CN

CN

Computer Networks

Varun Pandey

10-7-2011

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 browser
SMTP : Mail computation
FTP : File communication
NTP : Network time protocol
~~SNTP~~.

* 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

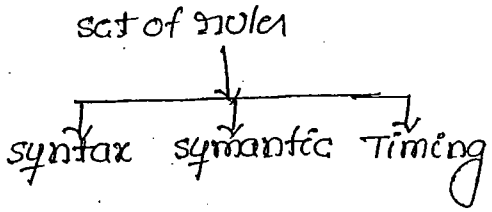
HTTP: 1.0, 1.1, 2.0 (Application protocols).

* RFC : Request for Comments => Stands for computer network.

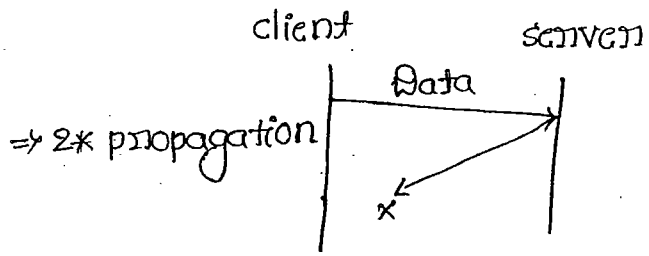
* concept of computer n/w have an RFC number

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.

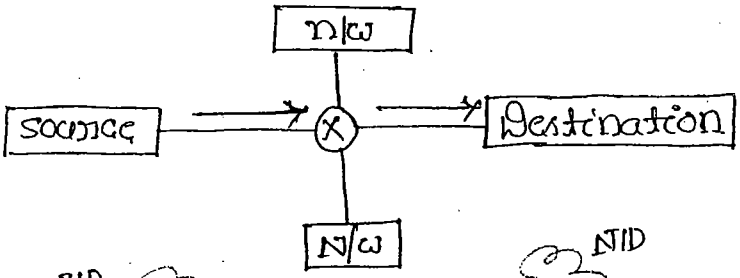
* IP address doesnot refer to a host actually, it really refers to interface, if a host is on two networks, it must have two IP. 3

* A system may have multiple ip addresses and multiple physical addresses.

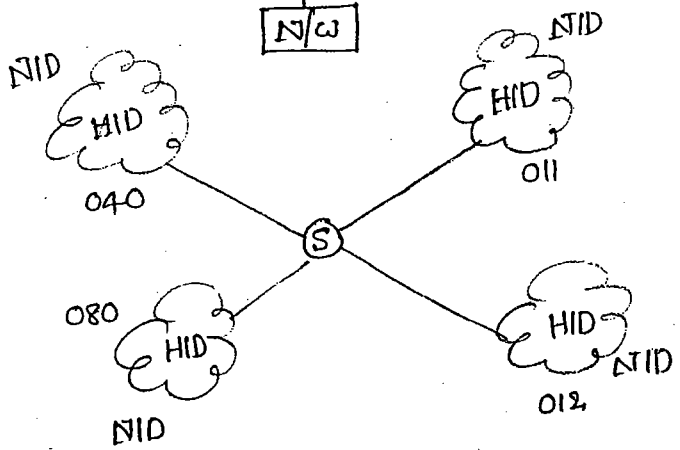
2. Identification:

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 / 3 — 4752469 / 7

02145 / 5 — 39764 / 5

078914 / 6 — 0823 / 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.

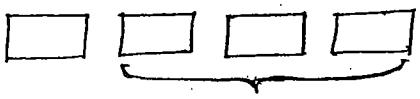
3. HID must be unique.

4. Hidden meaning.

Classification of IP Addresses:

To coverns the needs of diff types of organizations IP addreses are divideded into Five clases.

clas A:



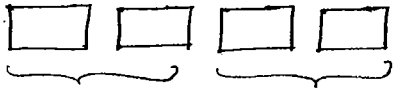
NID	HID
8	24
2^8 N/w	2^{24} hosts/NW
256	= 1.6 cr hosts/n/w.

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

eg: APSWAN Andhra pradesh state wide Area Network

* IP addres can be assigned to any electronic device.

clas B:



NID	HID
16	16
2^{16} N/w	2^{16} hosts/n/w
65,536	65,536

Eg: Big organizations, MNC, Banks.

clas C:

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

eg: engineering colleges.
Medium orgs

class A : 1–126

class B : 128–191

class C : 192–223

class D : 224–239

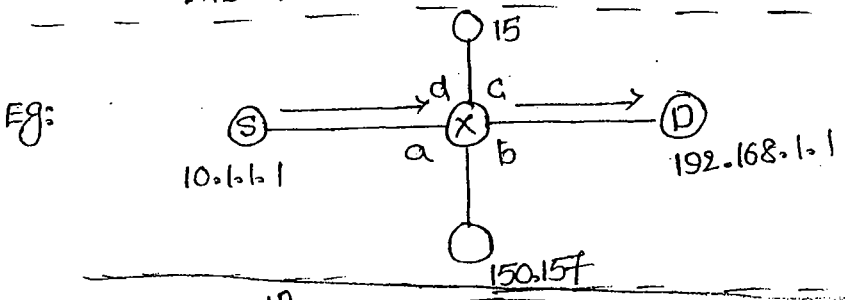
class E : 240–255

* 127 is a special IP address.

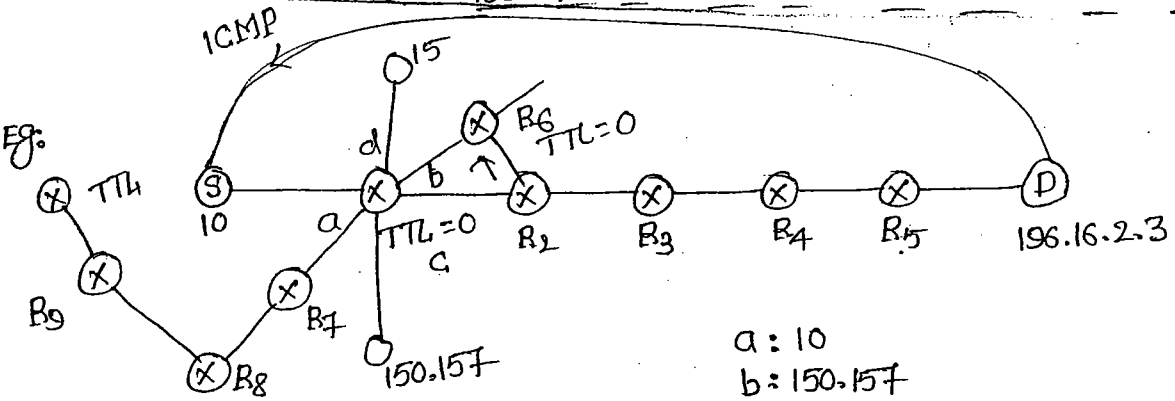
Eg: 150.167.1.1 — NID HID — class B

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 : deefault

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

* Make TTL = 0

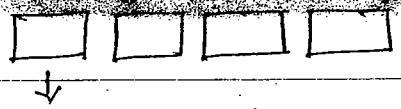
eg: TTL = 3 min = 180 sec.

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

Routing

source Router

Class A:



↓

0 reserved

00000000 → X
00000001 – 1
00000010 – 2

⋮

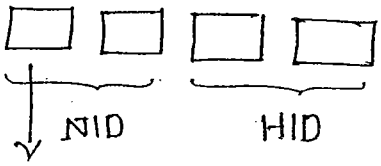
01111110 – 126
01111111 – 127 → X

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:



10 reserved

10000000 – 128
10000001 – 129

⋮

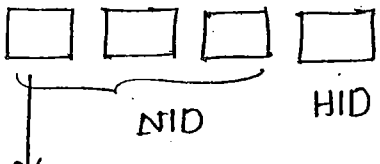
10111111 → 191

2^{16} N/w 2^{16} hosts/N/w.

⇓

2^{14} N/w $2^{16} - 2$ hosts/N/w.

Class C:



110 reserved.

11000000 – 192

⋮

11011111 – 232.

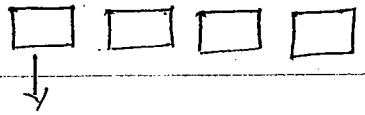
2^{24} N/w 2^8 hosts/N/w.

⇓

2^{21} 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.



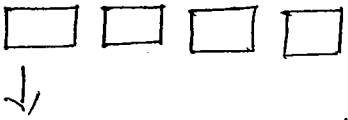
1110 → reserved.

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.

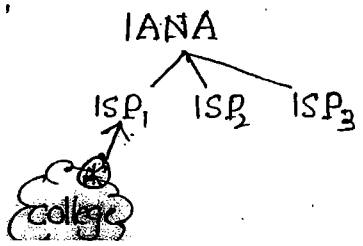
* IP_4 → 32-bit addressing system
* IP_6 → 128 Bit " "
* windows 7 supports IP_6
* Linux 10.6 also supports IP_6.

IANA: Internet Assigned Number 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 Eg.
but it is time consuming so a mediator known as ISP handles the connection IANA and Provides IP address.

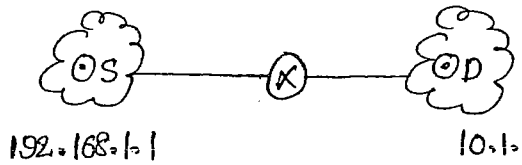
IANA (or) ICANN: Internet corporation for Assigned Names and Numbers.

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

Eg: sending group mail

yahoo.mail

Group IPaddress

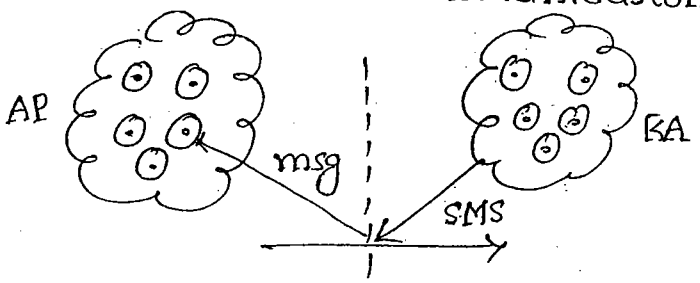
10.1.1.1
10.1.1.2
150.157.1.107
200.200.200.1

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 bits 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.

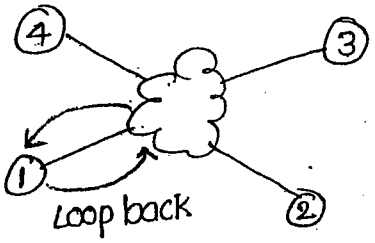
* so it has 1:1 and 1:all communication.

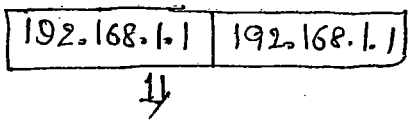
=

=> 127 Special IP Address:

* 127 IP address is used for connectivity purpose.

PING: Packet internet group.





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:

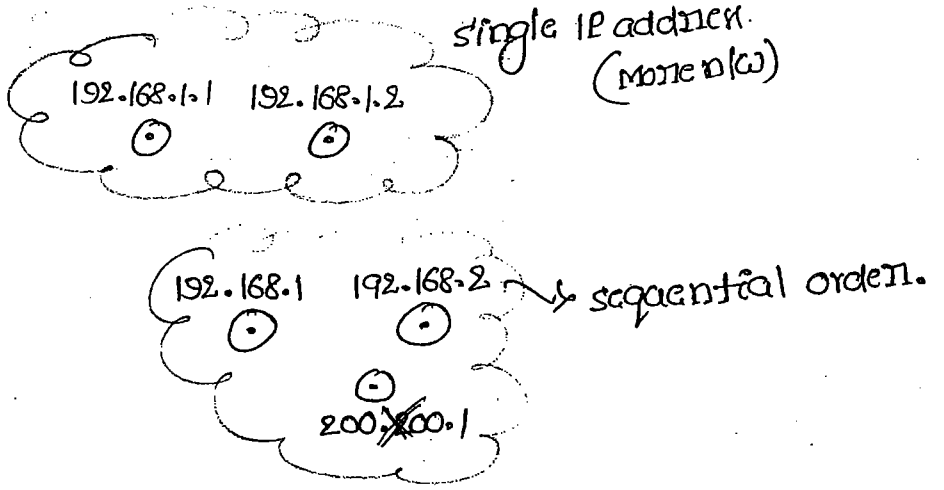
1. Supernetting
2. Subnetting
3. Physical Addressing system.

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 subnets 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 $= 2^9 - 2$.

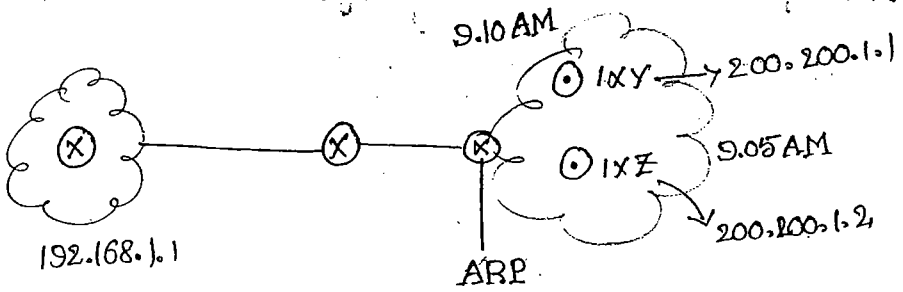
Limitations:

* 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:



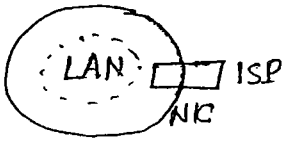
192.168.1.1	200.200.1.1

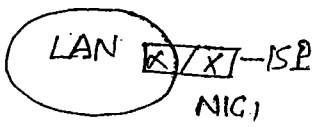
9.00 AM

* 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

IXY => 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 }
Assigned port number (Nos)
49,000 }
Dynamic port number (Application)
64,000 }

=

FTP : 20
SMTP : 45
HTTP : 80.

various types of objects in computer networking:

* workstations and servers (7 layers)
- L_1 * Hub - 1 (physical layer)
- L_2 * switch - 2 (physical, Data link layer)
- L_2 * Bridge - 2 (PL, DLL)
- L_3 * Router - 3 (PL, DLL, NL)
* Brouter - 3 (PL, DLL, NL)
* Gateway - 7.

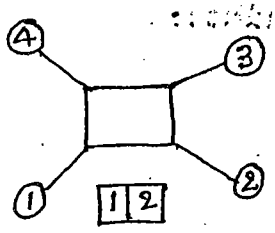
1. work stations and servers:

* 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:

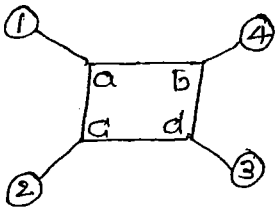
* Network traffic is high.
* causing unnecary distrabance at various systems.

2. 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 disturbances at various locations.
* Because of above two reasons performance is good.



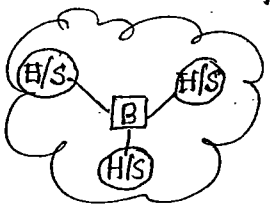
a	1
b	2
c	3
d	4

DisAdv:

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

3. 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

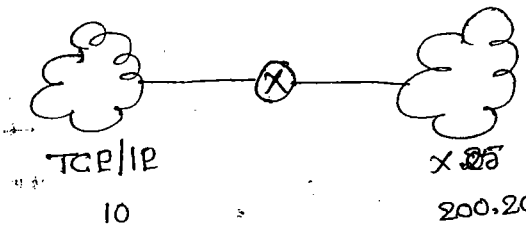
* All routing algorithms are running in a router. so the cost of a router is very high.

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.

System functionality

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

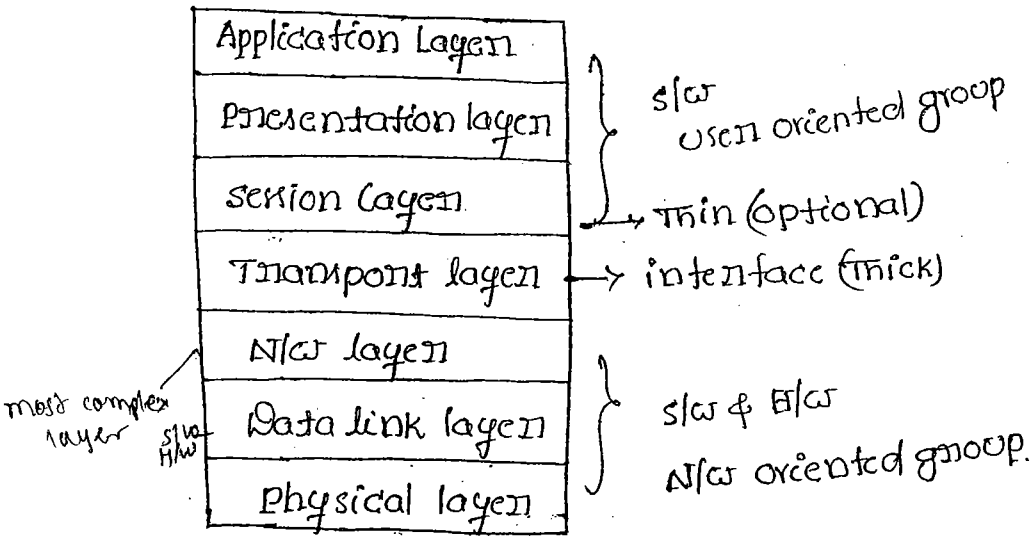
optional
- * compression
- * Encryption
- * Encoding
- * Routers.

Total => 7o functionalies

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

WAN
LAN

To access all these functionality reference model OSI

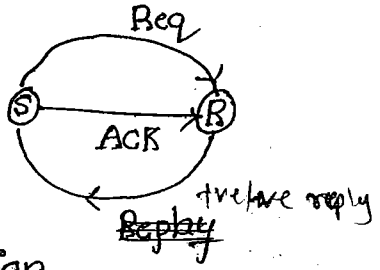


OSI reference model divide the 7o functionalities into 7 individual groups.

connection-oriented & connectionless communication:

connection-Oriented:

Three-way-handshake
1. connection establish
2. Transfer
3. Terminate connection



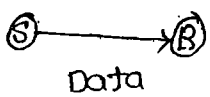
* Reliability is high

if accept => +ve reply

otherwise '-ve'

* Protocol is TCP (Transmission control protocol).

connection-less:



Directly send the data without ack

∴ UDP (User Datagram protocol)

User

AL [Msg]

TL [M | H1] → segment

NL [M | H2] → Datagram

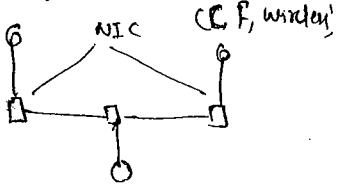
DLL [T1 | | H3] → frame

PL [1- PDU] => Protocol data unit (PDU)

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.

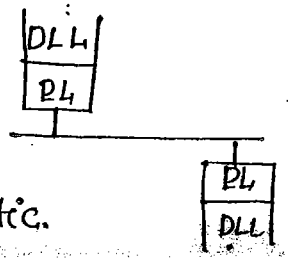


Representation of bits:

C: Electrical (Copper wire)

F: Light signal (Fiber optic)

wireless electromagnetic.



Physical layer converts the digital to electrical and vice versa.

* it defines transmission mode.

→ simplex => Keyboard cable

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

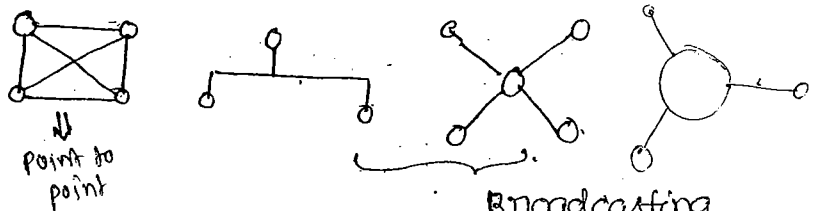
→ Full-duplex => Both can talk simultaneously

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

* 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

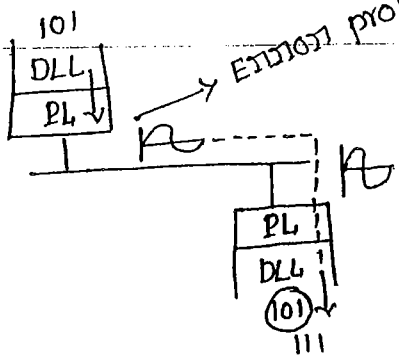
→ Access control

→ framing

→ physical addressing system 48-bit

MAC
Ethernet
LAN
NIC

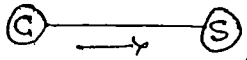
1. Error Control:



Distorded signals when error occurs.

* 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-transmision (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.



10 P/sec 10 sec 3P/sec (capability of server)

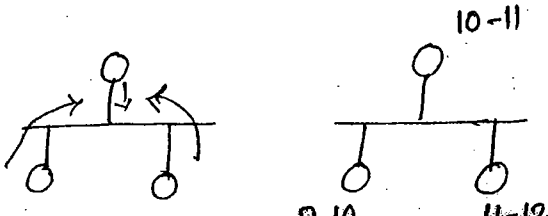
* Based on the server capability client sends the data.

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 collisions occurs.

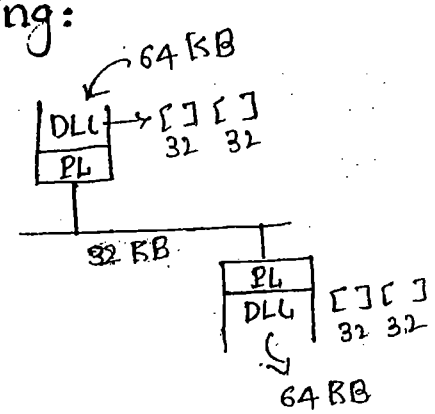


sophisticated accen control mechanisms:

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

* usen can generate any sized data.

Framing:



* Framing - LAN
* Segmentation - WAN

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

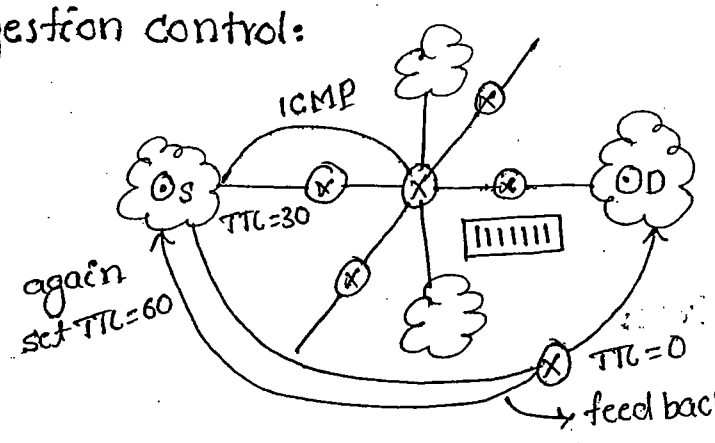
3. Network layen:

Responsibilitey:-

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

ICMP => Internet congestion Message protocol

congestion control:

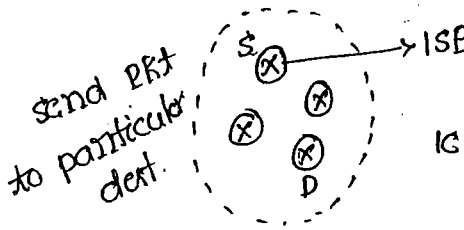


* if the data is full in all the buffens of the routens, then it is as congestion.
* To control congestion, noutens sends the messages to the source to stop transmission of packets by knowing

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.

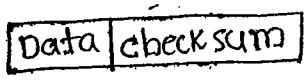
* TL offers end-to-end communication between end devices through a network.
* combining all the different protocols data and sending is called multiplexing.
* These are equally partitioned and sent through the media, at the received side, all these are combined and received which is known as de-multiplexing.

* Error verifications are done by 2 aspects

-> Link level (Datalinklayer)

-> End-to-end (Transport layer)

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



* CRC => check link errors => DLL.
* checksum => check n/w 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 :-

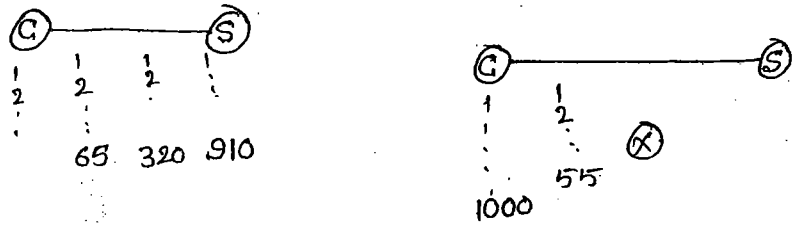
-> virtual connection b/w application entities
-> synchronization of data flow
-> creation of dialog units
-> connection parameter negotiations
-> partitioning of services into functional groups.
-> ack of data received during a session.
-> Maintaining checkpoints / synchronization points
-> Grooping of operations.

-> Token control

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 https 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 user scenario (HTTP & HTTPS back etc. must be main)
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: AL, PRL, SL → AL; TL; NL; DLL, PHL → DLL
→ 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 nlw 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 contrd.
* 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.

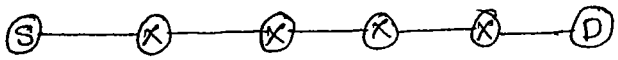
Different types of Delays:

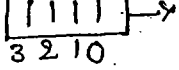
* Queing delay
* processing delay
* Transmission delay
* propagation delay.

* 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:

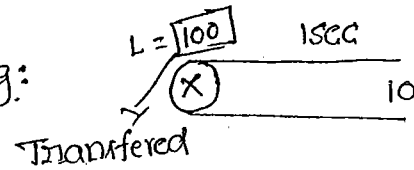
The amount of time taken by router to process a pkt [looking at destination IP, extracting n/w ID, searching in the routing table, identifying destination route] is known as "processing delay".

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

* Transmission Delay: (L/B)

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

Eg:



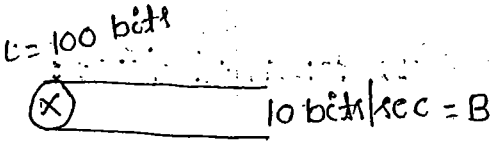
$\therefore L/B = \frac{100}{100} = 1$ sec for sending 100 bits.

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~~

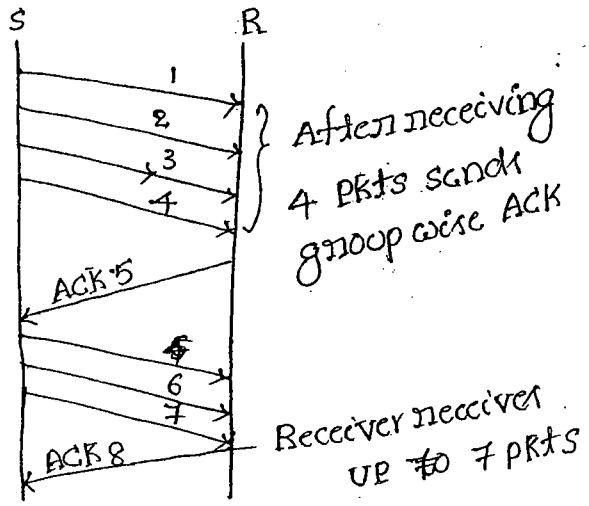
Round Trip Time (RTT) ≅ 2* Propagation delay

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

Time out = 2 * RTT.

TTL = 2 * Timeout

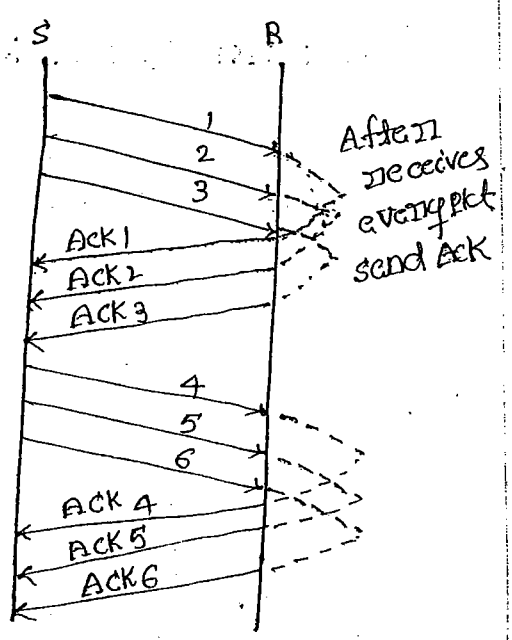
Cumulative:



=> Network traffic is low

=> Reliability is low.

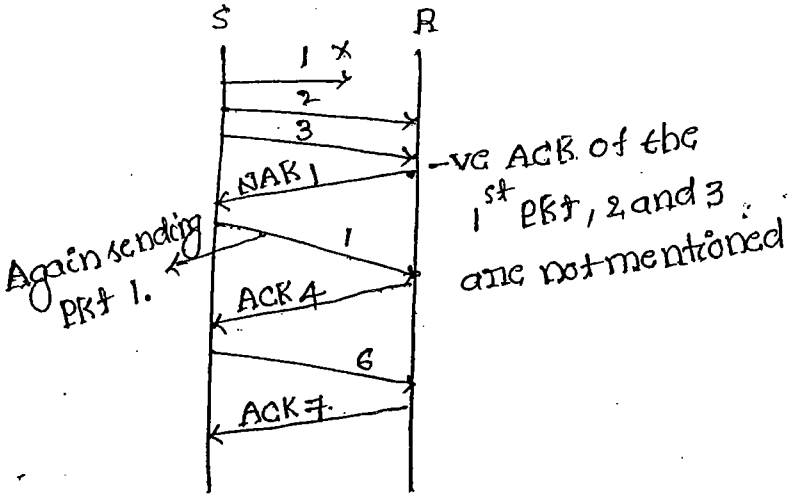
Independent:

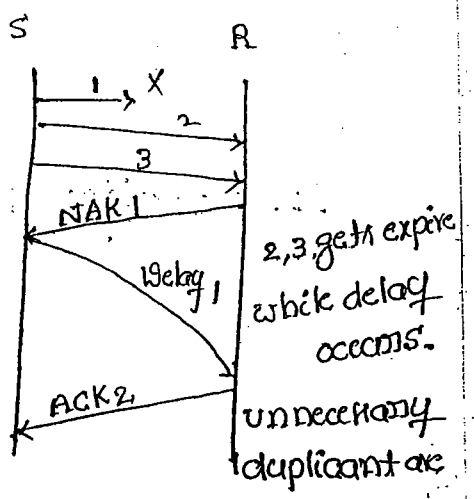


=> Network traffic high

=> Reliability is high.

Case study for commulative:

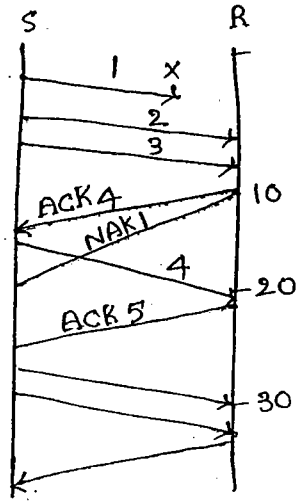




if the delay is high to send pkt 1, then at the time of receiving pkt 1, the packets 2,3 get expired, so again actual packets of 2,3 is sent.

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.

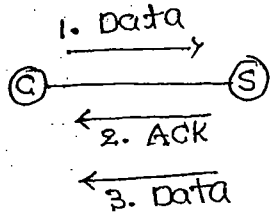
To overcome this problem repeat checking the pkts, improves reliability.

Piggy backing (web):

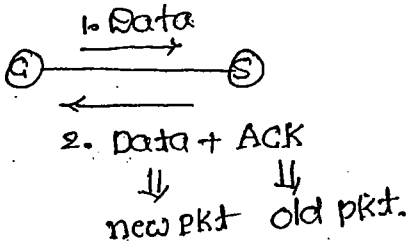
→ Mainly used in web services

→ To reduce the n/w traffic.

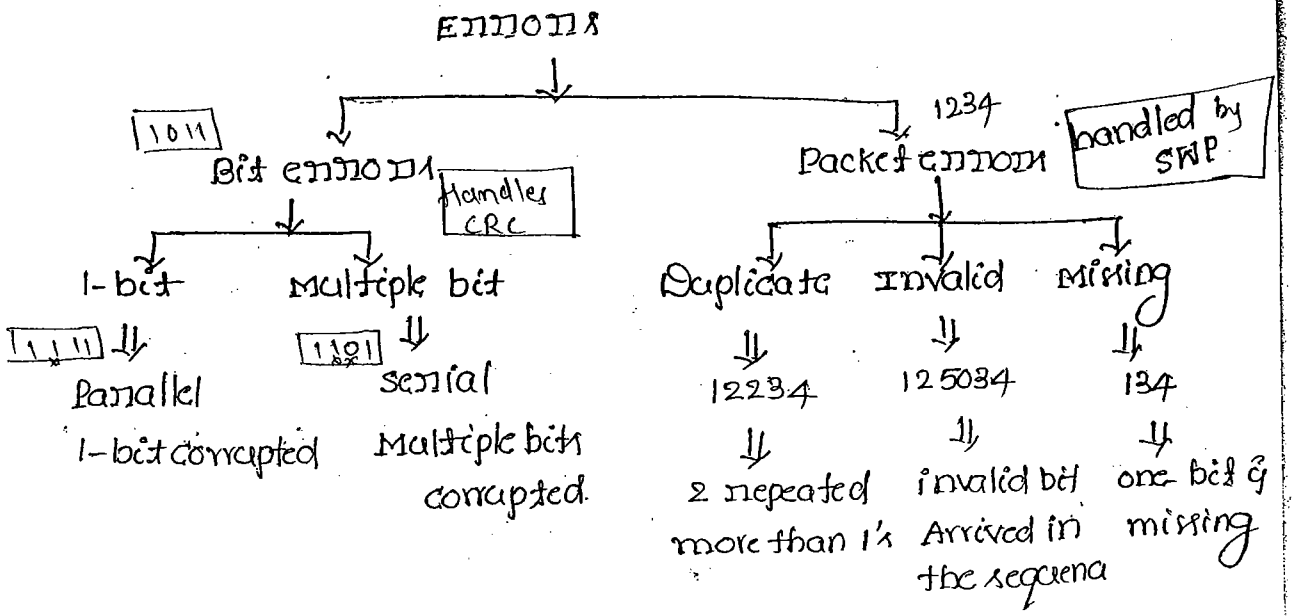
General Approach



Piggy backing:



Different types of errors:



Bit delay duration $= \frac{1}{B}$ B: Bandwidth.

B = 10 bits/msec

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

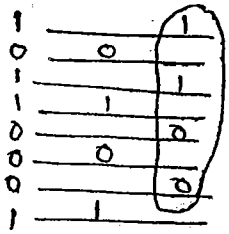
serial data transferred is : 10110001

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

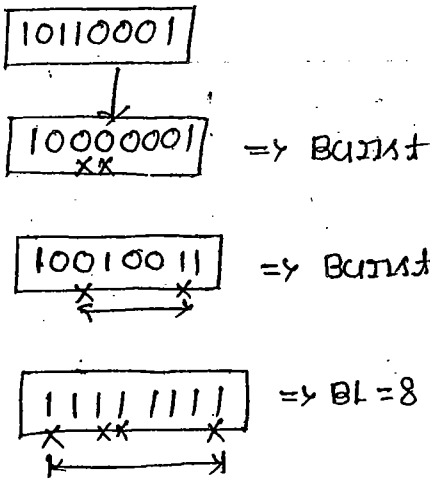
Parallel data transferred:
- 1 - -
- 0 - -
- 1 - -
- 1 - -
- 0 - -
- 0 - -
- 0 - -
- 1 - -

* 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.

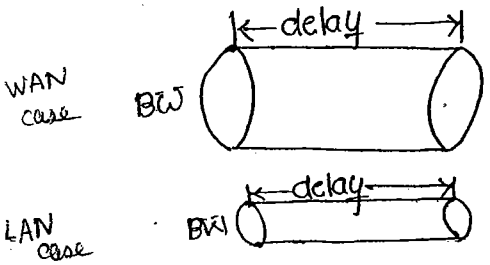


For synchronization and collecting the data bits a group. so for long distances it not support.



* 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:

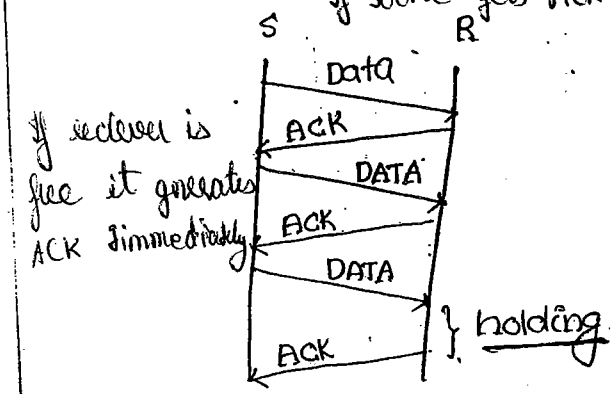


Stop-and-wait protocol:

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:

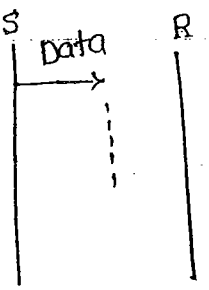
① 

fig: Lost data packet

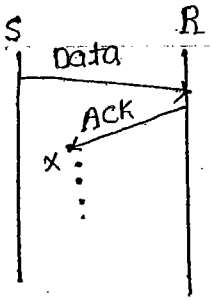
② 

fig: Lost ACK

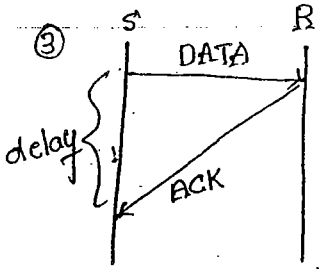
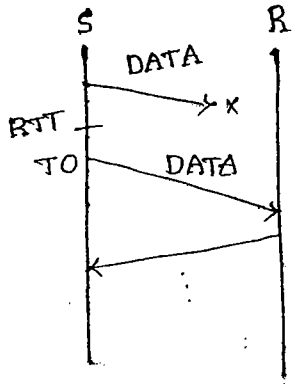
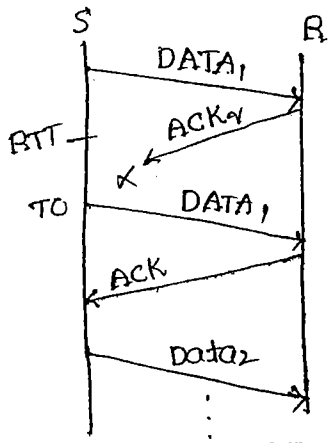
③ 

fig: Delayed ACK.

① 

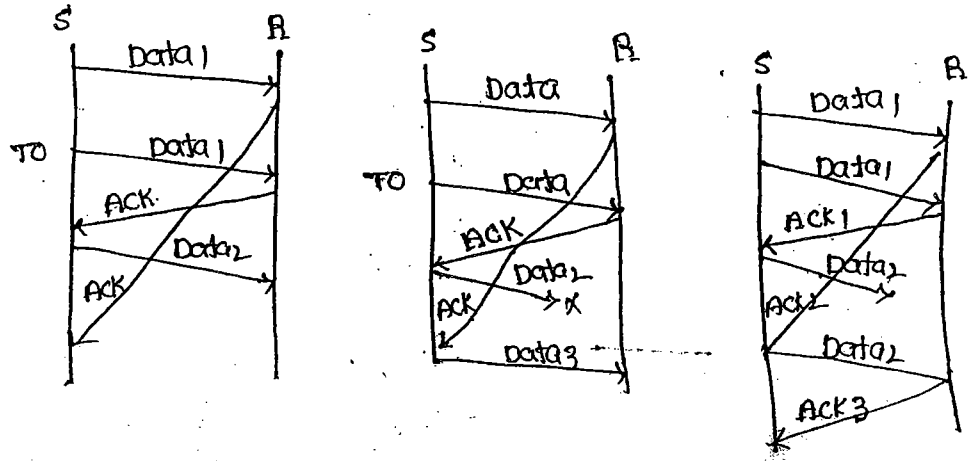
Either the lost data or ACK only the time out is considered. if within the given time ack is not received then next data is sent as represented it by timeout.

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)

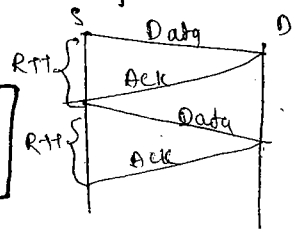
⇓ = Stop & wait ARQ

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

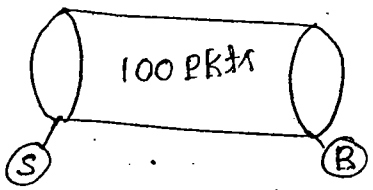
characteristics of stop & wait:

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

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



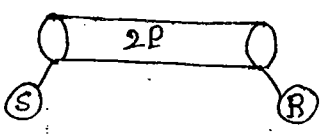
* if Bandwidth x delay product is very high then stop & wait Protocol becomes useless.



capacity = 100 pkts

filling pipe with 1 pkt then

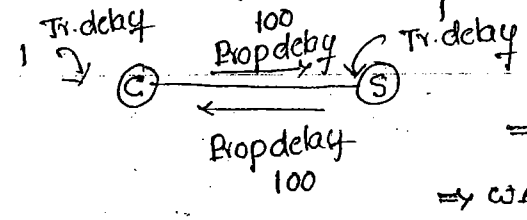
Efficiency = $\frac{1}{100}$ = 1%



⇒ Efficiency = ½ = 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.

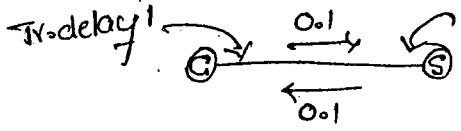
* Transmission delay is 1 mean upto 202 ms only 1 unit of time



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

$\Rightarrow$ WAN

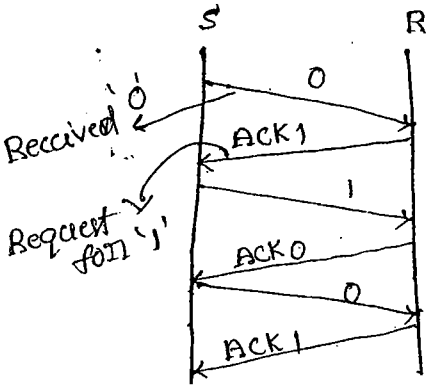
* Transmission delay is high compared to prop.delay



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

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

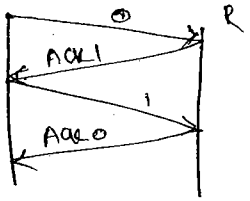
* Stop & wait protocol use only two sequence numbers.



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

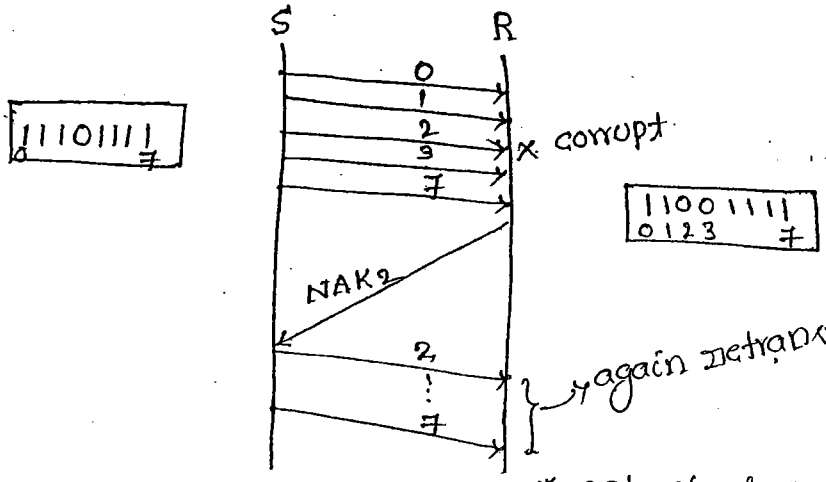
Stop & wait $\Rightarrow$ $S_W = R_W = 1$

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



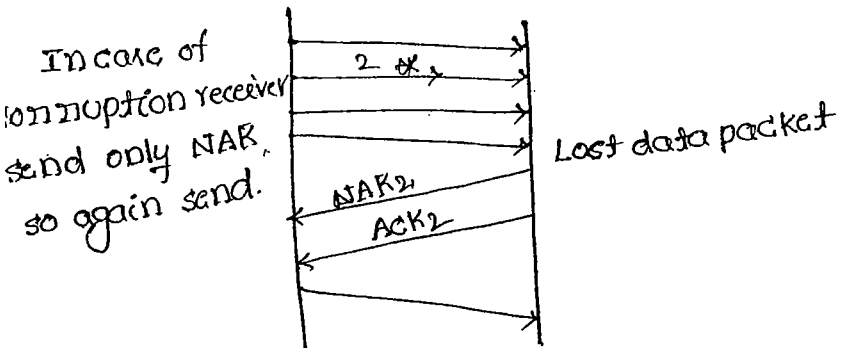
In this series sending packets if Pk_2 is missing and all the seven pkts are being sent then NAK_2 is sent. Then 3 to 7 packets are being discarded. and Pkt_2 is retransmitted

corrupted data packets:

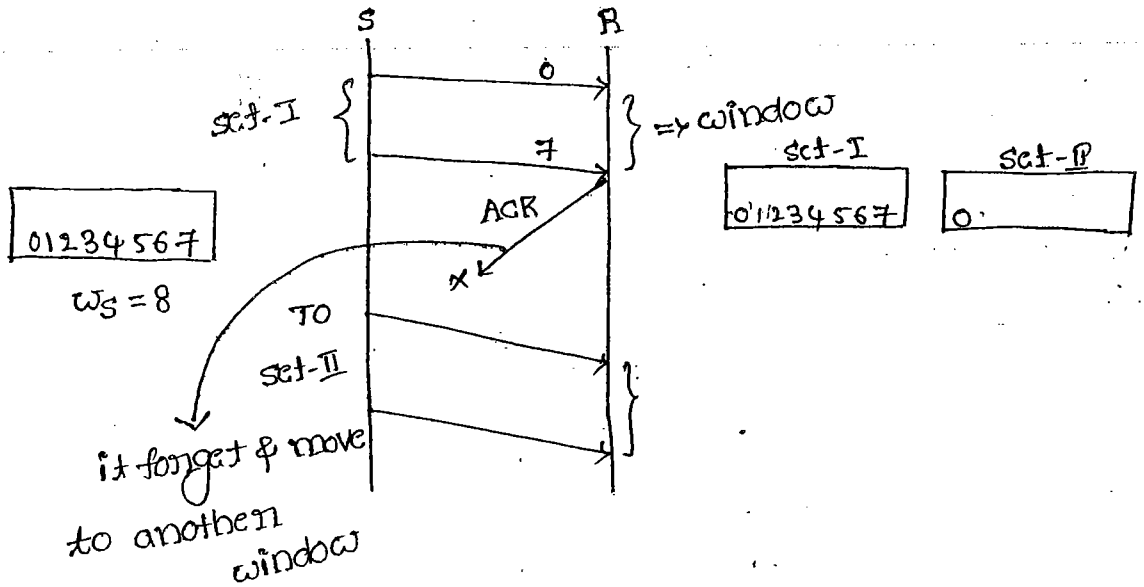


* only the lost packet have more impact that of the corrupted data Packet.

* 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.

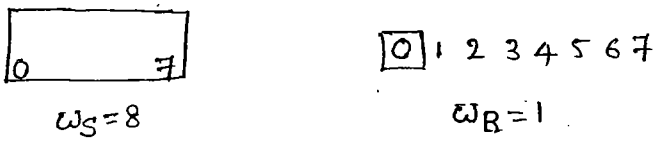


After time out, sender again send first window.

* 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 selecton '0' and if any other num other than 1 comes they are discard.

Case (b) w_S size:

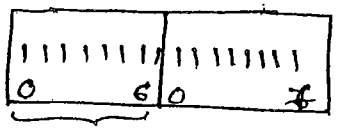
w_S size is calculated based on following formula

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

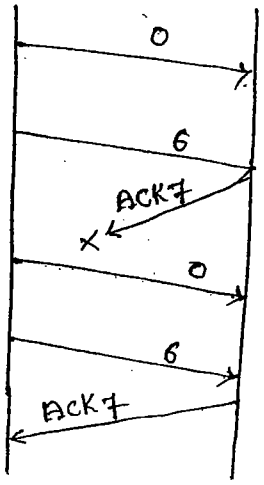
$$w_S = ASN - w_R$$

$$w_S = ASN - 1.$$

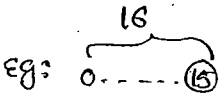
Adjusting window size:



$W_S = 7$



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



Max available sequence num = 16

$W_S = 15$

$W_R = 1$

Eg: Total sequence numbers = 10

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

case(1): Assume N = Max available sequence numbers

$\therefore W_S = N - 1$

$W_R = 1$

case(2): if N is defined as max sequence numbers

$W_S = N$

$W_R = 1$

case(3): if 'k' is no. of bits available in sequence number

$W_S = 2^k - 1$

$W_R = 1$

=

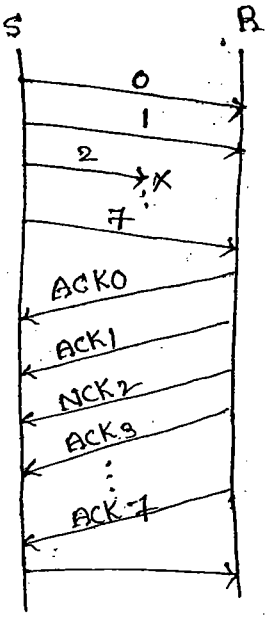
Selective Repeat:

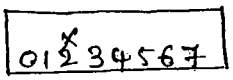
* selective Repeat receiver receives out of order packets.
* it's natural choice is independent ack (if possible, it will also use piggy-backing)

1.

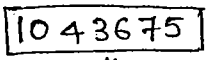
Missed $w_S = 8$

selectively send this packet to receiver.





$w_R = 8$



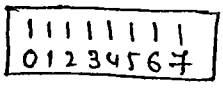
it receives any sequence for checking which pkt is lost it uses searching algor we take more time

* A searching algorithm is used.

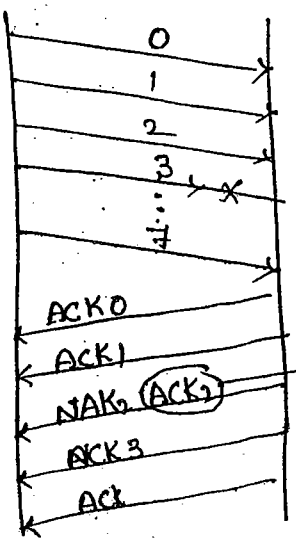
Dis Adv:

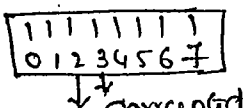
Time increases as it requires searching and sorting of num. of packets to be transmitted explicitly.

② corrupted:



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

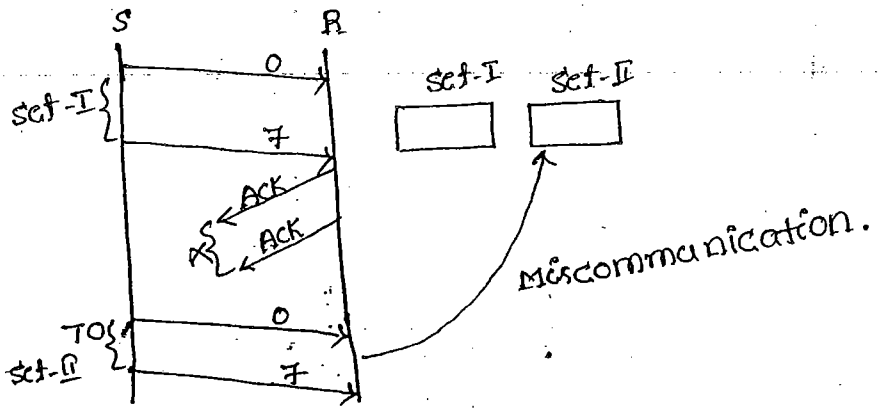




we can not command with sender that which Packet is lost and which is obtained since Ack, is not sent with NAK, which increases

"Ambiguity"

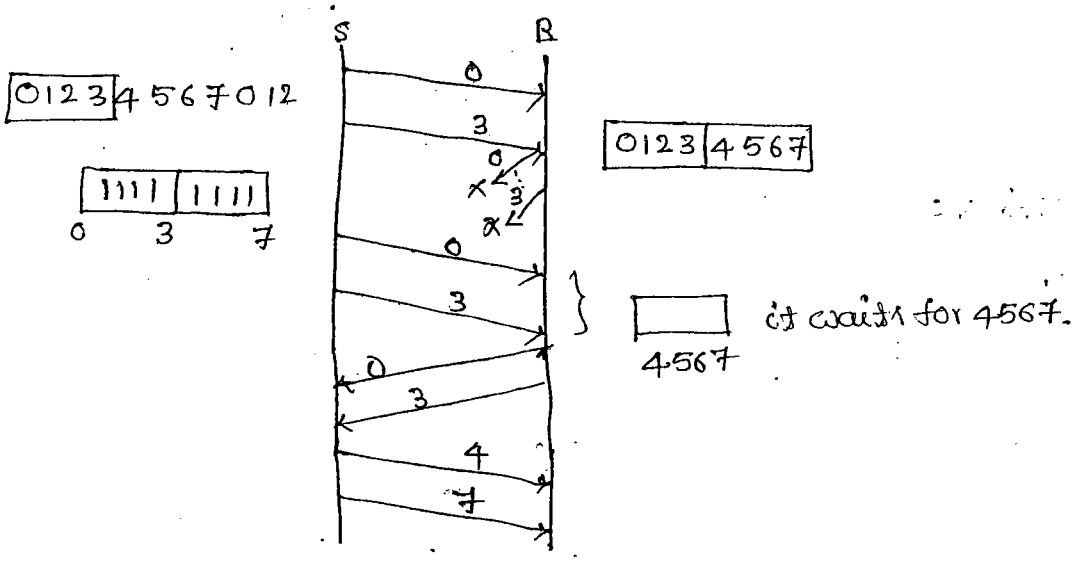
Lost Acknowledgement:



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	Stop&wait	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

Stop&wait formula:

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

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

$$= \frac{1}{1+2a} \quad \therefore a = \frac{T_{\text{Propdelay}}}{T_{\text{Trandelay}}}$$

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

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

$\therefore$ 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" (ω_{bits})
3. $\omega_{PKT} = \frac{\omega_{bits}}{(PKT\,size)_{bits}} = \omega_p$
4. sequence number required = ω_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

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

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

$= 0.121$

$= 12.1\%$

$= 12.1\%$

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 msec

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

(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 msec

$$T = \frac{1000 \times 8}{95.2 \times 500\ msec} = \frac{80\ mbps}{500} = 0.16\ mbps$$

=

(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 = 4Kbps

Propagation delay = 20m/sec

$\eta = 50\%$

RTT = 2 * propagation

= 40msec

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

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

= 160 bps

⑤ Propagation delay = 100 μs

d = 20 KM

L = 1KB = 1024×8

B = ?

RTT = Transmision delay

RTT = 200 μs

Transmision delay = L/B

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

= 40 mbps

⑥ B = 1Mbps

latency delay (or) propagation delay = 1.25 sec

L = 1KB

1. RTT = 2×1.25

= 2.5 sec

2. 1 sec 1×10^{6} bits

2.5 sec ?

$w_{bits} = 2.5 \times 1 \times 10^{6} \Rightarrow 2.5 \times 10^{6}$

3. $w_p = \frac{w_{bits}}{(Pkt\ size)}$

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

= 305. $\therefore K = 9$

4. Sequence num = w_p = 305

⑧

Gate: window size = 5 packets

Data packets = 1000 bytes

Transmission time for such packets = 50 µs

Propagation delay = 200 µs

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

RTT = Tr.delay + 2 * propagation

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

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

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

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

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

$=$

(9)

3960	40

S ——— R

100 × 3960 | 100 × 40 (H) | 40 (NAK)

396000 | 3960 + 40 (Retrans) | 8040

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

(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.

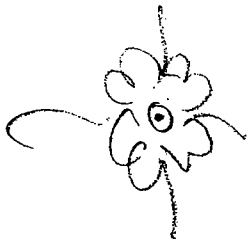
$t=1$, 0 arrives at B, ack, is made, meanwhile, 1 starts leaving "R" therefore 2 & 3 are in the Queue.

$t=2$, ack_1 arrives at R and then at A. Therefore 4 is released from A and immediately available at R. meanwhile arrives at B Hence ACK_2 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.

=



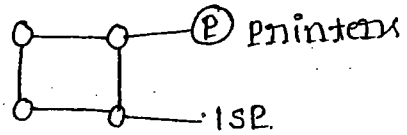
S. Konda Reddy

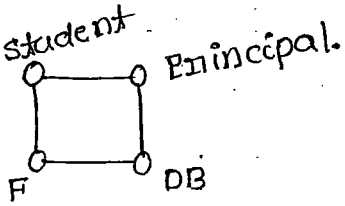
=

Lan Technologies

Advantages of LAN:

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





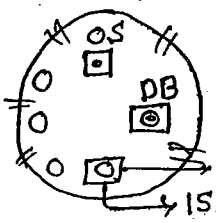
Types of LANs:

* 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 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 types of users there are some restrictions to some user to accer 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

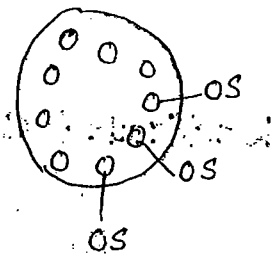
workgroup s/w ⇓ Peer-to-peer server LAN.

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.

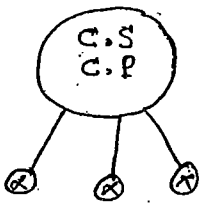
At the most we get 2-serial
2-parallel
4 USB ports so it has <10 systems

* No realtime application, and oracle application are possible.

LAN components:

1. Network operating system.
2. Cable
3 NIC

1. First generation

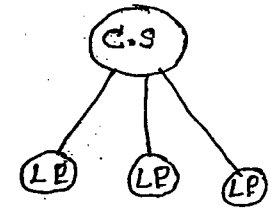


CPU ✗
HDD ✗

Eg: UNIX.

C.S = Central storage

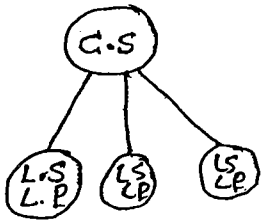
2. second generation



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.

User

↓

NOS

↓

HDD

NOS

↓

NIC

↓ server

2. Cable : Types of cables

10	base	2
10	base	5
100	base	T
100	base	F
10	base	36

→ distance (* 100 mts)

Bandwidth — Technology

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 ex use repeators.

0 —— [R] —— 400.

repeater

* 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 + DLC => (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 layers 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.

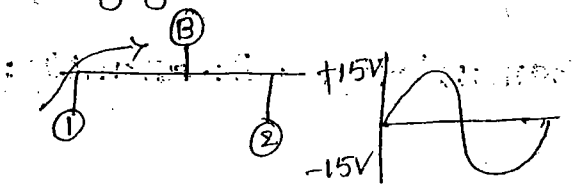
Ethernet

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)

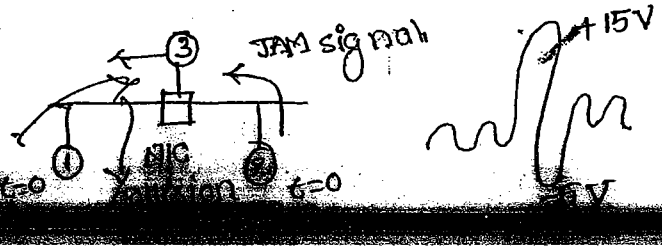


Multiple Access:

* 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".

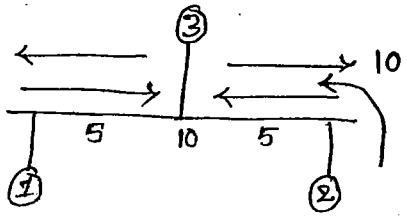
Collission Detection:

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 channel have different frequency => Bandwidth increases.



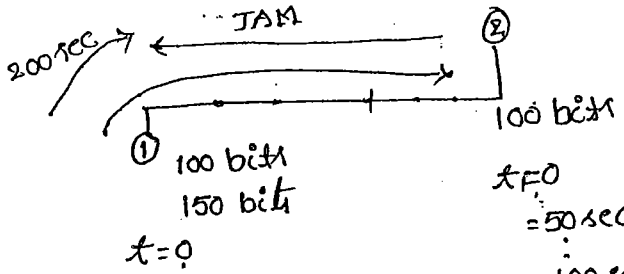
Minimum =20

100 | t=0 : =5 : =10

10 | 9 × | t=0 : =5 : =10

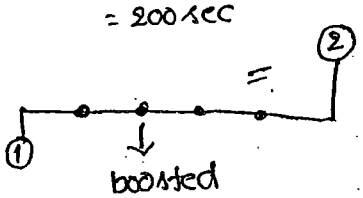
S_1 system have 100 bits, S_2 have 10 bits assume that they take the channel at a time then collision occurs. for recognizing collision, every system maintains min. frame size based on channel length.

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



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

t=0 : =50 sec : =100 sec



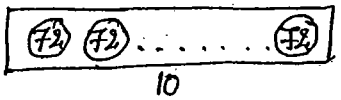
Repeators are allowed.

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

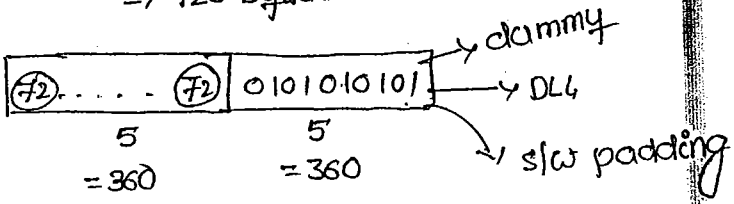
$57.6\ \text{msec} = \frac{L}{10 \times 10^6}$

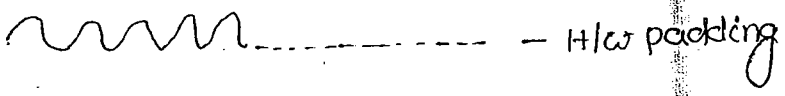
Basic Ethernet	Fast Ethernet	Gigabit Ethernet
10 mbps	100 mbps	1 Gbps
2500 mts	250 mts	250 mts
72 byts	72 bytes	72 bytes.

Basically 25 mts
720 bytes



=> 720 bytes





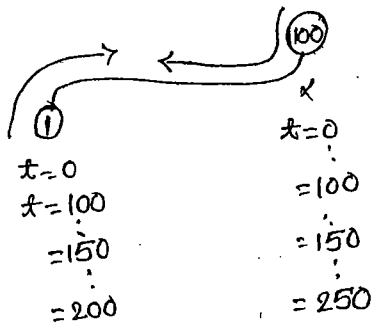
Backoff Algorithm:

it gives waiting time for stations that are involved in collision

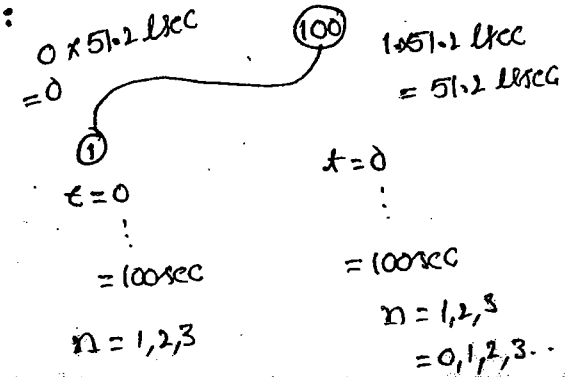
$$\text{waiting time} = K \times 51.2\ \mu sec$$

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

where n - collision number.



Case study:



Let $n=1$ | Let $n=1$

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

$\Rightarrow 0$ to $2-1$ | $\Rightarrow 0,1$

$\Rightarrow 0,1$

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

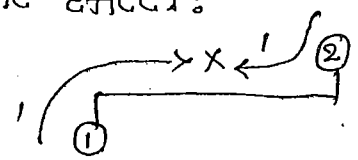
$= 0$

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 $n=1$ | Let $n=1$

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

$= 0,1$ | $= 0,1$

Then $\omega T = 0 \times 51.2$ μsec | $\omega T = 1 \times 51.2$ μsec

$= 0$ | $= 51.2$ μsec

$n = 2$ | ⇓

$K = 0$ to $2^n - 1$ | if after 51.2 μsec again another channel also wants to access the medium, then again backoff algorithm is applied then $n=2$

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

$= 0,1,2,3$

Then repeat same for $n = 3$

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

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

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

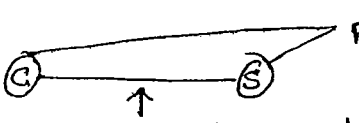
①		100		1		100	
01		0123		01		01234567	
0		0		0		0	
0		1		0		1	
0		2		0		2	
0	1/8	3	1/8	0	1/16	3	1/16
1		0		0		4	
1		1		0		5	
1		2		0		6	
1		3		0		7	
5/8				1			
				1			
				1			
				1			
				1			
				1			
				1			
				1			
				13/16			

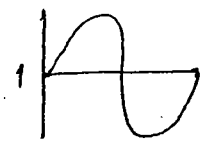
Data specifications:

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

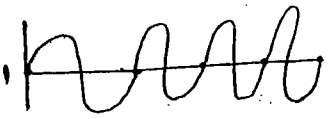
② signal
Manchester encoded signal

③ Addressing system
48-bit physical address.

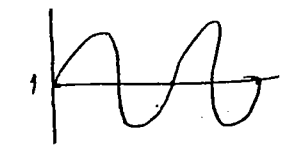




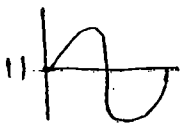
=> Baud = 1 x bit



Baud = 4 x bit



Baud = 2 x bit



= 1/2 bit

Ethernet:

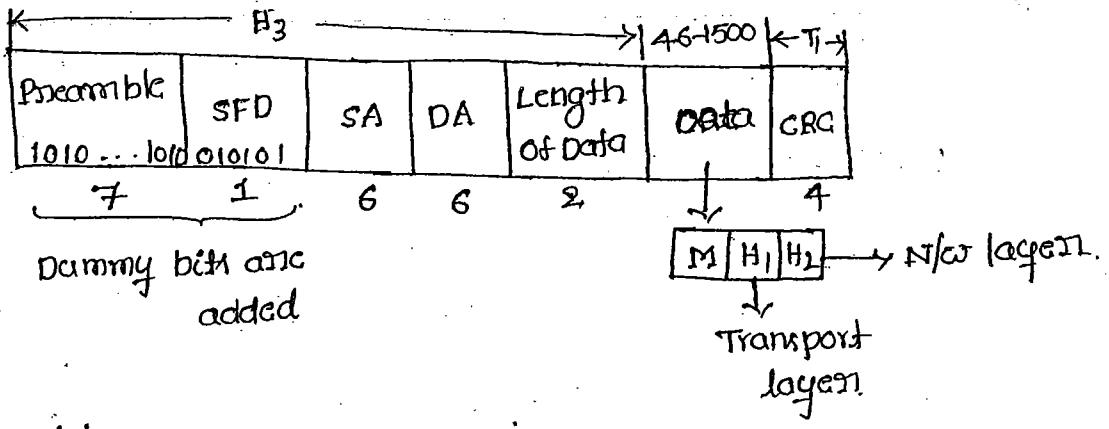
For a 10 mbps ethernet

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 (6) 10101010 (6)

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 monopolisation 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:

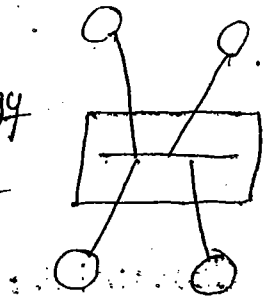
since data is varying from 46 to 1500 to keep track correct size of the data in packet we need "length of data field

CRC:

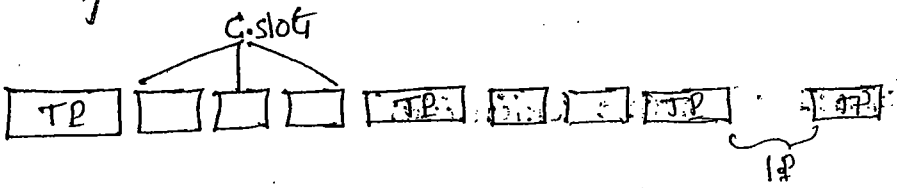
* it is added only at the tail to identify bit errors
* To avoide more no.of tranmissions we use CRC at tailend.

Implementation:

Physical Addrering - 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 tranmission 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 succes 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. $$\eta = \frac{TP}{TP + CP} = \frac{t_{trans}}{t_{trans} + 2t_{prop} * e}$$

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

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

2. $$\eta = \frac{T_t \cdot P}{T_t \cdot P + C \cdot P + t_{prop}}$$

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

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

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

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

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

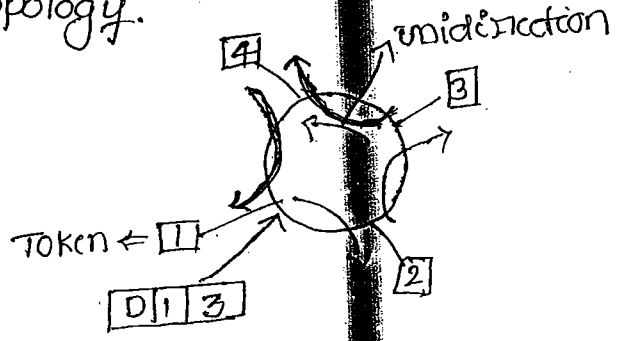
  eg: interactive application needs 1 or 2 bytes.

  eg: ATM.

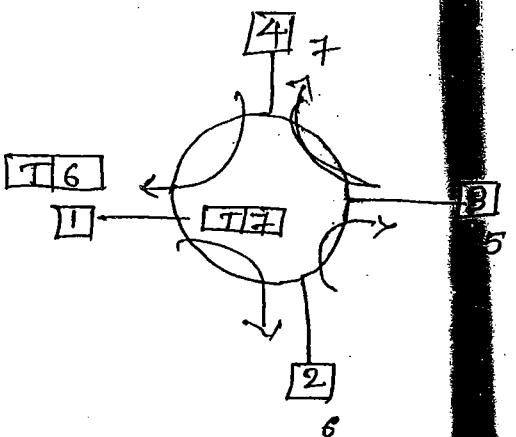
* If load increases, efficiency decreases.

TOKEN RING

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



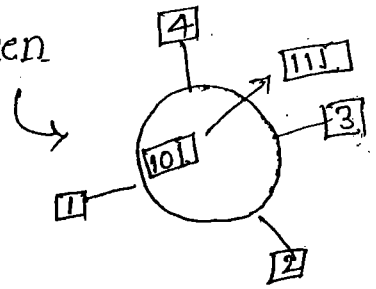
* Token is maintained at one station only then the data is sent to the other station, where it checks for source & destination. if same then it copies only and then sent the original data to other, Therefore there is no collision.
* if any station have high priority than the token or equal then it can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



Problems with Token Ring:

1. (A) Vanished Token

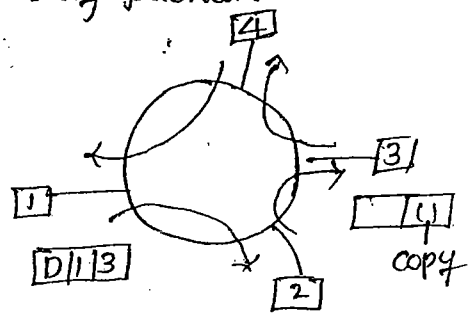
   (B) corrupted token



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

   A. Orphan packets

   B. Stray packets



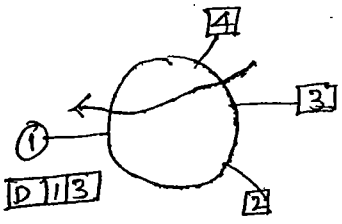
Orphan pkts => source trash rotate upto a time

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:

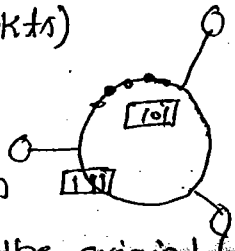


   A. safe operation

   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

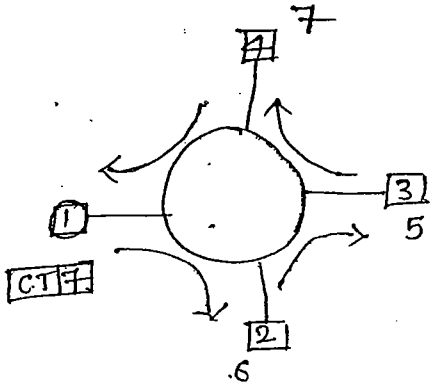
To overcome Token ring problems we have the following

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

* Monitor 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 crocesses a monitor station it makes a error stamp on it stamped pkts are not allowed.

3. Stray:

checking the validity of pkt while entering the monitor station.

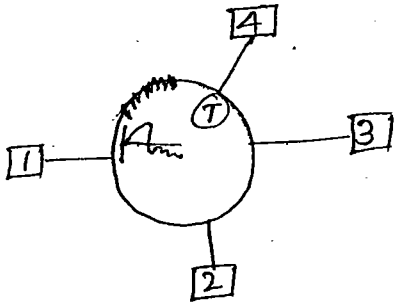
3. Destination:

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



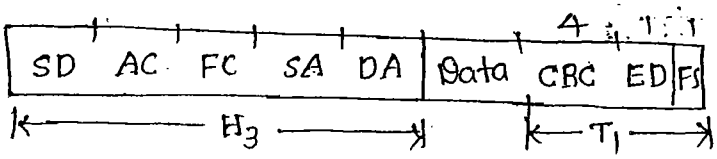
* A special frame is sent by monitor station for every 10 sec saying that it is available, if any frame is not received then it is assumed that monitor is crashed and there is a change of other stations to become a monitor station.

Specifications of Token Ring:

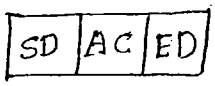
1. Data rate
   - * 4 Mbps
   - * 16 Mbps
2. signal : DME
3. Addressing system : 48-bit physical Address.

Frame format:

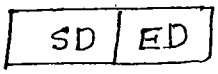
1. Dataframe



2. Token frame



3. Abort frame



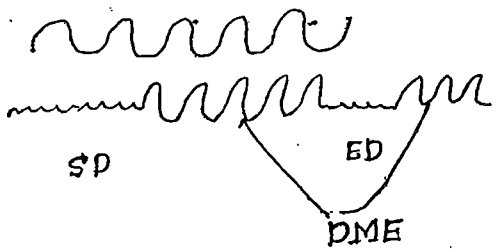
Start Delimiter, End Delimiter } used to indicate two extreme ends of the packets.

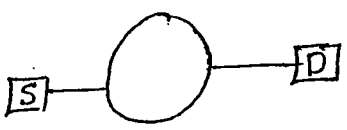
* They use DME signals.

SD : 10JK 10JK → other signal except DME

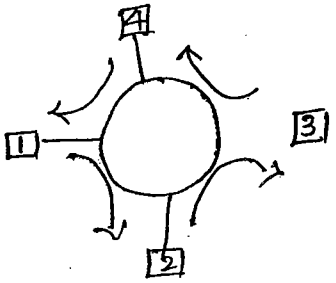
ED : 11JK 11JE → Error bit

↓ information bit.





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



if E=1 then it simply transiten

P	T	M	R

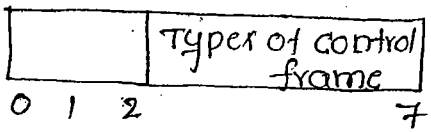
M => Monitor bit

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

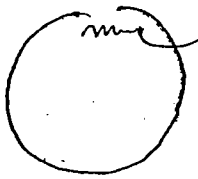


00 – Data
11 - control.

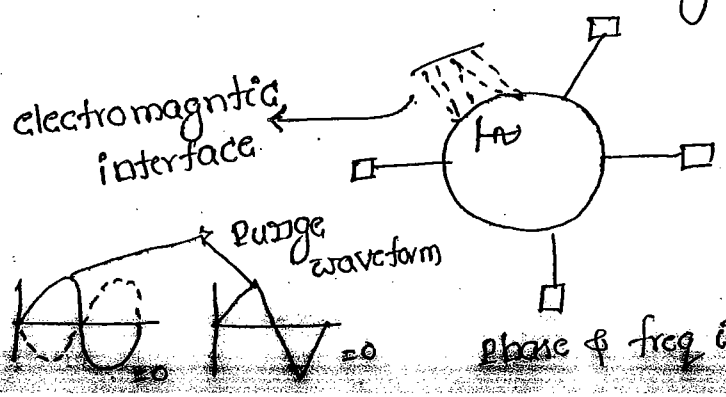
1. Client token: it is used in the election process of monitor.

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

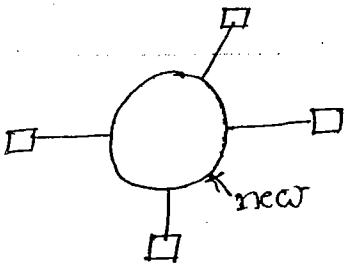
3. Becon: it is used to identify major cut in the ring.



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



5. Duplicate Address test frames:



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

⇓

new channels address.

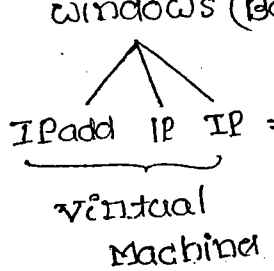
⇓

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

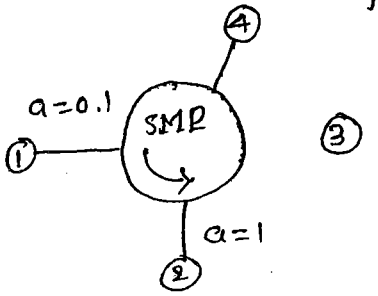


⇒ virtual physical address of virtual machines.

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

6. SMP (Standard by Monitor preserve):

it is used to carryout neighbour identification.



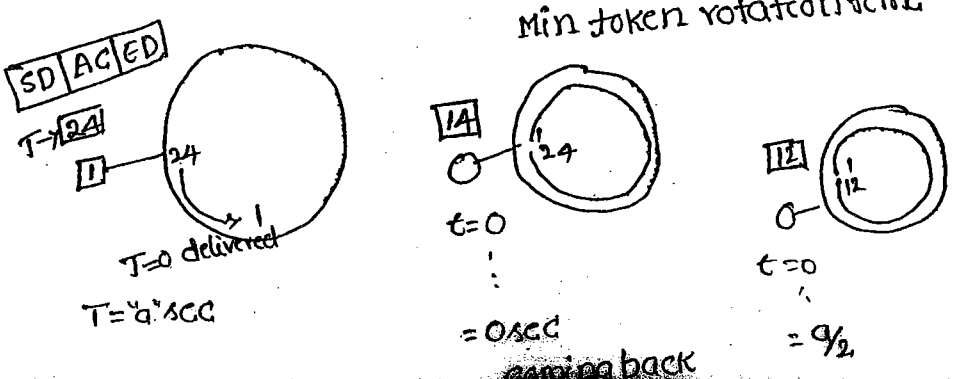
Upstream: From whom the channel receives the data packet.

Downstream: To whom the

Modes of operation:

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

Calculation of minimum size of token ring:



T_{prop} = "a" sec = trans. delay

$T_{prop} = T_{trans} \Rightarrow \frac{T_{prop}}{T_{trans}} = 1$

$\frac{T_{prop}}{T_{trans}} = 1 \Rightarrow$ min.

$> 1 \Rightarrow$ Max

$< 1 \Rightarrow$ overlap.

* Token rings used for big networks.

* Token ring: **propagation delay = Transmission delay**

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

Eg: $V = 2 \times 10^8$ m/sec

$L = 24$ bits

$B = 4$ mbps

$d = ?$

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

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

$= \frac{24 \times 2 \times 10^8}{4 \times 10^6}$

$d = 1.25$ km.

Eg: if Bandwidth of ring is 10 mbps, & frame size 200 bits velocity = 2×10^8 m/sec find min size token ring

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

$= \frac{200 \times 2 \times 10^8}{10 \times 10^6}$

$= 4000$ km.

=

Ring latency = Min TRT = Propagation delay in the ring
+
no. of active stations * Delay at each station

Propgation delay = $\frac{d}{V} + mb$
($\frac{d}{V}$: sec, mb : bits)

Bid delay $b = 1/B$

d = Total length of ring
B = bit delay at each station
V = Velocity propagation
R = bandwidth of ring
L = latency.

$$L = \frac{d}{V} + \frac{mb}{R} \text{ sec}$$

$$RL = \frac{dR}{V} + mb \text{ bits}$$

Various Token re-insertion strategies:

Delayed Token strategies	Early Token strategy.
* Token is released after getting entire data packet.	* Token is released after data is transferred.
* Efficiency is low	* Efficiency is high
* Reliability is high	* Reliability is low.
* it is used under 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
b → Ring latency
c → Token Transmission time.
d → propagation delay b/w station.

Problems:

① $d = 2500$ mts

$V = \frac{60}{100} \times 3 \times 10^8$ m/sec

$B = 10$ mbps

$L = ?$

RTT = Transmission delay

$2 \times \frac{d}{V} = L/B$

$L = 2 \times \frac{d}{V} \times B$

$= \frac{2 \times 2500 \times 10 \times 10^6}{1.8 \times 10^8}$

$= 277$ bits.

④

② $B = 1$ Gbps

$d = 1$ Km

$V = 200{,}000$ Km/sec

$L = ?$

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

$L = 2 * \frac{1}{200{,}000} \times 1 \times 10^9$

$= 10{,}000$ bits or 1250 bytes.

⑤

③ $B = 10$ Mbps

Propagation delay $= \frac{d}{V} = 225$ bit times

Bit delay $= b = 1/B = \frac{1}{10 \times 10^6} = 0.1$ usec

Transmission can be considered as either 1 bit delay or 0.1 usec

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 propagation

Assume 'A' started producing jam signal.

∴ At $t = 273\ (225+48)$, A finishes producing jam signals

⇓

Jam.

④

⑤ $B = 10$ Mbps

slot time = 51.2 μsec

$L = 512$ bytes

No. of slots = 1.716

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

Transmission time = L/B

$$= \frac{512 \times 8}{10 \times 10^6}$$

$$= 40 \text{ msec}$$

C.P = no. of slots * slot time

$$= 1.716 \times 51.2$$

$$= 87.8 \text{ μsec}$$

$$\eta = \frac{40 \times 10^{-3}}{40 \times 10^{-5} + 87.8 \times 10^{-6}}$$

$$=$$

(6) $B = 10$ Mbps

$d = 2.5$ km

$v = 2.3 \times 10^8$ m/sec

$L = 128$ bytes $\Rightarrow$ 98+30

overhead = 30 bytes

$$\eta = \frac{1}{1+6.44a} = \frac{1}{1+6.44(0.10)} \quad \because a = \frac{T_{prop}}{T_{tran}} = \frac{1.086 \times 10^{-5}}{1.024 \times 10^{-4}} = 0.10$$

$$= 57\%$$

$$T_{prop} = \frac{d}{v} = \frac{2.5 \text{ km}}{2.3 \times 10^8} = \frac{2.5 \text{ km}}{2.3 \times 10^5 \text{ km/sec}} = 1.086 \times 10^{-5}$$

$$T_{tran} = \frac{L}{B} = \frac{128 \times 8}{10 \times 10^6} = 1.024 \times 10^{-4}$$

(7) $B = 4$ Mbps

Token holding time = 10 msec

4 bits — 1 sec — 4×10^6

? — 10 msec — 10 msec — ?

longest frame = $4 \times 10^{+6} \times 10^{-3}$

= 4 Kbps.

(8) $R = 4$ Mbps

$m = 20$

$d = 20 \times 100$

$b = 2.5$ bits

$v = 2 \times 10^8$ m/sec

$$RL = \frac{dR}{v} + mb$$

$$= \frac{20 \times 100 \times 4 \times 10^6}{2 \times 10^8} + 20 \times 2.5$$

$= 90$ bits

$R = 16$ Mbps

$m = 80$

$$RL = \frac{dR}{v} + mb$$

$$= \frac{80 \times 100 \times 16 \times 10^6}{2 \times 10^8} + 80 \times 2.5$$

$= 840$ bits

(10)

(11)

A. Ean

B. Ack

(10) Station = m

$d = m \times 100$ $\quad V = 2 \times 10^8$ m/sec $\quad$ Transfer time $= \frac{L}{B} = \frac{1250 \times 8}{25 \times 10^6}$

$= 400$ μsec

$b = 8$ bits

$L = 1250$ bytes

$R = 25$ Mbps

$RL = \frac{d}{V} + \frac{mb}{R}$ sec

$= \frac{m \times 200}{2 \times 10^8} + \frac{m \times 8}{25 \times 10^6}$

$= m\left(\frac{200}{2 \times 10^8} + \frac{8}{25 \times 10^6}\right)$

$\frac{RL}{\text{Tr. time}} = 1$

$3.33 \times 10^{-3} m = 1$

$m = 300$

1 sec → 25×10^6

? $\quad 1250 \times 8 \Rightarrow \frac{1250 \times 8}{25 \times 10^6} =$

(11) $m = 32$

$L = 1000$ bit packet

$B = 10$ Mbps

latency/adapter = 2.5 bit

$d = 50$ mtr

$V = 2 \times 10^8$ m/sec

Data transmission $= a = \frac{L_D}{B}$

$= \frac{1000}{10 \times 10^6} = 10^{-4}$

$b = RL = \frac{d}{V} + \frac{md}{R}$ sec

$= \frac{32 \times 50}{2 \times 10^8} + \frac{32 \times 2.5}{10 \times 10^6}$

$= 880 \times 10^{-8}$

A. Early Token = $(a + c + d)$ sec

$= 10^{-4} + 24 \times 10^{-7} + 25 \times 10^{-8}$

$= 10$ msec

Token transmission $= c = \frac{L_T}{B} = \frac{24}{10 \times 10^6}$

$= 24 \times 10^{-7}$

Propagation delay $= d = \frac{d}{V}$

$= \frac{50}{2 \times 10^8}$

$= 25 \times 10^{-8}$

B. Delay token = $(a + b + c + d)$ sec

$= 10^{-4} + 880 \times 10^{-8} + 24 \times 10^{-7} + 25 \times 10^{-8}$

= 11 msec

2) it is heavily loaded, we suppose to use early token strategy

$C.T = a + c + d$

$a = \frac{LD}{B} = \frac{256}{10 \times 10^6} = 2.56 \text{ usec}$

$d = 1 \text{ km}$

$B = 10 \text{ Mbps}$

$L = 256 \text{ bit}$

$c = \frac{LT}{B} = \frac{8}{10 \times 10^6} = 0.8 \text{ usec}$

bit delay = 8 bits

$d = \frac{200 \text{ m/usec}}{2 \times 10^8 \text{ m/sec}} = 1 \text{ usec}$

Propagation speed = 200 m/usec

$C.T = 26.5 \text{ usec}$

26.5 usec $\Rightarrow$ 224

1 sec $= \frac{224}{26.5 \times 10^6} = 8.5 \text{ Mbps}$

$\eta = \frac{8.5}{10} \times 100 = 85\%$

3) $d = 200 \text{ km}$

$B = R = 100 \text{ Mbps}$

$V = 200{,}000$

$L = 1024 \text{ bytes}$

$a = \frac{LD}{B} = \frac{1024 \times 8}{100 \times 10^6} = 81.24 \text{ usec}$

$b = RL = \frac{d}{V} + \frac{mb}{R} \text{ sec} \quad \left(\because \frac{mb}{R} = 0\right)$

$= \frac{200 \text{ km}}{200{,}000} = 1 \text{ msec}$

$c = \frac{L_{TOKEN}}{B} = \frac{24}{100 \times 10^6} = 0.24 \text{ usec}$

$d \Rightarrow$ not given ignore

$C.T = a + b + c$

$= 81.24 \text{ usec} + 1 \text{ msec} + 0.24 \text{ usec}$

$= 1.08 \text{ msec}$

1.08 msec — 1024×8 bit

1 sec — ?

$= \frac{1024 \times 8}{1.08 \times 10^{-3}} = 7.6 \text{ mbps}$

$\eta = \frac{7.6 \text{ mbps}}{100 \text{ Mbps}} \times 100 = 7.6\%$

(14). propagation speed = 200 m/μsec

B = 1 Mbps

bit delay = $1/B = \frac{1}{1 \times 10^6}$ = 1 μsec

1 μsec ⟹ 200 mts

B = 40 Mbps Bit delay = $1/B = \frac{1}{40 \times 10^6}$ = 0.025 μsec

1 μsec – 200 mts

0.025 μsec – ?

⇒ 200 × 0.025

= 5 mts.

(15) B = 5 Mbps

Propagation speed = 200 m/μsec

bit delay = $\frac{1}{5 \times 10^6}$ = 0.2 μsec

1 μsec – 200 mts

0.2 μsec – ?

⇒ 200 × 0.2

⇒ 40 mts.

=

c_2

b *

c *

a *

c_1

a *

log

x

$\frac{1}{x}$ *

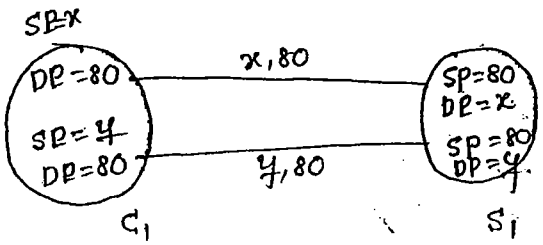
$\frac{1}{x}$ *

Transmission Control Protocol.

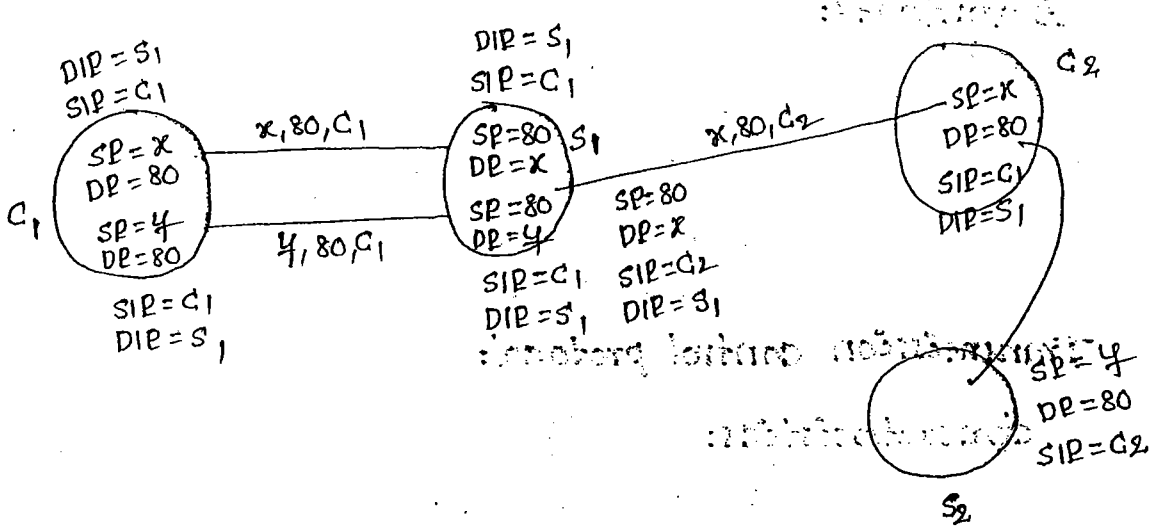
why we call network as TCP/IP networks

(or)

Relationship between TCP & IP.



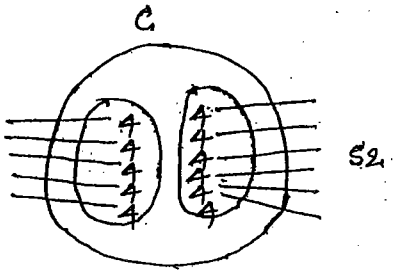
* ctrl + N => another connection
* while establishing a new connection source port & destination Port is addressed.
* server can handle more no.of clients, so introducing a new client involves both source port and destination port.



* In order to differentiate the destination IP address either for server1 (or) server2, the DIP addressed. where "80" represent the http and SIP represents the user's own 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 [illegible]

4 parameters { source port, Destination port, source IP, Destination IP.

Socket:



* socket is a logical component 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:

* Resource utilization
* Maintainance & Administration

→ Allows certain num-of connections for socket.

Transmission control protocol:

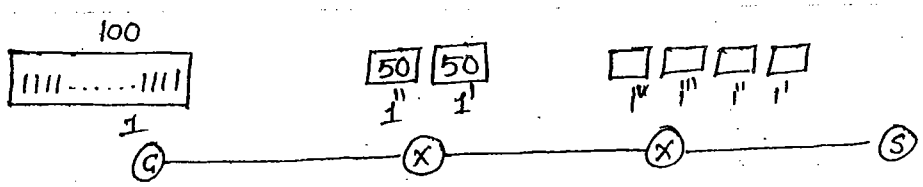
characteristics:

* it is reliable, byte oriented, point-to-point, transport layer protocol.

connection-oriented.

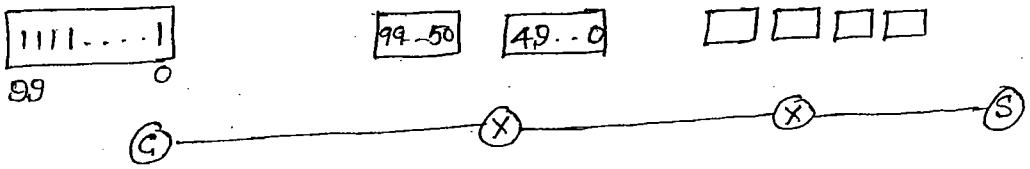
* Message oriented (UDP)
* Packet oriented (SWP)
* Byte oriented (TCP)
* Bit-oriented (HDLC).

Byte-oriented (TCP) / stream oriented



Burden on intermediate routers.

* The bits are splitted by half to 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 packet)



* The above problem can be overcome by not splitting the bits but just only dividing the ~~station~~ stream of bits and transfer so it has no burden on the intermediate routers.

* since the bits are transferred as byte (or) a stream, the TCP is considered as "stream oriented."

* TCP uses "cumulative acknowledgment".

* The connections are "full duplex". Therefore it is having two half-duplex connections.

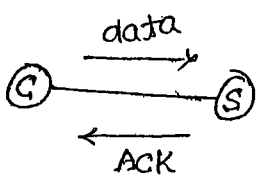


fig: full duplex

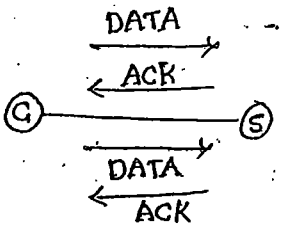
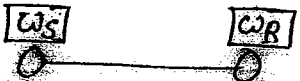


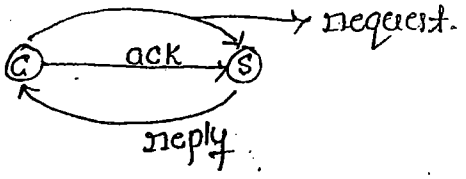
fig: Half duplex.

* TCP, uses, sliding window protocol (SWP) for its flow control. Therefore each TCP connection has 4 windows.



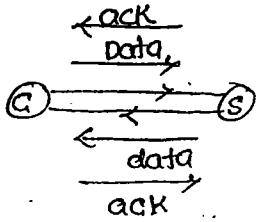
* TCP connections are having 3 phases.

1. connection establishment phase: /(negotiation phase)

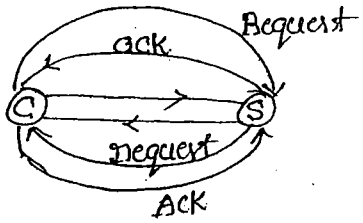


* it is a single step process.

2. Data transmission phase



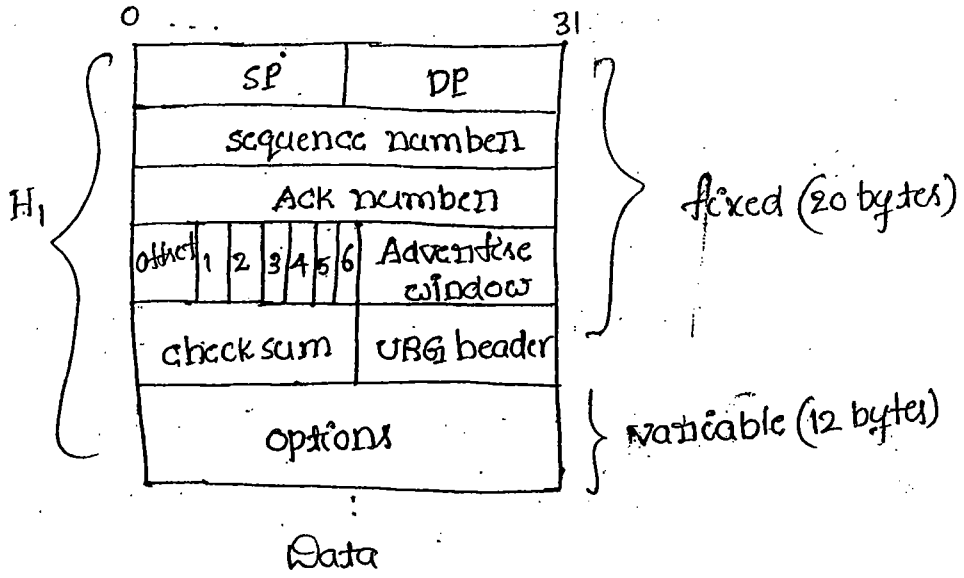
3. connection termination phase.



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

TCP operations:

TCP header:

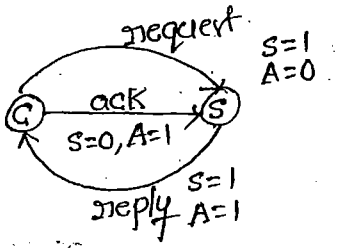


Flags:

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

1. SYN & ACK: SYN & ACK flags are used in connection establ

Phase of different request and reply packets



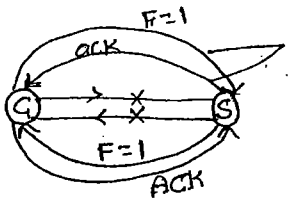
S=1 A=0 => Request

S=1 A=1 => Reply

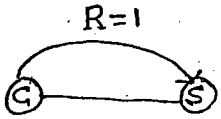
S=0 A=1 => ACK

S=0 A=0 => Data

2. FIN : it is used in connection termination phase.



3. RST Flag: it is used to reset the connections.

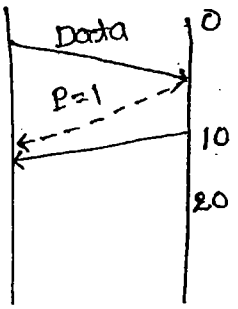


* New connection is establish
just refreshing the windo

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

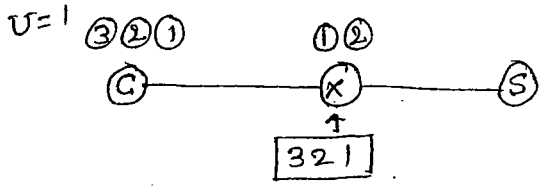
4. PSH flag:

* 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 sender sends the ack fastly as soon as data receiver without waiting for the time interval it have.

5. URG: it is used take care of "out of band rate"



sequential order

Inband: 1,2,3

outband: ③ 2 1

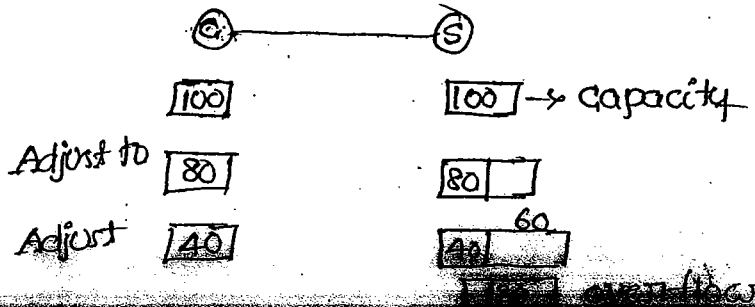
⇓

using URG Pkt.

* URGENT Pointer indicates the amount of the data that is important in the packet.
* it is valid only if URG=1
* if the packets ①②&③ sent to sender by representing URG=1 to ③ Packet then instead of 1 and 2, ③ packet if reached firstly, it represents an URGENT Packet.

Advertise window:

* it is used to implement flow control



* If the server have no empty space, it can't take further data. so it must represents 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 sender 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, then it can accept the data packet.

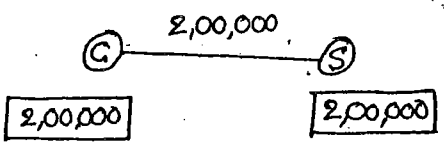
Silly window syndrome (SWS):

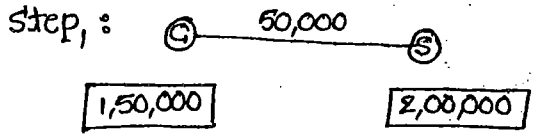
* when SWS occurs efficiency is "0".

* There are three reasons for silly window syndrome.
  - → 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. Possible to reduce the SWS value, so that efficiency increa





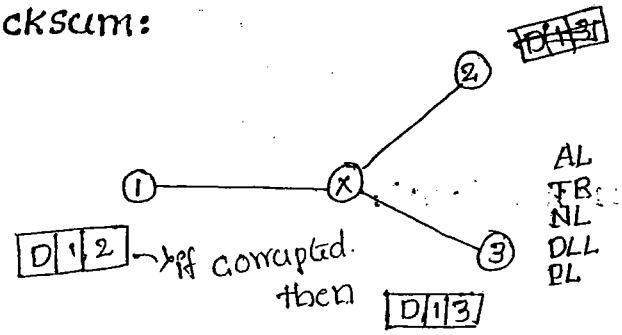
* There is a chance of sending all the 1,50,000 bits, at both the sides but we cannot transfer them because only 2^{16} bits

* if empty space in the server is more than 2^{16} then use scale factor in the - "option" field.

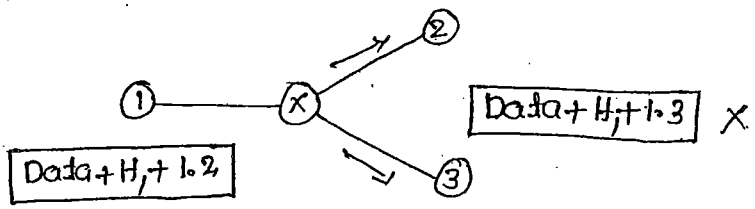
eg: if empty space is 1,50,000 advertise window = 50,000
& scale factor = 3.

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 application layer. Then application layer recognizes as a corrupted bit.
* so inorder not to have burden on application layer, before a packet reaches application layer, it gets corrected at the Transport layer by including the concept of "checksum".
* checksum includes "data + H_1 + pseudo-header" in its calculation.



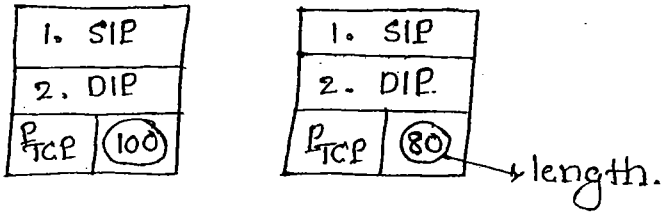
* calculate the checksum $\bar{c}(\text{Data} + H_1 + (1.2))$ at the sender side and send the checksum. at the receiver the check sum is again calculated. [Data + H_1 + (1.3)] → corrupted, so discard it by transport layer.

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

* it is prepared at the source and included in checksum calculations.

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

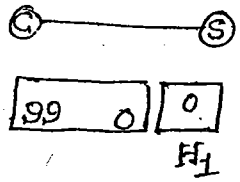
* if incoming checksum is similar to calculated checksum, then packet is consumed, else it is discarded.



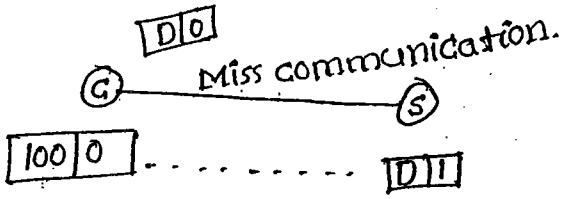
* sequence no. for the packet is first databyte sequence num. in the packet.

characteristics for Sequence num & Ack:

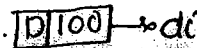
1. sequence no. for the packet is first databyte sequence num. in the packet.



2.



TCP user random initial sequence number.

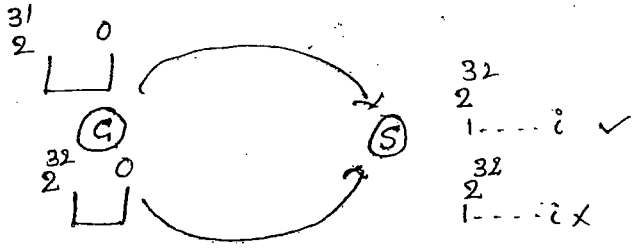


* The sequence numbers always not start with "0" it selects a random number among the set of $0-2^{32}$ and then sends the random number. if corrupted random num generates simply discard it.

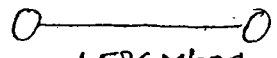
Eg:

3. Get randomly sequence numbers:

if two different packets of the same sequence num 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 packet which is different from the other packet.



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

Eg: 

1 sec = 1.536×10^6 bits ⇒ 1st pkt

1 sec = $\frac{1.536 \times 10^6}{8}$ bytes ⇒ 2nd packet

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

1.536 Mbps – 64 hrs

10 Mbps – 57 min

100 Mbps – 6 min

:

1.2 Gbps – 28 sec.

Eg: consider bandwidth of link = 100 mbps

sequence no. field = 24 bits

Find the "wrap around" of sequence numbers

↳ 1 sec = 100×10^6 bits

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

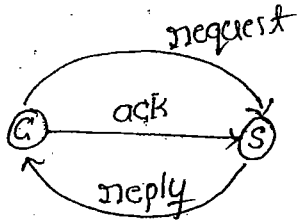
1 sec = $\frac{100 \times 10^6}{8}$ sequence num's

? 2^{24}

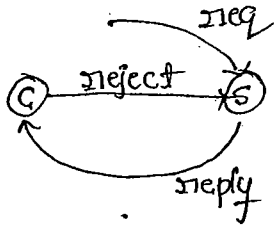
$\Rightarrow \frac{2^{24} \times 8}{100 \times 10^6} = 1.3$ sec.

Applications:

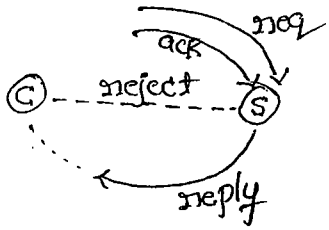
A.



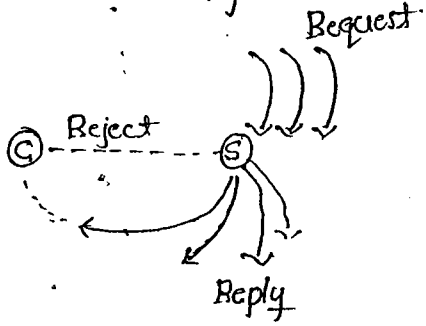
B.



C.



D.

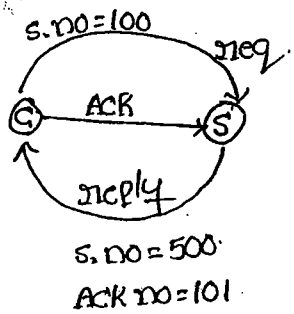


Denial of service attack:

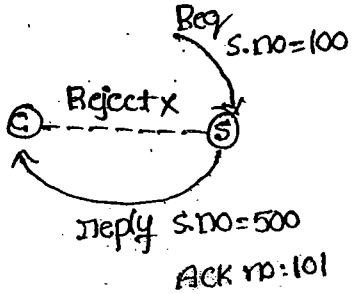
* server denies the client to server for a certain time inter

To overcome above problem we use "sequence number".

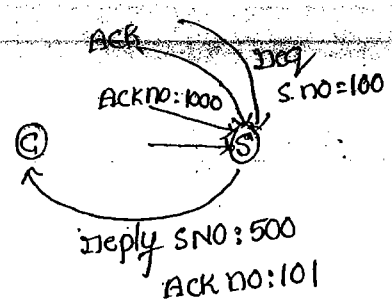
A.



B.



c.

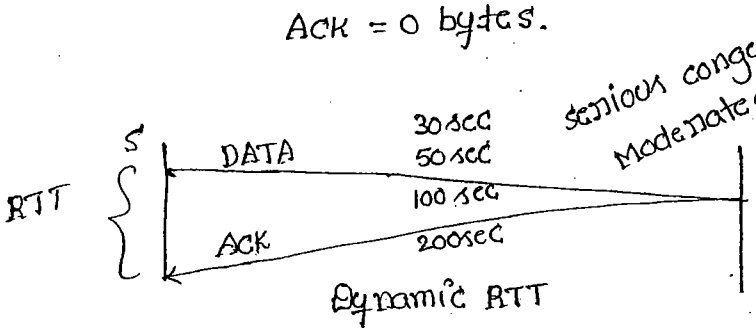


1.

Hacker can't know the random num generated by server so he guess simply rejected. if guess = exact no then the server cannot generate huge ack so it discard to send ack

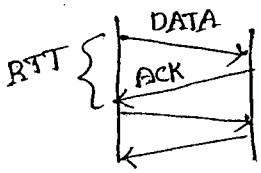
syn } 1 byte
FIN }

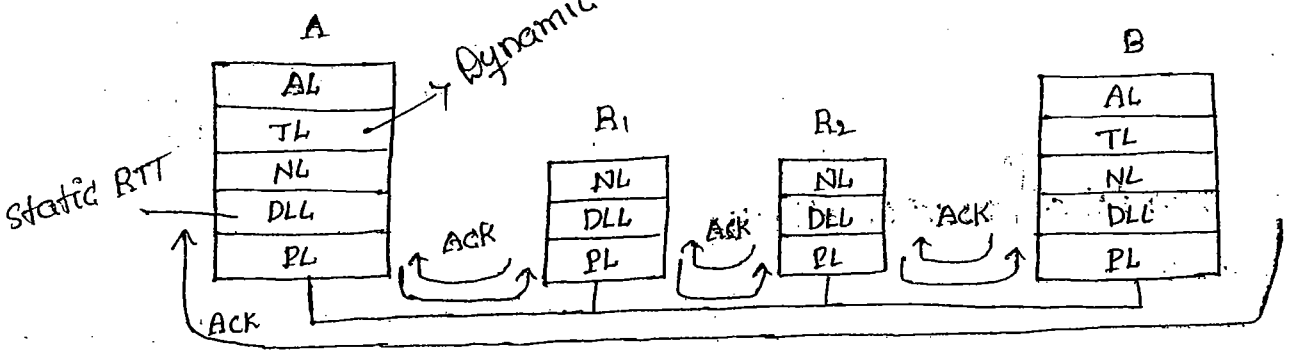
Ack = 0 bytes.

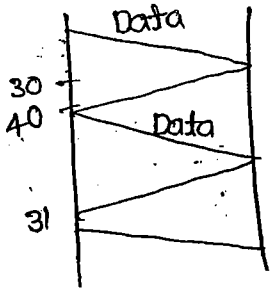


(3)

Unpredictable Timing
⇓
End-to-end
Link-to-link
⇓
Predictable Timing.







2. I

For the calculation of RTT we have certain Algorithms.

1. Basic Algorithm:

(IRTT) Initial Round Trip Time = 30 sec

(NRTT) New Round Trip Time = 40 sec

$\alpha = 0.9$

2. Estimated RTT = α IRTT + $(1-\alpha)$ NRTT

$= 0.9 \times 30 + (1-0.9)\,40$

$= 31$ sec

Time out (TO) = $2 \times$ ERTT

$= 2 \times 31$

$= 62$ sec

③ IRTT = 31 sec

NRTT = 50 sec

ERTT = α IRTT + $(1-\alpha)$ NRTT

$= 0.9 \times 31 + (1-0.9)\,50$

$= 32.9$ sec

Time out = $2 \times$ ERTT

$= 2 \times 32.9$

$= 65.8$ sec

④ IRTT = 32.9 sec

NRTT = 45 sec

ERTT = α IRTT + $(1-\alpha)$ NRTT

$= 0.9 \times 32.9 + (1-0.9)\,45$

$= 34.11$

Time out = $2 \times$ ERTT

$= 2 \times 34.11$

$= 68.22$ sec.

2. Jacobson's Algorithm:

IRTT = 30 sec

NRTT = 40 sec

$\alpha = 0.9$

initial deviation (D_i) = 5

② New Deviation (D_N) = $|IRTT - NRTT|$

$= |30-40|$

$= 10$

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

$= 0.9 \times 5 + (1-0.9) \times 10$

$= 5.5.$

$ERTT = \alpha IRTT + (1-\alpha) NRTT$

$= 0.9 \times 30 + (1-0.9) \times 40$

$= 31$

Time out = $4 * D_E + ERTT$

$= 4 \times 5.5 + 31$

$= 53.$

③ $IRTT = 31$

$NRTT = 50$

$\alpha = 0.9$

$D_i = 5.5$

$D_{New} = |31-50|$

$= 19$

$D_E = 0.9 \times 5.5 + (1-0.9) \times 19$

$= 6.2$

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

$= 32.9$

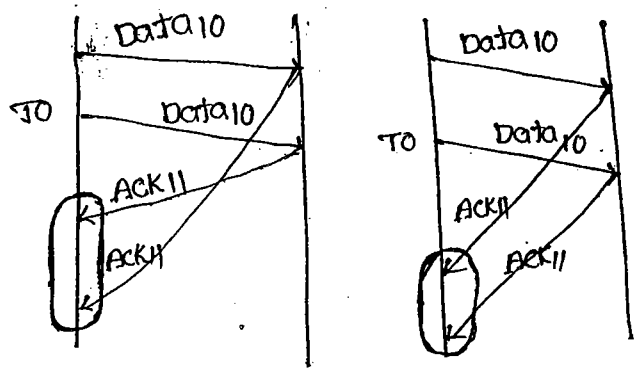
$TO = 4 \times D_E + ERTT$

$= 4 \times 6.2 + 32.9$

$= 57.$

* "Time out" is high under Basic algorithm then the Jacobson Algorithm.

Karn's Algorithm:



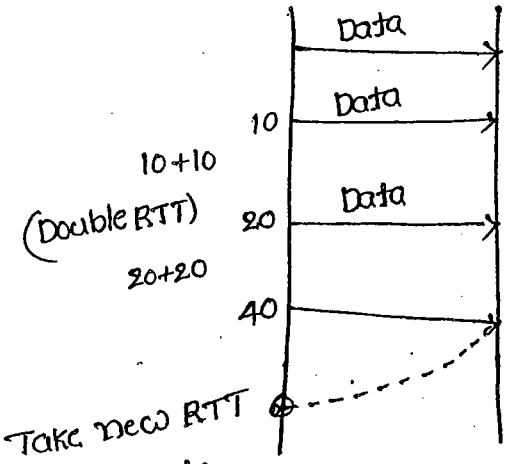
* if there is a time out, there is a possibility to receive 2 data packets
  1. From original packet
  2. From re-transmitted packet.

* Then there is an ambiguity that which ACK must be considered for next calculation.

∴ Therefore, Karn's has resolved this ambiguity by proposing the follows.

=> For every timeout double the timeout for the next transmision and continue this till to get a proper ACK.

=> Then we will go back to the jacobson's algorithm.



State Transition Diagram:

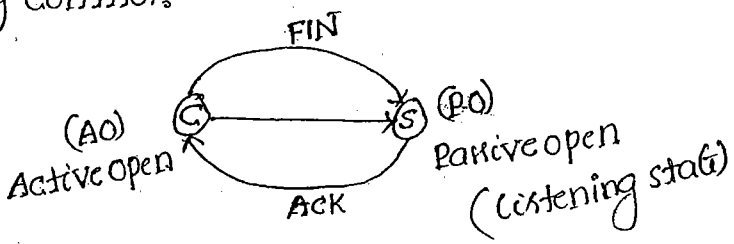
Need for state Transition dig:

* To evaluate any protocol, we use one of the following 2 methods.

1. Get the specification of the protocol develop a software for it, integrate with network operating system and evaluate it's features. it is time consuming process and costly.

2. Get the specification of protocol develop state transition dig for it and then evaluate it's features.
   it is a shortcut method but not so powerful.

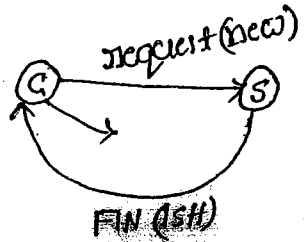
Dialog control:

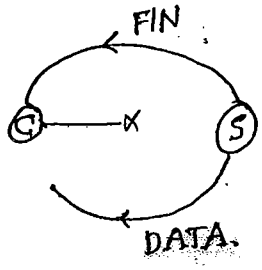


Purpose of Time wait state:

* As soon as Acknowledgement is generated client will go to time wait state instead of closed state by suspecting problem with acknowledgment. Even if ACK is lost and "FIN" server is re-transmitted.

* it is treated for some 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 FINS/ But it denies, 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 it is also allotted for "FIN" which is called as "Time wait state".

Limitations of State Transition dig:

* Error control procedures are not depicted in the dig
* Re-transmission are not shown in the dig.

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

* checking the server that it works connection 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 for which RTT is more for character typing.
* At such conditions, add the headers for all the bits & send it which improves performance.
* But it is not applicable in LAN technologies, but support WAN tech because of RTT and typing speed capabilities
* Round trip time is less but input speed is high.

Problems:

① Maximum data = 64 KB

= 65,535 ⇒ | 65515 | 20 |

Data Header.

② RTT = 30 msec

$\alpha = 0.9$

NRTT = 26

Basic algorithm = α (RTT) + (1−α) (NRTT)

= 0.9 × 30 + (1−0.9) (26)

= 29.6 msec

T.O = 2 * 29.6 = 59.2 msec

D_{new} = |30 − 26| = 4

DE = 0.9 * 4 + (0.1) * 4

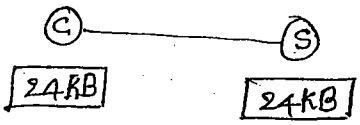
= 4

T.O = 4 * D.E + ERTT

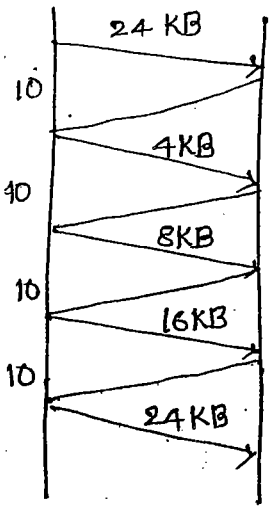
= 4 * 4 + 29.6

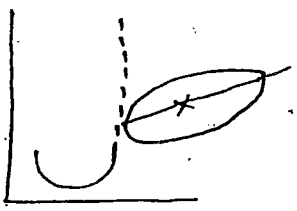
= 45.6 msec.

③



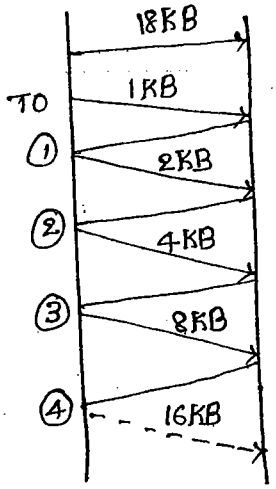
After 40 ms a full window is transmitted





congestion.

④



After time out occurs go back to window size = 1

Ans: 16KB.

⑤. TCP USES SWP

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

$$= \frac{65,535 \times 8}{20 \text{ msec}}$$

$$= 26.5 \text{ mbps}$$

$$\eta = \frac{26.5 \text{ Mbps}}{1 \text{GBPS}}$$

$$= 2.6\%$$

⑥. Transfort data unit

Total numbers available $= 2^8 = 256$ and they should be consumed in 30sec.

$$\text{Data rate per connection} = \frac{128 \times 8 \times 256}{30}$$

=

1

(9) Probability of sequence of 1 random number fall in 10^6

total no $= 2^{32}$

$$= \frac{10^6}{2^{32}} = 2.3 \times 10^{-4}.$$

=

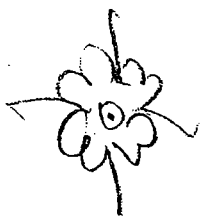
(11) A typist can type 600 characters for minute i,e to type a character takes 100 msec.

case:1: since RTT is very much less than typing speed. this algorithm cannot be implemented.

case:2: Since RTT is exactly equivalent to typing speed this algorithm cannot be implemented.

if RTT is more than 200ms then we able to implement this algorithm Nagle's algorithm.

=

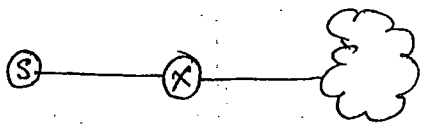


S. K. Reddy

User Datagram Protocol (UDP):

Need for UDP:

For multicasting and broad casting applications, TCP can't be used Hence we need TCP.



Server communicates to 1.6 crore systems in TCP, we require 1.6 crore connections which cannot support a huge connection.

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

  Eg: Rocket launching.

* Applications that requires bulk data transfer cannot use TCP

  Regulated flow in TCP, fluctuated flow in UDP.

* Applications that requires fastness than reliability cannot 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

* connection-oriented
* slow
* Reliable
* overhead is high
* HTTP, FTP, SMTP, Telnet are used

Applications

* web applications
* Mail, RSA applications

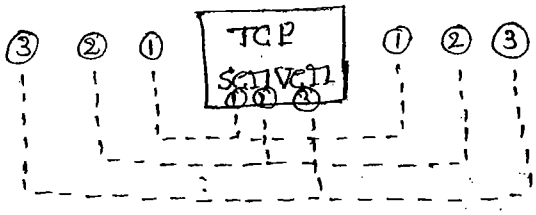
UDP

* connection less
* fast
* un-reliable
* overhead low.
* DNS, TFTP, NFS, SNMP, multi-media & Realtime.

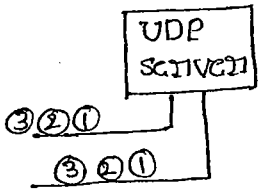
Applications.

* Name transfer Application
* N/w management applications
* Multimedia & Realtime appl's

concurrent process:



iterative process:



* TCP and UDP Port numbers are different.

Domain Name System (DNS):

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

it has four applications

→ Name Translation
→ Host Aliasing
→ Mail Aliasing
→ Lode balancing.

it is using 4 types of servers

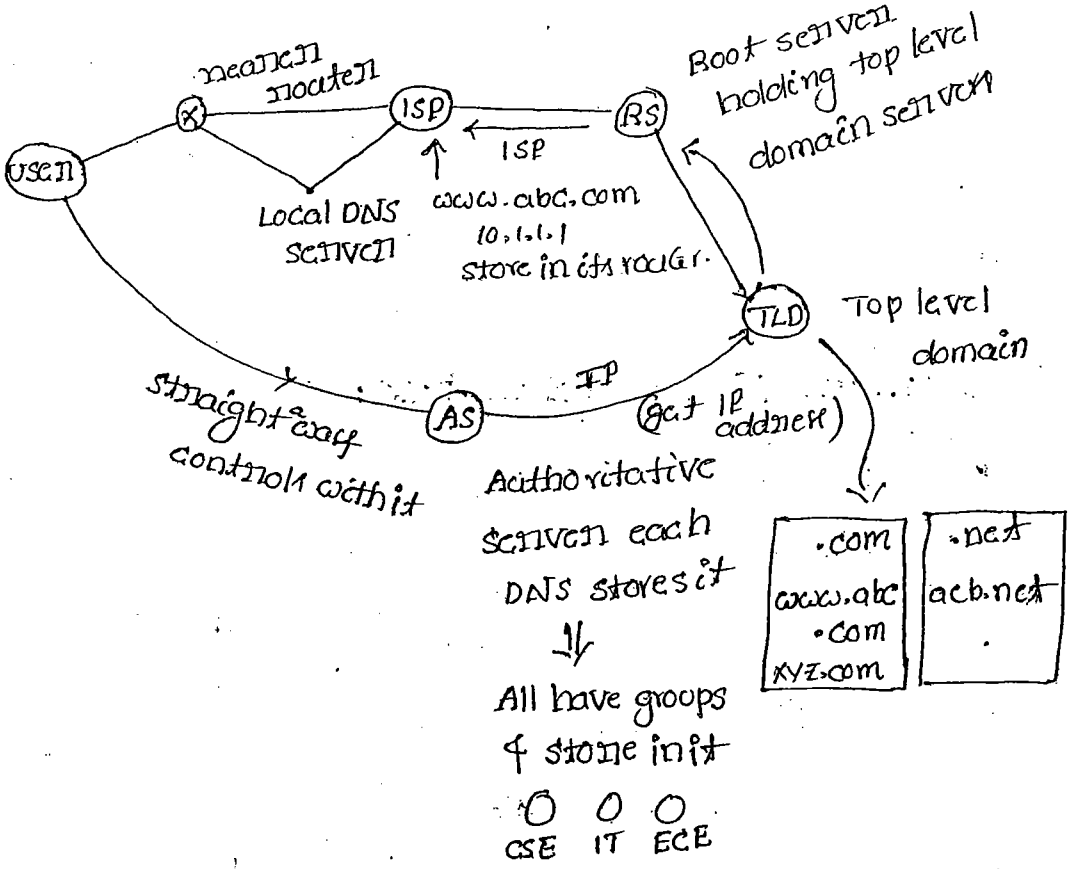
- → Root name server
- → Top-level domain server
- → Authoritative server
- → Local DNS server.

* it uses distributed database to perform its applications.

information about computers and services are stored in these servers in terms of resource records.

* Each resource records consists 5 attributes.

- → Name
- → TTL
- → class
- → Type
- → value.



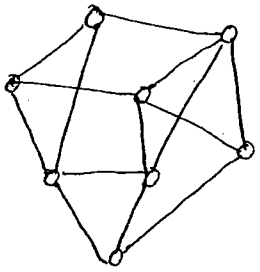
CSE IT ECE

Fault gateway: IP routers specifies the default address, suggesting address that it can't know particular address.

* once a request for a website is sent, it gets stored in ISP and the local routers, whenever again a request of same website is sent then there is no need to visit all the servers, and there is only subsequently request simply it shows the website without visiting root server.

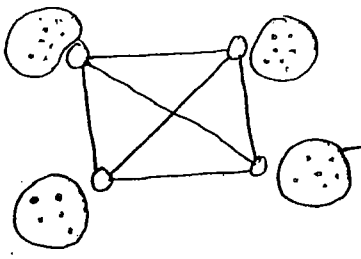
* Mainly 70% of internet services are provided by ISP & local routers.

* when Top level Domain servers maintained in terms of clusters. These are connected with MESH topology. it helps to improve efficiency and reliability.



Mesh connection

Rs maintains many routers and get connected not only single router.



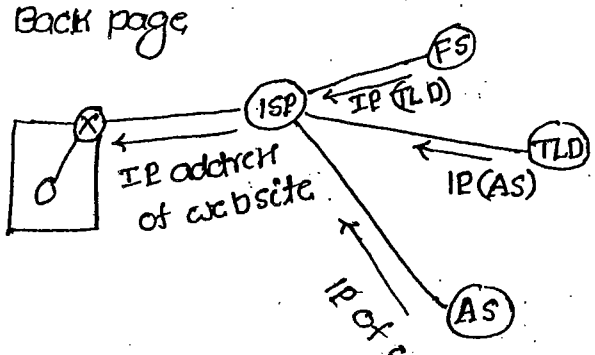
server in the form of clusters and distributed database.

* it will help for fast searching (effective usage)

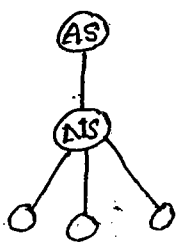
=> Getting IP address can be done in two ways.

1. Back page

2.



NS: Name Server



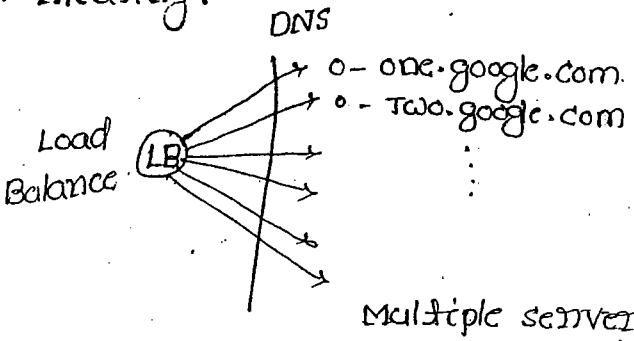
* Rs asks ISP to get connected

=> Giving names to systems in a network (Host aliasing):

L1.one.abc.com => by seeing name, one can understand position of the system.

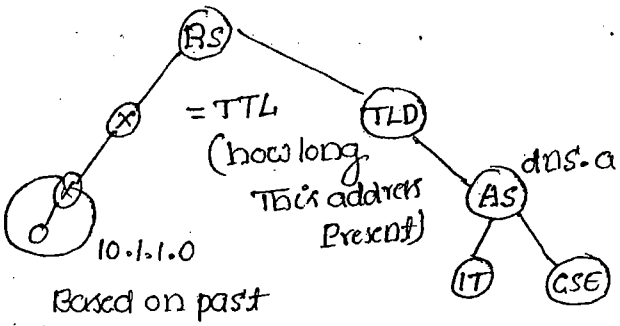
In "abc" college building, "one" lab, "one" first system

Mail Aleasing:

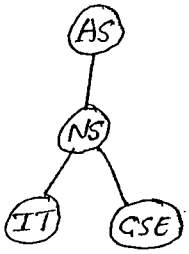


Multiple servers placed in different places.

Distributive Database:



Based on past data of a server



IT.abc.com 24 hrs in 10.1.1.3, www.abc.com 24hrs NS, dns.abc.com.

www.abc.com 2hrs 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 restricted from nearer router.

Circular dependency => glue record.

Replication => sharing data.

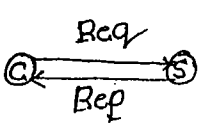
More replication => use TCP

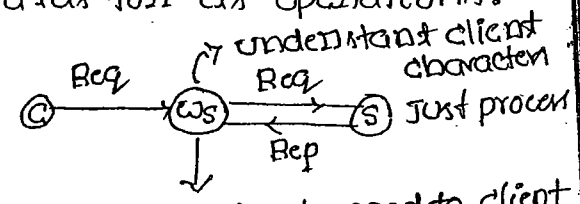
Translation => use UDP.

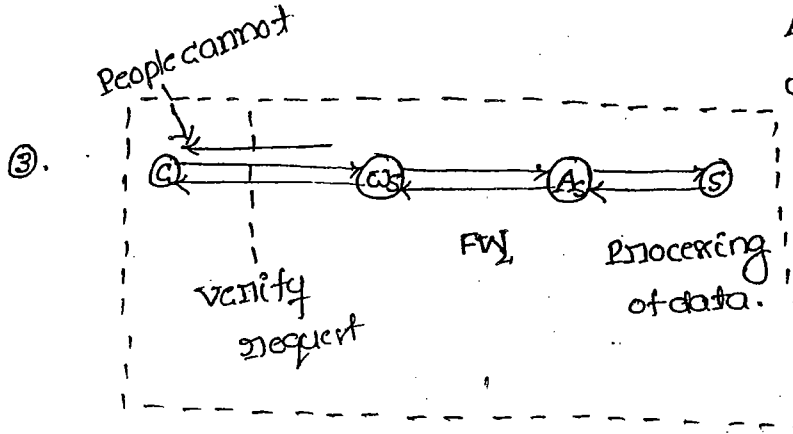
HTTP:

* it is a client server protocol using port 80 in TCP.
* it is stateless protocol.
* There are 2 types of HTTP protocols
  - → persistent
  - → Non-persistent.
* it have two types of messages → Request
  - → Response.
* HTTP will perform its operations by using 8 different methods
  - => Head: HTTP developed through ← web browser, version, os (all html pages stored in webserver)
  - => get Method.
  - => Put => creation (create an object in server)
  - => Post => changing (Modification)
  - => delete => delete
  - => Trace => debugging
  - => options => optimization.
  - => connect => Through the channel and users security Perform transactions.

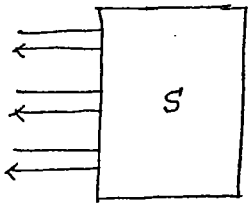
HTTP uses 3 different types of status for its operations:

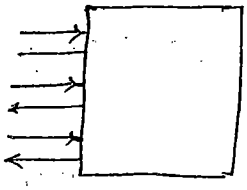
① 

② 

③ 

*On - persistent connection in 1.1 (in 2.0 is changed to persiste)





Persistent

Every time new connection is established

using some time, limit connection is placed.

2 - succesful
3 - redirecting
4 } Error Method.
5 }

* Each & every request express head method (client).

Display status error (stateless protocol).

File Transfer protocol (FTP):

* 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 operations.

  → Active mode
  → passive mode
  → Extended passive mode.

* There are 2 flavours of FTP

  FTP => Authorized users

  TFTP => Anonymous users.

* To keep track data transmission, FTP uses wide varieties of status codes and also it is supported with many no.of commands.

* TFTP: never requires username, and password. All the users within the applications can access the data.

Eg: LIC Policy application

fig: Active mode

*

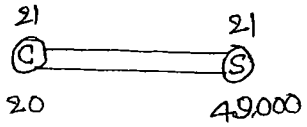


fig: Passive mode

* in passive mode, server generates a dynamic address and it is being get connected within the client.

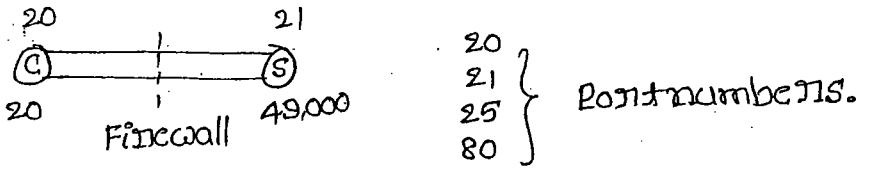


fig: Extended passive mode.

* in this mode, a firewall is being placed b/w 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, where the FTP must be monitored constantly in there time, so for this we use a no. of commands.

* The monitoring of FTP constantly assumes the checkcking of status codes.

HTTP + SSL => HTTP

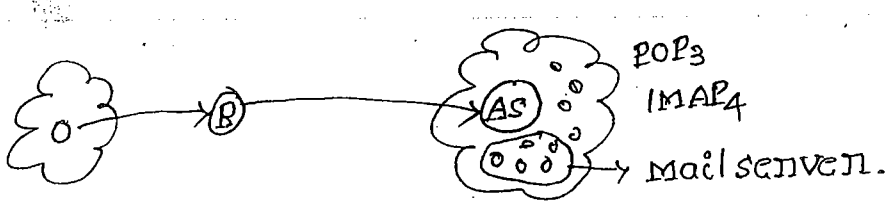
FTP + SSH => security.

* 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.
* it is having two components.
  - -> User agent
  - -> Mail Transfer agent.
* it is a part of push-pull mechanism in the mail commu
  ∴ SMTP is used to push the mail.
* POP-3 and IMAP4 are used for pulling the message.
* it is an example for asynchronisation communication.
  i.e client and server are indirectly connected.
* if client and server are directly communicated (connected) => synchronous commands

* 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 AS identifies particular host in the mail server and "push" the data into that hosts. 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 mechanisms POP_3 and $IMAP_4$ are used.

* $IMAP_4$ is more advantageous than POP_3 for this consider an example:

Before downloading a file, a msg is delivered to check it is SAFE (or) associated with any virus. if user is interested to continue (either it is SAFE or UNSAFE) then only it proceeds and if he is not interested simply "CANCEL" it => it is

advantages of $IMAP_4$ over POP_3

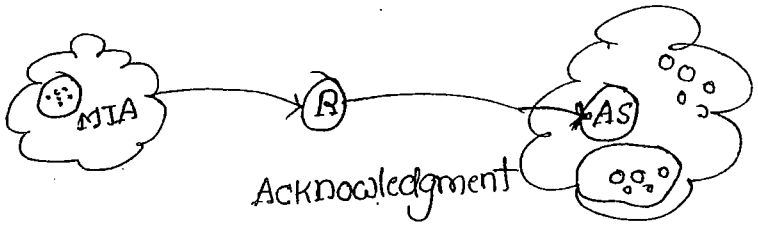
* $IMAP_4$ Push some of the dangerous mails to junk mails where as POP_3 cannot do.

Hierarchies in the inbox:

* A folder is created in the inbox and are configured with some mail address. so that there is no chance of missing important information.

Two components:

* User agent
* Mail Transfer agent (Incharge to negatiate with TCP for connection SMTP)
* Forward message => attachments are available with the message
* Reply message => all the attachments are automatically dropped.
* 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 an read it (or) not.
* while user reads the mail an acknowledgment is sent to the sending user that the recipient had read it.



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

Internet protocol.

Different special IP Addresses:

S.NO	source IP Addresses	Destination IP Address.
1	x	x
2	x	✓
3	x	✓
4	✓	x
5	✓	✓
6	x	✓

* The above 6 IP addresses are used only for special purpose within the internet protocol.

* some of the IP addresses are used to represent only source IP addressing and some are destination IP addresses. ¢c it represents to have NID and some HID.

1. NID (✓ x) HID (x 0) => filled by 0s

A: 10.0.0.0
B: 150.157.0.0
C: 192.168.1.0

Name: "This network" address.

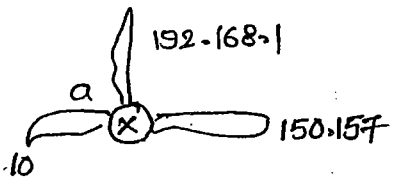
Purpose: used by Routers.

=> Represents different network

D	10.0.0.0	150.157.0.0

=> not valid

* 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 systems are used by routers to identify the network, for which it belongs to.

2. NID 1's HID => filled by 1's *

X ✓

A: 10.255.255.255

B: 150.157.255.255

C: 192.168.1.255

Name: Directed Broadcast system // Delivering packets to all system in some other network.

Purpose: To all in sender network

D	10.1.1.1	150.157.255.255	✓

D	150.157.255.255.	10.1.1.1	X

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

3. 1's NID 1's HID

255.255.255.255.

Name: Limited Broadcast address. // Delivering packets to all systems in our own n/w's

Purpose: To all in the local network.

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

4. 0's NID 0's HID

0.0.0.0

Name: Dynamic IP address.

Purpose: Dynamic Host configuration protocol (DHCP).

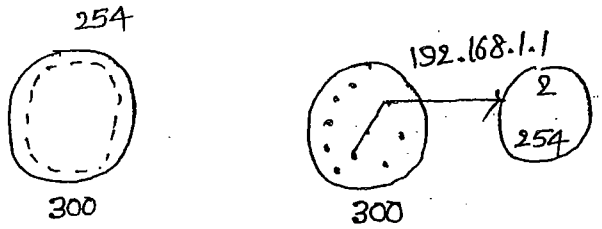
* In dynamic more no.of system, so it can be limited IP addresses.

* I
E
By
a-
* Lo
n
ar
* S

By
as
Ac
t
a

5.

* More IP addresses & less no. of systems



* 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, then the IP address is assigned to the other user.

* Likewise 254 IP addresses are managed by the server (but not client) in the FCFS basis. If there are more request an "Queue" is maintained.

* so it is used only for the source but not destination

D	0.0.0.0	192.168.1.1

Dynamic:

The operating system on the basis of administration, assigns the IP address to the system.

Auto: The operating system directly assigns the IP addresses to all the systems without the intervention of administrator automatically.

5. 0 ✓
NID HID

A: 0.1.1.1

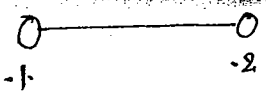
B: 0.0.100.1

C: 0.0.0.100

Name: Host in this network

Purpose: local communication

192.168.1



192.168.1.1	192.168.1.2

(or)

0.0.0.1	0.0.0.2

IP

* The communcation is done among the two host systems within the same network => local communication.
* The communication is not possible for 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.

6. 127... Any

127.1.1.1 or 127.100.0.255

Name : Loop back address

Purpose: interprocess communication

* self checking or self connectivity with checks

127.0.0.0	X

127.255.255.255	X

* Both IP addresses are not valid other than these two IP address all the others are valid. which starts with:

ID = 127.

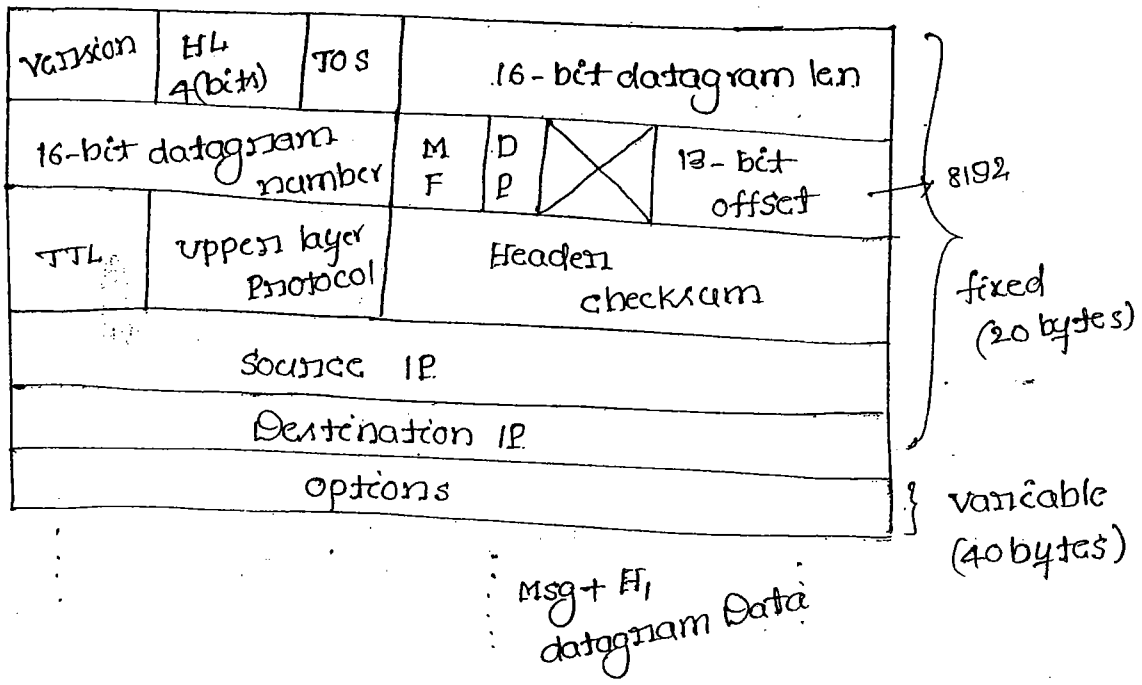
=> which of the following IP addresses are used as only source IP addresses

A. 10.1.1.1 (B.) 0.0.0.0 C. 0.0.0.1 D. 127.1.1.1

=> which one of the following IP addresses are used as both source and destination addresses. (6)

A. 10.1.1.1 B. 255.255.255.255 C. 10.255.255.255 D. 0.0.1.1

IP operations:



* Version => to indicate either IP_4 or IP_6 Packet (4-bits)

IP_6 less complicated than IP_4.

* Header Length: Maximum size => 60 bytes (40+20)

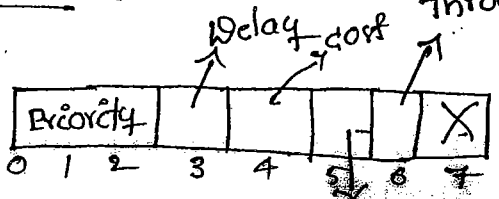
Minimum size => 20 bytes.

$2^4 = 0 \ldots\ldots 15$

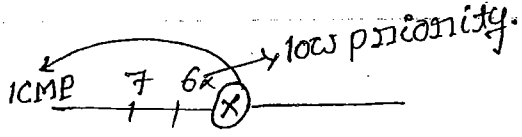
Constant scale factor = 4

$$\frac{\text{Actual header length}}{8} = \text{Available header length in PKT (4-bit)}$$

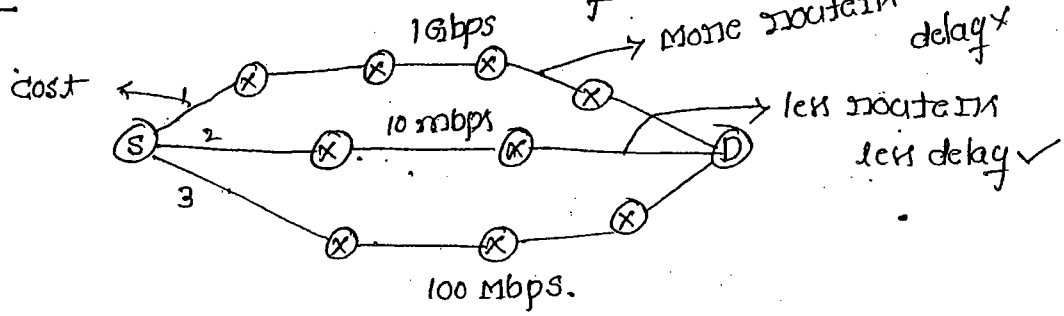
Types of service (TOS):



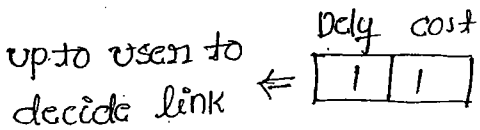
* Based on priority, packet is transferred to intermediate routers.



Delay: More routers more delay



Cost: considering bandwidth, num. of routers, error rate, distance among the routers, the cost is being calculated.



Reliability: it represents the "error rate".

Throughput: it depends on bandwidth, if high bandwidth for a link => then allows

2^{16} = 64 KB => ⁊c maximum size of the total Packet.

16-bit datagram number:

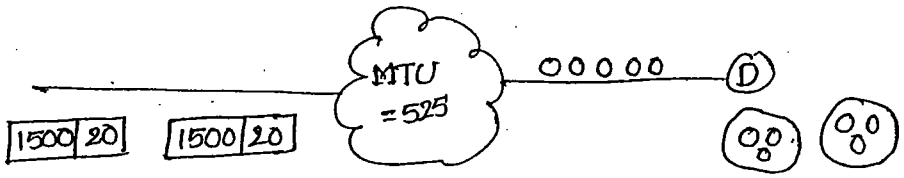
Every datagram associated with the sequence numbers starting with '0'.

More fragments (MF).

Maximum Transfer unit (MTU):

Fragmentation is applicable to only datagram packet but not the header.

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

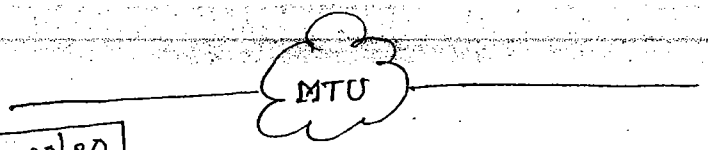


	①	②	③	④	⑤	⑥
504		504	492			
	505	505	490	505	505	490
	+ 20	+ 20	+ 20	+ 20	+ 20	+ 20
	5	5	5	6	6	6
MF	1	1	0 end	1	1	0
Offset	0/8	504/8	1010/8	0/8	504/8	1010/8
		504	1003			

CSF = 8

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.

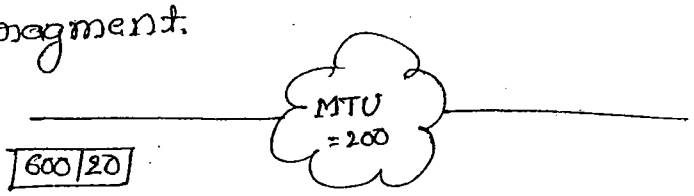


$\frac{64000}{8} = 8192.$

64000	20

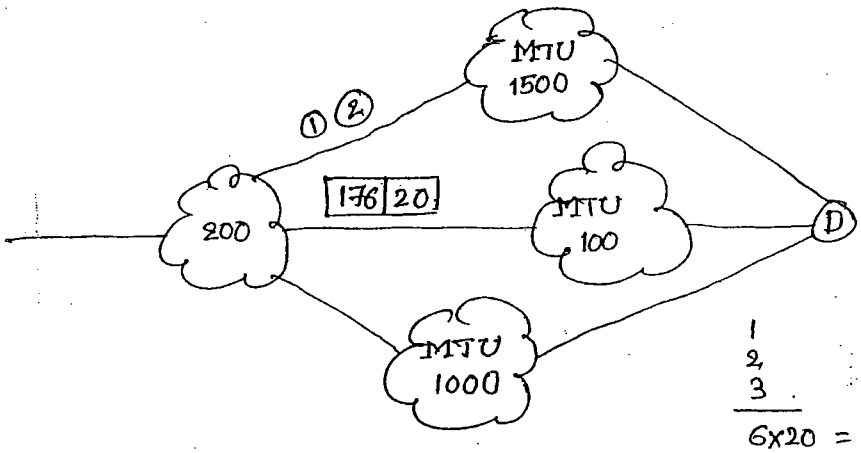
①	②	⑩	⑭
1000 + 20	1000 + 20	1,000 + 20	1000 + 20

* Datagram data (or) 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.



600	20

176	176	176	72
180	180	180	80
+ 20	+ 20	+ 20	+ 20
MF 1	1	1	0
offset 0	$(\frac{176}{8})$ 22	44	66.



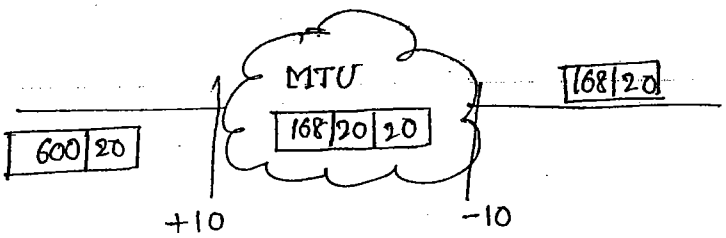
1
2
3

6x20 = 120
−20
100

* if offset = MF = 0 ⇒ Original packet.
* if any one of them is non-zero ⇒ fragment (intermediate fragment)

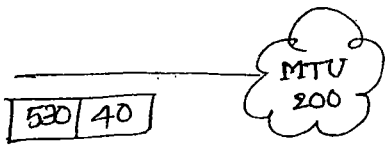
176	20

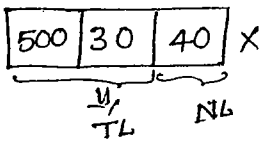
	80	80	16
	1	1	1
	20	20	20
MF	1	1	1 ⇒ Intermediate fragment.
offset	44	54	64



	168	168	168	96
	~~170~~	~~170~~	~~170~~	~~96~~
	+	+	+	+
	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

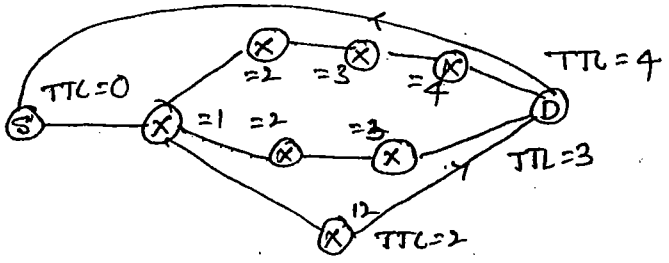




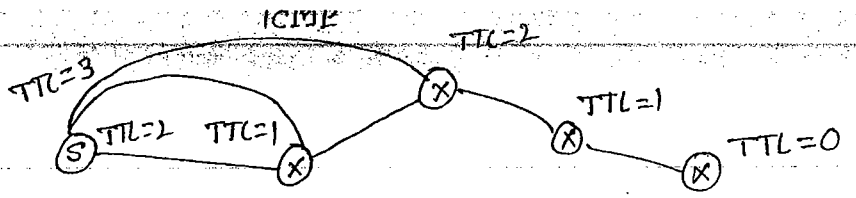
160 160 .....
\+ +
40 40

Time To Live (TTL):

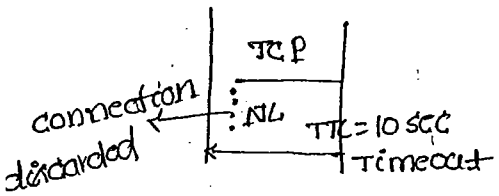
* it have four applications:-
  - -> To avoid infinite looping
  - -> To identify no. of routers between source & destina
  - -> To debug the network
  - -> To help upper layers in timer management

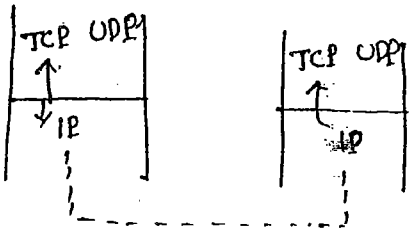


* It is possible to find no. of routers in a route by using

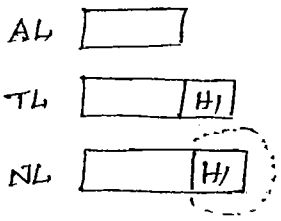


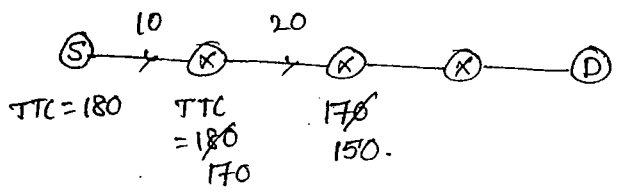
Timer Management:





* 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

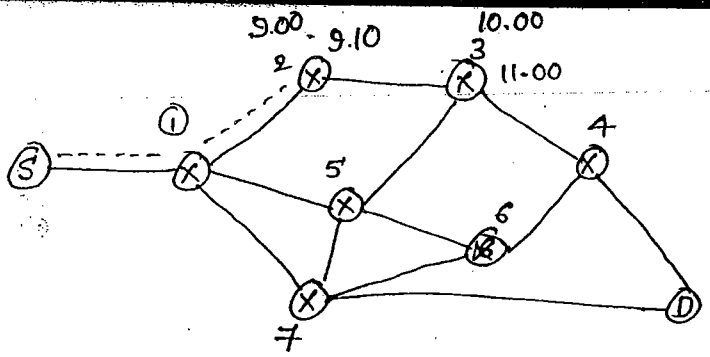
} ⇒ fixed.

Options:

* Strict source routing
* Loose source routing

} source will decide the route

* Record routing ⇒ Routers decides the route
* time stamp
* Security



Strict source routing: Each and every route is specified

(1, 2, 3, 4)

Loose source routing: 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 and Departure time of each and every packet is stored.

Security: Mails are sent along with certification which provides secured access for a page.

Q:

⇒ then which of the options are most 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 } most available in all the fragments.

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

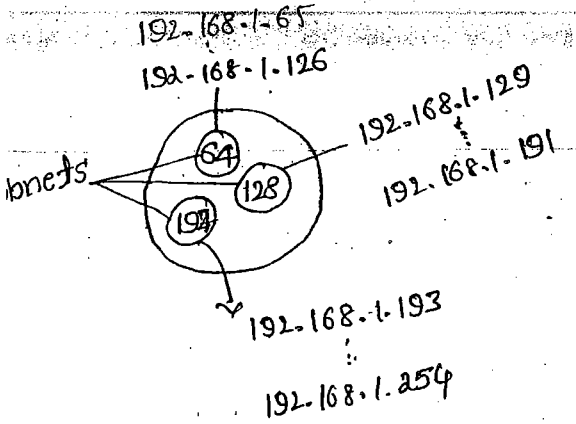


fig: 192.168.1

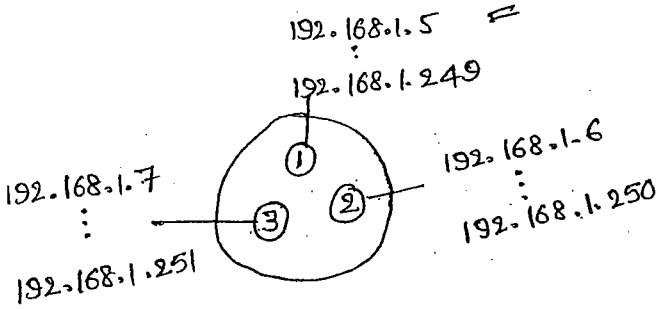
01 . . . . . .
01 000001 - 65
01 000010 - 66
⋮
01 111110 - 126

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

11 000001 - 193
⋮
11 000110 - 254

C: NID HID ⇒ borrow first 2 bits
24 2,6
SID HID
$2^2 = 4$
$2^6 - 2 = 62$

128	64	32	16	8	4	2	1
0	0	= 0					
0	1	= 64					
1	0	= 128					
1	1	= 192					



⇒ 192.168.1

NID HID
24 6,2

128, 64, 16, 8 4, 2, 1
0 0 - 0
0 1 - 1
1 0 - 2
1 1 - 3

. 01
00000101 = 5
00001001 = 9
⋮
11111001 - 249

. 10
00000110 - 6
00001010 - 10
⋮
11111010 - 250

* Subnet id's and IP address of the network are changing

checked

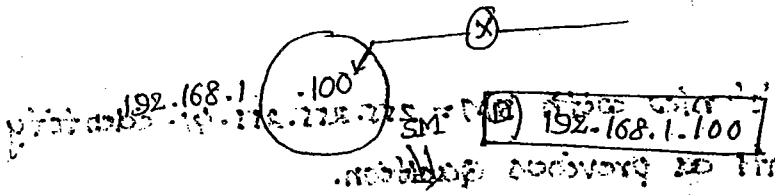
→ if not available then IP address is directly assigned to that.

→ if available then identify, the packet belongs to which subnet for that we use subnet mask (SM)

Subnet Masking:

* 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 2 rules.

1. No. of 1's in the subnet mask, indicates n/w id (or) subnet Id.
2. No. of 0's indicates Host Id part.



subnet mask = 255.255.255.0

SM: 11111111.11111111.11111111.00000000

Rule(1): $\overset{24}{NID} + \overset{0}{SID} = 24$ (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.

eg:

↳ SM: 255.255.255.192

.11000000

Rule(1): $\overset{24}{NID} + \overset{2}{SID} = 26$

HID = 6

No. of bits borrowed = 2

Their position is = 128^{th} bit, 64^{th}

eg:

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 address = 62.

eg: Consider a class 'c' n/w with SM = 255.255.255.41 - identify all data points as previous question.

SM: 11111111. 11111111. 11111111.00101001

$\overset{24}{NID} + \overset{3}{SID} = 27$

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 = $2^5 - 2$

Their subnet ID's =

32 8 1		32 8 1
0 0 0 = 0	011 = 9	1 1 0 = 46
0 0 1 = 1	100 = 32	1 1 1 = 41

eg: Consider a class B n/w with SM = 255.255.255.0. identify all the data points as previous ques.

↳ subnets are available

Entire 3rd packet are borrowed for subnet IDs

∴ no. of subnets = 2^8

Their ID's = (0-255)

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

Their IDs = (1 to 254)

eg: Consider a class C network with SM = 255.255.255.15.

SM: 11111111.11111111.11111111.00001111

NID + HID = 28
24 4

No. of bits borrowed = 4

Their position is = 1, 2, 4, 8

Possible subnets = $2^4 = 16$

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

eg: Consider a class C n/w proposed an appropriate subnet mask to have 7 subnets each with 25 systems.

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

3 bits must be borrowed (since, 7 subnets)

24 | 8
3 | 5
5 | 3

3-bits => $2^3 = 8$

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

eg: consider a class B n/w and propose an appropriate SM to have 150 subnets each with 200 systems.

$150 * 200 <= 64,000$

$150 \Rightarrow 8 \Rightarrow 2^8 - 2 = 254$

(required) 200

255.255.255.0
255.255.0.255
255.255.240.240
255.255.192.252

eg: consider a class C network. propose an appropriate SM to have 20 subnets each with 15 systems

$20 * 15 <= 256$

$300 <= 256$

not possible.

eg: consider a class C network, propose an appropriate SM of 60.60.120

class C => 8

2 6 1 7

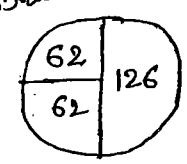
$2^2 = 4 \times 2^1 = 8$

$2^6 - 2 = 62$, $2^7 - 2 = 126$

(not possible) (not possible)

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

255.255.255.192



255.255.255.128

255.255.255.192

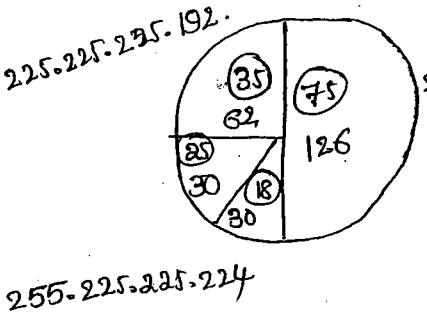
2^1, $2^6 - 2$

$= 2$ $= 62$

1 6

1 7.

eg: consider a class 'C' network propose an appropriate SM to have 4 subnets of 75, 35, 25, 18. Cf



2 6 : 1 7

$2^{4} = 4$: $2^{1} = 2$

$2^{6} - 2 = 62$: $2^{7} - 2 = 126$.

=

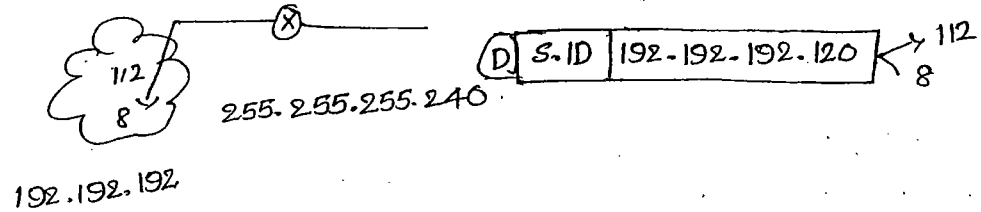
eg: consider a class C network, propose an appropriate SM to have 6 subnets of 30, 25, 22, 20, 18, 15.

class C = 8 : $2^{3} = 8$

2 6

$2^{6} - 2 = 62$

eg:



192.192.192

Identify subnet ID, Host ID and directed broadcast address

IP: 11000000.11000000.11000000.01111000

NID : SID HID

192.192.192

SM: 11111111.11111111.11111111.11110000

112 8

NID. SID NID

SID = 112

HID = 8

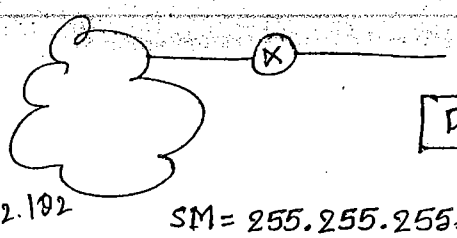
120

192.192.192.127

11000000.11000000.11000000.01111000 Broad

76543210 Addres

Eg:



D	S.IP	192.192.192.120

192.192.192 SM = 255.255.255.41

SID = 32+8+0 = 40

IP: 11000000 . 11000000 . 11000000 . 01111000

SM: 11111111 . 11111111 . 11111111 . 00101001

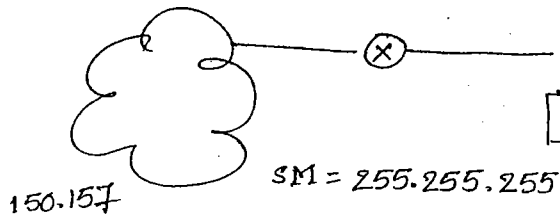
HID: 64+16+0+0 = 80

SID = 40
HID = 80

↳ 192.192.192.254 => Broadcast address.

*

Eg:



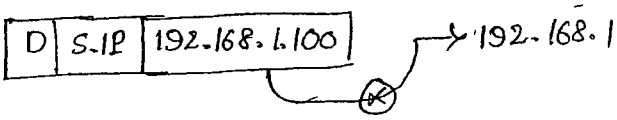
D	S.IP	150.157.100.70

150.157 SM = 255.255.255.0

SID : 100.0
HID : 0.70

Directed Broadcast address = 150.157.100.255.

Eg:



D	S.IP	192.168.1.100

→ 192.168.1

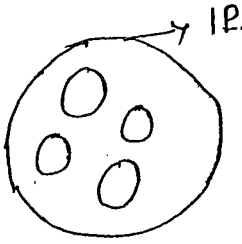
	IP	SM	c/f
	10.0.0.0	255.0.0.0	a
	157.157.0.0	255.255.0.0	b
	192.168.1.0	255.255.255.0	c
	0.0.0.0	0.0.0.0	
	0.0.0.0	0.0.0.0	

192.168.1.100	192.168.1.100	192.168.1.100
AND	AND	AND
255.0.0.0	255.255.0.0	255.255.255.0
192.0.0.0	192.168.0.0	192.168.1.0

* 0.0.0.0 => Default route subnet mask

* 255.255.255.255 => Host specific subnet mask

Supernet Mask:



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

8 8 6 2 8.

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

1. num.of one's in supernetmask indicates fixed part
2. num.of 0's indicates variable part.

11111111.11111111.11111100.00000000

SM = 255.255.252.0

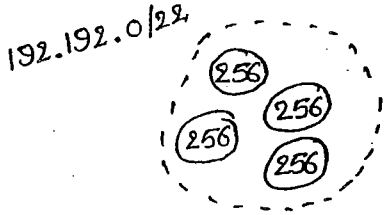
(1). 192.192.0/22 :

↳ Represents NID.

class C :

$24 - 22 = 2$

$2^2 = 4$



256 * 4 = 1024

/24 = class C

/16 = class B

/8 = class A

32

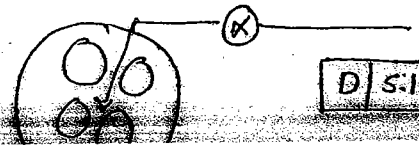
22 | 10

NID | HID

$2^{10} = 1024$

(2). 192.192.0

255.255.255.0



D | S.IP | 192.192.2.100

192

11000000

Difference Between Subnet mask & Supernet mask

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

=> CIDR aggregation (classless Inter Domain Routing) => another name for supernet

	A	B	C
255.0.0.0	subnet	subnet	supernet
255.255.0.0	subnet	subnet	supernet
255.255.255.0	subnet	subnet	subnet.

192.192.0/22 => NID

/24 => class C
/16 => class B
/8 => class A

/22 - ? }
/24 - ? } CIDR.

Routing Algorithms:

Routing is the process of forwarding packets from one network to another. All the information needed for a router to forward packets to a hop can be found in the router's routing table.

=> Static Routing: it occurs when you manually add route in each router's routing table.

=> Dynamic Routing: it is the process of using protocols to find and update routing tables on routers and to maintain a loop-free, single path to each network.

=> common fields in a routing table:

* Mask
* Network address
* Next-hop address
* interface
* Flags
  - U: up
  - G: Gateway
  - H: host specific
  - D: added by redirection
  - M: Modified by redirection.

=> Delivery semantics:

Unicast: delivers a msg to a single specified node.

Broadcast: " " " to all nodes in the network.

Multicast: Delivers a msg to a group of nodes that have expressed interest in receiving the msg

NTE: An autonomous system (AS) is a group of networks & routers under the authority of a single administration.

* Routing inside AS is called "intradomain routing"
* Routing between AS is called "interdomain routing".