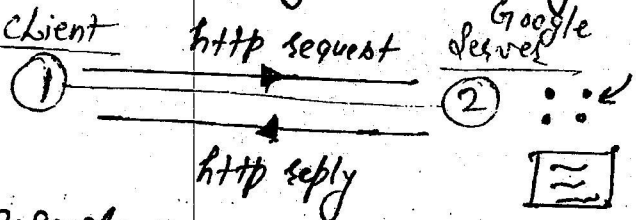
★ Application Layer :-

⇒ "http Protocol" :- (hypertext transfer protocol)



http://www.google.com

URL : uniform resource Locator → T.L. (Transport Layer)

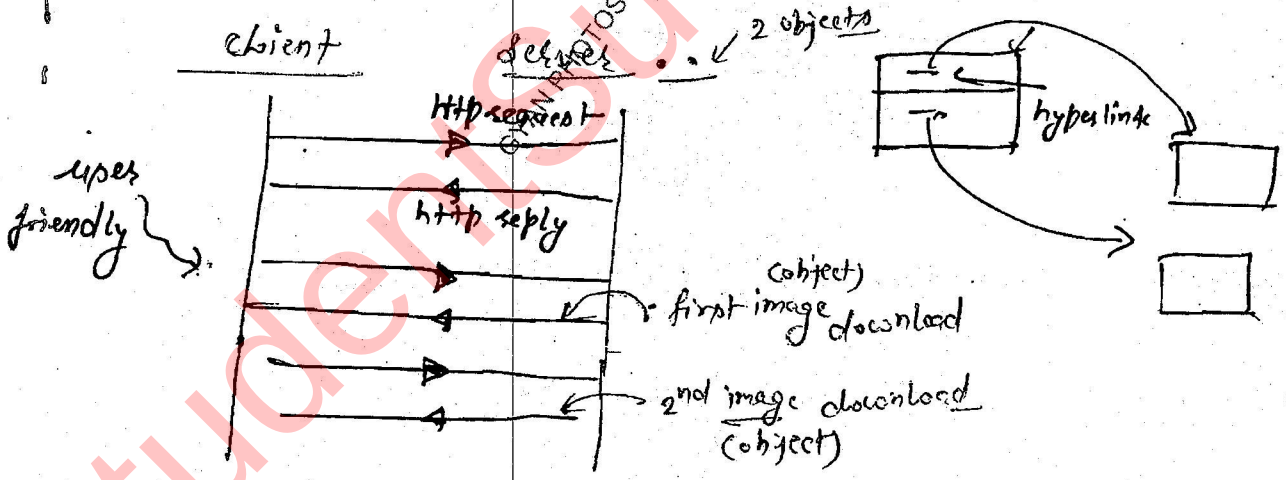
S.Port 65000, D.Port 80 ← http

★ http is a synchronous Protocal because both the clocks of client & server are synchronized.

★ http Connections :-

↳ (i) Persistent http Connection
(ii) Non-persistent http Connection

:- Persistent http :-

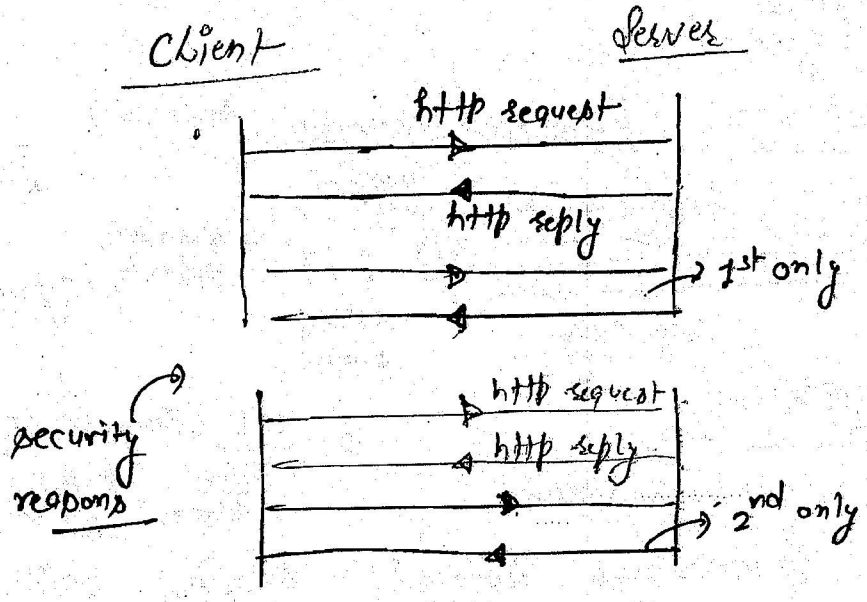


★ In case of persistent http Connection will be these only until all objects are accessed.

★ this is for user friendly requirement.

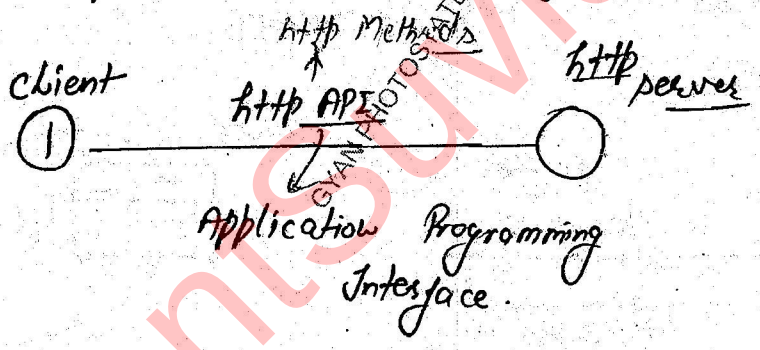
StudentSuvidha.com
CHANDRA PRAKASH TOSTATE MOB 8588058174

Download all Notes and papers from StudentSuvidha.com



★ In Non-persistent http, a seperate connection is eptablished for ~~ind~~ every individual data transfer. this is provided for security.

http API :-



Methods :- get, post, put, head, trace, connect

★ connect : http ⟶ https
connect

★ get method is used to retrieve the document
★ Post method is used to place the updated document in the server
★ Put method is used to modify the content of the document.
★ head method is used to get the information about the document

StudentSuvidha.com
GYAN PHOTOSTATE MOB 9388058
Download all Notes and papers from StudentSuvidha.com

★ Connect method is used to transmit the data in secure channel and that to in encrypted form.

★ http is Stateless protocol.

★ By default IPv6 is stateless but we can make it stateful with the help of DHCPv6 server.

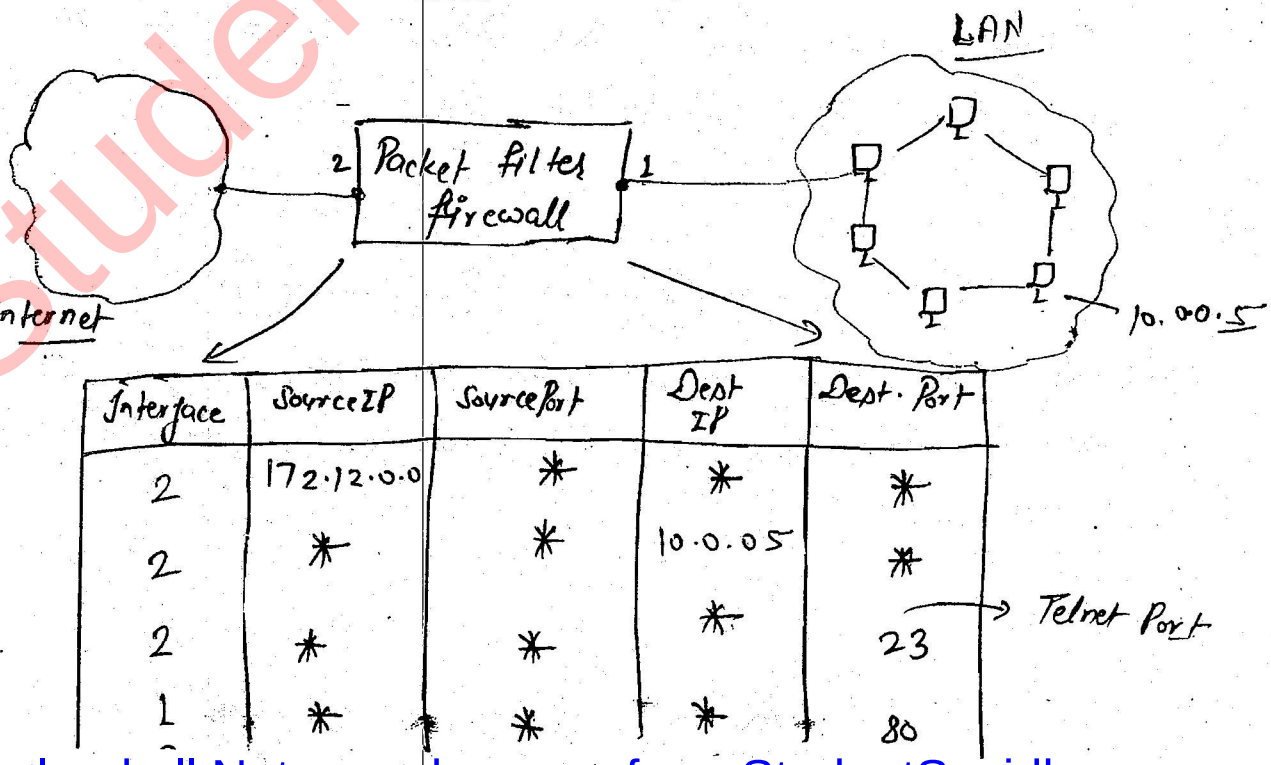
Note:- http is a stateless protocol because client will not store any information about the server once the transaction has been done.

★ cookies is a piece of code that is transmitted from the server to the client Browser.

★ The advantage of cookies is:
(i) faster Response
(ii) Authorization.

★ "Firewall" :-

:- Packet filter firewall :-



Interface	SourceIP	SourcePort	Dest IP	Dest. Port
2	172.12.0.0	*	*	*
2	*	*	10.0.05	*
2	*	*	*	23 → Telnet Port
1	*	*	*	80

StudentSuvidha.com
GYAN PHOTOSTATE MO 9858805174

★ Packet filter firewall is a firewall which blocks or forwards the data by observing the transport Layer and Network Layer 'Headers' of the content by comparing with firewall table.

★ There is no ideal firewall, every firewall will work according to its design.

★ Packets coming from a particular source Id i.e. 170.12.0.0 are blocked.

★ Packets destinated to 10.0.0.5 are blocked because this computer is used for internal LAN communication only.

★ Packets destinated to 'port-23' are blocked i.e. "Telnet" service is blocked. (No outside person can communicate directly to the internal LAN).

★ when a malicious software or a virus is placed in the application data then the packet filter firewall can not detect it.

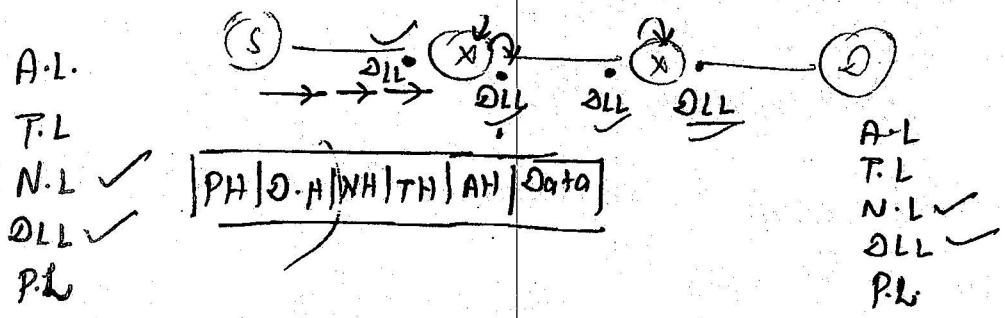
★ Encryption and decryption is done in Session Layer ~~create~~ in OSI Model where as it is done in Application layer in TCP/IP Model.

GYAN PHOTOSTATE MOB.8588058174

①

Calculate how many times data link layer, N.L are visited in this path from source to destination. (TCP/IP)

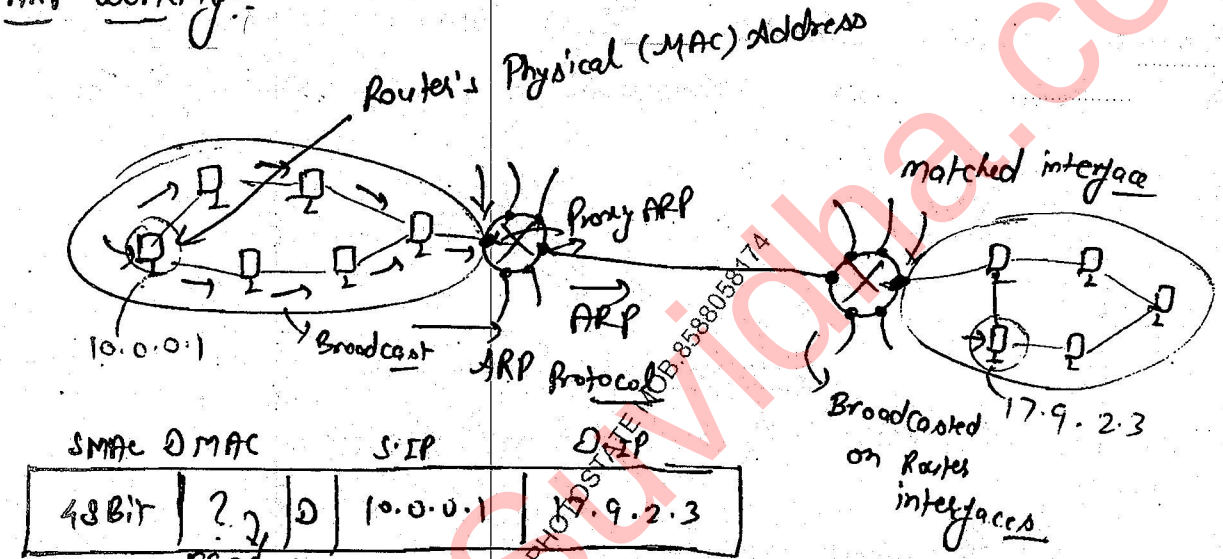
Download all Notes and papers from StudentSuvidha.com



N.L. = 4 times

D.L.L = 6 times

ARP working :-



GYAN PHOTOSTATE MOB.8588058174

* "FTP" :- (file transfer Protocol)

has No flow control at A.L.

has flow control at A.L.

FTP Protocal

Reliable → authenticated user

→ TCP ap T.L.

(i) Internet

(ii) purchasing reliable service

TFTP Protocal

unreliable data

Anonymous user

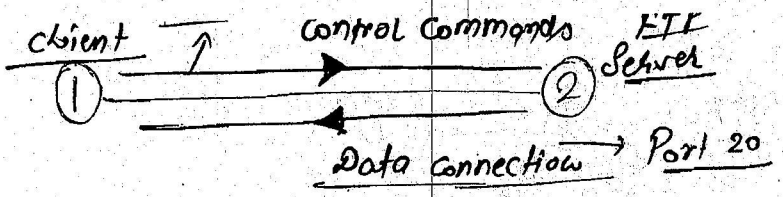
UDP ap. T.L.

(i) Internet service

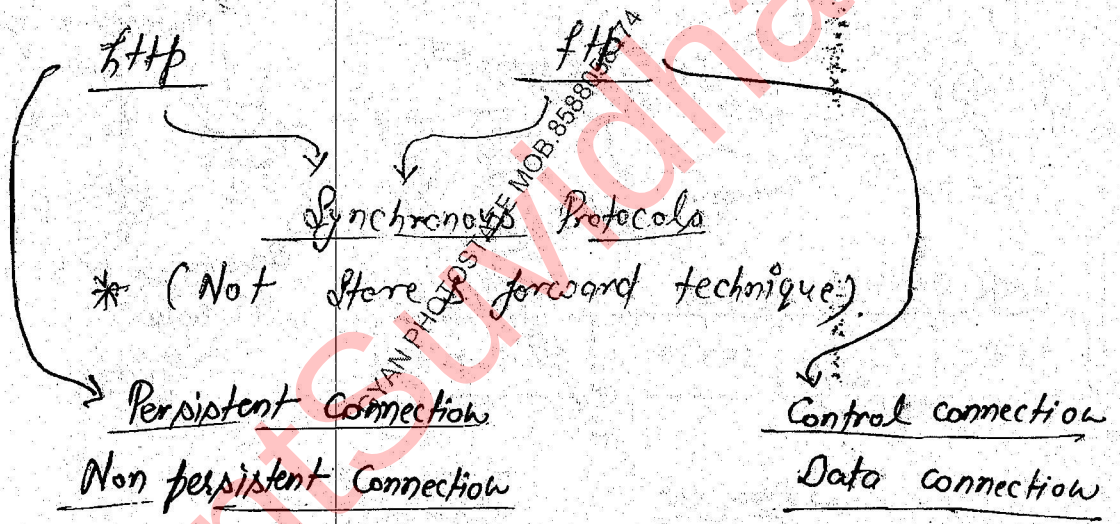
(ii) Antivirus Software

StudentSuvidha.com

Download all Notes and papers from StudentSuvidha.com



* FTP will send control commands via a control connection on Port - 21.
* When the file is about to download, seperate data connection will be established on Port - 20.
* Once the file is completly downloaded, data connection is closed but control connection will be there, to download some other files.



VYAN PHADSTARE MOB 8588096574

FTP :-

i) downloading a large file

ii) Control connection
Data connection

iii) Ports 20, 21 are used

TELNET :-

i) chat operations (Exchange of words)

ii) common connection.

iii) Port 23

Tcp as T.L.

StudentSuvidha.com

Download all Notes and papers from StudentSuvidha.com

SMTP :- (Simple Mail Transfer Protocol)

(1) text-baped Protocol

→ Internet → MIME Extension

→ multimedia internet mail Extension

(SMTP + MIME) = all type of data

★ Port - 25 , Base 64 Encoding

→ a-z ⇒ (0-25)
A-Z ⇒ (26-51)
0-9 ⇒ (52-61)
+ ⇒ (62, 63).

11 000 000 | 10 0000

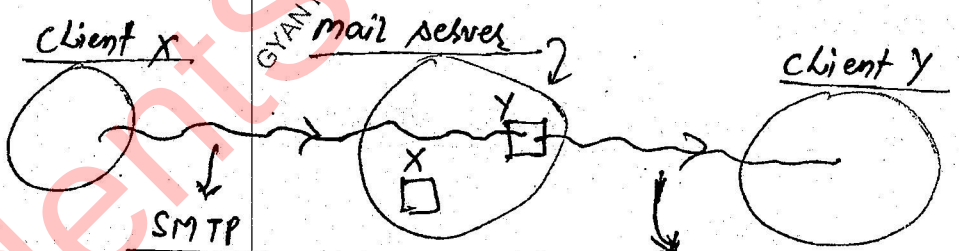
↓

48 10 0

w K a

★ TCP as T.L.

★



SMTP → Push Protocol

(POP3) → Post office Protocol
or
(IMAP4)

★ SMTP is known as 'Push Protocol' because it is used to send the mail into mail servers.

★ POP3 or IMAP4 are known as the 'pull protocols' because they are uped for retrieving the mails from mail servers.

IMAP4 :- (Internet message Access Protocol)

StudentSuvidha.com
GYAN PHOTOSTATE MOB 8588058174
Download all Notes and papers from StudentSuvidha.com

★ SMTP combined with POP3 ... known as client to client Protocol with the mediation done by mail server.

★ SMTP with POP3 is applying store & forward technique.

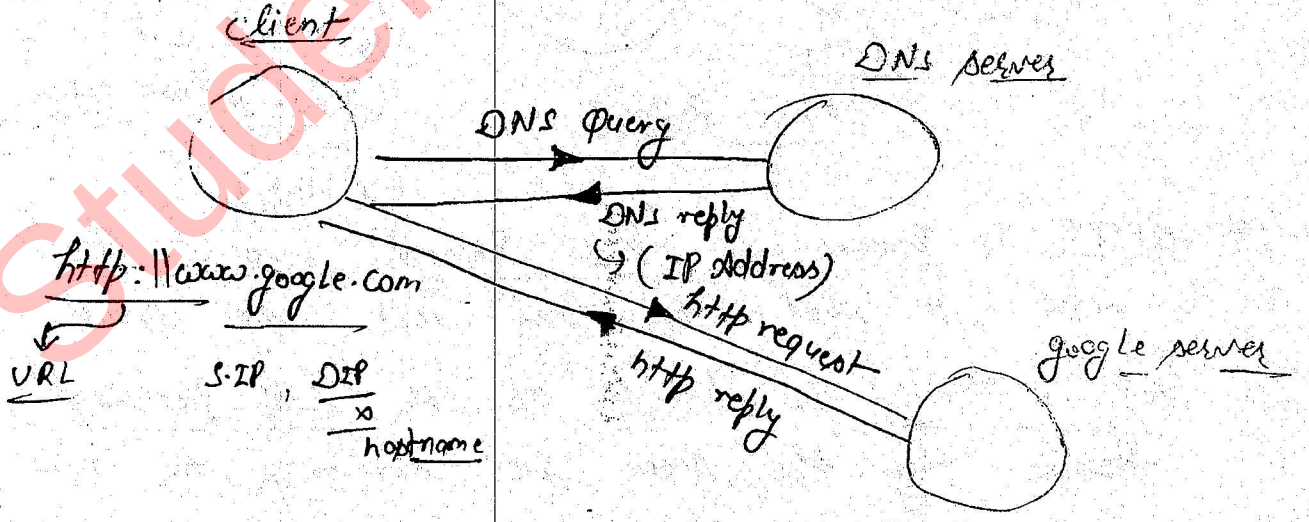
★ SMTP combined with POP3 is a 'asynchronous Protocol' because their clocks need not to be synchronized.

★ In case of SMTP multiple paths are possible when ~~and~~ TCP is used as T.L. because it is a session.

★ In POP3 ~~the~~ all mails are equal whereas in IMAP4 mails are kept in hierarchy.

★ IMAP4 is more secure than POP3, because it will scan for viruses before the file gets downloaded.

DNS : (Domain Name Space)



GYANBHOOMI STATE MOB.8588058174
StudentSuvidha.com

Download all Notes and papers from StudentSuvidha.com

★ The purpose of DNS is to find the destination IP Address for the required hostname. Or it is used for mapping hostnames to IP-Addresses.

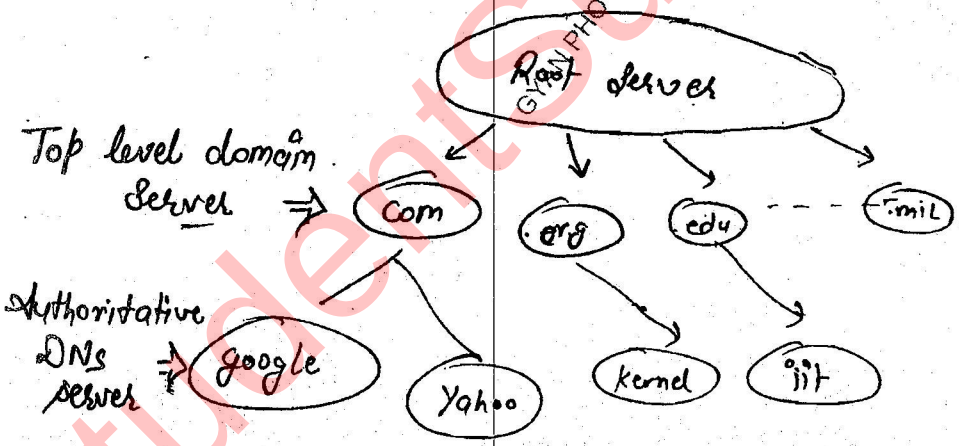
Design of DNS Server :-

(i) DNS servers placed in Heirarchy → Searching time will be less

(ii) DNS servers placed in different geographical Locations. → P.T. will be less

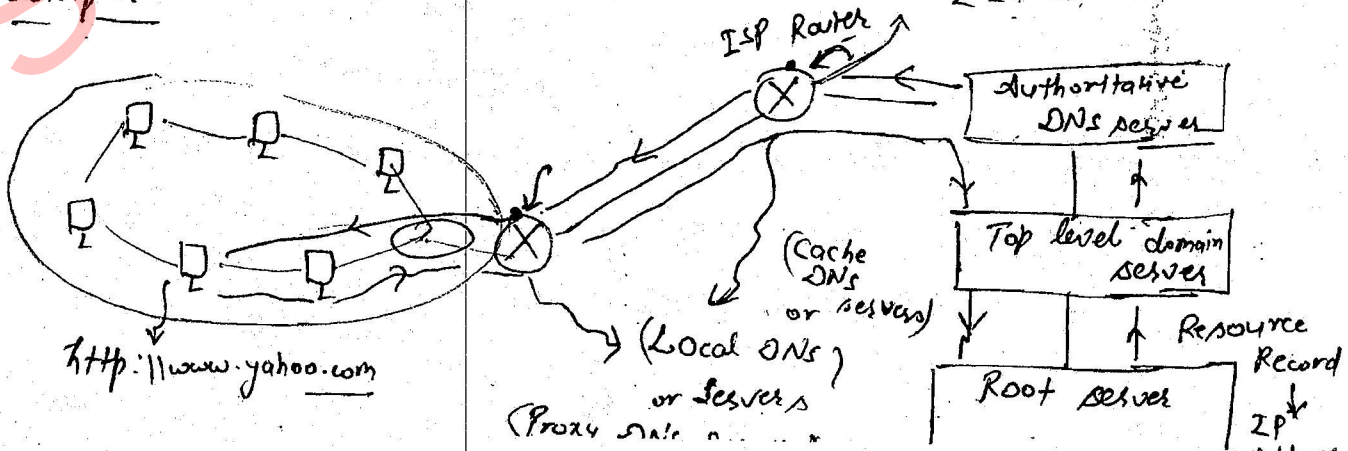
DNS servers

Root Server
Top level domain Server
Authoritative Server
Local DNS Server



Example :-

TTL ≥ 24 hrs, stable record
< 24 hrs, unstable record



GYAN PHOTOSTATE MOB.8588058174

StudentSuvidha.com

Download all Notes and papers from StudentSuvidha.com

* DNS uses UDP as a transport layer protocol.
* The DNS Reply Record, if it is storing for > 24 hours, it is treated as the stable record.

Que:-

DNS

Query size < 512 Bytes
↳ UDP as T.L.

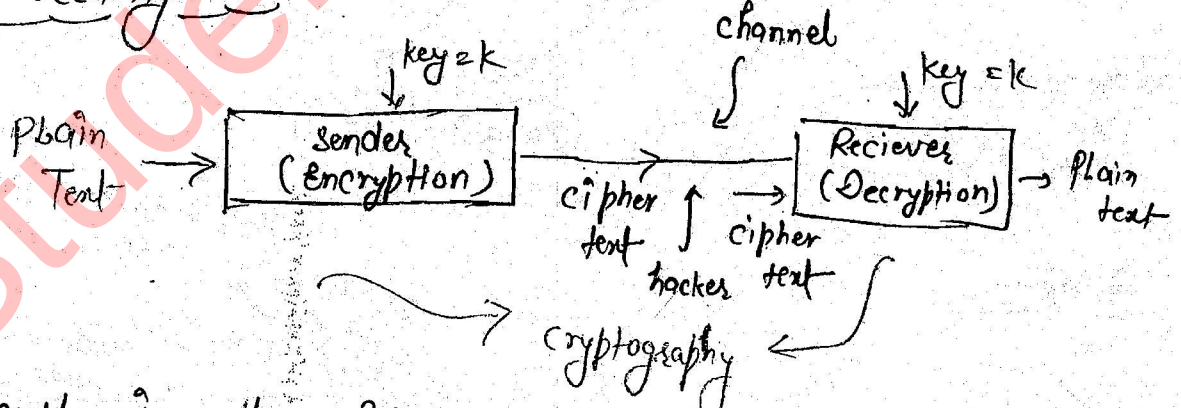
Query size ≥ 512 Bytes
↳ TCP as T.L.

* In the DNS Server, there are two zones :- 'Forward Lookup Zone', 'Reverse Lookup Zone'.
* 'Forward Lookup Zone' is used for mapping HostNames to IP-Addresses.
* Reverse lookup zone is used for mapping IP Addresses to Host. Name

GYAN PHOTOSTATE MOB.8588018174

Dated :- 21/06/2017

Basic Security :-



⇒ "Cryptography is the science or art of converting one form of data into other form, for providing security to the data is known as Cryptography."

Download all Notes and papers from StudentSuvidha.com

★ Converting Plain text to cipher text is known as Encryption.

★ Converting the ciphertext into plain text is known as Decryption.

★ "Steganography is the science of hiding the data behind an image or a video."

★ "The key is transmitted on the channel and later it is used for Encryption & decryption, it is treated as Public key."

★ "If the key is kept as secret and later it is used for Encryption and decryption, it is known as Private key."

"Cryptography"

- Symmetric key Cryptography
  - Ex: "Diffie Hellman key Exchange"
- Asymmetric key Cryptography
  - Ex: "RSA Algorithm"

★ In Symmetric key cryptography "same key" is used for both Encryption and decryption.

★ In Asymmetric key cryptography "different keys" are used for encryption & decryption.

StudentSuvidha.com
GYAN PHOTOSTATE MOB 8588805814

Download all Notes and papers from StudentSuvidha.com

Challenges of cryptography :-

(i) Authentication → authentication of user
authentication of data.

(ii) Confidentiality

* Proving user's identity is known as 'authentication'.
* Providing secrecy to the data is known as 'confidentiality'.

:- Key features of cryptography :-

1. Prime Numbers
2. challenges (Random number)
3. key values (Public key & Private key).
4. Timestamp.

* RSA Algorithm :-

Sender

Plain text P → encryption → C (cipher text)

hacker

Sender ← n, e

$C = P^e \bmod n$ → C

e = Public key

Reciever

P, q are Prime Numbers

$n = p * q$

$\phi(n) = (p-1)*(q-1)$

$(d * e) \bmod \phi(n) = 1$

Decryption

d = Private key

$P = C^d \bmod n$

GYAN PHOTOSTATE REG.8588058174

StudentSuvidha.com

Download all Notes and papers from StudentSuvidha.com

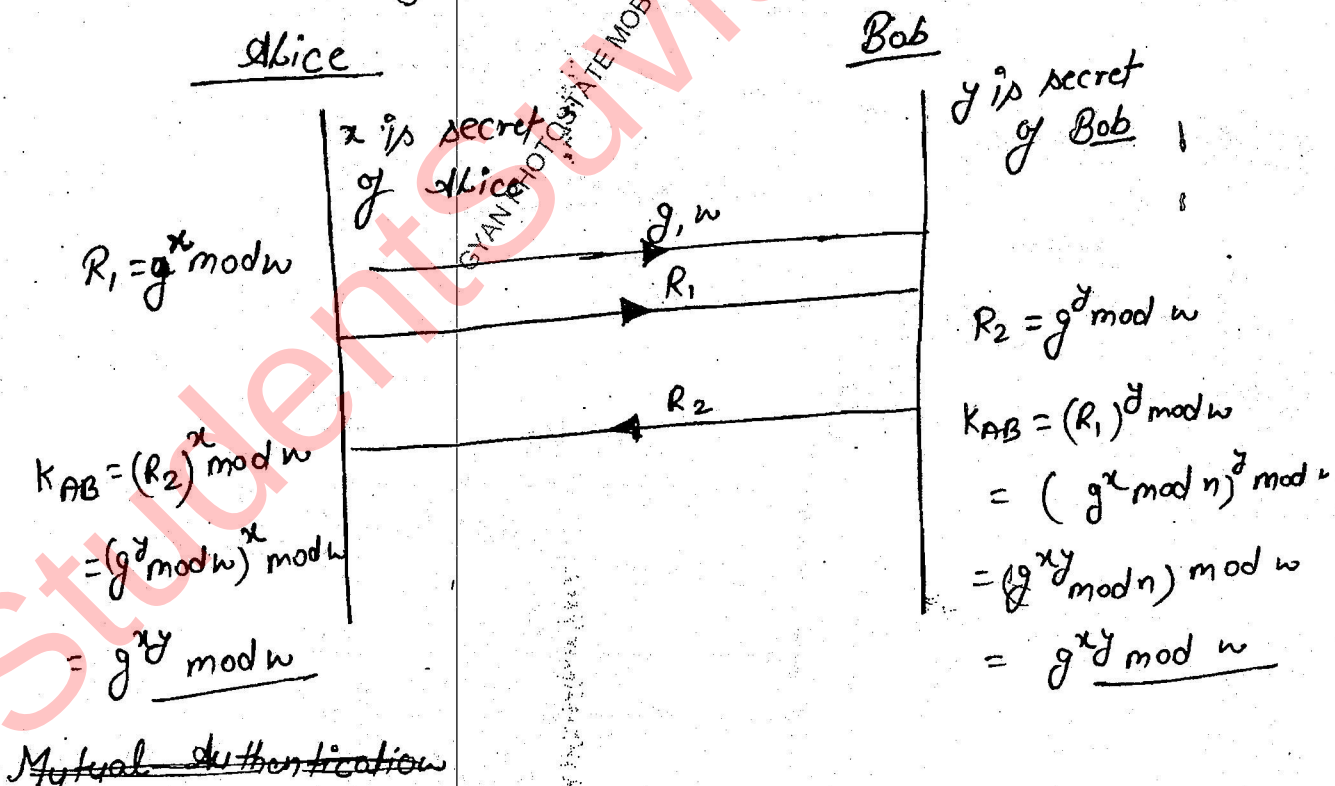
Confidentiality.

* In RSA Algorithm, If Sender is encrypted with Reciever's public key & Reciever is decrypted with his own private key then it is used to provide Confidentiality.

Que:- In RSA Algorithm sender is encrypting with Reciever's Private key. false

Que:- In RSA Algorithm, sender is encrypting with his own private key. True

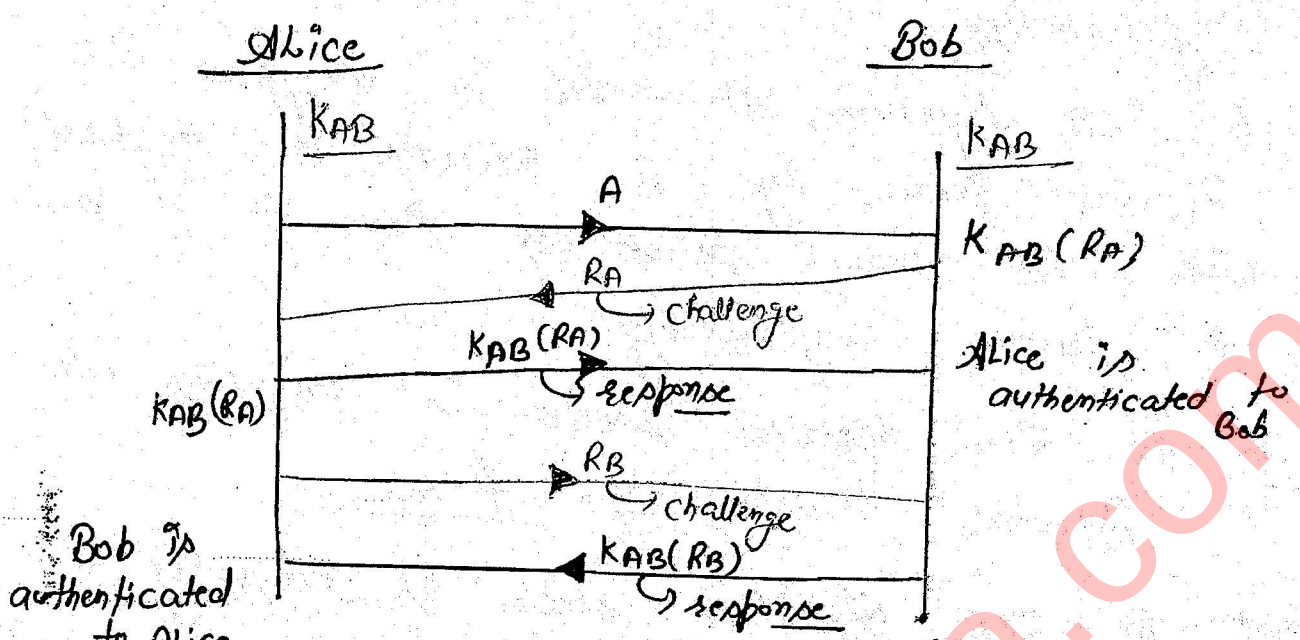
⇒ Diffie-Hellmann key Exchange :-

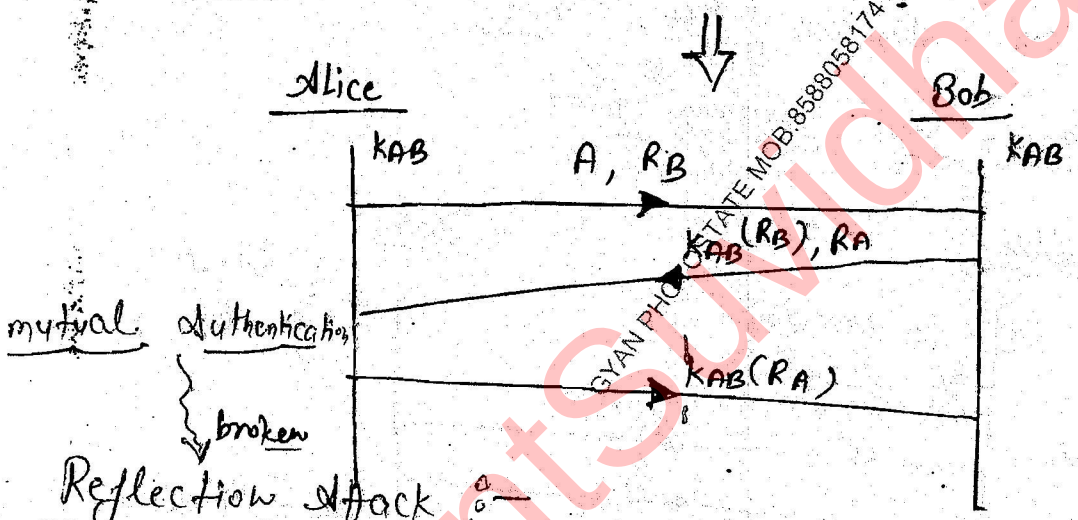


~~Mutual Authentication~~

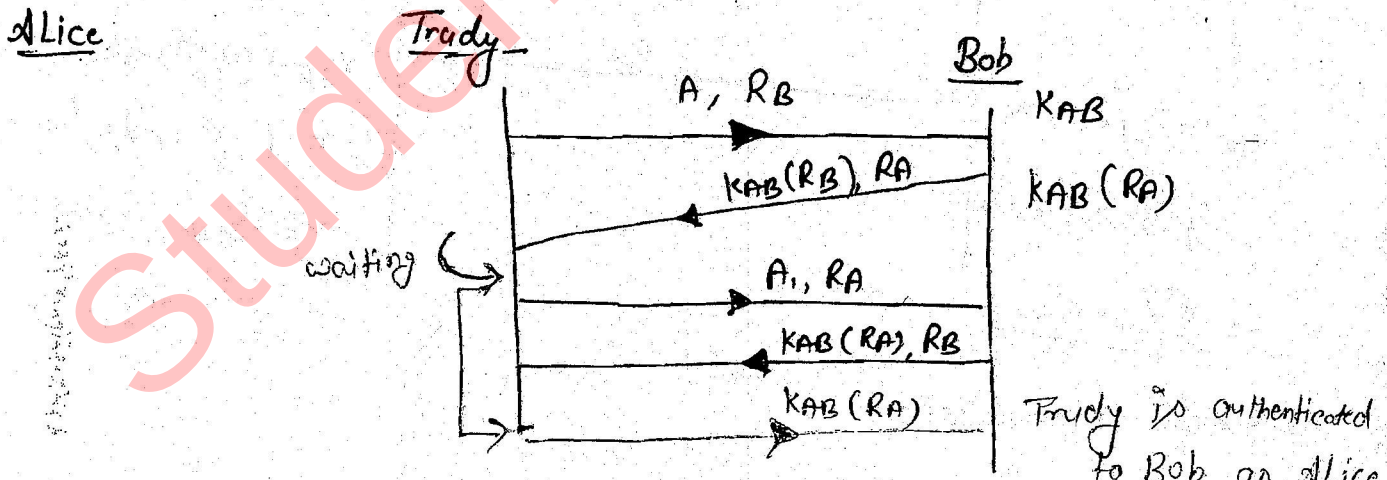
StudentSuvidha.com
GYAN PHOTOSTATE MOB.8588058174
Download all Notes and papers from StudentSuvidha.com

Mutual Authentication using Diffie-Hellman key exchange:





Reflection Attack :-



★ Mutual Authentication can be broken using Reflection attack.

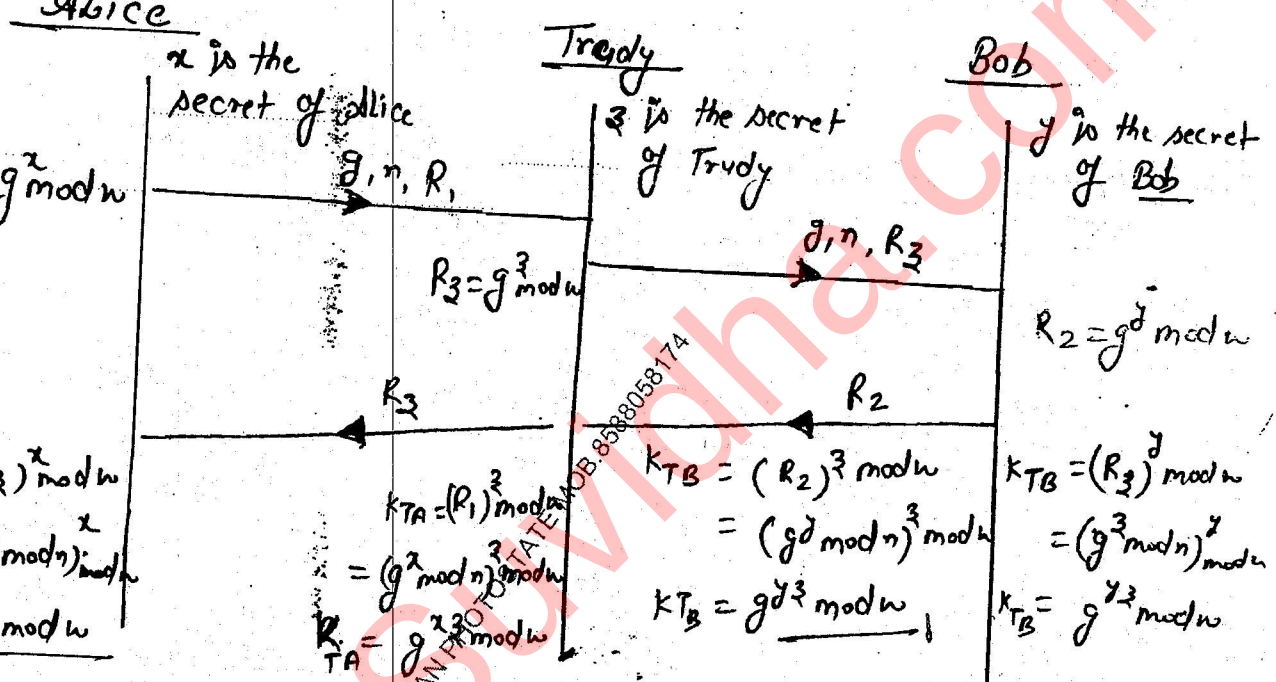
STATE MOB.8588058174 GYAN PHO

StudentSuvidha.com
Download all Notes and papers from StudentSuvidha.com

Man in middle attack :-

K_{AB} ↓ broken

★ whenever the packets are transmitted, If Hacker has modified the source IP then the request will go to the destination but the reply will come to Hacker.



★ Diffie Hellmann key itself can be broken using MAN in middle attack.

★ Drawback of Diffie Hellmann Exchange :-

X	y	for n' people
K_{xy}	K_{xy}	
X	z	n keys required.
K_{xz}	K_{xz}	
X	w	
K_{xz}	K_{xw}	

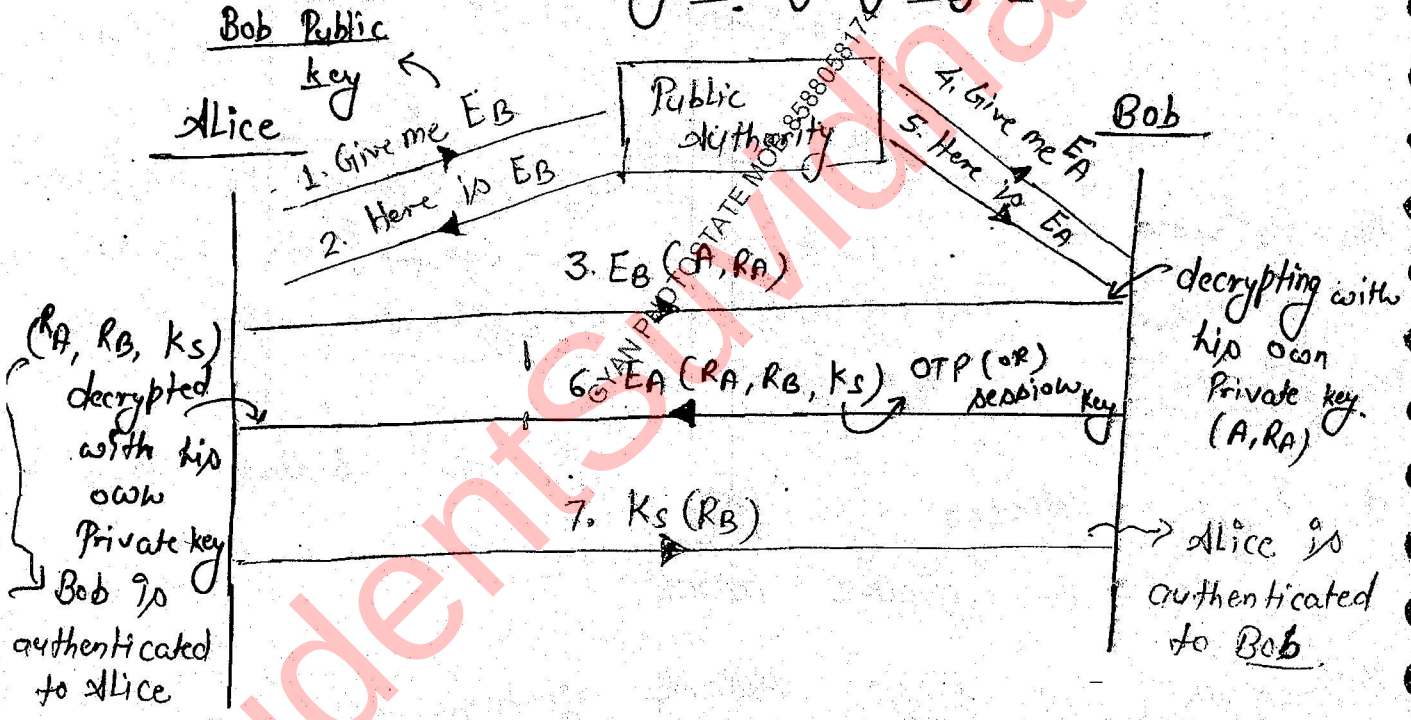
GYANPHOTOSTATE MOB.8588058174
StudentSuvidha.com
Download all Notes and papers from StudentSuvidha.com

* The drawback of Diffie Hellmann key is, if we want to communicate with n people then n keys are required.

* Remembering all the key values or maintaining a database of all the key values is difficult.

* So, the generation of the key is taken care by third party or certified Authority.

⇒ Mutual Authentication using RSA Algorithm :-
(or Public key Cryptography)



* Mutual Authentication using RSA Algorithm is better than mutual Authentication using Deffie hellman in terms of security.

* Mutual Authentication using diffie hellman key is better than mutual Authentication using RSA in terms of time.

Download all Notes and papers from StudentSuvidha.com

★ Alice

RSA Algo
(i) Private key of Alice
(ii) Public key of -

Bob → RSA Algo → Private key, Public key

Private key of Alice (Sender) → (A, E_B(A, R_A)) → Public key → decrypting with his own Private key A, R_A

Better than above: E_B (A, Private key of (A, R_A)) ✓
Alice

Que. ★★ (1)

A and B are only two stations on Ethernet. Each has a steady queue of frames to send. both A and B attempt to transmit a frame, collided and A wins the 1st back-off race. At the end of successful transmission by A both A and B attempt to transmit and collide. The probability that A wins the second Back-off race is : ?

A B

* A wins the Back-off race

A

new frame k = 1 ← * → same frame k = 2

$w.T_1 = (0,1) * P.T$

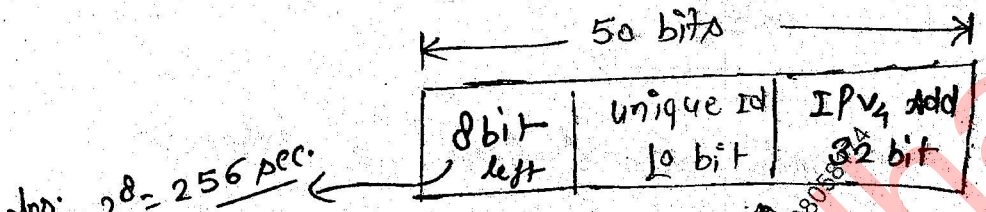
$w.T_2 = (0,1,2,3) * P.T$

A	B
0	0
P.T	P.T
	2 P.T
	3 P.T

$\Rightarrow \frac{3+2}{8} = \frac{5}{8}$

Student Suvidha.com
IMAGE PHOTOSTATE MO. 8588058174
Download all Notes and papers from StudentSuvidha.com

(2) Every Host in IPv4 network, has 1 sec. resolution real time clock with battery backup. Each host needs to generate upto 1000 unique identifiers per second. Assume that Each host has global unique IPv4 Address. Design a 50 bit global unique Id for this purpose. After what period (in sec.) will the identifiers generated by a host wrap around



Ans. $2^8 = 256$ sec.

1000 unique ~~genere~~ Identifier = 2^{10} ← 10 bits

$2^9 = 512$ not sufficient

Note :-

For Stop & wait Protocol $L.U. = 1 * \frac{T.T.}{T.T. + 2 * P.T.}$

For GBN Protocol $L.U. = \frac{N}{\text{No of frames}} * \frac{T.T.}{T.T. + 2 * P.T.}$

N ← window size

GYAN PHOTOSTATE MOB. 9588056854
StudentSuvidha.com

Download all Notes and papers from StudentSuvidha.com

Que:- Consider store & forward packet switched network. The B.w. of each link is 10^6 bits/sec. User on host A sense a file of size 10^3 Bytes to host B. in three different ways:-

Case:- (i) A single packet containing the complete file is transmitted from A to B.

(ii) The file is split into 10 equal parts. & these packets are transmitted from A to B.

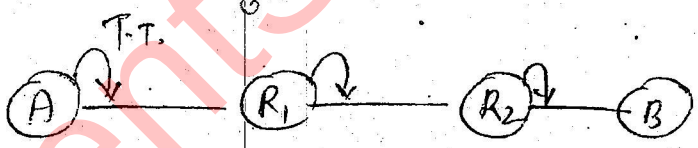
(iii) the file is split into 20 equal parts. (Each packet contains 100 Bytes of header along with the user data.) (Consider only transmission time & ignore Processing, Propagation delay)

Sol^n:-

File = 10^3 bytes

B.w. = 10^6 bits/sec.

$$\text{T.T. of Packet} = \frac{\text{Data size}}{\text{B.w.}} = \frac{(1000+100)*8}{10^6 \text{ bits/sec}} = \frac{8800}{10^6} = 8.8 \text{ millisec}$$

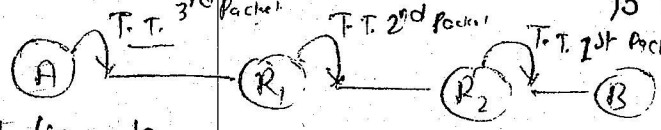


(i) A to B = 3 * 8.8 millisec = 26.4 millisec

(ii) $\frac{1000 \text{ bytes}}{10}$ = 100 bytes → Each packet size

100 bytes + 100 bytes header = 200 bytes

$$\text{T.T. Packet} = (100+100) = \frac{200*8}{10^6 \text{ bits/sec}} = 1.6 \text{ millisec}$$



Total time to reach B of TT1 = 3 * T.T. = 3 x 1.6 = 4.8 millisec

2nd Packet = 4.8 + 1 x 1.16 =

StudentSuvidha.com
GYAN PHOTOSTATE MOB.8588881
Download all Notes and papers from StudentSuvidha.com

10^{th} Packet $= 4.8 + 9 * 1.6$

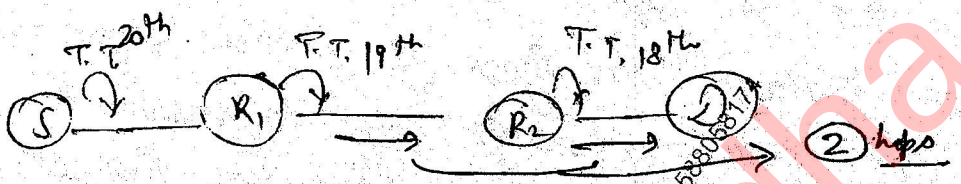
$= 19.2$ milli sec.

(iii)

$$\frac{1000 \text{ Bytes}}{20} = 50 \text{ Bytes} + \underbrace{100 \text{ Byte}}_{\text{Header}} = 150 \text{ Bytes}$$

↑ Each Packet size

$$\text{T.T.}_1 \text{ of Each Packet} = \frac{150 * 8}{10^6 \text{ bit/sec.}} = 1.2 \text{ milli sec.}$$



20 Packets $= 20 * 2 = 24$ milli sec.

~~19th Packet~~ $\Rightarrow 24 + 2 * 1.2 = 26.4$

GYAN PHOTOSTATE MOB 8580805817

StudentSuvidha.com

Download all Notes and papers from StudentSuvidha.com