PAGE NO.:
DATE: / /

OSI MODEL

7 Layers

Session

Application → URL decide करता, domain name बताता eg https://www.google.com (security)

Presentation → Encryption / Decryption → Cryptography (security of data)

Session → Dialog control, session control

Transport → TCP / UDP / SCTP

N/w → Routing Protocol + Congestion Control Algo

DLL → MAC, LLC } M2

Physical Layer → Transmission media } M1

Data Transfer

Transport → Process to Process → Transport layer meant for reliable data Transmission

Network → ~~Node to Node~~ Host to Host → means work on same network

Data Link → ~~Host to Host~~ Node to Node

If one person finds you

अगर वो Univer. तक पहुँच जाता – Host to Host

" " Department " " – Node to Node

" " आप तक या " " – Process to Process

Data Link Layer

Peer to Peer
- Go Back N
- Sliding Window

Broadcast
- ALOHA
- SLOTTED ALOHA

work of routers is to forward packet at least cost.

PAGE NO.:
DATE: / /

TCP → Connection Oriented → always ensure that data is received

UDP → Connectionless → flow is it doesn't ensure data receiver तक पहुँचा कि नहीं।

N/w Layer
- IP (V4, V6)
- IGMP
- ICMP (Internet Control Message Protocol) eg: ping
- ARP (Address resolution Protocol) eg: Domain name
- RARP

→ Routing the Packets

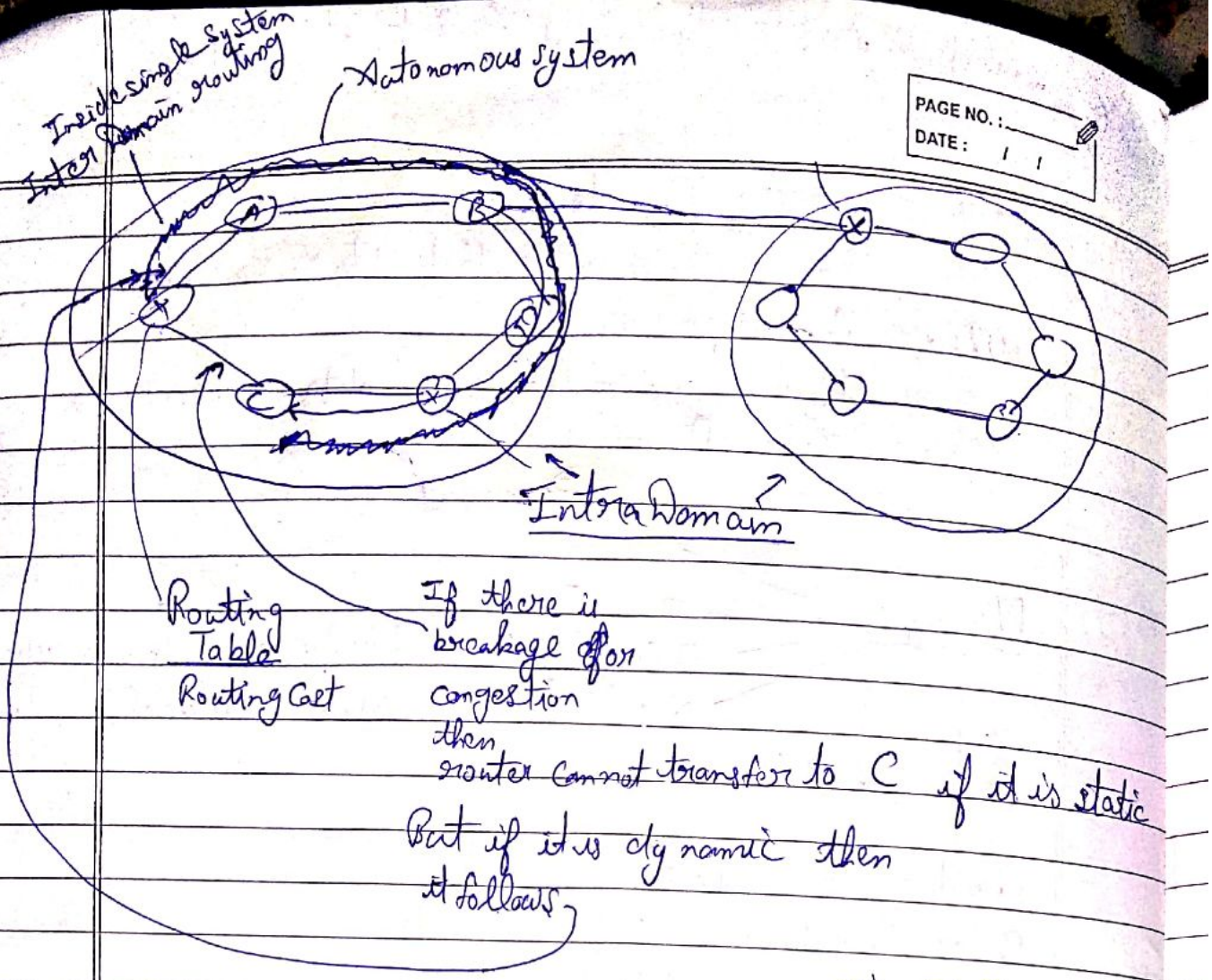
⇒ Router connect one LAN to another

LANs: Token ring, Ethernet, FDDI

There are different routing algorithms.

⇒ In routing the pathway the lowest cost is considered the best. A Router can find the optimal combination if it knows about the cost of each link. Several routing algorithms are meant for these calculations.

⇒ 2 types of routing Mechanism
- Adaptive (Dynamic)
- Non-Adaptive (Static)



Routing Table
Routing Cost

If there is breakage of or congestion then router cannot transfer to C if it is static
But if it is dynamic then it follows

V. Im

Routing Algorithm
1) Link State Routing
2) Distance Vector Routing

Two types of routing
i) Inter Domain routing
ii) Intra Domain routing

eg) जब Jio का router खराब हो जाए तो वो automatically nearest वाले से connect हो जाता है। Its dynamic.

Distance Vector Routing :-

In this each router share its knowledge about the entire network with its neighbour. The three keys of this algo. are :-
1) Knowledge about whole network
2) Routing only to neighbours
3) Information sharing at regular interval.

PAGE NO. :
DATE : / /

1) Knowledge about whole network :-

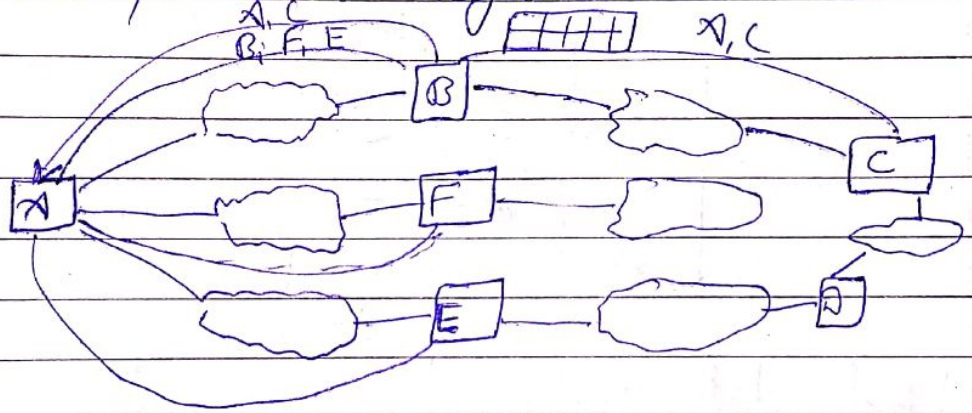
Each router share its know. about entire network. It sends all of its collective know. to its neighbour.

2) Routing only to neighbours :-

Each router periodically sends its knowledge about the n/w only to those router to which it has direct link

3) Info. sharing at regular interval :-

After ever 30 sec. for eg. each router sends its info. about whole n/w to its neighbour.

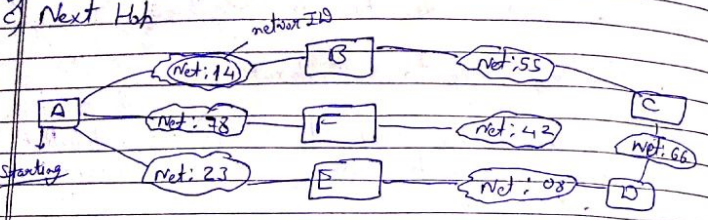


Flooding नहीं हुई only nearest neighbours को every 30 sec. वो msg किया है।
Due to this routing table is updated.

link State Routing :- ये flooding करता है।
Its type of mesh network.

PAGE NO. :
DATE : / /

Routing Table — 3 entries
a) Network ID
b) Cost
c) Next Hop



Routing Table

14	1	B
78	1	F
23	1	E
55	2	C
08	2	E
66	3	C

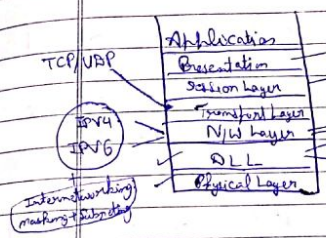
Link State Routing

In link state routing each router share the know. of its neighbourhood with every other router in the network. 3 keys are
Knowledge about neighbourhood
To all Routers
Info. sharing when there is a change

Does not maintain routing table.

⇒ When a router floods the n/w with info. about the neighbourhood, it is said to be advertising. The basis of advertising is a short packet called link state packet. Every router see the link state packet and store it in a info. called link state database.

CLASS MISS



Control files → zip, archive, pdf
Ebub/readers + writer

Security :-

Security in networking is based on cryptography which is the science of transforming messages to make them secure and immune to attack. Cryptograph can provide five different features to messages

i) Authentication → Features provided to messages → verifying
ii) Confidentiality
iii) Non-repudiation
iv) Integrity → Correctness
v) Entity Authentication

Messages + Entity Authentication
! means user

PAGE NO.:
DATE: / /

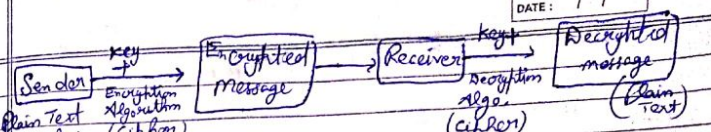
i) Authentication :- It is a service in which receiver needs to be sure that a 3rd party has not sent the message. (intruder)
message
means message is send by sender only.
1st Party - Sender
2nd Party - Receiver
3rd " - Intruder

ii) Confidentiality :-
It means sender & receiver send only messages which make sense to each other, for all others, the message shld be garbage.
→ This will discussed in cryptography techniques

iii) Non-Repudiation :-
It means that a sender must not be able to deny sending a msg that he/she has infact sent.
→ ie Neither Sender nor receiver can deny that ~~कोई~~ msg ~~भेजा~~

iv) Integrity :- It means data must arrive at receiver exactly as they were sent.
Some terms associated with Cryptography
a) Plain text & Cipher Text
(original text)
b) Key
c) Ciphers
=> ~~Algo~~

PAGE NO.:
DATE: / /



⇒ Algorithm can be type of Permutation or Combination

key
Symmetric
Asymmetric

Symmetric key Cryptography :- Sender & receiver have one same key
Also known as Private key cryptography.

Asymmetric Key " :- Sender & receiver has 2 key Public & Private.
BUT Sender Public key से encrypt करता है receiver Private key " decrypt करता है & vice versa.

2 categories of Cryptography
i) Symmetric key Cryptography → Also known as Private key cry.
ii) Asymmetric " " → " " " Public " cryptograph

Symmetric Key Cryptography :-
:- In this same key is used for encryption & as well as decryption. and it has traditional algo. (ciphers) associated with it.
(Encryption)

Traditional Ciphers
Substitution
Transposition
Mono alphabetic
Polyalphabetic

eg) Key- 3 alphabets आगे के eg A B C D E F G H I J K
D E F G H I J K

H E L L O

K H O O R
Encrypted message

Mono alphabetic

Poly-alphabetic :- If twice alphabetic occured it is not substituded by same character twice

eg) HELLO
K BOPR
Encrypted msg
not O twice
use diff. character for substitution

Transposition

Key { Plain Text: 2 4 1 3
Cipher Text: 1 2 3 4

+ we can add fake characters

eg) HELLO MY CLASS
↓
HELL OMYC LASS
↓
ELHL MCOY ASLS

Disadvantage :- If intruder को key मिल गई, तो decrypt कर लेगा।

~~Asymmetric Key Cryptography~~ :-

In modern ciphers

i) XOR ciphers
ii) Rotation Ciphers

XOR cipher :-
It uses exclusive OR operation for encryption as well as decryption.

Rotation Cipher :- In rotation cipher, input bits are rotated to the left or right.

Key { Plain Text 2 4 1 3
Cipher Text 1 2 3 4

• No of times of rotation is actually key.

IP address
↳ keeps on changing
TCP/IP
V4 V6
eg 10.19.13.17
8 bits
32 bits

MAC address
↳ Physical address
↳ change नहीं होता but in reality it can be changed

Now every device having ip address. So we use 128 bits for address
So we can give IP address to 2^{128} devices

⇒ DNS (Domain name Server)

www.goggle.com URL ⟺ IP
DNS → ~~connect~~ intermediate
We can also do this by IP address.

⇒ Commands

→ ipconfig
Ethernet or Local Area - -
IPV4 : 16.178.15.16

ii) ping www.google.com → Connectivity → Latency

echo request
Response

iii) traceroute

iv) arp

IP	MAC

Basically mapping of IP add. with mac address

v) netstat

In networking
Socket
IP address + port no.
address of process

	n/w	Host
A → 0-127	-	- - -
B → 128-191	- -	- -
C → 192-223	- - -	-
D → 244		

eg 123.17.16.15

eg) 175.18.19.6
175.19.3.5
→ Class B but not on same network bcz in class B we check 2 octet for network

Subnet को 1 से represent करते है |
Host को 0 " " " " "

Subnetting :- Why subnetting
↳ to easy organisation
↳ also provide security bcz any forward ip

Exercise

i) 4.23.145.90
n/w ID | host
Class A
4.0.0.0 n/w address

ii) 227.39.78.7
class D

iii) 11011101.11111011.10111101.00110011

Que 194.168.0.0 / 24 → represent bits of subnet
class C
we have to divide this into 2 parts and we require min. 50 host in each part.

2^x = no. of subnet → bits req. to represent subnet or (no. of subnet bits)

$2^1 = 2$
⇒ 1 bit
↳ से 1 bit कहाँ से आएगी

24 bit | Subnet | 7 bits for host

2^7 host we represent
128

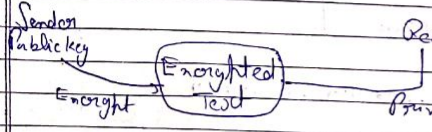
194.168.0.0 → 194.168.0.127 — one n/w
194.168.0.128 → 194.168.0.255 — 2nd network

$2^{(0)} - 2$ ⇒ no. of host
no. of 0's
minus 2 bcz last bit is reserved as well as very first bit

PAGE NO. :
DATE : / /

Asymmetric Cryptography:

In asymmetric or Public key cryptography there are 2 keys, i) Public & Private. Private key is kept by receiver & Public key is kept announced to Public.



Do from Book

There are 2 types of Algorithm

i) RSA under name of its inventor Rivest Shamir Adelman:-

In RSA the mechanism used is

a) Sender will choose two very large prime numbers 'p' & 'q'.
b) It multiplies these two prime numbers to find $n = p \times q$ another factor
c) Sender calculates other no. called ϕ i.e $\phi = (p-1)(q-1)$
d) Then it chooses random integer e and calculates d such that $d \times e = 1 \bmod \phi$

most imp. factor in RSA

e, n → Public
d, ϕ → Private

or

ii) Daiffee Hellman:- RSA is basically public key cryptosystem which is used for encryption and decryption.

Diffee Hellman on other hand is meant for key exchange.

forme no.

PAGE NO. :
DATE : / /

- If diffee hellman cryptosystem 2 parties, sender & receiver (Sender & receiver) creates a symmetric session key to exchange data. They don't have to need to agree on a key. It can be done through the internet.
  The 2 Parties they choose 2 prime no. 'p' & 'g'.
  ⇒ p is large prime no. of on the order of 300 decimal digits
  ⇒ 2nd no. g can be a random no.
  Sender will calculate $g^x \bmod p$ and send to receiver where x is random.
  Receiver will calculate: $g^y \bmod p$ where y is any random no.
  Then they interchange these no.

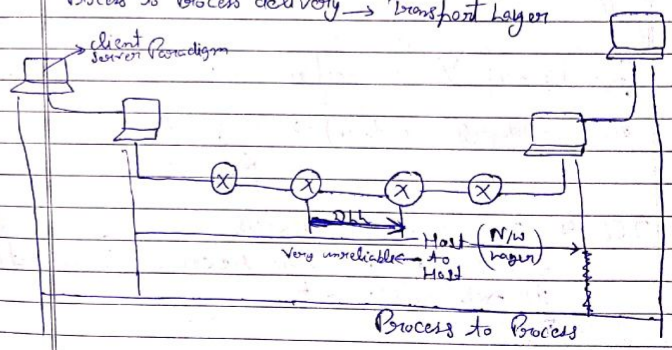
(Session खत्म होते ही सब कुछ discard हो जाएगा।)
i.e As session is expired, key is lost.

⟺

Transport Protocol (Layer)

Process to Process delivery → Transport Layer

Reliability — Error Flow



Intro

⇒ Whenever we need to deliver something to one specific destination, we need an Address.

- Transport layer uses socket address which is combination of IP address and Port no.

- Internet Assigned Number Authority (IANA) :- It has divided port numbers into 3 ranges
  i) Well known
  ii) Registered
  iii) Dynamic :- Neither controlled nor registered
  --- Ephemeral ---

Port no. range :- [0 to 65,535]

(0 to 1023) → upto these are valid Port number

⇒ The Port no. which are only register by IANA are not controlled by this authority. They are only used to prevent dublication.

Connection Less Vs Connection Oriented :-

UDP (User Datagram Protocol) → connectionless
↓
no need to remember sequence no.

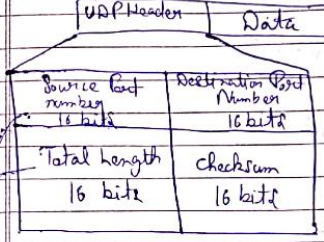
TCP → 3 way handshaking Process
i) Packet from sender to receiver (Echo packet)
ii) Acknowledgement
iii)

Transport layer service can be reliable or unreliable.

⇒ If application layer program need reliability then it use TCP

⇒ If it needs only error & flow control but only reliability then it use UDP.

User Datagram Format



All 4 की explanation भी करनी है।

⇒ 2-3 lines
Pseudo-Header for checksum ✗ नहीं करना

UDP Operation
i) Connectionless service :- neither sequence nor acknowledgement
ii) Flow & Error control.
iii) Encapsulation & decapsulation
iv) Queuing
1
2 Types of queue
i) Outcoming queue ii) Incoming queue

TCP
i) Process-to-Process connection :- fully take responsibility of msg
ie assign sequence & acknowledgement no.
ii) Stream Delivery Service :- TCP sends data in stream of bytes

iii) Sending or Receiving Buffer
iv) Full duplex communication
v) Connection Oriented.

☆ Virtual circuit & datagram subnet