

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 protocol are:

- HTTP : web browser
- SMTP : Mail communication
- FTP : File communication
- NTP : Network time protocol

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

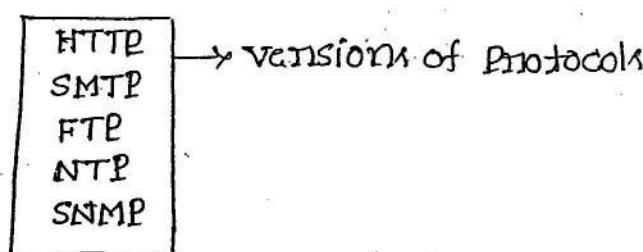
Network time protocol:

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



Network Management protocol:

DOS + All protocols = window NT



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

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

- * RFC Request for comment \rightarrow standard for computer networks.
- * Concept of computers n/w have an RFC number

RFC 1

RFC 2

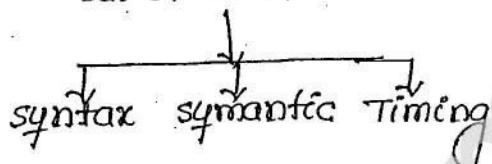
:

RFC 793 \rightarrow TCP/IP.

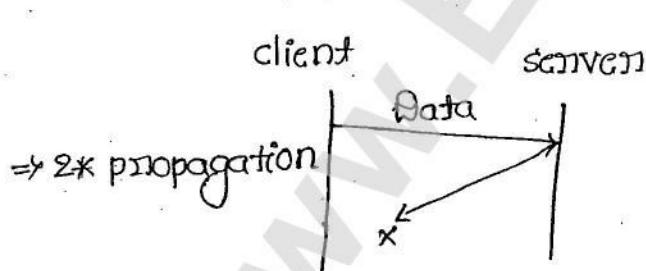
RFC 3700

Protocol: A set of rules and regulation or conventions

set of rules



- * Rules and regulations must be crystal cleared i.e. there must not be any duplicates and any invalid syntax is not acceptable.
- * Timing i.e. starting and ending a task must be mentioned.
- * syntax \rightarrow send acknowledge
- * semantic \rightarrow Receive acknowledgement.



* RTT is measure of delay b/w 2 hosts

- * Minimum ack. waiting time = $2 * \text{propagation (RTT)}$
- * Maximum ack. waiting time = $2 * (\text{min.ack. waiting time})$
 $= 2 * (2 * \text{propagation})$.
 $\therefore 2 * \text{RTT}$.

Round Trip Time \rightarrow RTT Turn over time \rightarrow Time out fil.

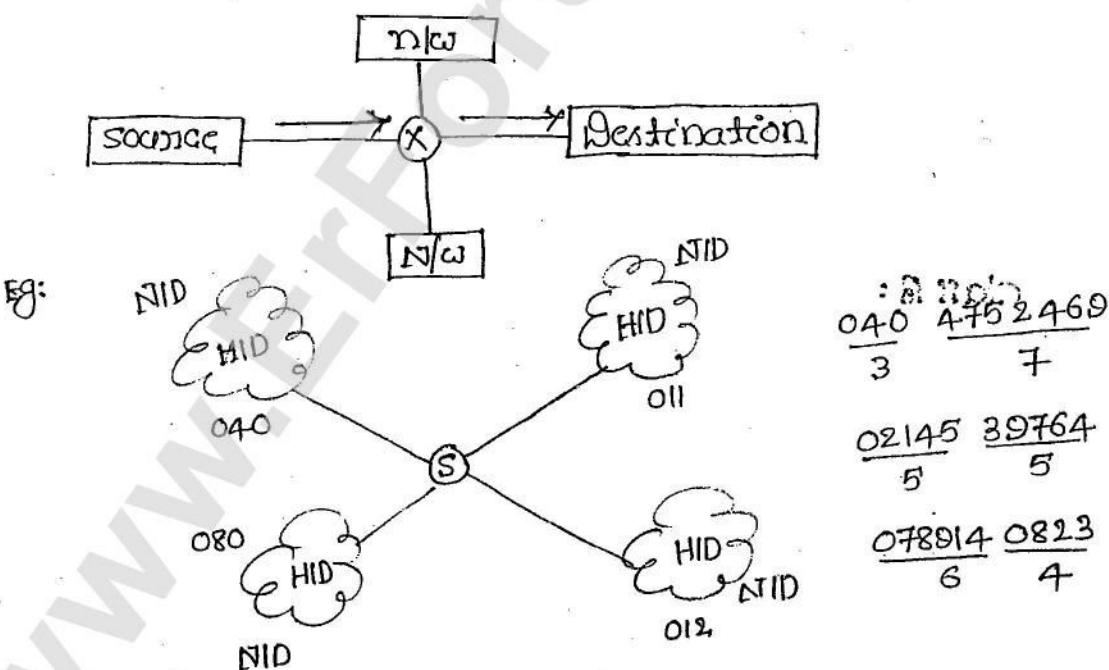
- * Protocol is an agreement between the communicating parties on communication is to proceed.

- * IP address does not refer to a host actually, it really refers to interface, if a host is on two networks, it must have 3 two IP.
- * A system may have multiple IP addresses and multiple physical addresses.

2. Identification:

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

- * identify the network \rightarrow logical
- * identify the host within the network, i.e. among all physical \leftarrow the destinations, one system is identified
- * identify the process within the host \rightarrow service point



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

1. 32-bit number

2. Two paths \rightarrow NID
 \rightarrow HID.

3. HID must be unique.

4. Hidden meaning.

Classification of IP Addresses:

To cover the needs of diff types of organizations

IP addresses are divided into Five classes.

class A:

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

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

eg: APSWAN Andhra pradesh state Wide Area Network

* IP address can be assigned to any electronic device.

class B:

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

Eg: Big organizations, MNC, Banks.

class C:

NID	HID
24	8
2^{24}	2^8
= 1.6 crn	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

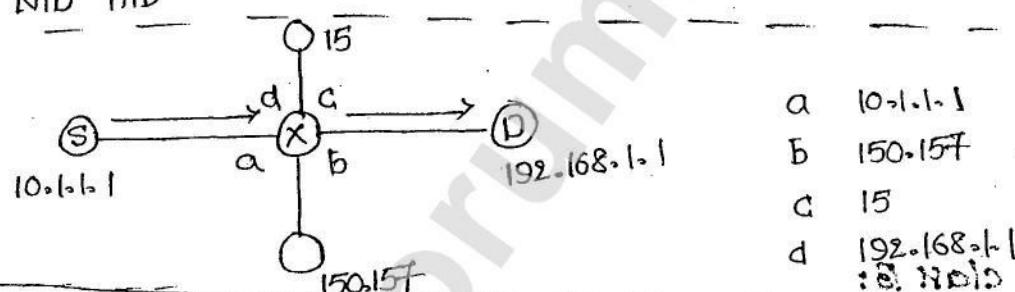
* 127 is a special IP address.

Eg: $\frac{150.167.1.1}{\text{NID} \quad \text{HID}}$ class B

} used in routing process

$\frac{192.168.1.1}{\text{NID} \quad \text{HID}}$ class C

Eg:



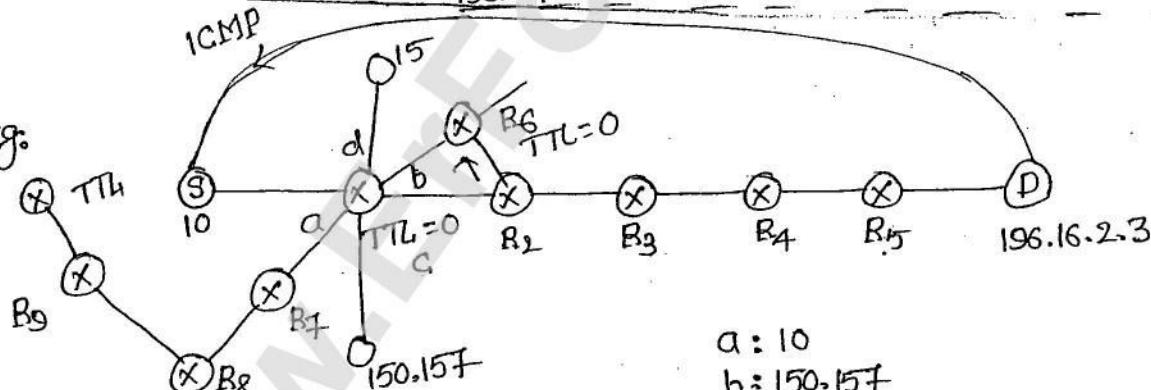
a : 10.1.1.1

b : 150.157

c : 15

d : 192.168.1.1
e : 8. No IP

Eg:



a : 10

b : 150.157

c : R2

d : 15

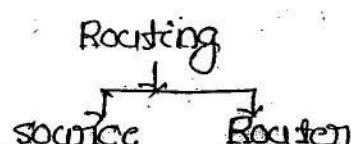
R2 : default

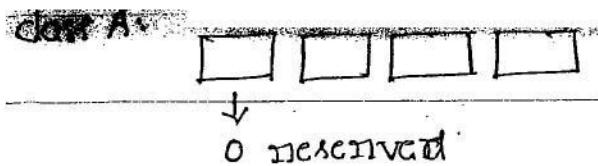
* consider default route (make dynamic route to avoid the wrong route through R7 to R9)

* MAKE TTL = 0

Eg: TTL = 3 min = 180 sec.

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





00000000 → X

00000001 → 1

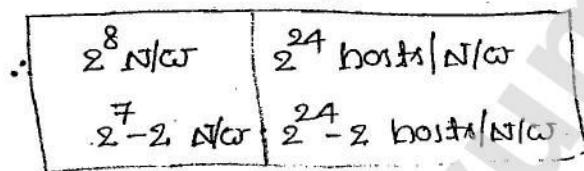
00000001 → 2

01111110 → 126

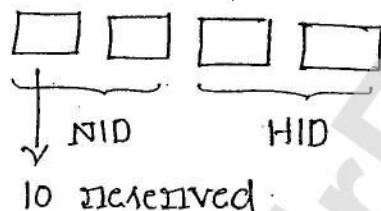
01111111 → 127 → X

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

∴ 10.0.0.0
10.255.255.255 } Not used



Class B:



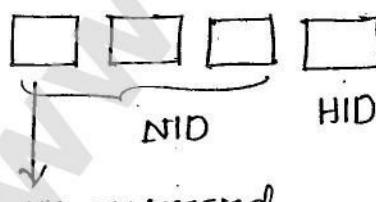
10 reserved

10000000 → 128
10000001 → 129

10111111 → 191

2^{16} N/W 2^{16} hosts/N/W.
↓
 2^{14} N/W 2^{16} hosts/N/W.

Class C:



110 reserved

11000000 → 192

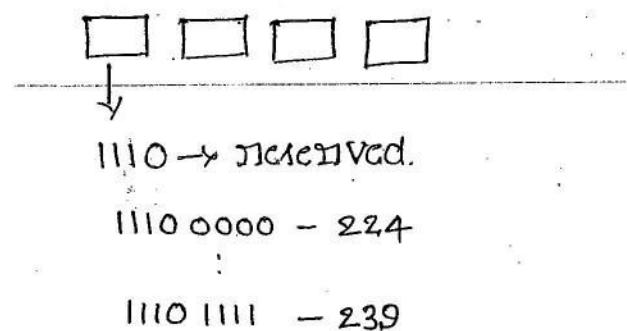
:

11011111 → 231

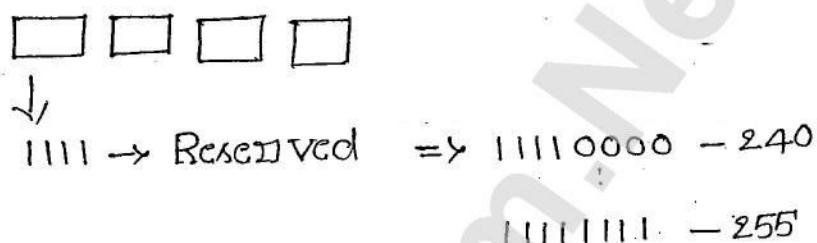
2^{24} N/W 2^8 hosts/N/W.
↓
 2^{21} N/W 2^8 hosts/N/W

Class D: it is designed for multicasting there is no NID on HID.

* The whole address is used for multicasting.



Class E: It is reserved for internet for special use.



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

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

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

* IP₄ → 32-bit addressing system

* IP₆ → 128-bit " "

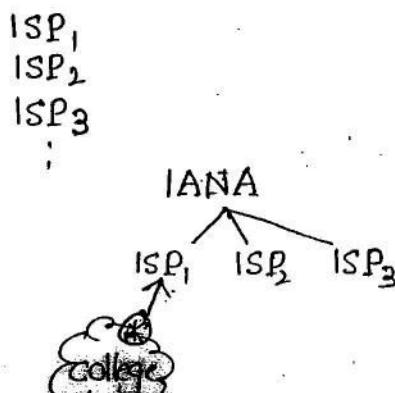
* windows 7 supports IP₆

* LINUX 10.6 also supports IP₆.

IANA: Internet Assigned Number Authority

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

ISP: Internet service provider.



- * A user can contact directly to IANA for address but it is time consuming so a mediation known as ISP handles the connection IANA and provider IP address.

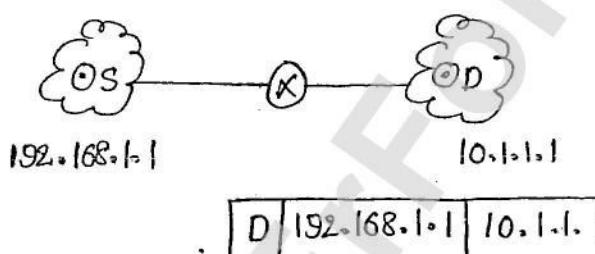
IANA (or) ICANN: Internet Corporation for Assigned Names and Numbers.

spoofing: using IP address of others by unauthorized users.

Types of communication:

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

Unicast:



Eg: Mail application (browsing webpage).

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, i.e. for group communication IGMP is used instead of IP.

Eg: sending group mail

yahoo.mail

Group IP address

10.1.1.1
10.1.1.2
150.157.1.107
200.200.200.1

192.168.1.1
224.8.10.10

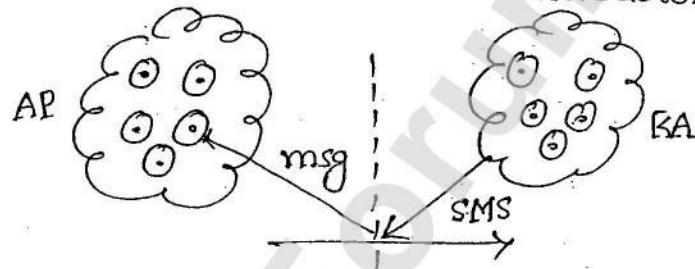
↓
source

↓
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.

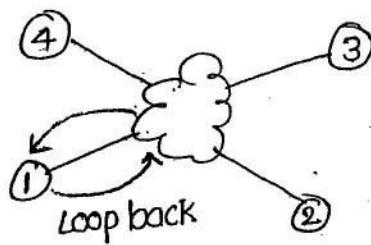
Eg: For any cast : Laptop.

- * 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.



* Address can be used source and destination 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 others then if there from others 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 others.

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 127.0.0.1 address. If source & dest. have similar address → not valid.

Limitations of logical addressing sys: :

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

Solutions:

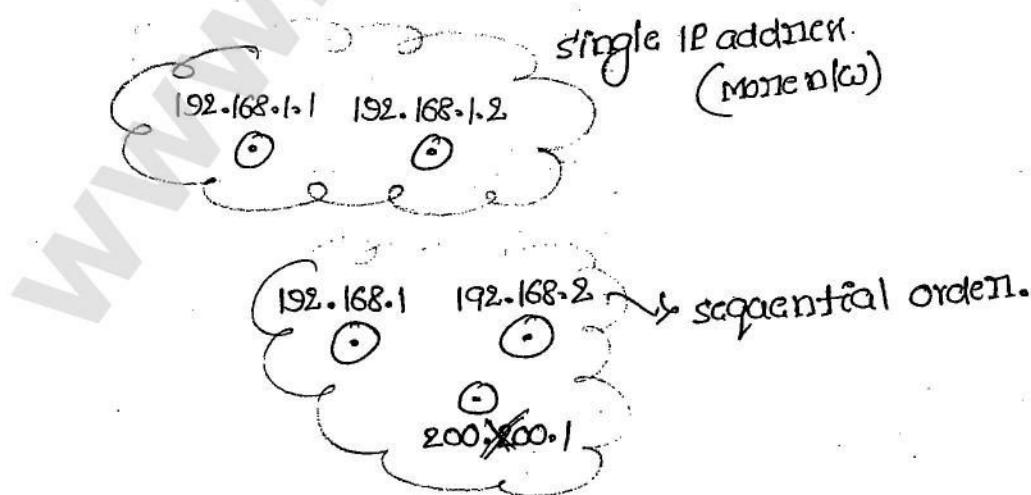
1. Supernetting
2. Subnetting
3. Physical Addressing system.

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 IDs 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".
- * process of dividing a single network into multiple subnets is subnetting.
- * Filtering and forwarding approach.

Advantages:

- * it improves security.
- * Maintenance and administration are simple.
- * Restructuring of the network 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 process of borrowing bits from host ID to generate subnet IDs is known as "subnet".
- * no. of bits borrowed is depend on our requirement.

Eg: To have 3 subnets in class C net, we suppose borrow 2-bits.

$$\therefore \text{No. of subnets possible} = 2^2 = 4$$

$$\therefore \text{no. of systems per subnet} = 2^{6-2}$$

Eg: class B net. we have 100 subnets, we need 7-bit from HID
 no. of subnets = 2^7

$$\text{No. of hosts per subnet} = 2^{9-2}$$

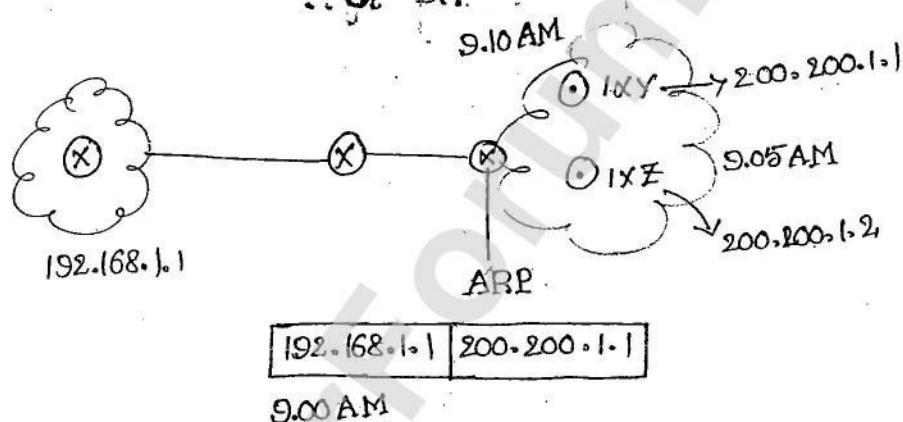
Limitations:

- * 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:

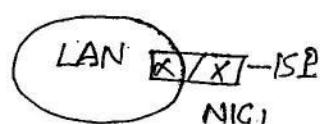
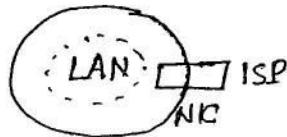


* If a system having IP = 192.168.1.1 sends data to other systems 200.200.1.1 at 9:00 AM. Meanwhile if the destination system changed its IP, then data is sent other systems.

* 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 \Rightarrow logical \Rightarrow different

IXY \Rightarrow physical \Rightarrow unique (IMEA)



* By using one IP address a hacker easily attack the sys
 so proxy IP address is maintained. such that if one IP₁ through then the connection b/w IP₁ and IP₂ is disconnected so the system within the LAN are safe.

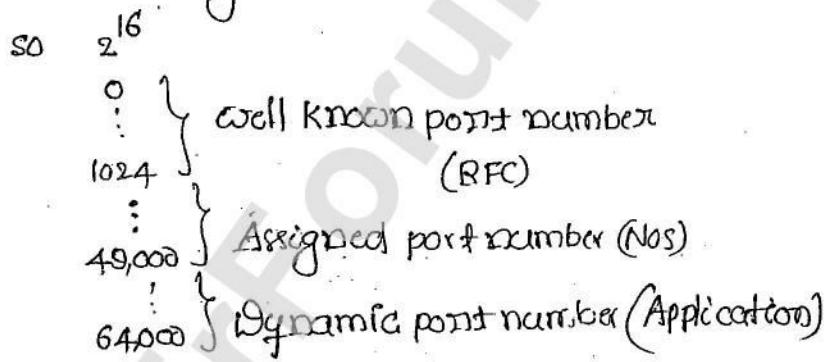
Logical: 32-bit - Network layer - IP - s/w → not permanent

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



various types of objects in computer networking:

- * workstations and servers (7 layers)
- L₁ * Hub - 1 (Physical layer)
- L₂ * switch - 2 (Physical, Datalink layer)
- L₂ * Bridge - 2 (PL, DLL)
- L₃ * Router - 3 (PL, DLL, NL)
- * Broadcast - 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 servers maintain some Access Control List (ACL) which represent the accessibility of programs by the client.
- * The unaccessible programs are denied by server.
- * Servers may have several applications.

Eg: OS server, DB server.

2. HUB:

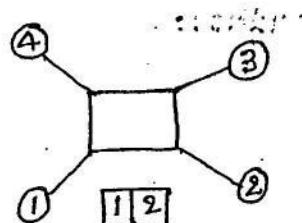
- * it is used to connect multiple workstations and servers.
- * it is a passive device, no sw associated with this.
- * it is a broadcasting device.

Advantages:

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

Disadvantages:

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

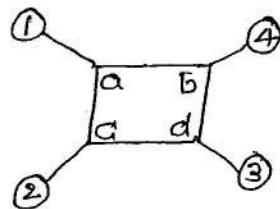


3. Switch:

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

Advantages:

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



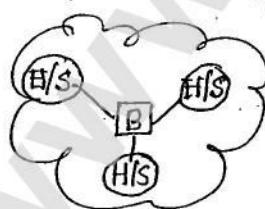
a	1
b	2
c	3
d	4

DisAdv:

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

4. Bridge: (PL, DLL)

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



H/S \Rightarrow Hub/switch.

Router:

- * it is a sophisticated WAN device and its principle is based on addressing system
- * it is used to connect two or more different similar networks.

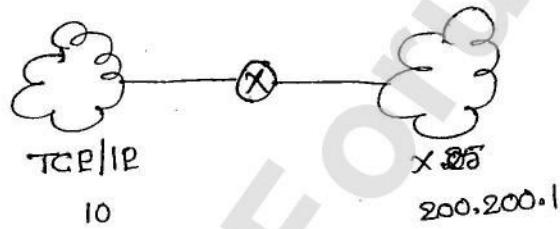
- * it requires a lot of configuration. while as bridge and switch are.
- * All routing algorithms are running in a router. so the cost of a router is very high.

6. BroUTERS:

- * Routers are devices that combine the functions of both bridges and routers.
- * They operate at both the data link and network layers.
- * It is combination of Router and Bridge.

7. GATEWAY:

- * It is used to connect 2 or more different & similar networks.

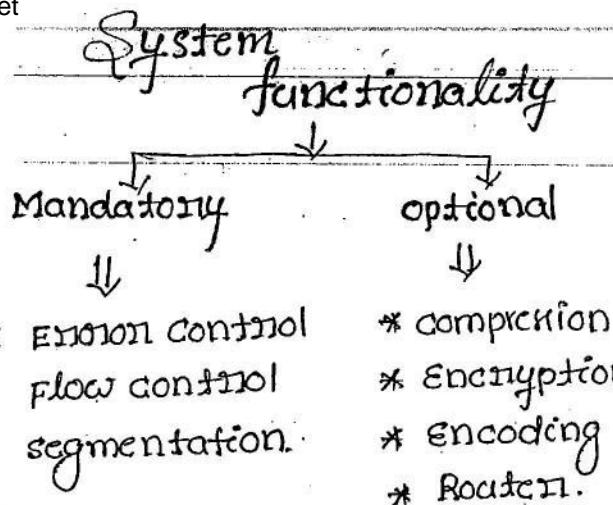


- * A gateway is a protocol converter.
- * A gateway can be
 - stand alone computer with special software and several NIC.
 - software installed in a router.
 - A front end processor (FEP) in a mainframe.

=

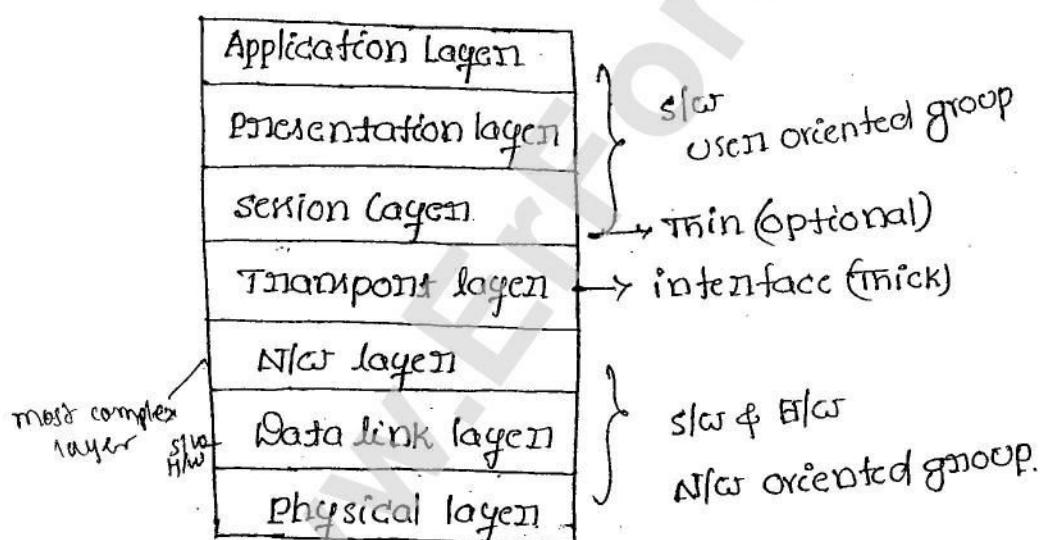
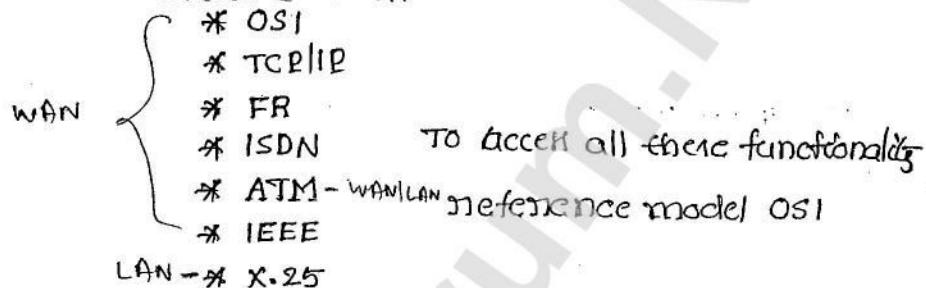
Appn layer Gateway = Router

Network layer Gateway = Gateway.



Total \Rightarrow 70 functionalities

Reference model:-



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

connection-oriented & connectionless communication:

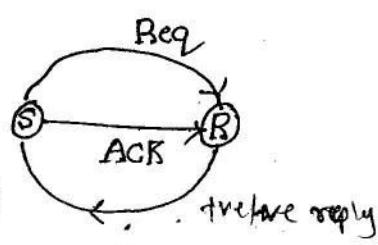
Connection-Oriented:

Three-way-handshake

1. Connection establish

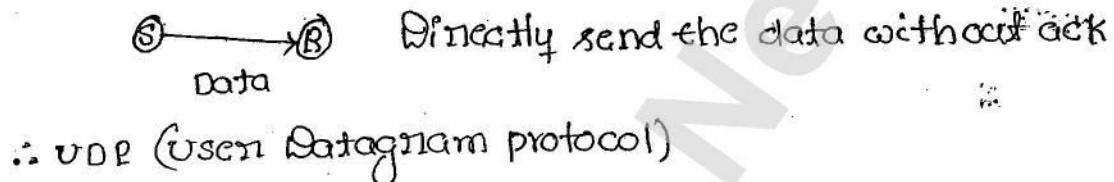
2. Transfer

3. Terminate connection

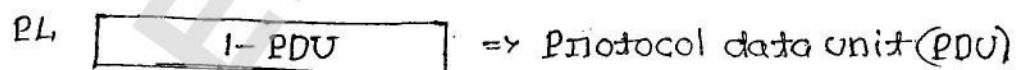
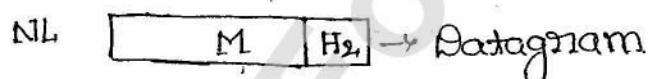
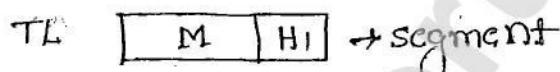


- * Reliability is high
if accept \Rightarrow +ve reply
otherwise -ve
- * Protocol is TCP (Transmission control protocol).

connection-less:



user



1. Physical Layer:

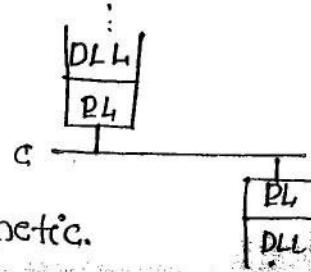
* it defines electrical, mechanical, functional and procedural specifications of interface and media are providing for sending a bit stream on a computer network.

through
 * interface is ^ NIC Network interface card.

Representation of bits:

C: Electrical
(coaxial)

F: Light signal



Physical layer converts the digital to electrical and vice versa.

1. it defines transmission mode.

→ simplex → Keyboard cable

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

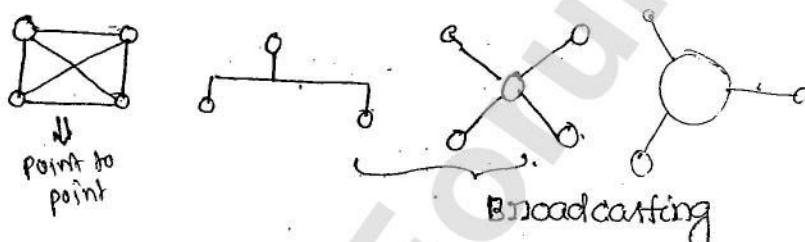
→ Full-duplex → Both can talk simultaneously.

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

2. it defines link configuration

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

* Broadcasting link (A single channel for all sources)



* it defines topology configuration.

→ it maintains fixed rules.

2. Data link layer:

* DLL transmits frames of data from computer to computer.

* Responsibility

→ Error control

→ Flow control

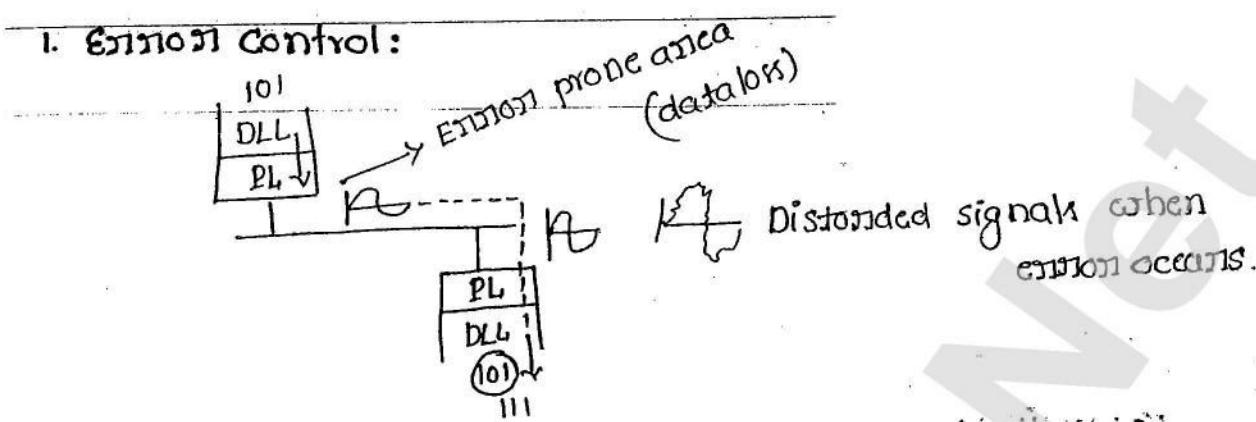
→ Access control

→ framing

→ physical addressing system 48 bit

MAC
Ethernet
LAN
NIC

1. Error Control:



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

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



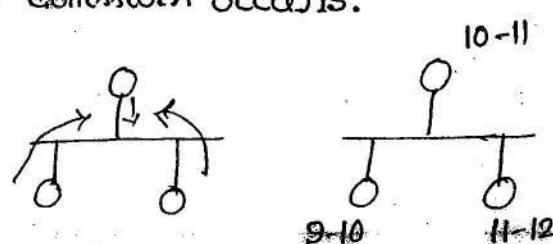
- * Based on the server's capacity client sends the data.

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

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

3. Access Control:

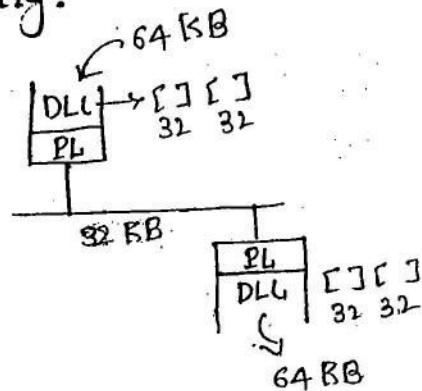
- * Time slot mechanism is allotted to all the stations since lot of collision occurs.



Sophisticated access control mechanisms:

- * ALOHA
- * CSMA/CD
- * CSMA/CA
- * TP.
- * User can generate any sized data.

Framing:



- * Framing - LAN
- * Segmentation - WAN

- * The link capacity is 32-bits.
- * PL converts any sized pkts into 64 KB.

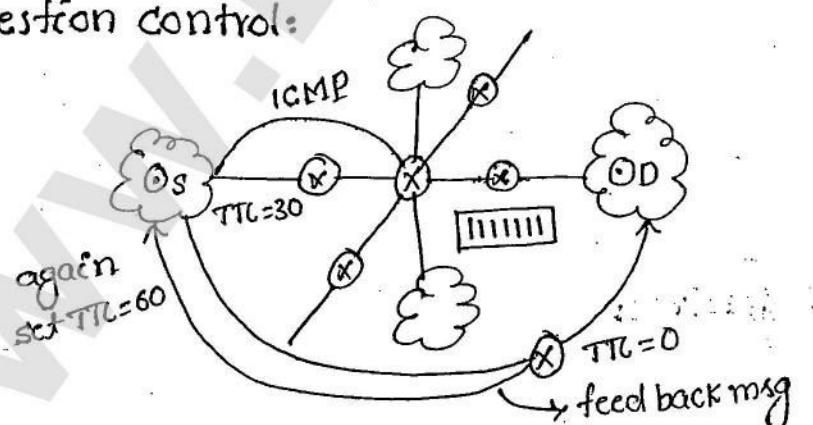
3. Network layers:

Responsibilities:-

- * Logical addressing system
- * congestion control
- * Routing
- * Feedback message \Rightarrow PING

ICMP \Rightarrow Internet Congestion Message protocol

Congestion control:

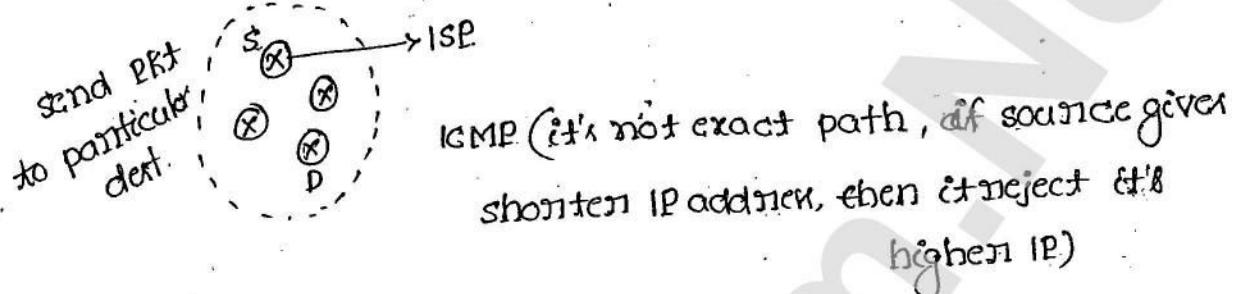


- * If the data is full in all the buffers of the routers, then it is called as congestion.
- * To control congestion, routers send the messages to the source to stop transmission of packets by knowing

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

Feedback message:

- * The receiver sends ICMP to the source.



- * Logical address system is temporary.

- * Physical address system is permanent.

4. Transport Layer:

Responsibilities:-

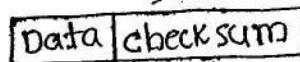
- * Application identification
- * client-side-entity identification
- * segmentation and Re-assembly
- * Multiplexing & De-multiplexing
- * service-point addressing system.
- * Error control.
- * Transmission error detection.
- * Flow control.
- * TL offers end-to-end communication between end devices 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 (Data link layer)

→ End-to-end (Transport layer)

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



* CRC → check Link errors → DLL.

* checksum → check end-to-end 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 parameters negotiations

→ partitioning of services into functional groups.

→ ACK of data received during a session.

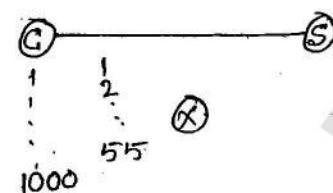
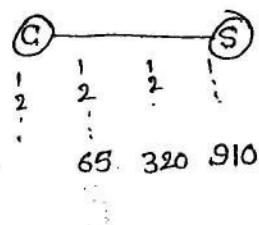
→ Maintaining checkpoints / synchronization points

→ Grouping of operations.

checkpoint maintenance :

Eg: Downloading files.

DAP supports checkpoints



* when a file is being downloaded, 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, upto 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
- Graphic formatting
- content translation
- system specific translation.

7. Application Layer:

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

Maintaining harmony among protocols:

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

Eg: ATM for checking a/c details, http protocol is used and for transaction http is used

- User Interface design
- for file transfers
- Electronic mail
- Electronic messaging
- Browsing the www.

↓

security

maintaining harmony:

information flow from one protocol to another (ex. HTTP to SMTP & back)

Understanding user scenario (HTTP & HTTPS back end ele. must be main roles & responsibilities of application layer)

Application	DNS, FTP, TFTP, BOOTP SNMP, SMTP, telnet, FINGER	Gateway
-------------	---	---------

Presentation	HTTP, SMTP, SNMP	Gateway, Redirector
--------------	------------------	---------------------

Presentation	IEEE 802, IEEE 802.2 ISDN	Repeater, Hubs, Multiplexer, Amplifier
--------------	------------------------------	---

Advantages of Layering systems:

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

Dis Adv:

- * interdependency among layering systems \Rightarrow TCP/IP
- * Duplication of functionality.

OSI- Reference

\rightarrow 7 (seven) layers

\rightarrow No definition for multicasting \rightarrow it is clearly defined in TCP/IP

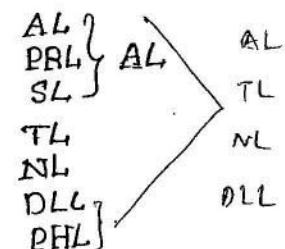
\rightarrow standards are ideal

\rightarrow NO flexibility

(Max. size of Pkt = 64 KB only)

TCP/IP

\rightarrow 5 layers



\rightarrow standards are practical.

\rightarrow Lot of flexibility.

(depends on characteristic of each layer.)



Sliding Window Protocol

Characteristics:

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

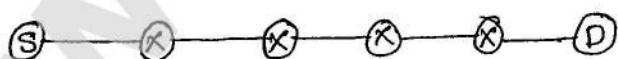
Different types of Delays:

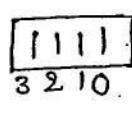
- * Queuing delay
- * Processing delay
- * Transmission delay
- * Propagation delay.

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

Queuing delay:

The amount of time packet is waiting in queue before being taken up for processing is known as "queuing 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 new ID, searching in the routing table, identifying destination route] is known as "processing delay".

- * It depends on router processing speed, but not size of the pkts.

* Transmission Delay: ($\frac{L}{B}$)

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

Eg:

$$\frac{L = 100 \text{ bits}}{B = 100 \text{ bits/sec}} = 1 \text{ sec}$$

Transferred bits

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

$$\boxed{\text{Transmission delay} = \frac{L}{B}}$$

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

Eg:

$$\frac{L = 100 \text{ bits}}{B = 10 \text{ bits/sec}} = 10 \text{ sec}$$

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

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".

$$\boxed{\text{Propagation delay} = \frac{d}{v}}$$

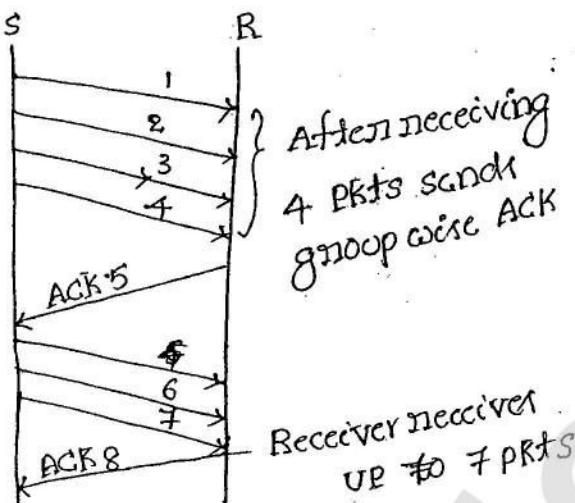
d = distance b/w routers

v = velocity of

$$RTT = 2 * \left[\text{propagation delay} + N \left(\text{queueing delay} + \text{transmission delay} + \text{processing delay} \right) \right]$$

Time out = $2 * RTT$
 TTL = $2 * \text{Timeout}$

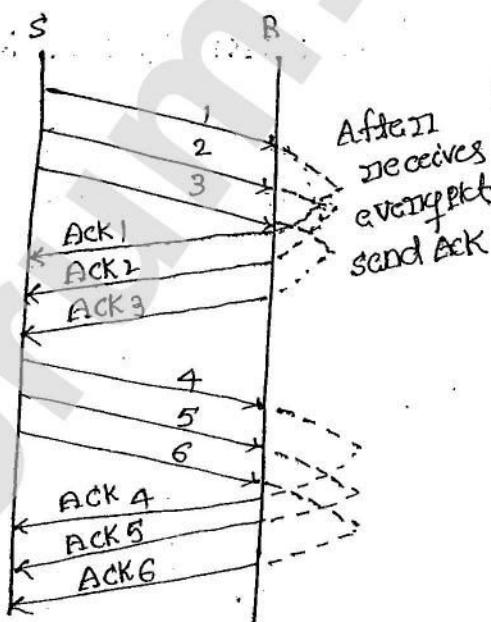
cumulative:



=> Network traffic is low

=> Reliability is low.

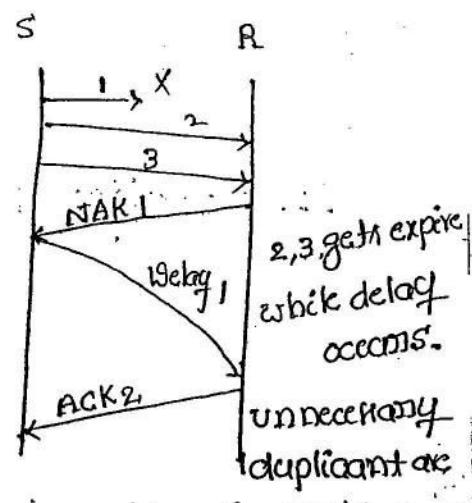
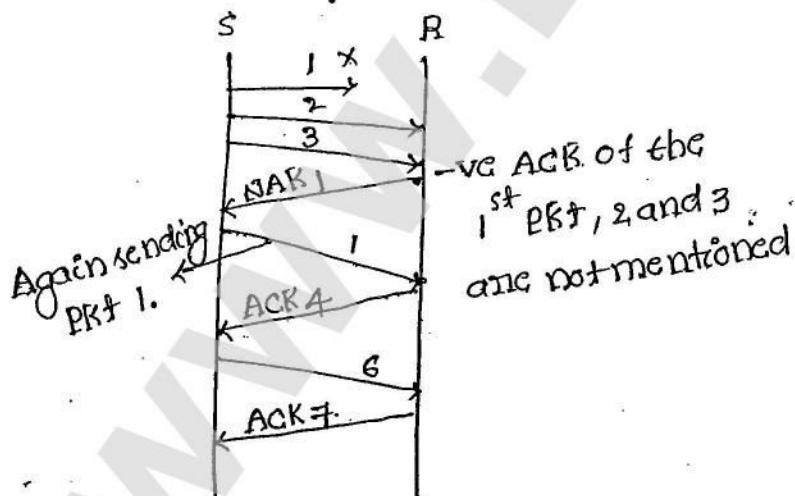
Independent:



=> Network traffic high

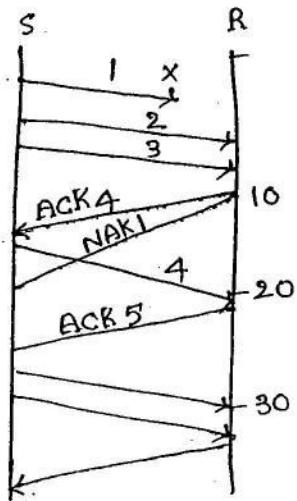
=> Reliability is high.

Care Study for cumulative:



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):
ie Maintaining certain time slots.



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

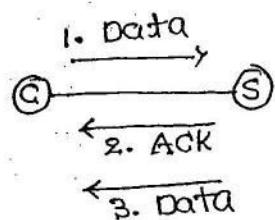
If first packet is lost at receiver side in cumulative after all packets are transmitted it send ACK. At the time the sender knows that first packet is lost.

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

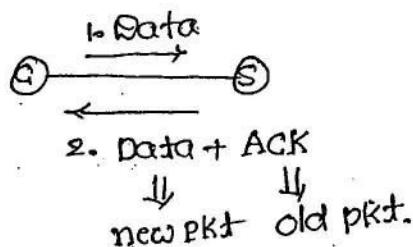
Piggy backing (web):

- Mainly used in web services
- To reduce the network traffic.

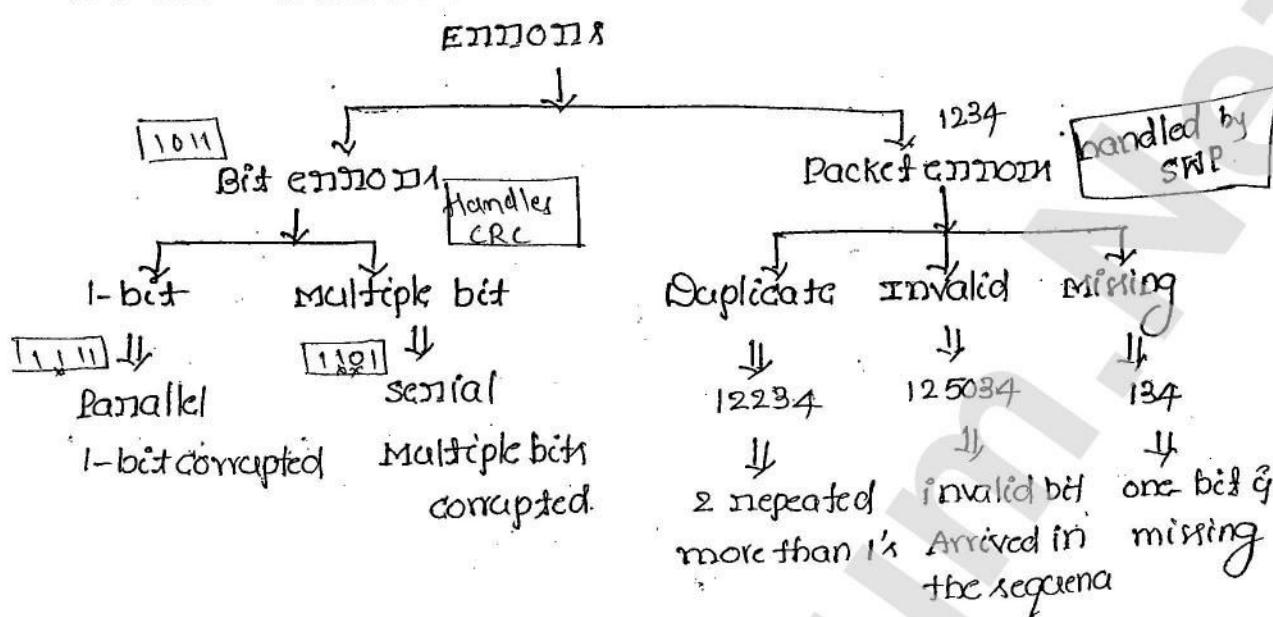
General Approach



Piggy backing:



Different types of errors:



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

B: Bandwidth.

$$B = 10 \text{ bits/msec}$$

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

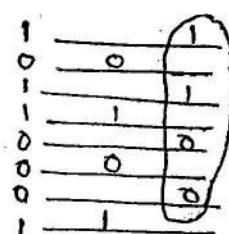
serial data transferred is : 10110001

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

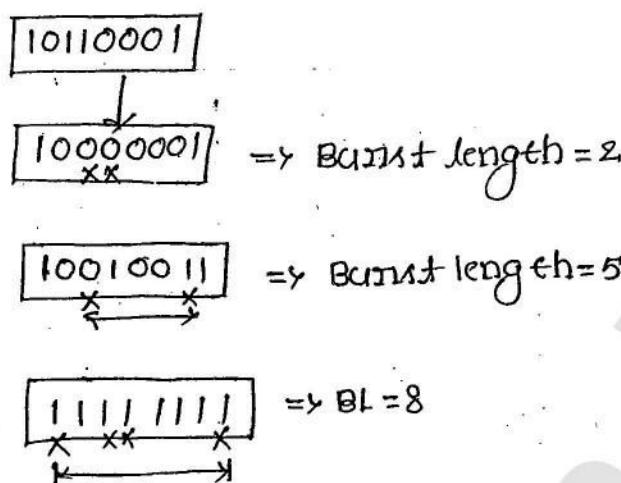
Parallel data transferred: - 1 -
- 0 -
- 1 -
- 1 -
- 0 -
- 0 -
- 0 -
- 1 -

* 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.

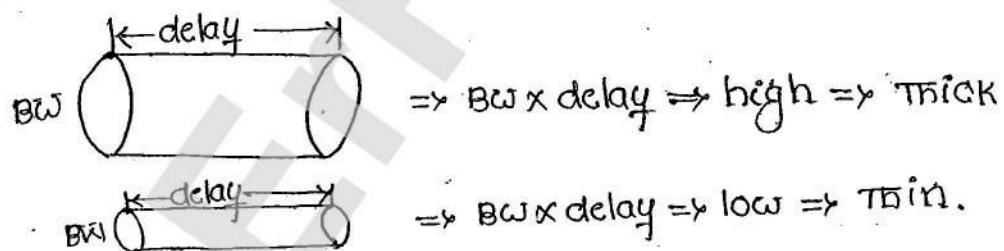


For synchronization and collecting the same bits a group. so for long distances it not support.



- * Burst length is calculated as bits present between starting and ending corrupted bits.
- * Burst length depends upon the type of OS, e.g. 32-bit OS the max BL = 32, (if) 64-bit OS then max BL = 64.
- * Based on the max BL CBC develops polynomials for error checking with x^{32} or x^{64} . $f(s) = s^{32} + \dots$ (if OS is of 32-bit frame check seq (FC))

Bandwidth delay:

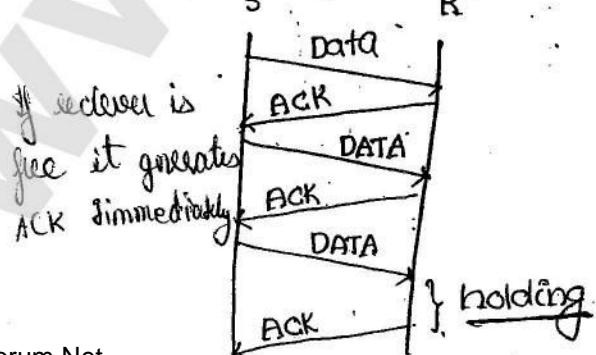


Stop-and-wait protocol:

STOP & USES 2 rules at sender side:

Rule: 1: Transfer only one packet at a time

Rule: 2: After receiving the ACK only then the other packet is transferred if source gets ACK for the pkt



for maintaining control

* 2 principles in sending

* 2 " " " " Received, it will hold ACK for a

when receiver busy it can't accept while & then releases the ACK. new PKTs, so at that time it won't send any ACK to sender.

Drawbacks:

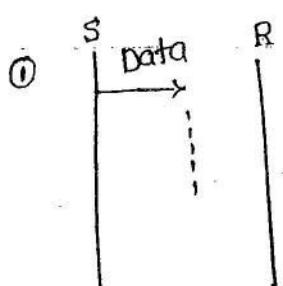


fig: Lost data packet

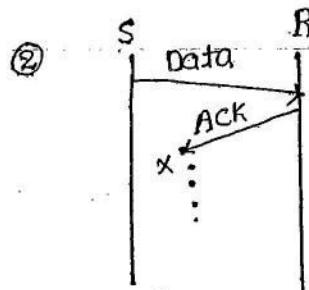


fig: Lost ACK

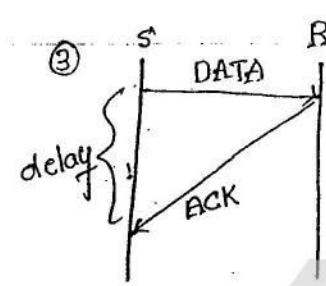
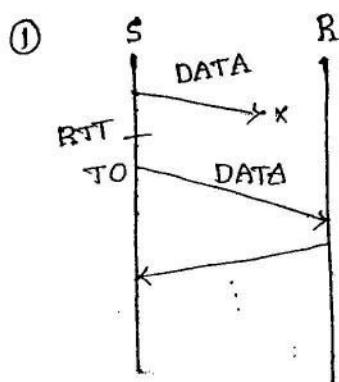
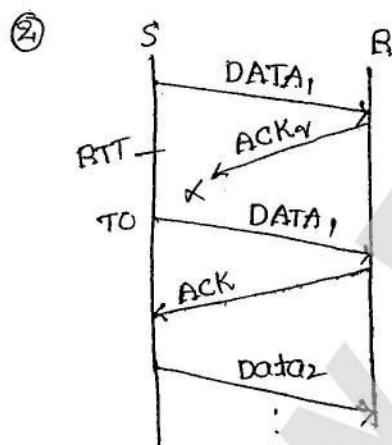


fig: Delayed ACK.



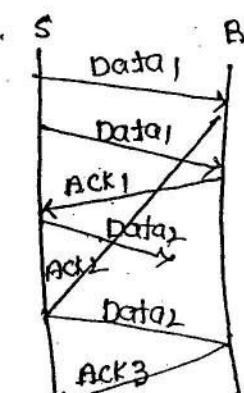
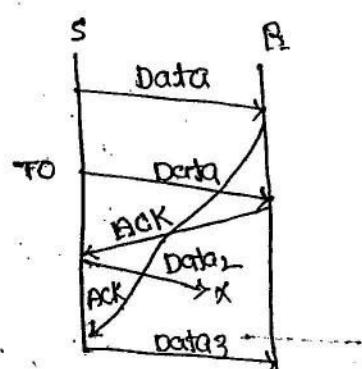
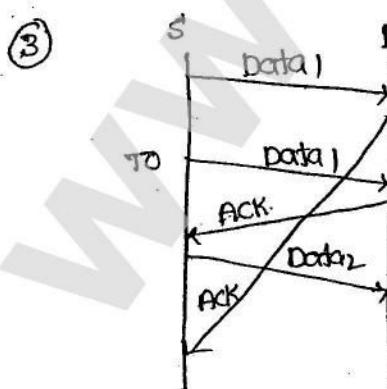
stop and wait + Time Out

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 by timeout.



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 means to have ACK of Data1, so not be get confused, sequence num is implemented.

stop & wait + Timeout + sequence num (Data)



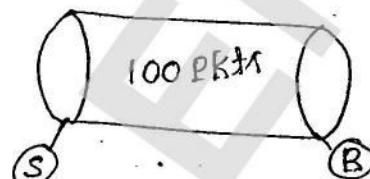
in order to not to get confused about the ACK of particular data packet, then the ACK sequence num also implemented.

$$\boxed{\text{stop\&wait} + \text{Time out} + \text{sequence num(Data)} + \text{Sequence num(ACK)}} \downarrow = \text{Stop \& wait ARQ}$$

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

Characteristics of stop\&wait:

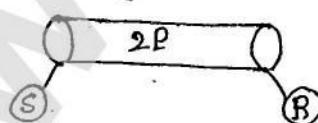
- * it uses the link between sender and receiver as a half-duplex link.
 - * Throughput of stop and wait protocol:
- $$\text{Throughput}(T) = \frac{1}{RTT} \text{Data}$$
-
- * if Bandwidth x delay product is very high then stop\&wait Protocol becomes useless.



$$\text{capacity} = 100 \text{ pkts}$$

filling pipe with 1 pkt then

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

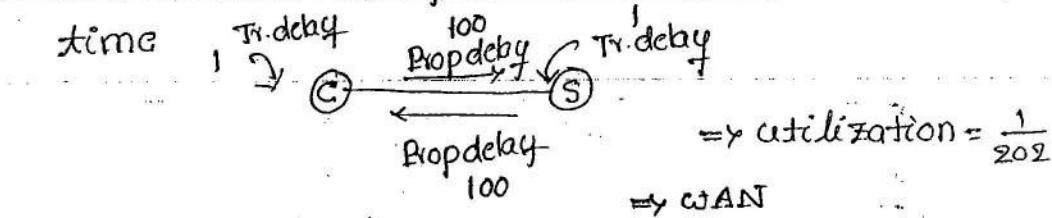


$$\Rightarrow \text{Efficiency} = \frac{1}{2} = 50\%$$

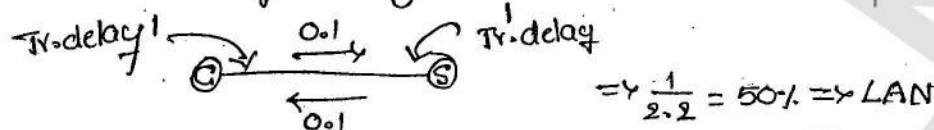
- * it is not suitable for WAN because delay is high only suitable for LAN.

- * If Propagation delay is high compared to transmission delay then, stop\&wait protocol becomes useless. efficiency is less.

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

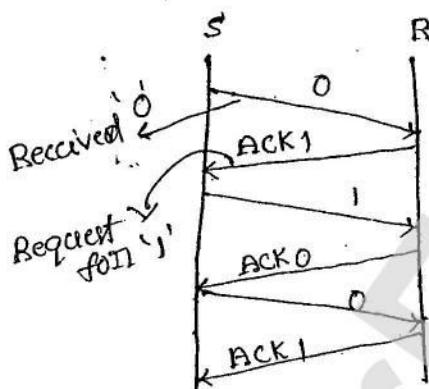


- * Transmission delay is high compared to prop.delay



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

- * Stop & wait protocols use only two sequence numbers.

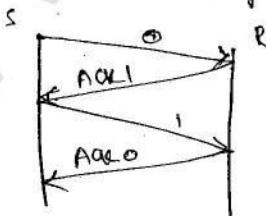


- * in special category of stop and wait protocol with window

Size is 1.

$$\text{stop\&wait} \Rightarrow S_W = R_W = 1$$

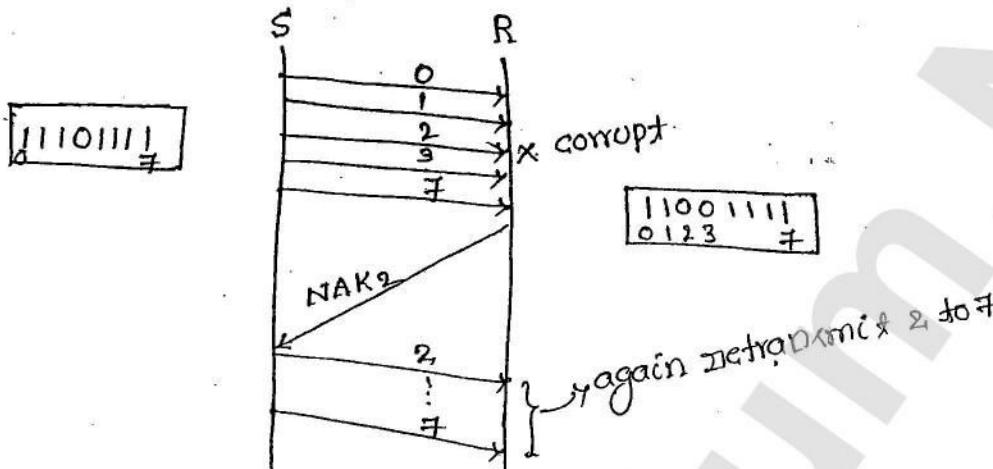
- * Stop & wait protocol req. only two seq. numbers (0,1)
irrespective of no. of packets sender is having.



www.ErForum.Net

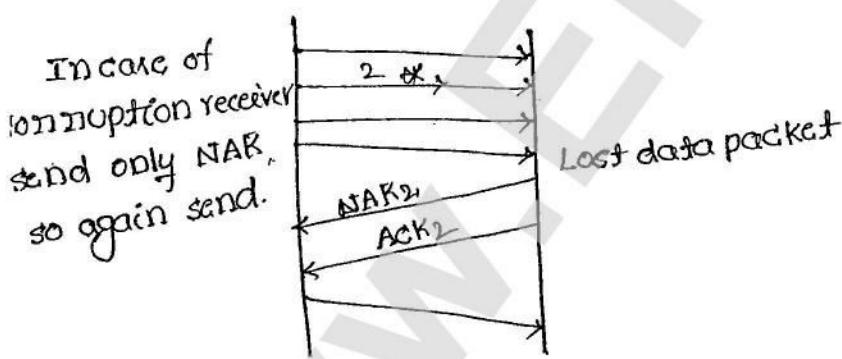
In this series sending packets if Pkt₂ is missing and all the seven pkts are being sent then NAK₂ is sent. Then 3 to 7 packets are being discarded and Pkt₂ is retransmitted

corrupted data packets:

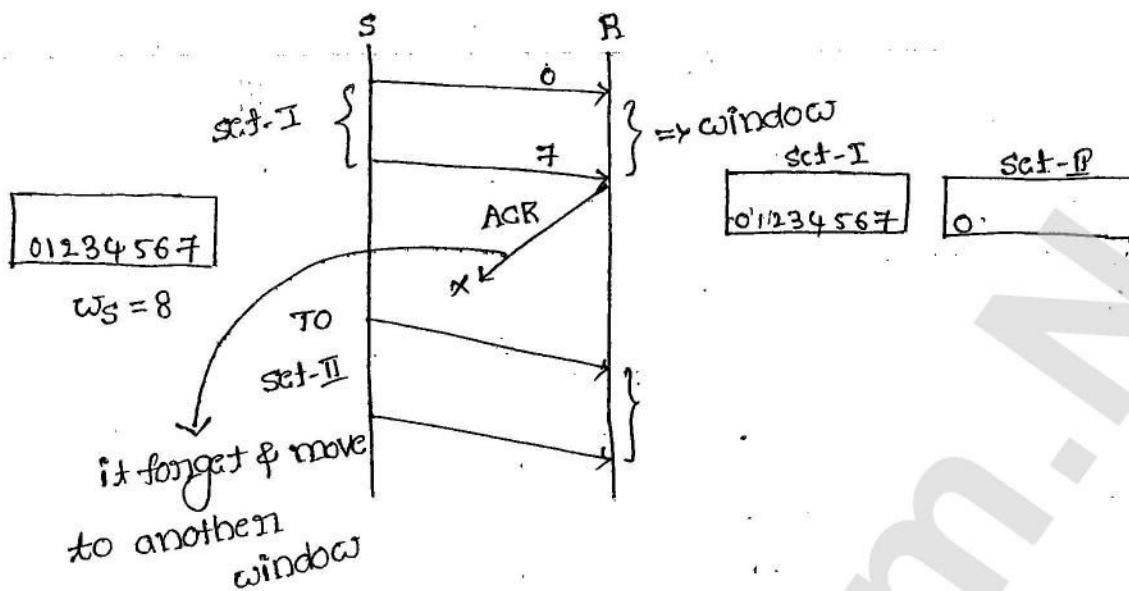


* only the lost packet have more impact than of the corrupted data packet.

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



so in order to overcome above problem of data lost while sending the NAK & ACK₂ is also being sent so that it represents that Pkt₂ is not received and then after sending Pkt₂ & can continue from ACK₂.



After time out, sender again send first window.

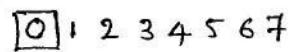
* To solve the above problem we have to re-adjust w_s, w_r size.

case(a): w_r size:

It is equal to 1 always irrespective of w_s size



$$w_s = 8$$



$$w_r = 1$$

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

case(b) w_s size:

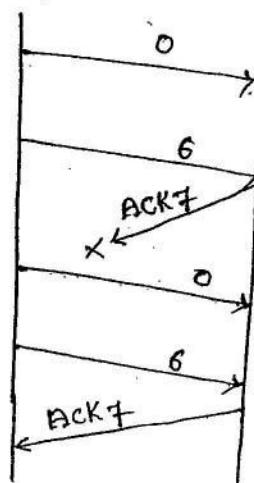
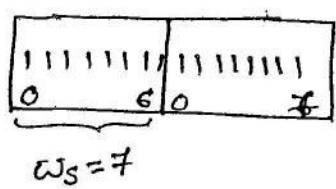
w_s size is calculated based on following formula

$$w_s + w_r \leq \text{Available sequence number (ASN)}$$

$$w_s = \text{ASN} - w_r$$

$$w_s = \text{ASN} - 1$$

Adjusting window size:



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

Eg: 0 15

Max available sequence num = 15

Eg: Total sequence number = 10

then $\omega_S = 9$, $\omega_B = 1$.

$\omega_S = 15$

$\omega_B = 1$

case(1): Assume $N = \text{Max available sequence number}$

$$\therefore \omega_S = N - 1$$

$$\omega_B = 1$$

case(2): If N is defined as max sequence number

$$\omega_S = N$$

$$\omega_B = 1$$

case(3): If 'R' is no.of bits available in sequence number R

$$\omega_S = 2^R - 1$$

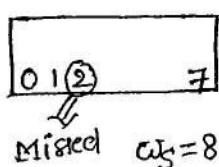
$$\omega_B = 1$$

=

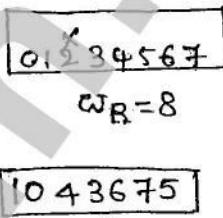
Selective Repeat:

- * Selective Repeat receiver never receives out of order packets.
- * It's natural choice is independent ACK (if possible, it will also use piggybacking)

1.



Selectively send
this packet to receiver.



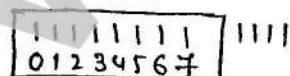
if receives any sequence
for checking which pkt is
lost it uses searching algo
we take more time

- * A searching algorithm is used.

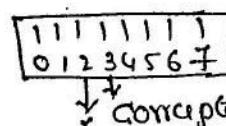
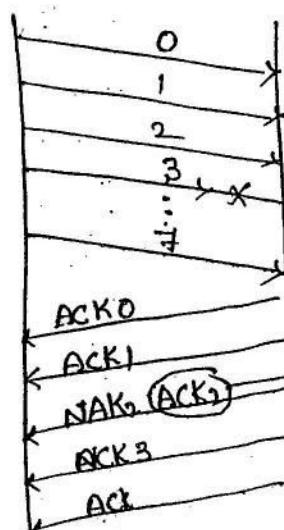
DisAdv:

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

② corrupted:

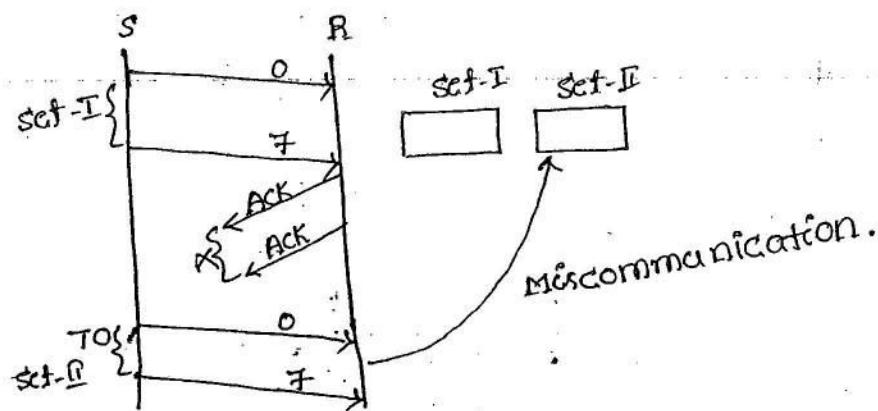


We won't resolve the
condition either packet is
lost or corrupted because
every time we send only
NAR



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

COST Acknowledgment:



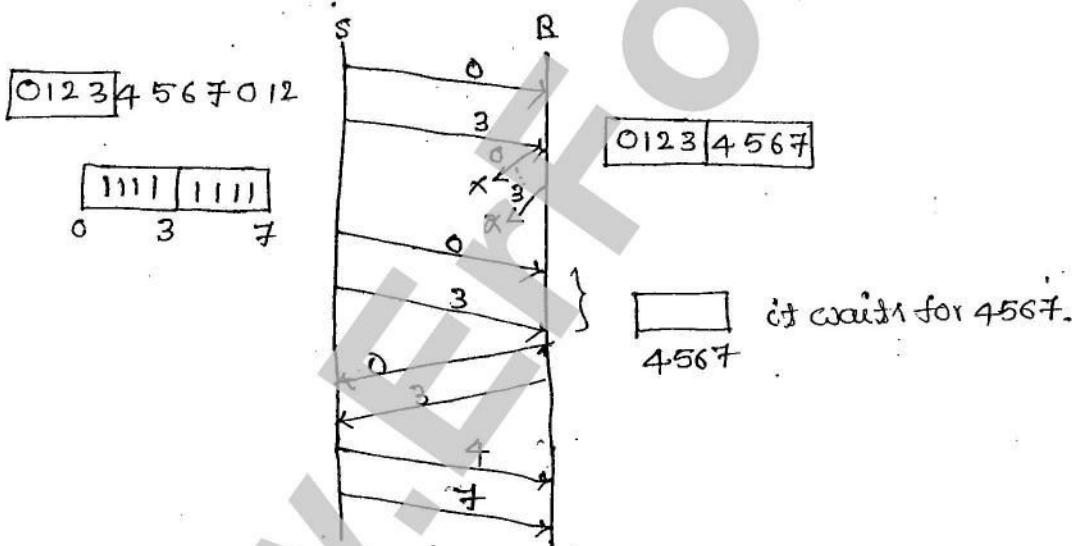
To solve the above problem, we re-adjust ω_S and ω_R based on the following formula

$$\omega_S + \omega_R \leq \text{ASN}$$

- * $\omega_S = \omega_R$

- * $\omega_S > \omega_R$

- * $\omega_S < \omega_R$.



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

$$\omega_S = \frac{N}{2}, \quad \omega_R = \frac{N}{2}$$

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

$$\omega_S = \frac{N+1}{2}, \quad \omega_R = \frac{N+1}{2}$$

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

$$\omega_S = 2^{R-1}, \quad \omega_R = 2^{R-1}$$

Eg: 8-bit sequence number.

Go-Back-N $\Rightarrow \omega_S = 7, \omega_R = 1$

Selective Repeat $\Rightarrow \omega_S = 4, \omega_R = 1$

For same available sequence number, GBN can transfer more packets

GBN $\omega_S = 7 \quad \omega_R = 1 \Rightarrow 8$

SR $\omega_S = 7 \quad \omega_R = 7 \Rightarrow 14$

Comparison:

Characteristic	Stop-and-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-and-Wait formula:

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

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

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

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

$$\therefore \text{Eff} L = BR \quad \eta = 50\%$$

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

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

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

Steps to be solved in stop process:

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 on "window of bits" (w_{bit})

$$3. w_{RTT} = \frac{w_{bits}}{(\text{Pktsize})_{bits}} = w_R$$

4. sequence number required = w_p

5. $z^K = w_p$ where $K = \text{no. of bits in sequence num. } P$.

Problems:

① $B = 1.5 \text{ Mbps}$

$\text{RTT} = 45 \text{ ms}$

$L = 1 \text{ KB}$

link utilization = ?

$$\begin{aligned} T &= \frac{\text{Data}}{\text{RTT}} \\ &= \frac{1024 \times 8}{45 \times 10^{-3}} = 182 \text{ Kbps} \end{aligned}$$

$$\begin{aligned} \eta &= \frac{T}{B} = \frac{182 \text{ Kbps}}{1.5 \text{ Mbps}} \\ &= \frac{182 \times 10^3}{1.5 \times 10^6} \\ &= 0.121 \end{aligned}$$

② packet size = 1000 bytes.

A) $d = 10 \text{ KM}$

B) $d = 5000 \text{ BM}$

$$\begin{aligned} v &= 70\% \times 3 \times 10^8 \text{ m/sec} \\ &= 0.7 \times 3 \times 10^5 \text{ Km/sec} \end{aligned}$$

$$v = 2.1 \times 10^5 \text{ Km/sec}$$

A) Propagation delay = $\frac{d}{v}$

$$= \frac{10 \text{ Km}}{2.1 \times 10^5 \text{ Km/sec}} = 0.476 \text{ msec}$$

$$\begin{aligned}
 RTT &= 2 * \text{propagation delay} \\
 &= 2 * 476 \\
 &= 952 \text{ msec}
 \end{aligned}$$

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

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

$$RTT = 95.2 \times 500 \text{ msec}$$

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

(3) Packet size = 1 KB

$$\text{Propagation time} = 15 \text{ ms.}$$

$$B = 10^9 \text{ bits/sec}$$

$$RTT = 30 \text{ msec} \quad \text{Transmission time} = \frac{L_B}{B} = \frac{1024 \times 8}{10^9} = 0.008 \text{ msec}$$

$$\begin{aligned}
 \text{Utilization} &= \frac{1}{30 + (0.008)2} \\
 &= \frac{1}{30.016} \\
 &= 0.033 \\
 &= 3.3\%
 \end{aligned}$$

④

$$B = 4 \text{ kbps}$$

Propagation delay = 20 m/sec

$$\eta = 50\%$$

RTT = $2 * \text{propagation}$

$$= 40 \text{ msec}$$

$$L = BR$$

$$\eta = 50 \text{ then } L = BR$$

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

$$= 160 \text{ bps}$$

⑤

Propagation delay = $100 \mu\text{s}$

$$d = 20 \text{ KM}$$

$$L = 1 \text{ KB} = 1024 \times 8$$

$$B = ?$$

RTT = Transmission delay.

$$RTT = 200 \mu\text{s}$$

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

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

$$= 40 \text{ mbps}$$

⑥

$$B = 1 \text{ mbps}$$

Latency delay (or) propagation delay = 1.25 sec

$$L = 1 \text{ KB}$$

$$\text{RTT} = 2 \times 1.25 \\ = 2.5 \text{ sec}$$

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

$$2.5 \text{ sec} \quad ?$$

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

$$3. \quad w_p = \frac{w_{\text{bit}}}{(\text{pkt size})}$$

$$= \frac{2.5 \times 10^6}{1024 \times 8}$$

$$= 305.$$

$$\therefore 2 = 305$$

$$\therefore K = 9$$

$$4. \quad \text{Session rate} = w_p = 305$$

Ques: window size = 5 packets

Data packet = 1000 bytes

Transmission time for such packets = 50 μs

Propagation delay = 200 μs

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

$$\begin{aligned}
 \text{RTT} &= \text{Tr.delay} + 2 * \text{propagation} \\
 &= \frac{5 \times 1000 \times 50 \times 10^{-6}}{200 \times 10^{-6}} \\
 &= \frac{5 \times 1000}{50 + 400 \times 10^{-6}} \\
 &= \frac{5 \times 1000 \times 8}{450 \times 10^{-6}} = \\
 &= 88.88 \times 10^{-6} \text{ bits} \\
 &= 11.11 \times 10^{-6} \text{ bytes.}
 \end{aligned}$$

⑨

3960	40
------	----

S → R
 100×3960
 $100 \times 40(H)$
 $40(NAK)$

$$\frac{3960 + 40(\text{Retrans})}{8040}$$

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

⑩



$$WS = 4 \quad T = 2$$

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

"O" starts leaving at R.

∴ 123 are in Queue.

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

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

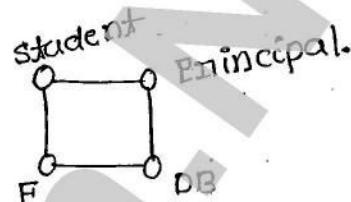
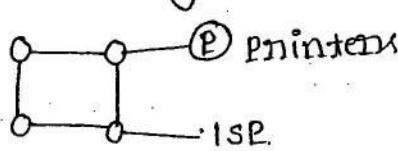
~~At t=5, 6 & 7 are in the Queue~~

~~t=10, 11 & 12 are in the Queue.~~

Lan Technologies

Advantages of LAN:

- * Resource sharing or resource utilization (Time & \$).
- * information sharing.



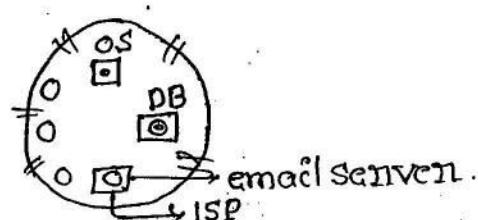
Types of LANs:

- * 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 (in) 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 pass no one can access	Based on types of user there are some restriction to some user to access data	There are restrictions on some data or some files.

Peer-to-peer LAN:

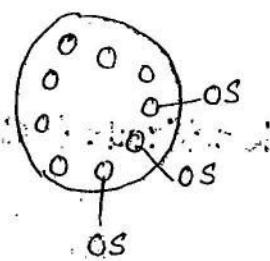
As in dedicated server LAN's, there is no requirement of network operating system and IP address.



ACE → workgroup



↳ 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 occurring "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: Banking 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 system

- * No real-time application, and Oracle application are possible.

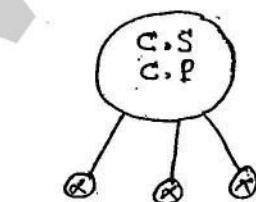
LAN components:

1. Network operating system.

2. Cable

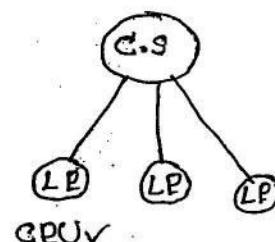
3. NIC

1. First generation

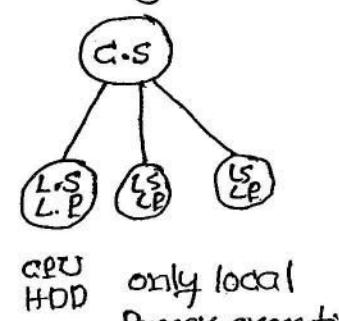


Eg: UNIX

2. Second generation 3. Third generation



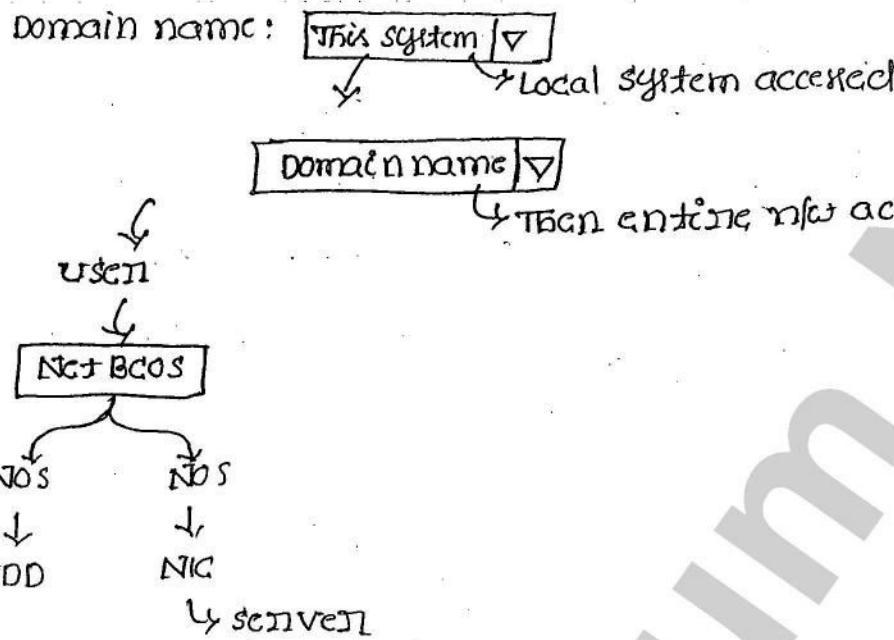
CPU
HDD
Thin client



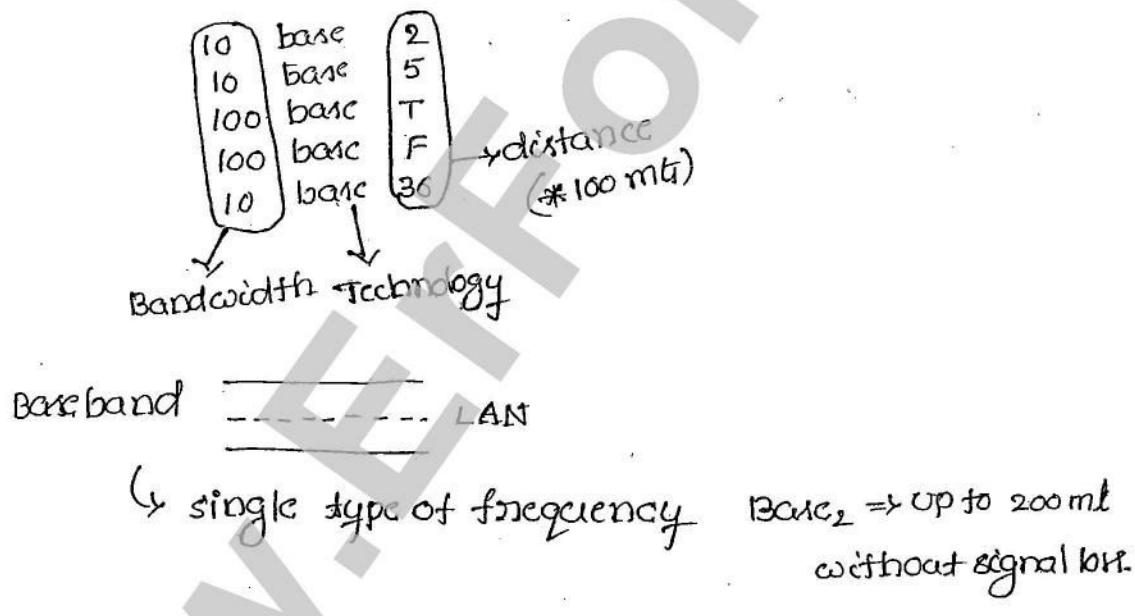
CPU
HDD
only local
process execute

Eg: Novell network

Eg: windows

UID :PWD :

2. Cable: Types of cables



Broadband : ----- WAN → Directly connected with
 ----- ISP → Dial-up connection

All types of frequencies are carried out.

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

Broadband 200 mtr we use repeaters.



- * Twisted pair \Rightarrow 100 mts 10 mbps
- * Fibre optic cable \Rightarrow 2000 mts
- * 100 base T \Rightarrow category 5 cables \Rightarrow bulky \Rightarrow RJ45 \Rightarrow connectors are used.
- * category 3 \Rightarrow incoming signals. To re-post the signals repeaters are used.

3. NIC: Hardware \rightarrow physical layer

PL + DLC \Rightarrow (combination of H/w & SW)

- * New 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.

LLC \Rightarrow 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
- 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.

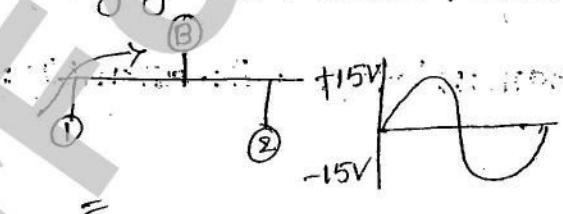
Ethernet

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 its transfer of data packet or else transmit the data packet from the current channel only.
- * The channel is sensed in terms of voltage if $V=0$ not wave form, i.e. no channel is engaged to transfer packet (Media is free)

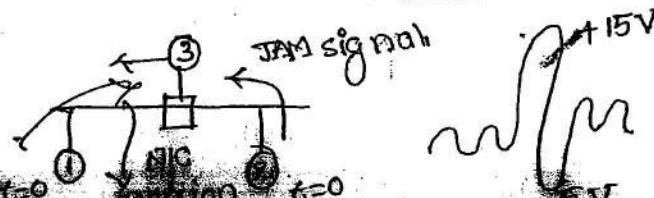


Multiple Access:

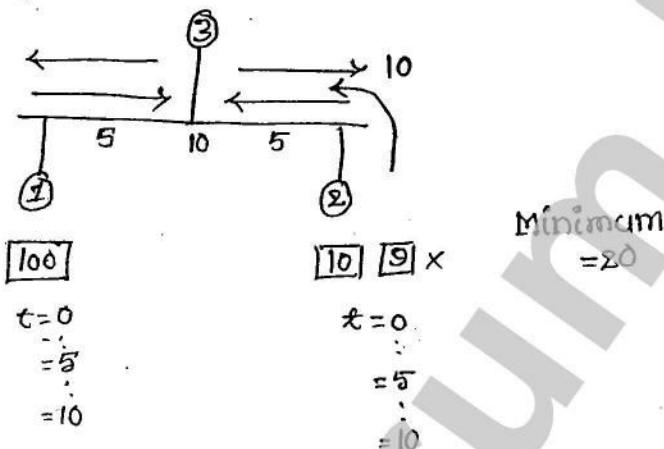
- * If more than one channel, sense the medium, both the channels try to access the medium and want to transfer data packets simultaneously then it is called "multiple access".

Collision Detection:

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

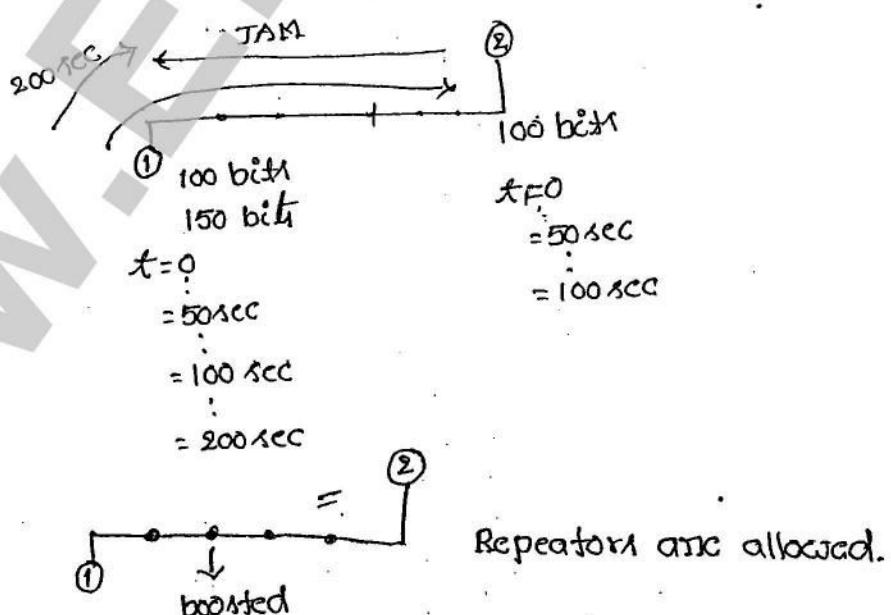


- * All channels are having different frequency and jam signals have different frequency so there is no chance of collision occurrence.
- * Since channels have different frequency \Rightarrow Bandwidth increases.



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.

$$\boxed{\text{RTT} = \text{Transmission Delay.}} \Rightarrow 2 * \frac{d}{v} = \frac{L}{B}$$



$$\Rightarrow 2 * \frac{d}{v} = \frac{L}{B} \Rightarrow 2 * \left(\frac{d}{v} + 4 * \text{Repeater delay} \right)$$

$$57.6 \text{ msec} = \frac{L}{v}$$

Basic Ethernet Fast Ethernet Gigabit Ethernet

10 mbps

2500 mts

72 bytes

100 mbps

250 mts

72 bytes

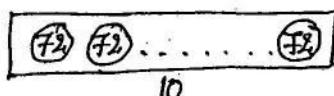
1 Gbps

250 mts

72 bytes

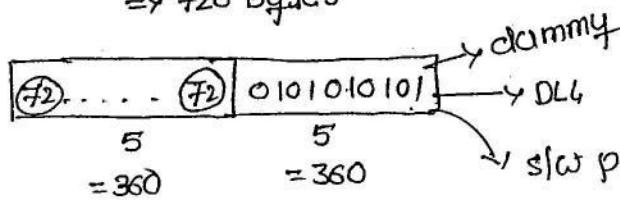
Basically 25 mts

720 bytes



10

=> 720 bytes

5
=3605
=360dummy
DLQ

slow padding

 - H/w packing

Backoff Algorithm:

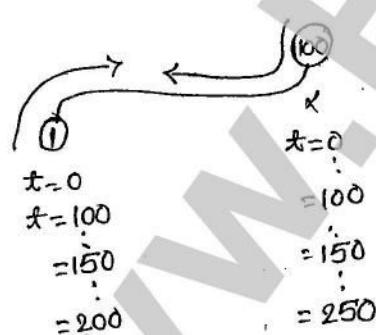
it gives waiting time for stations that are involved in collision

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

where $K \rightarrow$ randomly derived

from 0 to $2^n - 1$.

where n - collision number.



Case Study:

$$0 \times 51.2 \mu\text{sec} = 0$$

$$\epsilon = 0 \\ = 100\text{sec}$$

 $n = 1, 2, 3$

$$1 \times 51.2 \mu\text{sec} = 51.2 \mu\text{sec}$$

$$= 100\text{sec}$$

$$n = 1, 2, 3 \\ = 0, 1, 2, 3, \dots$$

$$\begin{aligned} \text{Let } n=1 \\ k=0 \text{ to } 2^n-1 \\ \Rightarrow 0 \text{ to } 2-1 \\ \Rightarrow 0,1 \end{aligned}$$

$$\begin{aligned} \text{Let } n=1 \\ k=0 \text{ to } 2^n-1 \\ \Rightarrow 0,1 \end{aligned}$$

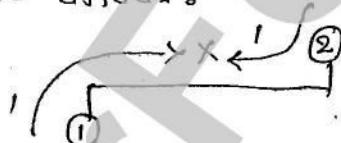
* if let us consider $k=0$ to channel 1 and $k=1$ to channel 100
then waiting time of channel 1 = $0 \times 51.2 \mu\text{sec}$
 $= 0$

waiting time of channel 2 = $51.2 \mu\text{sec}$.

.. so channel 1 have waiting time = 0, then it can transfer the data packets but channel 2 must wait upto $51.2 \mu\text{sec}$. & then again back-off algorithm is applied to proceed the transmission through either channel or others.

Limitations of Back-off Algorithm:

capture effect:



$$\begin{aligned} \text{Let } n=1 \\ \therefore k=0 \text{ to } 2^n-1 \\ = 0,1 \end{aligned}$$

$$\begin{aligned} \text{Let } n=1 \\ k=0 \text{ to } 2^n-1 \\ = 0,1 \end{aligned}$$

$$\text{Then } WT = 0 \times 51.2 \mu\text{sec} \\ = 0,$$

$$\begin{aligned} WT = 1 \times 51.2 \mu\text{sec} \\ = 51.2 \mu\text{sec} \end{aligned}$$

$$\begin{aligned} n=2 \\ k=0 \text{ to } 2^n-1 \\ = 0 \text{ to } 2^2-1 \\ = 0,1,2,3 \end{aligned}$$

↓

if after $51.2 \mu\text{sec}$ again another channel also wants to access the medium, then again backoff algorithm is applied then $n=2$.

Then repeat same for

$$n=3$$

$$\begin{aligned} k=0 \text{ to } 2^3-1 \\ \Rightarrow 0,1,2,3,4,5,6,7, \end{aligned}$$

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

①	100	1	100
0 1	0 123	0 1	0 1234567
0	0	0	0
0	1	0	1
0	2	0	2
0	3	1	3
1	0	0	4
1	1	1	5
1	2	1	6
1	3	1	7

Data specifications:

① Data rate

$$\Rightarrow 10 \text{ mbps}$$

$$\Rightarrow 100 \text{ mbps}$$

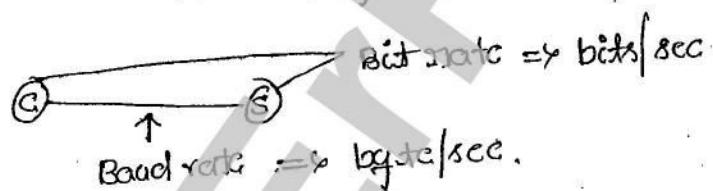
$$\Rightarrow 1 \text{ Gbps}$$

② signal

Manchester encoded signal

③ Addressing system

48-bit physical address.



~~A~~ \Rightarrow Baud = 1 x bit

~~AAA~~ Baud = 4 x bit

~~AB~~ Baud = 2 x bit

~~A~~ = $\frac{1}{2}$ bit

Ethernet:

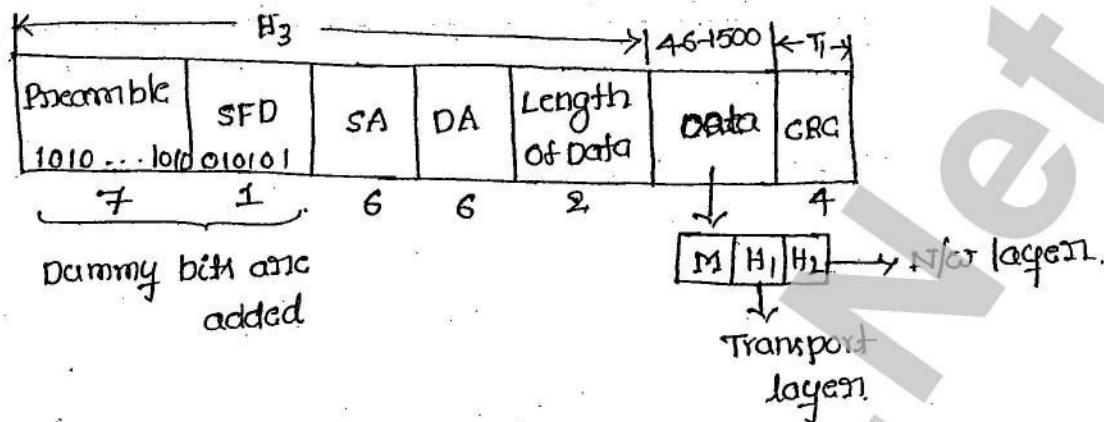
For a 10mbps ethernet

Baud rate = 20 megabaud.

For a 100 mbps ethernet

Baud rate = 200 megabaud.

Frame format of 802.3:



Preamble:

- * It contains continuously '1's & '0's from seven bits till 76.
- * It is used for synchronization purpose.

SFD (Start of frame Delimiter)

- * It signals actual start of the frame.
- * Dummy bits are represented by preamble 111010111 \oplus 1010101010

Source & Destination Address:

- * They are 48 bit physical addresses representing source & destination.
- * Maximum size of data = 46 bytes, so that we make out 76 byte frame.
- * Maximum size of data = 1500 bytes \rightarrow To avoid monopolization
change given to other channels also.

Min	Max
46	1500
72	1526 \rightarrow frame
64	1518 \rightarrow frame from source address \Rightarrow 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

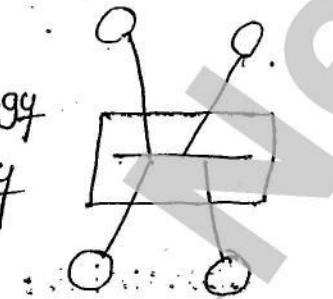
~~CRC:~~

- * it is added only at the tail to identify bit errors
- * To avoid more no. of transmissions we use CRC at tail end.

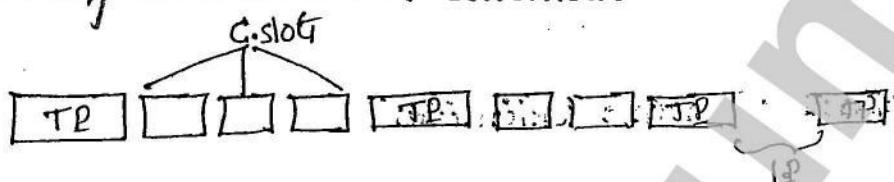
Implementation :

Physical Addressing - Star topology

Logical Addressing - Bus topology



Efficiency calculation of Ethernet:



T.P = Transmission period

C.P = Collision period

I.P = Idle period

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

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

Let $N \rightarrow$ Total no. of systems in network.

$P_s \rightarrow$ Probability of a station to transfer data pkt

$1-P_s \rightarrow$ Probability of a station not to transfer data pkt

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

- * $\frac{N-1}{(1-P_s)} \Rightarrow$ Probability for the remaining ($N-1$) stations not to transfer data packets.

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

$N P_S (1 - P_S)^{N-1} = A$ / \Rightarrow it is the probability of success
for any arbitrary station among 'N' stations

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

$$\text{If } N \rightarrow \infty \Rightarrow A = \frac{1}{e}$$

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

Contention period (C.P):

= No. of contention slots * slot duration

$$C.P = e * \Sigma \text{prop.delay}$$

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

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

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

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

$$\uparrow \eta = \frac{1}{1 + \frac{2dbe}{Lv}}$$

* if load increases,
efficiency decreases

* if pkt size increases,
then efficiency also
increases

$$\eta = \frac{T.P.}{T.P. + C.P.} = \frac{t_{trans}}{t_{trans} + 2t_{prop} * e}$$

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

$$= \frac{1}{1 + 2 \cdot \frac{d}{v}} = \frac{1}{1 + \frac{2d}{Lv}}$$

$$\begin{aligned}
 2. \quad \eta &= \frac{T \cdot P}{T \cdot R + C \cdot R + t_{prop}} \\
 &= \frac{T_{trans}}{t_{trans} + 2 \cdot t_{prop} \cdot c + t_{prop}} \\
 &= \frac{1}{1 + 2 \cdot \frac{t_{prop} \cdot c}{t_{trans}} + \frac{t_{prop}}{t_{trans}}} \\
 &= \frac{1}{1 + 2ae + a} \\
 \boxed{\eta} &= \frac{1}{1 + 6.44a}
 \end{aligned}$$

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

Advantages of Ethernet:

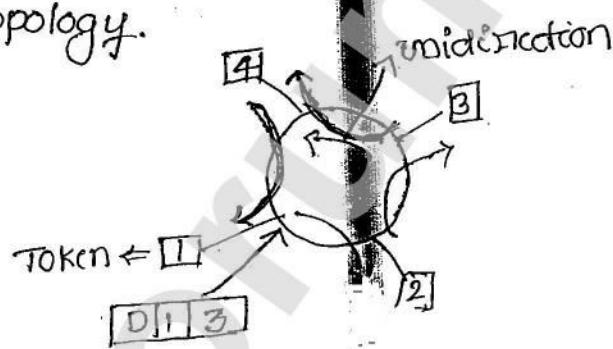
- * cost of ethernet is less.
- * ethernet cables are robust to noise
- * simple operation

DisAdv:

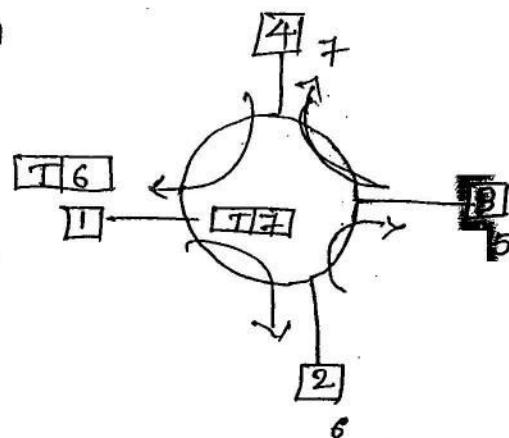
- * Ethernet offers non-deterministic service. Therefore, it is not suitable for real time applications.
eg: CNC machine.
- * There are ~~are~~ no priorities in ethernet. Therefore not suitable for client server applications.
- * There is a restriction on the min size of pkt, Hence it is not suitable for interactive applications.
eg: interactive applications 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 prioritized are possible & deterministic service is possible
- * it uses token-passing system as an access control method and ring topology.



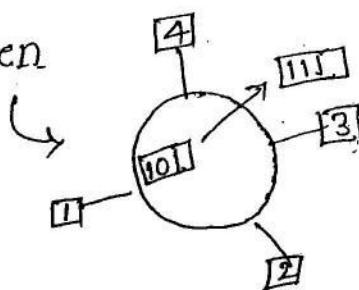
- * Token is maintained at one station only then the data is sent to the other station, where it checks for source & destination. If same then it copies only and then send the original data to others. Therefore there is no collision.
- * if any station have high priority than the token or equal then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



Problems with Token Ring:

1. A. vanished token.

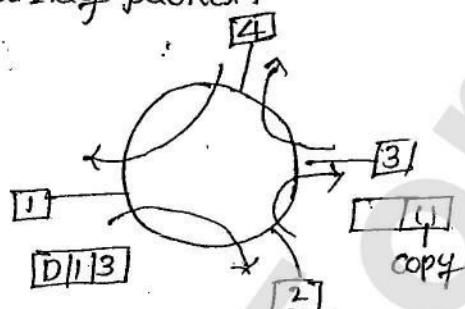
- B. corrupted token



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

- A. orphan packets

- B. stray packets



orphan pkts \Rightarrow source trash rotata upto a time

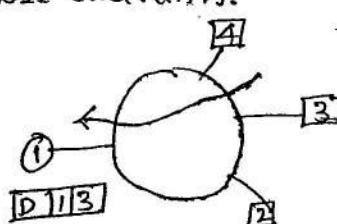
stray pkts \Rightarrow no one understands.

- C. Monopolization (Single man rule)

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

3. Destination:

- A. safe operation

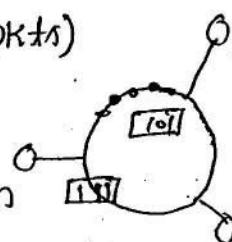


- B. Busy destination (not able to copy the frame)

- C. crash destination (Drop the pkts)

4. Ring :

* major cut in the ring, stops operation



* unhealthy token \Rightarrow no station can use the original token

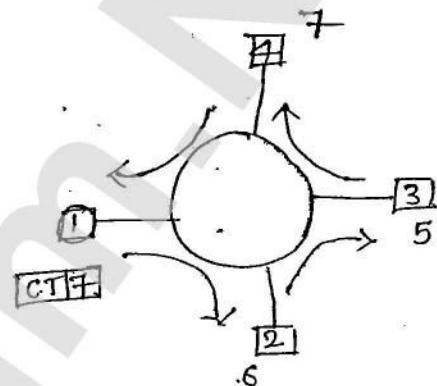
To overcome Token ring problems we have the following

1. Token Holding Time:

one station must release the token within 10 msec of time, it can transfer 20,000 pkts in 10 msec.

2.1. 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 nsec

No. of active stations * Delay at each station.

Maximum TRT = Propagation 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-bit.

2. Orphan:

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

3. Stray:

Checking the validity of PKTs while crossing the monitor station.

3. Destination:

Two fields 'A' & 'C' are attached :

$A=0$	$C=0$
$A=1$	$C=0$
$A=1$	$C=0$
$A=0$	$C=1$

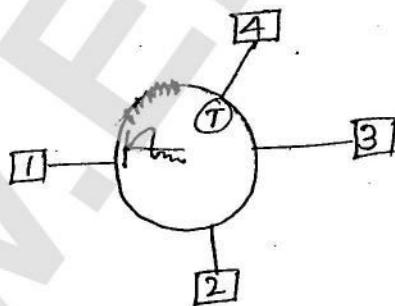
\Rightarrow Safe

\Rightarrow Destination Busy

\Rightarrow Destination not available but frame is copied & represents that other than destination station has copied the frame.

4. Ring: A special frame is introduced.

- * If continuously produce the pkt and no response, then cut it & produce a waveform at $t=0$ and if response within $t=1 \mu\text{sec}$ then it identifies as the major cut.



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

Specifications of Token Ring:

1. Data Rate

- * 4 Mbps

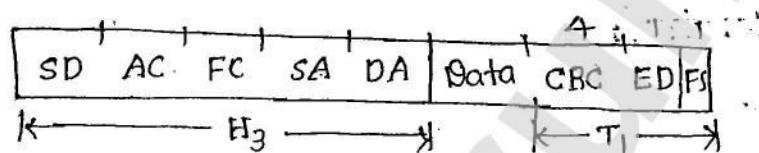
- * 16 Mbps

2. Signal: DME

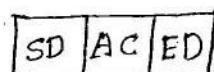
3. Addressing system: 48-bit physical Address.

Frame format:

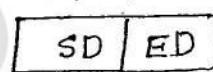
1. Dataframe



2. Token frame



3. Abort frame



Start Delimiter
End Delimiter

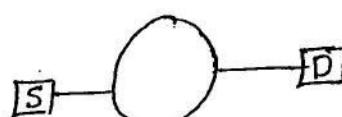
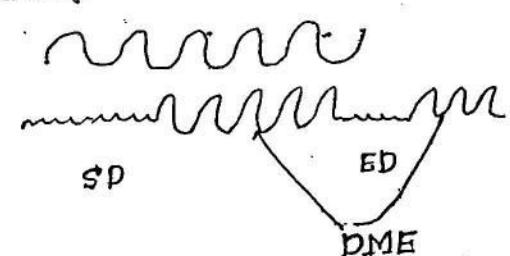
} used to indicate two extreme ends of the packets.

* They use DME signals.

SD: 10JR 10JR → other signal except DME

ED: 11JR 11JE → error bit

↓
information bit.

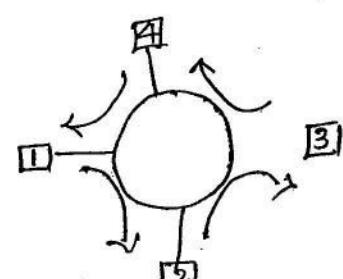


I = 0

2 = 0

3 = 0

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



if E=1 then it

simply transfer

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

M \Rightarrow Monitor bit

T=0 \Rightarrow Data

=1 \Rightarrow Token

M=0 \Rightarrow Before crossing monitor bit

=1 \Rightarrow After crossing the monitor bit.

↑

if again neglected it just eliminates it.

Frame control:

6 types of frame control

	Type of control frame
0	
1	
2	
7	

00 - Data

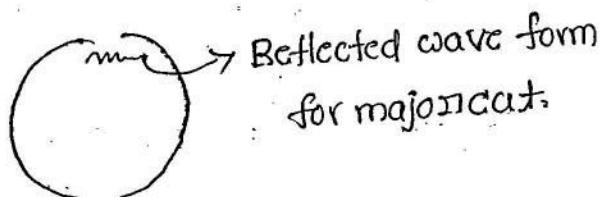
11 - Control.

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

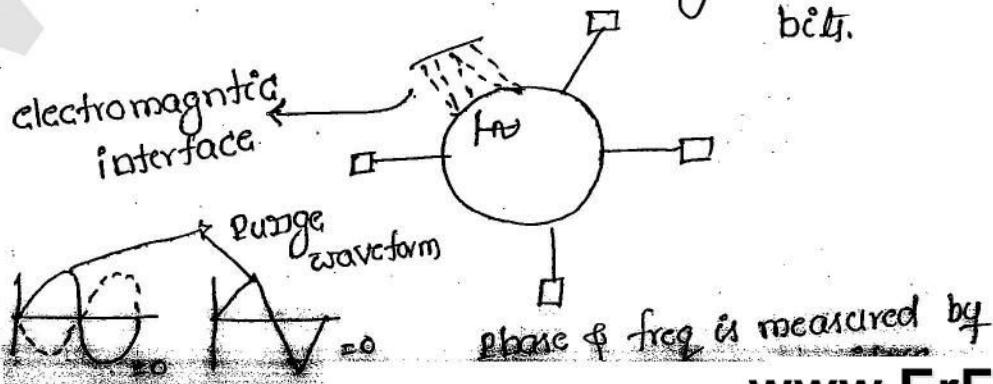
2. Active monitor presence:

it is issued by the monitor in equal intervals
to make its presence.

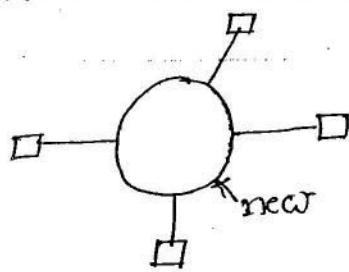
3. Becos: it is used to identify major node in the ring.



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 CBC, ED FS

↓
new channel address.

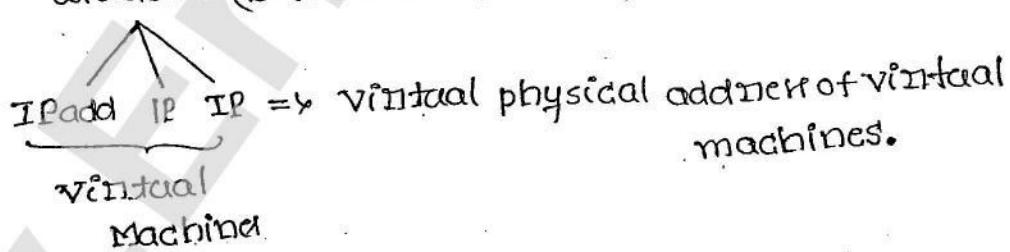
↓
it is being checked with all other channel who have this address. If any other address is given & again checked.

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

Virtualisation:

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

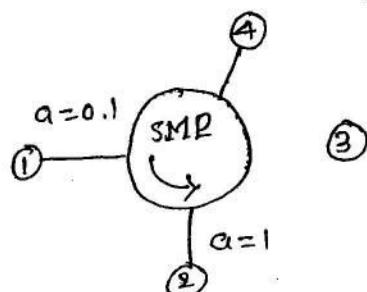
windows (Basic Machine)



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

6. SMP (standard by Monitor preserve):

It is used to carryout neighbour identification.



Upstream: From whom the channels receive the data packet.

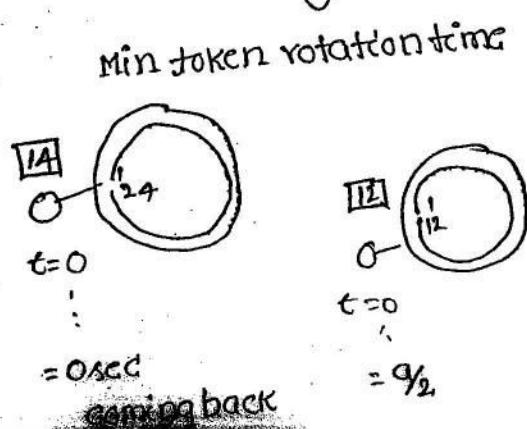
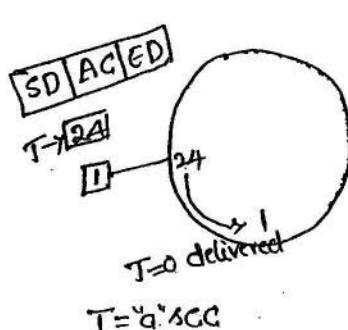
Downstream: To whom the

www.ErForum.Net

Modes of operation:

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

Calculation of minimum size of token ring:



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

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

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

$> 1 \Rightarrow \text{Max}$

$< 1 \Rightarrow \text{overlap.}$

* Token rings used for big networks.

* Token ring: propagation delay = transmission delay

$$\boxed{\frac{d}{v} = \frac{L}{B}}$$

$$\text{eg: } v = 2 \times 10^8 \text{ m/sec}$$

$$L = 240 \text{ bits}$$

$$B = 4 \text{ mbps}$$

$$d = ?$$

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

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

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

$$d = 1.25 \text{ KM}$$

Eg: if bandwidth of ring is 10 mbps, & frame size 200 bytes

velocity = $2 \times 10^8 \text{ m/sec}$ find min size token ring

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

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

$$= 4000 \text{ Km.}$$

=

Ring latency = $M \cdot n \cdot T_{RT} = \frac{d}{v} + m \cdot b + n \cdot b \cdot d$

$$\text{Propagation delay} = \frac{d}{v} + m \cdot b$$

↓ ↓
sec bits

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

d = Total length of ring

b = bit delay at each station

v = velocity propagation

B = bandwidth of ring

L = latency.

$$L = \frac{d}{v} + \frac{m \cdot b}{B} \text{ sec}$$

$$RL = \frac{d \cdot B}{v} + m \cdot b \text{ bits}$$

Various Token re-insertion strategies:

Delayed token strategies

- * Token is released after getting entire data packet.

* Efficiency is low

* Reliability is high

* it is used under load conditions.

$$\text{cycle time} = (a + b + c + d) \text{ sec}$$

where $a \rightarrow$ data transmission

$b \rightarrow$ Ring latency

$c \rightarrow$ Token Transmission time.

$d \rightarrow$ propagation delay b/w station.

early Token strategy.

- * Token is released after data is transferred.

* Efficiency is high

* Reliability is low.

* it is used under high load conditions.

$$\text{cycle time} = (a + c + d) \text{ sec}$$

Problems:

① $d = 2500 \text{ mts}$

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

$$B = 10 \text{ Mbps}$$

$$L = ?$$

$RTT = \text{Transmission delay}$

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

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

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

$$= 277 \text{ bits.}$$

②

$$B = 16 \text{ Mbps}$$

$$d = 1 \text{ Km}$$

$$v = 200,000 \text{ Km/sec}$$

$$L = ?$$

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

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

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

③

$$B = 10 \text{ Mbps}$$

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

$$\text{Bit delay} = b = \frac{1}{B} = \frac{1}{10 \times 10^6} = 0.1 \mu\text{sec}$$

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

at $t=0$ A & B started their communication.

At $t=225$ there is a collision

At $t=225$ the A & B will come to know about the collision

Assume 'A' started producing jam signal.

\therefore At $t = 273$ ($225 + 48$), A finishes producing jam signals
 \Downarrow
 Jam.

④

$$⑤ \quad B = 10 \text{ Mbps}$$

$$\text{slot time} = 51.2 \text{ uscc}$$

$$L = 512 \text{ bytes}$$

$$\text{No. of slots} = 1.716$$

$$\eta = \frac{T_o P}{T_o P + C_o P + I_o P} \quad (I_o P = 0)$$

$$\text{Transmission time} = \frac{L}{B}$$

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

$$= 40 \text{ msec}$$

$$C_o P = \text{no. of slots} * \text{slot time}$$

$$= 1.716 \times 51.2$$

$$= 87.8 \text{ uscc}$$

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

$$\textcircled{6} \quad B = 10 \text{ Mbps}$$

$$d = 2.5 \text{ Km}$$

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

$$L = 128 \text{ bytes} \Rightarrow \boxed{98+30}$$

overhead = 30 bytes

$$\eta = \frac{1}{4644\alpha} = \frac{1}{1+6.44(0.10)} \therefore \alpha \approx \frac{T_{prop}}{T_{tran}} = \frac{1.086 \times 10^{-5}}{1.024 \times 10^{-4}} = 0.10 \\ = 57\%$$

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

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

$$\textcircled{7} \quad B = 4 \text{ Mbps}$$

Token holding time = 10 msec

$$4 \text{ bytes} - 1.024 \text{ msec} = 4 \times 10^{-6} \\ ? \quad 10 \text{ msec} / 10 \text{ msec} = ?$$

$$\text{longest frame} = 4 \times 10^{-6} \times 10^{-3} \\ = 4 \text{ Rbps.}$$

$$\textcircled{8} \quad R = 4 \text{ Mbps}$$

$$m = 20$$

$$d = 20 \text{ Km}$$

$$b = 2.5 \text{ bits}$$

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

$$R = 16 \text{ Mbps}$$

$$m = 80$$

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

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

$$= 90 \text{ bytes}$$

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

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

$$= 840 \text{ bytes}$$

(10) $m = \text{station} = m$

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

$$B = 8 \text{ bits}$$

$$L = 1250 \text{ bytes}$$

$$R = 25 \text{ Mbps}$$

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

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

$$m = 300$$

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

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

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

$$18 \text{ sec} \rightarrow 25 \times 10^6$$

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

(11) $m = 32$

$$L = 1000 \text{ bit packet}$$

$$B = 10 \text{ Mbps}$$

$$\text{latency/adapter} = 2.5 \text{ bit}$$

$$d = 50 \text{ mtr}$$

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

$$\text{Data transmission} = a = \frac{L \times B}{B} = \frac{1000}{10 \times 10^6} = 10^{-4}$$

$$b = RL = \frac{d}{V} + \frac{mb}{B} \text{ sec}$$

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

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

A. Early token = $(a+c+d) \text{ sec}$

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

$$= 10 \text{ msec}$$

Token transmission = $c = \frac{LT}{B} = \frac{24}{10 \times 10^6} = 24 \times 10^{-7}$

B. Delay token = $(a+b+c+d) \text{ sec}$

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

$$= 11 \text{ msec}$$

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

$$= \frac{50}{2 \times 10^8} = 25 \times 10^{-8}$$

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

$$G.T = a + c + d \quad a = \frac{L_D}{B} = \frac{256}{10 \times 10^6} = 2.56 \text{ msec}$$

$$d = 1 \text{ km}$$

$$B = 10 \text{ Mbps}$$

$$L = 256 \text{ bytes}$$

$$\text{bit delay} = 8 \text{ bits}$$

$$c = \frac{L_T}{B} = \frac{8}{10 \times 10^6} = 0.8 \text{ msec}$$

$$d = \frac{200 \text{ m}/\text{msec}}{2 \times 10 \text{ m/sec}} = 20 \text{ msec}$$

$$\text{Propagation speed} = 200 \text{ m/sec}$$

$$G.T = 26.5 \text{ msec}$$

$$26.5 \text{ msec} \Rightarrow 224$$

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

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

$$Q) d = 200 \text{ km} \quad a = \frac{L_D}{B} = \frac{1024 \times 8}{100 \times 10^6} = 81.24 \text{ msec}$$

$$b = R_L = \frac{d}{v} + \frac{mb}{R} \text{ sec} \quad (\because \frac{mb}{R} = 0)$$

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

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

\therefore not given ignore

$$1.08 \text{ msec} = 1024 \times 8 \text{ bytes}$$

$$G.T = a + b + c$$

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

$$= 1.08 \text{ msec}$$

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

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

(14). Propagation speed = 200 m/msec

$$B = 1 \text{ Mbps}$$

$$\text{bit delay} = \frac{1}{B} = \frac{1}{10 \times 10^6} = 1 \text{ msec}$$

$$1 \text{ msec} \Rightarrow 200 \text{ mts}$$

$$B = 40 \text{ Mbps}$$

$$\text{Bit delay} = \frac{1}{B} = \frac{1}{40 \times 10^6} = 0.025 \text{ msec}$$

$$1 \text{ msec} = 200 \text{ mts}$$

$$0.025 \text{ msec} = ?$$

$$\Rightarrow 200 \times 0.025$$

$$= 5 \text{ mts.}$$

(15) $B = 5 \text{ Mbps}$

Propagation speed = 200 m/msec

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

$$1 \text{ msec} = 200 \text{ mts}$$

$$0.2 \text{ msec} = ?$$

$$\Rightarrow 200 \times 0.2$$

$$\Rightarrow 40 \text{ mts.}$$

=

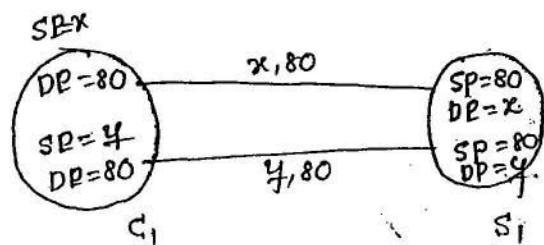
www.ErForum.Net

Transmission Control Protocol.

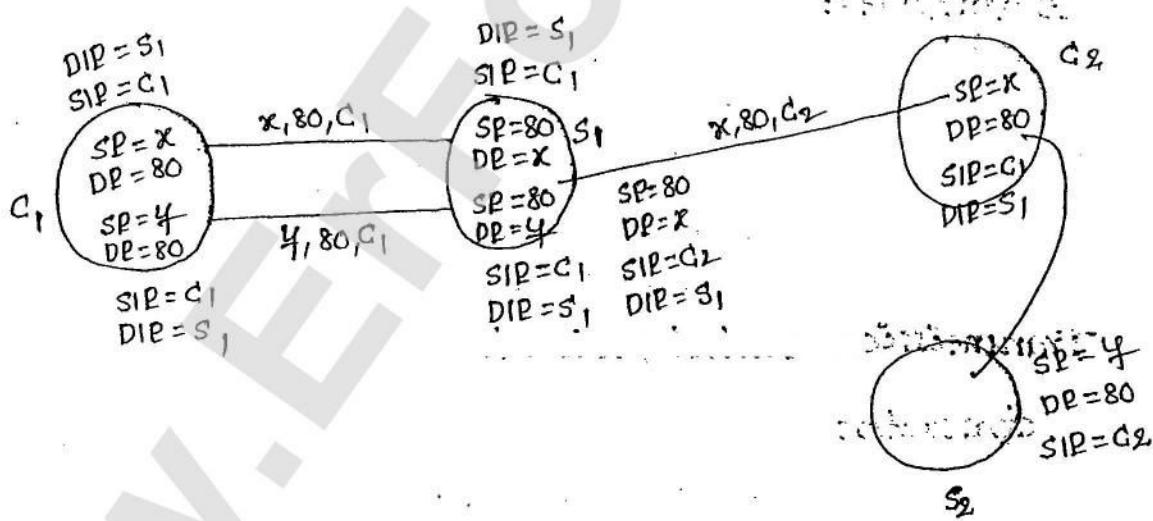
why we call network as TCP/IP networks

(on)

Relationship between TCP & IP.



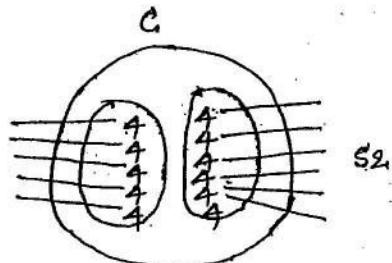
- * ctrl+N \Rightarrow another connection.
- * while establishing a new connection source point & destination port is addressed.
- * servers can handle more no. of clients, so introducing a new client involves both source port and destination port.



- * 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 \Rightarrow 2 ports parameters.
- * The source IP & Destination IP are handled by IP protocol in the ~~Transport layer~~ \Rightarrow 2 IP parameters.

4 parameters } source point
 Destination port
 source IP
 Destination IP.

socket:



- * socket is a logical component which groups a set of parameters for communication.

$$5 \times 4 = 20$$

$$6 \times 4 = 24$$

$$5 \times 2 = 10 + 2 = 12$$

$$6 \times 2 = 12 + 2 = 14$$

Advantages:

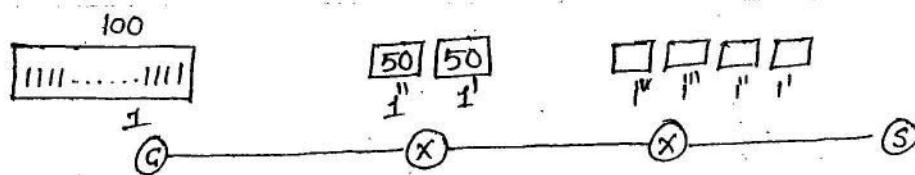
- * Resource utilization
- * Maintenance & Administration
 - Allows certain num-of connections for socket.

Transmission control protocol:

characteristics:

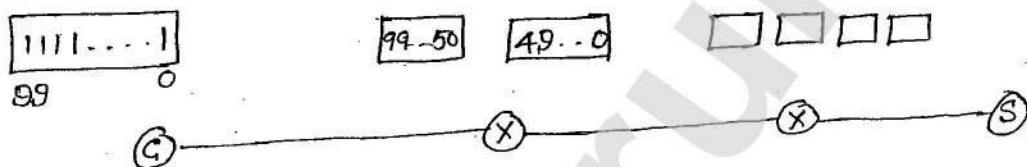
- * it is reliable, byte oriented, point-to-point, transport layer protocol.
 connection-oriented.
- * Message Oriented (UDP)
- * Packet oriented (SIP)
- * Byte oriented (TCP)
- * Bit-oriented (HDLC).

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 pkts 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.

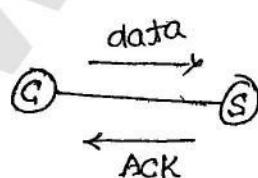


fig: full duplex

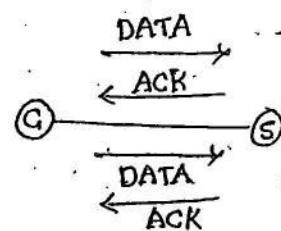


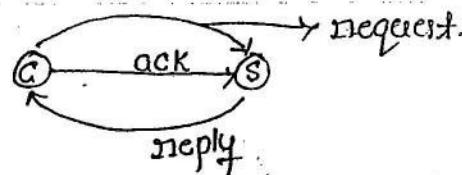
fig: Half duplex.

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



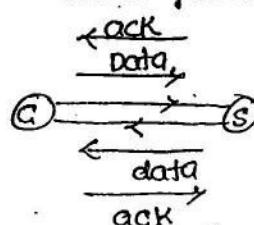
* TCP connections are having 3 phases.

1. connection establishment phase.: (negotiation phase)

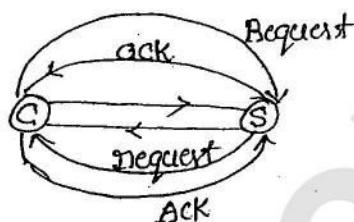


* it is a single step process.

2. Data transmission phase



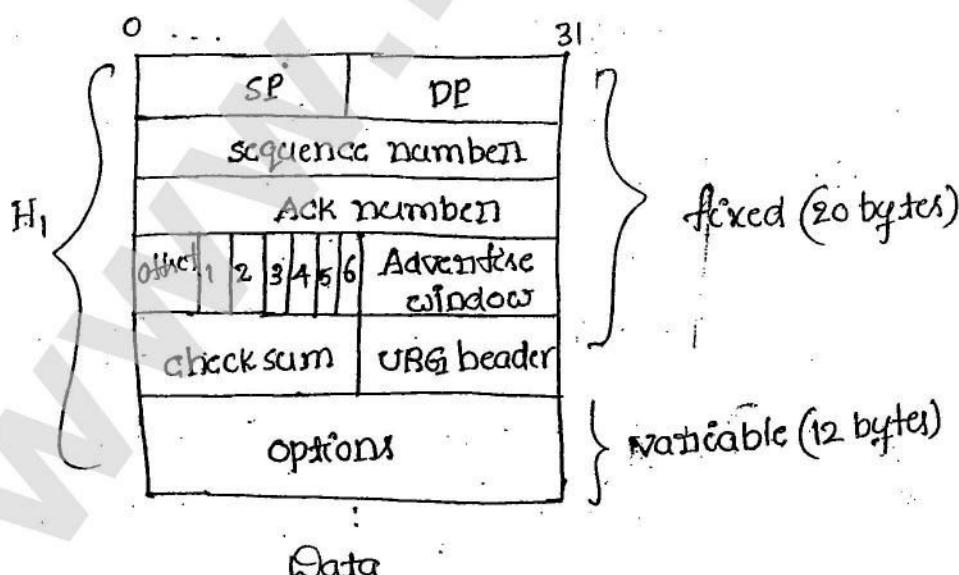
3. connection termination phase.



* it is not single step process even though it required for connection termination. The termination must done in both the system (not only one)

TCP operations:

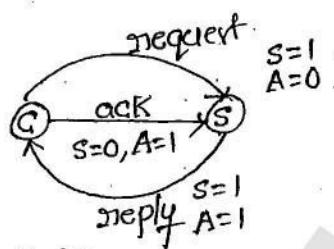
TCP header:



Flags:

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

1. SYN & ACK: SYN & ACK flags are used in connection establishment phase of different request and reply packets.



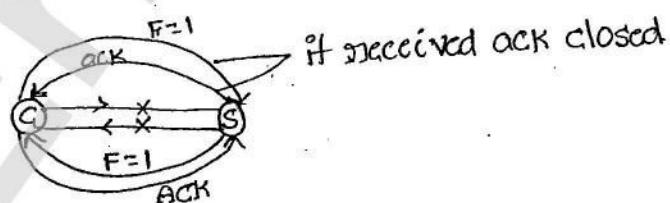
$S=1 \ A=0 \Rightarrow$ Request

$S=1 \ A=1 \Rightarrow$ Reply

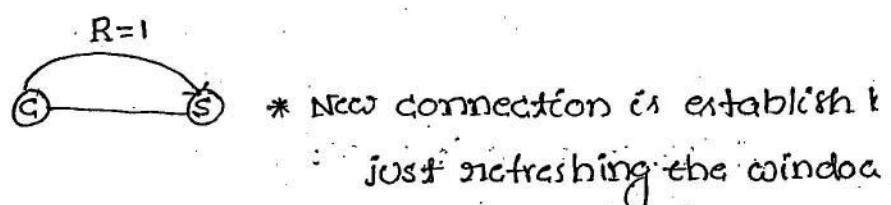
$S=0 \ A=1 \Rightarrow$ ACK

$S=0 \ A=0 \Rightarrow$ Data

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



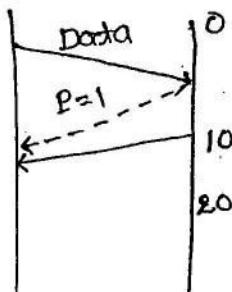
3. RST Flag: it is used to reset the connections.



* while transferring 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.

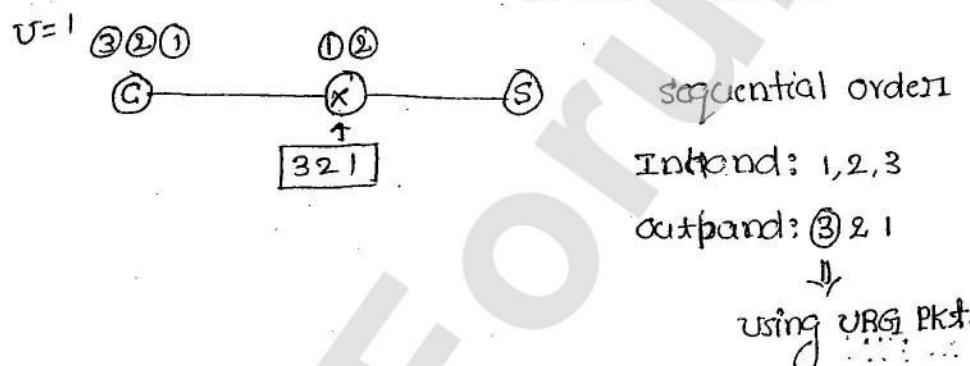
4. PSH flag:

- * 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 reaches without waiting for the time interval it have.

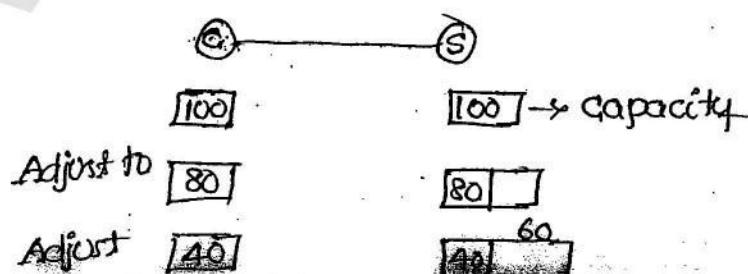
5. URG: it is used take care of "out of band rate"



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

Advertise window:

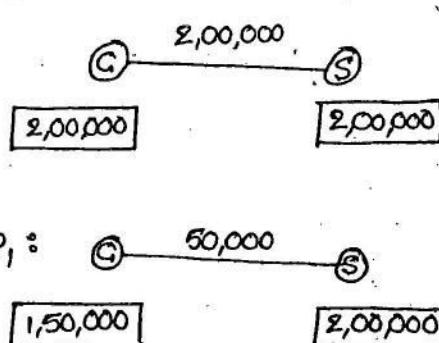
- * it is used to implement flow control



- * 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 in order to reduce viruses.
- * Always server needs to consume only one byte transfer. Possible to reduce the SWS value, so that efficiency increases.



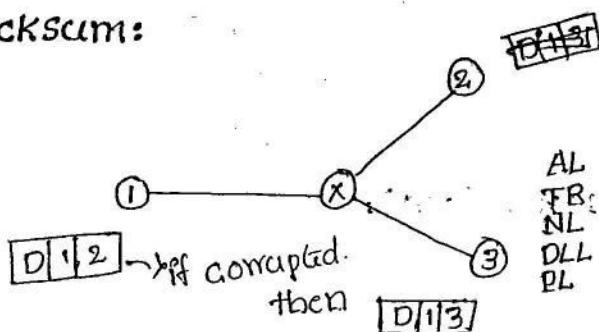
- * There is a chance of sending all the 1,50,000 bits, at both the sides but we cannot transfer them because only $1 \rightarrow 2$ bits

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

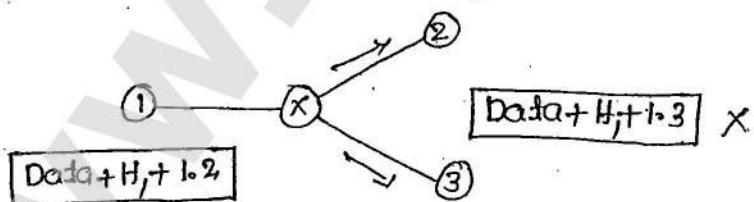
eg: if empty space is 1,50,000 advertise window = 50,000
if scale factor = 3.

eg: if empty space = 1,00,000 & advertise window = 50,000
then scale factor = 2.

checksum:

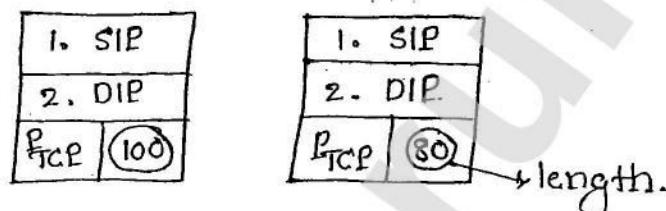


- * The transport layer transfers the corrupted data to the application layer. Then application layer recognizes as a corrupted bit.
- * so in order not to have burden on application layer, before a packet reaches application layer, it gets corrected at the Transport layer by including the concept of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



- * calculate the checksum of $(Data + H, + 1.2)$ at the sender side and send the checksum. at the receiver the check sum is again calculated. $[Data + H, + 1.3]$ → corrupted, so discard it by transport layer.

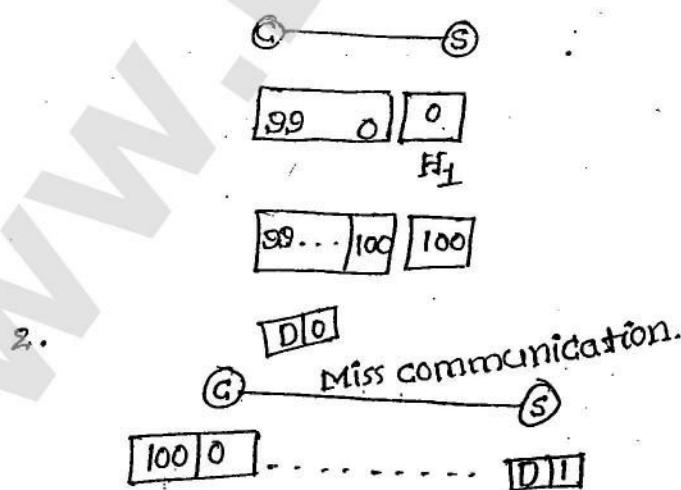
- * Pseudo-header is used to check whether data packet has been received by the correct destination or not.
- * it is prepared at the source and included in checksum calculations.
- * once packet is received by the destination again it is prepared by the destination with destination values.
- * if incoming checksum is similar to calculated checksum, then packet is consumed, else it is discarded.



- * Sequence no. for the packet is first data byte sequence num. in the packet.

characteristic for Sequence num of Ack:

1. sequence no. for the packet is first data byte sequence num. in the packet.



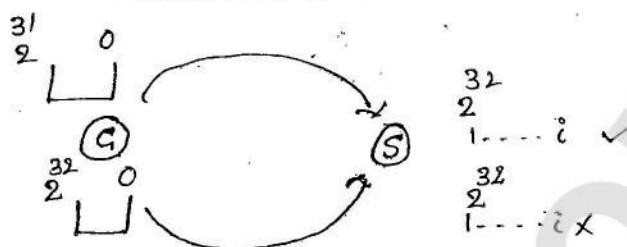
TCP uses random initial sequence numbers.

D 100 → discarded.

* The sequence numbers always not start with '0' if 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.

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: $0 \xrightarrow{1.536 \text{ Mbps}} 0$

$$1 \text{ sec} = 1.536 \times 10^6 \text{ bits} \Rightarrow 1^{\text{st}} \text{ pkt}$$

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

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

$$1.536 \text{ Mbps} - 64 \text{ bits}$$

$$10 \text{ Mbps} - 57 \text{ min}$$

$$100 \text{ Mbps} - 6 \text{ min}$$

$$1.2 \text{ Gbps} - 28 \text{ sec.}$$

Eg: consider bandwidth of link = 100mbps
sequence no. field = 24 bits

Find the "wrap around" of sequence numbers

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

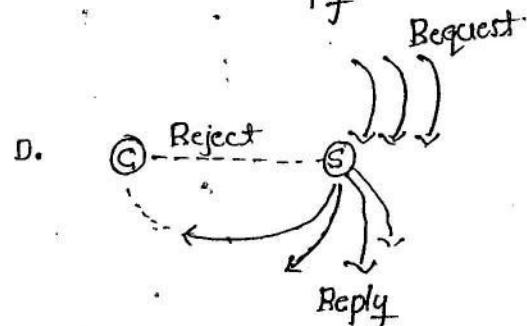
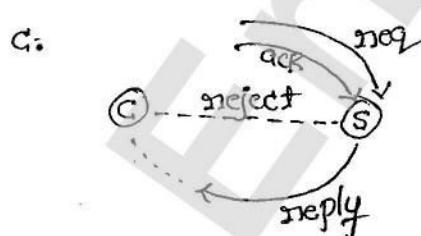
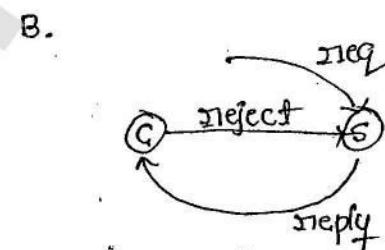
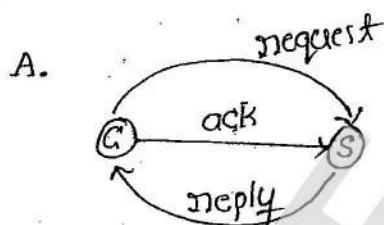
$$= \frac{100 \times 10^6}{8} \text{ bytes}$$

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

$$? \quad 2^{24}$$

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

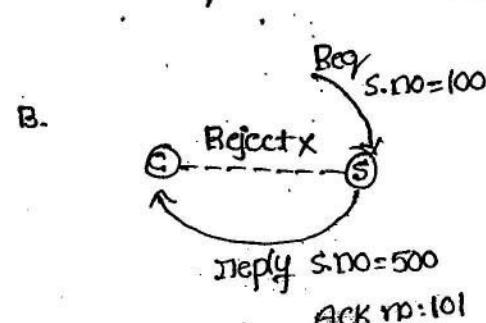
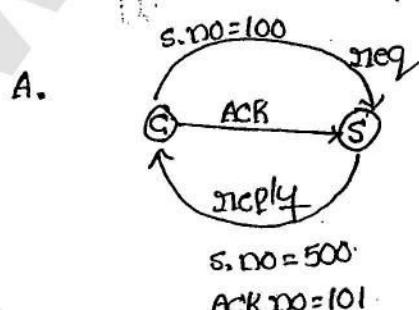
Applications:



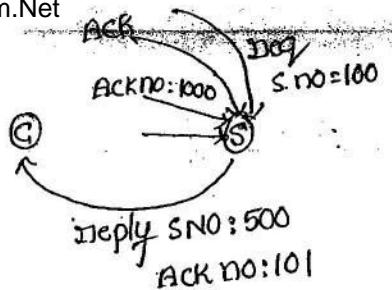
Denial of service attack:

* Server denies the client to server for a certain time interval

To overcome above problem use "sequence number".



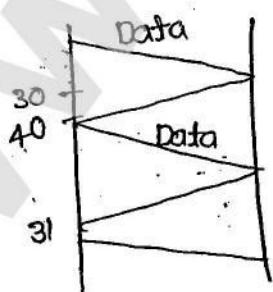
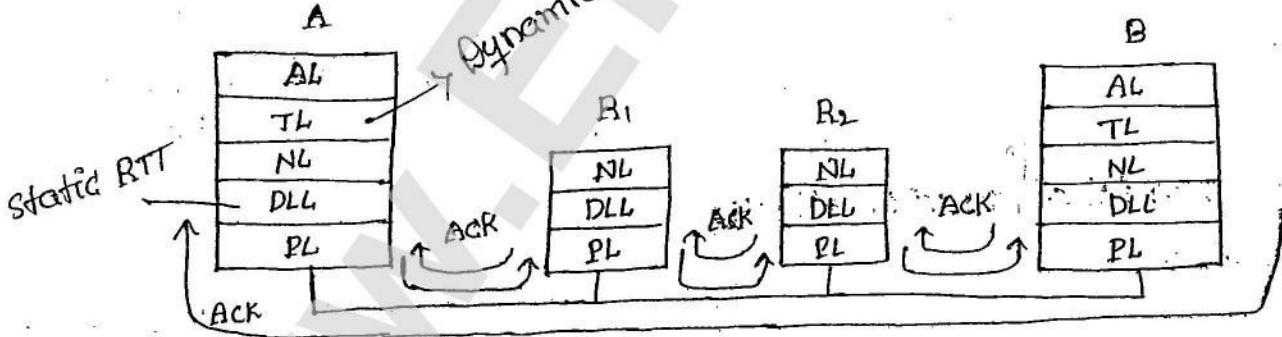
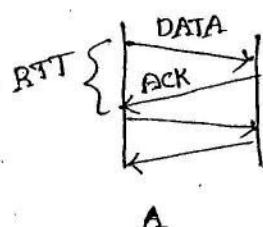
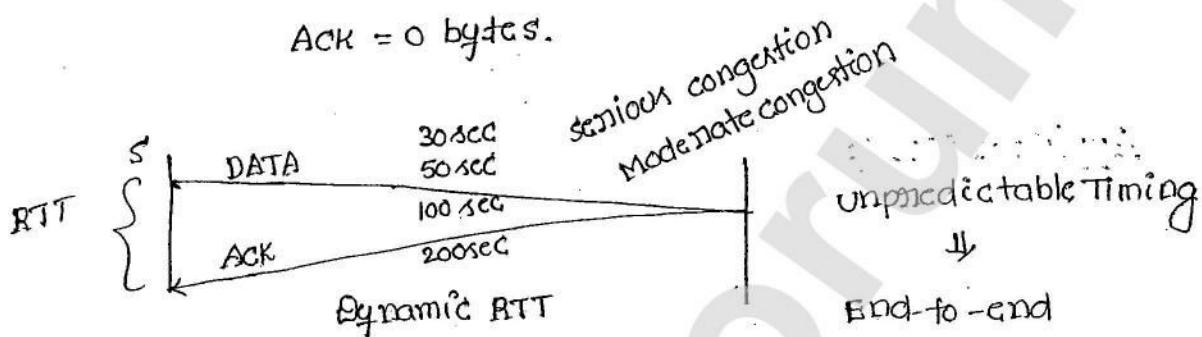
C.



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

$\begin{matrix} \text{syn} \\ \text{FIN} \end{matrix}$ } 1 byte

ACK = 0 bytes.



For the calculation of RTT we have certain Algorithms.

1. Basic Algorithm:

$$(IRTT) \text{ initial RoundTrip Time} = 30 \text{ sec}$$

$$(NRTT) \text{ New RoundTrip Time} = 40 \text{ sec}$$

$$\alpha = 0.9$$

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

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

$$= 31 \text{ sec}$$

$$\text{Time out (TO)} = 2 \times ERTT$$

$$= 2 \times 31$$

$$= 62 \text{ sec}$$

$$③ \quad IRTT = 31 \text{ sec}$$

$$NRTT = 50 \text{ sec}$$

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

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

$$= 32.9 \text{ sec}$$

$$\text{Time out} = 2 \times ERTT$$

$$= 2 \times 32.9$$

$$= 65.8 \text{ sec}$$

$$④ \quad IRTT = 32.9 \text{ sec}$$

$$NRTT = 45 \text{ sec}$$

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

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

$$= 34.11$$

$$\text{Time out} = 2 \times ERTT$$

$$= 2 \times 34.11$$

$$= 68.22 \text{ sec.}$$

2. Jacobson's Algorithm:

$$IRTT = 30 \text{ sec}$$

$$NRTT = 40 \text{ sec}$$

$$\alpha = 0.9$$

$$\text{initial Deviation } (\delta_0) = 5$$

$$\textcircled{2} \quad \text{New Deviation } (D_N) = |IRTT - NRTT| \\ = |30 - 40| \\ = 10$$

$$\text{Estimate deviation } (D_E) = \alpha D_i + (1-\alpha) D_N \\ = 0.9 \times 5 + (1-0.9) \times 10 \\ = 5.5.$$

$$ERTT = \alpha IRTT + (1-\alpha) NRTT \\ = 0.9 \times 30 + (1-0.9) \times 40 \\ = 31$$

$$\text{Time out} = 4 * D_E + ERTT \\ = 4 \times 5.5 + 31 \\ = 53.$$

$$\textcircled{3} \quad IRTT = 31 \\ NRTT = 50 \\ \alpha = 0.9 \\ D_i = 5.5$$

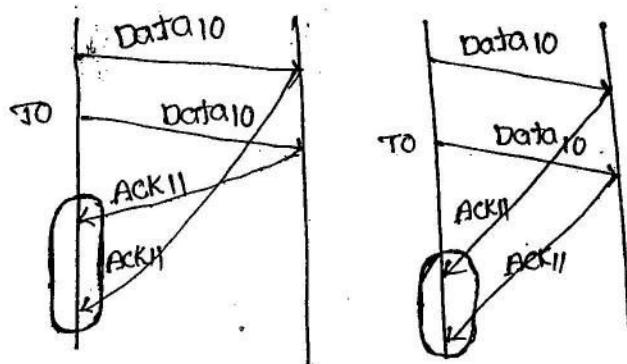
$$D_{NEW} = |31 - 50| \\ = 19 \\ D_E = 0.9 \times 5.5 + (1-0.9) \times 19 \\ = 6.2$$

$$ERTT = 0.9 \times 31 + 0.1 \times 50 \\ = 32.9$$

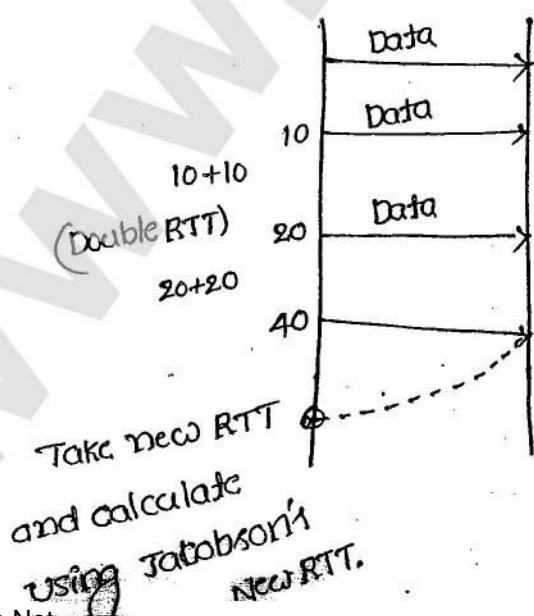
$$TO = 4 \times D_E + ERTT \\ = 4 \times 6.2 + 32.9 \\ = 57.$$

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

Korn's Algorithm:



- * if there is a time out, there is a possibility to reduce 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, Korn's has resolved this ambiguity by proposing the follows.
- ⇒ For every timeout double the timeout for the next transmission and continue this till to get a proper ACK.
- ⇒ Then we will go back to the Jacobson's algorithm.



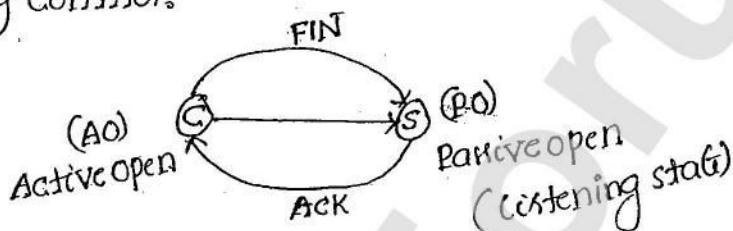
State Transition Diagram:

Need for state Transition diag:

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

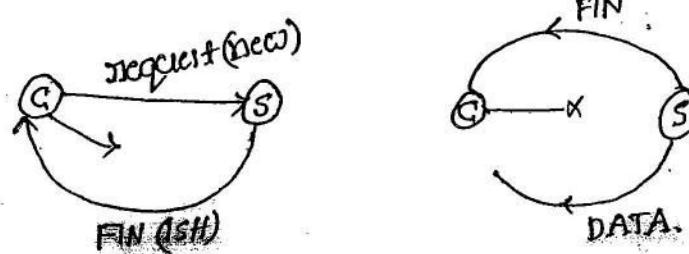
1. Get the specification of the protocol develop a software for it, integrate with network operating system and evaluate its features. It is a time consuming process and costly.
2. Get the specification of protocol develop state transition diag for it and then evaluate its features.
It is a shortcut 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 acknowledgement. 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 FIN. 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 dramatically, for checking 100 characters, one at a time for which RTT is more for character typing.
- * At such conditions, add the header for all the bits & send it which improves performance.
- * But it is not applicable in LAN technologies, but supports 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

$= 68,535 \Rightarrow$

65515	20
↓	↓
Data	headers.

② RTT = 30 msec

$$\alpha = 0.9$$

$$NRTT = 26$$

$$\text{Basic algorithm} = \alpha (RTT) + (1-\alpha)(NRTT)$$

$$= 0.9 \times 30 + (1-0.9) (26)$$

$$= 29.6 \text{ msec}$$

$$T.O = 2 * 29.6 = 59.2 \text{ msec}$$

$$D_{new} = |30 - 26| = 4$$

$$DE = 0.9 * 4 + (0.1) * 4$$

$$= 4$$

$$T.O = 4 * D.E + ERTT$$

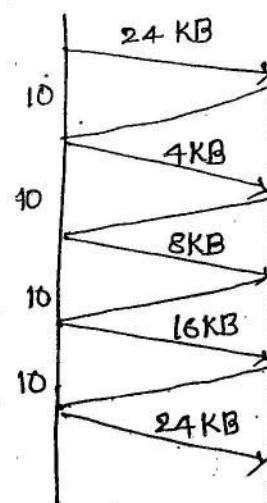
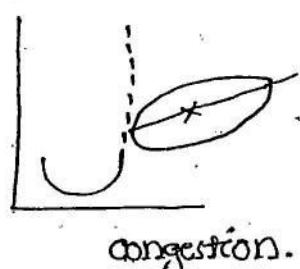
$$= 4 * 4 + 29.6$$

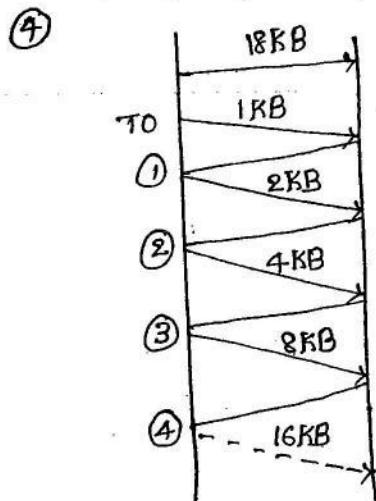
$$= 45.6 \text{ msec.}$$

③



After 40 ms a full window is transmitted





After time out occurs go back to

window size = 1

Ans: 16KB.

⑤. TCP USES SWP

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

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

$$= 26.5 \text{ mbps}$$

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

$$= 2.6\%$$

⑥. Transport data unit

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

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

⑨ Probability of sequence of 1 random number falls in 10⁶

$$\text{total no} = 2^{32}$$

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

- ⑩ 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. thus algorithm cannot be implemented.

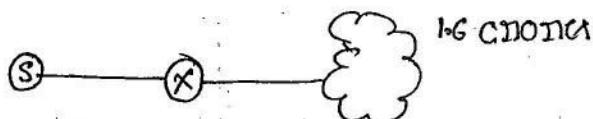
case:2: Since RTT is exactly equivalent to typing speed. thus algorithm cannot be implemented.

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

User Datagram Protocol [UDP]

Need for UDP:

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



Since server communicates to 16 clients in TCP, we require 16 connections which cannot support a huge connection.

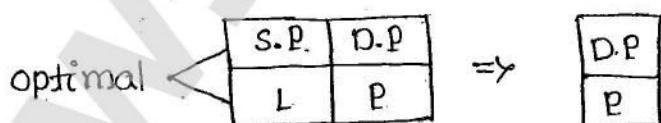
- * Applications that requires constant data flow, cannot use TCP. Hence UDP is being used

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.



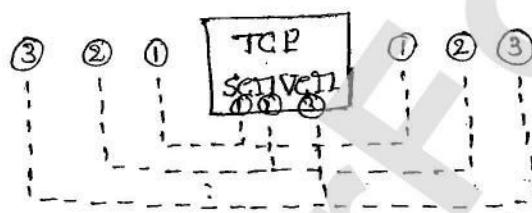
TCP

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

Applications

- * web applications
- * Mail, RSA applications

concurrent process:

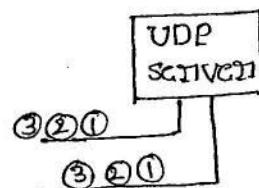
**UDP**

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

Applications.

- * Name transfer Application
- * Network management applications
- * Multimedia & Real time appl's

iterative process:



- * TCP and UDP Port numbers are different.

Domain Name System (DNS):

- * it is using UDP, its purpose is to keep track computer and services in a network environment.

it has four applications

- Name Translation
- Host Aliasing
- Mail Aliasing
- Load balancing.

If it is Using 4 types of SERVICES

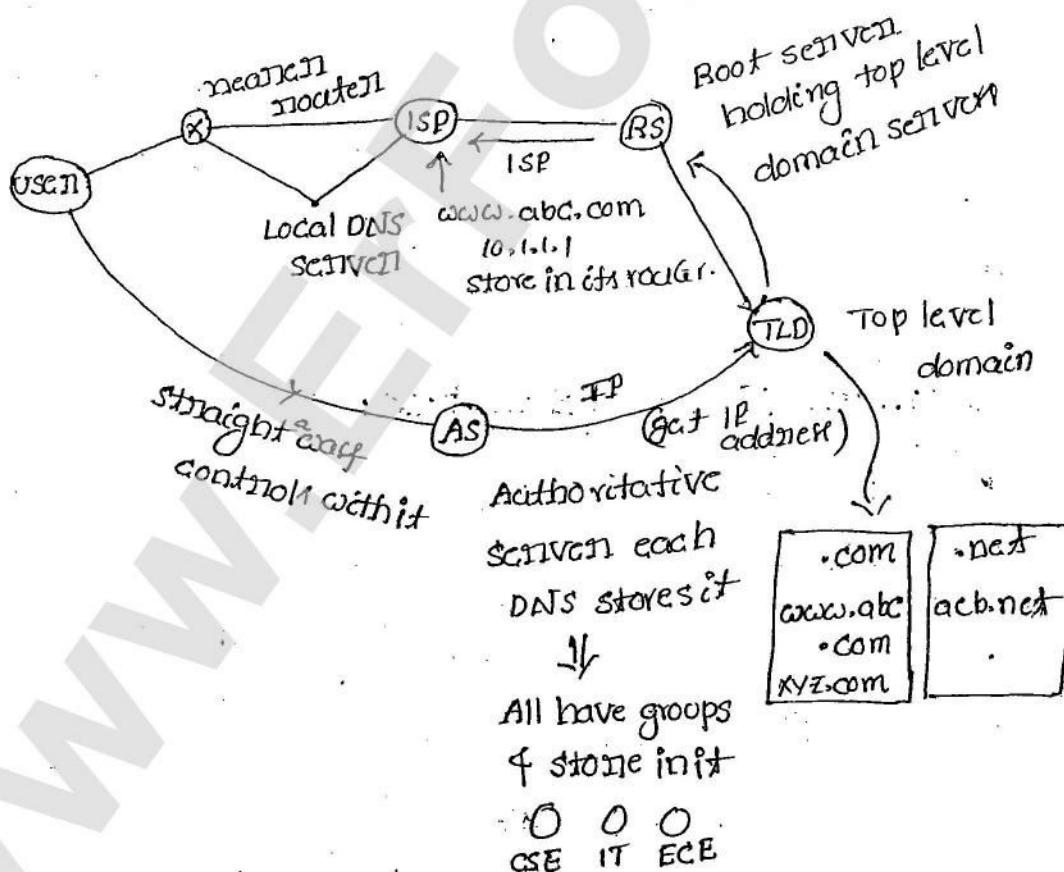
- Root name server
- Top-level domain server
- Authoritative server
- Local DNS server.

* It uses distributed database to perform its applications.

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

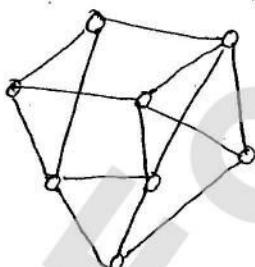
* Each resource records consists of 5 attributes.

- Name
- TTL
- class
- type
- value.



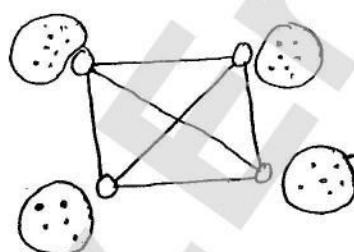
Fault gateway: IP routers specifies the default address, suggesting address that it can't know particular address.

- * once a request for a website is sent, it gets stored in ISP and the local router, whenever again a request of same website is sent then there is no need to visit all the servers, and there is only subsequent request simply it shows the 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.



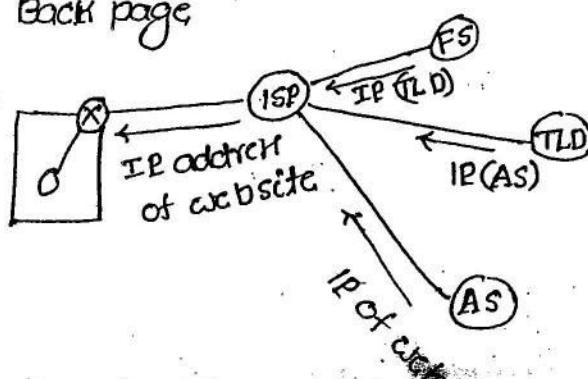
TLD server in the form of clusters and distributed database.

- * it will help for fast searching (effective usage).

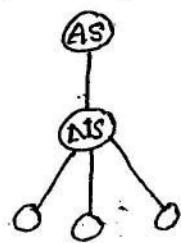
⇒ Getting IP address can be done in two ways.

1. Back page

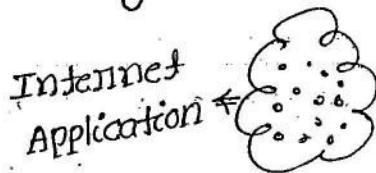
2.



NS: Name Server



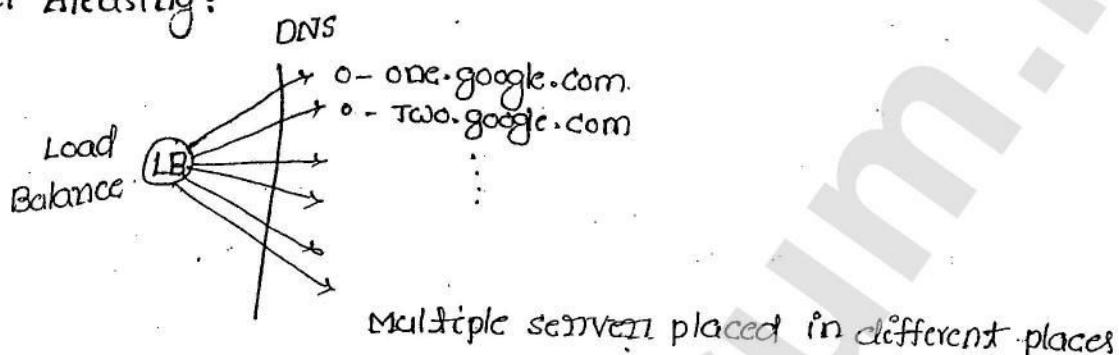
⇒ Giving names to systems in a network (Host Alcasing):



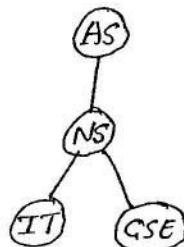
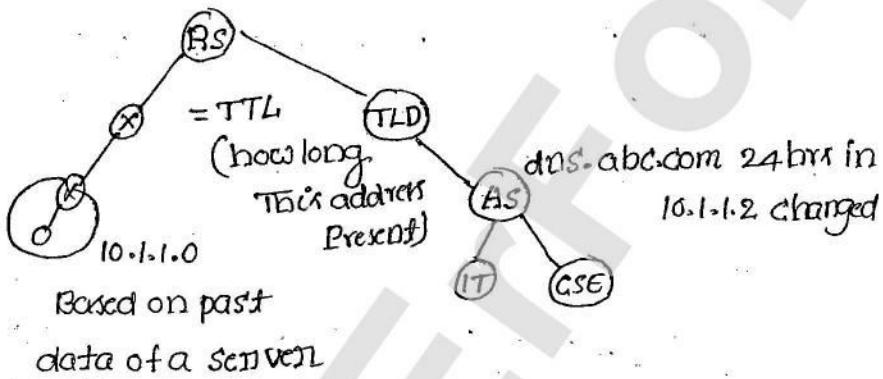
Ex. one.abc.com. → by seeing name, one can understand position of the system.

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

Mac Alcasing:



Distributive Database:



IT.abc.com. 24 hrs in
10.1.1.3, www.abc.com 24 hrs
NS, dns.abc.com.
www.abc.com 2 hrs change
backup.abc.com.

canonical name



Alternative name
for websites.

Circular dependency ⇒ glid. record.

Replication ⇒ sharing data.

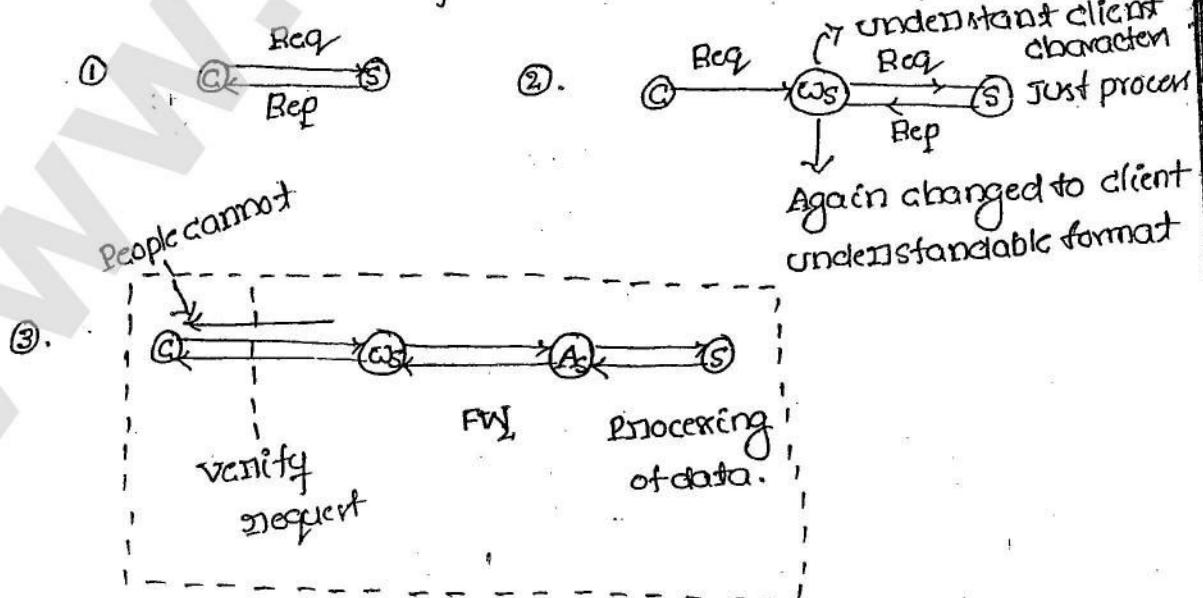
More replication ⇒ use TCP

Translation ⇒ use UDP

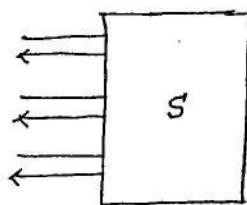
HTTP:

- * 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 has 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.
 - ⇒ Post ⇒ creation (create an object in server)
 - ⇒ Post ⇒ changing (modification)
 - ⇒ delete ⇒ delete
 - ⇒ Trace ⇒ debugging
 - ⇒ options ⇒ optimization.
 - ⇒ connect ⇒ Through the channel and uses its security to perform transactions.

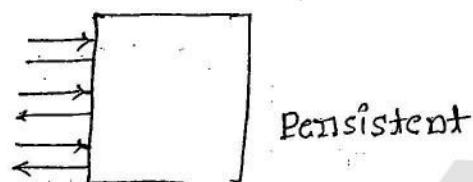
HTTP uses 3 different types of status for its operations:



* Non-persistent connection in 1.0 (in 2.0 it is changed to persistent)



Every time new connection
is established



using some time limit,
connection is placed.

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

- * Each & every request expnss 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

FTPS => 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.

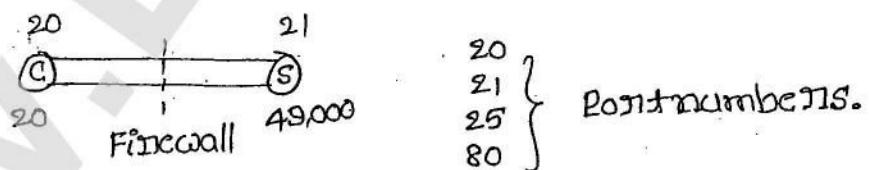


fig: Extended passive mode.

* 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 these time, so for this we use a no. of commands.

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

HTTP + SSL \Rightarrow HTTP.

FTP + SSH \Rightarrow security.

* By using SSH \Rightarrow 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's having two components.

\rightarrow User agent

\rightarrow Mail Transfer agent.

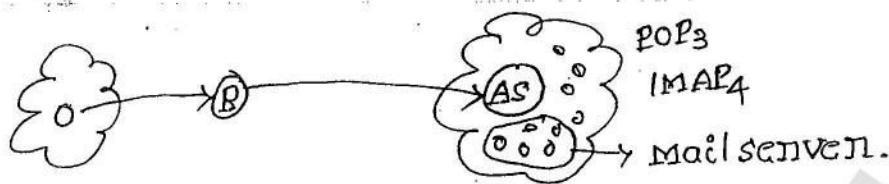
* It is a part of push-pull mechanism in the mail comm
∴ SMTP is used to push the mail.

* 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) \Rightarrow synchronous command

- * it is connected to DNS servers also.



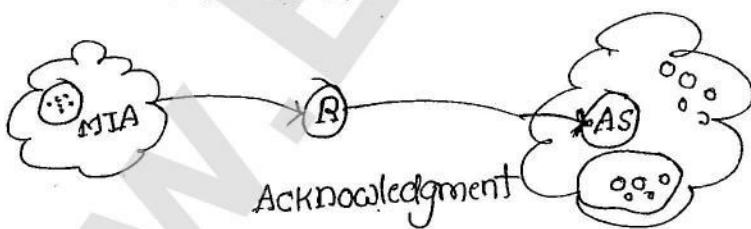
- * if a host is needed to send the data, then it gets connected to the router and then the router gets connected to the Authoritative server through SMTP protocol. The AS identifies a particular host in the mail server and "push" the data into that host. and if any other host requires the data within the network, then the data is being "pulled" by the server.
- * Hence the mechanism is being considered as the "PUSH-PULL" mechanism, for this mechanism POP₃ and IMAP₄ are used.
- * IMAP₄ is more advantageous than POP₃ for this consider an example:
 Before downloading a file, a msg is delivered to check it is SAFE (if) associated with any virus. If user is interested to continue (either it is SAFE or UNSAFE) then only it processes and if he is not interested simply "CANCEL" it => it is advantages of IMAP₄ over POP₃
- * IMAP₄ Push some of the dangerous mails to junk mails whereas POP₃ 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 negotiate with TCP for connection SMTP)
- * Forward message => attachment are available with the message
- * Reply message => all the attachments are automatically dropped.
- * Read Receipt component (if act) => Then user (who send a mail to others can able to know either the other user who received a mail) has received an read it or not.
- * while user needs the mail an acknowledgement is sent to the sending user that the recipient had read it.



- * User agent is used for handling the attachment and the detachments and mail transfer agent is an incharge to have a connection with mail 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. i.e it represents to have NID and some HID.

1. $\begin{matrix} \checkmark & X \\ NID & HID \\ X & X \end{matrix} \Rightarrow$ filled by 0's

A: 10.0.0.0

B: 150.157.0.0

C: 192.168.1.0

Name: "This network" address.

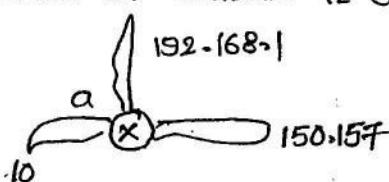
Purpose: Used by Router.

\Rightarrow Represents different network

D	10.0.0.0	150.157.0.0
---	----------	-------------

\Rightarrow not valid

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



10.0.0.0	a
150.157.0.0	b
192.168.1.0	c

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

NID HID \Rightarrow 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 1's
NID HID

255.255.255.255.

Name: Limited Broadcast address. // Delivering packets to all system in our own net'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 0's
NID HID

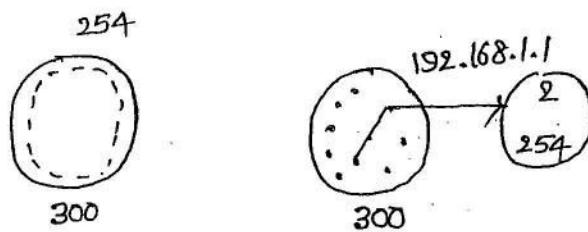
0.0.0.0

Name: Dynamic IP address.

Purpose: Dynamic Host Configuration protocol (DHCP).

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

- * 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 administrator, assigns the IP address to the system.

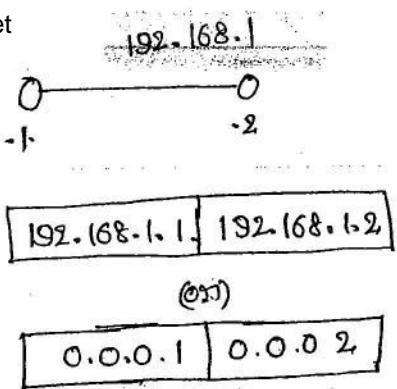
Auto: The operating system directly assigns the IP addresses to all the systems without the intervention of administrator automatically.

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



- * The communication is done among the two host systems within the same network \Rightarrow 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 as unique, and only the host ID alternates for every communication.

6. 127... Any

127.0.0.1 or 127.0.0.255

Name : Loop back address

Purpose: inter process communication

- * self checking or self connectivity with checker



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

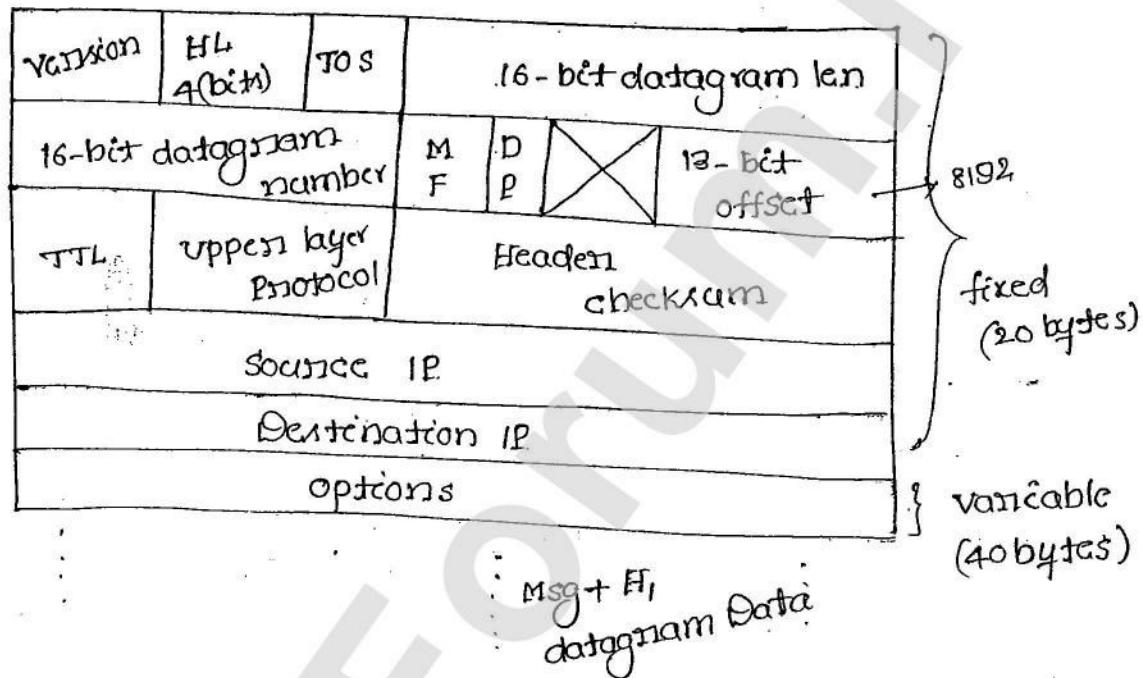
\Rightarrow which of the following IP addresses are used as only source IP addresses

- A. 10.1.1.1 B. 0.0.0.0 C. 0.0.0.1 D. 127.1.1.1

\Rightarrow which one of the following IP addresses are used as both source and destination addresses.

- A. 10.1.1.1 B. 255.255.255.255 C. 10.255.255.255 D. 0.0.0.1

IP operations:



* Version \Rightarrow to indicate either IP₄ or IP₆ packet (4-bits)
IP₆ less complicated than IP₄.

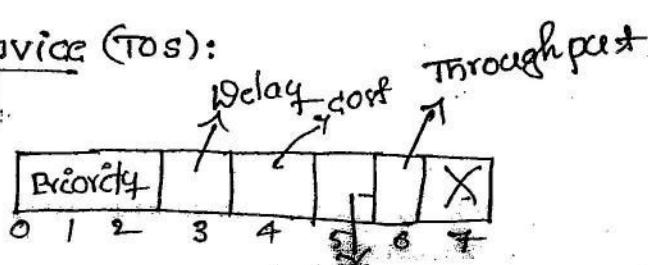
* Header Length: Maximum size \Rightarrow 60 bytes (40+20)
Minimum size \Rightarrow 20 bytes.

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

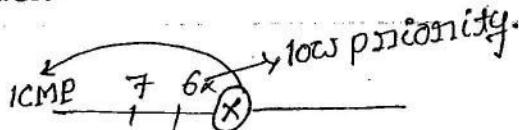
constant scale factor = 4

Actual header length = Available header length in PKT (4-bit)

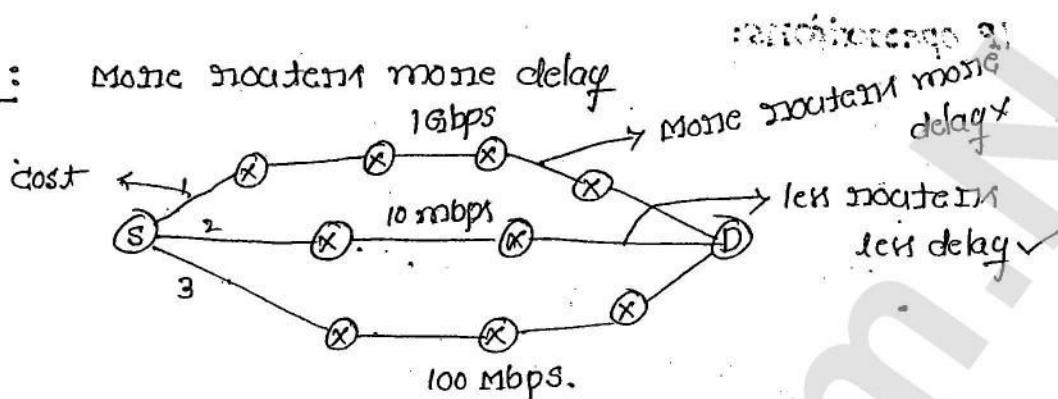
Types of service (TOS):



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



Delay: More routers more delay



path having less delay

More routers more delay

less routers less delay ✓

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

upto user to decide link \leftarrow

Delay	Cost
1	1

Reliability: It represents the "error rate".

Throughput: it depends on bandwidth, if high bandwidth for a link \Rightarrow then allows

$$2^{16} = 64 \text{ KB} \Rightarrow \& \text{c maximum size of the total packet.}$$

16-bit datagram numbers:

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

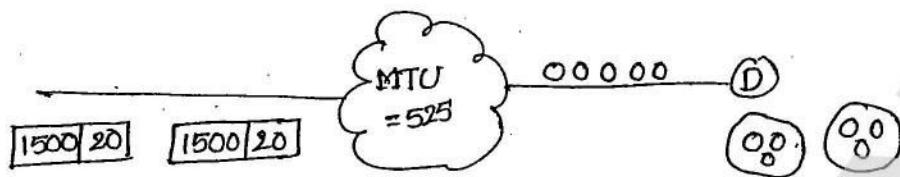
More fragments (MF).

Maximum Transfer unit (MTU):

Fragmentation is applicable to only datagram

Packet but not for header.

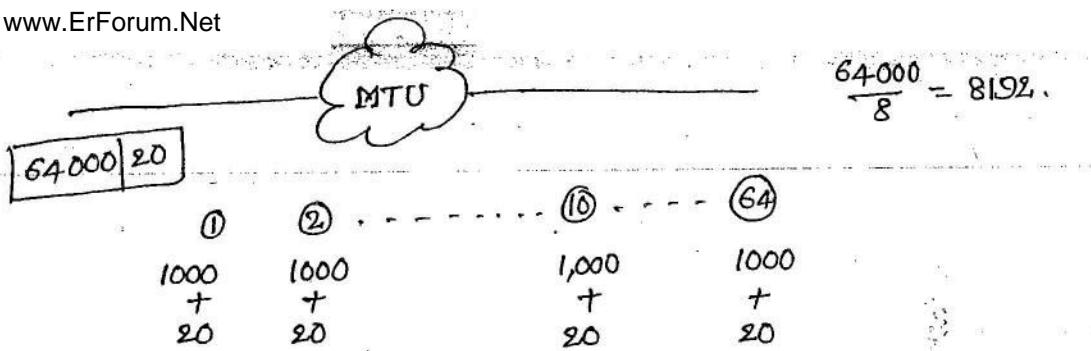
- * OFFSET indicates no.of data bytes ahead of this fragment in that particular packet.



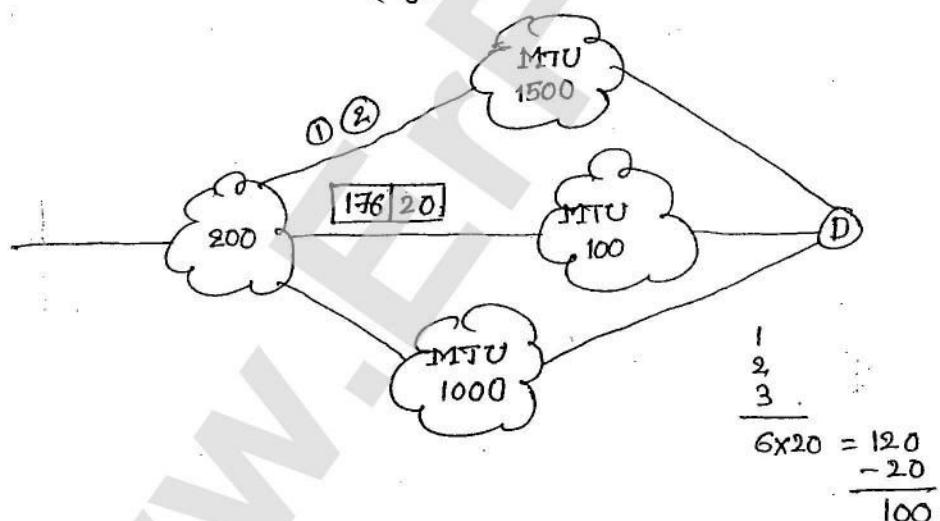
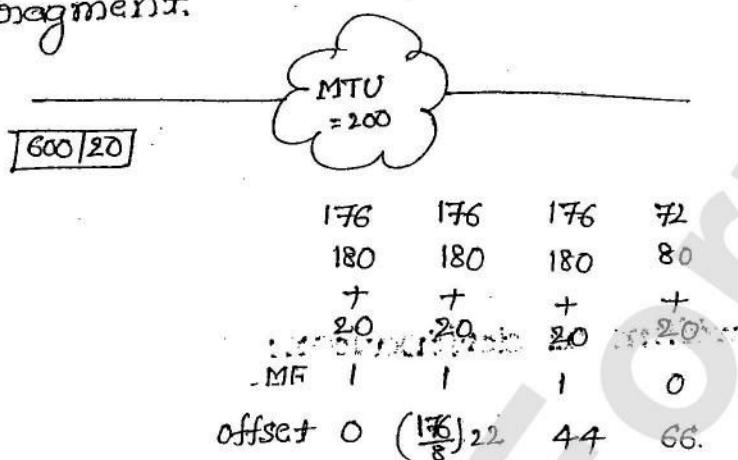
	①	②	③	④	⑤	⑥
504	504	504	492	505	505	490
	505	505	490	505	505	490
	+20	+20	+20	+20	+20	+20
	5	5	5	6	6	6
MF	1	1	0	1	1	0
	end					
Offset	0/8	505/8	1010/8	0/8	505/8	1019/8
	504	1003				
						CSF = 8

Re-assembly Algorithm at destination:

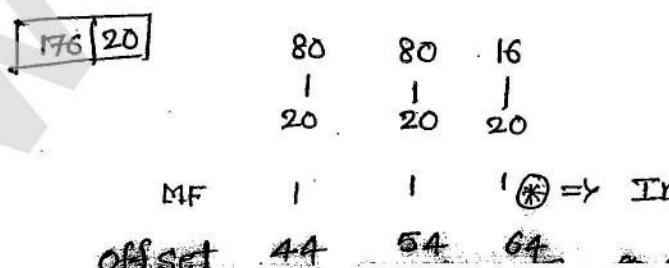
- * classify fragments based on 16-bit datagram number.
- * identify the fragment with offset=0 and designate it as a first fragment.
- * identify the fragment with MF=0 and designate it as a last fragment.
- * identify data in the first fragment and look for the fragment with same offset value and designate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

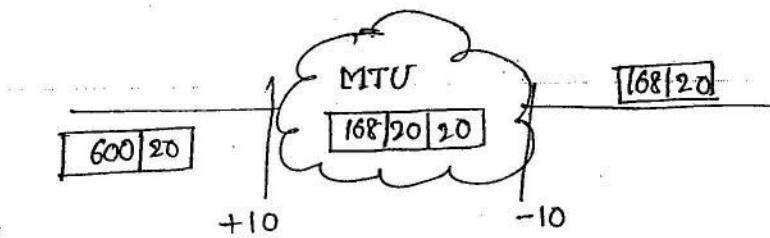


- * Datagram data (or) fragment data must be divisible with '8' if not adjust it's number so that it is divisible with '8'.
- * This rule is applicable for all the fragments except for last fragment.



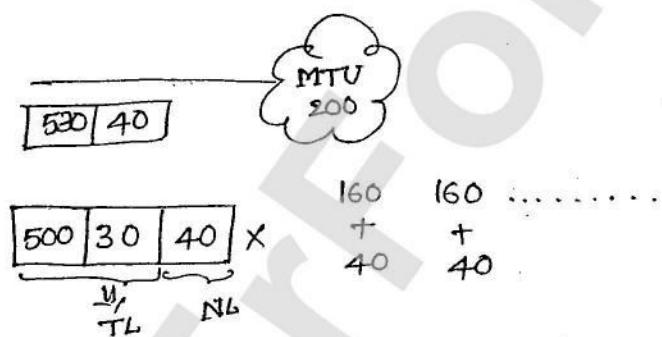
- * If offset = MF=0 \Rightarrow Original packet.
- * If any one of them is non-zero \Rightarrow fragment (intermediate fragment)





168	168	168	96
160	160	160	96
+ 20	+ 20	+ 20	+ 20
+ 10	+ 10	+ 10	+ 10
MF 1	1	1	0
offset 0	168/8	168 + 168/8

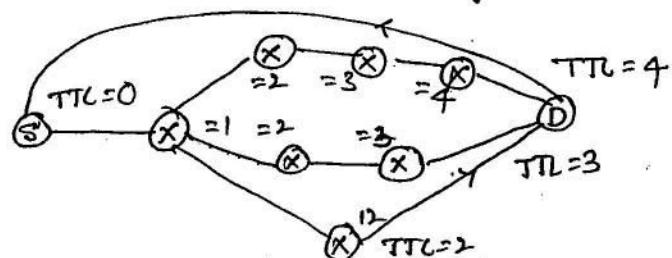
Msg : 500 { Datagram data.
 TCPH : 30
 IPh : 40
 MTU : 200



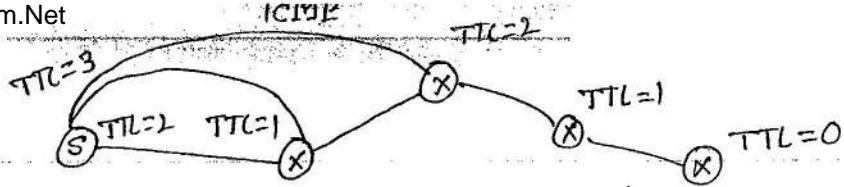
Time To Live (TTL):

- * it have four applications:-

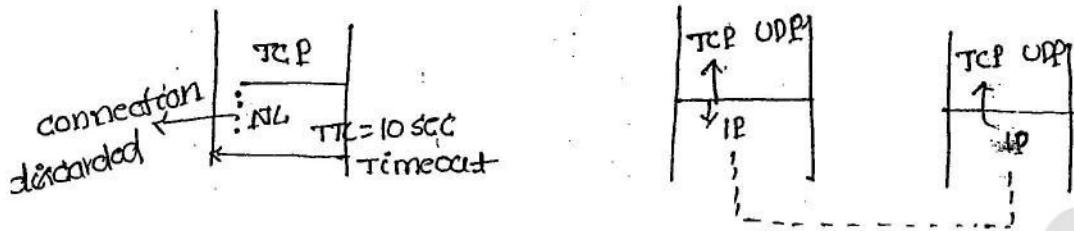
- To avoid infinite looping
- To identify no. of routers between source & destination
- To debug the network
- To help upper layers in timer management



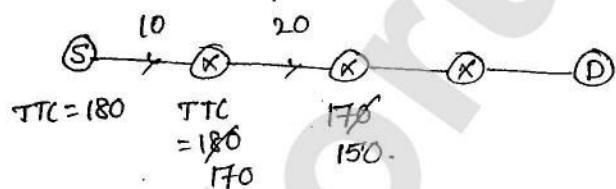
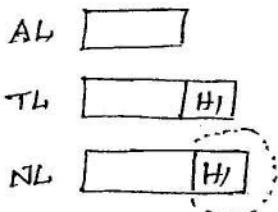
- * It is possible to find no. of routers in a route by using



Timer Management:



- * Header checksum is carried out at every router and only at Header.



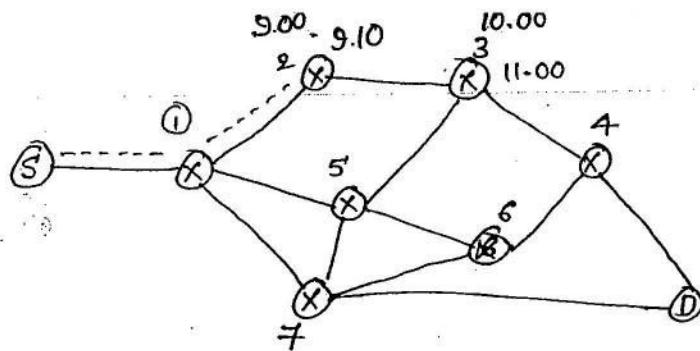
- TTL
- MF
- offset
- 16-bit datagram length
- options

→ tends to change
at every router
: (variable)

source }
destination } → fixed.

Options:

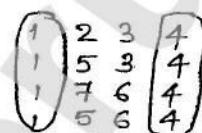
- * Strict source routing { source will decide the route
- * Loose source routing { source will decide the route
- * Record routing => Router decides the route
- * time stamp
- * Security



Strict source routing: Each and every node is specified

0, 1, 2, 3, 4

Loose source routing: only the important nodes are specified and the route is generated based upon those nodes \Rightarrow practical



Record Routing:

0, 1, 7, 5, 6

* Packet can be transferred as it wishes among all the nodes

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.



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.

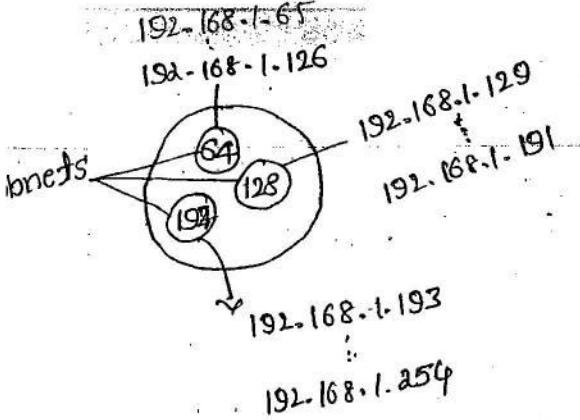


fig: 192.168.1

01-----

01 000001 - 65

01 000010 - 66

:

01 111110 - 126

10-----

10 000001 - 129

10 000010 - 130

:

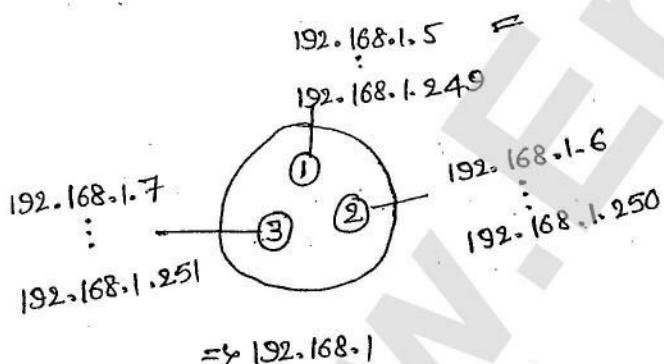
10 111110 - 191

11 000001 - 193

11 000010 - 254

C: NID HID
24 2,6 \Rightarrow borrow first 2 bits
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



NID HID

24 6,2

128, 64, 16, 8 4, 2,1

00 - 0
01 - 1
10 - 2
11 - 3

..... 01

0000010.1 = 5

0000100.1 = 9

..... 10
1111100.1 - 249

..... 10

00000110 - 6

00001010 - 10

..... 10
11111010 - 250

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

- Information regarding delivery of data packet, then following steps must be followed:
- Check if the port number is well known or not.
 - If no port is available then subnetting is available or not.
 - If not available then broadcast address of directly assigned to that.
 - If available then identify the packet belongs to which subnet for this we use subnet mask (SM).

Subnet Masking:

- * It is also a 32-bit system and it is used to indicate whether subnet are available (on) 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 network part or subnet id.
 2. No. of 0's indicates Host Id part.

Given IP: 192.168.1.100
 SM: 255.255.255.0
 Subnet ID: 192.168.1.100
 Host ID: 100
 Subnet mask = 255.255.255.0

SM: 1111111.1111111.1111111.00000000

Rule(1): $\frac{24}{NID} + \frac{0}{SID} = 24$ (since, class C)

(2): HID = 8 (since, no subnet, 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.

↳

$$SM: 255.255.255.192$$

$\cdot 11000000$

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

$$HID = 6$$

$$\text{No. of bits borrowed} = 2$$

Their position is = 128th bit, 64th

$$\text{Possible subnets} = 2^2 = 4$$

$$\text{Their subnet ID's} = \underline{11000000}$$

- 00 - 0
- 01 - 64
- 10 - 128
- 11 - 192.

$$\text{No. of systems per subnet} = 2^{6-2}$$

$$\text{Range of IP address} = 62.$$

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

$$SM: 1111111. 1111111. 111111. 00101001$$

$$\frac{24}{\text{NID}} + \frac{3}{\text{SID}} = 27$$

$$HID = 5$$

$$\text{No. of bits borrowed} = 3$$

Their position is 32, 8, 1

$$\text{Possible subnets} = 2^3 = (0, 1, 8, 32, 9, 40, 41, 33)$$

$$\text{No. of systems per subnet} = 2^{5-2}$$

$$\text{Their subnet ID's} = \begin{array}{c|c|c} 32 & 8 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{array} = 0 \quad \begin{array}{c|c|c} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{array} = 40 \quad \begin{array}{c|c|c} 32 & 8 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{array} = 41$$

Eg: Consider a class B network with SM = 255.255.255.0. Identify all the data packets or broadcast bytes.

→ Subnets are available

Entire 3rd packet are borrowed for subnet IDs

$$\therefore \text{No. of subnets} = 2^8$$

$$\text{Their ID's} = (0-255)$$

$$\text{No. of systems} = 2^8 - 2$$

$$\text{Their ID} = (1-254)$$

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

SM: 1111111.111111.111111.00001111

$$\begin{array}{r} 24 \\ \text{NID} + \text{HID} = 28 \\ 4 \end{array}$$

$$\text{No. of bits borrowed} = 4$$

$$\text{Their position} \in 1, 2, 4, 8$$

$$\text{Possible subnet} = 2^4 = 16$$

$$\therefore \text{No. of system per subnet} = 2^4 - 2 = 14$$

Eg: Consider a class C network proposed an appropriate subnet mask to have 7 subnets each with 25 systems.

$$7 * 25 = 256 \text{ (since, it is class C)}$$

3 bits must be borrowed (since, 7 subnets)

$$\begin{array}{r} 24 \\ \frac{8}{3 \quad 5} \\ 5 \quad 3 \end{array}$$

$$3\text{-bits} \Rightarrow 2^3 = 8$$

255.255.255.224

255.255.255.7

255.255.255.41

255.255.255.67

} all are possible but left to right ex appropriate

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

$$150 \times 200 <= 64,000$$

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

(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

$$\hookrightarrow 20 \times 15 <= 256$$

$$300 \neq 256$$

not possible.

Eg: Consider a class C network, propose an appropriate SM of ~~60~~ 60,60,120

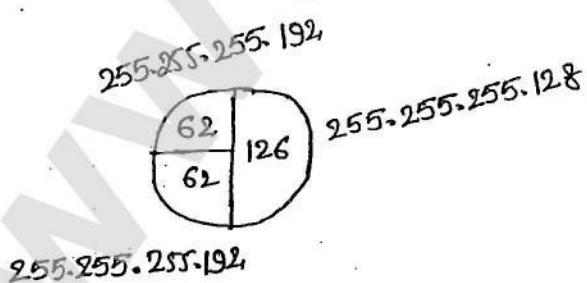
class C \Rightarrow 8

$$\begin{array}{cccc} \overline{2} & \overline{6} & \overline{1} & \overline{7} \\ \times & \times & \times & \times \\ 2 & 6 & 1 & 7 \\ \times 2 & \times 6 & \times 1 & \times 7 \\ \hline 6 & 12 & 2 & 14 \end{array}$$

$$\times 2-2 = 62, 2-2 = 126$$

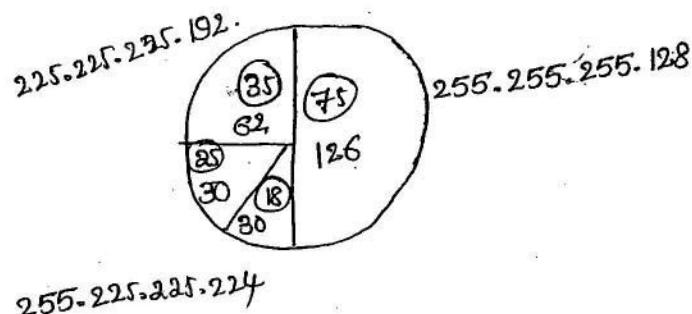
(Not possible) (Not possible)

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



$$\begin{array}{r} 1 \quad 6 \\ \times 2 \quad 2 \\ \hline 1 \quad 2 \end{array}$$

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



$$\begin{array}{cccc} 2 & 6 & 1 & 7 \\ 2^2 = 4 & & 2^1 = 2 & \\ 2^6 - 2 = 62 & & 2^7 - 2 = 126 & \end{array}$$

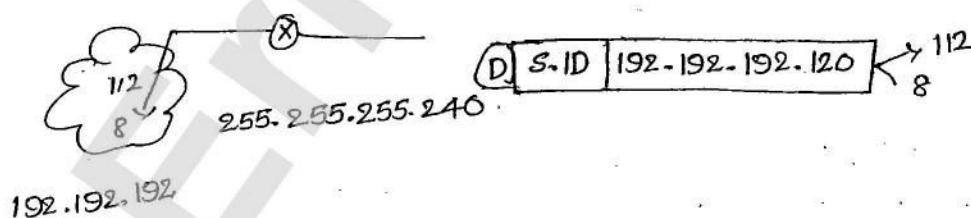
=

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

$$\text{class C} = 8 \quad 2^3 = 8$$

$$\begin{array}{c} 2 \ 6 \\ 2^6 - 2 = 62 \end{array}$$

Eg:



Identify subnet ID, Host ID and directed broadcast address.

IP: 11000000. 11000000. 11000000. 01111000
NID SID HID

192.192.192

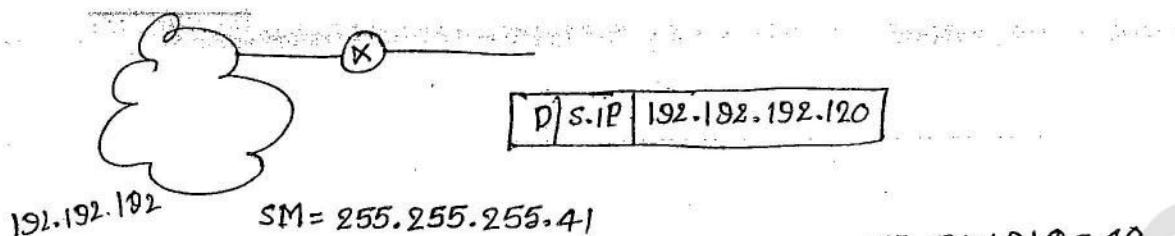
SM: 11111111. 11111111. 11111111. 11110000
NID SID NID

SID = 112

HID = $\frac{8}{120}$

192.192.192.127
11000000. 11000000. 11000000. 01111000 Broadcast Address
11000000. 11000000. 11000000. 01111000 Broadcast Address
11000000. 11000000. 11000000. 01111000 Broadcast Address
11000000. 11000000. 11000000. 01111000 Broadcast Address

eg:



$$SID = 32 + 8 + 0 = 40$$

IP: 11000000 . 11000000 . 11000000 . 011110000

SM: 1111111 . 1111111 . 1111111 . 00101001

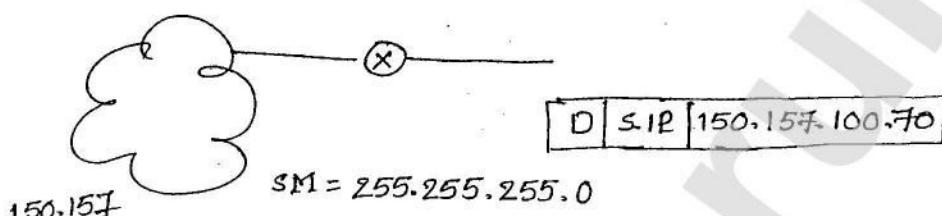
$$HID: 64 + 16 + 0 + 0 = 80$$

$$SID = 40$$

$$HID = 80$$

\hookrightarrow 192.192.192.254 \Rightarrow Broadcast address.

eg:

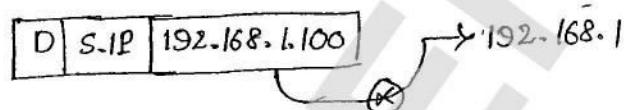


$$SID = 100.0$$

$$HID = 0.70$$

Directed Broadcast address = 150.157.100.255.

eg:



IP	SM	E/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

255.0.0.0

AND

255.255.0.0

AND

255.255.255.0

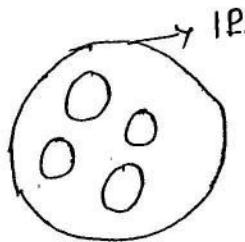
192.0.0.0

192.168.0.0

192.168.1.0

* 0.0.0.0 \Rightarrow Default or static subnet mask

Supernet Mask:



IP.

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 supernet mask indicates fixed part
- 2. num.of 0's indicates variable part.

111111.111111.1111100.00000000

SM = 255.255.252.0

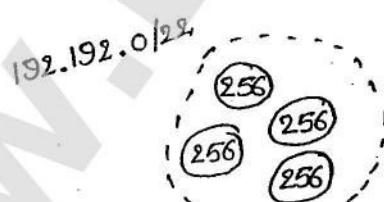
(1). 192.192.0/22 :

↳ Represents NID.

class C:

$$24 - 22 = 2$$

$$2^2 = 4$$



$$256 * 4 = 1024$$

/24 = class C

/16 = class B

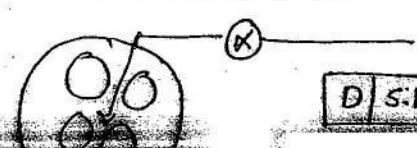
/8 = class A

22	10
NID	HID

$$2^{10} = 1024$$

(2). 192.192.0

255.255.255.0



D S IP 192.192.0.100

$$\begin{array}{r} 192 \\ \hline 4 \\ \hline 11000000 \end{array}$$

Difference Between Subnet mask & Supernet mask

SUBNET MASK

- * No. of bits in the subnet mask is either equal to network id or more than network id bits.
- * Bits are borrowed from NID.
- * It is applicable to single network.

SUPERNET MASK

- * No. of bits in supernet mask is always less than NID bits.
- * Bits are borrowed from NID.
- * It is applicable for two or more network.

** CIDR aggregation (classless Inter Domain Routing) \Rightarrow 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 \Rightarrow NID

/24 \Rightarrow class C

/16 \Rightarrow class B

/8 \Rightarrow 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 v: up
 G: Gateway
 H: host specific
 D: added by redistribution
 M: Modified by redistribution.

- ⇒ Delivery semantics:

unicast: delivers a msg to a single specified node.

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

Multicast: delivering a msg to a group of nodes that

~~have registered interest in the message~~

QTE: 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".

