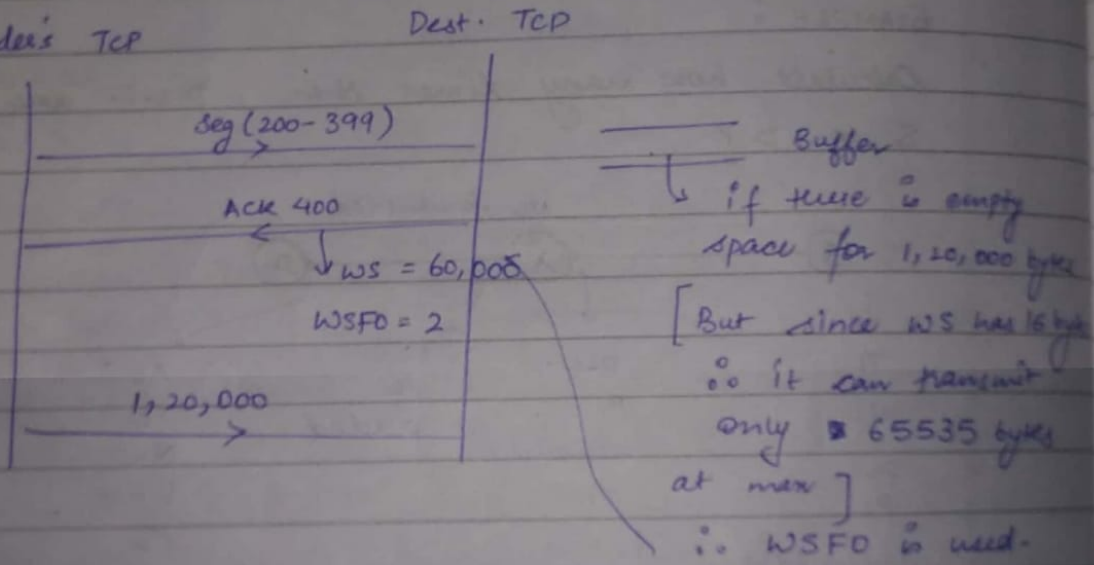
③ But for this data i.e. actually a segment, checksum is provided by TCP protocol

Scanned by CamScanner

* TCP calculates checksum only at the sources & again at only destination.

→ OPTIONS & PADDING :

1) WINDOW SCALING FACTOR OPTION : (WSFO)



* Thus, we can have segment of any size But the standard segment size is :

W.S. * W.S.F.O

$2^{16} * 2^{14}$ → This is provided by RFC

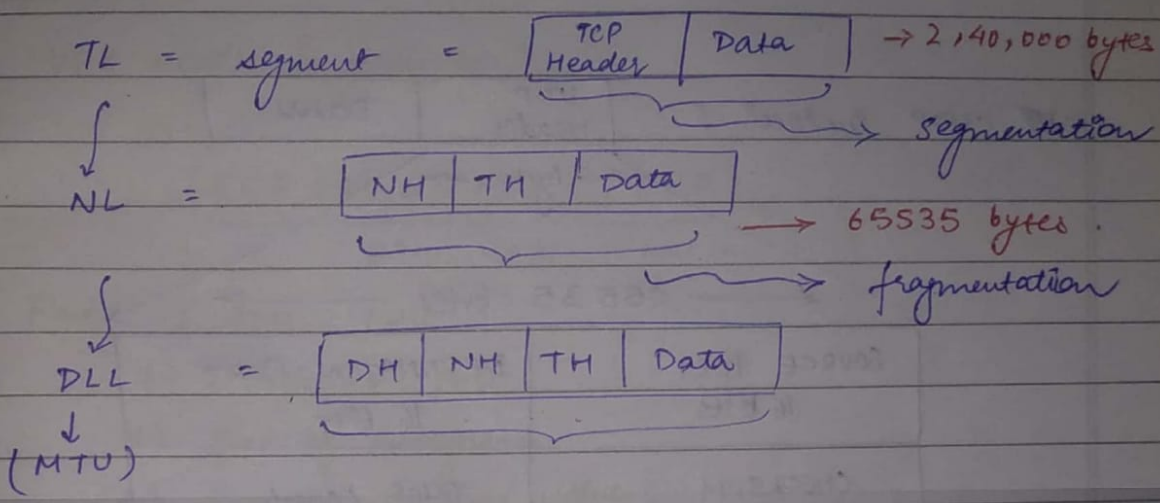
(Request for comment)

→ WSFO is used for 2G, 3G, 4G concept.
We get more speed if we send more data per segment.

Scanned by CamScanner

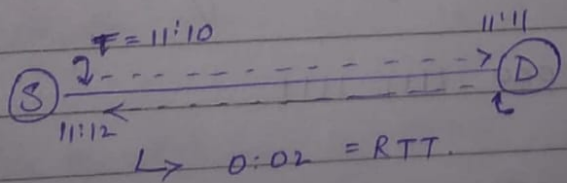
→ When TL is giving data to NL, segmentation is done to fit the data in max. allowed packet size of 65535 bytes.

Fragmentation is done by the routers when NL is giving data to DLL to fit it in the allowed MTU.



2.) TIME STAMP OPTION:

Time stamp option is used for calculating round trip time between ~~to~~ two end processes.



3.) NOP OPTION:

It is used to fill up the gaps b/w options.

4.) EOP OPTION:

End of operation option is used as a seperator b/w

Scanned by CamScanner

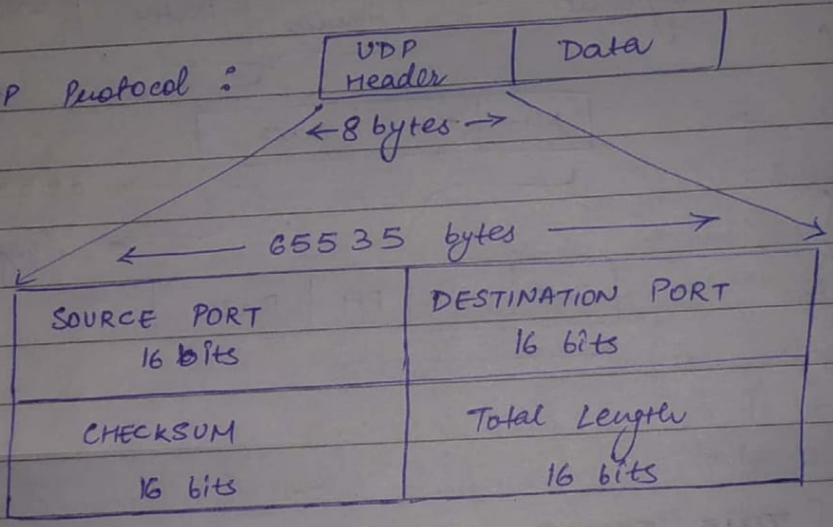
Date : / /
Page No.

4.) EOP ~~OPT~~ OPTION :

UDP Protocol :

↓ Datagram

~~UDP~~ UDP Protocol :



Example :

Total length bits of a datagram :

0000 0000 1111 1111

Find size of datagram

size of payload (data)

size of datagram = $2^0 + 2^1 + \cdots + 2^7$

= 255 bytes.

size of payload :

Scanned by CamScanner

Date : / /
Page No.

Header + Data = Datagram

$8 + x = 255$

$x = 255 - 8$

$= 247$ bytes.

EXAMPLE :

UDP Header is given as :

$(\underbrace{FFF}_{S.P.}\ \underbrace{000}_{D.P.}\ \underbrace{50}_{}\ \underbrace{FFFE}_{Checksum}\ \underbrace{FFFE}_{Total\ Length.})_{16}$

Find 1) Source port
2.) Destination port
3.) Size of datagram
4.) Size of payload value
5.) Is the datagram travelling from ~~xxxx~~ client to server or vice versa ?

1.) Source Port = FFF0 = 65520 → dynamic port

2.) Destination port = 0050 = 80 → fixed port / predefined port

3.) Size of datagram = FFFE
= 65534 bytes.

4.) Size of payload value = 65534 - 8
= 65526 bytes.

5.) the datagram is travelling from dynamic port to fixed port
∴ It is travelling from client to server.

Scanned by CamScanner

→

TCP	UDP
1.) Dynamic Header (20-60 bytes)	1.) Fixed Header (8 bytes)
2.) Flow control	2.) Has No flow control.
3.) Checksum is mandatory	3.) Checksum is optional
4.) Provides error control	4.) has No error control.

TCP is more reliable than UDP as it provides flow control, error control, checksum but it is slow but UDP is faster. but unreliable. (reliability is taken care at Application Layer)

5.) TCP does not support multicasting & broadcasting	5.) UDP supports both.
6.) HTTP, FTP, SMTP, TELNET.	6.) DNS, TFTP, SNMP
7.) TCP with IP is connection oriented protocol	7.) ~~TCP~~ UDP with IP is connectionless protocol

→ TCP is a connection oriented and IP protocol in NL is connectionless, unreliable & best effort

∴ TCP in TL and IP in NL together is connection oriented approach / protocol.

Scanned by CamScanner

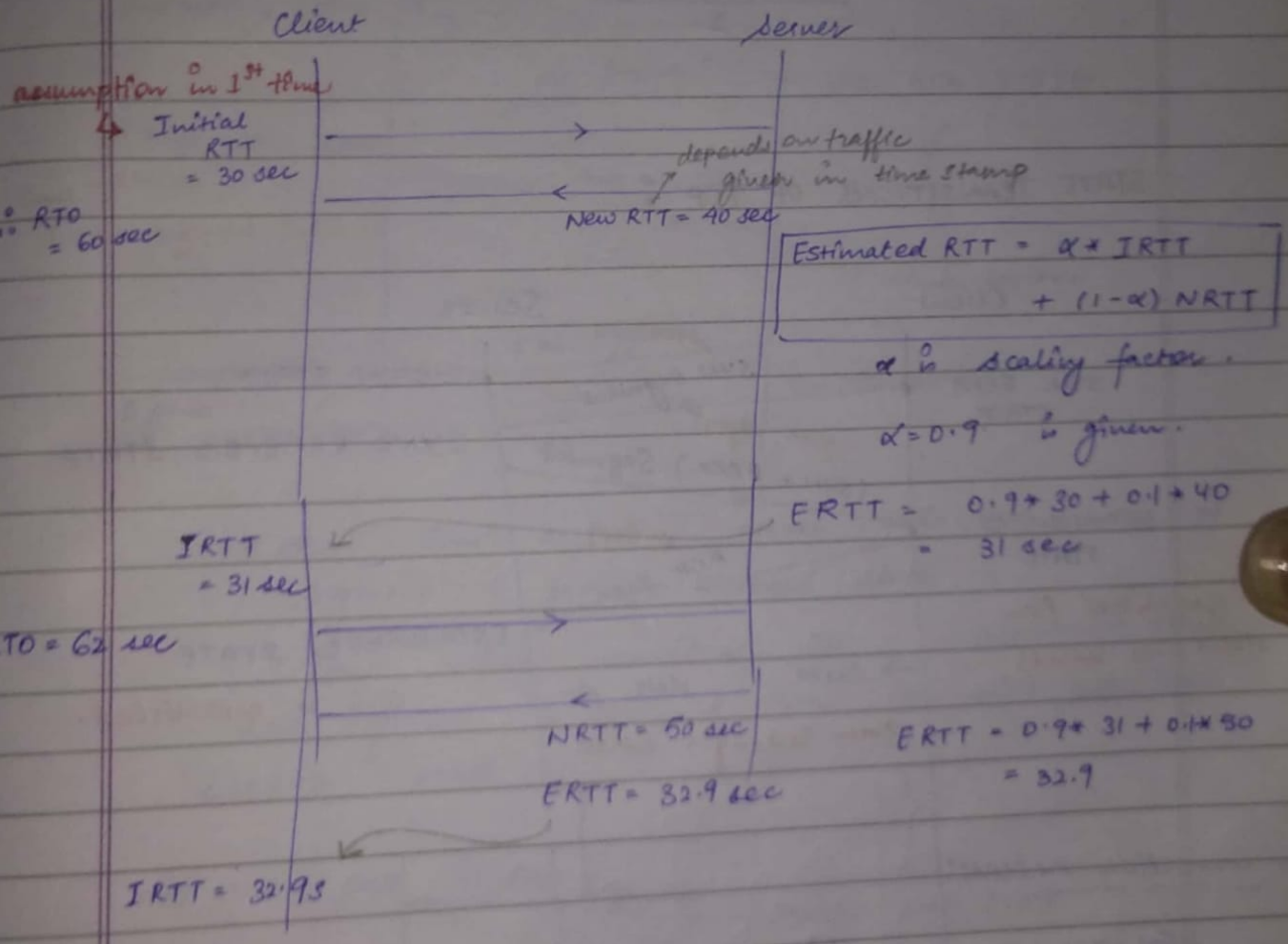
→ UDP ∴ connectionless

∴ UDP + IP Protocol = connectionless.

RTO TIMER OF TCP :

↓

Retransmission ~~timer~~ after time-out timer.



RTO timer is a dynamic timer and for back to back segments, same timer value is used.

Scanned by CamScanner

Date : / /
Page No.

EXAMPLE :

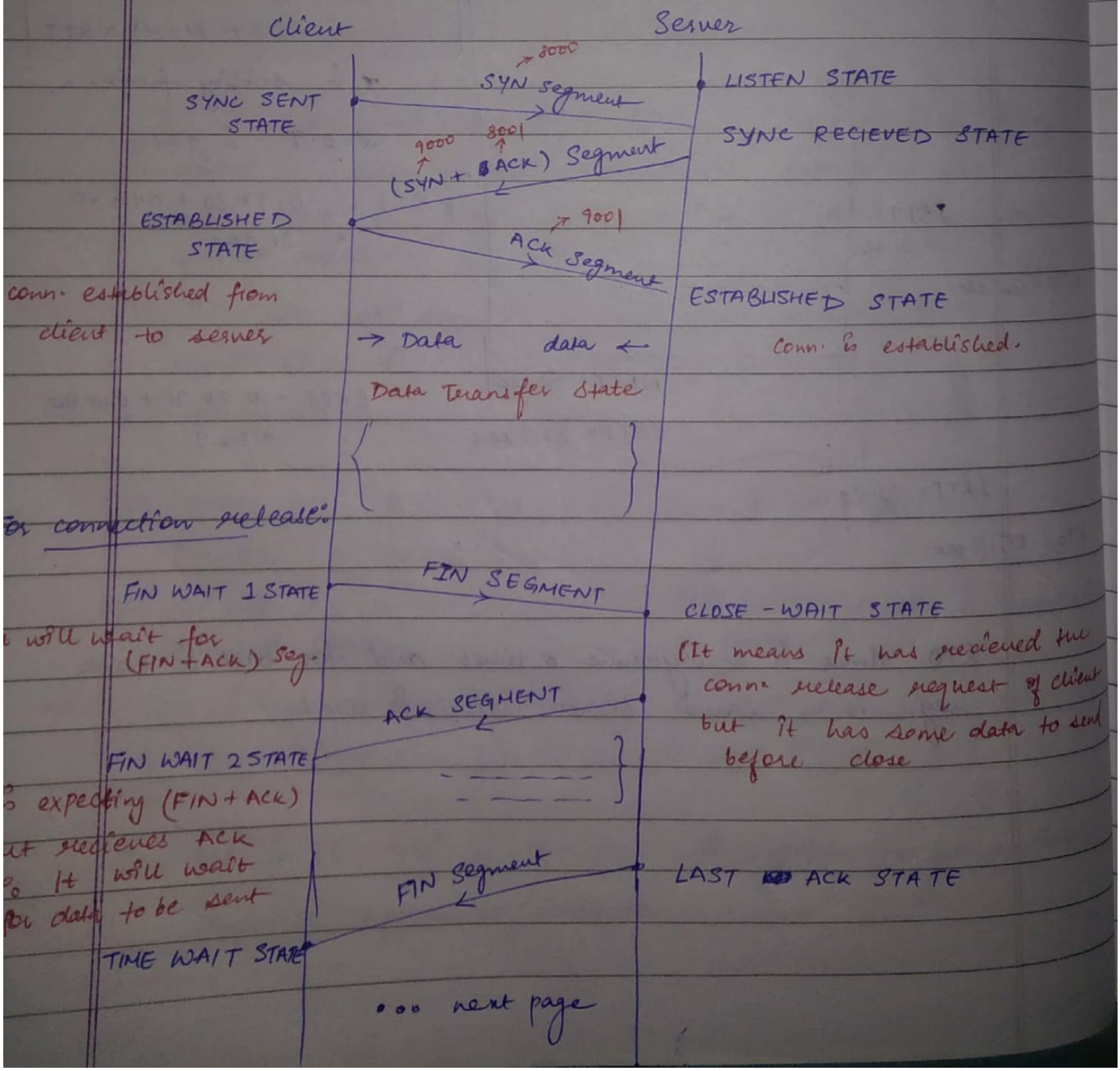
For what value of α, the estimated RTT will be the average of initial RTT and New RTT?

$\alpha = 0.5$

$ERTT = 0.5 * IRTT + 0.5 * NRTT$

$= \frac{IRTT + NRTT}{2}$ = avg. of IRTT + NRTT.

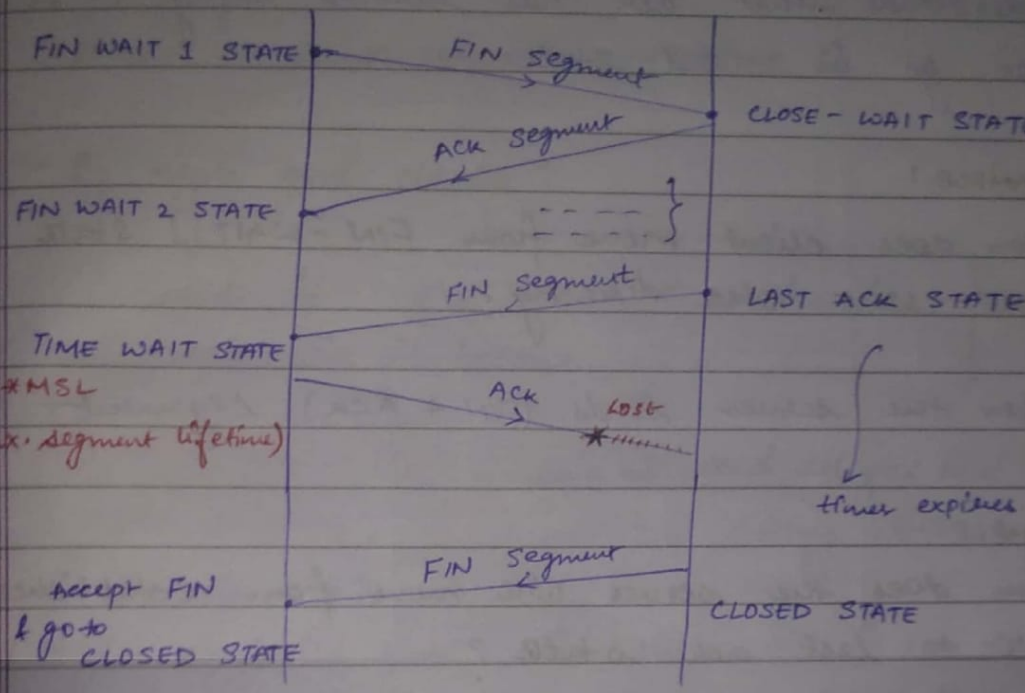
STATE TRANSITIONS OF TCP :



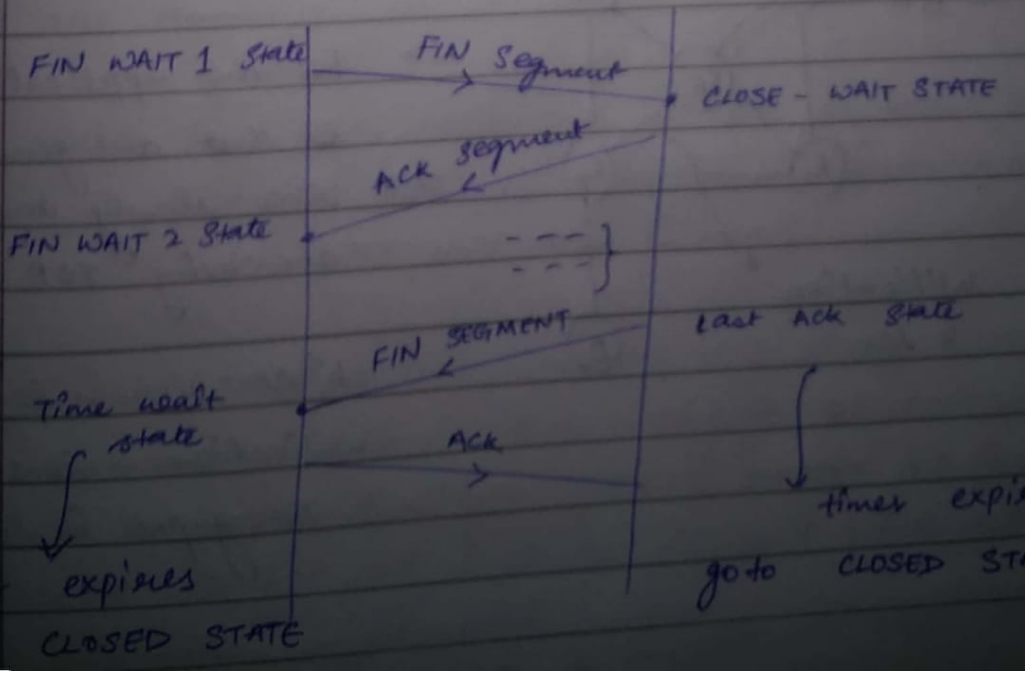
Scanned by CamScanner

Date : / /
Page No.

→ Both in FIN WAIT 1 & FIN WAIT 2 state, client will not send any data to the server but it recieves data from server. (It can only send control segments)



When timer expires, server sends one more FIN segment & goes to closed state.
Client when recieves FIN, understands that ack segment is lost, thus it also goes into CLOSED state



Scanned by CamScanner

Date : / /
Page No.

→ When last ack is recieved at server, then on expiring of timer go to closed state.
When the timer expires on client side, it understands that ack has reached safely. ∴ It will also go in closed state.

→ EXAMPLE :

When does client move from FIN - WAIT 1 state to TIME - WAIT state directly ?

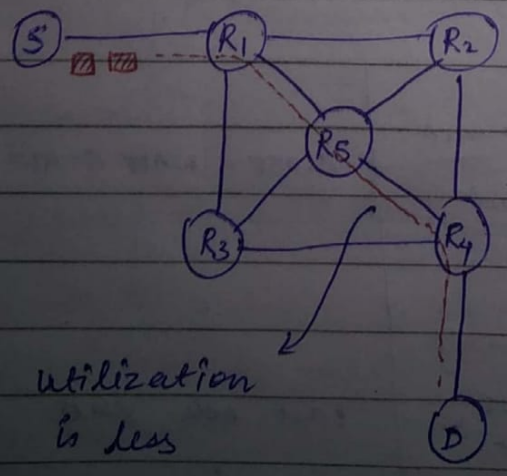
When the server sends (FIN + ACK) segment.

EXAMPLE

When does the server will move from established state to last ack state ?

When server sends (FIN + ACK) segment.

SILLY WINDOW SYNDROME :



utilization is less

→ For the applications ~~to~~ that are generating data slowly and we are using TCP

Window size is less
- utilization is less
∴ Throughput is less

Scanned by CamScanner

Date : / /
Page No.

→ Applications generating data slowly and TCP is used then window size is small. This is known as silly window syndrome.

SOLUTION OF SILLY WINDOW SYNDROME :

- By nagle and clarke :

↓

said if buffer size is < window size, wait till it becomes equal

said → send delayed ACK so WS will increase along with buffer size.

At sender's end :

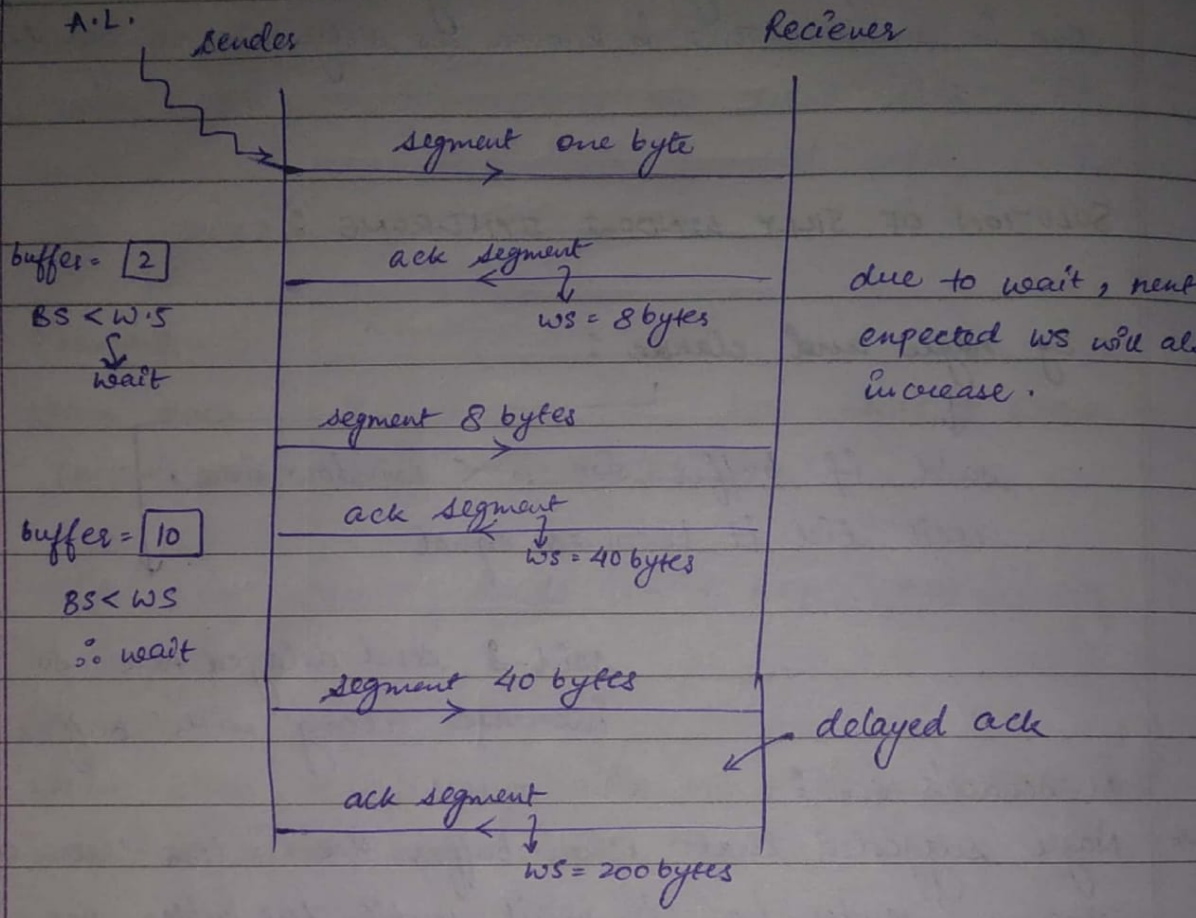
→ Nagle suggested that when buffer size is less than window size, sender has to wait until the buffer size is equal to window size and then start transmitting data.

During the waiting time, TCP is giving chance for transmitting the data by other processes.
Hence, the channel is not ideal. Some other processes are running.

→ Clarke has given suggestion at the reciever's end
- delay the ack, buffer size increases and parallely window size will also increase.

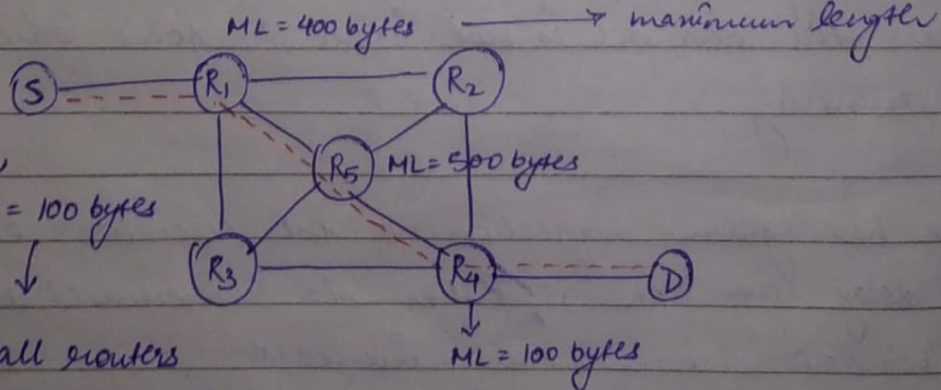
If the A.L. of reciever consumes data slowly & then sender keeps on sending data, then the buffer at reciever will be full & as soon as 1 byte space is created at reciever's end, ack will be sent & sender will send 1 byte data. Thus, utilization is decreased
∴ send delayed ack to increase the buffer size at reciever & thus to increase utilization

Scanned by CamScanner



→ If TCP sends long messages, then utilization is more.

CONGESTION POLICIES OF TCP:



ngestion window,
cwnd = 100 bytes

minimum of all routers

hence, later no router will object / block

cwnd is related to congestion in the middle of the network

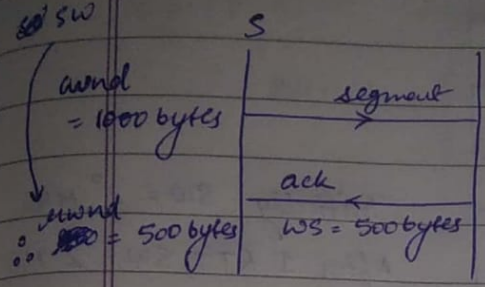
rwnd = reciever window
It is related to the congestion at the end of network

→ Congestion window is known in the connection establishment phase.

Scanned by CamScanner

Case 1 :

Rwnd << cwnd



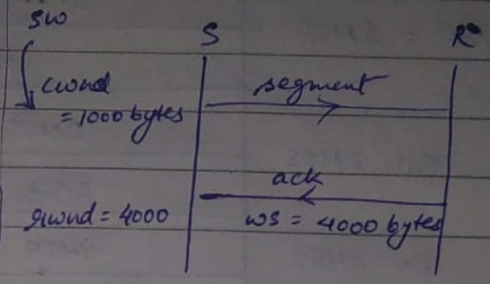
When, rwnd << cwnd

SW = rwnd

→ flow control policies of TCP are applied

Case 2 :

cwnd << Rwnd



When cwnd << rwnd

then SW = cwnd

→ Congestion policies of TCP are applied

∴ $\boxed{SW = \min(rwnd, cwnd)}$

Congestion Policies :

1.) Slow start (enponential)
2.) Congestion Avoidance (linear / additive)
3.) Congestion Detection (multiplicative decrease)

1. SLOW START ALGORITHM : EXPONENTIAL ALGORITHM.

In slow start algorithm, data will be transmitted in the form of MSS → Maximum segment size.

1MSS = 100 bytes

↓

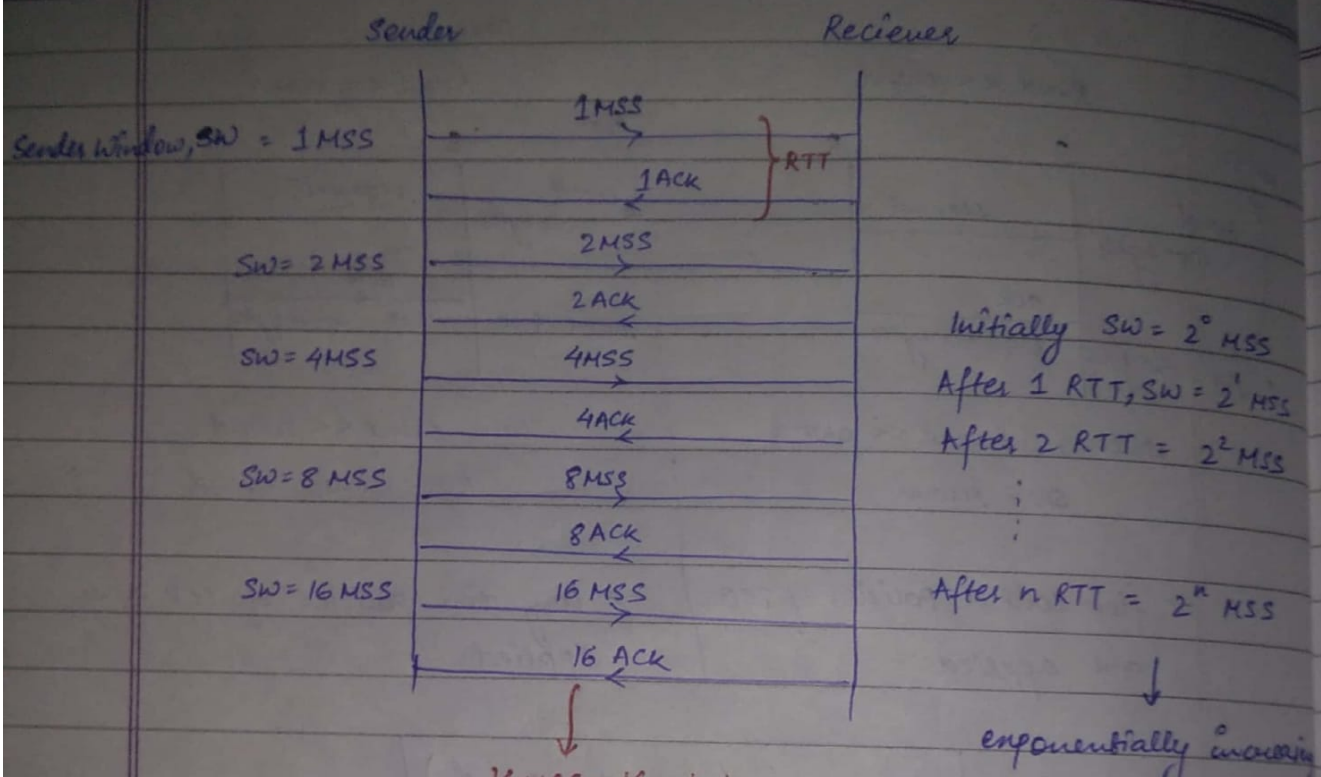
For one mss, we get one ack

cwnd = 3200 bytes

Slow start threshold = 1600 bytes.

Scanned by CamScanner

Date : / /
Page No.



→ The increase of sender window is based on no. of acknowledgements.

→ In slow start algo, SW increases exponentially upto slow start threshold.

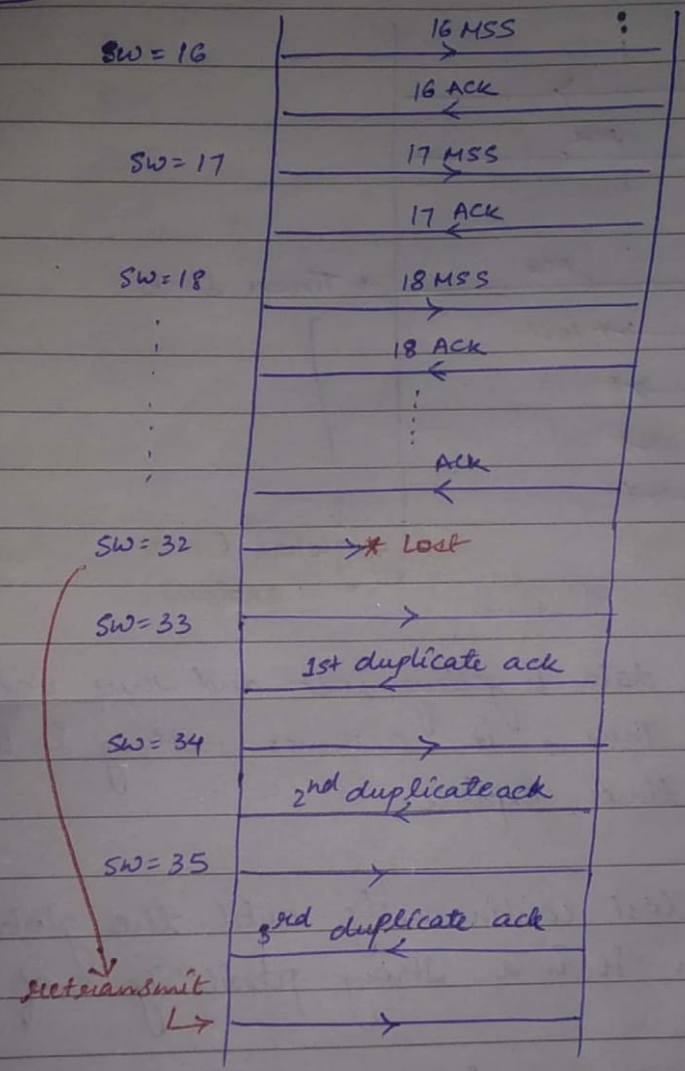
→ After this algorithm we use congestion avoidance algorithm.

Scanned by CamScanner

Date : / /
Page No.

2. CONGESTION AVOIDANCE : ADDITIVE INCREASE ALGORITHM

Case 1 :



In congestion avoidance technique, the SW increases linearly

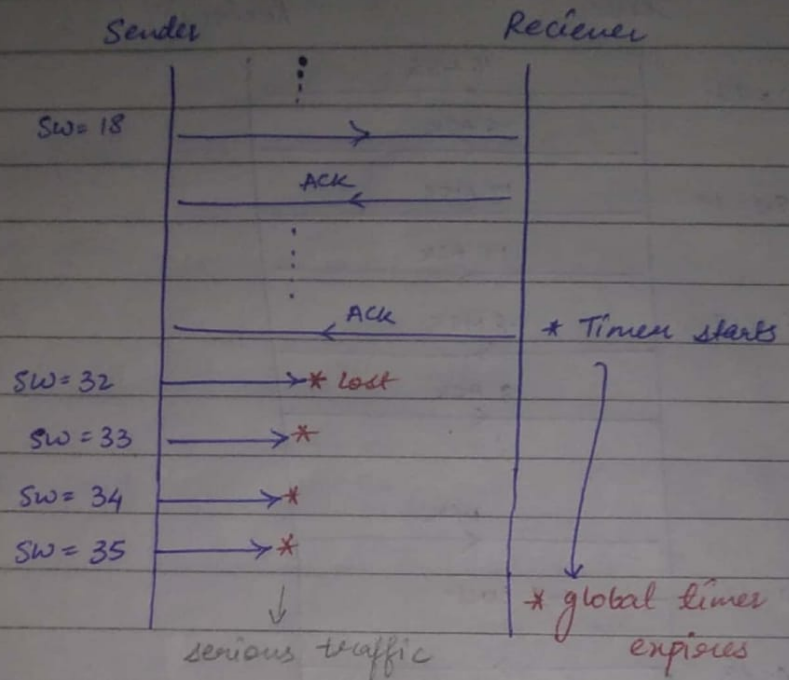
→ If the data is lost and we get 3 duplicate acknowledgments then after 3rd ack, data is retransmitted & is accepted.

→ This is known as weak possibility of congestion.

Scanned by CamScanner

Date : / /
Page No.

case 2: Strong Possibility of Congestion



Continuously the data is getting lost and thus nothing reaches to the reciever. Thus, it assumes nothing is happening & the global timer expires.

→ If the data is lost continuously until the global timer expires, then it is a strong possibility of congestion

3. CONGESTION DETECTION : MULTIPLICATIVE DECREASE

WEAK POSSIBILITY

- Act if data is accepted by retaining after 3 duplicate ack's

$SW = \frac{1}{2} * (\text{Present Window})$

PW → when data starts getting lost

- Apply congestion avoidance

STRONG POSSIBILITY.

- Act when global timer expires after data is lost continuously

SW = 1 MSS

Threshold = $\frac{1}{2} * (\text{Present Window})$

- Apply slow start algo.

Scanned by CamScanner

Date : / /
Page No.

Example: cwnd << swnd

slow start

SW = 100 bytes

200

400

800

1600 ← Threshold Apply CA

1700

1800

1900

2000 * lost

→ strong possibility of congestion

(data is lost continuously)

slow start

SW = 100

threshold = $\frac{1}{2}$ (2000)

= 1000

SW = 200

= 400

800 ← Threshold (Actually 1000 but went SW = 1600)

900

1000

1100

1200 * lost

→ weak possibility

(dat is lost in b/w & again accepted)

CA

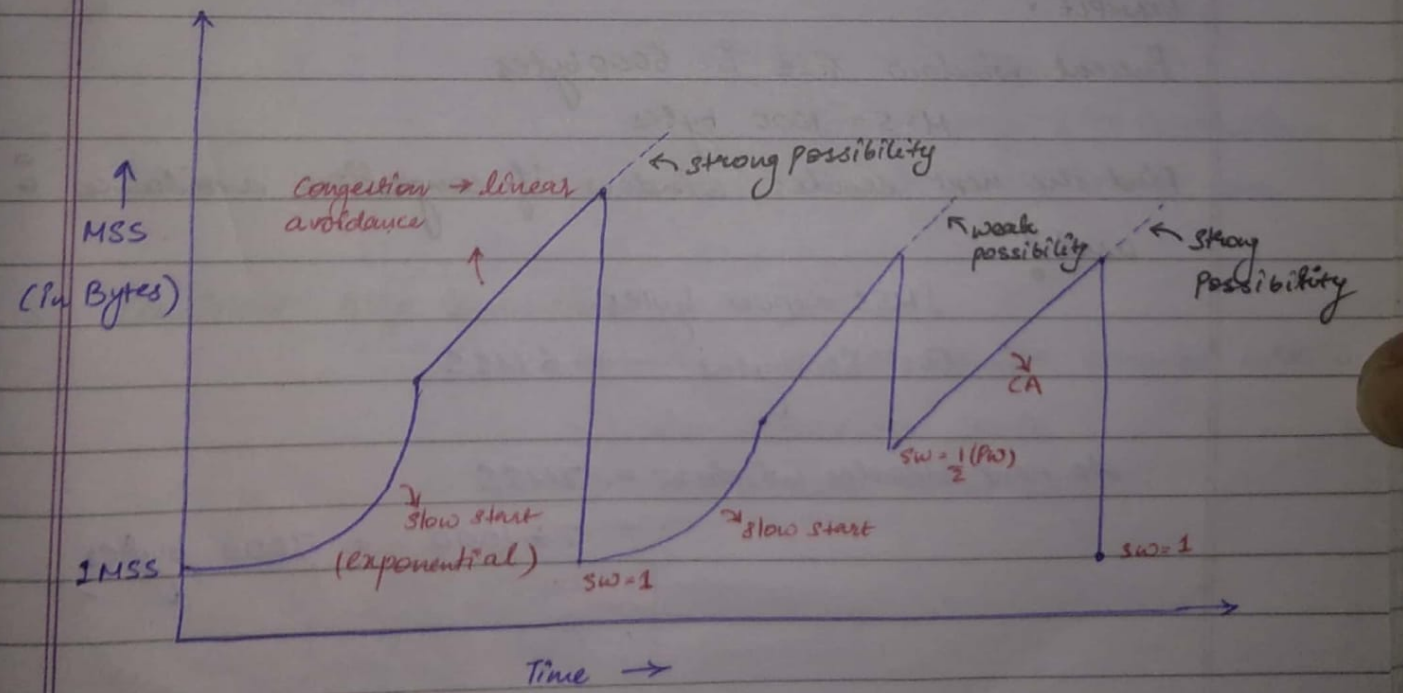
SW = $\frac{1}{2}$ * 1200

= 600

= 700

800

⋮



Scanned by CamScanner

EXAMPLE:

Present window size is 8000 bytes

MSS = 100 bytes

If slow start algorithm is applied, then find the next sender window?

1 MSS = 100 bytes

$\frac{1}{100} * 8000$ ← 8000 bytes

= 80 MSS for 8000 bytes.

∴ Next sender window = 160 MSS

= 160 * 100 = 16000 bytes.

EXAMPLE:

Present window size is 6000 bytes

MSS = 1000 bytes

Find the next sender window if congestion avoidance is used?

1 MSS = 1000 bytes

∴ For 6000 bytes → 6 MSS

So next sender window = 7 MSS

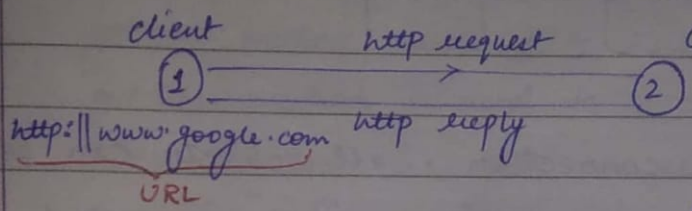
= 7 * 1000 = 7000 bytes.

Scanned by CamScanner

Date : / /
Page No.

Application layer :

HTTP Protocol : Hypertext Transfer Protocol

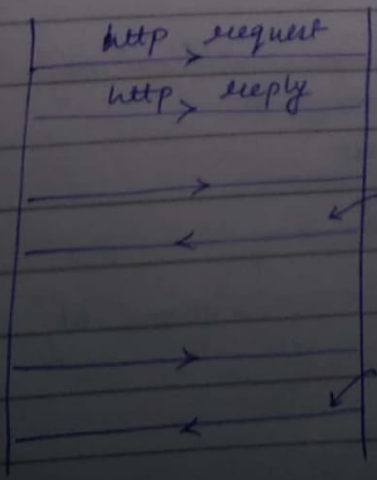


1.) Client - Server Protocol
2.) Synchronous Protocol
3.) Port 80.

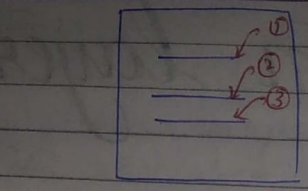
HTTP is a synchronous protocol because the clock of the client is synchronized with the clock of the server.

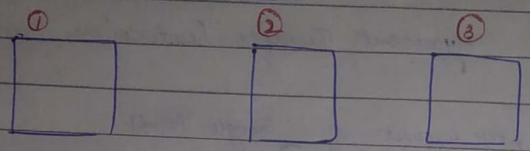
4.) http connection
(a) Persistent http Connection
(b) Non-Persistent http Conn.

Persistent Http Connection :
↳ Many windows can be accessed within one connection only
↳ It is user friendly



Scanned by CamScanner



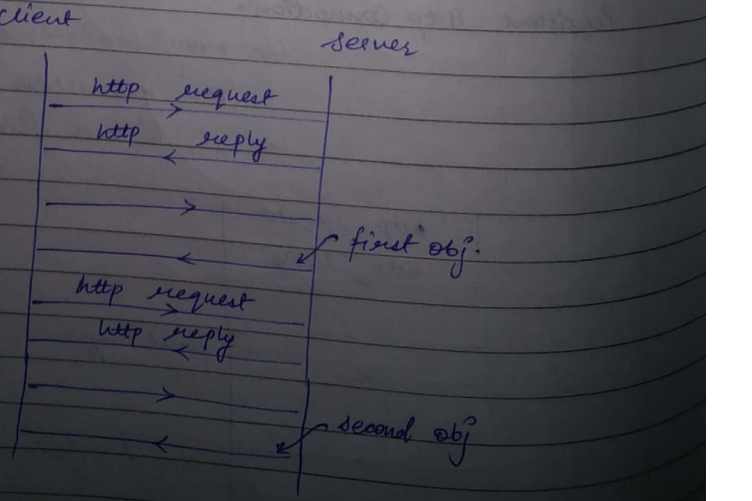


In persistent http connection, all objects can be accessed in same connection. This is called user friendly

Non - Persistent http connection:

In non-persistent http connection, for every individual data transfer, a seperate connection is established.

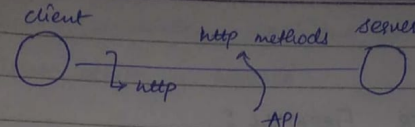
→ This is for security purpose.



Scanned by CamScanner

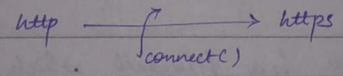
Date : / /
Page No.

(5.)



→ get() → put() → connect()
→ post() → head() → trace()

1.) get() method is used to receive the document
2.) put() method is used to modify the document
3.) post() method is used to place the modified document back to the server
4.) head() method is used to get the information about the document.
5.) When connect() method is used, the data will go via secure channel that too in encrypted form.



(6) http is a stateless protocol.

↳ because it does not store any information about the server in the client system.

Cookie is a piece of code that is transmitted by a server system or a mediating agency to the client browser

The advantage of cookies is :
1.) Faster response
2.) Authorization.

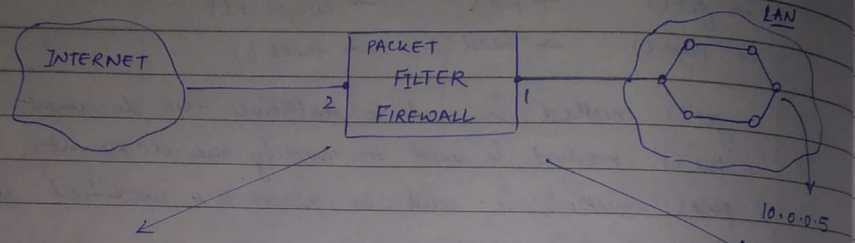
Thus, the state saved at the client system is due to cookies & not because of http.

Scanned by CamScanner

FIREWALL :

PACKET FILTER FIREWALL :

↳ stateless Firewall.



	Interface	S.IP	S. Port	D. IP	D. Port
1.)	2	144.15.0.0	*	*	*
2.)	2	*	*	10.0.0.5	*
3.)	2	*	*	*	23
4.)	1	*	*	*	80

→ Packet filter firewall is a firewall which blocks or forwards the data by ~~forwarding~~ observing the transport layer or network layer header of the content.

→ There is no concept like ideal firewall. Every firewall will work according to company policies.

Case 1: Packets coming from a source network i.e. 144.15.0.0 are blocked i.e. a particular network is blocked.

Case 2: Packets destinated to 10.0.0.5 are blocked because this computer is used for internal LAN only.

Scanned by CamScanner

Date : / /
Page No.

Case 3: Packets ~~destination~~ destinated to port 23 is blocked i.e. Telnet service is blocked.

Case 4: Packets destinated to port 80 are blocked i.e. HTTP service is blocked.

§ When a virus or a trojan horse is placed in the application data, then the packet filter firewall cannot detect it.

So software firewalls or antivirus softwares are required to protect the system.

→ Packet filter firewall is also known as stateless firewall because it does not store any information, it just checks for every incoming & outgoing packet that whether it is allowed or not

→ Stateful firewall :

Seq. No.					
200-399					
400-599					
42665					

(200-399) →
(400-599) →

If we store the seq. no.s of segments, then it becomes stateful firewall.

If the sequence nos. are stored, then for first segment the complete table is checked & if it is allowed, then all the following segments with sequence no. near about will be also be allowed.

But if seq. no. changes drastically, then it will be

Scanned by CamScanner

checked again.

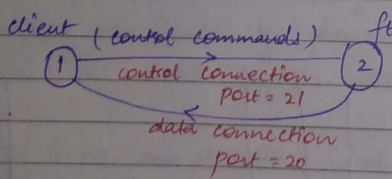
FTP Protocol:

↳ File Transfer Protocol.

→ FTP uses control commands via control connection on port 21

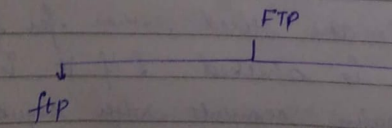
→ When the file is about to download, a seperate data connection is established on port 20.

→ Once the file is completely downloaded, the data connection is closed but the control connection is there only to download some other files.

1) 

2) Client - Server Protocol

3) Synchronous Protocol.

4) 

→ Uses TCP as T.L. protocol

→ Uses UDP as T.L. protocol

Scanned by CamScanner

Date : / /
Page No.

→ Authorized users
↓
all the details of the users are stored at ftp server before downloading of files.

→ Anonymous User
↓
User details are not required by server.

→ ftp has no internal flow control

→ ~~to~~ tftp has internal flow control.

→ Internet service is required (∵ Pay)

→ Internet service is required (∵ Pay)

→ ftp already has antivirus experts internally

→ tftp does not have it.
∴ Antivirus is required (∵ Pay)

→ Softwares on ftp are generally paid

→ softwares are generally free of cost over tftp.

FTP	TELNET
1.) Downloading a large bite.	1.) Chat operation or exchange of words.
2.) Two seperate connections: port 21 - Control connection port 20 - Data connection	2.) Single common connection ⇒ port 23.

↳ Both uses TCP as transport layer.

Scanned by CamScanner

FTP

Two seperate connections are:
1. control conn.
2. data conn.

↳ Both uses TCP as T.L.

↳ Both uses not store and forward technique at server end.

HTTP

Two seperate conn. are:
Persistent http
Non-Persistent http.

SMTP :

↳ Simple Mail Transfer Protocol

→ SMTP is a text based protocol.

But we can send graphical data like images, videos with the help of MIME Extension.

↓

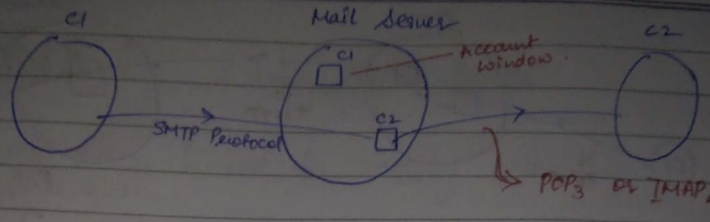
Multimedia Internet Mail Extension.

→ Port 25, TCP as T.L.

→ SMTP is a push protocol because it is used for sending the mail into mail server.

Scanned by CamScanner

Date : / /
Page No.



→ Each user has to sign up with mail server by giving all its user details, then the mail window is created for each user at mail server.
Now, when C1 wants to send a mail to C2, the mail will be pushed to mail server even though C2 is offline.
Now, whenever C2 signs in ~~with~~ with mail server, the mail from C1 is delivered to C2 by POP_3 or $IMAP_4$ protocol.

→ POP_3 or $IMAP_4$ are known as pull protocols because they are used for retrieving the mails from mail server.

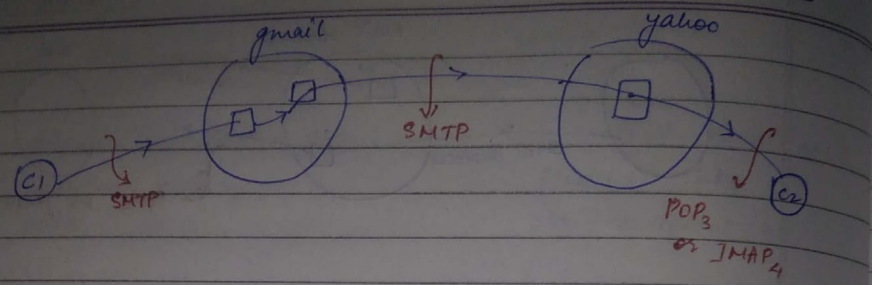
SMTP combined with POP_3 or $IMAP_4$ is a client-to-client protocol with the mediation is done by mail server.

POP = Post office Protocol.
IMAP = Internet Message Access Protocol

SMTP applies store and forward technique using mail server

Scanned by CamScanner

Date : / /
Page No.



When one mail server is sending data to another mail server, SMTP protocol is used.

→ In POP_3, all mails are equal whereas in $IMAP_4$, mails are kept in heirarchy

∴ Generally $IMAP_4$ is used.

→ $IMAP_4$ is giving protections to the files but POP_3 does not provide any protection.

→ SMTP combined with POP_3 or $IMAP_4$ is an asynchronous protocol

Scanned by CamScanner