Unit-4

Transport layer - (End to end layer)

- ↳ Ensure jo packets hai arrive hoe order mei.
- ↳ provide acknowledgement of successful data transmission & " of retransmits data agr Error Paya jata h.
- ↳ Ensure Karta hai jo data hoga vo Error free hoga with no losses or Dublications.
- ↳ Service provide → to application & take from network
- ↳ Divides message Recieved from upper laye into packets → source or Destination Resemble Karti hai again into message

Services

Connection oriented transmission	connection less transmission
→ Reliable transport method	→ doesn't acknowledge reciept of a packet
→ slower	→ faster
→ agr Data mein problem hoti hai, to Destination ~~Require~~ Requests Source for Retransmission by acknowledge packets jo usko Recognizable hai	→ Less Reliable

functions of transport layer -

1. segmentation of Messages into packet and Resambly of Packets into Message.
2. Message acknowledgement - Reliable End to End Message delivery
3. Session multiplexing -  EK mei convert kar deti hai Data packets ko
4. protocols - TCP, ATP, NWLINK
5. flow control - Ensure the Rate ~~they~~ of communication they both can handle.

Transport Layer Design issue -

1. **Reliability** - Data transmit between host is delivered Reliable. TCP Provides but UDP doesnt provide

2. **Flow control** - Process of Regulating the flow b/w two network nodes. It Results in better network utilization by avoiding Packet loss

3. **Congestion** - Preventing network from becoming traffic congested
TCP uses Effective congestion control to prevent Packet loss.

4. **Multiplexing & Demultiplexing** -

(DLD wala)

5. **Connection Establishment & termination** -
Befor data transfer, EK connection Establish hota hai jo after completion terminate ho jata hai.
TCP uses - 3 way handshake to Establish
4 way handshake to terminate

6. **Quality of service** - Ensures to provide an acceptable level of QOS for traffic.
Minimum Bandwith, max delay

Quality of Service (QoS)

↳ critical application require Reliability & timely data Delivery.

↳ Something a flow seeks to attain.

Flow characterstics

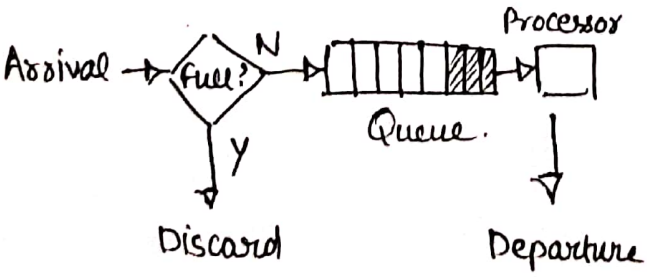
- **Reliability**: Means loosing a packet or acknowledgement Entails Retransmission.
- **Delay**: Applications can tolerate delays in different degress.
- **Jitter**: Variation in Delay for packets belonging to Same flow
  High → delay large
  low – small
- **Bandwith**: Different application Different Bandwidth.

Techniques to Improve QoS –

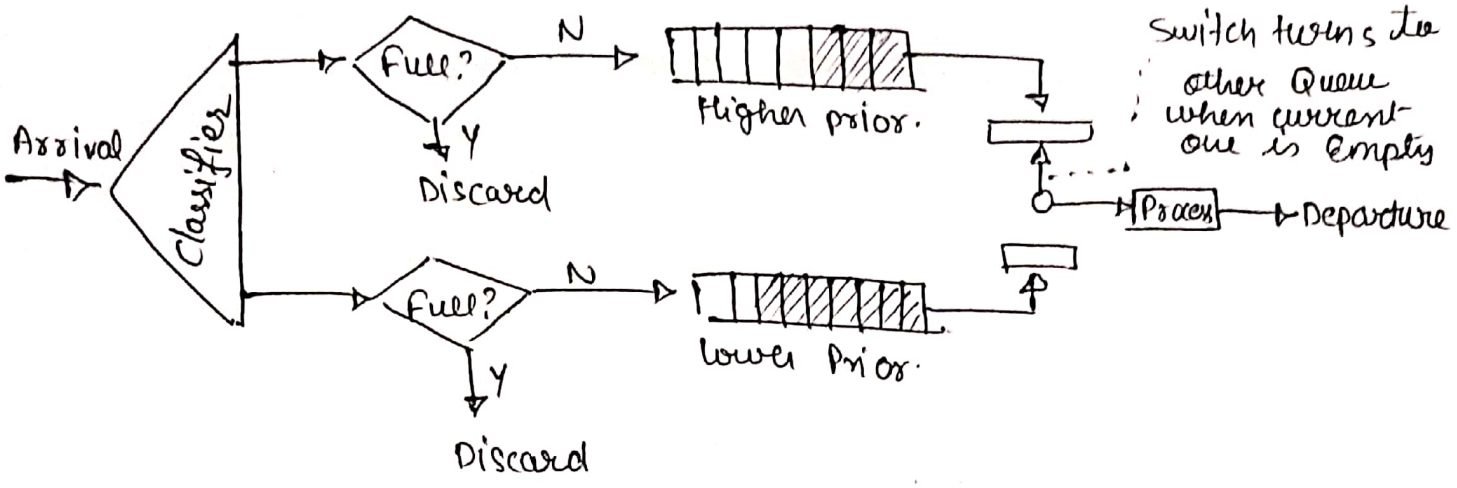
1. Scheduling
2. Traffic Shaping
3. Resourse Reservation
4. Admission control

1. <u>Scheduling</u> – Packets from different flows arrive at a switch or router for processing

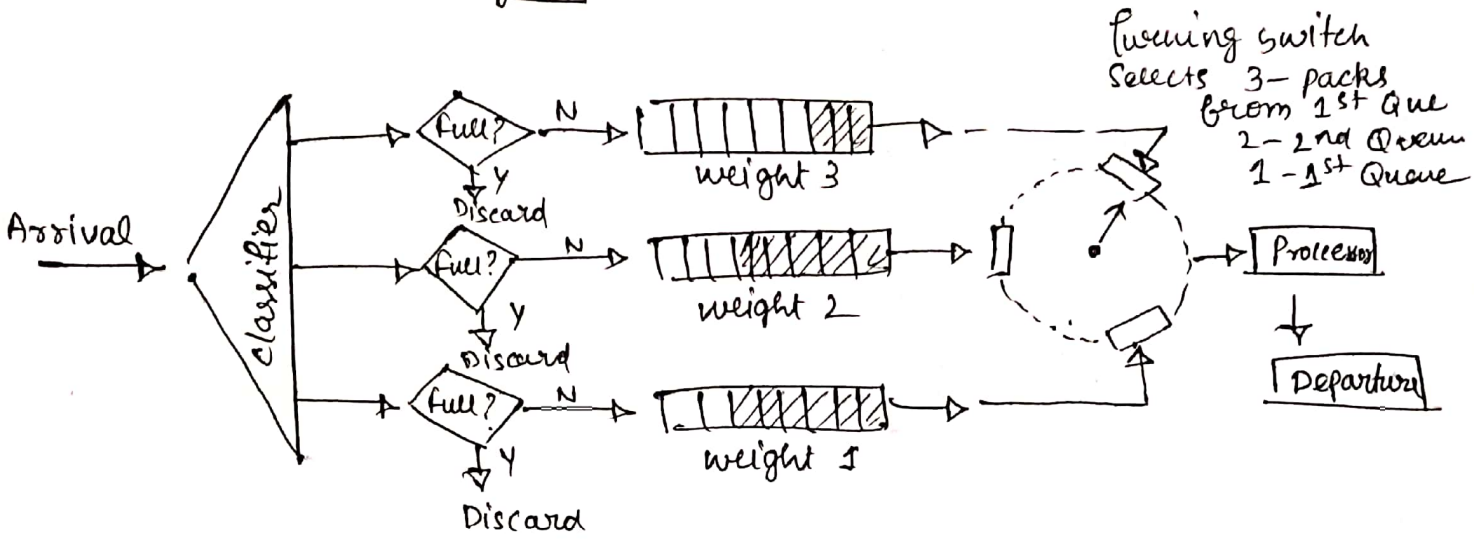
- FIFO Queuing
- Priority
- weighter fair



Priority Queue



weighted fair Queuing



2. **Traffic shaping** - Trafic is shaped before it enters network. Controls rate at which packets are sent.

algorithms

Leaky Bucket

- constant output Data rate
- If buffer overflows then Packets Discarded
- Results in uniform flow of Packets.
- when Packets → same size one Packet Per tick is okay.
- For variable, allow fixed no. of bytes/tick

Token Bucket

- allows output rate to vary
- Bucket holds token
- For one packet host must capture & destroy one token
- token generated at rate of one token Every Δt sec

Resource Reservation

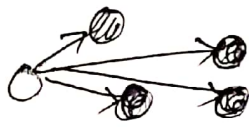
↳ Flow data needs resources such as buffer, bandwith cpu r - -

Admission control -

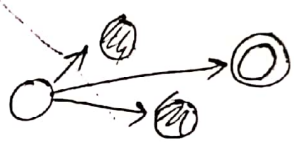
↳ a mechenism used by Router, switch, accept, reject a flow based on predefined parameters.

Transport layer Protocol

1. UDP - User Datagram protocol.
   - non sequential transmission
   - connnectionless (speed & size is imp)
   - adds checksum, Error control
   - Faster delivery of messages



Broadcast (one to all)



Multicast (one to several

Header	Data

identify port no.	Source Port (16 bits)	Destination (16 bits) → Packet destination Port
whole length	length (16 bits)	check sum (16 bits) → Error Detection

2. TCP - Transmission control protocol.
   connection oriented
   virtual circuits connected the Sender & Reciever

Header (20-60 bytes)	Data

Source Port (16)	Destination (16 bits)
Sequence no.	
Acknowledgment no.	
HLEN 4 / Reserved 6	window size
checksum	urgent Pointer
options & Padding	

SCTP
↳ Stream control transmission protocol.
↳ connection oriented.
↳ full duplex mode
↳ Reliable & Easier

IPV4 address

- 32 bit address uniquely & universally Defines connection of device (a computer/router) to internet
- unique one address defines only one connection to internet.
- Two devices can never have same address at same time.
- Ek address thode time ke lie Ek device ko deke or thode time Baad use vapis leke kisi or ko de skte hai
- agr device operate kar rha hai network layer pe m connections ke sath, to uske pass m addresses hone chaiee
- address space - total no. of addresses used by Protocol.
- agr protocol N bits use kar rha hai to define address. then address space = 2^N because each bit can two different values (0, 1) & N bits can have 2^N values

IPv4 notations

1. Binary

32 bit/4 byte
Octet → byte

EX: 01110101 10010101
00011101 00000010

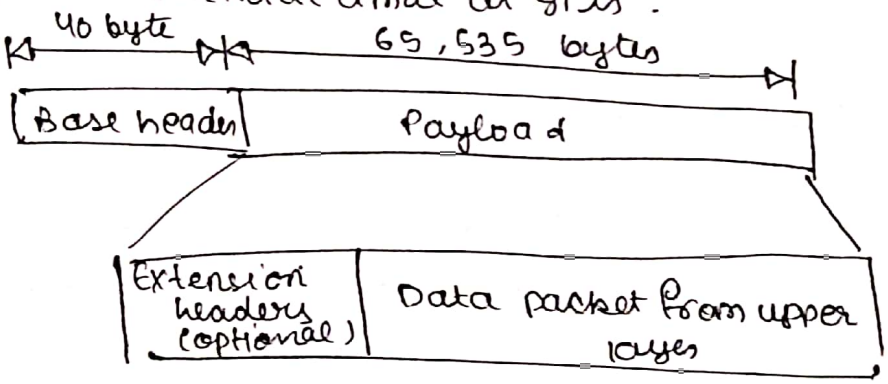
2. Dotted Decimal.

Ex: 117.149.29.2

- IPv4 host to host communication karata tha
- well Designed
- defecencies → unsuitable ine fast growing
  - → Subnetting, class addressing & NAT address deplition long term problem in internet
  - → Internet must accomodate Real time audio & video transmission which Requires minimum delays, Strategies & Reservation of resources (jo ki IPv4 mei nhi that)
  - → No Encryption & authentication.

in Kamiyon ko poora karne ke lie IPv6 proposed kia gya.

- Extensively modified to accomodate unforseen growth of internet.
- address consists of 16 bytes (128 bits long)
- To make address readable, specifices hexadecimal colon
- 128 bits divid into 8 Sections, 2 byte Each.
- 2 bytes = 4 hexadecimal digits.



IPv4	IPv6
# Provides 32 bit address	128 bits.
# Security by X	authentication, integrity & confidentiality ✓
# No protocol Enhancement	Features Hierarchial addressing
# divided into 5 classes	Doesn't have any
# Can be converted into IV6.	can't be to IPv4
# header can be from (20-60) byte	40 bytes
# Checksum field	not.
# Respersentation in Decimal	Hexadecimal.

SESSION LAYER

Data	Session Interhost communication

- provides Reliable & Secure communication b/w two devices by Establishing managing & terminating Sessions
- Regulates Data flow, Defines format of data sent to connections.
- manage - Kon Data send kar skta hai, in a certain amount of time & for how long.
- Reconnect Session if disconnects.
- Protocols - NetBIOS, Mail slots, Names pipes & RPC

functions -

1. Session Establishment - Establish connection b/w two devices before transmission Begins.
2. Session management - Keep track off session throughout its duration. In case of Error session term
3. Session termination - After completion.
4. Session Security - Encryption, authentication & authrization
5. Session Recovery - if connection lost or interrupt. Keep tracks.
6. Dialog management - jab device connect. hota hai to session layer Responsible hoti hai for Determining Konsa Device Communication mei part le rha hai as well as control the amout of Data that can be transmitted

Types of diaglog control
- simplex
- half duplex
- full duplex.

7. Synchronization - Handles synchronization between incoming & out going data stream by adding synchronization points → checkpoints Jiski help se session layer Retransmitting mei help kar pati hai easily & fastly

Quality of Service (QoS)

↳ Ability of network to prioritize & Deliver Data based on importance & Ensure certain level of performance.

Achieved through -

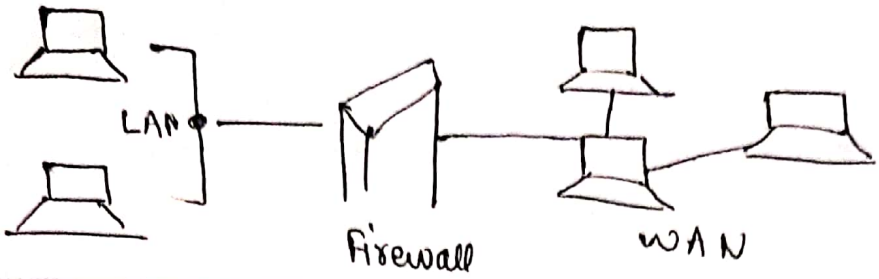
1. Traffic prioritization - Ensures high priority data send first. achieved by setting Different priorities for Each session Based on importance of Data.
2. Bandwith management - monitors amount of data being transmitted & allocating Bandwith on priority.
3. Congestion control. manage Rate & amount of data being transmitted which prevents Network overload, reduce packet loss.
4. Error handling & Recovery - Detects & correct Errors If error paya jata hai to SL action leti hai.

Firewalls

→ Security devices monitor & control network traffic based on predetermined security policies.

→ Helps to prevent unauthorized access & malicious attacks and Ensure only authorized sessions allowed.

Accept	→ allow the traffic
Reject	→ Block "unreachable Error"
Drop	→ Block traffic with no Reply



Seprate private from open Internet

Firewall

Packet

→ operate inline at junction points where devices → Routers, switches do their work.

→ Donot Route the packet rather Compare Every Recieved packet with Established criteria
Ex → Port no, ip address etc.

→ Flagged packets are 'dropped

Circuit

→ operate to monitor & control individual session

→ Establish circuit between ~~to mo~~ communicating Devices, to monitor control of flow

→ Session ID, source or Destination ke basis pe filter Karta hai.

Advantages of firewall

1) Security
2) Prevention
3) control of network access
4) Regulation compliance.
5) Monitoring of network activity

Disadvantages

1) complexity
2) Limited visibility
3) cost.
4) limited VPN support

APPLICATION LAYER

↳ topmost layer of OSI model & Enable communication b/w application on Different hosts

↳ Designed to communicate with specific application

↳ Establish, manage, terminate communication sessions & Enable data Exchange for specific application.

Protocols -

1. HTTP (Hyper text transfer protocol) -
   Designed for word wide web.
   used to transfer hypertext document & other data b/w web & clients.

2. FTP (File transfer protocol) -
   used to transfer files over network.
   Enable sharing & copying of files b/w Computers located on different networks.

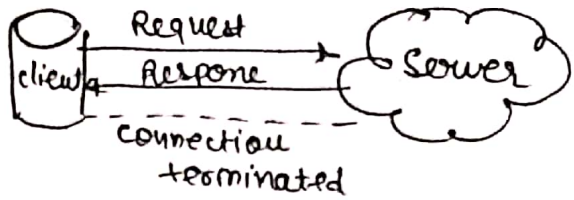
3. SMTP (simple mail transfer protocol)
   used to send Email message from one server to another.

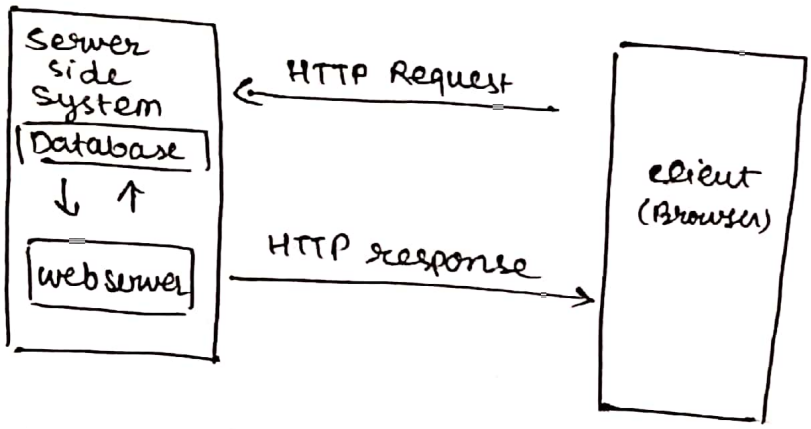
4. SNMP (simple network management protocol)
   used for network management & monitoring
   Enables network devices to be monitored, managed & controlled remotely.

5. DNS (Domain Name System)
   maps domain names to IP address & help translate human Readable domain names to computer Readable IP address.

HTTP

(1) The URL sent to DNS
↓
Check records for URL in Database
↓
Return IP address
↓
Browser send Req to server
↓
Server send data
↓
connection closed

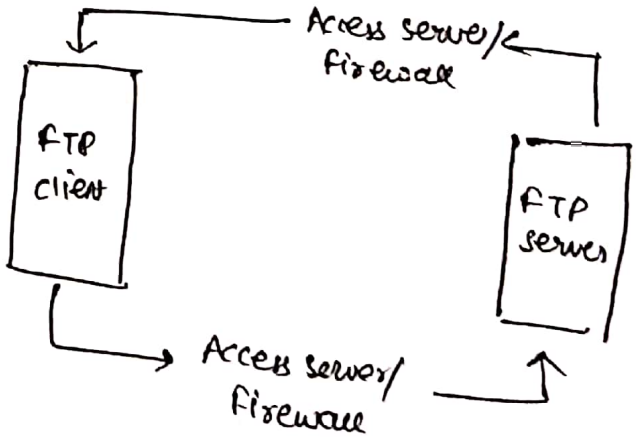




FTP (file transfer protocol)

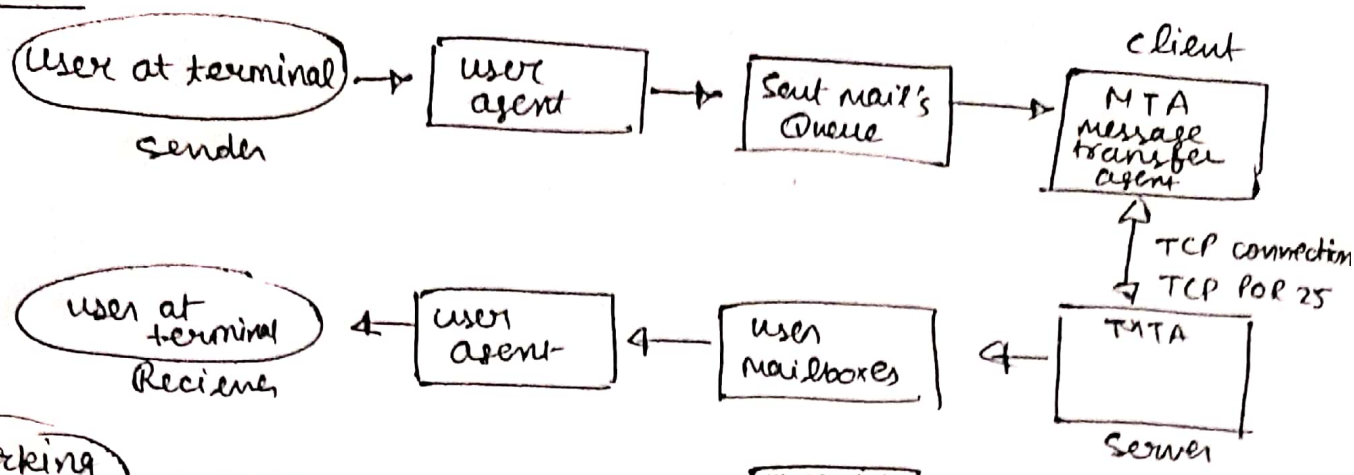
- Encourages direct use of remote computers.
- promotes sharing of files of other types of Data

Cliend contacts FTP server
↓
Obtain authorization
↓
Browse Remote directory
↓
Server Recieves a command
↓
after transfering server close connection

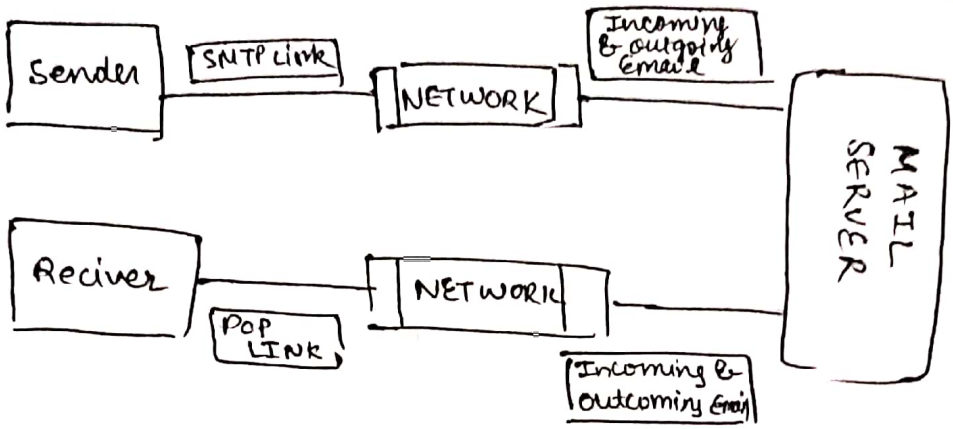


SMTP

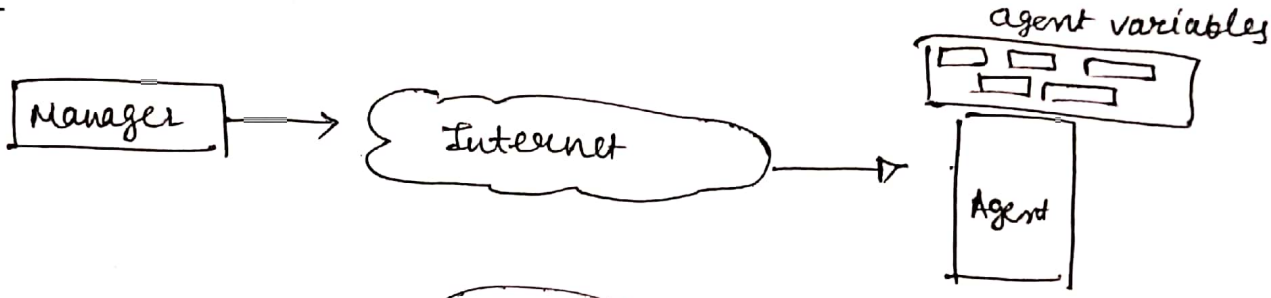
Model



Working



SNMP



Functions

- Configuration management
  - ↳ Reconfiguration
  - ↳ Documentation
- Fault management
  - ↳ Reactive
  - ↳ proactive
- Performance management
  - ↳ capacity
  - ↳ traffic
  - ↳ throughput
  - ↳ Response time
- Security Management
- Accounting