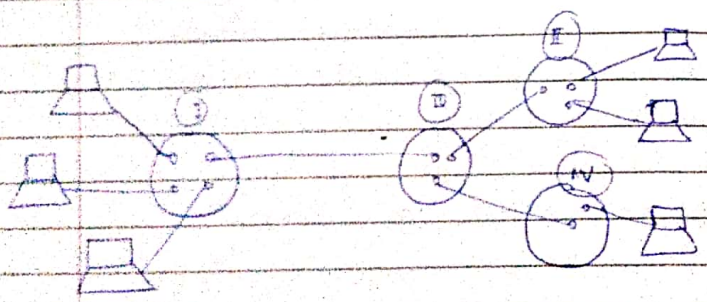
Class lecture 6

Switching Methods

- Circuit switching
- Packet switching
- Msg switching

Techniques here can determine how connections are made and how data means, hopped from source to destination.

(1) Circuit Switching



I, III, IV → switching nodes / Circuit Switches
II → Security Nodes.

Routing node must be connected to all ckt switching

→ Dedicated - 2-way communication
→ These N/w's requires setting up a connection before actual T/F of info takes place.

→ Commonly used in public N/wks

- In circuit switching routing decision is made when the path is set up
- After the T/F of info T/F link is disconnected.

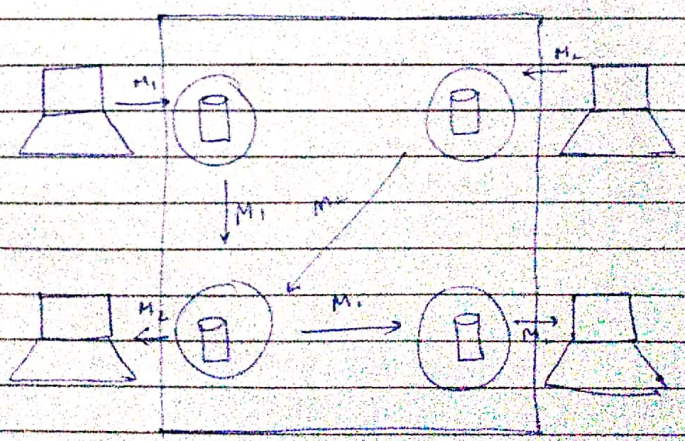
* Advantages

(1) Dedicated
(2) No Delay

* Disadvantages

(1) more B/W
(2) long time to make connection

(2) Message Switching



→ Not necessary to establish a dedicated path b/w 2 communication devices.

→ Each msg is treated as an independent unit & includes it's own destination address & source

→ intermediate nodes T/F data and ensure that msg reaches the destination.

→ intermediate device receives a msg. stores it until we next devices is ready to recieve it & then finds it to the next devices.

→ It is also called store & find n/w.

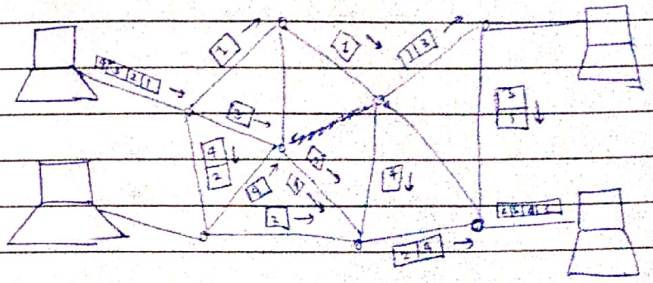
* Advantages:-

1. Channel sharing
2. Avoid congestion
3. Less Interfance
4. Reliable

Disadvantages:-

1. No dedicated links ⇒ time delay
2. costly

3. Packet Switching → Datagram
   → Packet Switching (logical connection)



Advantages:-

1. B.W is fed by splitting data into different routes.
2. If a link is broken during T, the remaining packets can be sent through another route

(a) Datagram Packet Switching

(b) Virtual Ckt Packet Switching

(1) It establishes a logical connection b/w sending and recieving devices called virtual ckt.

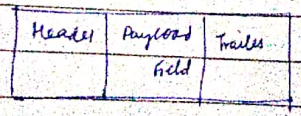
(2) Sending & Recieving devices agree upon parameters such as max. packet size & NW path to be followed.

Once this virtual ckt is estb. all packets travel through connection i.e. with the help of logical addrs, as a source & dest.

Adv in (1) BW is ↑ed

Class lecture 7

Data link layer
- Framing
- Node to Node
- Physical
- Access Control
- Flow Control
- Error Control



FRAME

DLL Design Issues
- services to DLL
- framing
- Error Control
- Flow Control

(1) Services provided to NLL

Types of services

(1) Unacknowledged connectionless service
(2) Acknowledged connectionless Services
(3) Acknowledged connection oriented

(1) Data sent from source to destination w/o having the destination m/c acknowledge them.

- no logical connection is established
- if the frame is lost due to noise or distortion, no attempt is made to detect the loss or recovers from it in DLL.
- this service is applicable when error rate is low, so that recovery is left to higher layers.
- Suitable for real time traffic such as speech.

(2) Ack. connectionless service.

no logical connection is established, but for each frame sent then receiver sends an acknowledgement if a frame is not received within specified time, sender will retransmit

Page No.
Date

Lecture 3

UNIT-II

Data Link Layer

DLL Design Issue

1. Services to DLL
2. Framing
3. Error Control
4. Flow Control

(3) Acknowledged connection oriented service

Source and destination m/c estb. a connection before T^ing the data, a counter is used to keep track of which frames have been T^ed successfully.

(i) Every phase frame are T^ed
(ii) Received frames are in same order as they were t^ed
(iii) Connection is released

(2) Framing

The raw bit stream provided by the physical layer must be broken down into discrete frames (CHKSUM) is computed for each frame which is done by DLL.

The bit stream receipt is not guranteed to be error free the no. of bits received may be equal, greater or less than the bits transmitted.

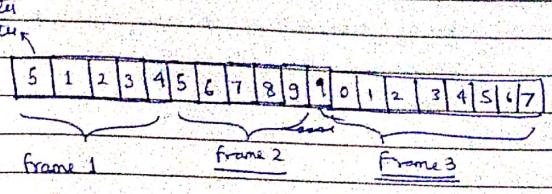
It is upto the DLL to detect & correct the errors if any. When the frame arrives at a destination CHKSUM is recomputed. If recomputed CHKSUM is diff than the one contained in the frame the DLL knows that error has occurred.

Methods of framing
1. Char. Count
2. Flag Bytes / Flag Byte Stuffing
3. Starting and Ending bytes with bit stuffing
4. Physical layer coding violations

Page No.
Date

(1) Character count.

Character Count



* Byte Stuffing :-

Each frame

* Flag Bytes with Byte Stuffing :-

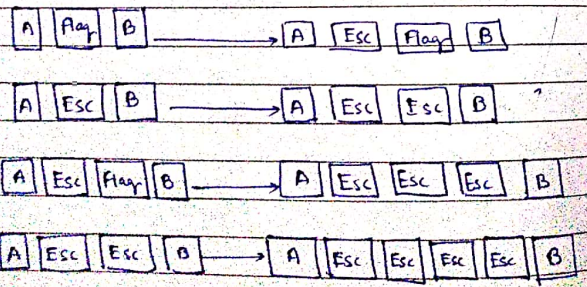
- Each frame starts and ends up to same byte but called flag byte as both starting & ending D-limiter (starting & ending of data) in this way if the received loses sync it can just search for the flag byte to find the end of the current frame.

Two consecutive flag bytes indicate end of one frame & start of the next one.

Problem: Binary data like floating point nos. are being transmitted, the flag byte e-bit pattern occurs in the data, it will interfere with frame.

Solution: Sender's data link layer inserts a special escape byte just before the flag byte in the data. The data link layer in the receiving end removes the
before the data is transferred to the N/W layer. This technique is called byte stuffing or character stuffing. Therefore we can distinguish frame in flag byte from the flag byte in the data by absence or presence of an escape byte before it.

Original Char | After Stuffing



- Disadvantage:
- Can't be used for 16 bit char. only for 8-bit char.

Bits

Here each frame begins and end with a special bit pattern 01111110. Whenever sender data link layer encounters 5 consecutive 1 in the data it automatically stuff a zero bit in the outgoing data stream. This process is called data stuff
When the receiver's data link layer encounters 5 consecutive incoming 1 bits followed by a zero bit, it automatically destuffs the zero bit.

Eg.

0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0 (original data)
0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0 (Bit-stuffed)

Method-4 Physical Layer coding

The method is applicable to the N/W in which encoding of physical medium, contains some written tendency.

For - e.g.

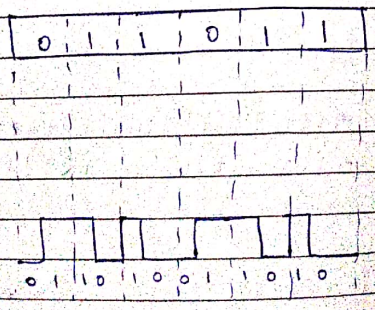
Some LANs encode 1 bit of data by using 2 physical bits.

Generally 1 Bit is the high low pair.

1 bit → high low pair (10)

0 bit → Low - high pair (01)

Manchester Encoding:-



high-high (11)

low-low (00)

are not used for the data bit are used for a timing frames in some protocols.

* Error Control

• Error Detection:

Here we check if the msg has reached the receiver or not that is to ensure reliable delivery, for that the receiver sends ~~a~~ an acknowledgement. Acknowledge

The data may be lost or the acknowledgement may be lost to, to deal with this, timers are introduced to deal into the data link layer.

• Flow Control

1. Feedback based flow control:

Receiver sends back information to the sender, giving it permission to send more data or atleast telling the sender to wait.

- Rate based Flow Control:

The protocol has built in mechanism, that limits the rate that sender may transmit the data without using any feedback from the receiver.

- Error Control

Error Detection
- Parity bit codes
- CRC (Cyclic Redundancy Check)
- Checksum

Error Correction
- Hamming Code

- Two Types of Error:-

a) Single Bit Error

b) Burst Error

Single - Bit - Error

eg 1 1 0 0 0 1 0 1 original data

1 0 1 0 0 0 1 0 1 recieved data.

Burst Bit Error:

2 or more bits are changed

eg 1 1 0 0 0 1 0 1 Hamming dist = 3

1 1 0 1 0 1 0 1 Hamming dist = 4. BE = 4.

LSB

Hamming Distance:-

- The no. of bit positions in which two corresponding bits differ is called Hamming dist.

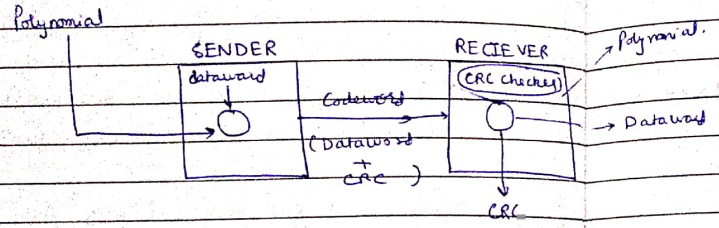
- The no. of bits from LSB to MSB in the received data code from first error bit is called length of the burst error.

Page No.
Date

Class Lecture-8

Error Detection

- PBC
  - Even PBC
  - Odd PBC
- CRC
- Check Sum



* CRC

(1) x^3+1
→ 1001
n = 3

(2) Eg. dataword → 11001010

11001011 0000 Remdr → 010 → CRC

XOR

A	B	y
0	0	0
0	1	1
1	0	1
1	1	0

Page No.
Date

Check

```
        11010000
1001 ) 11001011 0000
       1001
       ----
       1010
       1001
       ----
        0100
        0000
        ----
         1001
         1001
         ----
         0001
         0000
         ----
          0010
          0000
          ----
           0100
           0000
           ----
            1000
            1001
            ----
             0010
             0000
             ----
              010
```

(4) Codeword = Dataword + CRC

11001011 0010

10101 1000

Q. Check for the error using CRC method where your dataword

dataword = 11010

polynomial = x^4+x^2+1

Poly = $x^4 + x^2 + 1$ → 10101

$x^4 x^3 x^2 x^1 x^0$ →

Ans.

011 ×

1000 ✓

1010 ×

1101 ×

0101 ×

1111 ×

100 ×

1011 ×

```
        111 000
10101 ) 11010 1000
        10101↓
        01111
        10101 ↓
        1010 0
      - 1010 1 ↓
        000 10
        000 00 ↓
        00100
      - 00000 ↓
        01000
        00000
        1000
```

→ 4 append zeros.

Q. Find if this code have error or not?

Received codeword ⇒ 1100 1111 0010

```
        1111111
10101 ) 1100 1111 0010
        10101↓
        01100 1
          10101↓
        0110001
        - 10101↓
        0110001
        - 10101↓
        0110001
          10101↓
        0110101
          10101↓
        0101001
          10101↓
        0100101
          10101↓
        0000100
           10101↓
        0000001
```

There is error.

Page No.
Date

* Checksum

Step 1: Decompose the given dataword into groups of n bits, n is the length of the checksum.

Step 2: Perform binary addition on it, if result has a carry then add that carry with the sum and finally take 1's complement of it to produce the checksum. If no carry simply take 1's complement of the sum to produce the checksum.

Step 3: The created checksum will be appended as LSB with the dataword to produce the codeword.

eg. 01000110110001000101010100

let checksum length = 8

01000110
11000100
01010100
10101110

Page No.
Date

0 1 0 1 1 1 1 0
+ 1
0 1 0 1 1 1 1 1

1's complement → 10100000

Checksum.

Codeword = Dataword + Checksum

Reciever side

01000110
11000100
01010100
10100000
1 1 1 1 1 1 1 0

1 1 1 1 1 1 1 0
+ 1
1 1 1 1 1 1 1 1

1's comp → 00000000 → since all bits are zero ∴ answer has no error.

Page No.
Date

Note: 1. Checksum can detect all single bit error.
It can detect all burst error upto length n.

2. Burst error with length greater than n may or may not be detected.

Q. For the given dataword create a codeword using checksum technique, all check for the error at reciever's end.

dataword:- 0111 1110 1100 0111 01111100

0 1111110
1 1 0 0 0 1 1 1
+ 0 1 1 1 1 1 0 0
0 1 1 1 0 0 0 0 1
1 1 1 0 0 0 0 1 0
0 0 0 1 1 1 0 1

Hamming Codes

If dataword = m bits
then codeword = (m + r) bits

r → redundant bits

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

r → min integer value that satisfies this equation.

Q.

dataword m	redundant r	codeword (m+r)
1	2	
2	3	
3	3	
4	3	
5	4	
6	4	
7	4	
8	4	
9	4	

Q. Compute the hamming code for the given dataword = 11010101 when there is even parity using hamming code technique.

11010101 → DW

m = 8

r = 4

c = 12

$2^4 \geq$ 8

$2^0 = 1$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

1	1	0	1	r_8	0	1	0	r_4	1	r_2	r_1
12	11	10	9	8	7	6	5	4	3	2	1

	r_8	r_4	r_2	r_1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1
12	1	1	0	0
13	1	1	0	1
14	1	1	1	0
15	1	1	1	1

r_1 → 1, 3, 5, 7, 9, 11

r_2 → 2, 3, 6, 7, 10, 11

r_4 → 4, 5, 6, 7, 12

r_8 → 8, 9, 10, 11, 12

r_1 such that no. of 1 is even

r_1 → 1 3 5 7 9 11

r_1 1 0 0 1 1

$r_1 = 1$

r_2 → 2 3 6 7 10 11

r_2 1 1 0 0 1

$r_2 = 1$

r_4 → 4 5 6 7 12

r_4 0 1 0 1

0

r_8 → 8 9 10 11 12

r_8 1 0 1 1

1

Page No.
Date

Code word

1 1 0 1 1 0 1 0 0 1 1 1

12 11 10 9 8 7 6 5 4 3 2 1

let checkbit → c

C_1 → 1, 3, 5, 7, 9, 11 → 1 0 0 1 1 $C_1=0$

C_2 → 2, 3, 6, 7, 10, 11 → 1 1 1 1 0 0 1 $C_2=0$

C_4 → 4, 5, 6, 7, 12 → 0 0 1 0 1 $C_3=0$

C_8 → 8, 9, 10, 11, 12 → — 1 1 0 1 1 $C_4=0$

C_8	C_4	C_2	C_1
0	0	0	0

No error is detected

Page No.
Date

Take an eg.

C_8	C_4	C_2	C_1
0	0	1	1

= 3

↓

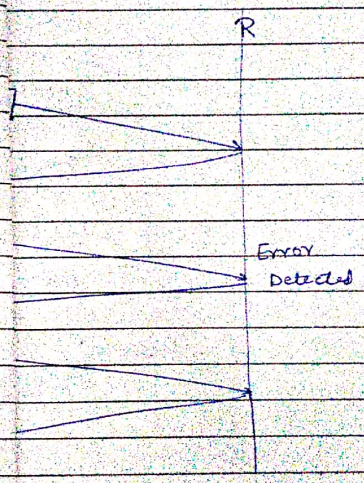
means at the 3rd part of the codeword there is an error.

Page No.
Date

Class lecture - 9

Page No.
Date

missions :-



Page No.
Date

Class lecture - 11

Medium Access Control Sublayer

→ Broadcast channels use also multi access channel or random access channel.

→ Mac sublayer consist of Access control or protocols used to determine which node, will get access to the channel when multiple nodes device share the same channel.

Channel Allocation (CA)

→ Static CA → FDM (Frequency Division multiplexing)
→ TDM (Time Division multiplexing)

→ Dynami CA → ALOHA → Pure ALOHA
→ Slotted ALOHA
→ CSMA → CSMA/CD
→ CSMA(CA)

If there are n users, the bandwidth is divided into n equal size portions, each user being assigned one portion.

Adv → Since each user has a private frequency band there is no interference b/w them.

Page No.
Date

Disadv → Out of channel portions
If more than n users want to communicate then some of them will be denied permission due to lack of bandwidth, if spectrum is cut upto n regions but number of users is less than n a large portion of valuable spectrum will be wasted

TDM (Time Division)

Each user is statically allocated every n^{th} time slot.

~~Dynamic Channel Allocation~~

Five Assumptions -

1) Station Model :- Model consists of n stations also called terminals. Once the frame is generated, station is blocked and does nothing until the frame has been successfully transmitted.

Page No.
Date

2) Singal channel for all comm.:- for transmission as well as for receiving

3) Collision assumption - If two frames are transmitted simultaneously they overlap in time and resulting signal is garbled. This is called collision. A collided frame must be retransmitted later.

4) Continous Time - frame can begin at any instant.

Slotted Time - time is divided into discrete intervals/slots & frame transmission begins at start of the slot.

5) Carrier Sense or No carrier Sense :-

Station can sense if the channel is busy before trying to use it.

* Multiple Access Protocols

1. ALOHA

a) Pure ALOHA

To avoid collision sender waits for an acknowledgement or feedback, if this feedback is not received within the allotted time then the sender waits

for a random amount of time called backoff time and resends the data.

T_f ⇒ frame time (Processing, transmission, propagation)

S → Avg no of successful transmission

- ~~Throughput~~
  → Throughput / Efficiency.

G ⇒ Avg. no. of total frames transmitted by T_f.

Vulnerable Time = 2 * T_f

→ time in which there is a possibility of collision.

- Probability that K frame are generated during a given frame time is given by poisson distribution:

$$P_1[k] = \frac{G^k e^{-G}}{k!}$$

When K=0

$P_1[0] = e^{-G}$

in an interval of vulnerable period, mean no. of frames = 2G

∴ Probability that other traffic is generated during entire vulnerable period is $P_0 = e^{-2G}$

∴ **Throughput (S) = $G e^{-2G}$**

Max throughput occurs at G = 0.5

∴ Max throughput (S_{max}) = $\frac{1}{2e} \approx 0.18$

18%

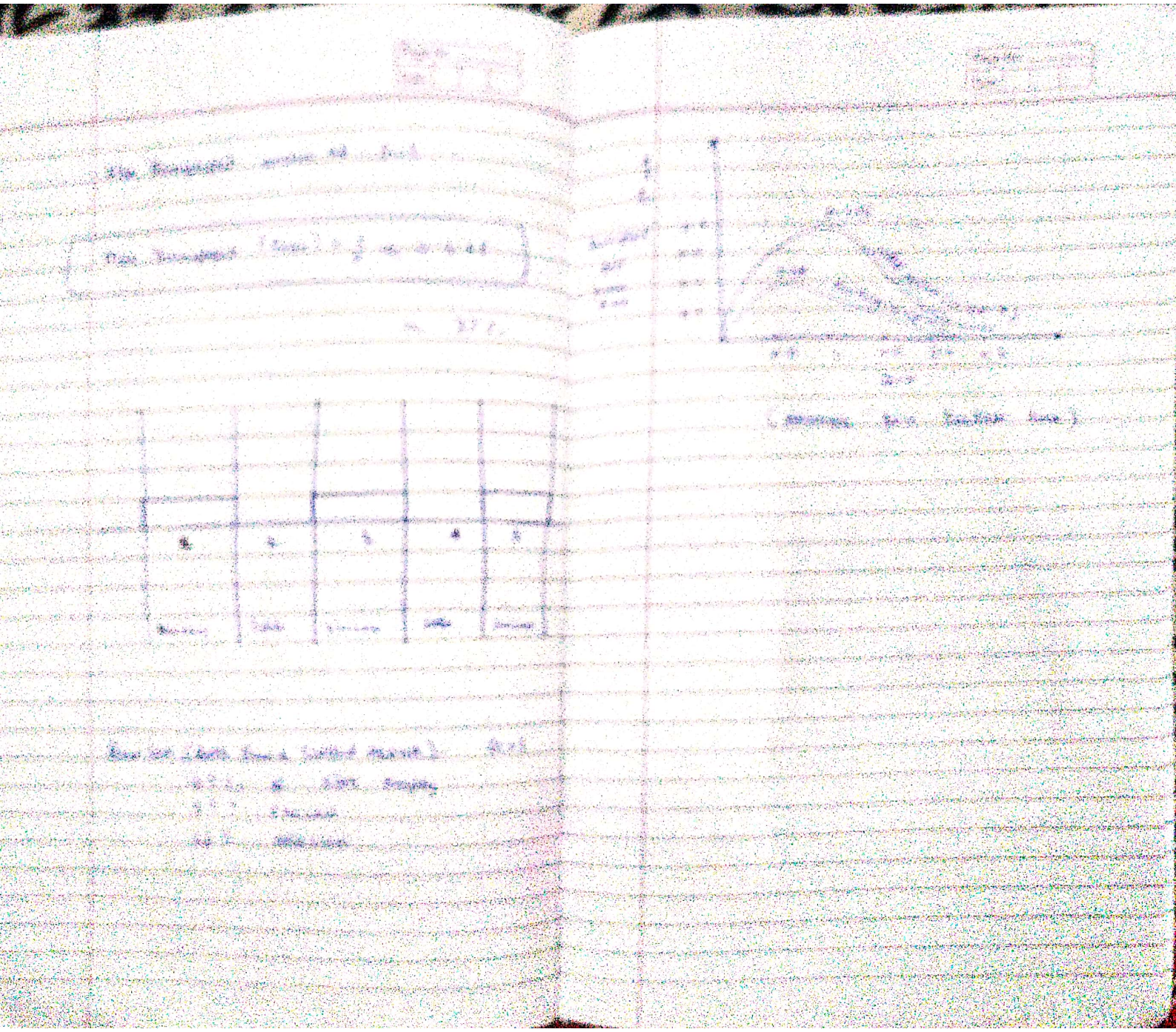
82% of channel ends up in collision

b) Slotted ALOHA

It is similar to pure ALOHA but here the time is divided into slots or time interval. In this method, If a m/c wants to transmit a data frame, it will only resend at beginning of time interval.

Throughput (S) = $G e^{-G}$

Max. Throughput occurs at G = 1

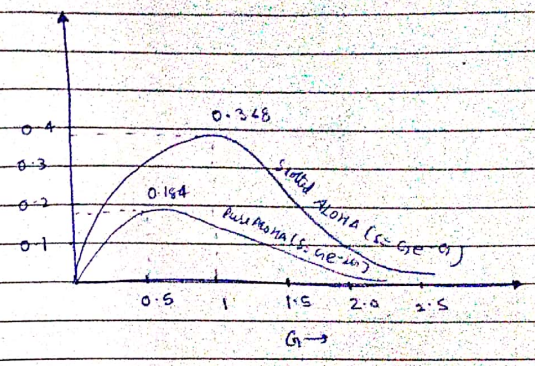


Page No.
Date

Max Throughput occurs at $G=1$

Max Throughput $(S_{max}) = \frac{1}{e} \approx 0.368$

$\approx 37\%$



(Attempts per Packet time)

1	2	3	4	5
Success	Idle	Success	Idle	Success

Best Case (Both Pure & Slotted ALOHA): $G=1$

37% of slots empty

37% success

26% collision.

Page No.
Date

UNIT - 3

Class lecture - 12

Network Layer

- Network Layer
  - Routing
  - Packets
  - End to End Communication
  - Logical Addressing
  - Congestion Control

→ In connectionless organisation data packets are called datagram.

* Routing Algorithms

- Static
  - Non-Adaptive
    - Dijkstra's Algo
    - Flooding
- Dynamic
  - Adaptive
    - Distance Vector Routing
    - Link State Routing
    - Hierarchal Routing

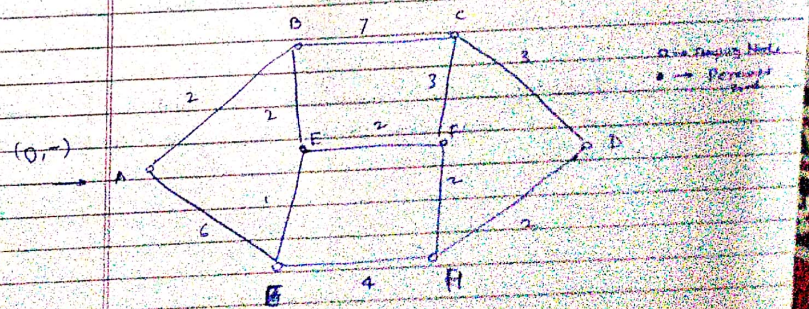
Optimality Principle - It state that if Router 'J' is on the optimal path from Router I to Router K then the optimal path from J to K also falls along the same route.

If Route I to J is r_1 & J to a is r_2. If a route better than r_2 exist from j to K, it could be concatenated with r_1 to improve the route from i to k. As statement that r_1, r_2 is optimal.

* Non-Adaptive Algo :-

a) Dijkstra Algo (shortest path algo) :

It works in two phase labelling phase and execution phase. In this algo at each node 3 fields are maintained (i) Predecessor (ii) Length



Scanned with CamScanner

A → B → I → F → H → D

min length = 10

(b) Flooding :-

In flooding every packet is sent out on every outgoing line except the one it arrived on, this generates a vast no. of duplicate packets.

Measures:

(1) Using Hop counter :- A hop counter is contained in header of each packet which is decremented at each hop, with the packet being discarded when the counter reaches zero. Ideally the hop counter should be initialised to the length of the path through the source to the destination.

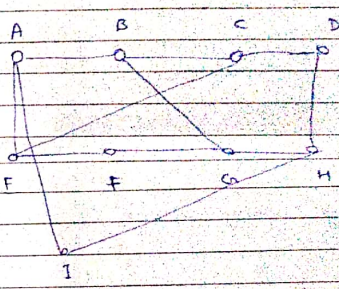
(2) To keep track of which packet have been flooded Sequence.

(3) Selected flooding : The routes do not send every incoming packet, only those lines which are going approx. on the right direction.

Adaptive Routing Algo :-

(1) Distance Vector Routing

Each router maintains a table called vector which gives the best known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbours. DVR also known as Bellman ford algo.



This table has two parts, 1st part shows preferred outgoing line to be used to reach the destination 2nd part estimated time or distance to the destination.

To	A
A	0
B	10
C	24
D	38
E	17
F	24
G	16
H	19
I	9

H
20
31
19
8
30
19
6
0
7

New estimated delay from router I

		Via
A	8	A
B	18	A
C	31	H
D		
E		
F		
G	18	H
H		
I		

IA
Delay = 8

IH
Delay = 12

Drawback:- Count to infinity problem & it's solution (Split Horizon) Algo.

- Problem
- Solution
- Other Soln

(2) Link State Routing :-

In this algorithm each router shares the information of it's neighbours to all other routers and the network using flooding algo.

Five operations performed - LSP.

(1) Each router should discover its neighbour and their network address.

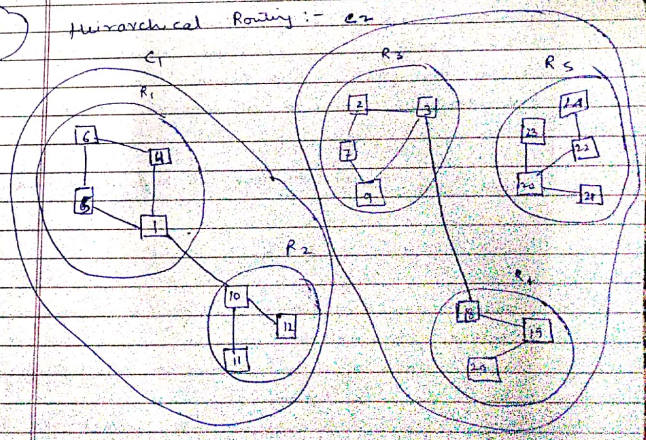
(2) Measure the delay or cost of each of it's neighbour.

(3) Construct a packet containing network address and delays of all the neighbours.

(4) Send this packet to all other routers.

(5) Compute the shortest path to every other routers.

(3) Hierarchical Routing :- eg



Page No.
Date

Country — Level 5
↓
Zones — Level 4
↓
Clusters — Level 3
↓
Regions — Level 2
↓
Routers — Level 1

* Congestion Control ~~Control~~

Principle of Congestion Control :-

Solutions of congestion problems can be divided into 2 categories open loop solution, closed loop solution.

(a) Open loop controlled is exercised by using methods such as, deciding when to accept new packets when to discard the packets, which packet are to be discarded and scheduling decisions at various points.

Draw

(b) Closed loop control : it uses some kind of feedback :-

It is based on 3 steps :-

(i) detect the congestion & locate it by ~~volunteering~~ monitoring the system.

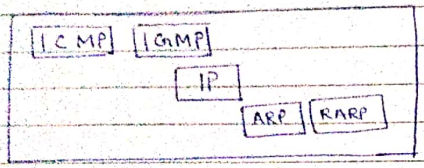
(ii) Transfer the info about congestion to places where action can be taken.

(iii) Adjust the system operation to correct the congestion.

Telco Dt.: Feb 21' 2020
Pg.:

Class lecture - 14

* Network Layer Protocol



* Address Resolution Protocol (ARP)

Sender knows the IP address of the target, internet Protocol (IP) orders ARP to create an ARP request packet or message which consists of sender's IP address or physical address and also target's IP address. This ARP packet is sent to the data link layer to be encapsulated in a frame and is broadcasted to every router and host, all the machines except the target mic drops this packet, the target mic then replys back with an ARP reply packet which contains it's physical address & is unicasted to the sender host ~~RARP~~

Telco Dt.:
Pg.:

* Reverse Address Resolution Protocol (RARP)

It maps Mac address to IP address. It allows the computer to obtain the IP address from the server when a disc less computer or workstation is booted on the network, it broadcasts a RARP request packet on the local network. for everyone to recieve, it includes it's own mac address, so the server will know where to return the reply. Server recieves the request, matches the target mac address to an IP address and then returns the IP address back to the work station.

* Internet Control Message Protocol (ICMP)

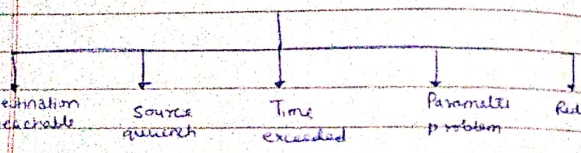
ICMP reports error and sends control msgs on behalf of IP, it simply attempts to report errors and provide feedback on specific conditions, ICMP msgs are carried as IP packets & are unreliable. Value of protocol field in IP datagram is equal to 1 to indicate that IP data is an ICMP message. Ping command uses ICMP as a pro to test whether a station is reachable, ping packages and ICMP Echo request message in a datagram and sends out to the selected destination IP address.

There are 2 types of ICMP msgs:-

(i) Error reporting msgs.
(ii) Query messages

- Error reporting msgs reports problem that a router or host encounters on parsing in receiving IP packets.

Error Reporting Msgs



(a) Destination Unreachable - When a router is unable to forward or deliver an IP packet to the destination.

(b) Source Quench - (i) It tells the source that the datagram has been discarded.
(ii) It gives warning to the source that it should slow down (quench) because congestion has taken place somewhere.

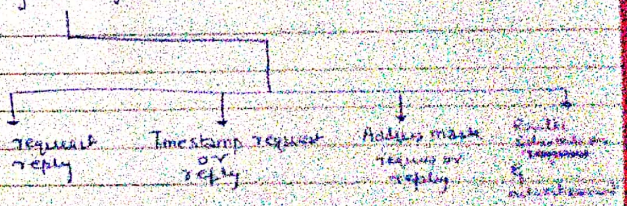
(c) Time Exceeded message - (i) If a router receives a datagram with zero in TTL (Time to live) field of the IP datagram then it discards the datagram and sends back a time exceeded msg to the source.

(ii) If all fragments do not arrive at the destination host within certain time.

(d) Parameter Problem - If a router or destination host finds any missing value or ambiguity in the datagram, then it discards it and sends a parameter problem back to the source.

(e) Redirection -

- Query messages



(a) Echo request or reply -

(b) Timestamp request or reply - It determines round-trip time needed for an IP packet to travel b/w them.

(c) Address mask request or reply - IP address of host contains network address subnet address and host ID. Host may know it's full address but may not know it's bifurcation, so it's sends an address mask request msg to the router, the router sends back the address mask reply switch.

(d) Router solicitation & Advertisement - Router can broadcast using router advertisement msg. If a host want to send data to another host or another n/w it must know the addresses of the routers connected to it's network, therefore we can use Router solicitation msg which can be broadcast or multicast.

* Internet Group Management Protocol (IGMP)

(i) It manages group membership.

(ii) It helps multicast router to create & update a list of loyal members related to each router interface.