Computer Networks & Internet protocol

Data communication - Data → Information
↳ Exchange of Information between two devices via some form of transmission medium.

Computer network -
A network → set of devicies connected by communication links.

interfaces across a distance → "peer to peer" interfaces.
local interfaces - 'services' interfaces.
Modules on each end are organized as sequence of function → layers
Set of modules organized as layers → "Protocol stack".

Computer Networks (Based on transmission Mode)

Simplex
- Communication is unidirectional.
- Only one can transmit the other can only Recieve

Half Duplex
- Communication is Bidirectional,
- Both station can Sent & recieve but not at same time

Full Duplex
- Both stations can transmit & recieve Simultaneously

Computer networks (Based on transmission time)

Synchronous
- Data is transmitted in continous Stream at constant Rate
- high speed communication
- Clock signal is used
- Sender & Reciver must be syncronized.

Asynchronous
- Data is sent in individual Characters or blocks, with Start & stop bits.
- No need to Syncronize the sender & Reciver

Based on authentication

Peer to peer connection
- ↳ no dedicated servers
- ↳ All computers are Equal so, termed as peer.
- ↳ function as both a client & server

Server Based connection.
- ↳ Dedicated server
- ↳ one computer serve as a server & can't be used as client.
- ↳ server control the clients

Based on Geographical location

LAN (Local Area Network)
- ↳ small high speed N/w.
- ↳ few no. of system interconnected
- ↳ distance ↑ speed ↓
- ↳ limited to few only
- ↳ used to link the devices in single office, building campus.
- ↳ owned by private people

WAN (wide AREA Network)
- ↳ Network speed is smaller
- ↳ connects system indirectly
- ↳ spread over the world. over more than one city, country & continent.
- ↳ WAN is slower than LAN
- ↳ owned by single owner So, Enterprise network
- ↳ combination of one more than one topology

MAN (Metropolitan area network)
- ↳ Extension of local area Network
- ↳ spread over city
- ↳ single network or a network of more than one local network & share the Resources

Based on Reliability

Connection-oriented
- → Reliable network service
- → Establish a session connection before Data can be sent.
- → Gurantee that Data will arrive in same order.

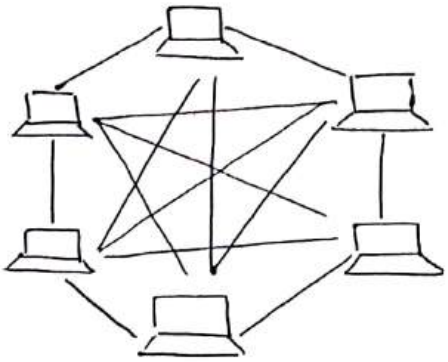
Connection less
- ↳ doesn't Require a session connecti
- ↳ provide minimal services.

Topology :-

→ Way in which a network is laid out physically
(दो या दो से ज्यादा devices connect hote hai link se to use topology bolte hai)

→ Geometric Repersentation of Relationship of all the links & liking devices to one anathor

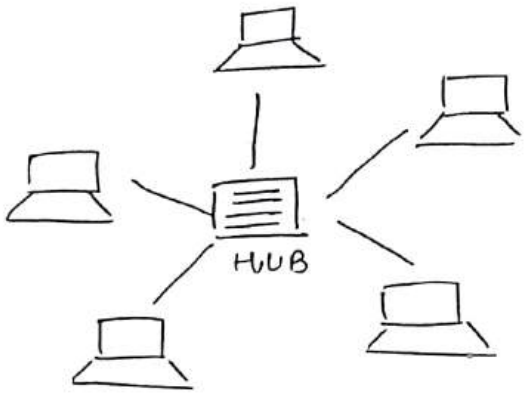
4 topologies



Mesh

Each node is connected directly to Every other node in Network

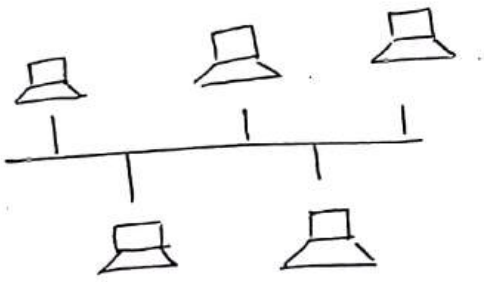
Point to point connection.



Star topology

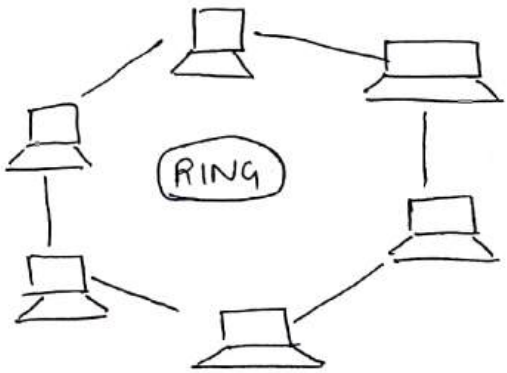
All nodes are connected to central point/device (hub)

indirectly connected to every other node through the central device



Bus

- all nodes are connected to a single communication line.
- har node ke pass data jata hai bus process vo karta hai, jiske lie intended hota hai

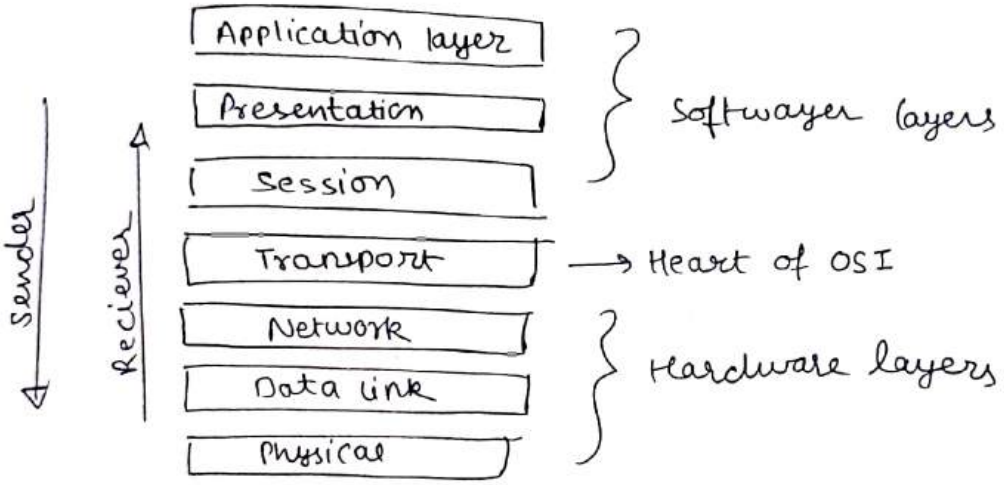


Each node connected to Exactly two other nodes,
forms a close loop or Rig structure.
Data travels in one direction
Pass through Each node until Reach its destination.

Network Models

International organization Standardization

- **OSI model** - 'Open system Interconnection)
  - ↳ ISO ne devlop kia
  - ↳ facilitate communication between two Different System bina change Kare logic ko hardware or Software ke.
- ↳ OSI model protocol nhi hai, model hai understanding & designing a network Architecture jo flexible, Robust & interportable ho
- ↳ 7 seprate but Related layer hoti hai, Har Risi Ka apna Kaam hota hai, poore process ke part ko define Karti hai.

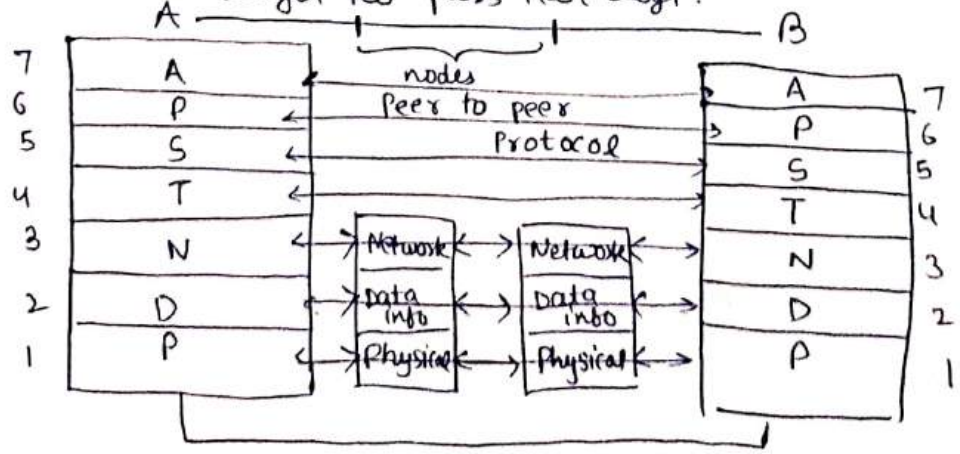


Aaj Phir Se test nhi dena pada

→ isme 2 device hong A & B.

→ communication hoga move down through layers on Device A & Back up through B.

→ Har layer Sending device mein add Kargi information ko message mein, jo bhi upr wali layer se Recieve karegi or apne se neeche wali layer ko pass Kar degi.



Physical layer

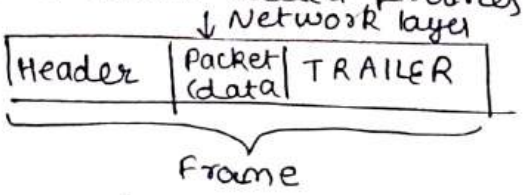
→ defines the characteristics of the interface between devices & transmission medium.

→ transmission rate (no. of bits sent each second) is also defined by Physical layer.

→ Physical topology is handled.

Data link layer -

→ Divides the stream of bits recieved from network into managable data units called Frames



→ agar Frames distribute karenge different system mein network ke. DLL adds a header & dfine sender & reciever

→ agr Rate of Reciving Data less hoga production of data se, to yeh layer impose karti hai flow control mechanism.

Network layer -

↳ Responsible for source to delivery to destination of a packet.

↳ logical addressing

↳ agr 2 system connected hai same layer se to network layer ki zarrot nhi hoti.

Transport layer -

↳ connection control

↳ Error control

↳ divide karta hai data ko small parts mein/segments mein for transmission or ressemble karta hai destination.

↳ flow control.

Session layer -

↳ Establish, maintain & synchronize karta hai interaction among communicating Systems.

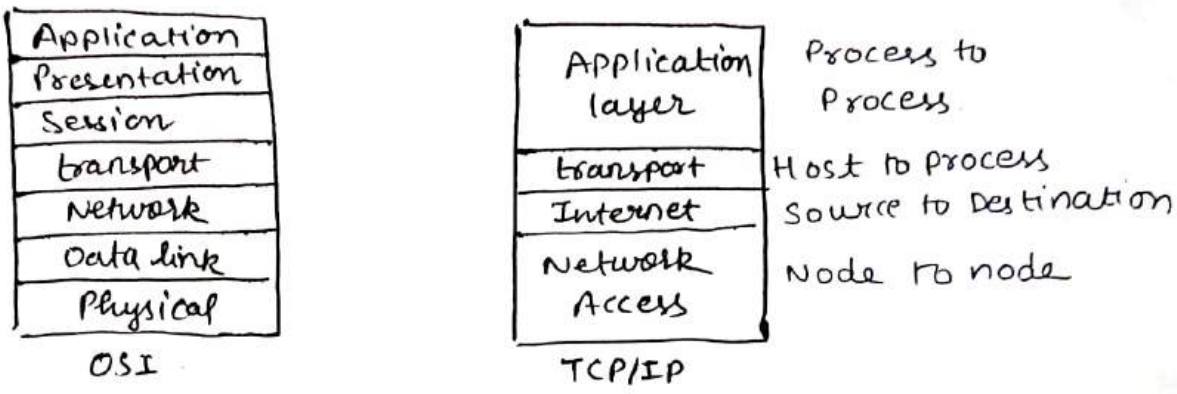
↳ Dialog control - communication b/w two process in half & full duplex.

↳ Synchronization - add check points to stream of Data

Presentation layer

↳ translation : converts Data formats
↳ Encryption : ~~Sou~~ Secures Data
↳ compression : compress data size

TCP/IP Protocol suit or Model -



There are 4 layers in TCP/IP model.

Network access -

↳ combination of physical layer + Data link layer (of OSI)
↳ Define how data should be sent Physically through the network.
↳ mainly Responsible for transmission of Data b/w two devices.
↳ It Encapsulate the IP datagram into frames transmitted by network & mapping of IP addresses into physical addressess.

Internet

↳ second layer
↳ main Responsibility is to send the packets of any network & they arrive at Destination irrespective of Route.

Protocols used by Internet layer -

IP Protocol

↳ IP addressing used by the Internet & higher layers to identify device.
↳ Host to Host communication : Determine the path through which Data is to be transmitted.
↳ Data Enscapsulation & Formatting Ensure the data is sent & recieved securly, Encapsulate the Data into message.
↳ Routing : jab source & destination dur hote hai to, IP datagram indirectly bheja jata hai.

Transport layer -

↳ Responsible for reliability, flow control & correction of Data jo send hona hai network ko

Protocols

(1) UDP (User Datagram protocol):
- → connectionless service & End to end delivery of transmission
- ↳ Discover Error, & ICMP protocol reps the Error to Sender

(2) Transmission control protocol (TCP):
- ↳ Full transport layer service to application
- ↳ virtual circuit between sender & Reciver active during transmission

Application layer -

↳ top most layer
↳ Responsible for handling high-level protocols, issues of Representation
↳ allow the user to interact with application.
↳ jab EK application layer dusri application layer se communicate karna chahti hai to vo data ko transport layer pe forward kar deta hai.

Main protocols of application layer -

HTTP - allow to access data over world wide web. transfer data in form of plain text, audio vedio.

SNMP - Simple Network management protcol
Provide framework used for Managing the device

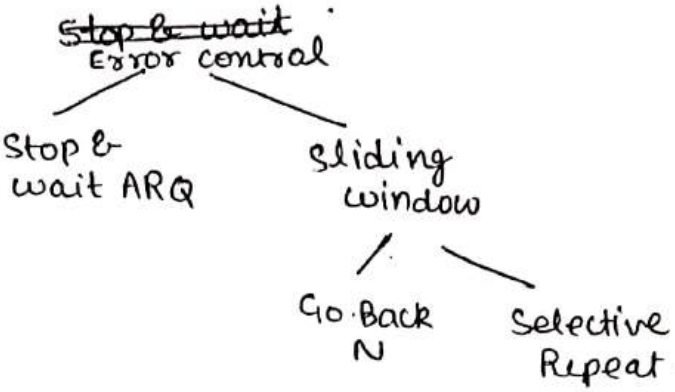
FTP - File transfer protocol (used for transmitting the files from one computer to anathor)

Unit - II

Data link protocols

→ Stop & wait protocols

Error control mechanism - used to Recieved data should be Exactly same whatever Sender has sent the Data.



Stop & wait

↳ jo bhi sender data send kar rha hai, reciver ko. After sending Sender waits karta hai tab tk jab tk usko acknowledgement Reciever nhi ho jata reciever se.

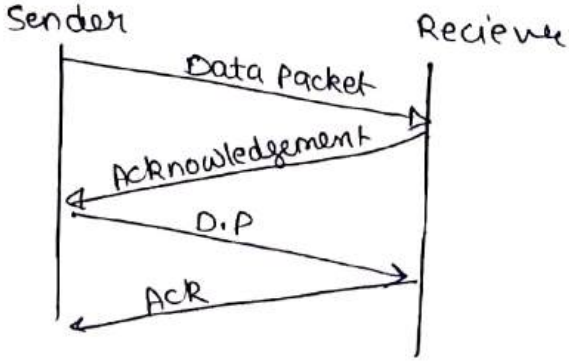
↳ flow control protocol hai, service of data link layer

↳ used for transmitting the data over noiseless channels.

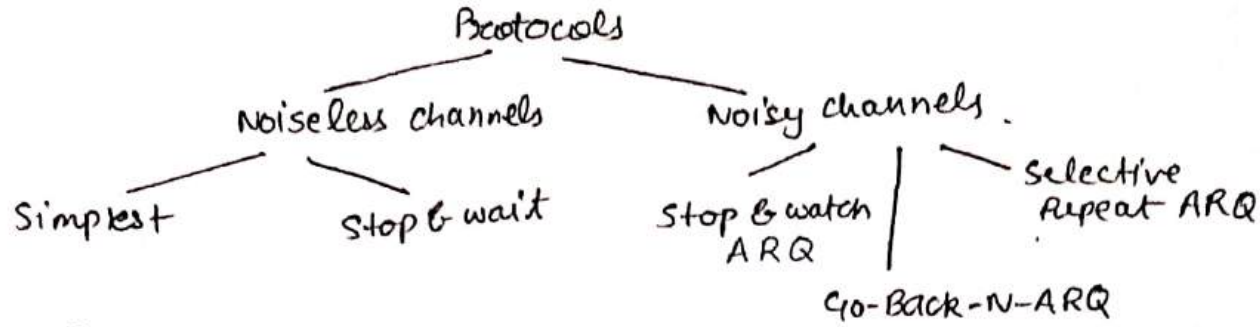
↳ unidirection (ya to send hoega ya reciever)

Primitives of stop & wait protocol :-

Sender :	Receiver :
Rule 1 Sender sirf one data packet send kar skta hai Ek baar m.	Rule 1 Recieve & consume Data pack
Rule 2 Sender next packet sirf tabhi send kar skta agar acknowledgement mil rhi hai previous packet ki toh.	Rule 2 jab consume ho jata ack send karo Sender ko.



Protocols



Protocols -

↳ defined set of Guidelines & Regulations jo control karta hai communication b/w Diff. devices in a network.

↳ yeh Guideline specify karte hai EK way jisme data format, timed, sequenced & check for Error during transmission

↳ Ensure accurate, Efficient, clear communication between ideas.

Simplest Protocol -

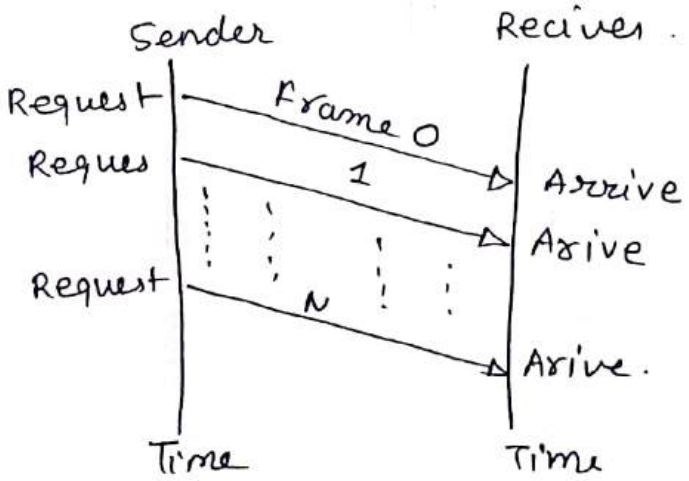
↳ involve Direct transfer of Data from the source to destination. without any intermediate processing.

↳ noiseless protocol hai (Matlab jaisa Data jayega vaise hi Recieve hoga)

↳ Doesn't have any mechanism for controlling the flow of Data or detecting & correcting

↳ one way protocol (allow data to flow from sender to reciever)

↳ unidirectional (no need for acknowledgement)



Stop & wait

↳ (Peeche ho gya)

Noisy channel protocol -

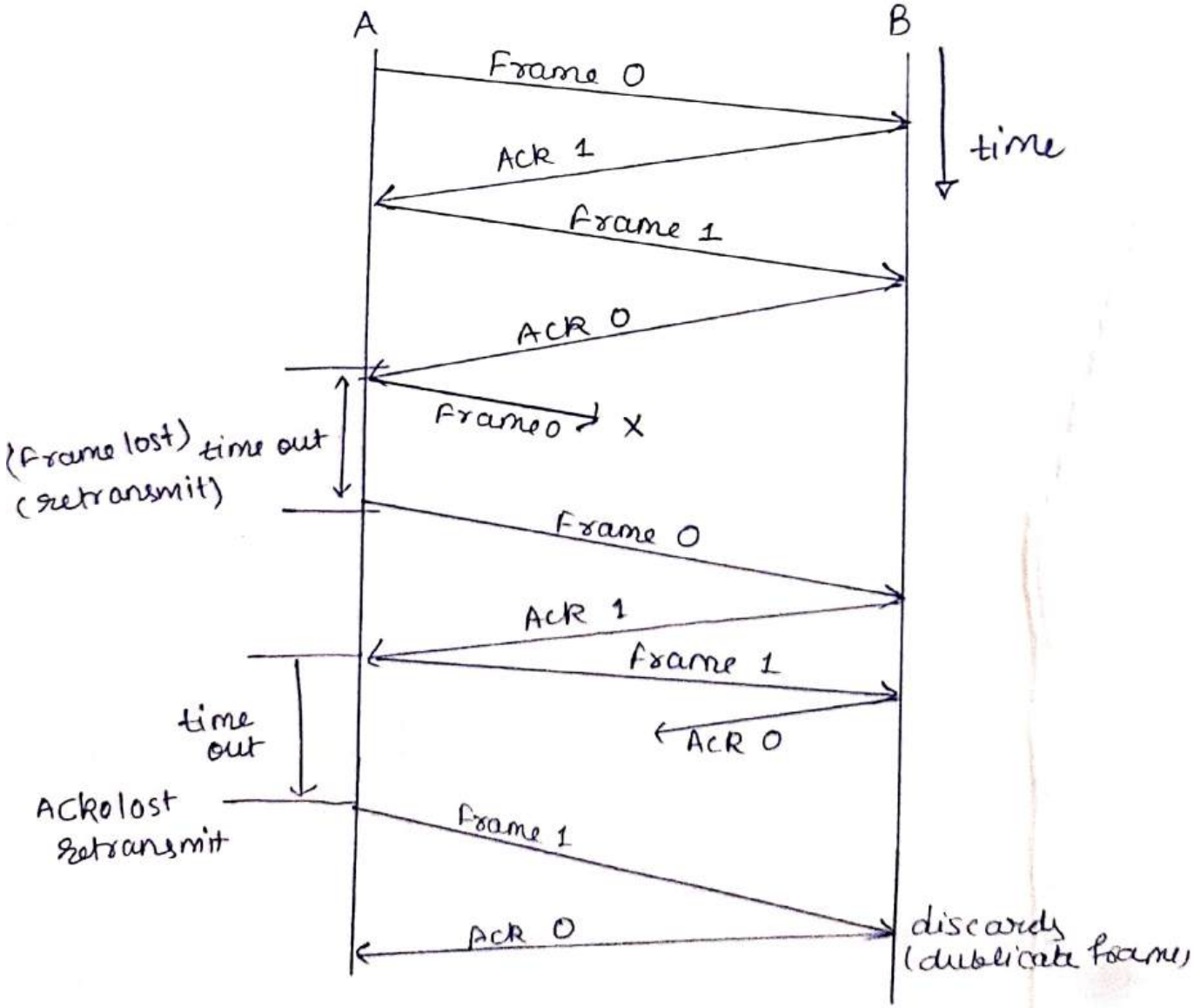
Stop & wait ARQ -

↳ used for reliable data transmission over a noisy channel

↳ Sender sirf Ek frame send karta hai & wait karta hai Ack ke lie before sending next frame.

↳ Yeh help karta hai jaane mein ki reciever ke pass data pauch gya (kaunki yeh noisy channel hai)

↳ Sender continously monitors the channel for errors, agar Error detect hota hai to next Ack ka wait karta hai, frame ko dubara bhejne se pehle.



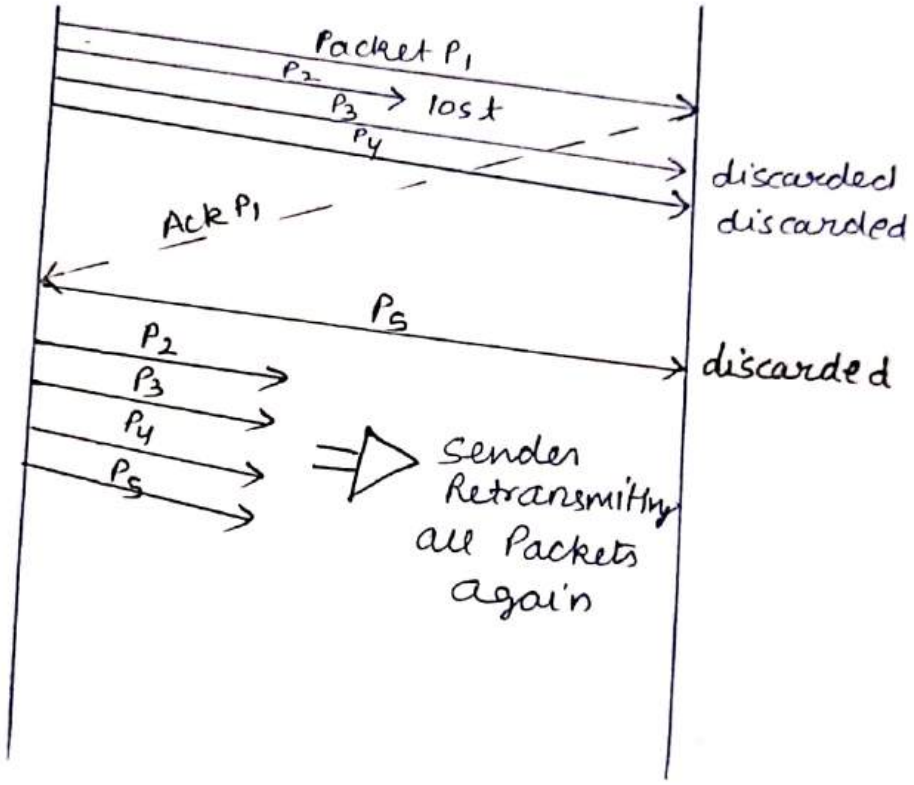
Go-Back N ARQ

↳ Error control protocols used in data communication to Ensure Reliable delivery of Data over Noisy channel

↳ type of sliding widow protocol

↳ Sender ek window of packets bhejta hai reciever ko. or Reciver ACK Send Karti hai

↳ in case agr sender ko shi time pe Ack Reciever nhi hoti, to sender Entire window ko dubara send karta hai



Sender side

(i) Packet send karega Reciver ko jisme (i+N-1) frame honge.

(ii) Sender set karega timer for each packet of window.

(iii) Sender wait karega Ack ka

Reciever

(1) reciver packet recive karega & check karega Error

(2) correct Recive hua hai to Ack send karga with seq. no jisme Reciever hue the

(3) agr Error ke sath recieve hua hoga to discard karega Nak bhejga.

Sender

(if No ack Rec)

↳ agr jo time hai ack Recieve Karne ka Usme ack Recieve nhi hui to sender vhii window Retransmit karega.

↳ time Reset Karga

↳ wait kaega ACK Brom Reciever

Reciver (In case of Nak)

→ agr Nak Recieve hua to vhii Packets dubara send karega jisme Error aya or Recieve nhi hue Reciever ko dhang se

→ Reset timer for Each packet

→ wait for ACK.

Selective Repeat ARQ

→ transmit a window of packets to Reciever, Reciever ack send karta to sender.

→ agr Error detect hota hai to Nak send karta hai Req. for retransmission.

→ sender maintains a timer for Each packet, agr ack nhi Recieve hui to retransmid hoega.

→ agr packet correctly Recieve hua to Reciever Ack send karga seq. no. Ke sath., agr Error ke sath Recieve hua to discard kaega Nak send karega & Retransmit Ke lie Req Karega.

→ ~~buffer~~ buffer maintain Rehta hai, throughout the process.

Sender

- (i+N-1) Packets send Karenge Ek window mein
- time set Karenge
- Ack ka wait Karenge

Reciver

1. check for Errors
2. Recieve correctly - then ack the packet
3. otherwise Nak & Req. for Retransmit

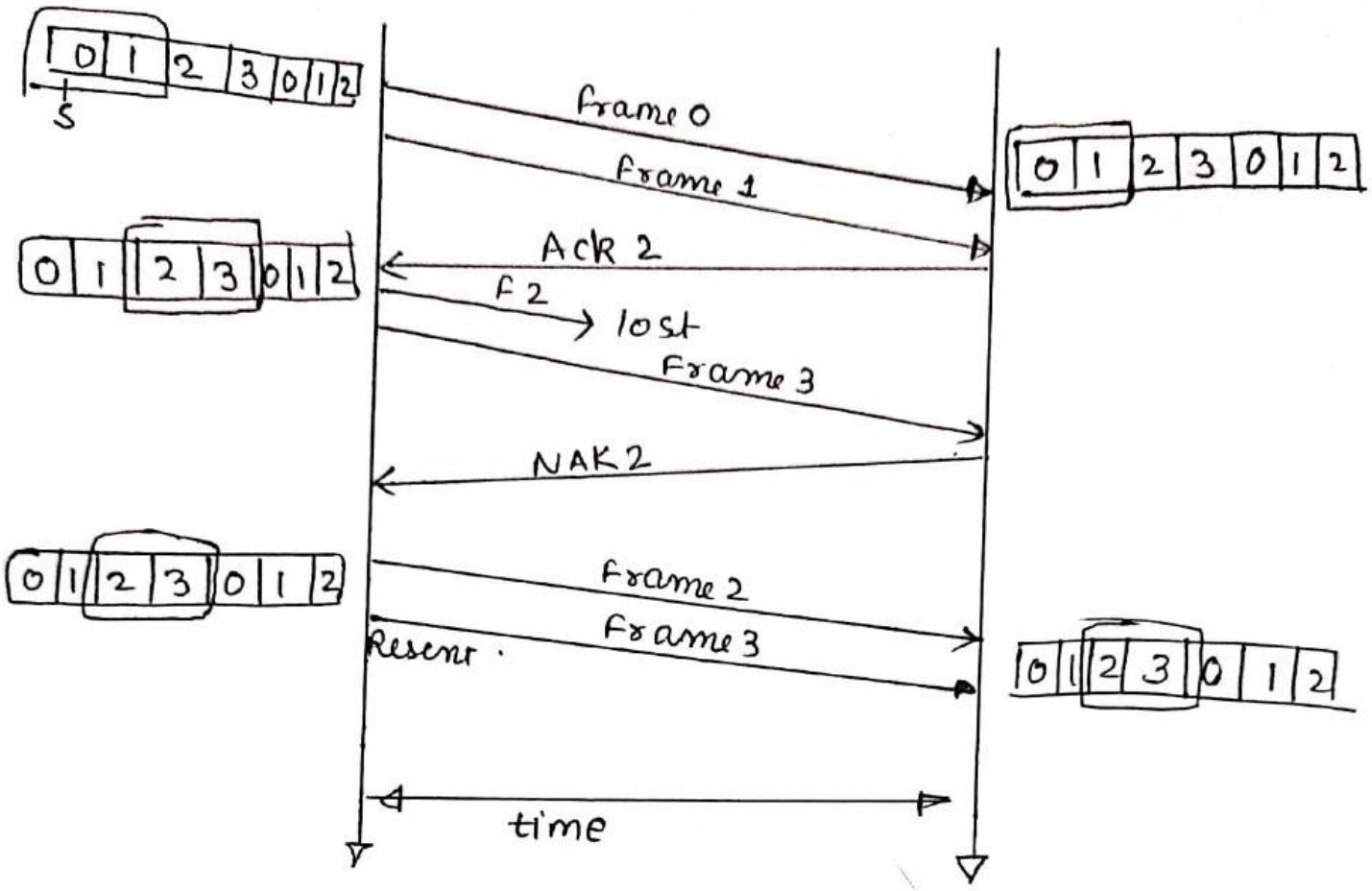
Sender (if no ack Recive)

1. time out se pehle ack nhi mila to · Sender Retransmit Karega
2. time set Karega.
3. wait karega ack ka.

(if Nak Recieve)

1. agr Nak Recieve hua Sender sirf vo Packets transmit karga jo correct Recive nhi hue
2. timer set Kaega
3. ack ko wit Karega.

M'


0 1 2 3 0 1 2
S
Frame 0
Frame 1
0 1 2 3 0 1 2
0 1 2 3 0 1 2
Ack 2
F 2
lost
Frame 3
NAK 2
0 1 2 3 0 1 2
Frame 2
Frame 3
Resent.
0 1 2 3 0 1 2
time

MAC layer.

OSI Model layered networking framework hai jo communication mein help karta hai 2 heterogenous systems mein.

Data link layer (2nd lowest layer)

- LLC (logical link control)
- MAC (Medium access control)

Functions of MAC -

↳ Determine karta hai kaise device access gain karta hai transmission medium mein, data ko transmit krne ke lie.
↳ used for addressing & identifying devices.
↳ Adds necessary header & trailer information to data to facilitate proper transmission & reception
↳ Error detection & Ensure Data integrity.
↳ Regulate the Rate of transmission between Devices

MAC address -

→ unique identifier alloted to network interface controller (NIC) of a Device.
→ used as a network address for Data transmission.
→ assigned to network adaptor at time of manufacturing.
→ MAC address comprises of 6 groups. (hexadecimal digits) Seprated by hypens, colons or no separators.

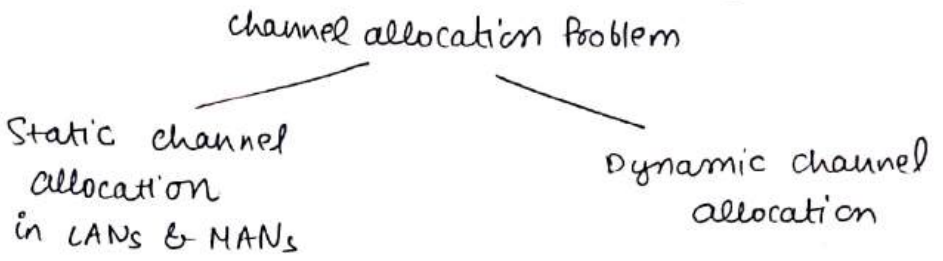
Ex 00:6A:89:5B:F0:11.

Channel allocation problem -

↳ signal channel ko divide karte hai & allocate karte hai to multiple user taki vo different task perform kar sake.

↳ Multiplexing is used

↳ channel allocation problem can be solved by two schemes



Static channel allocation in LANs & MANs.

→ classical or traditional approach of allocating a single channel among multiple competing users using Frequency Division Multiplexing (FDM)

→ if there are N users, the frequency channel is divided into N equal sized portions

→ not suitable for large no. of users.

→ not efficient to divide into fixed no. of chunks.

$$T = 1/(U * C - L)$$

$$T(FDM) = N * T(1/U(C/N) - 4N)$$

T = mean time delay
C = capacity of channel
L = arrival rate of frames.
1/u = bits / frame.
N = No. of sub channel
T(FDM) = Frequency Division Multiplexing time

Computer network components / Devicies -

→ NIC
→ ROUTER
→ Switch
→ MODEM
→ cable
→ HUB

NIC - Network Interface card -

- Used to connect computer with anathor component onto Network.
- Support a transfer Rate 10, 100 to 1000 MB/s
- NIC pe MAC address / Physical address Encoded hota hai jo ki assigned hota hai, IEEE as jo ki uniquely define Karta Network Card ko.
  MAC address store hota hai PROM me (Programmable Read only memory)

NIC

wired	wirless
(inside Motherboard) cables & connectors	contains ~~RTE~~ antena to obtain connection.

HUB :- Hardware device, divides Network connection among multiple device.

- jab computer request Karta hai kisi information ke lie. to vo Request Karta hai sbse pehle Hub se cable ke through
- HUB poore broadcast ko vo Req send Karta hai sb device check Karte hai ki Request unse Related hai ya nhi, agr nhi to drop the Req.
- HUB limits the amount of communication.

HUB

Active HUB	Passive HUB	Intelligent HUB.
• have their power supply & can clean, boost & Relay the signal along with network.	• collect wiring from nodes & power supply from Active HUB	• Includes remote management.
• Serve as repeater & wiring centre	• Relay signal onto the network without cleaning & boosting them	• provide flexible data Rates to network devices.
• Use to extend Maximum distance b/w nods	can't Extentend the distance b/w nodes	

Switch -

→ multiport bridge with Buffer + a design can boost its Efficiency & performance.

→ Data link layer Device.
→ can perform Error checking before Forwarding Data.
→ switch / Divides the collision domain of hosts, but broadcast Domain Remains same

types

1. unmanaged switches - home networks & small business
   - as they plug in & start work instantly stat doing their work
   - Require small cable connection only.
   - allow device on a Network to connect with Each other
   - least Expensive.

2. Managed switches - highest Security, Precision control & full management.
   - used in organization containing a large network.
   - customize to Enhance the functionality of a certain Network
   - Most costly, but ideal.

Router - hardware device, used to connect a LAN with Internet connection.
- used to Recieve, analyze & forward the incoming packets from another packet.

- Network layer mein kaam Karta hai, router ki.
- forward Karta hai packet based on info avilable in routing Device
- Determine best path from avilable for transmission.

advantages.

→ Security
→ Reliability
→ performance

Disadvantages

Modem

↳ hardware device allow computer to connect to internet over the existing telephone line.

↳ not integrated with motherboard, installed in the PCI slot.

↳ stands for modulator demodulator
converts digital data to analog signal

modem (Based on speed & transmission speed)

- Standard PC modem or Dial up model
- Cellular modem
- Cable modem

Cable & connectors -

↳ transmission media, used for transmitting a signal.

Cables

- twisted pair Cable
- Fibre-optic.
- Coaxial Cable

Repeater - • operates at physical layer.

• regenerate the signal over the same networks isse pehle ki wo weak/corrupted ho.

• jab signal weak ho jata hai to wo ~~break~~ ~~jata~~ hai copy karte hai bit by bit & Regenrate krte hai,

• It is 2-port device.

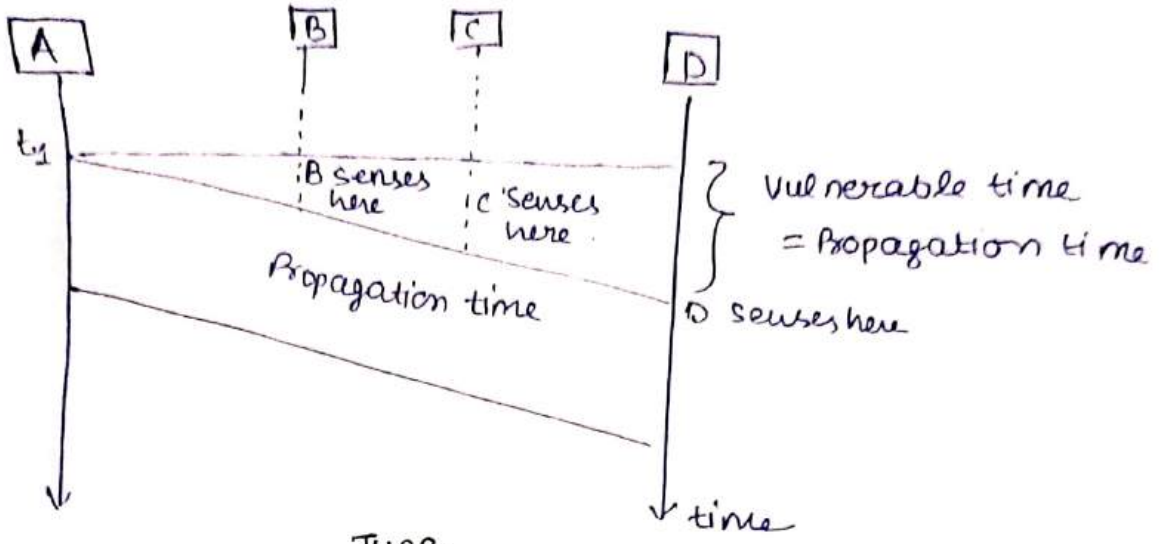
Bridge - operates at Data link layer, repeater hota hai ek type ka functionality → filter content by Reading the MAC address of source & Destination.

Bridge

- Transparent
  - → Stations are unaware of Bridge Existence.
  - → reconfiguration of stations is unecessary
- Source-Routing
  - → performed by sources station. Station & Frame specifies which route to follow

SMA (carrier Sense Multiple access)

ieveloped to decrease the chances of collision jab 2 or 2 se jyada stations signal sent karte hai data link layer ke



Type CSMA access mode

1 Persistent

Senses - shared channel first & deliver the data Right away if channel is idle agr nhi hai to continously track for channel jb tk idle nhi ho jata os phe brodcast Karega frame ko without any condition as soon as it does.

→ aggressive transmission algorithm.

Non persistent

access the channel befor transmitting data, agr channel idle hai to node transmit karega data agr nhi hai to station wait karega EK arbitrary amount of time ke lie (not continously) or jab dekhega ki ab Empty / idle hai to frame send karega.

P Persistent

(1 persis + Non persis)

Har node observe karegi channel ko 1 persistent main ek channel idle hai to send karega frame P probability ke sath., agr data transfer nhi hua to, frame restart karega. Kisi bhi time slot ke sath for q (1-p) Random period

O-Persistent

supervisory node order deti hai har node ko transmission ke lie. Node wait karti hai apne time period ke acc. jo alloted nota hai

Advantages of CSMA

(1) Efficiency ↑ → Ensure karta hai 1 time pe 1 hi device communicate kare, jisse collision kam hoga or Efficiency accuracy badhegi

(2) Simplicity - Easy to implement & doesn't require complex hardware or software.

(3) Flexibility - wide Range of network Environments use ho sakte h

(4) Low Cost - jyada complex hardware or software ki zarrot nhi hoti

Disadvantages -

(1) Limited Scalability - inefficient no. of devices hote hai network pe

(2) Delay - wait karna Medium ko sense karne ke lie or availability of channel ke lie Delay kar skta hai.

(3) Limited Reliability - affected by interferance.

Collision Detection in CSMA/CD.

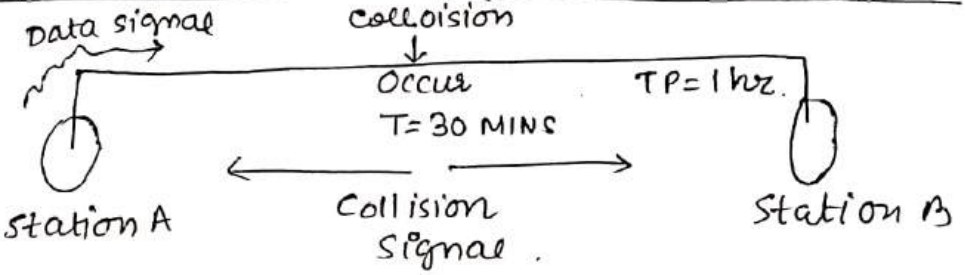
↳ measure for effective transmission.

↳ This protocol decides which station will transmit when so, that Data Reaches the destination without Corruption.

Working -

1) Check sender Ready hai packet serve karne ke lie ya nhi.
2) Check if transmission link is idle.
   Sender check karta Rehta hai ke transmission link/Medium idle hai, iske lie vo continously sense karta other transmission nodes ko. Sender dummy data send karega link pe or agr koi signal Recieve nhi hua collision ko, iska matlab idle hai us moment pe, otherwise or agr hua to Refrain kar
3) transmit the Data, check for collision.
   Sender transmit karega Data ko link pe CSMA/CD doesn't use an "ACK" system. yeh check karta hai successful & ~~unsuccessful~~ unsuccessful transmission through collision signal. agr transmission ke samay collision signal Recieve hota hai node ko to transmission Stop ho jayega. pher station transmit karega jam signal link pe and wait karega Random time interval ke lie. before it Resend the frame. Pher kuch Random time ke Baad vo again attempt karega transfer karne ke lie Data. and Repeat karega above process.
4) agr no. collision was detected in propagation, Sender complete its frame transmission & reset the counters.

How does a station know if its Data collide -



collision free protcols in computer Network

Almost sbhi collisions avoid kie ja skte hai, CSMA/CD mein phir bhi vo ho jate hai contention preid mein. or yeh adversly affects karte hai system performance ko.

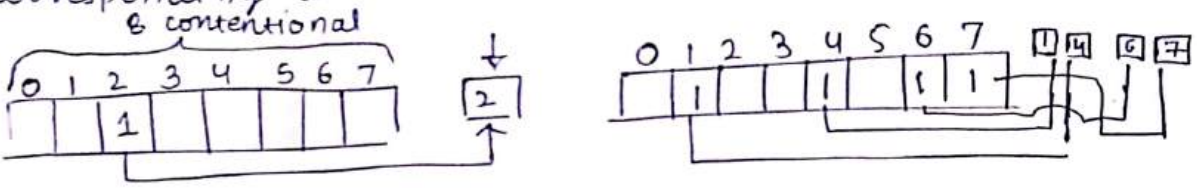
yeh tb hota hai jab cable long hoti hai or length of packet short. or yeh problem bohot serious bn jati hai jb fibre optic use karte hai.

Protocols bane hai unko resolve karne ke lie.

↳ Bit map protocol
↳ Limited contention
↳ Binary countdown
↳ Adaptive tree walk protocol.

1. Bit map protcol

- Each contention period Exactly N slots ka hota hai
- Agr kisi station ko frame send karna hai, to usko 1 bit corresponding slot ko transmit karni hogi.

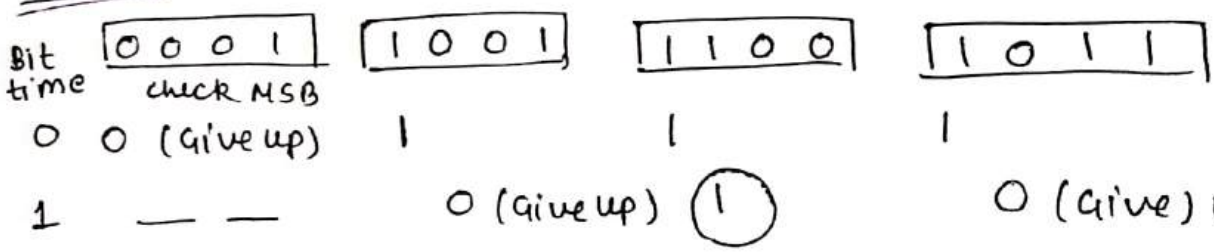


iski limitation yeh thi ke agr, hume 1000 Frame send karne hai to, 1000 bits chaiee honge. Matlab for large no. of frame we need same no. of bits.

Binary countdown - Binary station address use hota hai.

- jo station chanta hai send karna usk address lenge, or vo apni successive MSB compare karega, or karta rahega till End. agr MSB 0 hogi to ~~wait~~ wo give up kar dega otherwise, aage wali bit pe jayega compare karega

For Exp.



1100 will transmit data/frame.

ited contention protocol -

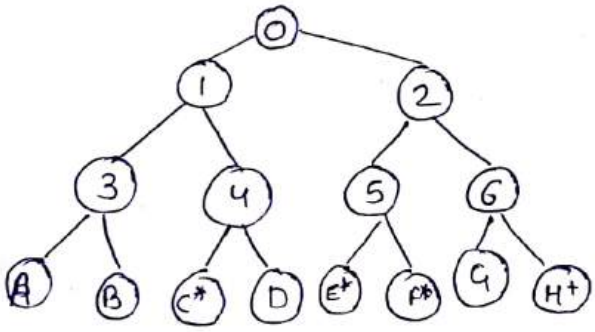
- collision Based protocols (Pure & slotted ALOHA, CSMA/CD) are good when network load low
- Collosion free protocol (Bit map, Binary countdown) are good when load high.

Adaptive tree walk protocol

- Partition the group of station & limit contention of each slot.
- under light load → each slot like aloha.
- under high load → only a group can try for each slot.

How?

- treat every stations as leaf of Binary tree
- First slot (after successful transmission), sb stations try karenge apna slot lene ka (under root)
- If no conflict, well & good.
- else, only nodes under sub tree get to try for next one (DFS)



Slot 0 : C*, E*, F*, H* (all nodes 0 ke under hai) conflict. Sb send karne ka try karengi.

Slot 1 : C* (all nods under 1 can try), C sends.

Slot 2 : E*, F*, H* (all nodes under 2) all try), conflict.

Slot 3 : E*, F* (all nodes under 5 all try), conflict.

Slot 4 : E* (all nodes under E) all try E sends.

Slot 5 : F* (all nods under F) all try F sends.

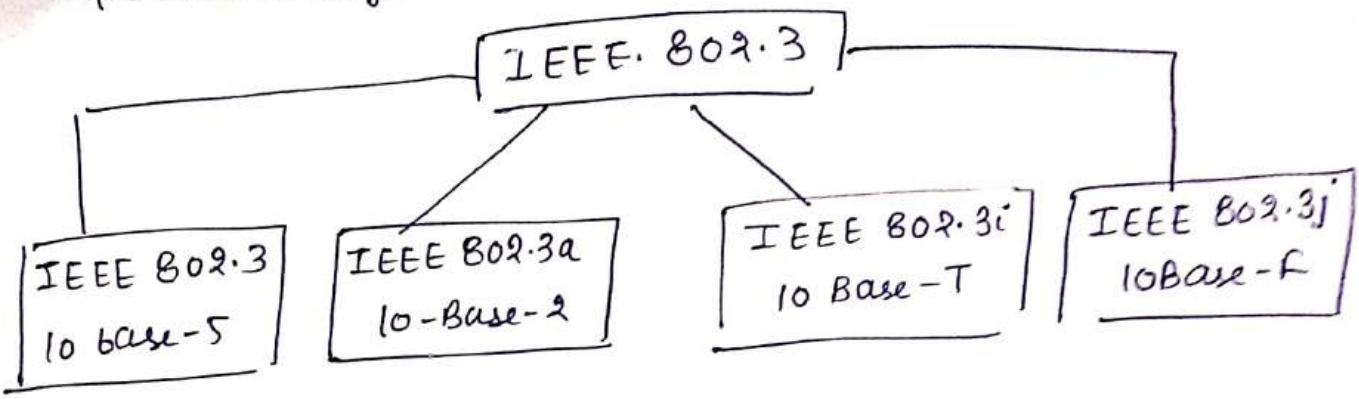
Slot 6 : H* (all nods under H) all try H sends

EEE 802.3

→ set of standards & protocol that define Ethernet-Based networks.

→ use LANs, iske use se yeh MANs mein bhi & WANs mein bhi use ho skta hai

→ defines Physical layer & medium access control (MAC) of Data link layer



Frame format -

- preamble - 7 Bytes. starting field provide alert & timing pulse for transmission
- Start of frame Delimeter : 1 byte field.
  ↳ contains an alternating pattern of ones & zero Ending with two ones.
- Destination address : 6 byte field
  ↳ Physical address of destination.
- Source address - 6 byte field
  ↳ Physical address of sending station.
- Length : 7 Bytes
  ↳ store the no. of Bytes in Data field.
- Data : variable sized (Max = 1500) carry Data from upper layer.
- Padding : 46 bytes → minimum data ke sath combination mein nota hai
- CRC - Cyclic Redundancy check. Errors detection (4 bytes)

Premeable 7 Bytes	SOF 1 Byte	DA 6 bytes	SA 6 bytes	Data + Padding Min = 46 Max = 1500 bytes	CRC 4 bytes

EE Standard

802.11.

IEEE 802.11 standard, popularly known as wifi.
architecture & specifications of wireless LAN's (WLANs)
↓
use high-frequency Radio waves instead of cabels for connecting device in LAN.

architecture

components

→ Stations (STA) - Comprises of all devices & Equipment that are connected to wireless LAN (wireless network interface controller hota hai)

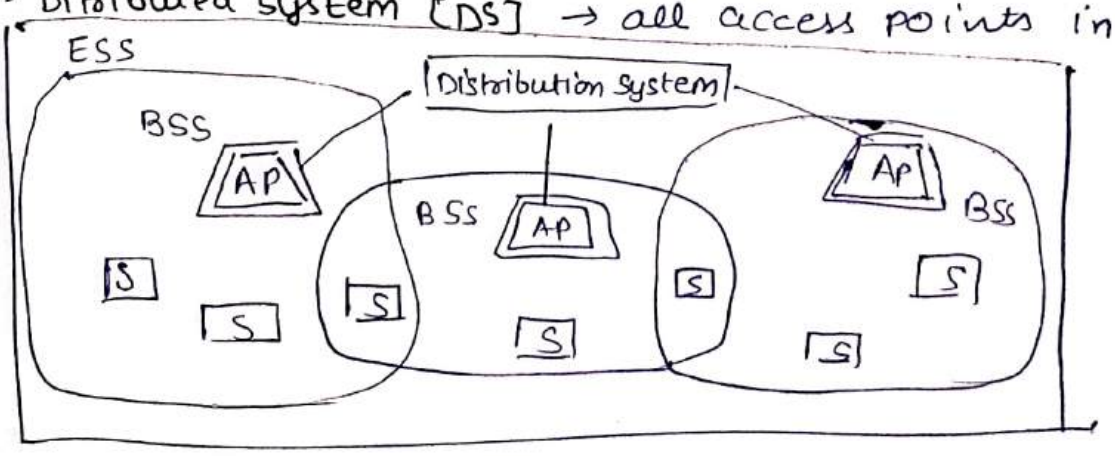
Station
- WAP (wireless access point)
  - wireless routors
  - base stations
- clients
  - → workstations
  - → computers
  - → laptop
  - → printers
  - → smartphones etc

→ Basic service set [BSS]: Group of station communicating at physical layer level.

BSS
- Independent (Peer to peer basis)
- Infrastructure (communication through access points)

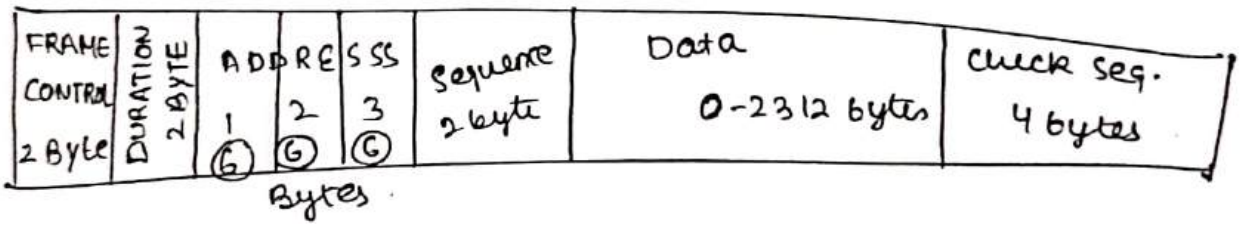
→ ESS (Extended service set) → all connected BSS

→ Dibributed system [DS] → all access points in ESS.



in field of frame.

- **Frame control** - 2 byte starting field composed of 11 subfields
  - ↳ control information
- **Duration** - 2-byte field
  - ↳ specify karta hai time period for which the frame & acknowledge occupy karte hai channel ko
- **Address fields** - 6 byte (three)
  - ↳ contain add. of source, immediate destination & final End point
- **Sequence** - 2 byte 3-field that
  - ↳ stores frame no.
- **Data** - variable sized
  - ↳ carry data from upper layers. (MAX = 2312)
- **Check sequence** - 4-byte field
  - ↳ contain error detection information.



FDDI - Fiber distributed data interface

↳ work on OSI model's physical & Data link layer.

↳ use optical fibre to transfer data much Quicker

↳ Dual ring system, transmit data in opposite Direction.

↳ suitable for LANs, MANs, CANs but not WAN

working

↳ works using token Ring protocol, used timed tokens
i.e., if koi host message send karna chahta hai, to vo transmitted token capture karega.

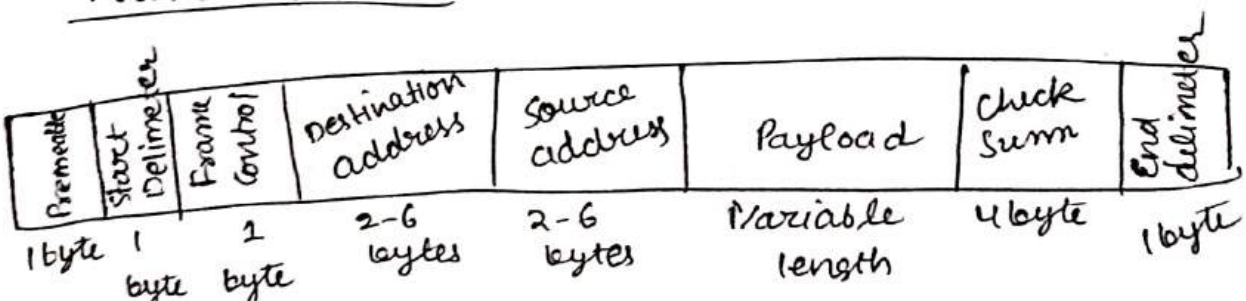
↳ host can transmit Data for fixted time (kuch der baad token further pass kar dia jayega)

↳ sb host access kar skte hai transmitted data ko & check kar skte hai "MAC address"

↳ Network host accept karega data ko, ager destination address match hota hai.

↳ Host transmit & Recieve kar skta hai data as frames

Frame format



Topology & Design -

↳ has two token passing ring, transmit in opp. direction

Primary secondary (Primary fails)

↳ Ring topology

Station connection

Single attached

↳ Stations connected to a primary or a secondary Ring, lack fault tolerance (Kisi ek se)

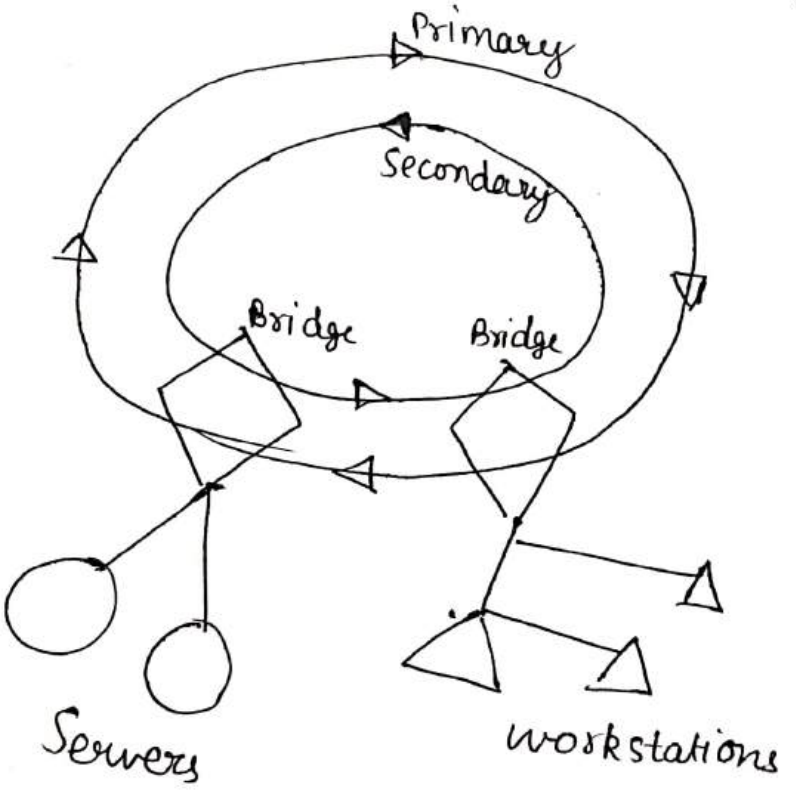
↳ can use them to connect Server to network backbone

Dual attached

↳ connect to both Rings of FDDI fibre networks.

↳ fault tolerance mast hoti hai

↳ Excelelent for network backbones



UNIT-3

NETWORK Layer : Design Issue

1. addressing
   - IP addressing - Each device on network must have unique address
   - Hierarchial - manage address Efficiently & Reduce size of Routing table.

2. Routing -
   - Path Determination - best path through the network
   - Scalability - protocols must be able to Scale as network grows

3. packet forwarding -
   - Forwarding technique - how packets are forwarded

4. Error handling & Diagnostics -
   - Error Detection & correction - Detect & correct Errors in transmitted Packet

5. Congestion control -
   - avoid congestion - techniques to prevent network congestion.
   - Handing - Packet dropping.

6. QOS (Quality of Service) -
   - Traffic prioritization - high priority traffic
   - Resource Reservation - along with network path

7. Security -
   - Secure Routing - protection from being tampered with

Network layer

- Third layer of OSI
- handles services from transport layer & further forwards the service Requests to Data link layer.
- translates logical address to physical addres
- Determines the route (source to Destination) manage traffic problems - Switching, Routing & Controls the congestion.
- **Role** - Network layer is to move packets from sending host to Reciving host.

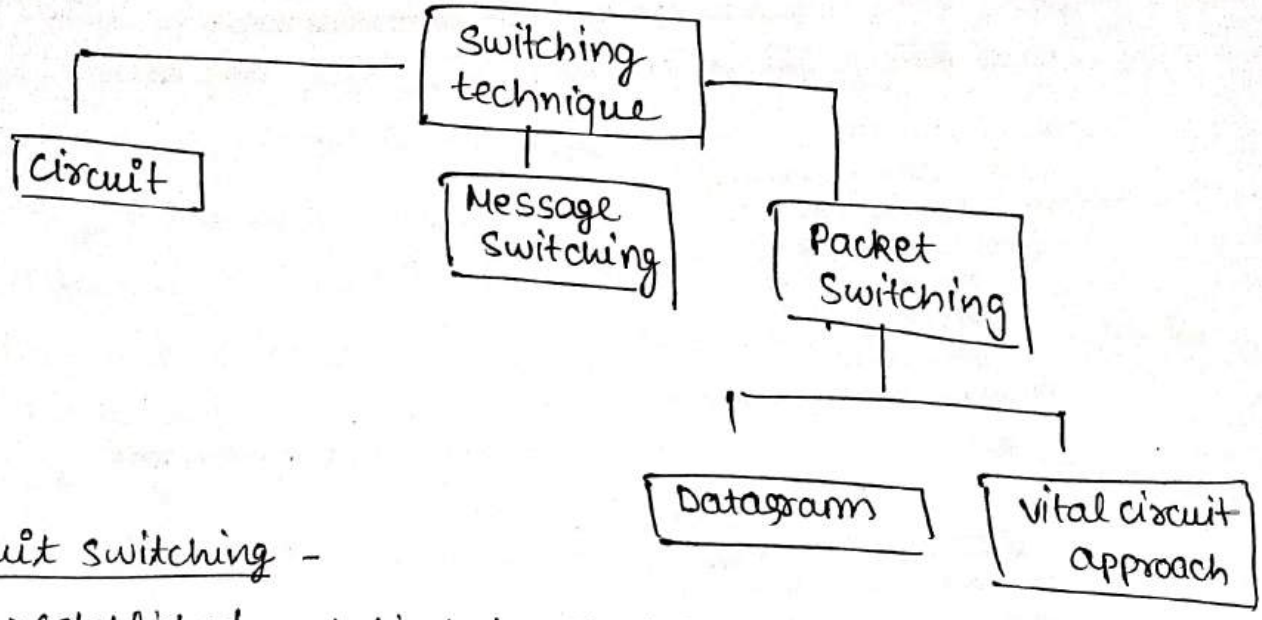
Main functions:-

1. Routing - jab packet router input link pe jata hai to Router usko output link pe bhej deta hai.
2. Logical Addressing - implements physical addressing & network layer implements the logical addressing. used to Distinguish b/w source & Destination System.
   It adds header to packet include logical address of Sender & Reciever
3. Fragmentation - breaking of packets into smallest individual Data units

PACKET SWITCHING

Switching → used to connect the system for making one to one communication.

Decide best Route for data transmission.



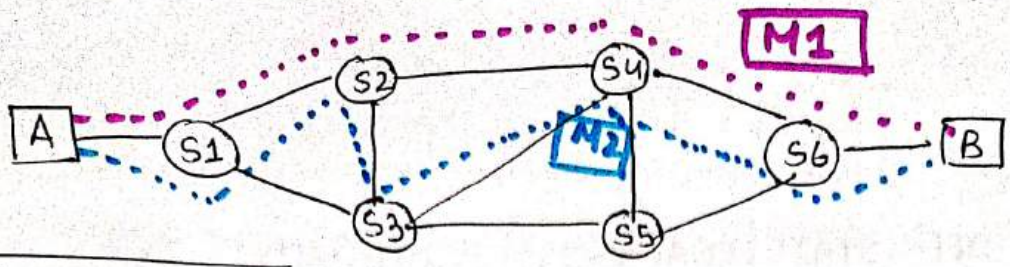
Circuit switching -

- Established a dedicated path between Sender & Reciever
- Ek baar jab connection Establish ho jata hai, jo dedicate Path hota hai it will remain Exist unit connection is terminated.
- Before Data transfer, counection will be Established first.

Phases - 1. Connection Establishment.
2. Data transfer.
3 counection Disconnection.

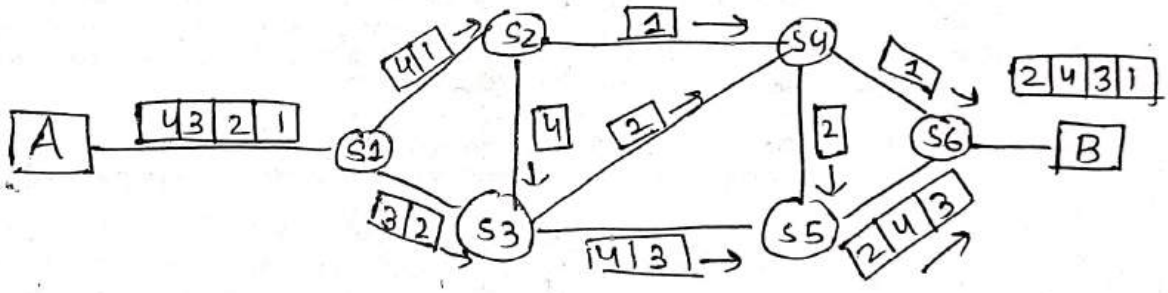
Message switching -

- Store & forward mechanism.
- Message is transferred as a complete unit & routed through immeatede nodes at which it is stored & fosward
- no Establishment of Dedicated path.
- Programmed in such a way so that they can provide the most Efficient Routes.



Packet switching -

- Message is sent in one go, but divided into small pieces
- Message splits into smaller pieces as Packets & given a unique number to identify order at recieving end.
- Every packet contains som info in header as source address, destination add & Seq. no.
- Packet travel across network, take shortest path as possible.
- all packet reassemble at reciever End.
- If any packet is corrupted or missing then message will be sent to Resend the message.
- If correct then ack.

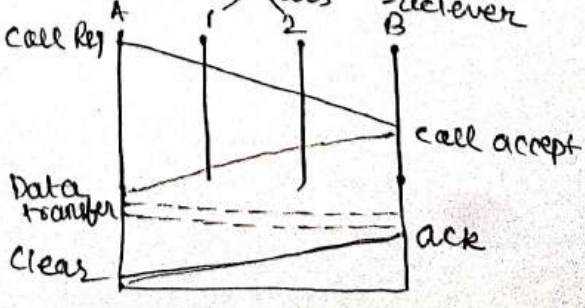


Datagram

- Packet Switching technology
  ↳ known as Datagram
  considered as an independent Entity
- Packet contains info about destination & switch uses this info to forward the packet to correct destination.
- Packet are reassembled at Recieving End
- the path is not fixed.
- Connectionless Switching.

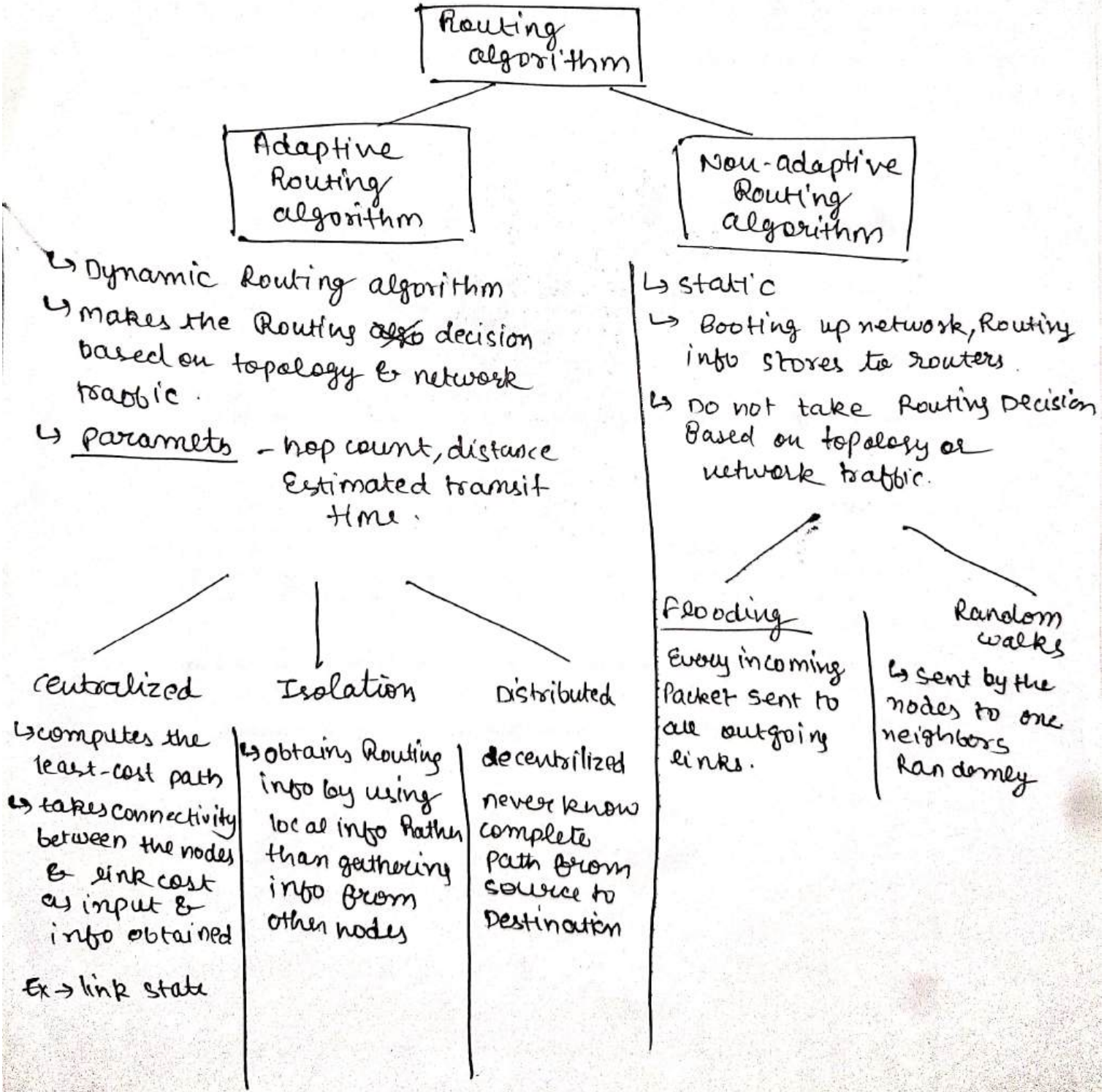
vital

- Connection oriented.
- Peplanned route is Established before the message are sent
- call Request & accept- packets are used to Establish the connection b/w sender & Reciever
- Path is fixed for duration



ROUTING ALGORITHM -

- Determines best route from Source to Destination through which Packets can be transmitted.
- Routing protocol at network layer provide this job.
  - Provides the Best path → "least cost path"
- Routing - process of forwarding the packets from source to Destination



(dynamic algo)

Distance vector Routing Algorithm -

Iterative
its process continues until no more info is available to be exchanged between neighbours

Asynchronous
doesn't Require all of its nodes operate in lock step with each other.

Distributed
(har node recieve karegi info from one or more directly attached neighbours. calculation perform karegi or result Back to Neighbours)

- Each router mainlains a distance table → "vector"

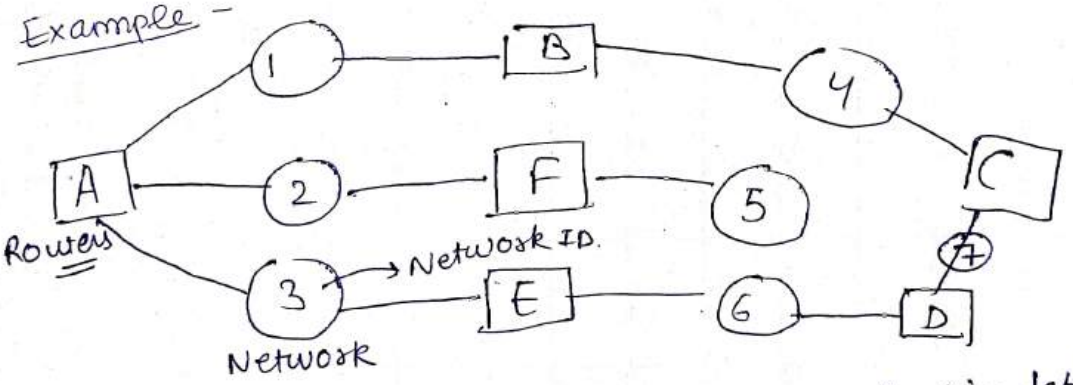
algorithm -

(1) A router transmits its distance vector to Each neigbors in Packet.

(2) Router recieves & Saves the most recently recieved distance vector from Each of its neighbour.

(3) Router recalculate distance vector when
   (1) it Recives a Distance vector from neighbour contain Diff. info.
   (2) Discover that link to a neighbour has gone Down.

Example -



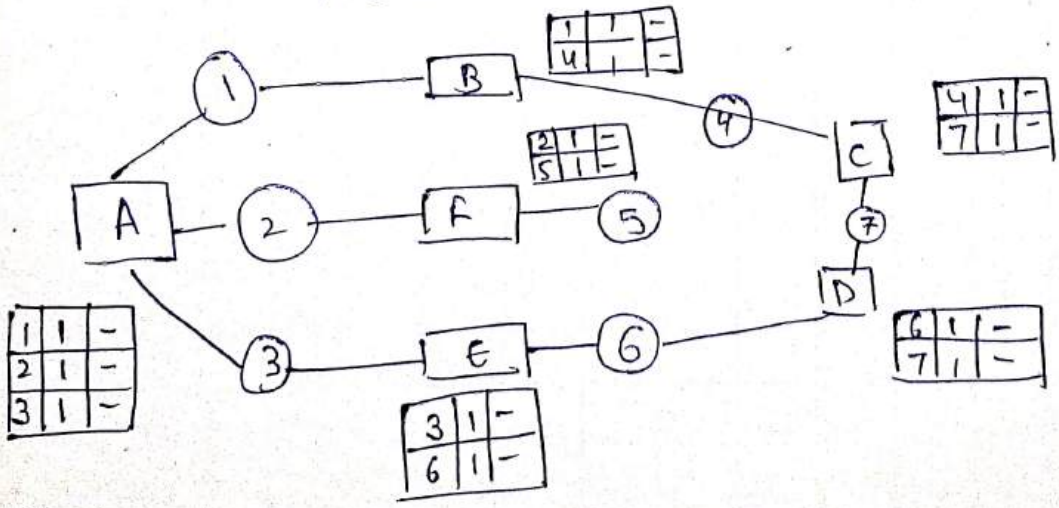
A → BFE
B → AC

C → BD
F → A
E → AD

D → EC

Routing table

ID	Cost	Next Hop



Updating table

1	1
4	1

+ one hop =

1	2	B
4	2	B

1	1	-
2	1	-
3	1	-

+

1	2	B
4	2	B

→

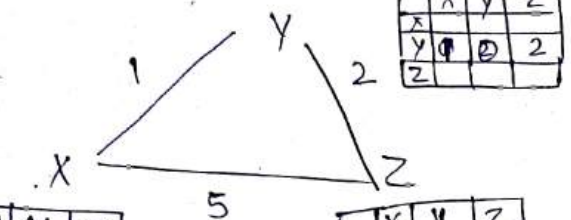
1	1	
1	2	B
2	1	
3	1	
4	2	B

duplicate Data ~~ki~~ sirf wahi Rakhega jiski cost kam hogi

=

1	1	
2	1	
3	1	
4	2	B

For Exp consider 3 Routers



	x	y	z
x			
y	1	0	2
z			

	x	y	z
x	0	1	5
y			
z			

	x	y	z
x			
y			
z	5	2	0

Same steps for y & z.

y =

	x	y	z
x	0	1	3
y	1	0	2
z	3	2	0

z =

	x	y	z
x	0	1	3
y	1	0	2
z	3	2	0

Exchange Routing table

x will get z & y Routing table

So, new Routing table will be like this -

x	x	y	z
x	0	1	~~5~~ 3
y	1	0	2
z	~~5~~ 3	2	0

now as we can see when y is intermediate node b/w x & z it have low cost (3 < 5)

	x	y	z
x	0	1	3
y	1	0	2
z	3	2	0

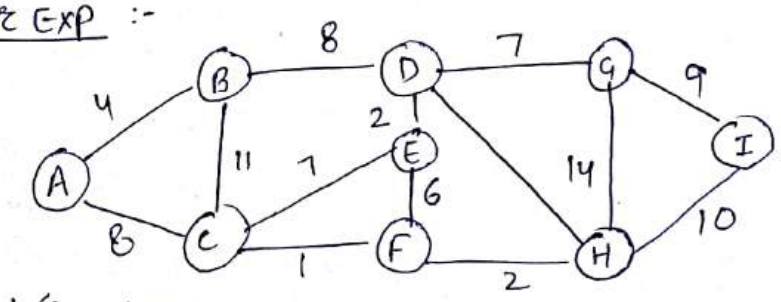
Link state

technique in which each router shares the knowledge of neighbourhood with every other router in internetwork.

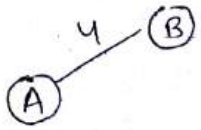
Phases

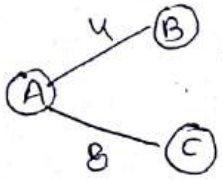
- Reliable flooding
  - Initial state (Each node knows cost of its neighbours)
  - Final state (Knows entire graph)
- Route cal.
  - ↳ Dijkstra's algo (used to find shortest path from one to every other node)
  - ↳ iterative, property hoti hai after K^{th} iteration of algorithm the least cost path are well known for K destination nodes.

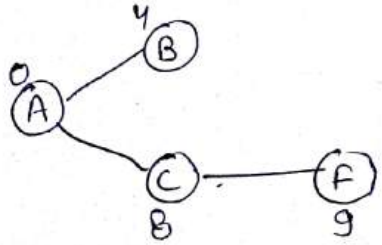
For Exp :-



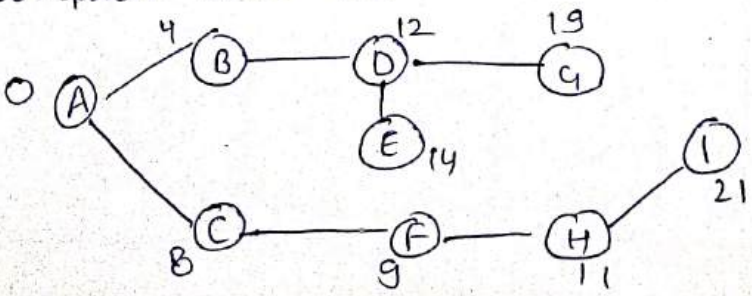
Let's start with A vertex,







Complete will be



Flooding -

Communication method where data packets are sent to all connected devices, Even if they are not intended recipient of data.

Why flooding

1. Address Resolution - translate IP to actual MAC.
2. Routing protocol - Link state Routing
3. multicast tree Establishment - create Multicast Distribution tree
4. Emergency Broadcast - regardless of location make sure that message reach all network device.

features

1. Broadcasting - Send to Every device connected to network
2. No prior Knowledge - Precise address of Device optional
3. Simple & Robust - Straightforward, simpl doesn't rely on intricate Routing algorithms
4. Loop prevention - use Time to Live counters to stop Data packets.
5. Security consideration - Expose private info to recipient who weren't intended.

Broadcasting -

→ allow message to be recieved by all nodes of network
→ transmission of signals from Radio or television.

Broadcasting

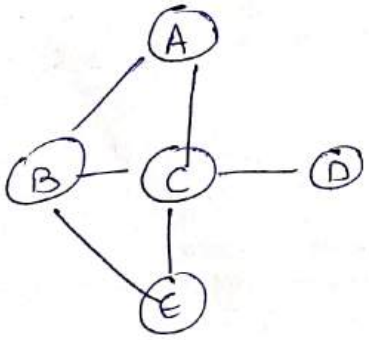
unicast
Ek source info send karta hai Ek hi Destination ko.
Ex → Phon call

multicast
multiple Destination ko hi Ek hi time
Ex → Radio

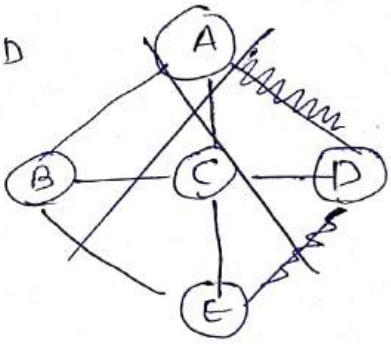
Flooding	Broadcasting
• Packets ko har node tak bhejna, bina kisi specific Routing ke.	ek source se multiple recipients tk info bhejna
• redundancy avoid ke lie	info Delivery ke lie
• limited to network infrastru.	coide Range
• Minimal control, Packets har node tak pauchte hai	controlled, specific to choosen medium/audiance
• network congestion & collosion	Efficiently reach large audiana

Flow Based routing -

- ek network routing technique hai jisme network traffic ko different flows mei catagorize karke route karte hai.
- har individual packet ko alag se route kia jata hai.



(A → D) = A → C → D
(B → E) = B → C → E
(A → E) = A → B → E



Multicast Routing -

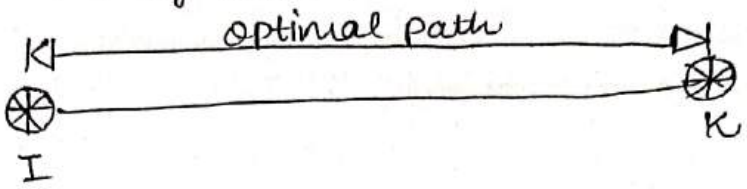
↳ ek single source se multiple destinations tk Data packets Efficiently bheje jate hai.

↳ sirf unko bhjti hai jo actively participate kar rahe hai

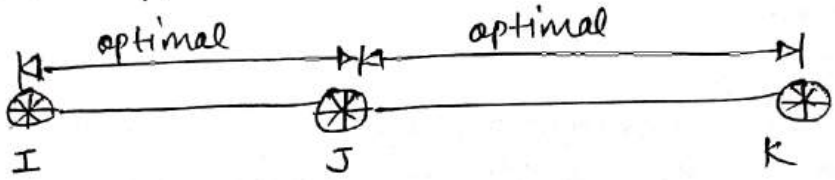
↳ Bandwith conserve karti hai.

Optimality principle

Statement - if the router J is On the optimal path from I to Router K, then optimal path bron J to K also falls along same route.



Now suppose J lies between I & K



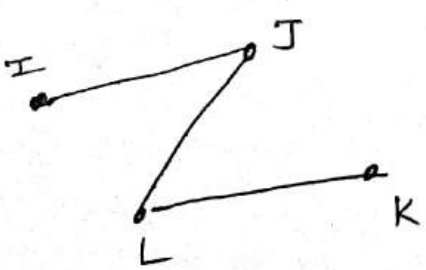
Importance -

* Efficiency → avoid wasting Resources by Exploring unnecessary paths.
* Loop prevention - Routing algorithm can prevent creating loops in network.

Limitations -

* Dynamic networks - assumes ki router have complete & up to date info. about network.
* cost metrices - Optimal path Kisi ke lie kuch bhi ho skta hai
least cost, fastest, shortest or Combination of factors.

For Exp. Let I J K, L are the Routers & connection between them.



Let suppose I → J → L → K is optimal path from I to K then J → L → K is the optimal path from J to K.

Flow control -

↳ technique used to Regulate the flow of Data b/w Different nodes in a network

↳ Ensure karta hai Sender ER dm se overwhelm na kare, (Matlab bohot sara Data ER sath Send na kare)

↳ goal : to prevent buffer overflow, lead to dropped packets & poor network performance.

Congestion control - (गति - गति)

↳ technique to prevent congestion in a network.

↳ yeh occur hota hai jab bohot sara Data ER sath bheja jata hai. network pe.

↳ lead to ~~pro~~ dropped packets & poor network performance.

Similarties

(1) Regulate the flow of Data.
(2) prevent packet loss.
(3) improve network Efficiency.

Flow	congestion
(1) Traffic from Sender to Reciever is controlled	Sender has to control/modulate own rate
(2) used in DDL, transport	used in network & transport
(3) Keeps the data from overwhelming	Keep networks from being congested
(4) Sender sends data slowly to Reciever	Slowly transmitted into network by transport layer.

	Datagram	virtual circuit network
circuit step	Not needed	Required
QOS	Difficult	Easy if Enough resources
Congestion control	Difficult	Easy if Enough Resources
Address	Each pack contain the full source & Destination address	contains a short VC number
Effect of Router failures	None Expect for Packets lost during crash	VC's passed through failed network are terminated
Routing	independent	choose VC, all packets follow it

Internetworking = inter + networking = connections b/w two complety distinct segments.

→ isme switches, gateways jaise Devices use hote hai.

→ jo data ko Ek network se dusre network tk pauchate hai.

① Internet - network ko Ek sath jodta hai jaise private, Edu. organization etc.

② Intranet - private network Ek organization ke internal use ke lie hota hai. Ex - employees, Department

③ Extranet - Extension of intranet (External parties se connect karta hai) limited access.

④ VPN → privacy & security

⑤ P2P → file aur resource sharing

Unit-4

Transport layer - (End to end layer)

↳ Ensure jo packets hai arrive hoe order mei.
↳ Provide acknowledgement of successful data transmission & " ob 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 Resembly of Packets into Message.
2. Message acknowledgement - Reliable End to End Message delivery
3. Session multiplexing -  ER 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.

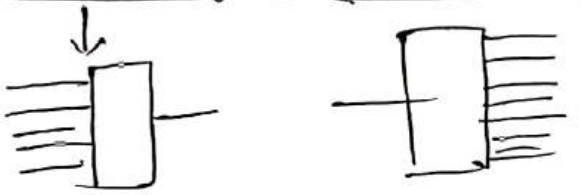
Transport Layer Design issue -

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 congested traffic. 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 characteristics

Reliability
Means loosing a packet or acknowledgement Entails Retransmission.

Delay
Applications can tolerate delays in different degress.

Jitter
Variation in Relay for packets belonging to same flow
High → delay large
low - small

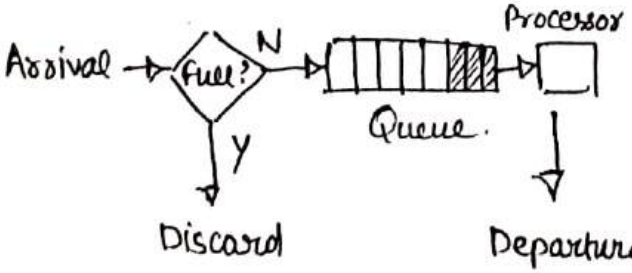
Bandwidth
Different application Different Bandwidth.

Techniques to Improve QoS -

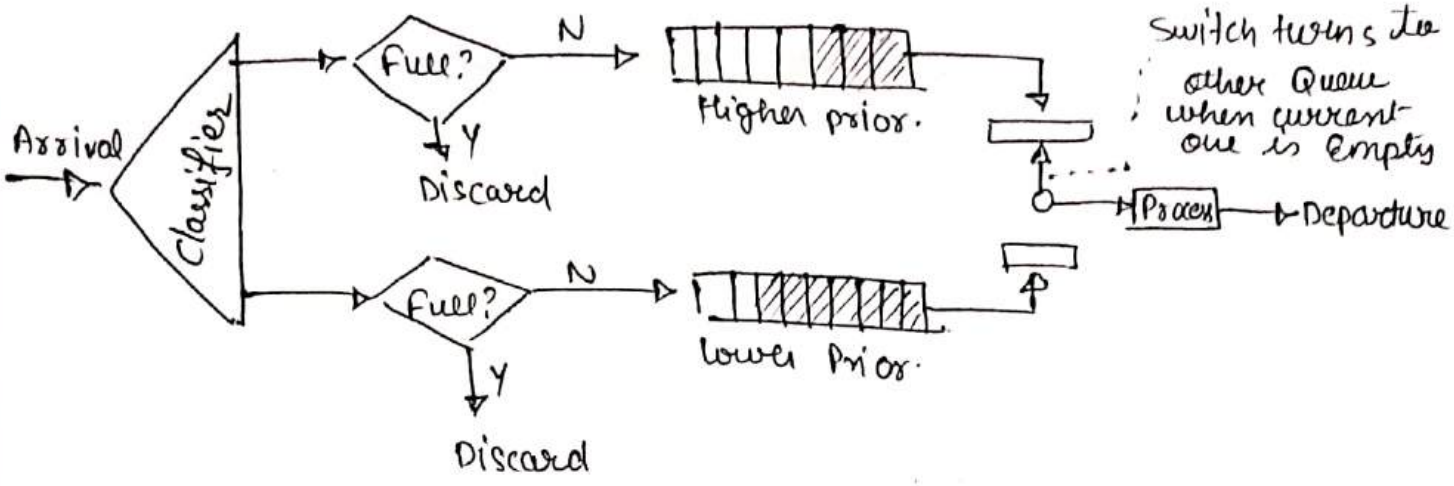
1. Scheduling
2. Traffic Shaping
3. Resource Reservation
4. Admission control

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

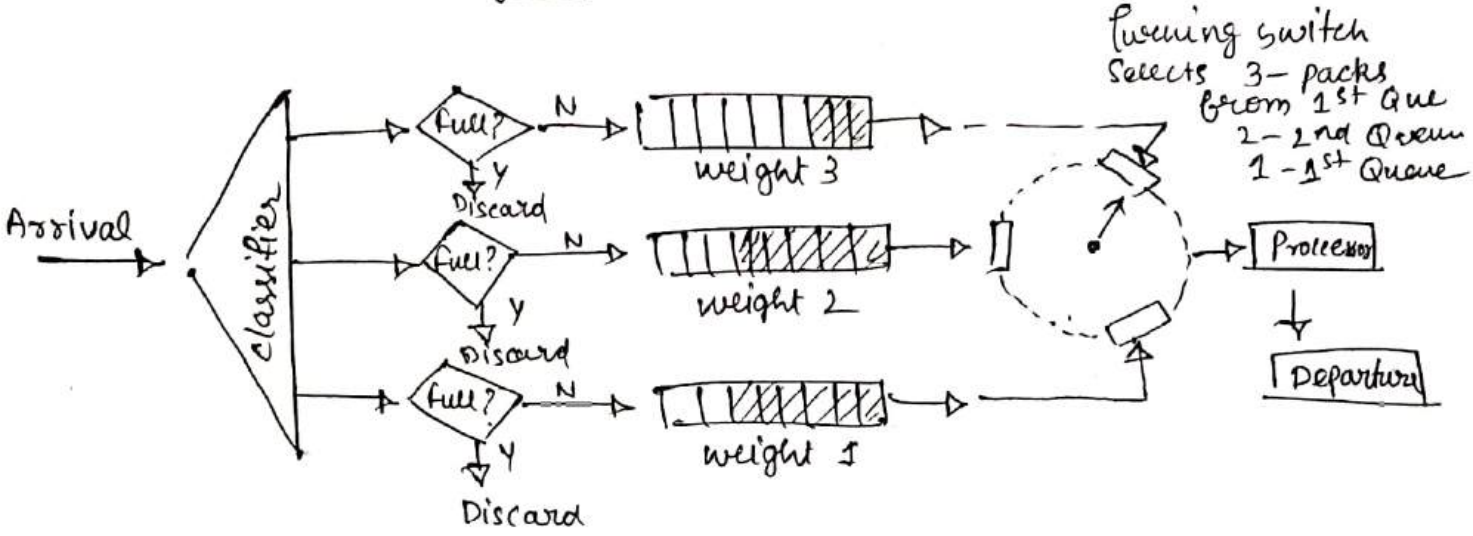
FIFO Queuing | Priority | Weighted fair



Priority Queue



Weighted Fair Queuing



2. **Traffic Shaping** - Traffic 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

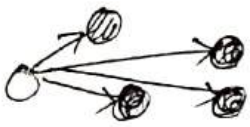
↳ Flow data needs resources such as buffer, bandwith cpu - -

Admission control -

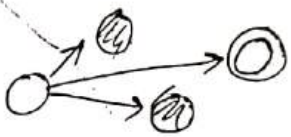
↳ a mechenism used by Router, switch, accept, reject a flow based on predefined parameters.

Transport layer Protocol

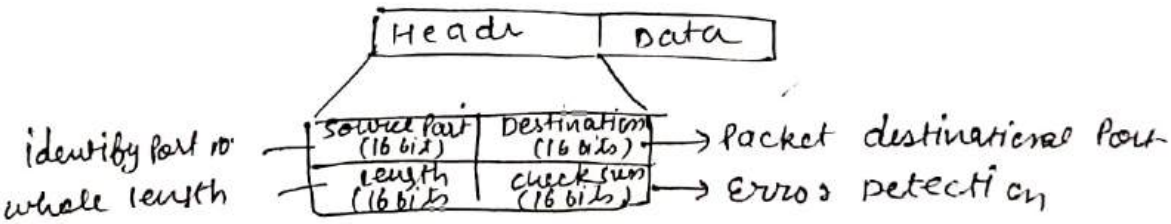
1. UDP – User Datagram protocol.
   - non sequential transmission
   - connectionless (speed & size is imp)
   - adds checksum, Error control
   - Faster delivery of messages



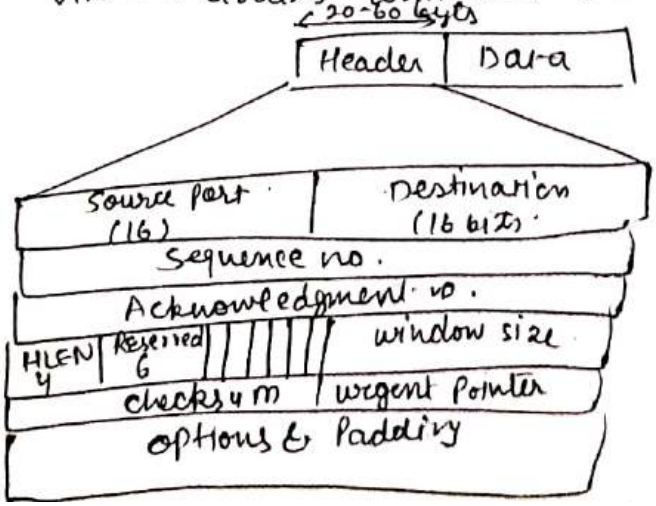
Broadcast (one to all)



Multicast (one to several



2. TCP – Transmission control protocol.
   connection oriented
   virtual circuits connected the sender & Reciever



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

IPV4 address

- 32 bit address uniquely & universally Defines conection 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 usse 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 value (0, 1) & N bits can have 2^N values

IPv4 notations

1. Binary

32 bit/4 byte
Octet → byte

EX: 01110101 10010101
00011101 00000010

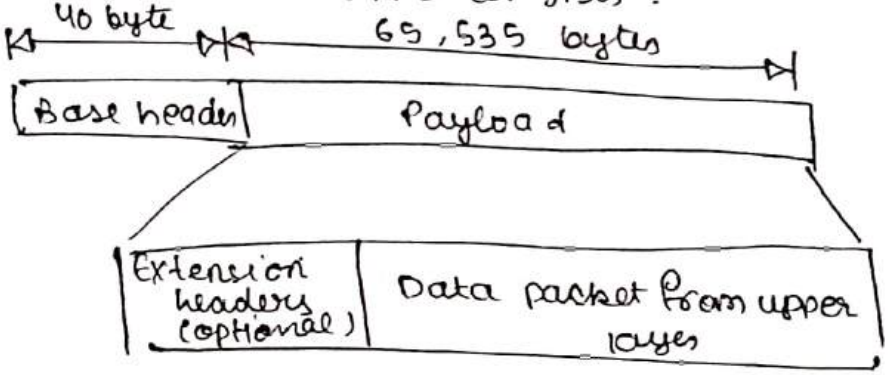
2. Dotted Decimal.

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 problim in interner
  → 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.
#	Secure 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 hong.
- 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 amount of Data that can be transmitted

Types of dialog contro < 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 Erross If error paya jata hai to SL action leti hai.

Firewalls

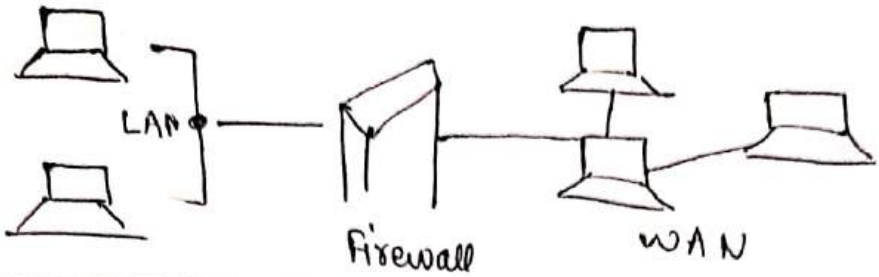
→ Security devices monitor & control network traffic based on predetermined security policies.

→ 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 me~~ communicating Devices, to monitor control of flow

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

Advantas of firewall

1) Security
2) Prevention
3) control of network acess
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 world 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

↓

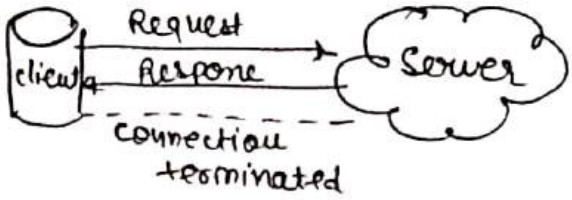
Browser send Req to server

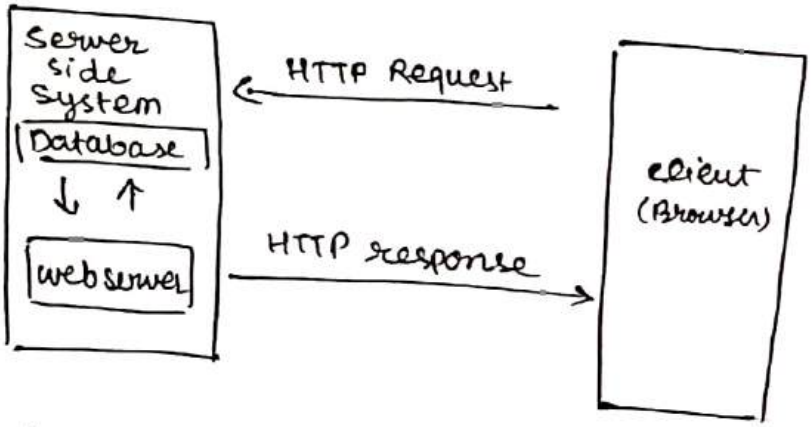
↓

Server send data

↓

connection closed





FTP (file transfer protocol)

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

Client contacts FTP server

↓

Obtain authorization

↓

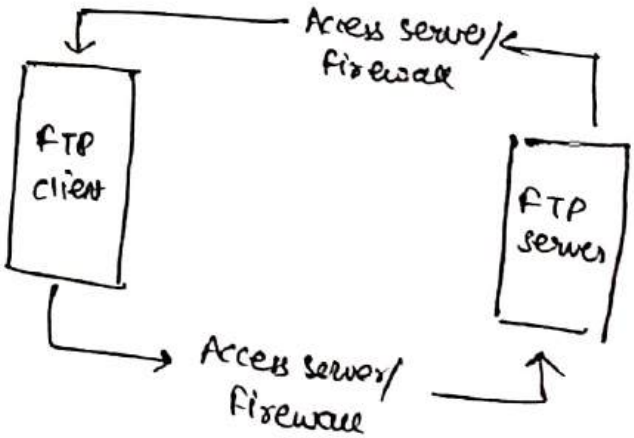
Browse Remote directory

↓

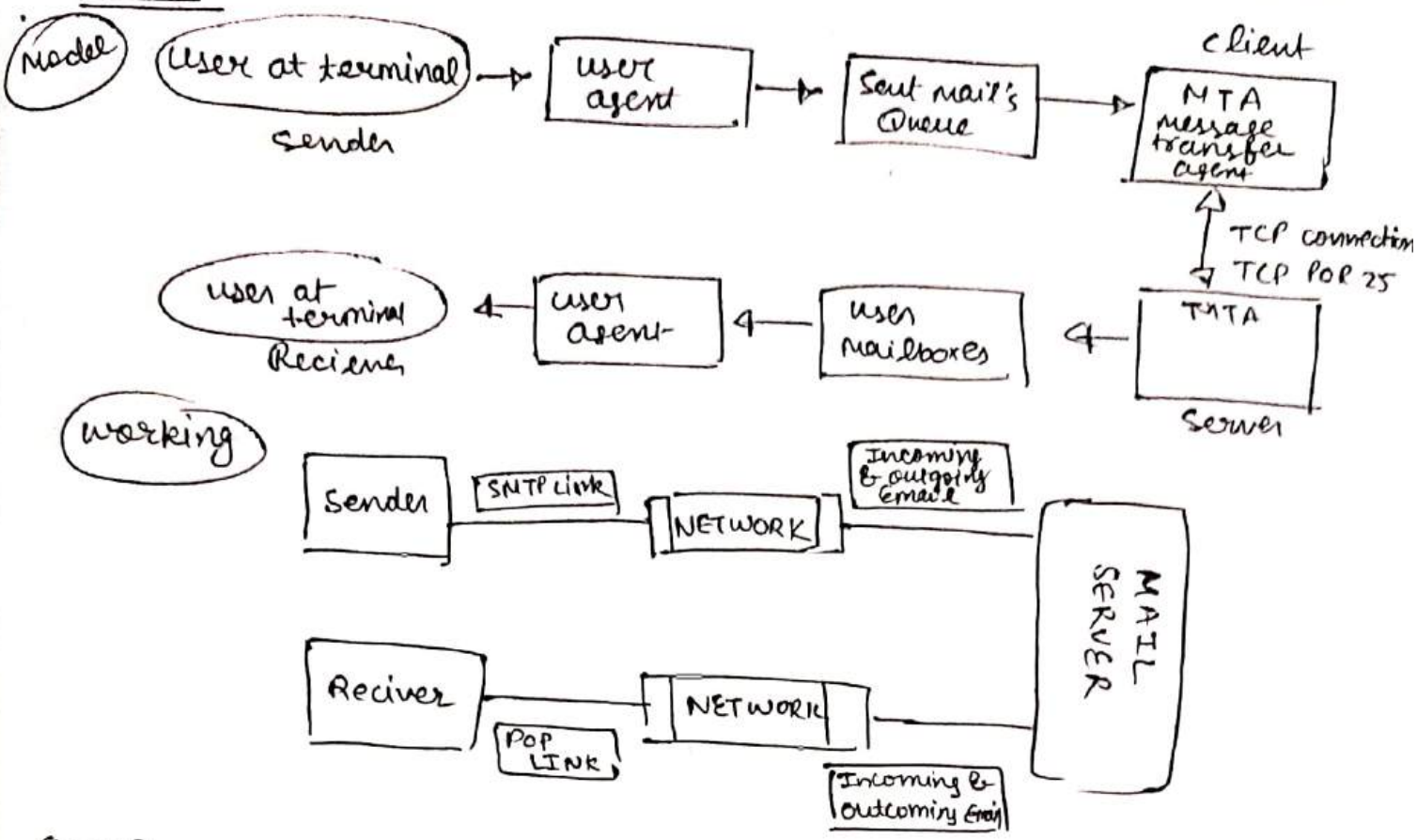
Server Recieves a command

↓

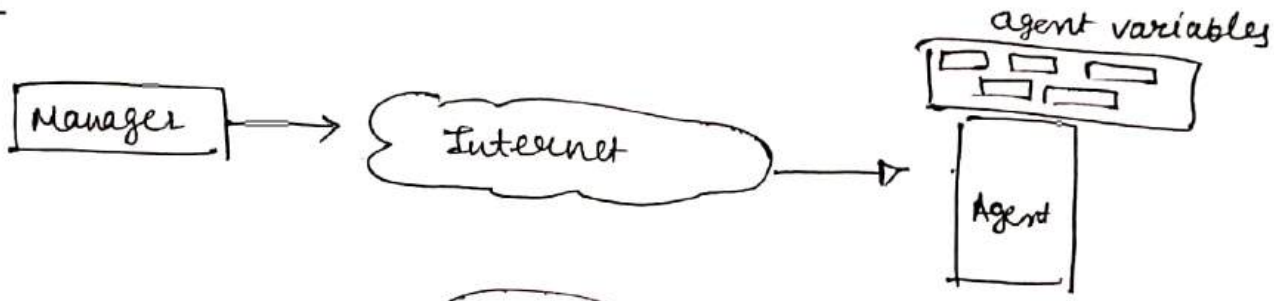
after transferiny server close connection

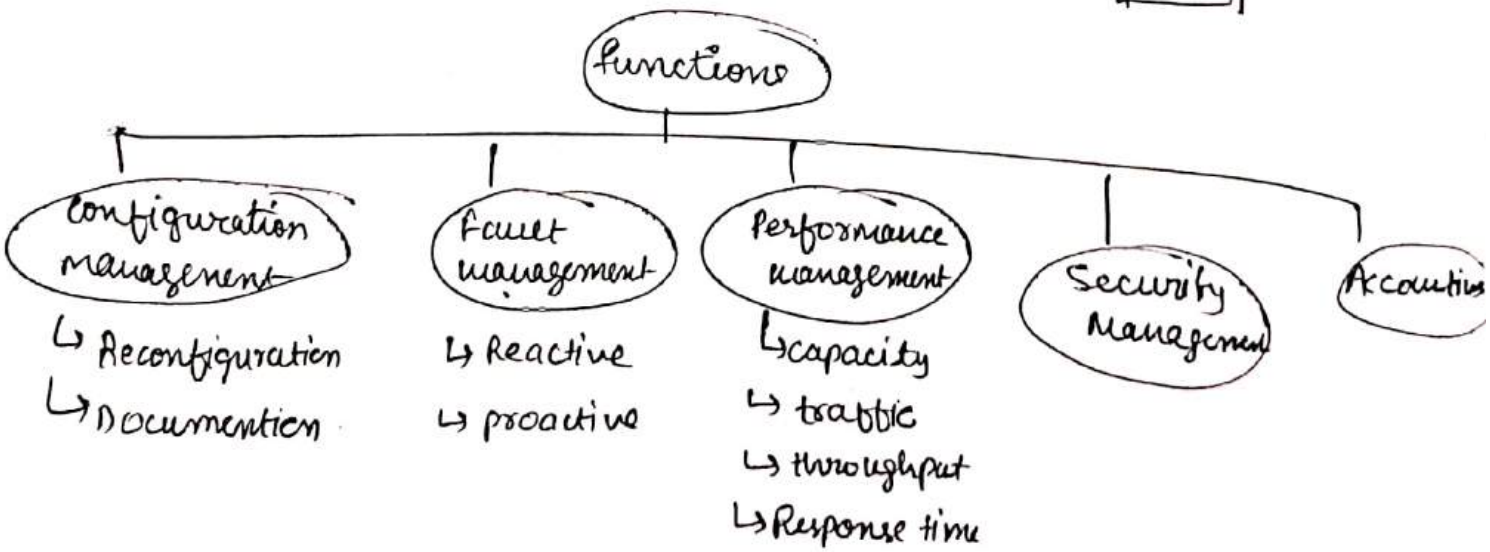


SMTP



SNMP





- CNIP

IPv4 ?

Internet protocol version 4 → primary version
brought into action for production ARPANET in 1983

32 bit addresses are 32-bit integers, Expressed in Decimal notation.

Parts of IPv4.

1) Network part: distinctive variety appointed to network
Conjoinly identifies category of network assigned.

2) Host part - uniquely identifies the machine on network.
assigned to every host

3) Subnet number - non-obligatory part of IPv4
local networks that have massive no. of host are divided into subnets and subnet no's are appointed to it.

Characteristic -

1) 32-Bit IP address
2) numeric, & seprated by a dot.
3) header fields → twelve
no. of
length of header field = 20
4) unicast, broadcast & multicast style of address
5) support virtual length subnet Mask

advantage

- permits encryption.
- Network allocation significant.
- Easy to attach to multiple devices
- Quality service
- redefined & permit flawless coding.

limitations

- Each network unique IP address
- complex.

- IPV6 - most common version of Internet protocol.
  - ↳ Internet protocol version 6.
  - ↳ Designed by Internet Engineering task force (IETF)

Types of IPV6 address.

Unicast	Multicast	Anycast
only one interface is specified by unicast. Packet moves from one host to destination host	represent a group of IP devices & can only be used as destination of datagram	same as multicast anycast address varies from other addresses it can deliver the same IP address to several servers or devices.

Advantages

- Routing Efficiency
- Reliability
- allocates address on its own.
- Security.
- faster
- stronger
- simple aggregation

Disadvantages

- conversion (long period.
- communication.
- cross protocol

IPV6	IPV4
128 bit address	32-bit address
hexadecimal	Decimal → Add. representation
header → 40 bytes	Header → 20-60 Bytes.
Checksum field not avilable	avilable
doesn't support VLSM	support VLSM.

Congestion control

↳ happen because of availability of many packets in network.

Effects ↳ decreases network performance.
↳ Packet delivery to reciver is delayed
(Packet loss)

Congestion control algo -

↳ Mechanism which control the entry of data packets into network, Enable a better use of shared network infrastructure & avoid congestive collapse.

- Used for shaping trafic
- Used to control the Rate at which traffic is sent to network, shape the brust traffic

Algorithm -

Each network interface ke pass leaky Bucket hoti hai

1. jab host packet send karta hai, to packet throw karte hai Bucket mei
2. Bucket leak karti hai constant Rate pe, meaning → network transmit packets at constant Rate
3. Brusty traffic → uniform.
4. Bucket → finite que bn jayega jo output dega finite rate pe.

Leaky Bucket algo kabhi-kabhi Disadvantage De deti hai, because agr kabhi boht jyada value mei Packets aae in the network tb bhi Ek particular value mein flow jayega jiski vjh se problem hogi.

is algo mei bucket ~~or~~ tokens contain karti hai. Each token define karta hai packet jo ki Ek predetermined size ka hota hai. Token delete kie jate hai buckets mi'n se acc to ability to share Packet

algo steps -

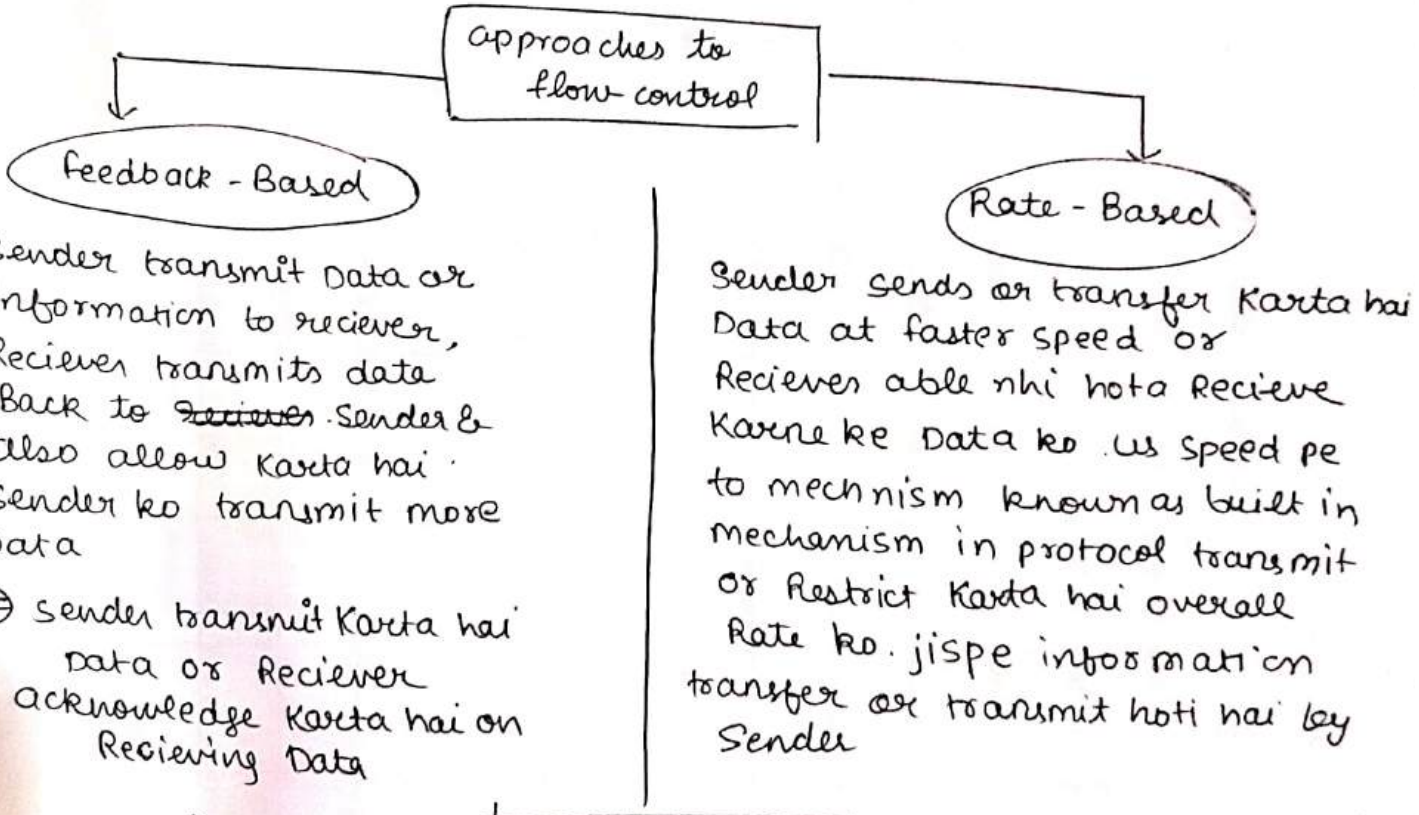
1. Regular interval mei throw karenge packet.
2. Bucket ki Max Capacity hogi.
3. agr packet Ready to sent hai, to token Remove karenge Bucket se or Packet Send karenge.
4. agr Bucket mei koi ~~packet~~ token nhi hai to ~~to[illegible]~~ Packet send nhi hoga

Flow control -

↳ a technique that gives permission to two of stations (Sender & Reciever) that are working to just communicate to one another.

↳ It Restricts & cordinates number of frames or amount of Data Sender can send. just before it waits for an acknowledgement.

↳ Set of procedures. jo Explain Karte hai, Sender Kitna ~~da~~ frames of Data transfer or trasmit Kar skte before Data overwhelms reciever.



Firewall -

- ↳ Network Security Device
- ↳ Monitors both incoming & outgoing traffic using Predefined set of Security
- ↳ Protective Barrier

Set of security Rules

- Accept → allow the traffic
- Reject → Block the traffic but reply with an "unreachable Error"
- Drop → Block the traffic with no reply.

working -

1. Packet Inspection → when data packets travel b/w networks, firewall Examine karta hai source & other attributes to determine security criteria meet kar rhe hai ya nhi
2. Filtering - compares the packet info with set of Rules agr match ho jata hai, allow to Pass otherwise Reject.
3. Access control - Block & unauthorized access attempts
4. Network access translation - hides internal IP address of devices, add Extra layer of Security by making it Difficult for attackers to directly target.
5. Logging & Monitoring - Keeps a record of all Network traffic & Events. Generate logs & alerts to notify administrators about potential security threats.

HTTP

↳ used for communication b/w web browser & web server.
↳ allows transfer of hypertext documents, such as webpage

(working) → type a website url, it send an Http request server process karta hai Request ko & send Back an Http response jo ki contain karta hai requested web, or wo display ho jata hai

SMTP → Simple mail transfer Protocol

- Protcol used for sending & Recieving Email messages.
- allow the transfer emails b/w mail server & internet

(working) - send an Email, client used Smtp to send message to recipient's mail server.
or uske Baad Smpt use hota hai reciver ke dwara to deliver email to recipient mail box.

FTP → File transfer protocol

↳ used for transferring files.
↳ Enable uploading, downloading, managging files on Remote server.

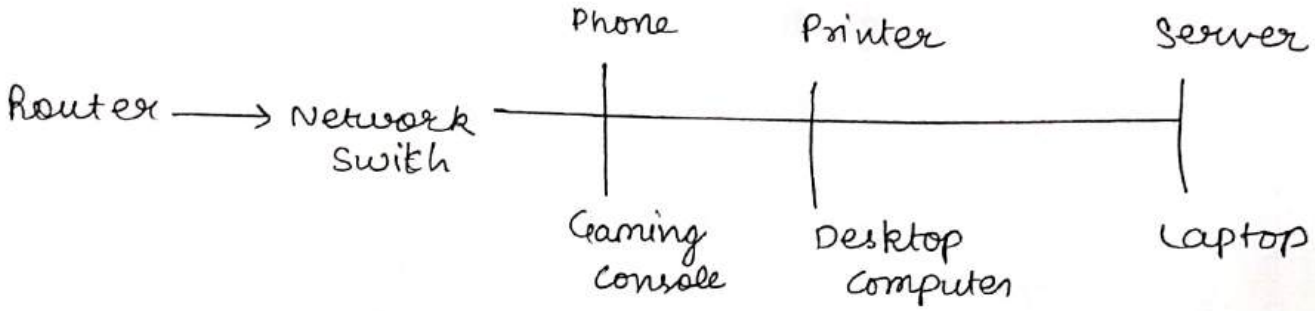
(working) - connect to Remote Server, authenticate karo khud ko, browse directories → transfer file

Switching -

- ↳ process of transfering Data packets from one device to another using specific devices → switches.
  ↳ take place at Data link layer of OSI Model.

Network switching -

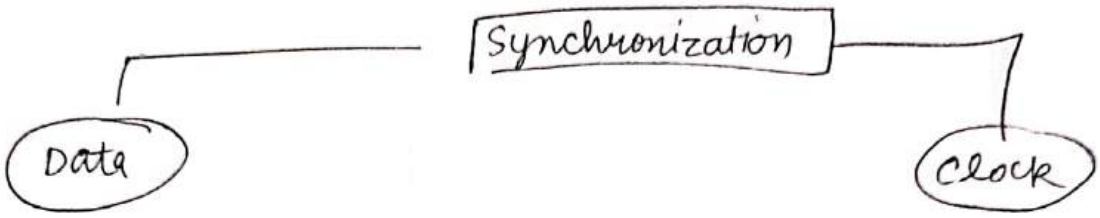
↳ Dedicated piece of computer hardware (incoming Data packets & tranfering them to Destination)



Synchronization

↳ cordination of Data Exchange b/w different devices or Systems.

↳ Ensure Data is transmitted & Recived correctly without Errors or collisions



Keep multiple copies of Data consistent across different location.

File

↳ Replication, mirroring & versioning technique

Database

↳ update Insert, deletions Replication.

Data transfer relies on precise timing. network device use karta hai synchronized clocks to ensure ke Data packets arrive ho correct order mein or Expected time pe.

↳ Global clock – accurate Event logging, transaction Sequencing.

↳ Network time protocol distribute time info to clients.

↳ precision time protocol high accuracy application

Routing algorithms -

- ↳ to Determine Best path for data travel from Source to destination
  - ↳ Find (shortest) & most Efficient paths for Data transmission.

① Shortest path -

1. Start at source node
2. Initilize shortest Distance to all other nodes as infinity.
3. Explore neighboring nodes & update shortest distance if shorter path found
4. Continue Exploring & updating distance until all nods have been visited
5. Select shortest path

② Distance vector

① Har node maintain Karega Routing table jo wo store Karegi shortest distance to other nodes

② Nodes Exchange Karengi Routing tables with neighbouring node.

③ jo Routing table recieve hoti hai, Each node update Karegi Routing table ko by considering shortest path

④ Process continue until all nodes have consistent Routing tables

③ Link State Routing algo -

① Har node gather Karegi info about its directly connected links, include State & cost.

② Node info Exchange Karengi other nodes ke sath network mein

③ Receive the link state information from all nodes & construct Network map.

④ Each node calculate shortest path to other using Dijikstra's

⑤ update Routing table calculate shortest paths

Design issue →

- ① Reliability → Data is delivered accuractely in correct order Even if there are Errors

② Flow control → Rate of Data transmission.

③ ~~Cog~~ Congestion control → Peeche jake Padho

④ Multiplexing → Allow Bohut sare application or services to use same network connection sath mein

⑤ Error Detection & correction →

⑥ Performance → minimize Delay, latency & overhead

⑦ Connection Establishment & termination –
Managing the setup & teardown of connection b/w sender & Reciever.