The link state Routing Algorithm

- In link state algorithm, the network topology and all link costs are known.
- In general cost could be a function of distance bandwidth, average traffic, communication cost, mean queue length, measured delay, router processing speed etc.
- Dijkstra's Algorithm:- computes the least cost path from one node to all other nodes in the network. (single source shortest path).

  $D(v)$: cost of the least cost path from the source node to destination v

  $p(v)$: previous node along the current least cost path from the source to v.

  N' : subset of nodes v

Algo → Initialization

$N' = \{u\}$

for all nodes v

if v is a neighbour of u

$D(v) = c(u,v)$

else

$D(v) = \infty$

Scanned by CamScanner

loop

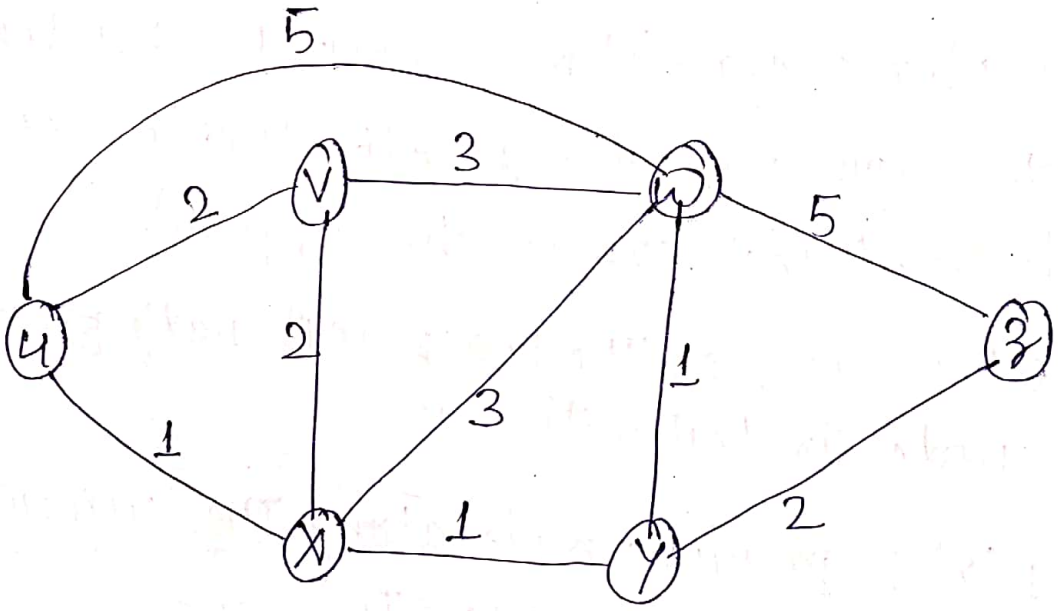
find w not in N'

add w to N'

update D(v) for each neighbour v of w and not in N'

$$D(v) = \min(D(v), D(w) + c(w,v))$$

until N'=N

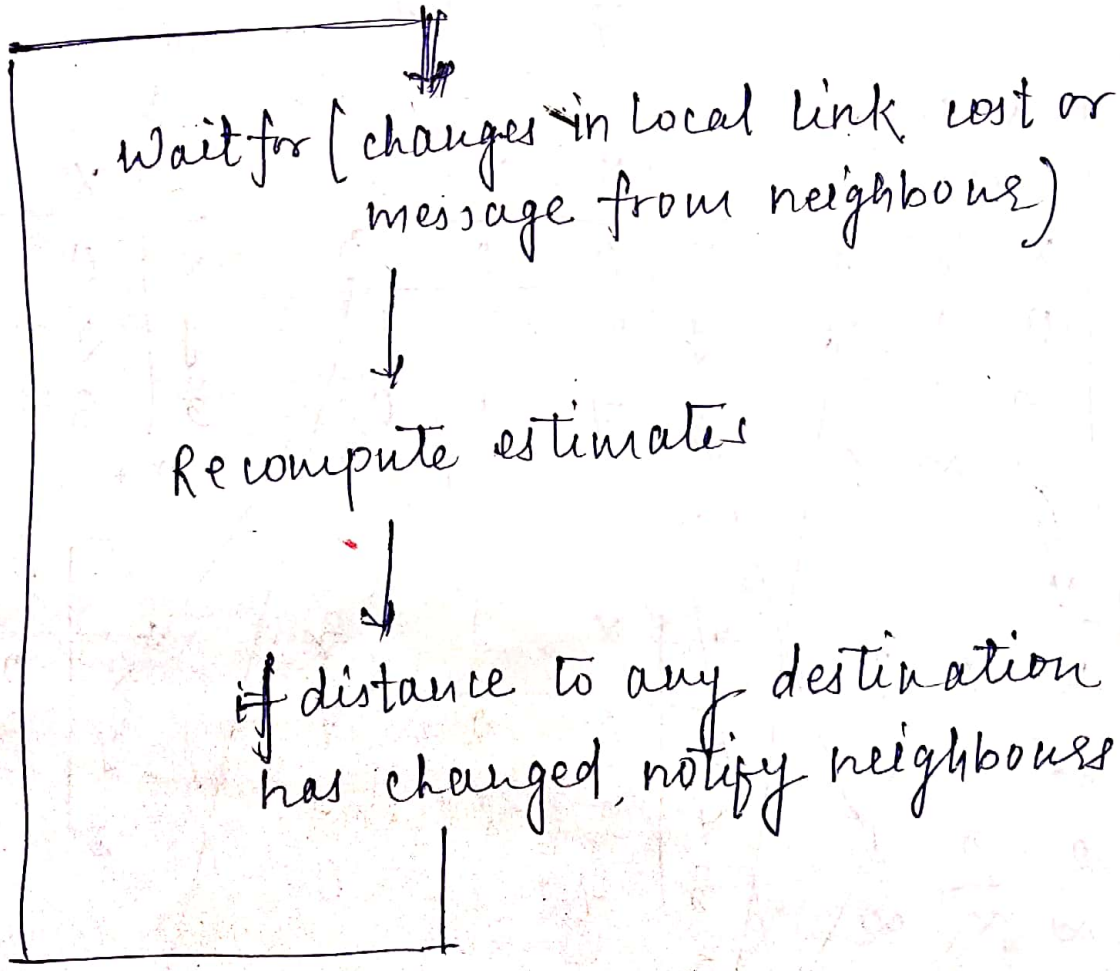


N'	D(v), p(v)	D(w), p(w)	D(x), p(x)	D(y), p(y)	D(z), p(z)
u	2, u	5, u	1, u	∞	∞
ux	2, u	4, x		2, x	∞
uxy	2, u	3, y			4, y
uxyv		3, y			4, y
uxyvw					4, y
uxyvwy					

Scanned by CamScanner

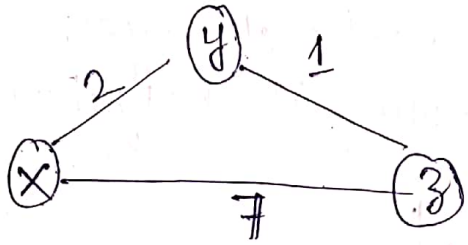
Distance Vector Algorithm

- Each node knows cost to reach each of its directly connected neighbours.
- Algorithm is iterative and asynchronous : each local iteration is caused by :-
  - local link cost change
  - Distance vector update message from neighbours.
- Distributed :- → Each node notifies neighbours only when its Distance vector changes.
  → Neighbours then notify its neighbours if necessary



Scanned by CamScanner

- $c(x,v)$ = cost of direct link from x to v
- $D_x(y)$ = estimate of least cost from x to y
- Each node v periodically sends distance vector to its neighbours:-
  → neighbours update their own distance vectors
  → $D_x(y) \leftarrow \min\{c(x,v) + D_v(y)\}$ for each node $y \in N$



Node x table

cost from \ cost to	x	y	z
x	0	2	7
y	∞	∞	∞
z	∞	∞	∞

	x	y	z
x	0	2	3
y	2	0	1
z	7	1	0

	x	y	z
x	0	2	3
y	2	0	1
z	3	0	1

Node y

	x	y	z
x	∞	∞	∞
y	2	0	1
z	∞	∞	∞

	x	y	z
x	0	2	7
y	2	0	1
z	7	1	0

	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

Node z

	x	y	z
x	∞	∞	∞
y	∞	∞	∞
z	7	1	0

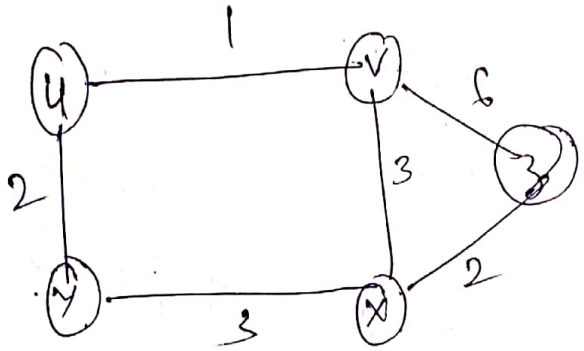
	x	y	z
x	0	2	7
y	2	0	1
z	3	1	0

	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

Scanned by CamScanner

Distance Vector routing of z

→ ~~Each node knows~~



(1)

	u	v	x	y	z
v	∞	∞	∞	∞	∞
x	∞	∞	∞	∞	∞
z	∞	6	2	∞	0

z → v → u

(2)

v	1	0	3	∞	6
x	∞	3	0	3	2
z	7	5	2	5	0

(3)

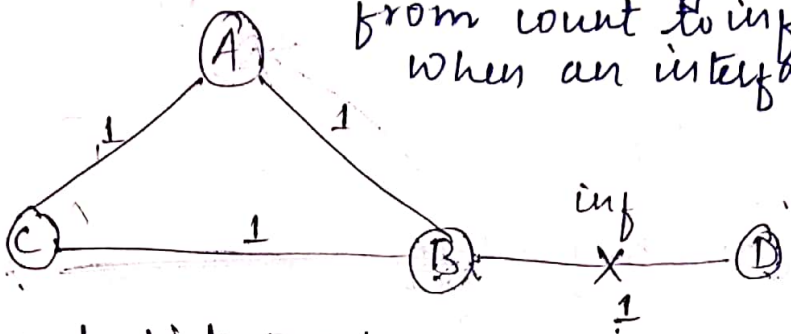
v	1	0	3	3	5
x	4	3	0	3	2
z	6	5	2	5	0

(4)

v	1	0	3	3	5
x	4	3	0	3	2
z	6	5	2	5	0

Scanned by CamScanner

Counting to Infinity :- The Bellman ford algo does not prevent ronting loops and suffers from count to infinity problem when an interface goes down.



suppose node link BD is broken and its cost is updated to infinity (∞). Now B will trigger update and update reaches to A and A update its distance vector to D as ∞. Suppose node C triggred periodic update before B reaches to C with updated cost, now as C has sent a distance reachable through B, A updates its distance vector as (3, C). Now due to A, B updates its distance vector, this process goes on until distance becomes infinity.

Distance to Node D from A, B, C

updates	A	B	C	
	2, B	1, B	2, B	(initial)
	2, B	∞, –	2, B	(Link broken)
B → A	∞, –	∞, –	2, B	
C → A	3, C	∞, –	2, B	(C send period update)
B → C	3, C	∞, –	∞, –	
A → B	3, C	4, A	∞, –	
C → A	∞, –	4, A	∞, –	

Scanned by CamScanner

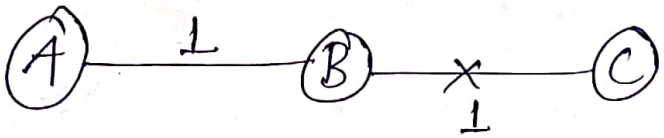
B → C	∞, –	4, A	5, B
A → B	∞, –	∞, –	5, B

until infinity

Solution :-

(1) Make infinity small
   → If we take hop count as cost, then make infinity like 16
   → It bounds the time.

(2) Split Horizon
   → Don't send routes I learn from a neighbour back to it.



Here A learns about C from B, so it does not send it distance vector of C to B.

(3) Poison reverse –
   → send the information to node through which it has learnt but make it ∞.
   e.g. A sends distance vector (∞, c) to B.

Scanned by CamScanner

Poison Reverse example :-

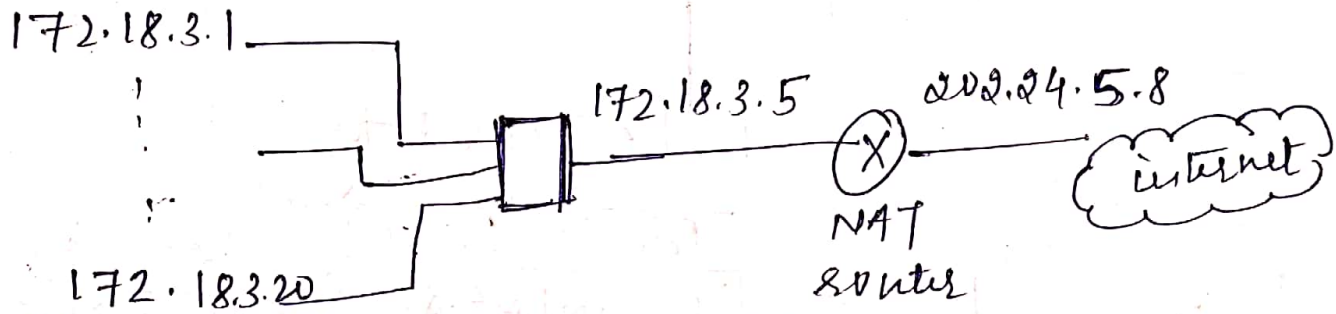
	A	B	C	
	2, B	1, B	2, B	(initial)
	2, B	∞, -	2, B	(link broken)
B → A	∞, -	∞, -	2, B	
C → A	3, C	∞, -	2, B	(C send periodic update)
B → C	3, C	∞, -	∞, -	
A → B	3, C	∞, -	∞, -	(A sent ∞ to B because it learnt from B)
C → A	∞, -	∞, -	∞, -	

Hence the count to infinity problem can be resolved through poison reverse.

Scanned by CamScanner

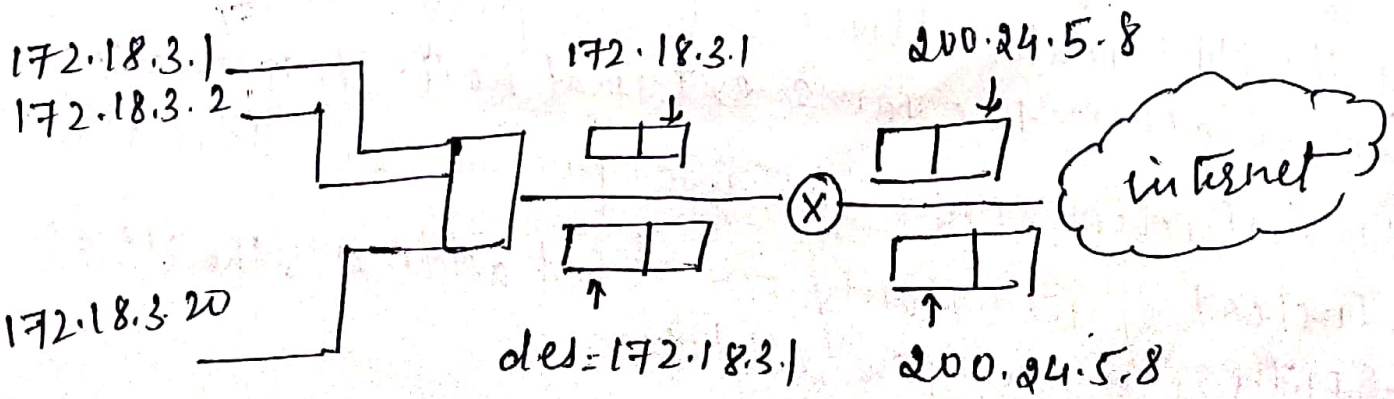
NAT (Network Address Translation)

A technology that can provide the mapping between the private and universal addresses, is network address translation. The technology allows a site to use a set of private addresses for internal communication and set of global internet addresses for communication with the rest of the world.



Address Translation –

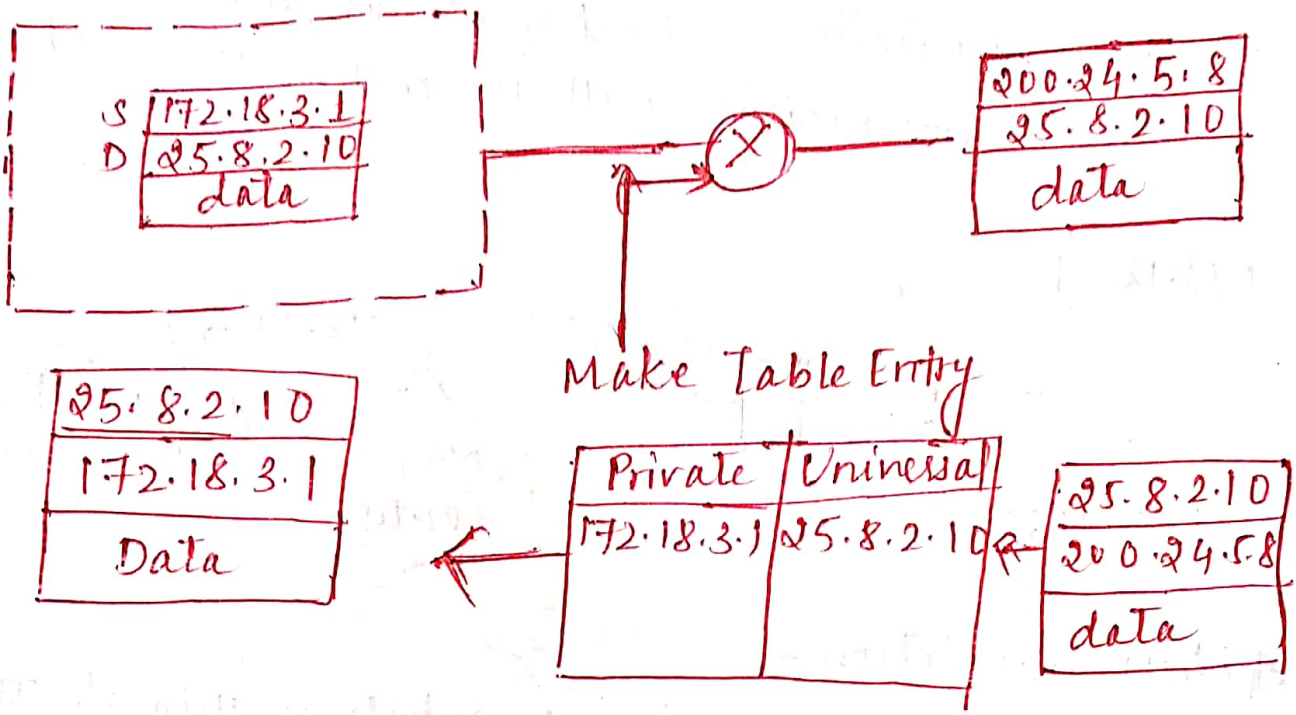
All of the outgoing packets go through the NAT router, which replaces the source address in the packet with global NAT address. All incoming packets also pass through the NAT router which replaces the destination address in the packet with appropriate private address.



Scanned by CamScanner

Translation table:- NAT router has translation table.

Using one IP address:- table contains two column the private address and external address.



In this strategy communication always be initiated by the private network. A private network can't run a server Program for clients outside of its network if it is using NAT technology.

Using a Pool of IP addresses:- Using only one global address by the NAT router allows only one private network host to access the same external host. To remove this restriction NAT can use pool of IP addresses.

e.g. Instead of using only one global address, the NAT router can use four addresses.

Scanned by CamScanner

Data link layer

* Over a given link, a transmitting node encapsulate the datagram in a link layer frame and transmits the frames into the link.

* The services Provided by the link layer

(i) Framing – Link layer protocol encapsulate each network layer datagram within a link layer frame before transmission oves the link.

(ii) Link access – A medium access ~~pro~~ control (MAC) protocol specifies the rules by which a frame is transmitted onto the link. (CSMA)

(iii) Reliable delivery: It guarantees to move each network layer datagram across the link without error.

(iv) Error detection and Error correction;- Bit error are introduced by signal attenuation and electro magnetic noise. Link layer protocol provide a mechanism to detect bit error.

* Where is link layer implemented

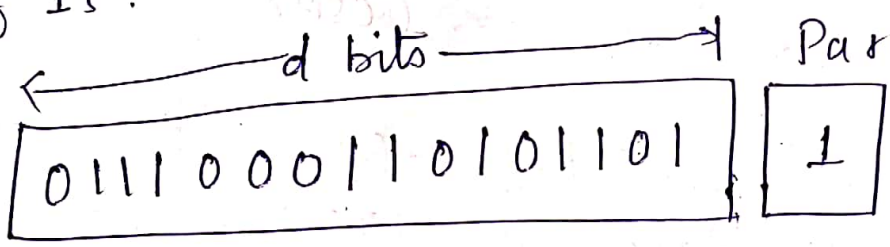
For Host → Network interface card / Network adapter

Scanned by CamScanner

Error Detection and correction Techniques

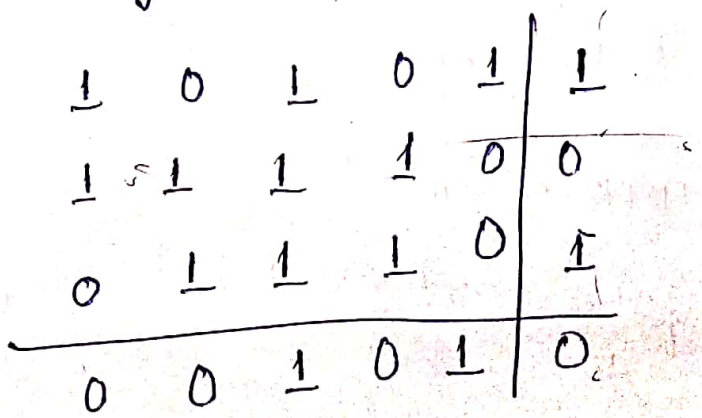
(1) Parity checks

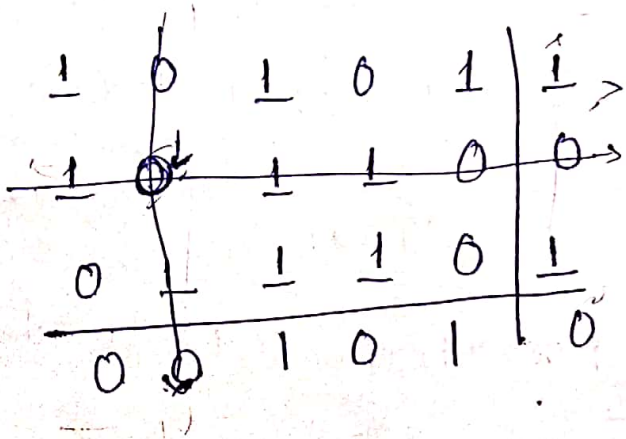
* In simple form there is an extra parity bit
* In an even parity scheme, the sender simply include one additional bit and chooses its value such that Total number of 1s in d+1 bits is even.
* For odd parity scheme, the parity bit value is chosen such that there is an odd number of 1s.



* It is not useful when even number of bit error occurs.

→ Parity Correction:-





Scanned by CamScanner

"Checksum" Methods

In this technique, the d bits of data are treated as sequence of k bits. Internet checksum is based on this approach - bytes of data are treated as 16 bit integer and summed. The 1's complement of this sum then forms the internet checksum that is carried in the segment header.

Data To be sent

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

For convenience let us divide this data To be 4 bits segment. Perform one's complement Addition

```
  1 0 1 1
  0 0 1 1
---------
  1 1 1 0
+ 1 0 1 0
---------
 [1] 1 0 0 0
     ↓ 1
---------
  1 0 0 1
  1 0 1 1
---------
 [1] 0 1 0 0
     → 1
---------
  0 1 0 1   → One's complement = 1010
```

Scanned by CamScanner

Now receiver side data will be

1011 0011 1010 1011 1010

Perform same addition as sender:-

```
 1 0 1 1
 0 0 1 1
---------
 1 1 1 0
 1 0 1 0
---------
 1 0 0 0
       1
---------
 1 0 0 1
 1 0 1 1
---------
 0 1 0 0
       1
---------
 0 1 0 1
```

→ Now add checksum value of it:-

```
 0 1 0 1
 1 0 1 0
---------
 1 1 1 1
```

→ Result is all 1 which is correct now packet is accepted and without error.

Scanned by CamScanner

Cyclic Redundancy check (CRC)

- CRC codes are known as polynomial codes.
- At first the sender and receiver must agree on r+1 bit pattern, known as generator.

(a)

Generator = $x^3 + 1$

binary = $x^3\ x^2\ x^1\ x^0$

= 1 0 0 1

Message = 1 0 1 1 1 0

Append highest degree of polynomial (3) numbers of 0's as in message and perform division with XOR operation

```
                1 0 1 0 1 1
          ┌──────────────────
1 0 0 1 ) 1 0 1 1 1 0 0 0 0
          1 0 0 1
          ---------
            0 0 1 0 1 0
              0 1 0 0 1
              ---------
                1 1 0 0
                1 0 0 1
                -------
                  1 0 1 0
                  1 0 0 1
                  -------
                    0 1 1   → CRC
```

Scanned by CamScanner

At receiver side append CRC to message and perform same calculation

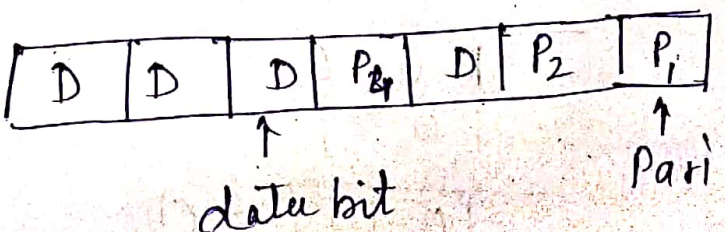
Message = 1 0 1 1 1 0 0 1 1

```
          1 0 1 0 1 1
        ---------------
1 0 0 1 | 1 0 1 1 1 0 0 1 1
          1 0 0 1
          -------
            1 0 1 0
            1 0 0 1
            -------
              1 1 0 1
              1 0 0 1
              -------
                1 0 0 1
                1 0 0 1
                -------
                    0
```

No error

Hamming Code

* It only detects single bit error.
* Parity bits are added in data bits at places like 2^n where $n >= 0$



Scanned by CamScanner

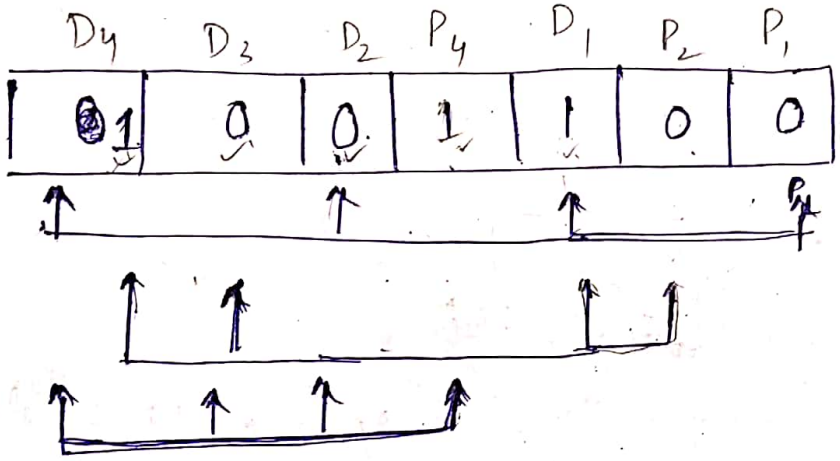
Data = 1 0 0 | default even

- we are using even parity.
- To fill the parity bit :-

P_1 → take 1, leave 1

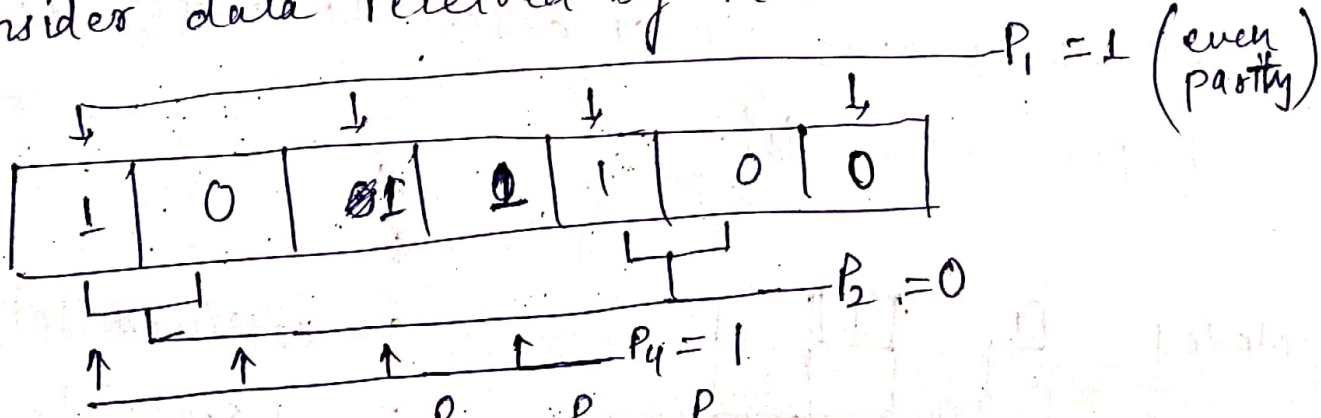
P_2 → take 2, leave 2

P_4 → take 4, leave 4



Receiver side → check parity for P_1, P_2, P_4.

Consider data received by receiver.



P_4	P_2	P_1
1	0	1

= 5th position there is a bit error

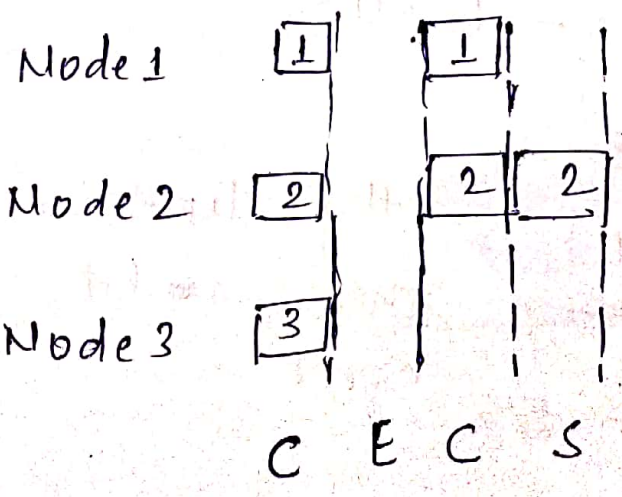
Scanned by CamScanner

Random Access Protocol

- A transmitting node always transmits at full rate of channel. When there is a collision each node involved in collision repeatedly retransmits its frame. When a node experiences a collision, it ~~does~~ waits a random delay before retransmitting the frame.

Slotted Aloha

- Simplest random access protocol
- All frames consist of L bits
- Time is divided into slots of L/R seconds.
- Nodes start to transmit frames only at the begining.
- If two or more frames collide in a slot, then all the ~~transmit~~ nodes detect the collision event before end of slot.



C = collision slot
E = Empty slot
S = succeful slot

Scanned by CamScanner

Efficiency of slotted Aloha

Let each node attempts to transmit a frame in each slot with probability p. Suppose there are N nodes.

Probability a given node is successfully transmitting

$= p(1-p)^{N-1}$

there are total N nodes so any node can transmit frame

$$\boxed{\eta = NP(1-p)^{N-1}}$$

Maximum efficiency of slotted aloha

$$\eta = NP(1-p)^{N-1}$$

$$\frac{d\eta}{dp} = N\left[(1-p)^{N-1}\frac{dp}{dp} + p\frac{d}{dp}(1-p)^{N-1}\right]$$

$$\frac{d\eta}{dp} = N\left[(1-p)^{N-1} - p(N-1)(1-p)^{N-2}\right]$$

For max efficiency $\frac{d\eta}{dp} = 0$

$$0 = N\left[(1-p)^{N-1} - p(N-1)(1-p)^{N-2}\right]$$

$$p(N-1)(1-p)^{N-2} = (1-p)^{N-1}$$

$$p(N-1) = \frac{(1-p)^{N-1}}{(1-p)^{N-2}}$$

Scanned by CamScanner

$$P(N-1) = (1-p)^{N-1-N+2}$$

$$PN - p = 1 - p$$

$$p = 1/N$$ we have max efficiency when $p = 1/N$.

put $p = 1/N$

$$\eta_{max} = N \cdot \frac{1}{N}\left(1 - 1/N\right)^{N-1}$$

$$= \frac{\left(1 - 1/N\right)^{N}}{1 - 1/N}$$

since $\lim_{N\to\infty} \left(1 - \frac{1}{N}\right) = 1$

then

$$\lim_{N\to\infty} \left(1 - 1/N\right)^{N} = 1/e$$

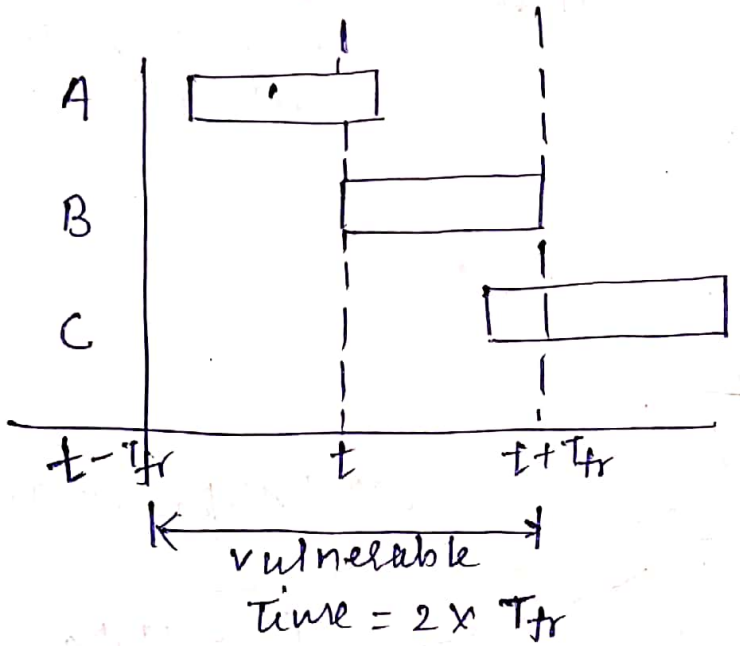
$$\eta_{max} = 1/e = 0.37$$

When a large numbes of nodes have many frames To transmit, then only 37% slots do useful work.

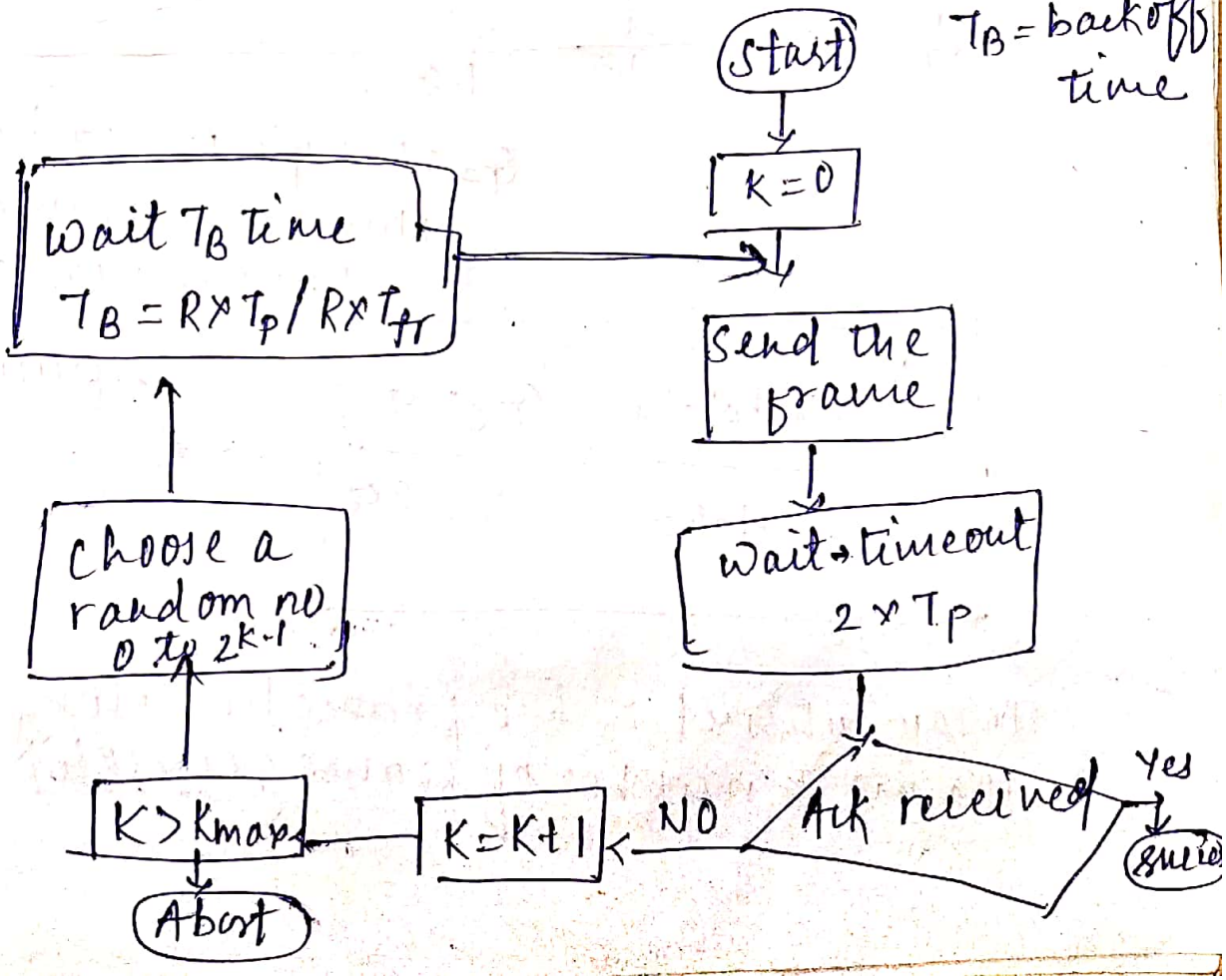
Scanned by CamScanner

Pure Aloha

* Pure Aloha permits user to transmit frame any time they like.
* Whenever two or more frames try to occupy the channel at the same time, there will be collision.



K = Numbers of attempts
T_p = Maximum Propo. gatio time
T_{fr} = Avg. transmission time for frame
T_B = back off time



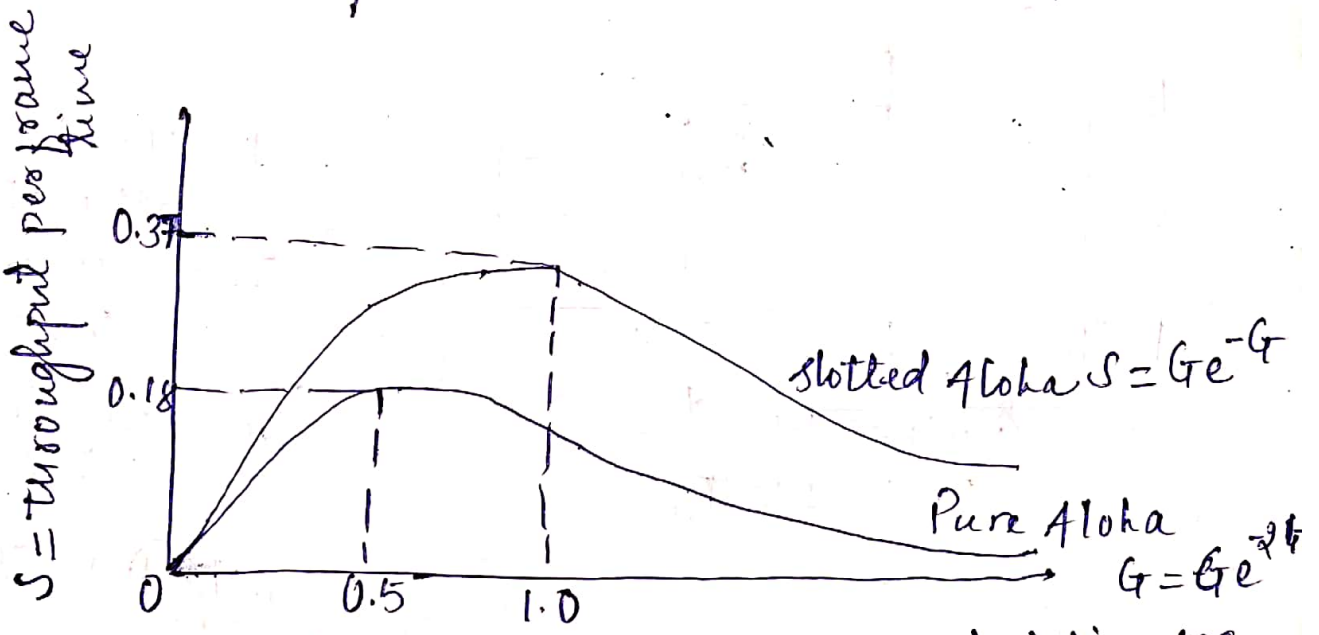
Scanned by CamScanner

throughput or efficiency of pure Aloha

$$\eta = NP(1-P)^{2(N-1)}$$

$$\eta_{max} = \frac{1}{2e}$$

(Homework) → Use derivation steps of slotted Aloha



G = attempts per packet time or Numbes of frame per transmission Time

(efficiency = S)

$$S_{slotted\ aloha} = Ge^{-G}$$

$$S_{pure\ aloha} = Ge^{-2G}$$

In an interval of two frame times long the mean numbes of frame generated is 2G.

Scanned by CamScanner

(Q) Consider a system generating 20 bit frames and connected through a shared 20 kbps channel. Find throughput in percent if slotted Aloha is used and frames rate is 1000 fps.

Ans Frame size = 20 bits

Bandwidth $R = 20$ kbps

Transmission time $T = \frac{L}{R} = \frac{20}{20 \times 10^3} = 10^{-3}$

Throughput $S = Ge^{-G}$

= Number of frames / T

$G = 1000 * 10^{-3} = 1$

$S = e^{-1} = 0.368 = \underline{36.8\%}$

Scanned by CamScanner

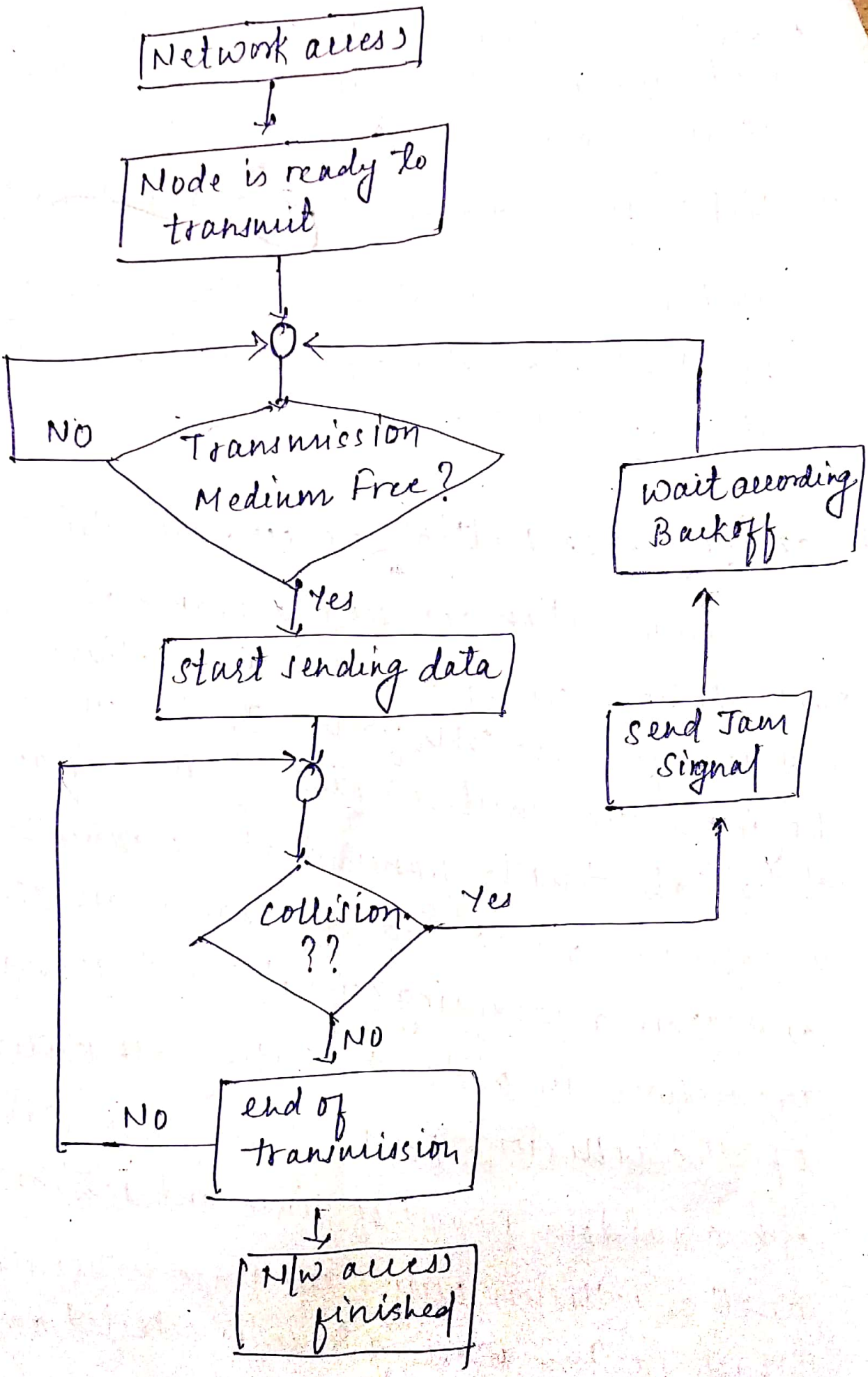
Carrier Sense Multiple Access (CSMA)

- In slotted Aloha, a node's decision to transmit is made independently of the activity of other nodes, thus generating collision.
- Listen first to make sure channel is idle.
- end to end channel propogation delay of a broadcast channel plays a crucial role in determining its performance.

- Carrier Sense Multiple Access with collision detection

Any station can send a frame at any time. Each station senses wheather the medium is idle and therefore available for use. If it is, the station begins to transmit its first frame. If another station also tries to transmit at the same time, a collision occurs and the frames are discarded and then a jamming signal is sent throughout the network in order to notify all stations of the collision. Each station then waits for a random period of time and retries. If another collision occurs, the time intervals from which random waiting time is selected are increased step by step. This is known as exponential backoff.

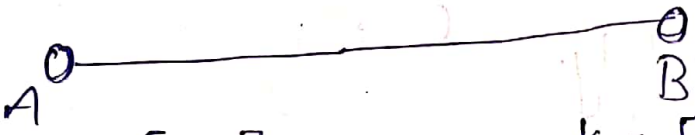
Scanned by CamScanner



Scanned by CamScanner

Binery Exponential Algorithm

* It is collision resolution mechanism used in random access protocol. This algorithm is used in Ethernet.
* If there is a collision, a node chooses the value of k at random from $\{0, 1, 2 \ldots 2^n - 1\}$
* For Ethernet, the actual amount of time node waits for is k. 512 bit times or k. 5.12 μs.
* For Ethernet max number of collision is 10.



First collision k = [0, 1]
Second collision k = [0, 1, 2, 3]

k = [0, 1]
k = [0, 1, 2, 3]

Efficiency of CSMA/CD

$$\eta_{CSMA/CD} = \frac{1}{1 + \frac{6.d_{prop}}{d_{trans}}}$$

Scanned by CamScanner

(Q) Let A and B be two stations attempting to transmit on Ethernet. Suppose A and B simultaneously attempt to send frame 1, collide and happen to chose backoff times 0XT and 1XT respectively meaning A wins the race and transmits its first frame.

(a) Give the probability that A wins his second backoff race immediately after first collision.

(b) Suppose A wins his second backoff race what is the probability A wins his third backoff race immediately.

Ans (a) For the second backoff race, A picks $k_A(2)$ to be from [0, 1], B picks $k_B(2)$ from [0, 1, 2, 3]. A wins backoff race if $k_A(2) < k_B(2)$.

value of k selected by A	value of k selected by B	winner
0	0	X
0	1	A
0	2	A
0	3	A
1	0	B
1	1	X
1	2	A
1	3	A

Scanned by CamScanner

A has 5 chances to win out of 8.
A wins the second backoff race = 5/8 = 0.625

Ans (b) In this case A picks from [0,1] & B picks from [0,1,2,3,4,5,6,7]

Repeat above procedure

P[A wins] = 13/16

* There are several Types of CSMA protocol:-
  - 1-persistent CSMA
  - P-persistent CSMA

1-persistent CSMA

- Sense the channel
  → If busy, keep listening to the channel and transmit immediately when the channel becomes idle.
  → If idle, transmit a packet immediately.
- If collision occurs:-
  → wait a random amount of time and start over again.

* The protocol is called 1-persistent because the host transmits with a probability of 1, whenever it finds the channel idle.

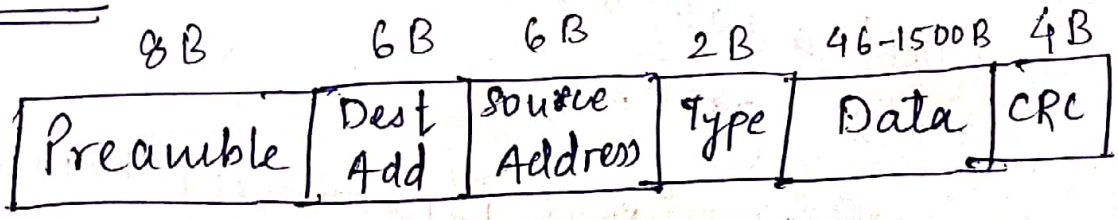
Scanned by CamScanner

P- persistent CSMA

- Optimal strategy - use P-persistent CSMA
- Assume channel are slotted.
- one slot = contention period (one round trip propogation delay)

1. Sense the channel
   - If channel is idle, transmit a packet with probability P.
     - → If a packet was transmitted, go to step 2.
     - → If a packet was not transmitted, wait one slot and goto step 1.
   - If channel is busy, wait one slot and goto step 1.
2. Detect collision
   - If a collision occurs, wait a random amount of time and goto step 1.

Ethernet



Scanned by CamScanner

Preamble (8 bytes):- Each of the first 7 bytes of Preamble has a value of 10101010, the last bytes is 10101011. The first 7 bytes of the preamble serve to wake up the receiving adapter and to synchronize their clocks to that of sender's clock. The last 2 bit alert adapter B that important stuff is coming.

Destination Address (6 bytes):- This field contains the MAC address of the destination

source address - This field contains the MAC address of the sender.

Type field : The host can use other network layer protocol besides IP (Novell IPX, AppleTalk). Each protocol has their type numbers.

Cyclic redundancy check (CRC) - detect bit error in frames.

Data field (46 to 1500 bytes) - The minimum size of data field is 46 bytes.

* An Ethernet device will detect a collision, while it is transmitting, only if the collision reaches it before it completes transmits the entire frame. If the collision reaches the transmitter, after it completed sending the entire frame, then the transmitter will

Scanned by CamScanner

not detect the collision; it will assume the collision occured because of some other frame. (Next Page)

(a) Suppose node A and B are on the same 10 Mbps Ethernet segment, and the propagation delay between the two nodes is 225 bit times. Suppose node A begins transmitting a frame, and before it finishes station B begins transmitting a frame. Can A finish transmitting before it detects B has transmitted? Why or why not?

Soln → At $t = 0$, A start transmitting.
At $t = 576$ bit time, A would finish transmitting.

In worst case B begins transmitting at $t = 224$.

so at worst case $t = 224 + 225 = 449$, B's first bit arrives at A.

Because $449 < 576$, A detects collision has occured and it should abort the transmission.

(a) Suppose node A & B are on the same 10 Mbps broadcast channel, and the propogation delay between the two node is 325 bit time. Suppose CSMA/CD and Ethernet packet are used for this broadcast channel. Suppose node A begins transmitting a frame and before it finishes node B begins transmitting a frame. Can A finish transmitting before it detects that B has transmitted

(Same Work)

Scanned by CamScanner

conversion of bit time into seconds :-

$$= \frac{\text{bit time}}{BW}$$

$$= \frac{512}{10 \times 10^6}$$

$$= 51.2\ \mu s$$

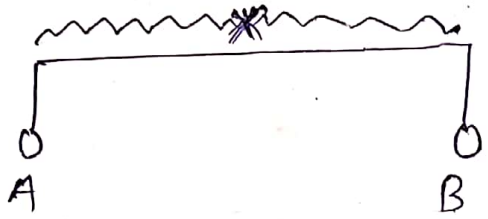
$$\boxed{\text{bits} = t_p(s) \times BW}$$

[The propogation delay in bits is the amount of data transmitted by the sender in time t_p]

[for 10 Mbps Ethernet]

[512 bit is minimum frame size of Ethernet excluding Preamble]

Q (cont)



For detecting collision

$T_t > T_p$ (T_t = Transmission Time, T_p = Propogation Time)

in worst case :-

$$\boxed{T_t \geq 2 * T_p}$$

For ethernet $\boxed{T_t = 2 * T_p}$

For $2 * T_p$, how much data I should have, this is called minimum frame size.

$$T_t \geq 2 * T_p$$

$$L/B \geq 2 * T_p$$

$$\boxed{L \geq 2 * T_p * B}$$

Scanned by CamScanner

If propogation delay in a CSMA/CD network is 500 bit times, what is the slot time if Jamming signal is 50 bits?, BW = 10 Mbps

→ $T_{prop} = \frac{500}{10 \times 10^6} = 50\mu s$

→ Jamming signal $= \frac{50}{10 \times 10^6} = 5\mu s$

Slot time = 2 × Propogation time + Trans for jamming signal

$= 2 \times 50 + 5$

$= 100 + 5 = \underline{105\mu s}$

Suppose that nodes A & B are attached to the opposite ends of a 900 m Ethernet cable and that they have one 1000 bit frame to send to each other. Suppose that there are 4 repeaters between A & B each inserting 30 bit delay. Transmission Rate is 10 Mbps. Assume that CSMA/CD with backoff interval of multiple of 512 bits used. Assume that there is a collision when both A & B transmit this packet simultaneously at $t = 0$. After collision, A draws $K=0$ whereas B draws $K=1$. Ignore Jam signal delay.

Scanned by CamScanner

a. What is the one way propagation delay. Assume the signal propagation speed is 2×10^8 m/s.

Soln –

$$\frac{900}{2 \times 10^8} + 4 \cdot \frac{20}{10 \times 10^6}$$

$$= (4.5 \times 10^{-6} + 8 \times 10^{-6})$$

$$= 12.5 \mu s$$

b. At what time is A's packet completely delivered at B.

Soln At $t = 0$, both A & B transmit

At $t = 12.5 \mu s$, A detects collision

At $t = 25 \mu s$, last bit B aborted transmission arrives at A.

since A draws $K = 0$ in backoff algo it can instantly start the retransmission at time $t = 25 \mu s$.

At $t = 37.5 \mu s$ first bit of A transmission arrives at B. This time is smaller than 512 bit time. B has to wait for backoff, Hence B does not start transmission since it detects A's transmission

At $t = 37.5 \mu s + \frac{1000}{10 \times 10^6} = 137.5 \mu s$

A's packet completely delivered at B.

Scanned by CamScanner

Now suppose that only A has a packet to send and that the repeaters are replaced with bridges. Suppose that each bridges has a 20 bit processing delay in addition to store and forward delay. At what time in second is A's packet delived at B?

Ans → Bridges introduce additional 1000 bit store and forward delay & 20 bit processing delay.

Total delay by bridges:-

$$= \frac{4(1000+20)}{10\times10^6}$$

$$= \frac{4080}{10\times10^6} = 408\ \mu s$$

A's packet reaches at B = 408 + 100 + 4.5

$$= 512.5\ \mu s$$

led

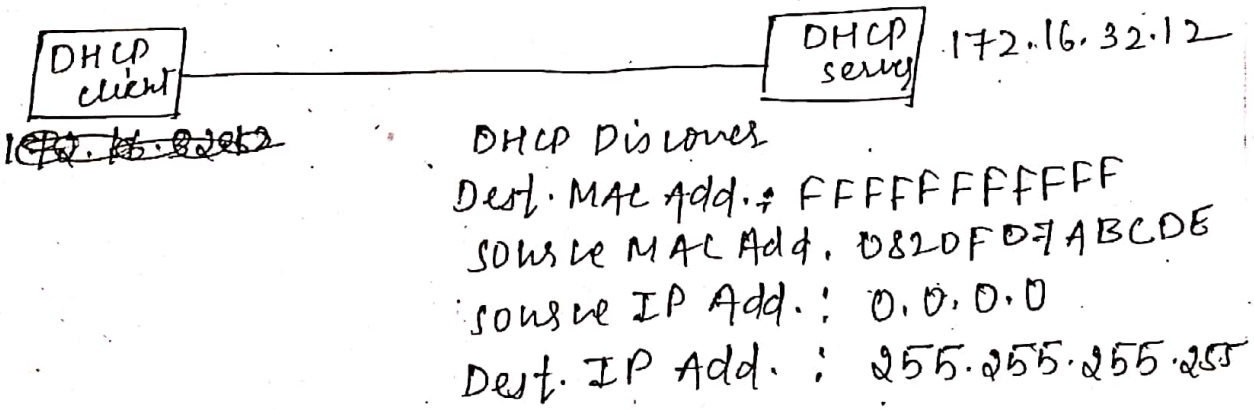
Scanned by CamScanner

Dynamic Host Configuration Protocol (DHCP)

DHCP is an application layer protocol, which is used to provide IP address. DHCP is based on client server model and based on discovery, offer, request and ACK. DHCP port number is 67 for server and 68 for client. IP addresses are assigned from pool of addresses.

DHCP messages:

1. DHCP discover message: This message is generated by client host in order to discover if there is any DHCP server are present in the Network or not. This message is broadcasted to all devices present in a Network to find out DHCP server.



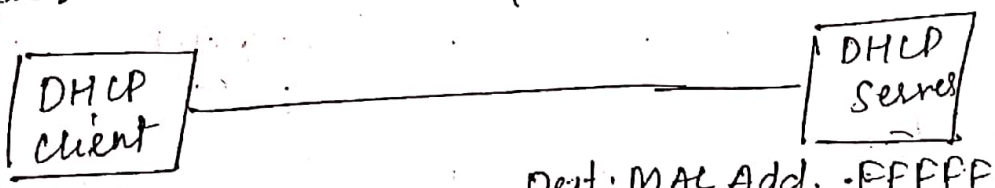
2. DHCP offer Message: The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This msg. is broadcasted by server. If there are more than one DHCP server present in the Network then client host will accept the first DHCP OFFER msg. it receives.

Scanned by CamScanner

DHCP OFFER:

Dest. MAC Add.: FFFFFFFFFFFF
Source MAC Add: 00AABBCCDDEE
Source IP Add. 172.16.32.12
Dest. IP Add: 255.255.255.255
offered IP Add: 172.16.32.51
server identifier: 172.16.32.12
client identifier: 0820F07ABCDE

DHCP Request Msg: The client will produce ARP in order to find if there is any other host present in the N/w with same IP address. If there is no reply by other host then there is acceptance of IP address.



Dest. MAC Add. FFFFFFFFFFFF
Source MAC Add; 0820F07ABCDE
Source IP: 0.0.0.0
Dest. IP: 255.255.255.255
Request IP: 172.16.32.5
server identifier: 172.16.32.12
Client identifier; 0820F07ABCDE

DHCP acknowledgement msg: In response to client the server will make an entry with specified id and bind IP address with lease time.

DHCP ACK:

Dest. MAC: FFFFFFFFFFFF
Source MAC: 00AABBCCDDEE
Source IP; 172.16.32.12
Dest IP: 255.255.255.255
YIP add: 172.16.32.5

Scanned by CamScanner

server identifier : 172.16.32.1
lease time : 72 hours

5. DHCP Negative ACK Msg : Whenever DHCP server receives a request for IP address that is invalid according to scope that is configured with, it sends DHCP NAK msg to client.

6. DHCP decline : If DHCP client determine the offered configuration parameters are diff. or invalid, it sends DHCP decline msg to the server.

7. DHCP release : A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.

Scanned by CamScanner