10th July, 2010
Saturday

* Problems associated with computer Network :

  * Communication
  * Identification
  * Connection.

Communication :

* Protocol is a language of computers needed for communication of the computers.

* Some of the protocols are :-

  HTTP – web, browser
  SMTP – mail computation
  FTP – file communication
  NTP
  SNMP

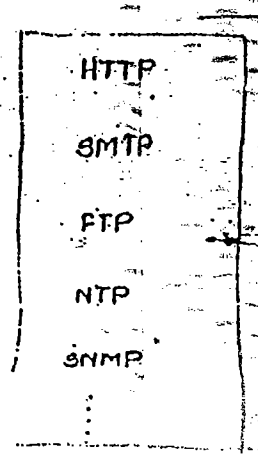
  } location is NOS (Network operating system)

NTP (Network Time Protocol) :-

Transactions are done by storing source timeslot and converting it to the destination timeslot and mailing to the user. Eg :- U.S.A (Time) → mail → India (Time)

SNMP (Network management Protocol) :-

DOS + All protocols = windows NT



→ versions of protocols

protocols

HTTP (Hyper Text Transfer protocol) : Browser requesting for a webpage.

HTTP - 1.0 - 1.1 - 2.0 (Application protocol)

RFC - Request for comments ⇒ Standard of computer networks

→ concept of computer Networks, have an RFC number.

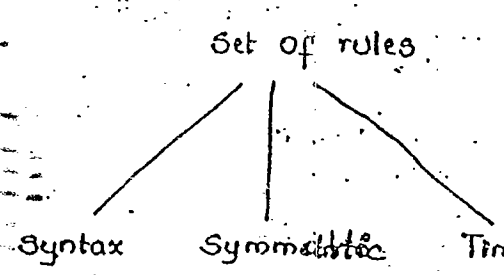
RFC 1

RFC 2

RFC 3700 +

ol :-

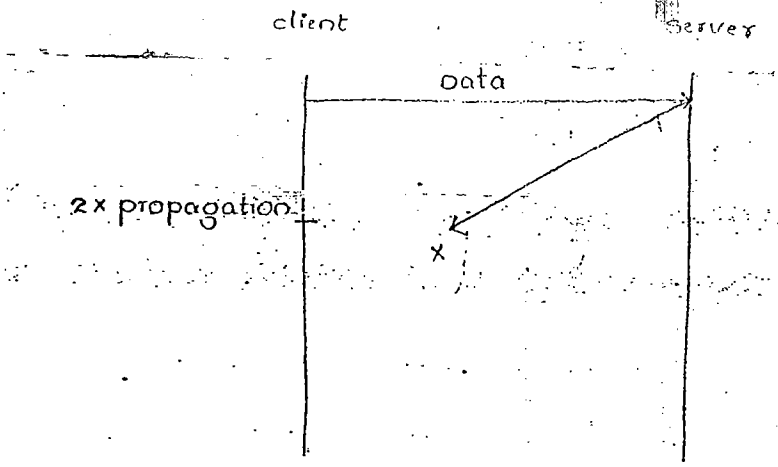
is a set of rules and regulations (or) conventions.



* Rules and Regulations must be crystal cleared (i.e., there must any duplicates and any invalid syntax that is not acceptable).

* Timing (i.e., starting and ending a task) must be mentioned.

  * Syntax → send acknowledgement
  * Semantic → receive acknowledgement



* min. ack. waiting time = 2 x propagation → R.T.T
* max. ack. waiting time = 2 * (min ack. w.time) → Turn over (Timeout)
  = 2 * (2 * propagation)

Round Trip Time → RTT Turnover Time → Time out (TO)

* Protocol is an agreement between the communicating parties on communication is to proceed.

* IP address doesn't refer to a host actually. It really refers to a interface, so if a host is on two networks, it must have two IP

⇒ A system may have multiple IP adelresses and multiple physical addresses.
← NIC.

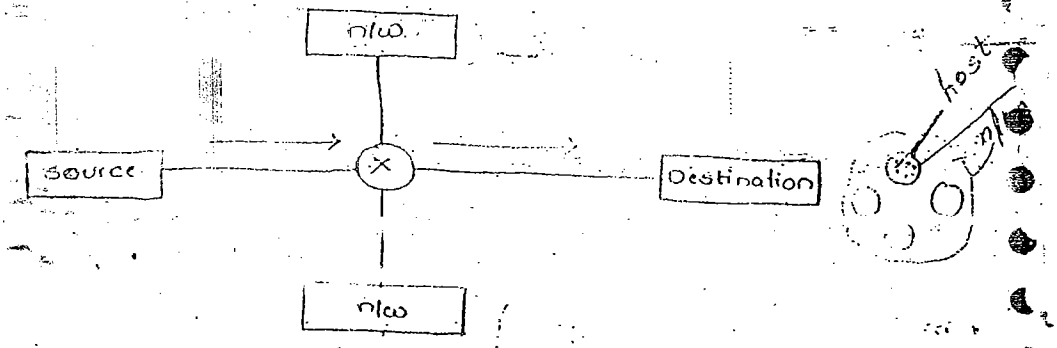
Identification :-

* To send a packet from source to destination, we have the fo identification steps :-

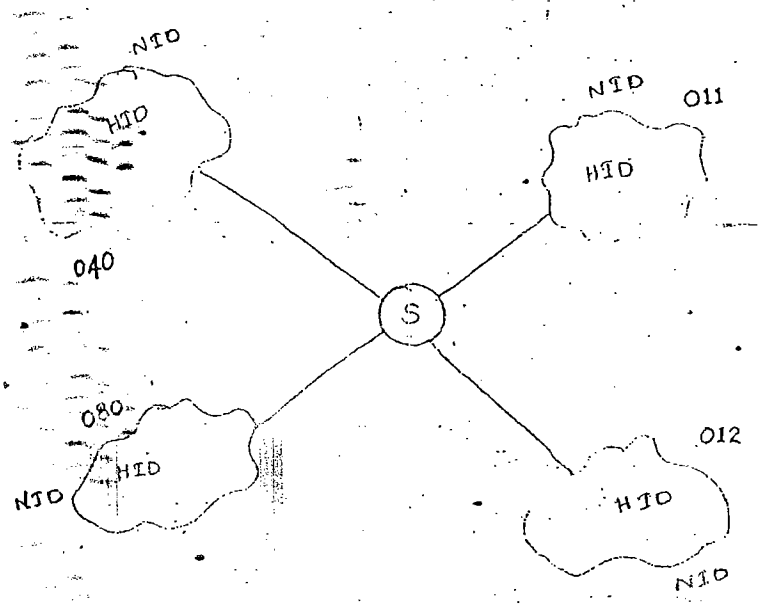
(1) Identify the network ⟶ logical

(2) Identify the Host within the network (i.e., among all the dist systems, one system is identified). ⟶ physical

(3) Identify the process within the host ⟶ Service point



Eg:-



040 / 3 — 4752469 / 7

08572 / 5 — 33607 / 5

085761 / 6 — 3362 / 4

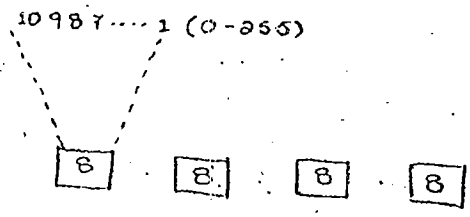
(1) Each no. is 10 digit

(2) Two paths.

(3) Each no. is unique

(4) Hidden meaning

(1) 32 bit number



(2) Two paths :-

* Network Id
* Host Id

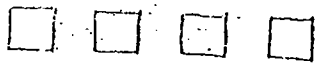
(3) Host Id must be unique

(4) Hidden meaning

* city - A class.
* Town
* village

Class A:

A :



NID HID

8 24

2^8 N/w 2^{24} hosts/nw.

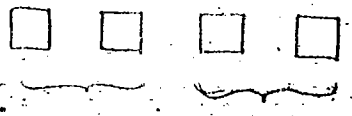
256 $\simeq$ 1.6 cr hosts/nw.

* Govt. organisation uses this huge network.

Eg:- APSWAN - Andhra pradesh state Wide Area Network Class A network

* IP Address can be assigned to any electronic device.

class B :



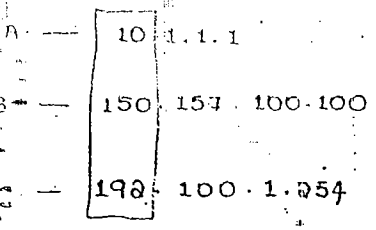
NID	HID
16	16
2^{16} N/w	2^{16} Hosts/N/w
64,000	64,000

Big organisations, MNC companies, Banks use this network.

class C :-

NID	HID
24	8
2^{24}	2^8
1.6 cr	256.

Engineering colleges., medium organisation.



1 — 126	A class
128 — 191	B class
192 - 223	C class
224 - 239	D class
240 - 255	E class

* 127 ⇒ special IP address

Eg.:- 150.167.1.1 → class B

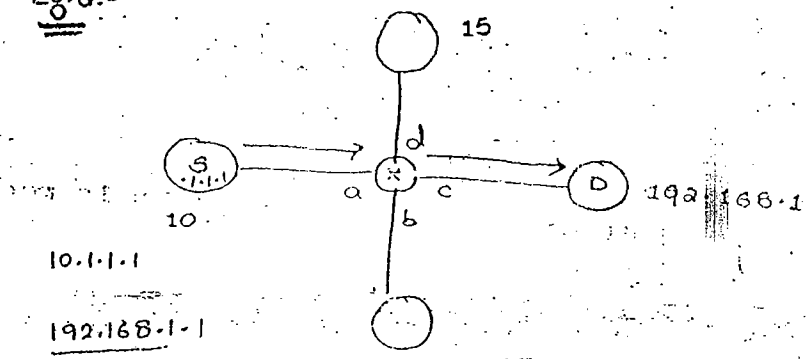
NID HID

Used to routing process

192.168.1.1 — class c

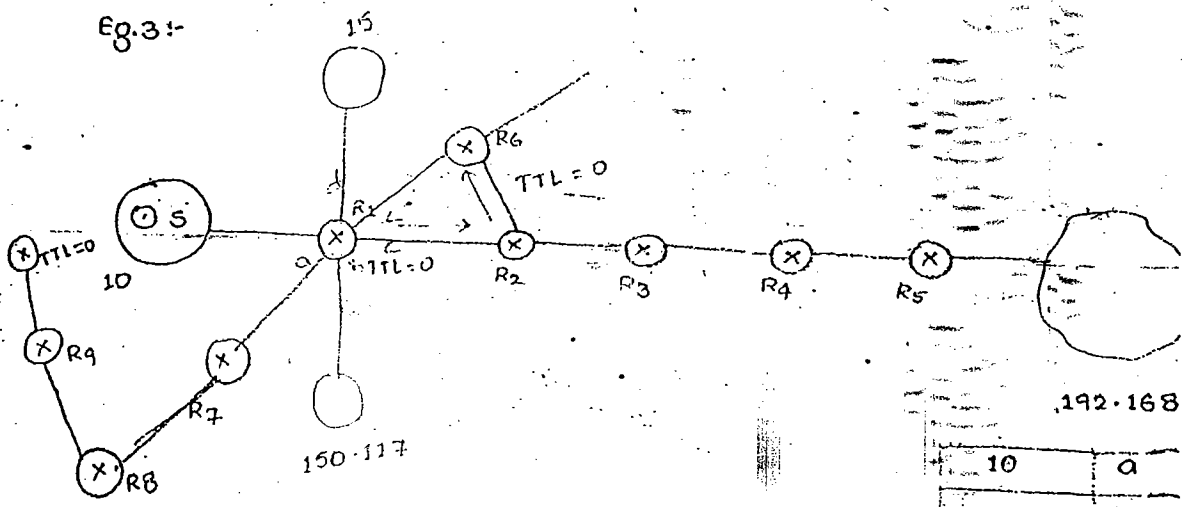
NID HID

Eg.2:-



10
150.167
192.168.1
15

Eg.3:-



10	a
150.167	b
R2	c
16	d
default	R2

(1) Consider default route (make dynamic default route)

(2) Make TTL = 0

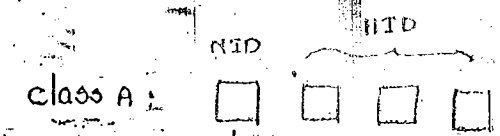
To avoid the wrong route through R7 to R9

Time To Leave

Eg.:- TTL = 3 min => 180 sec.

Routing

Source Router



Class A :

finding elements in nlw

① Default route

② Dynamic route

③ TTL = 3 min = 180 sec

0 → reserved

0 0000000 — 0 ×

0 0000001 — 1

0 1111110 — 126

0 1111111 — 127 ×

NOTE :-

* Having all zeroes (or) all one's either in Network Id or Host Id is ruled out and they are meant for special purposes.

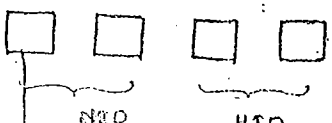
10.0.0.0 ×

10.255.255.255 ×

2^8 Nlw — 2^{24} hosts/nlw

$2^7 - 2$ Nlw — $2^{24} - 2$ hosts/nlw

Class B :



10

10 000000 — 128

10 000001 — 129

10 111111 — 191

2^{16} Nlw — 2^{16} hosts/nlw

2^{14} Nlw — $2^{16} - 2$ hosts/nlw

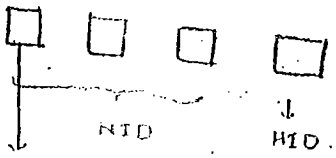
No all 0's & all 1's

10 ... nlw

150.157.0.0

150.157.255.255

class c :

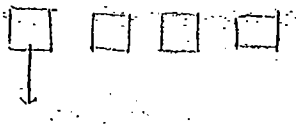


110 .....

110 00000 — 192

110 11111 — 223

class D :- (used in multicast)



1110 .....

1110 0000 — 224

1110 1111 — 239

A : $(2^7 - 2) * (2^{24} - 2)$

+

B : $2^{14} * (2^{16} - 2)$

+

C : $2^{21} * (2^8 - 2)$

4 billion IP addresses.

2^{24} N/w — 2^8 hosts/

2^{21} N/w — 2^8 - 2 hos

24 - 3 bits = 21

200.000.000.0

200.000.000.255

class E :

1111

1111 0000 — 240

1111 1111 — 25

* NO NID's and HID's present class D and class E.

* To store 4 billion IP addresses, cannot handle since it is 32 bi Hence IP_6 is introduced which 128 bit system.

IP_4 (32 bit addressing system) → IP_6 (128 bit)

* Windows 7 supports IP_6.

* Linux 10.6 also supports IP_6.

* IANA

It is used to assign the unique IP address for the systems.

ISP (Internet Service Provider)

ISP_1

ISP_2

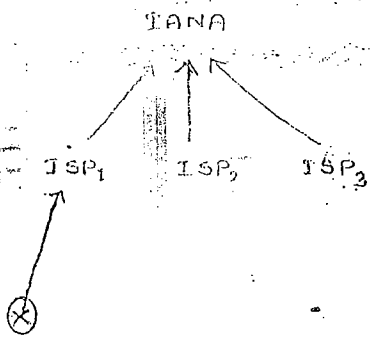
ISP_3

* Isp contacts with IANA instead of user.

A - 10

B - 2000

C - 1,00,000



www.ace.com → 400.400.1.1

Namespace/server

* A user can contact directly to IANA, for IP Address, but it is time consuming. So, a mediator known as ISP handles the situation where it contacts IANA and provide IP addresses.

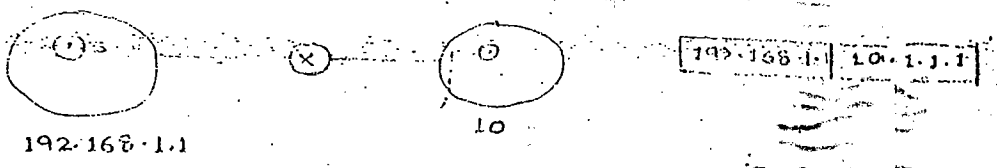
IANA (or) ICANN (Internet Corporation for Assigned Names and Numbers

Spoofing — Using IP address of others by unauthorized use

Types of communication:-

* Unicast (one - to - one)
* Multicast (one - to - many)
* Broadcast (one - to - all)
* Anycast (One to one & one-to-all)

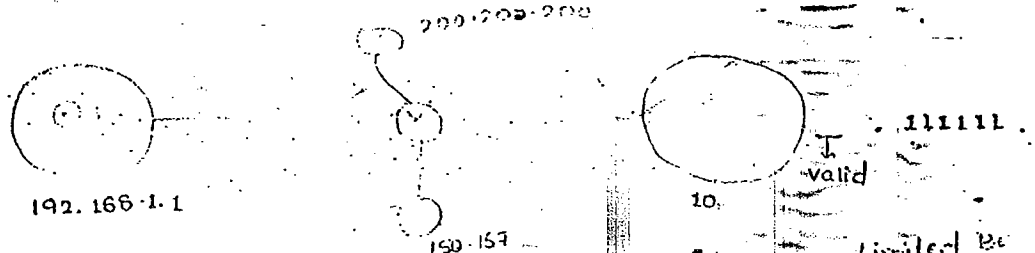
Unicast :-



Eg :- mail application. (Browsing webpages)

Broadcast :-

* Directed Broadcast :- (valid NID . All 111 1 ... 1 / 255 HID)
* Limited Broadcast



Class A:

Eg :- | 192.168.1.1 | 10.255.255.255 |

Directed Bc

| 192.168.1.1 | 192

| 192.168.1.1 | 255.

* Sending packets to all systems in some network — Directed BC.

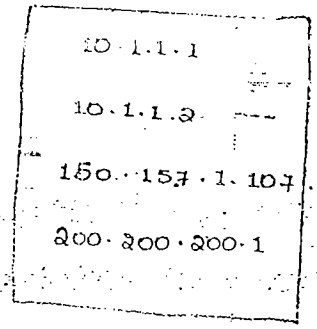
other

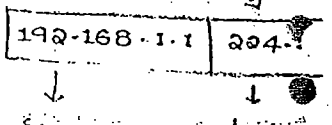
... in our own network — Limited

Multicast :-

* It is created from class D.
* All the IP addresses are stored in a group.
* for class D, i.e., for group communication, IGMP (Internet Gr Management protocol) is used instead of IP.

Eg :- 224.1.1.1 (Group IP address)





* Sending group mails

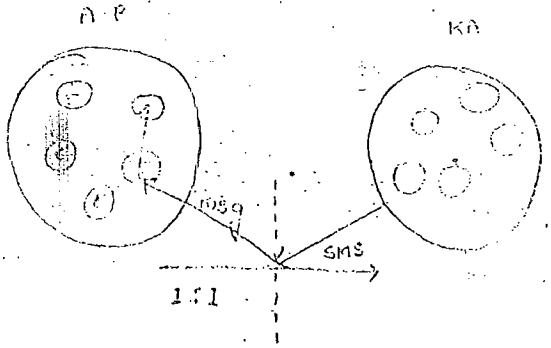
Eg :- Yahoo mails

majority of communications present in multicasting

Anycast :-

host

* It is also used in mobile communications.



: In multicasting 28 bits are available for identifying groups, so 250 million groups can exist at the same time.

Two kinds of group addresses are supported by multicasting.

* permanent
* Temporary (leaves the group in last process)

Each multicast router sends a hardware multicast to the hosts about once a minute, on it's LAN, to report back on the groups their processes currently to. Each host sends back responses for all class D addresses it interested in.

permanent → { 224.0.0.1 ⇒ All
224.0.0.2 ⇒ All }

These query and response packets use a protocol called IGMP (Internet Group Management Protocol) instead of IP.

11/07/2010

Sunday

Anycast :-

* It is used in mobile host communications.

Eg. :- Laptop.

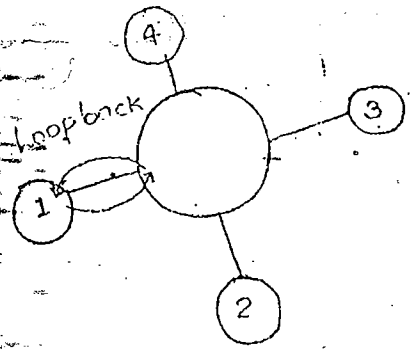
* The nearest access agent takes care of the communication particular mobile.

* So it has 1:1 and 1: all communications.

127 — Special IP addresses :-

* 127 is used for connectivity purpose.

PING - Packet Internet Group.



192.168.1.1 | 192.16

192.168.1.1 | 192.168.1

⇓

127.1.1.1 ⇒ localhos

* In command prompt type C:\192.168.1.2 to ping system 2 system 1.

* If a system sends the request i.e., ping to other, then if there from other, then it is called "requested timed out".

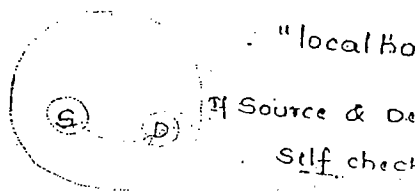
(1) positive message

(2) Requested timed out

(3) Destination unreachable

Characteristics of 127 addressing system :-

- It is called as loop back address because packet is delivere to the source and again received by the source.
- It's first octet should be 127 but no restriction on other
  - Eg: 127.0.1.1
  - 127.50.255
  - (Any other 255.
- It never falls under any classification.
- It is used to identify self connectivity process.
- It is also used for inter process communication (IRC).



- "localHost" is a URL to "127.1.1.1" addr
- Self checking, instead we use "127." address

Limitations of logical addressing system :-

* There is no flexibility
* There is no security
* It is not permanent.

Solutions for above limitations:-

Supernetting

Subnetting

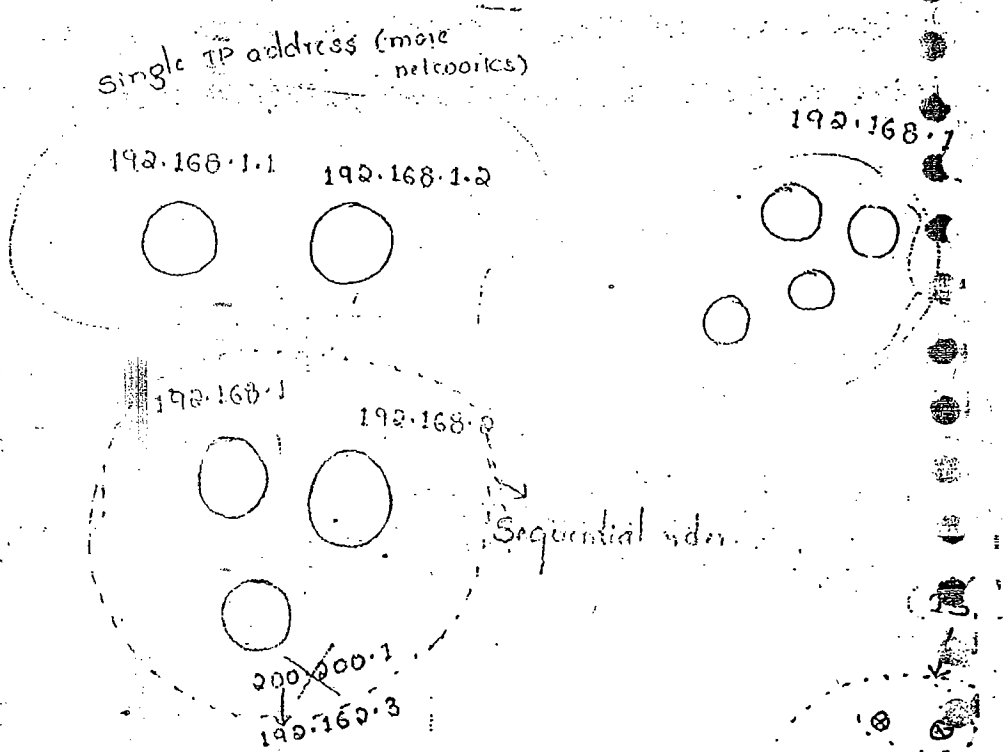
physical addressing system:

Supernet :-

* The process of aggregating two (or) more networks to gener
IP address for the group is known as supernet.

Limitations / Restrictions :

* It is applicable for two (or) more networks.
* All the networks in the supernet must be of same class
* Network ID's of the networks in the supernet must be in the Sequencial order.



Advantages:-

* It improves flexibility of IP allotments.
* It reduces no. of routing table entries.

Subnet :-

Network is partitioned into small subnets, and are connected connector called "Bridge".

Process of dividing a single network into multiple subnets is subnetting. ⇒ (Filtering & Forwarding Approach)

Advantages :-

It improves security.

Maintainance and administration are simple.

Restructuring of the network is simple.

Bridge used to join two or more subnet, of a N/w

Systems within the same subnet can communicate without any ir

But if a system within one subnet needs to communicate with within other subnet, then it must pass through the "Bridge".

Bridge implements Filter & Forward Approach

(Communication is difficult using this subnet)

Def :-

The process of borrowing bits from host ID to generate subnet ID's is known as subnet.

No. of bits to be borrowed is depends on our requirements.

Eg.1 :- To have 3 subnets in a class c network, we suppose borrow 2 bits.

Therefore, no. of subnets possible = $2^2 = 4$.

No. of systems per subnet = $2^6 - 2$

Eg. 2:-

consider a class B network to have 100 subnets, we need 7 bits from host ID.

Therefore, no. of subnets = 2^7

no. of host/ systems per subnet = $2^9 - 2$.

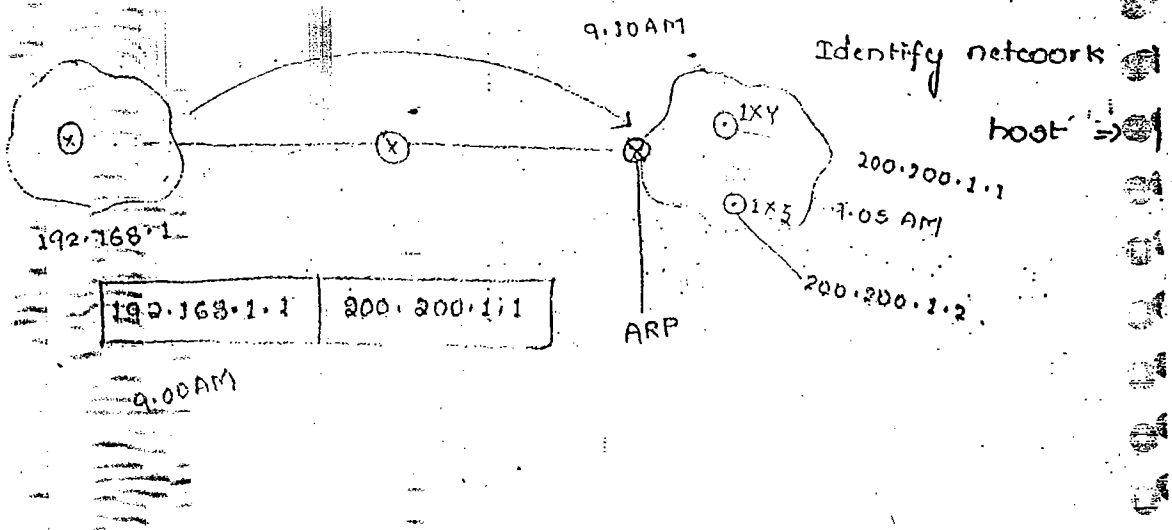
Limitations:

* It complicates communication process. (since 4 step procedure)
* We will loose IP addresses during this process.

* Step procedure:-

* Identify the network
* Identify the subnet network.
* Identify the host id
* Identify the process

Physical Addressing system:-



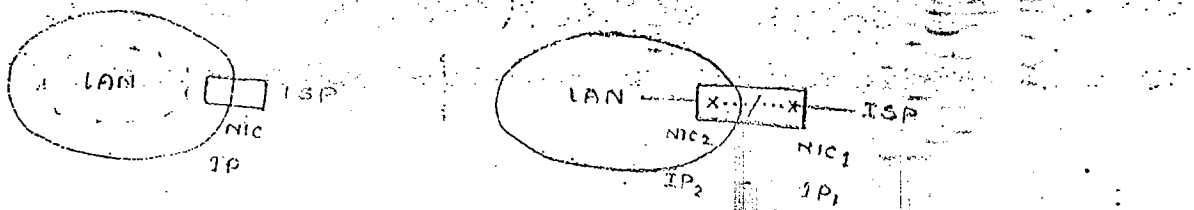
If a system having IP = 192.168.1 sends data to other system (200.200.1.1), at 9.00 AM. Meanwhile if the destination system changed it's IP, then the data is sent other system. In order not to have data misuse, a physical addressing system maintains the IP addresses of changed systems and provides the data to it.

ARP table		
200.200.1.1	1XY	5
200.200.1.2	1XZ	1

log file

200.200.1.1 ⇒ logical ⇒ different.

1XY ⇒ physical ⇒ unique (IMEA number) (like mobile)



By using one IP address, a hacker easily attack the systems. So proxy IP address is maintained. such that if he has IP_1 through then the connection b/w IP_1 and IP_2 is disconnected. So, the sy within the LAN are safe.

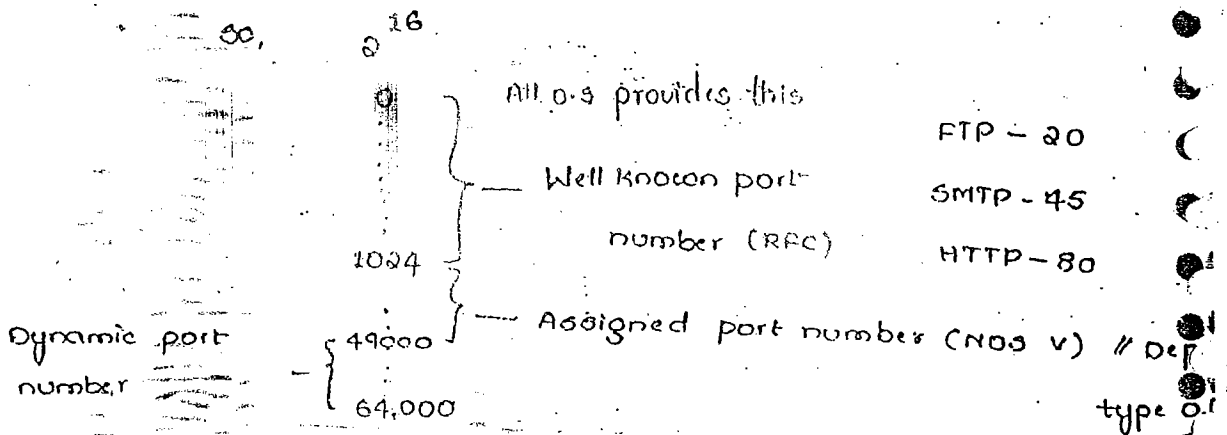
Logical :- 32 bit – Network layer – IP – software – not permar

Physical :- 48 bit – Datalink layer – ARP – Hardware – permanent. (No. plate, Engine no.)

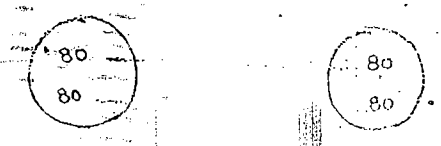
Service point :- 16 bit – Transport layer – TCP/UDP – s/w – fixed.

Service point addressing system:-

* It is 16 bit addressing system.



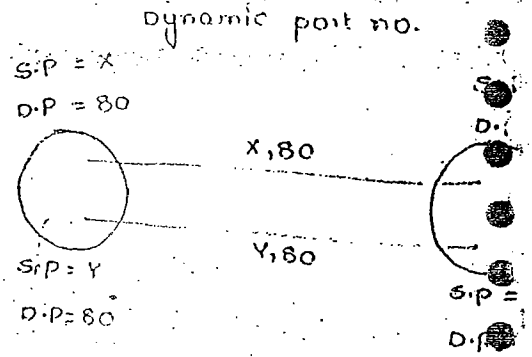
Distinct connections :-



80 → http.

Source port (S.p)

Destination port (D.p).



X → Any port no. from 4

Y → Any port no. from 49 other than x.

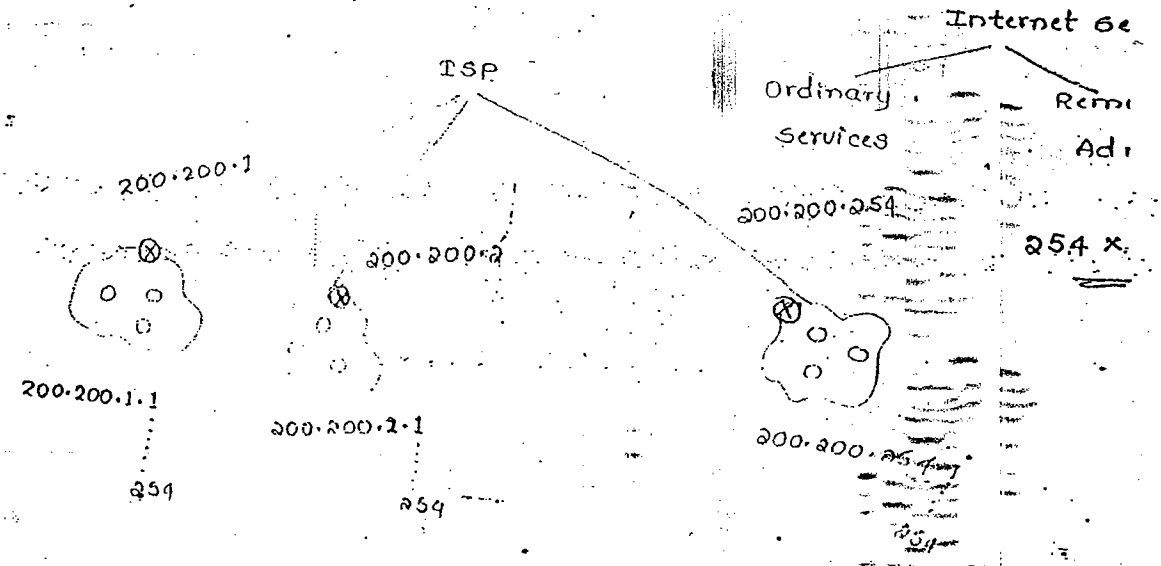
* If one system having S.p as 80 needs to communicate with D.P = 80, then the connection is established among them. And if system also needs to communicate, then the problem arises. So consider the S.p as distinct port no.'s within the range of Dynamic port no.'s.

Public Vs Private

* Public system have public IP addresses and it is powerful th private.

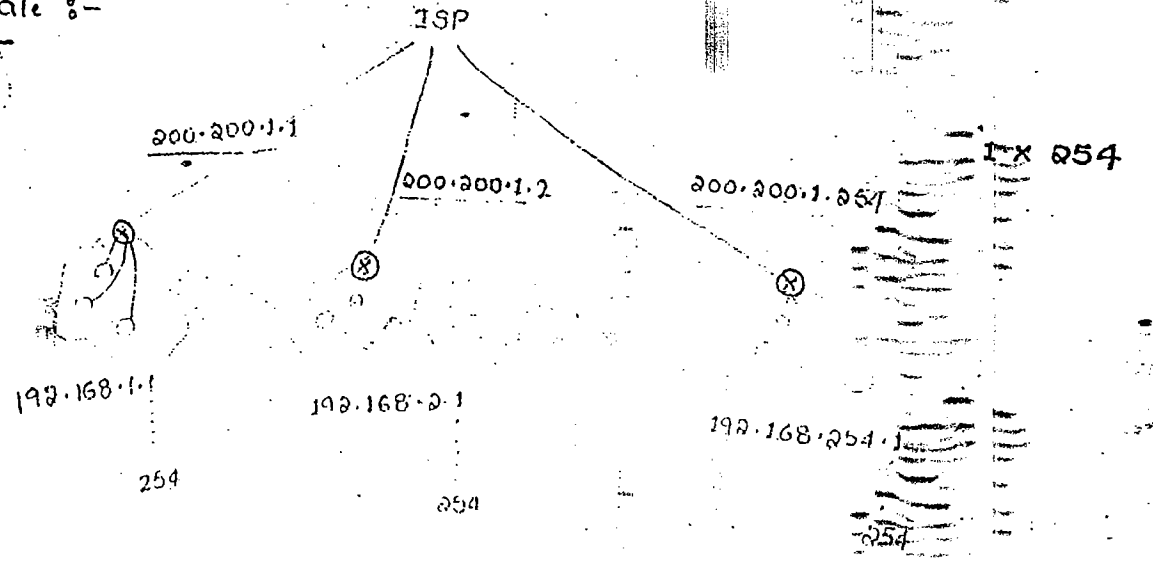
* One public system can control the other public system without to that particular system. It is known as "Remote system Ad.

* But, it is costly & powerful.



* Their visibility is identified. i.e., they can contact with the inte (ISP) directly. and no need to depend on the interface (router)

Private :-



IANA provides IP to private systems

A 10.0.0.0 – 10.255.255.255 — (1)

B 172.16.0.0 – 172.32.255.255. —— (16)

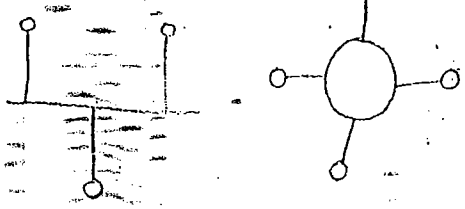
C 192.168.0.0 – 192.168.256.255 — (256)

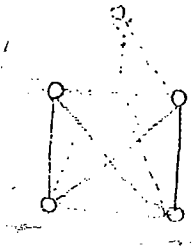
other than these are all public.

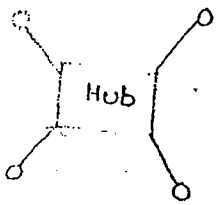
* The private system's visibility is not identified. i.e., Every syst contact the interface (router) to get connected with interne

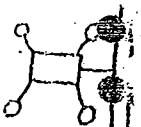
Connection :-

There are multiple ways of connecting systems. Some of the









Bus Topology	Ring Topology	Mesh	Star	Tr
C ✓	C x	C x	C ✓	
E x	E ✓	E ✓	E ✓	
R x	R x	R ✓	R ✓	
			(Browsing)	(corpora use

To choose the required topology, we need to have the following

* cost
* Efficiency
* Reliability

* In Browsing, we use star topology. But, in corporates, Tree topology is used.

* Various types of objects in computer networking :-

  * Workstations & Servers (7 layers)
  * Hub - 1 (physical layer)
  * Switch - 2 (PL, DLL)
  * Bridge - 2 (PL, DLL)
  * Router - 3 (PL, DLL, NL)
  * Brouter - 3 (PL, DLL, NL)
  * Gateway - 7

Workstations & Servers:

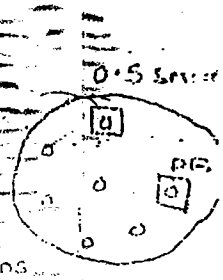
* A particular o.s server acts as the domain key and all the o. client systems acts as workstations.

* The server maintain some Access control lists (ACL) which rep the accessibility of programs by ther clients. (permissions)

* The unaccesoible programs are denied by server (if client attemp open it).

Servers may have several applications

For eg:- OS server, DB servers. etc.

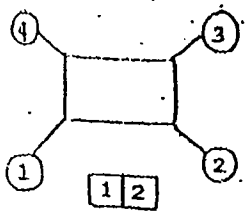


loads higher versions of s/w compare to other in nlca

Users

Hub:-

* It is used to connect multiple workstations & servers.
* It is a passive device, no software associated with this.
* It is a broadcasting device.



Disadvantages:-

* Network traffic is high.
* Causing unnecessary disturbances at various systems.
* Because of above two reasons performance is loco.

Advantages:-

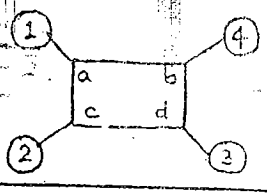
* Cost of the hub is loco.
* Operation is simple.

Switch:

* It is also used to connect multiple workstations.
* It is an active device associated with software.
* It maintains a look-up table to keep track all the systems.

Advantages:-

* Network traffic is less.
* No unnecessary disturbances at various locations.
* Because of above two reasons, performance is good.



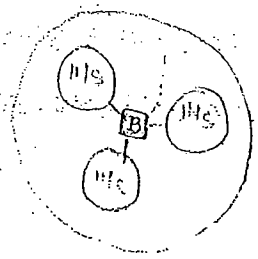
a	1
c	2
d	3
b	4

Disadvantage:-

* Cost of the switch is 2 to 3 times of the hub.

Bridge:-

* It is used to connect multiple LAN's on multiple subnets.
* Filtering and forwarding is it's design criteria.
* It's operation principle is based on physical addressing syst "Switch".
* It will also maintain a lookup table.



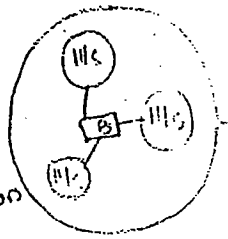
H/S ⇒ Hub/switch.

Router:

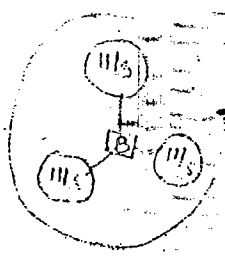
* It is a sophisticated WAN device and it's principle is based on l addressing system.
* It is used to connect two (or) more different similar networks.

It doesn't convert protocol,

It send's as it is info to destination



TCP/IP



TCP/IP

* It requires a lot of configuration where as bridge & switch are p -and- play devices.

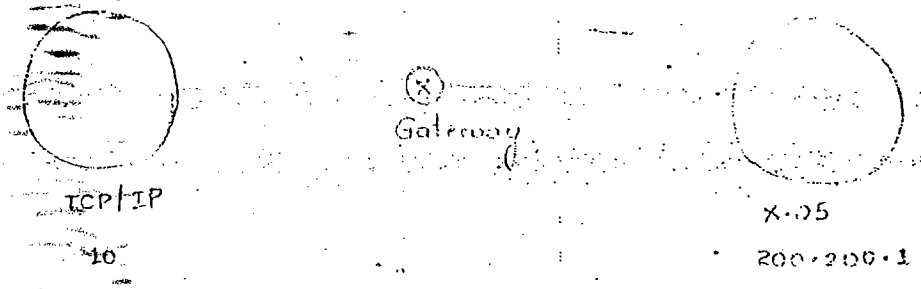
* All routing algorithms are running in a router. So, the cost of router is very high (in terms of lakhs / crores).

Brouter:

* It is a combination of Router and Bridge.

Gateway:

* It is used to connect two (or) more different dissimilar networ



* Gateway is also called as protocol converter. (It converts the TC network data to X.25 network data and send the data to des

14/07/2010

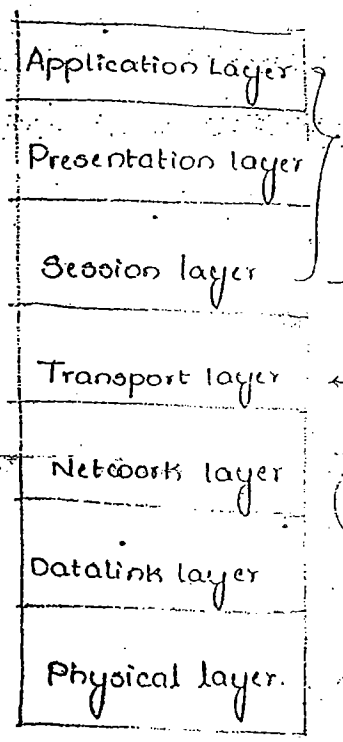
Wednesday

System Functionality

Total ⇒ 70 fur

mandatory	Optional
* Error control	* compression
* Flow control	* Encryption
* Segmentation	* Encoding
	* Routeri

* OSI
* TCP/I
* FR
* ISDN
* ATM -
* IEEE 5(
* X.25

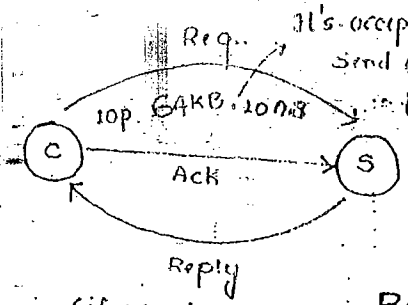


To access all th
functionalities, t
reference model
OSI.

OSI-reference model divides the 70 functionalities into 7 individual groups.

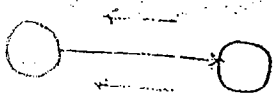
Connection-oriented & connectionless communication:

Connection-oriented:-



Three-way handshake

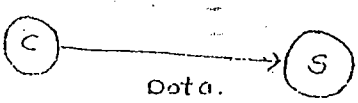
(if accept ⇒ (+)ve reply, not ⇒ (-)ve)



Data Transfer phase

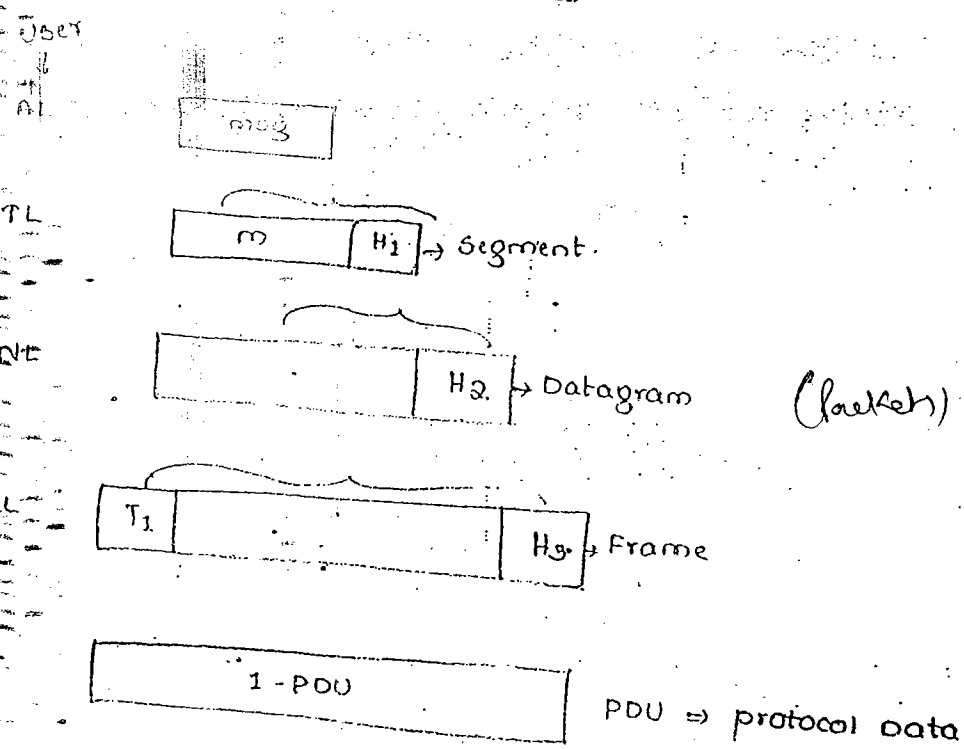
Reliability is high.

Connectionless:



Directly send the data without ack.

If there is connection (i.e. connection-oriented), we need session, other



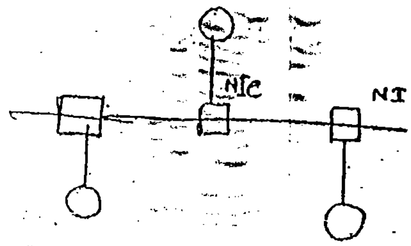
PDU ⇒ protocol data unit

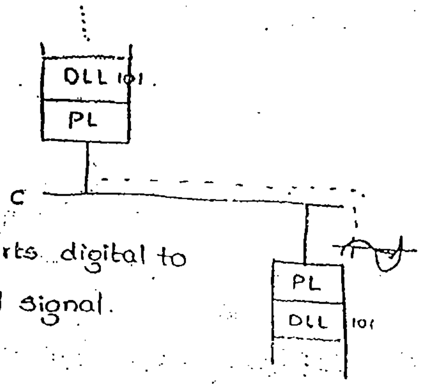
0/8

Physical layer (H/w):

(1) It defines electrical, mechanical, functional & procedural charac of interfaces and media.
(NIC)

Representation of bits:-





PL converts digital to electrical signal.

C - Electrical (c → copper core)
F - light signal
Wireless - Electromagnetic.

(2) It defines transmission mode. Simplex ⇒ Keyboard cable.

* Half duplex — One can talk at a time (walky-talky)

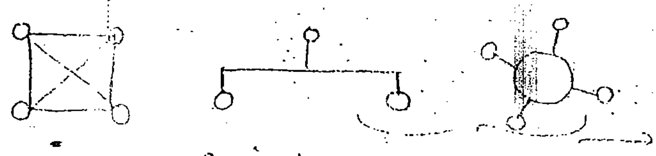
* Full-duplex Tele communication — Both can talk simultaneously

Session layer decides either half-duplex (or) full-duplex connect

(3) It defines link configuration.

* Point-to-Point link. (A dedicated channel for one source) ⇒

* Broadcasting link. (A single channel for all sources)



Broadcasting l?

(3) It defines topology configurations.

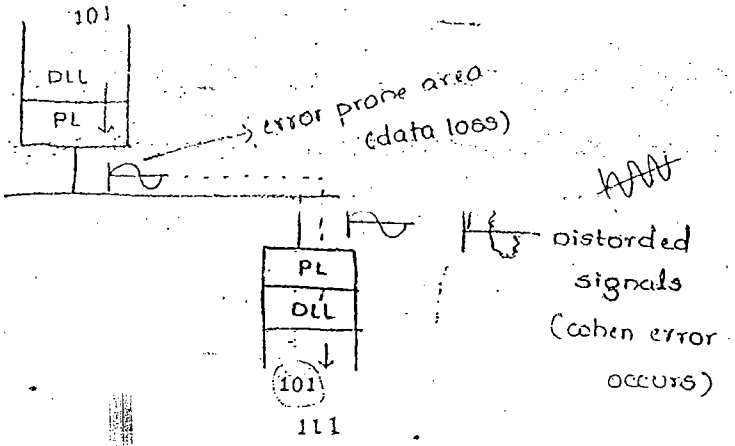
It maintains fixed roles.

Datalink layer (DLL):-

Responsibility :-

* Error-control
* Flow control
* Access control
* Framing
* Physical addressing system. — 48-bit MAC Ethernet LAN NIC

Error control :-

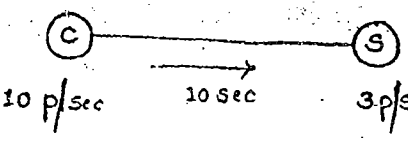


If there are errors in the transmission of bits as signals, then there a chance of distorted signals and bit representation is changed.

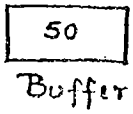
So, the destination DLL must have the functionality of verifying :-

* Error Detection
* Error-Correction
* Re-transmission (Sending negative acknowledgement to sender, it resend the bits)

Flow control:-



Based on server capability, client sends the data.

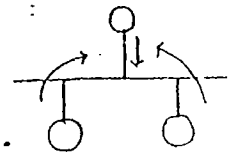


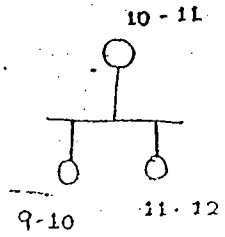
Sliding window protocol: To control the flow among client & server.

* Stop & wait
* GBN. - Go Back to N
* SR. -

Access Control :-

Time slot mechanism is allotted to all the stations, since lot of collise occurs.



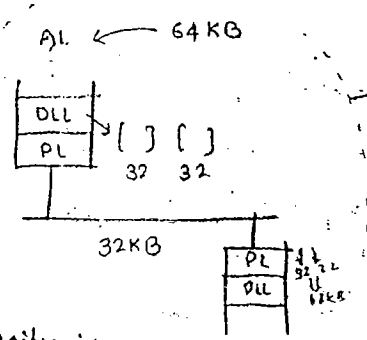


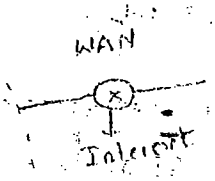
Sophisticated access control mechanisms:-

* ALOHA
* CSMA/CD
* CSMA/CA
* TP

* User can generate any sized data.

Framing :-

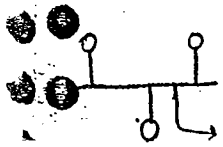




Framing at LAN.

Segmentation - WAN

PL converts the any sized pl into 64 KB.



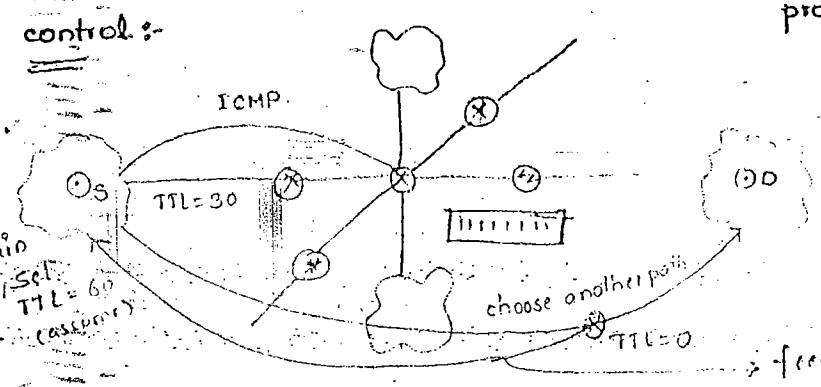
link capacity is 32 bit bit PL gives pkt to DLL as 64KB, based on cha

Network layer :- (complex).

* Logical addressing system.
* Congestion control.
* Routing
* Feedback messages ⇒ PING

ICMP ⇒ Internet control mes
protocol

Congestion control :-



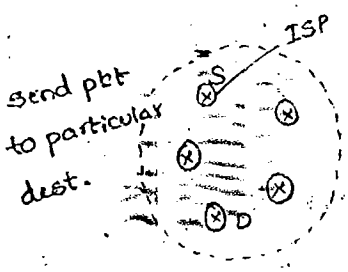
* If the data is fulle in all the buffers of the routers, then it is as congestion.

* To control congestion, router sends the message to the source to sto transformation of packets by knocoing it's IP address, rather than to all the adjacent routers.

directly

Feedbacks messages :-

* The receiver sends ICMP to the source.



ICMP (It's not exact path,
If source gives shorter IP address,
then it reject it, as it is higher IP)

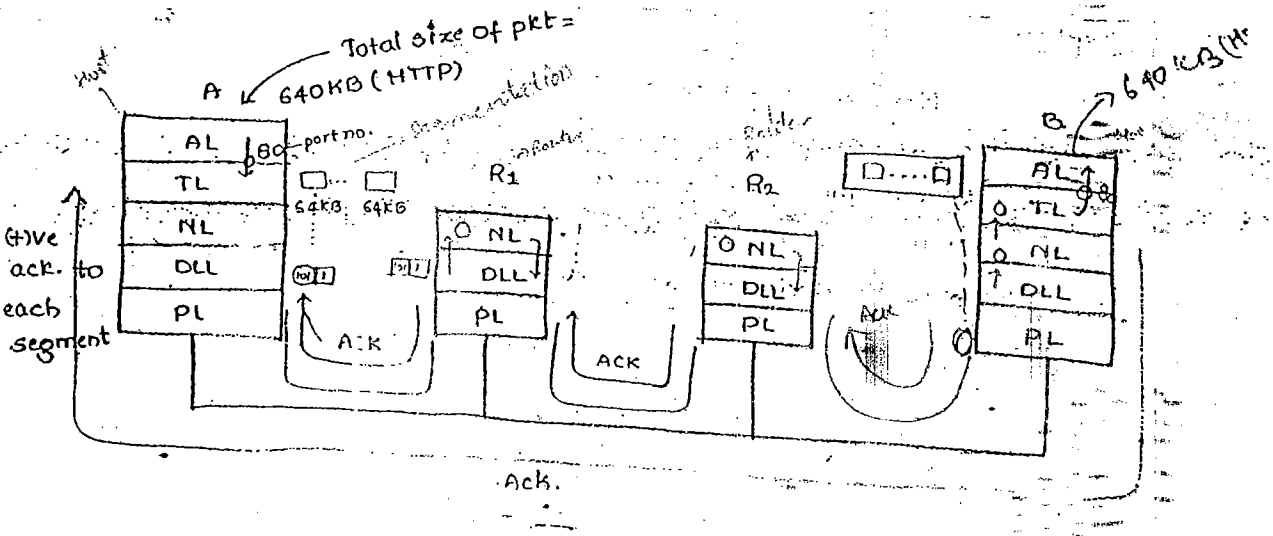
(1) ICMP
(2) TTL=0
(3) ping
(4) ICMP
the mi
routes.

⇒ In a system physical addresses is permanent for a packet logical

Transport layer:-

* Segmentation & Re-assembly
* Multiplexing & De-multiplexing.
* Service point addressing system.
* Error control
* Flow control.

⇒ DLL works b/w DLL & DLL between consecutive nodes only.



320KB (FTP)

640KB (SMTP)

640KB (HTTP).

TL divides pkts data into segmen

TL | CRC | 64KB | 80 | A | B | H3 | LE

After sending Ack. from R_1 to A.

NL adds another he

NWL | CRC | 64KB | 80 | A | B | Ap | R2p

After Sending Ack. from R_2 to R_1

DLL | CRC | 64KB | 80 | A | B | Ap | Rp

64KB | 80 | physical addr of source

DLL = frames NL = pkts, TL = segments

TL = end-to-end

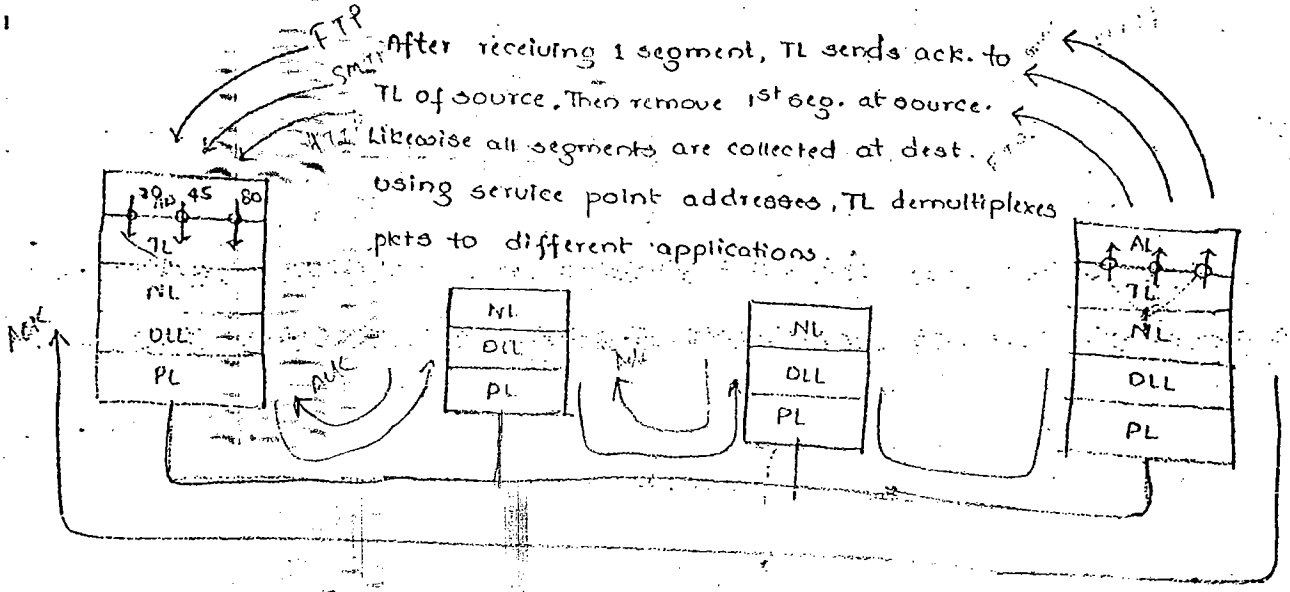
NL = link-to-link

R_1p ⇒ physical address of beside router, it is decided by NL.

Multiplexing & De-multiplexing:

* Combining all the different protocols data and sending is called multiplexing.

* These are equally partitioned and sent through the media. At the received side, all these are combined and received which is known as de-multiplexing.



* Error verifications are done by two aspects :-

1) * Link level (Datalinklayer)

2) * End-To-End-level (Transport layer)

TL have the extra field called "checksum" along with the data.

CRC ⇒ check link errors

⇓

DLL

Data	checksum

checksum ⇒ check N/w errors

⇓

Transport layer

Source & dest. generate CRC code & cross check, if correct, send ack. to source, & if ack. received by source remove the pkt.

R1 router

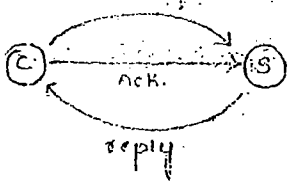
Flow control :-

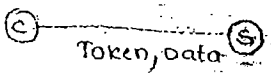
* If a problem occurs in Transport layer (of B), then it sends the -age (ack.) to the sender's Transport layer instead of Router

(This is called End-to-End Comm. or Transmission)

Session layer :-

* Dialogue control / Dialogue discipline (maintaining discipline of connecti with server) inorder not to exp the session)
* Maintaining checkpoints
* Grouping of operations

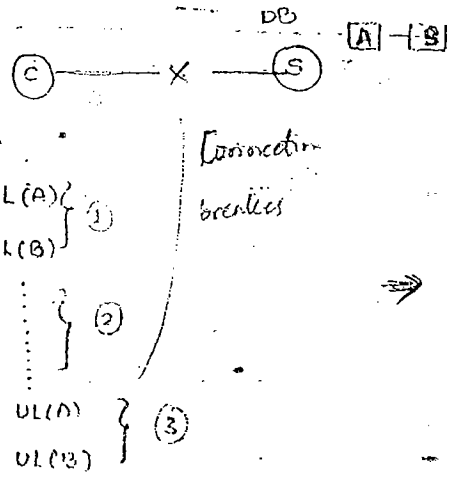


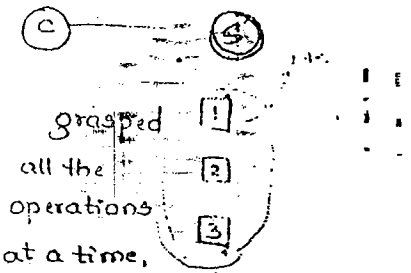


By using "Token", communic establishes, sending data r Token at the sende

If continuously sending 1's and 0's is considered as a dummy d. dummy packet.

Grouping of operations :-



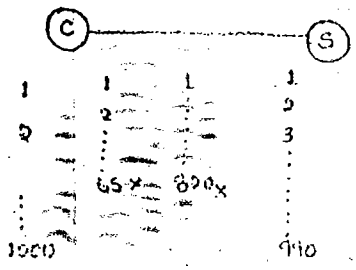


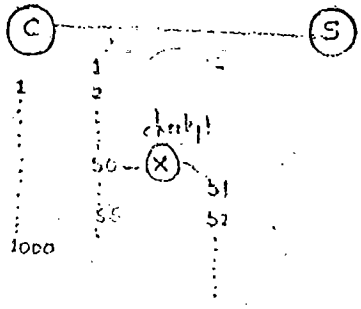
Session layer maintains all the group of operations.

* Checkpoint maintainance :

Eg:- Downloading files.

DAP supports checkpoints.





IE.
↓
not suppo

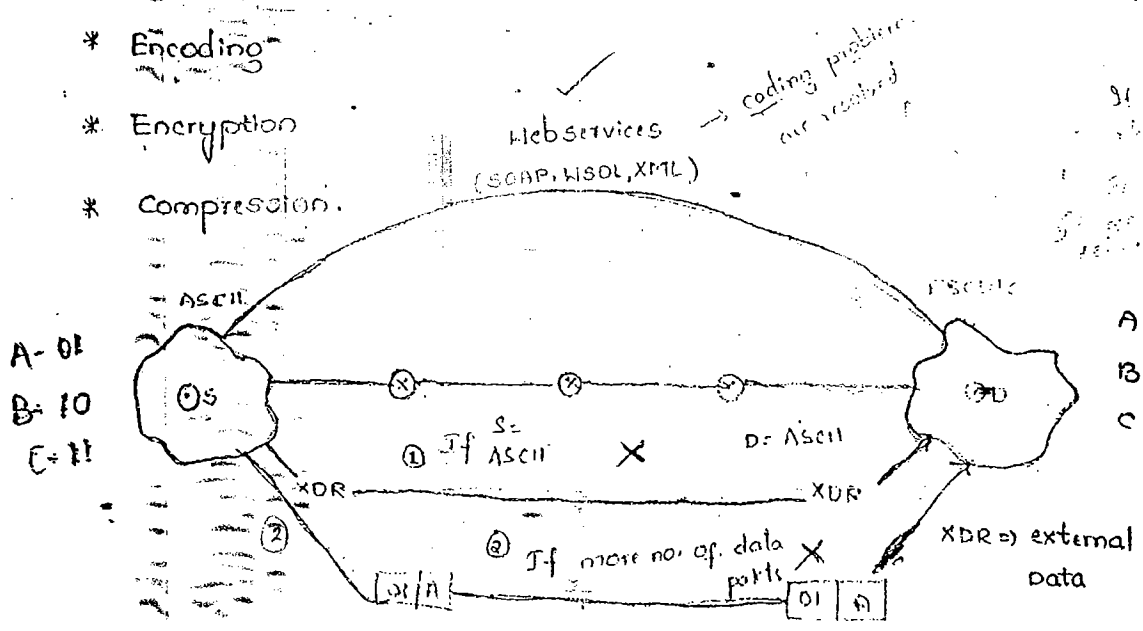
Downloa
Accept
program

* When a file is being downloading, then if connection is discarded in between the download, then the user have to start from the first. In order to overcome this problem, checkpoints are introduced which specifies the checkpoint upto completed file and continues at the same point when downloaded again e.g. in DAP.

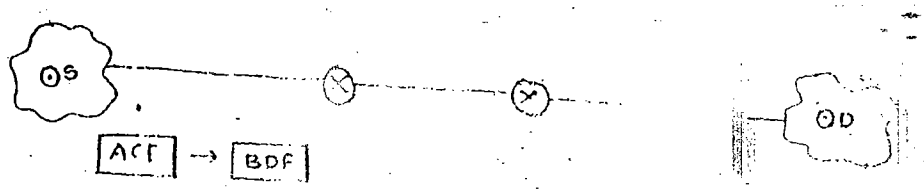
Presentation layer:-

Responsibilities:

* Encoding
* Encryption
* Compression.



Encryption :-



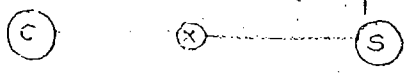
A → replaced with B
B — C K=1
C — D
⋮
52 keys possible

⇒ Easy to hack.
So, RSA, DES ..... algorithms introduced.

⇓

These keys takes seconds to break, where RSA takes some years break. so, we consider it as safe algorithm.

Compression :-



640KB —— 10 pkts
(Compression) 640KB — 320KB ... 50% ... etc
In decompression:
620KB ... 20KB is lo

Advantages :-

640KB — 480KB 25%
In decompression:
640KB

* Traffic is less. ⇒ LZW Algo used
* Time spent on sending packets is also less.

⇒ Good — Bad choosing a compression tools depends on situation

* In multimedia, compression of data is important. and in other applications, decompression is mainly considered.

① If source & dest. use same coded system, then it is waste to convert the given code into other code at source, & dest.

② source directly sends data (01) by representing it as an Ascii code (header), Then if dest. also uses same code, then no problem. If dest. uses other code, it m

Application Layer:

Responsibilities:

* Maintaining harmony among protocols.
* It's user Interface Design (UID) must be perfect

Maintaining harmony among protocols:

* Depending on user's preference, one protocol is converted into other and after completion of the task again converted to original protocol.

Eg.:- ATM, for checking account details, http protocol is used, and for transactions, https protocol is used.

User interface des[illegible] [illegible] critical [illegible]

works in layers

1. W S b Server – 7
2. Hub – 1 (PL)
3. Switches – 2 (PL/DLL)
4. Bridge – 2 (")
5. Routers – 3 (PL, DLL, NL)
6. Brouter – "
7. Gateway – 7

16/07/2010
Friday

Advantages of layering system:

* It uses Divide-and-conquer principle. Therefore, maintainance or administration is simple.

* It uses object-oriented principle like Abstraction & Encapsulati

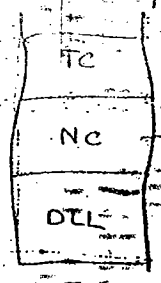
Abstraction - hiding the elements (performs operations, b

If any change of operation doesn't effect on application, then abstraction is perfect.

f1(); (1)

fa()
{ ≡ (x) (3)
}

doesn't represent the procedur



* Independently, the layers are changed without impact on others.

Disadvantages:-

* Interdependancy among layering systems — TCP/IP
TL NL
Not a major

* Duplication of functionality.

OSI - reference model	TCP / IP
(1) Seven layers	(1) 5 layers (AL, PrL, SL, TL, NL, DLL, PL → AL, AL, TL, NL, DLL)
(2) No definition for multicasting	(2) It is clearly defined in TCP/IP
(3) Standards are ideal	(3) Standards are practical
(4) No flexibility (max. size of pkt = 64 KB only) (pkt size is based on network size)	(4) Lot of flexibility (pkt size is defined based on the characteristics of each layer)

Sliding Window protocol :--

Characteristics:

* It is used in correction-oriented communication.
* It offers flow control and packet level error control.
* It is used both in Transport layer and Datalinklayer.
* It is a theoritical concept, practically implemented as :-
    * Stop-and-wait
    * Go-Back-N
    * Selective Repeat protocol.

16/07/2010

Friday

Advantages of layering system:

* It uses Divide-and-conquer principle. Therefore, maintainance or administration is simple.

* It uses object-oriented principle like Abstraction & Encapsulati

Abstraction - hiding the elements (performs operations, b doesn't represent the procedur

If any change of operation, doesn't effect on application, then abstraction is perfect.

f1(); (1)

f2()
{
(x) (2)
}

TC

NC

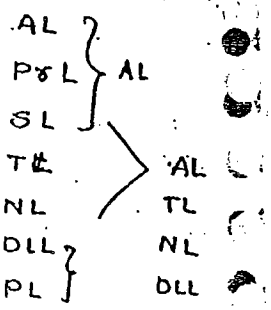
DLL

* Independently, the layers are changed without impact on others.

Disadvantages:-

* Interdependancy among layering systems — TCP/IP (TL / NL)

* Duplication of functionality.

OSI - reference model	TCP / IP
(1) Seven layers	(1) 5 layers 
(2) No definition for multicasting	(2) It is clearly defined in TCP/IP
(3) Standards are ideal	(3) Standards are practical.
(4) No flexibility (max. size of pkt = 64 KB only) (pkt. size is based on network)	(4) Lot of flexibility (pkt size is defined based on the characteristics) of each layer.)

Sliding Window protocol :-

Characteristics:

* It is used in connection-oriented communication.
* It offers flow control and packet-level error control.
* It is used both in Transport layer and Datalinklayer.
* It is a theoritical concept, practically implemented as :-
    * Stop-and-wait
    * Go-Back-N
    * Selective-Repeat protocol.

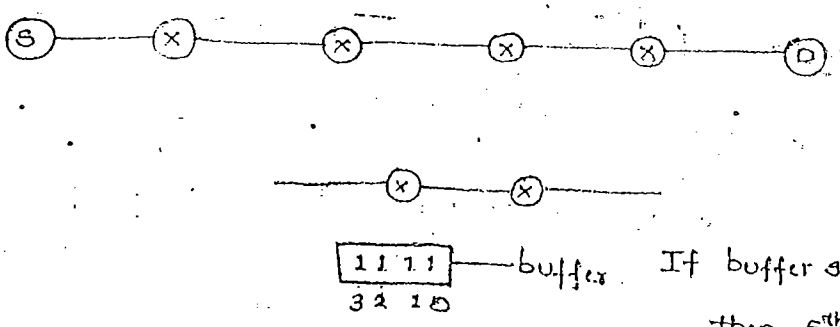
Different types of Delays :-

* Queing delay.
* Processing delay
* Transmission delay
* Propagation delay.

* The amount of time taken by the packet to be in Queue before entering into the router.
* The amount of time taken by the packet to be in queue before being taken out for processing is known as Queing delay

Queing delay :-

* Amount of time packet is waiting in the queue before being taken out for processing is known as Queuing delay.



If buffer size = 4 then 5th pkt is discard
∴ delay for " ∞

* It is varying from 0 to infinite
* It depends on router processing speed and buffer capacity.

Processing delay :-

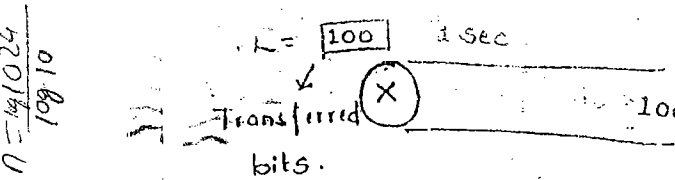
* The amount of time taken by router to process a packet (lookin at destination IP, extracting network ID, searching in the routing

table, identifying destination route) is known as processing delay.

* It depends on router processing speed. but not on size of the packet; because we are processing only header not entire message and header size is const for all size of packet.

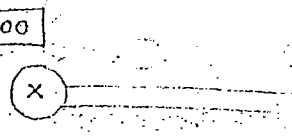
Transmission delay: $\left(\frac{L}{B}\right)$

* The amount of the time taken by the router to transfer the packet to outgoing link is known as transmission delay.



$\frac{L}{B}$ = 1 sec for sending 100 bits

$\frac{L}{B}$ = $\frac{\text{length of packet}}{\text{Bandwidth of the link}}$



$\frac{L}{B} = \frac{100}{10}$ = 10 secs for sending 100 bits

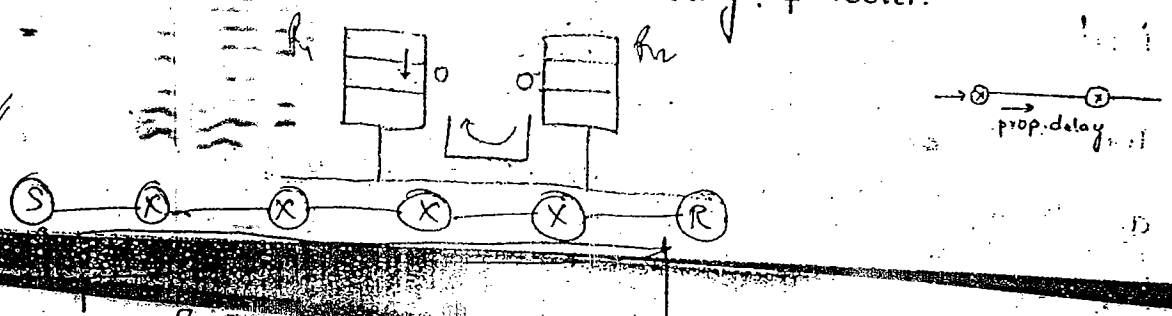
Propagation delay: $\left(\frac{d}{v}\right)$

Amount of the time taken by the packet to make a physical journey from one router to another router is known as propagation delay.

$$P.D = \frac{d}{v}$$

where d → distance between routers

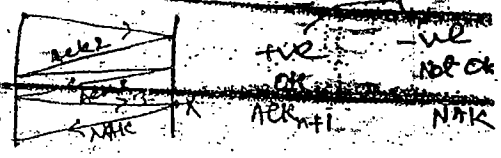
v → velocity of router.



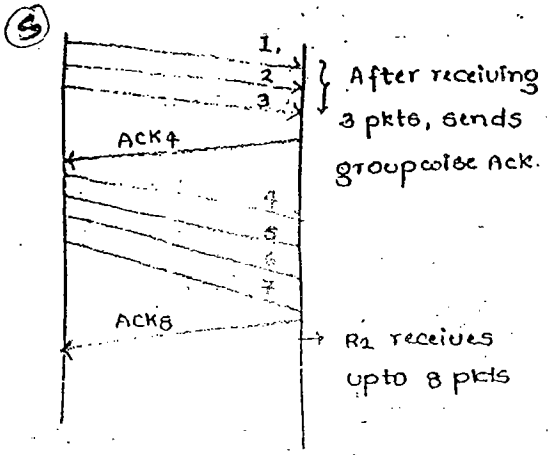
$RTT_{EE} = 2 * [\text{Prop. delay}_{EE} + N(\text{Q delay} + \text{Pr. delay} + \text{Tr. delay})]$.

+ Q. delay (R2)
+ Processing delay (R2)
+ Transmission delay (R2) ≈ (R1)
+ Prop. delay (R2)

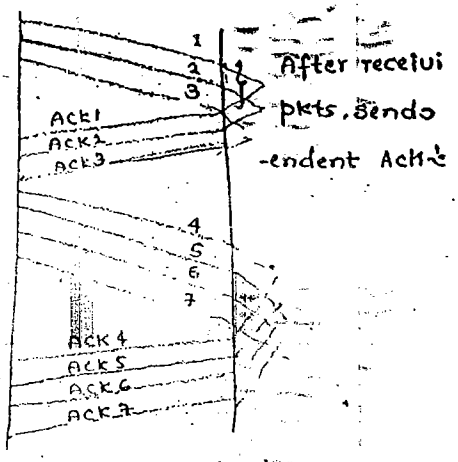
T.O = 2 * RTT



Cumulative



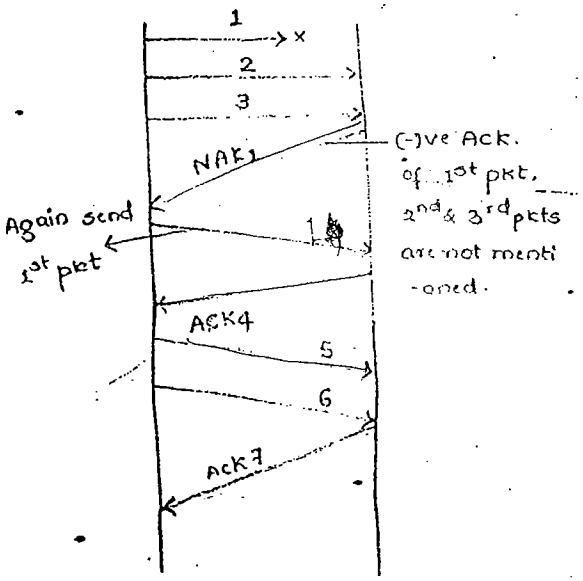
Independent

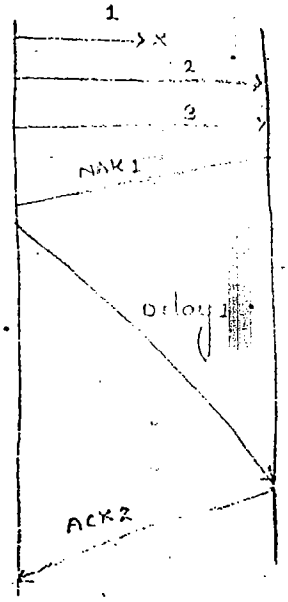


* Nlw Traffic is low.
* Reliability is low.

* Network Traffic is high
* Reliability is high

Case study for Cumulative :-





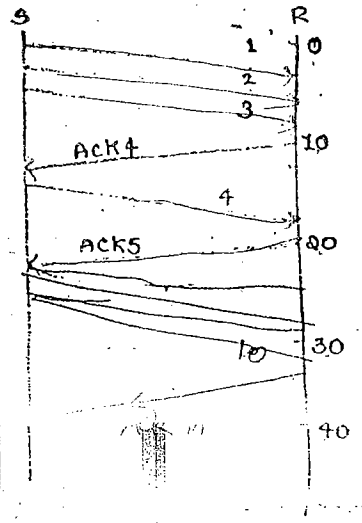
2,3 gets expired while delay occurs.

unnecessary duplicat formed in receiver.

If the delay is high to send packet 1, then at the time of receiving pkt 1, the o pkts 2, 3, ... get expired. So, again the acl of pkt 2 is sent, which is a drawback.

Combination of Cumulative and Independent (Realtime).

i.e., maintaining certain time slots., which is called practic



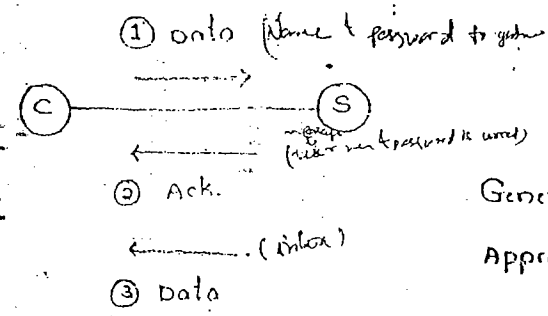
Suppose, consider 1,00,000 packe
are transfered.

If first packet is lost at rece
side. In cumulative, after all th
packets are transmitted, it sends
ack. At that time, sender knows
that first packet is lost.

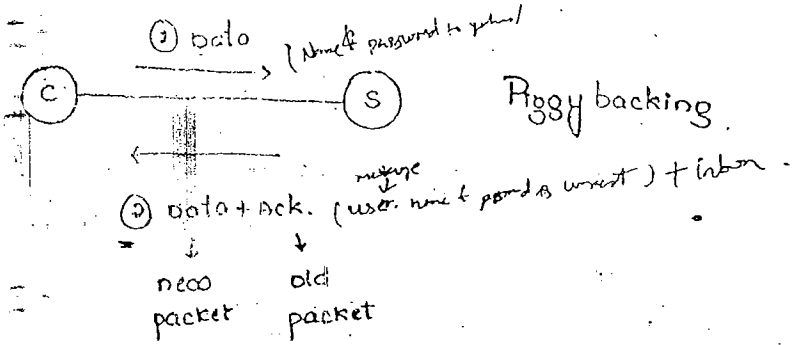
To overcome this problem, repeti
checking the slots, improves reliab

Piggy backing (web):

Mainly used in web services

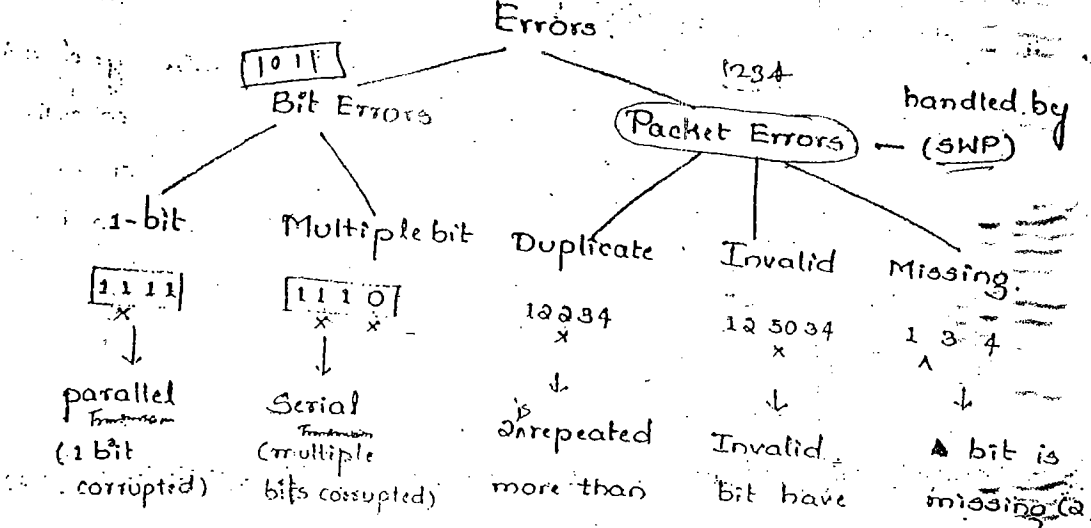


General Approach



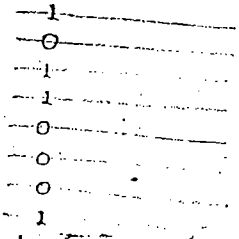
Piggy backing

Different type of errors :-



10110001 →

Serial



If link capacity = 10mbps — parallel.

In Parallel

$$\text{Bit delay} = \frac{1}{B} \rightarrow \text{Bandwidth}$$

$$= \frac{1}{10 \times 10^6}$$

$$= 0.1 \mu\text{sec}$$

In 1 msec., 10 bits are transferred in a channel.

single bit takes 0.1 msec

$0.1 \times 10 \Rightarrow 1$ msec (for 10 bits)

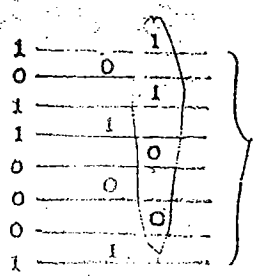
Suppose, any disturbance in 1msec, we loss 10 bits of information.

Noise is always $\frac{1}{10}$ μsec.

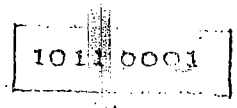
* If noise is present in serial transmission, that all the bits are corrupted, but in parallel, only that particular bit gets corrupted.

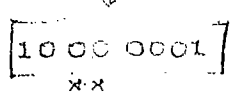
* Serial transmission is considered in computer networks.

* If length of communication is long (> 1 metre), we use serial transmission, else we use parallel transmission.

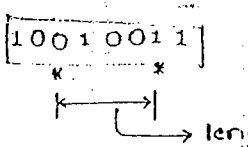


for synchronizing and collecting it takes more time (so, for long distances, it is not supportive)

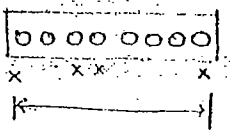




Burst length = 2.



BL = 5



BL = 8

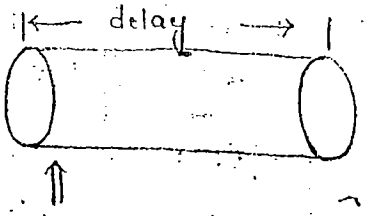
* BL is calculated as bits present between starting & ending corrupt bits.

* Burst length depends upon the type of O.S i.e., if 32-bit O.S then maximum B.L = 32. (or) If 64-bit os, then max. burst length = 64

Based on max. BL CRC develop polynomials for error checking either x^{32} (or) x^{64}

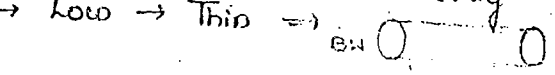
max. degree of polynomials

Bandwidth x delay :



BW x delay → high → Thick

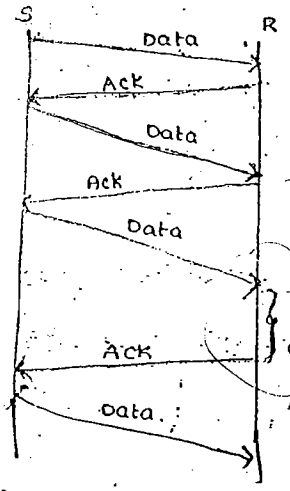
BW x delay → Low → Thin



Stop-and-wait protocol :- (part of sliding window protocol):

Rule 1 :- Transfer only one packet at a time.

Rule 2 :- After receiving the ack. only, the other packet is transferred

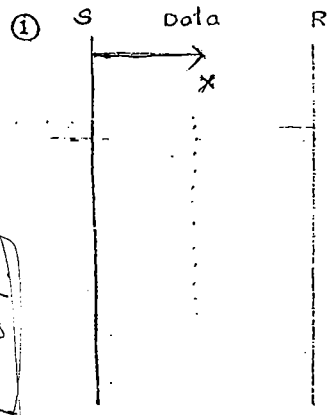


holding (when receiver is busy, it can accept new pkts, so, at that time it won't send any ack. to sender ⇒ which represents hc situation)

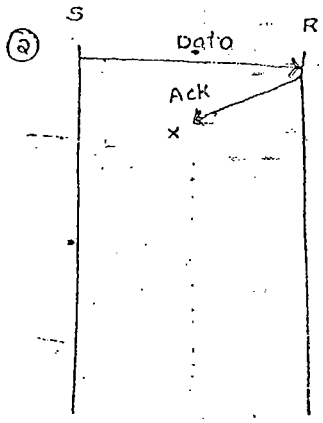
For maintaining control

* Two principles in sender
* Two principles in receiver

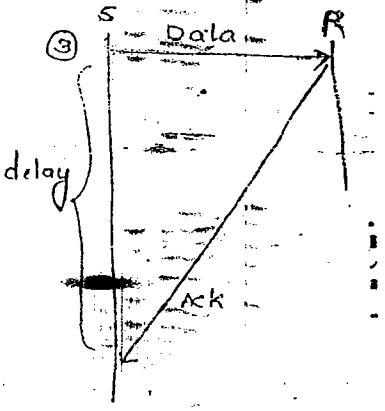
Drawbacks :-



Lost Data packet



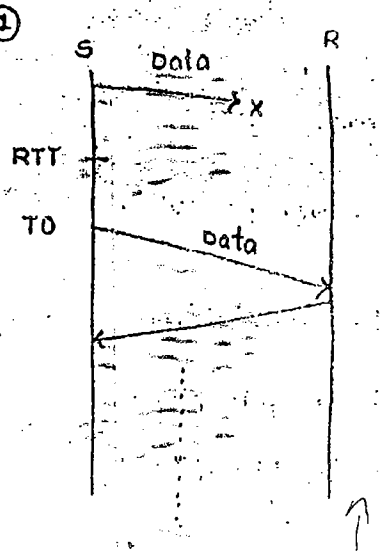
Lost Ack.



Delayed Ack.

Remedies for drawbacks

(1)

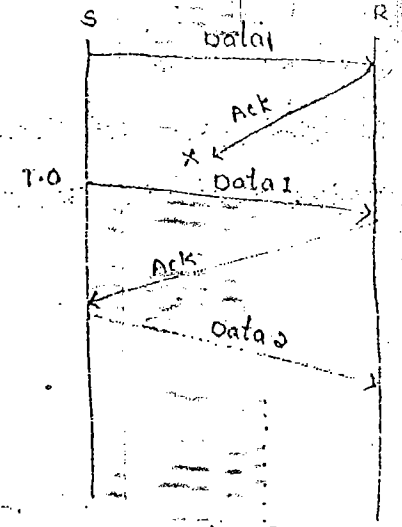


Either the lost is data (or) ack, only the timeout is considered.

If within given time, ack. is not received then next data is sent as representing it by Timeout.

Stop & wait + Timeout

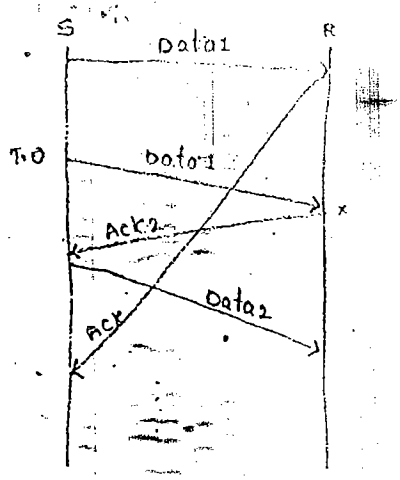
(2)

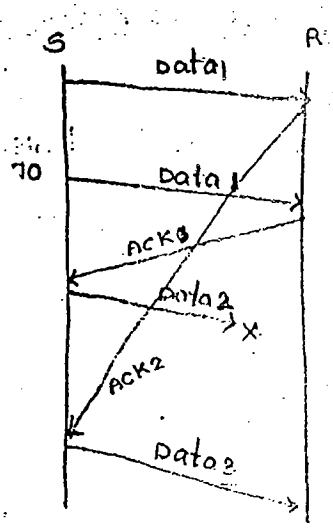


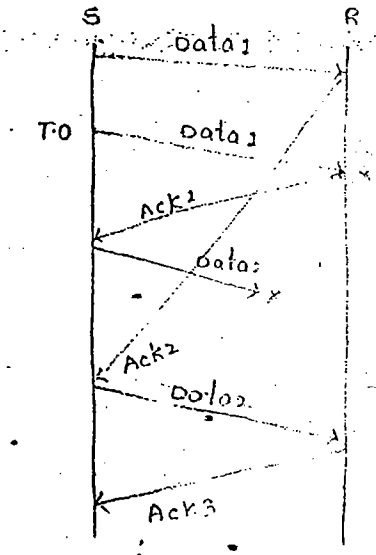
If within the time, ack of Data 1 is not received, and after data1 is received at receiver end, and sender received Ack of Data after some delay, it mean to have a ack of Data 1. So, not be get confused, Sequence no. (Data) is represented.

Stop & wait + Timeout + Sequence no. (Data)

(3)







In order not to get confused about the acknowledgement of particular data packet, the acknowledgement sequence numbers are also represented.

Stop & wait + Timeout + Sequence no.(Data) + Sequence no.(Ack)

⇓

* Automatic Repeat Request (ARR) ⇒ It controls packet level error control.

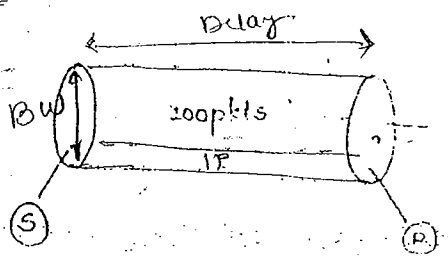
Characteristics of Stop & wait:-

* It uses the link b/w sender & receiver as a half-duplex link.

* Throughput of stop & wait protocol:

$$\text{Throughput } (T) = \frac{1 \text{ Data}}{RTT}$$

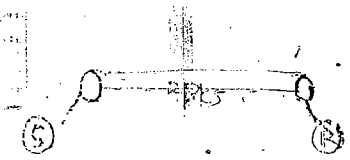
* If Bandwidth x delay product is very high, then stop & wait proto becomes useless.



capacity = 100pkts.

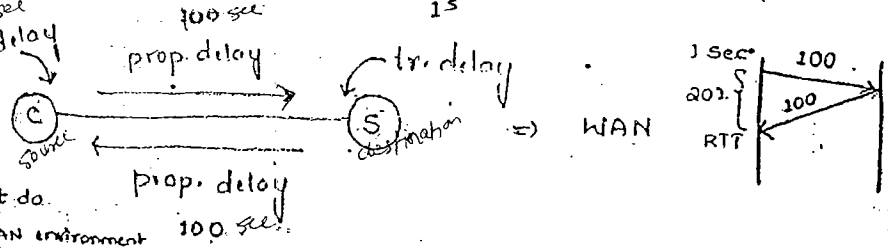
filling pipe with 1 pkt, then

$$\text{Efficiency} = \frac{1}{100} = <1\%$$



$$\text{Efficiency} = 1/2 = 50\%$$

* If propagation delay is very high compared to transmission delay, then stop & wait protocol becomes useless.

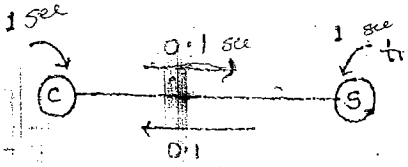


TD is 1 mean upto 202 ms. only 1 unit of time ⇒ system is busy. remaining time it don't do any work ⇒ not suitable for WAN environment

⇒ WAN

Transmission delay is high compared to propagation delay

$$\text{Utilisation} = \frac{1 \text{ sec}}{202 \text{ sec}}$$

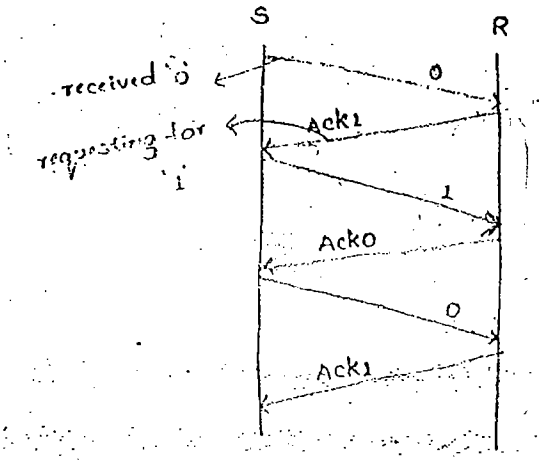


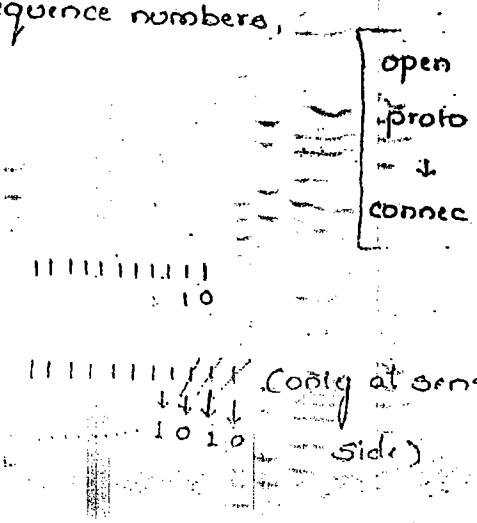
$$U_{CSMA} = \frac{1}{2.2} \Rightarrow \text{LAN}$$

depending on olp, adjust ilp

* It is an example for closed loop protocol (correction-oriented)

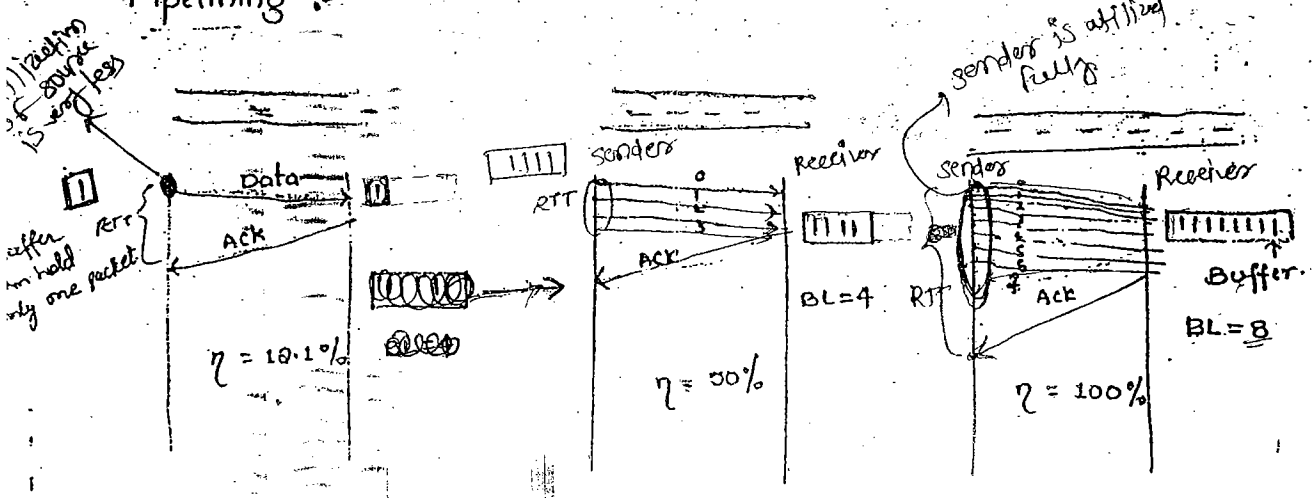
* Stop & wait protocol uses only two sequence numbers, they are : 0 and 1.





* It is a special category of stop & wait protocol with window size = 1

Pipelining :-



* Pipelining technique is a basis for Go-back-N and Selective Repeat protocols.

Limitations of pipelining technique:

(1) It requires more sequence numbers.

(2) It requires more buffer space.

1) Sender's utilization & link utilization are less, and they are not suitable for WAN environment ⇒ 3 problems (p.no: 18 : 1, 2, 3)

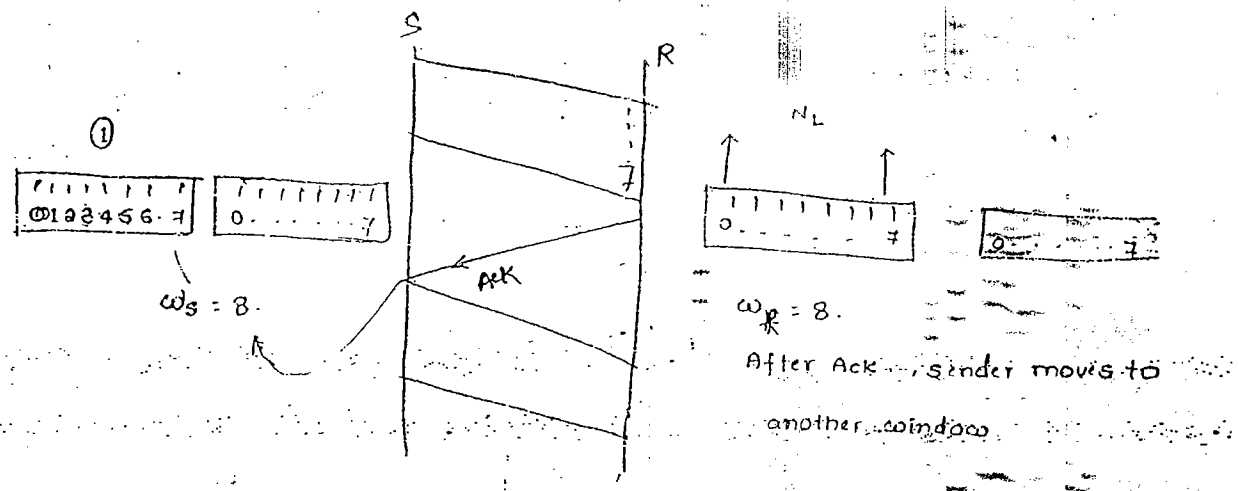
To solve these problems, we use "pipelining" Technique.

2) Within the RTT, carry as many packets as possible, which helps in improving efficiency ⇒ pipelining technique is basis for GBN and SR protocols.

Sliding-Window Protocol

17/07/2010

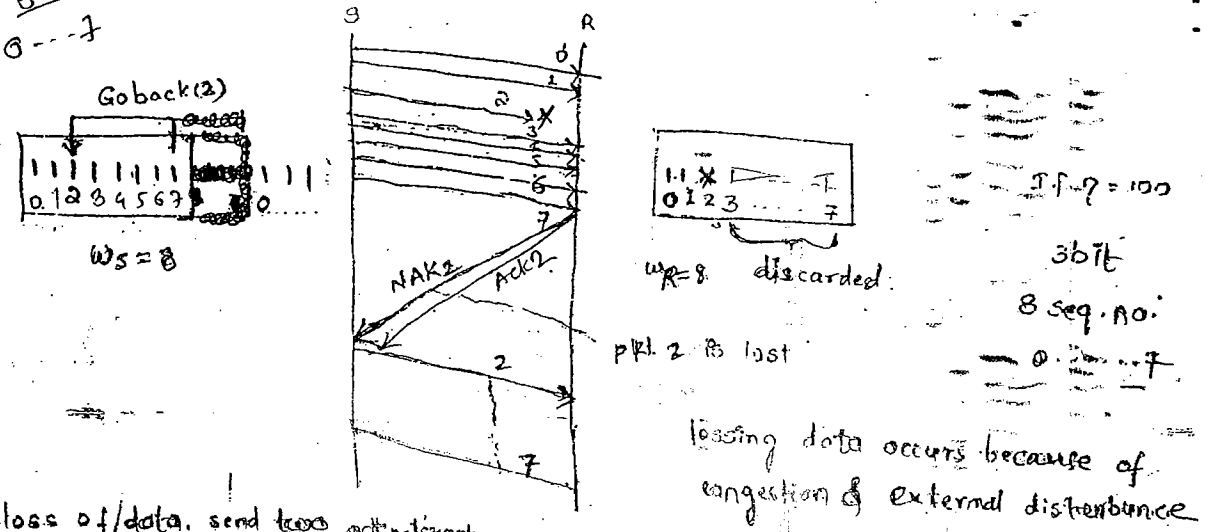
Saturday



After Ack --, sender moves to another window.

Go-back-N characteristics :-

* Go-back-N receiver never receives out-of-order packets.
* It's natural choice is cumulative ack. (if possible it also uses piggy-backing ack.)

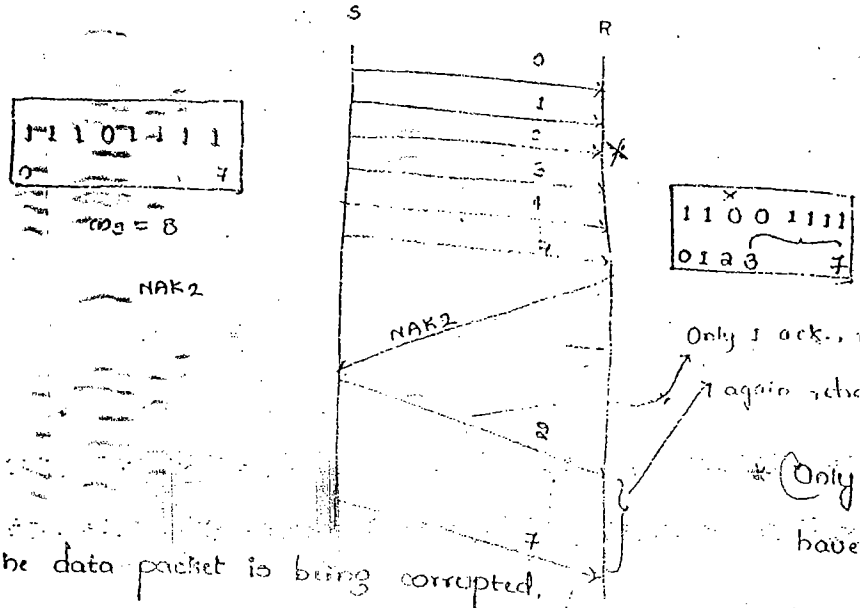


In loss of/data, send two acknowledgment NAK 2 & Ack 2.

loosing data occurs because of congestion & external disturbance

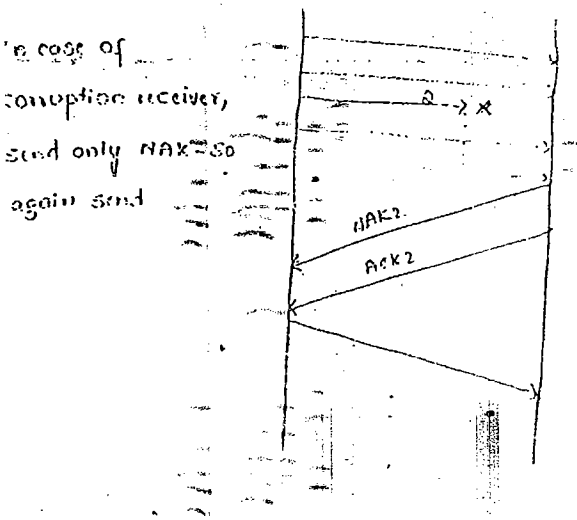
In the series sending packets, If pkt2 is missing, and all the seven pkts are being sent, then the NAK_2 is sent. Then, 3 to 7 pkts are being discarded and the pkt_2 is re-transmitted.

Corrupted data packets :-



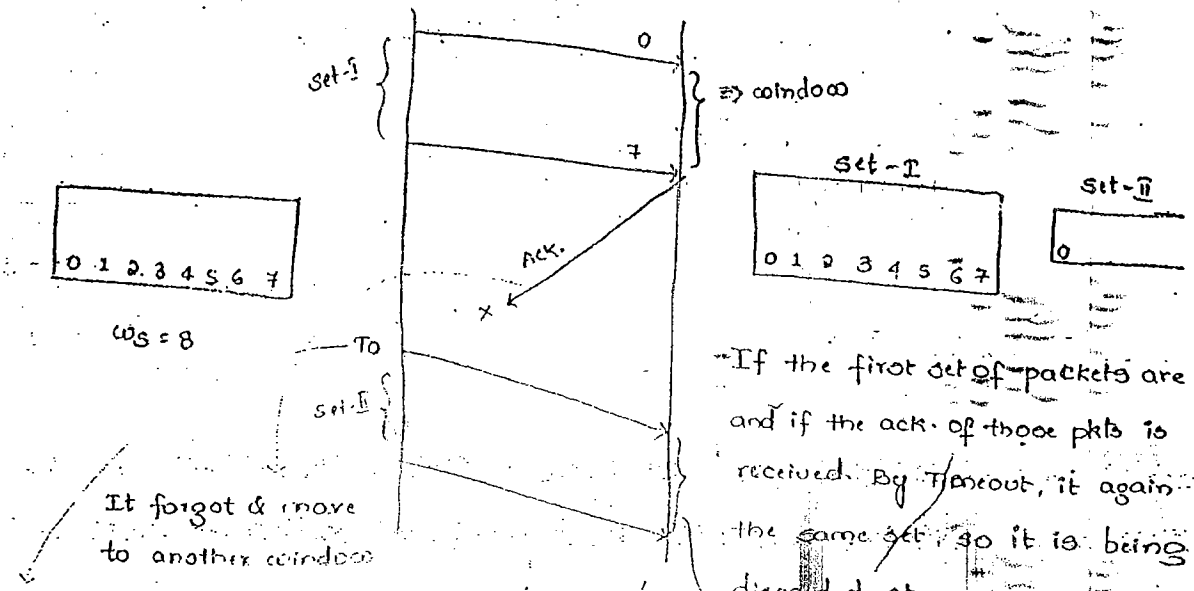
Here, the data packet is being corrupted, then also the remaining all the packets are also get discarded.

* Only the lost packet have more impact than that of the corrupted data packet.



$\Rightarrow$ Lost data packet.

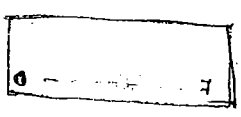
So, in order to overcome the above problem of data lost, while sending the NAK_2, ACK_2 is also being sent. so that it represents that pkt_2 is not received and then after sending pkt_2, it can continue from ACK_3.

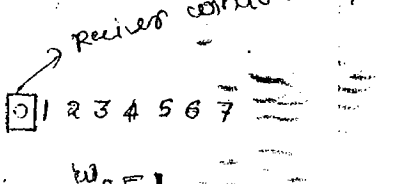


To solve the above problem, we have to re-adjust w_S, w_R sizes:

Case (a) : W_R Size

It is equal to 1 always irrespective of W_S size.





So, here it is waiting for 1 after completion of '0' and if any other numbers other than 1 comes, they are discarded.

Case (b) : W_S Size

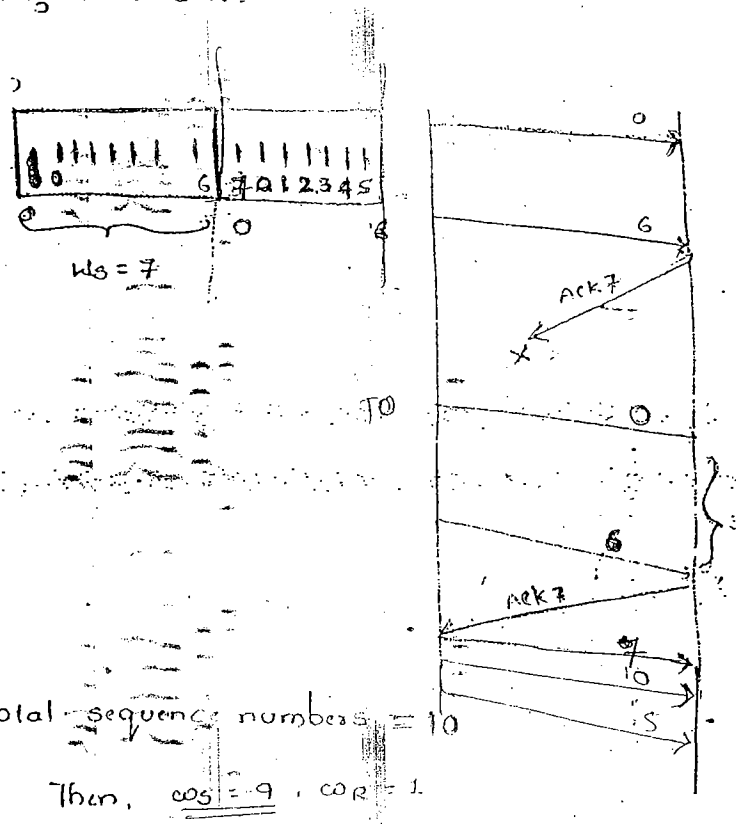
W_S size is calculated based on following formula :-

$W_S + W_R \leq$ Available Sequence number (ASN)

$W_S = ASN - W_R$

$W_S = ASN - 1$

Adjusting window size:



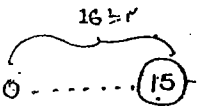
Generally ASN = 8

$W_S = 8 - 1 = 7$.

0 1 2 3 4 5 6 7 0 1 2 3 4 5 6

$W_R = 1$

It is waiting for 7



max. Sequence no's = 16

Total sequence numbers = 10

Then, $W_S = 9$, $W_R = 1$

$W_S + W_R \leq$ Avail. Sequence no

$W_S = 15$

$W_R = 1$

$W_S + W_R = ASN$

$W_S + 1 = 10$ (GBN)

$W_S = 10 - 1$

$W_S = 9$

(1) Assume N = maximum available sequence numbers.

$$\therefore \boxed{\omega_S = N - 1}$$

$$\boxed{\omega_R = 1}$$

(2) If 'N' is defined as maximum sequence numbers.

$$\therefore \boxed{\omega_S = N}$$

$$\boxed{\omega_R = 1}$$

(3) If 'k' is no. of bits available in sequence number 'p'.

$$\boxed{\omega_S = 2^k - 1}$$

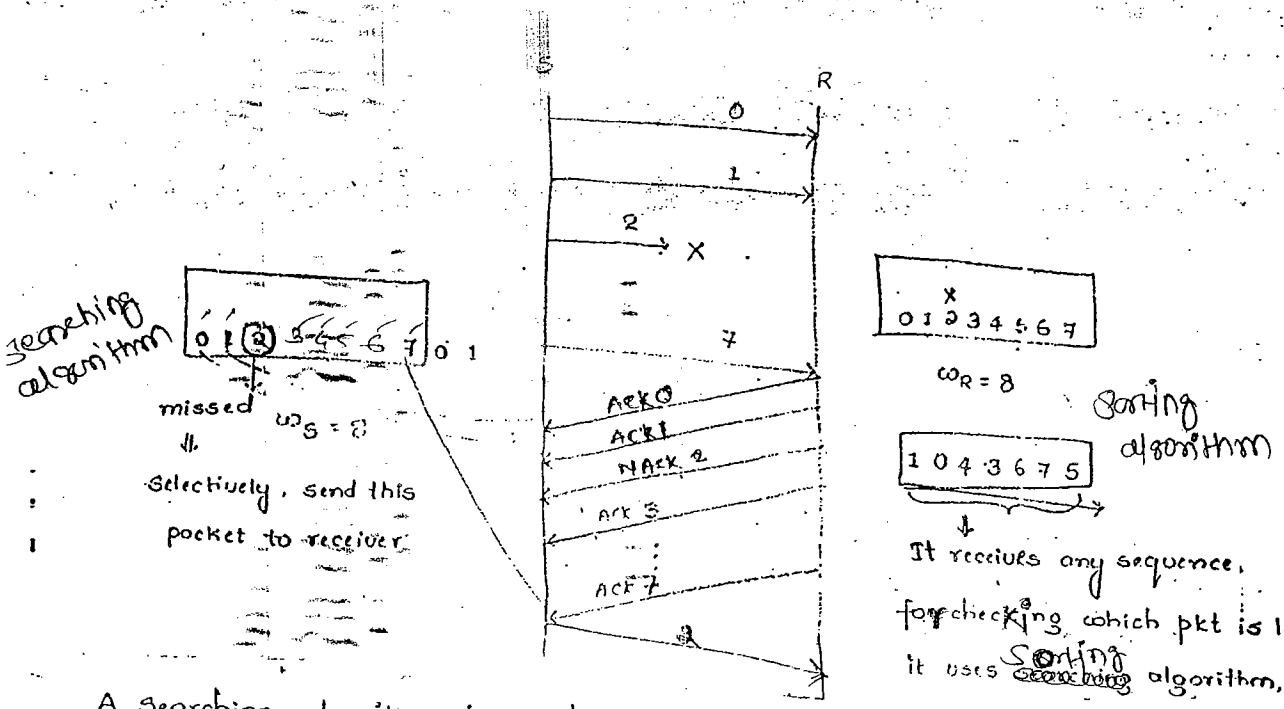
$$\boxed{\omega_R = 1}$$

	ω_S	ω_R	ASN
It represents →	1	1	8
Stop & wait protocol	2	1	
	3	1	
	4	1	
	5	1	
	6	1 ✓	≤ 8
	7	1 ✓	≤ 8

Selective Repeat Protocol:-

Characteristics :-

* Selective Repeat receiver receives out of order packets.
* It's natural choice is Independent ack. (if possible, it will also use piggy-backing).



A searching algorithm is used.

Disadvantages :-

(1) Time increases as it requires searching and sorting of nomber of packets to be transmitted, explicitly.

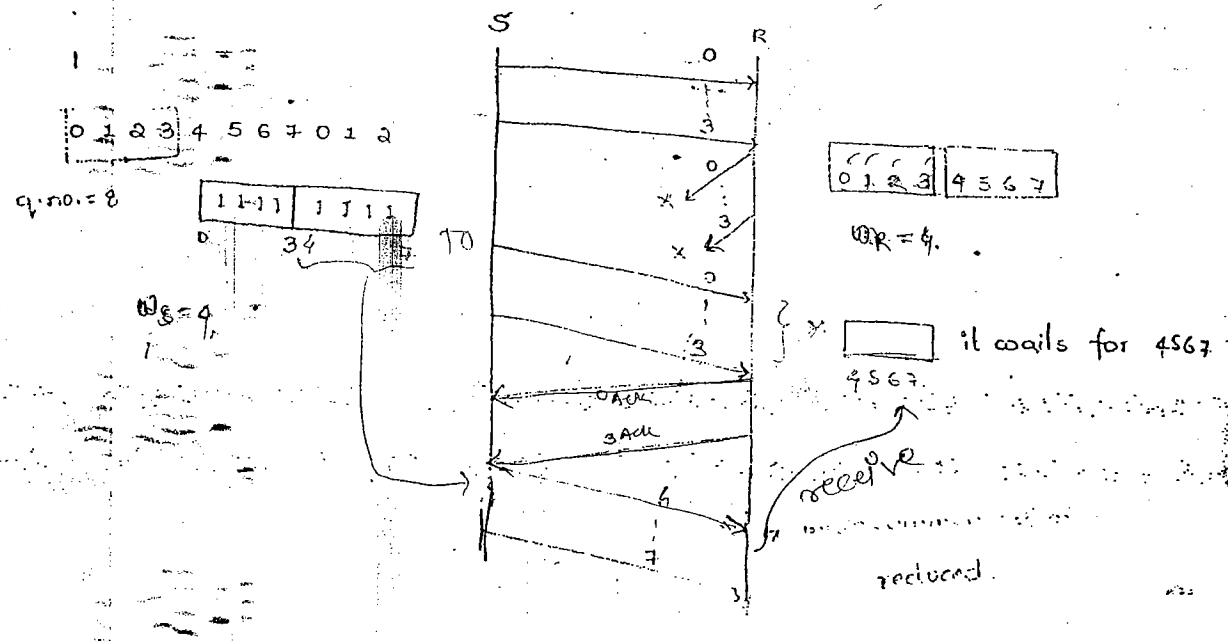
To solve the above problem, we re-adjust W_S and W_R based on the following formula

$W_S + W_R \leq ASN.$

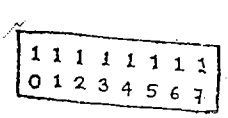
① $W_S = W_R$

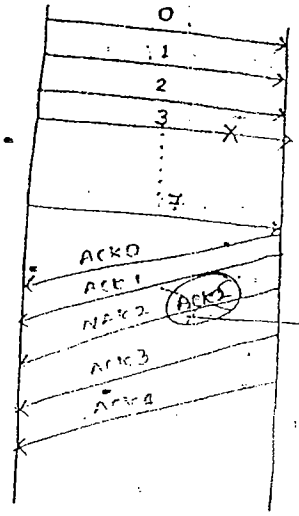
② $W_S > W_R$

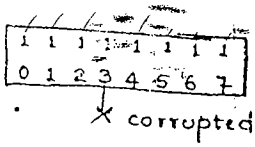
③ $W_S < W_R$: X (meaningless)



② Corrupted





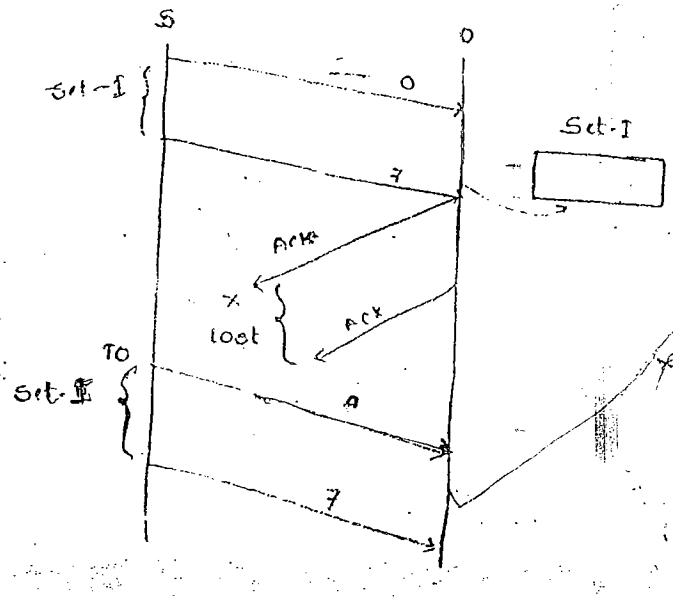


we coon't resolve the condition either pkt is lost (or) corrupted because everytime it sends only NAK.

we cannot communicate with sender that which packet is lost and which is obtained.

Since, ACK2 is not sent with NAK2, which represents a situation of "Ambiguity".

③ Lost Acknowledgement s-



it is waiting Indefi
of packets but
receiving
of pack
again.

Infinite communication

(1) If N is defined as max. available sequence no., then

$$W_S = \frac{N}{2} \qquad W_R = \frac{N}{2}$$

(2) If N is defined as max. sequence no. then.

$$W_S = \frac{N+1}{2} \qquad W_R = \frac{N+1}{2}$$

(3) If 'k' is defined as no. of bits in sequence number 'p'.

$$W_S = 2^{k-1} \qquad W_R = 2^{k-1}$$

3 bit
8 seq no.
$W_S = 2^{3-1} = 2^2 = 4$ | $W_R = 2^{3-1} = 2^2 = 4$

8 sequence number

Go back-N	$W_S = 7$	$W_R = 1$	⇒ It can transfer more packets
Selective Repeat	$W_S = 4$	$W_R = 4$	

for same available sequence number, GBN can transfer more packets.

GBN*	$W_S = 7$	$W_R = 1$	⇒ (8)
SR.	$W_S = 7$	$W_R = 7$	⇒ (14)

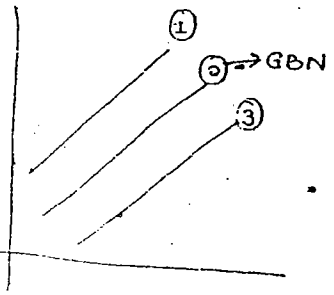
0 1 2 3 4 5 6 | 0 1 2 3 4 5 6

$W_S + W_R \leq ASN$ for SR

Comparision of

Characteristics	Stop & Wait	GBN	Selective Repeat
1. Operation	Simple	Medium	Complex
2. Requirement of Seq. numbers	Low	medium	High
3. Bandwidth utilisation	Low	Medium	High
4. Buffer Requirement	Low	Medium	High
5. Efficiency	Low	Medium	High

Stop & wait formulae :-



$$U_s = \frac{\text{Tran. delay}}{\text{Tran. delay} + 2 * \text{prop. delay}}$$

$$= \frac{1}{1 + 2\,\frac{\text{pro. delay}}{\text{Tran. delay}}} = \frac{1}{1 + 2a} \Rightarrow a = \frac{t_{prop}}{t_{trans.}}$$

$$= \frac{L/B}{L/B + R}$$

$$\eta = \frac{L}{L + BR}$$

$L = BR \quad \eta = 50\%$

$L > BR \quad \eta > 50\%$

$L < BR \quad \eta < 50\%$

Steps to be solved in sliding window :

(1) Calculate RTT.

(2) Based on given bandwidth and RTT, calculate no. of bits we are able to transfer within RTT and equate it as "window of bits" (W_{bits}).

(3) $W_{pkt} = \frac{W_{bits}}{(pkt\ size)_{bits}}$

(4) Sequence numbers required = W_p

(5) $2^k = W_p$,

where $k \rightarrow$ no. of bits in sequence number 'p'.

$RTT * BW = seqn\ bits$

L

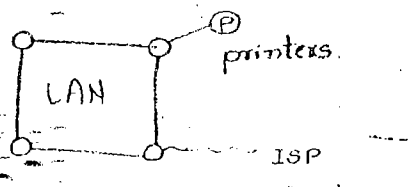
19/07/2010

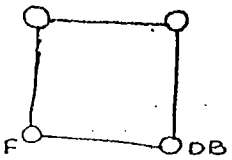
Monday

LAN Technologies:-

Advantages of LAN:-

* Resources sharing (or) resource utilization (Hlco & Slco)
* Information sharing





Types of LAN's:-

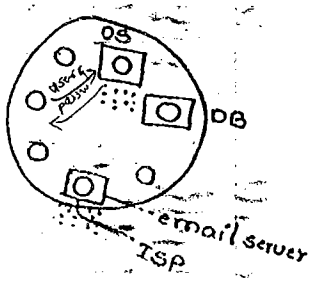
* Dedicated server LAN.
* peer-to-peer LAN
* zero slot LAN.

(College Campus) (Drawing centre)

	Dedicated server LAN	Peer to peer LAN	Zero slot LAN
Market share	80%	10-15%	5%
Security	High	Moderate	Loco
No. of system (Capacity)	Any	50-60	<10
Application	Any	feco	very feco.
Cost	High	moderate	Loco
Requirement	IP, NOS, NIC	NIC	≠ X

Dedicated Server LAN's :-

* To access os (or) Database, username and password must be submitted and then again to access internet, username & password are again needed to be submitted provided by ISP.



* Security is provided at three levels :-

Network level Security	User level Security	Application level Security
⇓	⇓	⇓
without userid and pwd, no one can access	Based on type of users, there are some restrictions to some users to access data.	There are restrictions on some data (or) some files.

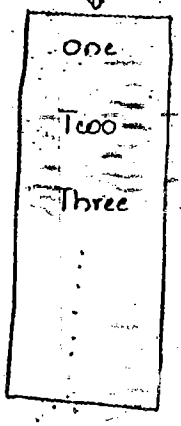
Peer-to-Peer LAN's :-

* As ~~As dedicated server~~ LAN's, there is no requirement of Network operating system and IP addresses.

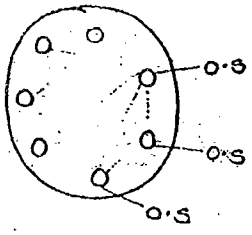
Right click ⇒ TCP/IP

- Domain also ⇓ dedicated Server LAN's
- workgroup also ⇓ peer-to-peer ~~Server~~ LAN's

ACE → work group



→ names of individual systems within a work group.



* Communication done among the systems within a work-group.

* Since, names are being included to individual systems, only a limited no. of systems are get connected. Because, there is a chance of occuring "naming conventions".

work group ⇒ All the systems are being connected for the purpose of communication among them.

* There is no particular leader in the work group. All the systems are considered equal. Hence it is called peer-to-peer.

Eg:- Browsing centre.

(contains no. of clients & only one system where internet facility is available. no of client can get internet access from that system without username & password providing)

* They have less security and more flexibility.

Zero slot LAN : (no slot is necessary for connection)

* NIC is not necessary.

Eg:- Home networks

(using USB ports, communication is done)

* No slot is necessary to insert the NIC into mother board.

At the most, we get 2 serial
2 parallel
4 USB ports, so it has < 10 systems

* No real time applications, and oracle applications are possible.

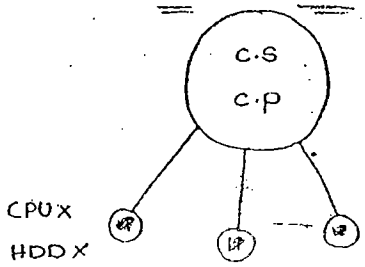
LAN components :

(1) Network operating system (NOS)

(2) Cable

(3) NIC

(1) First Generation

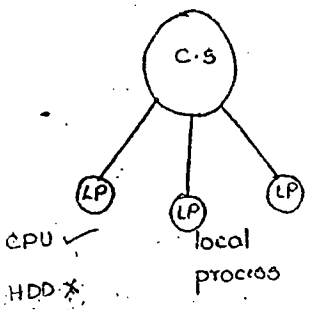


Eg:- UNIX

* Central storage
* Central process.

windows ⇒ distributed environment

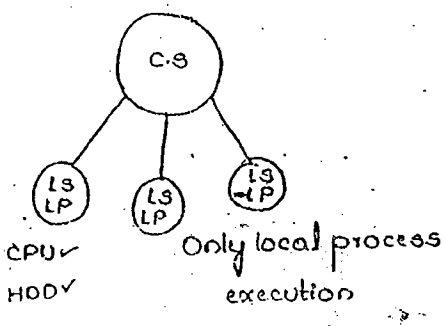
(2) Second Generation



Thin client

Eg:- Novell Networks

(3) Third Generation



Eg:- windows., Linux.

UID :

PWD :

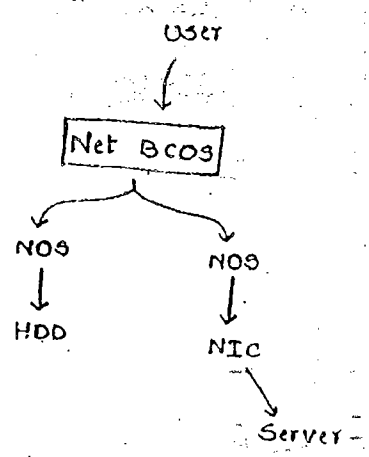
Domain name : This system ▽

↘ local system accessed.

If Domain name ▽

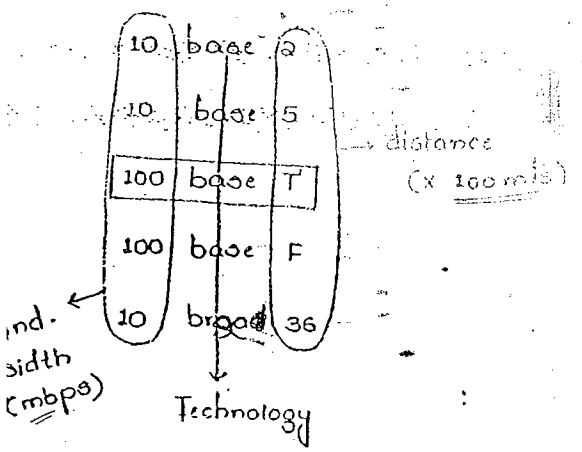
↓

Then entire nlw is accessed.



a) Cables :

Types of cables :



Base band ——— LAN

Broad band ——— WAN

Directly connected with ISP, (no tele-communi-cations)

Dial-up connections

⇓

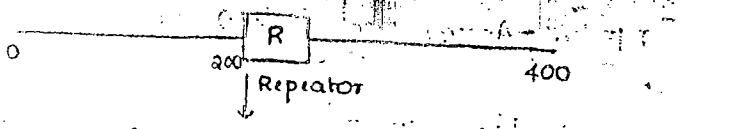
* Broad band ⇒ All types of frequencies are carried out (Airtel, Idea, ... etc)

Baseband ⇒ Single type of frequency. Base 2 : up to 200 mts, without signal loss

In cable TV networks,

"Boosters" are used within limited distance.

Beyond 200mts, we use "repeaters".



* Twisted pair ⇒ 100 mts
* Fibre optic cable ⇒ 2000.

functionality ⇒ based on connection, it used particular signal.

100 base T ⇒ category 5 cables ⇒ bulky ⇒ RJ45 connectors are used.

category 3 ⇒ Incoming signals. To repeat the signal, repeaters are used.

(3) NIC :-

Hardware — physical layer

PL + DLL (combination of HLC & SLC).

* Neco technology systems use these NIC cards

IEEE 802. :-

** These are exclusively meant for LAN's.

** Main layers :-

* Transport layer
* Network layer (If any problem at sender (or) receiver, then it is used)

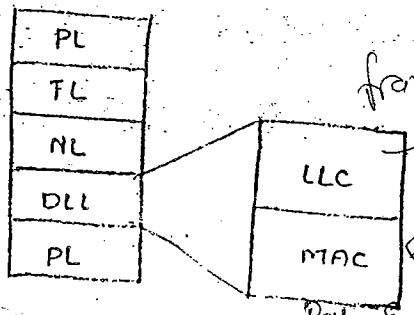
** Segmentation & Re-assembly :-

* In local network, no need of it.
* For LAN's Transport layer & Network layer's are not needed
* So, main focus is on Data link layer and physical layer.

LLC ⇒ framing.

Media Access Control (MAC):

* Error control
* Flow control
* Access control
* Physical address



Data encapsulation including frame assembly before transmission, & frame parsing/error detection during & after reception.

Different types of LAN's for different applications:-

* For real time applications, MAC is replaced with another MAC.

IEEE 802.1
- .2
- .3 Ethernet ✓
- .4 Token Bus
- .5 Token Ring ✓
- .11 Wireless LAN ✓
- .16 Wireless MAN ✓
- .17

Eg:- For real time application, MAC is replaced with 802.5

Ethernet:-

Characteristics:

* Ethernet offers connectionless communication.
* No flow control & packet level error control (bit level error control).
* No acknowledgement (either (+)ve or (-)ve).
* It uses bus topology.
* It uses CSMA/CD as an access control method.

Carrier Sense Multiple Access / Collision Detection (CSMA/CD):

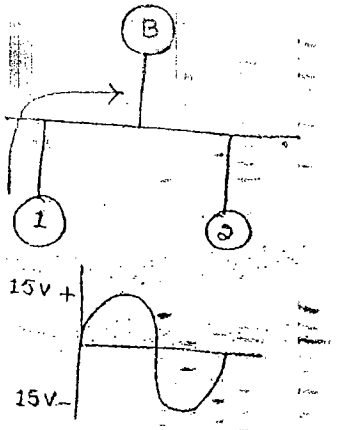
* Sense the channel, whether communication is taking place or not. If there, then wait for the another channel to complete its transfer of data packet or else transmit the data packet from the current channel only.

* The channel is sensed in terms of voltage.

If $\boxed{V=0}$ $\Rightarrow$ no waveform

i.e., no channel is engaged to transfer packet (media is free)

So, any channel can transfer the data packet.

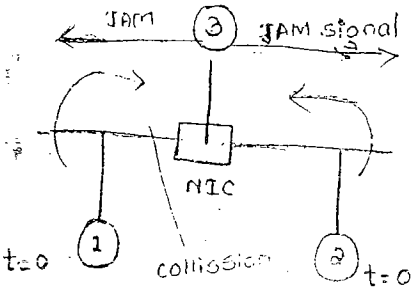


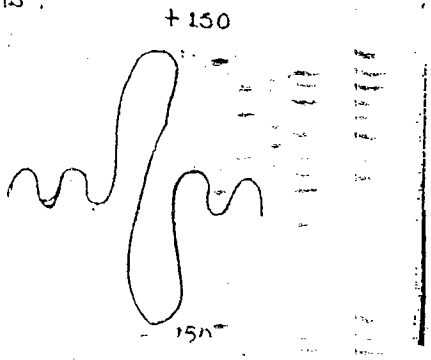
Multiple Access :-

* If more than one channel, sense the medium (then, if medium is free), both the channels try to access the medium and want to transfer data packets simultaneously then it is called multiple access.

Collision Detection:

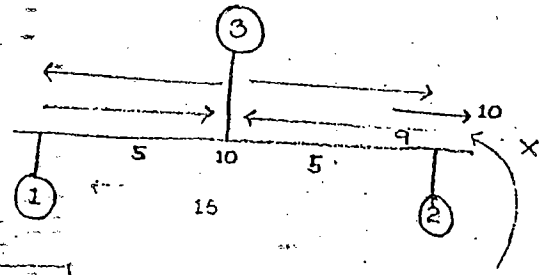
* At the situation of multiple access of channels, collision occurs while transferring data packet. So, a JAM signal is used to detect the occurence of collision and it is sent to both the channels.





* All channels are having different frequency and Jam signal have different frequency. So, there is no chance of collission occurance.

* Since channels have different frequency ⇒ Bandwidth increases.



100 | 10 | 9 | x | minimum = 20

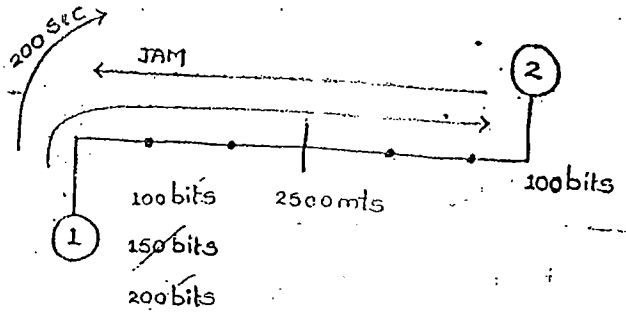
Si system have 100bits, t = 0
Sa have 10 bits, assume : 5
that they both take : 5
the channel at a time, : 10
then collission occurs. : 10

for recognizing collission, every system, maintains min. frame size based on channel length.

for min. size pkt,
condition is, :— RTT = Tr. Delay

RTT = 200 sec = tr. delay

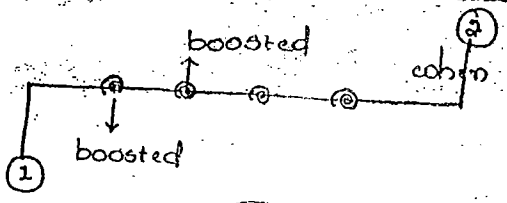
RTT = Trans. delay



for sending collision, one need atleast 100 bits.

t = 0
: 50 sec
: 100 sec
: 200 sec

t = 0
: 50 sec
: 100 sec



cohen repeators are allowed.

cohen repeators are allowed $\leftarrow 2 * \frac{d}{v} = \frac{L}{B}$

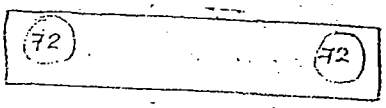
$2\left(\frac{d}{v} + 4 * \text{Repeator delay}\right)$

$57.6\ \text{msec} = \frac{L}{10 \times 10^6}$

L = 576 bits (or 72 bytes.

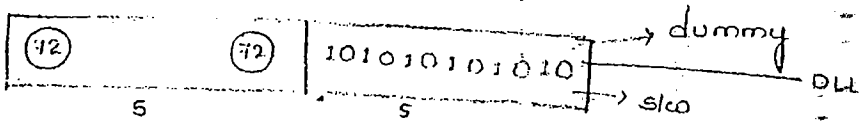
Basic Ethernet	Fast Ethernet	Gigabit Ethernet
10 mbps	100 mbps	1 Gbps
2500 mts	250 mts	250 mts.
72 bytes	72 bytes	72 bytes.

Basically,
25 mts,
720 bytes.



10

= 720



— llco padding

Back-off Algorithm:

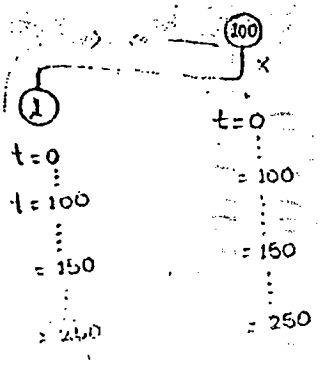
* It gives waiting time for the stations that are involved in collision.

Waiting time = $K \times 51.2\ \mu sec$ (Standard RTT)

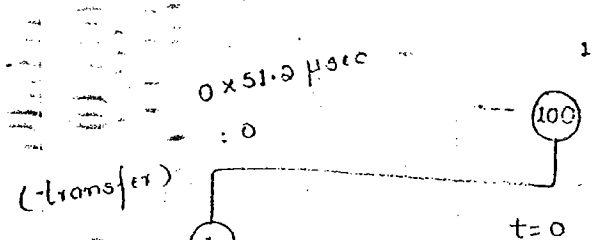
where $K \rightarrow$ randomly derived

from 0 to $2^n - 1$

where $n \rightarrow$ collision number.



Case study:-



$\eta = 50\%$

$= 25\%$

$= 12.5\%$

t=0

=100sec

n = 1 2 3

0 1 2 3 ... 9

Let n = 1 0 1 2 3 ... n

$\therefore K = 0$ to $2^n - 1$

$= 0$ to $2^1 - 1$

$= 0, 1$

t=0

=100sec

n = 1 2 3

0 1 2 3 ... 9

Let n = 1 n = 10

$K = 0$ to $2^n - 1$

$= 0, 1$

If let consider $K = 0$ to channel 1 and $K = 1$ to channel 100

then waiting time of channel 1 = $0 \times 51.2\ \mu sec$

$= 0$

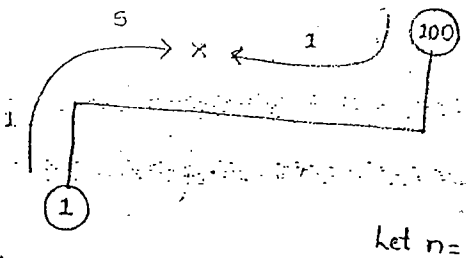
waiting time of channel 100 = $1 \times 51.2\ \mu sec$

$= 51.2\ \mu sec$.

∴ So, channel 1 have waiting time = 0, then it can transfer the data packets., but channel 100 most wait upto 51.2 μsec and then again back-off algorithm is applied to proceed the transmission through either channel 100 (or) others.

Limitation of Back-off Algorithm :-

* Capture Effect.



Let $n = 1$

$\therefore K = 0$ to $2^n - 1$

$= 0, 1$

Then, $\omega \cdot T = 0 \times 51.2$ μsec

$= 0$

Let $n = 1$

$\therefore K = 0$ to $2^n - 1$

$= 0, 1$.

$\omega \cdot T = 1 \times 51.2$

$= 51.2$ μsec.

$n = 2$.

$K = 0$ to $2^n - 1$ ⟸

$= 0$ to $2^2 - 1$

$= 0, 1, 2, 3$.

If, after 51.2 μsec, again another channel also wants to access the medium, then again back off alg. is applied, then $n = 2$.

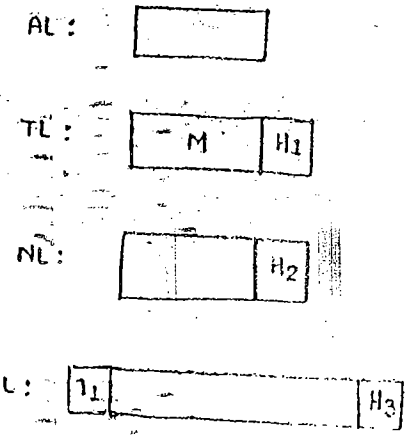
$\therefore$ ∀

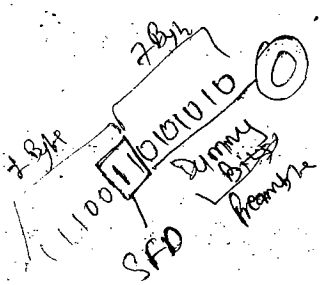
Then, repeat same for $n = 3$.

$K = 0$ to $2^3 - 1$

$= 0, 1, 2, 3, 4, 5, 6, 7$

Then, the probability of channel 1 and channel 100 to access the



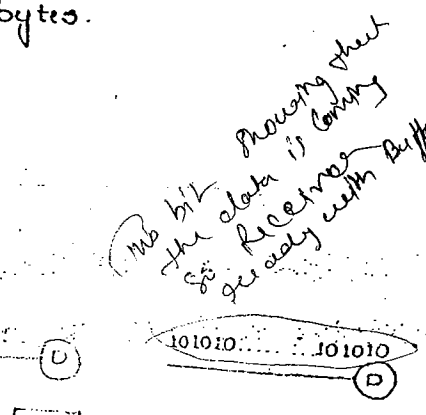


Preamble :-

* It contains continuously 1's & 0's for seven bytes.
* It is used for synchronization purpose.

SFD (Start of frame Delimiter) :-

* It signals actual start of the frame.
* Dummy bits are represented by preamble and SFD.



Source & Destination Address :-

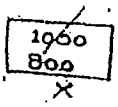
* They are 48 bit physical addresses representing source & Destination.
* Minimum size of data = 46 bytes, so that we make out 72 byte frame.
* Maximum size of data = 1500 bytes — To avoid monopolization ⇓ chance given to other channels also.

min.	max.	
46	1500	– data
72	1526	– frame
64	1518	– frame from source address

⇒ preamble & SFD are neglected.

Length of data : (no. of bytes present in data field)

* Since data is varying from 46 to 1500, to keep track correct size of the data in packet, we need "length of data" field.

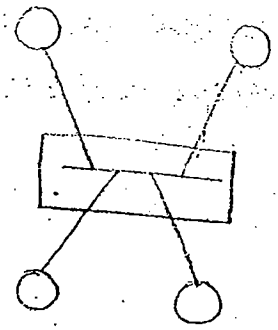


After 800, data start

CRC :-

* It is added only at the tail end to identify bit errors.
* To avoid more no. of transmissions, we use C.R.C at tail end.

Implementation:

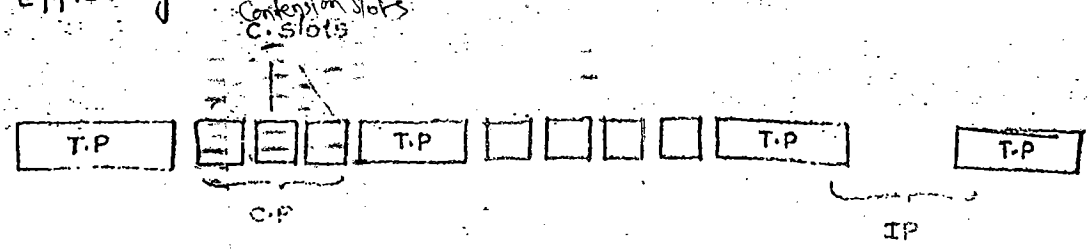


- Physical addressing - Star topology
- Logical addressing - Bus topology.

11/07/2017

Wednesday

Efficiency calculation of Ethernet:



T.P → Transmission period

C.P → Collission period

I.P → Ideal period

$$\text{Efficiency } (\eta) = \frac{T.P}{T.P + C.P + I.P \to 0}$$

$$\boxed{\eta = \frac{T.P}{T.P + C.P}}$$

Let N → Total no. of systems in network.

P_s → Probability of a station to transfer data packet.

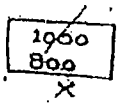
$1 - P_s$ → Probability of a station not to transfer data packet.

To get a successful transmission for a station, remaining (N-1) stations shouldn't transfer the data packet.

$(1-P)^{N-1}$ ⇒ probability for the remaining (N-1) stations not to transfer data packets.

Length of data : (no. of bytes present in data field)

* Since data is varying from 46 to 1500, to keep track correct size of the data in packet, we need "length of data" field.

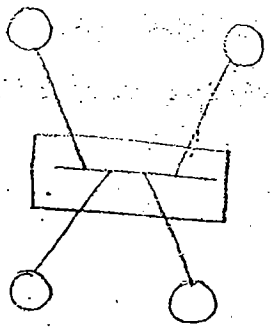


After 800, data start

CRC :-

* It is added only at the tail end to identify bit errors.
* To avoid more no. of transmissions, we use C.R.C at tail end.

Implementation:



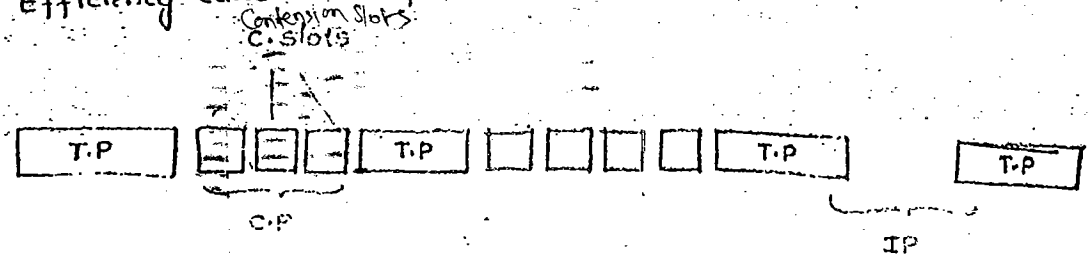
Physical addressing - Star topology

Logical addressing - Bus topology.

11/07/2017

Wednesday

Efficiency calculation of Ethernet:



T.P → Transmission period

C.P → Collission period

I.P → Ideal period

$$\text{Efficiency } (\eta) = \frac{T.P}{T.P + C.P + I.P}$$ (I.P → 0)

$$\eta = \frac{T.P}{T.P + C.P}$$

Let N → Total no. of systems in network.

P_s → Probability of a station to transfer data packet.

$1 - P_s$ → Probability of a station not to transfer data packet.

To get a successful transmission for a station, remaining (N-1) stations shouldn't transfer the data packet.

$(1-P)^{N-1}$ ⇒ probability for the remaining (N-1) stations not to transfer data packets.

$P_s(1-P_s)^{N-1}$ ⇒ Probability of the success for a single station.

$$NP_s(1-P_s)^{N-1} = A$$

⇩

It is the probability of success for any arbitrary station among 'N' stations.

No. of contention slots = $1/A$

If $N \to \infty$ ⇒ $A = \frac{1}{e}$ (exponential)

No. of contention slots = $\frac{1}{A}$

$= \frac{1}{1/e} = e$

Success rate 1 → 1 Attempt ; Successful

$\frac{1}{0.5} \to 2$

$\frac{1}{0.25} \to 4$

Based on 'A' value decide contention slots :

$A = 1/5 = 1/n = 5$

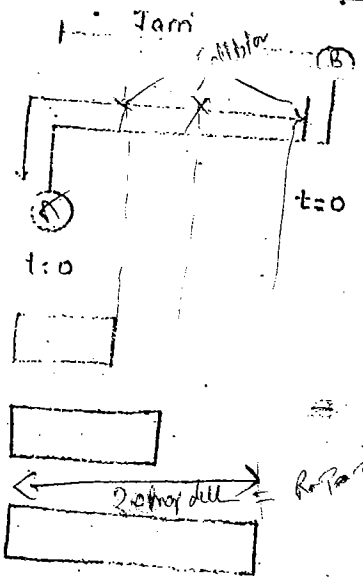
0 to $2^5 - 1$

0, 1, 2, ... 31 slots

Contention period (c.p) = No. of contention slots * slot duration

slot duration:

c.p = $e * 2$ prop. delay



Suppose out of possibility select '30' slot time duration.

= 30 * 2 * prop. delay

↓

max. slot value = 'e'.

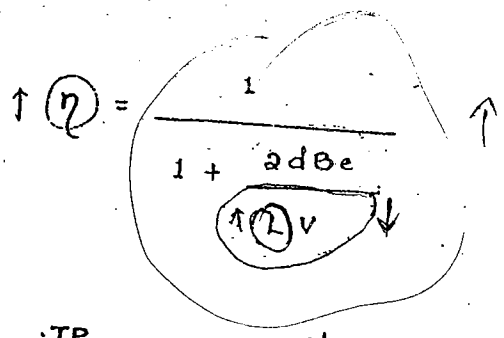
Transmission period = $\frac{L}{B}$

$$\eta = \frac{T \cdot P}{T \cdot P + C \cdot P}$$

$$= \frac{4B}{4B + 2 \times \frac{d}{v} \times e}$$

$$\boxed{\eta = \frac{1}{1 + \frac{2dBe}{Lv}}}$$

It Says that i give you a-callibility to transmit data after some time (waiting=free) you can send directly.

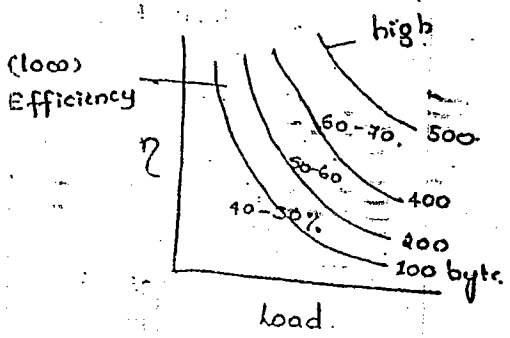


(1) $\eta = \frac{TP}{TP+CP} = \frac{t_{trans}}{t_{trans} + 2t_{prop}e}$

$= \frac{1}{1 + 2\frac{t_{prop}}{t_{trans}}e}$

$= \frac{1}{1+2ae}$

$\boxed{\eta = \frac{1}{1+5.44a}}$



If load increases, efficiency decreases.

If pkt size increases, then efficiency also increases.

★ (Q)

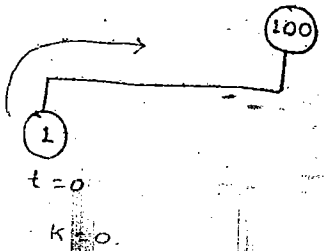
$\eta = \frac{T \cdot P}{T \cdot P + C \cdot P + t_{prop}}$

$= \frac{t_{trans}}{t_{trans} + 2t_{prop}e + t_{prop}}$

$= \frac{1}{1 + 2\frac{t_{prop}e}{t_{trans}} + \frac{t_{prop}}{t_{trans}}}$

$= \frac{1}{1+2ae+e} = \boxed{\frac{1}{1+6.44a}}$

calculation of aborted bits are possible within the transmission.



Every station must be coailed for one fraction time. After collission, aborting bits from collission point.

Advantages of Ethernet :

* Cost of Ethernet is less.
* Ethernet cables are robust to noise.
* Simple operation. (Admin. & Maintainance are simple)

Disadvantages:- of Ethernet :

* Ethernet offers non-deterministic service. Therefore, it is not suitable for real-time applications.

  Eg:- CNC machines.

* There are no priorities in ethernet. Therefore, not suitable for client-server applications.
* There is a restriction on the minimum size of packet. Hence, it is not suitable for interactive applications.

  (Size of packets in interactive app. is small. less than 46 b

  * Interactive applications needs 1 (or) 2 bytes.

  Eg:- ATM machines (options ⇒ bits.
  pin no. ⇒ bytes)

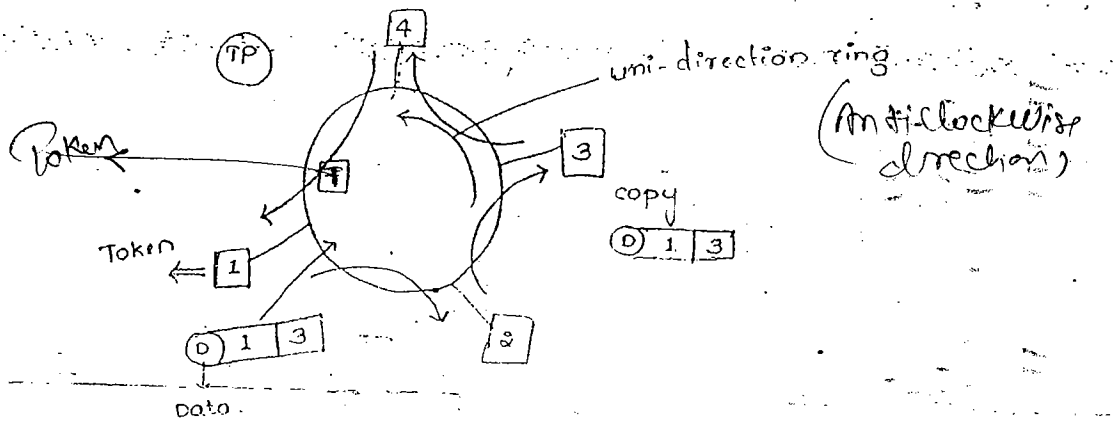
* If load increases, efficiency decreases.

Start ☆

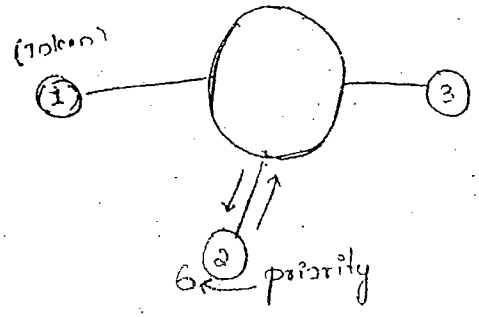
Token ring :-

Characteristics :-

* It also offers connectionless communication. There are priority no restriction on the minimum size of the data
* It uses piggybacking acknowledgement system.
* No restriction on minimum size of data, priorities are possible, and deterministic service is possible.
* It uses token-passing system as an access control method, and use ring topology.

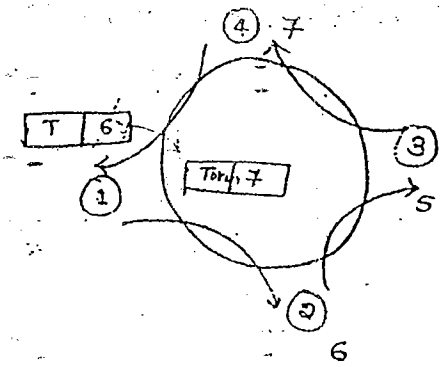


* Token is maintained at one station only. Then, the data is sent to the other station, where it checks for source & destination. If same, then it copies only and then sent the original data-to other. Therefore, there is no collission.



(priority is unique
0 - 7 priority available in token key
7 is highest and priority never repeated

* If any station have high priority than the token (or equal, then, it can access. And low priority cannot access. Therefore, no collission

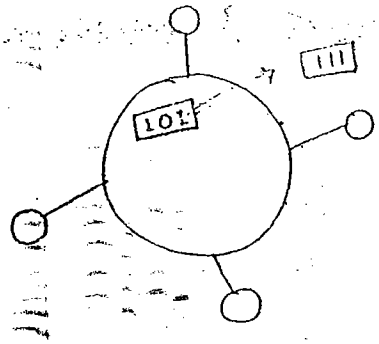


Problems with Token ring :-

Token Related problem :-

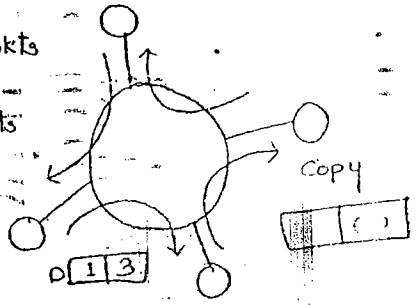
(a) Vanished Token. due to Electric Shock

(b) corrupted Token . due to External Effect } Rectify Probly



(2) Source :-

* Orphan pkts
* Stray pkts



during producing pkt Source get Crash so pkt is incomplete. So it is in Ring. So not understandable for other sources.

partial pkt is produced and so station is recognised by this partial pkt.

orphan pkts => source ~~crash~~ Crash rotate upto ∞ times

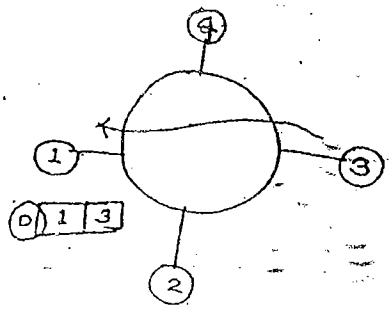
stray pkts => no one understands

(c) monopolization (Single man rule). due to High Priority

One station is being accessed cohole the time which cause problem to other stations.

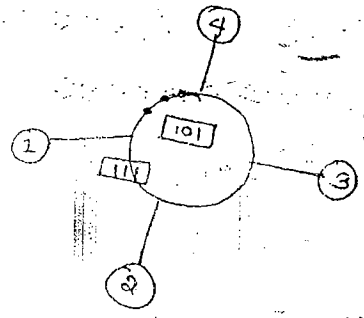
(3) Destination:-

* Safe operation
* Busy destination (not able to copy the frame / pkt) never take a copy of source ⇒ again send the pkt.
* Crash destination.
  ↓
  Drop the pkt.



(4) Ring :-

* major cut in the ring stops the operation.
* Unhealthy token ⇒ no station can use the original token.



To overcome these problems we have the following :-

(1) Token Holding Time :-

One station must release the token within 10 msec of time.

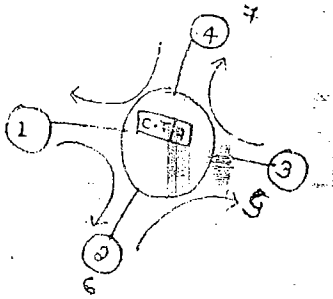
∴ It can transfer 20,000 pkts in 10 msec.

(2) Monitor :-

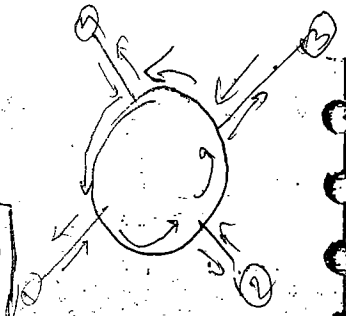
(leader for the ring).

To become a monitor station, it must release claim token, i.e., based on the priority of station.

Server are always monitor



* After monitor station is elected,



minimum TRT = prop. delay in the ring
+
No. of active stations * Delay at each station

100 sec

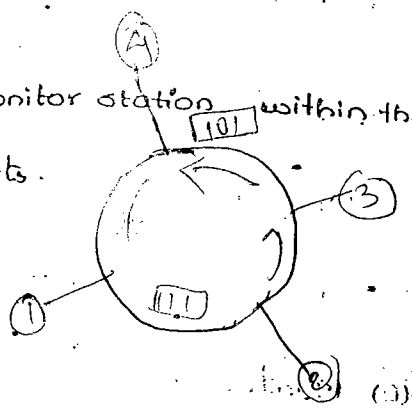
maximum TRT = prop. delay in the ring
+
No. of active stations * Token Holding time

200 msec

: Monitor station expect this token within these 200sec, if pkt not arrives, then it reproduce the token thinking that it is missing. So, it solves the vanishing token problem.

It also waits for 200sec more than 200sec.

: Corrupted tokens are recorrected by the monitor station within the 2nd cycle only. No other stations have 3 bits.



(2) Source :

(a) Orphans

when a packet crosses a monitor station, it marks a cross stamp on it. Stamped pkts are not allowed.

↓

allowed only one by time by monitor when stamped pkt created by Monitor and 2nd time it is not allowed.

(b) Stray :-

Checking the validity of pkt, while crossing monitor station.

Stayed pkt droped by the Monitor Station.

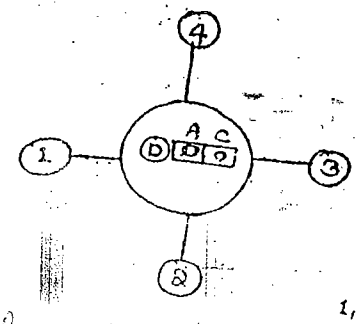
(3) Destination :

Availability → 'A' & 'c' ← copy are attached.

Two fields

A = 1	c = 1 ⇒ safe
A = 1	c = 0 ⇒ Destination Busy If receiver have time to its available time so it Retransmite otherwise leave (drop) it
A = 0	c = 0 ⇒ Destination is not available (crash)
A = 0	c = 1 ⇒ Dest. not available but frame is copied.

1, 3

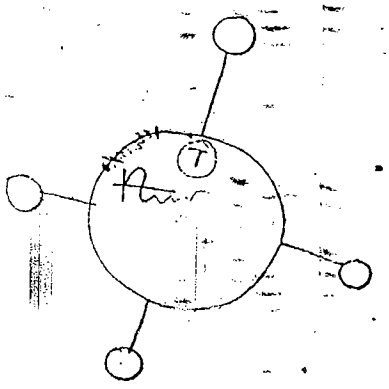


It represents that other than dest. station has copied the frame. (Illegal operation)

(4) Ring :-

* A special frame is introduced.

* If continuously produce the pkt and no response, then cut it & produce a waveform at t=0, and if response within t = 1 μsec, then it identifies as the major cut.



A special frame is sent by monitor station for every 10 sec, saying that it is available. If any frame is not received then it is assumed that monitor is crashed, and there is a chance of other stations to become a monitor station.

Mall-functionality :- Monitor is not performing its duty well. There is no soln to Resolve the Mall functionality problem of Monitor.

24/07/2010
Saturday

Specifications of Token ring:-

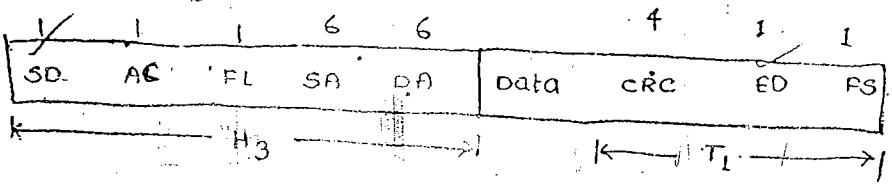
(a) Data rate
- * 4 mbps
- * 16 mbps

(b) Signal :- DME (Differential Manchester Encoding)

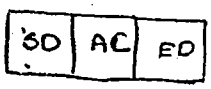
(c) Addressing system: 48-bit physical address

Frame format:-

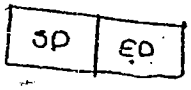
(a) Data frame



(b) Token frame



(c) Abort frame



* Start Delimiter
* End Delimiter. } used to indicate two extreme ends of the packet.

* They use DME signals

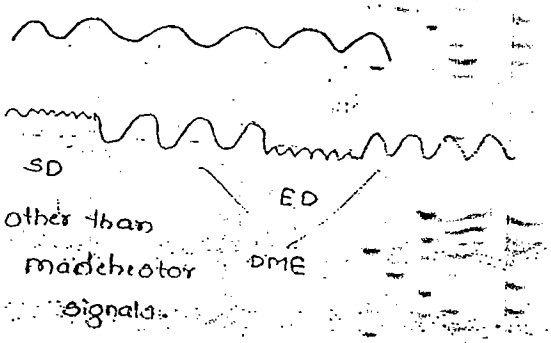
Invalid

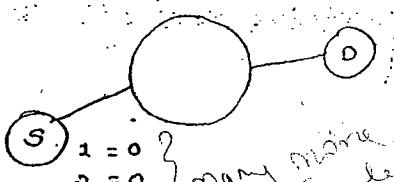
SD: 10 JK 10 JK → other signals except DME

ED: 11 JK 11 IE → Error bit

Information bit

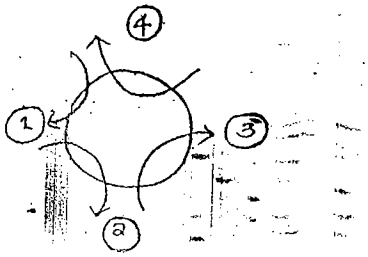
Here we use Some validation bits





1 = 0
2 = 0
3 = 0
4 = 1 ⇒ It gives indication of ending or last packet.

many more pck are left to come



If E = 1,
then it simply transfer considering it as error.

Ack. Access Control

P	T	M	R

m → monitor bit.

T = 0 — Data

= 1 — Token

m = 0 — Before crossing monitor bit

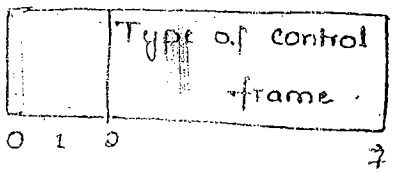
= 1 — After crossing monitor bit

⇓

If again requested, it just eliminates it.

Fracoe Control :-

6 types of -frame control.



00 - Data
11 - control
or 10-data
01-Control

(1) client Token :-

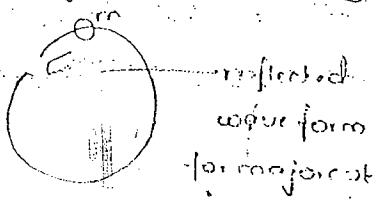
It is used in the election process of a monitor.

(2) Active monitor presence :-

It is issued by the monitor in equilateral intervals to make it presence

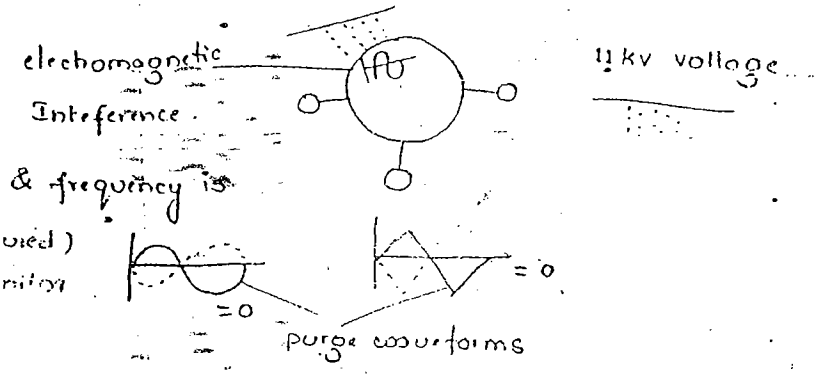
(3) Beacon :-

It is used to identify major cut in the ring

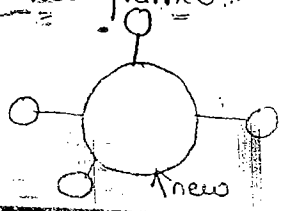


(4) Purge frame :-

It is used to clear the ring from unwanted bits.



) Duplicate Address Test frames :-



SD AC DAT 4 11.....11 Data CRC ED FS

↓

neco channel's address.

In specific conditions, only DAT is used not for all the physical addresses.

=> It is being checked with all other channels who have this address (if any). If there, then another address is given & again checked.

Virtualisation :-

windocos (Base machine)

IPadd IP IP => virtual physical addresses of machines

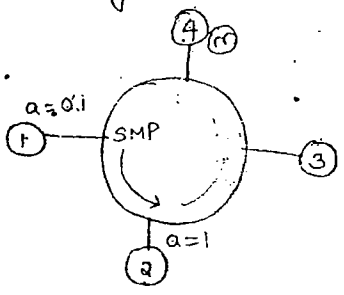
Virtual machines.

"DAT" case is only used in virtual physical addresses.

* Proxy physical addresses are also considered under the "DAT" case.

(6) SMP :- (stamped by monitor preserve)

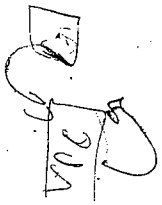
It is used to carryout neighbour identification.



✓ Upstream — from whom the channel receives data packet

Downstream — To whom the channel delivers

SD AC SMP 1 11.....11 Data CRC ED FS

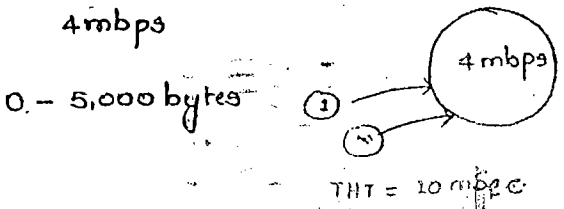


Source address & Destination address:-

* They are 48 bit physical addresses.

Data :-

No restriction on min. size of data, but maximum size depends on token Holding Time (THT) and Bandwidth of the ring.



1 sec — 4×10^6 bits

10 msec — ?

40,000 bits.

(or)

5,000 bytes.

1 sec — 16×10^6

10 msec — ?

1,60,000 bits

(or)

20,000 bytes

Consider a token ring with 100 mbps Bandwidth & THT = 50 msec. Find min. & maximum size.

1 Sec → 100×10^6 bits.

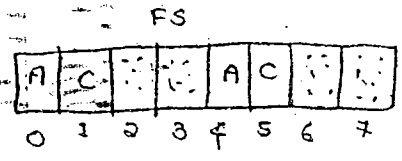
50 msec → x

$$x = \frac{100 \times 10^6}{1} \times 50 \times 10^{-3}.$$

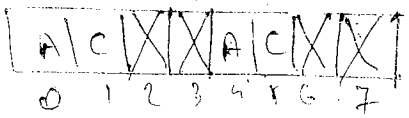
= 50,00,000 bits.

Token frame :-

Frame status:



Frame Status



A = 0	C = 0	
A = 1	C = 1	⇒ Safe
A = 1	C = 0	⇒ Busy
A = 0	C = 0	⇒ Dashed
A = 0	C = 1	⇒ Illegal.

Q) Why FS is not included in CRC calculations?

Ans: CRC is calculated by the source but FS is filled by destination. Hence while calculating CRC at the source, it is not possible to predict 'FS' value. or include into CRC

Q) Why FS is having two sets of A & C bits.?

Ans: Since, it is not included in CRC to have it's own error control using two sets of A & C bits. If both are same it is treated as correct, else treated as corrupted. (Company info.)

correct { A C = 1 1 ; A C = 0 0 } ⇒ corrupted

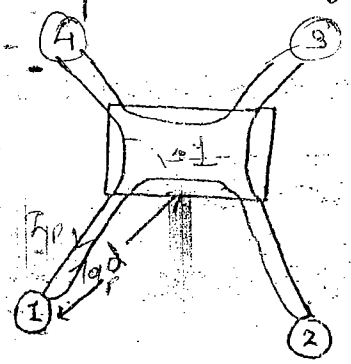
Purpose of abort frame :-

It is used to de-activate the token ring. It is used by the Monitor station

⇓

After one circulation all the channels stop the transmission.

Implementation of token ring



Physical = Star.
logical = Ring

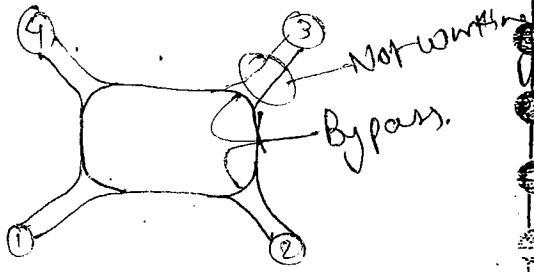
Total length of the ring = N * 2d.

= N * (I/p + O/p)
= N * (d + d)
= N * 2d

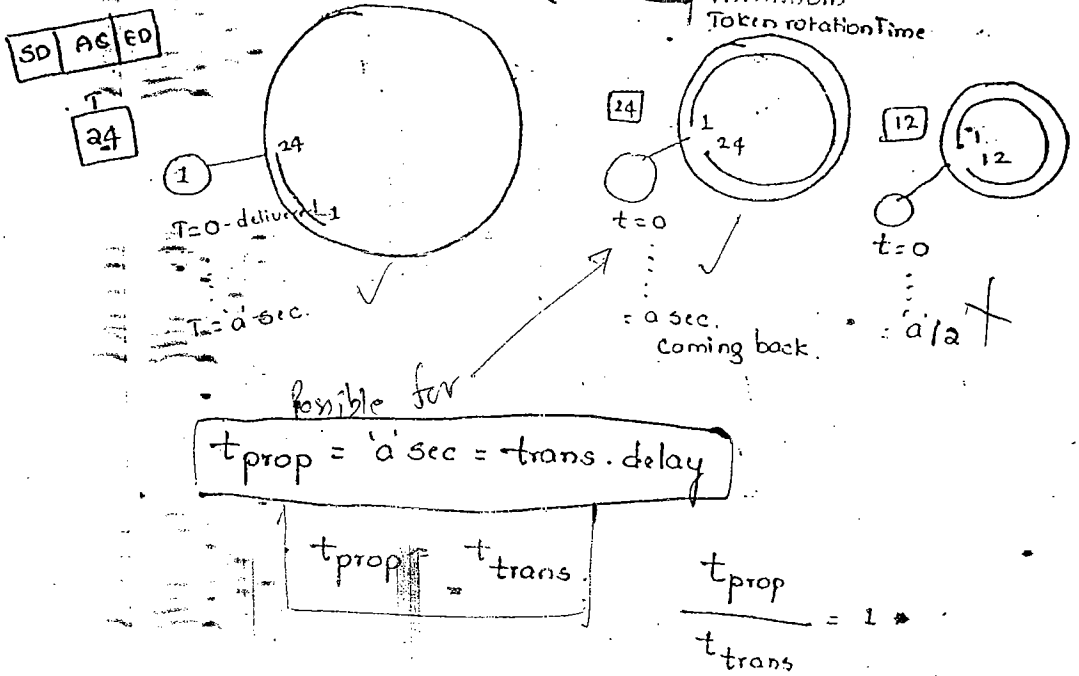
one incoming & one outgoing.

Modes of operation:-

* Transmission mode
* Listen mode
* Receiving mode
* Bypass mode



Calculation of minimum size of token ring:-



$t_{prop} = a \text{ sec} = t_{trans}.delay$

$t_{prop} = t_{trans}$

$\frac{t_{prop}}{t_{trans}} = 1$

Token rings are not suitable for small N/w they are suitable for large N/w

T_{prop} / T_{trans} = min. size of token ring

> 1 – max. size of token ring

< 1 – Overlap

$\frac{\text{min TRT}}{\text{fix. n. delay}} = L$

Token rings

⇓

used for bignetcoorks

16 mbps N/w

$d = \frac{L}{B} \times V$

$d = \frac{24 \times 2 \times 10^8}{16 \times 10^6}$

$= 300 \text{ mts}$

$V = 2 \times 10^8$ mbps

$\frac{\text{P. delay}}{\text{for}} = \frac{\text{P. delay}}{\text{for}}$

$\frac{d}{V} = \frac{L}{B}$

$L = 24$ bits

$d = \frac{L \times V}{B}$

$= \frac{24 \times 2 \times 10^8}{4 \times 10^6} = \boxed{1.25 \text{ km}}$ or 100 mts

To Reduce the distance we have to ↑ B.W of the Token Ring..

If Bandwidth of ring is 100 mbps & frame size = 200 bits. velocity = 2×10^8 msec, find min. size of token ring.

$d = \frac{L}{B} * V$

$= \frac{200 \times 2 \times 10^8}{100} = 4 \times 10^8$

* calculation of Ring latency:-

Ring latency = min. TRT = prop. delay in the ring

+

No. of active station * Delay at each station.

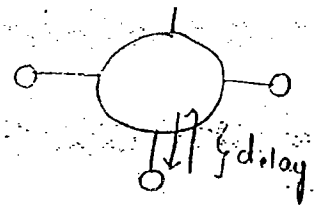
M ⇒ total no. of systems

d ⇒ Total length of the ring.

b ⇒ bit delay at each station

v ⇒ velocity of propagation.

R ⇒ Bandwidth of the ring.



$(\text{prop. delay}) = \frac{d}{v} + mb$

d/v → sec, mb → bits.

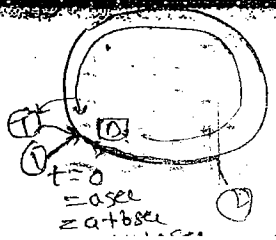
$\text{Bit delay} = \frac{1}{B} = \frac{1}{R}$

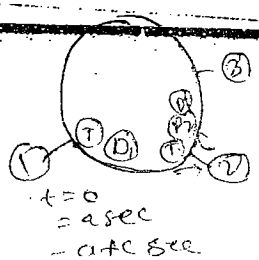
L ⇒ $\frac{d}{v} + \frac{mb}{R}$ sec. — either convert mb into sec by dividing R or converting propdelay by

RL ⇒ $\frac{dR}{v} + mb$ bits. — multiplying propdelay by R into bits.

Various Token re-insertion strategies:-

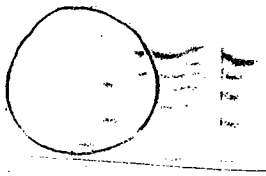
Delayed Token strategy.	Early Token strategy.
Token is released after getting entire data packet back.	Token is released after data is transferred. OR As soon as data is transfer token is released
Efficiency is low	Efficiency is high
Reliability is high	Reliability is low.
It is used under low load conditions.	It is used under high load conditions.
Cycle time = (a+b+c+d) sec	Cycle time = (a+c+d) sec
where a → data-transmission time	
b → Ring latency	
c → token transmission time	
d → prop delay betn two station	





c → Token Transmission time

d → prop. delay b/w stations



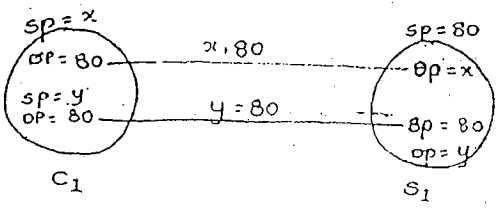
31/07/2010

Saturday

Why we call Networks as TCP/IP networks :-

(or)

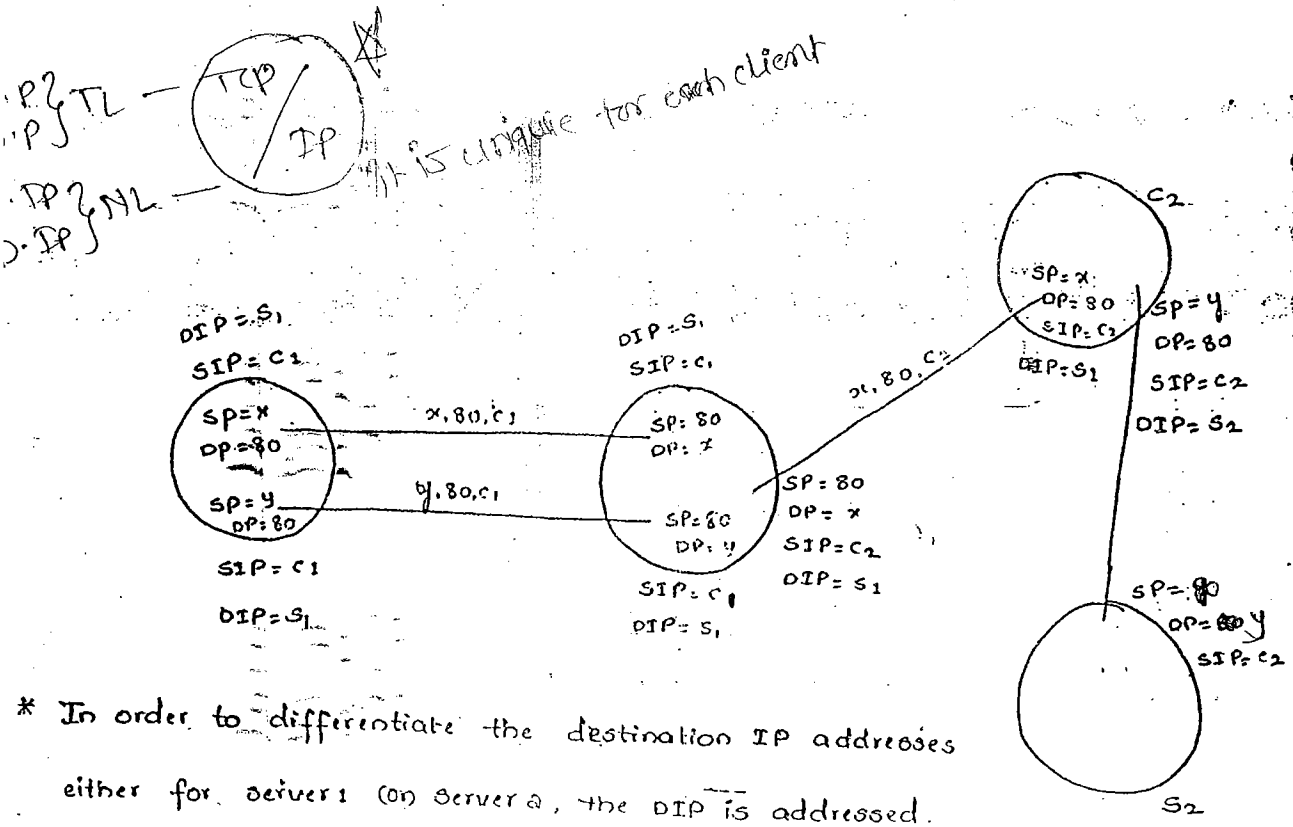
* Relationship between TCP & IP :-



* Ctrl+N ⇒ another connection

* While establishing a new connection, source port & Destination port is addressed.

* Server can handle more no. of clients, so introducing a new client, involves both s.p and d.p.



* In order to differentiate the destination IP addresses either for server 1 (or) server 2, the DIP is addressed. where '80' represents the http, and SIP represents the user's ocon address.

* The Source port & Destination ports are handled by TCP protocol in the Transport layer. => 2 ports parameters

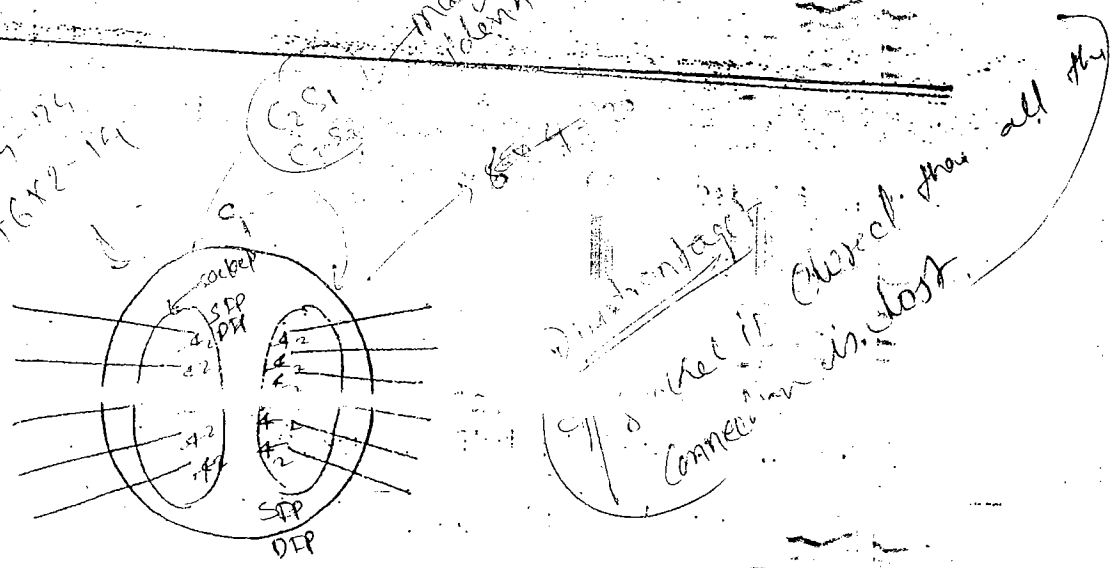
* The Source IP & Destination IP are handled by IP protocol in the network layer. => 2 ports parameters.

* So, combinely 4 ports are being handled by TCP/IP protocols.

4 parameters
- Source port
- Destination port.
- Source IP
- Destination IP.

Technical name of internet is TCP/IP.

Socket :-



* Socket is a logical component (a class) which groups a set of parameters for communication.

$5 \times 4 = 20$ $\quad$ $6 \times 4 = 24$

$5 \times 2 = 10 + 2 = 12$ $\quad$ $6 \times 2 = 12 + 2 = 14$

Advantages :-

* Resources ✓
* Maintainance & Administration :- ✓
  * Allows certain no. of connections for socket. ✓

Transmission control protocol (TCP) :-

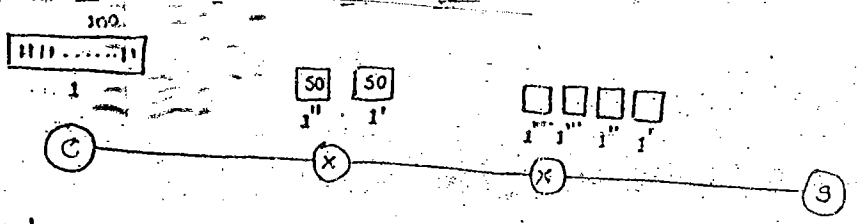
Characteristics :-

* It is reliable, byte oriented, port-to-port transport layer protocol. (bytestream)
  ↓
  connection-oriented.
- TCP is a byte oriented protocol

* Message oriented (UDP) * packet oriented (SWP)
* Byte oriented (TCP)
* Bit oriented (HDLC)

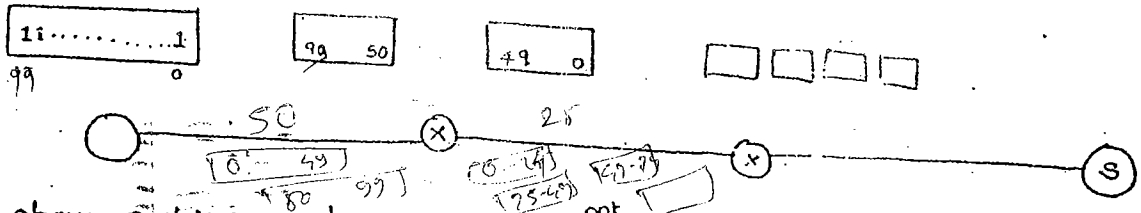
Bit - HDLC
Byte - TCP
msg - UDP
packet - SWP

Byte-oriented (TCP) / Stream oriented :-



Burden on inter-mediate routers.

* The bits are splitted by half to the router, as it can handle only certain set. So, it have a problem to exactly split. (if not, there is a chance of missing a pkt)

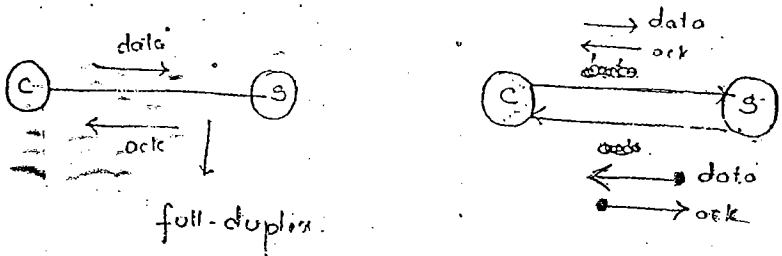


* The above problem can be overcome by not splitting the packets but just only dividing the stream of bits and transferring. So, it has no burden on the intermediate routers.

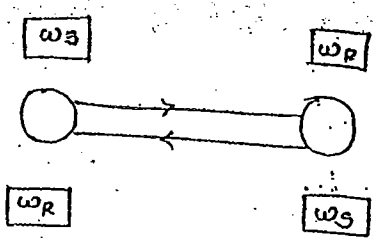
* Since the bits are transferred as a byte on a stream, the TCP is considered as stream oriented

* TCP uses cumulative acknowledgement.

* TCP connections are full-duplex connections. Therefore, it is having two half-duplex connections.



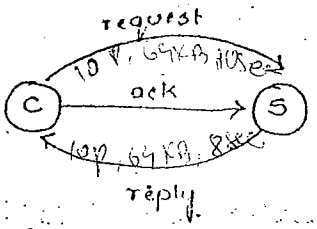
* TCP uses sliding window protocol (SWP) for its flow control. Therefore, each TCP connection have four windows.



due to this TCP is expensive.
In Half we need 2.
In full we need 4.

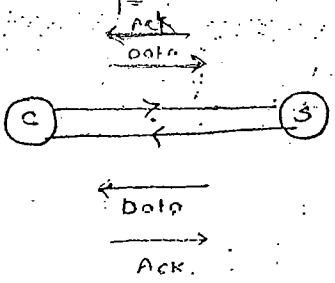
* TCP connections are having three phases:-

(1) Connection establishment phase :- / negotiation phase.

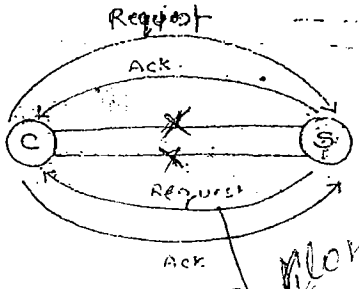


* It is a single step process.

(2) Data transmission phase :-



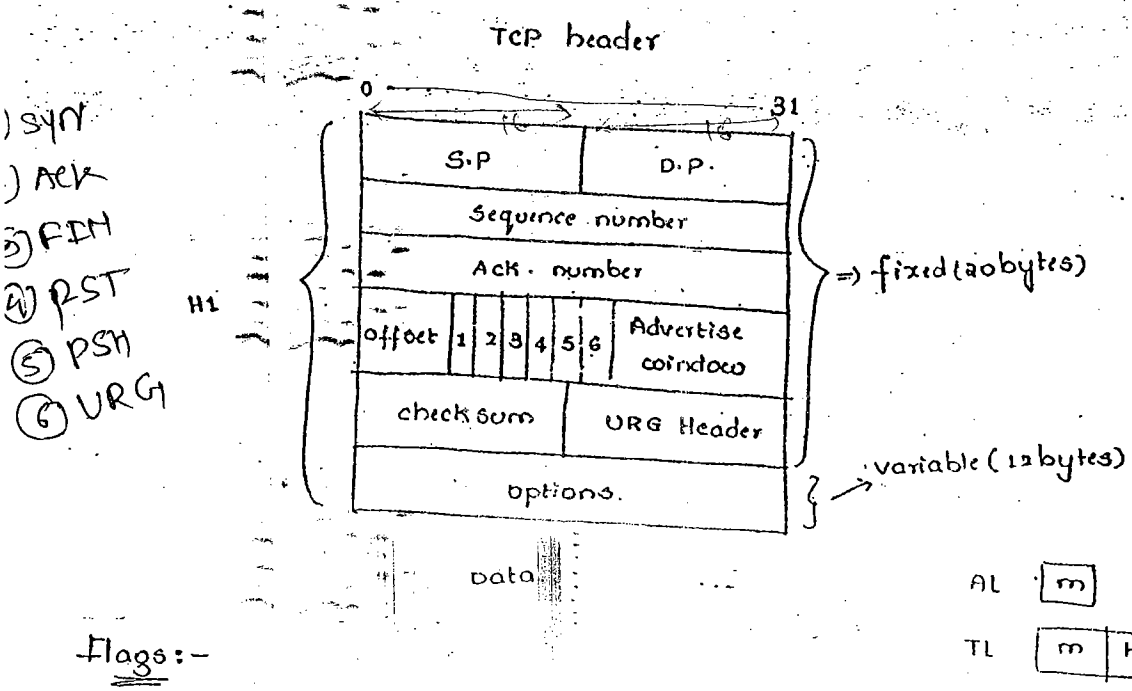
(3) Connection termination phase :-



To close the Connection from source side

* It is not single step process, eventhough it requested for connection termination. The termination must done in both the systems. not only one.

TCP operation :-

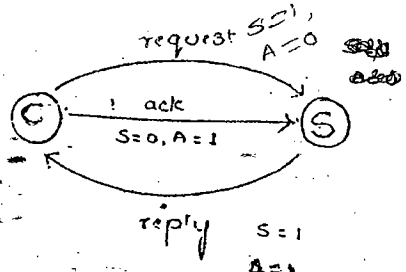


AL | m |

TL | m | H1 |

Flags :-

Syn & Ack flags are used in connection establishment phase to differentiate request and reply packets.

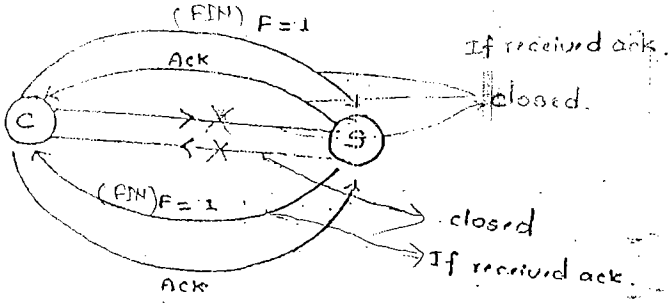


1. SYN & Ack
2. FIN
3. RST
4. PSH
5. URG

S=1	A=0	Request
S=1	A=1	Reply
S=0	A=1	Ack
S=0	A=0	Data, control packet

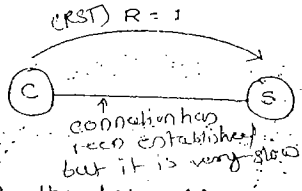
FIN flag:-

* It is used in connection termination phase.



RST flag:- (Reset)

* It is used to reset the connections.

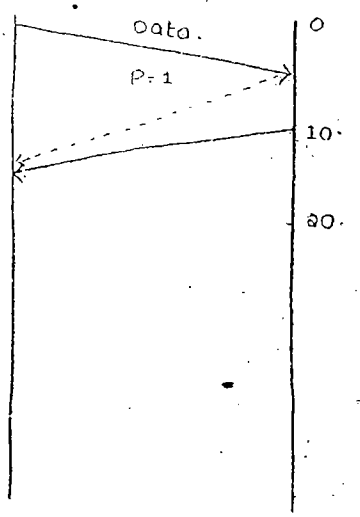


Reco Connection is established by just refreshing the windows.

* while transfering the data, if any problem arises, then the complete connection is cancelled, and a reco connection is made so, it is not suitable for every time to have reco connection. So, we use RST to resend

PSH flag:-

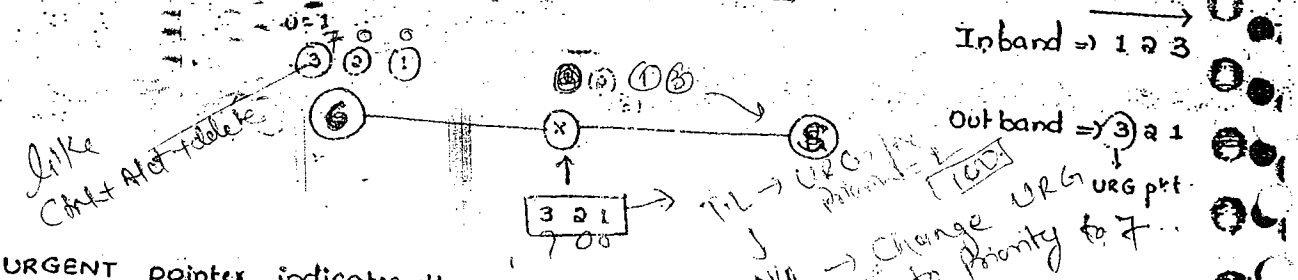
It is used for high priority packets to push the packet to upper layer, without waiting for time interval.



If the data is transferred and of high priority it needs a fast ack. from sender. So, by using PSH flag (if set to 1), sender sends the ack. fastly as soon as data reaches, without waiting for the time interval it have.

URG flag :-

* It is used to take care of "out of band data".



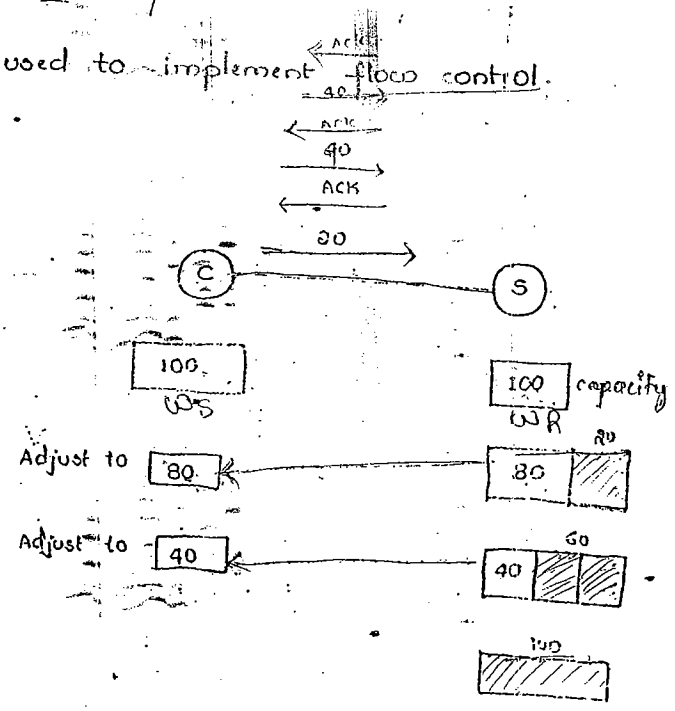
* URGENT pointer indicates the amount of the data that is important in the packet..

* It is valid only if URG=1.

* If the packets ①, ② & ③ sent to Receiver by representing URG=1 to ③ pkt then instead of ①, ② & ③ packets is reached firstly. It represents an URGENT packet.

Advertise window / Receive window

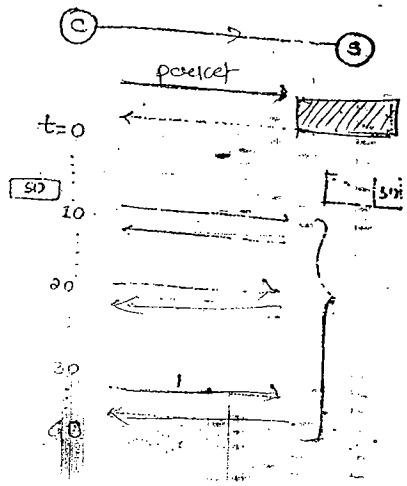
* It is used to implement flow control.



* If the server have no empty space, it can't take further data. so, it must represent that it has no empty space, but it is difficult to send to each and every client. so, we can solve this problem as follows:-

* At t=0, client sends the packet, and server have no empty space, so, simply discard it. It checks for all the time intervals.

* If suppose, server have empty space, at particular time interval, (say at t = 40), then it can accept the data packet.



Silly window syndrome (SWS) :-

* When SWS occurs, efficiency is '0'.

* There are three reasons for silly window syndrome (SWS):-

  * when server announces it's empty space is '0'.

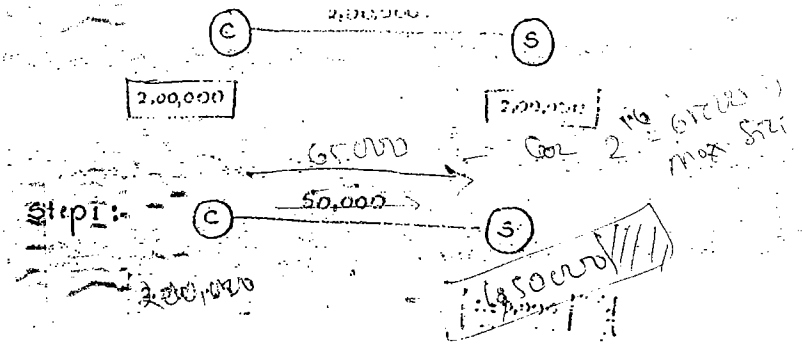
  * when client is able to generate only one byte at a time.

  * when server consumes only one byte at a time.

* Always ensure to transfer only one byte among all the bytes of data, inorder to reduce virus.

* Always server needs to consume only one byte & transfer.

As possible to reduce the SWS value, so that efficiency increases.



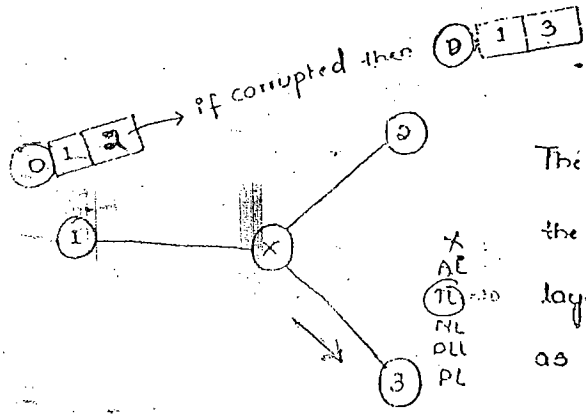
* There is a chance of sending all the 1,50,000 bits, at both the sides, but we cant transfer (even) them (because only 16 $\Rightarrow 2^{16}$ bits = 64,000) are being allowed to transfer.

* If empty space in the server is more than 2^{16}, then use scale factor in the "options" field.

Eg:- If empty space is 1,50,000 & advertise window = 50,000 and scale factor = 3.

Eg:- If empty space = 1,00,000 & advertise window = 50,000 then scale factor = 2.

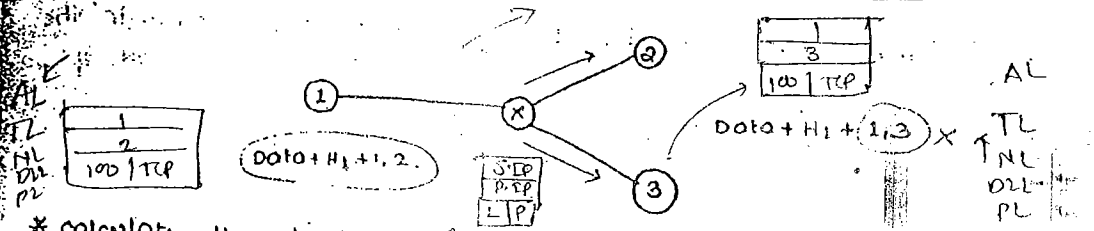
Checksum:-



The transport layer transfers the corrupted data to the app. layer. Then App. layer recognizes as a corrupted bit.

So, in order not to have burden on Application layer, before a packet reaches App. layer, it gets corrected at the Transport layer, by including the concept of "checksum".

* Checksum includes "data + H_1 + pseudo-header" in its calculation



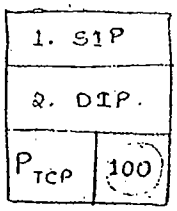
* calculate the checksum (i.e., Data + H_1 + (1, 2)) at the sender side. (Source, Dest.) and send the checksum. At receiver, the checksum is again calculated, (Data + H_1 + (1, 3) → corrupted), so, discard it by transport layer.

* Pseudo-header is used to check whether data packet has been received by the correct destination or not.

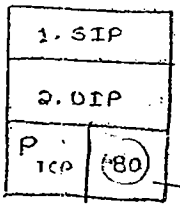
* It is prepared at the source and included in checksum calculation.

* Once packet is received by the destination, again it is prepared by the destination with destination values.

* If incoming checksum is similar to calculated checksum, then packet is consumed else it is discarded.



Source

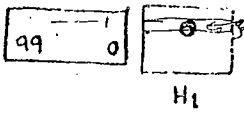


Destination

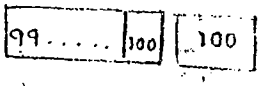
* Sequence no. for the packet is first databyte sequence no. in the packe

Characteristics for Sequence no. & Ack :-

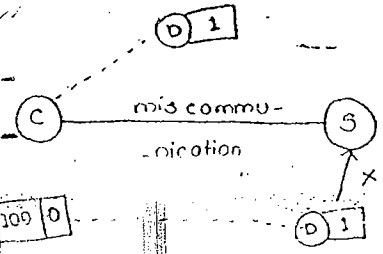
(1) Sequence no. for the packet is first databyte sequence no. in the packet. - first databyte no. in the data packet is specified as sequence no. of packet & it is inserted in sequence no. field.

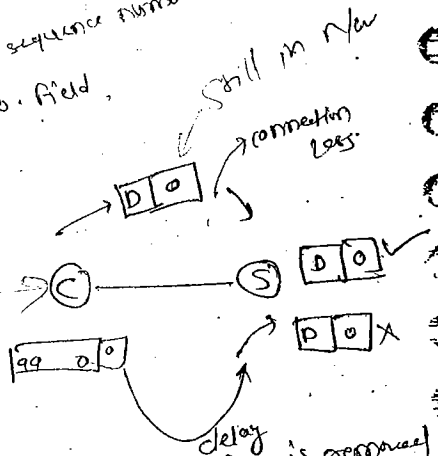


(2)

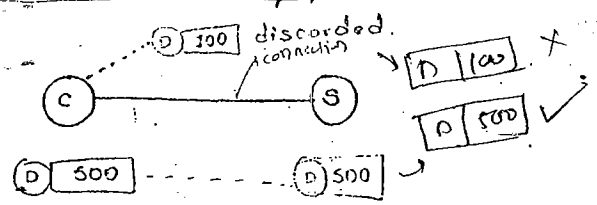


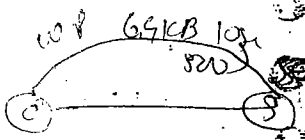
discard of new Connection
data
accept terminated
Connection data





(3) TCP uses random initial sequence numbers.



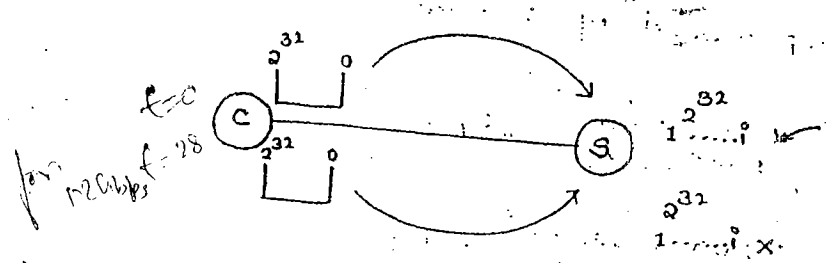


The sequence numbers always not starts with '0'. It selects a random number among the set of $0 - 2^{32}$ and then sends the random number. If corrupted random no. generates, simply discard it.

(3) Get randomly sequence numbers :-

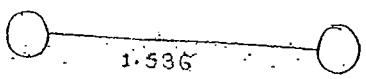
* If ~~both~~ two different packets of the same sequence numbers are generated simultaneously, then the server thinks that one is the

duplication of another packet and just discard one of the packet, which leads to a loss of a packet which is different from the othe packet.



* In order to overcome this problem, increase the value from 2^{32} to 2^{64}

Eg. :-



1 Sec = 1.536×10^6 bits $\Rightarrow$ 1st packet

1 Sec = $\frac{1.536 \times 10^6}{8}$ bytes. $\Rightarrow$ 2nd packet.

1 Sec = $\frac{1.536 \times 10^6}{8}$ sequence no. of 2nd packet.

@ 1.536 mbps — 6.4 hrs. → after this Sequence no. Starting Repeat

@ 10 mbps — 57 min.

@ 100 mbps — 6 min.

Problem

1.2 Gbps — 28 sec.

Eg:- Consider bandwidth of link = 100 mbps.

Sequence no. field = 24 bits.

Find the "corap around" of sequence numbers.

Sol:-

$$1 \text{ sec} = 100 \times 10^6 \text{ bits}.$$

$$1 \text{ sec} = \frac{100 \times 10^6}{8} \text{ bytes}$$

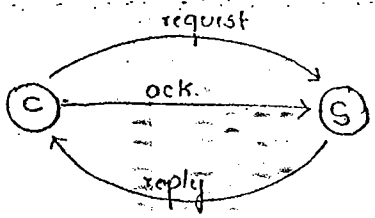
$$1 \text{ sec} = \frac{100 \times 10^6}{8} \text{ sequence no.}$$

$$? \text{ —— } 2^{24}$$

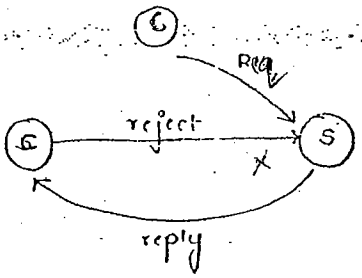
Applications :-

* Sequence numbers are used for authentication purpose.

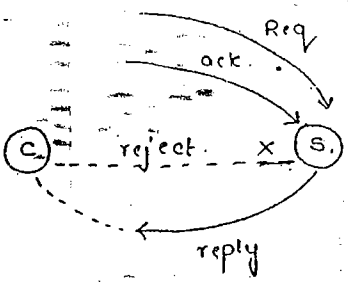
(a)



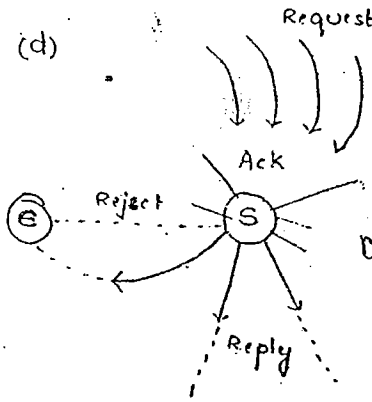
(b)



(c)



(d)



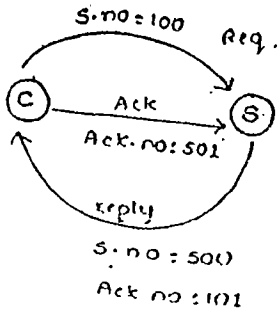
Denial of service attack

Denial of Service attack:-

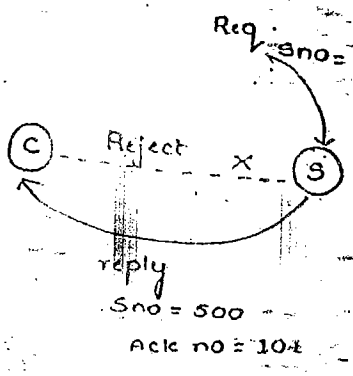
Server denies the client to serve for a certain time interval.

To overcome the above problems, we use "sequence numbers".

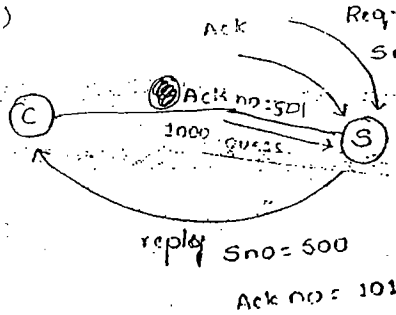
(a)



(b)



(c)



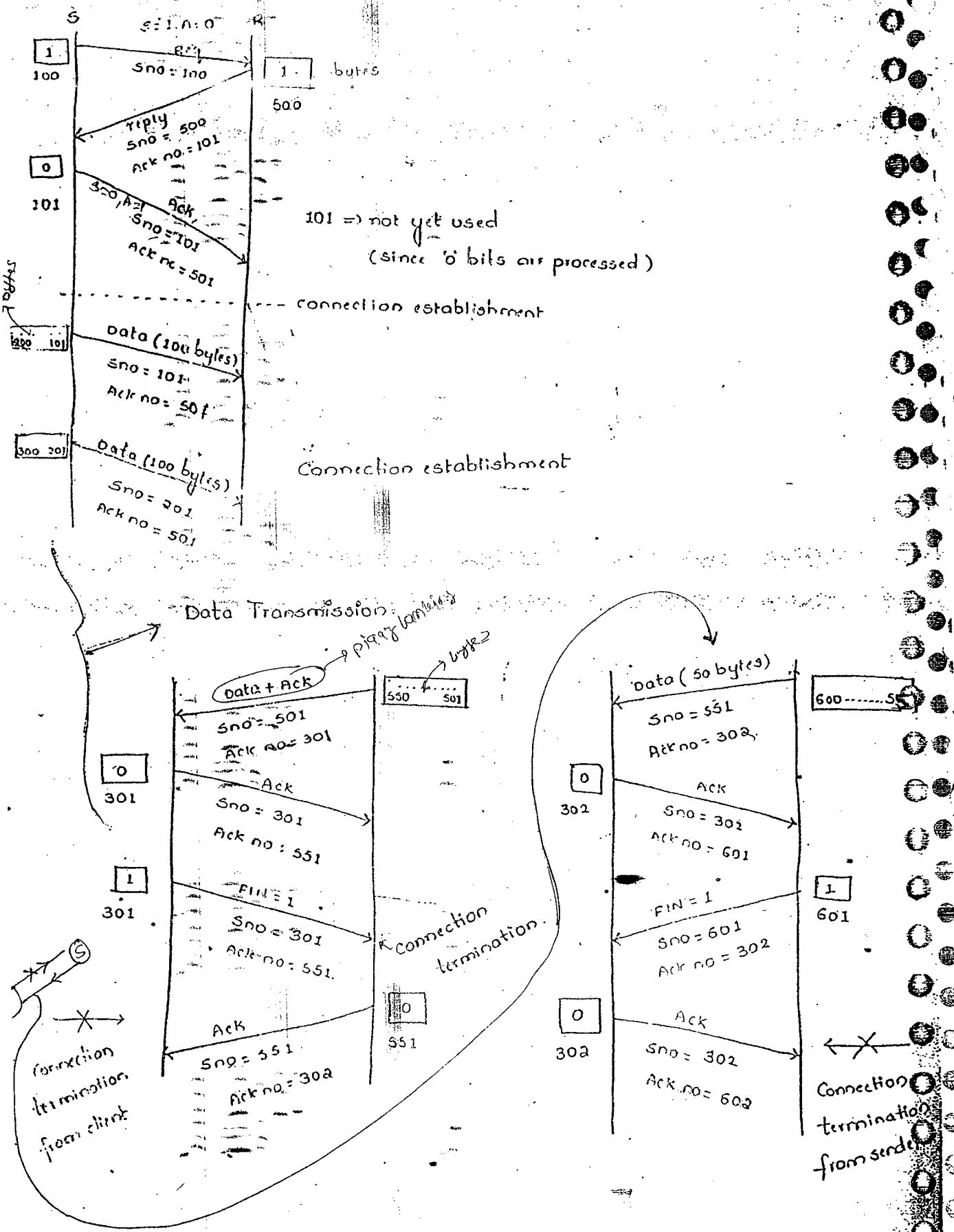
→ Hacker can't know the random no. generated by server. So, he guess (if 1000) simply rejected.

If guess = exact no., then the server cannot generate huge ack., so it also discard to send ack.

Syn, FIN } packet consume 1 byte

Ack = 0 bytes.

TCP connection Management



TCP Timer management:-

TCP uses the following four timers for its operation:-

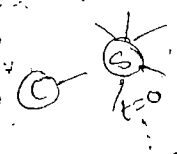
* Ack. Timer
* Keep Alive Timer
* Persistence Timer
* Timed wait Timer.

Persistence Timer:-

It is used in silly windoco syndrome (SWS) to send dummy byte packets (or) silly packets in equal intervals of time.

Keep Alive Timer:-

This is used to keep tracks of idle period of TCP connections. Once ideal period exceeds a pre-determined value, connection is closed automatically

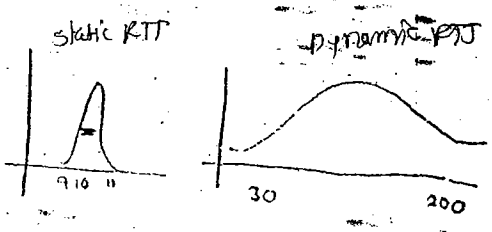


Eg:- If user.id & password entered, and leave system for certain time and then perform any operation on it, then it displays session expired.

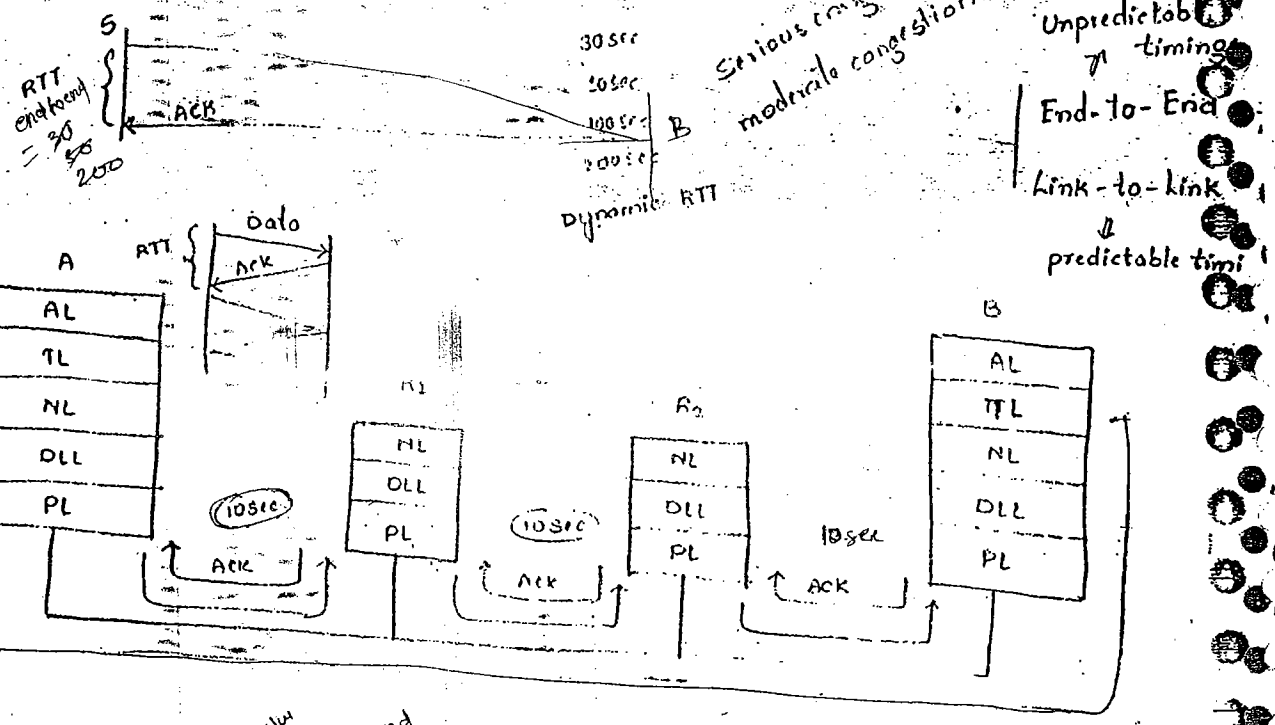
Ack. Timer :-

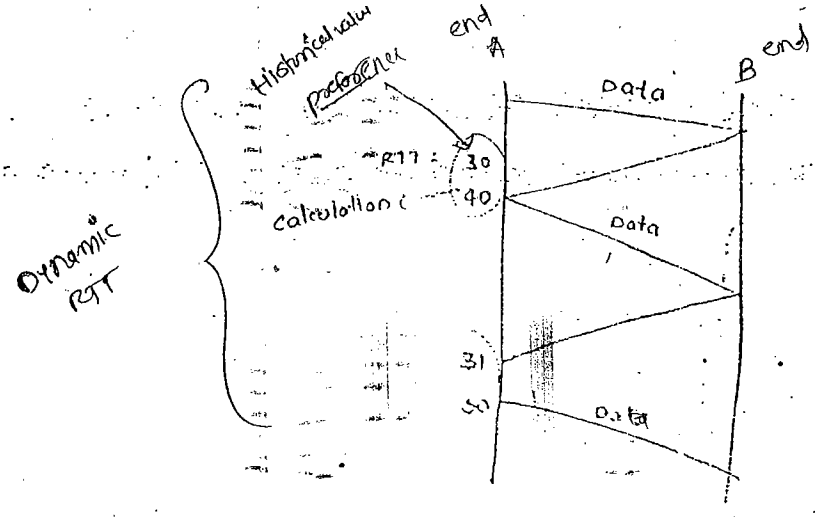
End-to-End => unpredictable Timing.

link-to-link => predictable Timing.



So, use Dynamic RTT.





Dynamic RTT is calculated as the given (Expiry) time and the packet sent time (by server) and then, the required value is obtained, where the pkt is sent (by client) ⇒ which is Dynamic RTT.

For the calculation of RTT we have certain Algorithms :-

(1) Basic Algorithm :-

$$\text{I RTT} = 30 \text{ sec} \quad \text{(Initial)}$$

$$\text{NRTT} = 40 \text{ sec} \quad \text{(new)} \qquad \alpha = 0.9$$

(2) Estimated RTT $= \alpha \text{ I RTT} + (1-\alpha)\,\text{NRTT}$

$$= 0.9 \times 30 + 0.1 \times 40 = 31$$

Time out = 2 x ERTT

= 2 x 31 = 62

③ IRTT = 31 (initial)

NRTT = 50 (neco).

ERTT = 0.9 x 31 + 0.1 x 50 = 32.9.

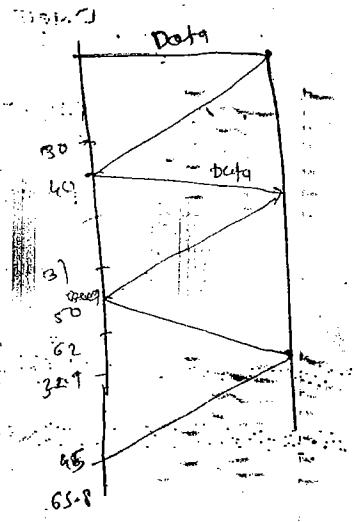
Time out = 2 x 32.9 = 65.8.

④ IRTT = 32.9 (Initial)

NRTT = 45 (neco).

ERTT = 0.9 x 32.9 + 0.1 x 45 =

Time out = 2 x



(2) Jacobson's Algorithm :-

initial RTT IRTT = 30 (Initial)

New RTT NRTT = 40 (Neco)

$\alpha = 0.9$

Initial Deviation (D_I) = 5

② New Deviation (D_N) = |IRTT - NRTT|

= |30 - 40| = 10.

Estimate deviation (D_E) = $\alpha D_I + (1-\alpha) D_N$

= 0.9 x 5 + 0.1 x 10 = 5.5.

ERTT = α IRTT + $(1-\alpha)$ NRTT.

= 0.9 x 30 + 0.1 x 40 = 31.

Time out = 4 * DE + ERTT = 4 * 5.5 + 31 = 53.

(5) ERTT = 31

NRTT = 50

$\alpha = 0.9$

$D_i = 5.5$

$D_{NEW} = |31 - 50| = 19.$

$DE = 0.9 \times 5.5 + 0.1 \times 19 = 6.9.$

$ERTT = 0.9 \times 31 + 0.1 \times 50$

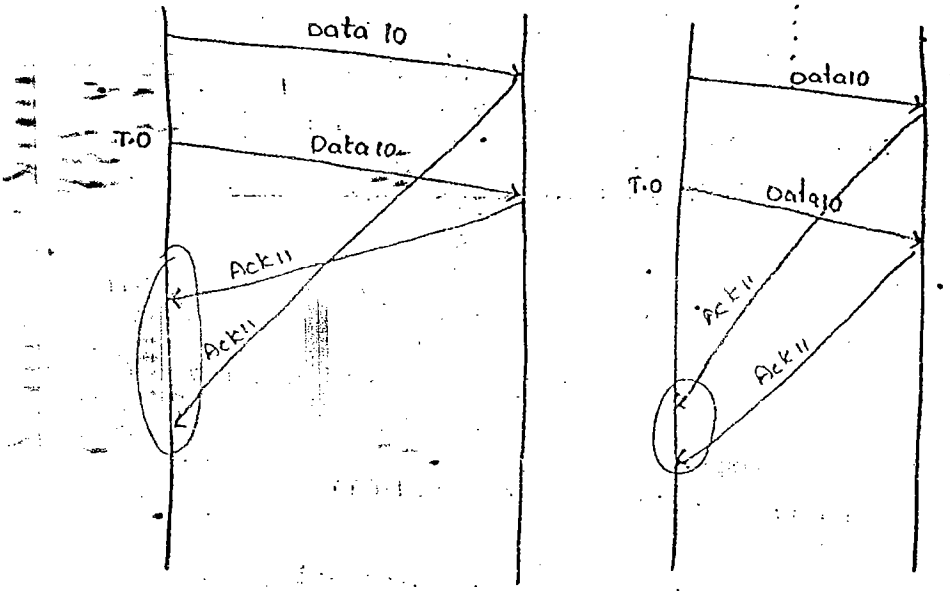
$= 32.9$

$Timeout = 4 \times 6.9 + 32.9$

$= 57$

* "Timeout" is high under Basic algorithm than Jacobson's Algorithm.

Korn's Algorithm:-



If there is a timeout, there is a possibility to receive two ~~data~~ Acknolegement packets

(1) From original packet

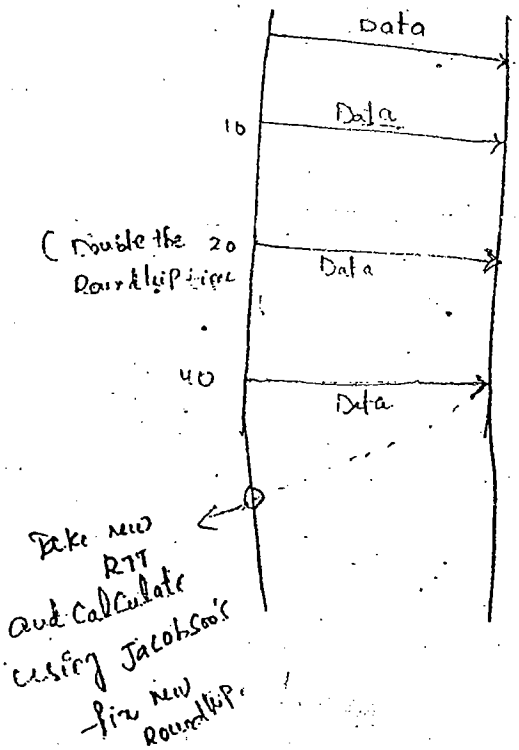
(2) From Re-transmitted packet

Then, there is an ambiguity that which ack. must be considered for next calculation. also what would be the timeout for retransmitted packet

Therefore, Korn's has resolved this ambiguity by proposing the following theory :—

* For every Timeout, double the Timeout for the next tranemission, and continue this till to get a proper acknowledgement.

* Then, we will go back to the Jacobson's algorithm.



for every timeout retransmit the packet and fixed the T.O value equal to the double of previous T.O value and continue this procedure till to get proper acknolegement and then go back to jacobson's Algorithm

03/08/2010

Tuesday

State Transition diagram :

Need for State Transition Diagram :

* To evaluate any protocol, we use one of the following two methods:

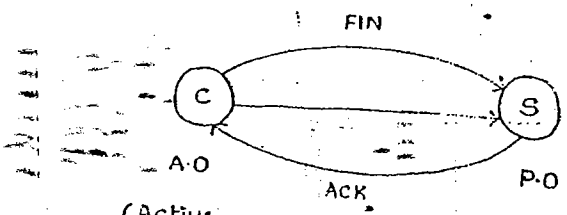
(1) Get the specification of the protocol, develop a software for it, Integrate with network operating system and evaluate it's features. (verify the protocol for its features)

It is time consuming process and costly.

(2) Get the specification of protocol, develop state Transition diagram for it and then evaluate it's features. (even though it is not powerful it is simple)

It is a shortcut method but not so powerful.

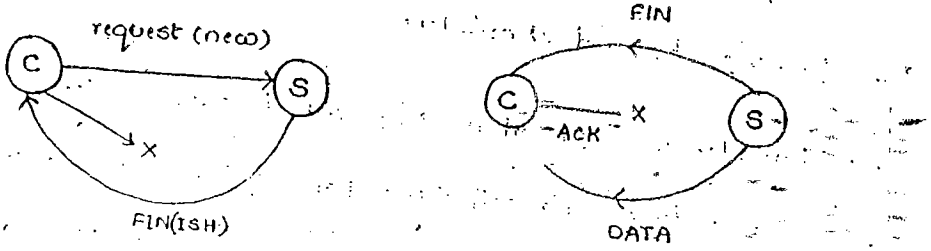
Dialog control :



Purpose of Time wait state :

As soon as Acknowledgements generated, client will go to Time wait State instead of closed state by suspecting problems with acknowledgements. Even if Acknowledgement is lost and "Fin" server is re-transmitted.

* It is treated for same connection as client is maintaining the connection in timed-wait state. If there is no such state, then retransmitted FIN is treated for new connection.



* Server wants to terminate the connection by using FIN. But it denies (suppose), then, before the time exceeds, client wanted to establish a new connection, so it requests a new connection to server. After the request reaches server, client gets the FIN.

* Then, client thinks that it is the termination of newly established connection, which is not True.

* In order to avoid such confusion, "sequence numbers" are given to FIN, at the same time, some time is also allotted for "FIN", which is called as (Time wait state).

Limitations of state Transition diagram :-

* Error control procedures are not depicted (shown) in the diagram.

* Re-transmissions are not shown in the diagram.

Nagle's Algorithm (used in wide Area Network):-

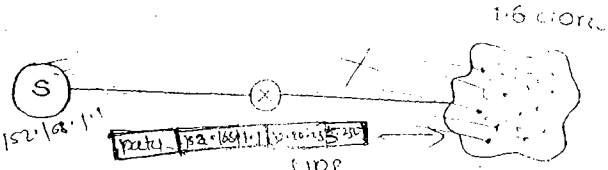
* Checking the server that it works correct (or) not using remote system.
  For checking it, send characters.
* One character is sent at a time which cause silly window syndrome efficiency reduces drastically, for checking 100 characters, one at a time. So, for which round-trip time is more for character typing.
* At such conditions, add the header for all the bits and send it, which improves performance.
* But, it is not applicable in LAN technologies, but supports WAN techn. because of RoundTripTime and typing speed capabilities.
* Round trip time is less but input speed is high.

User Datagram Protocol

(UDP)

Need for UDP :

For multicasting and broadcasting applications, TCP can't be used. Hence we need UDP.



Server communicates to 1·6 crore systems.

in TCP, we require 1·6 crore connections,

which it cannot support such a huge conn.

Applications that requires constant data flow, cannot use TCP. Hence, UDP is being used.

Applications that requires bulk data transfer (ex: multimedia), cannot use TCP. (TCP sends 1 byte, 2 byte, 4 byte, ...)

Applications that requires fastness than reliability, cannot use TCP. (or use UDP)

Since, UDP is a connectionless, many fields in TCP are not needed in it.

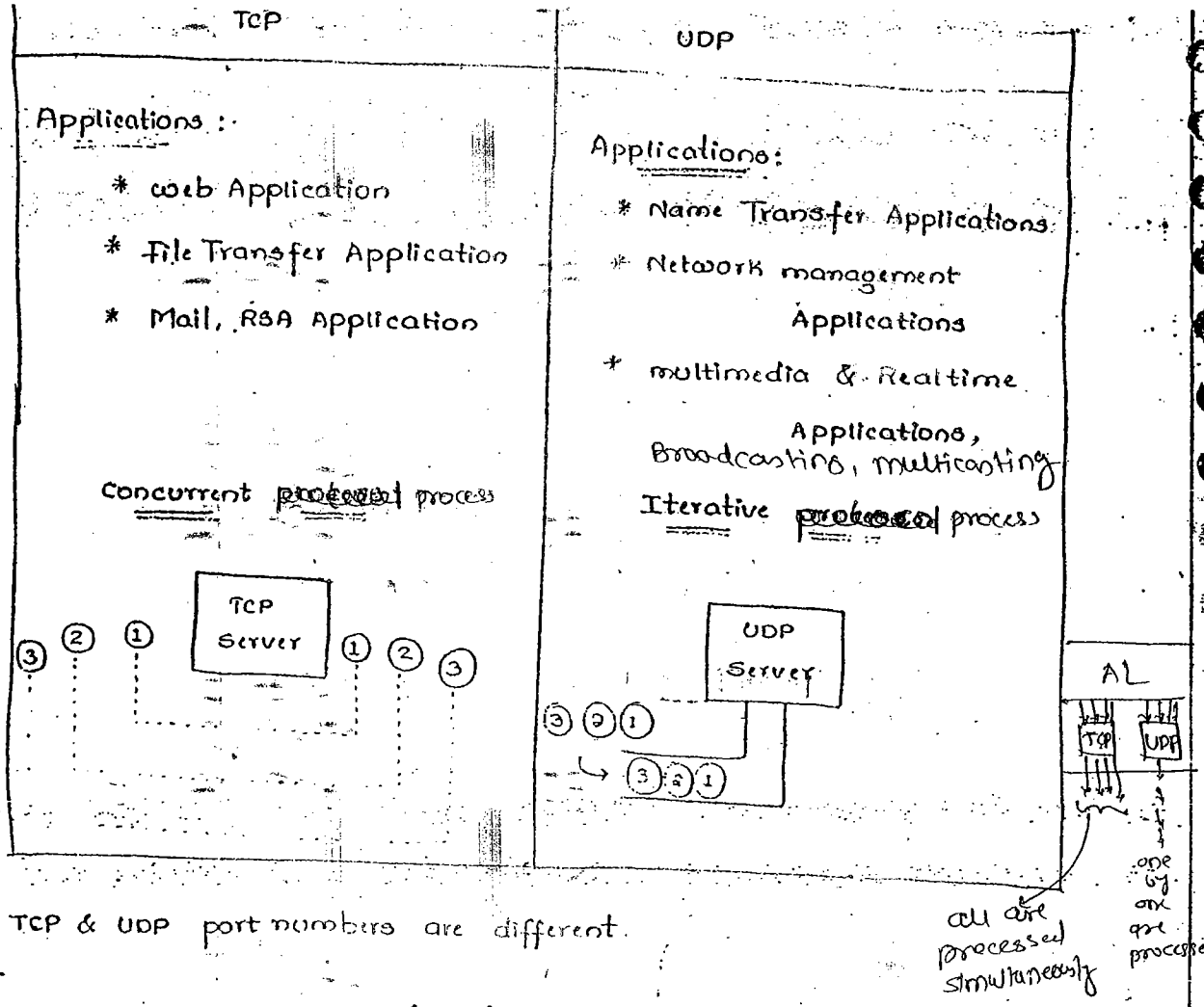
optimal

S·P	D·P
L	P

⇒

D·P
P

TCP	UDP
Connection-oriented	connectionless
Slow	Fast
Reliable	UnReliable
Overhead is high	Overhead is low
HTTP, FTP, SMTP, Telnet are used	DNS, TFTP, NFS, SNMP, multimedia &



TCP & UDP port numbers are different.

* Domain Name System (DNS):

It is using UDP, It's purpose is to keep track of computers and services in a network environment.

It has four applications :

* Name Translation
* Host Aliasing
* Mail Aliasing
* load balancing.

It is using 4 types of servers :

* Root name server
* Top-level domain server
* Authoritative server
* Local DNS server

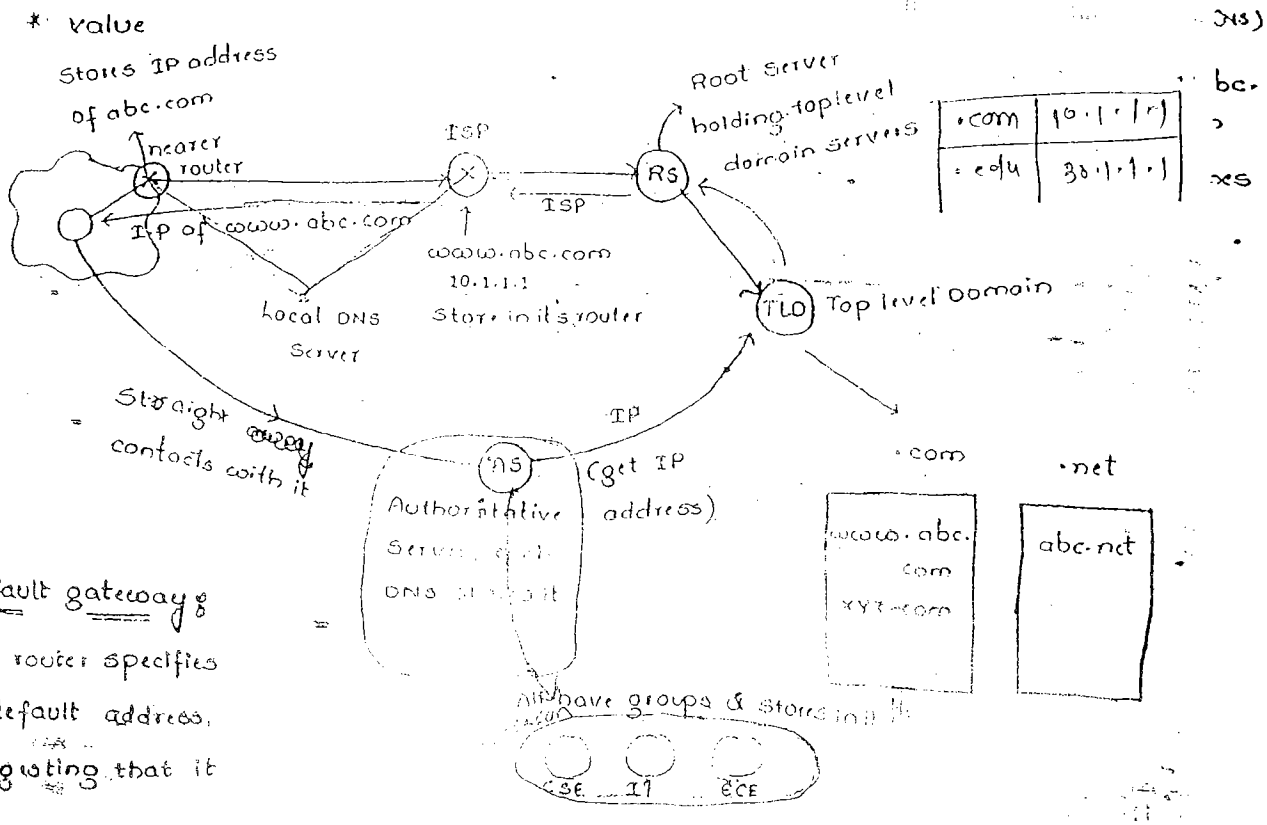
It uses distributed database to perform it's applications...

Information about computers and services are stored in these servers in terms of resource records. (Name, class, TTL, type, value)

It uses TCP as well as UDP. It uses glue record to avoid circular dependency.

Each resource record consists of 5 attributes. They are :

* Name
* TTL
* class
* Type
* Value



.com	10.1.1.1
.edu	30.1.1.1

Default gateway :

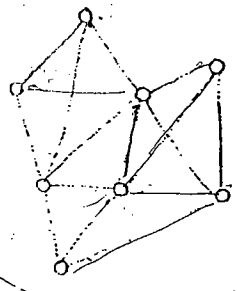
router specifies default address, saying that it don't know particular address.

item.

* Once a request for a website is sent, it gets stored in ISP and the local router. Whenever again a request of same website is sent, then there is no need to visit all the servers and there is only subsequent request simply it shows the websit without visiting root server.

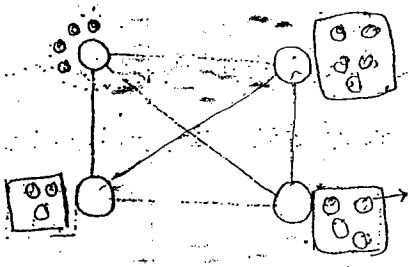
* Mainly 70.% of Internet services are provided by ISP & local routers.

* When Top level Domain servers maintained, in terms of clusters. These all are connected with MESH topology. It helps to improve efficiency and reliability.



→ with MESH connection

RS (maintains many routers and get connected) not only single router.



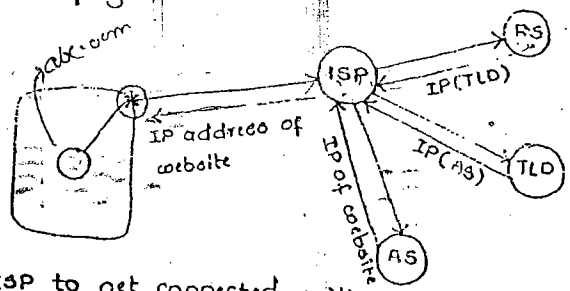
in the form of clusters & distributed data basis.

It will help for fast searching (effective usage)

Getting IP-address can be done in two ways :-

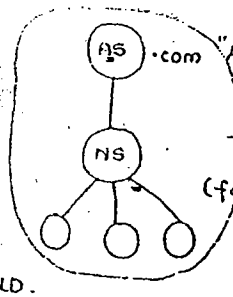
(1) Back page

(2)



RS, asks ISP to get connected with TLD by giving default TLD.

NS : Name Server



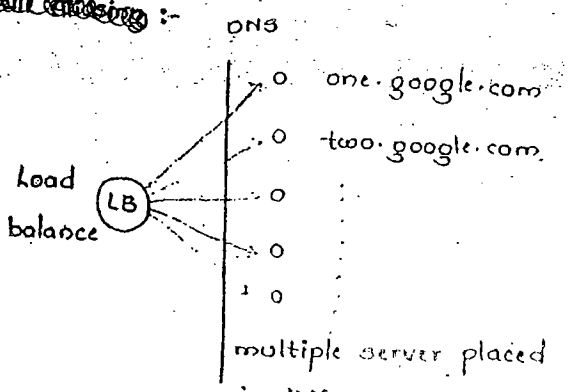
"AS" asks to "NS" to get the pages (for removing burden)

Giving Names to systems in a network (Host aliasing)

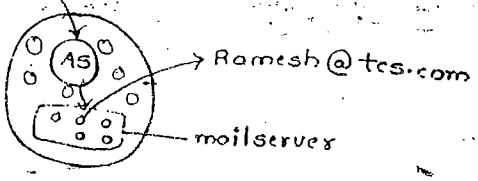
Intranet Application ⇐ $B_1.i_1.one.abc.com$ ⇒ by seeing name, one can understand position of the system.

In "abc" college building, "one" lab, "one" first system.

mail aliasing :-



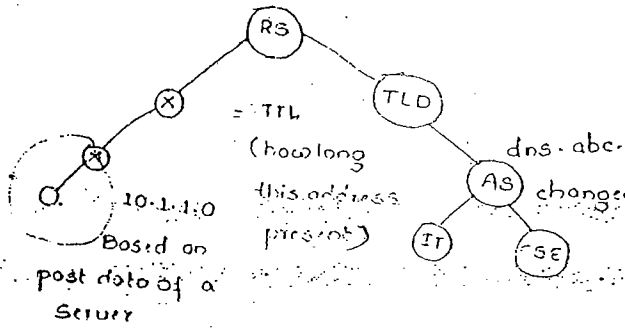
* mail aliasing :



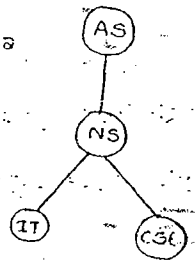
DNS

Ramesh@tcs.com c:/programfiles/ramesh

Distributive Database :-



It contain resource records :-



IT.abc.com 24hrs IN A 10.1.1.3

www.abc.com 24hrs NS dns.abc.com (value)

cocoo.abc.com 24hrs cname backup.abc.com

Canonical name ⇒ alternative names for websites.

Consider a request of page, for which the IP address is stored in router. If again, the same page is requested with little time gap, it is retrieved from nearer router.

circular dependancy ⇒ glue record

Replication ⇒ sharing data (If more replication ⇒ use TCP
Translation ⇒ use UDP)

HTTP :

(1) It is a client server protocol using port 80 in TCP.

(2) It is stateless protocol.

(3) There are two types of HTTP protocols < Persistent, Non-persistent

(4) It have two types of messages < Request, Reply

(5) HTTP will perform it's operations by using 8 different methods :-

* Head (HTTP developed through) ⇐ browser, browser version, operating system
(All html pages stored in webserver)

(2) Get ⇒ using Get method, client can get whatever information about web sites he wants

(3) Post ⇒ creation (Create an object in server)

(4) put ⇒ changing (modification)

(5) delete ⇒ delete (fatal error)

(6) Trace ⇒ debugging

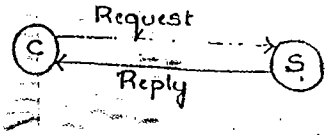
} unsafe method, Disabling, providing feedback message, redirecting to summary.

(7) options ⇒ optimisation (using "use Analysis" using user patterns)

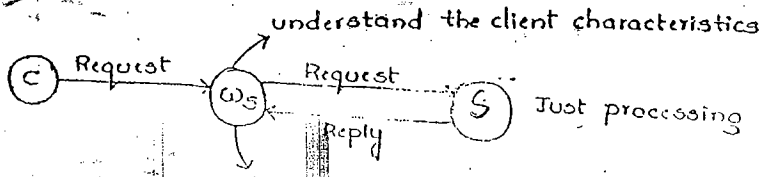
(8) connect ⇒ through the channel end_users security perform transactions) (may be any tampering)

HTTP uses 3 different types of status for it's operations :-

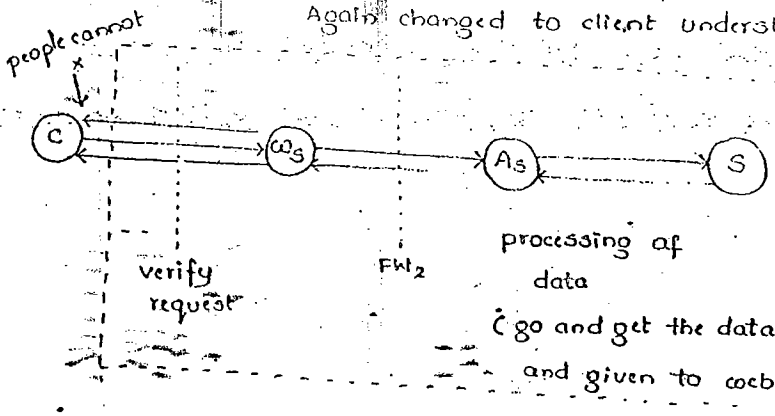
(1)



(2)

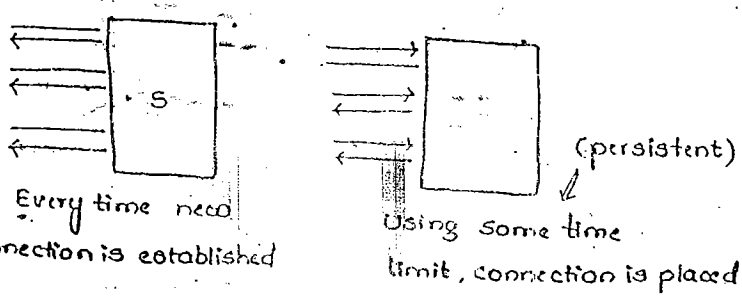


(3)



(go and get the data, and perform processing and given to webserver) ⇒ purpose of HTTP.

on-persistent connection in 1.1 (in 2.0 is changed to persistent)



2- Successful

3- redirecting

4, 5 } error methods

each & every request, express head method (client) (stateless protocol)

- Display status error.

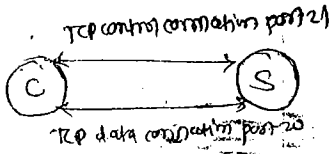
File Transfer protocol (FTP):

07/08/2010.

* It is a client server protocol. Uses port numbers ⇒ 20 & 21 on TCP.

* It have two types of connections :-

  * Data Connection (using port - 20).
  * Control connection (using port - 21)



* There are 3 modes of operation :

  (1) Active mode
  (2) passive mode
  (3) Extended passive mode.

* There are 2 flavours of FTP :-

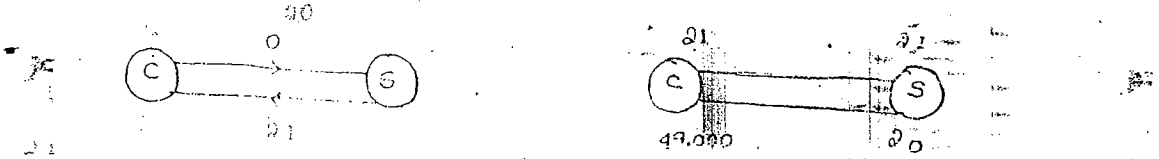
  FTP ⇒ Authorized users

  TFTP ⇒ Anonymous users

* To keep track data transmissions, FTP uses wide varieties of status codes and also it is supported with many no. of commands (To require connections)

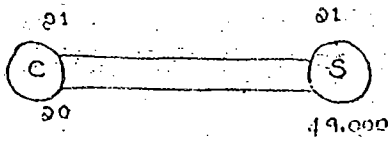
TFTP ⇒ never requires username and passwords. All the users within the applications can access the data.

Eg :- LIC policy application



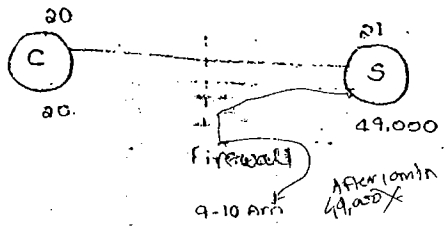
Active mode.

get connect (if poosible) with the same address.



Passive mode.

In passive mode, server generates a dynamic address and it is being get connected with the client.



20
21
25
80
} port numbers

Other than this not used.

Extended passive mode.

In this mode, a firewall is being placed between client and server, where the time is assigned to packet. If packet is received after the time, then firewall discards the packet.

To support the data connection perfectly. (i.e., ~~not~~ takes more time), where the FTP must be monitored constantly in these time, so, for this we use a no. of commands.

The monitoring of FTP constantly assumes the checking of status codes.

HTTP + SSL ⇒ HTTPS.

FTP + SSH ⇒ security (more)

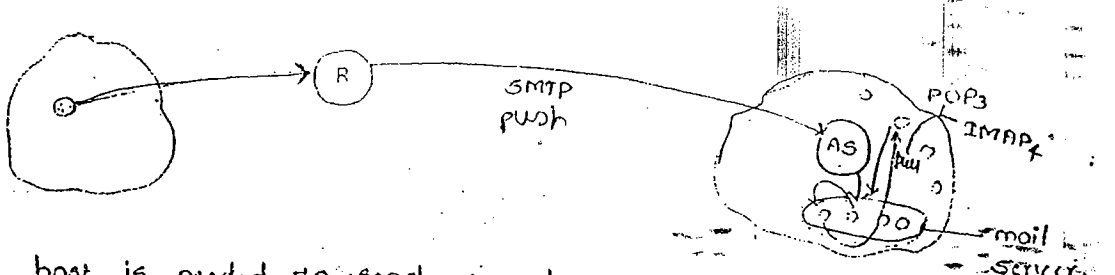
By using SSH ⇒ a secured pipeline is established which is used in FTP.

SMTP :-

* It uses port 25 at TCP.
* It is host-to-host transport protocol.
* It is text-based protocol, but enabled with multimedia with MIME extension.

  MIME — multipurpose Internet mail extension

* It is having two components :-
  * User agent.
  * Mail Transfer agent
* It is a part of push-pull mechanism in the mail communication. Therefore, SMTP is used to push the mail.
* POP-3 (post office protocol-3 — download mail), and IMAP4 are used for pulling the messages.
* It is an example for asynchronisation communication. (i.e., client and server are indirectly connected) — It is asynchronous protocol
* If client and server are directly communicated (connected) ⇒ Synchronous communication
* It is connected to DNS server also.



* If a host is needed to send the data, then it gets connected to the router and then the router gets connected to the Authoritative server through SMTP protocol. The Authoritative Server (AS) identifies

particular host in the mail server and gets "push" the data into that host. And if any other host requires the data within the network, then, the data is being "pulled" by the server.

* Hence, the mechanism is being considered as the "PUSH-PULL" mechanism, for this mechanism, POP3 and IMAP4 are used.

IMAP4 is more advantageous than POP3. for this consider an example:-

Before downloading a file, a message is delivered to check it. Is SAFE (or) associated with any virus. If user interested to continue, (either it is SAFE (or) UNSAFE) then only it processes, and if he is not interested simply 'CANCEL' it. ⇒ It is an advantage of IMAP4 over POP3.

IMAP4 push some of the (dangerous mails) to junk mails where as POP3 can't do so.

Hierarchies in the inbox:-

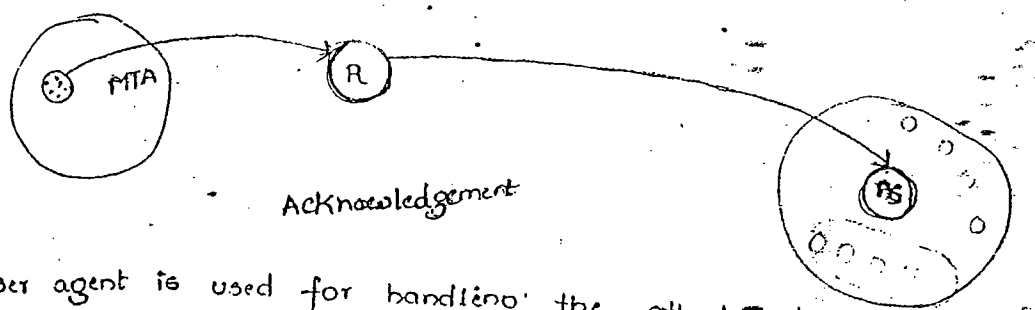
A folder is created in the inbox and are configured with some mail addresses (such as colleagues mails, friends mails, office mails etc) so that there is no chance of missing important information.

Two components:

* User agent
* mail Transfer agent (Incharge to negotiate with TCP for connection SMTP).

* Forward messages ⇒ attachments are available with the message. (All "To:", "Cc" and "BCc" are available).
* Reply messages ⇒ all the attachments are automatically dropped. (only "To:" and "Cc:" are available)

* Read Receipt component (if set) ⇒ then user (who send a mail to other can able to know either the other user (who received a mail) has received and read it or not.
* while user reads the mail, an acknowledgement is sent to the sending user, that the recipient had read it.



* User agent is used for handling the attachments and disattachments and mail Transfer agent is an incharge to have a connection with mails of SMTP through TCP.

Internet protocol (IP):-

Different Special IP addresses:

S.No.	Source IP addresses	Destination IP address
1	×	×
2	×	✓
3	×	✓
4	✓	×
5	✓	✓
6	×	✓

* The above 6 IP addresses are used only for special purposes, within the Internet protocol (IP).

* Some of the IP addresses are used to represent only source IP addresses and some are destination IP addresses.

(i.e. it represents to have network ID (NID) and some Host Id (HID))

Loopback address: 127.0.0.1

Link local addresses:

169.254.0.0 to 169.254.255.255

These addresses are automatically assigned to the local host by operating system in environment where no IP configuration is available. Only device in the same H/w can use these address range.

(1) ✓ ✗ 0

NID HID ⇒ filled by 0's

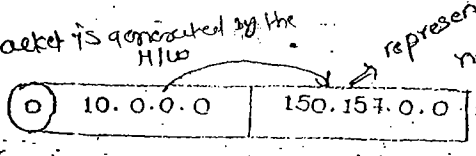
A : 10.0.0.0

B : 150.157.0.0

C : 192.168.1.0 (Network)

Name : "This network" address.

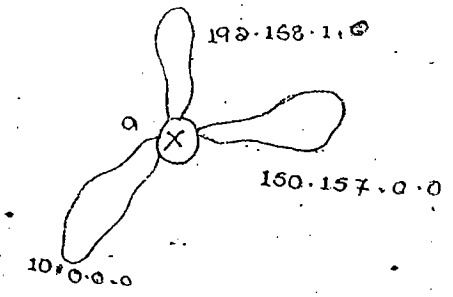
Purpose : used by Router.



⇒ not valid

but actually packet is generated by the systems in n/w

* They cannot be used as source IP address & dest. IP address.



10.0.0.0	a
150.157.0.0	b
192.168.1.0	c

* This type of IP addressing system are used by routers, to identify the network, for which it belongs to.

(2) NID HID ⇒ filled by 1's

1's

✗ ✓

A : 10.255.255.255

B : 150.157.255.255

C : 192.168.1.255 (Broadcast)

Given the network 192.168.1.0/24 → class C, H/w

192.168.1.0 (This network)

192.168.1.1 (default gateway)

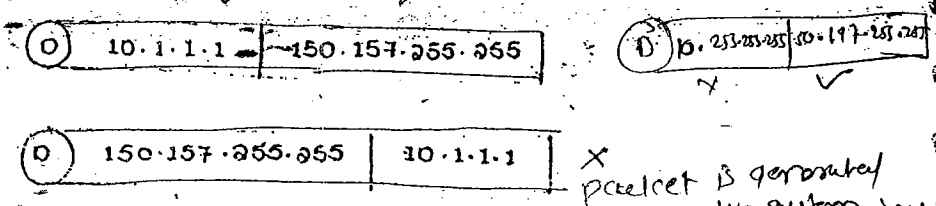
192.168.1.255 (Broadcast)

So, 192.168.1.2 ... (Host IP)

254

Name: Directed Broadcast address // Delivering packets to all systems in some other network

Purpose: To all in sender network.

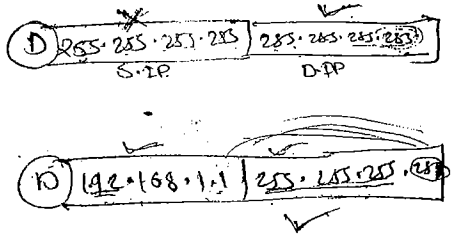


* Host ID is appended with all 1's, and network ID can be any other value.

(3) 1's 1's

NID HID

255.255.255.255



Name: Limited Broadcast address // Delivering packets to all systems in our own network.

Purpose: To all in the local network.

* Both the host ID and network ID's are being appended with 1's.

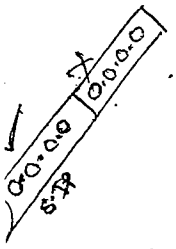
(4) 0's 0's

NID HID

0.0.0.0

(1) Auto
(2) Static
(3) Dynamic

Static: more IP address, less no. of systems

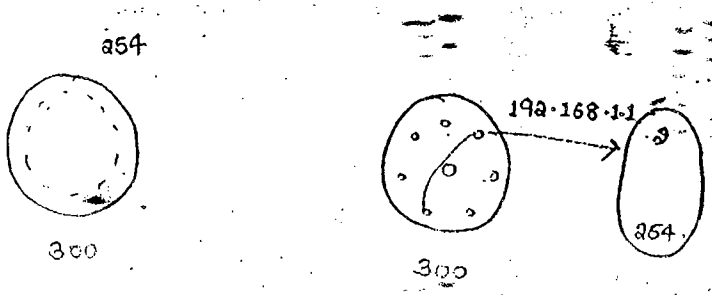


Name: Dynamic IP address. DHCP client

Purpose: Dynamic Host-configuration protocol (DHCP)

In Dynamic, more no. of systems, so it can be limited IP addresses.

(1) Static :-



* For a particular duration of time, an IP address is permanently given to the user. After performing the "logout" by any user on particular system, th the IP address is assigned to the other user.

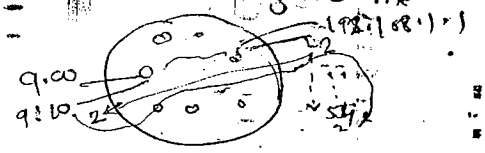
* Like wise, 254 IP addresses are managed by the server (but not clients directly) in the First Come First Serve (FCFS) basis. If there are more requests, an "Queue" is maintained.

* So, it is used only for the source but not destination.

Dynamic :-

C	0.0.0.0	192.168.1.1

* The operating system on the basis of administrator, assignes the IP address to the systems.



Auto :-

* The operating system, directly assignes the IP addresses to all the systems without the intervention of administrator, automatically.

(5)

0

NID HID

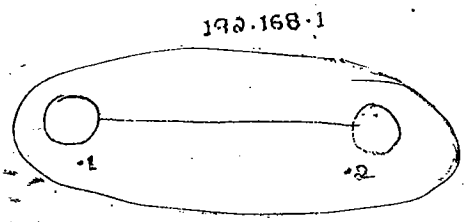
A : 0.1.1.1

B : 0.0.100.1

C : 0.0.0.100

Name : Host in this network.

purpose : local communication.



IP	192.168.1.1	192.168.1.2

(or)

	0.0.0.1	0.0.0.2
	SIP	DIP

The communication is done among the two host systems within the same network. ⇒ local communication.

The communication is not possible for the host in one network with the other host in other network.

Therefore, the network ID is fixed (or) unique, and only the host ID alternates for every communication.

→ we can use it on destination IP address only.

(6) | 127 . — . Any — |

127.1.1.1 (or) 127.100.0.255.

127.0.0.1
127.0.255.100

Name : Loop back address

purpose : * Interprocess communication.

127.0.0.0 X

127.255.255.255 X

* Self checking (or) self connectivity with checks.

127.0.0.0	×
127.255.255.255	×

(D) 192.168.1.1 | 127.1.1.1 ✓

* Both IP addresses are not valid. Other than these two IP address all the others are valid, which starts with ID = 127.

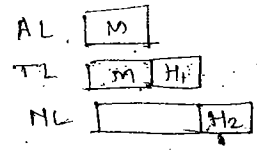
(1) which one of the following IP addresses are used as only source IP addresses.

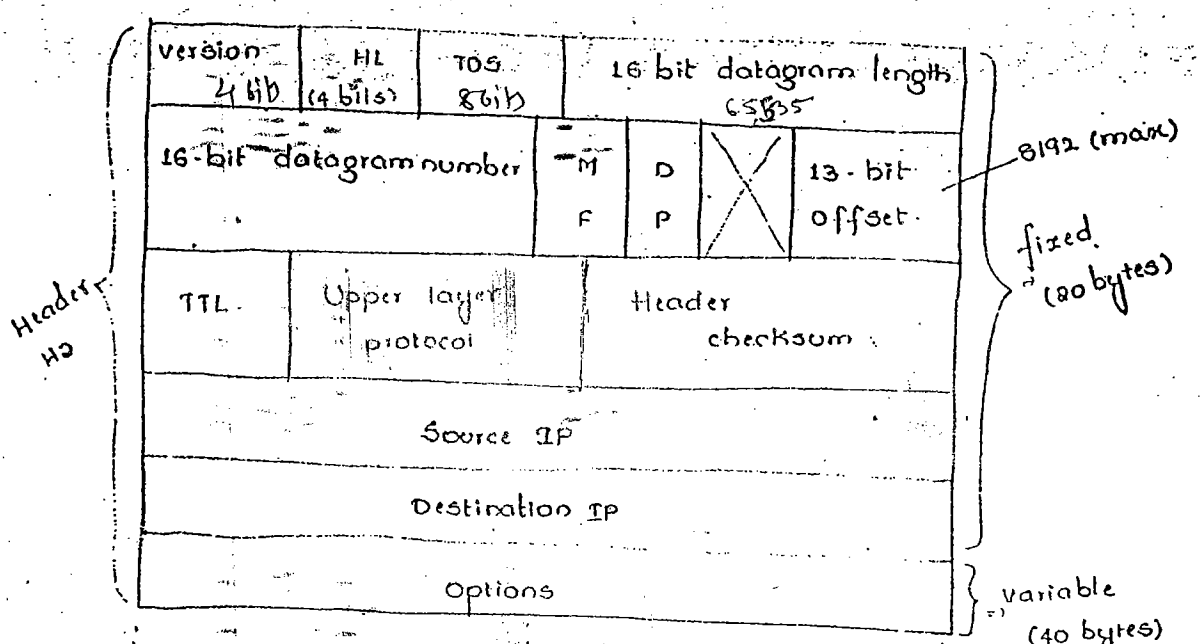
(a) 10.1.1.1 (b) 0.0.0.0 (c) 0.0.0.1 (d) 127.1.1.1

(2) which one of the following IP address are used as both source and destination addresses.

(a) 10.1.1.1 (b) 255.255.255.255 (c) 10.255.255.255 (d) 0.0.0.11

IP operations :-





version ⇒ To indicate either IP_4 (or) IP_6 packet. (4-bits)

IP_6 less complicated than IP_4.

HL (Header length) ⇒ minimum size ⇒ 20 bytes

maximum ⇒ 60 bytes

2^4 = 0 15

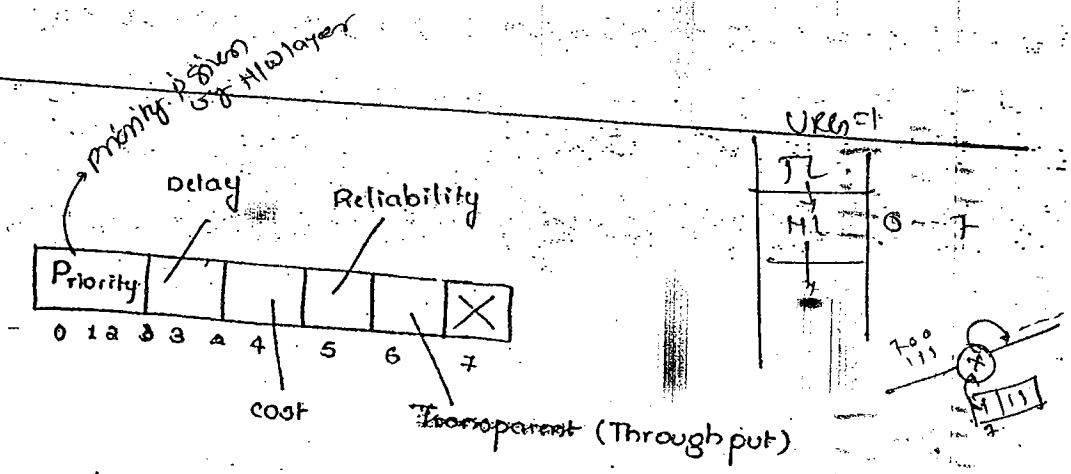
∴ 20 – 60 bytes

Constant scale factor = 4.

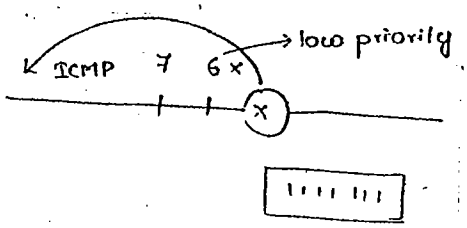
$\frac{\text{Act.-Header length}}{8}$ = Available header length in pkt (4 bit)

TOS :

(8 bit)



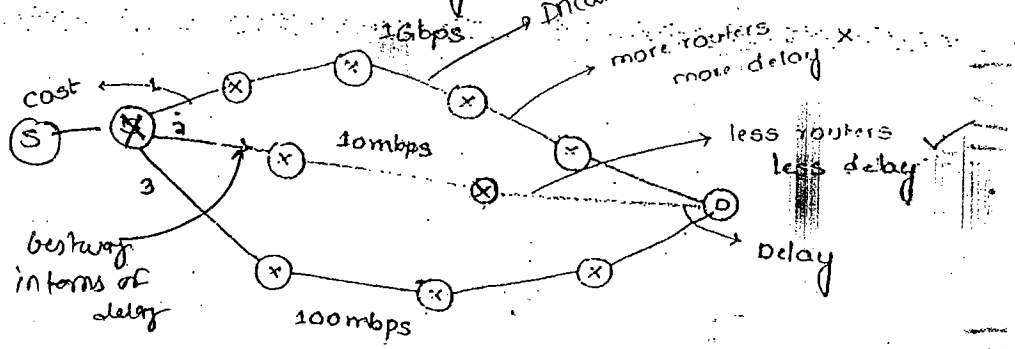
Based on priority, packet is transferred to Intermediate router.



Delay :-

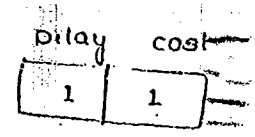
more routers more delay.

Incase of reliability, throughput (no. of links, no of routers, bandwidth, no. of links connected)



cost :-

Considering bandwidth, no. of routers, error rate, distance among the routers, the cost is being calculated.



to decide link.

Reliability :-

* It represents the "Error rate".

Throughput :

* It depends on bandwidth. If high bandwidth for a link ⇒ then allows

16 bit datagram length

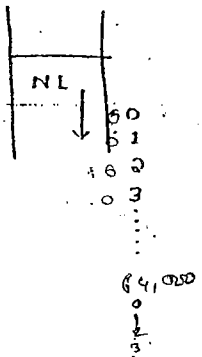
2^{16} = 64 KB ⇒ i.e., maximum size of the total packet.

16 bit datagram number :-

* Every datagram associated with the sequence numbers starting with '0'.

MF (More Fragments) :-

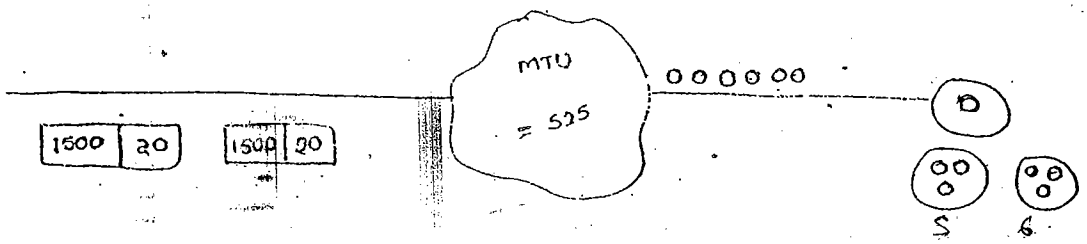
* Maximum Transfer unit (MTU).



* Fragmentation is applicable to only datagram (data) packet but not for header.

* OFFSET indicates no. of data bytes ahead of this fragment in that particular packet

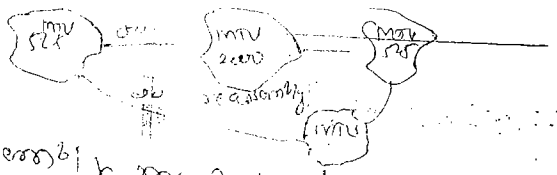
datagram data = MSD + H



	①	②	③	④	⑤	⑥
	504		504	492		
	505	505	490	505	505	490
	+	+	+	+	+	+
	20	20	20	20	20	20
	5	5	5	6	6	6
MF (is 0 for last packet)	1	1	0 (end)	1	1	0
offset (is 0 for first packet)	0/8	505/8	1010/8	0/8	505/8	1010/8
		504	1008			

505 is not divisible by 8 so take the nearest divisible no.

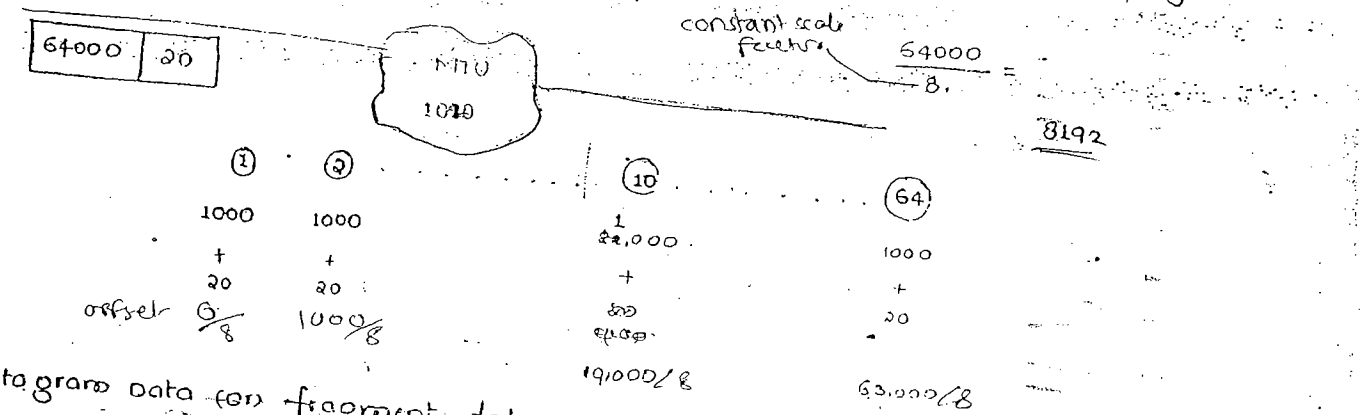
CSF = 8



One datagram is fragmented, reassembly must be done only at the destination, because of two reasons (1) different MTU may have different sizes therefore it should be done at every destination (2) All fragment may not follow the same route

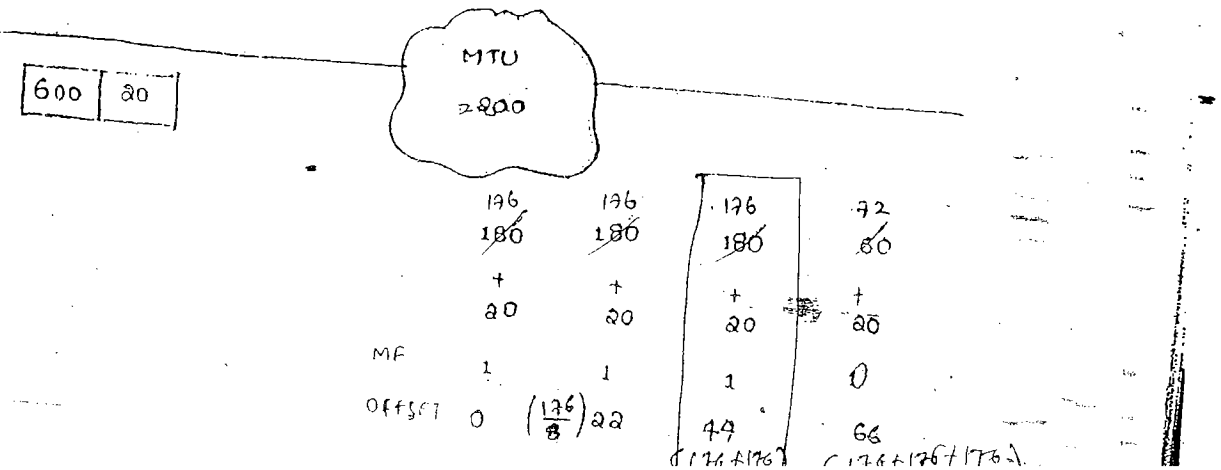
Re-assembly Algorithm at destination :-

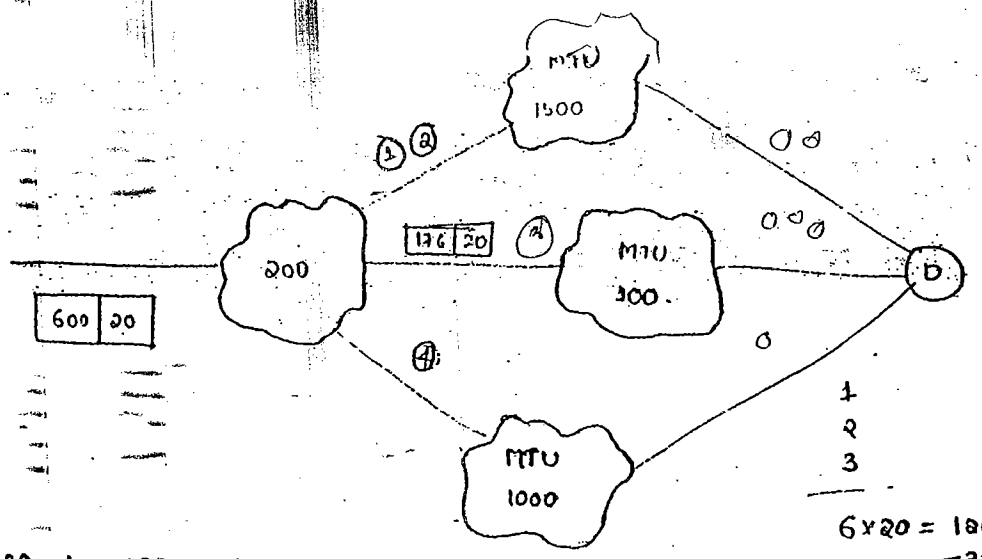
* Classify fragments based on 16-bit datagram number.
* Identify the fragment with offset = 0 and designate it as a first fragment.
* Identify the fragment with MF = 0 and designate it as a last fragment
* Identify data in the first fragment and look for the fragment with same offset value and designate it as second fragments.
* Repeat previous step as many times as possible to cover all the fragment



* Datagram data for fragment data must be divisible with '8'. If not adjust it's number so that it is divisible with '8'.

This rule is applicable for all the fragments except for last fragment.





$6 \times 20 = 180$
-20
100

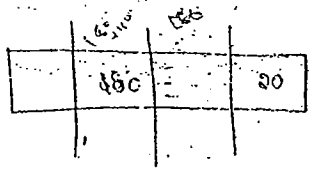
* If offset = MF = 0 ⇒ Original packet

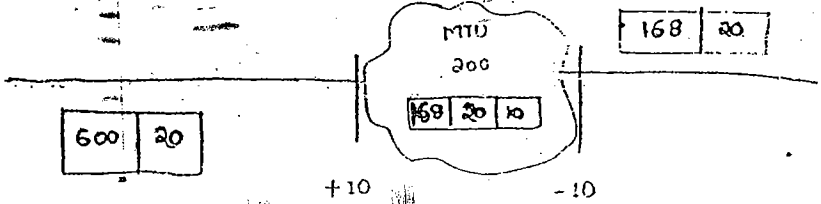
* If any one of them is non-zero ⇒ fragment (intermediate fragment)

176 | 20

	80	80	16
	20	20	20
MF	1	1	1 ⇒ Intermediate fragment
offset	44	54	64

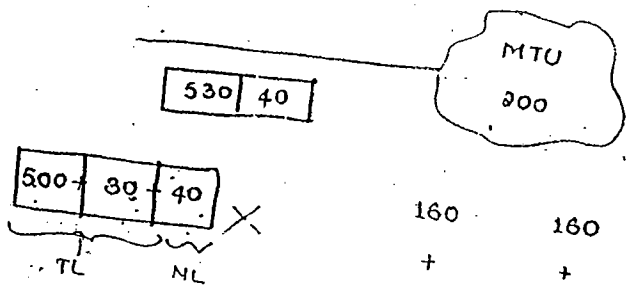
$(44 + \frac{80}{8})$ $(54 + \frac{80}{8})$





	168	168	168	96
	~~140~~	~~140~~	~~140~~	~~140~~
	+	+	+	+
	20	20	20	20
	+	+	+	+
	10	10	10	10
MF:	1	1	1	0
offset:	0	168/8	168+168/8	.....

Msg : 500
TcPH : 30 } Datagram data.
IPH : 40
MTU : 200.

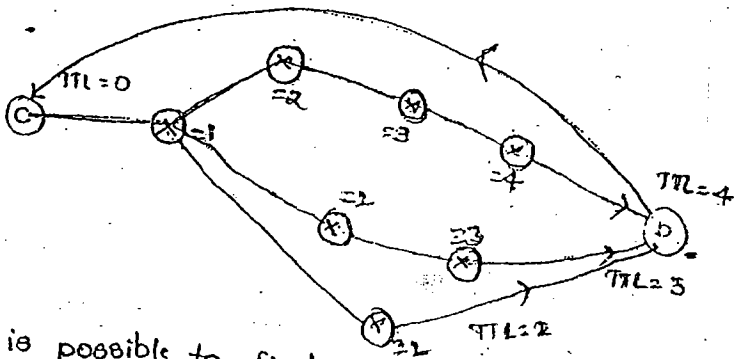


160 + 40 ..... 160 + 40

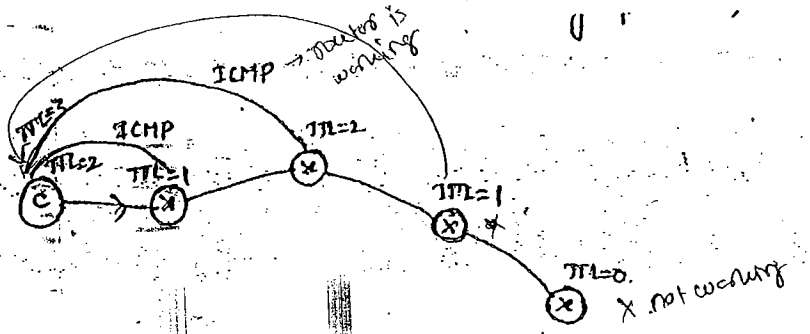
Msg
DF=1
Don't Fragment

11/08/2010
Wednesday

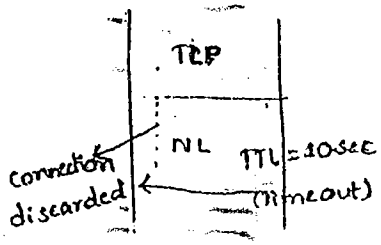
* Time To live (TTL) :-
* It have four applications :-
  * To avoid infinite looping
  * To identify no. of routers between source & destination.
  * To debug the networks.
  * To help upper layer in timer management.

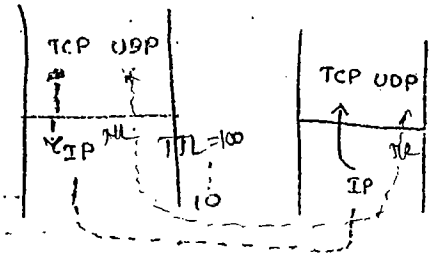


It is possible to find no. of routers in a route by using 'TTL' value.

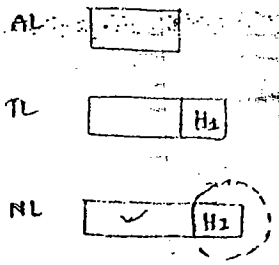


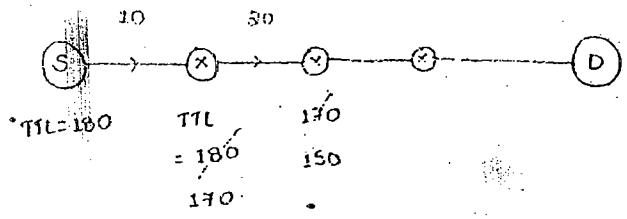
* Timer management :-





* Header checksum is carried out at every router (and only at Header)





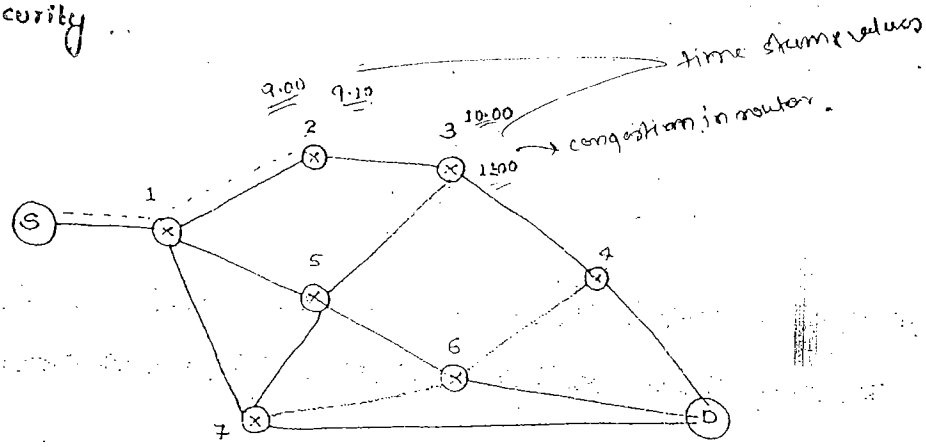
* TTL
* MF
* Offset
* 16-bit datagram-length
* options.

} ⇒ Tend to change at every router (variable)

Source, destination } ⇒ fixed

Options:

* Strict source routing } Source will decide the route (D) 1,2,3,4
* Loose source routing } (D) 1,4 (practical)
* Record routing ⇒ router decides the route
* Time stamp values
* Security



Strict source routing:

* Each and every route is specified (1,2,3,4)

Loose source routing:

(1 4)

* Only the important routers are specified and the route is generated based upon those routers ⇒ practical.

(1,2,3,4)
(1,5,3,4)
(1,7,6,4)
(1,5,6,4)

Record routing: (1,7,5,6)

* Packet can be transferred as it wishes among all the routers.

Time stamp:

* Arrival Time & Departure Time of each & every packet is stored.

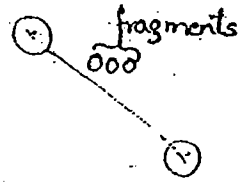
Security:

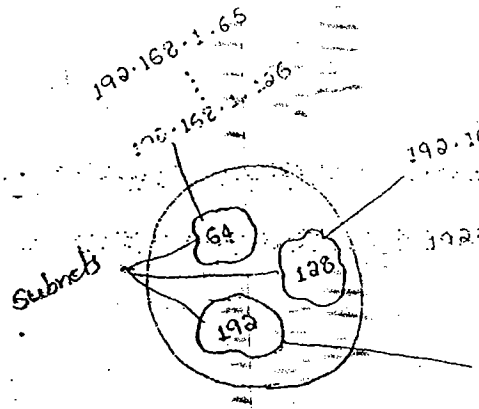
* Mails are sent along with certification, which provides secured access for a page.

Q) If a packet is fragmented into 3, then, which of the options are must available in all the fragments and which of them are necessary to present in any one of the fragments ?

Ans:- Strict source routing
loose source routing
} must available in all the fragments.

* Record routing
* Time stamp
* Security
} must be necessary in any one of the fragment.





class c : NID HID ← borrow first two bits

24 2 6

S10 H10

$2^2 = 4$

$2^6 - 2 = 62$

128 64 32 16 8 4 2 1

0 0 = 0
0 1 = 64
1 0 = 128
1 1 = 192

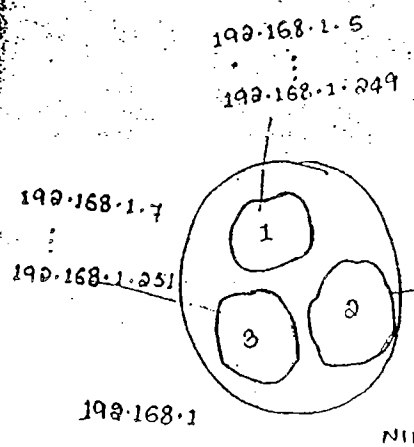
01.....

01 000001 - 65
01 000010 - 66
⋮
01 111110 - 126

10.....

10 000001 - 129
10 000010 - 130
⋮
10 111110 - 191

11 000001 - 193
⋮
11 111110 - 254



NID HID

24 6 2

128 64 32 16 8 4 2 1

0 0 - 0

0 1 - 1

1 0 - 2

1 1 - 3

.....01

000 00101 - 5

000 010 01 - 9

⋮

111110 01 - 249

.....10

000001 10 - 6

0000 110 10 - 10

⋮

111110 10 - 250

* Subnets id's and IP address of the networks ⇒ are changing.

* Inorder to deliver a data packet, the following must be checked :-

  * Either subnets are available (or) not.
  * If not available, the IP address is directly assigned to that.
  * If available, then identify the packet belongs to which subnet, for this we use subnet mask (SM).

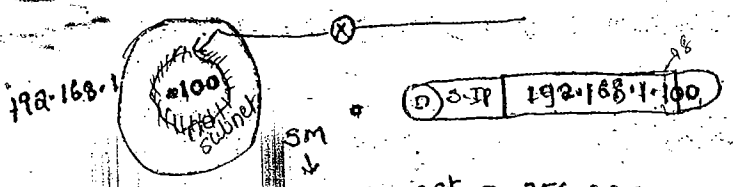
Subnet mask

* It is also a 32-bit system and it is used to indicate whether subnet are available (or) not in the network.

If available, it will give the information about no. of bits borrowed from host id and their position, based on the following two rules:-

(1) No. of 1's in the subnet mask, indicates network Id plus Subnet Id.

(2) No. of 0's indicates Host Id part.



SM

Subnet mask = 255.255.255.0

SM = 11111111 . 11111111 . 11111111 . 00000000

Rule (1): NID + SID = 24 (since, class c)

(2): HID = 8 (since, no subnets, nothing is borrowed from HID)

NID = 192.168.1

HID = 100

(Q) Consider a class c network with SM = 255.255.255.192. Identify no. of bits borrowed from HID and their position, possible subnets and their ID's, possible no. of systems for subnet and range of IP addresses in each and every subnet.

Sol:-

SM = 255.255.255.192

(NID: 24, HID: 8)

SM = 11111111 . 11111111 . 11111111 . 11000000

Rule(1): NID + SID = 26

HID = 6

No. of bits borrowed = 2.

Their position is = 128th bit, 64th

possible subnets = $2^2 = 4$

Their subnet ID's = 11000000

00 - 0

01 - 64

10 - 128

11 - 192.

No. of systems per subnet = $2^6 - 2$

Range of IP addresses =

(8) Consider a class c network with SM = 255.255.255.41. Identify all the data points as previous question.

SM = 11111111 . 11111111 . 11111111 . 00101001

NID + SID = 27

HID = 5

no. of bits borrowed = 3

Their position is = 32, 8, 1

possible subnets = 2^3 (0, 1, 8, 32, 9, 40, 41, 33)

No. of systems per subnet = $2^5 - 2$. = 30

32	8	1	
0	0	0	= 0
0	0	1	= 1
0	1	0	= 8
0	1	1	= 9
1	0	0	= 32
1	0	1	= 33
1	1	0	= 40
1	1	1	= 41

Their subnet ID's = 0, 1, 8, 9, 32, 33, 40, 41

Range of IP address for subnet 1

..0.0.1

00000001 - 1

00000101 - 5

00101001 - 41

(9) Consider a class B network with SM = 255.255.255.0.. Identify all the data points as previous question.

Sol:-

Subnets are available.

Entire 3rd octet are borrowed for subnet ID's.

∴ no. of subnets = 2^8

Their ID's = (0 - 255)

SM = 11111111 . 11111111 . 11111111 . 00000000

No. of systems = $2^8 - 2$.

Their ID's = (1 to 254)

Ex: consider class C network with SM = 255.255.255.15.

Sol:

SM = 11111111.11111111.11111111.00001111

24 4

NID + HID = 28

HID = 4

no. of bits borrowed = 4

Their position is = 1, 2, 4, 8

possible subnets = $2^4 = 16$

No. of systems per subnet = $2^4 - 2 = 14$

Q) consider a class C network. proposed an appropriate subnet mask to have 7 subnets each with 25 systems.

$7 * 25 <= 256$ (since, it is class C)

24 | 8

3 | 5

5 | 3

3 bits must be borrowed (since, 7 subnets $\Rightarrow 2^3 = 8$ (nearer value))

255.255.255.224 ✓*

255.255.255.7 ✓

255.255.255.41 ✓

255.255.255.67 ✓

} all are possible but left to right is appropriate

consider a class B network and propose an appropriate SM to have 150 subnets each with 200 systems.

$150 * 200 <= 64,000$

30,000

150 ⇒ 8 ⇒ $2^8 - 2 = 254$

(required) 200

255.255.255.0

255.255.0.255

255.255.240.240

255.255.192.252

(9) consider a class c network. Propose an appropriate SM to have 20 subnets each with 15 systems.

$20 * 15 <= 256$

$300 \not<= 256$

not possible

(8) consider a classc network. Propose an appropriate SM to have of 60, 60 120.

classc ⇒ 8.

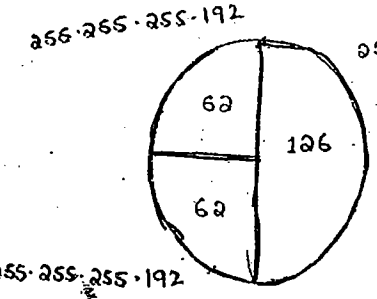
2	6	1	7

$2^2 = 4$ × $2^1 = 2$

× $2^6 - 2 = 62$ $2^7 - 2 = 126$

(not possible) (not possible)

So, in order to propose appropriate SM, we use the concept of VLSM.



255.255.255.128

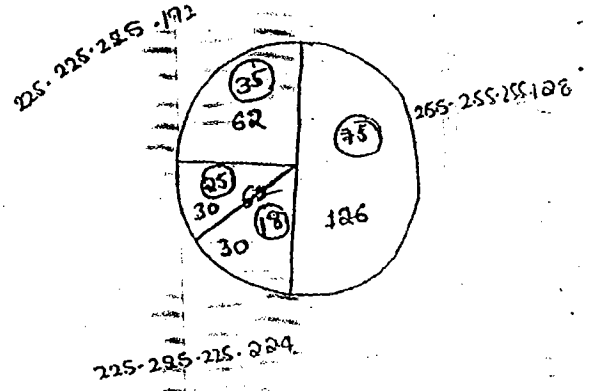
$2^1, 2^6 - 2 = 62$

1	6

1	7

(10) consider a 'c' network. propose an appropriate SM to have 4 subnets of 75, 35, 25, 18.

2	6	1	7
$2^2 = 4$		$2^1 = 2$	
$2^6 - 2 = 62$		$2^7 - 2 = 126$	

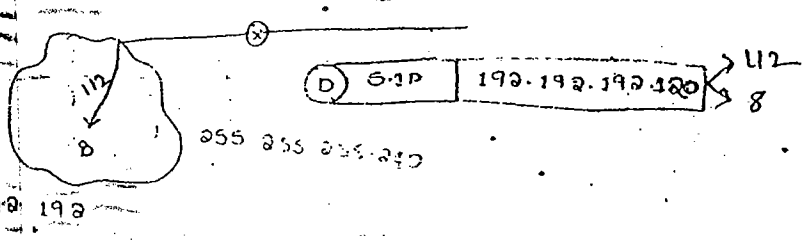


(9) Consider a class c network propose an appropriate SM to have 6 subnets of 30, 25, 22, 20, 18, 15.

Sol:- class c = 8 $2^3 = 8$

2	6	1	7

= 62.



Identify subnet ID, Host ID & directed broadcast address.

192.192.192 112 8

IP : 11000000 . 11000000 . 11000000 . 01111000

NID SID HID

SM : 11111111 . 11111111 . 11111111 . 11110000

NID SID HID

SID = 112

HID = 8

120

192.192.192.

64

192.168.1.65

1

192.192.192.127

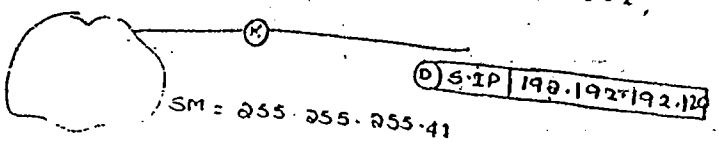
11000000.11000000.11000000. 0111 1000

7 6 5 4 3 2 1 0

Broadcast address

0111 1111

Eg:-



64 32 16 8 4 2 1

127

SID = 32+8+0 = 40.

IP : 11000000 . 11000000 . 11000000. 0111 1000

SM : 11111111 . 11111111 . 11111111 . 1 0 1 0 1 0 0 1

This is HID

SID

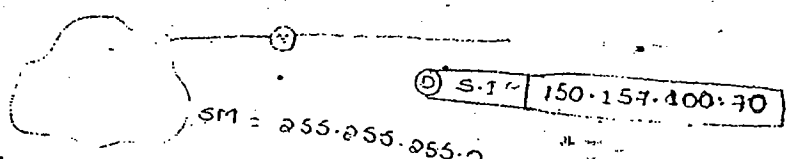
SID = 40

HID = 80

HID = 64+16+0+0 = 80.

⇒ 192.192.192.254 ⇒ Broadcast address

Eg:-



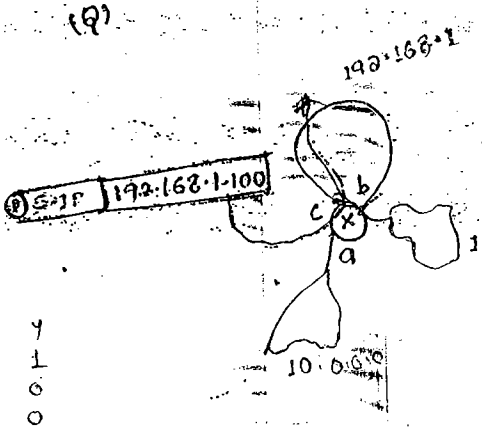
SID

SID = 100.0

HID = 0.70

Directed BC address = 150.157.100.255

(Q)



	IP	SM	i/f
	10.0.0.0	255.0.0.0	a
	150.150.0.0	255.255.0.0	b
✓	192.168.1.0	255.255.255.0	c
	0.0.0.0	0.0.0.0	Default route subnet mask.
	0.0.0.0	0.0.0.0	

192.168.1.100
AND
255.0.0.0
192.0.0.0

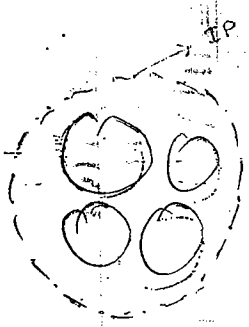
192.168.1.100
AND
255.255.0.0
192.168.0.0

192.168.1.100
AND
255.255.255.0
192.168.1.0

0.0.0.0 ⇒ Default route subnet mask

255.255.255.255 ⇒ Host specific subnet mask

Supernet :-



192.192.0.0 : 11000000.11000000.00000000.00000000
192.192.1.0 : 11000000.11000000.00000001.00000000
192.192.2.0 : 11000000.11000000.00000010.00000000
192.192.3.0 : 11000000.11000000.00000011.00000000

Supernet mask :

* It is a 32-bit system used to generate a single IP address for a group of networks based on following 2 rules :-

(1) no. of one's in supernet mask indicates fixed part.

(2) no. of 0's indicates variable part.

Supernet mask = 11111111. 11111111. 11111100. 00000000

SM = 255.255.252.0

(1) 192.192.0/22 : → represents NID.

class c :

$24 - 22 = 2$

2^2

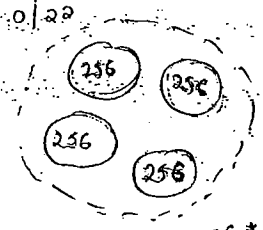
$2 = 4$

/24 = class c

/16 = class B

/8 = class A

(2) 192.192.0/22



256 * 4 = 1024

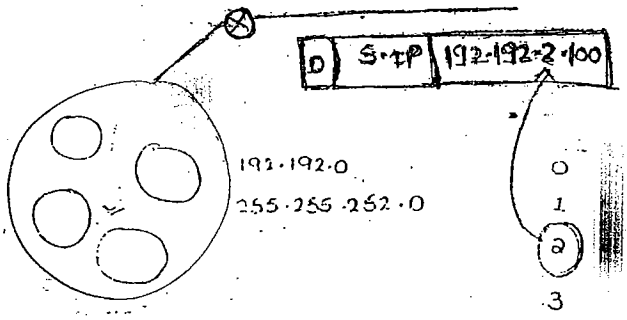
32

22	10
NID	HID

$2^{10} = 1024$

(2) 192.192.0

255.255.252.0



192

11000000

00 0
01 1
10 2
11 3

Differences between subnet mask and supernet mask:

SUBNET MASK	SUPERNET MASK
* No. of 1's in the subnet mask is either equal to network Id bits or more than network id bits.	* No. of 1's in supernet mask is always less than NID bit's.
* Bits are borrowed from HID.	* Bits are borrowed from NID.
* It is applicable to single network	* It is applicable for two (or) more networks.

* CIDR aggregation (classless Inter Domain Routing) => Another name for supernet.

A → NID bits = 8
B → NID Id = 16
C → NID = 24

	A	B	C
255.0.0.0	Subnet	~~Supernet~~ Subnet	Supernet
255.255.0.0	Subnet	Subnet	Supernet
255.255.255.0	Subnet	Subnet	Subnet

/24 - C
/16 - B
/8 - A
/22 - ?
/24 - ?
CIDR

192.192.0/22 => NID

/24 => class C

/16 => class B

/8 => class A

/22 — ?
/24 — ?
CIDR

14/08/2010
Saturday

* Adaptive (If problem occurs, re-calculated again)
* Non-Adaptive (If problem occurs, no re-calculation is done) ϕ

Page no: 90

Routing Algorithms

Shortest distance vector algorithm :

(1) How to find the distance blw source & destination.

(2) who take the decision

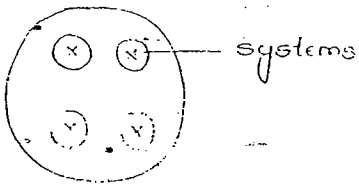
Adaptive → Time to Time, calculate the network

non-adaptive → whenever change happens, calculate the changes.

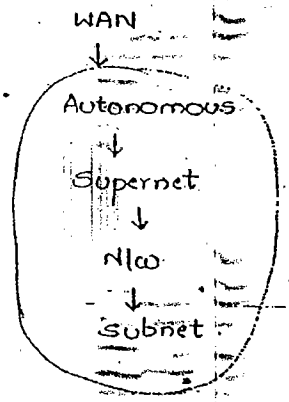
Autonomous system.

under single ISP

Page no: 92



one Autonomous system



Interior to Autonomous protocols ⇒ Interior algorithm

Outside Autonomous ⇒ Exterior algorithm.

Static routing table ⇓ Adaptive

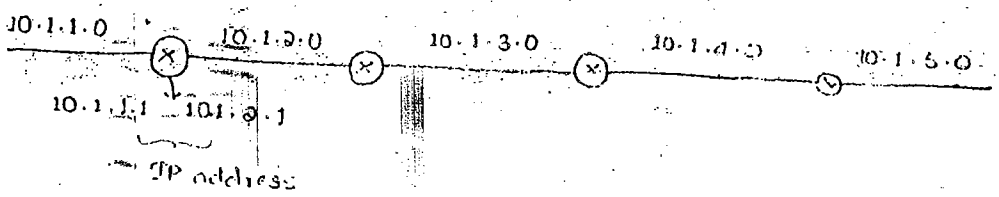
Dynamic routing table ⇓ Non-Adaptive

adaptive ↓ Interior ↓ Dynamic

exterior ↓ adaptive ↓ Dynamic

(periodic updates) with the help of neighbours.

more delay.



whenever new router added, (using broadcasting it is delivered to all routers), it directly gets update without checking, whatever the router sends. ⇒ Routing by Rumour

Page no: 97

So, there is count-Infinity problem (because of trusting neighbour).

page no: 96

Simple split horizon:

The ~~same~~ data obtained from a neighbour, must not be returned to same neighbour again.

* poisson reverse:

Send all the data except the information ~~that~~ained from the neighbour.

Abnormal information ~~getting~~

If a router have any abnormal information, then it not shares ~~with~~ its route table with any other.

Hold down Timers :-

Within some time interval (say, t=10), it is checked that whether the data is correct (or) not, if correct, then it is propagated.

p.no: 98

fig.. connecting the ethernet

Because of collision occurance, some time interval (t=30) is given to ec router to get connected with ethernet.

If collision occurs again (& again), then the time interval is increased (i. asynchronous timer) (t=90)

RIP ⇒ Routing Information Protocol

maximum hop count = 16 hops (restriction)

VLM ⇒ variable length masking
classless (supernetting) } never knows about these

p.no: 100

from 'c' ⇒ no information . 'B' ⇒ not gets any updation.

flushout [..... remove] . 'B' thinks that may be 'c' is in hold on wait state.

p.no: 99

Routing table header :

payload → table of router .

In NOVELL Netware ⇒ IP called as IPX

In ARPANET ⇒ CLNS

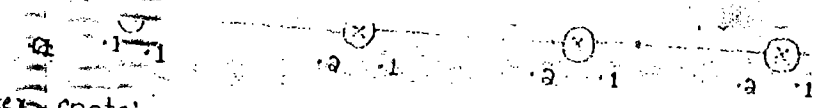
Internet Architecture :

Group of systems called Autonomous Systems ⇒ These are under single ISP many no. of Autonomous systems present under many ISP's.

In single Autonomous system, supernets present in each ~~supernet~~ netwo many networks under network subnets.

collectively, WAN contains this hierarchy.

WAN
Autonomous
↓
Supernets
↓
Network
↓



Single router contains any no. of IP addresses.

Above, router A contains two IP addresses 10.1.1.1 and 10.1.2.1.
router B contains 10.1.2.2 and 10.1.3.1.

Distance vector algorithm ⇒ share all the information with neighbours.

* when neco router is installed, for knowing the information about neco route it takes more time.

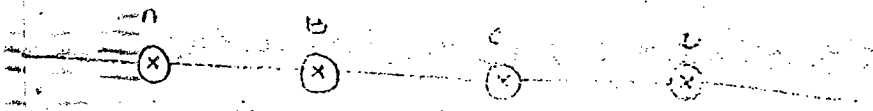
Within the given time, if any packet arrives from the set of netcoorks, then routing tables check for destination, if it's available, then sentl it. but routing table shows that no data available, eventhough that set of netcoork connected into the netcoork, because of this delay, packets wont reach the destination. To avoid this broadcasting the address to all stati without delay, updated information is used with the help of neighbours.

The main drawback of this algorithm, is "router accepts the data, whatever represented by it's neighbous without any checking, sometimes, it causes lot of problems.

Eg: count-to-infinity problem.

Time	Router A			Router B			Router C			Router D		
	NET	via	hops	NET	via	hops	NET	via	hops	NET	via	hops
	10.1.1.0	–	0	10.1.2.0	–	0	10.1.3.0	–	0	10.1.4.0	–	0
	10.1.2.0	–	0	10.1.5.0	–	0	10.1.4.0	–	0	10.1.5.0	–	0
Time t_1	10.1.3.0	10.1.2.2	1	10.1.1.0	10.1.2.1	1	10.1.2.0	10.1.3.1	1	10.1.3.0	10.1.4.1	1
				10.1.4.0	10.1.3.3	1	10.1.5.0	10.1.4.2	1	10.1.2.0	10.1.4.1	2
Time t_2	10.1.4.0	10.1.2.2	2	10.1.5.0	10.1.3.2	2	10.1.1.0	10.1.3.1	2	10.1.1.0	10.1.4.1	3
Time t_3	10.1.5.0	10.1.2.2	3	No new entries			No new entries					
Time t_4	No new data simply discard the data											

(a) To gather the information, router, simply depends on its neighbour.



Repeatedly A, B, C & D checks and updates information.

Suppose, assume that 'B' has no data available from 'c'. 'B' may think that 'c' is in hold & wait state. It is being waited upto "Hold & wait" (B) time even though no data available.

Then, up until "Timeout" time reaches 'c' entries are placed as "zero". If after that also no data available, then flush out the 'c'-entries.

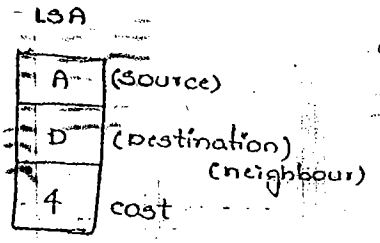
Link state algorithm:

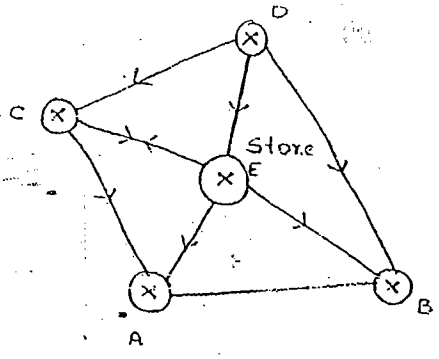
Itself, it calculates the shortest distance, (it don't depends on it's neighbours).

Process:

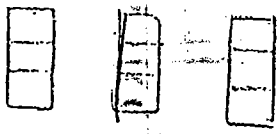
(1) Just identify neighbours and send hello packets to it's neighbours.

(2) Prepare LSA packets.





'A' have 3 neighbours:



(3) Broadcasts LSA packets to all the routers.

(flooding)

maintains LSA packets in router.

share all the packets of all routers ⇒ LSA Database

(4) Analyse the LSA packets

page no: 104

calculate cost

A - B - C - F = 2 + 1 + 2 = (5) → choose shortest path

A - D - E - F = if it is not available choose another shortest path.

A - B - E - F = 2 + 10 + 12 = 14

A - D - G - E - F =

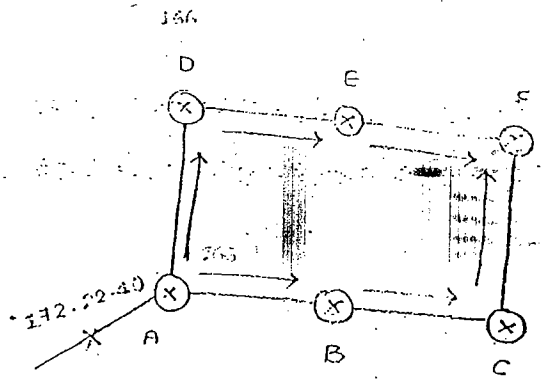
flooding using sequence numbers :

page no: 101

current sequence number = 166

165 ⇒ (discard) (don't receive) because old one

167 ⇒ receive, discard packet in the data-base and store it.



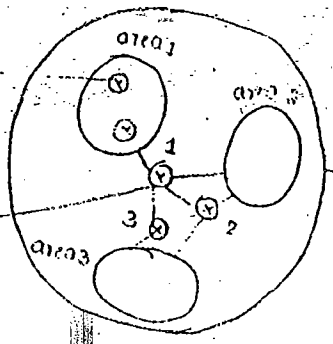
* If router is down, restart the router (it never knows which packet is available). It send '0' if available.

But current sequence number = 167, other router thinks that it is old packet and simply discard it.

To avoid this drawback, the new router asks it's neighbour that what the current sequence number is? and based on that next sequence number is used.

If all the sequence numbers are used, again start with "zero".

OSPF Algorithm (Identifying destination):



Internal router (IR)

Area Border Router (ABR)

Autonomous system border router (ASBR)

Backbone router

⇓

LSA database

⇓

contains all three router (1,2,3)

copy entire backbone database to ASBR.

SA - Stub Area (semisecured Area (Eg: only cse, IT))

Totally Stub Area - (TSA) (lot of restriction on many servers)

⇓ (not students)

Not so stub Area (NSSA)

20.1.1.1 ⇒ all default routers are closed (because TSA)

DR - Destination Router

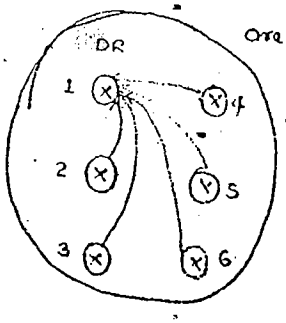
Send LSA packets only to DR.

Send this database to every one.

BDR - Backup Destinated Router:

If DR is lost, for availability purpose maintain BDR.

There are 'n' routers, 'an' messages are exchanged



1000 * 1000

⇓

To avoid many no. of exchanges OSPF application is introduced.

End

p.no: 106

Difference bleo RIP and OSPF :

RIP	OSPF
(1) "hop" bound limit = 60	(1) No limit
(2)	(2) Knows about cook.
(3) processing is very less	(3) It is highly complex.

p.no: 112

'OSPF' header :

Authentication type :

random numbers, username, password.

Grid :

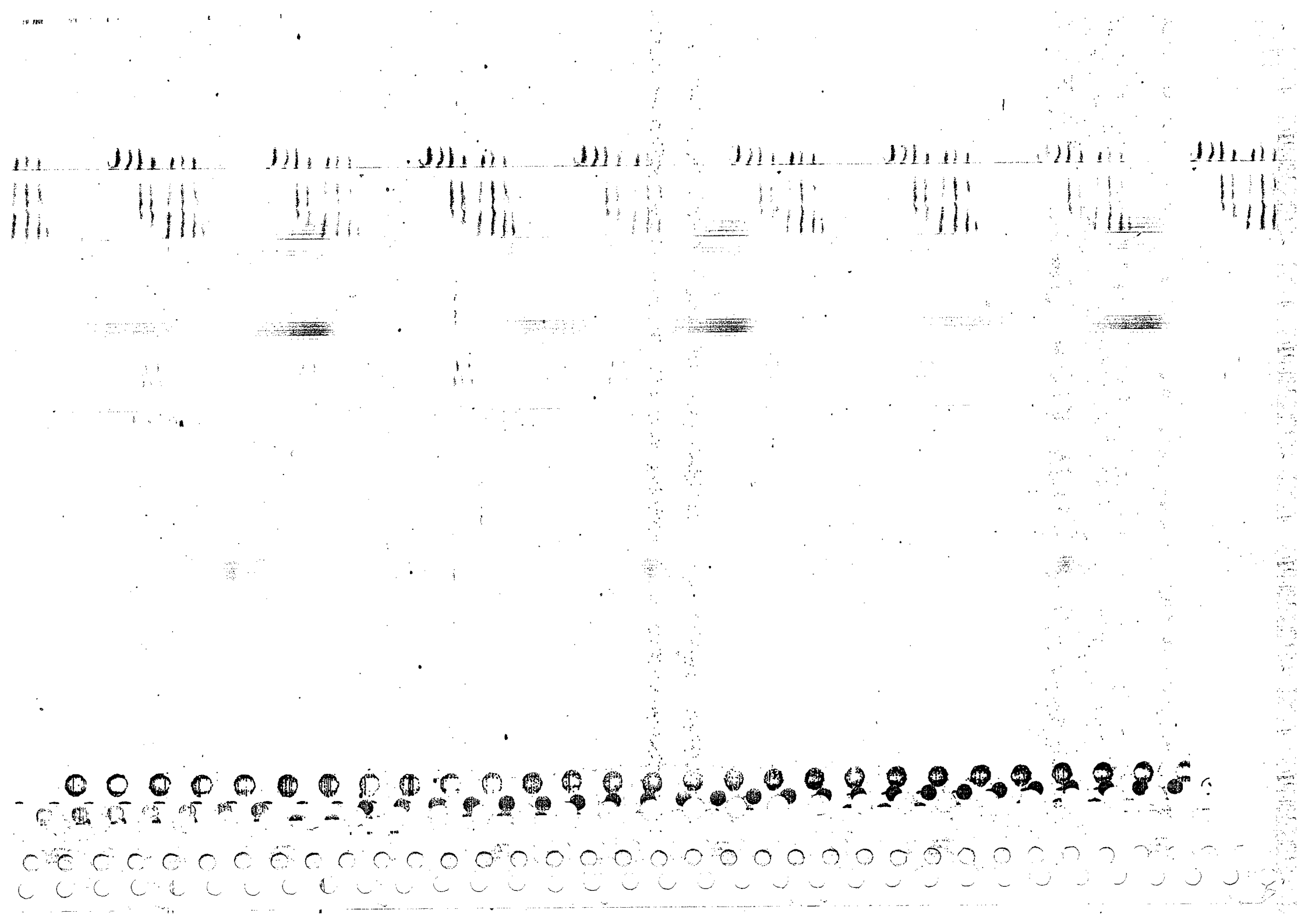
A	B	C	.....	Z
21	41	61		99

In addition to username & pswd, router asks to enter grid numbers of different alphabets, if it is correct, then it is processed => Authentication

5119
1024
4095
60

60)4095(67
360
495

(how much we transfer within one RTT,
=> maximum size of window)



16/07/2010

Friday

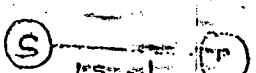
P.NO: 18

(1)

$$T = \frac{1 \text{ Data}}{RTT} = \frac{1024 \times 8}{45 \times 10^{-3}} = 182 \text{ kbps}$$

1kB

1024x8 bits



RTT = 45 msec

$$\eta = \frac{182 \text{ kbps}}{1.5 \text{ mbps}} = 12.1\ \%$$

(2)

$L = 1000 \times 8$ bits.

(a) 10 km.

(b) 5000 km.

$V = 0.7 \times 3 \times 10^5 \text{ km/sec} = 2 \times 1 \times 10^5 \text{ km/sec}$

$$T = \frac{1 \text{ Data}}{RTT}$$

RTT = 2 * prop. delay.

$$= 2 * \frac{d}{v}$$

(a) 10 km (LAN)

$$RTT = 2 * \frac{10 \text{ km}}{2.1 * 10^5 \text{ km/sec}}$$

$= 95.2 \ \mu\text{sec}.$

* It is useless for WAN

$$T = \frac{1 \text{ Data}}{RTT} = \frac{1000 \times 8}{95.2 \ \mu\text{sec}} = 80 \text{ mbps}.$$

(b) 5000 km : (WAN)

$$RTT = 2 * \frac{5000 \text{ km}}{2.1 \times 10^5 \text{ km/sec}}$$

$$= 95.2 \ \mu\text{sec} \times 500$$

$$T = \frac{1000 \times 8}{95.2 \ \mu\text{sec} \times 500} = \frac{80 \text{ mbps}}{500} =$$

)

$L = 1$ KB.

$= 1024 \times 8$ bits.

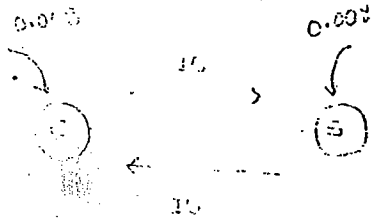
prop. time = 15 ms

$B = 10^9$ bits/sec.

$$\text{Trap. time} = \frac{L}{B} = \frac{1024 \times 8}{10^9} = 0.008 \text{ msec}$$

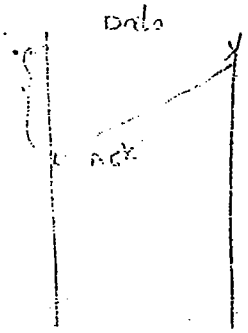
Utilisation =

(S)



(a) Data = Ack

$$U_S = \frac{0.008}{30.016} < 1\%$$



(b) Data ≠ Ack

$$U_S = \frac{0.008}{30.008} < 1\%$$

If Ack is small, then neglect it.

* From above 3 problems, we find that sender's utilisation and link utilisation is less and also it is not suitable for WAN.

* In order to resolve these problems we use "pipelining" technique.

17/07/2010
Saturday

(4)

$B = 4$ Kbps.

$R = 20$ m/sec.

prop. delay $= 2 * 20$

$RTT = 40$.

$L = 4 \times 10^3 \times 40 \times 10^{-3}$

$L = 160$ bits.

(5)

prop. delay $= 100\ \mu s$. $\Rightarrow$ $RTT = 200\ \mu sec$

$L = 1$ KB $= 1024 \times 8$ bits

$B = ?$

RTT = tran. delay

$200\ \mu sec = \frac{L}{B} = \frac{1024 \times 8}{B}$

$B = \frac{1024 \times 8}{200 \times 10^{-6}} = 40$ mbps

(6)

B = 1 mbps.

prop. delay = 1.25 sec.

L = 1KB = 1024 x 8 bits

(1) RTT = 2 x 1.25 = 2.5 sec.

(2) 1 sec — 1×10^6 bits.

2.5 sec — ?

$= 2.5 \times 10^6$ bits = W_{bits}

(3) $W_p = \frac{2.5 \times 10^6}{1024 \times 8} = 306.$

(4) Seq. num = W_p = 306

$2^K = 306$

$\therefore K = 9$ bits

(7) d = 3000 km

B = 1.536 mbps.

L = 64 x 8 bits.

prop. speed = 6 μsec/km.

prop. delay = 2 x 3000 x 6 μsec

$= 36000 \times 10^{-6}$

= 36 msec.

(1) RTT = 2 * 3000 x 6 μsec.

$= 36000 \times 10^{-6}$

= 36 msec

(2) $1 \text{ sec} \text{ —— } 1.536 \times 10^6 \text{ bits}$

$36 \text{ msec} \text{ —— } ?$

$36 \times 10^{-3} * 1.536 * 10^6 = (W_{bits})$

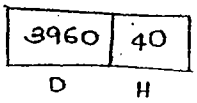
(3) $W_p = \dfrac{36 \times 10^{-3} \times 1.536 * 10^6}{64 \times 8}$

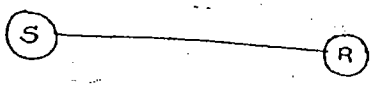
(4) Seq. num = $W_p = 10^7$

(5) $2^K = 10^7$

$K = 7$

(9)





100×3960

100×40 (H)

40 (NAK)

$3960 + 40$ (Re-trans)

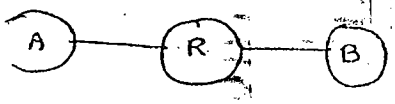
396,000

8040

$$\frac{3,96,000}{3,96,000+8040} = 98\ \%$$

$$\frac{8040}{3,96,000+8040} = 2\ \%$$

(10)



At t=0 packets are released at A and immediately they are available at R.

'0' starts leaving R.

∴ 123 are in Queue.

t t=1, 0 arrives at B, ack1 is made, meanwhile, 1 starts leaving R',

There fore 2 & 3 are in the Queue.

t=2, Ack1 arrives at R, and then at A. Therefore, 4 is released from A & immediately available at R. meanwhile, arrives at B and hence, Ack2 to '0' is made at the same time 2 starts leaving 'R' and therefore 3 & 4 are in the Queue.

Analogy at t=5 5 & 7 are in the Queue.

at t=10 11 & 12 are in the Queue.

$$T + \frac{K}{B} \quad F \quad R$$

$$W\left(T + \frac{F}{R}\right)$$

If

$$W\left(T + \frac{F}{R}\right) = 2 \times \left(T + \frac{F}{R} + \frac{D}{S}\right)$$

$$= 4000 \text{ mts}$$

(3)

Max. data rate = Throughput = $\frac{1 \text{ windoco}}{RTT}$

10pkts = $\frac{10 \times 100 \times 8 \text{ bits}}{800 \mu\text{sec}}$.

each pkt size = 100×8 bits

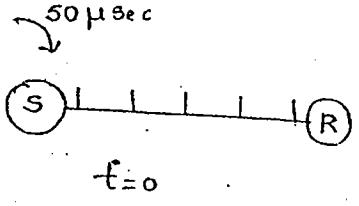
= 10 mbps.

$\eta = \frac{10}{20 \text{ mbps}} = 50\%$

(1)

Throughput = $\frac{1 \text{ windoco}}{RTT}$

= $\frac{5 \times 1000 \times 8 \text{ bits}}{400 \mu\text{sec}}$ = $\frac{5 \times 1000 \times 8}{450 \mu\text{sec}}$



= 88.68×10^6 bps.

11.11×10^6 bps.

At t=0, communication starts.

t=50μsec, first proctret is available on the link.

t=100 μsec, second packet is available.

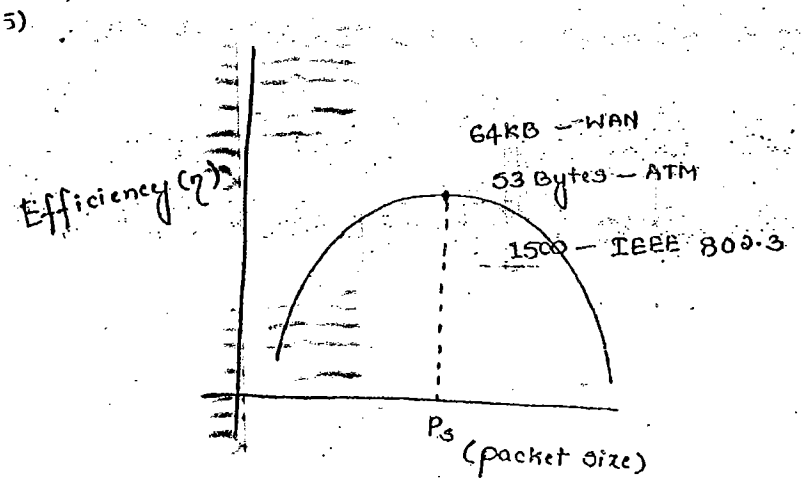
t= 250 μsec, last packet is available on the link, by that time first pkt is arrived at destination.

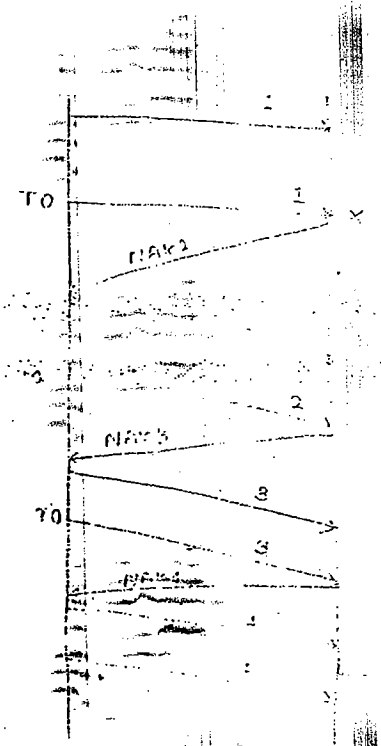
Hence, ack1 is made.

∴ At T = 450 μsec, ACK1 arrives at source, therefore, 1st packet in the second windoco starts its journey.

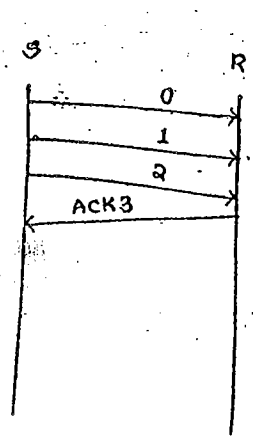
Hence, throughput = $\frac{5 \times 1000 \times 8}{450 \mu\text{sec}}$ = 88.68×10^6 bps

5)


Efficiency (η)
64KB – WAN
53 Bytes – ATM
1500 – IEEE 802.3
P_s (packet size)


T0
1
X
NAK2
2
NAK3
3
T0
3

(20)



K

0 1 2 [3] 4 5 6 7

01[2]3456 7 0

3 to 5

K to K+n-1

n → window size

K → next pkt in window.

29/07/2010

Monday

(2) minimum frame size

p.no: 37

Trans: delay = RTT

B = 1 Gbps

d = 1 km

v = 2,00,000 km/sec

$$\frac{L}{B} = 2 \times \frac{d}{V}$$

$$L = \frac{2 \times 1 \times 1}{2,00,000}$$

= 10,000 bits (or) 1250 bytes

(4) v = 2×10^8 m/sec = 2×10^5 km/sec

p.no: 39

B = 10^7 bps

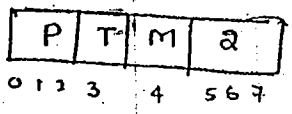
d = 2 km

$$\frac{L}{B} = 2 \times \frac{d}{V}$$

$$L = \frac{2 \times 2\,km}{2 \times 10^5\ km/sec} \times 10^7$$

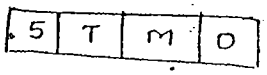
$$= 200 \text{ bits (or) } 25 \text{ bytes.}$$

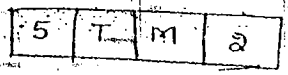
P.no:- 34 :-



In token frame;

SD, AC (Access control.





P.no:37 .

i). Ring latency

R = 4 mbps

m = 20

d = 20 × 100

b = 2.5

V = 2×10^8 m/sec.

$$RL = \frac{dR}{V} + mb$$

$$= \frac{20 \times 100 \times 4 \times 10^6}{2 \times 10^8} + 20 * 2.5 = 90 \text{ bits.}$$

for 16 mbps

$$R \cdot L = \frac{80 * 100 * 16 * 10^6}{2 \times 10^8} + 80 \times 2.5$$

$$= 840 \text{ bits}$$

m

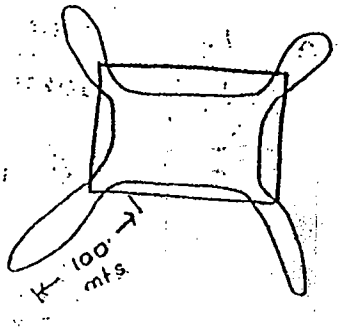
$d = m \times 200$.

$b = 8$ bits

$R = 25$ mbps

$L = 1250$ bytes.

$V = 2 \times 10^8$ m/sec



$$\frac{RL}{\text{tr.time}} = ?$$

$$\frac{t_{prop}}{t_{trans}} = \frac{RL}{\text{tr.time}} = 1.$$

$$\text{tr.time} = \frac{L}{B} = \frac{1250 * 8}{25 \times 10^6} = 400 \ \mu\text{sec}.$$

$$RL = \frac{d}{v} + \frac{mb}{R} \text{ sec} = \frac{m \times 200}{2 \times 10^8} * + \frac{m \times 8}{25 \times 10^6}$$

$$\frac{RL}{\text{tr.time}} = 3.33 \times 10^{-3} m = 1$$

$$\boxed{m = 300}.$$

To Transfer single data packet

$$1 \text{ pkt} = \frac{1250 * 8}{25 \times 10^6} \text{ sec}.$$

$$? = 1 \text{ sec}$$

$$\Rightarrow 2500 \text{ pkts/sec}.$$

(11) (a) Early token strategy

(b) Delay token strategy

$$a = \frac{L_D}{B} = \frac{1000}{10\times10^6} = 10^{-4}$$

2-stations

50 – distance

$$b = R_L = \frac{d}{V} + \frac{mb}{R} \text{ sec.}$$

$$= \frac{88\times50}{2\times10^8} + \frac{32\times2.5}{10\times10^6} = 880 * 10^{-8}$$

$$c = \frac{L_T}{B} = \frac{.24 \text{ (* assume)}}{10\times10^6}$$

d = prop. delay b/w stations

$$= \frac{\text{dist. b/w stations}}{V}$$

$$= \frac{50}{2\times10^8}$$

(a) Early = a + c + d =

(5)

P.NO:-37

B = 10 mbps

Slot time = 51.2 msec.

No. of slots = 1.716.

L = 512 x 8 bits.

$$\eta = \frac{T.P}{T.P + C.P + t_{prop}}$$

$C.P = 1.716 \times 51.2\ msec.$ $\quad T.P = \frac{L}{B} = \frac{512 \times 8}{10 \times 10^6}$

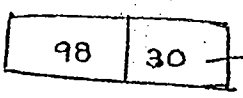
$$\eta = \frac{\frac{512 \times 8}{10^7}}{\frac{512 \times 8}{10^7} + 1.716 \times 51.2\ msec}$$

$\eta = 82\ \%$

(6)

B = 10 mbps. $\quad d = 2.5\ km. \quad v = 2.3 \times 10^8\ m/sec.$

$L = 128\ bytes. \quad = 2.3 \times 10^5\ km/sec.$



$$\eta = \frac{1}{1 + 6.440}$$

$= 57\%$ (maximum)

$$a = \frac{t_{prop}}{t_{trans}} = 0.11$$

$$t_{prop} = \frac{d}{v} = \frac{2.5\ km}{2.3 \times 10^5\ km/sec}$$

$$t_{trans} = \frac{L}{B} = \frac{128 \times 8}{}$$

For effective transmission,

$$t_{trans} = \frac{L}{B} = \frac{98 \times 8}{10 \times 10^6}$$

(or)

98	30
77%	23%

77 % of 57 % = 45 %

3) B = 10 mbps.

$t_{prop} = 225$

$$\text{Bit delay} = \frac{1}{B}$$

$$= \frac{1}{10} = 0.1 \text{ msec}.$$

Transmission can be considered as either 1 bit delay (or) 0.1 msec.

At t=0, A & B started their communication.

At $t = 225/2$, there is a collision.

At t = 225, the A & B will come to know about the collision, through back propagation.

Assume, A started producing jam signal.

∴ At t = 273 (225 + 48), A finishes producing jam signal.

⇓

Jam

(4) At $t=0$, A & B started their communication.

At $t = 12.5/2$ μsec, there is a collission

At $t = 12.5$ μsec, A & B will come to know about the collission through Back propagation.

Even though A's $K=0$, it has to wait for 1 prop. delay to get the clear link.

∴ To get the clr

∴ A starts it's communication at $t = 25$ μsec.

Trans delay for a packet $= \frac{L}{B}$

$= \frac{1000}{10 \times 10^6} = 100$ μsec.

∴ At $t = 125$ μsec, 'A' completes it's transmission.

But, A's last bit is delivered at B. at 137.5 μsec.

Because we have one more prop. delay

(1) cycle time

(a) Based on BW for cycle time, calculate no. of bits transferred in sec.

Ans:- Since, it is heavily loaded, coe suppose to use early token strategy.

(a) $C \cdot T = a + c + d$

$$a = \frac{l_D}{B} = \frac{2.56}{10 \times 10^6} = 2.56 \text{ msec.}$$

$$c = \frac{l_T}{B} = \frac{8}{10 \times 10^6} = 0.8 \text{ msec.}$$

d = prop. speed = 200 m/μsec.

1 km ⇓ 50 stations.

distance b/co 2 stations = 20 mts.

50 km

1 m = 1000 km

? = 5 km

$$= 0.1 \text{ msec.}$$

$$= 26.5 \text{ μsec.}$$

(b) 26.5 μsec ⇒ 224 bits.

$$1 \text{ sec} \Rightarrow \frac{224}{26.5 \times 10^{-6}} = 8.5 \text{ mbps.}$$

$$\eta = \frac{8.5}{10 \text{ mbps}} \times 10 = 85\%$$

(13) before regenerating the token ⇒ represents delayed.

- C.T = a + c + d + b

$$a = \frac{L_D}{B} = \frac{1024 \times 8}{100 \times 10^6} = 81.24\ \mu sec$$

$$b = RL = \frac{d}{v} + \frac{mb}{R}\ sec.$$

$$= \frac{200\ km}{2,00,000\ km} = 1\ msec$$

$$c = \frac{L_{Token}}{B} = \frac{24}{100 \times 10^6} = 0.24\ \mu sec$$

d = 0 ⇒ total no. of stations ⇒ not given

∴ C.T = 1.08 msec.

(b) 1.08 msec — 1024 × 8 bits

1 sec — ?

= 7.6 mbps.

(c) $\eta = \frac{7.6\ mbps}{100\ mbps} \times 100$

= 7.6 %.

p.no:39

(6) Delayed.

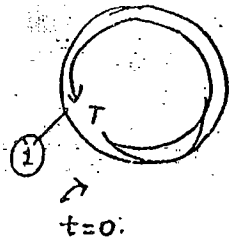
$$a = \frac{L_D}{B} = \frac{100 \times 8}{10 \times 10^6} = 80\ \mu sec$$

b = 400 msec.

$c = \frac{d_T}{B} = \frac{24}{10 \times 10^6}$

$= 2.4$ msec.

d = 400 msec



a + b + c + b

⇓

Same station (distance b/w the 1st & the dest. station is considered as RL)

c·T = 888 × 2.4 msec.

888.4 msec —— 100 × 8 bits

1 sec —— ? ⇒

$\eta = \frac{1 \text{ mbps}}{10 \text{ mbps}} \times 100 = 10\%$.

4)

prop. speed = 200 m/μsec.

① 1 mbps

② 40 mbps

Adding a station

⇓

introduce 1 bit delay.

1 bit delay $= \frac{1}{B} = \frac{1}{1 \times 10^6} = 1$ μsec.

$= 200$ m.

1 bit delay $= \frac{1}{40 \times 10^6} = 0.025$ μsec.

1 μsec —— 200 mts.

0.025 μsec —— ?

⇒ 5 mts.

(15)

B = 5 mbps.

prop. speed = 200 m/μsec

1 bit delay = $\frac{1}{5 \times 10^6}$ = 0.2 μsec

1 μsec — 200 mts.

0.2 μsec — ?

= 40 mts

03/08/2010

Tuesday

(58) Maximum data = 64KB

65,535 = | 65515 | 20 |

Data Header

(1) A:

(2) A: RTT = 30 msec.

α = 0.9

NRTT = 26

Basic algorithm ERTT = α (RRR) + (1 - α)(NRTT)

= (0.9)(30) + (0.1)(26) = 29.6 msec

T.O = 2 * 29.6 msec = 59.2 ms.

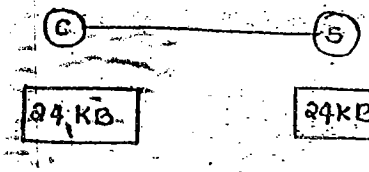
(b) D_{new} = |30 - 26| = 4

DE = 0.9 * 4 + (0.1) * 4 = 4

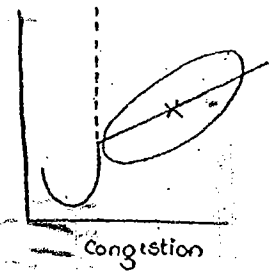
T.O = 4 * DE + ERTT

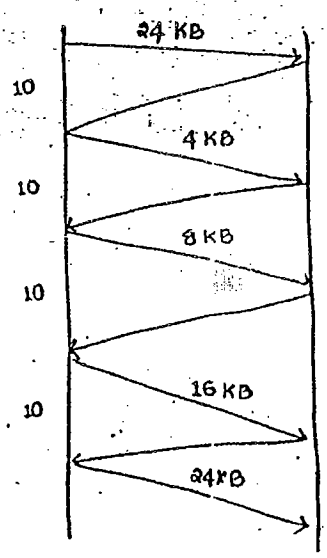
= 16 + 29.6 = 45.6 msec.

3A)

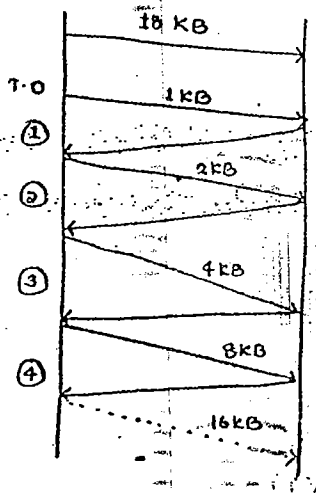


After 40ms a full window is transmitted.





A)



After timeout occurs go back to window size = 1

Ans : 16 KB

i) TCP uses SWP :

$$\therefore \text{Throughput} = \frac{1 \text{ window}}{\text{RTT}}$$

$$= \frac{65535 \times 8}{20 \text{ msec}} = 26.5 \text{ mbps}$$

$$\eta = \frac{26.5}{1 \text{ GBPS}} = 2.6\%$$

(8) 198.56.24.0 = 10100000.

198.56.25.0 =

198.56.26.0 =

198.56.27.0 =

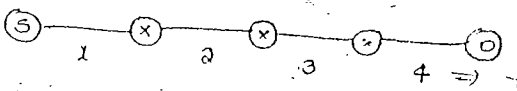
Subnetting cannot be applied for this group of address, as they bel to same network (198.56)

p.no:91

14/08/2010
Saturday

Routing algorithm

(1)



Link state algorithm => suggests about cost

(3) Decision place :

Link-state => distributed flooding => centralised

everyone can understand about it

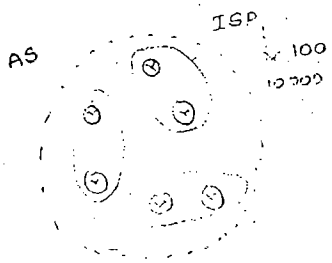
(5) Routing strategy :

Fixed => for every 1 hr.

Adaptive => 9.00 A.M → If any change occurs in nico, (either neco router is added) then calculate

(6) Checking the performance.

Highest level is called Autonomous systems.



WAN
Supernets
N/w
Subnets

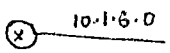
Static protocols => user need to build Routing table.

Dynamic

10:94

Periodic updates : normal (for every 30 sec, get updated with neighbours)

		hops
t = 0	10.1.1.0	0
	10.1.8.0	0



At t = 1500sec , a neco router is added called e

= 180

= 210

= 240

= 270 => 'A' can identify 'e'

But, A cannot have it's(e) address stored => 10.1.6.100.

∴ so, don't wait for time interval directly broadcast it.

Routing by Rumor:

If 'c' says, any thing, 'B' gets directly update it without checking.

verse Routing :-

Triggered :

no need to wait upto 30sec,

can be done at any triggered time

Id down Times:

10.1.5.0 => 10

t = 0

-30	1	X
-60	6	X
-90	10	

Asynchronous :

t = 0 R_1

↕ ⟶ the time slice must be

t = 5 R_2 increased. Inorder

10 R_3 to avoid collision

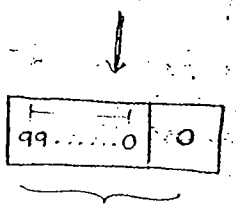
15 R_4

(6) Transport data unit

Total sequence numbers available = $2^8 = 256$ and they should be consumed in 30 sec.

∴ Data rate per connection = $\frac{128 \times 8 \times 256}{30}$

TPDU = Transport protocol data unit



How many such this packets.

(9) probability of soluting 1 random number falls in 10^6

total no = 2^{32}

$= \frac{10^6}{2^{32}}$

(11) A typist can type 600 characters for minute i.e., to type a charact. takes 100 ms.

case 1 : Since RTT is very much less than typing speed, this algorithm can be implemented.

case 2 : Since RTT is exactly equivalent to typing speed, this algorithm can be implemented.

If RTT is more than 200 ms then we able to implement this algoritha

(4) If there are more no. of matches with each entry, then select the first match.

longest match entries are placed in the first entry

Eg:- (1) 255.255.255.0 ✗

(2) 255.255.255.128 ✓ select it as 1st entry

(3) 255.255.31.0 ⇒ class 'B' address.

200.96.86.0 = 11001000.01100000.01010110.00000000

200.96.87.0 = 01010111

200.96.88.0 = 01011000

200.96.89.0 = 01011001

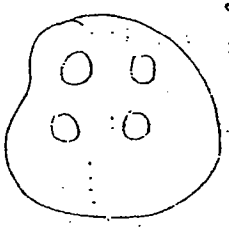
8 8 4 4 8

255.255.240.0

(1) 200.96.86/20 — 24 − 20 = 4

(2) 200.96.86 — $2^4 = 16$

255.255.240.0



200.96.86.0 ....

16

Q: 200.200.10/22 which is not part of it.

(1) 100.100.11.100

(2) 200.200.15.100 ✗

(3) 200.200.10.209

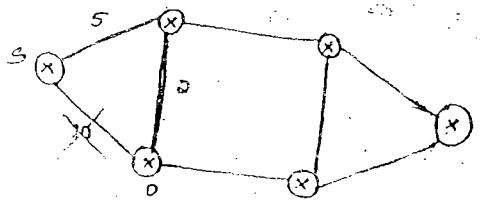
(4) 200.200.12.30.1

24 − 22 = 2

$2^2 = 4$

10
11
12
13

Distance vector algorithm doesn't have the "cost" mentioned for the route. only state link algorithm have it



At a particular time interval, 'B' cannot have any info. from 'c', and this that it is in Holddocon period. So, it starts timer:

If At t=0

Timeout ⟸ t=180 not received then, make it as = ∞

Flushout ⟸ t=270 not received then, permanently discard it

IP ⇒ In TCP/IP network

IPX ⇒ In novell networks, we call IP addresses as IPX)

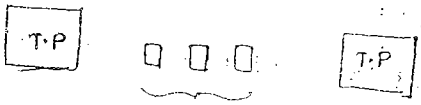
(48 bits) like ARPANET.

CCNS ⇒

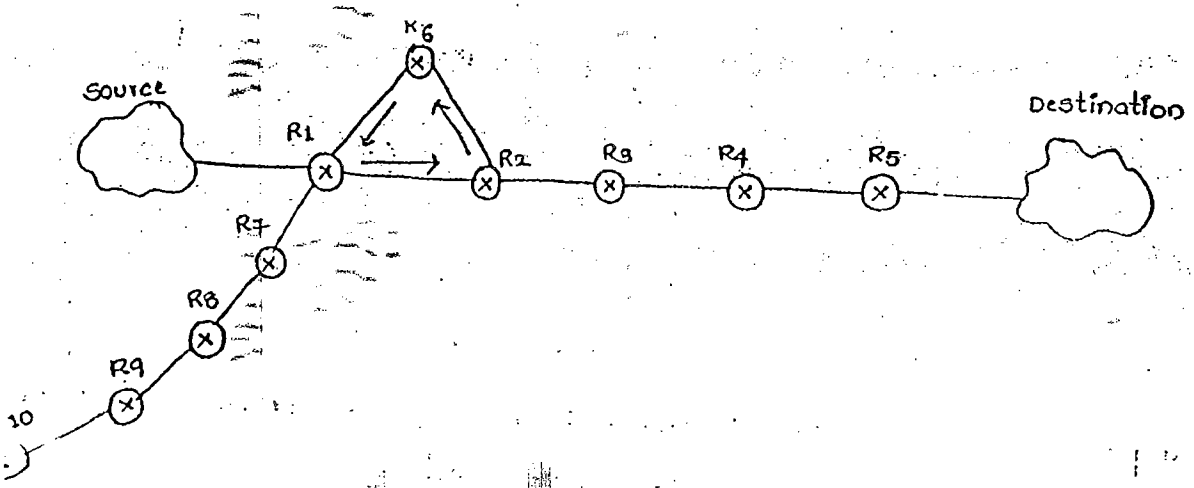
RIP is proprietary protocol of Sun Microsystems.

Intellectual property ⇒ patent (rights).

no: 39



$$\frac{1000 \text{ bytes}}{10 \times 10^6} = T.P$$



Every router maintains it's own routing table, as source sends the packet to a particular destination address. First, the pkt reaches router 'R_1', but it won't contain the dest. address, so to know next router, pkt is sent to all available paths which is drawback of transfering pkt to all routers in network. So, it is the best one, which maintain a Defaute route in last row of particular routing table.

Suppose that 'R_1' route table has 'R_2' (or) 'R_7' as default routes. Assume that 'R_2' is destined address, but given default route as 'R_7', then data is lost (i.e., not reach destination).

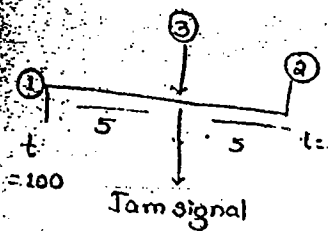
Suppose that, 'R_1' default route is 'R_2' and 'R_2's default route is 'R_6' and 'R_6''s default route is 'R_1'. Then, a loop is formed unnecessarily packet moves through loop. To avoid this loops. Fix TTL, based on path delay subtract it with TTL, if TTL = 0 ; simply discard the pkt.

Since, "default routing" can't satisfy to reach the destination, a concept called "Dynamic routing" ⇒ i.e., "After completion of R_7 router as default, drop the packet at that side and again send the pkt to R_2, so can find the destination.

General case, source sent 8 pkts to dest., it send 3 pkts to R_7, 5 to R_1, again R_1 send 3 pkts to R_6 & remaining to R_2. So, out of 8, 6 pkts are wasted & 2 reached dest., Dest address sends the ack. to source with the same path it reached.

⇓

to send remaining 6 pkts



3rd system informs (1) & (2) channels, a jam occured, they collide at '5' units distance away. Again Jam signal takes '5' units of time to inform (1) & (2) at that time (1) & (2) sends remaining bits.

for system '2', requires 10 units of time but at that time (2) comm. is completed, and it thinks that it is not for it, and can't send collided info- so, loss of info. occurs.

min. bits of (1) & (2) = 20 for successfully knowing (collission).

1 ms (1 millisecond) = 10^{-3} sec
1 µs (1 microsecond) = 10^{-6} sec
1 ns (1 nano second) = 10^{-9} sec

1 ks (1 kilosecond) = 10^{3} sec.
1 Ms (1 megasecond) = 10^{6} sec.
1 Gs (1 Gigasecond) = 10^{9} sec.

bit → bps
Byte → Bps

name	symbol	bit per second	bit per second formula
bit per second	bit/s	1	1
byte per second	B/s	8	8
kilobit per second	kbit/s	1000	10^3
megabit per second	mbit/s	1,000,000	10^6
gigabit per second	Gbit/s	1,000,000,000	10^9
terabit per second	tbit/s	1,000,000,000,000	10^{12}

kbps
Mbps / mbps
Gbps / Gbps
tbps

is a unit of data transfer rate or bandwidth or bit rate or throughput

EtherReal.

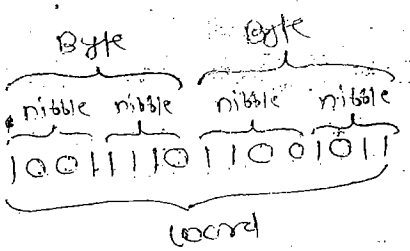
TCP Dump

1 bit = 0 or 1

4 bits = nibble

8 bits = byte

16 bits = word



1024 bytes = 1 KB (1 kilobyte) = 2^{10} bytes

1024 KB = 1 MB (1 megabyte) = 1024 KB = $2^{10} \times 1$ KB
$= 2^{10} \times 2^{10}$ bytes
$= 2^{20}$ bytes

1024 MB = 1 GB (1 Gigabyte) = 1024 MB = $2^{10} \times 1$ MB
$= 2^{10} \times 1024$ KB
$= 2^{10} \times 2^{10} \times 1$ KB
$= 2^{10} \times 2^{10} \times 1024$ bytes
$= 2^{10} \times 2^{10} \times 2^{10}$ bytes
$= 2^{30}$ bytes

1024 GB = 1 TB (1 Terabyte)
$= 2^{40}$ bytes

1024 TB = 1 PB (1 penta byte)
$= 2^{50}$ bytes

1 KB = 1024 bytes = 1024 × 1 bytes = 1024 × 8 bits
$= 2^{10} \times 2^3$ bits $= 2^{13}$ bits

1 KB	$= 2^{10}$ bytes $= 2^{10} \times 1$ byte	$= 2^{10} \times 2^3$ bits	$= 2^{13}$ bits = 1 Kbits
1 MB	$= 2^{20}$ bytes $= 2^{20} \times 1$ byte	$= 2^{20} \times 2^3$ bits	$= 2^{23}$ bits = 1 Mbits
1 GB	$= 2^{30}$ bytes $= 2^{30} \times 1$ byte	$= 2^{30} \times 2^3$ bits	$= 2^{33}$ bits = 1 Gbits
1 TB	$= 2^{40}$ bytes $= 2^{40} \times 1$ byte	$= 2^{40} \times 2^3$ bits	$= 2^{43}$ bits = 1 Tbits
1 PB	$= 2^{50}$ bytes $= 2^{50} \times 1$ byte	$= 2^{50} \times 2^3$ bits	$= 2^{53}$ bits = 1 Pbits