

Computer Network

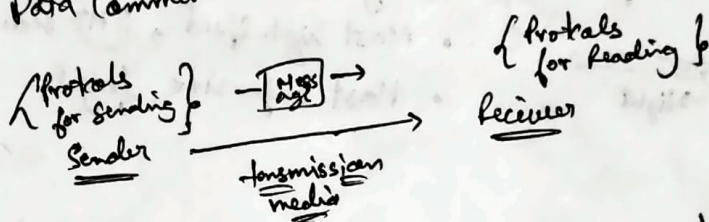
A set of devices connected through media link is called network.
(nodes)
Similarly computer networks are interconnected computing devices as nodes which can share and communicate between each other.

Application $\Rightarrow$

- Communication
- Resource Sharing
- Data Transfer
- Remote Access

Data Communication Components

The exchange of Data between two devices via transmission media is called Data Communication.



- Protocols are used at both ends for ensuring best data network.
- Message to be sent is sent in packets in the transmission media.

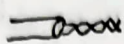
Types $\Rightarrow$ Point to Point (One to One)
of = Multipoint (Shared Media of transmission)
Connections

Transmission Modes

- Simplex (One way).
- Duplex Half (One way at one time for both direction).
- Duplex Full (Two Way communication).

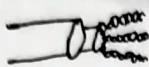
Transmission Media

* Twisted Pair Cable :- LAN's and Telephone Lines



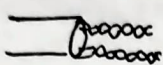
- Inexpensive & easy to install
- Limited Bandwidth, weak signals, Noise Prone

* STP STP :- Used for high EMI (Electromagnetic Interference)



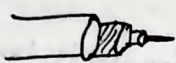
- Better at EMI
- Expensive & Bulkier than TP.

* UTP :- Most Common TP.



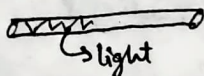
- Low cost in TP.
- EMI Prone, Limited distance.

* Coaxial Cable :- Television & Older Ethernet.



- EMI safe.
- Expensive & Bulky than all.

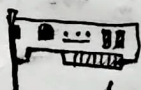
* Fibre Optics :- Long distance, high bandwidth.


→ light

- Most high Speed, EMI secure.
- Most Expensive, fragile.

Network Devices

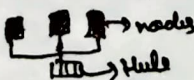
* NIC (Network Interface Card) :- Physical device installed in every device to connect device to the network media. Has Unique Mac Address. Mac address is used for host identification in network.



→ NIC Card

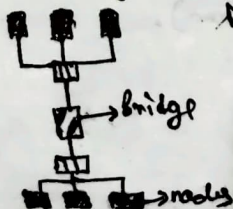
* Repeater :- Regenerates weak signals and amplifies them for further travel. Signal weakening due to media friction.

* Hubs :- Concentrate devices connection to view it as a single unit. Active Hubs also Repeats (Repeater) the signal.



Data Link Layer

* Bridges :- Repeater with add on functionality of filtering content by Mac Addresses of source & destination. Connection between LAN.



024

* Switches :- Intelligent data transfer, decides whether message should stay on the LAN or not & sends to connection it belongs to.
Performs Error checking.

Path
Link
layer

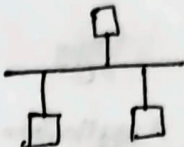
* Router :- Connects two or more LANs & WANs, routes messages and traffic based upon the destination and uses protocols for it.

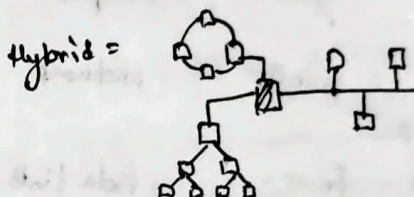
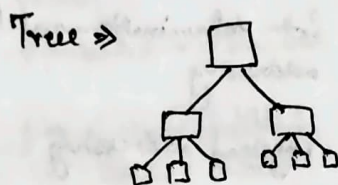
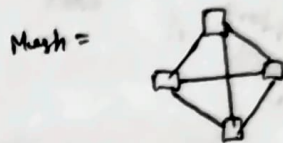
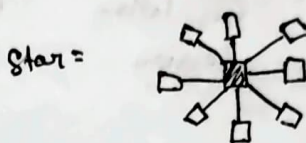
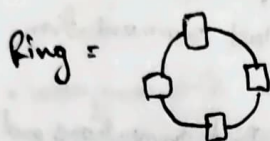
Network
layer

* Gateway :- Gateway connects two network which uses different protocol for communication.

Session
layer

Network Types $\Rightarrow$ LAN, MAN, WAN (PAN)

Network Topologies $\Rightarrow$ Bus = 



OSS- Model

7 $\Rightarrow$ Application

6 $\Rightarrow$ Presentation

5 $\Rightarrow$ Session

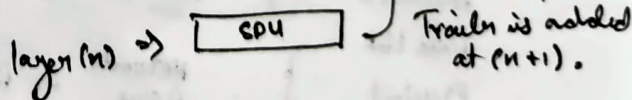
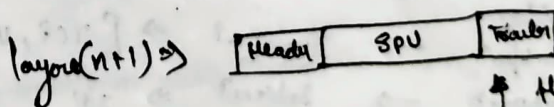
4 $\Rightarrow$ Transport

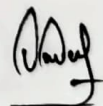
3 $\Rightarrow$ Network

2 $\Rightarrow$ Data Link

1 $\Rightarrow$ Physical

Every layer (n) follows some protocols, layer invokes ^{ctrl} functions or services of layer n using SAP (Service Access Points). layer (n+1) only passes data to layer n & process is repeated till by physical layer. data passed using PDU's.





Network layer (Just for Understanding a/lgn functions)

Addressing :- Source and destination addresses added to header of the frame, for ~~network~~ identification on the Internet.

Functions of Network layer

Routing :- It determines the best optimal path between source & destination.

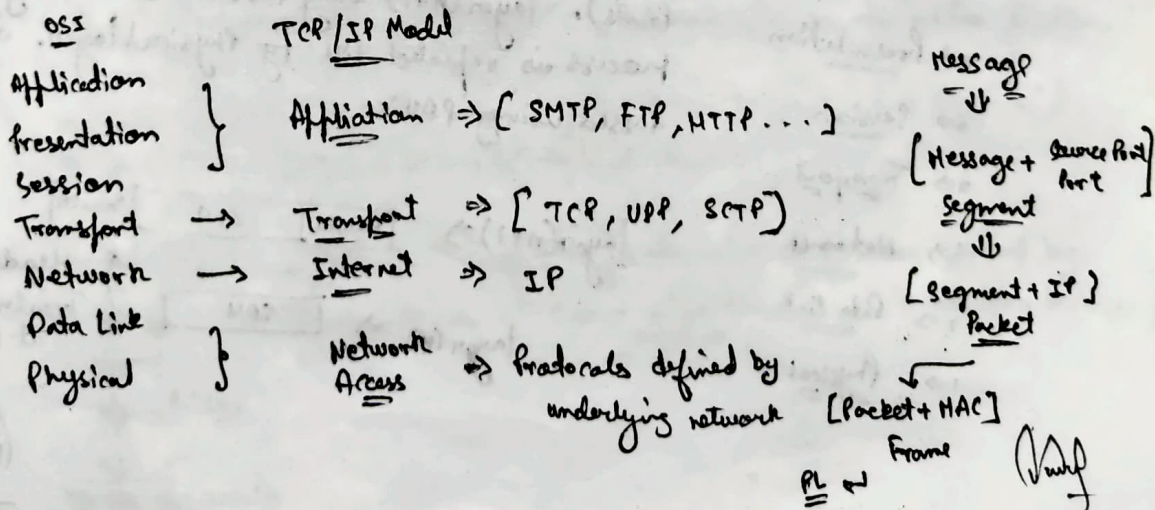
Packratization :- Converting upper layer data into packets using IP.

Inter networking :- Provides logical connection between different devices.

OSI - Layer Summary

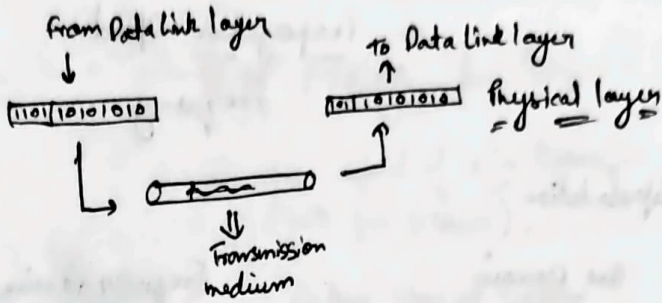
	<u>Data Unit</u>	<u>Layer</u>	<u>Function</u>
User Support layers	Data	Application Presentation Session	Network process to Application Data representation and encryption Inter Host communication
User Network	Segment	Transport	End to End connections and reliability
	Packet	Network	Path determination and logical addressing
Network Support layers	Frame	Data Link	Physical addressing
	Bit	Physical	Media, Signal & Binary Transmission

TCP/IP Model



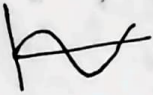
Physical Layer

- Main task of this layer is to convert data from data link layer into signals and send it to the transmission medium vice-versa.



Types of Data Transmission :-

Analog



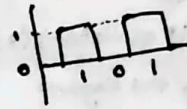
- waveform state
- Can be used for continuous values
- Represented by Sine wave

↑ => Capture subtlest smallest nature

↓ => - Loses Energy

- Regular Repeater can be used
- Noise
- Can't be Copied Perfectly

Digital



- on/off state (1) & (0)
- Only for discrete values (distinct)
- No simple way to represent

↑ => Fast Communication

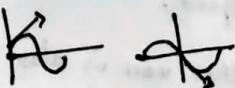
- Perfect Copying
- High Speed
- Less prone to Error

↓ => - Absorbers & Regenerator should be used for long distance.

* Frequency :- rate of change with respect to time.

$$f = \frac{1}{T}$$

* Phase :- Position of the waveform with respect to time 0.



↑ different phase

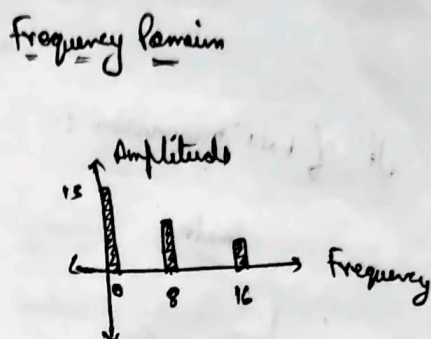
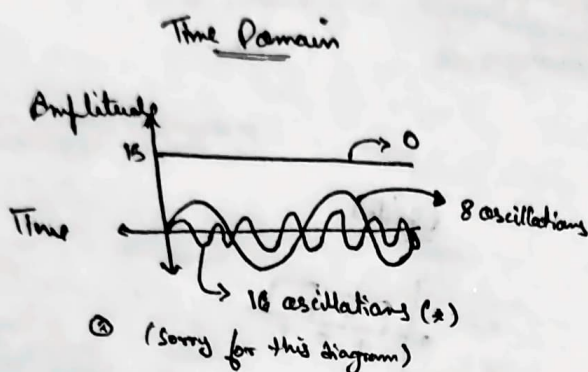
Day

* Wavelength :- The distance travelled at a propagation speed in one complete oscillation. (Time period)

Wavelength $\Rightarrow$ Propagation Speed $\times$ Period

$$\Rightarrow \frac{\text{Propagation Speed}}{\text{Frequency}}$$

Wave Representation :-



* Fourier Analysis $\Rightarrow$

- A composite function can be represented as combination of different sin waves.
- Periodic Composite can be discrete frequency.
- Non-Periodic sine waves with continuous frequency.

* Bandwidth $\Rightarrow$ Bandwidth of composite signal will be highest Frequency - Lowest frequency.

Baseband Transmission

Broad Band Transmission

* Impairment of Signals :-

Attenuation $\Rightarrow$ Reduction or loss of Energy in wave due to medium friction.

$$\text{Attenuation} = 10 \log_{10} \frac{P_2}{P_1} \rightarrow \text{lost}$$

$$\rightarrow \text{Original}$$

Distortion $\Rightarrow$ Distortion in composite signal if there is phase difference due to propagation speed.

Noise $\Rightarrow$ Noise occurs where another wave is also included (not the one)

$$SNR_{dB} = 10 \log_{10} (SNR), \quad SNR = \frac{\text{Signal Power}}{\text{Noise Power}}$$

Paul

* Network Performance :-

$$\text{Latency} = \text{Propagation Time Delay} + \text{Transmission Time Delay} + \text{Processing Time Delay} + \text{Queueing Time Delay}$$

Bandwidth = Range of frequency for Composite signal

- Data rate speed of data transfer in a channel. (bits per second).

$$\text{Channel Utilization} = \frac{\text{Active Time of Sender}}{\text{Total Time of 1 Cycle}}$$

• $t_t = \frac{f}{r} \rightarrow$ frequency
 $r \rightarrow$ bit rate

• $t_p = \frac{d}{r} \rightarrow$ distance
 $r \rightarrow$ propagation speed

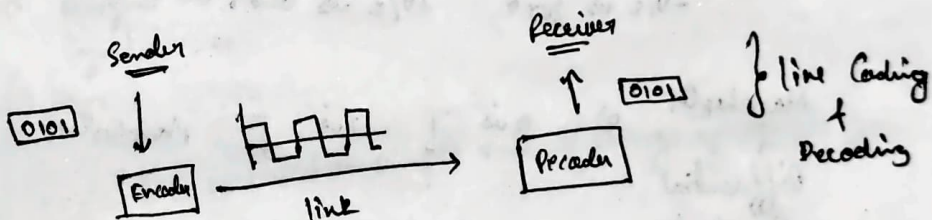
$$= \frac{t_t}{t_t + 2t_p} \rightarrow \text{Transmission time}$$

$$\rightarrow \text{Propagation time}$$

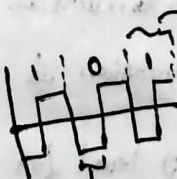
Throughput = Volume of data Produced in given time unit.

$$\frac{\text{Total Data}}{\text{Time taken}}$$

Line Coding & Decoding



* Signal & Data Element



Data Element $\Rightarrow$ Smallest Entity of information

Signal Element $\Rightarrow$ Smallest unit of digital signal

$$r = \frac{\text{no. of Data Element}}{\text{no. of Signal Element}}$$

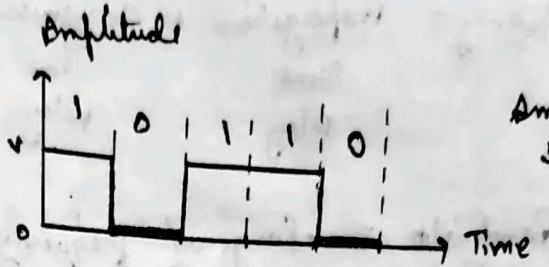
$$\text{Signal Rate} = \frac{\text{Data Rate (N)}}{r}, \text{ Avg Signal Rate} = C \times \frac{\text{Data Rate}}{r}$$

(loss factor)

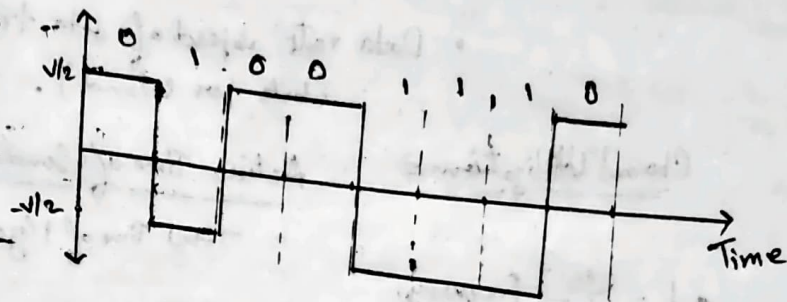
[Signature]

Line Coding Schemes

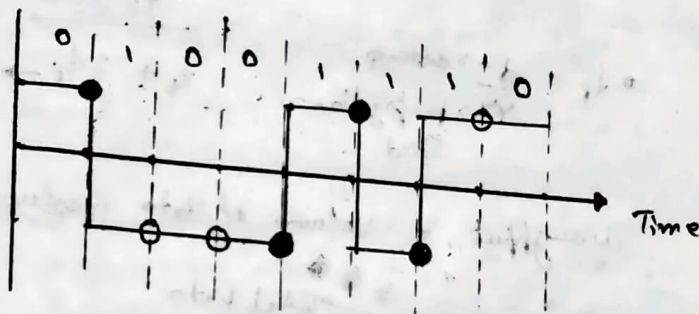
Unipolar NRZ $\Rightarrow$



NRZ-L $\Rightarrow$



NRZ-I $\Rightarrow$



Polar-RZ $\Rightarrow$

- first Half of the Signal element is for Data representation.
- Second Half returns to zero.
- V/2 is zero +V/2 is One.

Manchester
+
Differential
Manchester

$\Rightarrow$ 0 is $\left[\right]$ 1 is $\left[\right]$ Manchester

- no inversion is zero One.
- Inversion is zero.

Bipolar $\Rightarrow$ AMI = 0 level for zero

Next high level is One (if +V/2 was used before -V/2 is One)

Signature

PCM - Pulse Code Modulation



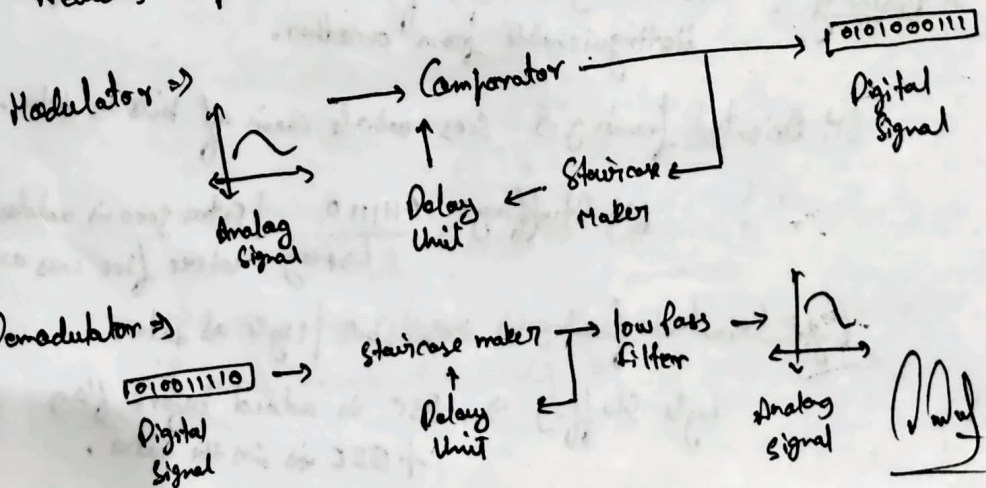
Nyquist Theorem

$$\Rightarrow \text{Nyquist rate} = 2 \times f_{\text{max}}$$

- 1 $\Rightarrow$ Analog Signal is received.
- 2 $\Rightarrow$ Analog Signal is sampled.
- 3 $\Rightarrow$ Sampled Signals are Quantized.
- 4 $\Rightarrow$ Quantized signals are assigned words (bits).
- 5 $\Rightarrow$ Assigned words are converted in Digital Signal.

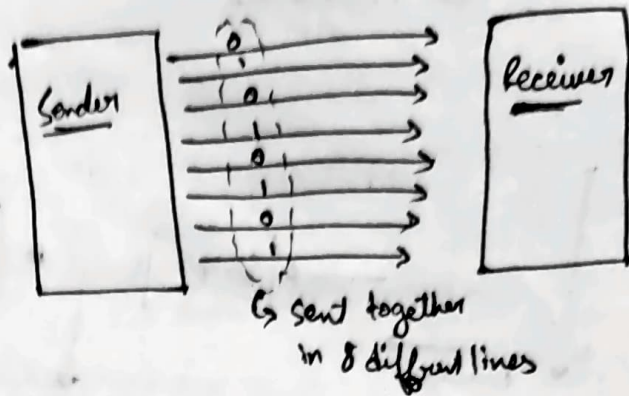
Delta Modulation

Delta Modulation is based on simple rule of change of sample from previous sample.

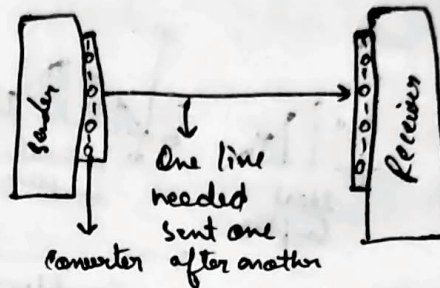


Transmission Modes

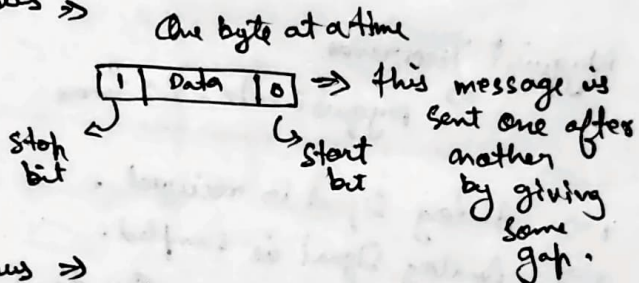
- Parallel transmission ⇒



- Serial transmission ⇒



- * Asynchronous ⇒



- * Synchronous ⇒

Data is sent in form of block & frames where a clock is used for info about new byte.

Data Link Layer

- Framing • Physical Address • Flow Control • Error Control

- * Framing :- • converting stream of bits or character into frame which distinguishable from another.

Bit Oriented framing ⇒ sees whole chain of bits as data.

Bit Stuffing = 0111110 | Extra zero is added at place where five ones are coming.

Byte Oriented framing ⇒ sees 8 bits / 1 byte as data.

byte Stuffing ⇒ ESC is added before flag + ESC is in the data.

Error Detection & Correction

6

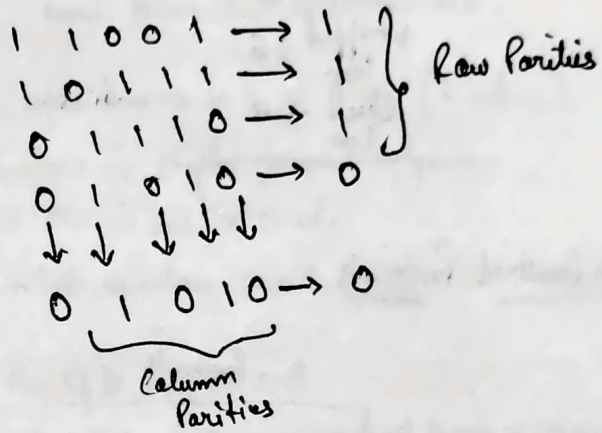
* Parity checker $\Rightarrow$

- Single Parity = Data $\boxed{}$ $\rightarrow$ Parity bit is added which will represent number of one's

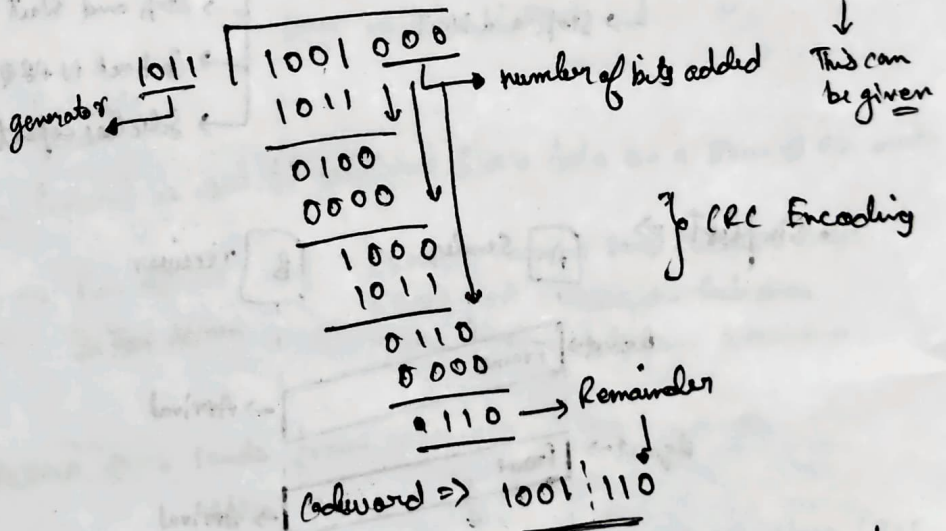
If Condition Satisfies correct $\left\{ \begin{array}{l} 1 \rightarrow \text{odd number of One's} \\ 0 \rightarrow \text{even number of zero's} \end{array} \right.$

- 2D Parity = Data is Organized in 2D Matrix.

- Max 3 bit error can be detected.



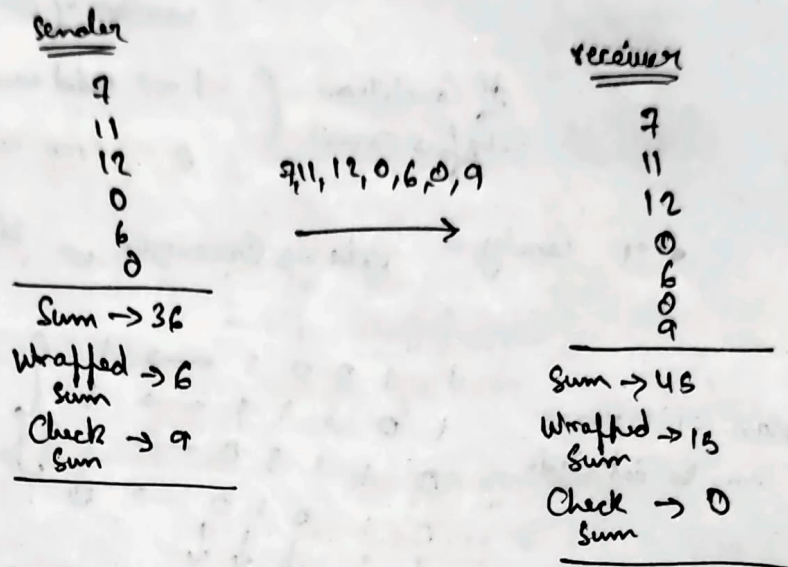
- Cyclic Redundancy Check = (CRC)



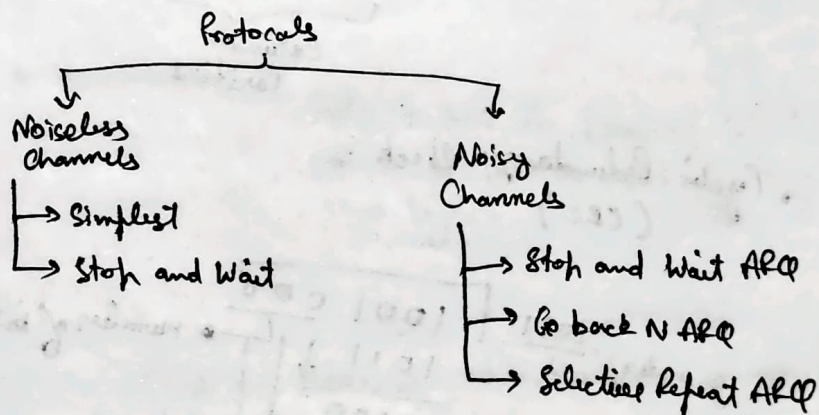
- CRC decoding, divide the code word using same generator if 000 remainder accept the code word else reject.

ADJ

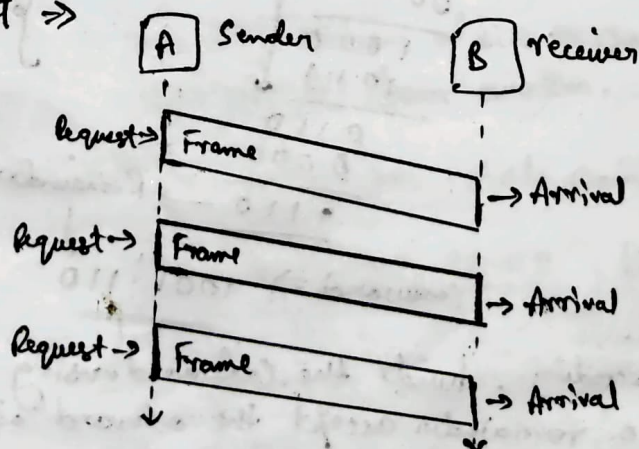
- Check Sum :- • The message divided into n-bits chunk & check sum is calculated.
- This check sum is sent with the data.
- If other side get zero the data is accepted.



Flow Control Protocols



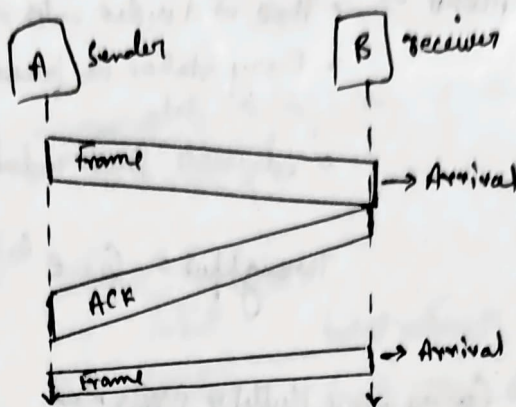
• Simplest $\Rightarrow$



[Signature]

• Stop and Wait

Sends next frame only after receiving ACK



• Stop & Wait ARQ $\Rightarrow$ - Frame Acknowledgment.
 - frame resent after ACK Timeout.
 Next frame sent after one ACK.
 max window size = 1
 both

• Go Back ARQ $\Rightarrow$ - Multiple frames sent at Once (Window).
 - Window is shifted to next only when one ACK is not received.
 - Whole window resent if ACK Not received.
 max sending = $2^K - 1$
 receiver = 1

• Selective for Go Back ARQ $\Rightarrow$ - Multiple frames sent.
 - Multiple ACK & NACK sent from receiver.
 - Only those frames are resent which received NACK and to fill window size some next are taken.
 max window $\frac{2^K}{2}$ both

Random Access Protocols

This protocol is used to send and share data on a shared channel.

ALOHA $\rightarrow$ Pure ALOHA
 Slotted ALOHA

CSMA - Carrier Sense Multiple Access
 CSMA / CD - Collision Detection
 CSMA / CA - Collision Avoidance

* Pure ALOHA $\Rightarrow$ • sends frame whenever it has a frame.
 • After time-out if no ACK.
 • Resends data after waiting for random time ($R \times T_p = T_R$)
 • vulnerable time is 2-time T_p .

Throughput = $G \times e^{-2G}$ G = number of stations trying to send data

Handwritten signature

- A Slotted ALOHA $\Rightarrow$
- Time is divided into slots of size T_{pr} .
 - Every station is forced to send data at beginning of the slot.
 - Vulnerable time reduced to $1T_{pr}$.

$$\text{Throughput} = G \times e^{-G} \quad \text{max efficiency} = 36.8\%$$

* CSMA - Carrier Sense Multiple Access $\Rightarrow$

"sense before transmit" or "listen before talk"

- before sending every frame station first checks for channel status.
- Sends when at only channel is IDLE.
- Collision may still occur due to propagation delay.
- 1-Persistent CSMA $\Rightarrow$ senses the channel continuously checking channel.
- non-Persistent CSMA $\Rightarrow$ senses the channel & waits for random time after busy.
- P-Persistent CSMA $\Rightarrow$ for slotted channels, waits until next slot for sensing if found busy. Continuously checks for busy of channel until sensing found idle.

- * CSMA / CD $\Rightarrow$
- After sensing the collision frame transmit is Aborted immediately.
 - Saves bandwidth.
 - Collision can be detected by power or pulse of received signal.
 - waits for random time & tries again.

- * CSMA / CA $\Rightarrow$
- Channel is free station waits for PFS time before sending data.
 - Contention window before transmit & Time-out period after sending.

Network Layer

IP-Addressing

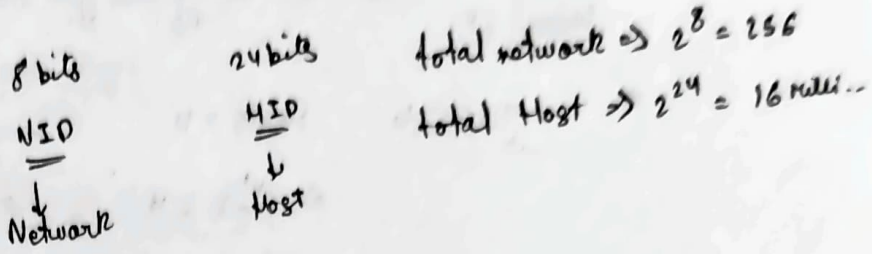
Routing

Only

IP- Addressing

IP - Addressing is important for identification of host & network

* Static Partitioning $\Rightarrow$



* IPv4 $\Rightarrow$ 32-bit address 2^{32} address space.

• Classful addressing $\Rightarrow$ IP Addresses are divided into classes with default subnet mask for network identification.

	first byte	second byte	third byte	fourth byte
(0-127) Class A	0.....	Host	Host	Host
(128-191) Class B	10.....	Host	Host	Host
(192-223) Class C	110...	Host	Host	Host
(224-239) Class D	1110...	-	-	-
(240-255) Class E	1111...	-	-	-

Subnet mask A $\Rightarrow 255.0.0.0$ B $\Rightarrow 255.255.0.0$ C $\Rightarrow 255.255.255.0$

• Classless Addressing $\Rightarrow$ IP Addresses are divided into blocks rather than classes.

Notation $\Rightarrow$ n.y.z.w/n
 $\downarrow$ no. of network bits

First Address $\Rightarrow$ network mask & with IP address given.
 Last Address $\Rightarrow$ network mask complement OR with IP address given.
 Network Address is the First Address.

Subnetting

Dividing IP addresses into logical blocks. FLSM VLSM

Handwritten signature

FLSM - Fixed Length Subnet Masking

We will divide one network into different blocks as a subnet using subnet masking.

We have to decide how many bits you have to assign for Subnet ID.

⇒ given = 4 Hosts = H Subnets = S

⇒ $2^{H'} - 2 \geq H$

⇒ $2^{S'} = S$

$32 - H' \Rightarrow$ number of Network or Subnet

$32 - S' \Rightarrow$ number of Subnet

Block Size $\Rightarrow 2^{H'}$ or $2^{S'}$

VLSM - Variable Length Subnet Masking

Same like FLSM here we divide net into subnet with one subnet mask assigned. but here each subnet has their own subnet mask. Block Size is decided.

Block Size $\Rightarrow 2^K - 2 \geq M \rightarrow$ requirement of Network Hosts

$2^K =$ Block Size, $\frac{32}{K} =$ number of bits for subnet

Ex:- $17.12.14.0/26$, Sales & Purchase = 120 hosts
 Development = 50
 Accounts = 26
 Management = 5

Sales & Purchase = 120 hosts

$2^K - 2 \geq 120$ | Block Size = $2^K = 128$ Network $\Rightarrow 17.12.14.0$
 $\boxed{K=7}$ Subnet $\Rightarrow 32 - 7 \Rightarrow 25$ bits $17.12.14.128$
 $\hookrightarrow 255.255.255.128$

Development = 50

$2^K - 2 \geq 50$ | Block Size = $2^K = 64$ Network $\Rightarrow 17.12.14.128$
 $\boxed{K=6}$ Subnet = $32 - 6 \Rightarrow 26$ $17.12.14.192$
 $\hookrightarrow 255.255.255.192$

Similarly $\Rightarrow 255.255.255.224 / 192 - 223$
 $255.255.255.240 / 224 - 239$ for others

[Signature]

Network Layer

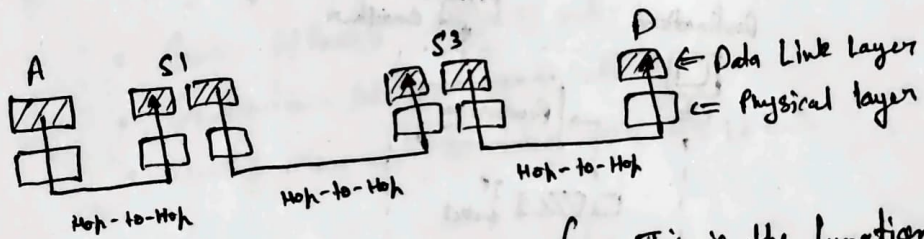
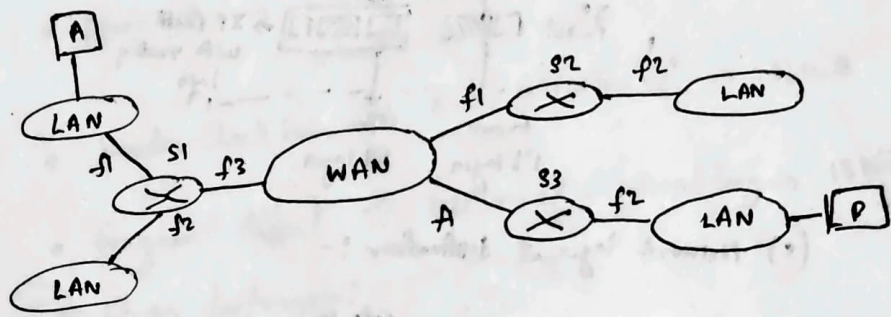
functions of Network layer is mainly to route data from different Protocol to the destination.

- Inter Networking
- Encapsulation
- Routing
- Fragmentation

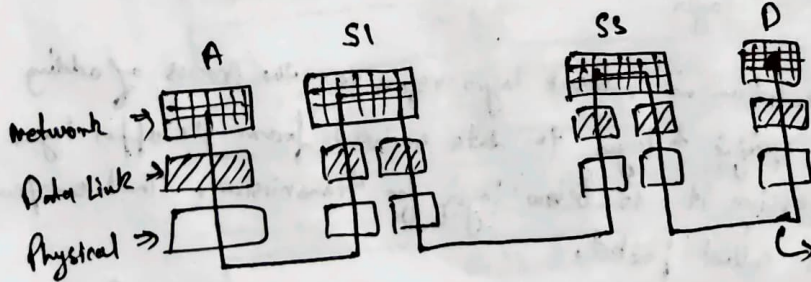
* Inter- Networking

connecting multiple networks to make an internetwork or internet. This concept also allows use of multiple networks as a bridge to the path between source & destination.

A → D
Source Destination



→ This is the functionality we need to get this done network layer is introduced.

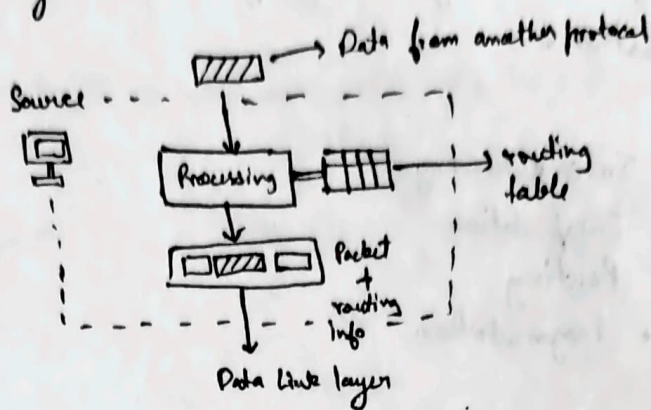


→ Network layer handles all the hop-to-hop directions

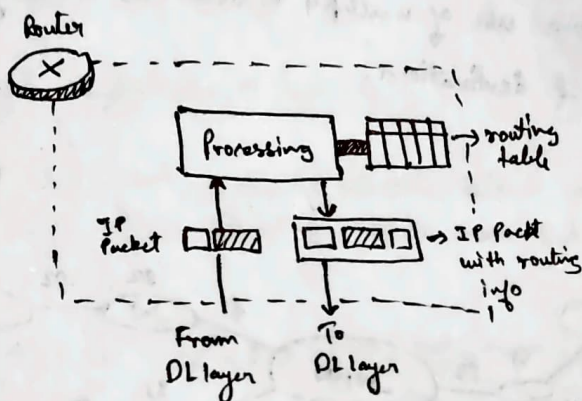
[Signature]

* Network layer at different level $\Rightarrow$

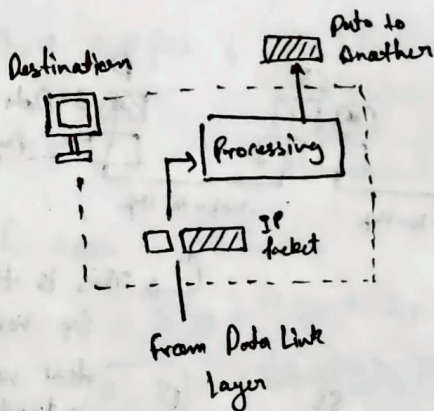
(a) Network layer at Source :-



(b) Network layer at a router :-



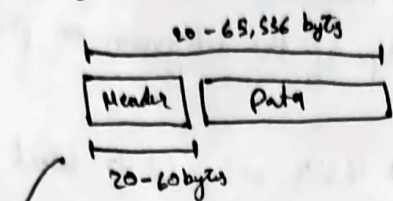
(c) Network layer at destination :-



* Encapsulation $\Rightarrow$ encapsulation in network layer refers to the process of adding headers specific to layer to data received from the upper layer before passing it to below layer for transmission. That encapsulated data is called packet.

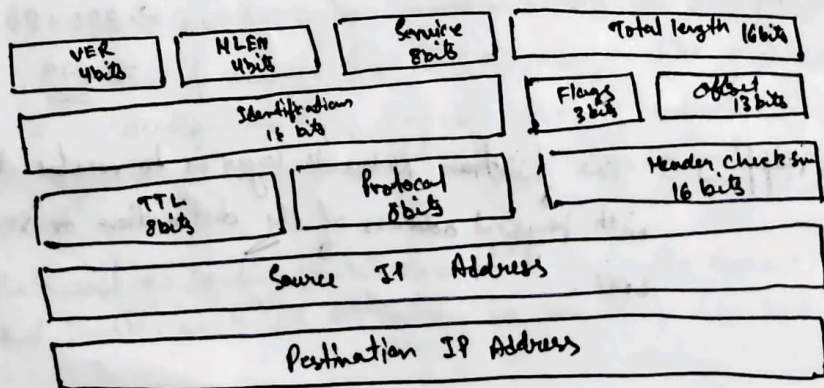
M

* IPv4 Datagram (Encapsulation):-



Header is the data or info added by IPv4

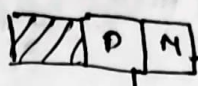
- VER (Version) → Version of IP Protocol → 4bits
- Header Length (HLEN) → the total length of the datagram header → 4bits (4byte word)
- Services → Service type → 8bits
- Total length → total length of Header + Data → 16 bits (8 byte word)
- TTL (Time to Live) → will changed whenever goes from a router → 8bits
- Protocol → Higher level Protocol which used this IP → 8bits
- Header Check Sum → Error detection of Header → 16bits
- Fragment Offset → position of Original frag. → 13bits
- Flags for fragment → 3bits
- Source Address → 32 bits
- Destination Address → 32bits
- Identification → fragment ID → 16 bits



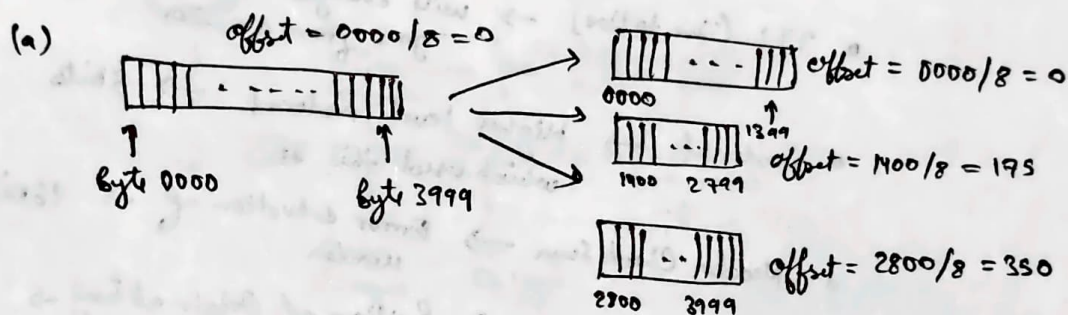
... Option

[Signature]

* Fragmentation :- Fragmentation occurs when IP Datagram or Packet travels through a network with Maximum Transmission Unit (MTU) that is smaller than size of the datagram or packet.

Fragmentation $\rightarrow$ Identification $\Rightarrow$ 16 bits assigned to label fragment with use of the source data.
 Fragmentation offset $\Rightarrow$ for Start bit position identification 13 bits
 Flags $\Rightarrow$  More fragment ahead
 Do not fragment

Example $\Rightarrow$



(b) offset Value = 100, HLEN = 5, TL = 100, first & last bit = ??
 (8 word) (4 word)

$$100 \times 8 \Rightarrow \text{Start byte} \Rightarrow \underline{800}$$

$$\text{Last byte} \Rightarrow 800 - (\text{Header Size}) - 1 + (\text{TL})$$

$$\Rightarrow 800 - (4 \times 5) + (100) - 1$$

$$\Rightarrow 800 + 80 - 1$$

$$\Rightarrow \underline{879}$$

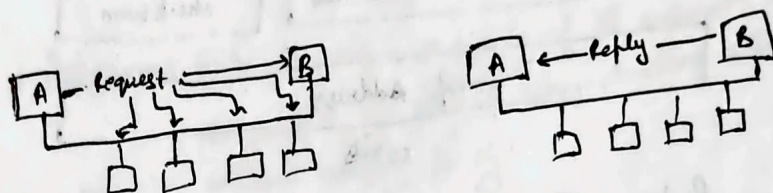
* Address Mapping :- This function Network layer is to resolve IP address with physical address of the destination or source in same LAN.

• ARP (Address Resolution Protocol) $\Rightarrow$ Mapping Logical Address to Physical Address

$\rightarrow$ The host or the router sends ARP query packet to all hosts.

$\rightarrow$ Packet includes Logical Address of sender & receiver & Physical Address of sender.

$\rightarrow$ Host with same address the sender host is finding, acknowledges by sending Physical Address



Cases of ARP Being Used $\Rightarrow$

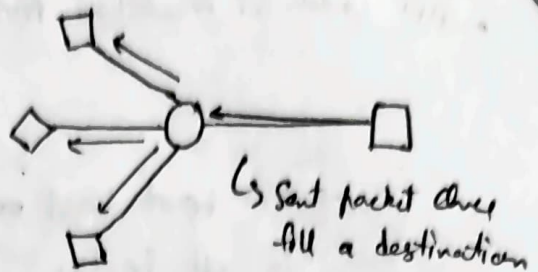
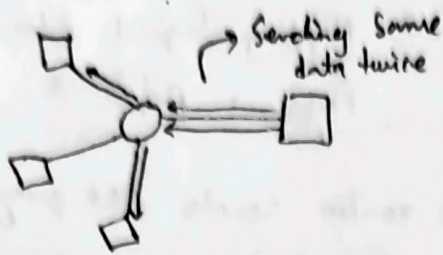
- (i) Host to Host
- (ii) Host to Router
- (iii) Router to Host
- (iv) Router to Router

• RARP $\Rightarrow$ Mapping Physical Address to Logical Address

RARP allows a device to discover its own IP address when it only knows its MAC address. The device sends a RARP request with its MAC address, a RARP server on the same LAN responds with Logical Address or IP address.

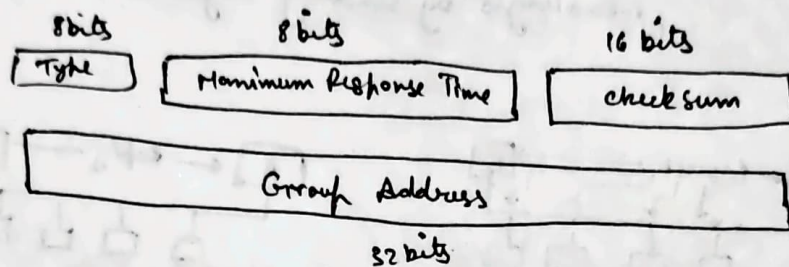
* IGMP :- There are two types communication in Interprotocol (IP) unicast & multicast. You can assume like giving a message a to destination once they ask directly to them, if same packet is required for other it will send again in different channel this is unicast.

Multicast is sending packet once till the router (nearest) and fetching that similar with all destination source.



IGMP is group management protocol. It helps a multicast router create and update a list of loyal members to each router interface.

IGMP Header $\Rightarrow$



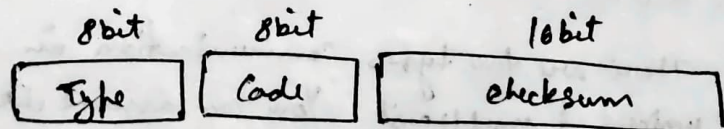
Maximum Response Time :- Specifies how long members can wait before responding

checksum :- Error checking for IGMP Message

Group Address :- Multicast Group address assigned

Type :- IGMP message type

* ICMP (Internet Control Message Protocol) :- This protocol is to solve two broad problems error-reporting & query messages for host management. Reports error messages to the original source.

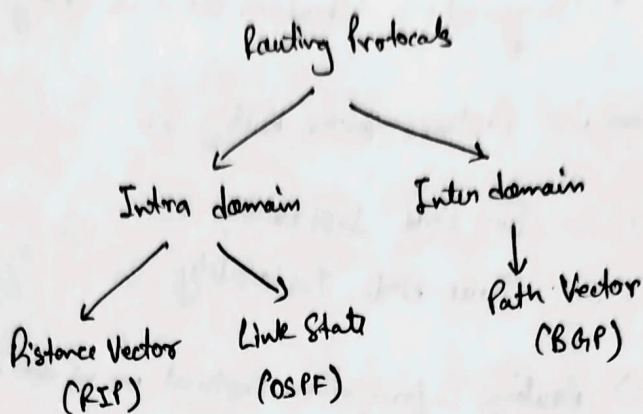


Errors $\Rightarrow$ Destination Unreachable, Source Quench, Time Exceeded, Parameter problems, Redirection

Query $\Rightarrow$ Echo, Timestamp request & reply.

Handwritten signature

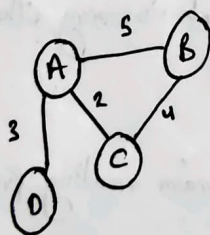
* Routing Protocols :- Routing Protocols are used for two main purpose
Dynamic Routing or Path selection & Routing Table Maintenance.



• Autonomous System $\Rightarrow$ AS is a group of IP Networks and routers under the control of single administrative entity that presents a unified routing policy.

Intra domain $\rightarrow$ Inside one single Autonomous System
Inter domain $\rightarrow$ Inside between two or more Autonomous System.

Distance Vector Routing $\Rightarrow$ In this method each node maintains a vector (table) of minimum distances to every node. These vector are initialize first and updated with shared info of neighbor distance vector.



1st $\rightarrow$ A's table =

To	Cost	Next
A	0	-
B	5	-
C	2	-
D	3	-

} Similarly All are initialized

B's table =

To	Cost	Next
A	5	-
B	0	-
C	4	-
D	∞	-

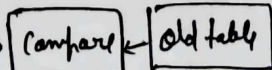
update $\Rightarrow$

A	2
B	4
C	0
D	∞

from C

A	4
B	6
C	2
D	∞

Now A Table



New table with entry of min distance

My

92
updating of routing table is done in two manner $\Rightarrow$

- Periodic $\rightarrow$ Once in 30 sec
- Triggered $\rightarrow$ Whenever there is change in Topology

Problem in Distance Vector Routing $\Rightarrow$

Two Node Instability

Three Node Instability

* RIP $\Rightarrow$ Routing Information Protocol is an intradomain routing protocol used inside an autonomous system. RIP implements distance vector routing directly with some considerations.

$$\text{Bellman-Ford} \Rightarrow d_n(y) = \min_v (c(x, v) + d_v(y))$$

• Link-State Routing :- Link State routing each node in the topology has the entire topology of the domain. Node uses Dijkstra Algorithm to build whole routing table.

LSP $\Rightarrow$ Creating a Link State Packet which a routing table with extra info

Flooding $\Rightarrow$ Send Sending LSP of every node to every node in the network.

Formation $\Rightarrow$ Creation of shortest path at each to every other node.

Updating $\Rightarrow$ Updating routing table.

* OSPF $\Rightarrow$ Open Shortest Path First is an intra domain routing protocol based on link state routing.

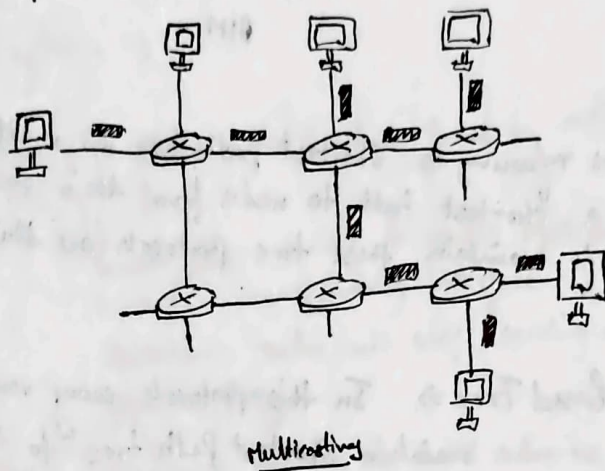
Areas in Autonomous System

Ans

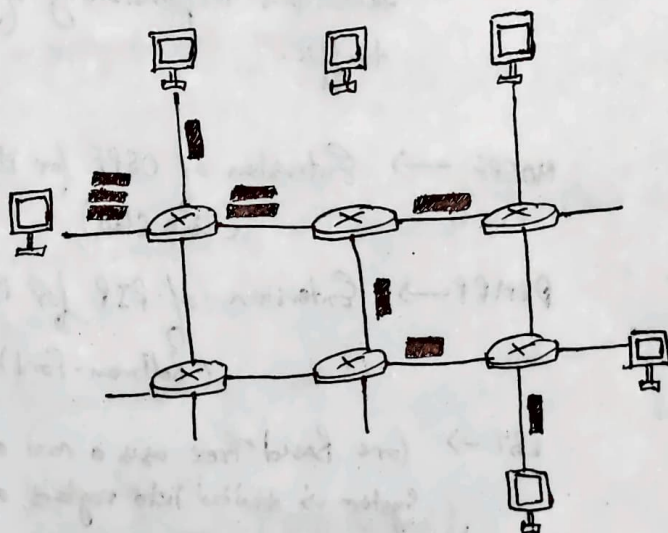
16 Change multicast IP Address 238.92.24.9 to an Ethernet multicast physical address. Given, Ethernet multicast physical address range is 01:00:5E:00:00:00 to 01:00:5E:7F:FF:FF. (13)

* Multicast Routing vs Unicast Routing

Multicasting starts with one single packet from the source that is duplicated by the routers. The destination address in each packet is the same for all duplicates.

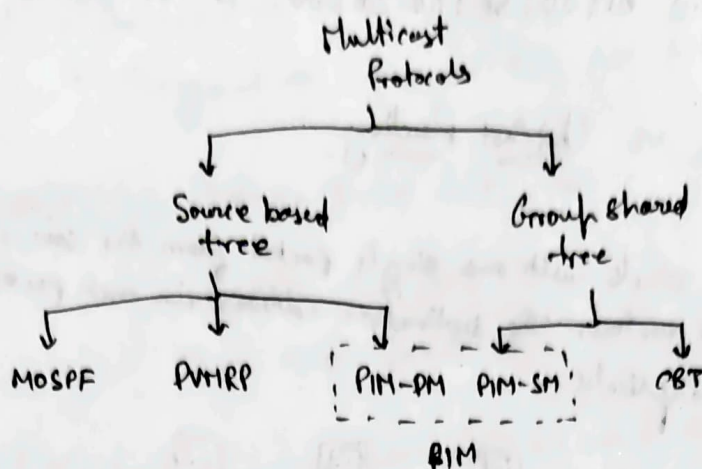


Unicasting several packets start from the source. If there are five destinations, five packets will be sent, each with different unicast address of destination.



13

Multicast Protocols



Tree is referring to shortest path tree in multicast routing. This tree maintains a shortest path to nodes from their source. By using different approach to maintain these tree protocols are divided.

Source Based Tree $\Rightarrow$ In this protocols every router is designated to maintain shortest path tree to the destination groups.

Group Shared Tree $\Rightarrow$ In this instead of each router maintain shortest path to all groups. One designated router (core) takes this responsibility of distributing multicast traffic.

MOSPF $\rightarrow$ Extension of OSPF for Multicast (link state)

PIMRP $\rightarrow$ Extension of RIP for Multicast (Bellman-Ford)

CBT $\rightarrow$ Core Based Tree uses a core as the root, an Autonomous system is divided into regions, and a core is selected for each region.

PIM-DM $\rightarrow$ Uses RPF & Pruning, Grafting technique to handle multicasting.

Reverse Path

RPF, RPB, RPM → Multicasting these methods collectively used to implement loop free multicasting with pruning & grafting.
↓
Forwarding → Broadcasting

- RPF → Checks incoming interfaces validity for loop prevention
- RPB → Forwards only to child links.
- RPM → Prunes inactive branches.

* Pruning & Grafting ⇒

Pruning = The process starts when found no active members in group.

Sends prune packet to router upstream so that it will exclude corresponding interface.
Upstream router will stop sending multicast messages for that group.

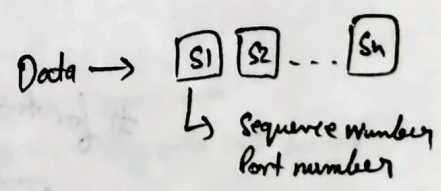
Grafting = Leaf node realises about its activeness through IGMP and to get packet from router it will send graft message upstream to router.

Graft message forces router to start sending packets or messages to the group.

Transport Layer

This layer of OSI model is 4th layer in it. Main task & function for this layer are :-

- Segmentation of Data.
- Flow Control
- Error Control (End to End)
- Process to Process Communication



Amal

* TCP Segment Header

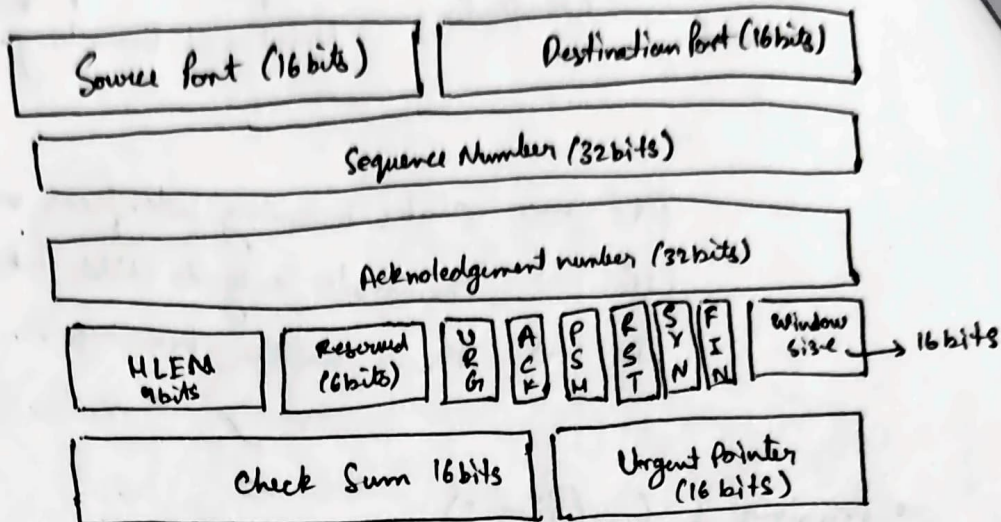
Port Range $\Rightarrow$

$$2^{16} - 1 \Rightarrow 65535$$

Network Socket $\Rightarrow$

I.P + Port

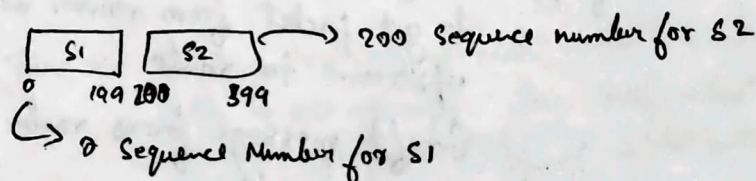
$\hookrightarrow$ These are used to locate which process the data should get or sent by.



Note: - It has no system or mechanism for Acknowledgement which makes it unreliable, to solve this reliability TCP is used at Transport layer.

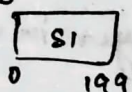
o Sequence Number & Acknowledgement Number (32 bits) :-

Sequence Number is to identify which part of data is this segment.



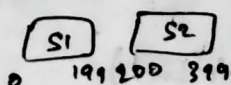
Acknowledgement Number is to identify whether the segment was received properly or not.

for Only 1 Segment



$$\begin{aligned} \text{Ack No.} &= \text{Sequence Number} + \text{Segment Size} \\ &= 0 + 200 \\ &= \boxed{200} \text{ This} \end{aligned}$$

for two Segment

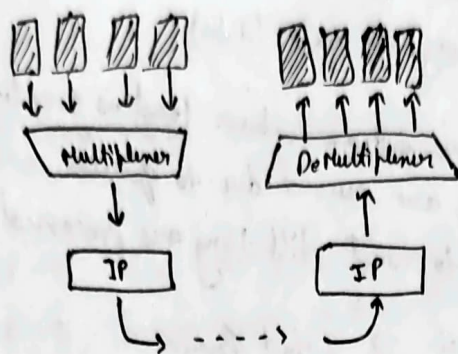


$$\text{Ack No} = \boxed{400} \text{ This will indicate All packets or segments were received.}$$

[Signature]

• Multiplexing & De-Multiplexing

15



- At Sender there can be many processes sending data (e.g. WhatsApp, Gmail, YT). Doing the transmission of data of one process at a time is absurd, to manage this Multiplexer is used.
- De-Multiplexer does the end job of collection packets & giving them to respective process in destination.

• Connection Oriented & Connectionless Service

Connection means a logical binding between two nodes, which ensures data delay is not there, order of the data and other error prone phenomena.

Connection Oriented Service →

- Connection Establishment using handshake methods etc.
- Data Transfer.
- Connection release.

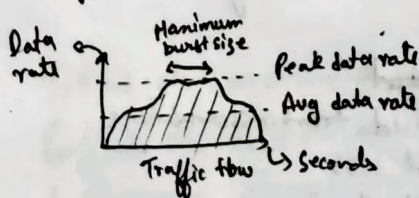
Connectionless Service →

- No Connection establishment.
- Packets sent directly.
- No data delay or order checking.

Congestion Control in Transport Layer

Congestion control means to manage data traffic, traffic congestion is avoided.

Traffic Metrics



Peak data rate → maximum

Avg data rate → Avg data rate needed

burst size → Normal length of time with max dr.

effective bandwidth → bandwidth need to allocated for flow. functional throughput

[Signature]

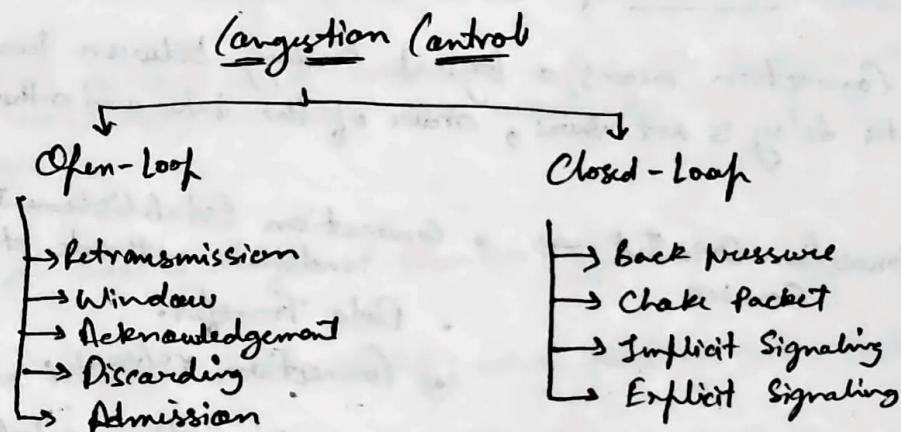
traffic profiles {

- Constant Bit rate
- Variable Bit rate
- Bursty Bit rate (data)

Congestion is the condition when load is greater than the capacity. Congestions are caused due to queues in routers which makes packets to wait till they are processed.

Three queues are there →

- Input Queue
- Processing Queue
- Output Queue



Open-loop → Tries to resolve Congestion by Preventing.

Closed-loop → Tries to resolve Congestion by Removal.

• Back Pressure ⇒ Data traffic went under congestion, then a congestion is occurred packet is sent to source via upstream sending of the message, which conveys to reduce stream.

• Choke Packet ⇒ Choke packet is a packet sent by a node to the source directly inform about the congestion.

Implicit Signaling →

- Reduced
- Increased transmission delays
- Packet loss
- Duplicate Ack
- Timeouts

022

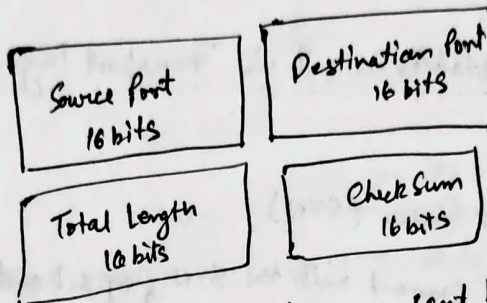
(16)

Explicit Signaling → Sending Packet
↳ choke packet
↳ back pressure

Types of Protocols in Transport Layer

UDP → User Datagram Protocol → Connectionless Service
TCP → Transmission Control Protocol } Connection-Oriented Service
SCTP → Stream Control Transmission Protocol }

* User Datagram Protocol :-



UDP is connectionless each datagram sent by UDP is independent. There is no flow control and hence it is unreliable. The receiver may overflow with incoming messages. UDP queues are directly associated with ports.

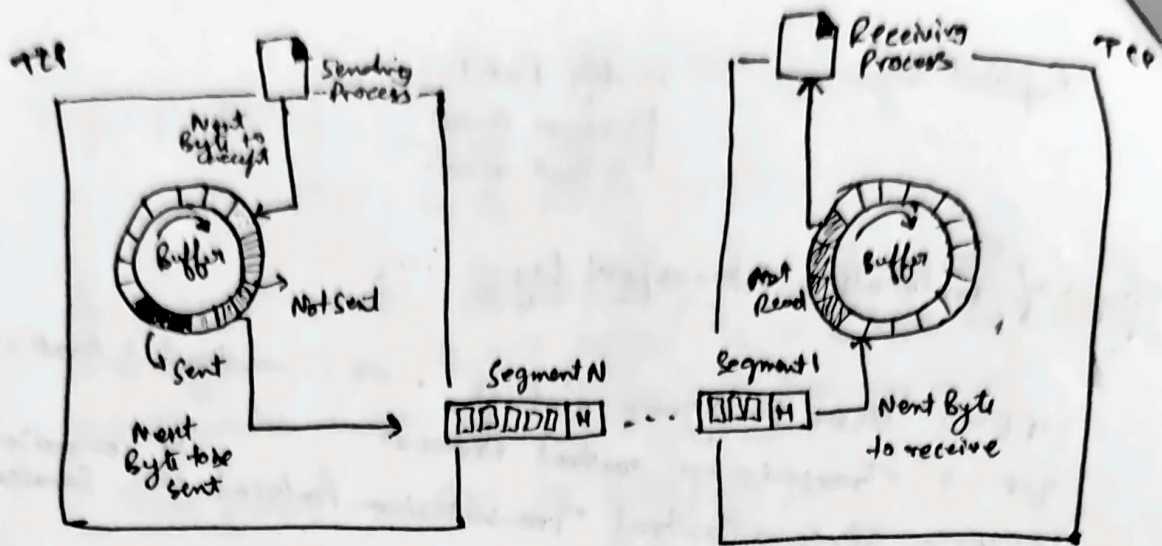
* Transmission Control Protocol :-

TCP is connection oriented protocol, it creates or establishes connection first and maintains that logical binding throughout the data transfer. Offers Flow Control, Error Control & Congestion Control.

Datagram On Page 14.

TCP is stream oriented protocol. Data flows as a stream of bytes. Buffers are used to handle disparity between production & consumption of streams. Streams are then chunked in packets called segments.

Amul



The value of Ack for the segment sent will be next byte size the receiving end should expect.

* Connection establishment in Transport layer (TCP)

1. Client to Server (SYN)

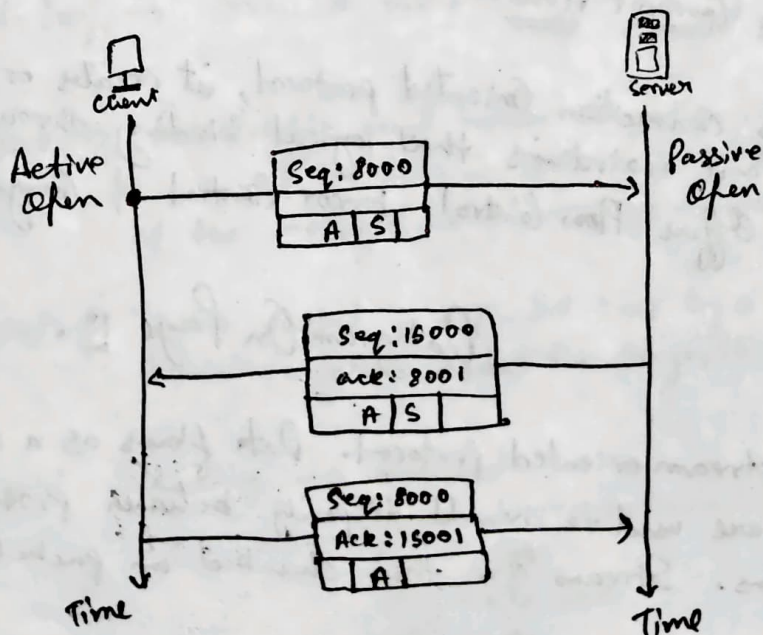
TCP segment with the SYN flag set and its ISN.

2. Server to Client (SYN-ACK)

TCP segment with SYN & ACK flags (ISN+1)

3. Client to Server (ACK)

Client sends final ACK segment by ^{ACK}ISN changed to (ISN+1)



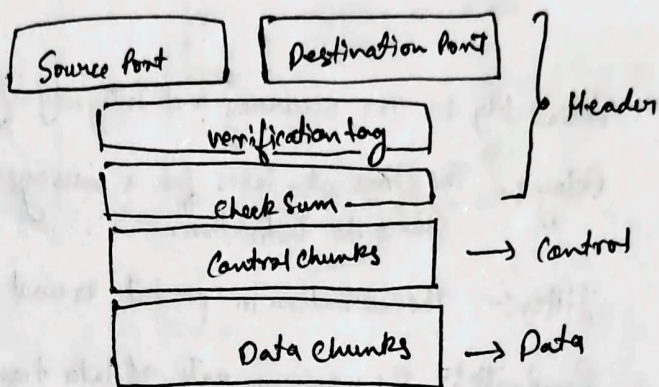
DDF

Similarly like Three way Connection Establishment, Termination is also executed. Just instead of SYN FIN is used.

SCTP - Stream Control Transmission Protocol

SCTP combines both features of UDP & TCP. Connection Oriented.

In SCTP connection is called association, data are exchanged in both directions. Multiple connections.



Verification tag in SCTP is association Identifier.

Connection Establishment $\Rightarrow$

1. INIT (Client to Server)
2. INIT-ACK (Server - Client)
3. COOKIE-ECHO (Client to Server)
4. COOKIE-ACK (Server - Client)

(1) $\Rightarrow$ Parameters like IP Address & Initial Sequence etc.

(2) $\Rightarrow$ INIT-ACK containing state cookie

(3) $\Rightarrow$ Cookie-echo with validation & user data.

(4) $\Rightarrow$ Cookie-ACK to the sent echo.

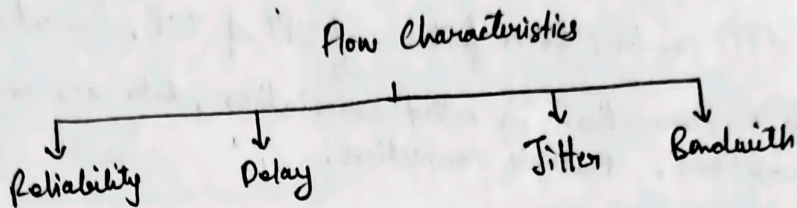
Connection Termination $\Rightarrow$

1. SHUTDOWN (Initiator to Receiver)
2. SHUTDOWN-ACK (Receiver to Initiator)
3. SHUTDOWN-COMplete (Initiator to Receiver)

[Signature]

Transport Layer - Quality of Service

Quality of Service can be imagined like the characteristics flow of data as packets tries to achieve.



Reliability :- The accuracy and Integrity of delivered data.

Delay :- The time it takes for a message to travel from source to destination.

Jitter :- The variation in packet arrival time.

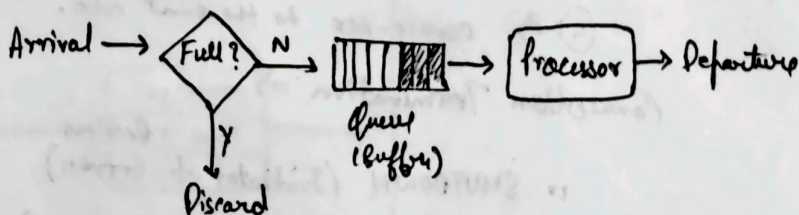
Bandwidth :- The maximum rate of data transfer across a network path.

Methods to Improve QoS $\Rightarrow$

- Scheduling
- Traffic Shapping
- Admission Control
- Resource Reservation

* Scheduling (QoS) $\Rightarrow$

(i) FIFO Queue $\Rightarrow$ Uses a Queue as a buffer, discards if arrival rate of packet is higher than processing rate.



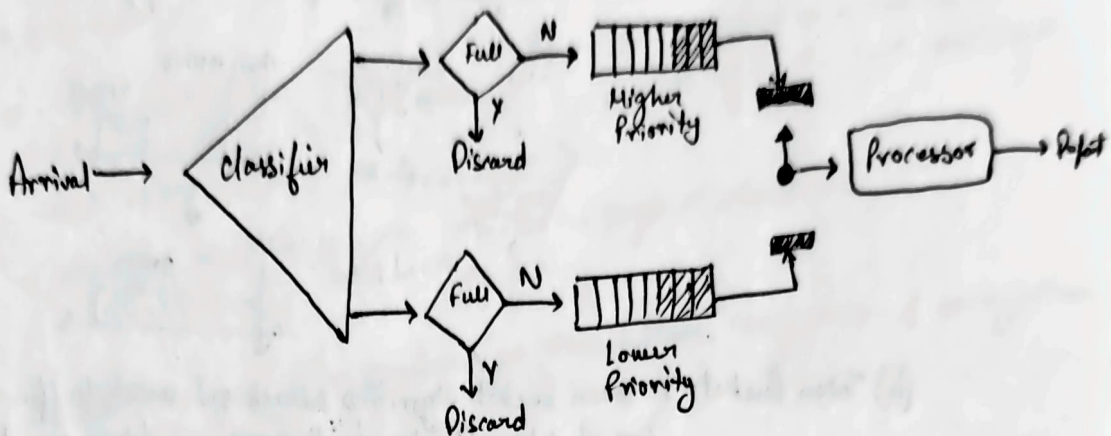
AD

(ii) Priority Queuing $\Rightarrow$ Multiple buffers are maintained respective to different Priorities.

Classifier is Used for channeling traffic into Queues.

! Starvation of Packets

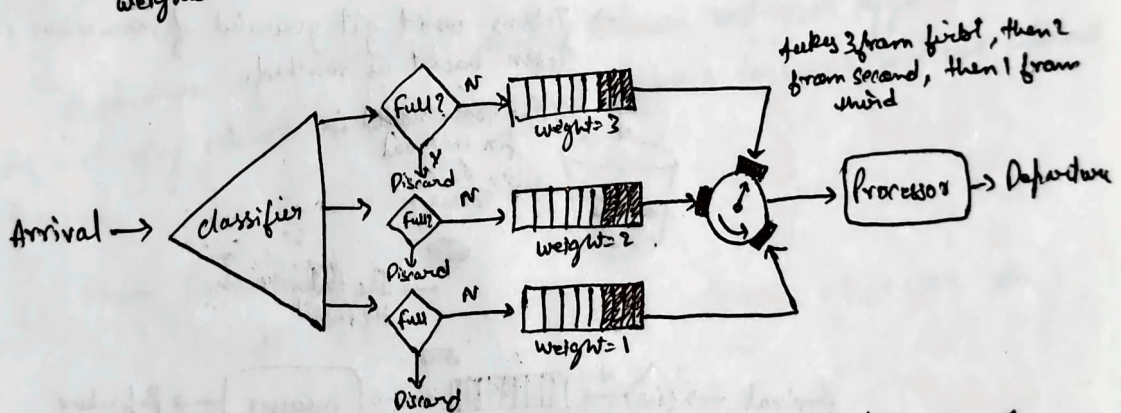
Higher Priority are processed first.



(iii) Weighted fair Queuing $\Rightarrow$ Multiple Queues of different Priority, with weights assigned to each queue.

Packets are received at Processing according to weights.

↑ Higher Priority Higher weights



Round-robin fashion is used to process multiple packets from the queue.

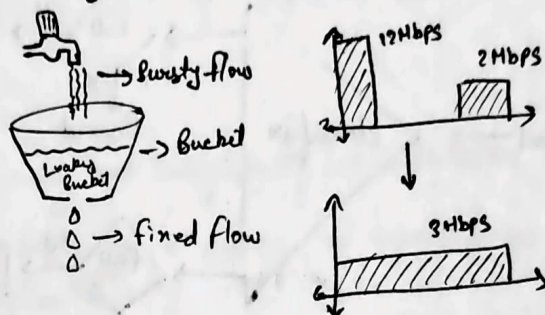
* Traffic Shaping $\Rightarrow$ Traffic Shaping is a mechanism to control the amount and the rate of the traffic sent to the network.

- Leaky bucket
 - Token bucket
- $\rightarrow$ Methods for traffic Shaping

[Signature]

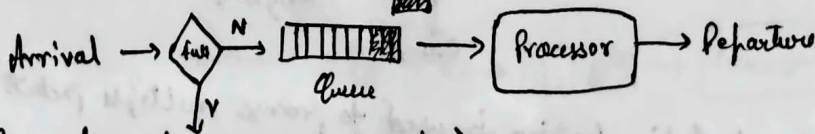
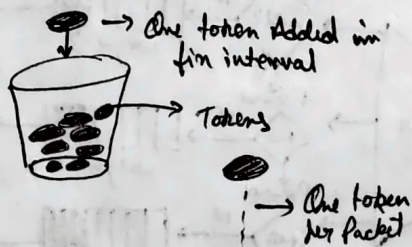
(i) Leaky Bucket $\Rightarrow$ Leaky Bucket Algorithm smooth out bursty traffic by storing bursty chunks in a bucket & sent out at an average rate. May drop packets if bucket is full.

- Working $\Rightarrow$
- $\rightarrow$ Packets arrive at any rate (burst or steady)
 - $\rightarrow$ Packets are stored in the bucket (buffer)
 - $\rightarrow$ Packets exit (are transmitted) from bucket at fixed, constant rate, regardless input rate.
 - $\rightarrow$ Bucket overflow (buffer is full), incoming packets are dropped.



(ii) Token Bucket $\Rightarrow$ Token Bucket Algorithm smooth out bursty traffic & issues of loss of data while bursty time, it uses token concept to achieve this.

- Working $\Rightarrow$
- $\rightarrow$ Token Generation at a fixed interval & added to the bucket.
 - $\rightarrow$ Sending data with consumption of one token for each packet sent.
 - $\rightarrow$ Token accumulation will facilitate the burst flow.
 - $\rightarrow$ Tokens won't get generated if maximum capacity of Token bucket is reached.



* Resource Reservation & Admission Control $\Rightarrow$

Resource Reservation is the process of pre-allocating system resources like bandwidth, buffer space or processing power in advance for particular application or data flow.

(Signature)

Admission Control is the process by which a network device decides to commit for resource reservation. This ensures of not overcommitting resource reservation.

Session & Presentation Layer

Session Layer is responsible for dialog control and synchronization of the data stream.

- This involves syn checkpoints which allows recovery and resumption of communication in case of a failure, so data after the last checkpoints need retransmission.
- Managing Multiple Sessions. (ex: Yahoo & google at same time).

Presentation layer is responsible for translation, compression & encryption of the data stream.

- Encryption process of converting Plaintext to cipher text using key.
- Data compression is to represent an information as accurately as possible using the fewest non number of bits.

Application Layer

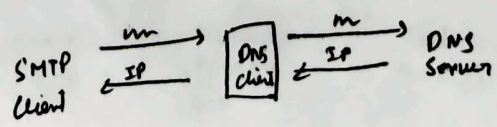
Application layer acts as the interface between end-user applications and the underlying network, enabling users and software to access and use network services.

Major Protocols →

• SMTP • FTP • HTTP • DNS • SNMP • TELNET etc...

DNS - Domain Name Service

Domain name service is component of internet that translates human-readable domain names into machine readable IP addresses. This allows users to access websites and online services.



(Signature)

IP Address is used to access a program file or data. To assign names to these machines namespaces are used. Domain Name Space is a hierarchical name space.

- Domain name space is defined in an inverted tree structure with the root at the top. Tree can have 128 levels level 0 (root) to level 127.

- Each node in the tree has a label, which is a string with max 63 characters.

- Parent & Child node string can't be same for uniqueness.

FQDN
↓
Fully Qualified Domain Name ⇒ end with null string

PQDN
↓
Partially Qualified Domain name ⇒ end with not a null string

DNS Messages ⇒

Query → Header & Question Records

Response → Header, Question Records, Answer Records, Authoritative Record & Additional Record.

DDNS ⇒ Dynamic DNS service that automatically updates DNS records to reflect changes of IP-Addresses, ensuring that a domain name always points to the correct, current-IP even it changes frequently

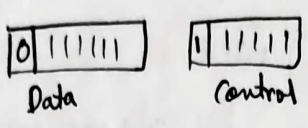
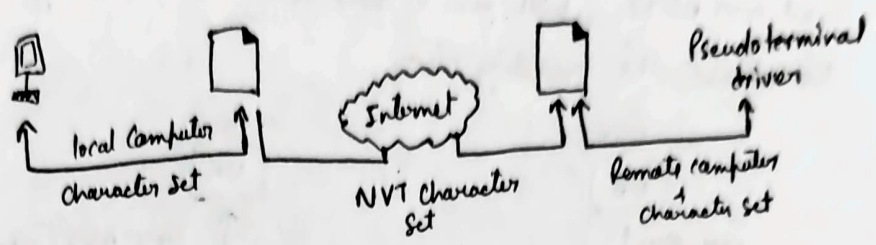
* DNS Uses UDP most of the time, but for some TCP port 53 is used.

TELNET - Terminal Network

TELNET is a network protocol and application used to remotely access and control computers over a network. In simpler terms Application Programs on remote computers.

Only

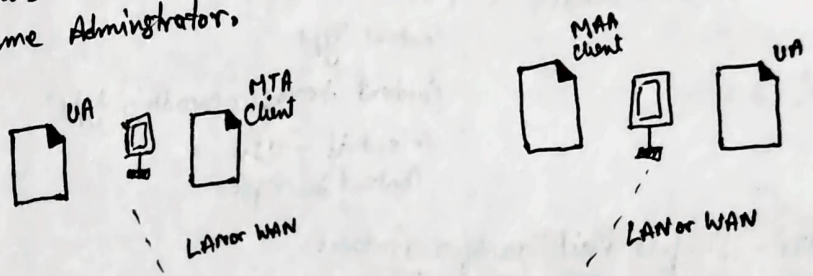
User sends keystroke to the terminal driver, where the local OS accepts it & characters are sent to TELNET which transforms it in NVT characters and delivers them to local TCP/IP protocol stack.



Uses TCP with Port 23 & Client at ephemeral port

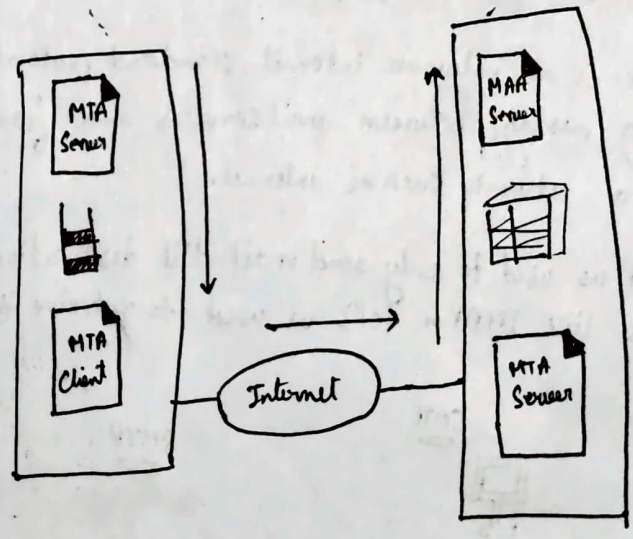
Electronic Mail

Electronic Mail is most used service of Internet, where the sender & receiver sends & receives mail to their mail box service created by their Administrator, sometimes same Administrator.



- UA - User Agent.
- MTA - Message Transfer Agent.
- MAA - Message Access Agent.

UA → push retrieves message from MTA client to server
 ↑
 Vice Versa for Pull



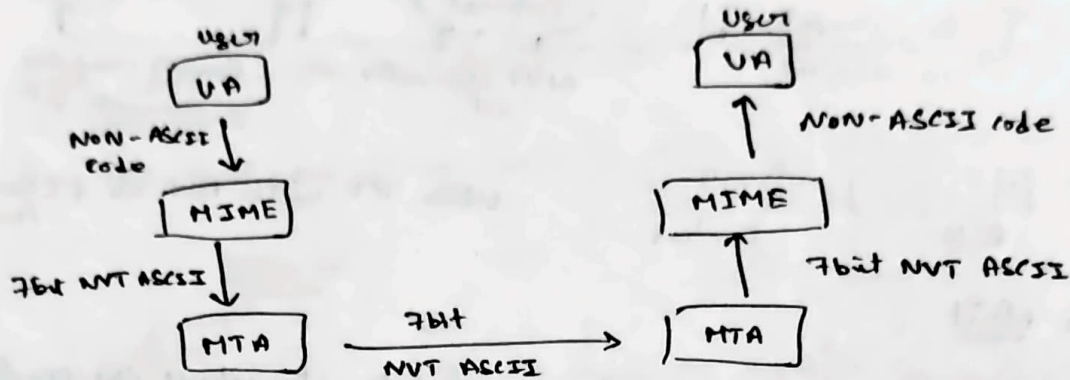
User Agent ⇒
 Composing message
 Reading message
 Reply to message
 Forwarding message
 Handling mail box

Email Address
 ⇒ local @ Domain name
 ↓ ↓
 Address of mail box Address of the mail server

(Signature)

Multipurpose Internet Mail Extensions (MIME)

MIME is a supplementary protocol to encode NON-ASCII data into 7-bit NVT ASCII which can be sent using MTA (Message Transfer Agent). To reverse the encoding also.



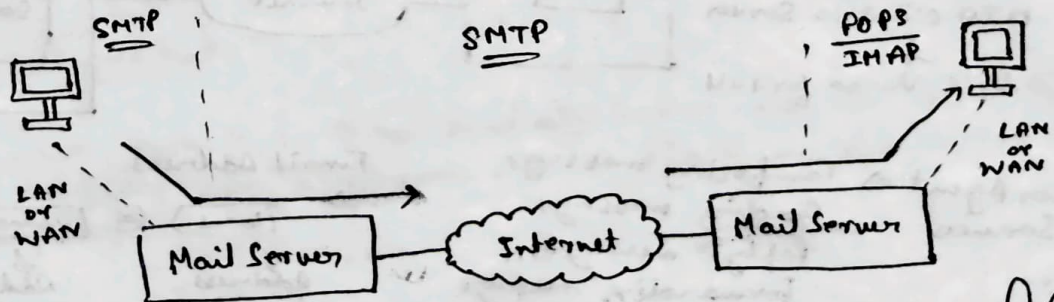
MIME Header $\Rightarrow$

- MIME Version
- Content Type
- Content transfer encoding type
- Content id - UID
- Content descriptor

SMTP - Simple Mail Transfer Protocol

SMTP is an network internet standard protocol used for sending or relaying message between mail servers and from email clients to servers over a network such as Internet.

SMTP is used to only send mail till destination mail server, after that protocols like IMAP or POP3 is used to retrieve the message.



uses command & response for sending message.

[Signature]

POPS & IMAP4

POP - Post Office Protocol IMAP - Internet Mail Access Protocol

POP ⇒ Two modes Delete & Keep (After retrieval).

Server POP software should be downloaded server, similarly client.

↓ Can't Organize mail on the server, & different folders.

↓ Can't check Partial content.

IMAP ⇒ Advanced than POP.

Check header prior to downloading.

Searching capability.

Partial email retrieval.

Customizations on mailboxes. (CRUD)

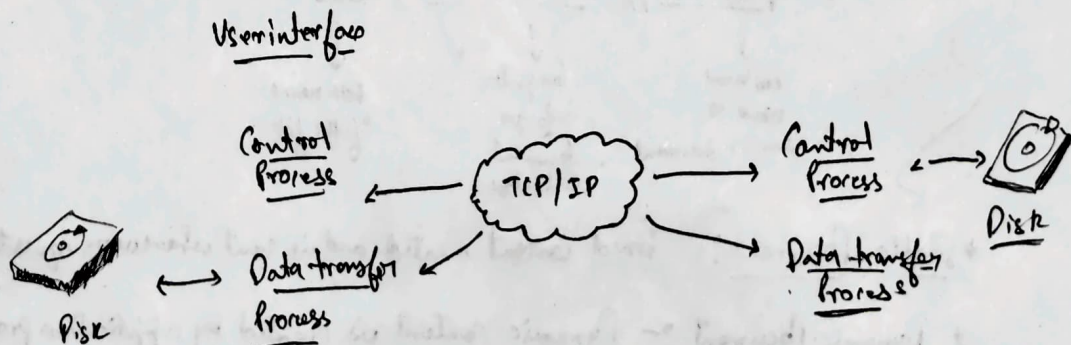
Folders for mailboxes.

FTP - File Transfer Protocol

FTP is used to send file from client disk space to server disk space, uses two TCP communication channels to achieve this. (21 for connection) (20 for data).

Control Channel ⇒ Sending commands such as login, directory navigation & for receiving server response. Client defines type of file.
(21)

Data Channel ⇒ Data used for actual file data sending when uploading & downloading
(20)



* Not secure due to lack of encryption

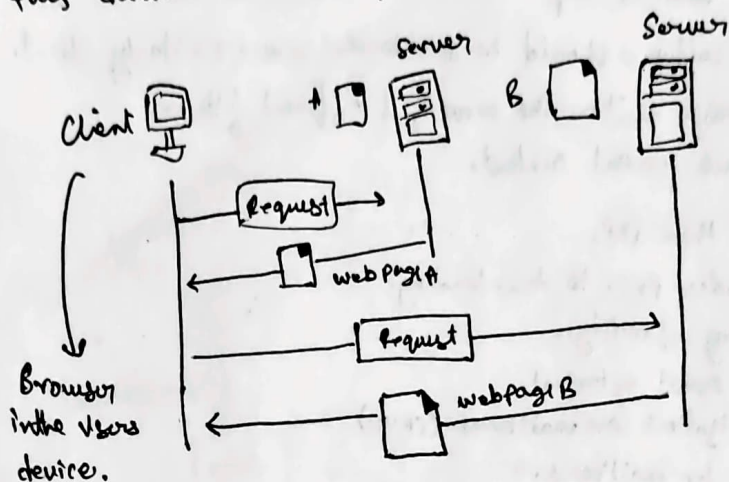
SFTP ⇒ FTP with layer of Security, encryption, Authentication, connection oriented, Port 22.

TFTP ⇒ FTP for LANs, UDP used, No security during transfer.

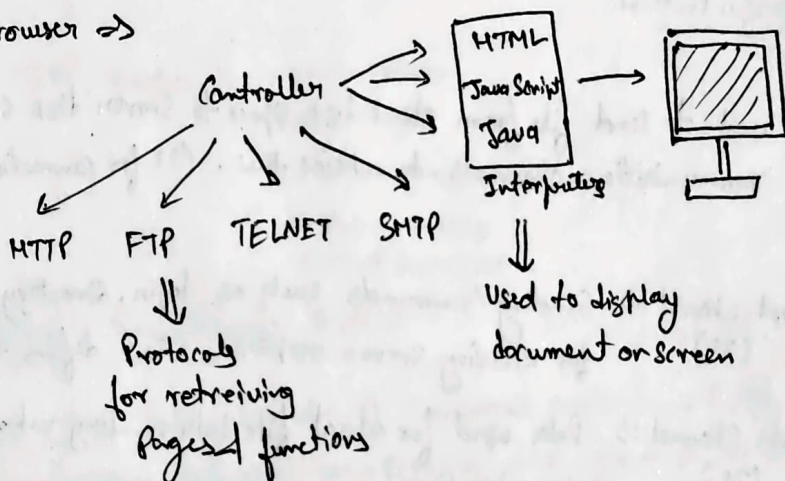
(Signature)

WWW - World wide Web

World wide web is a repository of information linked together, information is present on web documents and are stored in server, this documents are retrieved to user using clients like browser.



Browser $\Rightarrow$



URL $\Rightarrow$

Protocol : // Host : Port / Path

↓
Protocol used to access document

↓
Computer info on document is located

↓
Path name of the file

* Static Document :- fixed content created and is sent whenever requested.

* Dynamic Document :- Dynamic content is created by application program on server & is sent whenever requested.

CGI - Common Gateway Interface used for Dynamic content.

* Active Documents :- Some documents or program needs to be run on client side $\rightarrow$ JS & Applet.

(Signature)