Data Communication & Computer Networks

When we communicate we share information either locally or on remote systems. The word 'data' refers to the information presented in a form agreed upon by different parties that are creating & using the data.

Data communication are the exchange of data b/w 2 devices via some form of transmission medium.

For data communications to occur the communicating devices must be a part of communication system made up of combination of hardware & software.

The effectiveness of Data communication system is based on 4 characteristics:-

1) ~~Delivet~~ delivery - The data must be delivered to the correct destination.
2) Accuracy - The system must deliver data accurately.
3) Timeliness - The system must deliver the data timely without any delay.
4) Jitter - It refers to variation in packets arrival time. It is uneven delay in the ~~del~~ delivery of various signals that are related

Components

1) Sender - Its is device that sends the data message.
2) Receiver - " " " receives the " "
3) Message - Info that has to be shared
4) transmission channel or medium - It is the physical path b/w sender & receiver over which the

data is transmitted,

5) protocol - It is required to govern the data comm.

- Data representation

1) Text format which is representated as a bit pattern, a sequence of zero's or ones, different bit patterns represent diff text symbols.

2) Numbers - also represented by bit patterns however for

3) Images composed of a matrix of pixels where each pixel is a small dot so the images are also represented by bit patterns. The size of the image depends on the resolution.

- Audio representation =

Audio signals are continuous signals or non-discrete values.

Audios refers to recording or broadcasting of sound.

Video

It refers to recording or broadcasting of a movie It can be produced as a continuous entity or a combination of images i.e a descrete entity.

Data flow :-

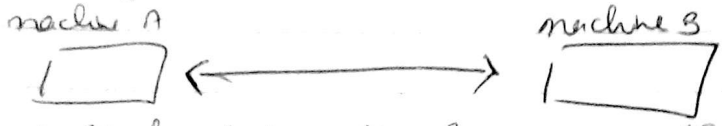
There are 3 modes of data communication :-

1) simplex mode
2) half-duplex
3) full-duplex

1) simplex mode

Only machine A can transmit data.

2) half duplex



cannot send data at the same time.

Eg:- e-mail.

3) full duplex

can send data simultaneously. same ~~as~~ channel is divided in 2 parts.

broadband width is shared b/w 2 machines.

Networks

A network is a set of nodes connected by comm. links.

~~Links~~ Network performance

→ performance can be measured using transit time and response time. Transit time is the amt. of time required for a message to travel from one device to another. Response time is the elapse time b/w an inquery and a response.

→ Performance of a network depends on no. of factors including no. of users transmission medium need capability of hardware & efficiency of software.

Physical Structures

→ Reliability
Network reliability is measured by frequency of failures, the time it takes to recover from a failure.

→ Network security
issues include protecting data from unauthorized access and implementing policies & procedures for recovery from ~~breaches~~ of data loses.

Physical Structures

connection points.

1) point-to-point connections (p to p)
In this a dedicated link b/w 2 devices is provided The entire capacity of the link is reserved for transmission b/w these 2 devices.

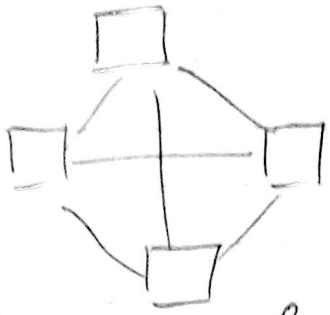
2) multi-point connection
It is a connection in which more than 2 specific devices share a single link. In this, the capacity of the channel is shared.

1) Physical topology

It refers to the way in which a network is established physically. It is a geometric representation of the relationship of all the links and linking

devices to one another.

a) Mesh topology –
Every device has a dedicated p to p link to every other device.



Advantage
→ Alternatives paths are available.

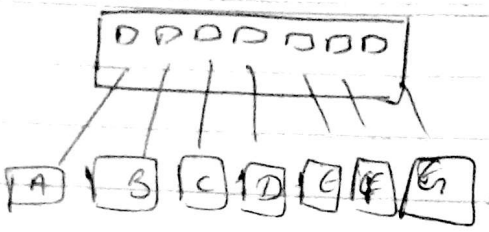
Drawbacks
→ ~~fault detection will be complex.~~
→ cost will increase.
→ managing is difficult

We need $\frac{n(n-1)}{2}$ physical links to connect n nodes.

Advantages
1) dedicated link.
2) robust
3) privacy & security.
4) fault identification and isolation is easier.

Disadvantages
1) No. of cables increases
2) No. of i/o ports increases.
3) Installation & reconnection is difficult.
4) Expensive.

b) Star topology
In this topology, each device has a dedicated p-to-p link only to a central controller usually called a hub. Star topology does not allow direct traffic b/w devices. The controller acts as exchange manager.



Advantages

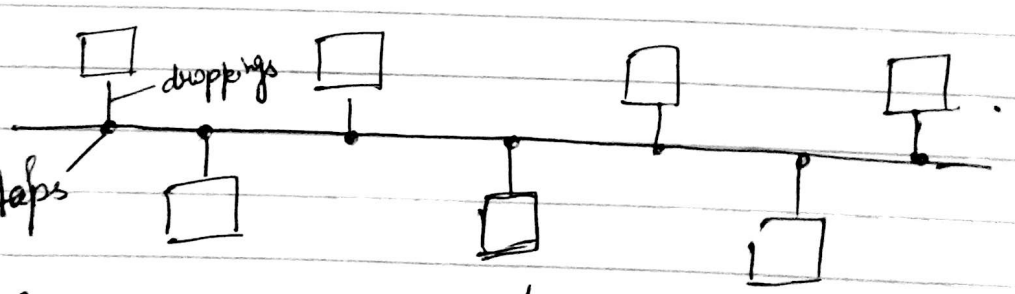
1) less expensive
2) easier to installer
3) no of cables is reduced. ~~addition & deleti~~
4) addition & deletion of node is easier.
5) identification & isolation is easier

Disadvantages:

1) central dependency on hub.
   if hub is dead all nodes will fail.

c) Bus topology

It is a multi-point topology. In this a long cable acts as a backbone to link all the devices over the network.



Advantages

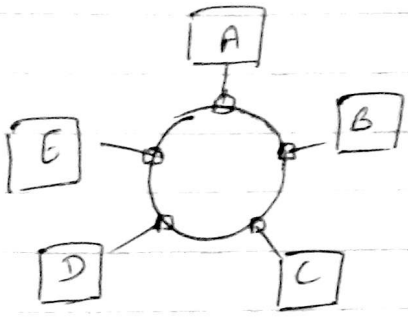
1) lower cost
2) easy installation
3) less cabling

Disadvantages

1) difficult reconnection
2) difficult to add new or delete nodes.
3) fault isolation is difficult
4) if backbone fails entire network fails.

d) Ring topology

In this, each device has a dedicated p-to-p connection with only the 2 devices on either side of it. A signal is passed along the ring in one direction from one device to another. Each device has a repeater attached to it.



It can be unidirectional and bi-directional.

If we have to send data from A to C then first it must pass through B, then C, D and E.

Advantages

1) fault identification is easier.
2) ~~easy~~ easier to install.
3) less expensive.

Disadvantages

1) repeaters cost is overhead.
2) If one node fails, transmission stops.

Network models

It provides the way of representing objects & their relationships. It also provides the standard so that different networks can communicate with one another. The 2 standard models are OSI & Internet model.

Protocols & Standards

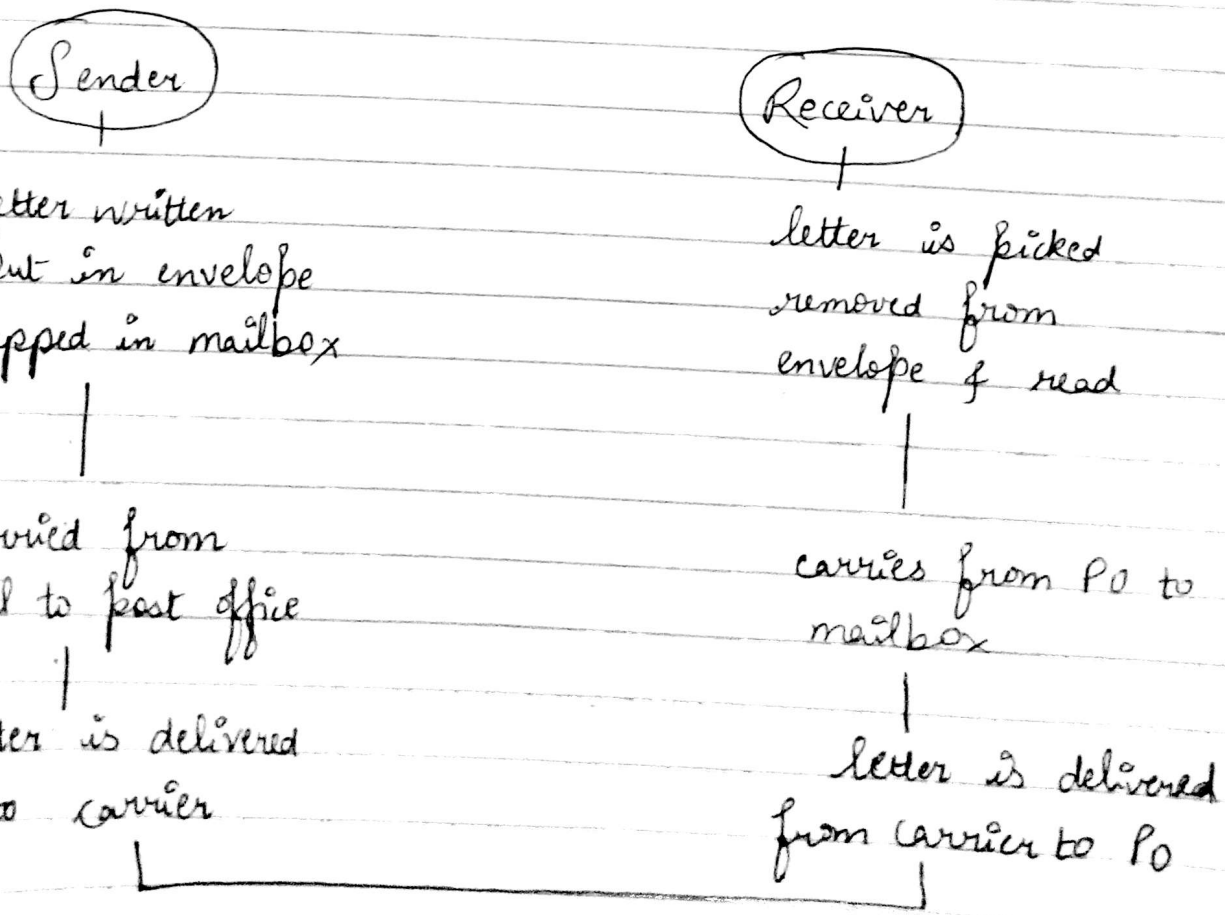
For communication to occur the entities must agree on a protocol which is a set of rules that govern the data communication. A protocol defines what is communicated & how it is communicated & when it is communicated.

Key elements of protocol.

1) syntax
2) semantics ~~syntax~~
3) timings.

Layered tasks

Example:



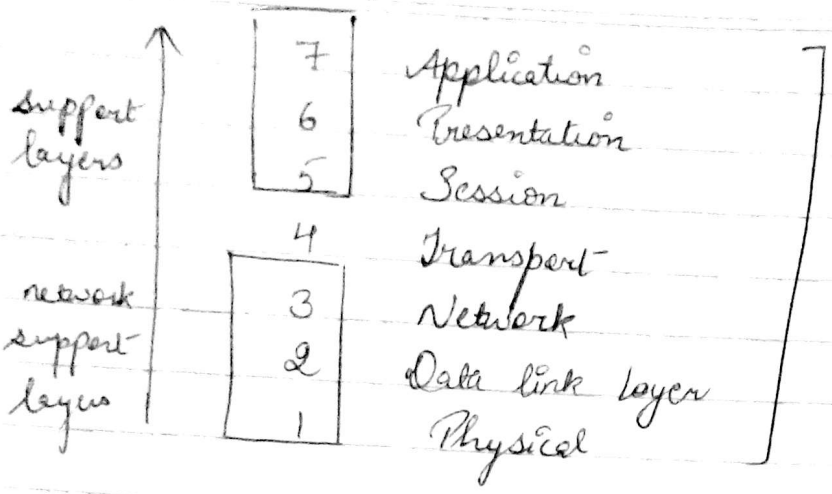
Estb - 1947
Implement (started, Not completed).

Each layer at the sending side uses the services of the layer immediately below it. The layered model that deminated data communications and networking was the OSI model.
The TCP/IP protocol deminated commercial architecture over the internet.

All 7 layers will be present in the same order in both sender and receiver machines. They are related (Peer-to-peer).

OSI model
It was established in 1947. An ISO standard (Intt Org for standardization) that covers all aspects of network comm. is the open system Interconnection (OSI) model.
An 'open system' is a set of protocols that allows any 2 different systems to communicate, regardless of their architecture and the purpose was to show how to facilitate comm. b/w different systems w/o requiring changes to the logic of hardware and software.

OSI model is a layered framework for the design of network systems that allows comm. b/w all types of systems. It consists of 7 seperate but related layers, each layer defines a portion of the process of transmitting data over the network.



Each layer in the sending device adds its own info to the message it receives from the layer just above it and passes the whole package to the layer just below it.

The passing of data and network info down through the layers of sending device & back up through receiving device is made possible by an interface b/w each pair of adjacent layers; & that defines the info & services, a layer must provide for the layer above it.

→ 1, 2, 3 = network support layer, defines how data will be transmitted from source to ~~des~~ destination.

→ 5, 6, 7 = support layer, Interact within users, using diff softwares.

(I) Physical layer

It coordinates the functions required to carry a bit stream over a physical medium.
It deals with electrical specifications of the interface and transmission medium. It also defines procedures, to be performed by physical devices for transmission to occur.

Functions:

1) Physical characteristics of interfaces & medium
2) Representation of bits: The physical layer transmits the bits which must be encoded into signals, either electrical or optical.
3) Data rate (Bits per second)
4) Syncronisation of bits.
5) Line configuration.
6) Physical topology.
7) Transmission mode.

II DLL

It transforms the physical layer, a raw transmission facility to a reliable link (HOP to HOP delivery)

Functions:

1) Framing: converts data into manageble layers, when data is huge.
2) Physical addressing (Local networks)
3) Flow control.
4) Error control
5) Access control.

Frame : bigger than Packet

Routers & switches → work on network layer.

III Network

Source to destination delivery is done by Network layer. It delivers packets across multiple links It also ensures that each packet get from its points of origin to find destination. It is responsible for logical addressing (for networks crossing huge distances).

Functions:

1) Logical addressing.
2) Routing.

IV Transport layer

~~Source to destination~~ It is responsible for process to process delivery.

Responsibilities of transport layer -

1) Service point addressing.
2) Segmentation and reasembling.
3) connection control.
4) flow control.
5) Error control.

V Session layer

It is responsible for dialogue control & syncronization.

Read about → hubs, switches, gateways, bridge, router, OSI layer.

VI Presentation layer

It is responsible for syntax & semantics of the info exchanged b/w the 2 systems.

Responsibility of this layer:—

1) Translation
2) Encryption.

VII Application layer

It enables the user to access the network. It provides user interfaces and support services etc. to the user.

Functions

1) provide network virtual terminal.
2) file transfer & management.
3) e-mail forwarding & receiving.

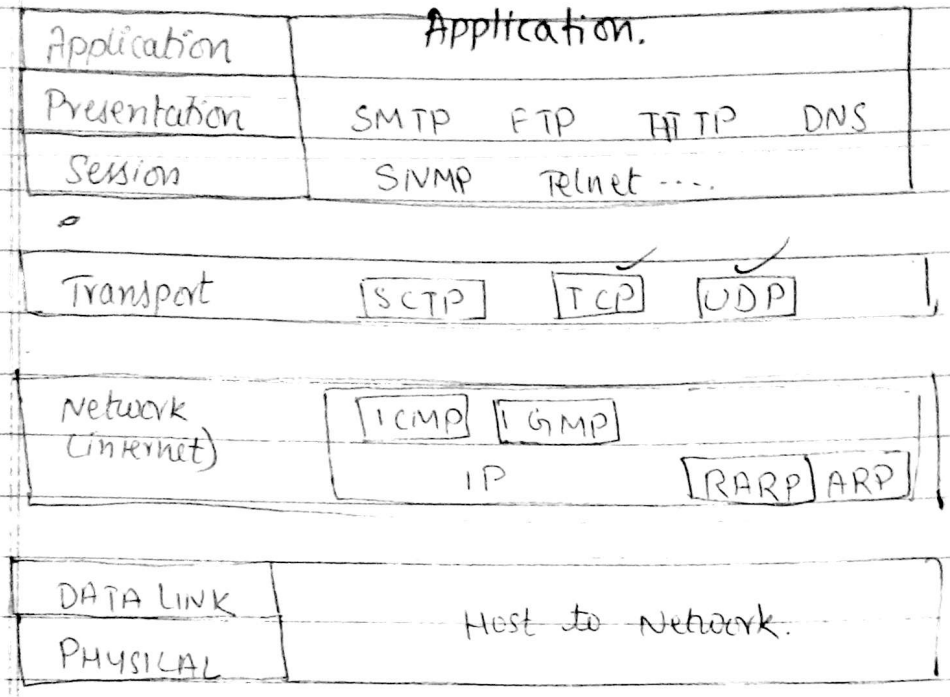
TCP/IP protocol

Application Presentation Session	SMTP FTP HTTP DNS SNHP Telnet...
Transport	SCTP TCP UDP
Network (Internet)	TCHP IGMP IP RARP ARP

SMTP – Simple mail transfer protocol

DNS – domain name service

TCP/IP protocol suit



TCP/IP is a hierarchial protocol made up of interactive modules each of which provides a specific functionality.
At transport layer, TCP/IP defines 3 protocols.

UDP - User data gram protocol
SCTP - Screen control transmission protocol
TCP - Transmission control protocol

At network layer,
ICMP - Internet control message protocol
IGMP - Internet Group message protocol
RARP - Reverse Address Resolution protocol
ARP - Address Resolution protocol

Physical and data link layer
At this layer, TCP/IP supports all

the standard and proprietary protocols. A network in a TCP/IP can be LAN or WAN

Network layer is also known as inter network layer

Internetworking protocol (IP)

IP is an unreliable and connection less protocol It provides no error checking or tracking. IP transports data in packets called data grams

The data gram is transported separately by a differen route and can arrive out of sequence or duplicated

ARP (Address Resolution Protocol)

ARP is used to associate a logical address with a physical address. Over a LAN, each device is identified by a physical address (usually printed on NIC card now ARP is used to find a physical address if its internet address is known.

DATA LINK LAYER.

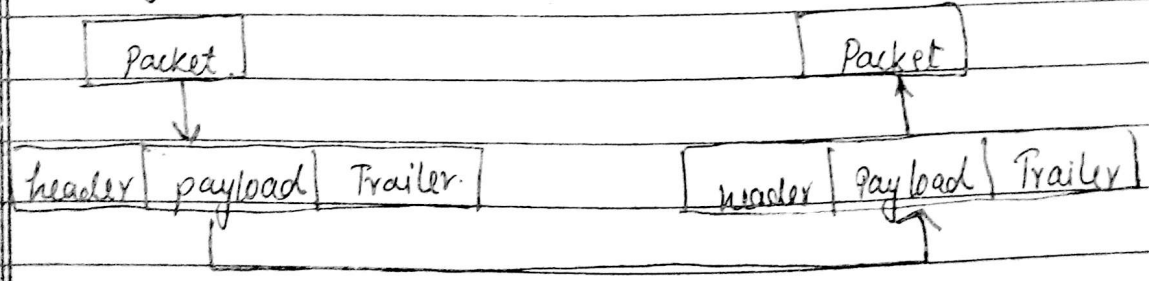
DLL design issues:-

The DLL has a number of functions, it can carry out these functions include:-

1) providing a well defined service interface to network layer.
2) dealing with transmission error
3) regulating the flow of data, so that the slow receiver are swamped by the fast senders.

→ To fulfill these goals, DLL accepts packets from the network layer and make frame for transmission.

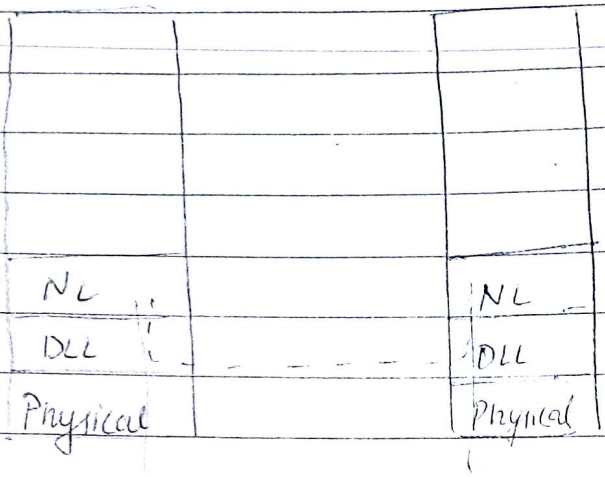
– Each frame has 3 things
- header
- payload
- trailer



– frame management is the main role of DLL.

function/service of DLL.

- principle service is transferring data from network layer on one machine, to the network layer on another machine.



(primary) (I)

- The DLL can be designed to offer various services:-
  i) unacknowledged connectionless service.
  ii) acknowledged connectionless service
  iii) acknowledged connection oriented service.

unacknowledged connectionless service consists of having source machine, send independent frames to the destination machine without having the destination machine to acknowledge them. no logical connection is established in advance. No attempt is made to detect the lost frame.

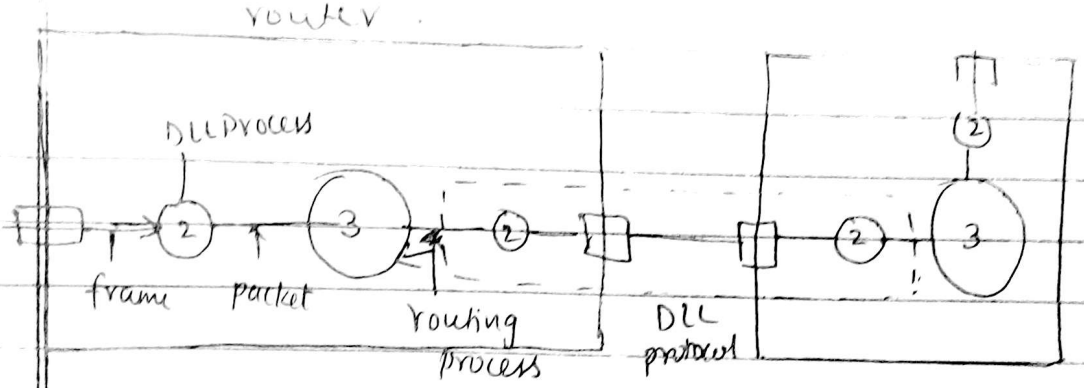
This is appropriate when the error rate is very less and is appropriate for voice traffic (real time traffic).

Acknowledged connectionless - no logical conn. is established before hand but each frame send is acknowledge Sender knows wether frame has arrived correctly or not. if not it can send it again.

This type of service is suitable over unreliable channel. Each frame have a fixed length but the packets do not have.

connection oriented service - The connection is established in advance. Each frame sent is numbered DLL guarantees that each frame is received and inorder exactly once.
with connection oriented service transfer gothrough three different phases:

i) connection establishment
ii) transmission
iii) connection release.



creation of frames.

- To provide service to the network layer, DLL uses services provided by physical layer.
- physical layer accept raw bit stream and deliver it to the destination.
- Bit streams is not error free, i.e. DLL has to detect and correct these errors.
- The DLL divides the bit streams into frames, for each frame, it computes the checksums, and at the destination, this checksums is recomputed.

By comparing these 2 values of checksum, DLL gets to know about the error.

Topic

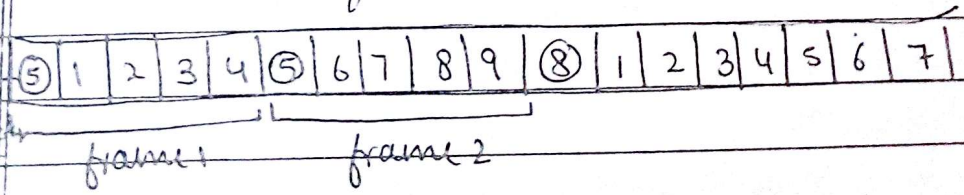
Breaking the data into frames is difficult. One way is to insert gaps b/w frames. It is too risky to count on timing to mark start and end of the frame.

Other methods are

i) ~~Character~~ character count.
ii) Flag bytes with byte shuffing.
iii) Starting & ending flag with bit shuffing.
iv) physical layer coding violations.

i) Character count.

This method uses a field in the header to specify the number of characters in the frame. When DLL at the destination sees the character count, it knows about the number of characters and the end of the frame.



problem with this method is, count can be garbled, which leads the destination out of synchronization.

Destination does not know, from where the data starts. Sending the frame back to sender does not help even. It is rarely used.

It is rarely used.

flag byte with byte shuffing-

each frame starts and end with special bytes. most protocol use same bytes for start and end. These bytes are known as flag bytes.

flag bytes can also become the part of the data, to overcome this problem, we insert special escape byte before each flag byte. The reciving DLL removes the escape byte, this is called byte shuffing.

starting and ending with flag bit shuffing.

Data frame contain arbitrary number of bits. Each frame begins and end with a special bit pattes 01111110.

Whenever the senders DLL encounters five consicutive 1's in the data, it automatically shuffs a zero bit into the outgoing bit stream.

Whenever, the reciever see's 5 consecutive incoming 1's bits followed by a zero. it automatically delets the zero bit.

If the user data, contains the flag pattern, 01111110, this flag is transmitted as 01111101.

Physical layer coding violation -

It is used where, encoding is different on physical medium. every bit has a transfer in the middle to locate the bit boundaries, which makes it easy for the reciever &

Error Control -

to make sure all frames, delivered to the destination and in proper order.

To ensure reliability the sender should receive the feedback from sender.

+ve or -ve acknowledgment are sent by the receiver, +ve means frame is arrieved safely -ve means something is wrong and frame has to be retransmitted.

The hardware trouble may cause a frame to vanish completely. In this case, the reciever will not react at all. The protocol will hang forever. if a frame is lost due to the hardware.

The soln. is to use the timer into DLL, when the sender transmits a frame, it also starts the timer. The timer is set to expire after an interval long enough for the frame to reach the destination, processed there and acknowledgement propogates back to the sender.

If either the frame or acknowledgement is lost, the timer will go off. and the sender will retransmit the frame again, which may lead to duplicacy at the reciver end. To over come this problem sequence number are assigned to the outgoing frame.

flow control

flow control mechanism is provided to deal with the problem, that the sender sends faster than the reciever accepts the frame.

The soln. to this problem is :-

1) feedback based flow control - the reciever sends back the info to the sender giving it permission to more data.
2) rate based flow control - the protocol has a builtin mechanism that limits the rate at which sender may transmit data without using the feedback.

Error detection and corrections :-

Network designers have developed 2 basic strategies for dealing with error.

detection + correction

1) include enough info. along each block of data, send which enables the receiver to deduce what the transmitted data must have been.
2) include only enough redundancy to allow the receiver to deduce that an error occured but not which error and request for retransmission.

error detection

On channels that are highly reliable such as fiber, it is cheaper to use error detection. However on unreliable channels, such as wireless it is better to add enough data to each block rather than relying on retransmission.

On channels that are highly reliable such as fibre, it is cheaper to use error detection. However on unreliable channels like wireless it is better to add enough data to each block rather that relying on retransmission.

Normally a frame consists of m data bits and are (r) redundant bits / check bits. Let the total length be n etc. ($n = m + r$) and n bit unit containing data & check bits are referred to as n-bit code word.

The no. of bit positions in which the 2 codes words differ is called hamming distance.

Example of error detection code is single parity method In this a parity ~~metre~~ bit is appended to the data

With the help of parity check method, single errors are detected.

m = message bits
r = redundant bit
$n = m + r$

$m + r + 1 \leq 2^r$

1 0 1 1 0 1 0 1 → sena
1 0 1 1 1 1 0 1 received
there is change in one bit so we can say that there is error in transmission using parity method.
(checks only for one bit)

Hamming code

Bits are numbered from left to right. Bits that are power of 2 are check bits rest all bits are filled up with message bits.

Q 1001000 = m

$m + r + 1 \leq 2^r$

let

$r = 1$

$7 + 1 + 1 \leq 2^1$ ×

$r = 2$

$7 + 2 + 1 \leq 2^2$ (false)

$r = 3$

$7 + 3 + 1 \leq 2^3$ false

$r = 4$

$7 + 4 + 1 \leq 2^4 \Rightarrow 12 \leq 16$ (true)

This means we will use 4 check-bits.

$n = m + r$

$= 7 + 4$

$= 11$

Step 1

1	2	3	4	5	6	7	8	9	10	11
_	_	1	_	0	0	1	_	0	0	0
2^0	2^1		2^2				2^3			

these positions are the check bits We will not add bits in that position.

Check-bits

1 = 1, 3, 5, 7, 9, 11

2 = 2, 3, 6, 7, 10, 11

4 = 4, 5, 6, 7

8 = 8, 9, 10, 11, 12, 13, 15

Step 2

1 = 1 0 1 0 0 = 0 (use exclusive - OR)

2 = 1 0 1 0 0 = 0

4 = 0 0 1 = 1

8 = 0 0 0 = 0

Step

0	0	1	1	0	0	1	0	0	0	0
1	2	3	4	5	6	7	8	9	10	11
2^0	2^1		2^2				2^3			

0 0 1 1 0 0 1 0 0 0 0

(we have changed data in 3rd position.)

0 0 0 1 0 0 1 0 0 0 0

1 2 3 4 5 6 7 8 9 10 11

1 = 0⊕0⊕1⊕0⊕0 = 1 (using exclusive-OR)

2 = 0 0 0 1 0 0 = 1

4 1 0 0 1 = 0

8 = 0 0 0 0 = 0

C_8 C_4 C_2 C_1

0 0 1 1

= 3 (it means we have changed the 3rd bit)

→ It will only help us to detect error if only 1 bit is changed.

(CRC) Cyclic redundancy check / Polynomial code.

In this method bits are represented as polynomials.
A K-bit frame contains K terms that is the degree of the polynomial ranges from 0 to (K-1)

1 1 0 1 0

$1\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 1\cdot x^1 + 0\cdot x^0 = x^4 + x^3 + x$ vice versa

1 1 0 1 0

generated polynomial | data + redundant bits

(rest are will be 0)

Q.

x^4+x+1 | 1101 0110 11

1 0 0 1 1

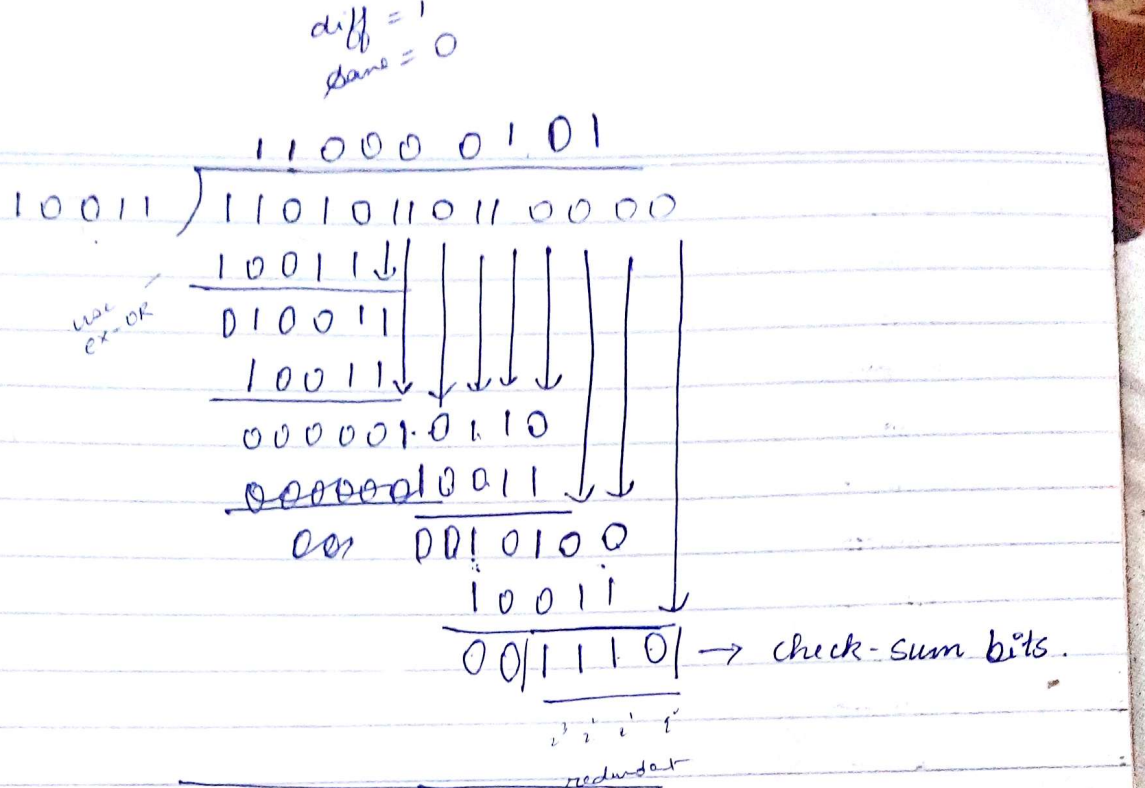
no. of redundant bits.

10011 | 1101011011 0 0 0 0 — initially we will add 0.

now to add redundant bits to data.

- highest degree of generator polynomial will be the no of redundant bits added.

here highest degree = 4 ⇒ = no. of redundant bits.



Sender : no of check bits 4-bits.
appended to the data.

$G_r(x)$ of ÷ data bits
check sum (remainder). – replace it with 0000

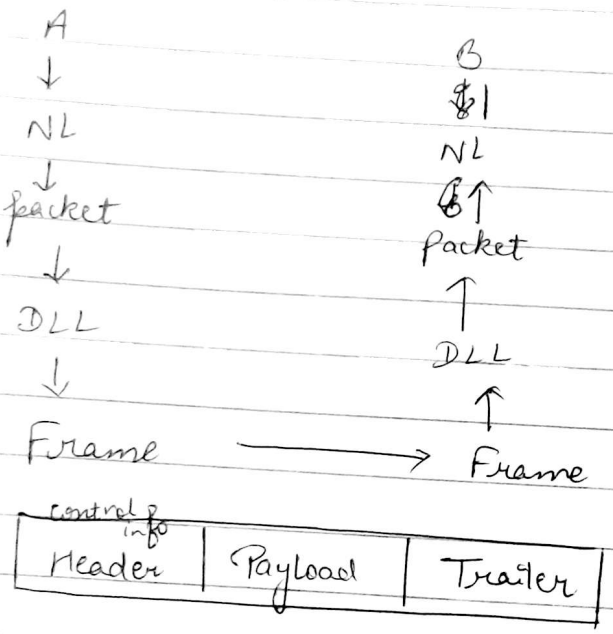
Rver updated ÷ $G_r(x)$
if remainder = 0 (OK).
run ≠ checksum (error)

3 protocols of complexity are unrestricted protocol, a simplex stop & wait protocol, a simplex protocol for noisy channel.

Assumptions
1) we assume that in the physical, DLL & are independent communicate by passing messages back & forth.

2) Machine A wants to send a long stream of data to machine B using a reliable connection oriented service.

3) Machines do not ~~crash~~ crash i.e. the protocols deals with communication errors but not with the problems caused by computer crashing or booting issues.



Protocol

- Initially receiver has nothing to do i.e. it waits for something to happen.
- Destination DLL waits for something to happen wait for event (& event)
- It returns only when something has happened (frame has arrived)
- On returning the variable event tells what has happened.
- When frame arrives, the hardware calculates the check-sum.
- If check-sum is incorrect DLL is informed with event

checksum error checksumerror.

- If checksum is correct. DLL is informed with the event frame arrived
- The data link layer then gets the next frame from physical layer using this function.

Q Why the network layer is never given any part of the frame header.

Ans
- To keep the network & DLL completely seperate
- If any changes are made in the frame format it does not require changing the network layer software. It also simplifies the software design.

Common declarations

5 data structures are defined

1) boolean
2) seq-n
3) packet (MAX_PKT)
4) Frame_kind
5) Frame.

→ Boolean is an enumerated type, can accept only true & false value

→ A seq-n is an integer value used to number the frame. Range is from (0 - MAX_SEQ)

→ A packet is the unit of information exchanged b/w the network layer & DLL

→ A frame is composed of 4 fields (kind, seq, ack, info)
control info actual data

The control fields are added to the frame header.

- kind field tells whether frame has data or only the control info.

- The sequence and acknowledgement acknowledgement fields are used for sequence nos. and ack acknowledgement.
- Acknowledgement - The info field contains (+ve or -ve or only -ve)
- ~~If~~ info fields contains the single packet.

Unrestricted simplex protocol

- The data is transmitted ~~is~~ in one direction only.
- Both transmiting and receiving network layer are ready.
- Processing time is ignored.
- Indefinite buffer space.
- Communication channel never loses the data.
- It has 2 procedures sender & receiver. Sender procedure runs on source DLL. Receiver procedure runs on destination DLL.
- No sequence no. and acknowledgement is used.
- Only event type is framearrival.
- No error and flow control.

Simplex stop & wait protocol

- Limitation on the buffer space, communication channel is error free, data traffic is simplex.
- problem to be handled - how to prevent sender from flooding the receiver with the data.
- Solution → sender insert a delay into protocol, to slow it down sufficiently to keep from swamping the receiver.
  → If the network designers calculate the worst

* behaviour of the receiver, they can program the sender to transmit so slowly that even if every frame suffers from maximum delay there will be ~~now~~ no flooding.

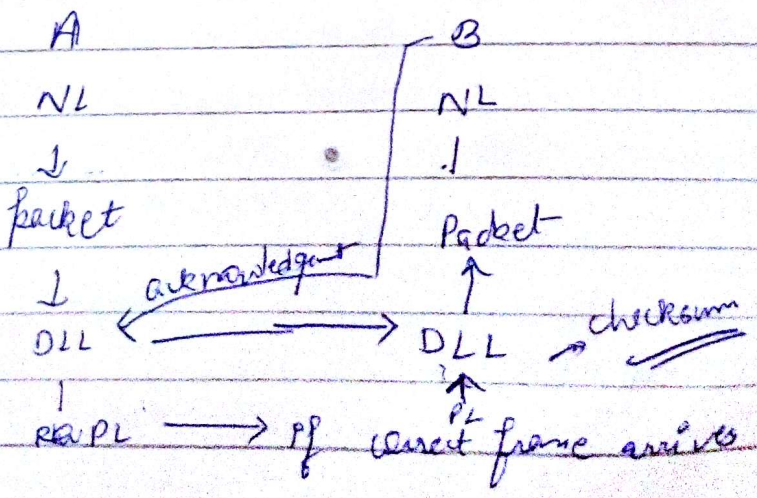
① Problem with the solution is no optimum utilisation of bandwidth. Lisa

→ Receivers send dummy frames to the sender to tell him to send the next frame.

- Protocols in which sender sends one frame and wait for acknowledgement is called stop & wait protocol.

Simplex protocol for a Noisy Channel.

- Communication channel creates errors
- Frame may be damaged or lost.
- If frame is damaged, receiver will get to know about this on checking the value of checksum.
- If the checksum bits is corrupted then this protocol fails.
- In this we use the timer
- Sender sends a frame but ~~from~~ receiver sends the acknowledgement only when frame arrive correctly.



- If acknowledgement is lost on sender side, as a result timer times out or expire. This sender assumes that frame is lost & it re-transmit it.
- Problem is duplicate frame arrives at receiver and is passed to the network layer leading to a duplicacy in a complete file.

Solution is put a sequence number in the header

Q How many bits are required for the sequence no.?

The only ambiguity in this protocol is b/w frame m and its direct successor m+1.

If frame m is lost the receiver will not acknowledge and sender will keep trying to send it again.

Once the frame arrives correctly at the receiver the receiver sends an acknowledgement to the sender.

Depending on the acknowledgement received or lost the sender sends frame m or m+1.

A one bit sequence no. 0 or 1 is therefore sufficient

When a frame containing the correct sequence no arrives it is accepted and is passed to the network layer.

Then the expected sequence no. is incremented.

Protocols in which the sender waits for a positive Prq acknowledgement before advancing to the next data item are often called PAR. (+ve ack with retramission) or ARQ (automatic repeat request).

Sliding window protocol

- Full duplex data transmission
- solution is to have 2 seperate channels, one for data and other for acknowledgement.
  Bandwidth of reverse channel is wasted.
- Better sol^n is to use the same circuit for both directions. Kind field in the header tells that a frame is a data frame or ack.
- Another sol^n is instead of sending seperate control frame receiver waits till it passes to the network layer and sends acknowledgement along the next data frame. This is called piggy backing.

- Advantage of piggy backing is better use of bandwidth.
- Ack field in header cost only few bits but separate frame needs header, ack, checksum and other control information.

Q How long the DLL waits for a packet onto which piggy back the acknowledgement.?

or

What are the complications attached to piggy backing techique?

Ans: Timer is used at the sender side. If the data link layer waits longer than the sender's time out period, the frame will be retransmitted failing the purpose of acknowledgment. The solution is DLL wait for some time if packet arrives it adds the acknowledgement to it if data does not arrive in that time then it must send a separate ack frame.

- Next 3 protocols are bidirectional and they all belongs to sliding window protocol.
  The 3 protocols differs on 3 things.
  1) Efficiency
  2) complexity
  3) buffer requirements.

missed

- Frames are send in order
- The sequence numbers in the sender window represent the frames that have been send or can be send but are not acknowledged.
- When new packet arrives it is given a sequence no. and window is advanced by 1. ~~When~~
- When acknowledgement comes, lower edge is advanced by 1
- The sender keeps all the frames in its memory because the frames may be damaged or lost therefore for the window size n, the sender needs n buffers.

- Receiver data link layer window rejects all the frames whose sequence no. are not there in its window.

1-bit sliding window protocol

→ The max window size is 1.
→ This protocol uses stop & wait until sender sends a frame and waits for the acknowledgement.
→ Only one of the DLL sends the frame and contain 2 physical layer and start timer procedure calls.
→ The starting machine ~~to~~ fetches the packet from the network layer makes the frame & transmit it.
→ When the frame arrives the receiver checks for the duplicacy. If it is the expected one it is passed to the network layer and the receiver slides up the window.

For eg: Machine A sends the frame 0 to machine B and B is trying to send fram 0 to A.
Suppose A sends the frame to B and A's timeout interval is very less. A may timeout repeatedly and sends the same frame again with sequence no. 0. When B receives a frame it is accepted and frame expected is set to 1. All subsequent or duplicate frames are rejected because B is now expecting a frame with sequence no 1.

A sends (0, 1, A0) → B gets (0, 1, A0)
B sends (0, 0, B0)

(0, 1, A0): 0 = seq no, 1 = ack no for the last frame received
(0, 0, B0): 0 = ack for A0 frame

Go back-N protocol

The problem with one-bit sliding window protocol is sender waits for acknowledgement

missed
frame 5

Network layer (Ch)

- It is responsible for sending packets from source to destination that is end to end transmission.
- NL must know about the topology of the communication channel so that it can appropriately choose the path while choosing the path it takes care to avoid over-loading

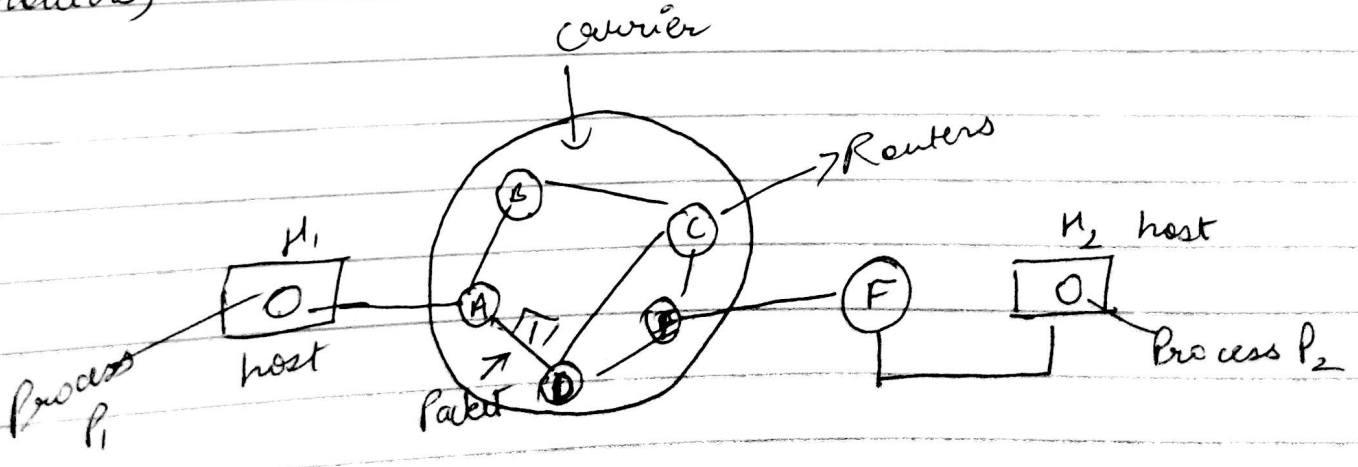
NL design issues

Some of the issues that the designer of network layer struggle with are —

1) Services provided to the transport layer and
2) Internal design of the sub-nets.

Store and forward packet switching

The major components of the system are carriers equipment (routers)



A host with a packet to send transmit it to the nearest router either on its own LAN or over point to point link over a carrier.

A packet is stored until it has fully arrived so checksum can be verified and it is forwarded to the next router. This is known as store & forward technique.

Services provided to the transport layer

Q1. what kind of services the NL provides to the transport layer

Q2. What are the goals that are kept in mind while designing NL services?

→ The services should be independent of the router technology.

→ The transport layer should be shielded from the number, type and topology of the routers present.

→ Network addresses available to the transport layer should be uniform in numbering.

- NL provides both type of services, connectionless and connection oriented.

→ In case of connectionless, the routers job is to move the packets around and nothing else. No flow control is there, no packet ordering is followed, network is considered as unreliable and do the error control & flow control with the help of packets.

SEND_PACKET
RECEIVED_PACKET] Primitives

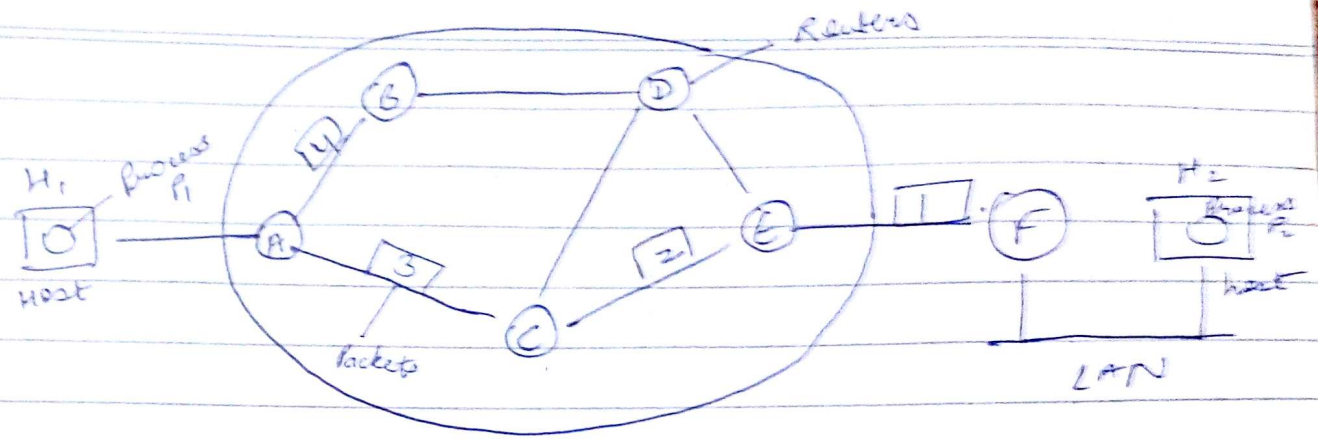
- Each packet carries the full destination address because packets are send independently of its predecessors.

→ In case of connection oriented, 1) connection is established before hand.
2) The quality of service is better mostly used in real time traffic i.e voice & video.

Implementation of connectionless service

2 different organisations are possible depending on the type of service offered.

connectionless	connection oriented
• packets are send independently • No path is setup is advance • packets in this type of network are called datagrams & the subnet is called datagram subnet.	• A path is set from source to destination router in advance This connection is known as virtual circuit & the entire subnet is known as virtual subnet.



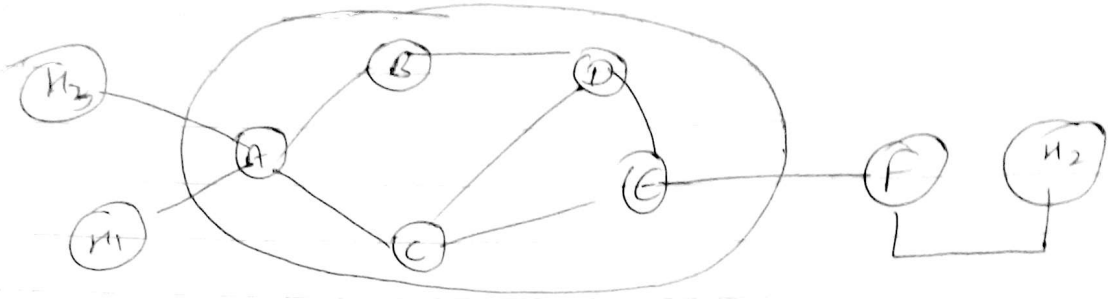
- Suppose Process P_1 has a long message for P_2. It hands it to the transport layer with the instruction to deliver it to P_2. Transport layer appends transport header and forward it to network layer

Assumption:- Msg is ~~not~~ greater than max. packet size so is divided into 4 parts.

- Every router has internal table which tells it where to send packet for each possible destination

Connection Oriented Service

- Virtual circuit is ~~to~~ established.
- It avoids to select a new root for every packet send.
- A route from source to destination is chosen and stored in the table of routers. When connection is released
- All packet follow the same route. Virtual circuit is terminated. ~~each~~
- Each packet carries an identifier telling it which virtual circuit it belongs to



A

H_1	1	C	1
H_3	1	C	2

in out

C

A	1	E	1
A	2	E	2

In out

This concept is known as label switching.

Comparison b/w ~~datagram~~ virtual circuit & datagram subnets

Issues	datagram	virtual
circuit setup	~~Circuit setup~~ circuit setup is not required	1) required in advance.
Addressing	Full source destination address is added to packet itself.	Virtual circuit identifier is added to the packet.
State info	Not required	required
Routing	do not follow the same path	routed on the same virtual circuit.
Effect of router failure	No effect on network	circuit will be terminated, communication stops.

Quality of service	difficult	better in virtual circuit, follow the same path.
Congestion control	No congestion control facility is available.	Congestion is is more. less.

Routing Algorithm

- Main fn of network layer is routing packets from source to destination.
- Packets have to travel from multiple hops.
- The algos that choose the routes and the data structures are known as routing algo.
- Routing algorithms helps in deciding which output line and incoming packet is send.
- If subnet uses datagrams then this decision is made for every packet.
- If subnet uses virtual circuit then routing decisions are made only when a new virtual circuit is being setup. This type of routing is called session routing.
- Routers have 2 processes, one of them handles each packet as it arrives looking up the outgoing line to use for it in the routing tables. This process is called forwarding process. The other process is responsible for updating and filling the entries in the router table.

- Properties of routing algorithm
  1) correctness
  2) simplicity
  3) robustness (if any failure occurs, how routes controls)
  4) stability
  5) fairness
  6) optimality.

- Routing algorithms are grouped into 2 classes — adaptive & non-adaptive.

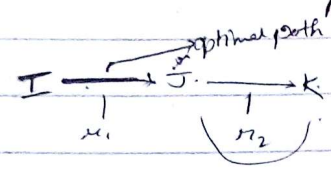
→ Non-adaptive algorithms do not base their routing algorithms on measurements ~~and~~ or estimates of the current traffic & topology. The choice of the route to use is decided in advance and is downloaded to the routers when the network is booted. This is called static routing.

→ Adaptive algorithms change their routing decisions to reflect change in ~~their~~ the topology & the traffic. Adaptive algo get their info from adjacent routers in every ∆t sec ~~step~~. The decision depends upon the distance, the no. of hops or estimated transit time etc.

Optimality principle

It states that if router J is on the optimal path from router I to router K then the optimal path from J to K also falls along the same route. Let us call the part of the route from I to J as r_1 and the rest of the route to r_2. If a route better than r_2 existed from J to K it

could be concatenated with r_1 to improve the route from I to K.



- Sink tree is a tree that shows the set of optimal routes from all sources to a given destination.

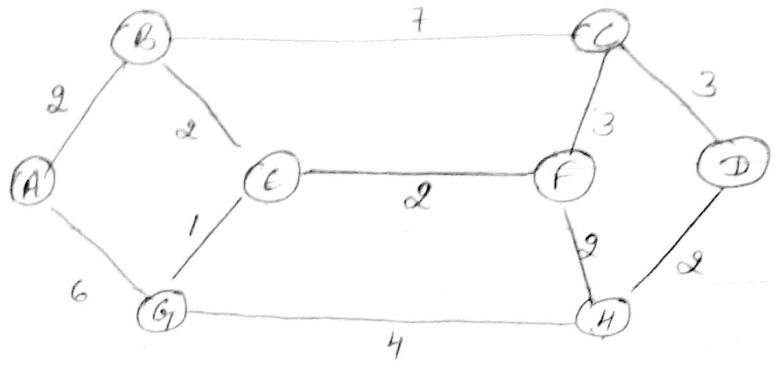
- Shortest path routing

In this, we build a graph of a subnet where each node represents a router and each connection represents. Each connection represents a comm. link. To choose a route b/w a given pair of routers the algorithm finds the shortest path b/w them on the graph.

- Labels on the arcs could be computed as a function of distance, bandwidth, avg traffic, comm. cost, length, measured delay or any other factor.

- Several algo for computing the ~~the~~ shortest paths b/w for 2 nodes ~~are there~~ of a graph are there:—

1) Dijkstra algo — In this, each node is labelled with its distance from source ~~no~~ node along best known path. Initially no paths are known so all the nodes are labelled with infinity. As the algorithm proceeds & paths are found, the labels may be changed A label may be tintative or permanent.

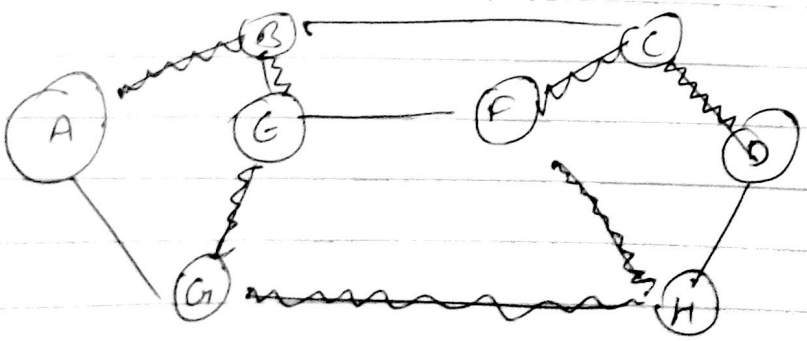


The shortest path from source A to destination D

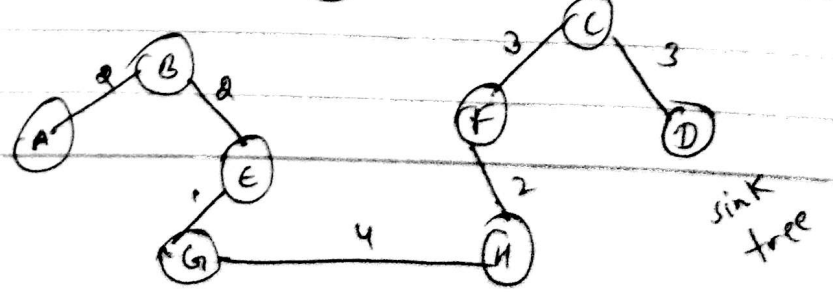
Q = { A, B, C, D, E, F, G, H }. [∞ - infinity]
0 ~~2~~ ∞ ∞ ∞ ∞ ~~9~~ ∞
2(A) 9 2
means via A

Q = { B, C, D, E, F, G, H }
0 ~~7~~ ∞ ~~4~~ ∞ 6 ∞
7(B) 4(B)

Q = { C, D, E, F, G, H }
7 ∞ 8 8 ∞ ∞



Result :-



Flooding

Every incoming packet is send to every outgoing line It generates vast no. of duplicate packets. To stop or control duplicacy we use the hop counter in the header of each packet which is decremented at each hop. The counter should be initialised to the length of the path from source to the destination.

An alternative technique for damping the flood is to keep track of which packets have been flooded, ~~so~~ to avoid sending them out for second time. To ~~achive~~ achieve this, the source router put a seq. no. in each packet it receives from its host. Each router then needs a list per source router telling which seq no originating at that source that have already been seing. If an incoming packet is on the list it is not flooded again.

To prevent the list from growing without bound, each list should be augmented by a counter K meaning that all seq. nos through K have been seen