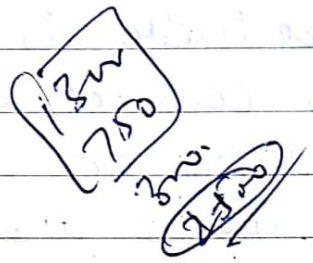
Date

The seven layers of OSI are : APSTNDP

A	Application layer
P	Presentation
S	Session
T	Transport
N	Network
D	Data-link
P	Physical

Sunday



Physical layer :

- Its concerned with transmitting bits over a communication channel.
- The design issues have to do with making sure that when one side sends a one (1) bit it is received on the other side as 1 bit.

Application layer :

- Contains a variety of protocols required by users.
- Commonly used app protocol is http (basis for WWW)
- Other protocol used are email, ftp, network news.

Data-link layer : (DLL)

The main task of DLL is to transfer

a bit transmission facility into a line, that appears free of undetected transmission errors to the network layer.

- Its achieved by having the sender break up the I/p data into the data frames and transmit the frames sequentially.
- [redacted]he receiver is reliable, the receiver [redacted]iums correct receipt of each frame by [redacted]ing back an acknowledgement frame.
- [redacted]ther issue that arise in the DLL is to communicate a fast transmitter to a slow receiver.
- Some traffic regulation mechanism is often required to let the transmitter know how much buffer space the receiver has at the moment.
- This flow regulation and error handling work together.
- A sublayer of DLL called MAC (Medium access control) deals with how to control access to the shared channels.

NETWORK LAYER:

It controls the operation of the subnet. A key design issue is based on how packets are routed from source to destination.

Date

- Routes can be based on static or dynamic table.
- In static state, if too many packets are present in the subnet (channel between source & destination) at the same time, they will come in one another's way causing, BOTTLENECK PROBLEMS.
- The control of such congestion also belong to network layer. The quality of services is also a network layer issue.

When packets travel from one network to another, many problems arise, like —

1.) The addressing used by the 2nd network may be different from the first.
2.) Second may not accept the packet, becoz the size is too large.
3.) The protocol may be different.

Eg.

Transport layer:

- The basic function is to accept data from the upper layer and split it into smaller units & pass to network layer, and to

Shipra

ensure that all pieces arrive in a sequential order.

- It also defines what type of services to provide to the session layer, ultimately to the user of network.
- The most popular type of transport connection is error free point to point channel that delivers messages in the order in which they are sent.
- In other kinds of transport services, are the transportation of the isolated messages with no guarantee of the order of delivery and broadcasting of msgs to multiple destinations.
- The type of service is defined when the connection is established. This layer is a end to end layer, all the way from source to destination.

Session Layer :

- It allows the user to establish on different machines, session between them.
- Session provide 3 kinds of services —
  - Dialog control
  - Token management
  - Synchronisation

  → Preventing 2 parties from attempting the same critical operation at the same time.

Date

Presentation Layer:

- Its concerned with syntax & semantics of the information transmitted.
- In order to make it possible for computer with different data rep to communicate, the data structure to be exchanged and can be defined in an abstract way, along with standard encoding to be used on the wire. The presentation layer manages these abstract data structures and allows higher level " " to be defined & exchanged.

TCP-IP Reference Model

It has 4 layers -

→ Application — telnet, ftp, smtp, dns
→ Transport — tcp, udp
→ Internet — ip
→ Host to Network - lan - satnet
arpanet - packet radio

udp = user datagram pro (wireless)
tcp = transmission control protocol
ftp = file transport protocol
smtp = simple mail transfer protocol
dns = domain name service

Date

Application layer :

- The TCP-IP model doesn't have the session & presentation layers.
- In application layer it contain all the higher level protocols.

1) TELNET - teamviewer
2) ftp
3) smtp - Ex. MS Outlook
4) dns
5) http

Host to Network layer :

- TCP-IP reference model doesn't have knowledge about what happens there.
- They generally know that the user has to connect to network using some protocols, so it can sent IP packets to it.
- This protocol is not defined for network and host to host communication.

Internet layer :

- Permits host to inject packets to any network and then travel independently to destination.
- They may even arrive in a different order, than in which they were sent.
In this case transport layer is responsible for rearranging them.

Shipra

Date

Transport layer :

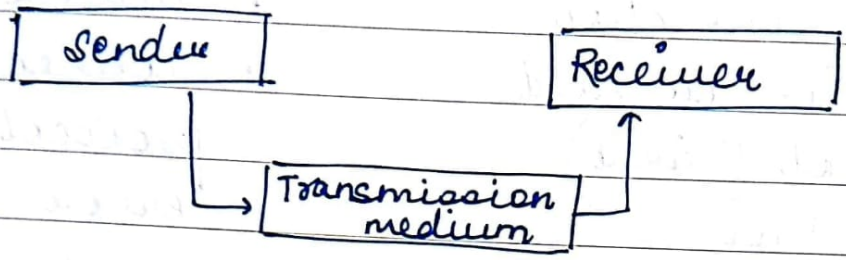
TCP	UDP
• reliable connection	• unreliable
• connection oriented protocol (wired)	• connectionless protocol (wireless)
• error free transmission	• error oriented packages are sent
• broadcasting area is less	• area is more
• follow sequence	• sequence is not followed.

TRANSMISSION Media

I. Guided (wire-oriented)
- ↳ Co-axial cable
- ↳ Twisted pair cable (speaker, air disturbance ↑)
- ↳ fibre optics (for long distance comm.)

II. Unguided (wireless)
- → free on air space.

Transmission Media: A transmission medium is defined as anything that carries info from source to destination.



I Guided Media:

- Twisted pair & co-axial cables are using copper conductors and transport signals in the form of electric current.
- Fibre optics Transport signal in the form of light.

* TWISTED PAIR CABLE:

- It contains 2 conductors, each with its own plastic insulation. One of the wire contains current & the other is grounded.
- Noise & cross communication may affect both wires & create unwanted signals.

We can categorize twisted pair cables into two parts —

- ~~UDP~~ UTP: Unsheilded twisted pair eg. (LAN)
- STP: Sheilded twisted pair eg (high voltage cables)

Shipra

Date

Performance:

- A twisted pair cable can pass a wide range of frequencies.
- They may be used for transmission of both analog & digital signal.
- For analog signal, repeaters are required for every 5-6 Km.
- For digital signal repeaters are reqd. for every 2-3 Km
- As compared to other transmission (guided) media, twisted pair cable is limited in BW, distance & data rate.

Application:

- Used in telephone lines to provide voice & data channels.

CO-AXIAL CABLES:

- It carries signals of higher frequency ranges than twisted pair cables.
- Instead of having 2 wires, we use central core copper wire enclosed with an insulating layer.
- The outer metallic ~~wrapping~~ serves as a shield against noise and works as second conductor, thus completing the circuit.
- The metallic sheild is insulated by black or white plastic layer.

Co-axial cable connectors:

We use Bayone Neill Concelman (BNC) to attach 2 co-axial cables & to connect 3 co-axial cables we use BNCT type of connectors.

Application:

- Its used in television distribution
- long distance telephone communication
- Short run computer system links,
- LAN

Performance:

- high freq. rate
- noise immunity is high
- carries high data rate BW
- for long distance commu.
- cross commu. effect is lessened.

FIBRE OPTICS:

- Its made of glass or plastic and transmits info in the form of light.

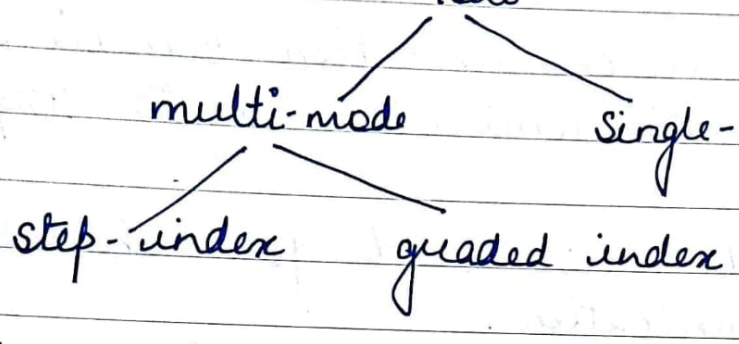
An optical fibre cable has a cylindrical shape and has 3 layer -

- core-part
- cladding
- jacket

Date

Propagation mode:

There are three types of propagation modes-



Multimode is used because multiple beams from a light source move by in the core in different paths. How these light beams move within depend on the structure of the core.

In multimode step index fibre density of the core remains constant from centre to the edge. A beam of light moves by this constant density in a straight line, until it reaches the interface of the core.

- At the interface, there can be a change of angle by its density.
- The step-index multimode refers to instant changes of signal those passes by the fibre.

Singlemode : Its used to transmit laser light for long distance communication.
- It can travel upto 100 kms without using any repeaters.
- Its used for telecommunication services for high data rate transmissions upto 10Gbps.

Graded index mode : Its used for short distance communication.
- Its ranges from 3km to 6km. It does not follow the pattern of angles & straight lines.
- It follow technique of wavelength which is dependent on voltage density.

II UNGUIDED MEDIA :

- It transport electromagnetic waves without using any physical conductor.
- This type of communication is called wireless communication. Signals are normally broadcasted by free space & are available to anyone who has device capable of receiving them.
- Unguided Signal can travel from source to destination in the following 3 ways -
- ground
- sky
- line of sight

Shipra

Date

- In ground propagation, radio waves travel by the lowest portion of the atmosphere.
- These low frequency signals are then transmitted in all directions.
- Distance coverage depends upon the amount of power in the signal.
- In electromagnetic field, greater the power, greater the distance.
- In terms of frequency (wave), the greater the power, shorter the distance.

- In sky propagation, higher radio frequency waves move up into the ionosphere, where they are reflected back to the earth.
- This type of transmission allows for lower output power, and greater distance.

- In line of sight propagation, very high frequency signals are transmitted in straight line from antenna to antenna.
- Antennas must be directional, facing each other and either tall enough or close enough, not to be affected by the geographical curvature of the earth.

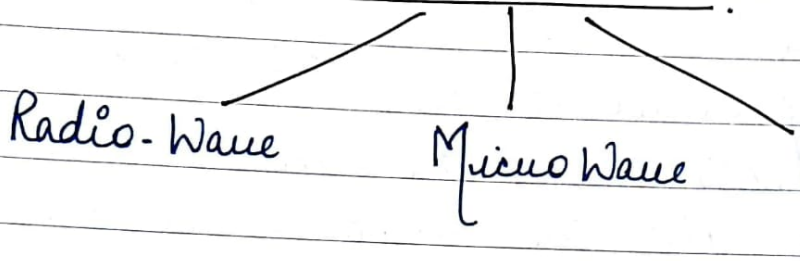
Date

BAND	RANGE	PROPAGATION	APPLICATION
VLF	3-30 KHz	ground	- long range radio navigation
LF	30-300KHz	ground	- navigation system
MF	300K - 3MHz	sky	- AM radio
HF	3-30 MHz	sky	- aircraft comm.
VHF	30-300MHz	sky & line of sight	- FM radio
UHF	300M - 3GHz	line of sight	- satellite, cellular phones, pager network
SHF	3-30 GHz	line of sight	- satellite
EHF	30-300GHz	line of sight	- satellite - radar

SHF = Super high freq.
UHF = Ultra " "
VHF = Very " "
MF = medium "
EHF = Extremely " "
VLF = Very low freq.

Date

Wireless Transmission



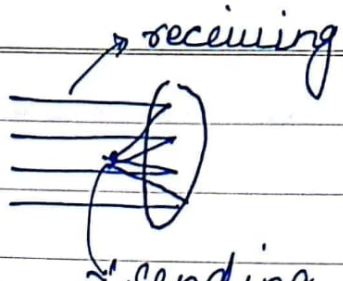
Radiowave :

- In radio waves, freq range is 3KHz to 1GHz
- communication takes place omni-directionally
- Used in AM, FM communication.
- Used in TV, cordless phone, pager services.

Microwave :

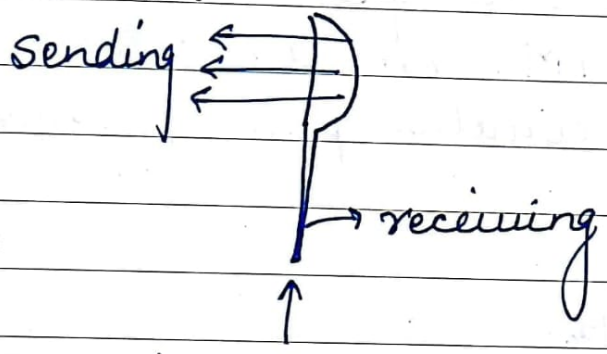
- 1 KHz to 300 GHz
- In very high freq. microwaves, they cannot penetrate walls.
- Microwave band is relatively wide almost 299 GHz, so high data rate is possible.
- Its use of certain portion of the band requires permission of the authority.
- Works unidirectionally i.e receiving antennas need to be aligned.
- There are two types of unidirectional antennas —
  - * dish antenna / Parabolic dish antenna
  - * Horn antenna

Paraboloic dish antenna :



- Its based on geometry of paraboloa
- Every line parallel to line of sight reflects from the curve at angles such that all line meet a certain point called focus.

Horn antenna :



single I/p ; multiple O/p's

Infrared Wave :

- Works in freq. range of 300GHz to 400THz.
- Used in short range communication.
- It cannot penetrate walls.
- Advantages of remote (T.V).

Date

Satellite Communication :

There are 3 satellite communication categories:-

- Geo
- Meo
- Leo

- Geo satellite works in the altitude of 35 km to 35786 km.
- Meo satellite are located in the altitude of 5000 to 15,000 km.
- Leo are below 2000 km.

Frequency band for satellite communication :

Band	Downlink (GHz)	Uplink (GHz)	Bandwidth (MHz)
L	1.5	1.6	15
S	1.9	2.2	70
C	4.0	6.0	500
KU	11.0	14.0	500
KA	20	30.0	3500

Geo Satellite:

- Line of sight propagation requires that the sending and receiving antennas to be locked onto each other location at all times.
- For this reason, a satellite that moves faster or slower than the earth rotation is useful only for short period.
- To ensure constant communication, the satellite should move at the same speed as the earth.
- Such satellite are called geostationary.
- Only one orbit can be geo-stationary / but one geo-stationary satellite cannot cover the whole earth; it takes minimum of 3 satellites equidistant from each other in geostationary earth orbit, to provide full global transmission.

Meo Satellite:

Medium earth orbit

- These satellite are positioned between 2 alien belts.
- It takes 6-8 hours to circle the earth.

Ex. GPS (Global Positioning System): It works in 15000 km above the earth.

↳ The system contains 24 satellites and is used for land, sea, and air navigation to provide time & location for ships and vehicles.

Date

↳ GPS uses 24 satellites in 6 orbits. Each orbit is designed such that, at any time, four satellites are visible from any pt. on Earth.

* Triangulation GPS is based on the triangle concept. On the map, if we know our distance from 3 pts., we know exactly where we are.

Application : used in aircraft, vehicle navigation.

Synchronisation – Book

Leo satellite : (max. speed)

- Low earth orbit satellite have polar orbits.
- The altitude is between 500 km to 2000 km with rotation period of 90 - 120 minutes. The satellite has a speed of 20,000 km/hour to 25000 kmph.
- Leo system normally has a cellular type of access, video conferencing & T.V services.
- In leo system, no: of satellites work together as a network, each satellite works a switch (one i/p, many o/p's)

Date

- Satellite which are close to each other are connected by inter satellite links (ISL).
- A mobile system communication with the satellite is called user mobile link (UML).
- A satellite also communicates with Earth stations, by a gateway link (GWL).

- Leo satellites are of 3 types –
  * little leo – 1 GHz
  * Big leo – 1 to 3 GHz
  * Broadband leo – use services like fibre optic networks

Global Star : is another leo satellite and uses 48 satellites in 6 polar orbits, with each orbit hosting 8 satellites.
- The orbit is located at altitude of 1400 km.

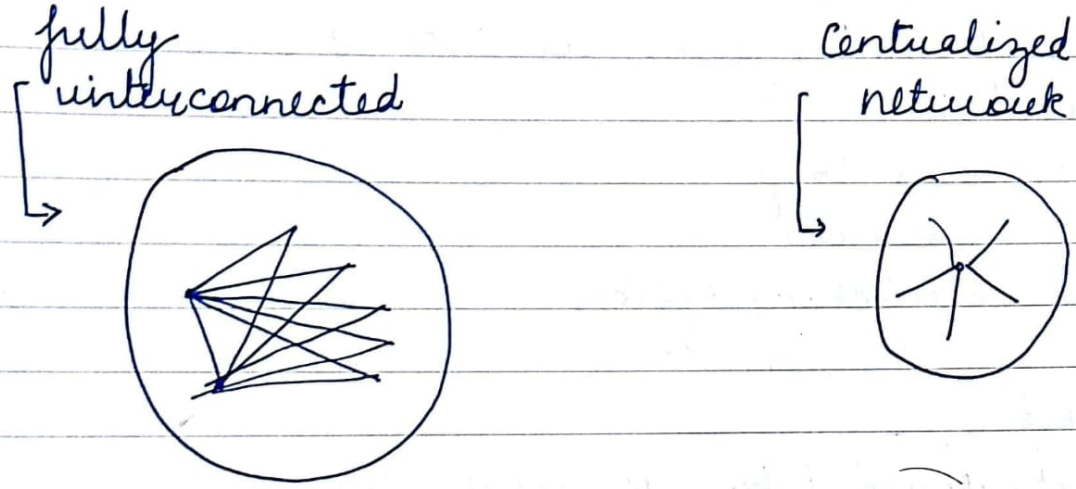
Date

PSTN

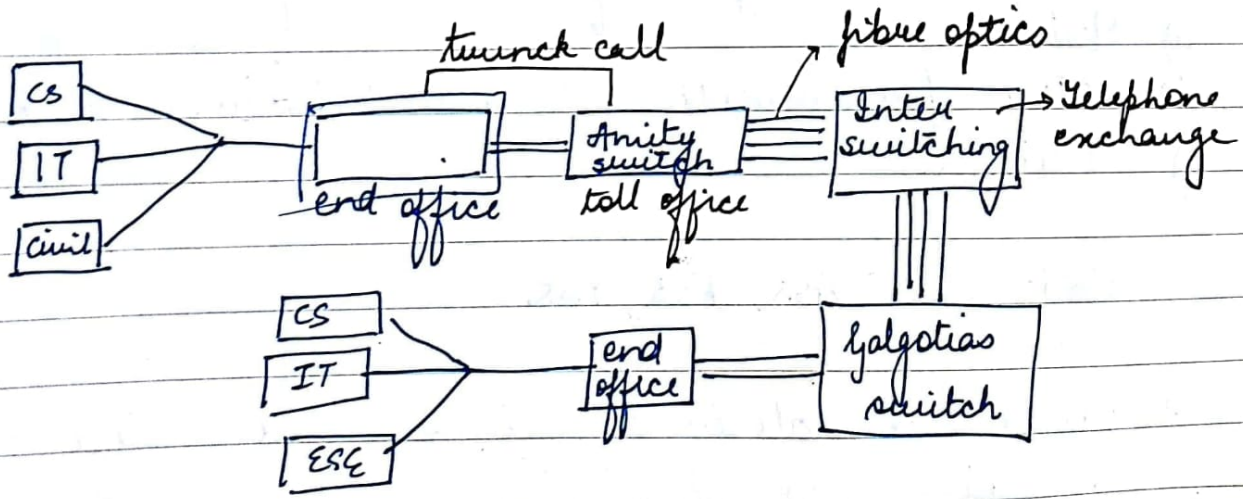
Public Switch Telephone Network :

PSTN was designed for transmitting the human voice in more or less recognisable form.

Structure of telephone system :



Ex.



Date

- If the receiving telephone is attached to another end office a different procedure has to be used.
- Each end office has a no. of outgoing lines; to one or more nearby switching centres called TOLL OFFICES.
- These lines are called toll connecting trunks.
- If we are communicating in different offices, we are using inter toll trunks.
- The telephone system consists of 3 major components —
  - local loop
  - trunks
  - switching offices

Local loop :

We have three types of local loops.

a) Modem
b) ADSL (asymmetric Digital Subscriber link/line)
c) Wireless

Write abt ASK, FSK, PSK

→ Causes to distruct transmission line —
- noise
- cross talk
- increase in distance / electromag field,

- Simplex (only one-speaking)
- Full duplex (using mobile - both speak)
- Half duplex (at a time one speak (walkie-talkie))

→ Techniques & Multiplexing
- FDM
- TDM
- WDM

→ Switching

There are 3 types of switching -
- Circuit switching
- packet
- message

Circuit Switching ← slower ∵ time is taken in making ckt first

- When you make a call the switching equipment within the telephone system looking out a physical path, all the way from your telephone to the received telephone.
- This technique is called circuit switching.
- When a call pass by a switching office, a physical connection is established between the lines of sender & receiver.
- The physical path between two telephone lines may be microwave or fiber link;

Date

onto which thousand of calls are multiplexed.
- Once a call has been setup a dedicated path b/w the two will be created & will exist until the call is finished.

The alternative to ckt switching is Packet Switching
- In this technology individual packets are sent as required with no dedicated path being set-up in advance.
- It is upto each package to find its way upto the destination.

Message Switching :
- In this switching technology, no physical path is established in advance, between sender & receiver.
- When the sender has a block of data to be sent it is initially stored in the first switching office & then is forwarded later ; one "hop" (frame) at a time.
- Each block is received, what is inspected for errors & retransmitted.
- This method is called store & forward network.

Date

Q. Difference b/w circuit & package switching?

Item	circuit	Package
1) call setup	yes	No
2) Dedicated physical path	yes	No
3) Each packet follows same route	Yes	No
4) Packet arrive in order	Yes	No
5) B.W available	fixed	dynamic
6) Time of possible congestion	at setup time	on every packet
7) Store & forward transmission	No	Yes
8) Transparency	yes	No
9) Potentially wasted B.W	Yes	No.

Imp. ★ Date

Error detection & Correction technique :

Network designers have developed a basic strategies -

- 1st strategy : for dealing with error :
  - i) ↳ Replication information along each block
  - ii) Retransmission frames

There are 3 types of error :

- Single-bit
- Burst error
- Multi-dimensional

To handle error detection & correction we follows 4 techniques :-

1) PARITY CHECK (either even or odd)
2) CHECKSOME
3) CRC (cyclic repetition cycle)
4) HAMMING CODE

bit stream broken into frames & error is checked

even

Parity check :

Multi-dimensional

	1	1	0	0	1	1	1	1
Apply	1	0	1	1	1	0	1	1
X-OR	0	1	1	1	0	0	1	0
	0	1	0	1	0	0	1	1
	0	1	0	1	0	1	0	1

If the result is even or odd, the whole lot is correct.

Shipra

Date

2) CHECKSOME:

Initial frame: 1 0 1 0 1 0 0 1
0 0 1 1 1 0 0 1

Apply → 1 1 1 0 0 0 1 0 → 1's compliment

Adder

0 0 0 1 1 1 0 1 → send to receiver.

1's compliment

→ 0 0 0 1 1 1 0 1
1 0 1 0 1 0 0 1
0 0 1 1 1 0 0 1

Add. 1 1 1 1 1 1 1 1

If all are 0's or 1's then the transmission is error-free.
i.e the pattern bits are uniform.

3) CRC:

Ex: $x^4 + x^3 + 1$ ← 4 3 2 1 0 → 11001

$1x^4 + 0x^3 + 0x^2 + 1x^1 + 1$

1 0 0 1 1 → 1

16 8 4 2 1

The terms which exist mark as 1 and others 0.

(5)-19

(4)-15

Date

x^4+x+1 → 10011

```
        11010110110000
      ) 11010110110000
        10011
        -----
         10011
         10011
         -----
         00001
         00000
         -----
          00010
          00000
          -----
           00101
           00000
           -----
            01011
            00000
            -----
             10110
             10011
             -----
              01010
              00000
              -----
               10100
               10011
               -----
                01110
                00000
                -----
                 1110
```

EX-OR

1101011011110 → regd. Transmission

Error detected

(11)

The given frame is error oriented ∵ remainder is not equal to zero.
And apply EX-OR on each step
If we apply the remainder instead of 4 zeros the answer is 0 & transmission is error-free.

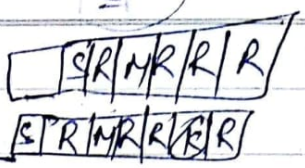
$2^0, 2^1, 2^2, 2^3, 2^4$ (5)

$2^{5-1} \geq 10$ $\quad 2^{4-1} \geq 7$

16 ≥ 10 $\quad$ 8 $\quad$ 4 = n

Date

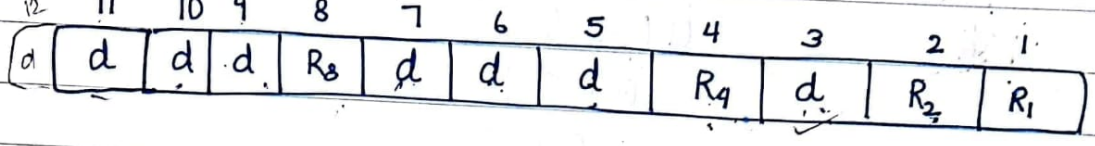
4) HAMMING CODE:



Suppose there are 7 bits ASCII code which requires 4 repeation bits that can be added to the end data bits or in-between the original data bits.

These unit positions are 1, 2, 4, 8 & we call them R_1, R_2, R_4, R_8.

7 9 11



R_1 =

r_1 → represents ↳ starting ✓
↳ group ✓
↳ gap ✓

$2^{n-1} \geq 7$

$4 \leq$

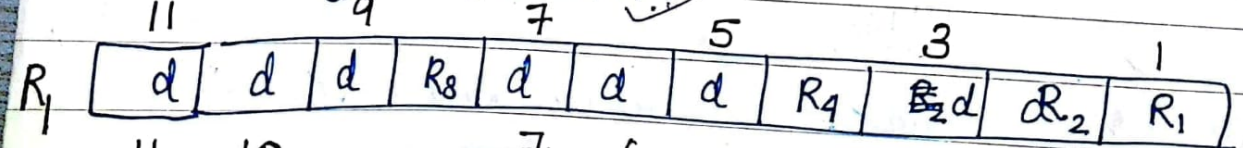
even parity

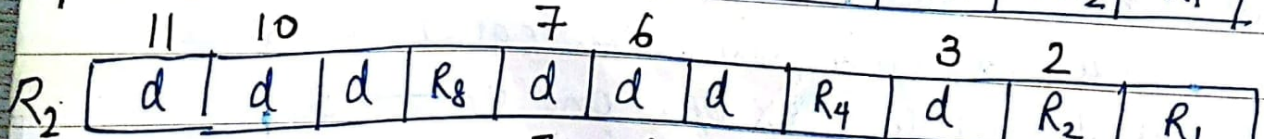
r_1 = (1), (3), (5), (7), (9), (11)

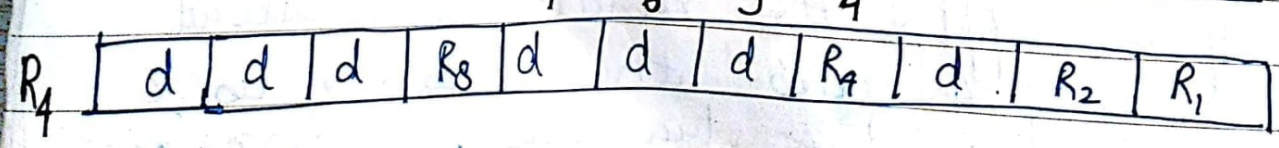
r_2 = 2 3, 6 7, 10 11

r_4 = 4 5 6 7, 8 9 10 11, —

r_8 = 8 9 10 11







Shipra

Date

	11	10	9	8							
R_8	d	d	d	R_8	d	d	d	R_4	d	R_2	R_1

Each data bit may be included in more than 1 calculation.

In the sequence of original data bits, is included in atleast two bits while the R bits are only located in one place.

m (original bits sent)	R (no: of R bits for data bits)	m + R
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

If sum = total bits sent then it is error free

Shows it is error free..

FROZOAN:

DATA-LINK LAYER PROTOCOL:

We divide the protocol in 2 parts -

1. For Noiseless channel (error free)
2. For Noisy channel (error omitted)

DLL Protocol

- (Unidirectional) Noiseless channel
  - Simplest protocol
  - Stop & wait
- (also known as sliding window protocol) Noisy channel
  - Stop & wait ARQ
  - Go-Back N ARQ
  - Selective Repeat ARQ

Shipra

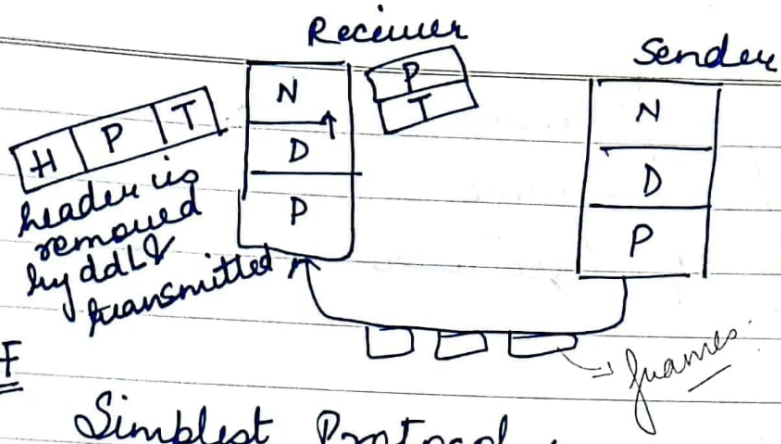
All the protocols are unidirectional in the sense that data frame travels from one node to another. Even special frames called ACKNOWLEDGEMENT (ACK) & N-ACK (Negative ACK) flow in opp. direction, for flow & error control purpose.
Data flow works only in one direction. In real life, DLLP implemented as bidirectional. In these protocols flow and error control techniques as ACK & N-ACK is included in the data frames by using specific techniques which is called — PIGGY BACKING.

⊙ In DLL we use flow control, stop & wait DLL protocols.
a) Data frames are transmitted in one direction, where each frame is individually ACK by the receiver by a separate ACK frame.
b) A sender starts a times & wait for ACK frame from the receiver before sending another frame.
c) A time-out period is used where frames not ACK by the receiver are retransmitted automatically.
d) Bit sequence no is used to differentiate the original frame or duplicate frame.

→ We use three kinds of protocols in this —
i) Unrestricted Simplex protocol
ii) A simplex stop & wait protocol
iii) A simplex the ACK with retransmission protocol

Shipra

Date



Gupta type house
house
Bridge stone, stage

F

Simplest Protocol :

→ It is a unidirectional protocol in which data-frames are travelling in only one direction from sender to receiver.

→ The receiver can handle any frame it receives with a processing time, i.e small enough to be negligible.

→ The DLL of the receiver immediately removes the header from the frame and transmits the data packet to its network layer, which also accepts the data packet immediately.

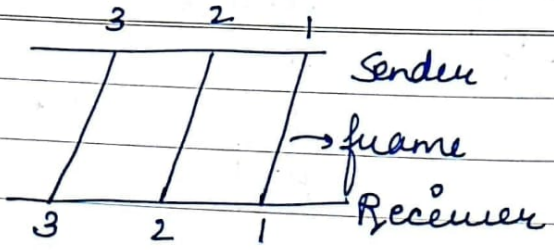
→ There is no need of flow control in this protocol.

→ The DLL at the sender side gets data from its network layer & makes the frame out of data & sends it.

→ The DLL at the receiver side receive a frame from its physical layer & extract data from frame & delivers the data to its network layer.

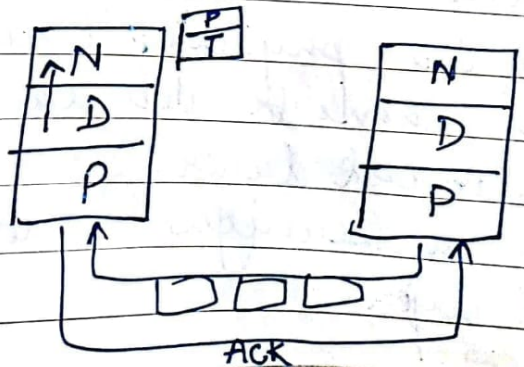
→ DLL use the services provided by the physical layer.

Shipra



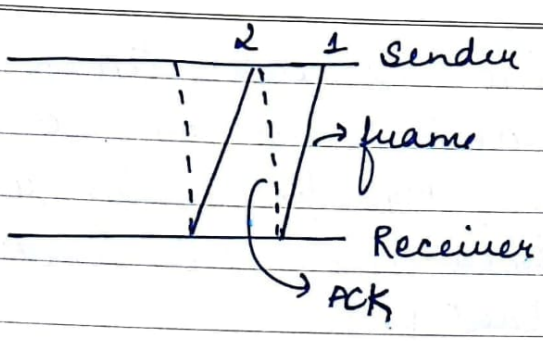
STOP & WAIT PROTOCOL:

- If the data frames arrive at receiver side faster than they can be processed then the frame must be stored until they can used.
- Normally, the receiver does not have enough storage space.
- If it is receiving data from many sources, this may result either discarding of frames or bottleneck situation.
- To prevent from this situation, sender needs to slow down.
- There must be feedback from ~~sender~~ receiver to sender known as acknowledgement (ACK)
- In that protocol sender sends one frame & stops until it receives confirmation from receiver.



Shipra

Date



NOISY CHANNEL:

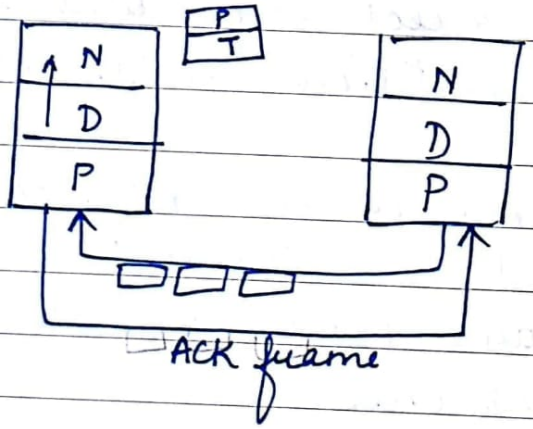
(Also known as sliding window Protocol)

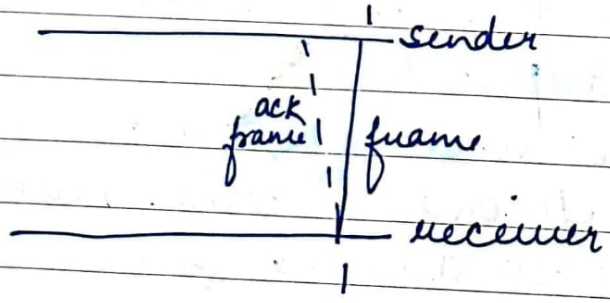
1) STOP & WAIT ARQ (Automatic repeat Request)

- In this we add a simple error control mechanism.
- To detect & correct corrupted frame we need to add repeatition bits to our data frames.
- When the frame arrive at receiver side, it is checked & discarded if corrupted.
- Lost frames are more difficult to handle than corrupted ones.
- The received frame could be in correct order or duplicate form.
- When the received, receive a data frames i.e out of order this means frame was either lost or duplicated.
- The corrupted & lost frame needs to be resend in this protocol.
- In this protocol, the sender keeps a copy of the send frame.

Shipra

- At the same time it uses timer. If the timer expires and there is no ACK for the sent frame, the frame is resent. The copy is held by the sender & the timer is restarted.
- Since, ACK frame can be corrupted & lost so it also needs repetition bits and sequence number, this protocol handles all these kinds of situations.





2) GO-BACK N ARQ:

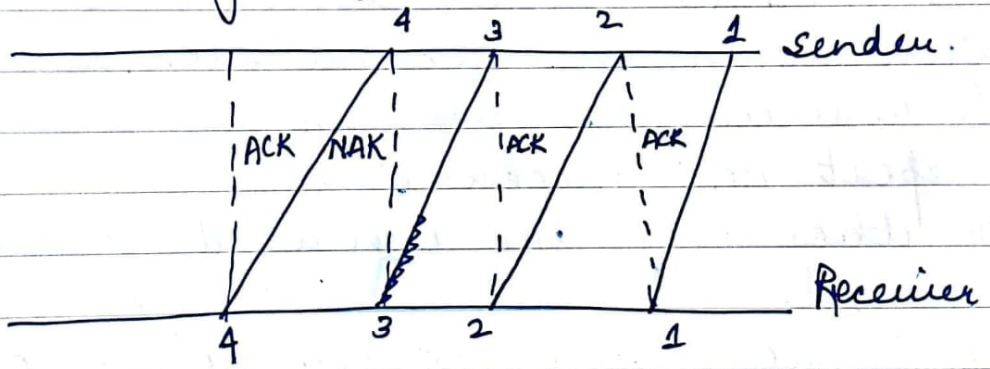
- To improve efficiency of transmission

Date

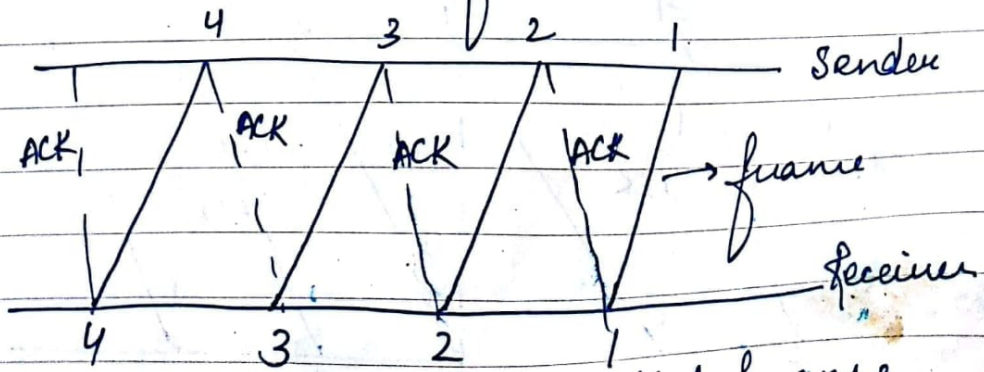
multiple frames must be in transmission line while waiting for ACK.

- In this protocol, we can send several frame before receiving ACK.
- We keep copy of these frames until ACK arrives.

→ Sequence no.
→ Timer
→ ACK ← negative +ve.
→ Resending a frame



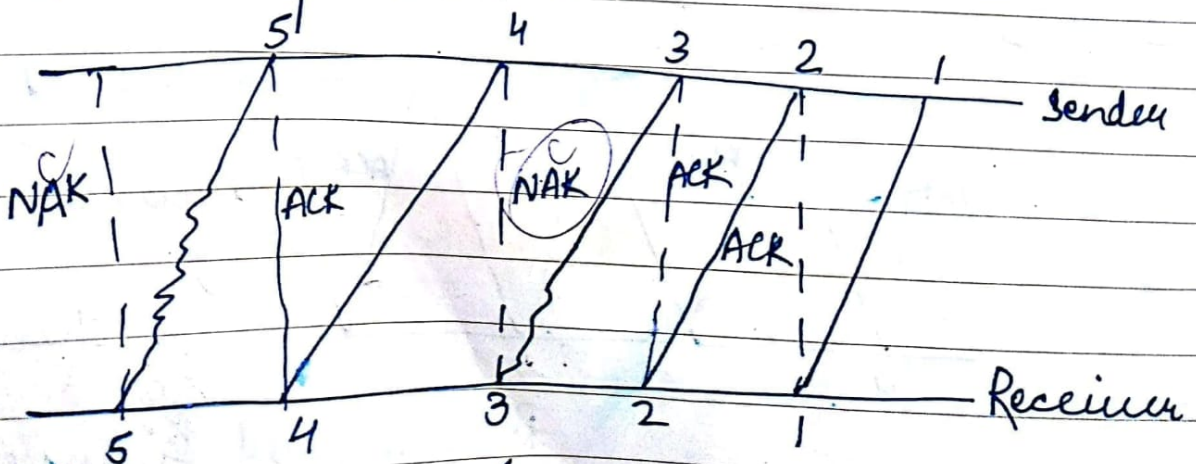
Now, it is retransmitted from the 3rd frame.



Retransmitted frame.

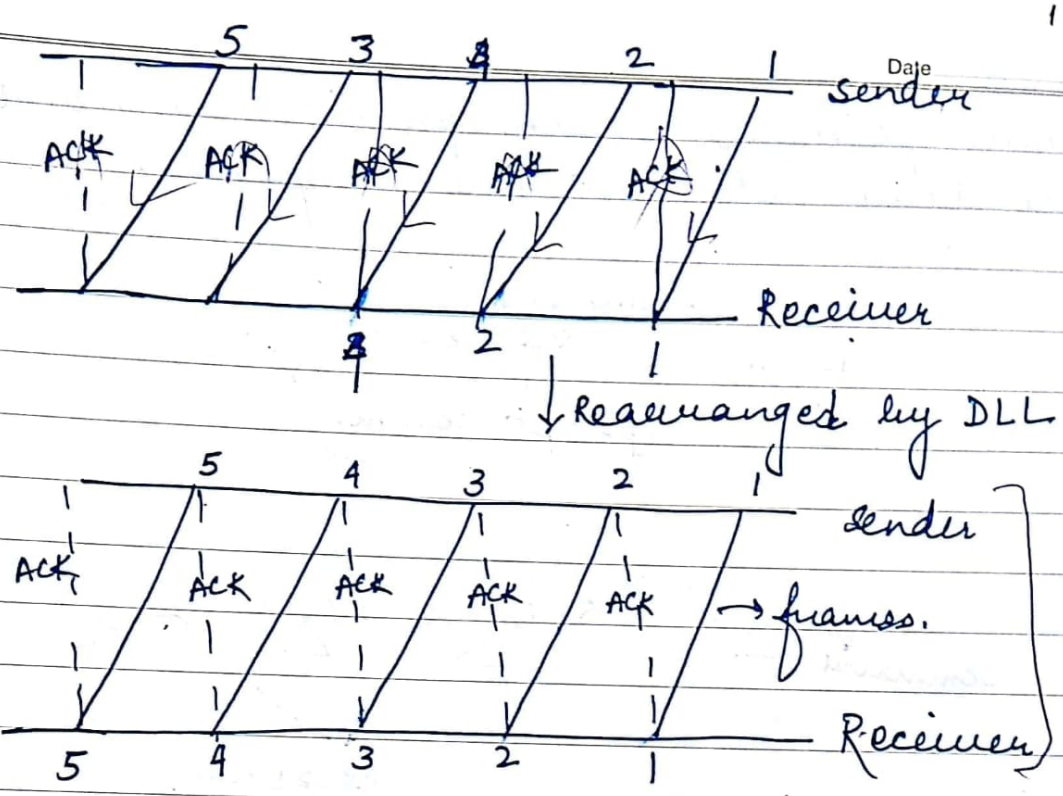
3) Selective Repeat: ARQ

- In this, the receiver keeps track of only one variable.
- There is no need to buffer out of order frame they are simply discarded.
- That is why, go-back N ARQ is very inefficient for noisy link.
- In of noisy transmission, a frame has max^m no: of chances to get damage or corrupted which means resending of multiframes which uses Bandwidth & slow down the transmission.
- To resolve this problem we use selective repeat ARQ mechanism.
- In this only the damaged frame is resend.
- It is more efficient for noisy comm.
- But the processing at the receiver is more complex.



Only 3 & 5 frames are resent

Shipra



I HDLC : (High level data link Control)

This frame is bit oriented protocol. It is used for point-to-point communication & multi pt. communication.

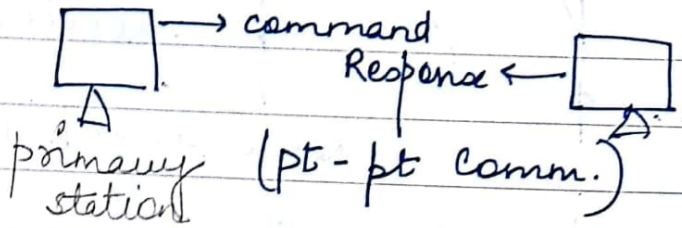
HDLC - configuration :

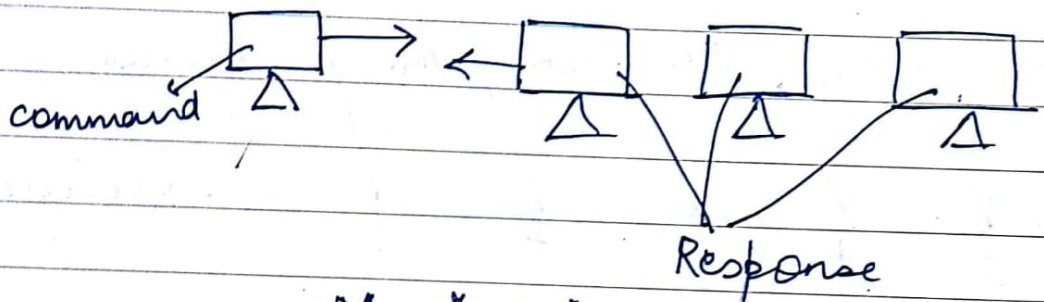
It is of 2 types —

1) NRM called Normal Mode
2) ABM called Asynchronous Mode

→ In normal mode, communication goes to take place pt-pt & multipoint.

where primary station provides command & secondary station give response.

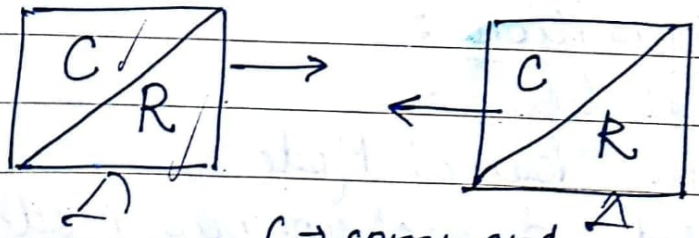




MULTI-POINT

2) ABM

It is used for pt-pt communication. where primary station & secondary station do the same job.



C → command
R → response

Date

Frame format:

In HDLC we follow 3 types of frame formats -

i) INFORMATION FRAME (i-frame)
ii) SUPERVISORY FRAME (s-frame)
iii) UNNUMBER FRAME (u-frame)

i-frame:

It contains user control information.

s-frame:

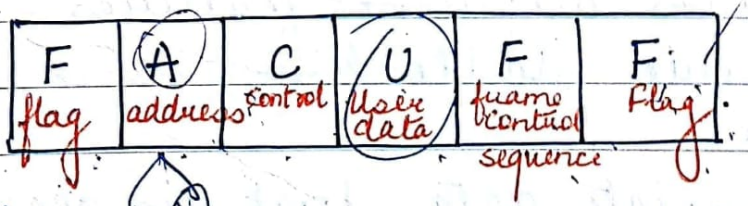
It gives command to user data.

u-frame:

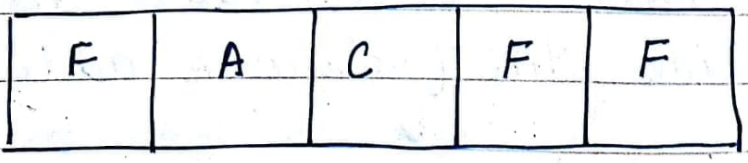
It is used to manage system.

FACKUFF

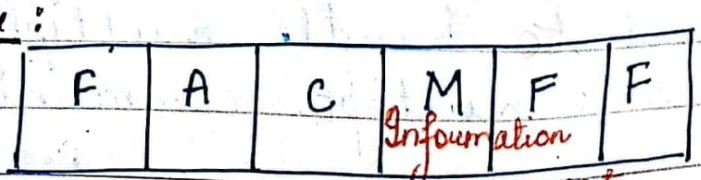
I-frame:



s-frame:



u-frame:



Shipra

Flag: We use 8-bit sequence, starting from 01111110 ~~00000000~~

* Address: ~~In this size can be 1-1500 byte and 1 byte can handle 128 stations. Byte Size can be increased by negotiation.~~

Control: It is used for error & flow control.

FCS (frame control sequence): It is used for error detection.

It takes 2 or 4 bytes

II PPP (Point to Point Protocol) (Byte oriented)

- The internet needs a point to point protocol for different purposes, including router-to-router communication & home user to ISP traffic.

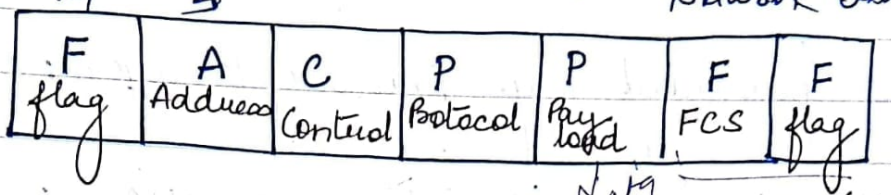
PPP provides different features –

- It provide multi-link communication b/w frames.
- It encapsulate data that is received from Network layer to DLL.
- Frame format handles error detection.
- It provide NAC (network address control).

* It is used to handle multiple terminals for pt-pt & multipt. communication.

Date

Frame Format:



(1 byte = 8 bits)

Flag:
PPP frame start with HDLC flag byte & its sequence will be 01111110!

Address:
In this default value is constant. PPP does not provide reliable transmission using sequence number & ACK.

Control:
PPP does not provide any error or flow control.
It believes that transmission is error-free.

Protocol:
It defines which data type is used. If there is only one byte to transmit the ending bit will be zero. If more than 1 byte or large amount of bytes then ending bit will be 1.

Payload:
In this size can be 1-1500 byte and 1 byte can handle 128 stations.
Byte size can be increased by negotiation.

FCS: used for error detection.

Shipra

Date

TCP

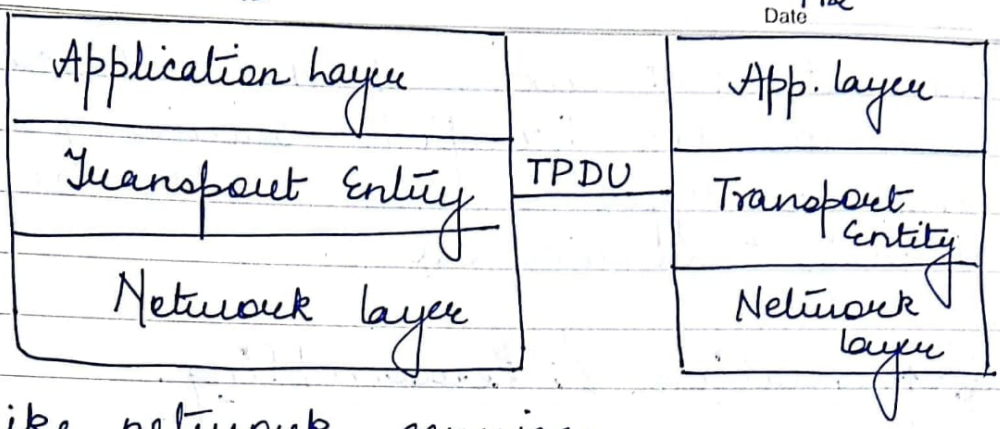
Transport Control Protocol:

Services provided by Transport layer:
or
Explain the Transport Services:

- Services provided to the upper layer
- Transport service primitives.
- Berkeley socket
- Reliable connection
- Multiplexing & demultiplexing
- Addressing
- Error control & flow control
- Segmentation & Reassembling

1. **Service provided to the upper layer:**
   - → The ultimate goal of the TL is to provide efficient, reliable & cost effective services to its users.
   - → The H/W & S/W within the transport layer that does the work is called the transport entity.
   - → The transport entity can be located in the O.S kernel.
   - → In a separate user process or on the network interface card (NIC).
   - → In TP there is a relationship b/w app, network & Transport Layer.

Shipra



As like network services, There are 2 types of transport services—

1. Connection oriented Transport Services
2. Connectionless oriented

In Transport service connection have 3 phases —

i) Establishment
2) Data - Transfer
3) Release

→ Transport layer works similar as Network layer but it has some advantages over network layer.
→ TL services are more reliable compared to network layer.
→ Lost packet & duplicate packets can be handled by TL.
→ TL hides the network address from other users.

- The bottom 4 layers of the OSI can be seen as the Transport Service provider, and the upper 3 layers can be seen as the transport Service user.

2) Segmentation & Reassembling:

- A message is divided into segments by the transport layer, with each segment given a sequence no. These sequence no. enable the destination TL to reassemble the segment in exact order as they were sent by the sender.

3) Addressing:

- As many processes may be running on the communicating host at the same time, it is necessary to Identify the required process out of many processes.
- For this TL header must include a code address in each segment.

4) ~~Error~~ Flow Control:

The TL is responsible for controlling the

Date

flow of data such that no sending process should send segments at a rate faster than the receiving process.
- It provides end to end flow control.

5) Error Control:
- The transport layer, functions in such a way that the receiving process not only detect the error but also define the location of error.
- It provide process-to-process error control.

6. Transport service primitives:

Primitive	Packet Sent	Meaning
1) Listen	0	Block until some process try to connect
2) Connect	Connection Reqd.	Establish a connection
3) Send	Data	send information
4) Receive	Data	Receive information
5) Disconnect	Disconnection request	one of the side wishes to release connection

Shipra

Date

Primitives	Meaning
• socket	Create a new column end point
• listen	Announce willingness to accept connection.
• Accept	Block other calls until a connection attempts to arrive
• Connect	Establish a connection
• Send	Send information
• Receive	Receive "
• Close / Disconnect	Release connection

3 way or 2 way hand shaking

Elements of Transport Protocol:

We have 5 type of elements for transport protocol.

- Addressing
- Connection Establishment
- Connection Release
- Flow Control & Buffering
- Multiplexing
- Crash Recovery

Date

ADDRESSING:

- When an app. process wishes to set up a connection to a remote app. process it must be specified which one to connect.
- The method to define transport address is ports.
- We also use TSAP (transport service access point).
- Addressing is used to define unique payload.

ESTABLISH A CONNECTION:

- One transport entity it sends a request to the destination & wait for a connection accepted reply.
- The problem can occur when the connection crash or lost the packets, During the transmission of acceptance reply.
- The problem can happen in different ways.

→ Using thrown away transfer addresses - Each time a transport address is req'd. & a new one is generated, when a connection is released the address is discard & never used again.

Shipra

Date

→ Give each connection a connection identifier. After each connection is released, each transport entity could update a table listing obsolete connections. Whenever a connection request comes in, it could be checked against the table to see if it belong to a previous release connection.

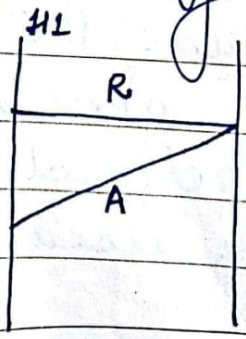
→ Rather than, allow packets to live forever within the subnet —

- There is a mechanism to delete old package those are not usable for long time.
- Packet lifetime is based on following techniques —

- Restricted sub-net design
- timestamping each packet

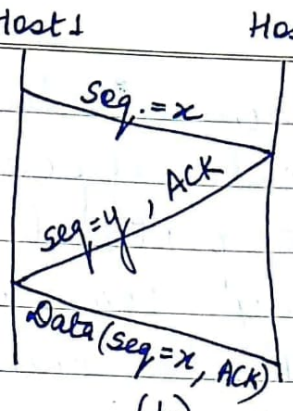
In connection establishment, we follow a kind of technique —

1) 2 way handshaking
2) 3 way handshaking



R → Request
A → acceptance

Date



ACK - acknowledge

(b) 3-way

CONNECTION RELEASE:

There are two types —
- Symmetric
- Asymmetric

& FLOW CONTROL & BUFFERING:

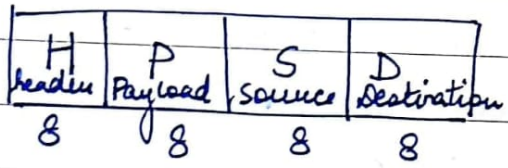
- Flow control problem in TL is same as in DLL.
- But in some ways it is different.
- The main difference is a router has relatively few lines & a host may be connected by different connections.

INTERNET TRANSPORT PROTOCOL:

2 types —
- UDP
- TCP

UDP: (wireless communication)

- The internet protocol support a connectionless transport protocol
- UDP provides a way for applications to send encapsulated IP datagrams & without establishing a connection.
- UDP transmits segments consisting of a 8 byte header followed by payload.
- used source and destination codes.



32 bytes

Source Code:

- It is required when a reply must be sent back to the source. Reply can be acknowledgement.

Destination code:

- It is needed to have the address of the receiver.

Source	Destination
UDP length	Checksom

32 bytes

Date

UDP length:
Its length field includes 8 byte header & 8 byte payload.

Checksum: is optional and not computed.

- UDP doesn't provide any flow control, error control or retransmission policy.
- It is all upto the user to handle the contents.
- UDP is specially useful in client server communication.

When a client sends a short request to the server & expect for a reply; if reply is lost, the client can just time out & try again.

UDP is of two types:

1) RPC (Remote procedure control)
2) RTP (Real time Transport Protocol)

RPC:
When a process on machine 1 calls a procedure on machine 2, Calling process on 1 is suspend & execution of the called procedure takes place on 2.

Date

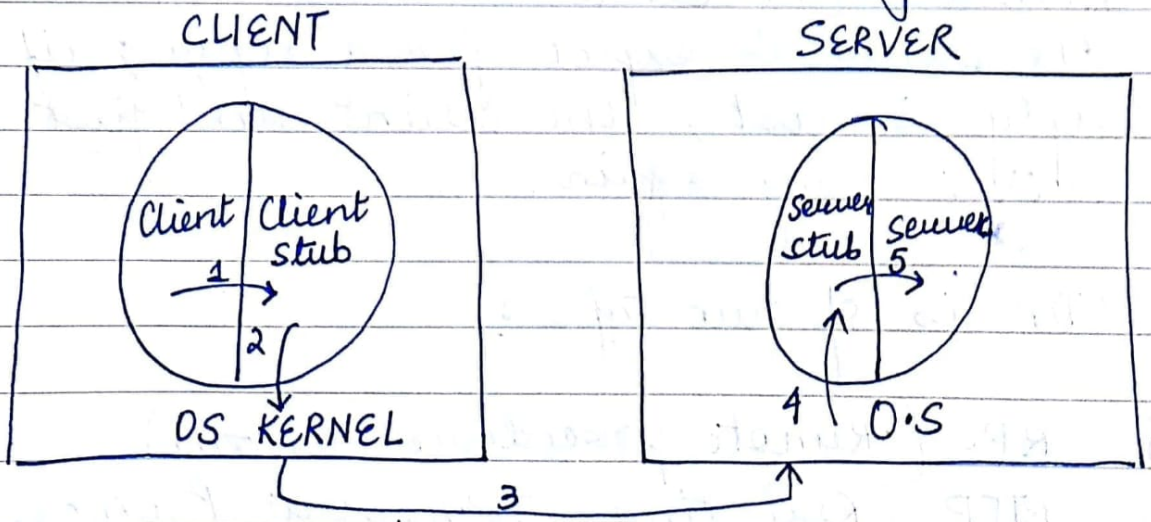
- No msg passing is visible to programmer. This technique is called RPP & used for networking app.

STUB:

It is a piece of code used for converting parameters passed during RPC.

Marshalling:

- Packing the parameters passed by client to stub is called marshalling.



RPC Steps:

Step 1: is the client calling the client stub. This call is a local procedure call with the parameters pushed onto the stack in a normal way.

Shipra

Date

2) Step II : is client stub packing the parameters into a message & making a system call to send the msg. Packing the parameter is called Marshalling.

3) Step III : is Kernel sending the msg from the client machine to the Server machine

4) Step IV: Kernel passing the incoming packets to the server stub.

5) Step V : In this server stub calling the server procedure with unmarshalling parameters. The reply follows the same path in other direction.

Problems with RPC :

1) With RPC, passing pointer is impossible bcoz the client and server are in different address areas.

2) It is perfectly legal to write a procedure that computes the inner product of 2 vectors/array without specifying how large each one is.

Shipra

Date

Each could be terminated by a special value by the sender on the receiver.
Under these circumstances, it is impossible for the client stub to marshall the parameters.

- 3rd problem is relevant to type of parameter does not specify the value. Ex) printf (each parameter is not defined like char, int)
- It is related to the use of global variables.
  If the called procedure moved to a remote machine the code will fail because global variables are no longer shared.

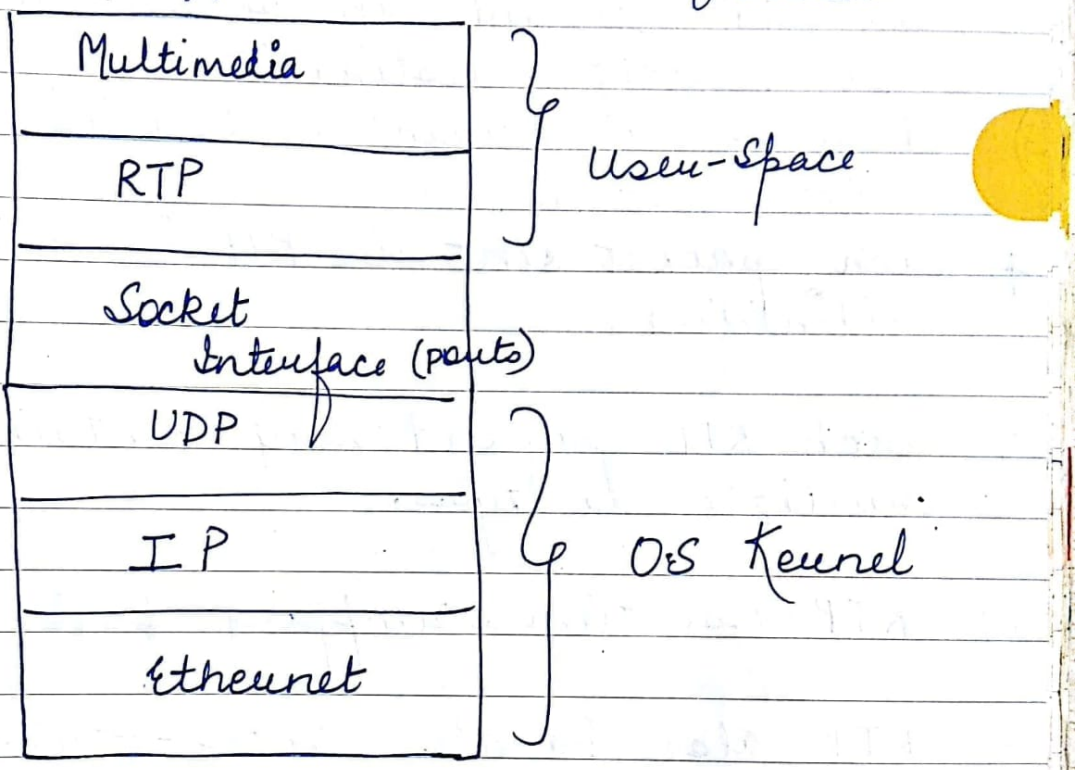
Real time Transport Protocol (RTTP):

- Real time multimedia application is like Internet radio, music on demand, video conferencing etc. use RTTP.
- The Position of RTP in the protocol stack is different.
- The multimedia app. consists of multiple audio-video texts & possibly other streams.

Shipra

Date

- RTP & multimedia app used in user space. These are fed into RTP library & this library then multiplex the stream & encode them into RTP packets & then stuff it into a ~~software~~ socket.



At the other end of the socket, UDP packages are generated & embedded ~~in~~ in IP packets.

If the computer is ON & ETHENET then the IP packets are put into ethernet frames for transmission.

Shipra

Functions of RTTP:

1) The basic function is to multiplex several real time data streams onto a single stream of UDP packets
2) The UDP stream can be sent to a single or multiple destination.
3) There is no guarantee of delivery or jitter control.
4) Each packet sent in RTP is uniquely identified.
5) Each RTP payload may contain multiple daldtypes.
6) RTP use time stamping features.
7) RTP also handles inter-stream synchronisation.

TCP:

- INTRODUCTION to TCP
- TCP Service Model
- TCP Protocols
- TCP Segment header

- TCP connectionment establishment
- TCP connection Release
- TCP connection management
- TCP Transmission policy
- TCP congestion contud
- TCP timer management
- Wireless TCP & UDP
- Transactional TCP

INTRODUCTION TO TCP:

- TCP was designed to provide a reliable end to end byte stream over unreliable network.
- An inter-network can be different from a signal network because different geographical location has different topologies - bandwidth, delay, packet-size & other parameters.
- TCP was designed to dynamically adapt 2 properties of the inter-network.
- Each machine supports TCP & it has a TCP Transport entity; either a library procedure, user process or a part of Kernel (O.S).
- A TCP entity accepts packet from local process & break them up into pieces not exceeding 64 KB & sends

Date

each packet as a separate IP datagram.

- When datagram arrives at a machine they are given to TCP entity which reconstruct the ~~TCP~~ original byte stream.

TCP SERVICE ~~PROVIDER~~ MODEL:

TCP service is obtained by both the sender and receiver making end points which are called sockets. Each socket has a socket number consisting of IP addresses of the host & 16 bit no local to that host which is called port.

- A socket may be used for multiple connections at a same time or 2 or more connections may terminate at a same socket.
- Connections are identified by socket identifiers like socket 1, socket 2, ...

Contd...

Date

- All TCP connections are full duplex and point to point.
- TCP does not support multi-tasking & broadcasting.
- TCP connection is a ~~xxxx~~ byte stream not a message stream.
- When an application transmit data to TCP, it may send immediately or buffer it.
- To transmit content immediately application may use PUSH FLAG which tells TCP not to delay the transmission.

PORT	PROTOCOL	USE
• 21	FTP	file transfer Protocol
• 23	TELNET	Team Viewer (Remote Login)
• 25	SMTP	Simple mail Transport Protocol for e-mail.
• 80	http	world wide web
• 110	POP3	Remote e-mail access

Shipra

TCP Protocol :

- In that every byte on a TCP connection has its own 32 bit sequence number, & separate 32 bit sequence number are used for acknowledgement.
- The sending & receiving TCP entities exchange data in fourth of segments.
- The TCP segments consisting of fixed 20 byte header part.
- The segment size including the TCP header must fit in the 65515 by IP payload.
- Each network has maximum transfer units called as MTU & each segment fit into the MTU.
- The basic protocol used by TCP entity entity is sliding window protocol.
- When a sender transmit a segment it also & starts a timer.
- When the segment arrive at destination, the receiving TCP entity sends back a segment which contain ACK number against the received packet.
- If the sender timer goes off before the ACK is received, the sender

Date

transmits the segments again.

** TCP Segment header:

Every segment in TCP starts with a fixed format which is 20 byte header part.
The fixed header may be followed by header option.
After removing the 20 bytes payload used 65495 data bytes.

(Source-point) S	(Destination) D
Sequence No.	
ACK	
TCP header length	Window Size
Checksum	Urgent Pointer
Options	
Data	

Diag. of TCP.

a) ACK: The ack bit is set to 1 to indicate that acknowledgement no. is valid. If ACK is 0 the segment does not contain an acknowledgement i.e no transmission takes place.

b) Source, Destination Port :- They identify the local end pts. of the connection. The source and destination pts. together identify the connection.

c) Sequence no. : It performs the usual function. It defines the expected next byte. Both ACK & seq. no. are 32 bit long.

d) TCP header length : It defines the size of header.

e) Window size: defines the total segment size.

f) Urgent pointer : If URG set to 1, It means urgent pointer is in use.

g) Checksum : For error detection.

h) PSH bit : It indicates push data. The receiver request to the transmission channel not to buffer data until it has been received.

i) RBE : Reset BIT is used to reset a connection that becomes confused due to host crash or some other reason.

Date

It is also used to reject invalid segments.

j) SYN : It is used to establish a connection.
If SYN = 1 & ACK = 0 (connection established but no transmission)
SYN = 1 & ACK = 1 (connec. establishment, data trans)
SYN = 0 & ACK = 0 (no connection establishment)

k) FIN : final / finish but . It is used to release a connection.
It specifies that sender has no more data to transmit. Both SYN & FIN segments follow sequence no. in a correct order.

l) Option : This field provides a way to add extra features not covered by regular header / segment.

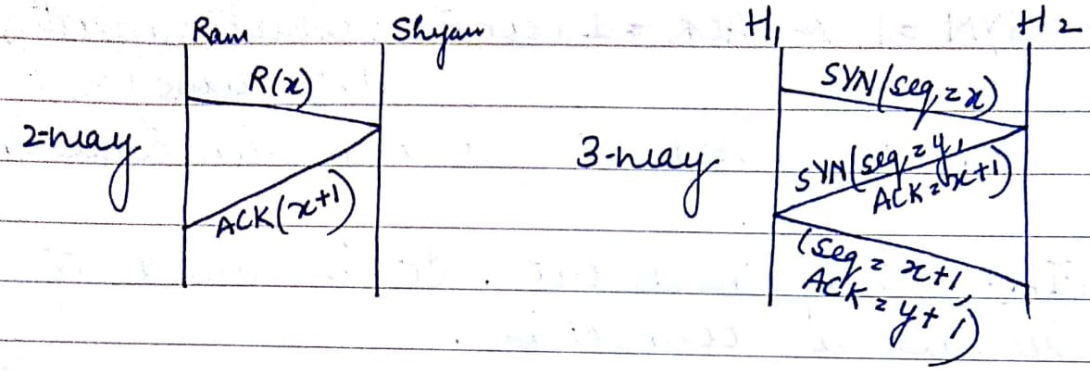
3. TCP Connection Establishment :

- Connections are established in TCP by using 2 way handshaking or 3 way handshaking.
- To establish a connection one side say the server passively wait for incoming connection by executing the listen &

Date

accept primitives.

- The other side, say the client execute a connect primitives specifying the IP address & port to which it wants to connect.



(4) TCP Connection Release:

TCP connections are full duplex. To release a connection we can also use simplex technique. TCP can release the connection by sending FIN bit. An ACK bit is removed in other direction. If a response to FIN is nt coming time out system will work there is specific applications to release the connections.

(5) TCP connection management Model -

(1) CLOSED — no connection is active
(2) LISTEN — the server is waiting for incoming call.

Shipra Shipra

Date

(3) SYN Receive	connection request has arrived.
(4) SYN SEND	application has started to open connection
(5) Establish	Data Transfer
(6) FIN wait 1	client sends 'it is finished'.
(7) FIN wait 2	other side agrees to release.
(8) Timed wait	wait for all packets to die.
(9) Closing	Both side try to close at the same time.
(10) Close wait	Other side has initiated a release.
(11) Last ACK	wait for all packets to die

(6) TCP congestion Control:

- In internet, network layer tries to manage congestion, But most of the congestion is handled by TCP. The real soln to congestion is to slow down the data rate.
- The idea of congestion control is like that, control the injecting a new packet into the network until old one leaves.
- In TCP, to control the connection when a connection is established, a suitable window size needs to be choosen.
- The receiver can specify a window size based on its buffer size because overflow creates congestion.

Supra

Date

- There are 2 sides of congestion problems —
  (a) network capacity
  (b) Receiver capacity
- To handle this situation, ISP provider and receiver used ACK frames on feedback system

(Diag. From book)

Transactional TCP - (RPC)

The normal sequence of packets for doing RPC over TCP follows 9 packets.

1. The client sends a SYN packet to establish a connection.
2. The server sends an ACK packet to ACK SYN packets.
3. The client completes the 2 way or 3 way handshaking.
4. The client sends or receive the contents / data packets.
5. The client sends a FIN packet.
6. The server acknowledge the request & the FIN.
7. The server sends the reply back to the client.
8. The server sends a FIN packet
9. The client sends last ACK to the server's fin.

Date

DNS :

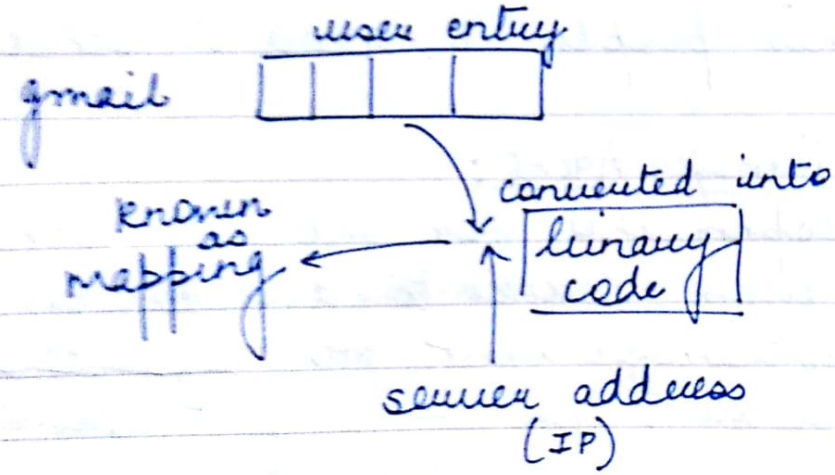
Domain name System:

When thousands of PC were connected to the net, they need unique IP.

IP addresses can conflict, nobody can remember millions of thousands of IP addresses.

To solve these problems DNS was invented.

- It was used to map a name onto an IP address;
- And application programs calls a library procedure called the resolver passing it the name as a parameter.



- com for commercialisation
- edu education
- au country
- in India

Email :

Email use FTP (file transfer Protocol) with the convention that the first line of each msg contained the receiver address.

- Sending email
- Reading e-mail
- Receiving email

Architecture & Services :

Email system is based on the 2 sub-systems -

1) User agent :
   It allows people to read & send email.
2) Message Transfer Agent :
   It is responsible for moving the msgs from source to destination.

- The msg transfer agent run in the background but the user agent services works on the user's space.

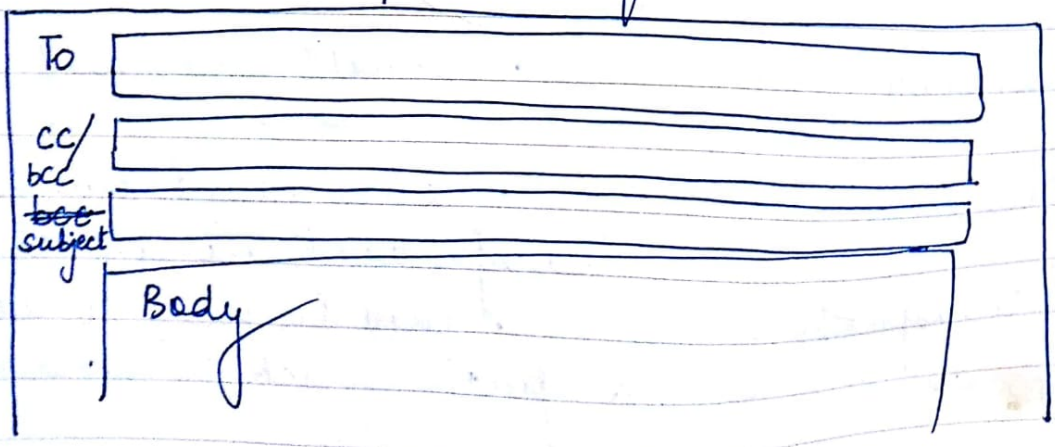
Services :

Critically email system support 5 basic functions -

Date

- **Composition:**
  It refers to process of creating messages & answers.
- **Transfer:**
  It refers to moving msgs from source to destination.
  In this part we need to establish a connection to the destination by using intermediate machines.
- **Reporting:**
  It gives ~~at~~ information about msg are delivered or not.
- **Display:**
  Incoming msg is reqd. to be displayed in such a manner so that people can read their unread emails.
- **Writing:**

Draw-pattern of email



Shipra

email formats :

There are 3 types—

1) RFC 822
2) ~~A22~~
3) MIME (multi purpose internet mail extension)
4) SMTP (simple mail transfer protocol)

RFC 822 :

Header	Meaning
1) To	• Receiver (primary)
2) CC	• secondary receiver
3) bCC	• Blank carbon copy
4) From	• who create a msg.
5) Sender	• e-mail address of actual sender
6) Received	• Line added by each transfer agent along with the route
7) Return path	• can be used to identify a path back to sender.

Date

MIME:

Mime use RFC822 format but have some additional features & protocols to make the mail system more reliable.

formats to define encoding rules for non-ASCII msgs

Date

SMTP :

- It is a simple mail Transfer Protocol.
- Within the internet, email is delivered by having the source machine established a TCP connection to port 25 of destination machine.
- Listening to this port is called SMTP.
- This protocol accept incoming connections & copies msgs from them into the mail boxes.
- If a msg cannot be delivered a error report is transmitted to the sender.
- SMTP is a simple ASCII protocol.
- After establishing the TCP connection to port 25 the O.S sending machine works as a client.
- Wait for the receiving machine to reply back; if it is not replying the client release the connection & tries again later.

World-Wide-Web — Do Yourself

Multiple Access Protocols

Date

Module-3

Channel Allocation Problems:

We have two types of allocation techniques -

1) Static
2) Dynamic

Static:

- In tiaditional way, allocating a single channel we use FDM technique.
- If there are n users the bandwidth is divided into n-equal sized portions. FDM is very simple & efficient allocation mechanism
- But if users are more than the n participations FDM is not able to handle this situation.
- If the spectrum is divided into n parts & user are less than n, the spectrum will be wasted.
- If more than n users wants to communicate, some of them will be denied permission due to lack of bandwidth.
- To handle this problem we follow 2 techniques
  → Dynamic Channel Allocation -
  ⇕
  → Static channel Allocation

Shipra

Dynamic channel Allocation :
in LAN & MAN

- In dynamic, we follow five techniques —

→ Station model

- The model consists of n independent stations
- Each station generate frames for transmission.
- Stations are sometimes called terminals.
- Once a frame has been generated, the station is blocked until the frame has been transmitted successfully.

→ Single channel Assumption

- A single channel is available for all communication.
- All stations can transmit on it & receive on it.
- As per concern of H/W, all stations are equal. They may use different protocol.

→ Collision Assumption

If 2 frames are transmitted at the same time, they will create collision.
All station can detect collision & collided frames must be transmitted again.

Date

→ Continuous time

a) Frame transmission can start at any time. There is no master clock dividing time into discrete intervals.

b) SLOTTED TIME: Frame transmission start at specific time. There is a master clock dividing time into discrete intervals.
A slot may contain 0, 1 or more frames.

→ a) Carrier Sense
Station can tell if the channel is in use before trying to use it.
If the channel is busy, it has to wait untill the channel is idle again.

b) No Carrier Sense
Station cannot sense the channel before using it & go ahead.
This leads to more collisions.

Multiple-Access Protocols:

ALOHA:

- It resolves the problem of channel allocation problem.
- We will discuss two versions of ALOHA.

Date

1) Pure Aloha
2) Slotted Aloha

Pure Aloha does not require global time synchronisation but slotted requires it.
In Slotted Aloha, time is divided into discrete slots in which all frames must be fit.

Pure Aloha:

- The basic idea of aloha system is simple.
- Let users transmit whenever they have data to be sent, there will be collisions & colliding frames would be damaged.
- Due to feedback property, station will listen the channel.
  With a LAN, the feedback is immediate & with a satellite there is a delay of 270 msec before the sender knows if the transmission is successful or not.
- If the frame was destroyed the sender just wait a random amount time & sends it again.
- System in which multiple users share a common channel that can lead to conflict and is known as contention System.
- Whenever 2 frames try to occupy the channel at the same time, there will be collision.

Shipra

Date

- If the 1st bit of new frame overlaps with the last bit of a last frame, both frames would be totally destroyed & both frames will have to be retransmitted later.
- A user is always in 2 states :-
  - → typing
  - → waiting
- Initially all user are in typing state. When a line is finished, the user stop typing & wait for response.
- The station then transmit a frame containing the user lines & checks the channel, if it was successful ; if not the user retransmit frame at a random amount of time untill it has been successfully sent.

Imp.

Let the (frame time) define the amount of time required to transmit fixed length frame.
We assume that infinite no: of users generate new frame with mean N and frames per frame time.
If N>1, the user generally frames at a higher rate then channel can handle that. In that case, every frame will suffer a collision. For best o/p we can expect
0<N<1

Shipra

Date

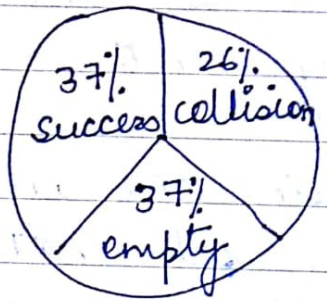
- Pure Aloha Output,

$$S = Ge^{-2G}$$

Slotted Aloha:

Efficiency, $S = Ge^{-G}$

In this, we divide time into discrete intervel. Each interval corresponding to one frame.
In a slotted aloha when $G = 1$, the o/p will be twice better that Pure Aloha.
If system is operating based on slotted aloha at $G = 1$, the probability of empty slot is 0.036.



The best we can hope for using slotted aloha is 37% of slot is empty, 26% collision & 37% of success.
Operating at higher value of G reduce the no: of empty slot but increase the no: of collisions.

Date

CSMA:

Carrier Sense Multiple Access Protocol

- With slotted ALOHA, the best channel utilisation can be achieved by 1/e.
- In slotted ALOHA, when other station start transmitting frame without paying attention to what the other station are doing they are bound to no: of collissions.
- Protocols in which station can listen for a transmission & act accoudingly are called carrier sense Protocol.
- We have 3 kinds of techniques for
  → CSMA
    ↳ Persistent & Non-Persistent CSM
    ↳ p-persistent
    ↳ 1- persistent

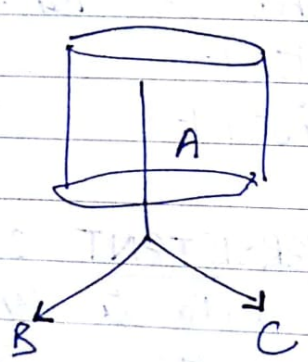
PERSISTENT & NON-PERSISTENT CSM:

- When a station has data to send, it first listen to the channel to see if anyone else is transmitting at the moment.
- If the channel is busy, the station waits untill it become idle.
- When the station detect an idle channel, it transmit a frame.

Shipra

Date

- If a collision occurs, the station waits a random amount of time & starts all over again.
- This protocol is also called 1-persistent.
- The propagation delay has an important effect on the performance of protocol.
- There is small chance that just after a station begins sending another station will become ready to send & sense the channel idle.
- It will result in collision.
- If the propagation delay is zero, there can be also a collision, if 2 stations become ready 1 is propagating the 2 will collide when channel becomes idle.



NON-PERSISTENT:

- In this protocol, a station sense the channel before transmitting the frames.

Date

- If no one else is sending, the station starts transmitting frame but if the channel is already in use, the station does not sense it negatively & waits for random amount of time.
- This leads to the better channel utilisation but longer delay than persistent CSMA.

p- PERSISTENT :

- The p-persistent method is used on slotted channels.
- When a station becomes ready to send, it sense the channel.
- If it is idle, it transmit the frame with probability of p; with prob. of q it waits until last frame is transmitted.

$$q = 1 - p$$

→ CSMA with Collision Detection : (CD)

- Persistent & non-persistent CSMA protocols are better than ALOHA protocol.
- But in case of transmission of two frames in the time, collision will be already there in persistent & non-persistent protocol.

Shipra

Date

- To resolve this problem we use CD technique.

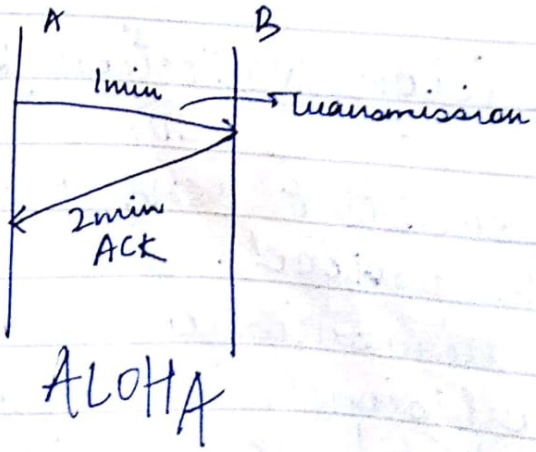
Procedure:

- CSMA/CD is similar to one of the feature of ALOHA protocol but there are no! of differences.

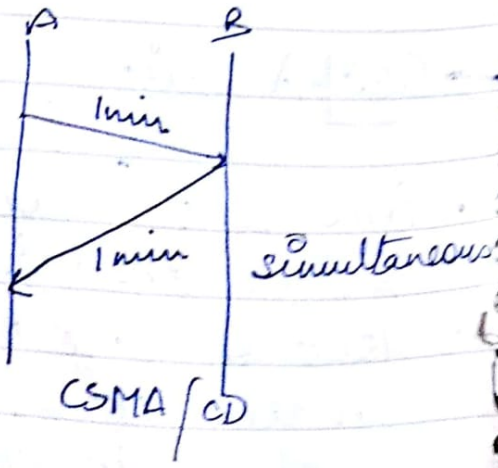
→ In CSMA/CD we need to sense the channel before sending the frame but in ALOHA, it does not sense the channel & just transmits the frame.

→ In ALOHA, we first transmit the entire frame & then wait for an acknowledgement but in CSMA/CD, transmission & collision ~~In ALOHA~~ detection is a parallel process.

→ We don't need to send the entire frame & then look for a collision.
We constantly monitor 2 condition — either transmision is successfully done or a collision is detected.



ALOHA



CSMA/CD

Date

Energy level:

We have 3 types of energy levels —

- zero
- Normal
- Abnormal

- At the zero level, channel is idle.
- At normal level, a station has successfully captured the channel & transmits its frame
- At the abnormal level, there is a collision as multiple stations try to access the channel.

OUTPUT:

In CSMA/CD output is greater than Pure aloha as well as slotted ALOHA.,
for 1-persistent method, the max^m % is 50 when $G=1$.
for non-persistent, the O/P can go upto 90% when $G = 3$ to 8.

CARRIER | CSMA/CA

~~The basic idea~~ In a wire oriented network, the received signal is of almost the same energy as the sent signal as

Shipra

Date

there are no. of repeater that amplify the energy b/w sender & receiver.
But in wireless network sent energy is lost in transmission.
The received signal has very less energy. This is not useful for effective collision detection.
To avoid collision on a wireless network we use collision avoidance technique which is called CSMA/CA.
We have 3 type of techniques —

a) Contention Window

b) Acknowledgement

c) Inter-frame Space (IFS)

IFS:

- Collisions are avoided by rejecting transmission even if the channel is found idle.
- An idle channel is found, the station does not send immediately.
- It waits for a period of time which is called IFS.
- In CSMA/CA the IFS can also be used to define the priority of a station.

Date

CONTENTION WINDOW:

- It is an amount of time divided into slots.
- A station can choose any random no: of slots.

The no: of slots in the window change according to the no: of stations.
The station needs to sense the channel after each time slot.
If the station find the channel busy it just stop the timer & restart it when the channel is sensed as idle.

ACKNOWLEDGEMENT:

The +ve ACK & -ve ACK & timer system gives assurity about the successful transmission.

WIRELESS LAN:

IEEE 802.11: IEEE has defined the specification for wireless lan which is called IEEE 802.11 which covers pjsical & DLL.

Architecture:

- 802.11 defines 2 kinds of services -
  - → BSS (Basic service set)
  - → ESS (Extented service set)

Shipra

Date

BSS:

- IEEE 802.11 defines the basic service set as the building block of a wireless lan.
- It is made of mobile wireless stations and central base station which is known as access point.
- The BSS without an AP is a stand alone network & cannot send data to other BSS.
- It is called as adhoc architecture. In this architecture, stations can not form a network without the need of an AP.
- They can search one another station & create unreliable BSS.

ESS:

An extended service set is made up of 2 or more BSS with AP's. In this case BSS are connected by a central server which is usually wire-oriented LAN. When bss are connected the stations within the reach of one another can communicate without the use of AP.

Station types:

IEEE 802.11 defines 3 types of stations based on their mobility in a wireless LAN.

1) No transition
2) BSS transition
3) ESS transition

- A station with no transition moves only inside a BSS.
- A station with BSS transition mobility can move from 1 BSS to another BSS but the movement is confined inside a 1 ESS.
- A station with ESS transition can move from one ESS to another ESS.

802.11 Protocol Stamp: (Architecture)

The protocol used by 802 variants ~~eg~~ including ethernet have some common infrastructure facilities.

N D P { LLC, MAC

In 802 protocol we split the data link layer b/w 2 sublayer — MAC & LLC.
(logical link control)

MAC sublayer define how the channel is allocated & it defines who will get the channel next.

Shipra

Date

- LLC sublayer's job is to hide the difference b/w different 802 variants.

Physical Layer:

In Physical layer, we define 3 different transmission techniques.

1) The infrared method : used the technology as television remote control can do. Infrared technology used for short distance communication.

The other 2 techniques are —

1) FHSS - which is called frequency hoping spread spectrum.

2) DSSS called direct sequence spread spectrum.

All 3 technologies does not require licensing but these techniques can operate at maximum 1 or 2 mbps speed.

In 1999, 2 ~~tec~~ new techniques were introduced to achieve higher bandwidth.

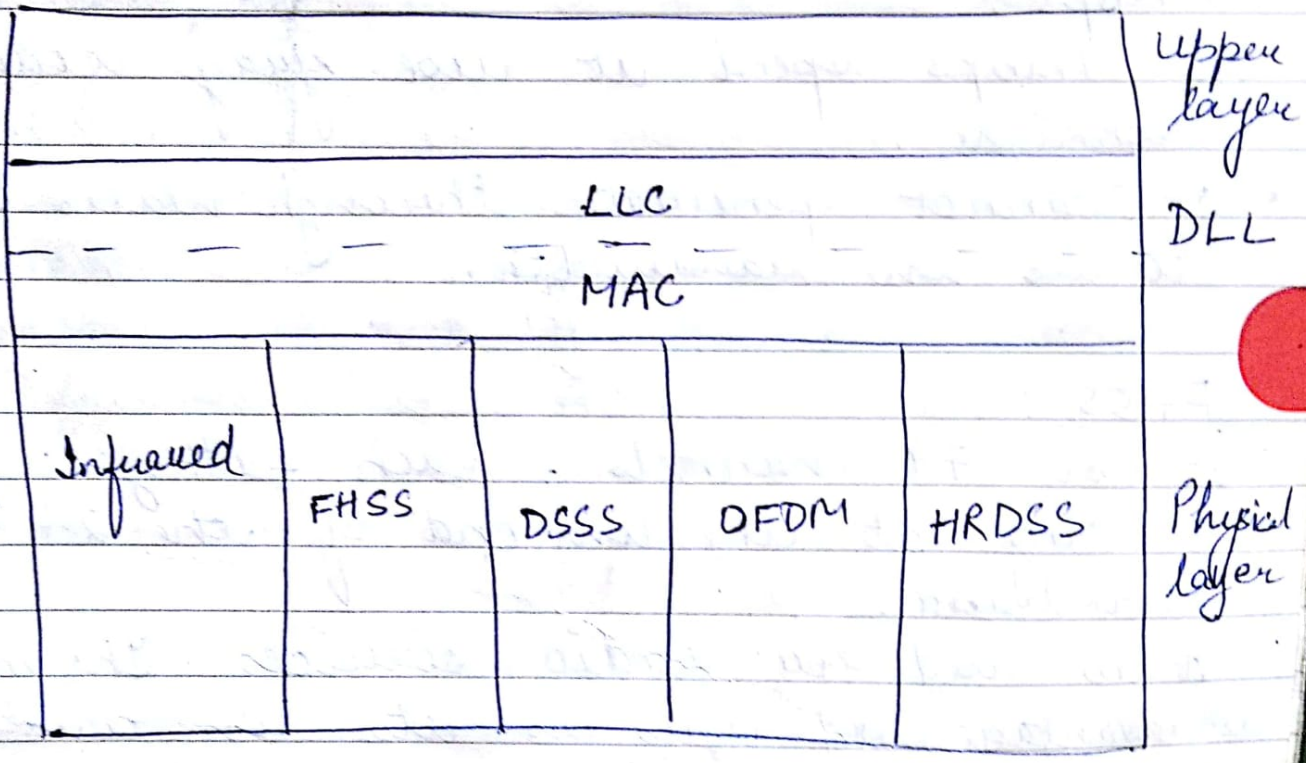
Shipra

Date

They can operate upto 54mbps.
Three techniques are —

1) OFDM : Orthogonal frequency division multiplexing

2) HRDSSS : High rate direct sequence spread spectrum.



Architecture of 802.

Date

802 point Physical layer:

INFRARED:

It is uses ~~the~~ ~~the~~ diffused transmission technique (non-line-of sight transmission technique) at 0.85 or 0.95 microns.

It can transmit at a speed of 1mbps or 2 mbps.

- At 1mbps speed it use Gray code technique.
- It cannot penetrate through walls due to its low bandwidth.

FHSS:

- It use 79 channels, each 1 MHz wide. Starting at the low end of the 2.4 GHz ISM band.

It is used for radio services. The main disadvantage of this is its low bandwidth. Once the longer distance, signal lost is a major issue.

DSSS:

- It operates in the 2.4 GHz ISM band at data rate 1 mbps or 2mbps.

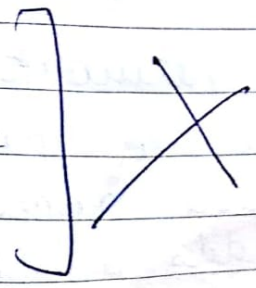
It does not require licensing for transmission

Date

• **OFDM:**
- This method use 5 GHz ISM band.
- It is similar to FDM technique but there 1 major difference — In OFDM, all the sub-bands are used by one source at a given time.
- It uses PSK & QAM modulation techniques.

HRDSSS:
- It uses 2.4 GHz ISM bands, at the data rate of 11 mbps.
- It is called 802.11B but does not follow 802.11A.
- It is used for longer distance communication with higher bandwidth.

- Satellite method
- Cellular phone
- Sonet dish



Shipra

Q. Explain Flame relay & ATM?
Q. Define Channel allocation problem & explain CSMA?

Logical Link Contud

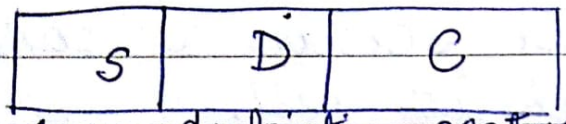
IEEE has defined 1 protocol which is called LLC that can run on the top of ethernet & other 802 protocols.
It hides the difference b/w the various kind of 802 networks by providing a single format & interface to the network layer.
This format & protocols are closely related to HDLC protocols.

WORKING:

The network layer on the sending machine pass a packet to LLC by using the LLC access rights, den LLC sublayer adds a LLC header containing sequence & ACK no. where frame structure contain source part, designation & contrul part.

Date

- LLC provides 3 kinds of services —
  * Unreliable datagram services
  * Acknowledged datagram services.
  * Reliable connection oriented service.



} explain?

MAC (Media access Control)

In the MAC sublayer, it can sense the channel, allocate channel & provide channel to particular station.

Ex. Station C is transmitting to station B if A sense the channel it will not hear anything & start transmitting to B which will create collision.

Imagine, Here B wants to send to C so it listen to the channel, it hears a transmission & conclude that C is already busy, but actually C is idle.

→ To resolve half duplex problem, we use 2 modes of operation —

1) DCF (Distributed Co-ordination function)

Shipra

Date

- It does not use any kind of central control, it is actually a distributed system

2) PCF (point coordination function)
- It use the base station to control all activities in all its cell.

DCF use a protocol CSMA/CA. In this protocol both physical channel sensing & virtual channel sensing are used. Two methods of operations are supported by CSMA-CA.

In the 1st method when a station wants to transmit it sense the channel.
- If it is idle, it just start the transmission.
- It does not sense the channel when it is busy.

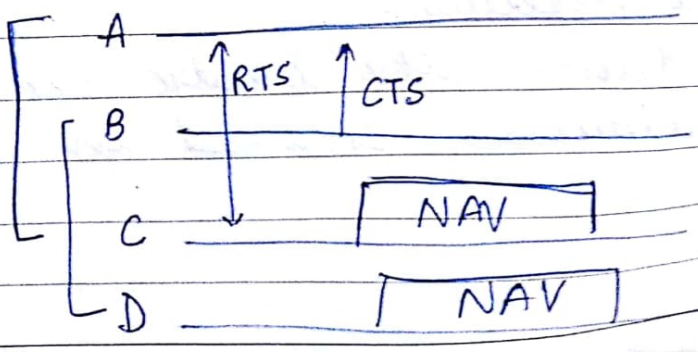
If a collision happen, the colliding stations wait for a random amount of time & try again later.

The other mode of CSMA-CA is based on virtual channel sensing.

Date

Ex: A wants to send contents to B. C is a station within a range of A. D is a station within a range of B but not within a range of A. The protocol start when A decides to send data to B. It begins by sending an RTS frame to B to get permission from B. When B receive this request it may decide to grant permission & sends back a CTS frame. A now sends its frame & starts ACK timer. By receiving the correct data frames B responds with ACK frame & terminate the exchange. But if A's ACK timer expires before the ACK gets back to it, the whole protocol is run again.

Now, consider this exchange from viewpt of C & D. C may receive RTS frame. It will realize that someone is going to send data soon. So it will keep himself virtually busy which is called as network allocation vector (NAV).



Shipra

hub – works as repeater 173

PCF

In PCF mode, transmission order is completely controlled by the base station. No collision can occur. The basic mechanism for base station is to broadcast a BECON frames periodically.

BECON frame: It contain all the info of network & transmit signals regularly to other stations to announce the presence of wireless LAN network.

- It contains system parameters, clock synchronisation & FHSS technique.
- It gives a guarantee of quality of services.
- It is more reliable than DCF.

BRIDGES:

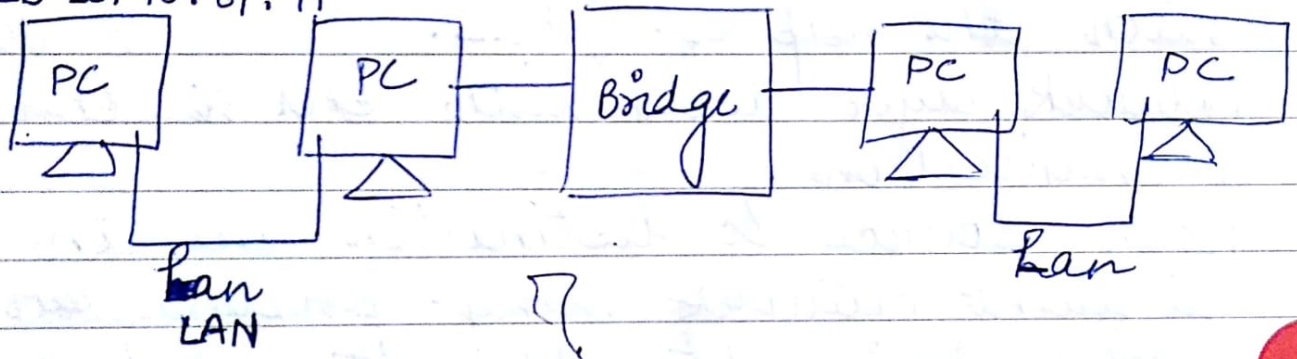
- A bridge operates in the physical & DLL.
- As a physical layer device it regenerate the signal it receives.
- As a DLL device the bridge can check the physical addresses contained in the frame.

!Pconfig/all

Date

- A bridge has filtering capability. It can check the destination address of the frame & decide whether the frame should be forwarded or not.
- If the frame is to be forwarded, it specify the ~~port~~ port no.

Mac address
71:2B:1B:45:61:41



Photocopy.

Module - IV

Network layer Design Issues

Network layer is concerned with getting packets from the source all the way to the destination. Getting to the destination it requires many intermediate routers on the way.

This layer's working structure is possible with the help of DLL.

Network layer deals with end to end communication.

When source & destination are in different network many problems can occur. It is upto the network layer to deal with these problems.

Network layer Design issue :-

There are no. of design issues with the network layer.

(1) Store & forward package switching.

Host H_1 is directly connected to one of the routers A by leased line.

H_2 is on LAN with a router F

F router is on on managed by H_2 owner.

Date

- A host with a packet ~~to~~ send's ~~forwards~~ it to the nearest router either Its/ Own LAN or over a point to point communication. The packet is stored in the router until it has fully arrived so that the checksum can be verified.

Then it is forward to next router along the shortest path until it reach toward the destination.

Problems with Store and forward :

- occupy buffer space of router
- slow speed [store + checksum + the forwards]
- Checksum at every level, ~~customer~~ consumes more time.

(2.) Services provides to Transport layer ? :

The network layer provides services to the Transport layer ~~and~~ at the network/ transport layer interface.

The network layer services has been design ~~to~~ with complete goals in mind.

(i) The services should be independent of the router technology.

(ii) The transport layer should be shielded from the no. type & topologies of the router system.

There was a major discussion whether the network layer should provide connection oriented service or connectionless services.

One can argue that the router job is to move packets here & there.

In their point of view communication channel is unreliable. No matter how it is defined.

So, it is mandatory to follow error control & flow control tech. This network service was connectionless. No packet ordering flow control was actually done.
Main motive was to hide data rate transmission with WAN.

Shipra

Date

The other camp argued that subnet should be reliable. They believe in quality & services for voice & data transmission.

Best ex. of both can be seen by ATM.

Routing Algorithms :

We have 4 types of routing algos -
1) Shortest path "
2) Distance vector "
3) Link - straight routing → OPEN shortest path first
4) Multi- ~~cast~~ cast routing.
5) Flooding

Distance vector routing :
→ Routing Information Protocol [RIP]

* Border Gateway Protocol (BGP)

The routing algo is that part of the network layer in which S/W is responsible for deciding which O/P line will forward the incoming packet.

Shipra

- If the subnet use datagram internally, the root may be chosen after arriving of the data packet.
- If the subnet use virtual circuit internally routing decision are made only when virtual connection are set-up.
- Router handles 2 process inside at the same time. One of them handles each packet as it arrives & looking up the outgoing line to transmit to its next destination. This process is called forwarding. Router is also responsible for updating the routing table.
- Routing algo should be able to handle changes in the topologies and traffic without creating problems to other jobs.
- Stability is also imp. role for routing algo
- Routing algo also can be grouped into 2 classes —
  - i) Non-adaptive routing
  - ii) Adaptive routing

Date

Non-Adaptive:

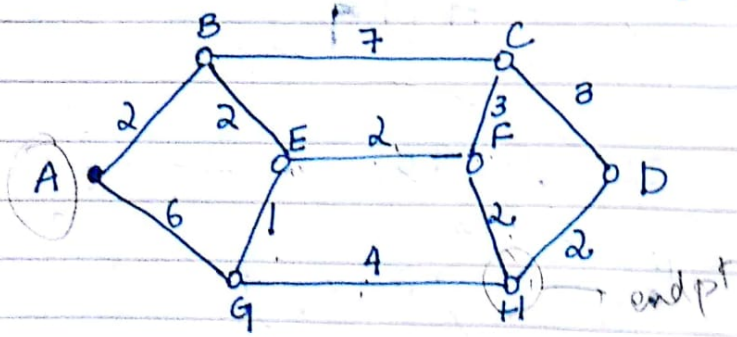
These do not base their routing decision on current traffic & topologies.
But the root is already computed in advance.
This technique is called static routing.

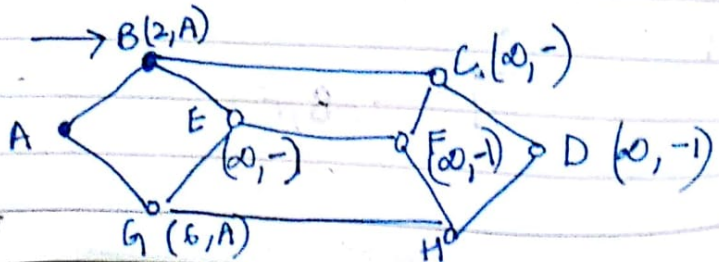
Adaptive:

These base their routing decision on current traffic & topologies.
It does have any pre-defined root; it changes acc. to requirement.
This technique is called dynamic routing..

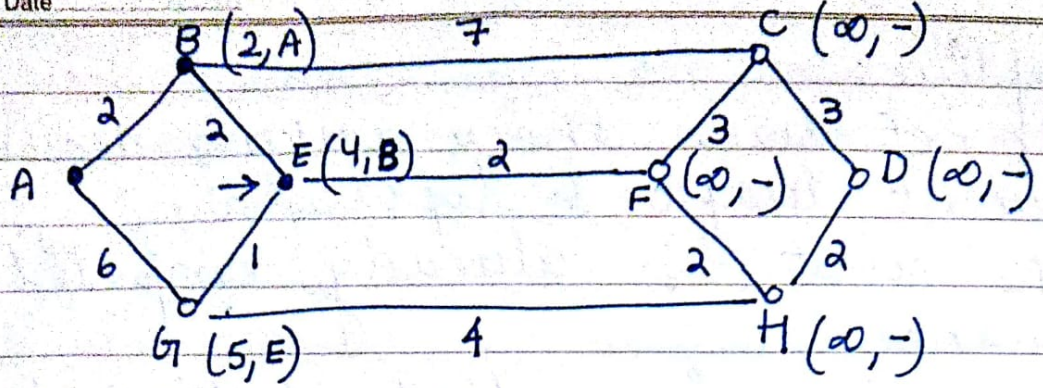
** Imp.

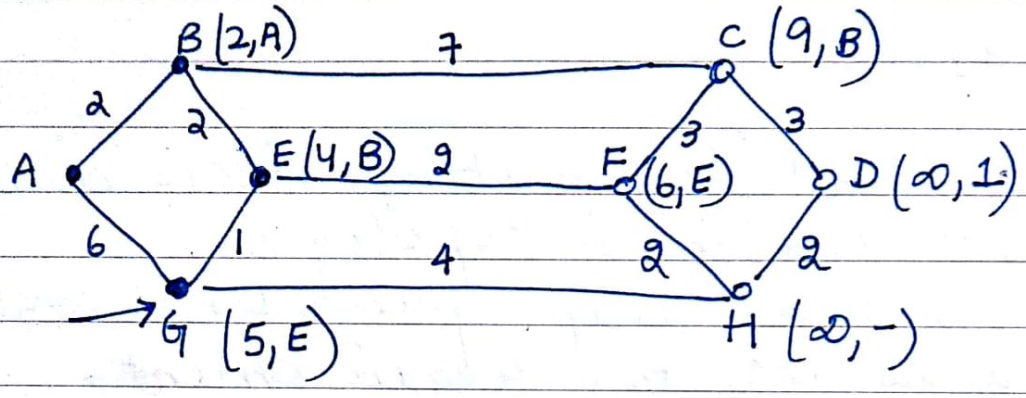
Shortest PATH ALGO (Dijkastra)

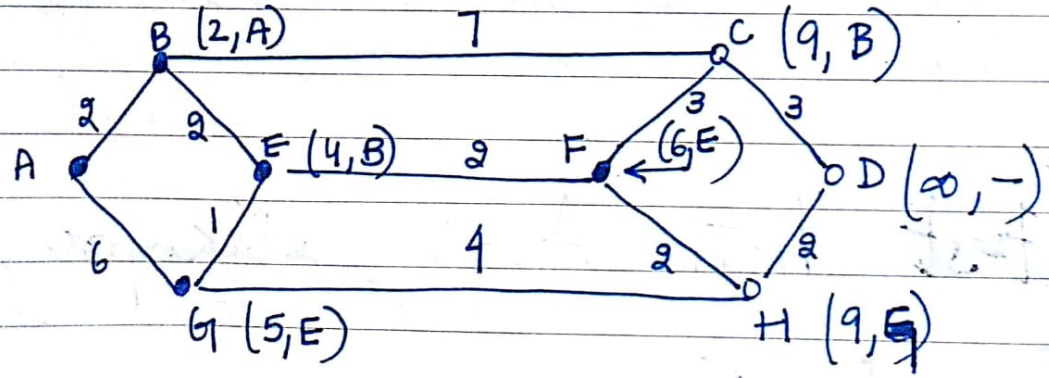


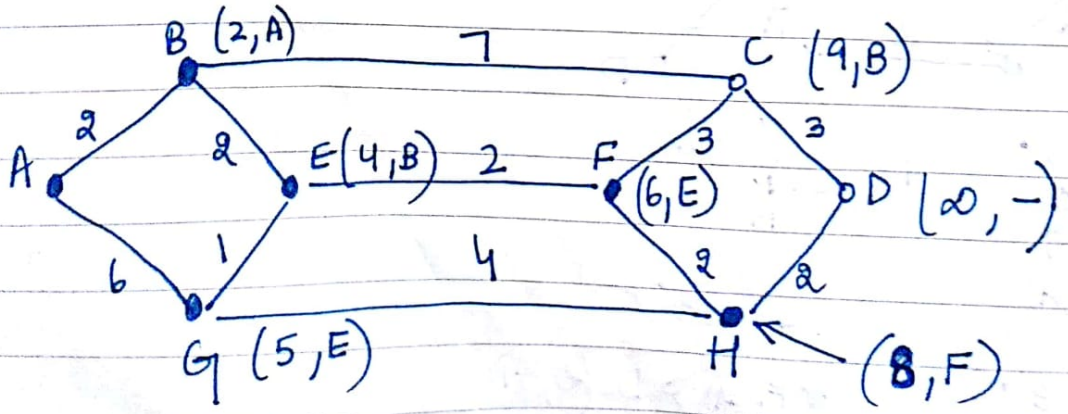


Shipra





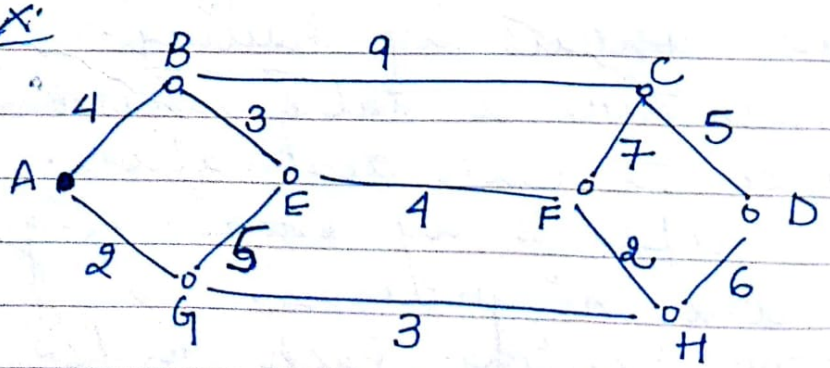




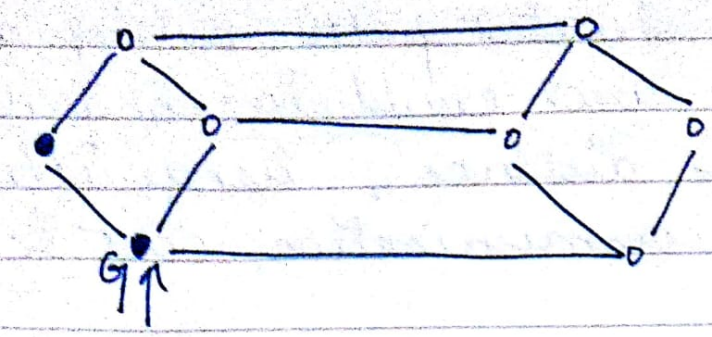
Date

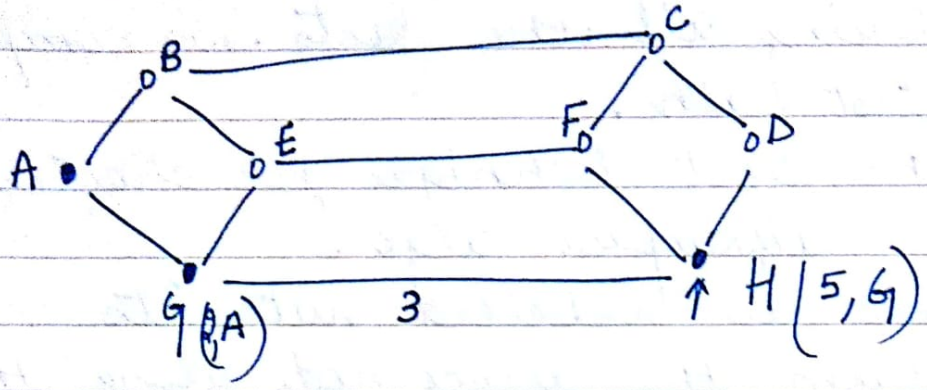
In general case for shortest path routing algo the labels on the arc could be computed as a function of distance, bandwidth, average traffic, communication cost & other factors.
By considering all the facts we compute the shortest path.
One of the best technique for shortest path is dijkaspra algo.
Each node is labelled with its distance from the source node along the best node path.
Initially no path are known, so all nodes are labelled with ∞.
As the algo proceeds paths are found, the label may change reflecting ~~dif~~ better path.
In label may be either temporary or permanent.

Ex:



A to H.





2) Distance-Vector Routing

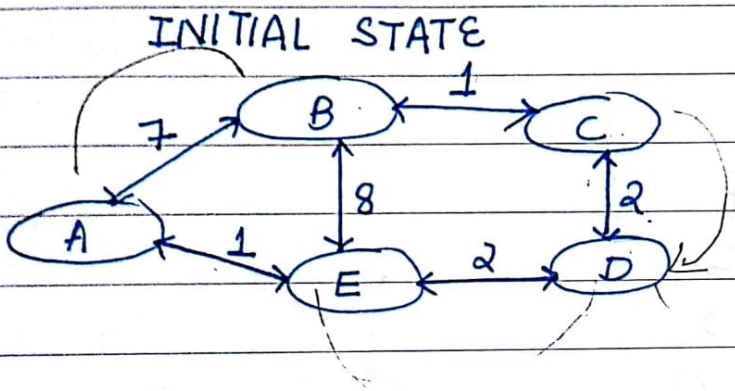
Modern computer network use dynamic routing algo rather than static.
2 dynamic algo we use —
1) Distance-Vector Routing
2) Link State Routing

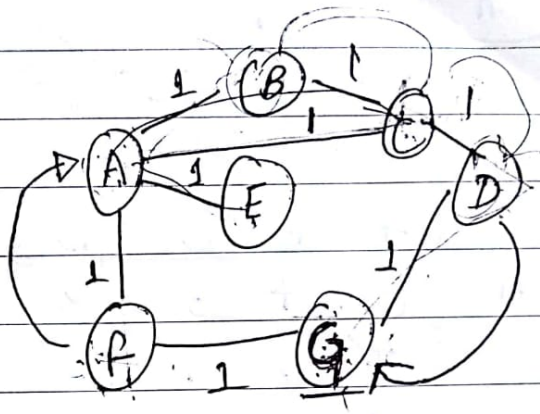
Distance Vector R. algo operate by having each router maintain a table which is the best distance to each destination. These tables are updated by exchanging info^m with the neighbours.
In distance vector routing each router maintains a table indexed by and containing one entry for each router

Date

in the subnet.

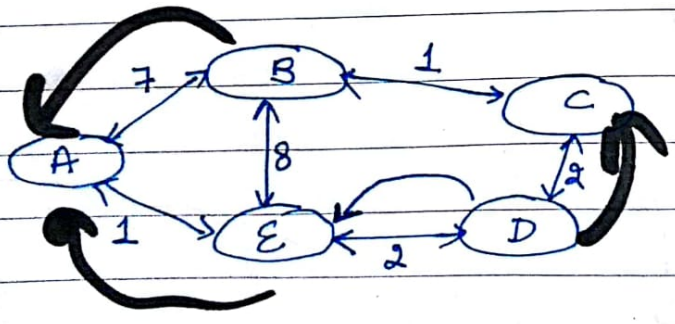
- This entry contains 2 parts — i) the preferred outgoing line to use that destination.
  ii) about estimate of time.





	A	B	C	D	E
A	0	7	∞	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞ 3.	2	0	2
E	1	8	∞	2	0

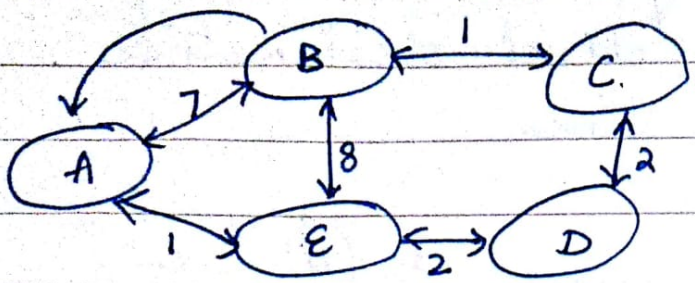
D sends vector to E



	A	B	C	D	E
A	0	7	∞	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	4	2	0

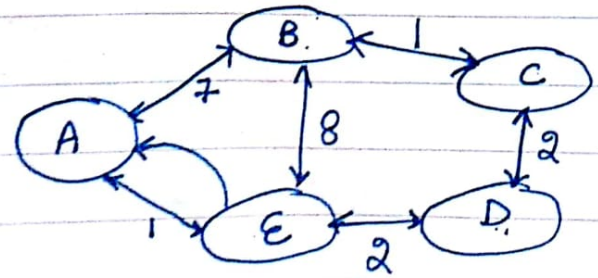
Shipra

B sends vector to A



	A	B	C	D	E
A	0	7	8	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	4	2	0

E sends vector to A

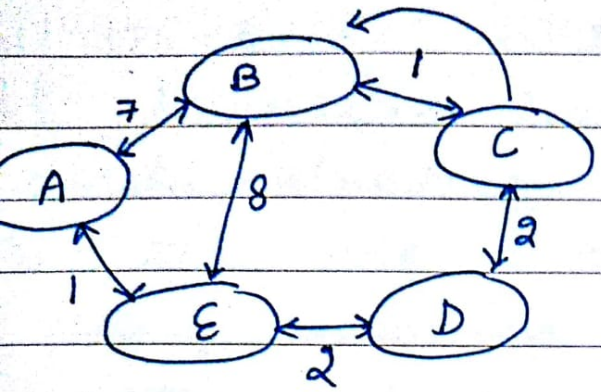


	A	B	C	D	E
A	0	7	5	3	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	4	2	0

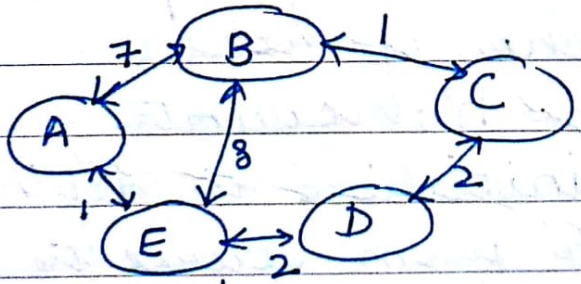
Date

C sends to B

& ultimate Diagram



	A	B	C	D	E
A	0	6	5	3	1
B	6	0	1	3	5
C	5	1	0	2	4
D	3	3	2	0	2
E	1	5	4	2	0



Node B is distance vector

	A	E	C
A	7	9	6
C	12	12	1
D	10	10	3
E	8	8	5

Take any node as distance vector

B

* Explain difference b/w static & dynamic routing? (8)

Date

Node A is distance vector

	B	E
B	7	6
C	8	5
D	10	3
E	12	1

3) FLOODING :

Another static algo. is flooding in which every incoming packet is sent out on every outgoing line except the one it arrived on.

Flooding generates vast no. of duplicate packets. In flooding one of the measuring technique is HOP count. This HOP counter is initialised to define the length of the path from source to destination.

An alternative technique to stop flooding is to keep track of which packet have been flooded to avoid sending them out at a second time.

- To achieve this goal source router put a sequence no. on each ~~router~~ packet.
- By this technique when a packet comes

Date

in to the destination, it is easy to check if the packet is duplicate it is discarded.
An alternative technique to stop flooding is selective flooding.
In this algo, the router do not send every incoming packet out on every incoming line, only on those lines that are going in right direction.
It will consume less bandwidth & channel utilisation will be optimized.

Flooding is not practical in most of the applications.
It is used in some specific areas—
→ It is used in military applications where large no: of routers are inter-connected & instant transmission is highly desirable.
→ In distributed data application to update all the databases at the same time.
Ex. Windows
→ In a wireless network, all messages transmitted by a station can be received by all other stations within its radio range.
→ It is used as a Metric against which other routing algo can be compared.

Shipra

4) Multi-Casting Algo:

Some applications require that different process work together in a group. An example of this is distributed database system.

If the group is small it can just send each other member point to point message. If the group is large this strategy is expensive.

Sometime broadcasting can be used to transmit message to large group but it is not reliable.

To provide reliability, we use multi-casting technique by using routing algo.

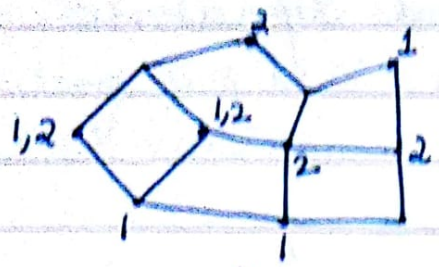
It is called multicast routing.

It require group management. Some way is needed to create & destroy group & to allow processes to join & leave groups.

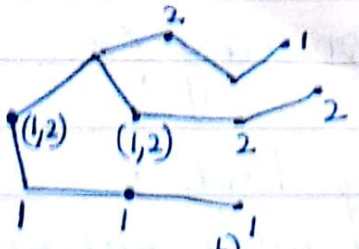
It is totally dependent multicasting routing.

Using spanning Tree Date

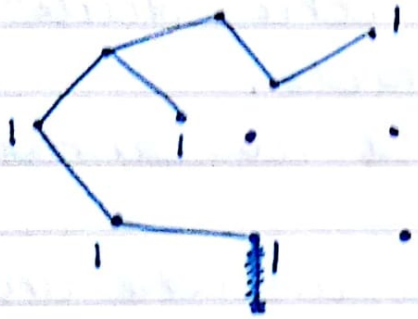
Ex.



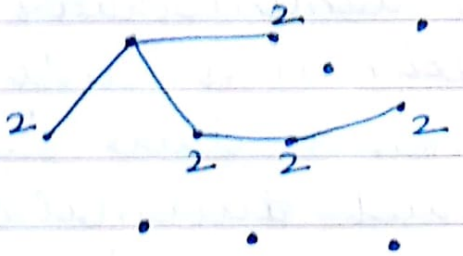
a)



b)



c)



d)

- represent host

Tanenbaum - Pg. 370 (Diagram)

Date

Q. Difference between static and dynamic routing?

Static Routing Table:
It contains info entered manually.
The administrator enter the rule for each destination into the table.
when a table is created it cannot be updated automatically.
When there is a change in the internet the table must be manually changed by the administrator.
A static can be used in a small internet that does not require to change frequently or in experimental internet for troubleshooting.
It is poor strategy to use static routing in wide network.

Dynamic Routing Table:
It is updated periodically by using one of the dynamic routing protocol like RIP (routing info protocol), OSPF (open shortest path first), BGRP (border gateway routing protocol).
Whenever there is a change in the internet such as shut down of

Shipra

Date

routers on breaking of a link, the dynamic routing protocol update all the tables in the routers.
The routers in a WAN needs to update dynamically for efficient delivery of the IP packets.

Routing Table Format :

Mask	Network Address	Next hop address	interface	flag	Reference Count	Use

Use : This field shows the no. of packets transmitted by the router.

Reference Count : It gives the info about no. of users using a specific route in the router.

Flag : We have 5 types of flag -
1) U : Up
2) G : Gateway
3) H : Host specific
4) D This flag specifies that this route is created by a redirect
5) M modified

1) U flag indicates the router is up & running.

Shipra

Date

If this flag is not present, it means router flag is down, the packet cannot be forwarded.

2) G → Gateway
It means that destination is in another network.
The packet is delivered to next hop router for delivery.
When this flag is missing it means destination is in the same network.

3) H → host specific
H flag indicates that the entry in the network address field is a host specific address.

4) D → Added by redirection
D flag indicate the routing info from source to destination.

5) M → Modified by redirection
M flag indicate that the routing info for the destination is modified by ICMP (Internet Control Message Protocol)

Date

Interface : This shows the name of the interface.

Next hop address : This field defines the address of next hop router to which next packet is delivered.

Network Address : It defines the network address to which the packet is finally delivered.

MASK : This defines the Mask ~~required~~ applied for the entry.

Static	Dynamic
Advantage : Minimum CPU/memory overhead. • No bandwidth overhead. • Security • Choose specific path for communication. **Disadvantage** : • Infrastructure changes must be manually adjusted. • No dynamic fault tolerance scheme. • Not useful on WAN or MAN	**Advantage** : Simple to configure on a large network. • It handles congestion. **Disadvantage** : • Updates are shared b/w routers so it consumes more bandwidth. • Max. CPU/memory overhead • Security is less than static Routing.

Shipra

Date

⇒ Linked State Protocol -

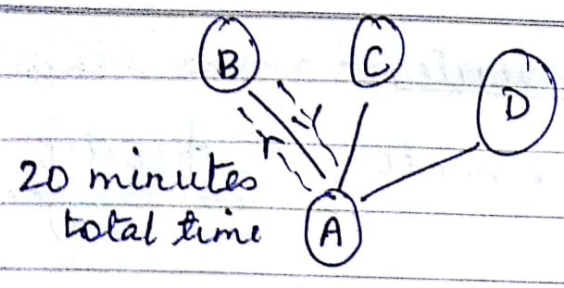
- The distance vector routing problem & shortest path routing problem is count to ∞ for a next neighbour hop.
- For these reasons it was replaced by new algorithm which is called linked state routing.
- Linked state routing achieved ~~to~~ 5 diff. tasks for each router —

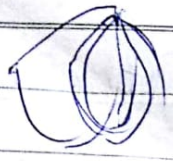
1) Discover its neighbour & learn their network address.
2) Evaluate the delay or cost to each of its neighbour.
3) Transmit a packet to all its neighbour to know their presence. (Send this packet to all other routers)
4) Compute the shortest path to every other router.

(1) Learning about the neighbour :
When a router is booted then the 1st task is to learn who its neighbour are. To achieve this goal it sends a "hello" packet at each pt. to pt. line.
The routers on the other side sends back a reply by their unique no/address.

Shipra

Date



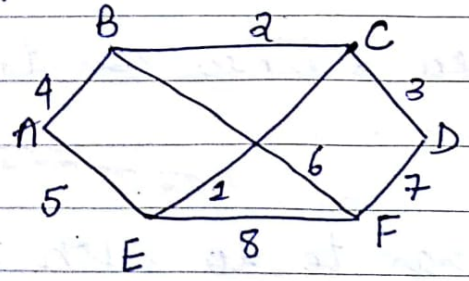


explain diag.?

(2) Calculating line out :

- Linked state routing algo requires each router to know at least reasonable estimate of the delay to each of its neighbour.
- The most easier technique to find this delay is to send a special 'ECHO' packets that the other side is required to send immediately.
- By calculating the total time for sending & receiving & diviiding it by 2, the sending router can get a reasonable estimate of the delay.

(3) Building linked state packets -



Linked States -

	A
B	4
E	5

	B
A	4
C	2
F	6

	C
B	2
D	3
E	1

	D
C	3
F	7

	E
A	5
C	1
F	8

	F
B	6
D	7
E	8

Chipra

Date

(4) Computing the new routes -

Shortest path, distance vector ki theory.

⇒ Congestion Control Algorithm:

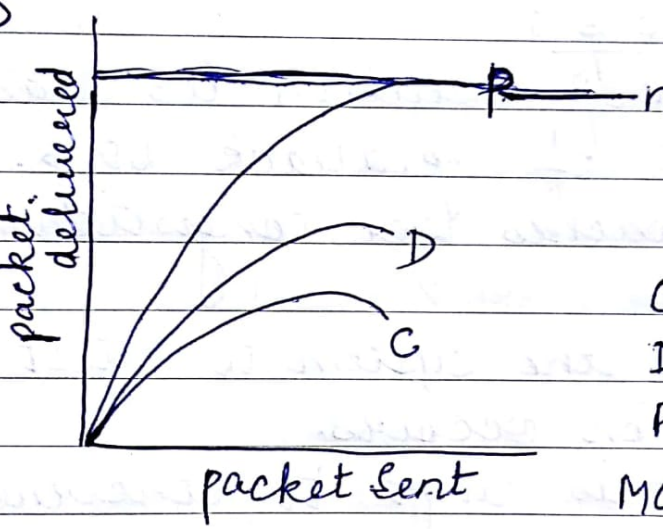
- When too many packets are present in the subnet, performance degrades this situation is called congestion.
- If traffic rises rapidly, the routers are not able to handle this situation & start using no. of packets.
- Congestion can be possible by several factors
  (1) If all of a sudden stream of packets start arriving on 3 or 4 i/p lines and all need the same o/p line, a queue will build up if there is insufficient memory to hold all of them, packet will be lost, this will be a congested situation.
  (2) Slow CPU speed is another source of congestion.
  (3) Difference between 2 lines bandwidth also create congestion.
- Congestion control has to do with making sure that the subnet is able to carry current traffic.

Shipra

Date

- It uses store & forward technique within the router.
- It uses flow control technique to avoid collision

1. General principles of congestion control
2. Congestion prevention policies.
3. Random early detection.
4. Jitter Control
5. CSMA - CA
6. CSMA - CD



C: congested
D: desirable
P: Perfect
MCC: max. carrying capacity

1. General principles of congestion control –

To resolve congestion, problem in computer networks we follow 2 technique –

a) open loop b) closed loop

a) Open loop:
Open loop solutions try to solve the problem by good design, specific architecture & testing technique.
- Once the system is up & running in b/w connection is not possible.
- Tools for doing open loop control include deciding when to accept new packet or discard packet it is upto open loop.

b) Closed loop:
Closed loop solution is based on the concept of feedback loop. It follows 3 approaches for congestion control—

(1) Monitor the system to detect when & where congestion occurs.
(2) Pass this info to concerned node where action can be taken.
(3) Adjust system operations to correct the problem.

2. Congestion prevention Policies

Layers	Policies
1) Transport	(1) Retransmission Policy (2) ACK Policy (3) flow control Policy (4) Time out determination

Date

(2) Network	(1) Routing algo (2) Packet discard policy (3) Virtual & datagram ckt. (4) Packet priority.
(3) Datalink	(1) Error detection (2) flow control policy (3) retransmission " (4) acknowledgement "

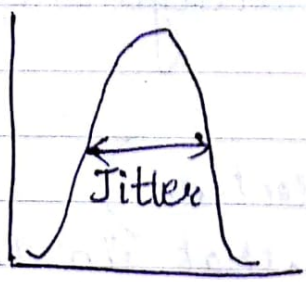
⟹ RED (Random Early Detection)

- It is ~~tool~~ well known that in dealing with congestion after it was detected is more effective than handle in b/w the work.
- The idea discards packet before all the buffer space is actually exhausted.
- A popular algo for doing this is called RED.
- To define when the algo starts discarding packages, rather than maintain an avg. queue length.
  When the avg. queue length takes more time for ack it means lines is congested, action is req.

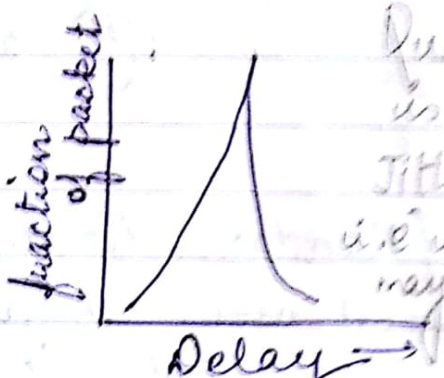
Shipra

- Since the router cannot tell which server is creating most trouble.
- Picking the packet randomly helps the algo to find the problem which is only possible by RED.

⇒ Jitter Control:



High jitter



Low jitter

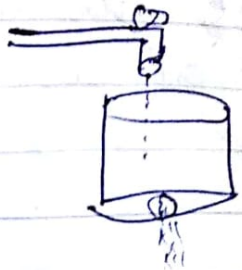
Quality of service is not good if Jitter is high i.e. uneven pattern is not desirable.

Jitter ↓ Quality ↑

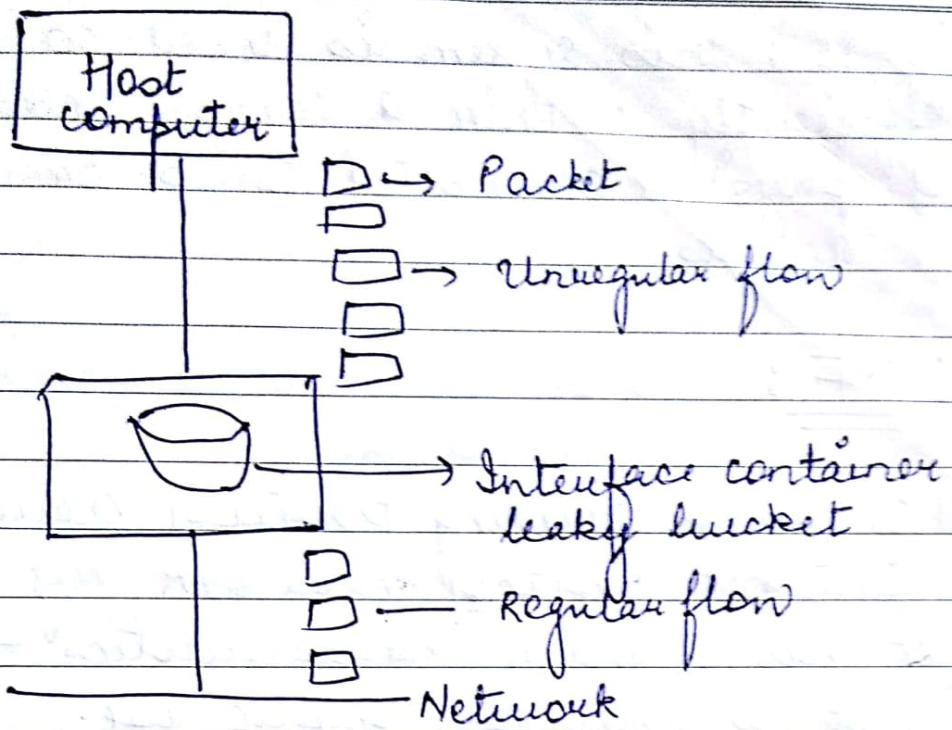
Quality of Services

Technique for achieving good Quality of service —

1. Over provisioning
2. Buffer space
3. Traffic shaping
4. Leaky Bucket algo



Date



⇒ Interior gateway Routing Protocol (IGP) within an organisation

* communication internal
2 types of techniques —

- Distance vector Routing
  - RIP (Routing info protocol)
  - IGRP (Interior gateway Routing protocol)
- Link-state Routing
  - OSPF (Open Shortest path first)
  - is-is (Intermediate system to intermediate system)

IS-IS : This system is used to move info efficiently within a comp. Network, a group of physical connected comp. or similar devices.

OSPF : 2 or more nodes communicate then the comm. is through shortest path.

This is a routing protocol developed for Internet protocol network by IGP.

It has 2 main characteristics —

1. It is open for public use.
2. It is based on SPF algo.

OSPF supports 3 kinds of connections —

1. pt - pt between 2 routers.
2. multi-access network with broadcasting
3. " " " without "

DSPF packet format

Byte size	1	1	2	4	4	2	2	8	variable
	status no.	type	packet length	router ID	area ID	check-sum	authen-tication type	Authen-tication	Data