Q.No.

Computer Networks

Q. 1. The OSI and TCP/IP models are both a method of organization of various parts and layers of Networking in Computers. They help us learn about the way each layer interacts with the other.

The comparison between these models is given below:

[Open systems Interconnection] [Transfer Control protocol / Internet protocol]

	OSI	TCP/IP
(1)	Gives 7 layers of Networks	Gives only 4 layers of Networks
(1)	Application layer	(1) Application layer
(2)	Presentation layer	
(3)	Session layer	
(4)	Transport layer	(2) Transport layer
(5)	Network layer	(3) Internet layer
(6)	Data link layer	(4) Physical layer.
(7)	Physical layer	

Q.No.	OSI	TCP/IP
(2)	Provides a vertical approach	Provides a horizontal approach.
(3)	Provides Application, presentation and session as separate layers	Provides only Applic layer
(4)	More complicated, elaborate, specific and thorough	Simple and straight foward.
(5)	Transport layer does ~~not~~ guarantee reliable transmission always	Transport layer ensures reliable transmis of data with TCP and unreliable with ~~UDP~~ UDP
(6)	Based on more generic protocols	Based on specific and standard Internet protocols
(7)	Provides connectionless and connection oriented servic from its network layer	Provides connection less service in its network layer

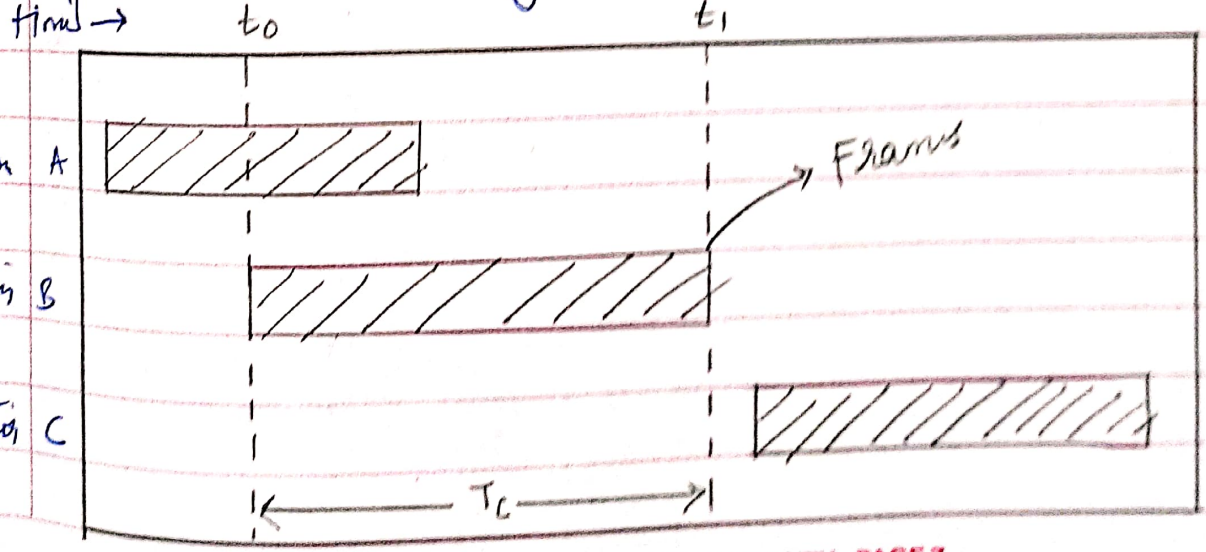
Q.No. (2) Comparison between Pure and Slotted ALOHA

(A) The Data link layer deals with sending frames from one Node to another. To manage multiple frames being sent from one computer to another, you need some sort of protocol, otherwise the frames will often collide and get destroyed.

(A) The Multiple Access Protocol manages this and has several ways to manage this situation. One such way is Randomly allowing stations to send data. This is where ALOHA comes in.

1. Pure ALOHA

→ There is a longer conflict window
→ Station are allowed to begin sending frames at any time in the channel.



Q.No.

As shown in above figure, The conflict Interval can be a maximum of 2 such frames

$$T_c = 2 T_f$$

T_c – conflict time, T_f = Time for 1 frame

The efficiency of Transmission then is

$$\eta e \approx G \cdot e^{-2G}$$

which would be maximum for

$$G = 0.5$$

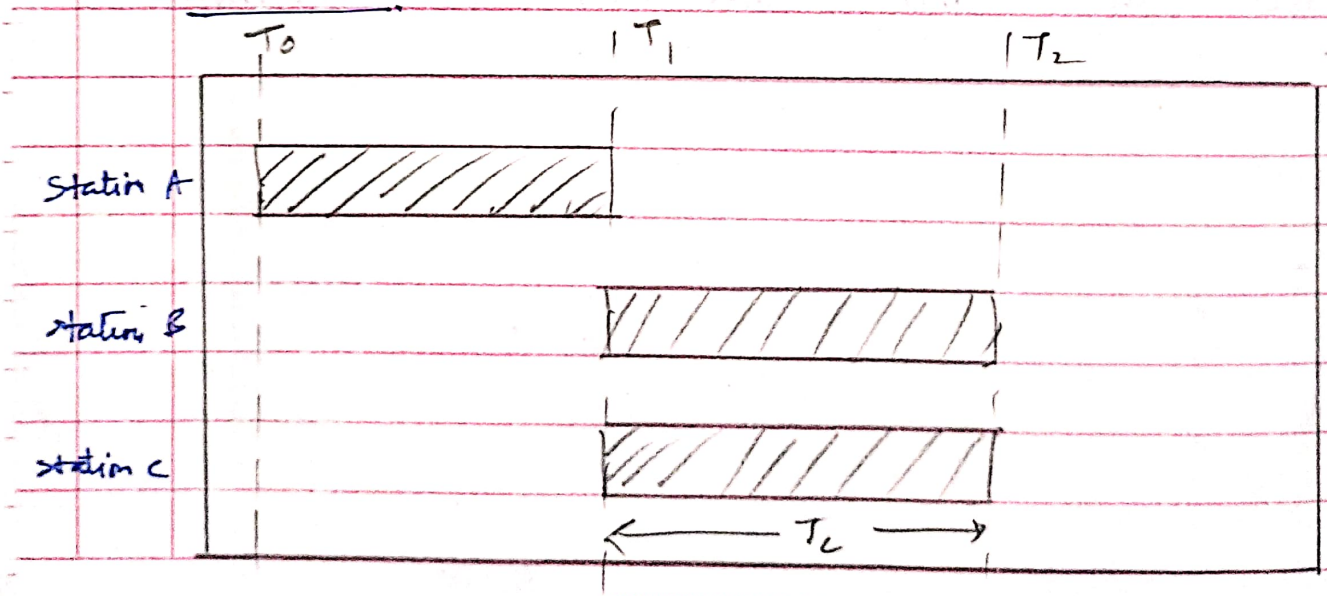
so $e = 0.18$ or 18 %

→ Not very efficient; is fast one of the worst algorithms

→ Slotted ALOHA introduced to improve efficiency.

→ Due to random time, most frames collide.

SLOTTED



Q.No.

→ Stations can only send frames at given time slots

→ $T_c = T_f$

→ Efficiency then is

$$\eta = G \cdot e^{-2G}$$

Maximum for $G = 1$

So $\eta = \boxed{0.368}$ or $\boxed{36.8\ \%}$

→ Improvement over pure aloha.

→ Stations can now only send frames at the very beginning of the alloted time slots

→ channel is divided into "~~st~~ SLOTS".

→ Thus efficiency is better than Pure ALOHA

Q.No. (3) Subnetting.

given address : 201.70.64.0

class - C so cidr = 24

But given no. of Subnets required = S = 5.

as 5 < 8,

network bits required = 3

as $2^3 = 8$

$2^2 = 4$

2 (2) so 2 bits are not sufficient.

So CIDR value = 27

Network (1)

201. 70. 64. 000 00000

network bits | host bits

So Network Id =

201.70.64.0

First IP = 201.70.64.000 00001

= 201.70.64.1

Q.No.

Last IP = 201.70.64.000 11110

= 201.70.64.30

Broadcast IP = 201.70.64.000 11111

= 201.70.64.31

Network (2) : Similarly,

Net Id = 201.70.64.32

First IP = 201.70.64.33

Last IP = 201.70.64.62

Broadcast IP = 201.70.64.63

Network (3)

Net IP = 201.70.64.64

First IP = 201.70.64.65

Last IP = 201.70.64.94

Broadcast IP = 201.70.64.95

Network (4)

Net ID = 201.70.64.96

First IP = 201.70.64.97

Last IP = 201.70.64.126

Broadcast IP = 201.70.64.127

Q.No. (5)

Network (5)

Net IP = 201. 70. 64. 128

First IP = 201. 70. 64. 129

Last IP = 201. 70. 64. 158

Broadcast IP = 201. 70. 64. 159

Q. (4) Distance Vector Routing Protocol - RIP

RIP - Routing Information Protocol

→ It is based on Distance Vector Routing.

→ Uses Bellman-Ford algorithm to calculate shortest path

→ Updates all routers within a few minutes

→ Updates each single routing table of a router at every regular time interval (say 20 seconds)

→ All routers communicate their distances via packets with each of their neighbours

→ Using this information, each router updates its ~~post~~ table that is maintained.

→ To send packets with the best route, the router then uses this table and calculates the best route.

→ This causes CPU overhead at each router

→ RIP has V_1 and V_2

→ It takes time to stabalize

Q.No. (3)

Network (5)

Net IP = 201. 70. 64. 128

First IP = 201. 70. 64. 129

Last IP = 201. 70. 64. 158

Broadcast IP = 201. 70. 64. 159

Q. (4) Distance Vector Routing Protocol - RIP

RIP - Routing Information Protocol

→ It is based on Distance Vector Routing

→ Uses Bellman-Ford algorithm to calculate shortest path

→ Updates all routers within a few minutes

→ Updates each single routing table of a router at every regular time interval (say 30 seconds)

→ All routers communicate their distances via packets with each of their neighbours

→ Using this information, each router updates its table that is maintained

→ To send packets with the best route, the router then uses this table and calculates the best route.

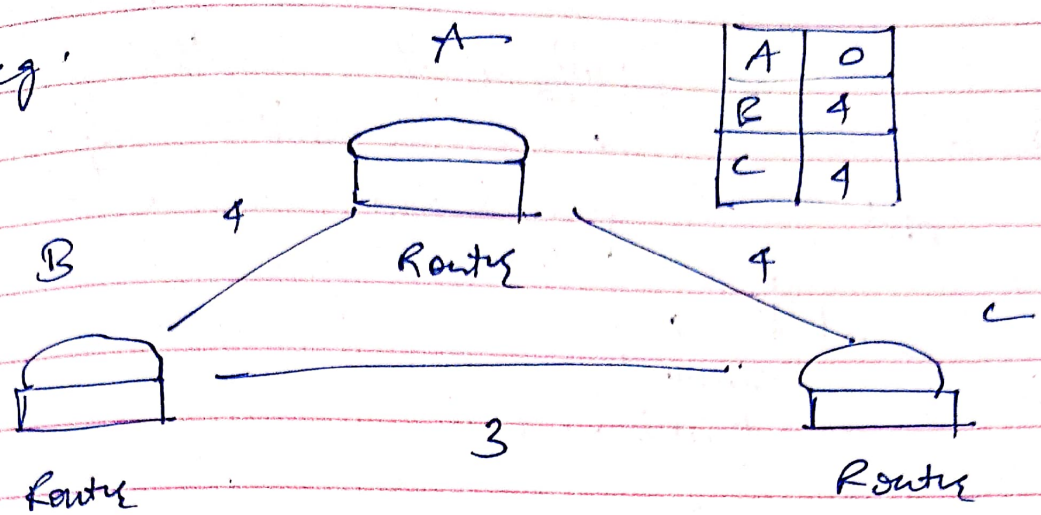
→ This causes CPU overhead at each router

→ RIP has V_1 and V_2

→ It takes time to stabalize

Q.No.

eg.



A	0
B	4
C	4

A	4
B	0
C	3

A	4
B	3
C	0

Fig: RIP

(*) Link state Routing Protocol : (OSPF)

→ OSPF is an example

→ A link state router knows beforehand what the best route is.

→ Uses Dijkstra's algorithm to calculate the best path

→ It is faster and has less overhead.

→ Provides basic authentication between routers

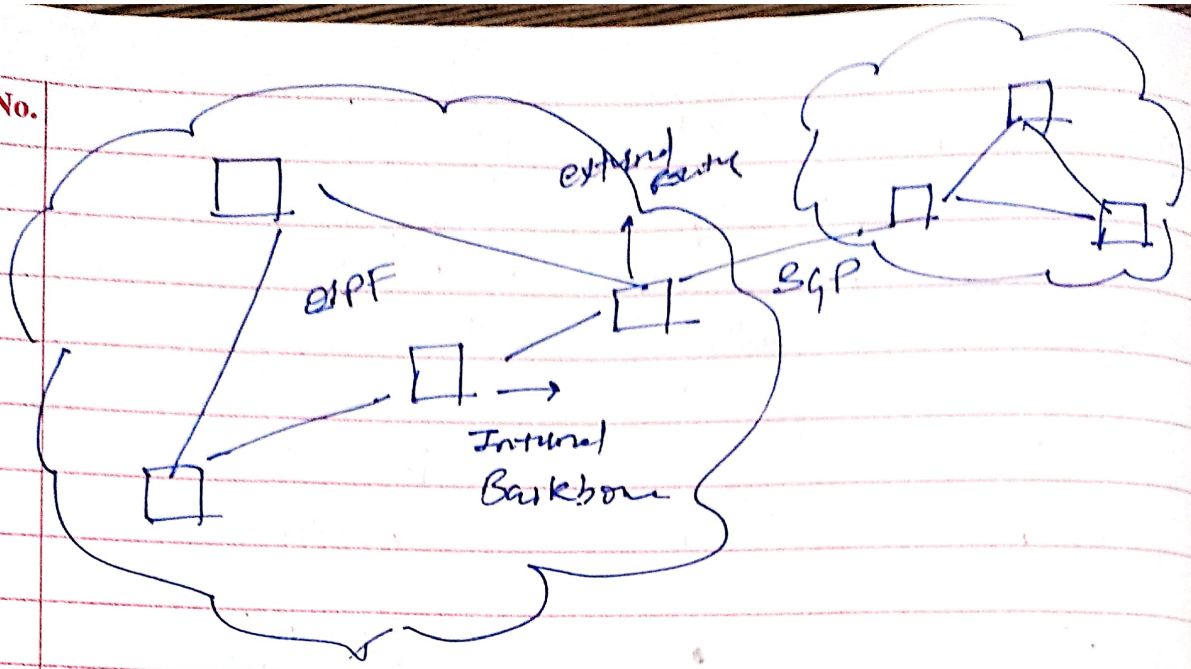
→ Little safer than RIP.

→ Each router exchanges its information and distances to neighbours in the beginning of the setup.

→ Tables are not maintained here.

→ Common as an Internal routing alg for Autonomous Systems.

Q.No.



Q.5 Difference between TCP and UDP

	TCP	UDP
1.	Transfer Control Protocol	User Datagram Protocol
2.	Connection oriented protocol	Connection Less protocol.
3.	Provides a very reliable connection.	~~Post~~ Does not provide any reliability.
4.	TCP makes sure to provide reliability of data transmission over network layers that have unreliable protocols like IP.	It does not care about how unreliable the layer beneath the Transport layer are.

Q.No.	TCP	UDP
5.	Provides flags, and fields in its header for flow control and error control. It has checksum and flags for setting packet priority.	→ Only provides one checksum segment in its header
6.	~~Com~~ More complex header. Large Header	→ Simple header - only has source port, destination port, header length, and checksum.
7.	Invokes : . socket () Bind () Listen () Accept () Send () Recieve () close	→ only Invokes Socket () Bind () send () ~~Rec~~ Recieve () close ()
8. →	Used in HTTP, FTP and other protocols that demand reliability	Used in applications that need speed over reliability eg. RTTP, streaming, DNS, & TFTP etc
9.	Slower, ↑ overhead.	→ Faster ↓ overhead.

Q.No. (6) TCP control Flags of TCP Header

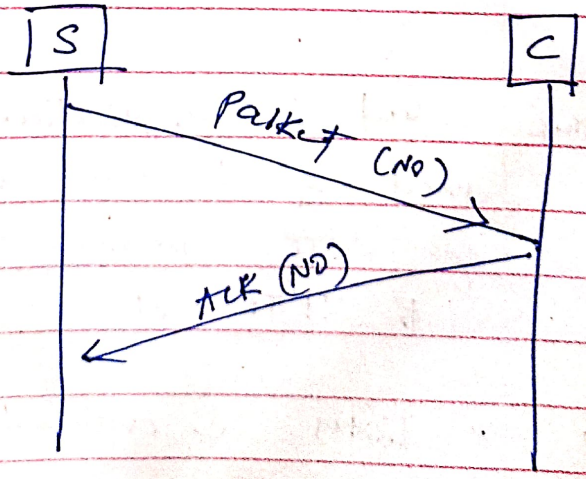
1. URG – The urgent flag

→ The advantage of TCP over UDP is its reliability and sequential data transmission ; This sequential data transmission can be often overridden by client or server during packet exchange

→ If say client needs to send a packet urgently ; and needs for it to be put at the beginning of the TCP processing stack (the receive window Left side),

→ then it sets this flag to high. As a result, packet is processed faster.

2. ACK – The acknowledgement flag



Q.No.

→ To maintain reliability, the server ensures that every packet is sent using the client's acknowledgment for its previously sent packets.

→ ACK flag is usually accompanied with a number piggybacked to another packet next in line for full Bridge communication.

→ Also used in 3-way handshaking.

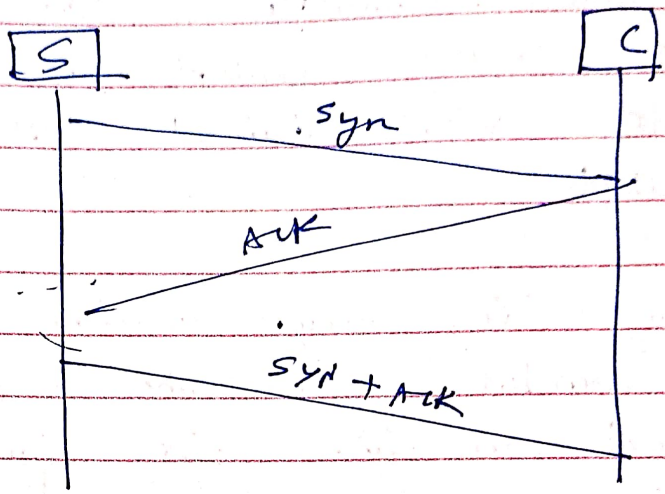
(3.) PSH — Push flag — used by client and server when a packet needs to be pushed to the TCP stack. Often accompanied by data from the above layers.

(4) RST — Reset flag — when a connection gets congested and client needs the server to reset the entire connection, the Reset flag is used. The server then interprets this and resets the connection socket and resends unacknowledged packets depending on algorithm used.

(5) SYN — Synchronization Flag used to initiate server and client connection, 3-way handshake, and synchronization of packets sent.

Q.No.

~~FIN~~



3- way - handshake

FIN: Used to terminate the connection from the client or server. It then triggers transmission of 4 more packets to ensure safe closing of server and client sockets.

8.1.7 Q.8

1. Mapping URLs to numeric addresses — done by DNS (Domain Name Server)

2. Dynamically assign IP addresses to clients — DHCP (Dynamic Host Configuration protocol.)

~~3.~~ ~~Control proto.~~

Q.No.

3. Display web pages — HTTP — (hypertext transfer protocol.)

4. Allows viewing of messages on email clients — IMAP

5. Send Email Messages — SMTP
Simple Mail Transfer Protocol.

Q.7	POP3	IMAP
(1) →	Post office Protocol	Internet Mail addressing protocol
(2) →	Both allow clients to read their mails	Allows clients to read pending messages
(3) →	Maintains a buffer of unread emails	Maintains a Buffer of unread mails
(4)	Simple in structure and functionality	Complex in structure and functionality.
(5)	does not allow users to see partial mail	Allows users to see the mail partially.
(6)	Does not allow reading to download mail partially	Allows header viewing and partial downloads.

Q.No.	POP3	IMAP4
(6)	Both work on client to Mail server side	Works on client to server side.
(7)	Mails stored on ~~server~~ so ~~span~~ client side computers	Mails stored on servers so it is more secure.
(8)	So span is not a problem	Span could be a problem in the future
(9)	Less secure	More secure
(10)	Not so easily accessible on multiple devices	Can be used easily on many devices as mails are stored on server.