Problems associated with Computer Network:

* communication
* identification
* connection.



1.communication: Protocol is a language of computers needed for communication of the computers.

some of the protocols are:

HTTP : web browsers
SMTP : Mail computation
FTP : File communication
NTP : Network time protocol
SNMP.



* Location of the protocol is NOS (Network operating system)

Network time protocol:

Transactions are done by storing source time slot and converting to the destination time solt and mailing to the user.

Indian time ——Mail——> U.S.A Time.

Network Management protocol:

DOS + All protocols = window NT

HTTP
SMTP
FTP
NTP
SNMP
→ versions of Protocols

HTTP: (Hyper text transfer protocol): Browser requesting for a web page

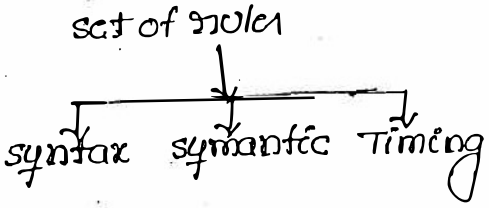
HTTP: 1.0, 1.1, 2.0 (Application protocols).

* RFC : Request for Comments => Standard for computer networks.

* concept of computer n/w have an RFC number

RFC1
RFC2
:
RFC 793 -> TCP/IP.
RFC 3700

**Protocol:** A set of rules and regulation or conventions

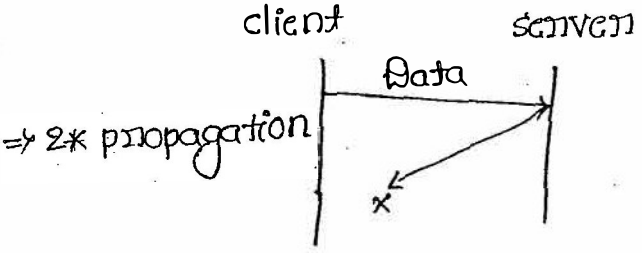



* Rules and regulations must be crystal cleared i.e there must any duplicates and any invalid syntax is not acceptable.

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

* syntax -> send acknowledge

* semantic -> Receive acknowledge.




* RTT is measure of delay b/w 2 hosts

* Minimum acknowledge waiting time = 2 * propagation (RTT)

* Maximum ack. waiting time = 2 * (Min. ack. waiting time)
= 2 * (2 * propagation).
= 2 * RTT.

Round Trip Time -> RTT  Turn over time -> Time out (to)

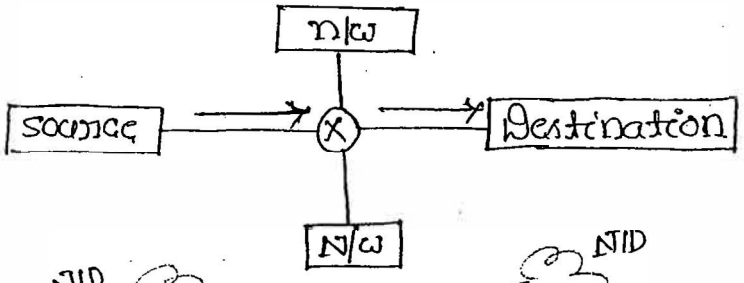
* Protocol is an agreement between the communicating parties on communication is to proceed.

* IP address doesnot refer to a host actually, it really refers to interface, if a host is on two networks, it must have two IP.
* A system may have multiple ip addresses and multiple physical addresses.

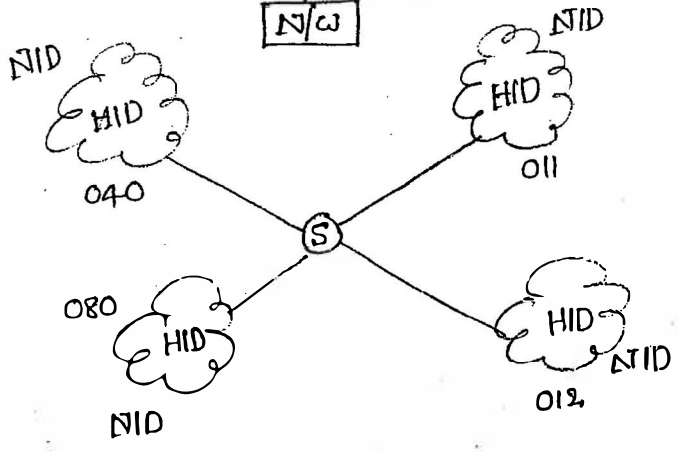
## 2. Identification:

To send a packet from source to destination we have the identification steps:

* identify the network → logical
* identify the host within the network. i.e among all the destinations, one system is identified ← Physical
* identify the process within the host → service point




Eg:




040 4752469
3 7

02145 39764
5 5

078914 0823
6 4

* Each num is 10 digits
* Two paths.
* Each num is unique
* Hidden meaning.

=

1. 32-bit number □ □ □ □
   8 8 8 8
2. Two paths → NID
   → HID.

3. HID must be unique.

4. Hidden meaning.

## Classification of IP Addresses:

To covers the needs of diff types of organizations IP addresses are divideded into Five classes.

### class A:

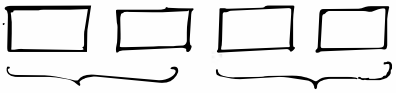
| NID | HID |
|---|---|
| 8 | 24 |
| $2^8$ N/w | $2^{24}$ hosts/NW |
| 256 | = 1.6 cr hosts/n/w. |

* Govt. org uses this network, eg: Defense n/w

eg: APSWAN Andhra pradesh state wide Area 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 |
| 65,536 | 65,536 |

eg: Big organizations, MNC, Banks.

### class C:

| NID | HID |
|---|---|
| 24 | 8 |
| $2^{24}$ | $2^8$ |
| = 1.6 cr | 256 |

eg: Engineering colleges.
Medium org's

NOTE:

class A : 1–126

class B : 128–191

class C : 192–223

class D : 224–239

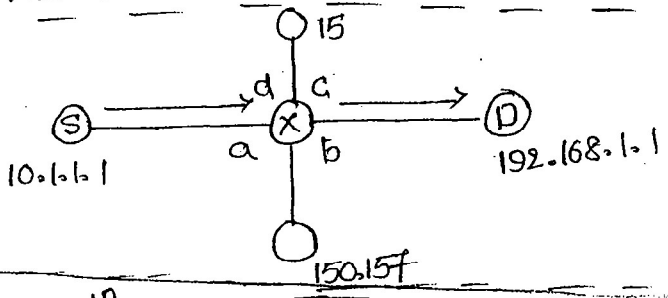
class E : 240–255

* 127 is a special IP address.

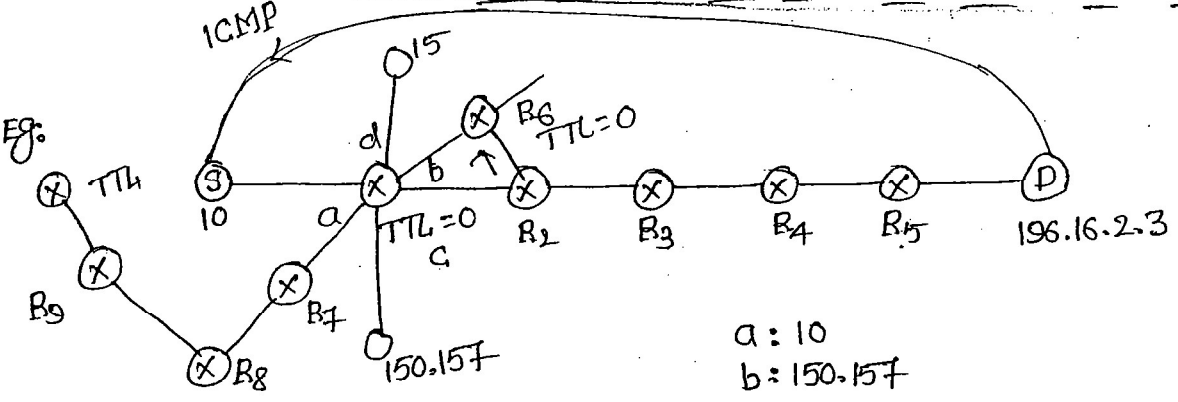
Eg: 150.167.1.1 — NID / HID — class B

192.168.1.1 — NID / HID — class C

} used in routing process




a 10.1.1.1
b 150.157
c 15
d 192.168.1.1




a : 10
b : 150.157
c : $R_2$
d : 15
$R_2$ : default

* consider default route (make dynamic route to avoid the wrong route through $R_7$ to $R_9$)

* Make TTL = 0

eg: TTL = 3 min = 180 sec.

NOTE: TTL is used for to avoid the infinite loop.

Routing

source — Router

class A:

0 reserved

00000000 → X
00000001 – 1
00000010 – 2
⋮
01111110 – 126
01111111 – 127 → X

NOTE: But "0" and 127 are reserved for special purpose,

∴ 10.0.0.0
10.255.255.255 } Not used

| | |
|---|---|
| $2^8$ N/w | $2^{24}$ hosts/N/w |
| $2^7 - 2$ N/w | $2^{24} - 2$ hosts/N/w |

class B:

NID HID

10 reserved

10000000 – 128
10000001 – 129
⋮
10111111 → 191

$2^{16}$ N/w → $2^{14}$ N/w

$2^{16}$ hosts/N/w → $2^{16} - 2$ hosts/N/w.

class C:

NID HID

110 reserved.

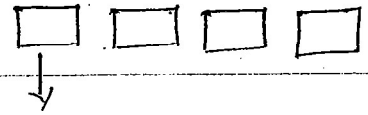
11000000 – 192
⋮
11011111 – 232.

$2^{24}$ N/w → $2^{21}$ N/w

$2^8$ hosts/N/w. → $2^8 - 2$ hosts/N/w

class D: it is designed for multicasting there is no NID or HID.

* The whole address is used for multicasting.



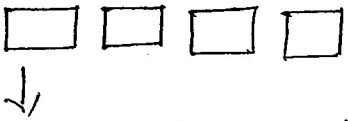
1110 → reserved.

1110 0000 – 224

:

1110 1111 – 239

**Class E:** it is reserved for internet for special use.



1111 → Reserved => 1111 0000 – 240

:

1111 1111 – 255

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

+

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

+

C: $(2^{21}) * 2^{8}-2$ = 4 billion IP Address.

* $IP_4$ → 32-bit addressing system
* $IP_6$ → 128 Bit " "

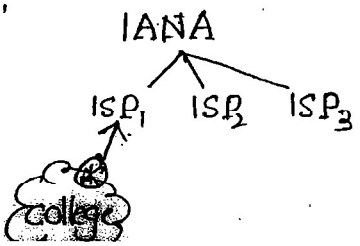
* windows 7 supports $IP_6$
* Linux 10.6 also supports $IP_6$.

**IANA:** Internet Assigned Numben Authority

→ it is used to assign the unique IP address for sys.

**ISP:** Internet service provider.

$ISP_1$
$ISP_2$
$ISP_3$
:



* A user can ~~not~~ contact directly to IANA for address but it is time consuming so a mediator known as ISP handles the connection IANA and Provides IP address. Eg.

**IANA (or) ICANN:** Internet corporation for Assigned Names and Numbers.

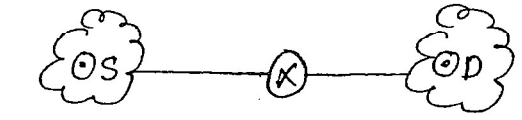
**Spoofing:** using IP address of others by unauthorized users.

NOTE: *

## Types of communication:

* unicast → one to one
* Multicast → one-to many
* Broadcast → one-to-all
* Anycast → one to one and one to all.

**unicast:**




| D | 192.168.1.1 | 10.1.1.1 |
|---|---|---|

Eg: Mail application (browsing webpages).

**Broadcast:**

→ Directed Broadcast
→ Limited Broadcast.

* sending packets to all systems in same n/w → Directed BC
* sending the packets to other sys in our own n/w → Limited BC

**Multicast:**

* it is created for class D.
* All the IP addresses are stored in a group.
* For class D, i,c for group communication IGMP is used instead of IP.

Eg: sending group mail

yahoo.mail

Group IPaddress

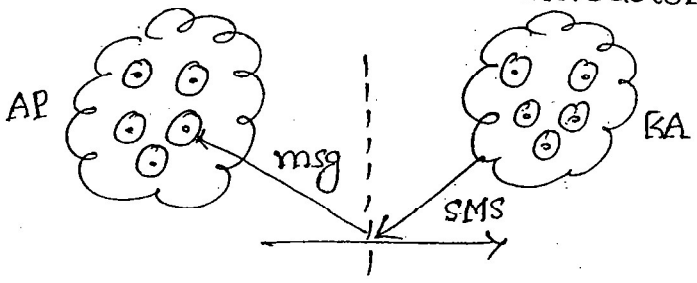
| |
|---|
| 10.1.1.1 |
| 10.1.1.2 |
| 150.157.1.107 |
| 200.200.200.1 |

| 192.168.1.1 | 224.8.10.10 |
|---|---|
| ↓ | ↓ |
| source | Destination. |

NOTE: * Majority of communication present in multicasting.

**Anycast:**

* it is used in mobile host communication.




* in multicasting 28 bit are available for identifying group. so million groups can exist at the same time.

* Two types of group addresses are supported for multicasting

  -> permanent

  -> Temporary.

Eg: For any cast : Laptop.

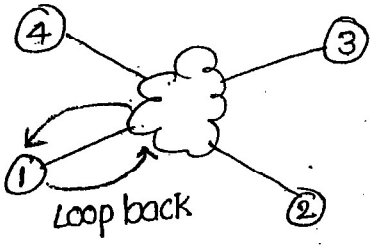
* The nearest access agent takes care of communication of particular mobile.

* so it has 1:1 and 1:all communication.

## => 127 Special IP Address:

* 127 IP address is used for connectivity purpose.

PING: Packet internet group.




| 192.168.1.1 | 192.168.1.1 |
|---|---|

↓↓

127.1.1.1

* Address can be used source and destinations are same.
* in command prompt type: c:|192.168.1.2 to ping system 2, to system 1.
* if a system sends the request i.e ping to other then if there from other than it is called "requested timeout".

→ positive message
→ Requested timed out
→ Destination unreachable.

### Characteristics:

* it is called as loop back address because packet is delivered the source and again received by the source.
* its first octet should be 127 but no restriction on other

eg: 127.0.1.1
127.50.255.255

* it never falls under any classification
* it is also used for interprocess communication (IPC).
* "localhost" is a URL to 127.1.1.1 address. if source & dest. have similar address → not valid.
* self checking instead we use '127' address.

## Limitations of logical addressing sys:

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

### See solutions:

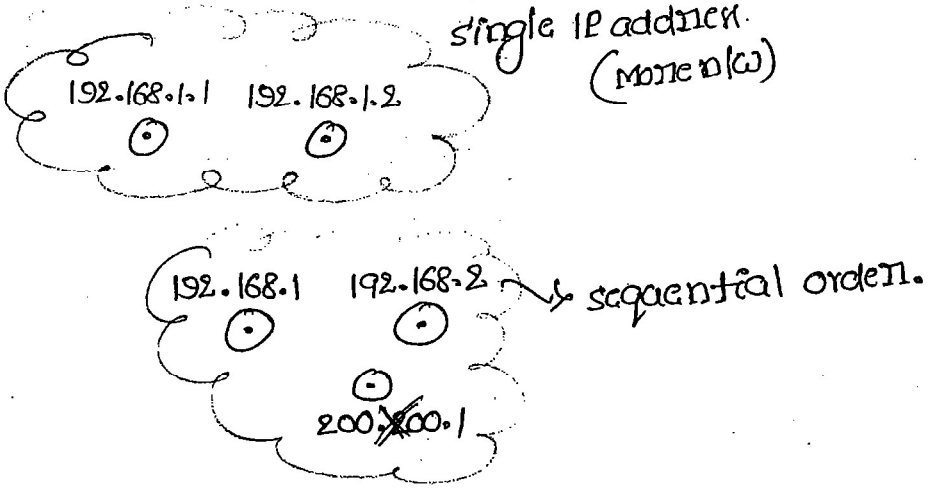
1. Supernetting
2. Subnetting
3. Physical Addressing system.

### Supernet:

The process of aggregating two or more networks to generate the IP address for the group is known as "Supernet"

### Limitations:

* 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 order.




### Advantages:

* it improves flexibility of IP allotments.
* it reduces no.of routing table entries.
* it is used to improve security.

## Subnet:

* Network is partitioned into small subnets and are connected connector called "Bridge".
* processing of dividing a single network into multiple subnet is subnetting.
* Filtering and forwarding approach.

### Advantages:

* it improves security.
* Maintainance and administration are simple
* Restructuring of the n/w is simple.
* systems within the same subnet can communicate without any bridge.
* if a system within one subnet needs to communicate with other subnet then it must pass through the "Bridge".

NOTE * The processing of borrowing bits from host ID to generate subnet ID's is known as "subnet".

* no. of bits borrowed is depends on our requirements.

Eg: To have 3 subnets in class c n/w, we suppose borrow 2-bits.

∴ No. of subnets possible $= 2^2 = 4$

∴ no. of systems per subnet $= 2^6 - 2$

Eg: class B n/w. we have 100 subnets, we need 7-bits from HID

no. of subnets $= 2^7$

No. of hosts per subnet $= 2^9 - 2$.

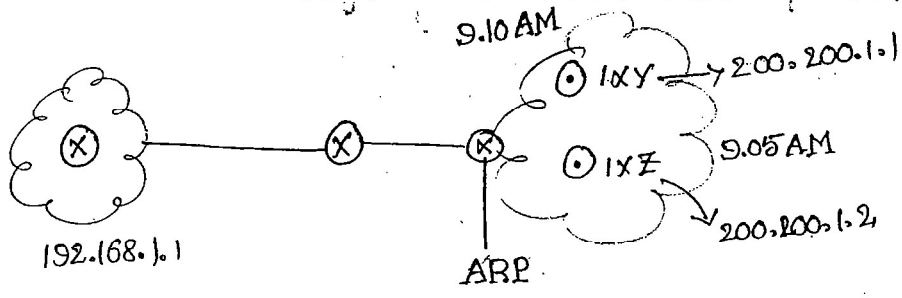
## Limitations:

* it complicates communication process. (4 step process)
* we will loose IP address during this process.

Step procedure:

→ identify the network
→ identify the subnet network
→ identify the host id.
→ identify the process.

## Physical Addressing system:




| 192.168.1.1 | 200.200.1.1 |
|---|---|

9.00 AM

* if a system having IP = 192.168.1.1 sends data to other systems 200.200.1.1 at 9.00AM. Meanwhile if the destination system changed its IP, then data is sent other systems.
* In order not to have data misusage, a physical addressing system maintains the IP addresses of changed systems and provides the data to it.

200.200.1.1 => logical => different

1XY => physical => unique (IMEA)

* By using one IP address a hacker easily attack the sys 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 system within the LAN are safe.

Logical: 32-bit - Network layer - IP - s/w → not permenant

Physical: 48-bit - Datalink layer - ARP → H/w → permanent

service point: 16-bit → Transport → TCP/UDP - s/w → fixed.

## Service point Addressing sys:

* it is 16-bit addressing system

so $2^{16}$

0 } well known port number (RFC)
1024 }
49,000 } Assigned port number (Nos)
64,000 } Dynamic port number (Application)

FTP : 20
SMTP : 45
HTTP : 80.

# various types of objects in computer networking:

* workstations and servers (7 layers)
  - L1 * Hub - 1 (physical layer)
  - L2 * switch - 2 [physical, Data link layer]
  - L2 * Bridge - 2 (PL, DLL)
  - L3 * Router - 3 (PL, DLL, NL)
  - * Brouter - 3 (PL, DLL, NL)
  - * Gateway - 7.

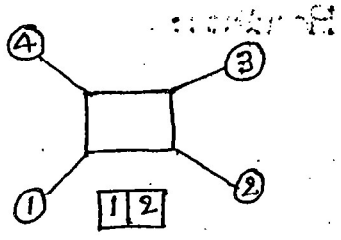
## 1. work stations and servers:

* A particular OS server acts as the domain key and all the client systems acts as workstations.
* The server maintain some Access control list (ACL) which represents the accessibility of programs by the client.
* The unaccesible programs are denied by server.
* Servers may have several applications.

  Eg: OS server, DB server.

## 2. HUB:

* it is used to connect multiple workstations and servers.
* it is a passive device, no s/w associated with this.
* it is a broadcasting device.




### Advantages:

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

### Disadvantages:

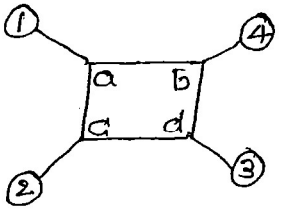
* Network traffic is high.
* causing unnecessary disturbance at various systems.

## 3. Switch:

* combination of a hub and bridge
* used to connect multiple workstations.
* it maintains a look-up table to keep track all the systems.

### Advantages:

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



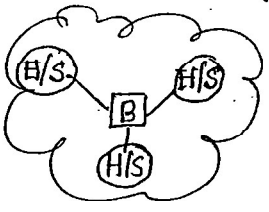

| | |
|---|---|
| a | 1 |
| b | 2 |
| c | 3 |
| d | 4 |

### DisAdv:

cost of switches is 2 to 3 times of the hub.

## 4. Bridge: (PL, DLL)

* A bridge can be used to connect multiple LAN's (similar) or multiple subnets.
* it's design criteria is filtering and forwarding.
* it's operation principal is based on physical addressing sys.
* it also maintain lookop table.




H/S => Hub/ switch.

### Routers:

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

* it requires a lot of configuration where as bridge and switch are.
* All routing algorithms are running in a router. so the cost of a router is very high.

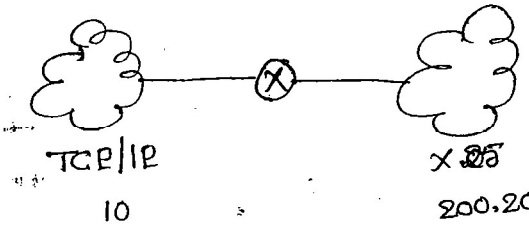
stems.

## 6. Brouters:

* Brouters are devices that combine the functions of both Bridges and routers.
* They operate at both the data link and n/w layers.
* it is combinations of Router and Bridge.

## 7. Gateway:

* it is used to connect 2 or more different dissimilar n/w




* A gateway is a protocol converter.
* A gateway can be
  - → stand alone computer with special s/w and several NIC's
  - → software installed in a router.
  - → A front end processor (FEP) in a mainframe.

=

Appl$^n$ layer Gateway = Router

Network layer Gateway = Gateway.

functionality

Mandatory
- * Error control
- * Flow control
- * segmentation.

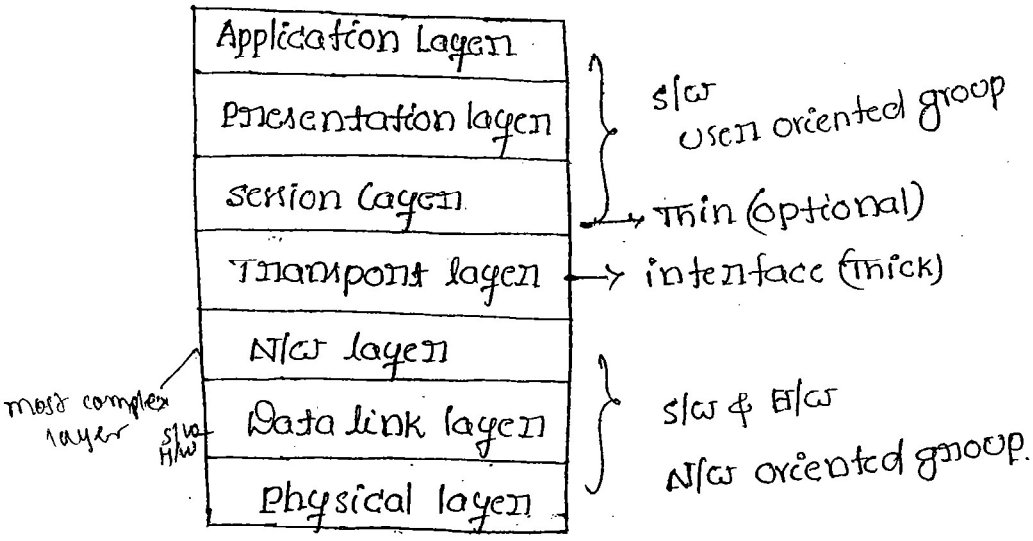
optional
- * compression
- * Encryption
- * Encoding
- * Routers.

Total => 70 functionalities

Reference model:-
- * OSI
- * TCP/IP
- * FR
- * ISDN
- * ATM - WAN/LAN
- * IEEE
- * X.25

WAN
LAN

To access all these functionalities reference model OSI



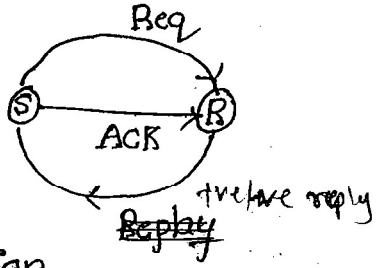

OSI reference model divide the 70 functionalities into 7 individual groups.

## connection-oriented & connectionless communication:

Connection-Oriented:

Three-way-handshake

1. connection establish
2. Transfer
3. Terminate connection



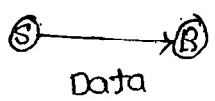
* Reliability is high

if accept => +ve reply

otherwise "-ve"

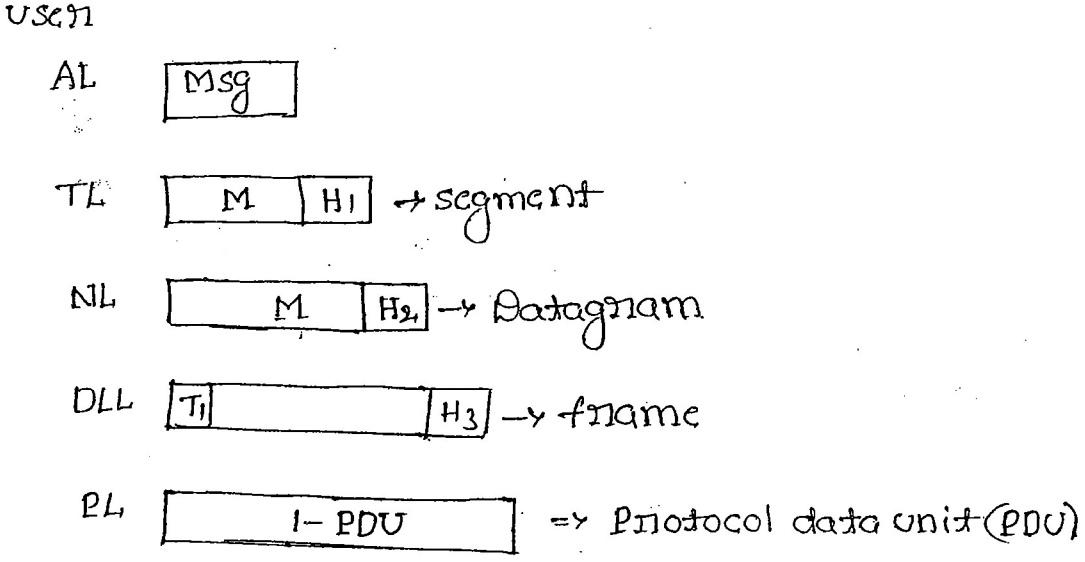
* Protocol is TCP (Transmission control protocol).

connection-less:




Directly send the data without ack

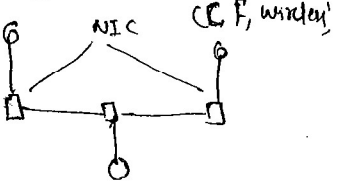
∴ UDP (User Datagram protocol)




## 1. Physical Layer:

*1. it defines electrical, mechanical, functional and procedural specifications of interface and media are providing for sending a bit stream on a computer network.

* interface is through NIC Network interface card.

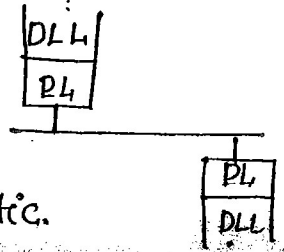



### Representation of bits:

C: Electrical (Copper wire)

F: Light signal (Fiber optic)

wireless electromagnetic.




Physical layer converts the digital to electrical and vice versa.

2. it defines transmission mode.

→ simplex => Keyboard cable

→ Halfduplex => one can talk at a time simultaneously (walky-talky)

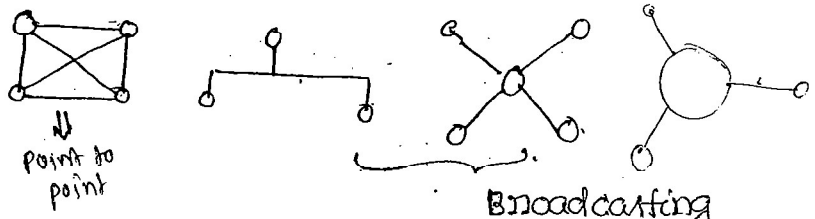
→ Full-duplex => Both can talk simultaneously.

NOTE: session layer decides either half duplex or full duplex connection (Upper layer protocol)

3) it defines link configuration

* point-to-point link (A dedicated channel for one source)

* Broadcasting link (A single channel for all sources)




* it defines topology configuration.

→ it maintains fixed rules.

## 2. Data link Layer:

* DLL transmits frames of data from computer to computer.

* Responsibility

→ Error control

→ Flow control

→ Access control

→ framing

→ physical addressing system 48 bit

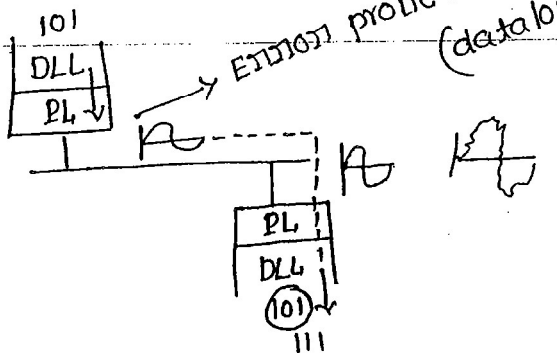
MAC

Ethernet

LAN

NIC

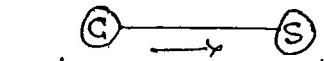
## 1. Error control:




* if there are errors in the transmision of bits as signals then a chance of distoned signals and bit representation is changed.
* so the destination of the DLL must verify these functionalities
  - → Error Detection
  - → Error correction
  - → Re-transmission (sending -ve ack to sender ther sending again).

## 2. Flow control:

→ A fast sender and slow receiver is leading to flow problems.
→ It is used only in connection oriented.



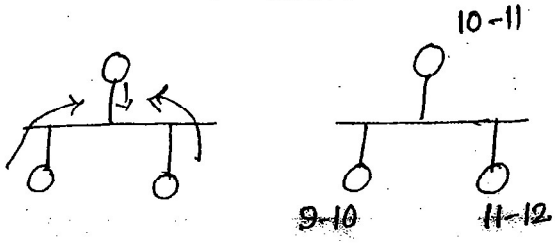

* Based on the server capability client sends the data.

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

* stop & wait
* Go-back N.
* Select-Reject.

## 3. Access control:

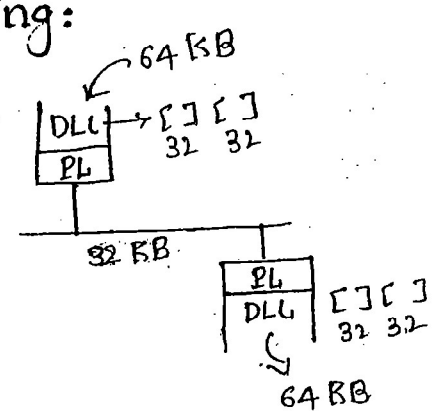
* Time slot mechanism is allotted to all the stations since lot of collission occurs.



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

* User can generate any sized data.

## Framing:




* Framing – LAN
* Segmentation – WAN

* The link capacity is 32-bits,
* PL convers any sized PKTs into 64 KB.

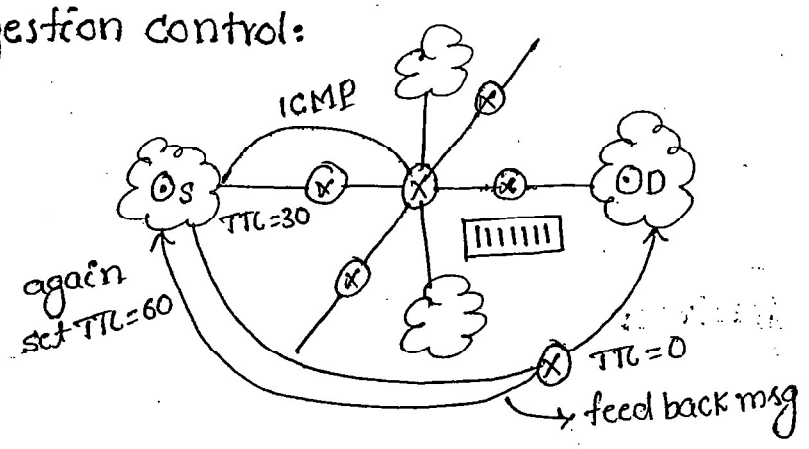
## 3. Network layer:

Responsibilities:-

* Logical addressing system
* congestion control
* Routing
* Feedback message => PING

ICMP => Internet congestion Message protocol

### congestion control:



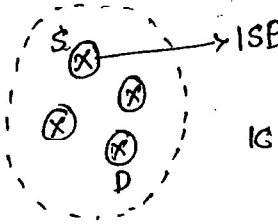

* if the data is full in all the buffers of the routers, then it is as congestion.
* To control congestion, routers sends the messages to the source to stop transmission of packets by knowing

it's IP address, rather than to all the adjacent routes.



Feedback message:

* The receiver sends ICMP to the source.




ICMP (it's not exact path, if source given shorter IP address, then it reject it's higher IP)

* Logical address system is temporary.
* Physical address system is permanent.

4. Transport Layer:

Responsibilities:-

* Application identification
* client-side-entity identification
* segmentation and Re-assembly.
* Multiplexing & De-multiplexing
* service-point addressing system.
* Error control.
* Transmission error detection.
* Flow control.

* TL offers end-to-end communication between end devices through a network.

* 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 verification are done by 2 aspects

→ Link level (DataLinkLayer)

→ End-to-end (Transport layer)

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

| Data | checksum |
|---|---|

* CRC => check link errors => DLL.
* checksum => check nlw errors => Transport layer.
* Logical address of the pkt : permanent
* physical address of the pkt : Temporary.

=> source and destination generates CRC code and checks, if correct send ack to source, if ack received by source the packet is remove.

* if a problem occurs in Transport layer of receiver, then it sends the -ve ack, to the sender. then retransmit.



## 5. Session Layer:

* This session layer allows applications, functioning, on devices to establish, manage, and terminate a dialog through a network.

Responsibilities :-

→ virtual connection b/w application entities

→ synchronization of data flow

→ creation of dialog units

→ connection parameter negotiations

→ partitioning of services into functional groups.

→ ack of data received during a session.

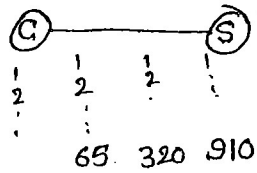
→ Maintaining checkpoints / synchronization points

→ Grooping of operations.

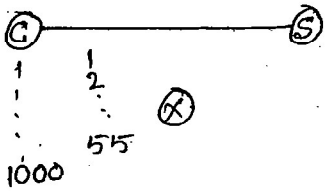
→ Token ~~passing~~

checkpoint maintainance:

Eg: Downloading files.




DAP supports checkpoints




*when a file is being downloading, then if connection is discarded in the download, then the user have to start from the first.

* in order to overcome this problem checkpoints, are introduced which specifies, up to completed file and continues at the same point when download again.

## 6. presentation Layer:

* The presentation layer is responsible for how application formats the data to be sent out on the network.

Responsibilities:-

→ Encryption and decryption of msg for security.

→ compression and expansion

→ Graphics formating

→ content translation

→ system specific translation.

## 7. Application Layer:

An interface for the end user operating a device connected to a network.

Maintaining harmony among protocol:

→ 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 a/c details, http protocol is used and for transaction http is used

↓

Security

→ User interface design
→ for file transfers
→ Electronic mail :
→ Electronic messaging
→ Browsing the www.

Maintaining harmony:
Information flow from one protocol to another (eg. HTTP to SMTP & back)
Understanding what scenario (HTTP & HTTPS back etc. must be maintained)
roles & responsibilities of application layer

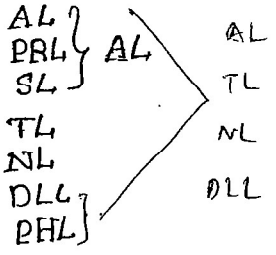
| | | |
|---|---|---|
| Application | DNS, FTP, TFTP, BOOTP SNMP, SMTP, telnet, FINGER | Gateway. |
| Presentation | HTTP, SMTP, SNMP | Gateway, Redirector |
| Session | RPC, Pipes, ASP | Gateway. |
| Transport | TCP, UDP | Gateway, Brouter. |
| Network | IP, IGMP, ICMP | Brouter, Router |
| Datalink | LLC, MAC | Bridge, Switch |
| Presentation | IEEE 802, IEEE 802.2, ISDN | Repeater, Hubs, Multiplexer, Amplifier. |

## Advantages of Layering systems:

* it uses divide-and-conquer principle. Therefore maintaince and administration is simple.
* it uses Object-oriented principles like Abstraction & encapsulation.
  ∴ Security is high, extensibility is simpler.
* Abstraction ⇒ hiding the elements.
* independently, the layers are changed without impact on others.

## Dis Adv:

* interdependency among layering systems ⇒ TCP/IP
  ⇓ ⇓
  TL NL
* Duplication of functionality.

| OSI - Reference | TCP/IP. |
|---|---|
| → 7 (seven) layers | → 5 layers   |
| → No definition for multicasting | → it is clearly defined in TCP/IP |
| → standards are ideal | → standards are practical. |
| → No flexibility | → Lot of flexibility. |
| (Max. size of Pkt = 64KB only) | (depends on characteristic of each layer.) |

OSI's focus only on n/w where TCP/IP defines packets on

# Sliding Window Protocol:

## Characteristics:

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

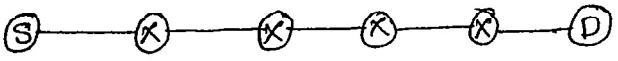
## Different types of Delays:

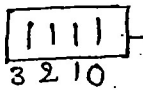
* Queing delay
* processing delay
* Transmission delay
* propagation delay.

* The amount of time taken by the process to be in queue before entering into the router.

## Queing delay:

The amount time packet is waiting in queue before being taken up for processing is known as "Queing delay"




-> Buffer, if buffer size = 4 then 5th pkt is discarded.

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

## Processing delay:

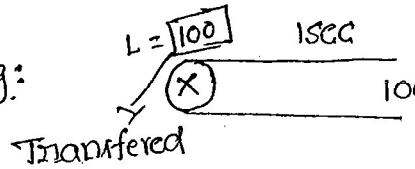
The amount of time taken by router to process a pkt [looking at destination IP, extracting nlw ID, searching in the routing table, identifying destination route] is known as "processing delay".

* it depends on router processing speed. but not size of the pkts.

## * Transmission Delay: ($L/B$)

The amount of the time taken by the router to transfer the packets to outgoing link is known as the "Transmission delay".

Eg:

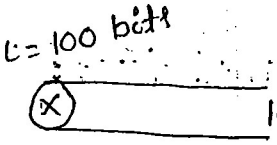



$\therefore L/B = \frac{100}{100} = 1$ sec for sending 100 bits.

**Transmission delay = $L/B$**

L = length of the packet
B: capacity of the channel or Bandwidth of the link

Eg:




$\Rightarrow L/B = \frac{100}{10} = 10$ sec for sending 100 bits.

## Propagation Delay:

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

**Propagation delay = $d/V$**

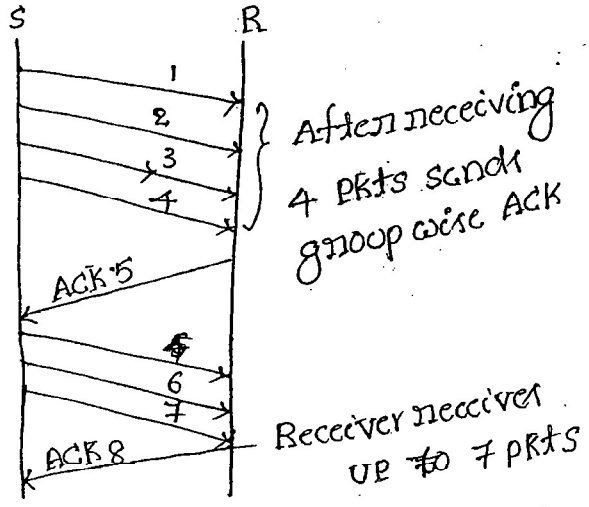
d = distance b/w routers
V = velocity of ~~routers~~

RTT = 2 * [propagation delay + N (queuing delay + transmission delay + processing delay)]

Time out = 2 * RTT.

TTL = 2 * Timeout

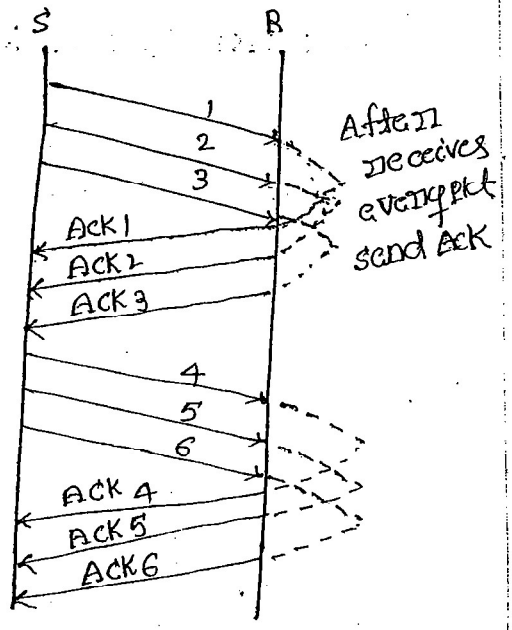
Cumulative:




=> Network traffic is low

=> Reliability is low.

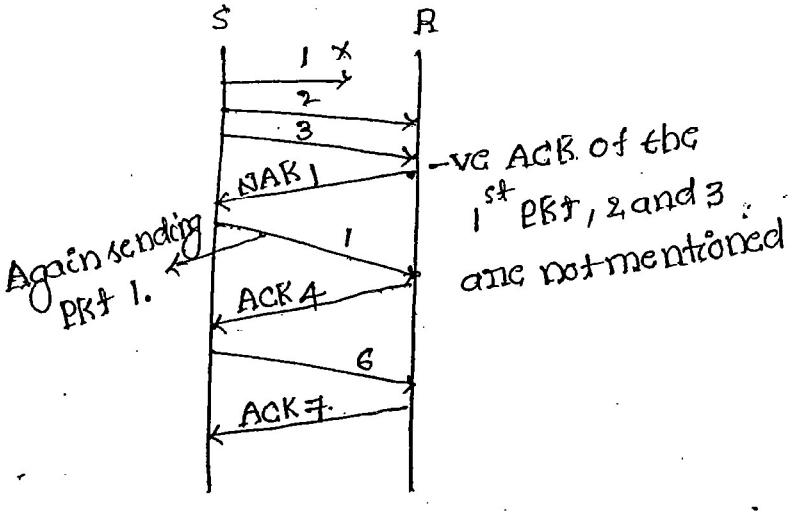
Independent:

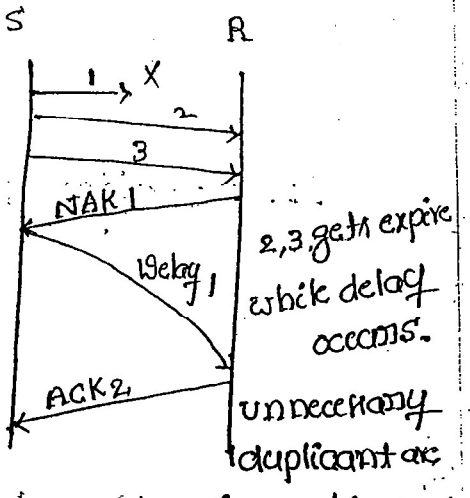



=> Network traffic high

=> Reliability is high.

Case study for commulative:

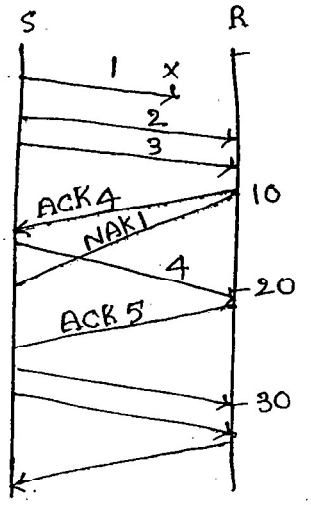



if the delay is high to send pkt 1, then at the time of receiving pkt 1, the packets 2,3 get expired, so again actual packets of 2,3 is sent.

## Combination of cumulative and Independent (Real time):

i.e Maintaing certain time slots.




suppose, consider 1,00,000 packets are transfered.

If first packet is lost at receiver side in cumulative after all packets are transmitted it send ack. At the time the sender knows that first packet is lost.

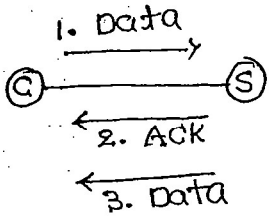
To overcome this problem repeat checking the pkts, improves reliability.

## Piggy backing (web):

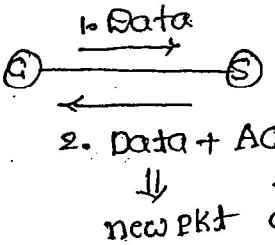
→ Mainly used in web services

→ To reduce the n/w traffic.

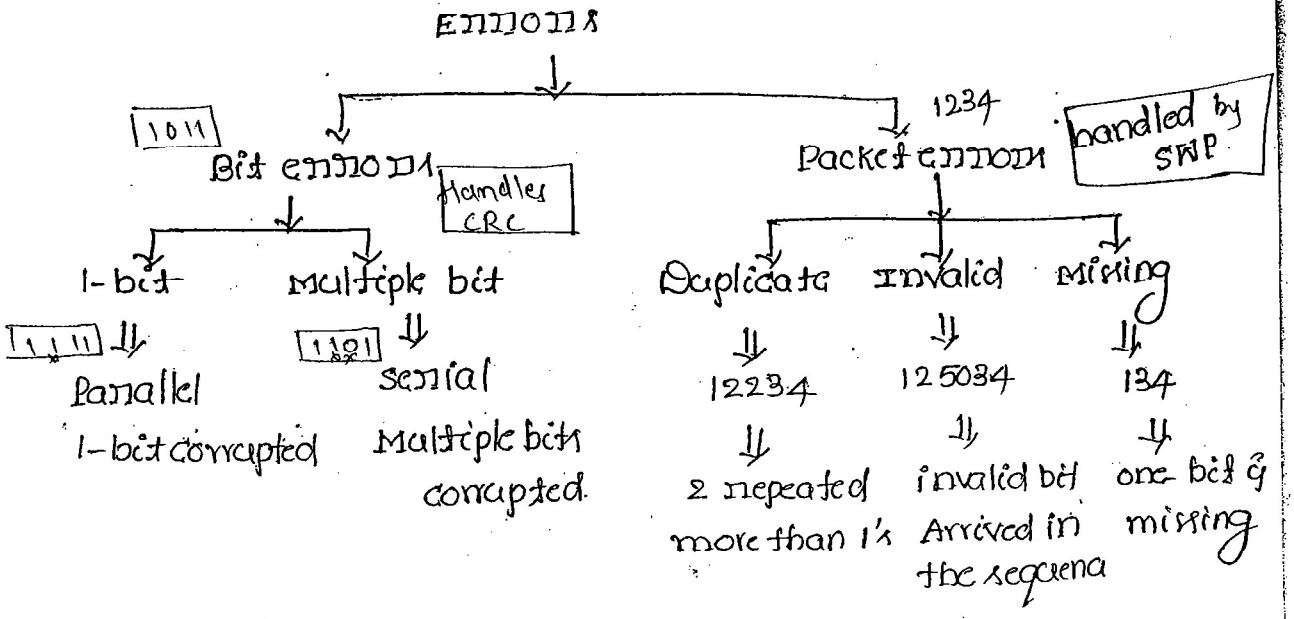
General Approach




Piggy backing:



# Different types of errors:




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

B: Bandwidth.

B = 10 bits/msec

$$= \frac{1}{10 \times 10^6} = 0.1 \mu sec.$$

serial data transferred is : 10110001

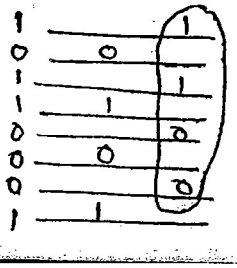
* if noise is present in serial transmission that all the bits are corrupted.

Parallel data transferred:
- 1 - -
- 0 - -
- 1 - -
- 1 - -
- 0 - -
- 0 - -
- 0 - -
- 1 - -

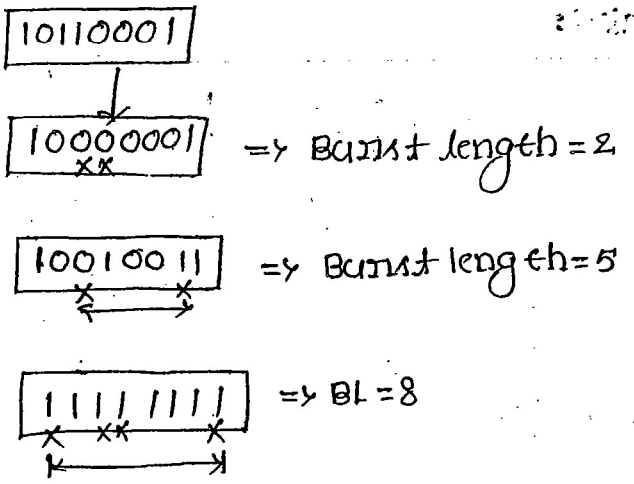
* in parallel transmission only that particular bit gets corrupted.

* Serial transmission is considered in computer n/w.

* if length of the communication is long (≥ 1 meter) we use serial transmission, else we use parallel transmission.

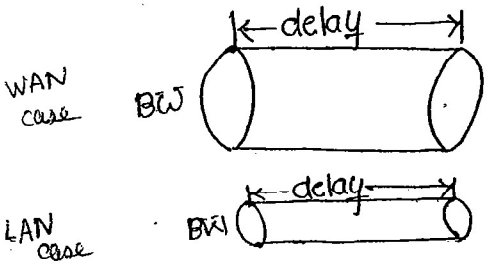



For synchronization and collecting the bits a group. so for long distances it not support.




* Burst length is calculated a bits present between starting and ending corrupted bits.
* Burst length depends upon the type of OS i.e 32-bit OS the max BL = 32, (or) 64-bit OS then max BL = 64.
* Based on the max BL CRC develop polynomials for error checking with $x^{32}$ or $x^{64}$. FCS = $x^{32}$ + ..... (if O.S. is of 32 bit Frame check seq (FCS))

Bandwidth delay:

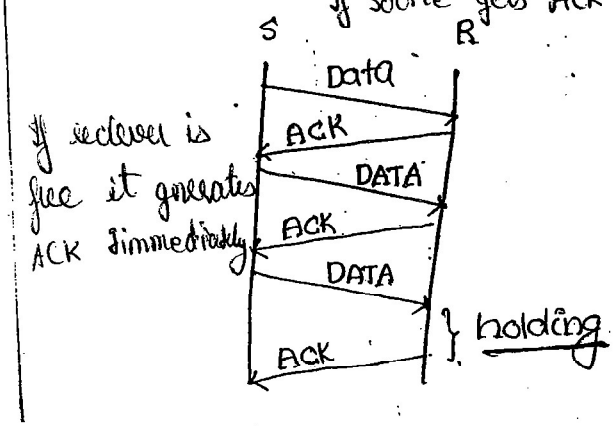



## Stop-and-wait protocol:

STOP & USES 2 rules at sender side:

Rule:1: Transfer only one packet at a time

Rule:2: After receiving the ACK only the other packet is transferred




For maintaing control

* 2 principles in sender
* 2 " " Receiver.

when receiver busy it can't accept new pkts, so at that time it won't send any ack to sender => i.e holding

it will hold ACK for a while & then releases the ACK.

Drawbacks:

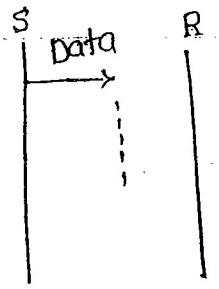
① 


fig: Lost data packet

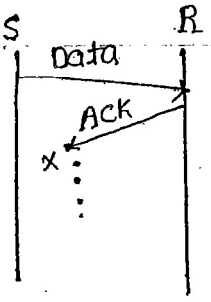
② 


fig: Lost ACK

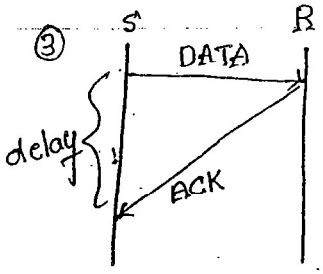
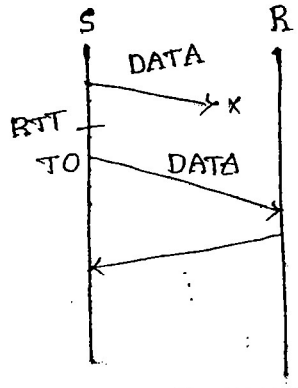
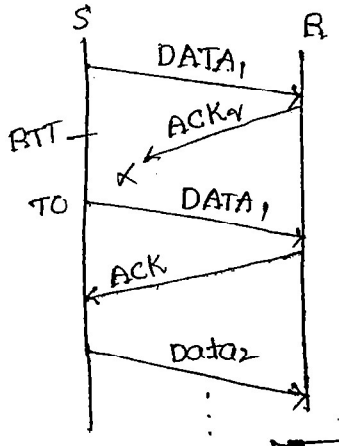
③ 


fig: Delayed ACK.

① 

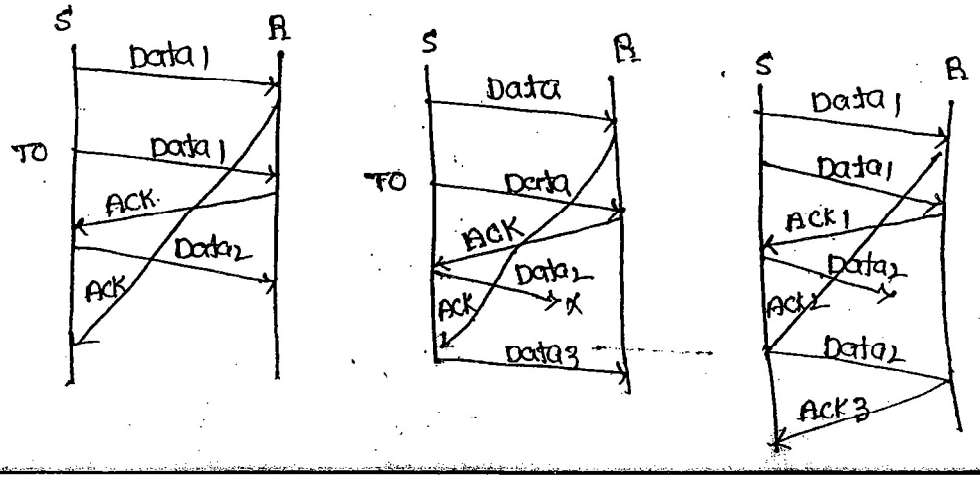

Either the lost data on ACK only the time out is considered. if within the given time ack is not received then next data is sent as represented it by timeout.

**Stop and wait + Time out**

② 


· if within time ack of data is not received and after data is received at receiver end and sender received ack of after TO data. it mean to have ack of Data1, so not be get confused, sequence num is increased.

**Stop & wait + Timeout + Sequence num (Data)**

③ 

in order to not to get confused about the ack of particular data packet, then the Ack sequence num also represented.

stop & wait + Timeout + sequence num(data) + sequence num (Ack)

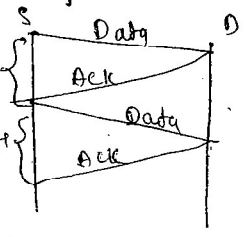
⇓ = Stop & wait ARQ

Automatic Repeat Request ⇒ it controls the packet level error control.

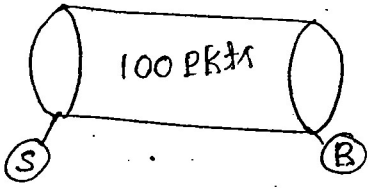
## characteristics of stop & wait:

* it uses the link between sender and receiver as a half-duplex link.
* Throughput of stop and wait protocol:

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



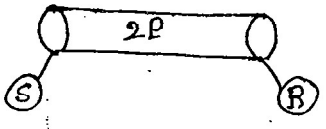

* if Bandwidth x delay product is very high then stop & wait Protocol becomes useless.




capacity = 100 pkts

filling pipe with 1 pkt then

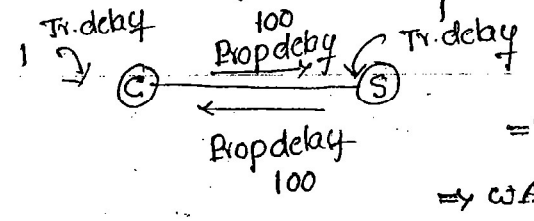
Efficiency = $\frac{1}{100}$ = 1%




⇒ Efficiency = $\frac{1}{2}$ = 50%

* it is not suitable for WAN because delay is high only suitable for LAN.
* if Propagation delay is high compared to transmission delay then, stop & wait protocol becomes useless. efficiency is less.

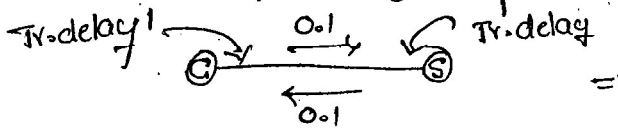
* Transmission delay is 1 mean upto 202 ms only 1 unit of time




$\Rightarrow$ utilization = $\frac{1}{202}$

$\Rightarrow$ WAN

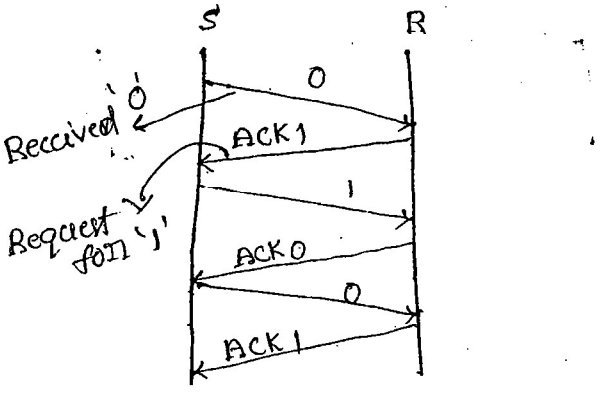
* Transmission delay is high compared to prop.delay




$\Rightarrow \frac{1}{2.2} = 50\% \Rightarrow$ LAN

* Stop and wait an example of closed loop protocol (connection-oriented)

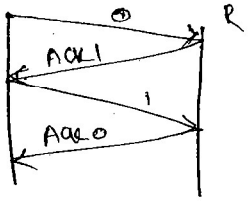
* Stop & wait protocol use only two sequence numbers.




* In special category of stop and wait protocol with window size is 1.

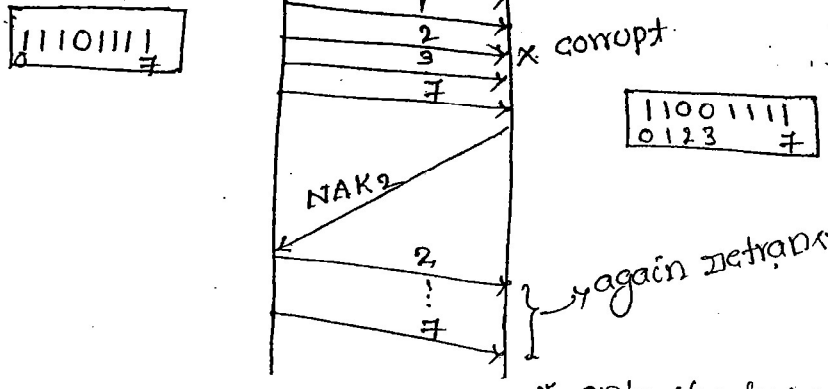
| Stop & wait $\Rightarrow$ $S_W = R_W = 1$ |
|---|

* Stop & wait protocol req. only two seq. numbers (0, 1) irrespective of no. of packets sender is having.



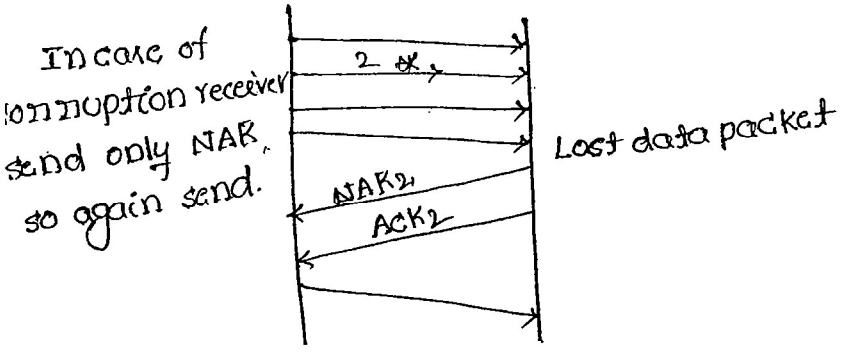
In this scheme sending packets of $Pkt_2$ is normally also all the seven pkts are being sent then $NAK_2$ is sent. Then 3 to 7 packets are being discarded. and $Pkt_2$ is retransmitted

corrupted data packets:

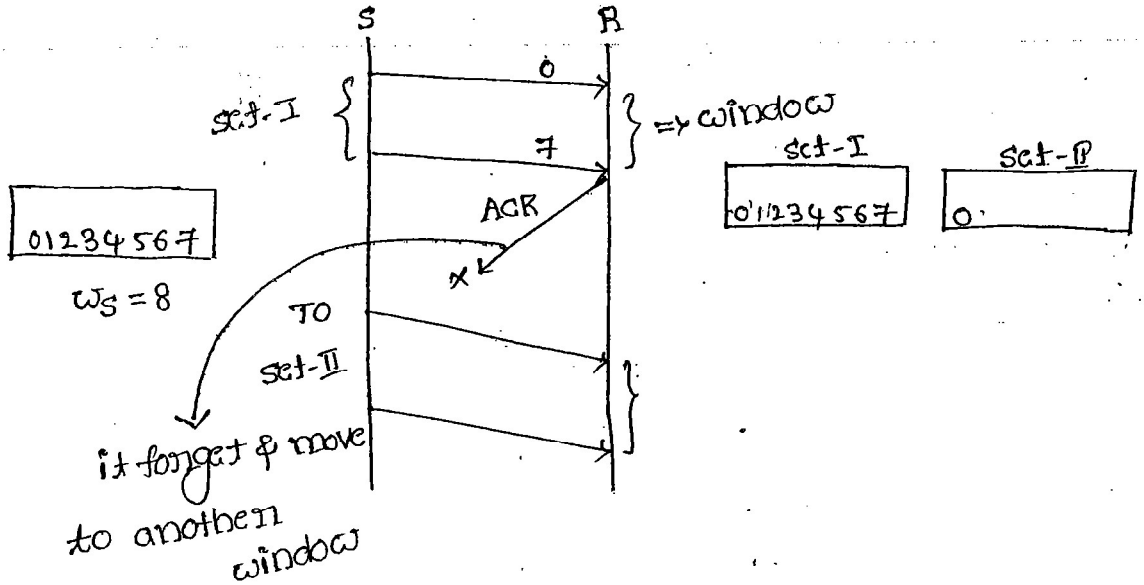



* only the lost packet have more impact that of the corrupted data Packet.

* Here the data packet is being corrupted then also the remaining all the packets are also get discarded.
* high reactivity problem.




so in order to overcome above problem of data lost while sending the NAK# $ACK_2$ is also being sent. so that it represents that $Pkt_2$ is not received and then after sending $Pkt_2$ it can continue from $Ack_2$.

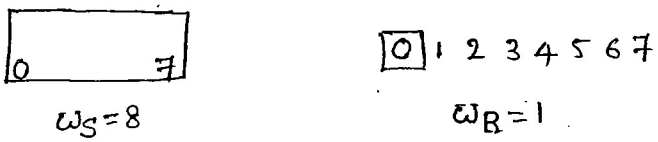



After time out, sender again send first window.

* To solve the above problem we have to re-adjust $w_S$, $w_R$ size.

**Case (a): $w_R$ size:**

it is equal to 1 always irrespective of $w_S$ size




so here it is waiting for 1 after selection '0' and if any other num other than 1 comes they are discard.

**Case (b) $w_S$ size:**

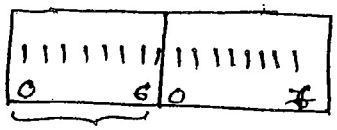
$w_S$ size is calculated based on following formula

$$w_S + w_R \leq \text{Available sequence number (ASN)}$$

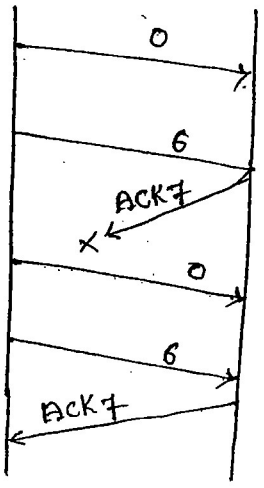
$$w_S = ASN - w_R$$

$$w_S = ASN - 1.$$

# Adjusting window size:




$W_S = 7$




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

eg: 16 — 0 ..... 15

Max available sequence num = 16

$W_S = 15$

$W_R = 1$

Eg: Total sequence number = 10

then $W_S = 9$, $W_R = 1$.

Case (1): Assume $N$ = Max available sequence number

$\therefore W_S = N - 1$

$W_R = 1$

Case (2): if $N$ is defined as max sequence number

$W_S = N$

$W_R = 1$

Case (3): if 'K' is no. of bits available in sequence number

$W_S = 2^K - 1$

$W_R = 1$

=

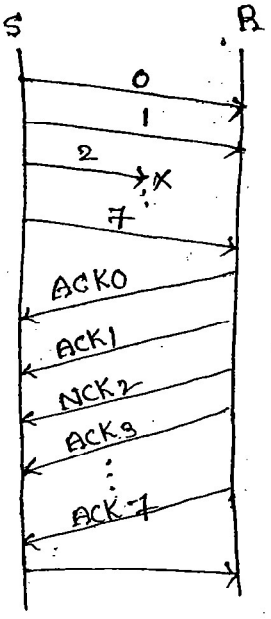
# Selective Repeat:

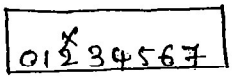
* Selective Repeat receiver receives out of order packets.
* It's natural choice is independent ack (if possible, it will also use piggy-backing)

1.

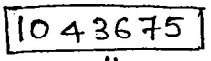

Missed $w_S = 8$

selectively send this packet to receiver.




$w_R = 8$




⇓

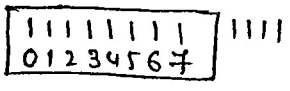
it receives any sequence for checking which pkt is lost it uses searching algorithm we take more time

* A searching algorithm is used.

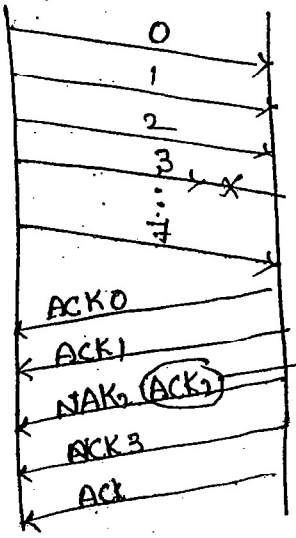
Dis Adv:

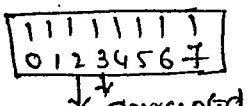
Time increases as it requires searching and sorting of num. of packets to be transmitted explicitly.

② corrupted:




we won't resolve the condition either packet is lost (or) corrupted because every time it sends only NAK

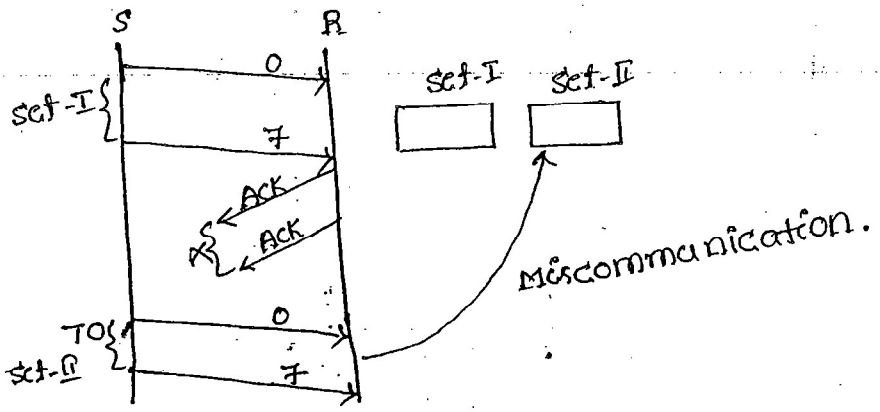



we can not command with sender that which packet is lost and which

"Ambiguity"

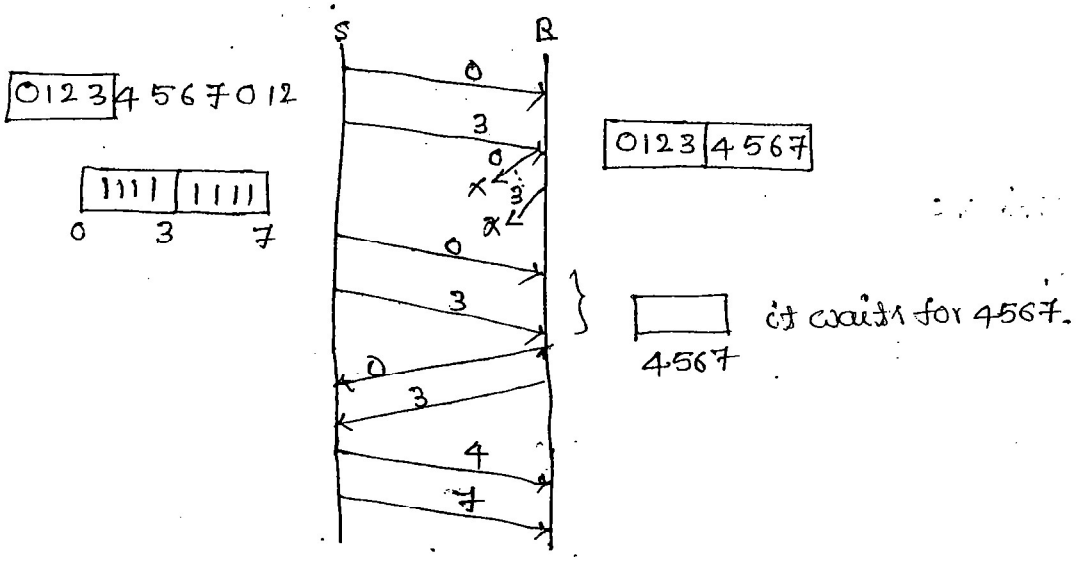
is obtained since Ack, is not sent with NAK, which receiver




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

$$W_S + W_R \leq ASN$$

* $W_S = W_R$
* $W_S > W_R$
* $W_S < W_R$. ✗




Case (i): if N is defined as max available sequence num then

$$W_S = \frac{N}{2}, \quad W_R = \frac{N}{2}$$

case (ii): if N is defined as max sequence no. then

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

case (iii). if K is defined as no. of bits in sequence number

$$W_S = 2^{K-1}, \quad W_R = 2^{K-1}$$

eg: 8-bit sequence number.

Go-Back-N => $w_S = 7$, $w_R = 1$

Selective Repeat => $w_S = 4$, $w_R = 1$

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)

Comparision:

| characteristic | stopfwait | GBN | Selective Repeat |
|---|---|---|---|
| 1. operation | simple | Medium | complex |
| 2. Requirement of sequence num | Low | Medium | High |
| 3. Bandwidth utilization | Low | Medium | High |
| 4. Buffer requirement | Low | Medium | High |
| 5. Efficiency | Low | Medium | High |

Stopfwait formula:

$$\text{Efficiency} = \frac{\text{Tran.delay}}{\text{Tran.delay} + 2 * \text{propdelay}}$$

$$= \frac{1}{1 + 2\frac{\text{Propdelay}}{\text{Tran.delay}}}$$

$$= \frac{1}{1+2a} \quad \therefore a = \frac{T_{propdelay}}{T_{trandelay}}$$

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

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

$\therefore$ If $L = BR$ $\eta = 50\%$

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

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

Steps to be solved in swp procedure:

1. calculate the 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" ($\omega_{bits}$)
3. $\omega_{PKT} = \frac{\omega_{bits}}{(PKT\,size)_{bits}} = \omega_p$
4. sequence numbers required = $\omega_p$.
5. $2^K = \omega_p$ where $K$ = no. of bits in sequence num P.

Problems:

① $B = 1.5$ Mbps

$RTT = 45$ ms

$L = 1$ KB

link utilization = ?

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

$= \frac{1024 \times 8}{45 \times 10^{-3}} = 182$ Kbps

$\eta = \frac{T}{B} = \frac{182\,Kbps}{1.5\,Mbps}$

$= \frac{182 \times 10^3}{1.5 \times 10^6}$

$= 0.121$

$= 12.1\%$

② Packet size = 1000 bytes

Ⓐ $d = 10$ KM

Ⓑ $d = 5000$ KM

$V = 70\% \times 3 \times 10^8$ m/sec

$= 0.7 \times 3 \times 10^5$ Km/sec

$V = 2.1 \times 10^5$ km/sec

Ⓐ Propgation delay $= \frac{d}{V}$

$= \frac{10\,km}{2.1 \times 10^5\,km/sec} = 0.476$ msec

RTT = 2 * Propagation delay

= 2 * .476

= .952 μsec

$$\text{Throughput} = \frac{1\,\text{Data}}{RTT} = \frac{1000 \times 8}{0.952 \times 10^{-6}} = \frac{8}{.952} \times 10^3 =$$

(B) = $T_{prop} \times \frac{d}{v} = \frac{5000\,KM}{2.1 \times 10^5\,km/sec} = 95.2 \times 500$

RTT = 95.2 × 500 μsec

$$T = \frac{1000 \times 8}{95.2 \times 500\,\mu sec} = \frac{80\,mbps}{500} = 0.16\,mbps$$

=

③ Packet size = 1KB

Propagation time = 15 ms.

$B = 10^9$ bits/sec

RTT = 30msec Transmission time = $L/B = \frac{1024 \times 8}{10^9} = 0.008$ msec

$$\text{utilization} = \frac{1}{30 + (0.008)2}$$

$$= \frac{1}{30.016}$$

$$= 0.033$$

$$= 3.3\%$$

④ B = 4 Kbps

Propagation delay = 20m/sec

$\eta = 50\%$

RTT = 2 * propagation

= 40m/sec

$L = BR$ $\eta = 50$ then $L = BR$

$= 4 \times 10^{3} \times 40 \times 10^{-3}$

= 160 bps

⑤ Propagation delay = 100 μs

d = 20 KM

L = 1 KB = 1024 × 8

B = ?

RTT = Transmission delay

RTT = 200 μs

Transmission delay = $L/B$

$B = \frac{1024 \times 8}{200 \times 10^{-6}} =$

= 40 mbps

⑥ B = 1 Mbps

latency delay (or) propagation delay = 1.25 sec

L = 1 KB

1. RTT = 2 × 1.25

= 2.5 sec

2. 1 sec $1 \times 10^{6}$ bits

2.5 sec ?

$\omega_{bit} = 2.5 \times 1 \times 10^{6} \Rightarrow 2.5 \times 10^{6}$

3. $\omega_p = \frac{\omega_{bit}}{(Pkt\ size)}$

$= \frac{2.5 \times 10^{6}}{1024 \times 8}$ $\therefore 2^{K} = 305$

= 305. $\therefore K = 9$

4. Sequence num = $\omega_p = 305$

Gate: window size = 5 packets

Data packets = 1000 bytes

Transmission time for such packets = 50 µs

Propagation delay = 200 µs

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

RTT = Tr.delay + 2 * propagation

$$= \frac{5 \times 1000 \times 8}{50 + 400 \times 10^{-6}}$$

$$= \frac{5 \times 1000}{50 + 400 \times 10^{-6}}$$

$$= \frac{5 \times 1000 \times 8}{450 \times 10^{-6}} =$$

$$= 88.88 \times 10^{-6} \text{ bits}$$

$$= 11.11 \times 10^{-6} \text{ bytes.}$$

$=$

(9)

| 3960 | 40 |
|---|---|

S ——— R

100 × 3960 — 100 × 40 (H)

40 (NAK)

396000 — 3960 + 40 (Retrans)

8040

$$\frac{396000}{3,96,000 + 8040} = 98\% \qquad \frac{8040}{3,96,000 + 8040} = 2\%$$

(10)

A ——→ R ——→ B

WS = 4 T = 2

At t=0 packets are released at A and immediately available at R.

"0" starts leaving at R.

∴ 123 are in Queue.

$t=1$, 0 arrives at B, ack, is made, meanwhile, 1 starts leaving "R" therefore 2 & 3 are in the queue.

$t=2$, ack, arrives at R and then at A. Therefore 4 is released from A and immediately available at R. meanwhile arrives at B Hence Ack, is made at the same time 2 - starts leaving "R" and therefore 3 & 4 in the the queue.

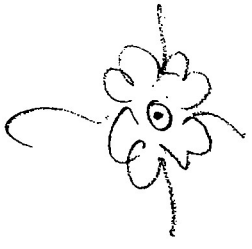
At $t=5$, 6 & 7 are in the Queue

$t=10$ 11 & 12 are in the Queue.

=

S. Jonda Reddy

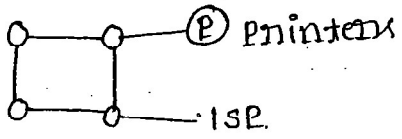
=

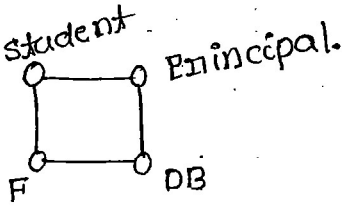


# Lan Technologies

Advantages of LAN:

* Resource sharing on resource utilization (H/w & S/w).
* information sharing.



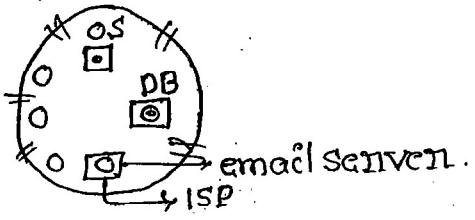

Types of LANs:

* Dedicated Server LAN
* peer-to-peer-LAN
* Zero slot LAN.

| | Dedicated Server LAN | peer-to-peer LAN | Zero-slot-LAN. |
|---|---|---|---|
| Packet share | 80% | 10-15% | 5% |
| Security | high | Moderate | low |
| No. of systems | Any | 50-60 | < 10 |
| Application | Any | few | very few |
| cost | High | Moderate | low |
| equipment | IP, NOS, NIC | NIC | X |

## Dedicated Server LAN's:

* To acces OS (or) database, username and password must be submitted and then again to acces 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 types of users there are some restrictions to some user to access data | There are restrictions on some data (or) some files. |

Peer-to-peer LAN:

As in dedicated server LAN's, there is no requirement of network operating system and IP address.

Right click → TCP/IP

Domain s/w → ⇓ dedicated server LAN

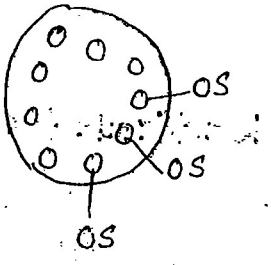
workgroup s/w → ⇓ Peer-to-peer server LAN.

ACE → workgroup

⇓

one
two
three
⋮

→ names of individual systems within a workgroup.




communication done among the system within a workgroup.

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

workgroup: All the systems are being connected for the purpose of communication among them.

* There is no particular leader in the workgroup. All the systems are considered equal. Hence it is called "peer to peer"

Eg: Browsing centre
(contains no. of clients & only one server)

* 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.

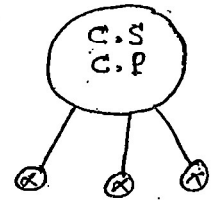
At the most we get 2-serial
2-parallel
4 USB ports so it has < 10 systems

* No realtime application, and oracle application are possible.

LAN components:

1. Network operating system.
2. Cable
3 NIC

1. First generation

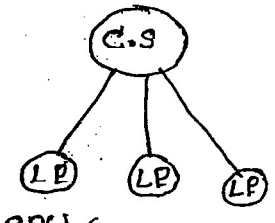



CPU ✗
HDD ✗

Eg: UNIX

C.S ⇒ Central storage

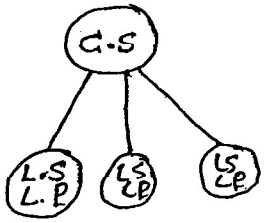
2. second generation




CPU ✓
HDD ✗
Thin client

Eg: Novell network

3. Third generation




CPU
HDD
only local Process execute

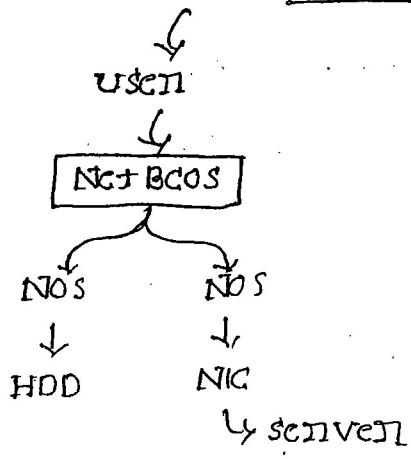
Eg: windows.

UID :

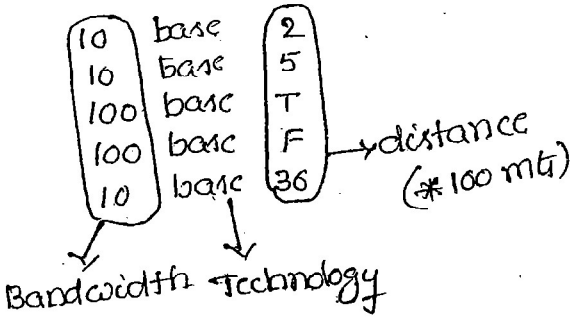
PWD :

Domain name: [This system ▽] → Local system accessed

[Domain name ▽] → Then entire n/w accessed.




2. Cable: Types of cables




Baseband ——— LAN

↳ single type of frequency  Base$_2$ => up to 200 mts without signal loss.

Broadband : ——— WAN => Directly connected with ISP => Dial-up connections

=> All types of frequencies are carried out.

* In cable TV networks "Boosters" are used within limited distance.

Baseband 200 mts so use repeators.

* Twisted pair => 100 mts 10 mbps
* Fibre optic cable => 2000 mts
* 100 base T => category 5 cables => bulky => RJ45 => connectors are used.
* category 3 => incoming signals. To repost the signal repeaters are used.

3. **NIC:** Hardware -> physical layer

PL + DLL => (combination of H/w & S/w)

* Near technology systems use the NIC cards.

IEEE 802:

These are exclusively meant for LAN.

Main layers: Transport layer.

Network layer.

Segmentation & Re-assembly:

* In local network, no need of it.
* For LAN's Transport & network layer's are not needed.
* Main focus on datalink layer and physical layer.

LLL => framing

Medium Access Control (MAC):

Error control
flow control
Access control
physical address.

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

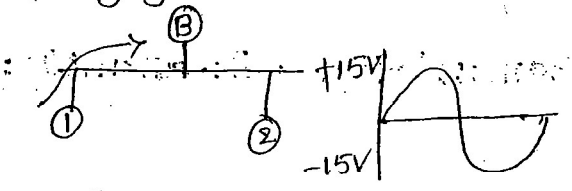
eg: For real time applications MAC is replaced with 802.5.

characteristics:

* Ethernet offers connectionless communication
* no flow control & packet level error control
* no acknowledgment [either +ve) or -ve)]
* it uses bus topology
* it uses CSMA/CD as an access control method.

CSMA/CD:

* The channel, whether communication is taking place or not if there then, wait for the another channel to complete it's transfer of data packet or else transmit the data packet from the current channel only.
* The channel is sensed in terms of voltage if V=0 not wave form, i,e no channel is engaged to transfer packet (Media is free)

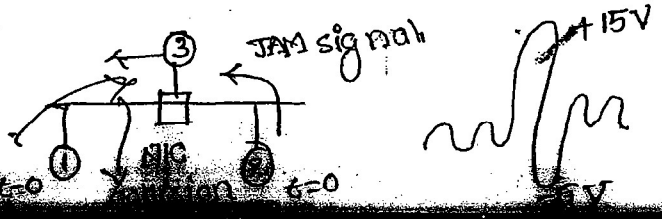



Multiple Access:

* if more than one channel, sense the medium, both the channels try to access the medium and want to transfer data packets simultaneously then it is called "Multiple access".

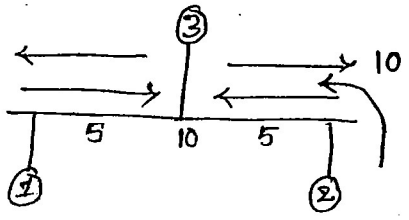
Collission Detection:

At the situations of multiple access of channel collision occurs while transferring data packet. so a JAM signal is used to detect the occurance of collision and it is sent to both channels



* All channels are having different frequency and jam signals have different frequency so there is no chance of collision occurance

* Since channels have different frequency => Bandwidth increases.

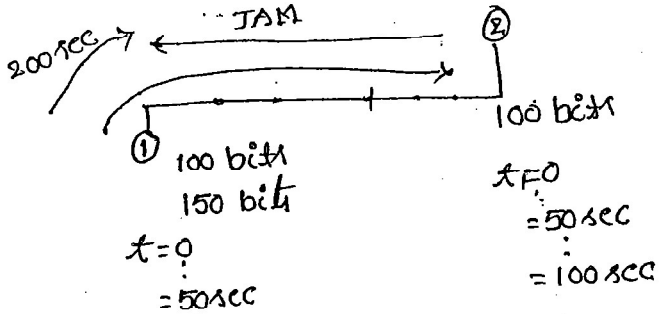


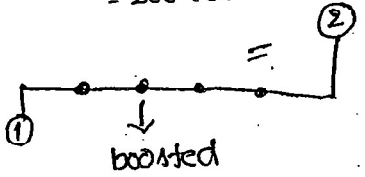

Minimum = 20

| 100 | 10 | 9 × |
|---|---|---|
| t=0 | t=0 | |
| =5 | =5 | |
| =10 | =10 | |

$S_1$ system have 100 bits, $S_2$ have 10 bits assume that they take the channel at a time then collision occurs. for recognizing collision, every system maintains min. frame size based on channel length.

RTT = Transmission Delay. => $2 * \frac{d}{V} = \frac{L}{B}$



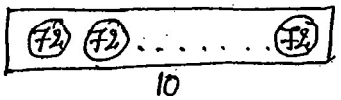

Repeators are allowed.

=> $2 * \frac{d}{V} = \frac{L}{B}$ => $2\left(\frac{d}{V} + 4 * \text{Repeator delay}\right)$

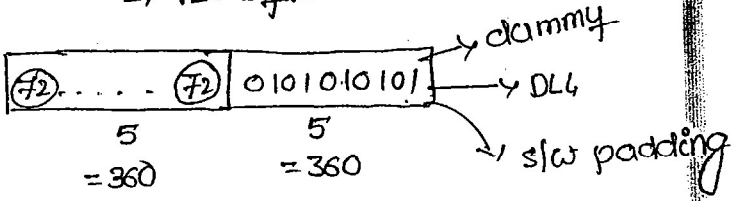
$57.6 \text{ msec} = \frac{L}{10 \times 10^6}$

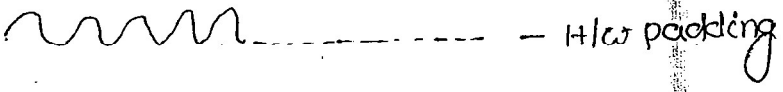
| Basic Ethernet | Fast Ethernet | Gigabit Ethernet |
|---|---|---|
| 10 mbps | 100 mbps | 1 Gbps |
| 2500 mts | 250 mts | 250 mts |
| 72 byts | 72 bytes | 72 bytes. |

Basically 25 mts
720 bytes




=> 720 bytes



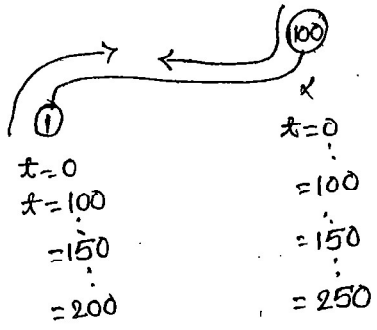

## Backoff Algorithm:

it gives waiting time for stations that are involved in collision

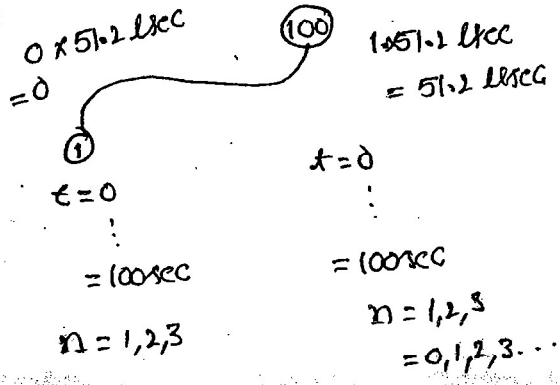
$$\text{waiting time} = K \times 51.2\ \mu sec$$

where K → randomly derived from 0 to $2^n - 1$.

where n - collision number.




Case study:



Let $n=1$

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

$\Rightarrow 0$ to $2-1$

$\Rightarrow 0,1$

Let $n=1$

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

$\Rightarrow 0,1$

* if let as consider $K=0$ to channel 1 and $K=1$ to channel 100 then waiting time of channel 1 = $0 \times 51.2$ μsec

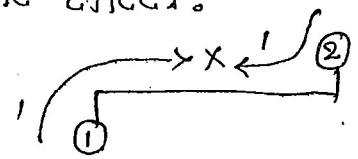
$= 0$

waiting time of channel 2 = 51.2 μsec.

∴ so channel 1 have waiting time = 0. then it can transfer the data packets but channel 2 must wait up to 51.2 μsec. & then again back-off algorithm is applied to proceed the transmission through either channel 2 or others.

## Limitations of Back-off Algorithm:

### capture Effect:




Let $n=1$

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

$= 0,1$

Then $wT = 0 \times 51.2$ μsec

$= 0$

Let $n=1$

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

$= 0,1$

$w.T = 1 \times 51.2$ μsec

$= 51.2$ μsec

$n = 2$

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

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

$= 0,1,2,3$

Then repeat same for $n = 3$

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

$\Rightarrow 0,1,2,3,4,5,6,7,$

⇓

if after 51.2 μsec again another channel also wants to access the medium, then again backoff algorithm is applied then $n=2$

Then the probability of channel 1 and channel 100 to access the medium and transmission are under same [illegible]

| 01 | 0123 |
|---|---|
| 0 | 0 |
| 0 | 1 |
| 0 | 2 |
| 0 | 3 |
| 1 | 0 |
| 1 | 1 |
| 1 | 2 |
| 1 | 3 |

5/8 — 1/8

13/16

| 01 | 01234567 |
|---|---|
| 0 | 0 |
| 0 | 1 |
| 0 | 2 |
| 0 | 3 |
| 0 | 4 |
| 0 | 5 |
| 0 | 6 |
| 0 | 7 |
| 1 | 0 |
| 1 | 1 |
| 1 | 2 |
| 1 | 3 |
| 1 | 4 |
| 1 | 5 |
| 1 | 6 |
| 1 | 7 |

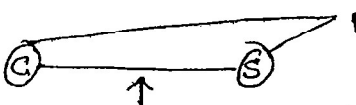
1/16

## Data specifications:

① Data rate
- => 10 mbps
- => 100 mbps
- => 1 Gbps

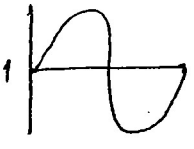
② signal
Manchester encoded signal

③ Addressing system
48-bit physical address.

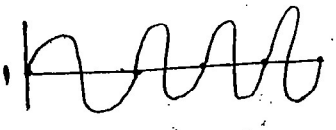



Bit rate => bits/sec

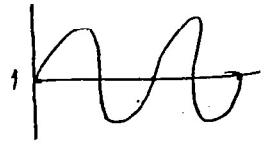
Baud rate => byte/sec.



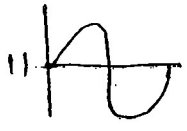

=> Baud = 1 x bit




Baud = 4 x bit




Baud = 2 x bit




= 1/2 bit

## Ethernet:

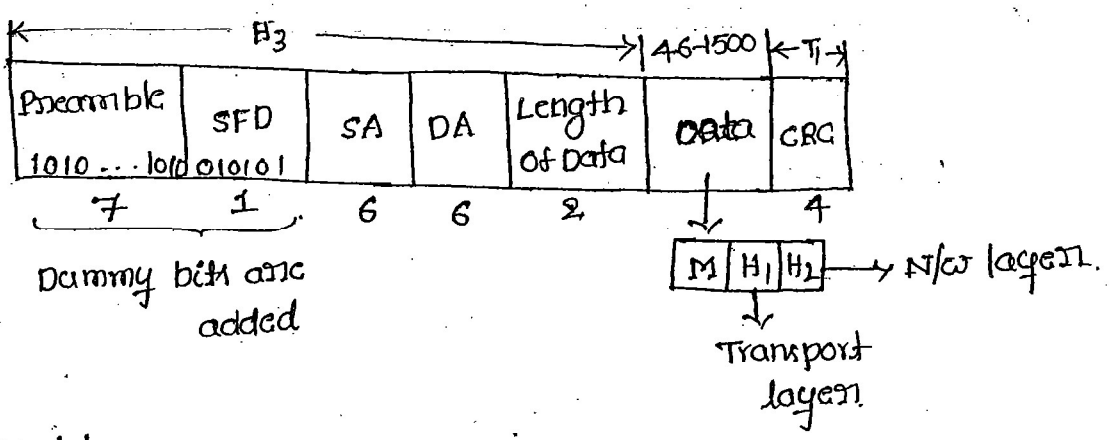
For a 10 mbps ethernet

Baud rate = 20 megabaud.

For a 100 mbps ethernet

Baud rate = 200 megabaud.

Frame format of 802.3:




**Preamble:**

* it contains continously 1's & 0's for seven bits
* it is used for synchronization purpose.

SFD (Start of frame Delimiter)

* its signals actual start of the frame.
* Dummy bits are represented by preamble 11110101111 ⓞ 10101010 ⓔ

Source & Destination Address:

* They are 48 bit physical address representing source & Destination
* Maximum size of data = 46 bytes, so that we make out 76 byte frame.
* Maximum size of data = 1500 bytes → To avoid monopolisat

  ↓↓
  change given to other channels also.

| Min | Max |
|---|---|
| 46 | 1500 |
| 72 | 1526 → frame |
| 64 | 1518 → frame from source address } => Preamble & SFD are neglected |

=

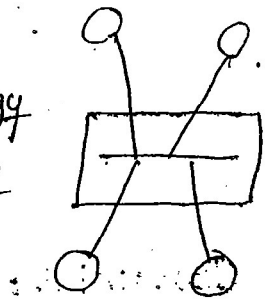
**Length of the data:**

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

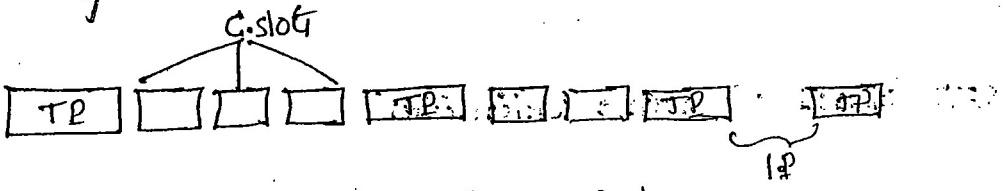
* it is added only at the tail to identify bit errors
* To avoide more no.of tranmissions we use CRC at tailend.

Implementation :

Physical Addressing - Star topology
Logical Addressing - Bus topology



Efficiency calculation of Ethernet:




T.P = Transmission period
C.P = collision period
I.P = ideal period

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

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

Let N → Total no.of systems in network.

$P_S$ → Probability of a station to transfer data pkt

$1-P_S$ → Probability of a station not to transfer data pkt

* To get a succesful transmission for a station remaing (N-1) station shouldn't transfer the data pkt.

* $\underline{(1-P)^{N-1}}$ => Probability for the remaining (N-1) stations not to transfer data packets.

* $\underline{P_S(1-P_S)^{N-1}}$ => Probability of the succes 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 $N \to \infty$ => $A = 1/e$

No. of contention slots = $1/A = 1/(1/e) = e$

Contention period (C.P):

= No. of contention slots * slot duration

C.P = e * 2 prop.delay

Transmission period = $L/B$

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

$$= \frac{L/B}{L/B + 2 * \frac{d}{V} * e}$$

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

$$\uparrow \eta = \frac{1}{1 + \frac{2dBe}{LV}}$$

* if load increases, efficiency decreases

* if pkt size increases, then efficiency also increases.

1. $$\eta = \frac{TP}{TP + CP} = \frac{t_{tran}}{t_{tran} + 2t_{prop} * e}$$

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

$$= \frac{1}{1 + 2a \cdot e} \Rightarrow \eta = \frac{1}{1 + 2ae}$$

2. $\eta = \frac{T_{trans}}{T_{trans} + C.P + t_{prop}}$

$= \frac{T_{trans}}{t_{tran} + 2.t_{prop} * c + t_{prop}}$

$= \frac{1}{1 + 2.\frac{t_{prop}}{t_{tran}} * c + \frac{t_{prop}}{t_{tran}}}$

$= \frac{1}{1 + 2ac + a}$

$\boxed{\eta = \frac{1}{1 + 6.44a}}$

Every station must be waited for one fraction time, after collision aborting bits from collision point

Advantages of Ethernet:

* cost of ethernet is less.
* Ethernet cables are robust to noise
* Simple operation

DisAdv:

* 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 min size of pkt, Hence it is not suitable for interactive applications

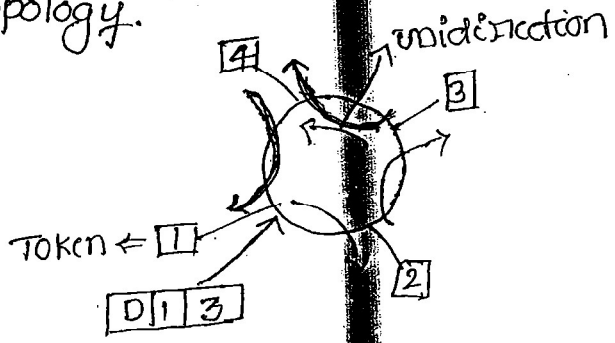
  eg: interactive application needs 1 or 2 bytes.

  eg: ATM.

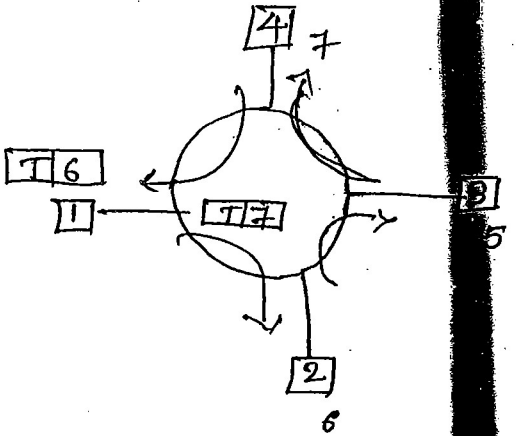
* if load increases, efficiency decreases.

# TOKEN RING

* characteristics:
* it also offers connectionless communication
* it uses piggybacking acknowledgement system
* No restriction on number of min size of data priorities are possible & deterministic service is possible
* it uses token-passing system as an access control method and ring topology.



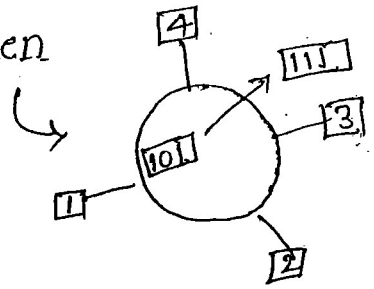

* Token is maintained at one station only then the data is sent to the other station, where it checks for source & destination. if same then it copies only and then sent the original data to other, Therefore there is no collision.
* if any station have high priority than the token or equal then it can access and low priority cannot access. Therefore no collision



Problems with token ring:

1. (A) Vanished token

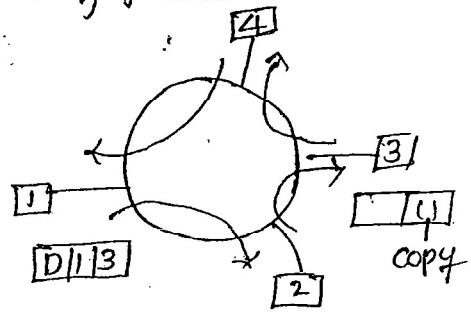
(B) corrupted token




2. Source: partial packet is produced and the station is recognised by this partial pkts.

A. Orphan packets

B. Stray packets



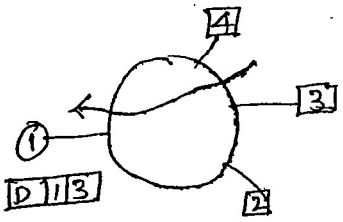

orphan pkts => source trash rotate upto $\alpha$ times

stray pkts => no one understands.

(C) Monopolization (Single man rule)

one station is being accessed whole the time which cause problem to other stations.

3. Destination:

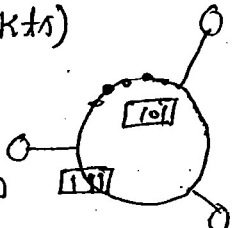



A. Safe operation

B. Busy destination (not able to copy the frame)

C. crash destination (Drop the pkts)

4. Ring:




* Major cut in the ring, stops operation

* unhealthy token => no station can use the original token

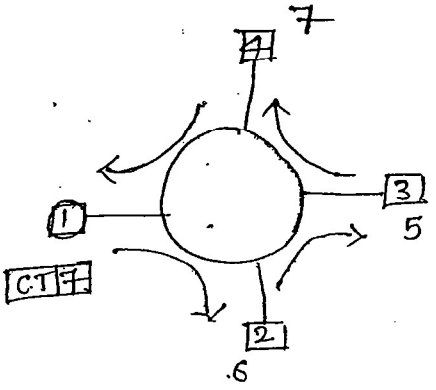
To overcome token ring problems we have the following

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




Minimum TRT = Propagation delay in the ring
+
100 sec
No. of active stations * Delay at each station.

Maximum TRT = Propgation delay in the ring
+
No. of active stations * Token holding time

* Moniton station expect this token within these 200 sec. if Packet not arrives then it reproduce the token thinking that it is missing so it solves the vanishing token problem

it also waits for 20 sec more than 200 sec.

* corrupted tokens are recorrected by the monitor station within the 2nd cycle no other station have 3-bits.

2. Orphan:

when a packet crosses a monitor station it makes a error stamp on it stamped pkts are not allowed.

3. Stray:

checking the validity of pkt while crossing the monitor station.

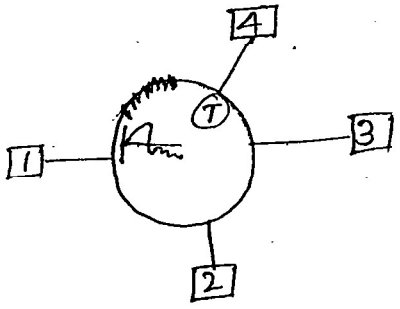
3. Destination:

Two fields 'A' & C are attached

| | | |
|---|---|---|
| A=0 | C=0 | |
| A=1 | C=0 | => Safe |
| A=1 | C=0 | => Destination Busy |
| A=0 | C=1 | => Destination not available but frame is copied it represents that other than destination station has copied the frame. |

4. Ring: A special frame is introduced.

* if continously produce, the pkt and no response, then cut it & produce a wave form at t=0 and if response within t=1 μsec then it identifies as the major cuts



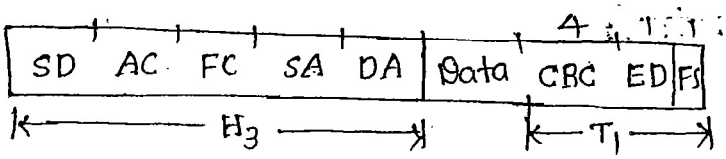

* A special frame is sent by monitor station for every 10 sec saying that it is available, if any frame is not received then it is assumed that monitor is crashed and there is a change of other stations to become a monitor station.

# Specifications of Token Ring:

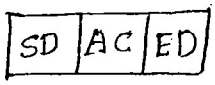
1. Data rate
   * 4 Mbps
   * 16 Mbps
2. signal: DME
3. Addressing system: 48-bit physical Address.

## Frame format:

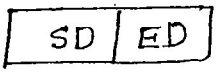
1. Data frame




2. Token frame




3. Abort frame



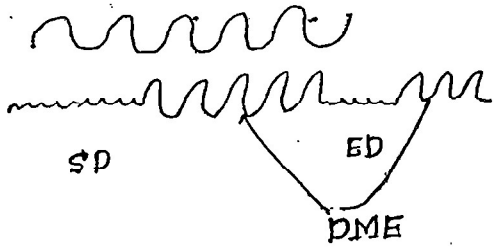

Start Delimiter, End Delimiter } used to indicate two extreme ends of the packets.

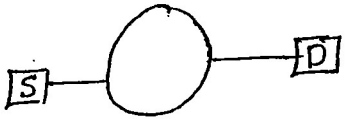
* They use DME signals.

SD: 10JK 10JK → other signal except DME

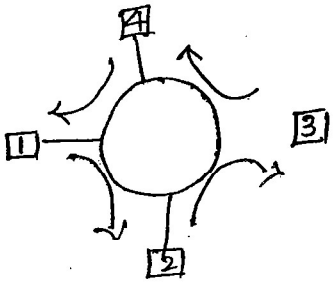
ED: 11JK 11JE → Error bit

→ information bit.




1=0
2=0
3=0
4=1 ⇒ it gives indication of ending on last packet




if E=1 then it simply transfer

| P | T | M | R |
|---|---|---|---|

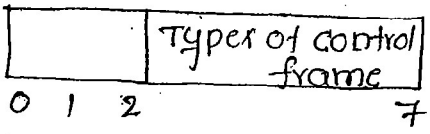
M => Monitor bit

T=0 => Data
=1 => Token

M=0 => Before crossing monitor bit
=1 => After crossing the monitor bit
↓
if again requested it just eliminate it.

Frame control:

6 types of frame control

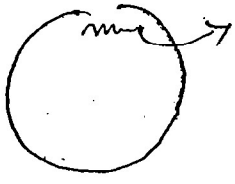



00 – Data
11 - control.

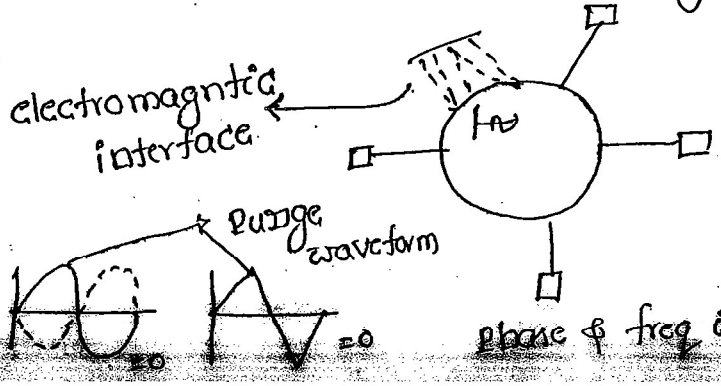
1. Client token: it is used in the election procen of monitor.

2. Active moniton presence:
it is issued by the monitor in equal intervals to make it presence.

3. Becon: it is used to identify major cut in the ring.

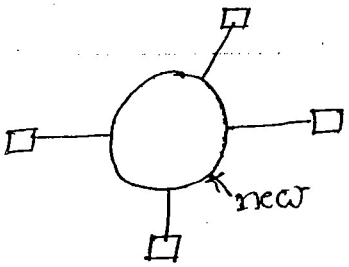



4. purge frame: it is used to clear the ring from unwanted bits.




phase & freq is measured by monitors.

5. Duplicate Address test frames:




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

⇓

new channels address.

⇓

it is being checked with all other channel who have this address. if any other address is given 4 again checked.

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

Virtualisation:

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

windows (Base Machine)

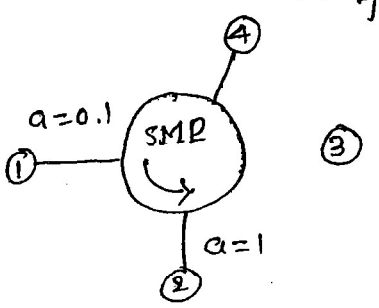
IPadd IP IP ⇒ virtual physical address of virtual machines.

virtual Machine

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

6. SMP (Standard by Monitor preserve):

it is used to carryout neighbour identification.




Upstream: From whom the channel receives the data packet.

Downstream: To whom the