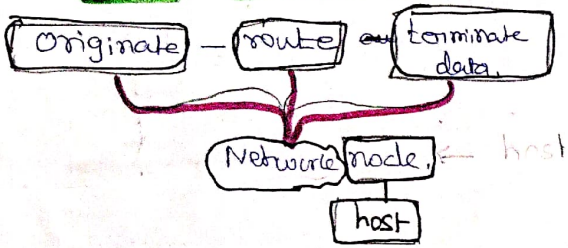
Introduction to Networks and Communication media

Protocol standard

Network and Communication Media:

- Computer or data network is a telecommunication network that allows to exchange data.

* Network computer device



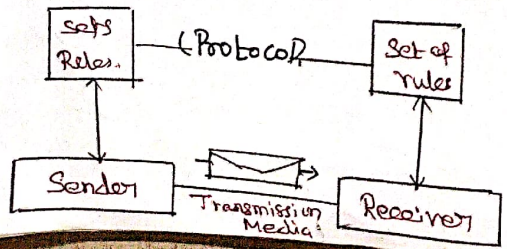
Data Communication:

- It is a process of exchange data

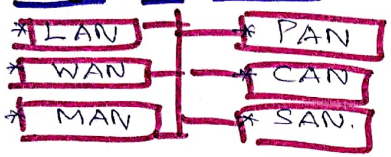
Characteristics:-

* Delivery
* Accuracy
* Timeliness
* Jitter

Components:-



Categories of Network:



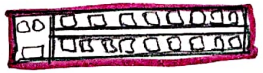
Network Hardware:-

Network Card - Provide over a [NIC] Computer connection over a Nlw 10/100/1000 Mbps

Bridge:

LAN to Another LAN. that use Same Protocol.

Switch:- Hardware device that Joins multiple Computer together with LAN



Router: A hardware device designed to take incoming packets, analyze the packet, moving the packet to another Nlw.

Repeater: It regenerate incoming signals to extend range of LAN.

Network Software:-

- All Computer systems implement their protocol as part of OS.
- Exports the network functionality, API.

API Specifies ways

* Create Sockets
* attach the Socket
* Send / receive
* Close the Socket

Type of Connection.

Point-to point - dedicated link.

multipoint - Shared a Common link.

Protocol:

Set of rules that determine how data to be transmitted b/w device in the network.

STANDARDS IN NETWORKING

- Standard provide guidelines to product Manufactures

De facto :- * by fact or Convention
* Not approved by any organized body.

De jure :- * By Law or regulation
* approved by body that is officially recognized.

Example of Standard create Committees.

* ISO
* ITU-T
* ANSI
* IEEE
* EIA [Electronic Industries Associates]

Example Forum

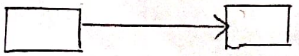
* ATM
* MPLS
* Frame relay

Regulatory Agencies

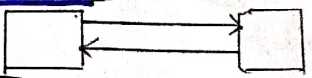
- Federal Communication Committee (FCC)

Direction of Data flow

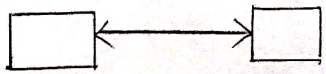
Simplex



Half duplex



Full duplex



Topology

Defn:

- Arrangement of Networks that Comprises nodes and Connecting line.

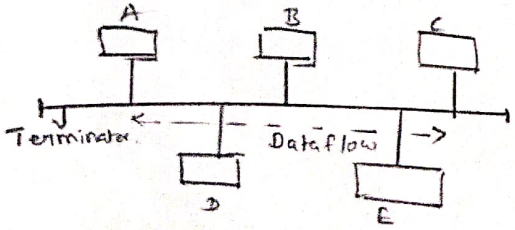
Network Topology - Types

- Bus
- Ring
- Star
- Mesh
- Tree

Bus Topology

All devices share single Communication line or Cable.

- Use CSMA/CD or one host as Master to Slave.



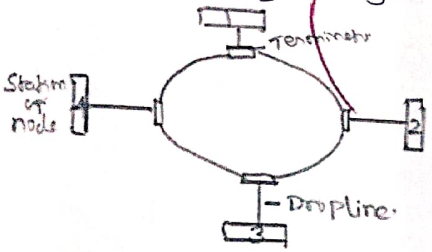
Adv: If N devices are Connected to each other in bus - Cables - 1 and N drop lines. (n-1)

Problem: - network Traffic is heavy increase Collision
- Cable fails, Entire N/w Crash down.

∞

RING Topology:

- It forms a ring Connecting devices with exactly two neighboring devices.
- Transmission is unidirectional.
- Use Token Ring Passing Protocol



- For n devices in a network n cables are required

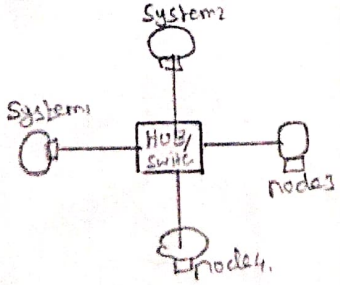
Adv: * Possibility of Collision is minimum
* Cheap to install and expand

Problem:
* Trouble Shooting is difficult in this topology
* Less secure

∞

STAR Topology

All the devices are Connected to a Single hub through a cable.



Adv:
- If N device are Connected, number of Cables required N.
- Each device requires only 1 port.

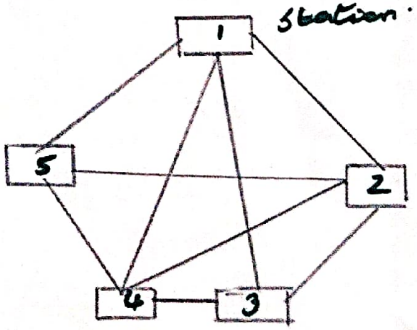
Problem: - Cost of installation is high
- If the Concentrator (Hub) on which the whole topology fails.

* It is robust, if one link or node fails only that link will affect.
* Easy to fault identification and fault isolation.

∞

Mesh Topology

- Every device is Connected to another device via a particular channel.
* Uses the protocols AHCPC ad Hoc Configuration protocol) DHCP, etc.



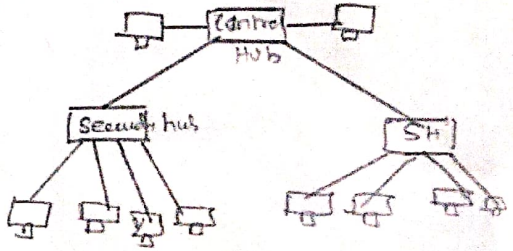
* Suppose, N number of devices are Connected with each other. total Number of port required by each device is N-1.
- Total Number of Ports required N(N-1).
* Suppose, N Number of devices are Connected with each other. Total Number of dedicated link required is $^{N}C_2 = N(N-1)/2$
- 5 devices Connected each other $5*4/2 = 10$.

Adv: * Provide security and Privacy
* Fault is diagnosed easily

Problem * Installation and Configuration are difficult.
* maintance cost is high.

Tree Topology

It is the variation of Start topology and as hierachical flow of data.



Adv: - It allows more devices to attached
- It allows to get isolated and also Prioritize from different Computer.

Problem: Cost is high because of Cabling

∞

Hybrid Topology.

It Contains a Combination of all different types of networks.
- Example Internet.

OSI Model - TCP/IP Model.

OSI Model:

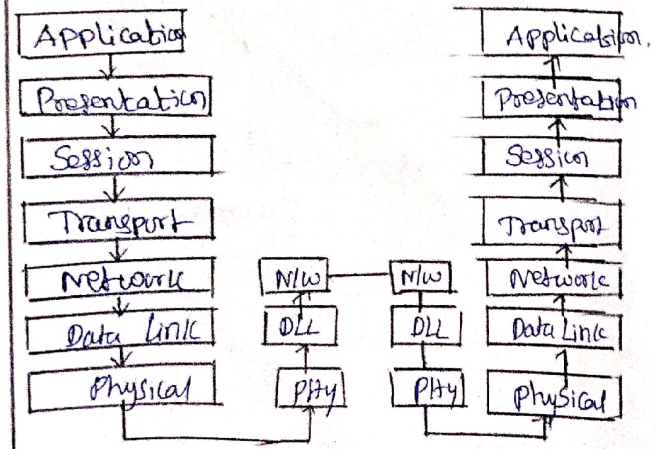
- Internal Function of Communication
- Conceptual model.
- layered Approach.

Application layer
Presentation
Session.
} Software Layers

Transport layer - Heart of OSI

Network layer
Data Link layer
Physical.
} Hardware layers.

Reference Model:



Physical layer

- Connection b/w devices

Function
- Bit Synchronization
- Bit rate control
- Transmission mode
- Topologies

Data Link Layer

- node to node delivery

Two Sublayers
- LLC — Logical Link Control.
- MAC — Media Access Control

Function
- Framing
- Physical Addressing
- Flow Control
- Access Control

Network:

- Host to Host Connection.

Function — Routing
- Logical Addressing

Transport layer:

- Process-to-process Communication
- TCP and UDP
- retransmit data if an error.

Session layer:

- maintenance of Session.

Function
- *Synchronization
- Dialog Controller.

Presentation:

- Encryption / Decryption
- Compression.

Application:

- Service to service Communication

Function:
- Virtual Terminal
- mail Services
- Delivery Services

TCP/IP

- Control protocol with internet protocol.

Application	SMTP	FTP	HTTP	
		DNS		
Transport	SCTP	TCP	UDP	

Network (Internet)
- ICMP
- IGMP
- IP
- ARP
- RARP

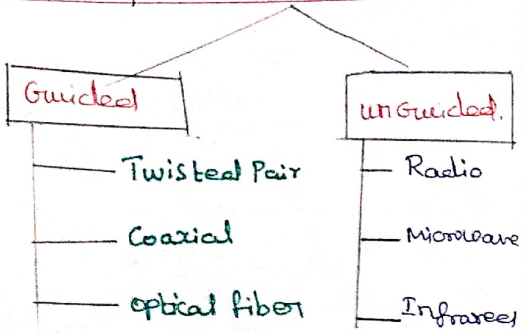
Network Interface
- Host-to Host N/w

* Connection oriented
* reliable delivery
* Stream oriented

Transmission Media

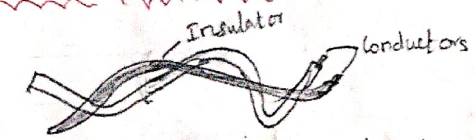
A transmission medium is a physical path between the transmitter and the receiver.

Types of Transmission Media



Guided Media: Contained with physical boundaries.

Twisted Pair Cable:

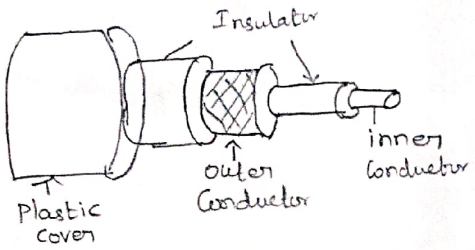


- It Consists of two conductor, each with its own plastic insulation

Characteristics:
* Repeater every 5-6 km (for along signal) or 2-3 km (for digital signal)
* Cable Shielded or unShielded
* Crosstalk problem might occur

Coaxial Cable:

- Carries signals of higher frequency ranges than twisted Pair cable.
- Frequency range 100 Khz to 500MHz



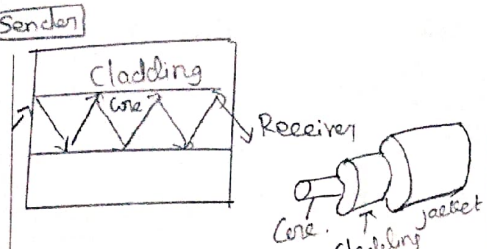
* 50 ohm cable - Baseband
* 75 ohm cable - Television Broad band Coaxial Cable.

Performance: * Higher bandwidth

Application:
- Telephone Systems for long distance lines
- Cable Tv networks and Traditional Ethernet LAN.

Fiber optic Cable:

- transmit signal in the form of light.
- A fiber is made of glass or plastic and transmit signals in the form of light.



- At the center is a glass core, through which the light propagates.

UnGuided Media

The Media is usually not directional, like air, space, etc.

Wireless Transmission:

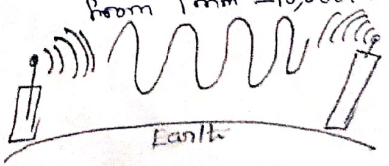
It involves no physical line established between two or more devices.

Radio:

* easy to generate and because of its large wavelength it can penetrate through wall and structures.

Frequence range - 3Hz to 300Hz (or 1GHz)

from 1 mm - 10,000 km.

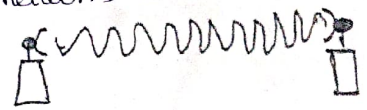


Microwave Transmission:

Electromagnetic waves having frequency between 1 and 300 GHz.

* unidirectional and line of Sight.
* VHF cannot Penetrate walls

Application:
Cellular phones, Satellite networks and Wireless LANs.

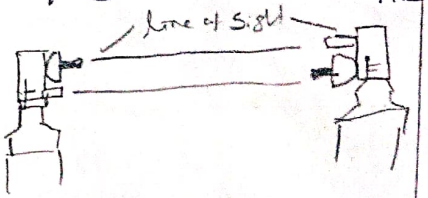


Infrared

wave lies in between Visible light spectrum and microwaves.

wave length - 700nm to 1mm

frequency range - 300GHz to 430 THz



Laser works as Tx (transmitter) and photo-detectors works as Rx (receiver).

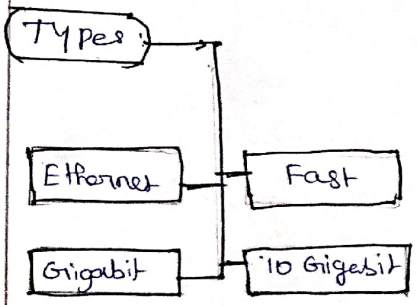
* we cannot use Infrared waves outside a building because sun rays that can interfere with communication.

Application:
- keyboard, PCs, Pointers.
- very high data rate.

Ethernet Standard - Interface and Configuration

Ethernet Standard:

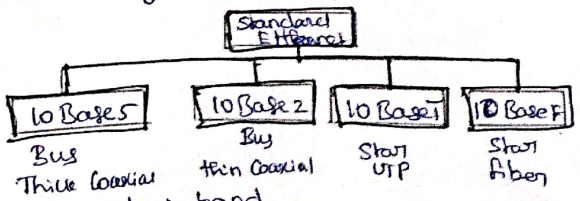
An Ethernet Standard describes the properties, functions and implementation a specific media type



Ethernet:

It is most popular physical layer LAN technology in use today.

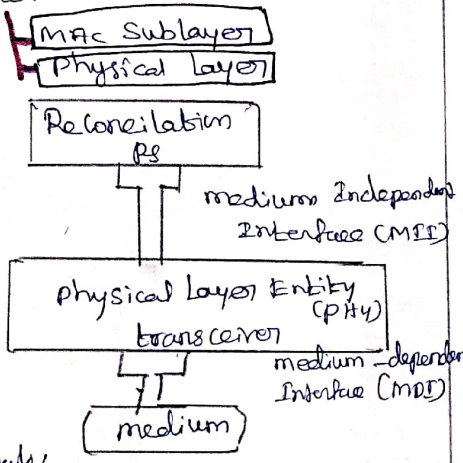
- It can transmit data rate up to 10 Megabits (10mbps).



10 Base 5 → base band.
→ Stands for 500 meters (broadband) maximum length.
↳ Refers for transmission speed

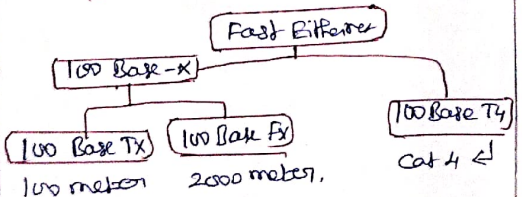
Fast Ethernet:

IEEE 802.3u has been established for Ethernet networks that need higher transmission speed.



Goals:

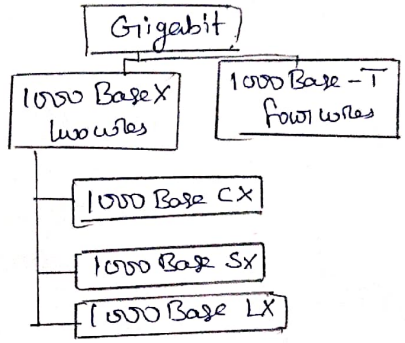
- Data rate - 100 mbps
- 48 bit addresses
- Same frame format



Gigabit:

It was developed to transmit higher data rate, based on Ethernet frame format and protocol used in LAN.

Provides a data rate 1 billion bits per second (1 gigabit)



1000 Base - CX:

- maximum length - 25 meters
- IEEE 802.3z standard
- Use Shielded twisted pair cable

1000 Base - SX

- pair of fiber optic cables of shorter wavelength.
- 770 - 860 nm diameter
- maximum segment length.
- 220 - 550 meters

1000 Base - LX:

- Longer wavelength having 1270 - 1355 nm diameter
- maximum segment length is 500 meters
- Uses NRZ line encoding 8B/10B block encoding.

1000 Base T - use a pair four lanes of twisted pair cables (Cat-5, Cat-5e, Cat-6, Cat-7)

- maximum segment length - two meters
- uses trellis code modulation technique.

Ethernet Interface:

It refers to a circuit board in personal or mobile device to connect to LAN.

Configuring network interface involves assigning IP address parameters and hardware dependent values specifying network interfaces.

ip-config-mode identifies the configuration mode.

ip-route manage static routes in the routing table

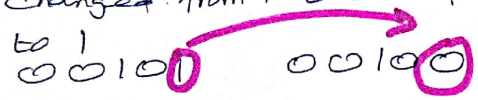
ip-secondary-address - Manage secondary network addresses for the Ethernet interface.

(5.1) Error Detection and Correction

Types of Errors

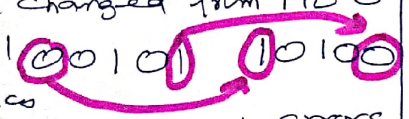
1. Single bit error

Only one bit of a given data is changed from 1 to 0 or from 0 to 1



2. Burst Errors

The term burst error means that two or more bits in the data unit have changed from 1 to 0 or 0 to 1



Redundancy

To detect or correct errors, we need to send extra bits with data.

Error Detecting codes

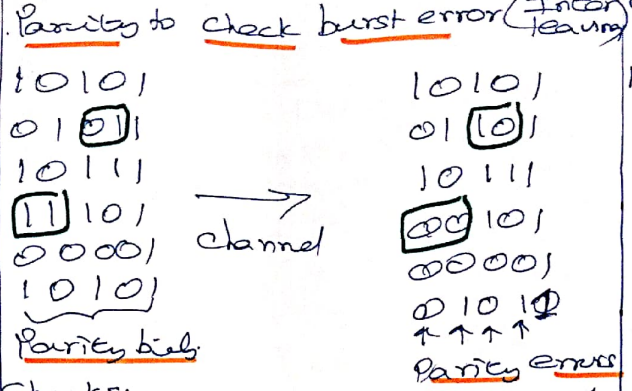
1. Parity
2. Checksum
3. Cyclic Redundancy Check (CRC)

Parity – A single Parity bit is appended to the data. The Parity bit is chosen so that the number of 1 bits in the codeword is even (or odd)

Even Parity → data 1011010 no. of 1 = 4 so zero is added 10110100

Odd Parity → data 1011010, one is added 10110101

Parity to check burst error (Interleaving)



Checksum – means a group of check bits associated with the message regardless of how they are calculated. Group of Parity bits is one example of Checksum

CRC – Uses Generator Polynomial which is known to Sender & Receiver

k → no. of bits in the key (G(x))

Sender Side.

1. Append k-1 zeros at the end of data
2. Use modulo-2 binary division to divide data by the divisor and store the remainder.
3. Append the remainder at the end of data and send

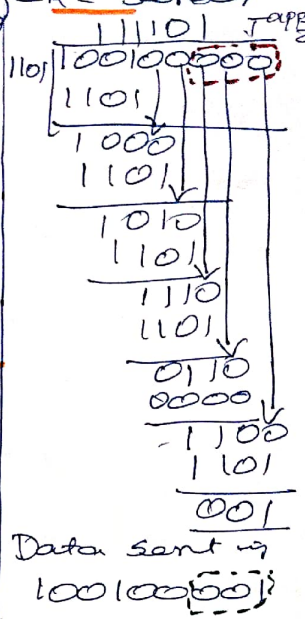
Receiver Side

Perform the modulo-2 division with the same divisor. If the remainder is zero → no error.

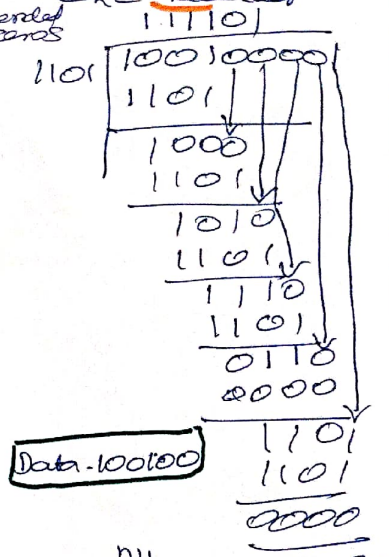
Error Correction

Hamming distance – between two words is the number of differences between corresponding bits 000 011 → Hamming distance 2.

CRC Sender



CRC Receiver



Error Correction – Hamming Codes Algorithm.

- An information of d bits are added to the redundant bits r to form d+r
- The location of each of the (d+r) digits are assigned a decimal value
- The r bits are placed in the position $1, 2, \ldots 2^{k+1}$
- At the receiving side, Parity bits are recalculated. The decimal value of the Parity bits determine the position of the errors.

(5)2 HAMMING CODE – ILLUSTRATION

Data → 1010

Total number of database d=4

Number of redundant bits r :-

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

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

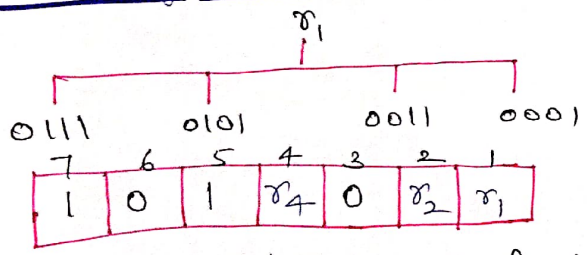
∴ r=3

Total no. 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

Determing r_1 bit :-



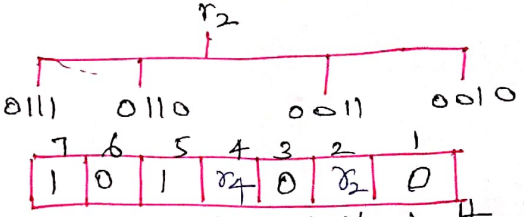
r_1 is calculated by performing a Parity check on the bit positions whose binary representation includes 1 in the first position.

The total number of 1 at these bit positions (1, 3, 5, 7) is even

∴ $r_1 = 0$

Determing r_2 bit :-

r_2 bit is calculated by performing a parity checks on the bit positions whose binary representation include 1 in the second position.

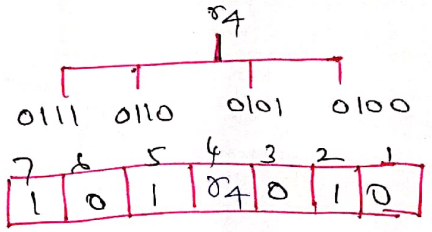


The total number of 1s in the bit position (2, 3, 6, 7) is odd, so as to ensure even parity, $r_2 = 1$

$r_2 = 1$

Determining r_4 bit :-

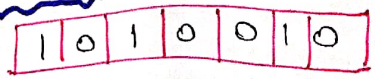
r_4 is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the third position



The total number of 1's (4, 5, 6, 7) is even

$r_4 = 0$

Data sent :-

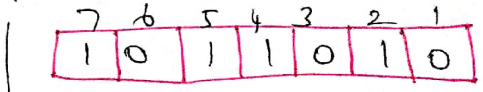


Receiver Side :-

One error occured.

4th bit is changed.

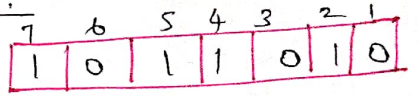
r_1 :- 1 0 1 (1) 0 1 0



1, 3, 5, 7

0 0 1 1 → even ∴ $r_1 = 0$

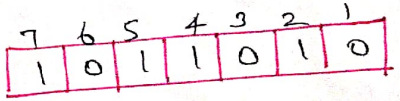
r_2 :-



7, 6, 3, 2 → 1001 → even

∴ $r_2 = 0$

r_4 :-



7 6 5 4

1 0 1 1 → odd

∴ $r_4 = 1$

The Redundent 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).

TOPIC : 6

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

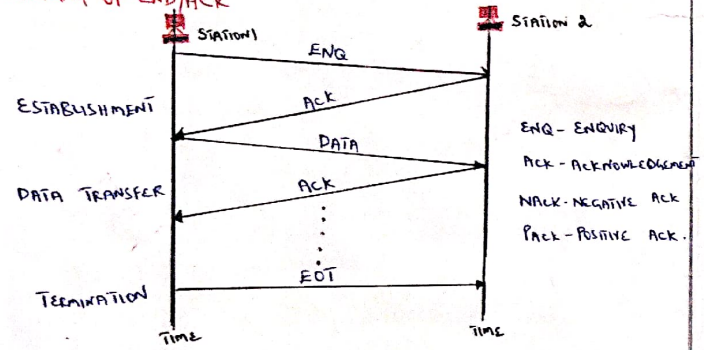
SERVICES:

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

LINE DISCIPLINE

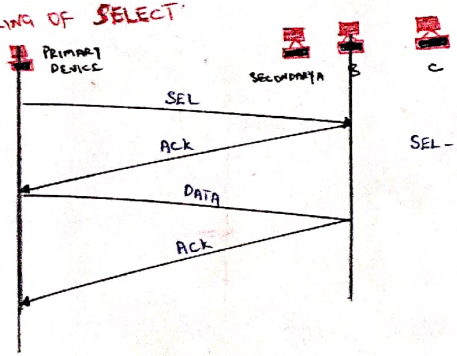
END/ACK POLL/SELECT

WORKING OF END/ACK



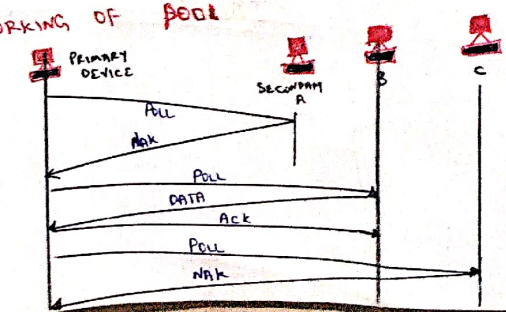
ENQ - ENQUIRY
ACK - ACKNOWLEDGEMENT
NACK - NEGATIVE ACK
PACK - POSITIVE ACK.

WORKING OF SELECT



SEL - SELECT

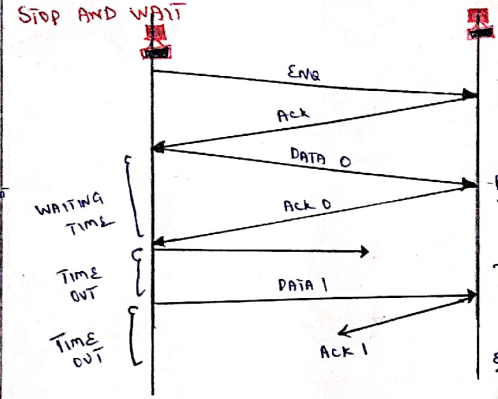
WORKING OF POLL



FLOW CONTROL

STOP AND WAIT SLIDING WINDOW

STOP AND WAIT



TRANSMISSION DELAY

$T_d = \frac{D}{B}$ — DATA SIZE / BANDWIDTH

PROPAGATION DELAY

$T_p = \frac{d}{s}$ — DISTANCE / SPEED

TOTAL TIME

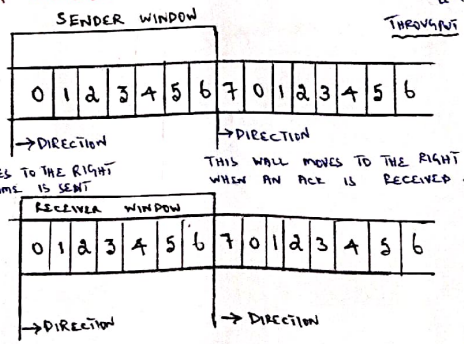
$T_t = T_d + T_p + T_p$ (DATA + ACK)

EFFICIENCY

$\eta = \frac{T_d}{T_d + (2T_p)}$ — USEFUL TIME / TOTAL TIME

THROUGHPUT = $\eta * B$

SLIDING WINDOW:



THIS WALL MOVES TO THE RIGHT WHEN A FRAME IS SENT

THIS WALL MOVES TO THE RIGHT WHEN AN ACK IS RECEIVED.

THIS WALL MOVES TO THE RIGHT WHEN A FRAME IS RECEIVED

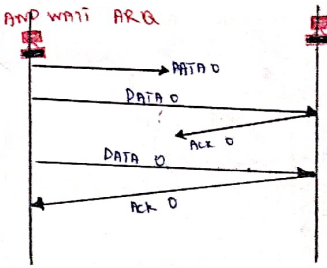
THIS WALL MOVES TO THE RIGHT WHEN AN ACK IS SENT.

* SENDER CAN TRANSMIT THE SEVERAL FRAME WITHOUT ACK
* MULTIPLE FRAME CAN BE SENT
* SINGLE ACK ACKNOWLEDGE MULTIPLE FRAME
* WINDOW SIZE → MODULO - n If n=3 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

STOP AND WAIT ARQ



* DAMAGED FRAME
* LOST FRAME

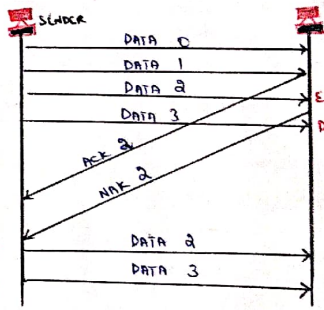
DISADV:
* ONLY ONE PACKET
* IF $D_t \uparrow$ $T_p \uparrow$ $T_p/T_t \uparrow$ $\eta \downarrow$

SLIDING WINDOW ARQ

* GO-BACK - N
* SELECTIVE - REJECT.

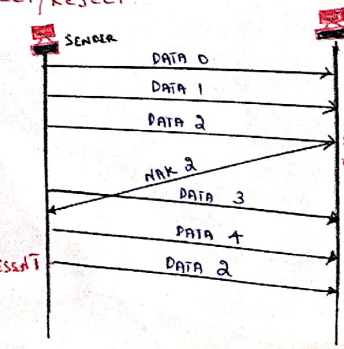
SLIDING WINDOW ARQ - CONTINUOUS TRANSMISSION ERROR CONTROL

GO-BACK - N - IF ONE FRAME LOST/DAMAGED RETRANSMITS ALL (EXCEPT PACK)



* DAMAGED FRAME
* LOST DATA FRAME
* LOST ACKNOWLEDGEMENT

SELECT/REJECT: PARTICULAR FRAME RETRANSMIT (NACK RECEIVED)



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

TOPIC : 7

MULTIPLE ACCESS PROTOCOLS

DATA LINK LAYER
- LOGIC OF DATA LINK CONTROL
  - * FLOW / ERROR CONTROL
  - * MEDIA ACCESS CONTROL
- * TO REDUCE COLLISION
- * TO AVOID CROSSTALK

RANDOM ACCESS PROTOCOLS	CONTROLLED ACCESS PROTOCOLS	CHANNALIZATION PROTOCOLS
* ALOHA	* RESERVATION	* FDMA
* CSMA	* POLLING	* TDMA
* CSMA/CD	* TOKEN PASSING	* CDMA
* CSMA/CA		

RANDOM ACCESS PROTOCOLS

ALL STATION HAS THE EQUAL PRIORITY TO SEND THE DATA OVER A CHANNEL

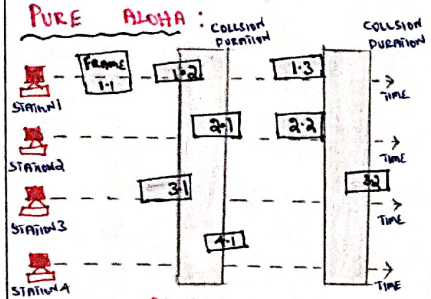
DIS ADV: COLLISION (OR) CONFLICT

ALOHA RANDOM ACCESS PROTOCOL

ALOHA RULES:
* ANY STATION CAN TRANSMIT DATA TO A CHANNEL AT ANY TIME
* NO CARIER SENSING
* COLLISION / DATA LOST MAY OCCUR
* NO COLLISION DETECTION
* RETRANSMISSION OF DATA AFTER SOME RANDOM AMOUT OF TIME

TYPES OF ALOHA
- PURE ALOHA (WITHOUT CHECKING CHANNEL IDLE/not)
- SLOTTED ALOHA (FIXED TIME INTERVAL - CHANNEL DIVIDED)

PURE ALOHA:

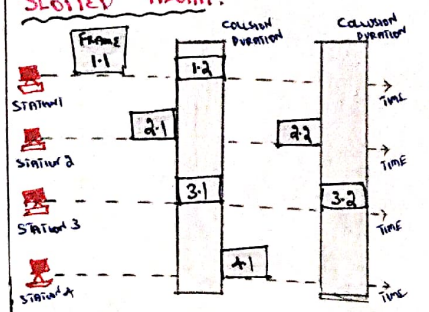


TOTAL VULNERABLE TIME
$2 * T_{fr}$

MAXIMUM THROUGHPUT
$G = 1/2$ 18.4%

SUCCESSFUL TRANSMISSION OF DATA FRAMES
$S = G * e^{-2G}$

SLOTTED ALOHA:



TOTAL VULNERABLE TIME
T_{fr}

MAXIMUM THROUGHPUT
$G = 1$ 37%

SUCCESSFUL TRANSMISSION OF DATA FRAME

CARRIER SENSE MULTIPLE ACCESS

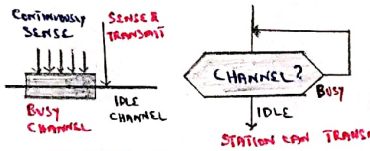
LISTEN (CARRIER SENSE) SILENCE (PRESET TIME)

MULTIPLE ACCESS - MANY DEVICE CONNECT/SHARE SAME NETWORK

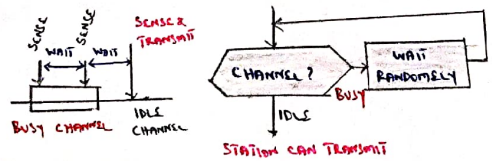
ADVANTAGE: COLLISION ↓ PERFORMANCE ↑

CSMA
- 1-PERSISTENT
- NON PERSISTENT
- P-PERSISTENT
- O-PERSISTENT

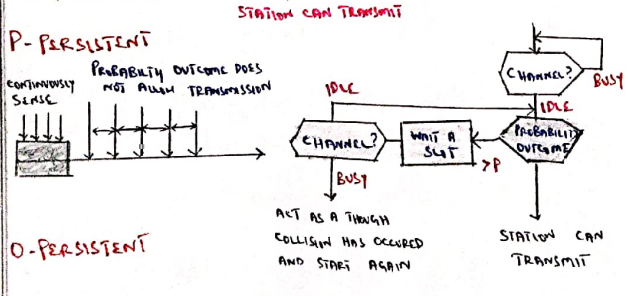
1 PERSISTENT



NON PERSISTENT



P-PERSISTENT



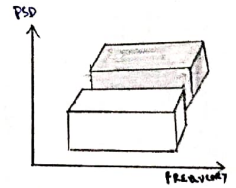
O-PERSISTENT

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

CHANNALIZATION PROTOCOLS

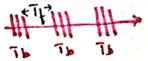
TIME DIVISION MULTIPLE ACCESS

PRE ASSIGNED / DEMAND ASSIGNED



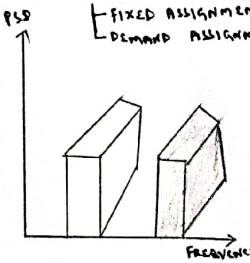
* SINGLE CARRIER FREQUENCY
* NON OVERLAPPING TIME SLOTS
* DISCONTINUOUS TRANSMISSION (BURST)
* DUPLEXER NOT REQUIRED
* ADAPTIVE EQUALIZATION
* HIGH SYNCHRONOUS OVER HEAD

BUFFER CAPACITY $m = R_b T_f$ $R_{TDMA} = n/T_b = n(T_f/T_b)$



FREQUENCY DIVISION MULTIPLE ACCESS

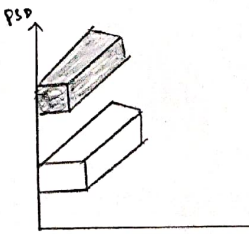
FIXED ASSIGNMENT / DEMAND ASSIGNMENT



* 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, MAINTANANCE DIAGNOSIS

DIS ADV: FADING, FREQUENCY MODULATION, INTERMODULATION

CODE DIVISION MULTIPLE ACCESS:



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

NEAR FAR PROBLEM.

TYPES: SPREAD SPECTRUM, FREQUENCY HOPPING.

(8)

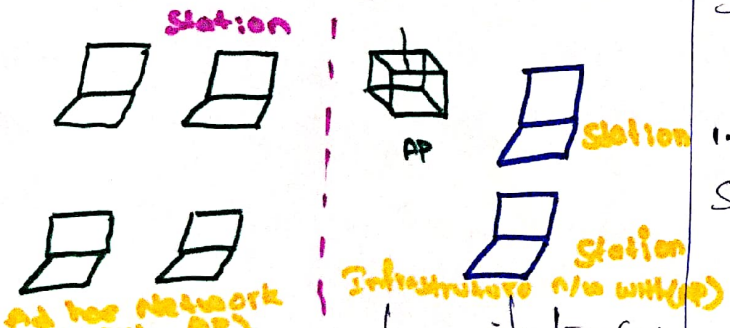
IEEE 802.11 wireless Lan

Architecture:-

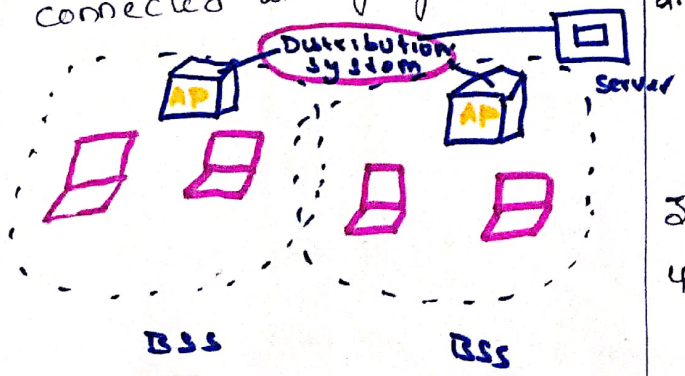
Ess - Extended Service Set

BSS - Basic Service set

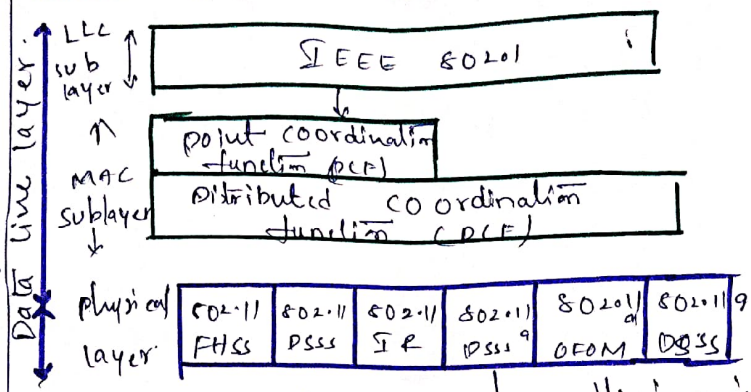
BSS → It is the building block as a wireless LAN. It is made up of stationary (or) mobile wireless stations and an optional central base station.



Ess - is made up of two (or) more Bss with APs. Bss are connected usually by wired LAN.



MAC layer is 802.11 standard



DCF is used to prevent collisions in IEEE 802.11. It uses CSMA/CA - Carrier Sense Multiple Access / collision Avoidance protocal.

1. Before Sending a frame, Sensor station Senses the medium.
   a. channel back-off until the channel
   b. when a channel becomes idle, station waits for some time Sends a control frame. Request to send (RTS)
2. After receiving RTS, after waiting for a time, the destination station sends clear to send (CTS) to source station.
3. the soure station sends data.
4. the destination station sends an acknowledge frame to show that the frame has been Received.

PCF → It is an optimal access method that is used mostly for time sensitive transmission.

Subfileds in fc field.

version	0
type	Management (00), control (01) data (10)
Sub type	RTS, CTS, Ack
To DS	Desired later
From DS	Desired later
more flag	when set no 1, more frames
Retry	when set no 0, retransmi
pwr mgt	when set no 1, station is in power management mode
more data	when set no 1, station has more data to send.
WEP	wired equivalent privacy
Rsvd	Reserved.

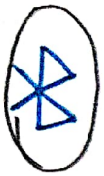
D - duration of the transmission

sc - sequence control - sequence no. of frame.

Wireless Communication

Bluetooth

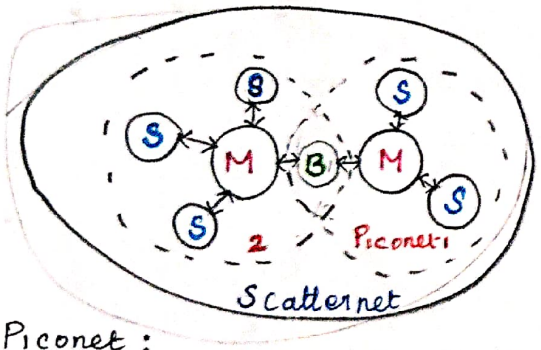
→ Short range communications.
→ LAN - Very limited Coverage.



→ RF for communication
→ Freq. modulation for Radio wave.

Two Types.

↳ Piconet
↳ Scatternet.



Piconet:

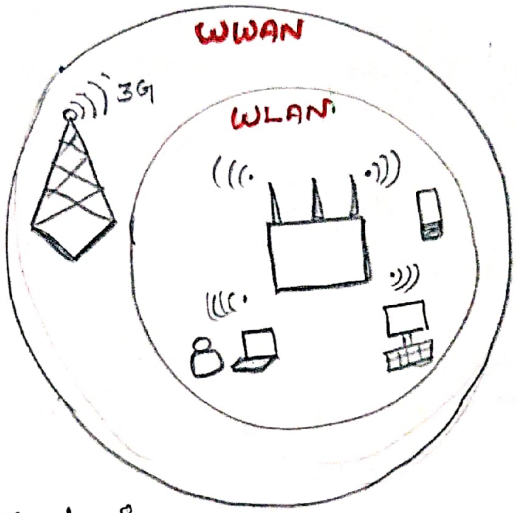
1. Master and slave in piconet
2. one master – max 7 slave
3. No direct connection b/w slave.

Scatternet:

→ Bridge b/w two or more piconet

Spectrum: 2.4 to 2.485 GHz
range : 1 m to 3 feet
Data rate: 3 Mbps from v.2.0.

Wireless WANs.



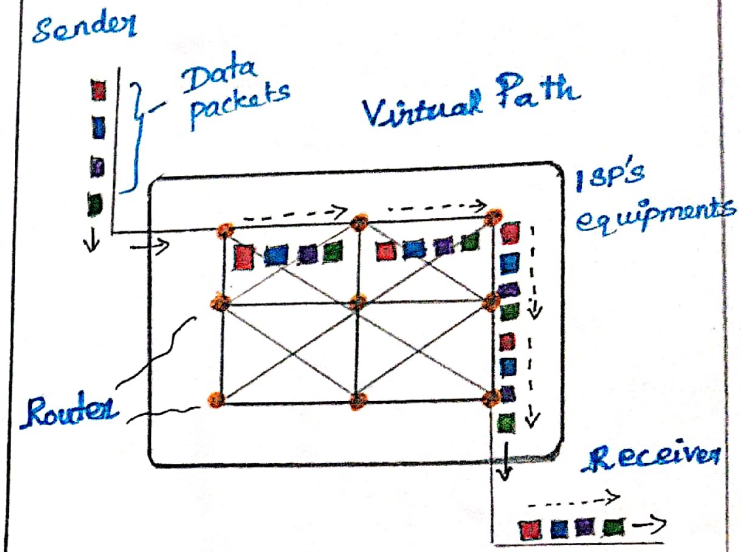
→ Used in cellular device.
→ LAN - WIFI - room
→ Outside - Internet - 3G, 4G etc.

→ Types:

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

→ WWAN - 128 bit encryption security
→ Covers large geographical area.
→ Based on package - limited usage.

Virtual Circuit Network



→ Path b/w Source & distination.
→ physical path - dedicated path
→ Logical - managed pool ckt.

Features of VCN:

* All data using same path.
* resources link & buffers the bw reserved.

Phases of Virtual Ckt:

* Setup phase → route through switch
* Data transfer → packets follows route
* Tear down phase → Data transfer Complete.

FRAME RELAY

→ It is a packet switching N/w.

→ Fragmented into trans.units called frames

→ Exclusive conn during transmission called Virtual Conn.

Layers:

→ physical layer

→ Data link layer

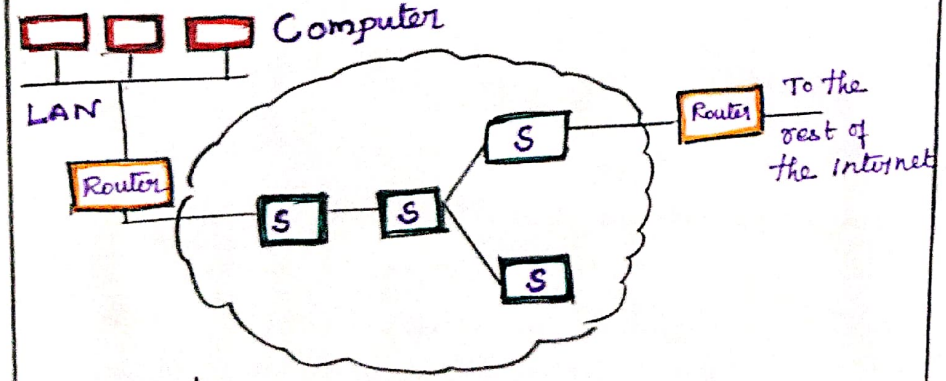
NEED:

→ Higher data rate

→ Transfer bursty data

→ Lower overheads.

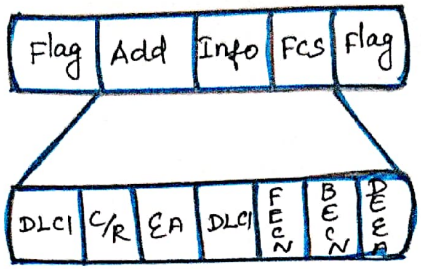
Frame Relay Architecture: (WAN)



Two type:

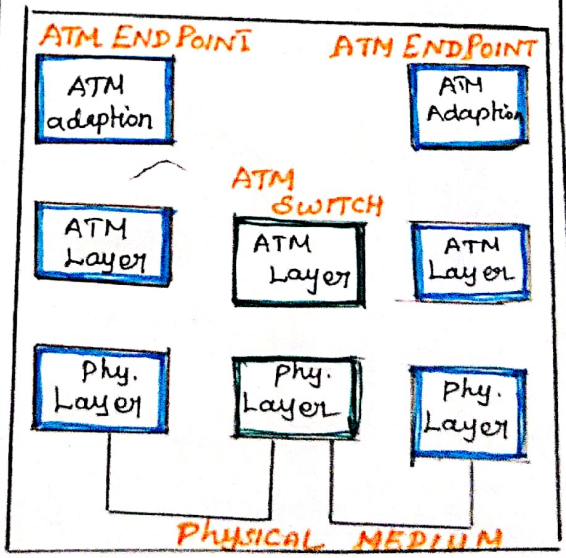
1. permanent Virtual Circuits (PVC)
2. Switched Virtual Circuits (SVC)

FRAME



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

ATM



→ ATM [Asynchronous Transfer mode]

→ TDM for Data Comm.

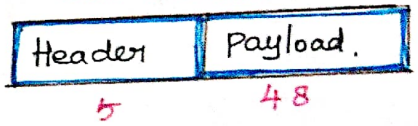
→ Supports video, Voice & data Comm

→ Encodes data into small fixed size

Functions:

1. physical layer → Calls into bits
2. ATM layer → Routing, Traffic, Mux
3. AAL → Existing to ATM N/w
4. ATM End point → Interface
5. ATM Switch → Accepts incoming Calls.

Cell Format.



→ Call are transmitted Ansynchronously.

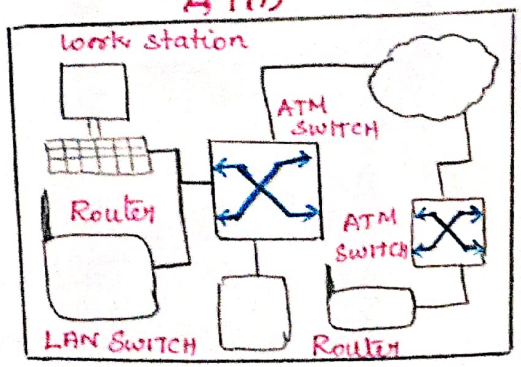
→ Connectio oriented

→ Follow same path sequencly.

→ Both constant and variable traffic

→ Indipendent transmi ssion.

ATM



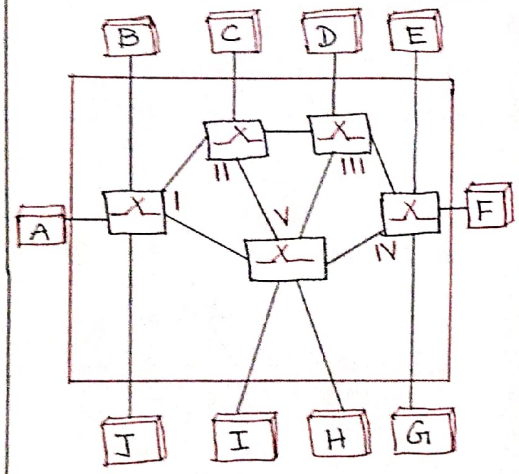
Topic 11 : Packet Switching And Datagram Approach

Packet Switching

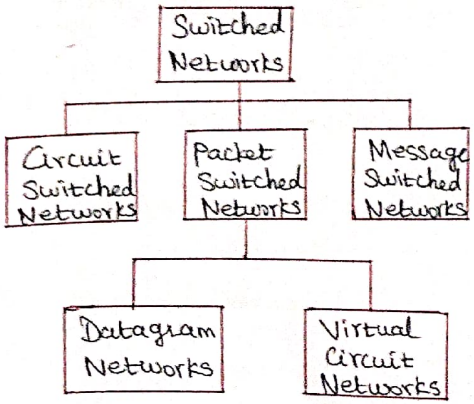
Switch - Connection between i/p & o/p port

Packet Switching - Transfer of small pieces of data

Switched Network



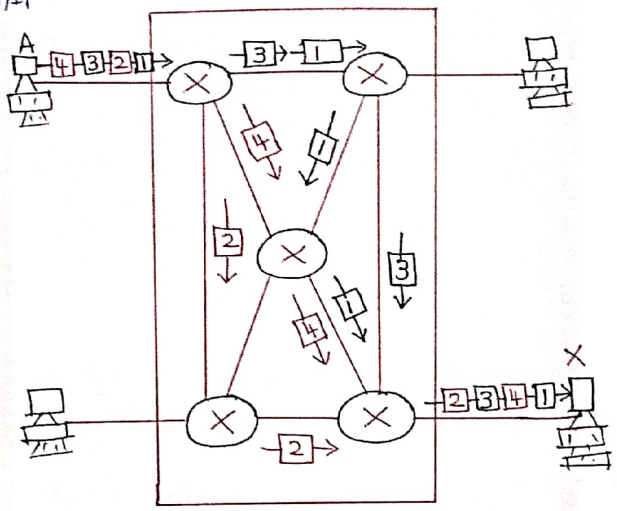
Taxonomy of Switched Networks

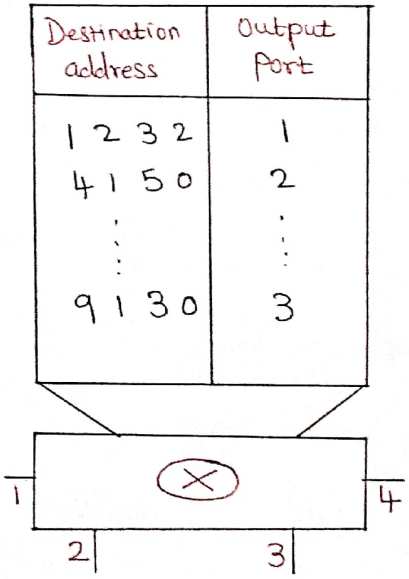


* Networking Protocols divide messages into packets
* Part of the basis for WAN, X.25, TCP/IP
* Packet Switching Networks
* Needs to be divided into packets
* Size - Determined by the n/w
* Connectionless n/w
* Message
  - Number of Units (packets)
    - Source → Destination
* No resource allocation
  - no reserved bandwidth
  - no Scheduled processing time
* Done on a first Come, first Served basis
* Datagram Approach
* Packet is treated independently
* Packets (refers) Datagrams
* Datagram Network
* Connectionless n/w
* doesnot keep information (Connection State)
* No setup (or) teardown 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

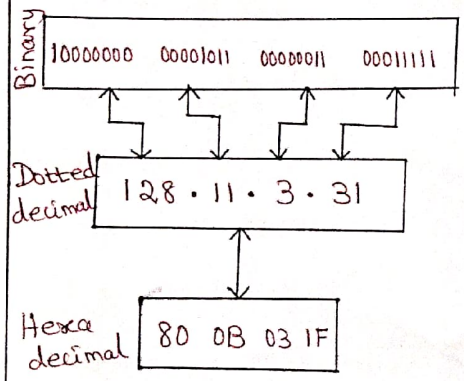
* Efficiency
  - Better than Ckt switched n/w
  - more efficient transfer
  - Various network devices.
* Delay
  - Greater delay in datagram n/w
  - bandwidth increases
  - transmission delay decreases
* Types
  - transmission delay
  - Propagation delay
  - queuing delay
  - processing delay.

Topic 12 : IPV4 Addressing Methods and Subnetting

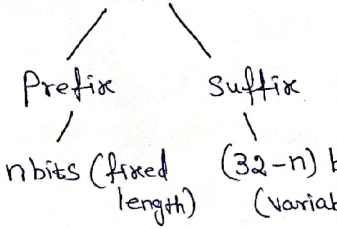
IPV4 Addressing Methods

* IP layer - TCP/IP Protocol
* Identify - Connection (each device)
  (IP address)
* 32 bit address
* Uniquely defines - Connection (host)

* Three different notations in IPV4 addressing

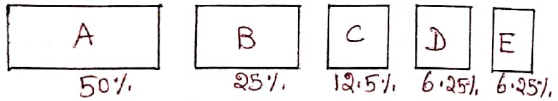


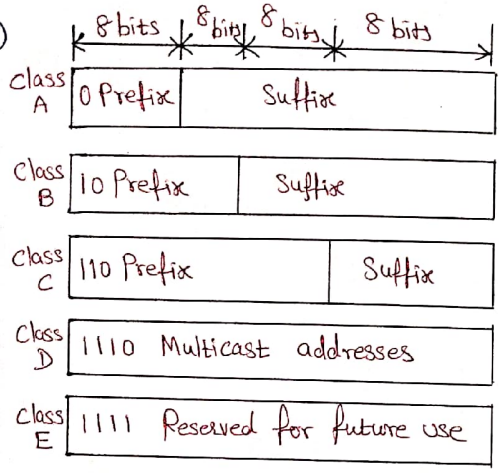
* Hierarchy in Addressing



* Classful Addressing
  - fixed length prefix

- whole address space

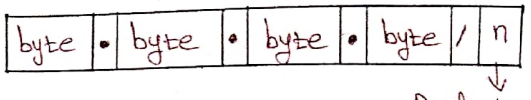




Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

* 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)



Examples:
12.24.76.8/8
23.14.67.92/12

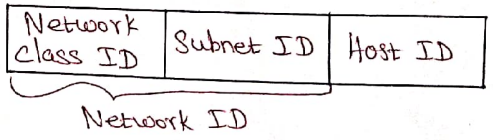
SUBNETTING

* Divide a n/w to Smaller n/ws
  (Subnets)

* Reasons
  - Reduce n/w traffic
  - Improve n/w Performance
  - management

* allocate host bits for Subnet bits.

* Subnet Mask
  - 32 bit string
  - 1s and 0s
  - Specifies no. of bits for n/w ID
    (IP address)

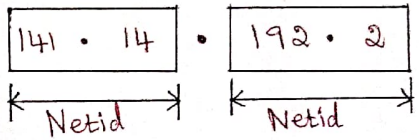


* Designing Subnets
  - Total no. of addresses N
  - Prefix length n

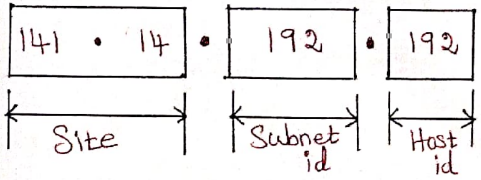
* Steps to be followed
  - no. of addresses (Power of 2)
    (each sub n/w)
  - Prefix length
    $n_{sub} = 32 - \log_2 N_{sub}$
  - Starting address (divisible by the no. of addresses)

* Address aggregation
* CIDR Strategy.
* ICANN assigns ISP

* Without Subnetting



* With Subnetting



* To create a 3rd address level
  - Network id
  - Subnet id
  - Host id

Topic 13 : Routing (DVR – LSR and Multicast)

Routing :

* Selecting path
* Along with send network traffic

Goals :

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

Routing Algorithms :

1. * Distance vector Routing
2. * Link state Routing

Distance vector Routing :

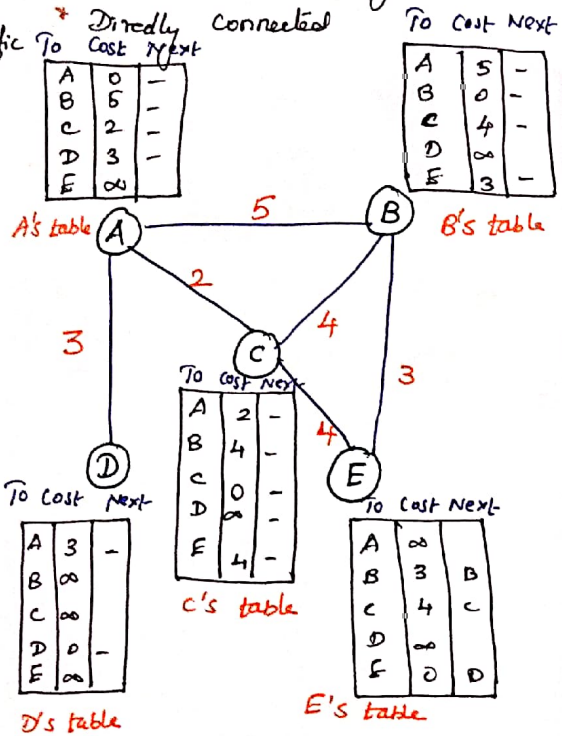
* Periodically shares knowledge
* About the entire network
* Within neighbours
* Table of information
* Updated by exchange information with
* Immediate neighbours

Three Important Aspects

* Initialization
* Sharing
* updating

Initialization :

* Distance between itself and
* its immediate neighbors.
* Directly connected



Sharing :

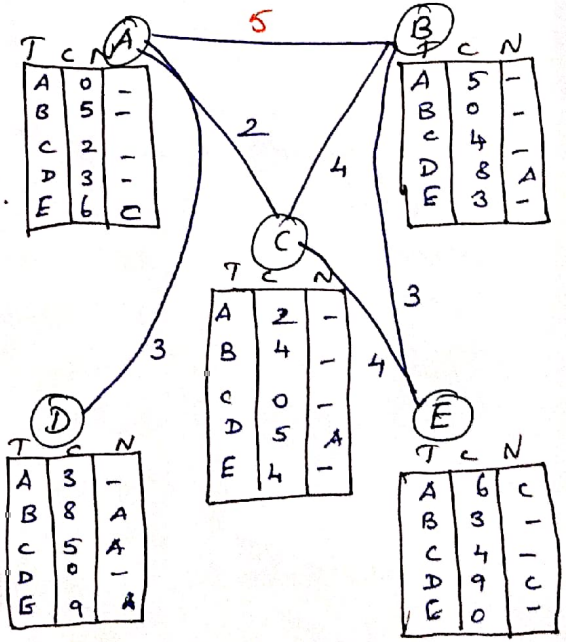
* Information between Neighbors
* Node A does not know about node E.
* Node C does
* C share its routing table
* To Reach node D
* Node A shares its routing
* Improve routing table
* Help Each Other

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
* Old table

Final Diagram

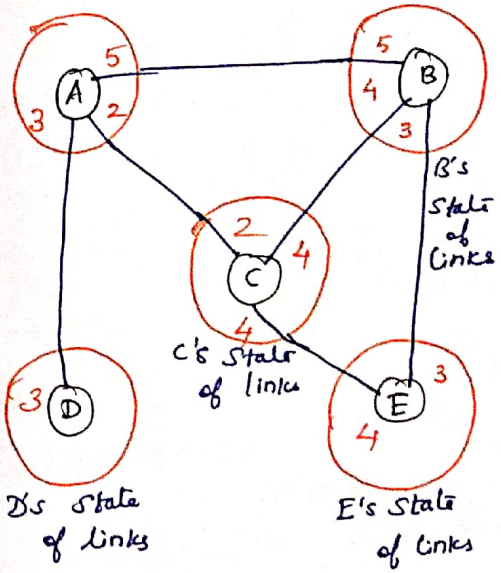
To – T
Cost – C
Next – N



Link state – Routing :

* Global knowledge
* Each node has partial
* knowledge (Type, condition & cost)

A's State of Links



Building Routing Tables :

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

Multicast – Routing

* Efficient distribution
* one – to many traffic

Eg Computer device
Ip phones

– x –

Dr. G. Charlyn Pushpalatha

Topic: 14. Transport Layer and its duties

Transport Layer Duties:

* Gateway of transport layer.
* Chunks of data
* Receives from different Sockets
* Encapsulate them
* Passing the resulting
* Segments 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 Applica tion Layer
* Segmentation
* Divides Message
* Segmentation enhanced.
* Add source
* Add Destination
* Port numbers
* Header Segments

At the Receiver's Side:

* Receives data From n/w Layer
* Reassembles Segmentation
* Reads its header
* Identifies port number
* Forwards 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 Cusec : ...-datagram Protocol

⇒ Connection - Oriented protocol
⇒ Establish Robust connection

Multiplexing:

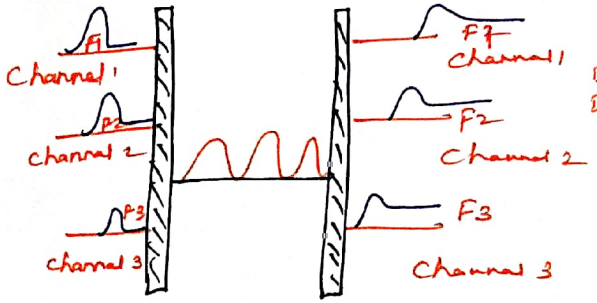
* Analog and Digital
* Streams of Transmission
* Processed over
* shared links

Frequency - Division Multiplexing

* Time - Division Multiplexing
* Wavelength Division Multiplexing

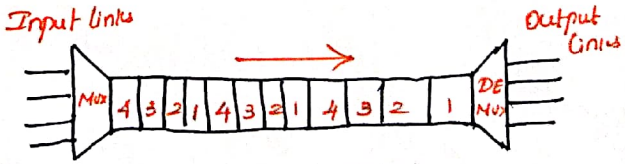
① Frequency Division Multiplexing

* Analog technology
* Spectrum or Carrier Bandwidth
* Logical channels.



② Time Division Multiplexing

* Digital Technique
* Frequny Division Multiplexing
* Technique
* All signals Operates
* User takes control
* Fixed Amount of time.



Two types of TDM:

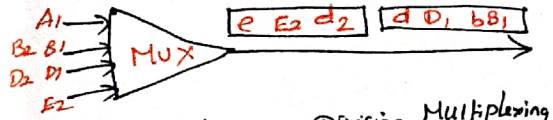
* Synchronous Time Division
* Statical (ASynchronous)

Synchronous TDM:

* Input Frame to Output

Statistical TDM:

* Address particular Data
* Sent output Frame



③ Wave - length Division Multiplexing

* Light wavelength colors
* Fiber optical mode
* Multiple optical Carrier Signals

Code Division Multiplexing:

⇒ Orthogonal codes
⇒ spread Signals
⇒ Technology of NDM
⇒ Optical Transport n/w
⇒ Rapid growth Data
⇒ Quality capacity
⇒ Transmission Equipments
⇒ Network Bandwidth
⇒ Multi - Service transmission

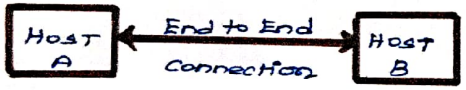
TRANSMISSION CONTROL PROTOCOL (TCP)

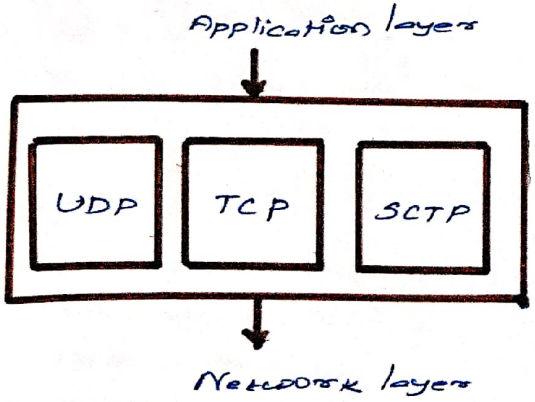
- Transport layer protocol
- Transmit the packets from source to destination
- Connection-oriented.
- Used in IP (TCP/IP)

Features :-

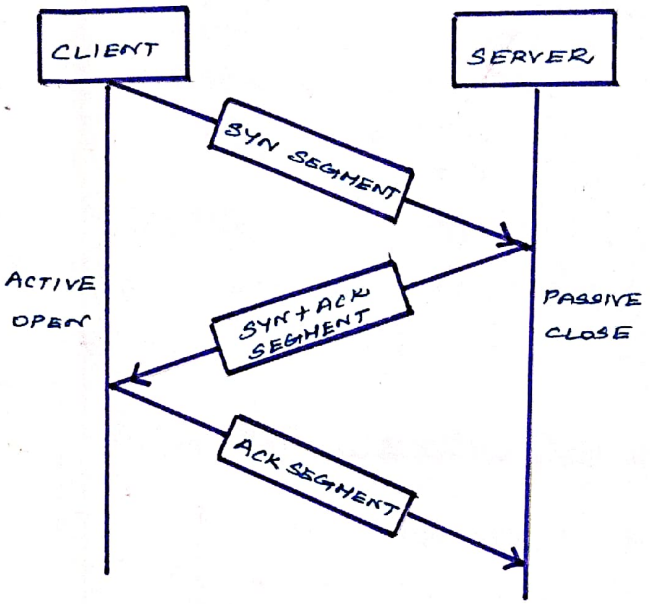
- Reliable
- Order of data
- Full duplex
- Stream oriented.

Purpose :-





Working :- ① Connection Establishment



- Three way handshaking
- No need of packet fragmentation
- Segment tracking
- Message divided for efficient routing.

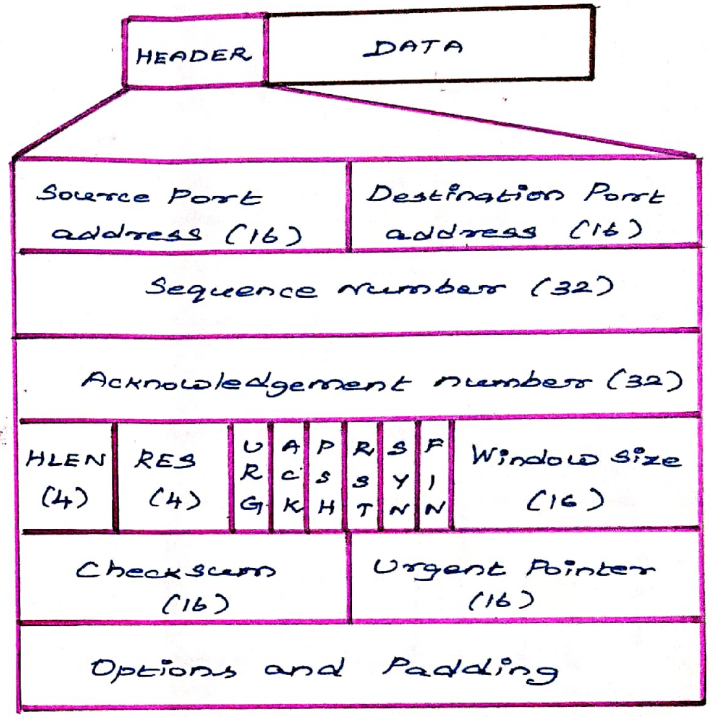
Advantages :-

- Flow control mechanism
- Error detection - checksum
- Error control
- Eliminate congestion

Disadvantages :-

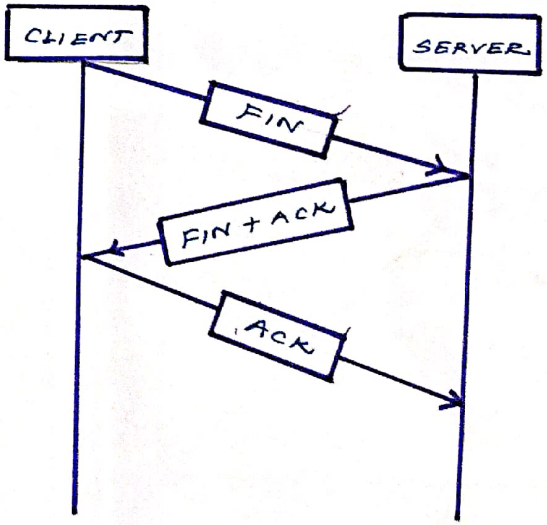
- Not generic in nature.

TCP HEADER FORMAT



② Data transfers phase

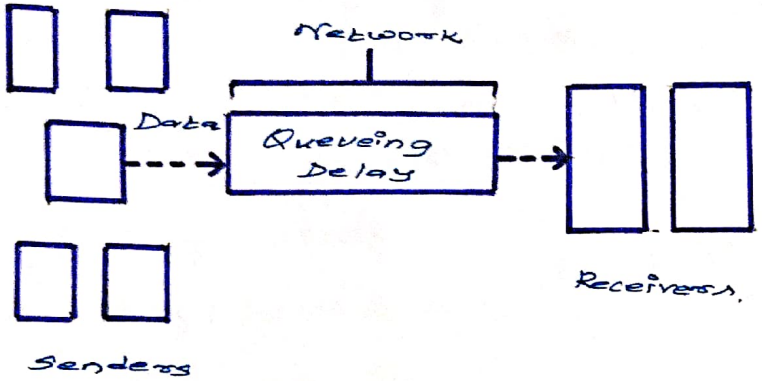
③ Connection termination phase.



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 N/w traffic
- Bandwidth
- Segmenting and Prioritizing
- Assess your devices
- Assess your Network

CONTROL METHODS :

- Open loop congestion control
- Closed loop congestion control

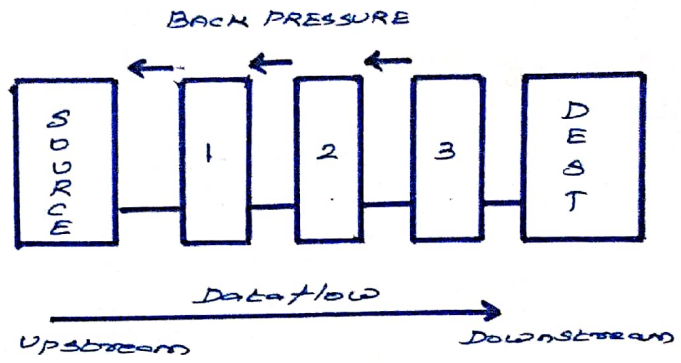
Open loop congestion control

- Retransmission policy
- Window policy
- Acknowledgement policy
- Discarding policy
- Admission policy

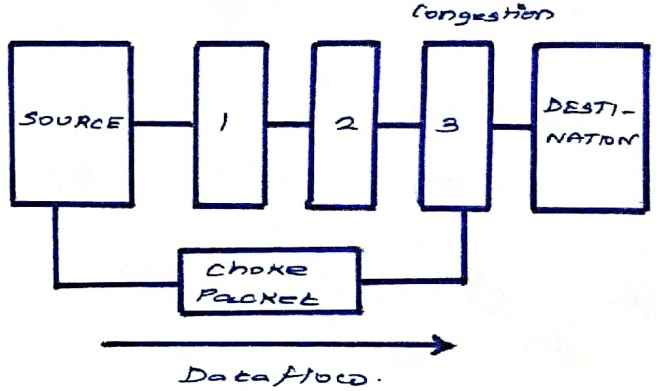
Closed loop Congestion Control

- Back pressure
- Choke packet
- Implicit signaling
- Explicit signaling

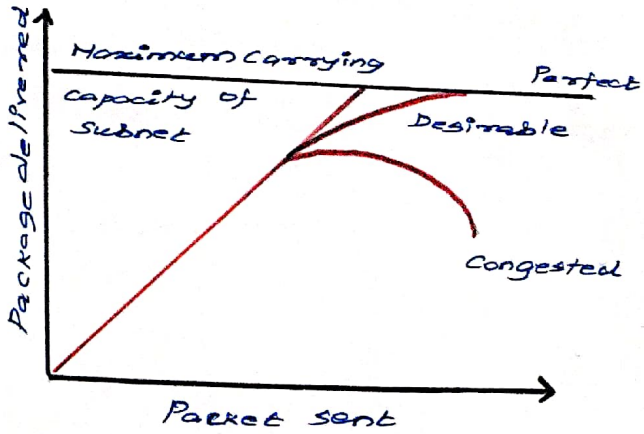
Back Pressure Method :



Choke Packet :



Concept of Congestion



QUEUING ANALYSIS

• The objective of queuing analysis is to predict the system performance such as how many customers get processed per time step, the average delay a customer endures before being served and the size of the queue or waiting room required.

Queuing Models:

1. Single Server Queue
2. Multiserver Queue
3. Networks of Queues

Single Server Queue

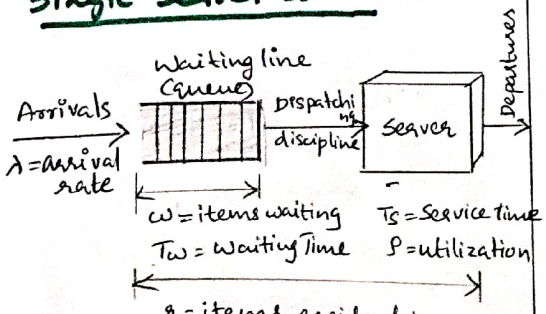


Fig: Queuing system Structure and Parameters for Single-Server Queue

Method of Operation Steps:

1. The central element of the system is a server, which provides some service to items.
2. Items from some population of items arrive at the system to be served.
3. If the server is idle the item is served immediately.
4. Otherwise, an arriving item joins a waiting line.
5. When the server has completed serving an item, the item departs.
6. If there are items waiting in the queue, one is immediately dispatched to the server.

The server in this model can represent anything that performs some function or service for a collection of items.

Examples:

i) A processor provides service to the processes

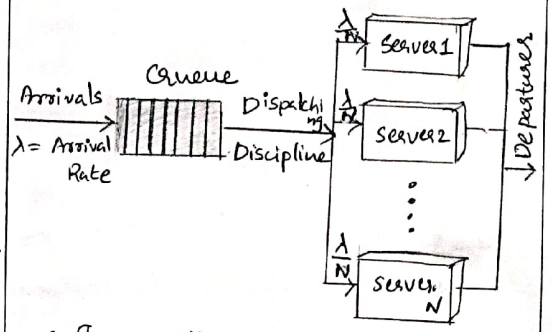
ii) A transmission line provides a transmission service to packets or frames of data.

iii) an I/O device provides a read or write service for I/O requests.

Queue Parameters:

- Item population
- Queue size
- Dispatching Discipline

Multiserver Queue



• In Multiserver queue, all servers sharing a common queue

• If an item arrives and at least one server is available, then the item is immediately dispatched to that server. It is assumed that all servers are identical.

• If all servers are busy, a queue begins to form.

• As soon as one server becomes free, an item is dispatched from the queue using the dispatching discipline in force.

• If we have N identical servers then 'ρ' is the utilization of each server, then 'N_ρ' is the utilization of the entire system, this utilization is N×100%, then the theoretical maximum input rate is:

$$\lambda_{max} = \frac{N}{T_s}$$

Basic Queuing Relationships

Assumptions:

The fundamental task of a queuing analysis is as follows:

- Arrival rate
- Service Time

Provide the output information concerning:

- Items waiting
- Waiting Time
- Items in residence
- Residence time

Networks of Queues

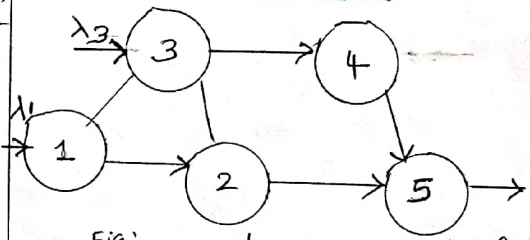
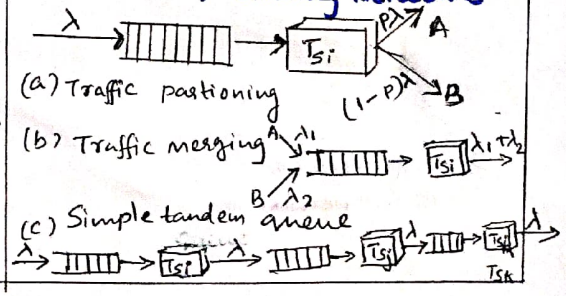


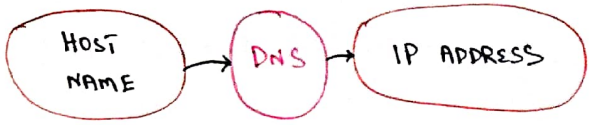
Fig: Example of a Network of Queues

Elements of Queuing Networks

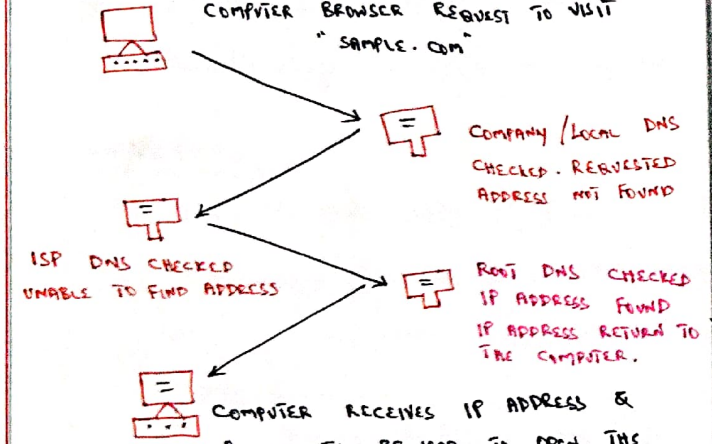


DNS & SMTP

DNS: DOMAIN NAME SERVICE / DOMAIN NAME SYSTEM.



HOW DNS WORKS:

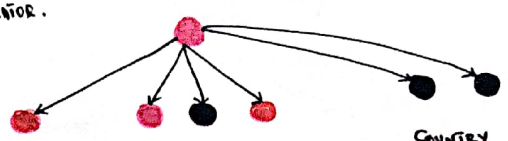


NEED FOR DNS:

* IP ADDRESS → NOT STATIC
  ↳ MAY CHANGE DYNAMICALLY
* IP ADDRESS → COMPLEX SERIES OF NUMBERS
  ↳ DIFFICULT TO REMEMBER IP NUMBERS.

DOMAIN:

. → SEPARATOR.



INVERSE DOMAIN
* FORWARD LOOK UP
* REVERSE LOOK UP

GENERIC DOMAIN
EXAMPLE:
.com, .edu, .gov
.info, .aero, .biz
.org, .net, .mil

COUNTRY DOMAIN
EXAMPLE:
.in, .us, .uk

FOR EXAMPLE:

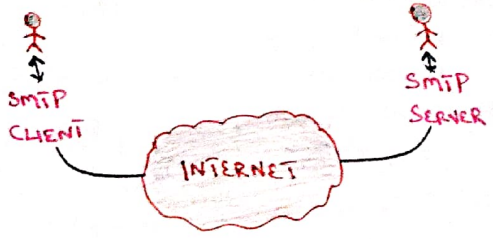
132.147.165.50

ftp.Edusoft.com

SMTP

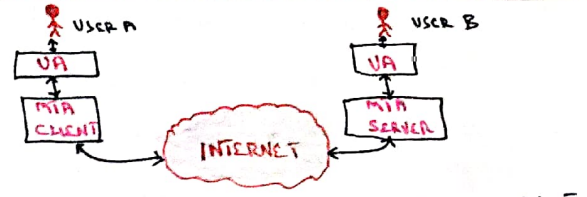
SIMPLE MAIL TRANSFER PROTOCOL

SET OF COMMUNICATION GUIDELINES THAT ALLOWS SOFTWARE TO TRANSMIT AN ELECTRONIC MAIL OVER THE INTERNET.

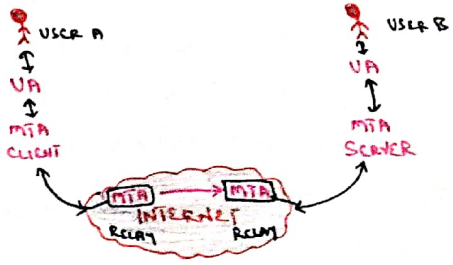


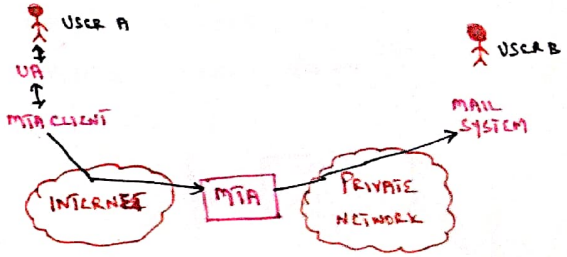
SUPPORTS:

* SINGLE MESSAGE TO ONE OR MORE RECEIPIENTS
* TEXT, VIDEO, VOICE OR GRAPHICS
* MESSAGE ON NETWORKS OUTSIDE THE INTERNET



UA - USER AGENT MTA - MAIL TRANSFER AGENT





WORKING OF SMTP:

* COMPOSITION OF MAIL
* SUBMISSION OF MAIL
* DELIVERY OF MAIL
* RECEIPT & PROCESSING OF MAIL
* ACCESS & RETRIEVAL OF MAIL

FTP & HTTP

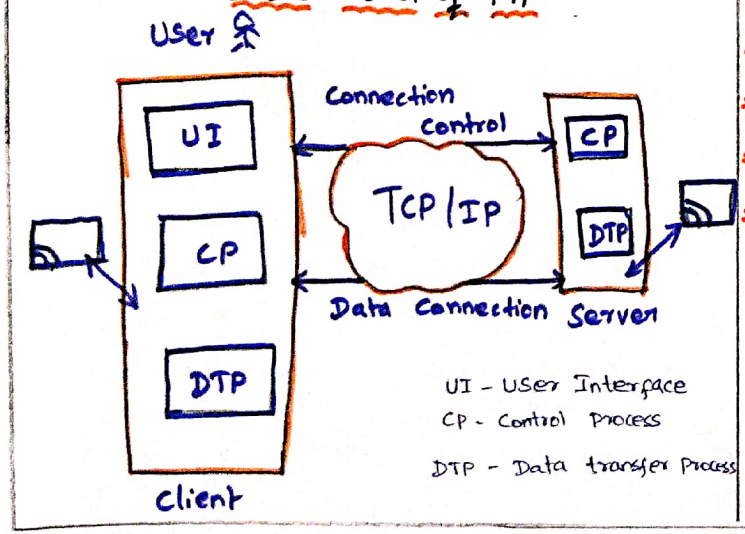
FTP:

- 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:

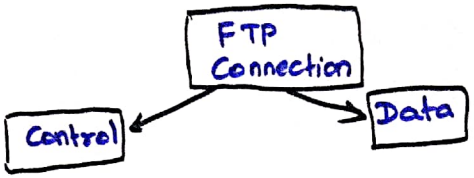
- Provides the sharing of files
- Encourage the use of remote Computers.
- Transfer the data more reliable & Efficiently.

Basic Model of FTP



UI - User Interface
CP - Control Process
DTP - Data transfer Process

Types of Connections in FTP:



Control Connection:

- Simple rules for Communication.
- Connection blw the control processes.
- Connected during the entire FTP session.

Data Connection:

- Complex rules as data types may vary.
- Made blw data transfer processes.
- It opens when command comes for Transfer.
- It closes when the file is transferred.

Advantages:

- Speed
- Efficient
- Security
- Back & forth Movement

Disadvantages:

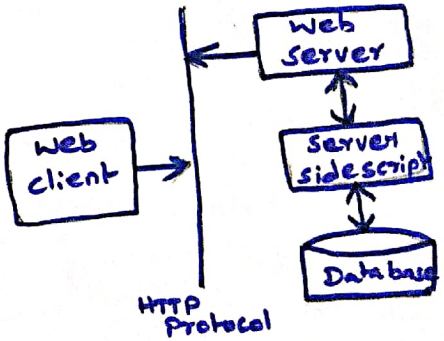
- Not all the FTP providers are equal.
- Not all the providers offer Encryption.
- Size limit is 2GB only.
- doesn't allow transfer to Multiple servers.
- Not Compatible with every System.

HTTP: Hypertext Transfer protocol

- Application level protocol
- Distributed, collaborative, hypermedia Information systems
- 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 clients & servers.

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

Server: Responds with a status line. Message's Protocol, version, success or Error code, MIME-like message. Server

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 & terminates multimedia session.

→ Used to create two party, multiparty session.

→ run on UDP, TCP.

SIP Messages.

Invite ACK BYE OPTIONS Cancel Register

SIP Addresses :- (Formats)

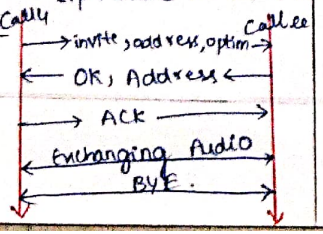
sip: bab@172.18.10.2 | sip: bab@gmail.com | sip: bab@91-9847508344

SIP- SIMPLE SESSION :-

→ Establishing

→ Communicating

→ Terminating

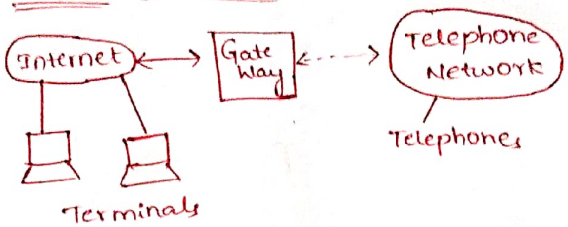


2. H.323 protocol :-

→ ITV standard

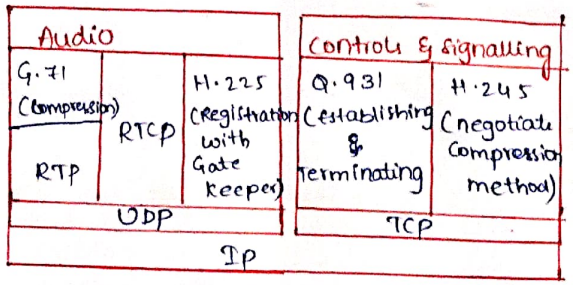
→ Allow telephone talk to computers connected to internet.

H.323 Architecture :-

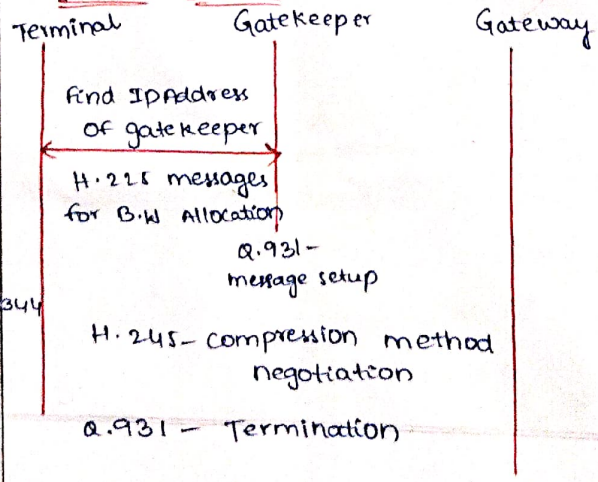


H.323 protocols :-

- Establish and maintain voice (or) video communication.

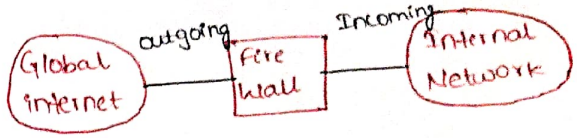


H.323 Operation :-



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 Hotal session level
- easily configuration.
- Allow (or) block traffic without significant resources.