CSA 07 – COMPUTER NETWORKS

PHYSICAL LAYER AND MEDIA

- Introduction to Networks and Communication Media
- Network Hardware
- Network Software
- Components and Categories
- Types of Connections
- Topologies
- Protocols and Standards
- ISO / OSI model - Reference Models.
- Basis for data communication
- Transmission Media
- Wireless Transmission
- Ethernet Interface and Configuration

DATA LINK LAYER

- Error Detection and Correction
- Data Link Control,
- Multiple Access
- Wired/Wireless LAN
- Connecting LANs
- Backbone Networks
- Wireless LANs – 802.11
- Bluetooth and Wireless WANs
- Virtual-Circuit Networks
- Frame Relay ATM and MPLS.

NETWORK LAYER

- Packet Switching and Datagram approach
- IPv4 addressing methods
- Subnetting
- Routing
- Distance Vector Routing
- Link State Routing
- Multicast
- ICMP
- IPv6 addresses
- Internetworking

TRANSPORT LAYER

- Duties of transport layer
- Multiplexing
- DE multiplexing
- TCP Sockets
- User Datagram Protocol (UDP),
- Multicast
- Transmission Control Protocol (TCP)
- Congestion Control
- Quality of services (QOS)
- Queuing Analysis
- Priority Queues
- Network of Queues
- Congestion and Traffic Management

APPLICATION LAYER

- Domain Name Space (DNS)
- SMTP
- FTP
- HTTP
- Electronic Mail
- POP - SNMP – P2P
- Communication, VOIP
- Overlay Network
- SSL Security, firewalls, DoS, etc.

PHYSICAL LAYER AND MEDIA

Networks and Communication Media
- Data Communication
- Components and Categories

Network Hardware
- Bridge
- Switch
- Router
- Repeater

Network Software
- API

Types of Connections
- Point to Point
- Multipoint

Protocols and Standards
- Elements of Protocols
- Standards in Network

Basis for data communication
- Simplex
- Half Duplex
- Full Duplex

Topologies
- Bus
- Ring
- Star
- Mesh
- Tree
- Hybrid

ISO / OSI model - Reference Models.
- Physical
- Datalink
- Network
- Transport
- Session
- Presentation
- Application

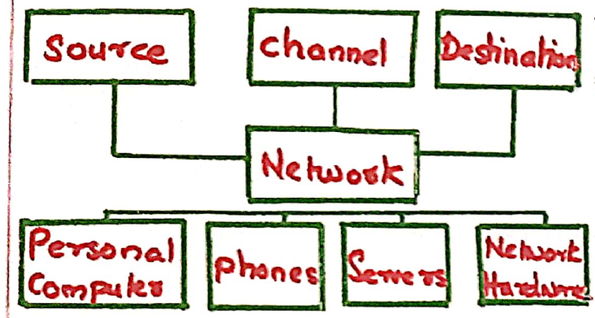
Transmission Media
- Guided
  - Twisted
  - Coaxial
  - Fiber Optics
- Unguided
  - Microwave
  - Radiowave
  - Infrared

Ethernet Interface and Configuration
- Standard
- Goals
- Interface
- Configuration

Network & Communication

Group of computers/ devices to exchange data

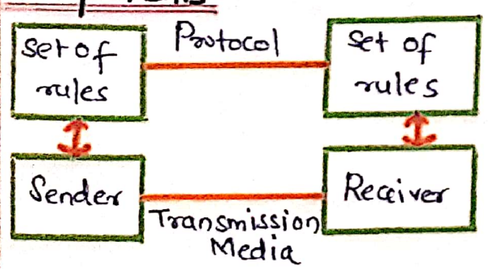
Network computer Devices



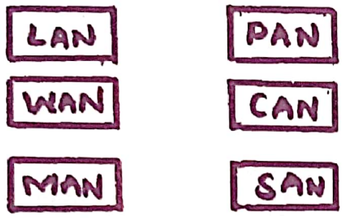
Data Communication

- Process of exchanging data characteristics:
  - * Delivery
  - * Accuracy
  - * Timelines
  - * Jitter

Components



Categories of Network



Network Hardware

* NIC - Network Interface Card
* Provides connections between Computers and network.

Bridge

→ connects LAN to another LAN that uses the same protocol.

Switch

→ Joins multiple computers together with LAN

Router

→ Analyse the upcoming packets
→ Move the packets to another network.

Repeater

→ Regenerates incoming signals

Network Software

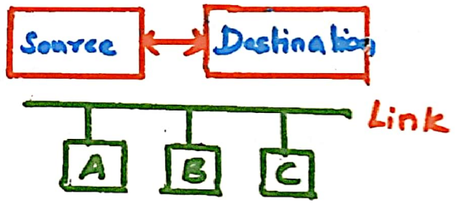
→ Implement protocols as a part of OS
→ Exports the network functionality
→ API
→ Application programming Interface.

API functions

→ create sockets
→ Attach socket
→ send/receive
→ close the socket

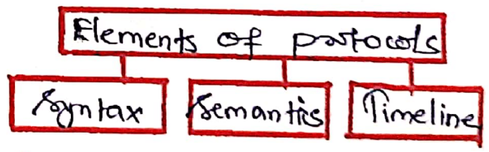
Types of Connection

→ point to point
  * dedicated link
→ Multi-point link
  * share a common link



Protocols

→ set of rules that determine how data to be transmitted



Standards in Networking

→ standards provide guide-lines to product vendors
→ de-fact : Not approved by any organized bodies
→ De-jure : approved by a body that is officially recognized.

Example of standard organisations

* ISO
* ITU-T
* ANSI
* IEEE
* EIA

Example Forum

* ATN
* MPLS
* Frame Relay

Basis of data communications

Media < Wired / Wireless

Direction of dataflow

Simplex

Half-duplex

Full-duplex

TOPOLOGY

→ Arrangement of network nodes and lines

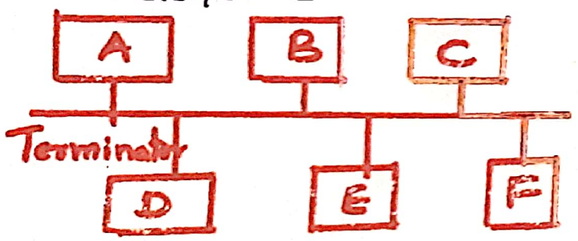
Types

* Bus
* Ring
* Star
* Mesh
* Tree

Bus Topology

→ All devices share single line

→ Use CSMA/CD. (or) Master/slave



Advantages:

→ Bus topology is simple to configure

→ If N devices are connected to each other

* Cable - 1
* drop lines - (N-1)

Limitations:

→ when the traffic is heavy Collision occurs

→ If the cable fails entire network fails/crash

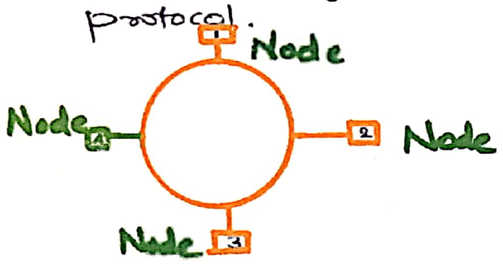
Ring Topology

→ forms a ring connecting devices

→ Two neighboring devices

→ Transmission may be unidirectional / bidirectional

→ Use Token ring passing protocol.



→ for N devices in a network N cables are required.

Advantages

→ possibility of collision is minimum

→ cost effective

→ scalability

Limitations

→ Troubleshooting is difficult

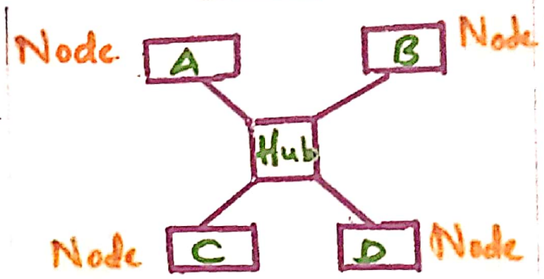
→ Less security

Star Topology

→ All devices are connected to a single hub

→ Hybrid topology

* combination of all Topologies



Advantages:

→ Each device requires only one port

→ for N devices cables are required (ie) N

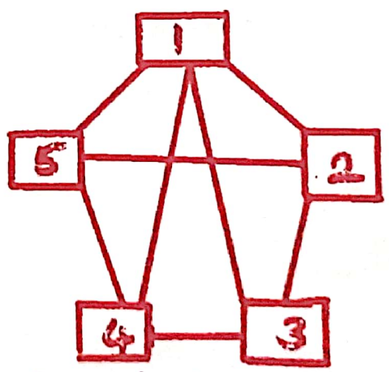
Disadvantages:

→ High cost

→ If hub fails then the entire network fails.

Mesh Topology

→ Every device is connected to another device



→ If N devices are connected with each other.

→ Number of port required by each device is (N-1)

→ Total number of ports = N(N-1)

→ If N devices are used

→ Number of dedicated links $NC_2 = N(N-1)/2$

eg:

→ If the number of devices in the network = 5

The links required = $\frac{5(5-1)}{2} = 10$

Advantages:

→ provides security & privacy

→ fault diagonosis is easy.

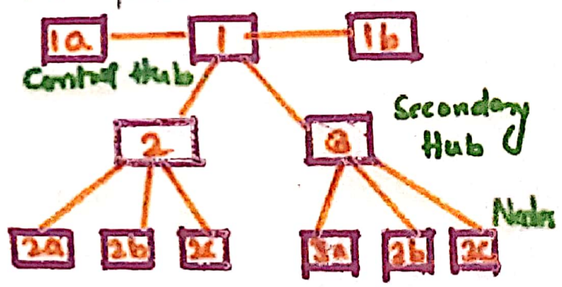
Disadvantages:

→ High Maintenance cost

→ Installation and Configuration is difficult

Tree Topology

→ It follows hierarchy



Advantages:

→ allows more devices to connect

→ allows to get isolated

Disadvantages:

→ High cable cost

OSI Model - TCP/IP REFERENCE MODEL

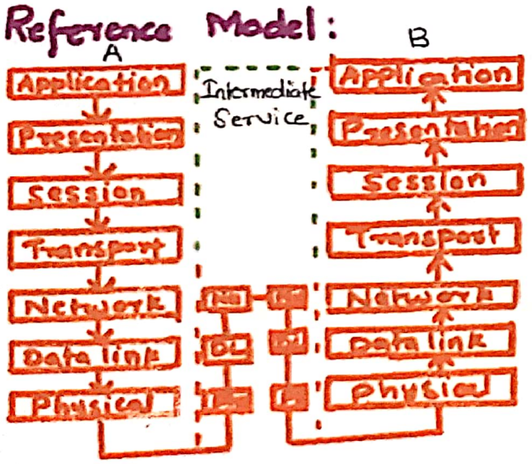
OSI Model:

→ open System interconnection
→ Conceptual Model
→ Layered Approach
→ Internal functions of communication.

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Datalink layer
- Physical Layer

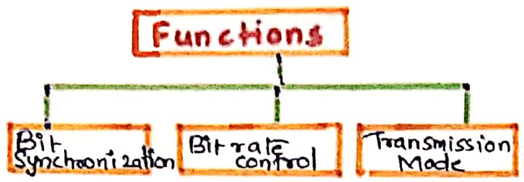
Software Layer (Application, Presentation, Session)
Heart of OSI (Transport)
Hardware Layer (Network, Datalink, Physical)

Reference Model:



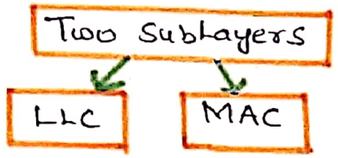
Physical Layer:

→ Connection between devices



Data Link Layer

→ node to node delivery



Function:

→ Framing
→ physical Addressing
→ Flow control
→ Access control

Network Layer:

→ Host-to-Host Connection

Functions:

→ Routing
→ Logical Addressing

Transport Layer:

→ process to process Communication
→ retransmit data if an error
→ Segmentation and reassembly

Session Layer

→ Maintanence of Session

Functions:

→ Synchronization
→ Dialog controler

Presentation Layer:

→ Encryption/Decryption
→ Compression

Application Layer:

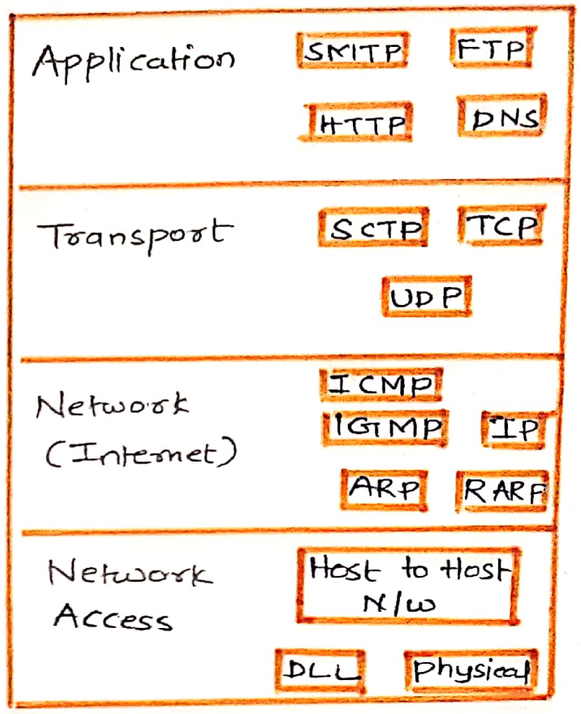
→ Service to service communication

Functions:

→ Virtual Terminal
→ Mail Services
→ Delivery Services

TCP/IP

→ control protocol with Internet protocol
→ It contains four layers
  * Application Layer
  * Transport Layer
  * Internet Layer
  * Network Access layer
→ It is more reliable
→ TCP/IP follows a horizontal approach
→ It refers to Transmission Control protocol



* Connection oriented

IP protocol

* IP addressing
* Host-to-Host communication
* Data Encapsulation and formatting
* Fragmentation and Reassembly
* Routing

TCP

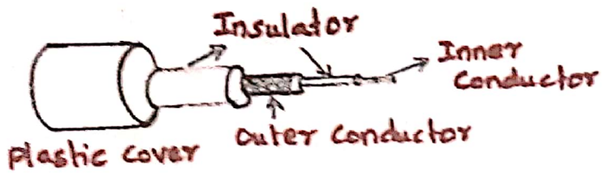
* virtual circuit between Sender and Receiver
* It ensure acknowledgement received all segments

Transmission Media & Ethernet Standard

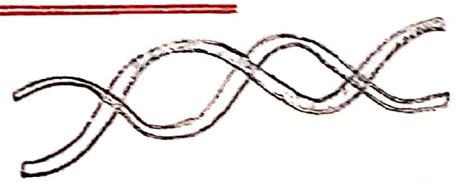
Guided Media

Coaxial Cable:

- Higher frequency Range
- 10/100/1000 Mbps.
- 100 KHz to 500 MHz
- Baseband - 50 ohm
- Television - 70 ohm



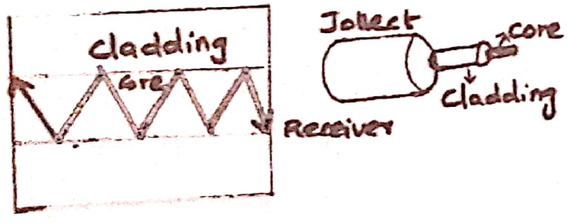
Twisted Pair:



- 100 Hz to 5 MHz.
- Connector RJ45.
- 100 Mbps.

Fiber Optic:

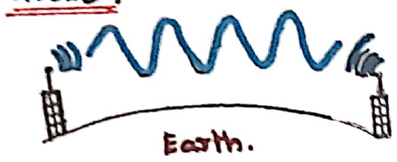
- Light Beam
- Made of Glass
- Fast transmission
- Data rate 1000 Mbps & more



UnGuided Media:

- Not directional: air, space, etc.,
- No physical link.
- Established devices.

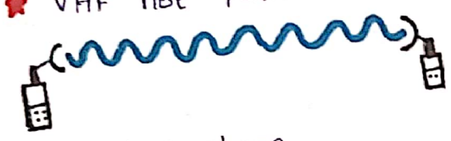
Radio:



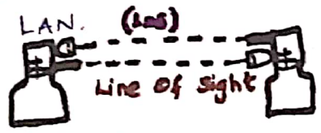
- Large Wavelength
- Frequency range: 3Hz to 300 HZ upto 1 GHz.

Microwave:

- Electromagnetic Waves
- Frequency 1 and 300 GHz.
- Uni directional.
- VHF not penatrate the walls



- Cellular phone
- Satellite Network.
- Wireless LAN.

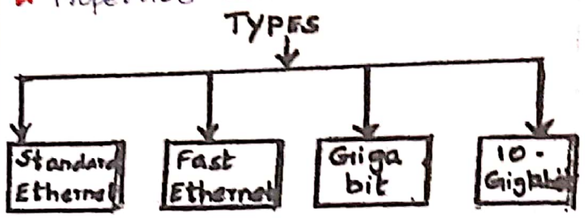


Infrared:

- Visible light Spectrum
- Microwave
- Frequency range 300GHz to 430 THz.
- Wavelength 700 nm to 1mm.
- Laser Works (Transmitter) - red beam.
- Works photo Detectors
- very high data rate

Ethernet Standard:

- Properties and Functions



Standard Ethernet:

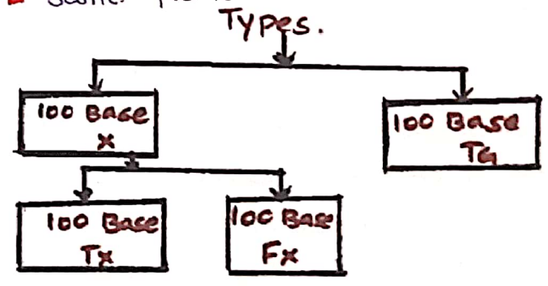
- Data rate 10 Mbps
- 10 Base 5 - Thick
- 10 Base 2 - Thin
- 10 Base T - star UTP.
- 10 Base F - Star Fiber.

Fast Ethernet:

- IEEE 802.3U
- Higher transmission Speed
  - MAC layer
  - Physical Layer

Goals:

- 100 Mbps data rate
- 48 bit address
- Same frame.



Giga bit:

- Transmit Higher data rate
- 1 Billion bits per sec.
- Maximum length: 25 meters.

- IEEE 802.3z Standard
- Segment Length 220 - 550m

Ethernet Interface:

- Circuit based connections
- Configuring network Interface
- Assigning Ip address

Ip Config. - Mode:

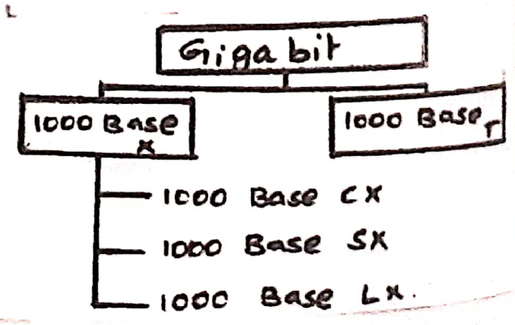
- Identifier configuration Mode.

Ip Route:

- Manage static routers

Ip Secondary Address:

- Manage secondary Network address
- Hardware dependent values
- Specific N/w interface
- Bind Address
- Used as a Source Ip address
- The IP address and subnet Mask.



DATALINK LAYER

Error Detection

- Types of Error
  - Single Error
  - Burst Error
- Error Detecting Codes
  - Parity
  - Check Sum
  - Cyclic Redundancy Code (CRC)
- Error Correction
  - Hamming Code illustration

Data Link Control

- Line Discipline
- Flow Control
  - Sliding Window
  - Stop and Wait
- Error Control
  - Sliding Window
  - Stop and Wait Window
  - Select / Reject Window

Multiple Access Protocol

- Random Access Protocol
- Aloha
  - Pure Aloha
  - Slotted Aloha
- Carrier Sense Multiple Access
  - I – Persistent
  - Non – Persistent
  - P – Persistent
  - O – Persistent
- Channelization Protocol
  - TDMA
  - FDMA
  - CDMA

Wired/Wireless LAN

- Connecting LANs
- Backbone Networks

Wireless LANs – 802.11

- Architecture
- MAC Layer
- Hidden Station Problem
- Physical Media

Bluetooth and Wireless WANs

- Bluetooth
- Wireless WANs
- Virtual-Circuit Networks
- Frame Relay
  - Architecture
  - PVC
  - SVC
  - Frame Format
- ATM

MPLS

ERROR DETECTION AND CORRECTION

→ Single bit error : Only one bit corrupted

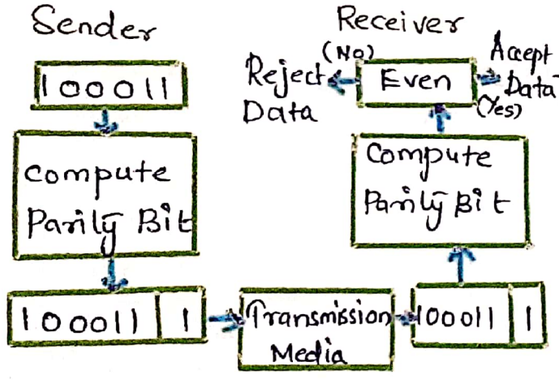
→ Multiple bit error: More than one bit corrupted

→ Burst error: More than one consecutive bit corrupted

Error Detection Techniques

→ parity check, check sum, cyclic Redundancy check (CRC)

Simple parity check



* 1 Added if odd number of 1's
* 0 Added if even number of 1's

Check Sum

→ DATA → divide into k segments

→ Segments Added

→ sum complemented (checksum)

→ checksum segment along with data segment

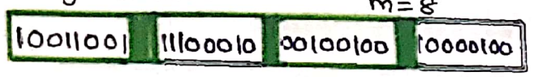
→ All receive segment added

→ Sum complemented

→ 0 - Accepted else rejected

original data

k=4
m=8



Sender	Receiver
10011001	10011001
11100010	11100010
01111011	01111011
1	1
01111100	01111100
00100100	00100100
10100000	10100000
10000100	10000100
00100100	00100100
1	1
00100101 Sum	00100101
11011010	11011010
checksum	11111111 (Sum)
	00000000 (Complement)

Accept Data

Note:

If the result is zero, the received data is accepted otherwise discarded.

CYCLIC REDUNDANCY CHECK

CRC - Sender

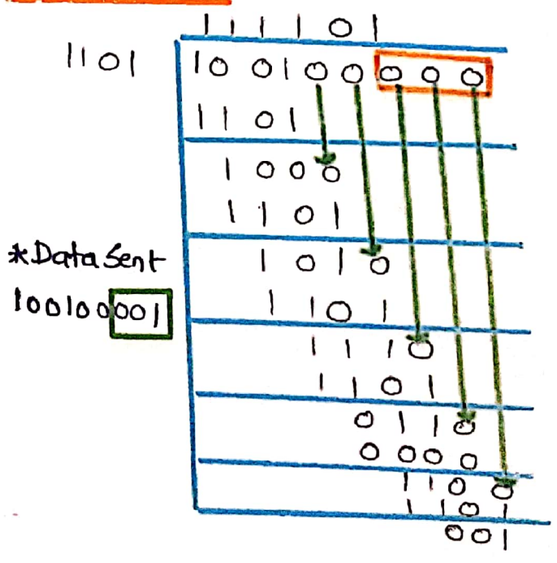
* Generate polynomial G(x)
* k - number of bits in G(x)
* Append k-1 zeros no data
* Perform binary division
* Append remainder to data

CRC - Receiver

* Perform binary division
* Remainder
  * zero - no error
  * non zero - error

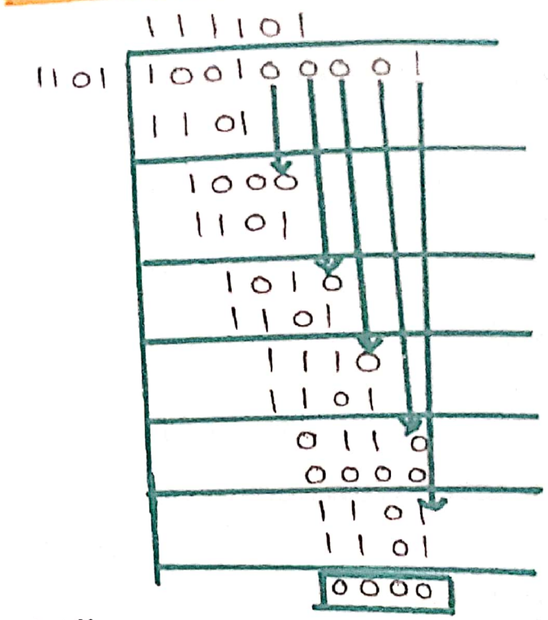
* Data - 100100
* G(x) = 1101

CRC - Sender



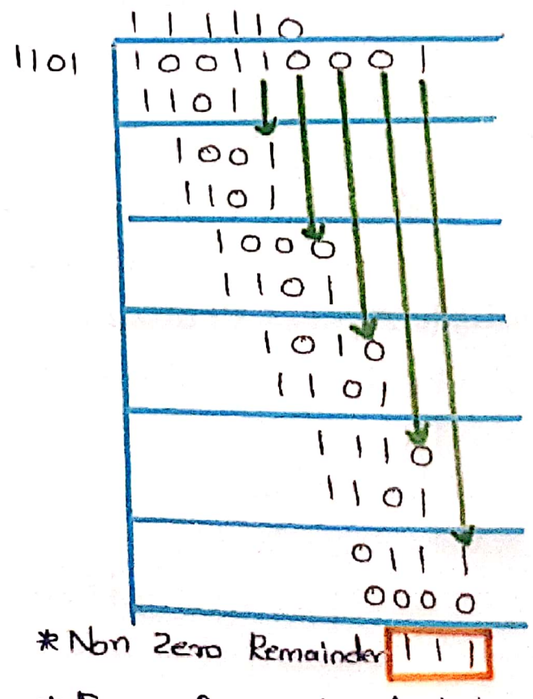
*Data Sent
100100001

CRC Receiver - No error



* All zeros - no errors

CRC - Receiver - With error



* Non zero Remainder 111
* Error in received data

HAMMING CODE

HAMMING CODE – ILLUSTRATION

DATA → 1010

TOTAL NUMBER OF DATABASE $d = 4$

NUMBER OF REDUNDANT BITS r :-

$$2^r >= d + r + 1$$

LET $r = 3$; $8 = 4 + 3 + 1$

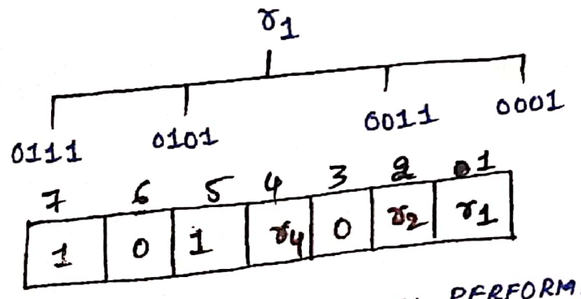
$\therefore r = 3$

TOTAL NUMBER OF BITS $= d + r = 4 + 3 = 7$

THE THREE BITS ARE REPRESENTED BY r_1, r_2, r_4 their CORRESPONDING POSITION ARE $1, 2^1, 2^2$

r_1 r_2 r_4

DETERMINING r_1 BITS :-



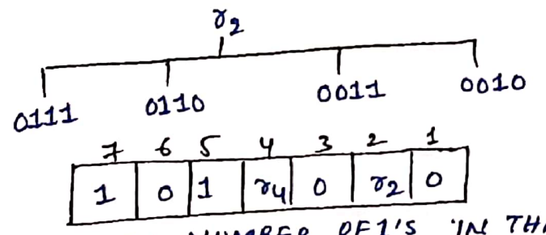
r_1 IS CALCULATED BY PERFORMING A PARITY CHECK ON THE BIT POSITIONS WHOSE BINARY REPRESENTATION INCLUDES 1 IN THE FIRST POSITION.

THE TOTAL NUMBER OF 1 AT THESE BIT POSITIONS (1,3,5,7) IS EVEN

$\therefore \boxed{r_1 = 0}$

DETERMING r_2 BIT :-

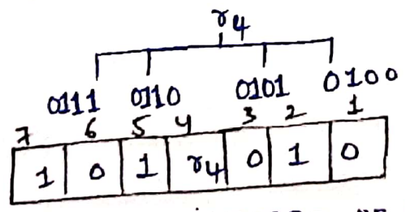
r_2 BIT IS CALCULATED BY PERFORMING A PARITY CHECK ON THE BIT POSITIONS WHOSE BINARY REPRESENTATION INCLUDE 1 IN THE SECOND POSITION.



THE TOTAL NUMBER OF 1's IN THE BIT POSITION (2,3,6,7) IS ODD, SO AS TO ENSURE EVEN PARITY, $r_2 = 1$ $\boxed{r_2 = 1}$

DETERMINING r_4 BIT :-

r_4 IS CALCULATED BY PERFORMING A PARITY CHECK ON THE BIT POSITIONS WHOSE BINARY REPRESENTATION INCLUDES 1 IN THE THIRD POSITION



THE TOTAL NUMBER OF 1's (4,5,6,7) IS EVEN : $\boxed{r_4 = 0}$

DATA SENT :-

1	0	1	0	0	1	0

RECEIVER SIDE :-

ONE ERROR OCCURED.

4th BIT IS CHANGED.

r_1 :- 1 0 1 (1) 0 1 0

7	6	5	4	3	2	1
1	0	1	1	0	1	0

→ 1,3,5,7 → 0 0 1 1 → even

$\therefore r_1 = 0$

r_2 :-

7	6	5	4	3	2	1
1	0	1	1	0	1	0

→ 7,6,3,2 → 1001 → even

$\therefore r_2 = 0$

r_4 :-

7	6	5	4	3	2	1
1	0	1	1	0	1	0

7 6 5 4 → 1 0 1 1 → odd

$\therefore r_4 = 1$

THE REDUNDANT BITS ARE r_4, r_2, r_1

⇒ 100 ⇒ DECIMAL VALUE → 4

THEREFORE THE ERROR IS IN 4th BIT POSITION . THE VALUE TO BE CHANGED TO CORRECT THE ERRORS.

DATA LINK CONTROL
(RELIABLE DATA TRANSFER OVER THE PHYSICAL MEDIUM)

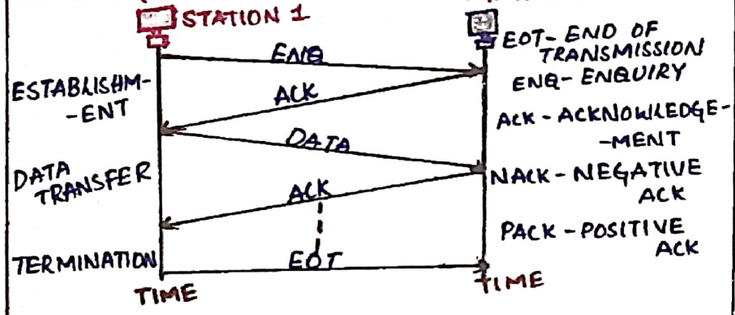
- **LINE DISCIPLINE** — WHO SHOULD SEND THE DATA?
- **FLOW CONTROL** — HOW MUCH DATA SHOULD BE SENT?
- **ERROR CONTROL** — HOW CAN ERRORS CAN BE DETECTED AND CORRECTED

SERVICES
- FRAMING & LINK ACCESS
- RELIABLE DELIVERY
- FLOW CONTROL
- ERROR CONTROL
- ERROR CORRECTION
- HALF DUPLEX & FULL DUPLEX

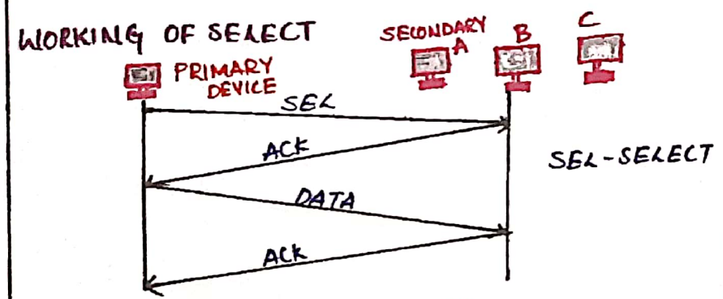
LINE DISCIPLINE

END/ACK — POLL/SELECT

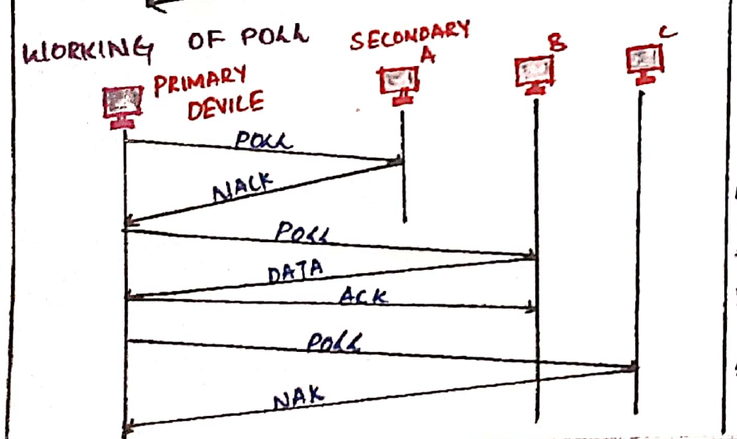
WORKING OF END/ACK



WORKING OF SELECT



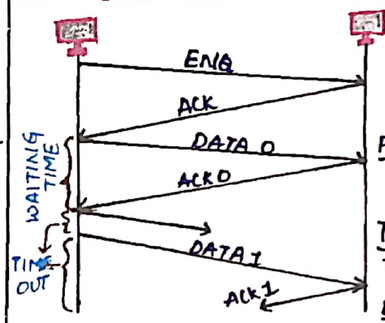
WORKING OF POLL



FLOW CONTROL

STOP AND WAIT — SLIDING WINDOW

STOP AND WAIT



TRANSMISSION DELAY
$T_d = \frac{D}{B} = \frac{\text{Datasize}}{\text{Bandwidth}}$

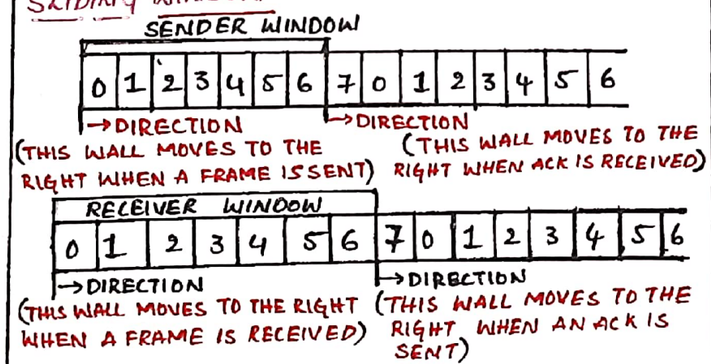
PROPAGATION DELAY
$T_p = \frac{d}{S} = \frac{\text{Distance}}{\text{Speed}}$

TOTAL TIME
$T_T = T_d + T_p + T_{p\,data+Ack}$

EFFICIENCY:-
$\eta = \frac{T_d}{T_d + (2T_p)} = \frac{\text{USEFUL TIME}}{\text{TOTAL TIME}}$

THROUGHPUT:-
$\eta * B$

SLIDING WINDOW

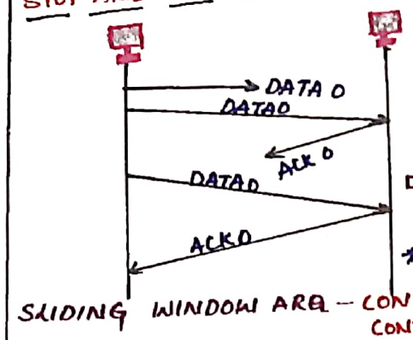


- *SENDER CAN TRANSMIT THE SEVERAL FRAMES WITHOUT ACK.
- *MULTIPLE FRAME CAN BE SENT
- *SINGLE ACK ACKNOWLEDGE MULTIPLE FRAME
- *WINDOW SIZE → MODULO-N If n=8, FRAME = 0,1,2, 3,4,5,6,7,0,1,2,.....
- *MAXIMUM n-1 frame CAN BE SENT BEFORE ACK.

ERROR CONTROL

STOP AND WAIT ARQ — SLIDING WINDOW ARQ
- *Go-Back n
- *SELECTIVE-REJECT

STOP AND WAIT ARQ:-

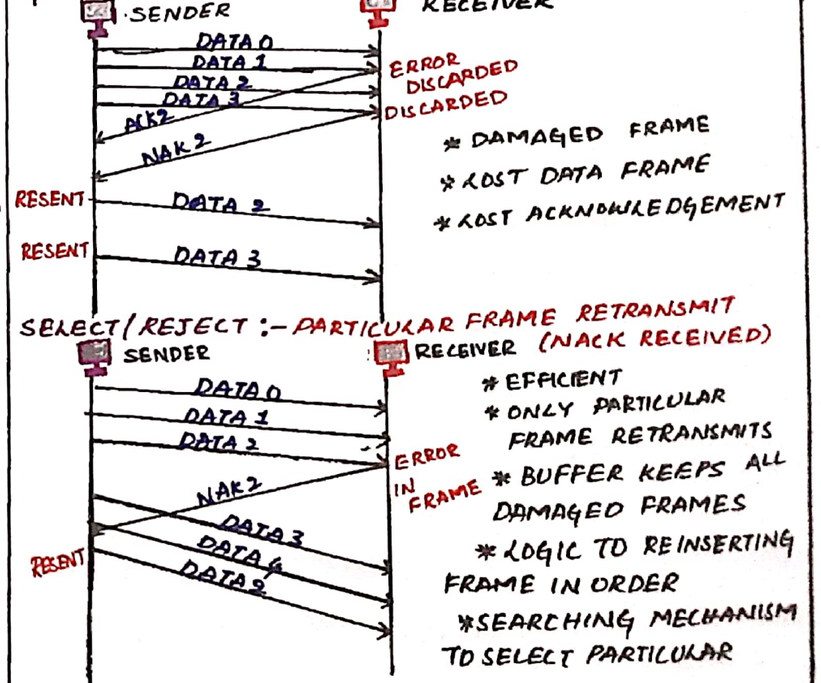


- *DAMAGED FRAME
- *LOST FRAME

DISADVANTAGES:-
- *ONLY ONE PACKET
- *IF $P_f \uparrow, T_p \uparrow, T_p > T_d, \eta \downarrow$

SLIDING WINDOW ARQ — CONTINUOUS TRANSMISSION ERROR CONTROL

Go-Back n — IF ONE FRAME LOST/DAMAGED, RETRANSMITS ALL



- * DAMAGED FRAME
- * LOST DATA FRAME
- * LOST ACKNOWLEDGEMENT

SELECT/REJECT :- PARTICULAR FRAME RETRANSMIT

- * EFFICIENT
- * ONLY PARTICULAR FRAME RETRANSMITS
- * BUFFER KEEPS ALL DAMAGED FRAMES
- * LOGIC TO REINSERTING FRAME IN ORDER
- *SEARCHING MECHANISM TO SELECT PARTICULAR FRAME

MULTIPLE ACCESS PROTOCOLS

- **LOGIC OF DATA CONTROL**
  - DATALINK LAYER
    - LINK
      - * FLOW/ERROR CONTROL
    - MEDIA ACCESS CONTROL
      - * TO REDUCE COLLISION
      - * TO AVOID CROSS TALK
- **RANDOM ACCESS PROTOCOLS**
  - * ALOHA
  - * CSMA
  - * CSMA/CD
  - * CSMA/CA
- **CONTROLLED ACCESS PROTOCOLS**
  - * RESERVATION
  - * POLLING
  - * TOKEN PASSING
- **CHANNALIZATION PROTOCOLS**
  - * FDMA
  - * TDMA
  - * CDMA

RANDOM ACCESS PROTOCOLS

ALL STATIONS HAS THE EQUAL PRIORITY TO SEND THE DATA OVER A CHANNEL.

DISADVANTAGE:- COLLISION (OR) CONFLICT

ALOHA RANDOM ACCESS PROTOCOL

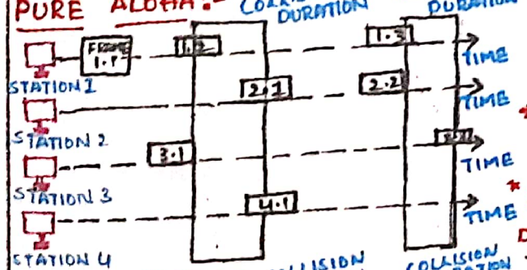
ALOHA RULES:

* ANY STATION CAN TRANSMIT DATA TO A CHANNEL AT ANY TIME
* NO CARRIER SENSING
* COLLISION / DATA LOST MAY OCCUR
* NO COLLISION DETECTION
* RETRANSMISSION OF DATA AFTER SOME RAMDOM AMOUNT OF TIME

TYPES OF ALOHA

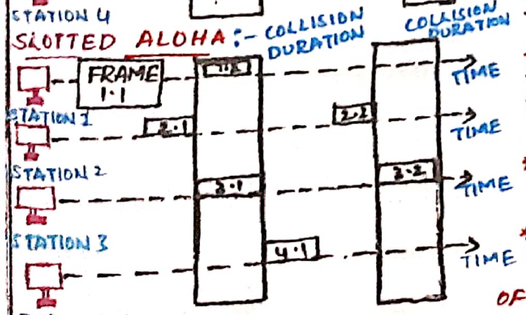
- PURE ALOHA (WITHOUT CHECKING CHANNEL IDLE/NOT)
- SLOTTED ALOHA (FIXED TIME INTERVAL- CHANNEL DIVIDED)

PURE ALOHA:-



* TOTAL VULNERABLE TIME $2 * T_{fr}$
* MAX THROUGHPUT $G = \frac{1}{2}$ 18.4%
* SUCCESSFUL TRANSMISSION OF DATA FRAME $S = G * e^{-2G}$

SLOTTED ALOHA:-



* TOTAL VULUNERABLE TIME T_{fr}
* MAX THROUGHPUT $G = 1$ 37%
* SUCCESSFUL TRANSMISSION OF DATA FRAME

CARRIER SENSE MULTIPLE ACCESS

LISTEN (CARRIER SENSE) SILENCE (PRESET TIME)

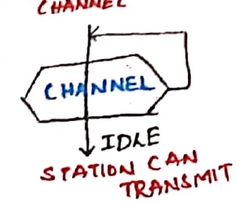
MULTIPLE ACCESS - MANY DEVICE CONNECT / SHARE SAME NETWORK

ADVANTAGE:- COLLISION ↓ PERFORMANCE ↑

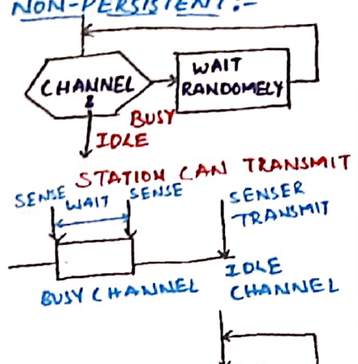
CSMA

- 1-PERSISTENT
- NONPERSISTENT
- P-PERSISTENT
- O-PERSISTENT

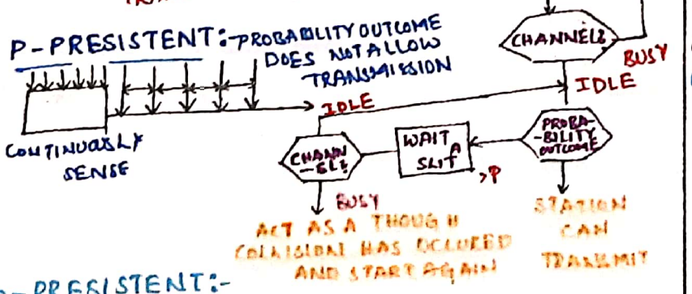
I-PERSISTENT:-



NON-PERSISTENT:-



P-PRESISTENT:- PROBABILITY OUTCOME DOES NOT ALLOW TRANSMISSION



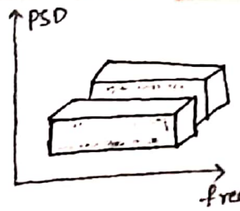
O-PRESISTENT:-

* SUPERIORITY OF THE STATION
* IF CHANNEL INACTIVE, EACH STATION WAITS FOR TURN TO RETRANSMIT THE DATA

CHANNALIZATION PROTOCOLS

TIME DIVISION MULTIPLE ACCESS:-

- PRE ASSIGNED
- DEMAND ASSIGNED



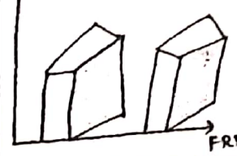
* SINGLE CARRIER FREQUENCY
* NON OVERLAPPING TIME SLOTS
* DISCONTINUOUS TRANSMISSION (BURST)
* DUPLEXER NOT REQUIRED
* HIGH SYNCHRONOUS OVERHEAD.
* ADAPTIVE EQUALIZATION

BUFFER CAPACITY $M = R_p T_F$

$R_{TDMA} = \frac{M}{T_b} = n\left(\frac{T_f}{T_b}\right)$

FREQUENCY DIVISION MULTIPLE ACCESS:-

PSD — Fixed Assigned / Demand Assigned

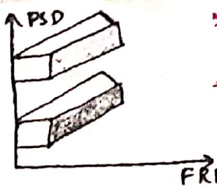


* INDIVIDUAL CHANNEL TO INDIVIDUAL USER
* NO OTHER USER CAN SHARE THE SAME FREQUENCY BAND
* CONTINUOUS/SIMULTANEOUS TRANSMISSION
* NARROW BAND SYSTEM
* NO EQUALIZATION REQUIRED
* SYNCHRONIZATION → CALL SETUP,

Disadvantage:- FADING, MAINTANANCE DIAGNOSIS

FREQUENCY MODULATION, INTERMODULATION.

CODE DIVISION MULTIPLE ACCESS:-



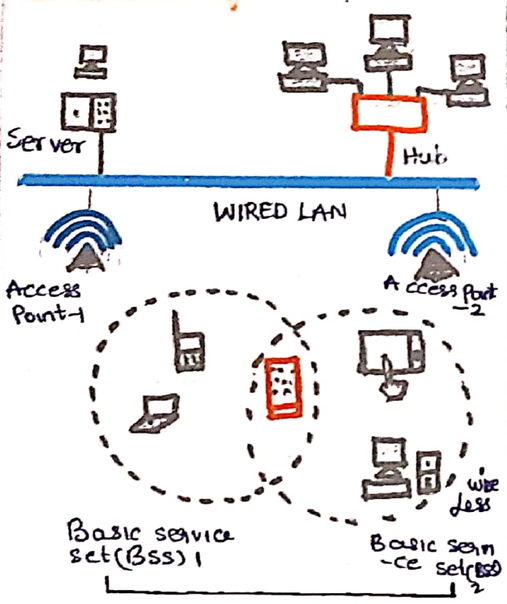
* MANY USERS CAN SHARE SAME FREQUENCY
* SOFT CAPACITY LIMIT
* LESS FREQUENCY DEPENDENT T_x
* LARGE SPECTRUM
* CHANNEL DATA RATE (VERY HIGH)
* SOFT HAND OFF

TYPES:- SPREAM SPECTRUM, FREQUENCY HOPPING

IEEE 802.11 WIRELESS/WIRED LAN, IEEE 802.11 wireless LAN ARCHITECTURE, HIDDEN STATION PROBLEM & IEEE 802.11 FHSS

⇒ IEEE 802.11 WIRELESS/WIRED LAN :-

Connecting LAN:-



Connecting devices to correct Segment of LAN :-

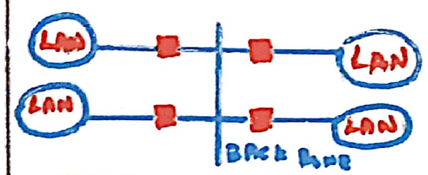
* AT Physical Layer → Active Hub & Passive Hub
* AT Physical & DATALINK LAYER → Bridge or two Layer switch
* At physical Datalink & Network Layer → Router or Three Layer switch
* All five Layers (Except Presentation & session Layer) → Gateway

Back Bone :-

Allows several lans to be connected
No station is directly connected to Back bone

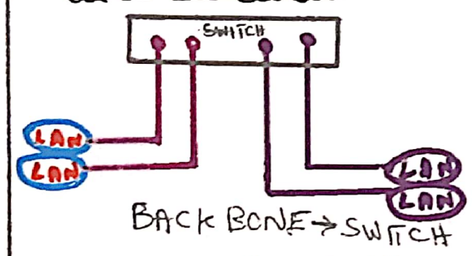
Back bone connects lan.

BUS BACKBONE



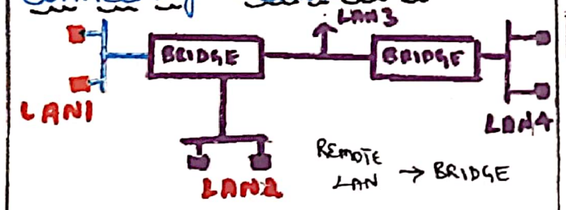
BACKBONE → BUS TOPOLOGY

STAR BACKBONE



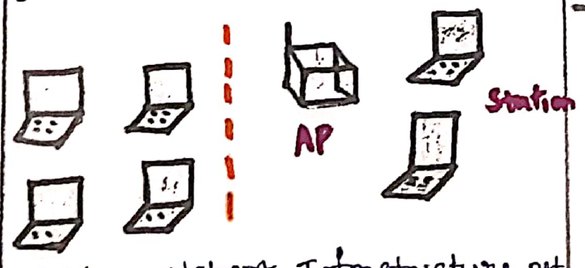
BACKBONE → SWITCH

Connecting Remote Lans:



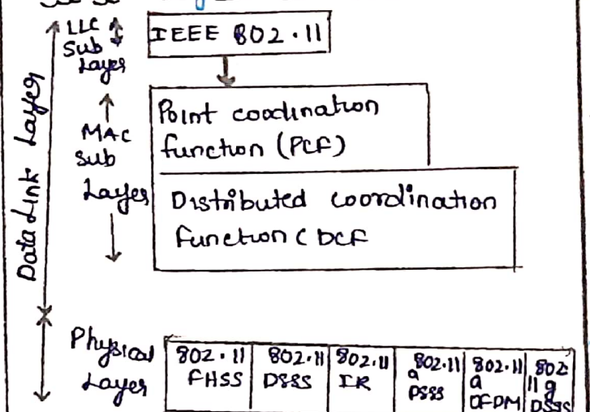
⇒ IEEE 802.11 Wireless LAN Architecture :-

ESS - Extended service set
BSS - Basic service set

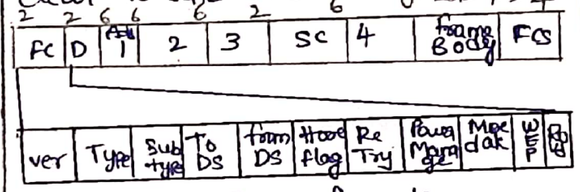


Ad hoc Network Infrastructure network

MAC Layers in 802.11



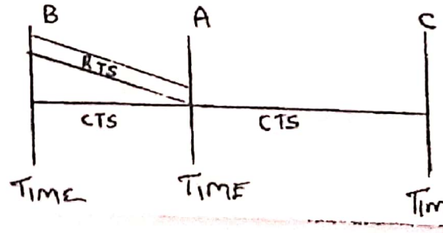
DCF uses CSMA/CA
Request to send RTS
Clear to send CTS



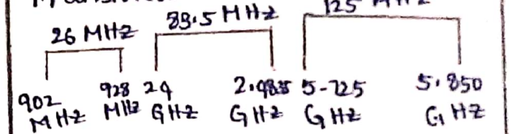
Frame formate.

Hidden station Problem :-

A → within the rage of B & C
B → Outside the range of C
C → Out side the range of B
B2C → transmits to A at same time
Collision occurs



Hand shaking to Prevent Hidden station Problem
RTS from B reaches A not C
CTS from A Reaches C
Transmission refrained.



ISM Band.

IEEE 802.11 FHSS :-

* USE FHSS
* 2-4 GHz ISM band
* 79 Sub bands (1MHz)
* FSK
* 1 or 2 Mbps.

IEEE 802.11 DSSS :-

* Use DSSS
* 2-4 GHz ISM band
* BPSK / QPSK
* 1 or 2 Mbps

IEEE 802.11 Infrared

* 800-950 nm
* 9PM
* 2Mbps

IEEE 802.11a OFDM

* Use OFDM
* 5 GHz ISM band
* 52 Sub bands [48+4]
* PSK / QAM
* 18Mbps to 54 Mbps.

IEEE 802.11 b DSSS :-

* HR DSSS
* 2.4 GHz ISM band
* 8 PSK / QPSK
* 1.375 Mbps

IEEE 802.11 g

* OFDM + FEC
* 2.4 GHz ISM band
* 22/54 Mbps, Backward

WIRELESS COMMUNICATION

BLUETOOTH

→ Short range communication

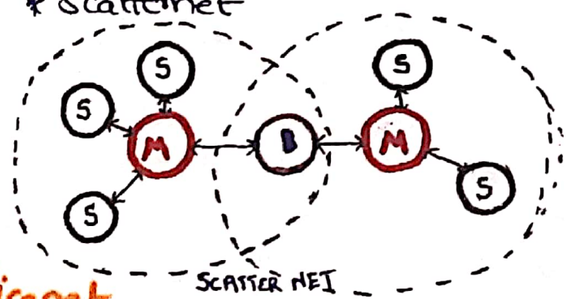
→ LAN - very limited coverage

→ RF for communication

→ Frequency modulation for radio wave

Two types

* Piconet
* Scatternet



Piconet

1. Master and Slave in Piconet
2. One Master - Maximum 7 Slave
3. No direct connection between Slave

Scatternet

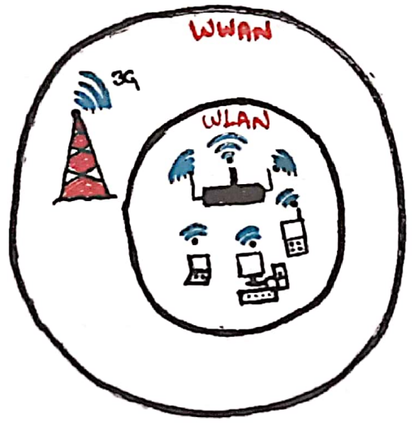
→ Bridge between two or more piconet

→ Spectrum : 2.4 to 2.485 GHz

→ Range : 1m to 3 feet

→ Data Rate : 3 Mbps from V.2.0

WIRELESS WANS



→ used in cellular device

→ LAN - WIFI - room

→ outside - internet - 3G, 4G etc.

Types:

1. GPRS
2. GSM
3. UMTS
4. WIMAX

→ WWAN - 128 bit encryption security

→ covers large geographical area

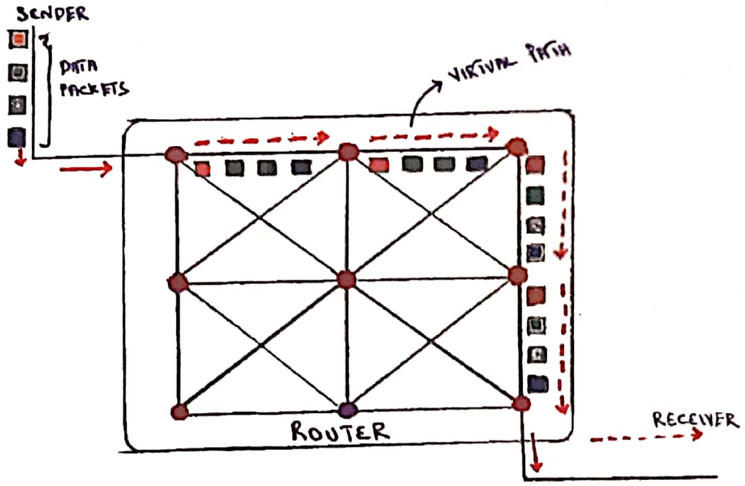
→ Based on package - limited usage

→ M : Master

→ S : Slave

→ only one piconet can be active.

VIRTUAL CIRCUIT NETWORKS



→ path between source and destination

→ physical path - dedicated path

→ Logical - managed pool circuit

Features of VCN:

→ All data using same path

→ Resources link and buffers the bw reserved

Phases of virtual ckt:

→ Setup phase → route through switch

→ Data transfer → packets followers route

→ Tear down phase → Data transfer complete

→ VCN - Network Layer

→ Path - Data packets allocated

→ Same path

FRAME RELAY, ATM, MPLS

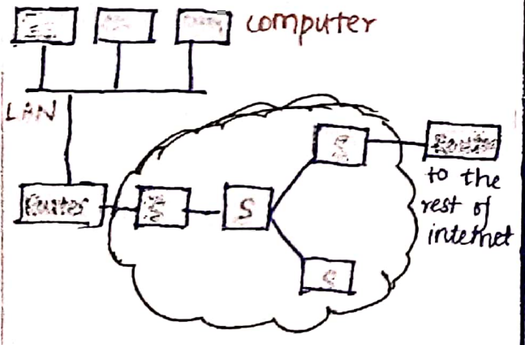
FRAME RELAY

- Packet Switching Network.
- Fragmented into trans. units called Frames.
- Exclusive Communication during transmission called Virtual Connection.

Layers:
- Physical Layer.
- Data Link Layer.

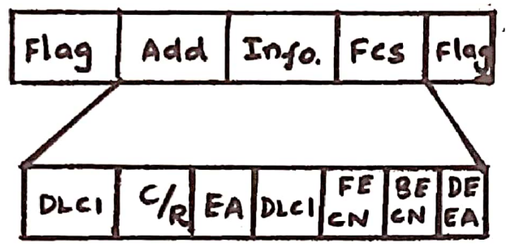
NEED:
- Higher data rate.
- Transfer bursty data.
- Lower overheads.

Architecture:



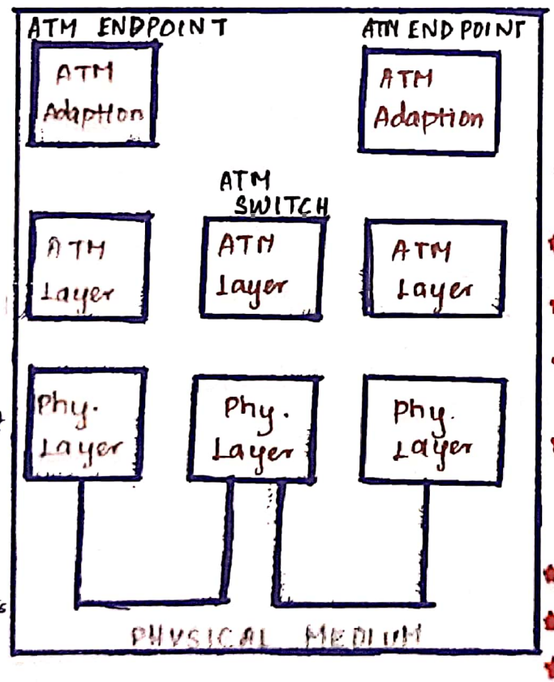
Two Types:
1. Permanent Virtual Circuits (PVC)
2. Switched Virtual Circuits (SVC)

Frame:



1. DLCI Field
2. Command / Response
3. Extended Address CEA)
4. Forward Explicit Congestion
5. Backward Explicit Congestion.
6. Discard Eligibility.

ATM



- ATM [Asynchronous Transfer Mode].
- TDM for Data Communication.
- Supports Video, voice & data Communication.
- Encodes data into small fixed size.

Functions:
- Physical Layer - Calls into bits
- ATM Layer - Routing, Traffic, Mgmt.
- AAL - Existing to ATM N/w.
- ATM End point - Interface
- ATM Switch - Accepting incoming calls.

Header Payload

- Call are transmitted Asychrono-usly.
- Connection Oriented.
- Follow same path Sequencly.
- Both Constant and Variable traffic
- Independent transmission.

MPLS

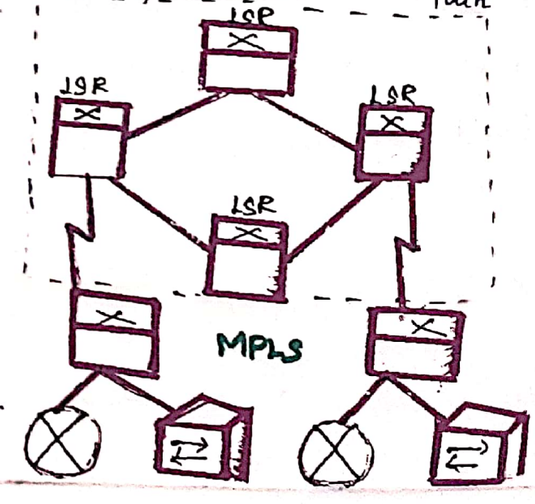
- Multiple Label Switching
- Network Technology
- Routes traffic using Shortest path.
- Based on Labels.
- To handle forwarding over Private WAN.
- Speed and control - N/w traffic.
- Scalable, Protocol independent.
- Works with IP, Ethernet, FR, & ATM.

Working Principle:
- By Prefixing 32-bit labels with MPLS Header.
- 32-bit label contains:
  - Label value - 20 bits
  - Traffic value - 3 bits.
  - Bottom stack flag - 1 bit
  - Time to live (TTL) - 8 bits.

Ingress Router → Label Edge Router (LER)
- Label is added.

LER decides the virtual path - Label Switched path (LSR)

Egress Router → LER
- Labels are removed.
- original IP packet is forwarded.



NETWORK LAYER

Packet Switching and Datagram approach

- Switched Network
  - Taxonomy of Switched Network
  - Packet Switching Network
- Datagram Approach
  - Datagram Network
  - Packet Flow
  - Routing Table
  - Destination Address
  - Efficiency
  - Delay
  - Types

IPv4 addressing methods

- Types
  - Hierarchy
  - Classful
  - Classless
- Subnetting

Routing

- Goals
- Routing Algorithm
  - Distance Vector Routing
  - Link State Routing

ICMP

- Error Reporting Messages
- Query Messages

Multicast Routing

- Ethernet
- IP

IPv6 addresses

- Features
- Addressing Methods

Internetworking

- Tunneling
- Packet Fragmentation

Topic 11 :- Packet Switching And Datagram Approach

Packet Switching

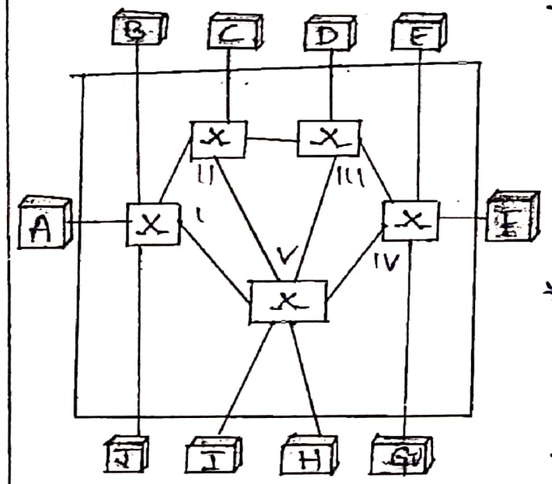
⇒ Switch - Connection b/w i/p & o/p port.

⇒ Packet Switching - Transfer of data / small pieces of data.

⇒ Networking protols divide messages into packets.

⇒ Part of the basis for, WAN, X.25 & TCP/IP.

* Switching Network :-



* Packet Switching Network

→ Needs to be divided into packets.

→ Size - Determined by the n/w.

→ Connectionless n/w

→ Message

No. of units (packets)

Source — Destination.

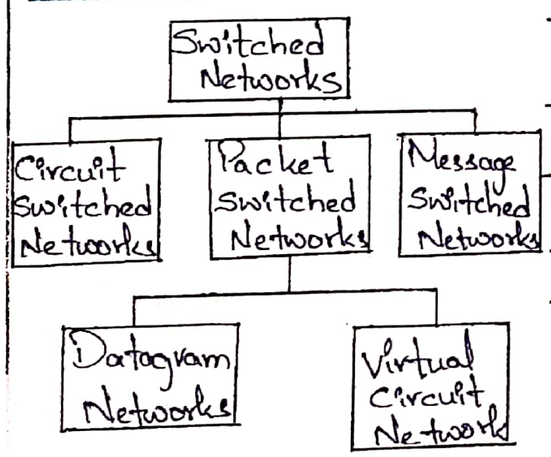
* No Source Allocation

No reserved bandwidth

No scheduled processing time.

→ Done on a first come first served basis.

Taxonomy of Switched Networks :



Datagram Approach

→ Packet is treated independently.

→ Packets (refers) → Datagram.

Datagram Network :-

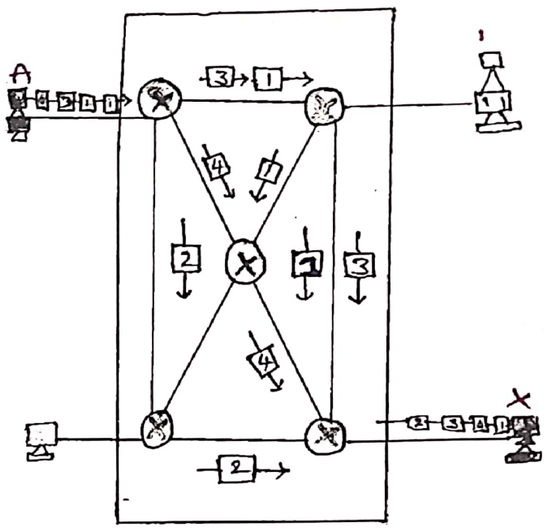
→ Connectionless n/w.

→ Doesnot keep information. (Connection state)

→ No setup (or) Tear down phases.

Packet Flow

→ odd packets
→ Even packets



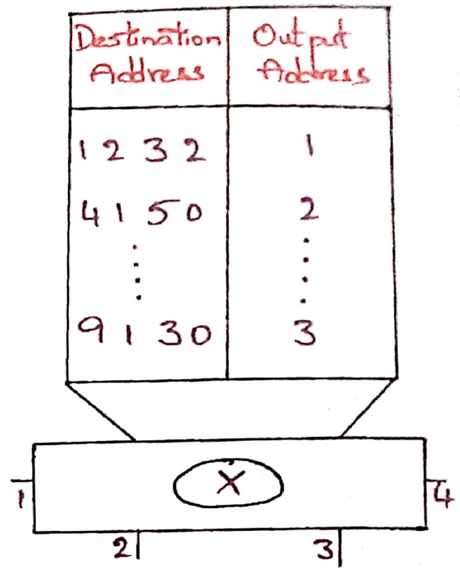
↳ Each packet has a routing table.

↳ Based on the destination address.

↳ Routing table
Dynamic
Updated periodically.

↳ Destination address
Forwarding o/p ports
Recorded in the tables
Every packet carries a header
Routing table finds corresponding port

Destination Address	Output Address
1232	1
4150	2
⋮	⋮
9130	3



* Efficiency :-

→ Better than ckt Switched n/w

→ More efficient transfer

→ Various network devices

* Delay :-

→ Greater delay in datagram n/w

→ Bandwidth increases.

→ Transmission delay decreases.

* Types :-

→ Transmission delay

→ Propagation delay

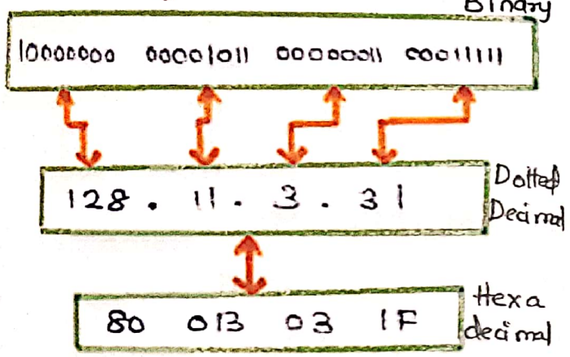
→ Quening delay

→ Processing delay

IPV4 Addressing Methods

* IP layer – TCP/IP Protocol
* Identify – connection (each device)
  ↓
  (IP address)
* 32 bit address
* uniquely defines – connection (Host)

Three different notations in IPV4 addressing



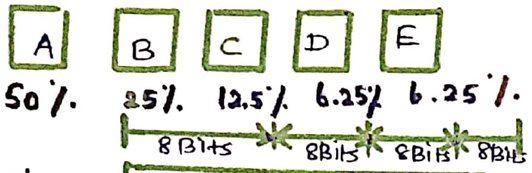
Hierarchy in Addressing

- Prefix → n bits (fixed length)
- Suffix → (32−n) bits (variable length)

classful Addressing

→ fixed length prefix
→ whole address space

class A | class B | class C | class D | class E

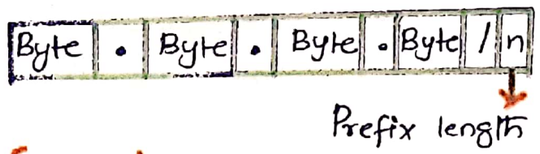


class	Prefixes	First Byte
A	n = 8 Bits	0 to 127
B	n = 16 Bits	128 to 191
C	n = 24 Bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Classless Addressing

→ whole address space (variable length blocks)
→ prefix – block (n/w)
→ suffix – node (device)
→ $2^0, 2^1, 2^2, \ldots 2^{32}$ addresses.

SLASH NOTATION (CIDR)



→ prefix length : n

Examples :

12.24.76.8/8
23.14.67.92/12

SUBNETTING

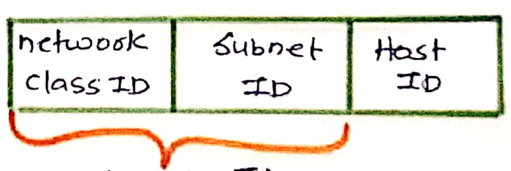
→ divide a n/w to smaller network (subnets)

Reasons

→ Reduce n/w traffic
→ Improve n/w performance
→ management
→ Allocate Host bits for Subnet bits

Subnet Mask

→ 32 bit string
→ 1's and 0's
→ Specifies no of bits for network ID (IP address)



Designing Subnets

→ Total no of address : N
→ prefix length : n

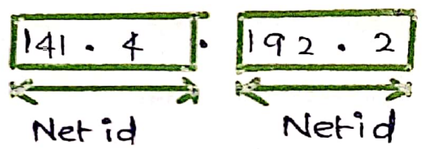
Steps to be followed

→ no of addresses (power of 2) (each sub n/w)
→ Prefix length
$n_{sub} = 32 - \log_2 N_{sub}$
→ Starting address (divisible by the number of addresses)

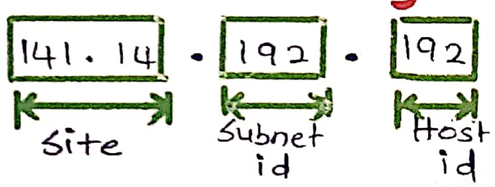
Address Aggregation

→ CIDR strategy
→ ICANN assigns ISP

Without Subnetting



With Subnetting



* To create a 3rd address level
  → network id
  → Subnet id
  → Host id

ROUTING (DVR - LSR and Multicast)

Routing :

* Selecting path
* Along with send network traffic

Goals :

* Correctness
* Simplicity
* Robustness
* Stability
* Fairness and optimality

Routing Algorithms :

* Distance vector Routing
* Link state Routing

Distance Vector Routing:

* Periodically shares knowledge
* About the entire network
* Within neighbours
* Table of Information
* Updated by exchange information
* Immediate neighbours

Three Important Aspects

* Initialization
* Sharing
* Updating

Initialization

→ Distance between itself and its immediate neighbours

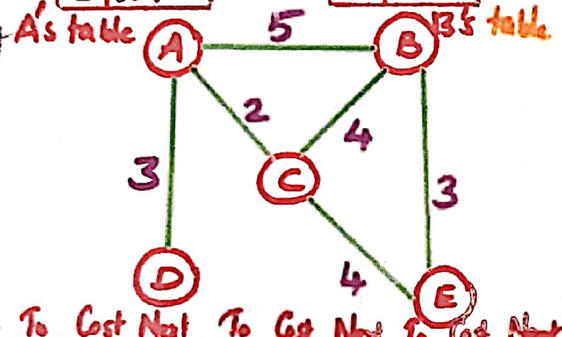
→ Directly connected.

A's table

To	Cost	Next
A	0	–
B	5	–
C	2	–
D	3	–
E	∞	–

B's table

To	Cost	Next
A	5	–
B	0	–
C	4	–
D	∞	–
E	3	–



D's table

To	Cost	Next
A	3	–
B	∞	
C	∞	
D	0	–
E	∞	

C's table

To	Cost	Next
A	2	–
B	4	–
C	0	–
D	∞	–
E	4	–

E's table

To	Cost	Next
A	∞	
B	3	B
C	4	C
D	∞	
E	0	D

Sharing :

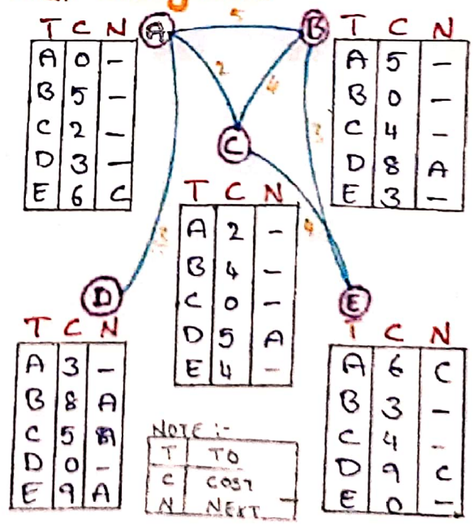
* Information between neighbours
* Node A does not know about node E

* Node C does
* C share its routing table
* To reach node D
* Node A shares its routing
* Improve routing table
* Help each other

Updating

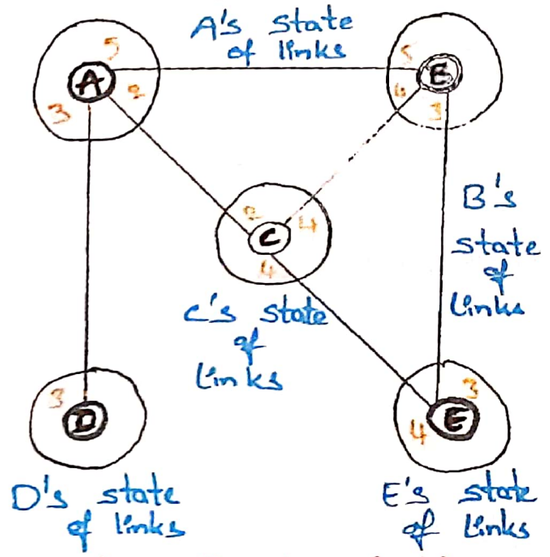
* Receives two-column table
* Updates routing
* Receiving node needs
* Add the cost
* Send node to each value
* Second column (x+y)
* Receives node uses information
* Receiving node needs to compare each rows with old table

Final diagram



Link State

* global knowledge
* Each node has partial
* Knowledge (Type, Condition & Cost)



Building Routing tables :

* Creating of the states
* Flooding efficient
* Reliable way
* Formation of shortest path
* Calculate of routing table

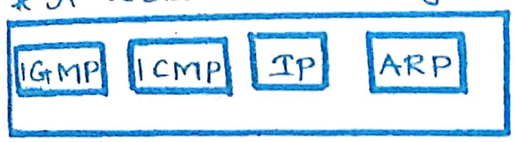
Multi-cast Routing:

* Efficient distribution
* One to many traffic

(example: Computer devices, Ip phones)

ICMP PROTOCOL

* Internet Control Message Protocol
* Network Layer Protocol
* Used - Error Handling in the network layer
* Primarily used on network devices - routers
* ICMP used to report the errors and to debug the errors
* It resides in IP layer



position of ICMP in the network layer

Messages

* The ICMP Messages are usually divided into 2 categories
  - → Error-reporting Message
  - → Query Messages

Category	Type	Message
Error Reporting Messages	3	Destination Unreachable
	4	Source Quench
	11	Time exceeded
	12	Parameter Problem
	5	Redirection
Query Messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

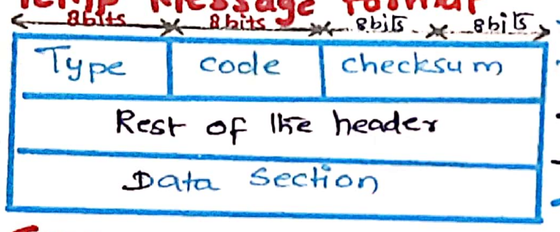
Error-reporting Messages

* The router encounters a problem when it processes an IP packet then it reports a message

Query Message

* Messages - Helps the host to get specific information of another host

ICMP Message format



Type

* 8 bit field
* ICMP Message type
* $ICMPV_6$ values ranges from 0 to 127
* values from 128 to 255-Info

Code

* 8 Bit field
* Sub type of ICMP Message

checksum

* 16 bit field
* To detect whether the error exists in the message or not

Note: ICMP protocol always reports the error Message to the original source

Destination unreachable

→ It occurs when the packet does not reach the destination
→ Intermediate router reports to the sender
→ Type 3, code (0 to 15)

Source quench

→ No flow Control
→ Congestion control mechanism
→ ICMP provide feedback to sender
→ High datarate to lower rate by source quench message to sender
→ Type 4, code - 0

Time exceeded

→ Many router that exists b/w the sender & the Receiver
→ type 11, code - 0 or 1

Parameter Problem

→ Router and destination host can send parameter problem msg
→ Type 12, code : 0 or 1

Redirection

→ The routing table is gradually augmented & updated
→ A redirection Message → router Host on the same n/w

ICMP Query Message

→ Echo - request & reply Msg
→ Timestamp request & reply Msg

MultiCast Routing

→ Group Communication
→ Send data to multiple receivers
→ one to many & Many to Many
→ Transmission across LANs/WANs
→ Helps in Minimize data frame
→ Similar to Broadcasting
→ Information is sent to the specific members of the n/w
→ It allows a single transmission
→ Split up among multiple users
→ Reduces the bandwidth of signal

Applications

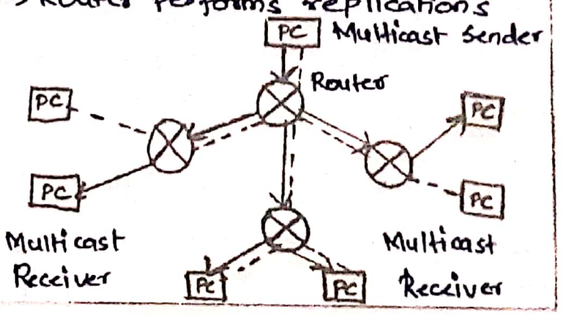
→ Internet Protocol (IP)
→ Streaming Media

Ethernet Multicast

→ Datalink layer for Ethernet n/w
→ Ethernet frames - 1bit in LSB
→ First Byte of destination addr

IP Multicast

→ provides one to many communication
→ Destination nodes → sends → Join/leave Messages
→ Router performs replications



IPV6

Internet Protocal Address Version 6

* Developed by Internet Engineering Task force (IETF) 1998.
* IPV4 produces 4 billion Address
* IPV_4 - 32 bit address, IPV_6 - 128 bit address

x:x:x:x:x:x:x:x

* 8 different selections, each selection 16 bit Hexa decimal.
* Range 0 to FFFF, Seperated by colons(:)
* xxxx Contains 16 bit hexadecima, x-4 bit Hexadecimal.

FDEC:BA98:0000:0000:0600:BDFF:0004:FFFF

* Remove the starting zeros (0) of each 16 bit section.
* Compress the consecutive sections 16 bit zeros (0:0) using double colons(::)

FDEC:BA98::600:BDFF:4:FFFF

340 Undecillion Possible Address = 2^{128}

FEATURES :-

- → larger Address space
- → Simplified header
- → End to End Connectivity
- → Auto Configuration
- → Faster formarding/routing
- → IPSec
- → No broadcast
- → Puncast support
- → Mobility
- → Enhanced priority support
- → Smooth translation
- → Estensibility.

* IPV6 Header

Version	Traffic class	Flow Label
Payload length	Next header	Hop limit
Source Address		
Destination Address		

IPV6 header

IPV_6 Addressing Methods :-

UNICAST : * Single network interface
* Delivered to be identified address

MULTICAST : * Multiple hosts → Group (multicast destination address)
* Geographically not together
* Distributed to all interfaces corresponding to that multicast address.

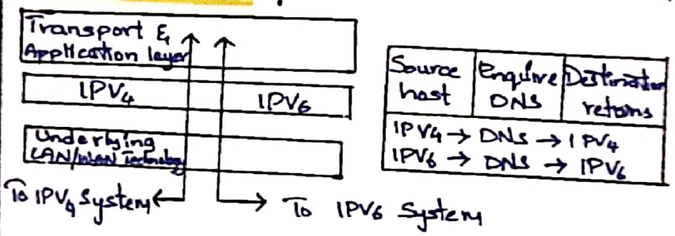
Anycast : * Packet sent to anycast address will be delivered to only to one member interface (mostly nearest host)

Transition from IPV_4 to IPV_6 :

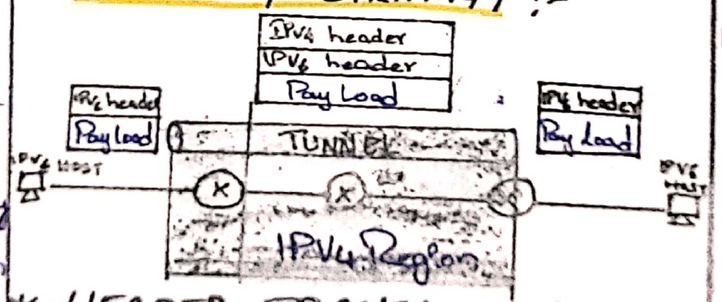
Transition strategies

DUAL STACK | TUNNELING | HEADER TRANSLATION

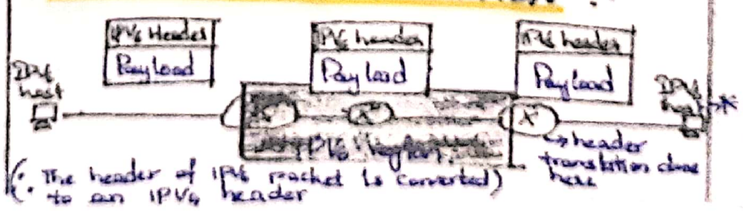
* **DUAL STACK** :



* **TUNNELING STRATAGY** :-



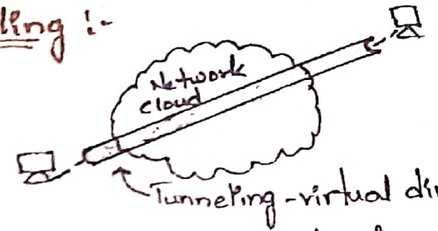
* **HEADER TRANSLATION** :-



(*. The header of IPV6 packet is converted to an IPV6 header)

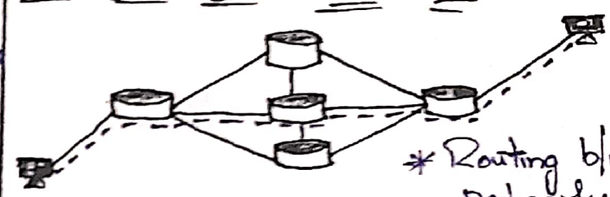
INTERNETWORKING

Tunnelling :-



* Two or more same networks Communi-cate with each other by passing intermediate complexities.

INTERNETWORK ROUTING :-



* Routing b/w two networks.
* Interior gateway protocols (IGP) : within organization
* Exterior gateway protocols (EGP) : different Organization.

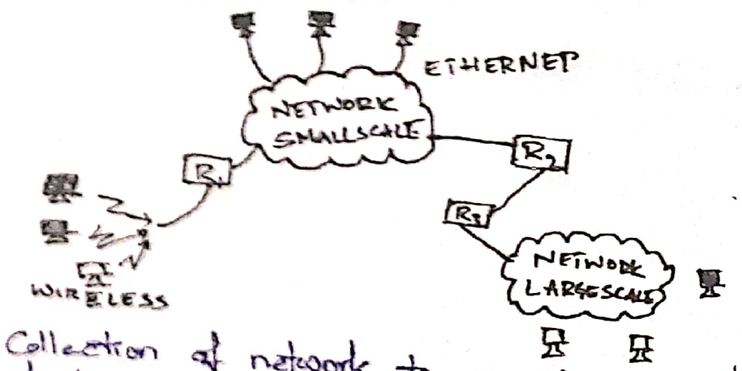
Packet fragmentation :

Data packet size ≤ size of packet Transmit network can handle → Protocol processed

If larger → Broken into smaller pieces & forwarded

Fragmentation → Source address, Destination address, Routing path

INTERNETWORK :



* Collection of network to provide some sort of host-host to packet delivery Services.

TRANSPORT LAYER

Transport layer and its Duties

- Duties of Transport Layer
- Multiplexing - Demultiplexing
  - FDM
  - TDM
  - CDM
  - WDM

Transmission Control Protocol (TCP)

- Feature
- Purpose
- Working
- TCP Header

User Datagram Protocol (UDP), Multicast

Congestion Control

- Network Congestion
- Control Methods
  - Open Loop Congestion
  - Closed Loop Congestion
  - Back Pressure Method
  - Choke Packet
- Concept

Quality of Services (QOS)

- QoS Characteristics
- Scheduling
  - FIFO Queuing
  - Priority Queuing
  - Weighted Fair Queuing
- Traffic Shaping

Queuing Analysis

- Models
- Single server
- Multi-server

Network of Queues

- Elements of Queuing Networks

Congestion and Traffic Management

TRANSPORT LAYER AND IT'S DUTIES

TRANSPORT LAYER DUTIES :-

- GATERING OF TRANSPORT LAYER
- CHUNKS OF DATA
- RECEIVES FROM DIFFERENT SOCKETS.
- ENCAPSULATE THEM
- PASSING THE RESULTING
- SEGMENT N/W LAYER
- MULTIPLEXING DONE AS WELL AS DEMULTIPLEXING

WORKING OF TRANSPORT LAYER:-

- TAKES SERVICES FROM NETWORK LAYER.
- PROVIDES SERVICES TO APPLICATION LAYER.

AT THE SENDER'S SIDE :-

- RECEIVES DATA FROM APPLICATION LAYER
- SEGMENTATION
- DIVIDES MESSAGE
- SEGMENTATION ENTRACED
- ADD SOURCE
- ADD DESTINATION
- PORT NUMBER
- HEADER SEGMENTS

AT THE RECEIVER'S SIDE :-

- RECEIVES DATA FROM N/W LAYER
- REASSEMBLES SEGMENTATION
- READ IT'S HEADER
- IDENTIFIES PORT NUMBER
- FORWARD'S MESSAGE
- APPROPRIATE PORT APPLICATIONS

RESPONSIBILITIES OF TRANSPORT LAYER:-

- PROCESS TO PROCESS DELIVERY
- MAC ADDRESS (48) BITS
- A PORT NUMBER 16 BITS
- CLIENT-SERVER PROGRAM

END TO END CONNECTION BETWEEN HOSTS:-

- TCP SECURE
- UDP (USER DATAGRAM PROTOCOL)

⇒ CONNECTION-ORIENTED PROTOCOL.

⇒ ESTABLISH ROBUST CONNECTION.

MULTIPLEXING :-

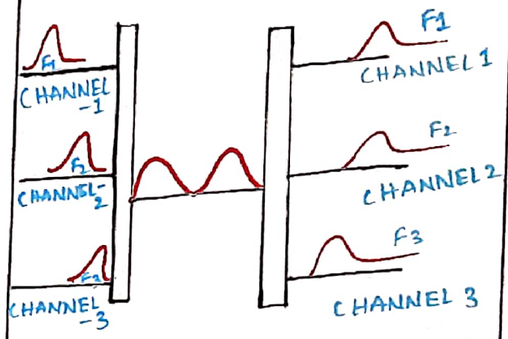
- ANALOG AND DIGITAL
- STREAMS OF TRANSMISSION
- PROCESSED OVER
- SHARED LINKS.

TYPES :-

- FREQUENCY DIVISION MULTIPLEXING
- TIME DIVISION MULTIPLEXING
- WAVELENGTH DIVISION MULTIPLEXING

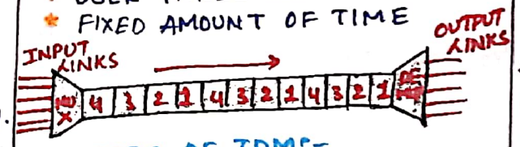
FREQUENCY DIVISION MULTIPLEXING:-

- ANALOG TECHNOLOGY
- SPECTRUM (OR) CARRER BANDWIDTH
- LOGICAL CHANNELS



TIME DIVISION MULTIPLEXING:-

- DIGITAL TECHNIQUE
- FREQUENCY DIVISION MULTIPLEXING
- TECHNIQUE
- ALL SIGNALS OPERATES
- USER TAKES CONTROL
- FIXED AMOUNT OF TIME



TWO TYPES OF TDM:-

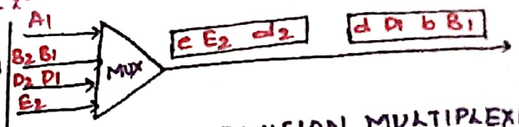
- SYNCHRONOUS TIME DIVISION
- STATICAL (ASYNCHRONOUS) TIME DIVISION.

SYNCHRONOUS TDM:-

- INPUT FRAME TO OUTPUT

STATISTICAL TDM:-

- ADDRESS PARTICULAR DATA
- SENT OUTPUT FRAME



WAVELENGTH DIVISION MULTIPLEXING:-

- LIGHT WAVELEGTH COLORS
- FIBER OPTICAL MODE
- MULTIPLE OPTICAL CARRIER SIGNALS.

CODE DIVISION MULTIPLEXING:-

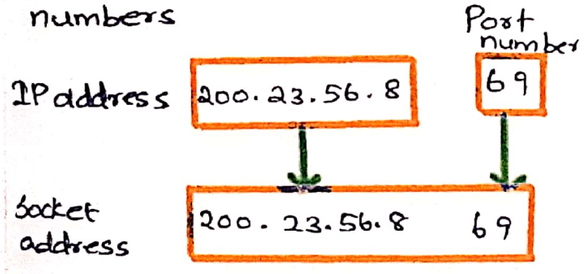
- ORTHOGONAL CODES
- SPREAD SIGNALS
- TECHNOLOGY OF WDM
- OPTICAL TRANSPORT N/W
- RAPID GROWTH DATA
- QUALITY CAPACITY
- TRANSMISSION EQUIPMENTS
- NETWORK BANDWIDTH
- MULTI-SERVICE TRANSMISSION

DEMULTIPLEXING :-

- DELIVERING RECEIVED SEGMENTS AT THE RECEIVER SIDE TO THE CORRECT APP LAYER PROCESSES IS CALLED THE DEMULTIPLEXING.
- CONNECTIDN ORIENTED
- CONNECTIONLESS
- UNWRAPPED AND CONSTITUENT MESSAGE.
- REVERSE OF MULTIREX PROCESS.

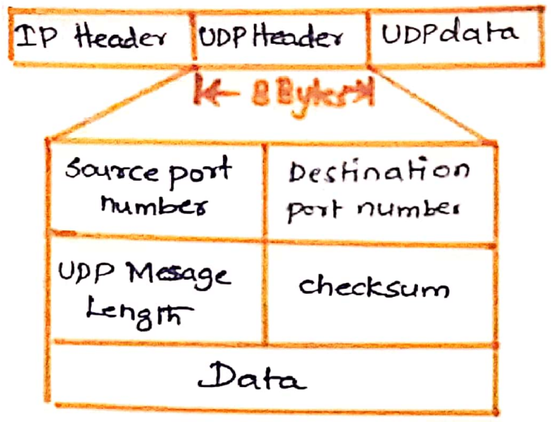
TCP SOCKETS

→ proces to process delivery
* Needs two identifiers
→ Combination of IP address and port number is called as Socket address
→ Socket address designs the process uniquely
→ Transport layer needs a pair of socket addresses
→ Client & server socket addresses
→ TCP header contains port numbers



UDP_User Datagram Protocol

→ Supports unreliable transmission
→ Host to host delivery
→ Supports unicast & multicast
→ Connectionless protocol
→ Fast, Simple and efficient
→ developed by David P. Reed in 1980.



→ Connectionless delivery
→ no handshaking
→ Source port
  * 16 Bit field
  * Identify sending port
→ Destination port
  * 16 Bit field
  * Identify receiving port
→ Length
  * 16 Bit field
  * Identifies the combined length of UDP header + data
→ checksum
  * 16 Bit field for error control

Features:
→ Transport layer protocol
→ Connectionless
→ ports
→ faster transmission
→ ack mechanism

COMPARISON

TCP	UDP
* Connection Oriented	* Connectionless
* Reliable	* Not Reliable
* Use extensive error mechanism	* Use only basic checksum
* Acknowledge segment used	* No acknowledge is used
* Ensure packets are arriving in order	* Not concerned with order of arrival of packet
* Three way Handshake	* No handshake
* Slower than UDP	* Faster, Simple and efficient than TCP

Multicast_Transport Layer (TCP)

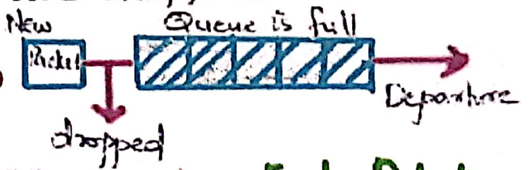
→ Multicast is the transmission from one device to many receipients
→ In TCP before transmission 3 way handshake is used
→ acknowledgement is sent to ensure packets are received
→ In multicast, no acknowledgement needed
→ TCP is not preferred for multicast
→ UDP can be used

Congestion & Traffic Management

→ Congestion & Traffic Management is a tool to improve network performance
→ reduce packet loss
→ keeps track of network traffic
→ predicts and avoids network congestion

Tail drop

→ default congestion avoidance method
→ treats all traffic equally
→ when queue is full, packets are dropped.



RED. Random Early Detection

→ ideal for high speed network
→ does not wait for tail to drop
→ random packets are discarded when the queue is about to get filled.

WRED - Weighted Random Early Detection

→ when queue is about to fill only a few packets are dropped.
→ Based on weight the packets are dropped when the queue is almost filled

TCP

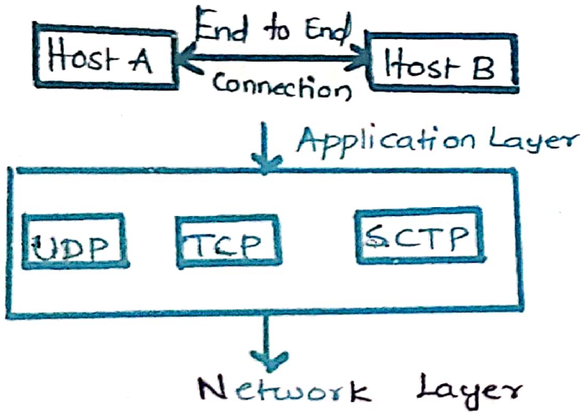
TRANSMISSION CONTROL PROTOCOL (TCP)

→ Transport Layer Protocol
→ Transmit the packets from Source to destination
→ Connection - oriented
→ Used in IP (TCP/IP)

Features :

→ Reliable
→ order of data
→ full duplex
→ stream - oriented

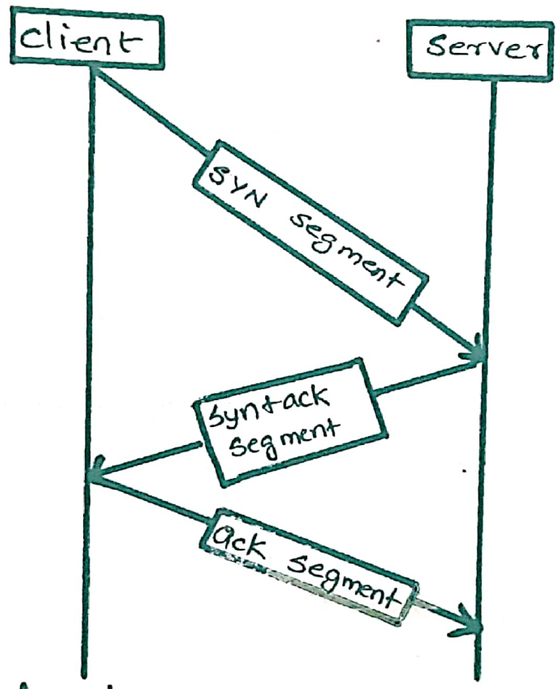
Purpose :



Working :

① Connection Establishment
→ Three way Handshaking

→ no need of packet fragmentation
→ Segment Tracking
→ Message divided for effiient routing



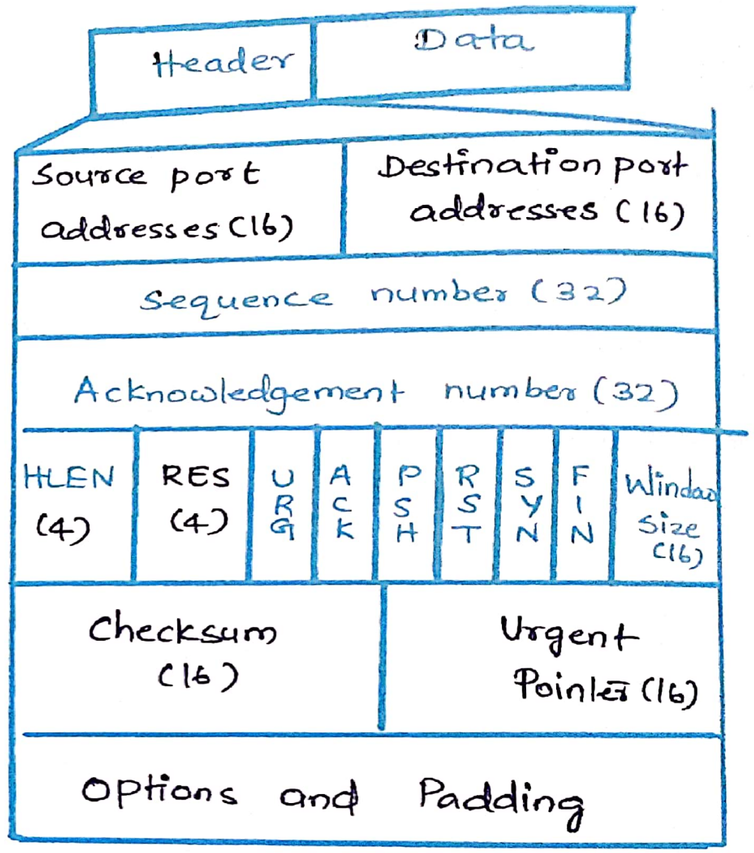
Advantages:

→ flow control mechanism
→ Error detection - checksum
→ Error Control
→ Eliminate Congestion

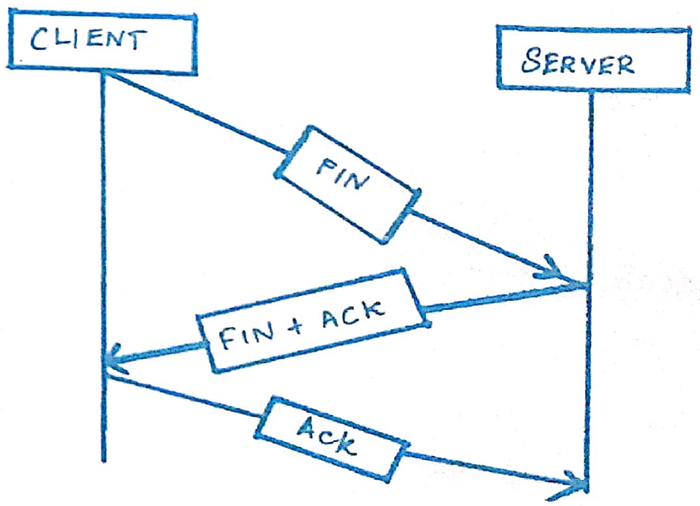
Disadvantages:

→ not generic in nature

TCP Header Format



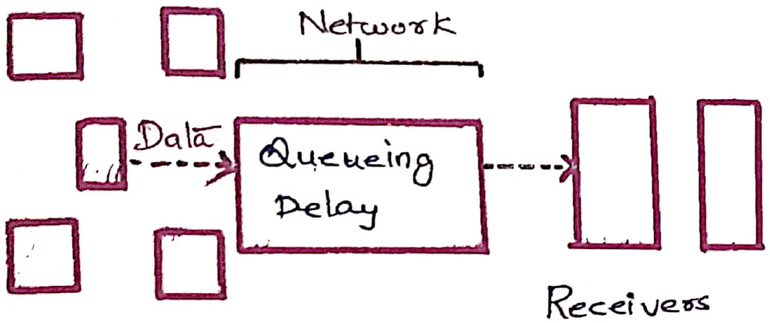
② Data Transfer phase
③ Connection termination phase



CONGESTION CONTROL

Congestion

→ Refers reduction in QoS
→ Packet Loss
→ Queueing delay
→ Blocking new connection



Network Congestion:

→ Bandwidth usage
→ Latency
→ Jitter
→ Packet retransmission
→ collision

Reason:

→ over Subscription
→ Unneeded Traffic
→ faulty devices
→ Security attacks
→ Misconfigurations

How to solve network Issue

→ Monitor and Analyze network traffic
→ Bandwidth
→ Segmenting and prioritizing
→ Assess your devices
→ Assess your network

Control Methods:

→ open loop Congestion control
→ closed loop Congestion control

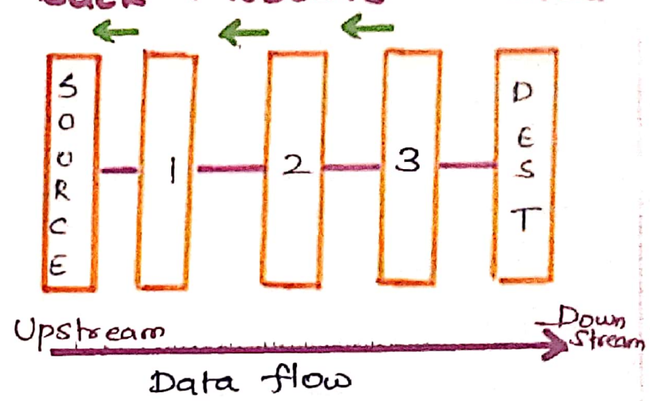
open loop Congestion Control

→ Retransmission policy
→ Window policy
→ Acknowledgement policy
→ Discarding policy
→ Admission policy

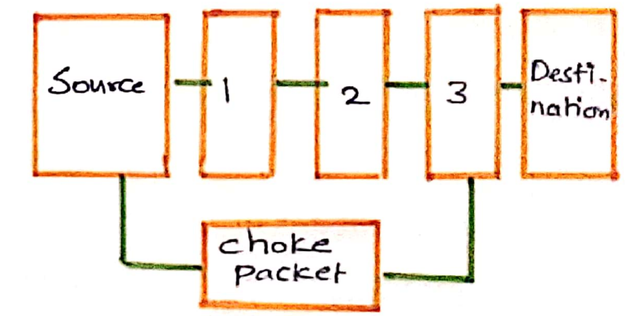
closed loop Congestion Control

→ Back pressure
→ choke packet
→ Implicit Signaling
→ Explicit signaling

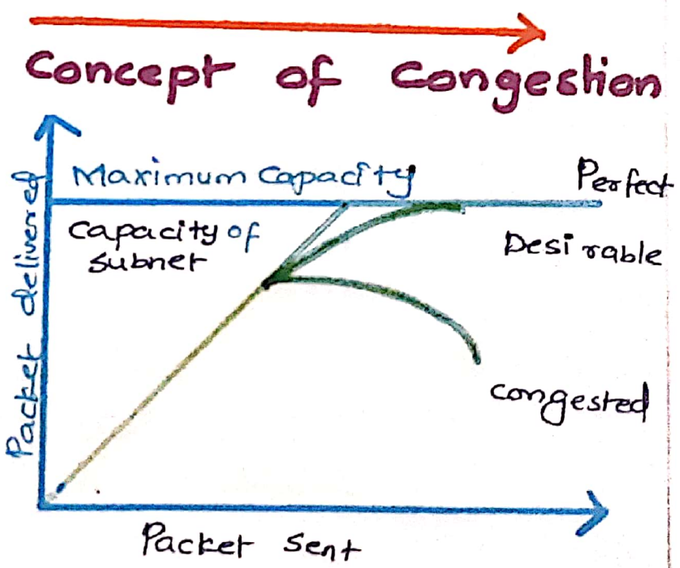
Back Pressure Method



Choke Packet



Concept of Congestion



QoS

Quality of Service (QoS)

Goals:

1) Provide quality services to a network
2) Manages traffic to reduce
   i) Packet loss
   ii) Delay
3) Priority for specific type of data.

QoS characteristics:

⇒ Reliability
⇒ Delay
⇒ Jitter
⇒ Bandwidth

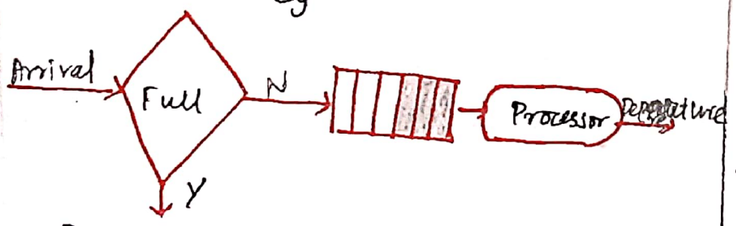
Techniques to improve QoS:

- Scheduling
- Traffic shaping
- Admission control
- Resource reservation

Scheduling

- FIFO Queuing
- Priority queuing
- weighted fair queuing

1. FIFO Queuing:



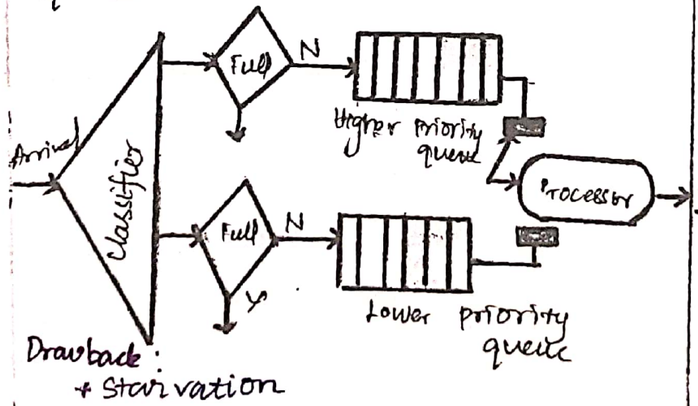
Packet leave the queue in the order they arrive in queue.

Drawback:

If Packet arriving rate > packet processing rate. the packet after queue filled will be discarded.

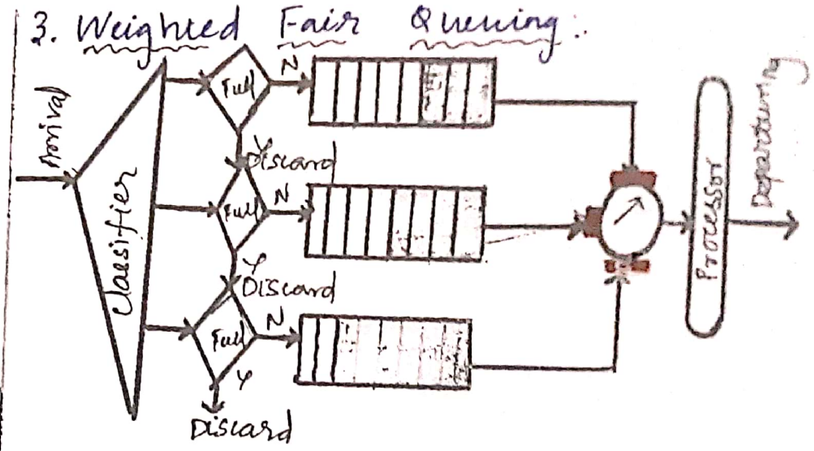
2. Priority Queuing:

* Packets are assigned to priority class initially.
* Each Priority class has its own queue



Drawback:
* Starvation

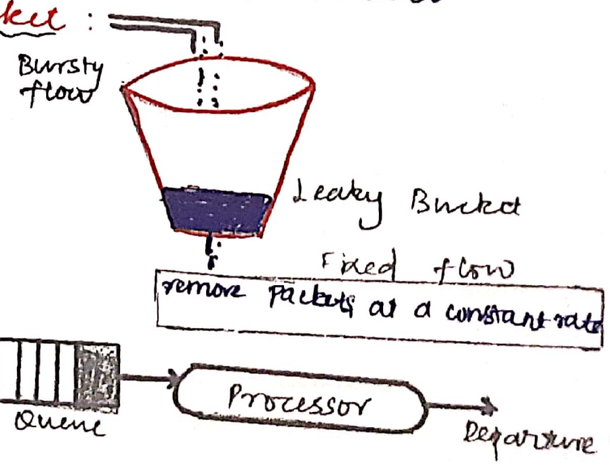
3. Weighted Fair Queuing:



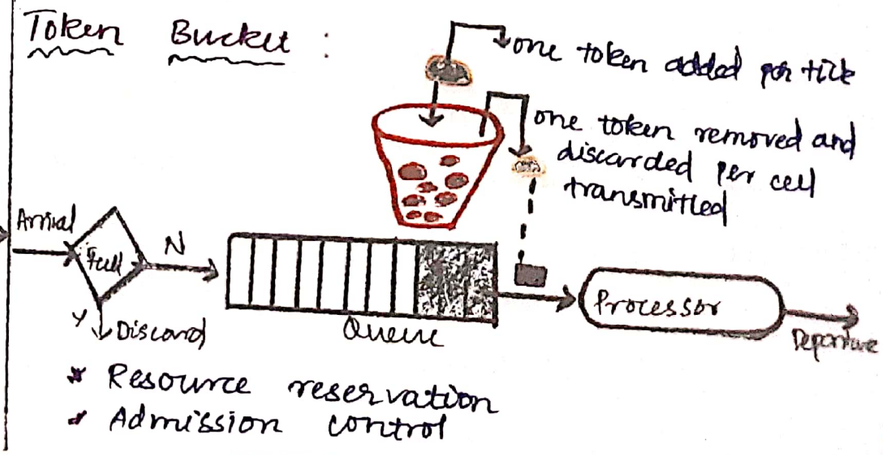
Traffic shaping:

Two Techniques: Leaky Bucket and Token Bucket

Leaky Bucket:



Token Bucket:



* Resource reservation
* Admission control

✳ Queuing Analysis

Objective :-

To predict the system performance such as,

- No. of customers processed per time step.
- Average delay a customer endures.

Analysis Methods :-

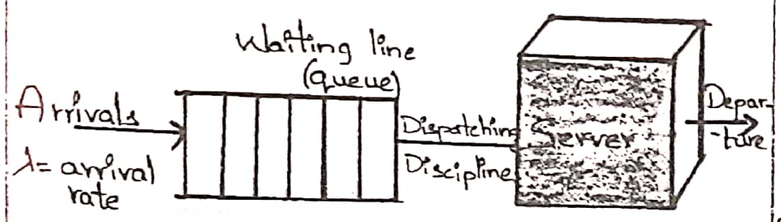
- After the fact analysis
- Predict Some simple trends
- Develop analytical model
- Run Simulation

Queuing Models :-

1. Single Serve Queue.
2. Multi Serve Queue.
3. Network of Queue.,

are three types of queuing Models.

* Single Serve Queue :

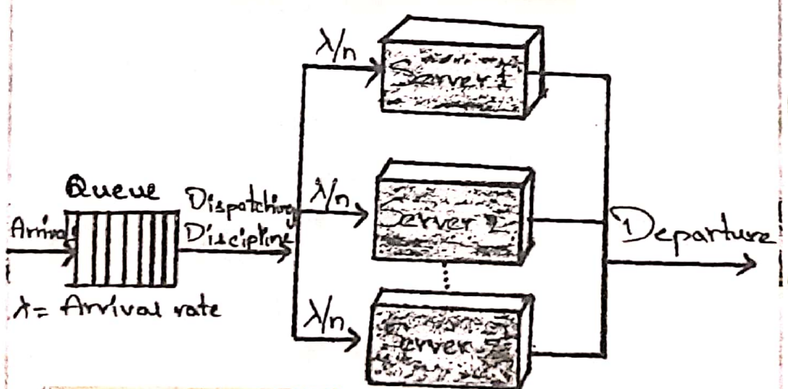


w = items waiting
T_w = waiting time
T_s = Service time
ρ = utilization
n = items resident in queuing system
T_r = Residence time.

⇒ Queue Parameters :

- Item population
- Queue size
- Dispatching Discipline

⇒ Multi - Serve Queue :-



$\lambda_{Max} = N/T_s$

* Basic Queuing Relationship

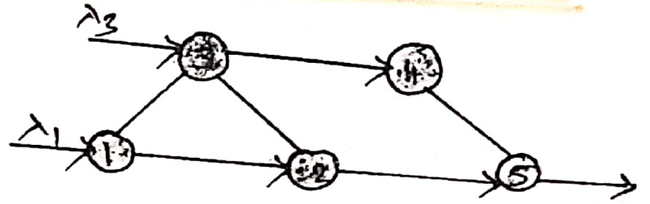
Assumptions :

- Arrival rate
- Service rate

Provide the output information about:

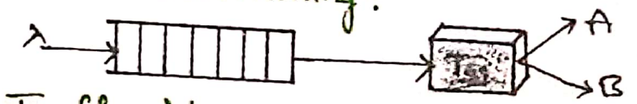
- Items waiting
- Waiting time
- Items in residense
- Residence time

* Network of Queues :-



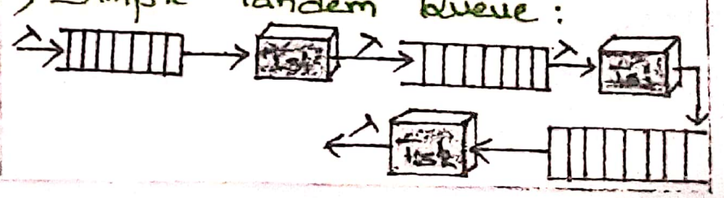
⇒ Elements of Queuing Networks :

a) Traffic Partitioning :



b) Traffic Merging :

c) Simple Tandem Queue :



APPLICATION LAYER

Domain Name Space (DNS)
- How DNS works
- Need for DNS
- Domain
  - Inverse
  - Generic
  - Country

SMTP
- Working of SMTP

FTP
- Objectives
- Types of connections
  - Control Connection
  - Data Connection
- Advantages and Disadvantages

HTTP

Electronic Mail
- Components
- Services
- Architecture

POP
- Characteristics
- Working

IMAP

SNMP
- Components
- Roles

P2P Communication
- Bit Torrent

VOIP
- SIP Protocol
- H.325 Protocol

Overlay Network
- Cashing Overlays
- Routing Overlay
- Security Overlay

SSL Security
- Fragmentation
- Message Integrities
- Confidentiality
- Cryptographic secrets

Firewalls
- Packet Filter
- Proxy

DoS
- Distributed DOS
- Types
- Buffer Overflow attacks
- Targets

DNS & SMTP

DNS : Domain Name service / Domain Name System.

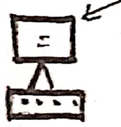
How DNS WORKS :

computer Browser Request to visit "SAMPLE.COM"

COMPANY/LOCAL DNS CHECKED. REQUESTED ADDRESS NOT FOUND

ISP DNS checked unable to find address

ROOT DNS CHECKED
IP ADDRESS FOUND
IP ADDRESS RETURN TO THE COMPUTER



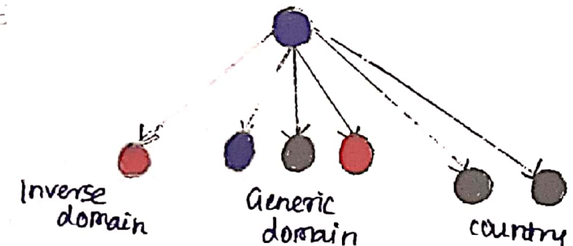
COMPUTER RECEIVES IP ADDRESS & PROMPTS THE BROWSER TO OPEN THE GIVEN ADDRESS.

Need for DNS :

- IP Address → Not Static
  - → MAY CHANGE DYNAMICALLY
- IP Address → complex series of numbers
  - → DIFFICULT TO REMEMBER IP NUMBERS

Domain :

• → SEPARATOR



* Forward look up
* Reverse look up

(eg)
• com, • edu, • gov, • info, • aero, • biz, • org, • net, • mil

(eg)
• in, • us, • uk

For Example :

132.147.165.50

ftp • Edusoft • com

SMTP

Simple Mail Transfer Protocol

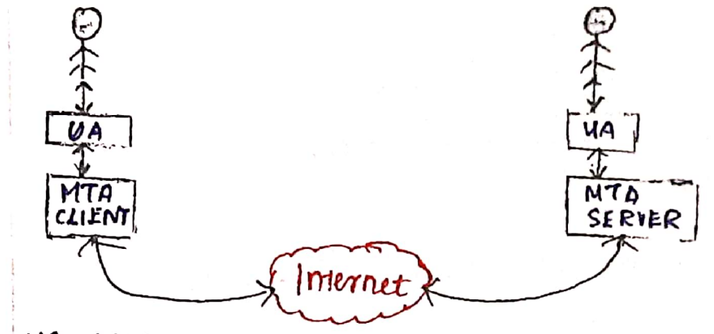
Set of communication guidelines that allows software to transmit an electronic mail over the internet

Supports :

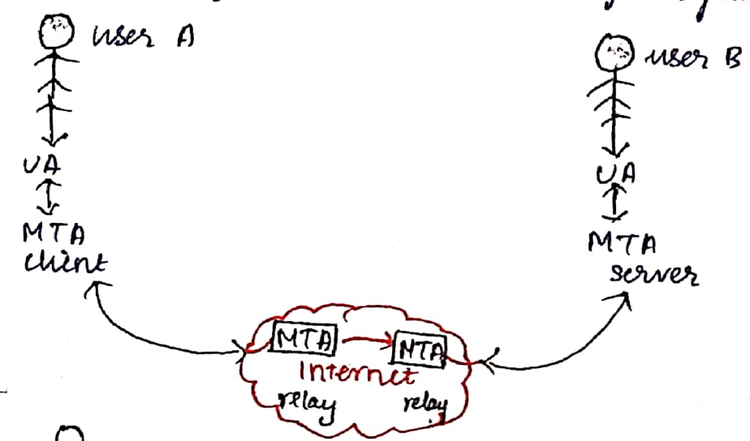
=> Single message to one or more recipients

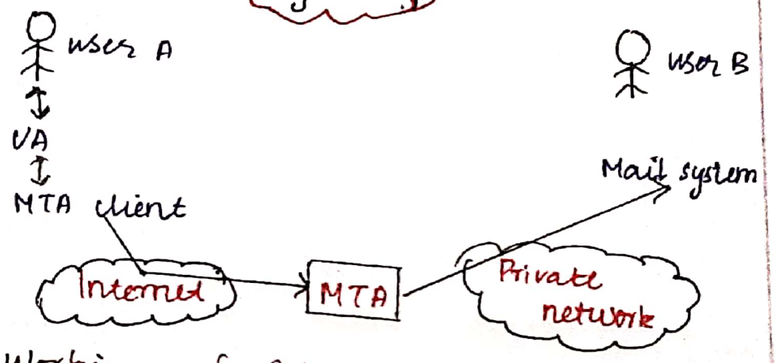
=> Text, video, voice or graphics

=> Message on networks outside internet



UA => User Agent ; MTA - Mail Transfer Agent





Working of SMTP :

* composition of Mail
* Submission of Mail
* Delivery of Mail
* Recepit and Processing of Mail
* Access and Retrieval of Mail

FTP & HTTP

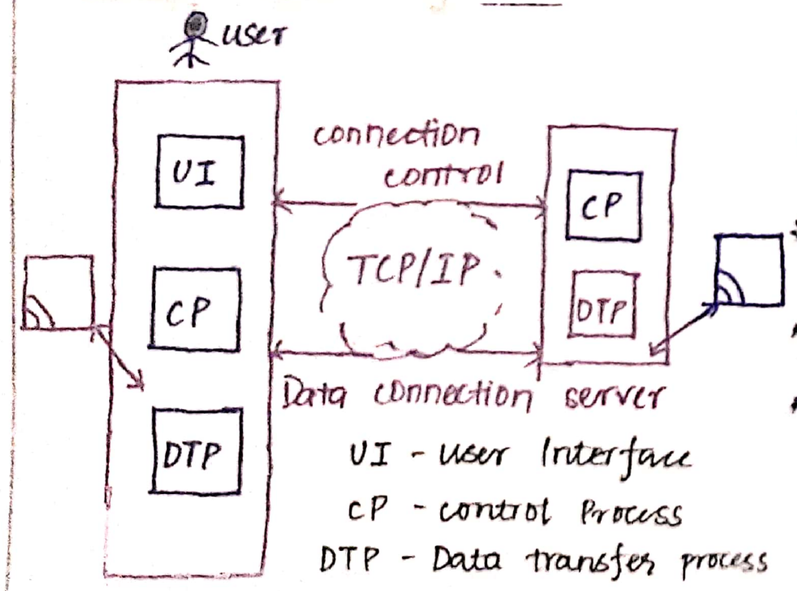
FTP :

⇒ File Transfer Protocol
⇒ Standard internet Protocol
⇒ TCP / IP
⇒ Transferring Web Page files to the computer
⇒ Server for other computer
⇒ Downloading the files to computer

Objectives :

⇒ Provides the sharing of files
⇒ Encourage the use of remote
⇒ computers.
⇒ Transfer the data more reliable of efficiency.

Basic Model of FTP



Types of Connections in FTP :

Control Connection :

⇒ Simple rules for communication
⇒ connection b/w the control processes
⇒ connected during the entire FTP session

Data connection :

⇒ complex rules as data type may vary.
⇒ Made b/w data transfer process
⇒ It open when command comes for Transfer
⇒ It closes when file is transferred.

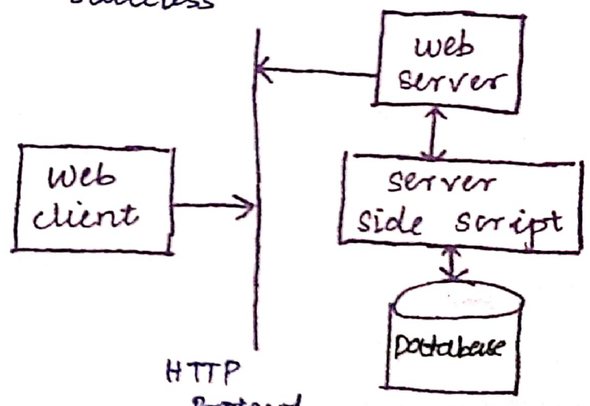
Advantages	Disadvantages
* Speed	* not all the FTP providers are equal
* Efficient	* not all providers offers encryption.
* Security	* size limit is 2GB only
* Back and forth movement	* doesn't allow transfer to multiple server
	* not compatible with every system.

HTTP : Hypertext Transfer Protocol

⇒ Application level protocol
⇒ Distributed, collaborative, hypermedia information system.
⇒ It is generic and stateless protocol.
⇒ TCP/IP based communication protocol
⇒ Deliver data on the WWW.
Default port TCP 80
Request data → server → respond

Features :

⇒ HTTP is connection less.
⇒ Media independent
⇒ Stateless



Act like HTTP client & server

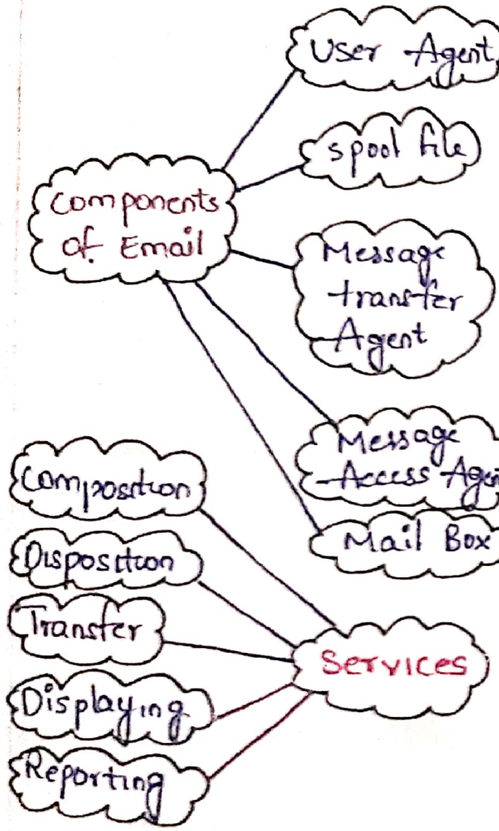
client : sends a requests → URI & Protocol version. MIME, client information, over TCP/IP.

Server : Respond with a status line. Message's protocol version, Successor Error code, MIME - like message server

Electronic Mail, POP, IMAP & SNMP

⇒ Electronic Mail:-

- Electronic Mail used mail Servers of Internet



MAA:-

Mail Access Agent (MAA)

- It is used for Email delivery [SMTP]
- Two protocol used to Access that is *POP & *IMAP

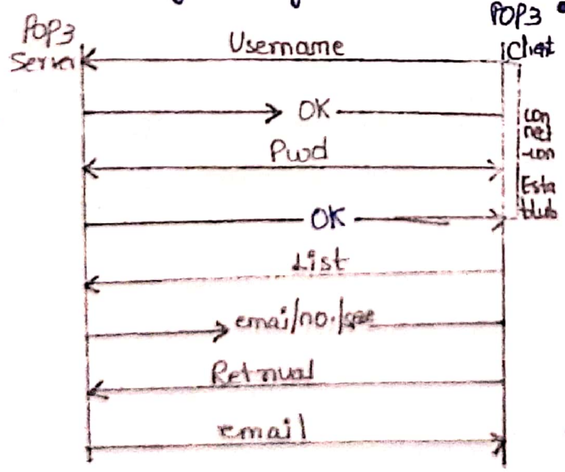
⇒ POP :-

Post office Protocol [POP]

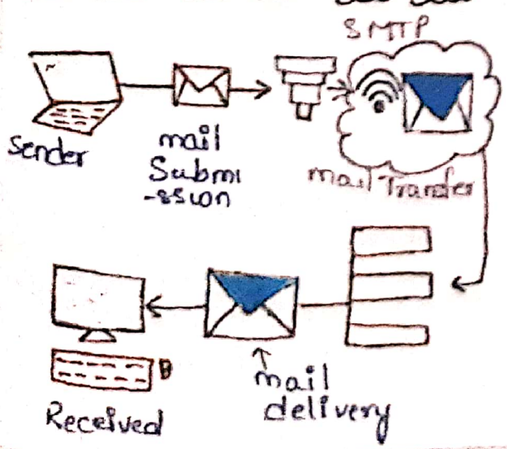
- Message request Protocol
- Establish the connection client/server.

Characteristics:-

- Open Protocol – RFCs.
- It allows access platform types
- Even offline download and delete will supports.
- No mail gateways



Architecture of E-MAIL:-

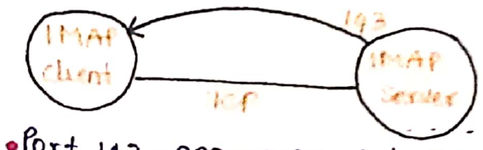


Network:-

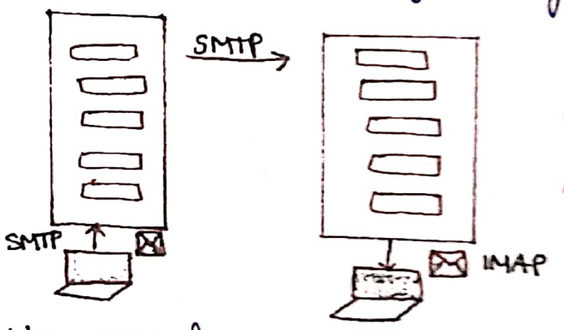
- Base stations
- Client equipment
- Network switches
- Routers
- Fire wall

⇒ IMAP :- [Internet Message Access Protocol]

- It follow client/server model



- Port 143 – non-encrypted IMAP Port
- Port 993 – Connect through securely



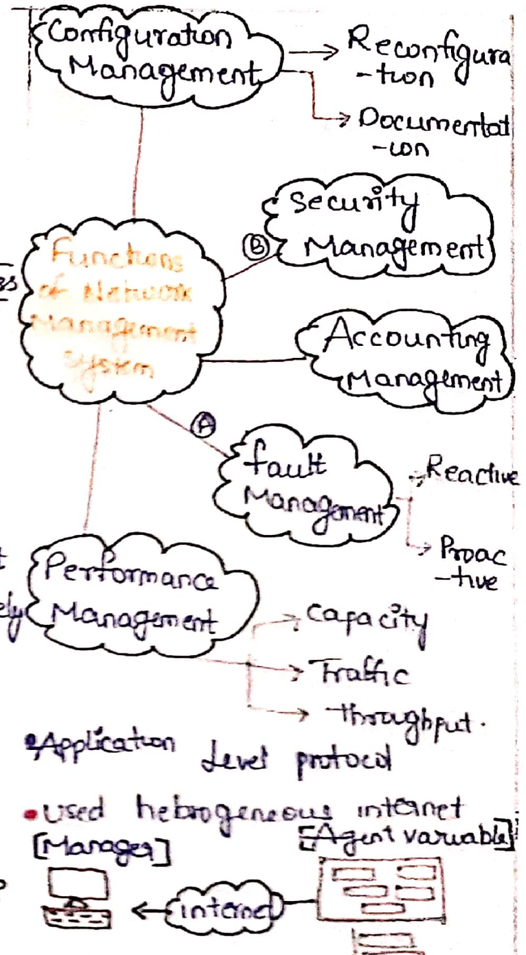
- Uses TCP for communication to ensure the delivery

Simple Network Management System [SNMP] :-

- It Monitoring configuring testing and trouble shooting

Components :-

- Structure of Management Information SMI
- Management Information Base MIB



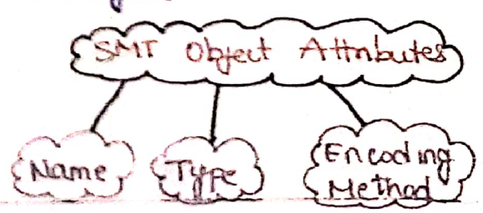
- Application level protocol
- Used heterogeneous internet

Basic ideas:-

- Checks behaviour of agent
- Resetting values in agent database
- warning the manager for unusual situation

Roles of SNMP:-

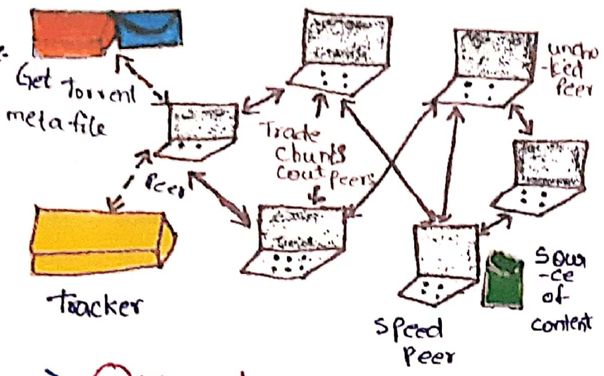
- Exchange packet b/w Manager and agent

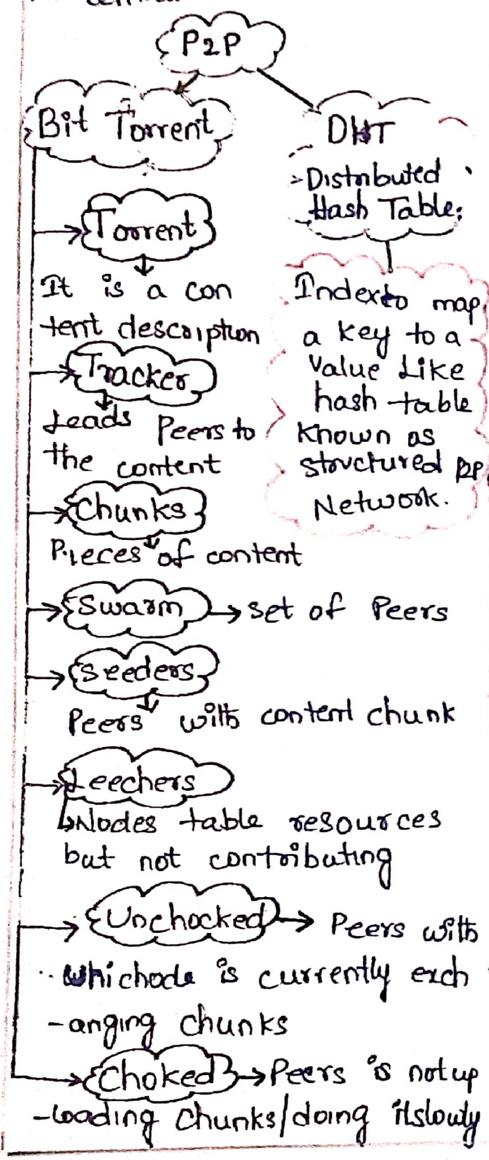


P2P Peer to Peer, Over Lay, SSL [Secure Socket Layer] & DOS [Denial of Service]

⇒ P2P Peer to Peer Network

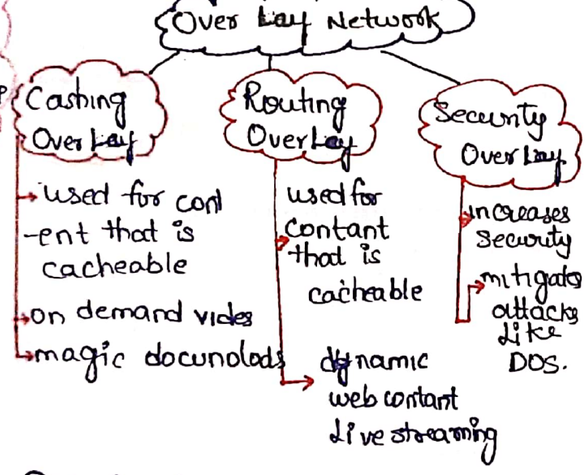
- Many computers come together & share keysources
- Can act as a client and Server
- No dedicated infrastructure
- No central can't as control





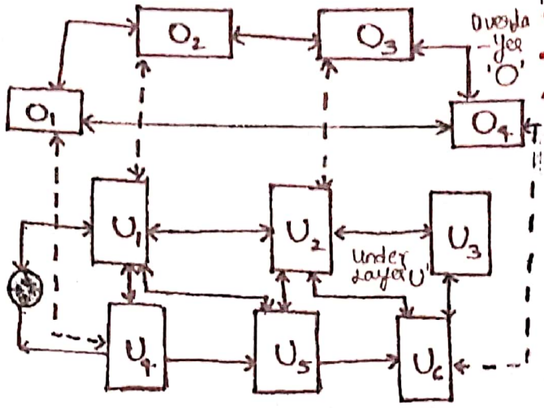
⇒ Over Lay Network

- Connects isolated hosts and networks using other networks.
- It is overlaid on the base Network
- VPN is a overlay network on top of Public network.



Disadvantages:
- Extra layers of management
- needs trouble shooting for both over-key & underkey

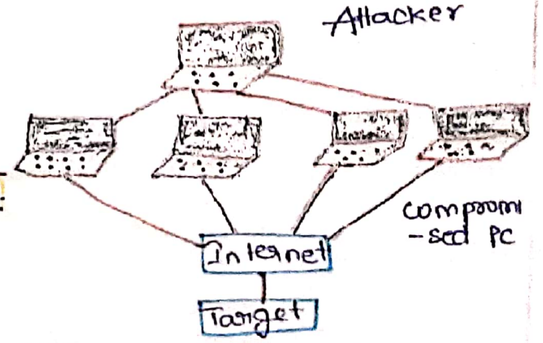
Advantages:
- Central storage of Data
- Faster Problem-Solving
- Reliability



- III - client encryption key
- IV - Server encryption key
- V - client initation vector
- VI - Server initation vector

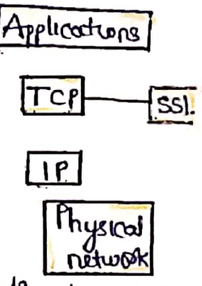
⇒ DOS [Denial of service]

- intreder's goal is to shut down the target
- request have false source addresses
- Sends legitmate Packets in great nums.
- do it till traget collapse.



⇒ SSL [Secure Socket Layer]:-

- Protocol to Provide securety at the transport layer.
- Uses mostly HTTP
- Content from application is compressed (optimal), signed and encrypted



Fragmentation:- • SSL divides data 2^{14} bytes.

Message integrity:- • Uses a keyed-hash function to create MAC.

Confidentiality: • Original data & MAC are encrypted using symmetric key cryptography

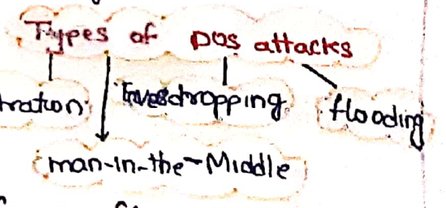
Framing: • A header is added

Cipher suite:- • Starts with SSL followed by key exchange algorithm

Cryptographic secrets:- • SSL uses six secrets.

- I - Client authentication key
- II - Server authentication key

DDOS - [Distributed DOS]:-
- When an attaker b creates into many systems
- Commands all to attack the same target.



Buffer overflow attacks
- ICMP flood
- SYN flood
  - It is difficult to identify the attacker in DDOS
- Targets → • Banks, commerce media government organisations

VOIP & FIREWALL

VOICE OVER IP (or) INTERNET TELEPHONY

↳ Real time interactive audio/video application.

↳ Communication over packet switched network.

Two Protocols :-

- SIP - Session Initiation protocol.
- H.323

1. Session Initiation Protocol (SIP) : (IETF standard)

→ Application Layer Protocol.
→ Establishes, manages & terminate multimedia session.
→ Used to create two party, multiparty session.
→ Run on UDP, TCP.

SIP MESSAGES

Invite, Ack, Bye, Options, Cancel, Register

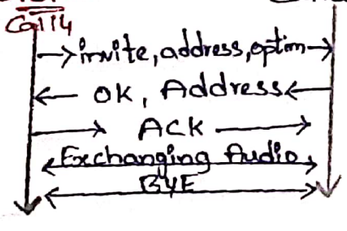
SIP Addresses :- (FORMATS)

sip: bab@172.18.10.2 | sip: bab@gmail.com

sip: bab@91-9847508344

SIP - SIMPLE SESSION :-

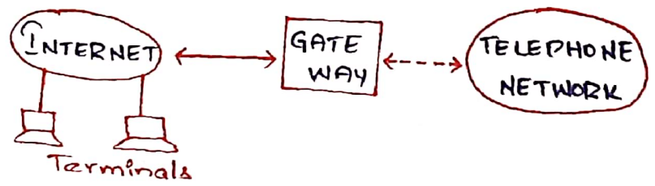
→ Establishing
→ Communication
→ Terminating



2. H.325 PROTOCOL :-

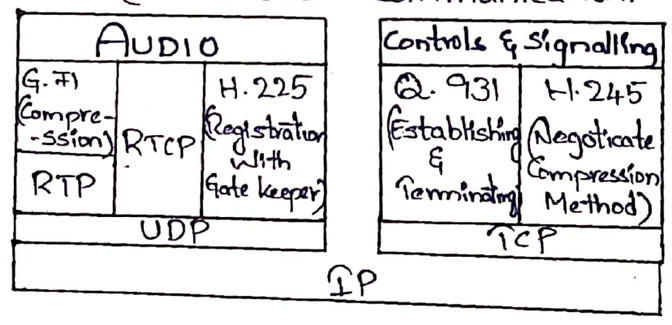
→ ITV standard.
→ Allow telephone talk to Computers connected to internet.

H.323 Architecture :-

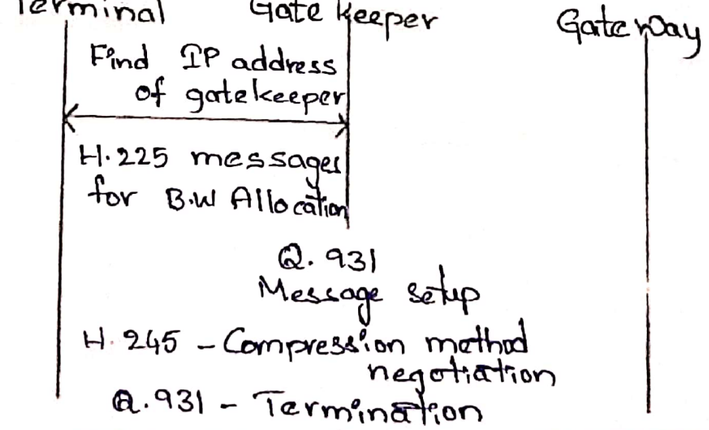


H.323 PROTOCOLS :-

→ Establish and maintain Voice (or) Video Communication.

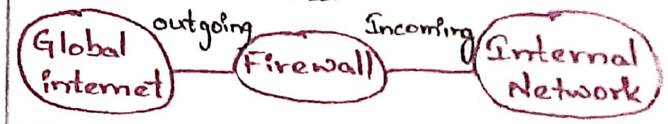


H.323 OPERATION :



* FIRE WALLS :-

→ Device installed between internal network and rest of internet.
→ Forward some packets &,
→ Filter others.



TYPES :-

PACKET FILTER
⇓
N/W (or) Transport Layer
⇓
Forward (or) block packed based on IP & Port Addresses
⇓
Uses filtering table to decide packets discarded (or) forwarded

PROXY
⇓
Application Layer
⇓
Filter based on information available in the message itself.

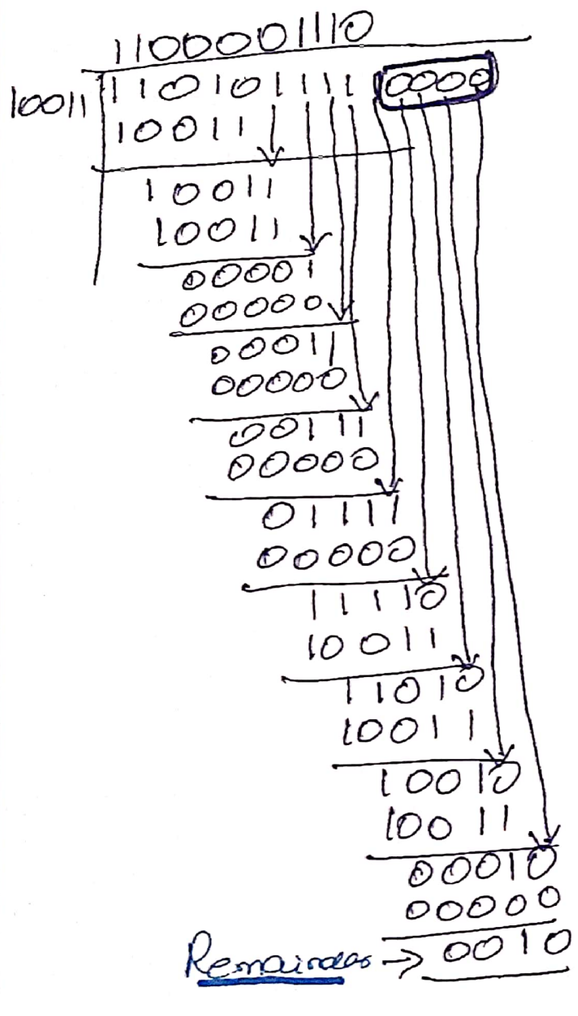
CIRCUIT LEVEL
⇓
OSI Hatal Session Layer
⇓
Easily Configu-ration.
⇓
Allow (or) block traffic without significant resources.

↳ The main perpose of firewall is to allow non-threaterning traffic in & keep dangerous traffic out.
↳ Firewalls can be Software or Hardware.
↳ Enables user to easily handle and update Security protocols.

Cyclic Redundancy Check (CRC)

Data: 11010111111

G(x): 10011



Remainder → 0010

Transmitted data

11010111111 0010

$G(x) = 10011$

$= x^4 + x + 1$

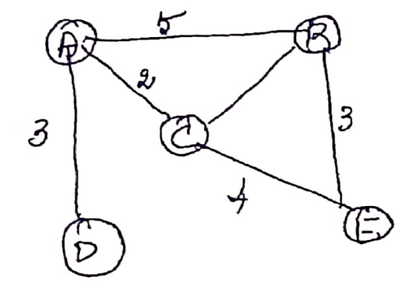
If $G(x) = x^3 + 1$

then $= x^3 + 0(x^2) + 0(x) + 1$

$= 1001$

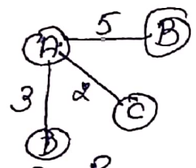
COMPUTER NETWORKS CSA07

Link State Routing



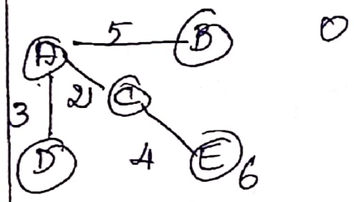
Root

Set A as root

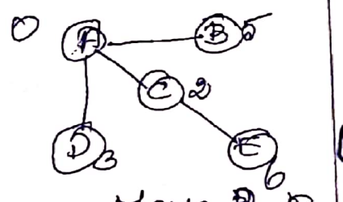


A - Permanent

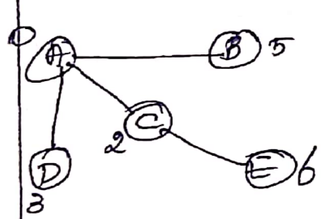
B, C, D - Tentative



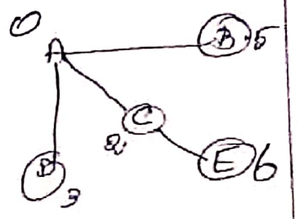
Move C - Permanent



Move D to Permanent



Move B to Permanent



Move E to Permanent

Permanent	Tentative
A(0) C(2)	B(5) D(3), E(6)
A(0) C(2) D(3)	B(5), E(6)
A(0), B(5), C(2), D(3)	E(6)
A(0), B(5), C(2), D(3) E(6)	EMPTY

IP Addressing

1. (a) Change the following IPV4 addresses from dotted decimal to binary

111.56.45.78

01101111 00111000

00101101 01001110

(b) Change the following IPV4 addresses from binary to dotted decimal

10000001 00001011

00001011 11101111

129.11.11.239

2. Find the error, if any in the following IP4 addresses

1. 111.56.045.78

↓

no leading zero

2. 221.34.7.8.20

No numbers more than four

3. 75.45.301.14

Each number needs to be less than or equal to 255.

4. 11100010.24.14.68

Mixture of binary & dotted decimal notation not allowed

3. Find the class of each address

(a) 00000001 00001011

00001011 11101111

The first bit is zero

∴ class A address

(b) 11000001 10000011

00011011 11111111

The first 2 bits are 11 & third is 0 ∴

class C address

(c) - 14.23.120.8

First byte is 14 ∴

class is A

(d) 252.5.15.111

First byte is 252

the class is E.

4. What is the Subnet addr if the destination address is 200.45.34.56

Subnet mask is

255.255.240.0

11001000 00101101 00100010

. 00111000

11111111 11111111 11110000

00000000

11001000 00101101 00100000

00000000

The subnet address is

200.45.32.0.

GATE QUESTIONS

COURSE CODE: CSA07, COURSE NAME: COMPUTER NETWORKS

(1) A bit stuffing based framing Protocol uses an 8-bit delimiter Pattern of 01111110. If the output bit String after Stuffing is 011111001011, then the input bit String is

(A) 0111110100
(B) 011111011
(C) 0111111101
(D) 0111111111

Correct Answer : 'B'

Since the output bit string after Stuffing is 011111001011

(2) A Computer on a 10mbps Network is regulated by a token bucket. The token bucket is filled at a rate of 2 Mbps. It is initially filled to Capacity with 16 Megabits. What is the max. duration for which the Computer can transmit at the full 10mbps?

(A) 1.6 Seconds
(B) 2 Seconds
(C) 5 Seconds
(D) 8 Seconds

Correct Answer : 'B'

Since, Capacity of token bucket (b) = 16 Mbits
Maximum Possible transmission rate (M) = 10mbps
So, the maximum burst time = b/(M-r)
= 16/(10-2) = 2 Seconds

(3) Consider an instance of TCP's AIMD Algorithm where the window Size at the Start of the Slow Start Phase is 2 MSS and the threshold at the Start of the first transmission is 8 MSS. Assume that a time out occurs during the fifth transmission. Find the Congestion window size at the end of the tenth transmission.

(A) 8 MSS
(B) 14 MSS
(C) 7 MSS
(D) 12 MSS

Correct Answer : 'C'

Since, Slow Start is used, window Size is increased by the number of Segments Successfully Sent. In both of the above Situation, window Size will be increased linearly. If there is timeout, window Size will be reduced to half.

(4) An organization has a class B Network and need to form Subnet for 64 departments. What would be the appropriate Subnet Mask

(A) 255.255.0.0
(B) 255.255.64.0
(C) 255.255.128.0
(D) 255.255.252.0

Correct Answer : 'D'

Since organization has a class B, Network, in class B 16 bits are used for host ID and 16 bits are used for Network ID. Since organization went to form 64 Departments So 6 bits are used to identify the 64 departments So Subnet mask will be
11111111.11111111.11111100.00000000
which is 255.255.252.0

(5) How many networks Can be allowed in class C under IPV4?

(A) 2^{14}
(B) 2^{17}
(C) 2^{21}
(D) 2^{24}

Correct Answer : 'C'

Since we know that under IPV4 IP addressing in class C, 32 bits IP address consist two Parts host ID, N/w ID, 8 bits are used for host ID and 24 bits are used for N/w ID. Among these 24 bits 3 bits are fixed as 110 SP remaining 21 bits are used to form Networks

(6) A 2km long broadcast LAN has 10^7 bps bandwidth and uses CSMA/CD. The Signal travels along the wire at 2×10^8 m/s. what is the minimum Packet Size that can be used on this Network?

(A) 50 Bytes (C) 200 Bytes
(B) 1000 Bytes (D) None of the Above

Correct Answer : 'C'

Total distance for RTT = 4 km
Transfer rate = 2×10^8 ms^{-1}
Time to transfer = 2×10^{-5} Sec
Data rate = 10^7 bps
Packet Size = $2 \times 10^{-5} \times 10^7$ bytes
= 200 bytes

(7) How many 8 bit Characters Can be transmitted Per Second over a 9600 band Serial Communication link using esynchronous mode of transmission with one Start bit, eight bits and one parity bit?

(A) 600 (C) 800
(B) 876 (D) 1200

Correct Answer : 'C'

Since, Band is the Symbol which is Sent over the link, band = 9600 bits 1 8 bit Character has 12 bits So, band Size of no. of Characters = 9600/12
= 800

(8) Suppose the round trip Propagation delay for a 10mbps Ethernet having 48 bit jamming Signal is 46.4 μs. The minimum frame Size is

(A) 94 (C) 464
(B) 416 (D) 512

Correct Answer : 'D'

Link Speed = 10 mbps
Delay = 46.4 μs
Total bits transfered = $10 \times 46.4 \times 10^6 \times 10^{-6}$
= 464 bits
But 48 bit jamming signal also required. So frame Size = 464+48
= 512 bits

Subnet Example.

Host IP address: 138.101.114.250

Network mask: 255.255.0.0

Subnet Mask: 255.255.255.192

Step 1 Translate host IP address & Subnet mask into binary

	138	101	114	250
Ip	10001010	01100101	01110010	11111010
Mask	11111111	11111111	11111111	11000000
	255	255	255	192

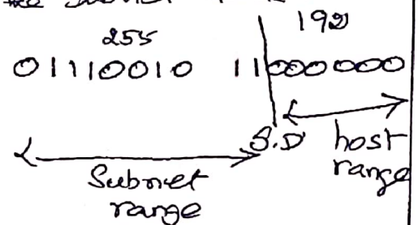
Step 2: Find the Subnet address

Perform bitwise AND on IP address and Subnet mask.

10001010 01100101 01110010 11111010
11111111 11111111 11111111 11000000
10001010 01100001 01110010 11000000
138 101 114 192

Step 3: Subnet range / Host range

- use network mask 255.255.0.0 and Circle divide from the rest of the address.
- use Subnet mask 255.255.255.192 and Small divide the Subnets from host between the last 1 and the first 0 in the Subnet mask.



Step 4: First host / Last host.

First host	138	101	114	193	11000000 (193)
Last host	138	101	114	254	11111110 (254)
Broad Cast	138	101	114	255	11111111 (255)

COMPUTER NETWORKS

TCP

1. a) Calculate the effective throughput for transferring a 1000kB file assuming TCP using slow start congestion Control. Given the round trip time 100 ms, & the maximum segment size is 1460 bytes. Assume there are no losses and both the bandwidth and the receiver window size is infinite.

MSS - max. Segment Size = 1460 B

RTT = 100 ms

CWND Size approximately double on every RTT

Number of MSS to send
= 1000kB / 1460B ≈ 685.

1 MSS → 1 RTT
2 MSS → 2 RTT
4 MSS → 3 RTT
8 MSS → 4 RTT
16 MSS → 5 RTT
32 MSS → 6 RTT
64 MSS → 7 RTT
128 MSS → 8 RTT
256 MSS → 9 RTT
(511 MSS sent till now)
Remaining 685 - 511 = 174.
174 MSS → 10 RTT

Total time to send 685 MSS
= 10 × RTT = 1000 ms.

Total Data Sent = 1000kB.

Throughput = Total data Sent / Total time
= 1000kB / 1.000 × 10^3 sec
= 1 Mbps

CSA07

1(b). If the size of the TCP segment is 1kB and header length value is 6, seq no = 3500 URG flag = 1 & URG Pointer = 45 Then what is the total size of the data. How many of them are urgent. Give the Sequence numbers of urgent data.

Solution:

URG Pointer = 45, then upto the Sequence number 3500 + 45 = 3545 data is urgent ie total of 46 bytes

46 bytes of urgent data

Sequence number is 3500-3545

UDP Header.

The following UDP header (in Hex)

06 32 00 0D 00 1C E2 17

a) What is the source port number
b) Destination port number
c) Length of UDP d) Length of data.
a) Source Port = $0632_{16} = 1586$
b) Destination Port = $000D_{16} = 13$
c) Total length = $001C_{16} = 28$ bytes
d) Header is 8 bytes, ∴ data length is 28 - 8 = 20 bytes.
e) The IP header is minimum 20 bytes ⇒ Payload of 65515 bytes. To fit a UDP header of 8 bytes, we get data
65515 - 8 = 65507 bytes.

UDP has four parts source port, destination port, length & Checksum.

Comparison of TCP & UDP

1. A client uses UDP to send data of 16 bytes. Calculate the efficiency (Ratio of useful bytes to total bytes).
2. A client uses TCP with 16 bytes. Calculate the efficiency. (No options)

1. UDP header is 8 bytes the ratio is 16/16+8 = 2/3

2. TCP 16/20+16 = 4/9.

3. Suppose TCP operates over 1 Gbps link.

a) How long TCP would take the sequence numbers to wrap around. Completely. Sequence number is 32 bit. At most there will be 2^{32} bytes in 1 Gbps link. The transmission time is $(2^{32} \times 8)/(1 \times 10^9) = 34.36$ sec

(b) Suppose an added 32 bit timestamp field increments 1000 times during the wrap around time of 34.36 sec. How long could it take for the timestamp to wrap around?

Each increment of time stamp = 34.36/1000 = 34.36 ms

Total time = $34.36 \times 10^{-3} \times 2^{32}$
= 1.48×10^8

One year = 31,556,952 sec
= $1.48 \times 10^8 / 31556952$
= 4.68 year

Adding timestamp, it will

Analog & Digital Signals

Wavelength = $\frac{\text{Speed of Propagation}}{\text{Frequency}}$

$$\lambda = \frac{c}{f}$$

(1) When frequency $f = 4 \times 10^6$ Hz

Find the wavelength

$$\lambda = \frac{c}{f} = \frac{3 \times 10^8}{4 \times 10^6} = 0.75 \times 10^{-6} \text{ m}$$

$\lambda = 0.75$ micro m.

(2) A Periodic Signal has a bandwidth of 20 Hz. The highest frequency is 60 Hz. What is the lowest frequency?

Bandwidth $B = f_H - f_L$

$20 = 60 - 2$

$f_L = 40$ Hz

(3) Assume we need to download text documents at the rate of 100 pages per minute. What is the required bit rate of the channel.

A page is an average of 24 lines with 80 characters in each line. Assume that one character requires 8 bits

The bit rate is

$100 \times 24 \times 80 \times 8 = 1.636$ Mbps.

(4). A line with a bandwidth of 3000 Hz assigned for data communications. The Signal to Noise to ratio (SNR) is 3162. Find the capacity (highest bit rate) of this line.

Shannon Capacity

$$C = B \log_2 [1 + SNR]$$

$$= 3000 \log_2 [1 + 3162]$$

$$= 3000 \times 11.62 \simeq 34860 \text{ bps}$$

$$\log_2 x = \log_{10} x / \log_{10} 2 = \frac{\log_{10} x}{0.3}$$

5. Throughput.

A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10000 bits. What is the throughput of this network?

$$\text{Throughput} = \frac{12000 \times 10000}{60}$$

$= 2$ Mbps.

Bandwidth is 10 Mbps

∴ Throughput is $\frac{1}{5}$ of the bandwidth.

Propagation Time

$$\text{Propagation Time} = \frac{\text{Distance}}{\text{Propagation Speed}}$$

6) What is the Propagation time if the distance between the two points is 12000 KM? Assume the Propagation Speed in the cable is 2.4×10^8

$$\text{Propagation time} = \frac{12000 \times 1000}{2.4 \times 10^8}$$

$= 50$ ms

Transmission Time

$$\text{Transmission time} = \frac{\text{Message size}}{\text{Bandwidth}}$$

7) What are the Propagation time and transmission time for a 2.5 kbyte message (an e-mail) if the bandwidth of the network is 1 Gbps. The distance is 12000 KM & speed is 2.4×10^8 m/s

$$\text{Propagation time} = \frac{12000 \times 1000}{2.4 \times 10^8}$$

$= 50$ ms.

$$\text{Transmission time} = \frac{2500 \times 8}{1 \times 10^9}$$

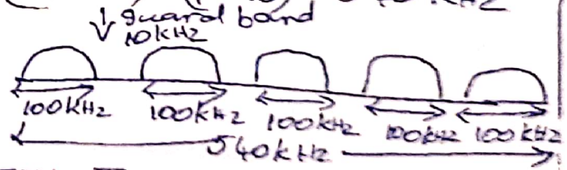
$= .02$ ms.

FDM - Frequency Division Multiplexing

8) Five channels each with 100 kHz bandwidth are to be multiplexed together. What is the minimum bandwidth of the link if there is a need for a guard band of 10 kHz between the channels to prevent interference

The required bandwidth

$= (5 \times 100) + (4 \times 10) = 540$ kHz



TDM - Time Division Multiplexing

9) In TDM, each frame carries 1 byte from each channel. Four channels are there. The size of each frame is $4 \times 1 = 4$ bytes = 32 bits. Each channel is sending 100 bytes/sec. Find the bit rate.

The frame rate is 100 frames/sec since each frame contains 32 bits, bit rate $32 \times 100 = 3200$ bps

ALOHA

The throughput for Pure ALOHA

$S = G \times e^{-2G}$

G → average number of frames generated.

10) A Pure ALOHA network transmits 200 bit frame on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces 1000 frames per second.

If system creates 1000 frames/sec

$S = G \times e^{-2G} = 0.135$.

Throughput $= 1000 \times 0.135 = 135$ frames

Only 135 frames out of 1000 will probably survive

Slotted ALOHA

The throughput for Slotted ALOHA $S = G \times e^{-G}$.

11) A Slotted ALOHA network transmits 200 bit frames using a shared channel of 200 kbps bandwidth. Find the throughput if frame transmission time is $200/200$ kbps $= 1$ ms

$S = G \times e^{-G} = 0.368$

The throughput is $1000 \times .368$

$= 368$ frames

Only 368 frames out of 1000 frames will probably survive

$G = 1$

$S = 1 \times e^{-1} = \frac{1}{e} = 0.368$

$S = 36.8$ percent.

1. Consider sending a large file of F bits from host A to host B. There are three links and two switches between A & B and the links are not congested.
Segment Size = S bits
Header Size = 80 bits
Length of the Packet = 80+S
Transmission rate = R bps
Find the value of S that minimizes the delay of moving the file from host A to host B. Disregard Propagation delay.

Ans File Size = F
Number of Segments = F/S
Transmission delay
$T_{delay} = L/R = (80+S)/R$ seconds
Time(T) required for the first Packet to receive
$T = T_{delay} \times$ Number of links
$= (80+S)/R \times 3$
$T = L/R \times 3$

2. An organization is granted the block 16.0.0.0/8. The administrator wants to create 500 fixed length Subnets.
i) Find the Subnet mask
ii) Find the number of addresses in each Subnet
iii) Find the first and last address in the first & last Subnet.

Ans (i) The number of Subnets needs to be the power of 2.
$2^9 = 512$
We need 9 more extra 1's. Possible Subnets = 512
The Subnet Prefix is /17
The Subnet mask is 255.255.128.0
(ii) Each Subnet has $2^{32-17} = 2^{15} = 32,768$ addresses
(iii) First address is the beginning of address of the block.
The first address in Subnet 1 is 16.0.0.0
To find the last address write 32767 in base 256
$= 0.0.127.255$
∴ Last address in Subnet 1 is 16.0.127.255
Last Subnet
First address in Subnet 1
$= 16.0.0.0$
Number of addresses
$= 0.249.128.0$
First address in Subnet 500 = 16.249.128.0.
Number of addresses
$= 0.0.127.255$
∴ Last address in Subnet 500 = 16.249.255.255

3. A Computer on a 10Mbps network is regulated by a token bucket filled at a rate of 2 Mbps. It is initially filled to capacity with 16Mbits. What is the maximum duration for which the computer can transmit at the full 10Mbps?

Ans Max rate = $\frac{C + rt}{t}$
C → Capacity
r → rate
t → time
$10Mbps = \frac{16Mb + (2Mbps \times t)}{t}$
$10Mbps\,t - 2Mbps\,t = 16Mb$
$8Mbps\,t = 16Mb$
$t = 2$ seconds

4. A Packet has arrived with (a) M bit Value of 0
(b) M bit Value of 1
(c) M=1, fragmented offset is 0
(d) Offset Value = 100
(a), (b) & (c) → Find is this the first, or last or middle fragment. (d) Find the number of first and last byte.

Ans M → more fragments
(a) M=0, so no more fragments, hence this is the last fragment or may be the Packet was not fragmented.
(b) M=1 → more fragments this fragment may be first or middle one but not last one.
(c) M=1, offset = 0
This is the first fragment
(d) Offset value = 100.
Multiply offset value by 8.
First byte number = 800
Last byte number can be calculated Provided the length of the data is known.

1. In an IPV4 Packet, the value of HLEN is 1000 in binary.

a) How many bytes of option are carried by this Packet

b) HLEN = 5_H & the value of total length field is 0028_H. How many bytes of data are being carried by this Packet?

c) An IPV4 Packet has arrived with the first 8 bits as 01000010. The receiver discards the Packet. Why?

Ans

HLEN → Header length

(a) HLEN = 1000 = 8

$\therefore 8 \times 4 = 32$ bytes

(b) $5_H = 5$

$0028_H = 40$

Total number of bytes in the header $= 5 \times 4 = 20$ bytes

Data carried by the Packet $= (40 - 20) = 20$ bytes

(c) IPV4 → 01000010

The 4 leftmost bits 0100 is the Version which is correct. The next 4 bits 0010 ($2 \times 4 = 8$) incorrect header length.

2. HTTP is stateless and inband. Do these factors make HTTP a better Protocol or not?

Ans

HTTP is stateless it does not have a memory of previous requests, it reduces response time and complexity.

HTTP is inband means both control and data are transmitted in a single band which saves bandwidth reduces the time and saves the bandwidth. Thus these two factors help HTTP.

3. Slotted ALOHA totally Prevents Collision of frames. Do you agree with this statement? Validate your answer.

Ans

In ALOHA, users can transmit frames at random time.

- High Probability of collision.
- In slotted ALOHA, a user is allowed to send a frame only at the beginning of a time slot. So, Probability of collision is reduced. But when two users are ready with the frame and trying to send them at the beginning of the time slot, there will be a collision.

So slotted ALOHA reduces collision but cannot totally Prevent it.

4. In designing a network that handles multimedia traffic alone, would you prefer TCP or UDP Substantiate your answer.

Ans. In dealing with multimedia traffic speed is important rather than the integrity of the data like audio or video. So UDP is preferred over TCP in this case since UDP is faster than TCP but less reliable than TCP.

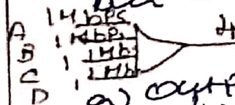
5. a) In designing a link from Chennai to Tirupati to support 1 Mbps data rate, Engineer A uses optical fiber and Engineer B uses coaxial cable. Whose design, A or B is better? Justify your answer.

To transmit 1 Mbps over a nearly 200 KM link, may be the coaxial cable copper links can be chosen since it is the cost effective design. If the data rate required increases in future, copper cables can be replaced by optical fiber cables.

b) In TDM, there are four channel each with 1 Mbps input rate.

a) Find the output data rate

b) Find the input & output bit duration.



a) output data rate $4 \times 1 = 4$ Mbps

(b) $\frac{1}{1 \text{ Mbps}} = 1 \mu s$

$\frac{1}{4} = 0.25 \mu s$

o/p bit duration