Lecture-01

COMPUTER NETWORK

25. Aug : 20

COMPUTER NETWORK

NETWORK: A network is a collection of nodes which are connected to each other three some medium (wired/wireless) to communicate or exchange information (or any stuff) among them.

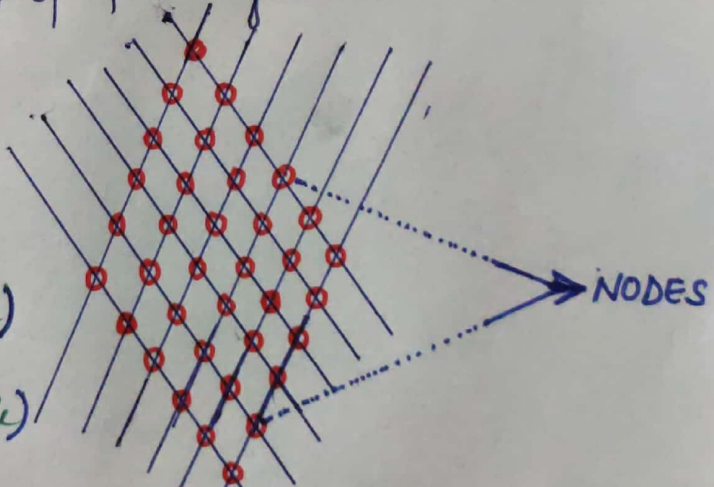
These nodes (as a part of network system) can play different roles in the network.

Depending upon the role and the type of nodes, a NETWORK gets a lable to it, to be recognized by.

eg: Electrical Network, Neural Network, Humon N/W Railway Network, Computer Network etc.

A → NODE → Node could be any of followings:

1) Train (Railway Network)
2) Electrical devices (Electrical N/W)
3) Neurons: (Neural Network)
4) Automobiles & Cities (Road Network)
5) Theive: (Thieves Network)
6) ~~Compupe~~ Computers (Computer Network)



So, On the bases of above observation, we now can define-

COMPUTER NETWORK: Hence, a "COMPUTER NETWORK" is a collection of computer nodes which are interconnected, three some medium, with each other in order to communicate or exchange information among them.

Lecture-01 Cont....

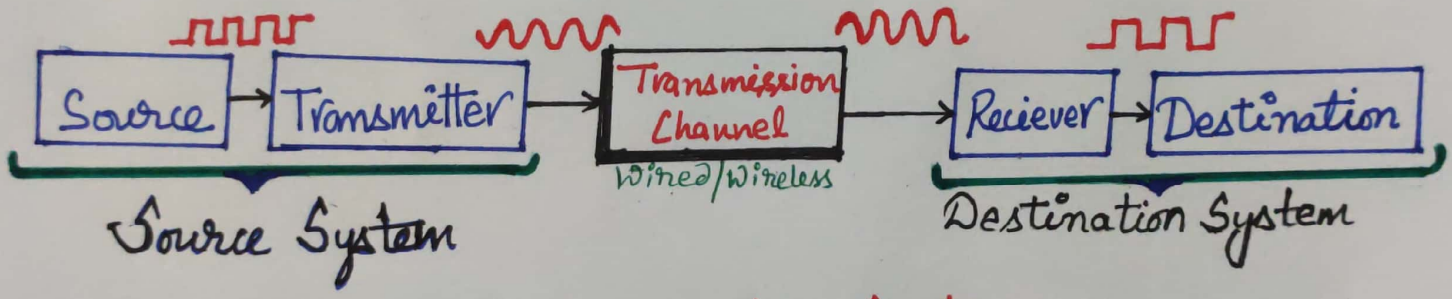
CS-305

25 Aug 20

COMPUTER NETWORK

→ **Data Communication:** It refers to the exchange of data between two devices over a transmission medium. For data communication to occur, both the devices should be able to transmit and receive data on its own. Moreover, Data Communication is a two-way process.

→ **Basic Communication Model:** A basic communication system is consist of a sender(source), a reciever(destination) and a communication channel(transmission Medium) as depicted in figure below—



→ **Factors affecting Communication System:**

1) **Delivery:** The system must be able to send/deliver data to the correct user. Data must be recieved by intended user.

2) **Accuracy:** Correct data should reach at destination that is the the data sent and the data recieved must be exactly same

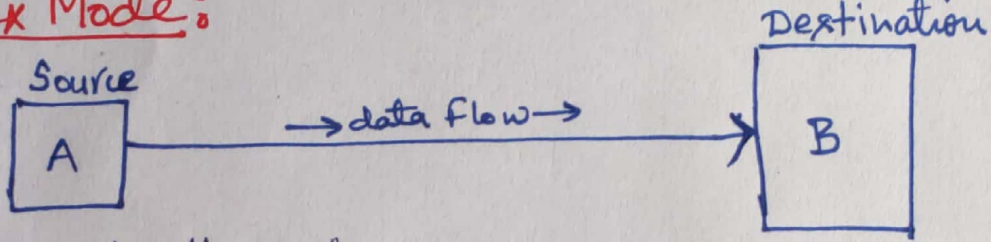
3) **Timeliness:** Data sent, must ~~reath~~ reach at destination within specified time. Data arriving late at destination may no longer be useful or effective.

4) **Jitter:** It refers to the variation data packet arrival time at destination. eg: uneven delay in the delivery of data packects. It is not desirable & acceptable especially in the delevery of audio & video data-communication.

DATA FLOW:

For communication to occur, there must be two-way exchange of data from both sides (sender/Reciever).
The exchange of data (transmission & Recieval) can happen in following-3 ways.

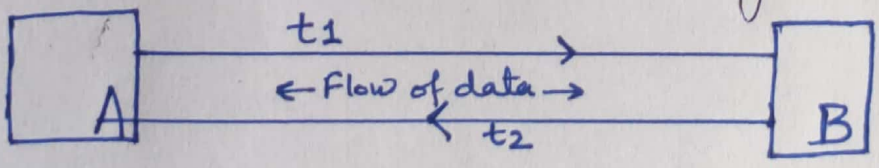
1) Simplex Mode:



In this mode there is only one-way transmission (flow) of data for all the time. Reciever can never send data back to the sender **examples:** Radio, Television etc

2) Half Duplex:

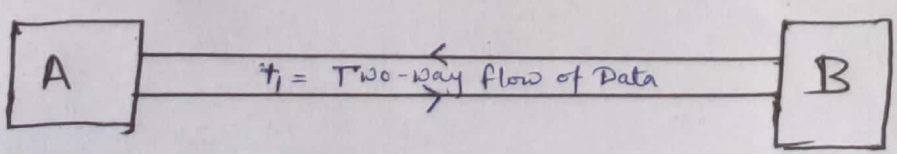
In this mode sender and reciever both can send and reciene data but not simultaneously
eg: At time t_1 "A" is sending & "B" is receiveng data where as at time t_2 "B" is sending and "A" is recieving data.



examples: Walkie-Talkie
Cordless (Police)

3) Full Duplex:

This mode is most frequently used or in almost every communication. It allows simultaneous two-way flow of data from both side. User A & B can send & reciene data at any point of time simultaneously **Examples:** Telephone
Mobile Phone
Wireless Network



LECTURE-02
Computer Network

COMPUTER NETWORK

Components of N/W Communica^{n} System:

A communication system is essentially consist of followings-

1) **Message:** A message is nothing but a piece of information or data to be sent (transmitted) to destination.
eg: text, audio, video, pictures etc.

2) **Sender:** Sender is a computing device which is responsible to transmit/send data over a communic^{n} medium. eg: Computer, Laptop, Mobile etc.

3) **Reciever:** Recieve is also a computing device which is supposed to recieve the data sent by sender.
eg: Comp. Mobile, Workstation, Handsets etc.

4) **Transmission Medium:** It is a physical path along which the transmitted data (signals) travels from source (sender) to destination (Reciever).

5) **Protocols:** It is a well defined set of rules which monitors, governs and supervise the data communication process b/w communicating devices. The communicating must agree upon these set of rules laid by ~~protocol~~ network protocol(s).

Lecture-03
COMPUTER NETWORK

29.08.2020

COMPUTER NETWORK

Network Criterea:

A computer network is assessed on the basis of certain criteria that it must meet to. These criteria are known as network criteria

eg: 1) Reliability
3) Performance
4) Security

1). Reliability: The degree of capability of a network to remain active or keep offering its same-services despite of having failure within it.

or

The network reliability can be measured by the frequency of failure in network, the time taken to recover from failure, and the network robustness.

2) Performance:

1) **Transit time:** The amount of time for a messag to travel from source node to destin node.
2) **Response time:** The time duration a data query is requested and data is received by the host

or

It is the time elapsed between data is requested and received by host.

The factors which affect performance

1) The Capability of Hardwares used (Ram, Processor etc.)
2) The type of transmission Medium (Wired / Wireless)

Wired Medium → Twisted Pair Cable
→ Coaxial Cable

Wireless Medium → Radio Waves

3) The Number of User on the network (Load): N/B

4) Efficiency of the Software: How beautifully and efficiently the software is written by programmers.

---

(3) **Security**: The network security refers to the ~~protection~~ protection of data and nodes from unauthorized users or access. It addresses following issues —

* Protecting data from unauthorized access
* Safguarding data from being damaged & developed thru illegitimate ways & means.
* Implementing rules & policies to ensure the recovery from security breach and data losses.

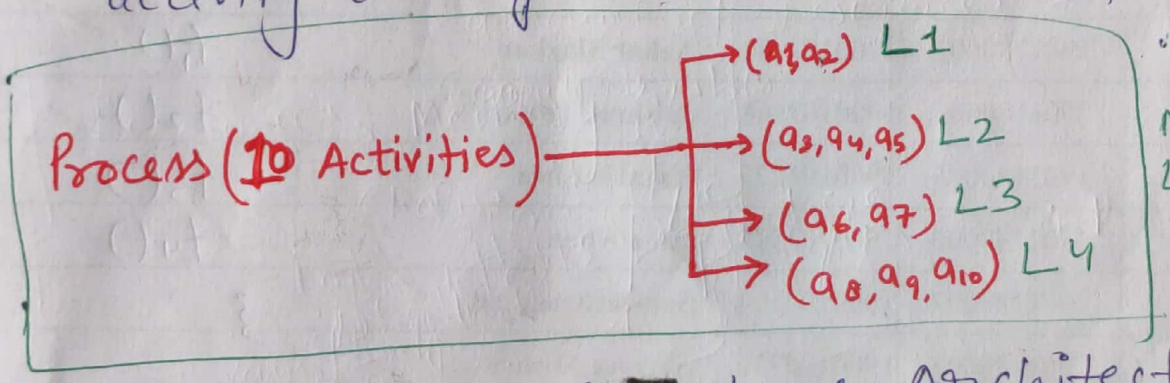
Lecture-04
CS-305

01-Sep 2020

COMPUTER NETWORK

* **Network Architecture:** Layers of Network + Protocols
* **Terminalogies in Network:** Various term which are used frequently to address network related issues etc.

1) N/W Architecture: A layer in n/w is responsible for & supervising or governing specific activity during the communication process.



Process & Need of Layering

1) OSI-Model: 7-Layer Architecture
2) TCP/I Model: 5-Layer Architecture.

* IEEE standards
* Network Protocols

* Terminalogies in N/W

(Φ) **Throughput:** The effective bandwidth. It measures how many packets arrive at destination successfully. (Productivity) $\Phi = \eta * B$

(τ) **Delay:** The time difference between sending and receiving data.

(B) **Bandwidth:** The capacity of a network channel to carry data through it. B = Bits/Sec

(η) **Efficiency:** The rate of effectivity. How much a network is efficient to exchange data during a communication.

$$\eta = \frac{\text{Data Received}}{\text{Total Data Sent}} \times 100$$

OSI Reference Model: It's abbreviated as Open Systems Interconnection.

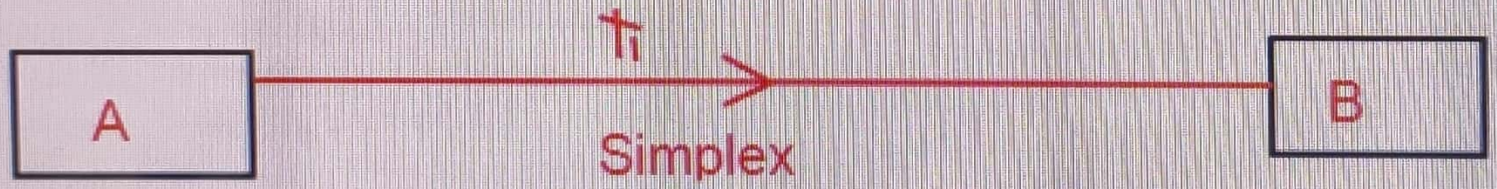
It is a layered framwork and consist of 7 layers. The pirepose of each layer is to offer ertain types of services to the higher Layers. Every layer owns specific protocols to ensure its services for an ongoing communication on network.

1-Physical Layer
2-Data Link Layer
3-Network Layer
4-Transport Layer
5-Session Layer
6-Presention Layer
7-Applocation Layer

This slide left blank for whiteboard

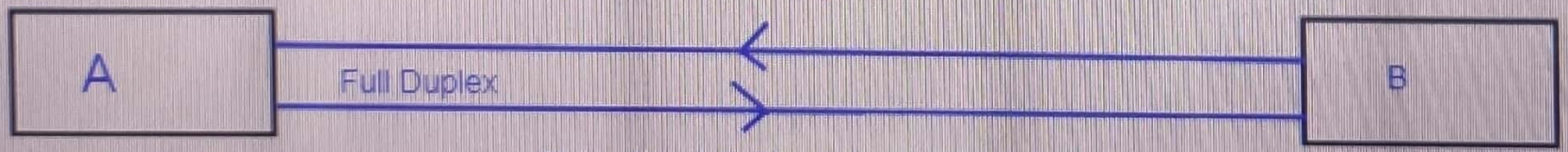
1-Physical Layer:

1. To activate, maintain and deactivate physical connection.
2. To define volatge and data rates for transmission.
3. To convert digital bits into electrical signal.
4. To decide whether the transmissson is simplex, half-duplex full duplex.



exmples:
TV, Radi

Exm.
Walkie-
Talkie



Exm.
Mobile
Phone etc.

This slide left blank for whiteboard

Slide 3

2- Data Link Layer: It offers following services.

1. It deals with data in form of "FRAME".
2. It deals with modulation/demodulation rate.
3. It performs "Error" control (Error detection & Correction).
4. It deals with "Flow Control" (prevents fast senders over slow running reciever vice versa)
5. It deals with "Access Control" (LLC, MAC)
6. It deals with physical address of machines(MAC Address)

7- Protocols: HDLC, SDLC, X.25

This slide left blank for whiteboard

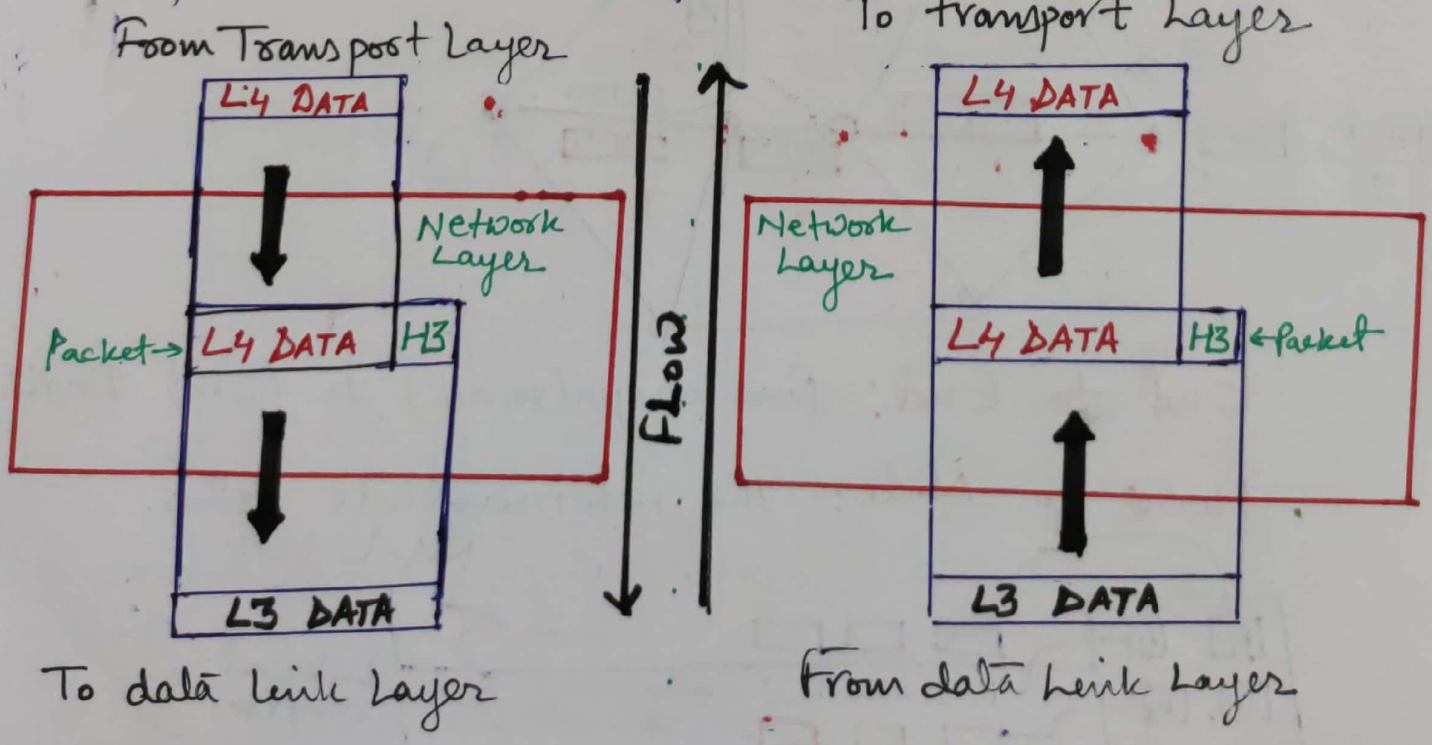
Lecture-07
Computer Network

08. Aug. 20

COMPUTER NETWORK

3- NETWORK LAYER:

1) It deals with data in form of packets.
2) It with logical addressing (IP address).
3) It devides outgoing message into packet and ressembles incomming packets into message.
4) It perform routing: It decides the best suitable (shortest) path for each packet to be sent along.
5) It is concerned with switching eg (message, packet, cincuit)
6) It provides connection services eg: N/W layer flow control
7) It assigns priority over packets so that they can be processed accordingly as part of quality of service.



4-TRANPORT LAYER: It's 5th layer of OSI

1) It deals with service-point address (socket Address)

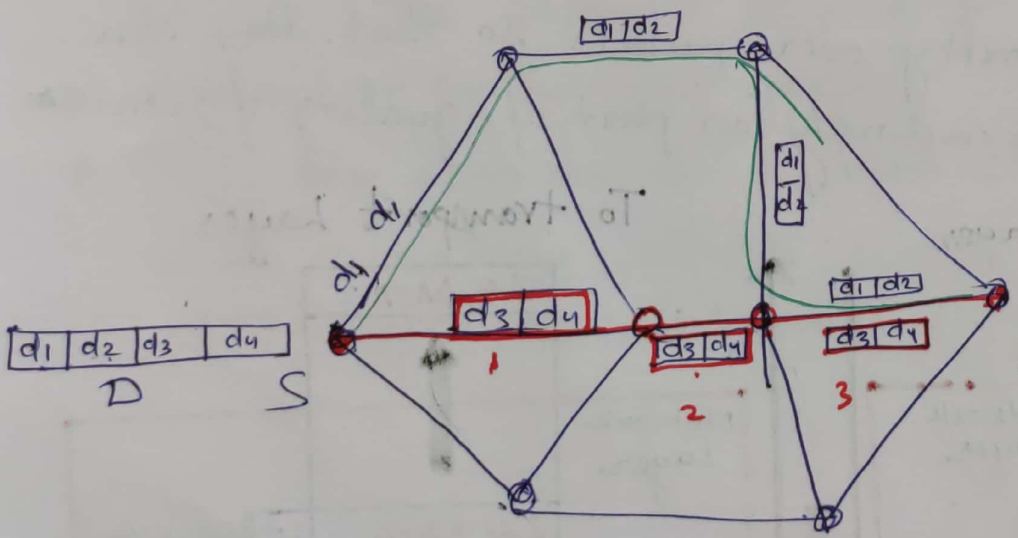
Socket: Port No. of Comp. Machine + Ip Address

2) It deals ~~with~~ data inform of message.

3) It performs end to end flow control.

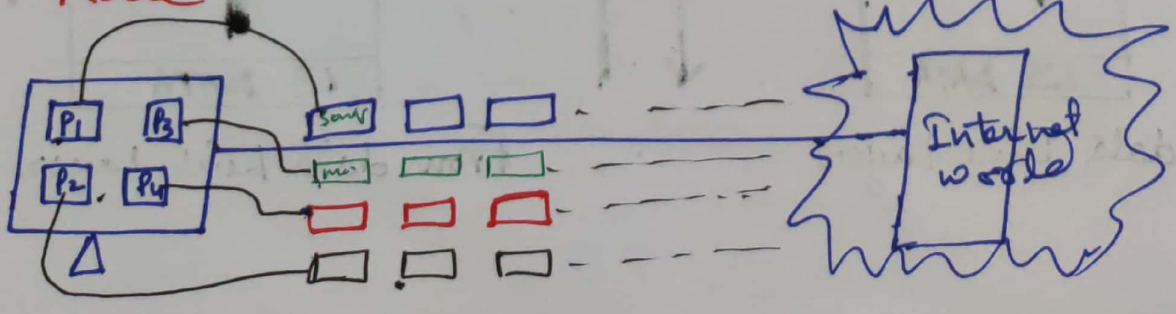
4) It ensure ~~d messages are~~ Packets arriving at destination are in order and ~~intact~~. intact.

5) It perform end-to-end error control



End to End: from origin(source) to final Destination

Node to Node: The intermediate Paths.



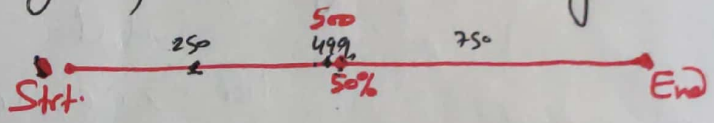
Lecture-08

COMPUTER NETWORK

Computer Network

5- SESSION LAYER: It a 5th layer of OSI model & it resides between Transport (4) layer & presentation (6) layer.

* It creates "SYNCHRONIZATION POINTS" to maintain ~~the~~ a Log of user activity over a time period —



* The "synchronoz" point helps in recovering from failure with least amount of losses (of data).

* It creates sessions (time period) for users to ensure the safety & security of user from ~~unau~~ unauthorized access.

* The ~~sto~~ session is a restriction over a time duration after which the user gets logged off automatically (if remains inactive).

* It co-ordinates the connection and disconnection between two applications (client-server).

* It ~~de~~ controls logging in & logging off.

* It decides who sends when (authentication).

6. Presentation Layer:

Translation

1) It performs translation of data b/w the sender & receiver and decide the format of data (ASCII, EBCDIC, Unicode).

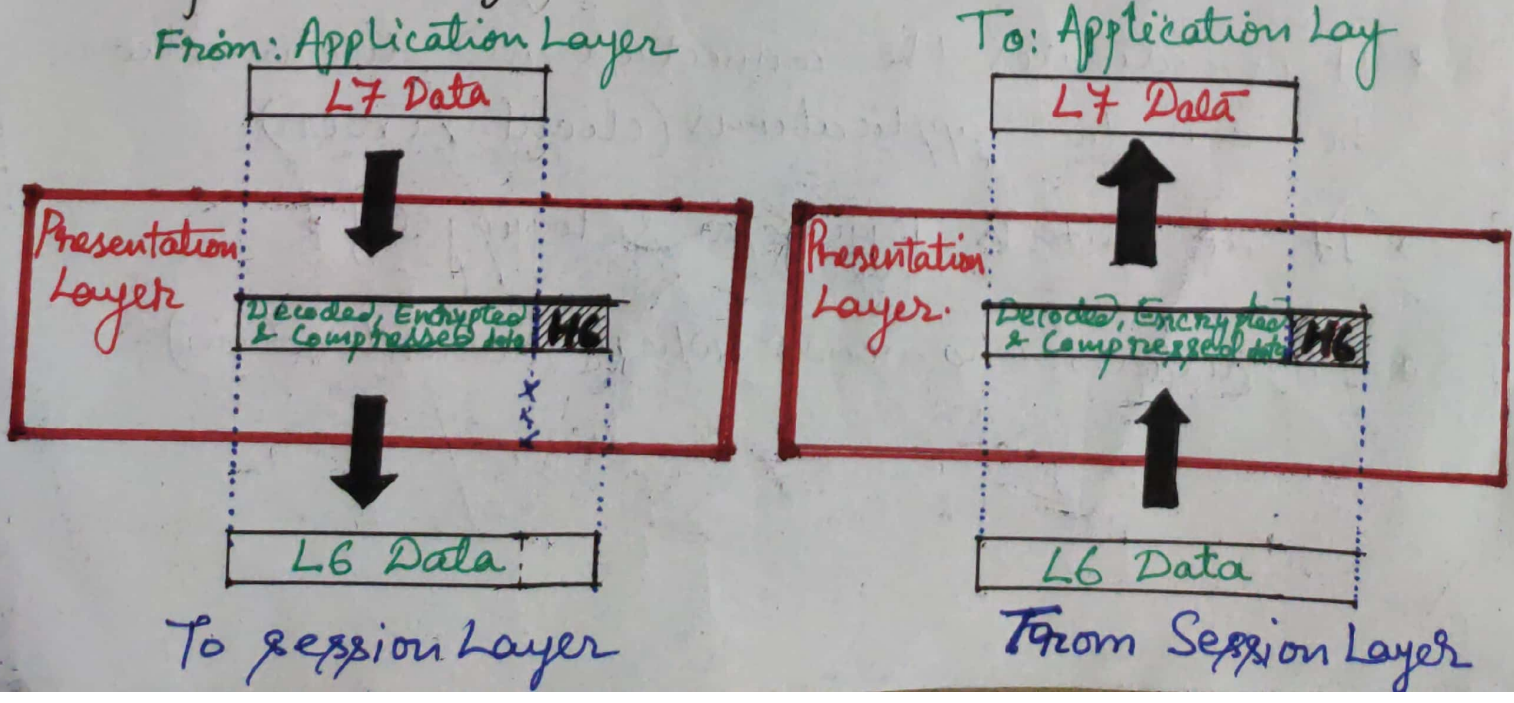
2) **Encryption:** It encrypts data and decrypts data b/w sender & receiver ends for security purpose.

Substitution
Encryption Algo : A → B → C → D - - - - Y → Z → A

DATA ⟶ EBUB ⟶ OTP

3) **Compression/Decompression:** It performs compression to minimize the size of data to be sent and hence it optimizes the network bandwidth.

4) It facilitates protocol conversion system for heterogeneous network environments.



Lecture-08 Cont.....
Network

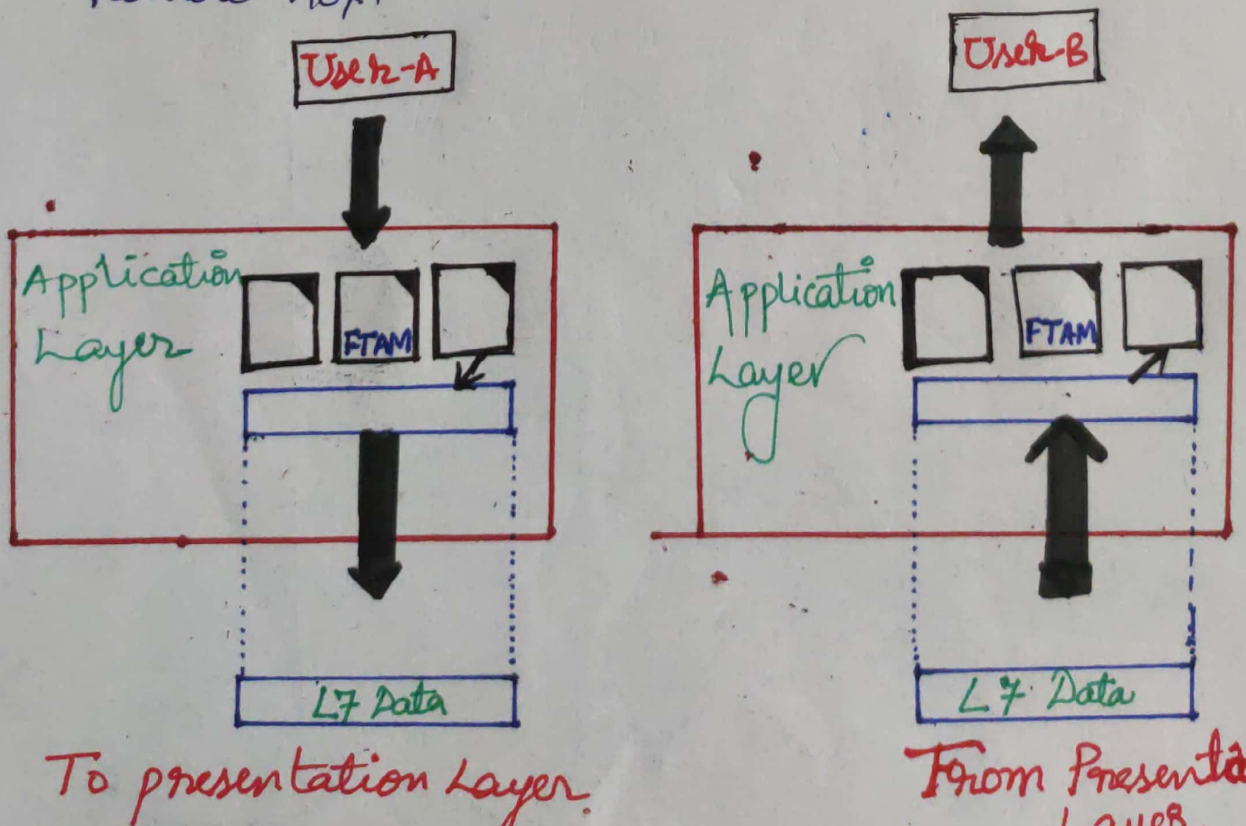
7. Application Layer :

1) It provides FATM services to user and enable them to access, transfer and retrieve a file ass well as ~~the~~ do management of files on a remote computer.

2) It provides a basis for email forwarding & storing.

3) It provides distributed database and access to the world wide web (WWW) information across the internet world.

4) It creates a Virtual Terminal at both end which is a kind of software emulation of remote host.



⇒ Merits of OSI Model

1) The protocols in OSI model are bttter hidden therefor it can be easily updated & modified without affecting other (layers or protocols)
2) It supports both connection-less and connection oriented services.
3) It distinguishes between the services, enter-faces and protocols very clearly.

⇒ Demerits of OSI Model

1) This is mere a reference model
2) This model was derived before the invent of ~~pro~~ its protocols therefore it lacks on practical ground eg; It has problem of fitting protocl into a model
3) Session & Presentation Layers doesn't have much to do and are rarely used in practicals.

LECTURE-09

Computer Network

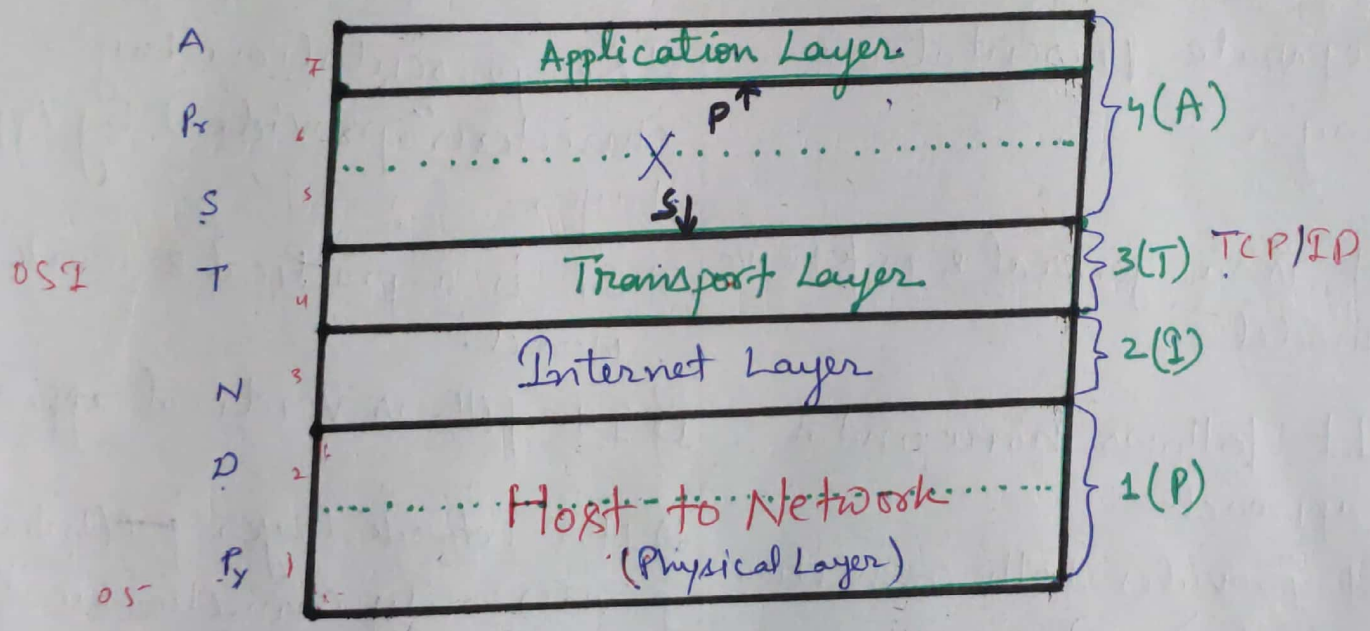
COMPUTER NETWORK

→ TCP/IP Model

→ Differences b/w TCP/IP & OSI

TCP/IP Model → Working Model -(4)

OSI Model → Reference Model (7)



TCP/IP Layers

TCP/IP Layers & Associated Protocols

LAYERS:	PROTOCOLS
* Application Layer: →	TELNET, FTP, DN HTTP, SNTP, NNTP
* TRANSPORT LAYER: →	TCP, UDP
* INTENET LAYER: →	IP
* Host to Network LAYER: →	ARPANET, SATNET LAN Pactet-Radio

* Difference between TCP/IP & OSI Model

OSI	TCP/IP
1) It has 7-layers	1) It has 4 layers
2) Seprate Session layer	2) No session layer, but the charecteristics are provided by its transport layer.
~~3) Separate.~~	
3) Separate Presentation layer	3) No presentation layer but charecteris" provided by Applicato layer.
4) It is a general & reference model	4) It is a practical & working model.
5) It follows horizontal approach	5) It follows vertical approach.
6) It provides both connection oriented and conn"less services at its network.	6) Its network layer ~~pro~~ (Internet layer) provides only connection-less service.
7) The protocols are better hidden and can be easily modified/updated ~~this~~ without having affected other layers	7) Protocols are susceptible to change ~~of~~ and could not be replaced easily.
8) ~~It~~ Transport layer gaurantees delivery of packets	Transport layer does not gaurantees delivery of packet.

COMPUTER NETWORK

LECTURE-10

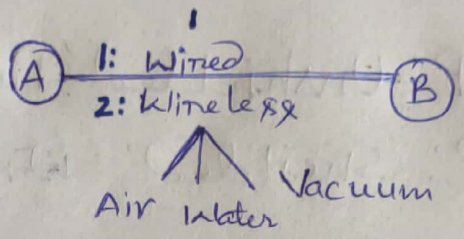
Computer Network

15.09.20

COMPUTER NETWORK

1) Transmission Media:

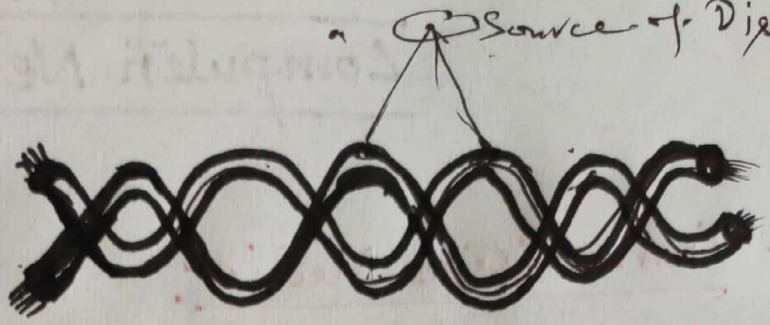
Guided Media
Unguided Media



Transmission Media

- Guided Media
  - 1 → Twisted Pair Cable
  - 2 → Coaxial Cable
  - 3 → Fiber Optics
- Un-guided Media
  - 1 ← Radio Waves
  - 2 ← Microwaves
  - 3 ← Infrared Waves

1) Twisted Pair Cable:



UTP: Unshielded Twisted Pair

STP: Sheilded ~~Wire~~ Twisted Pair

* Twisting is done to cancel the noise effect at destination.

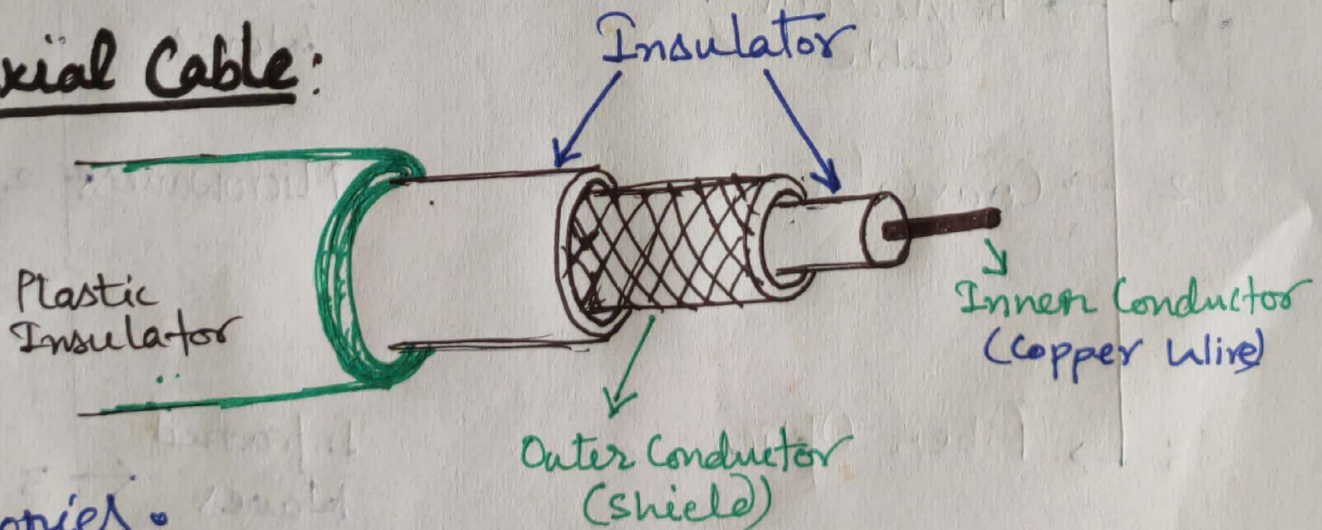
* Twisted pair cable are used in LAN, T-Lines & Telephones Cables

* Data Rate: 2 Mbps to 600 Mbps

↘ SSTP (Sheilded Screen Twisted Pair)

* Connectors: RJ45

2) Coaxial Cable:



Categories:

RG-59 —— Cable TV

RG-58 —— Thin Ethernet

RG-11 —— Thick Ethernet

Lecture-10
Network

COMPUTER NETWORK

Guided Media

1) Twisted Pair Cable

- Consist of 2 conductors (Copper)
- Each conductor owns a plastic insulation
- One wire carries signal, other carries ground reference
- ~~Other one~~ Receiver uses the deffrence b/w these two.

Types:

a) **U.TP (Unsheilded TP):** Normal TP wire without any extra insulation or wrappings.

b) **STP (Shielded TP):** It has a metal foil or braided mesh covering the encases each pair of insulated conductors.

Applications of Twisted Pair:

~~Unguided~~

1) Telephones lines to carry voice and data signals.
2) In the local loop line.
3) In DSL/ADSL line
4) In LANs eg 10 Base-T & 100 Base-T cables.
5) In ISDN (Integrated Services Digital Network).

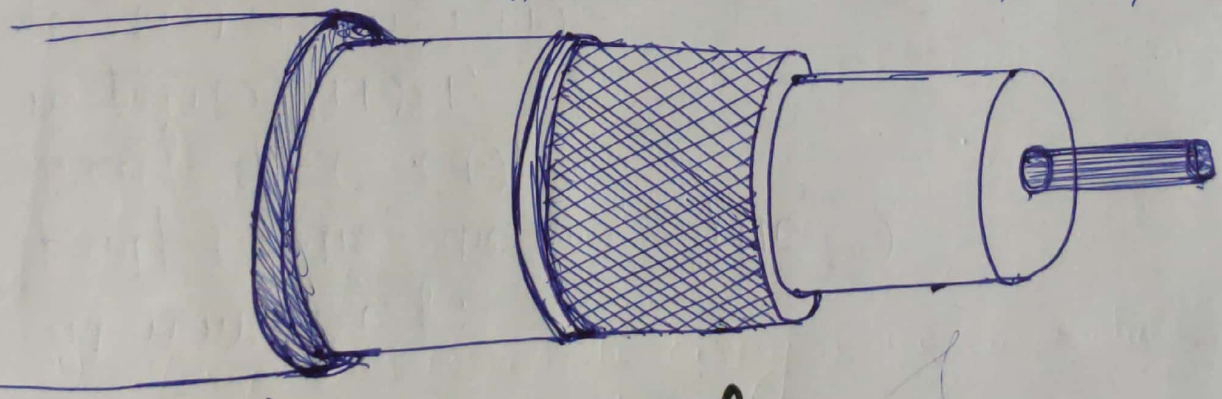
Note: Why twisting is done.

* Twisting reduces the noise-effect or cross-talk and other external interference.
* Number of twist per unit length of wire detemines the quality of cable. More twisting contributes higher quality.

Lec. 10 Cont....

2) Coaxial Cable: It is meant to carry signals of higher frequencies than T.P.

- It has a central core conductor of solid coppe wire, enclosed within insulating seath.
- The inner core is further encased in an outer conductor of metal foil, braid or combination of these two..
- The outer mesh covering of metal foil acts both as a conductor and as a sheild against noise.
- It has less attenuation than twisted pair cable.

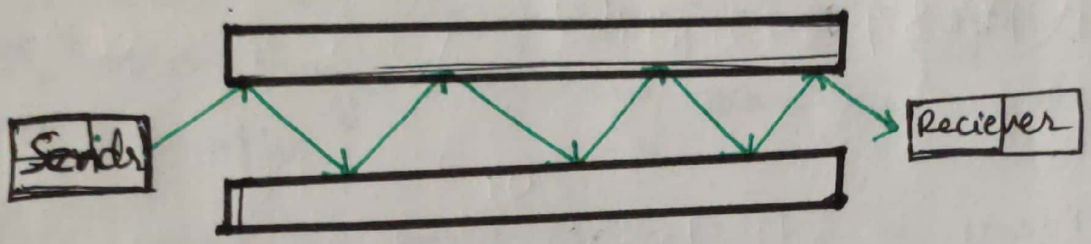


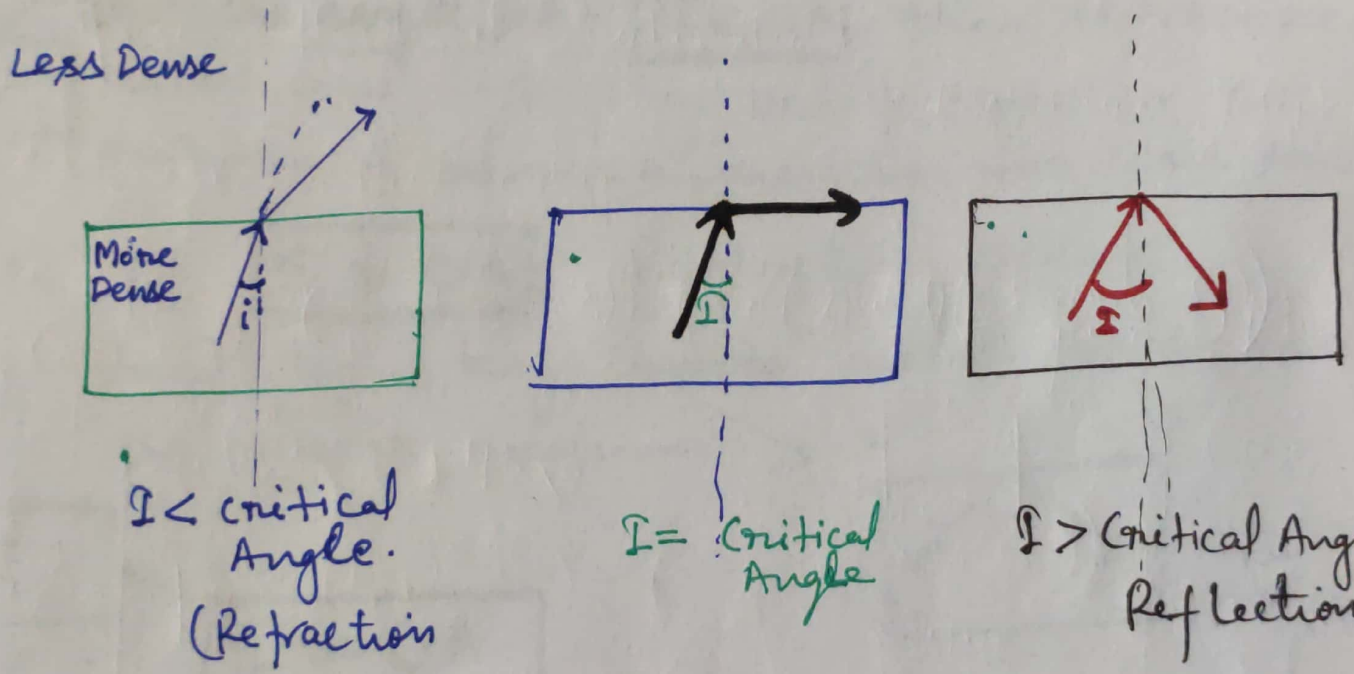
Applications of Coaxial

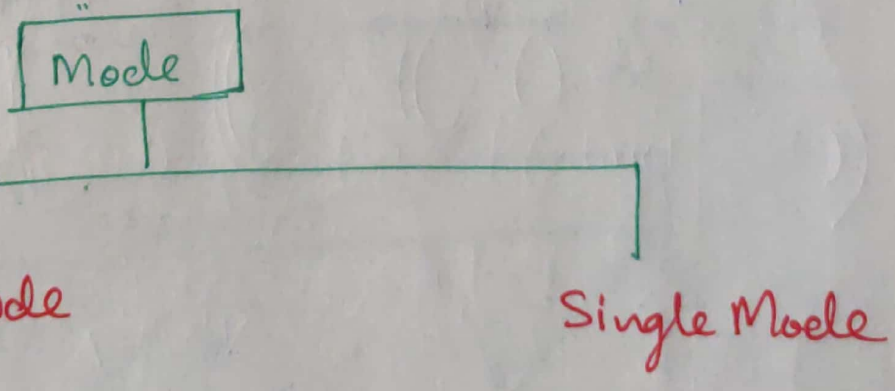
1) Analog Telephone Network.
2) Cable TV
3) Digital Transmission
4) Digital Telephone Network
5) Traditional Ethernet LANs
6) Thick & Thin Ethernet(s).

Lecture-10(2) Cont...
Comp. Network

2) Guided Media : Fiber Optical Cable

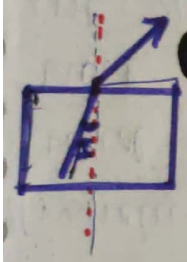




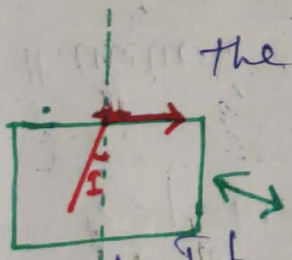


3) Fiber Optic Cable

- It is made of glass or plastic and transits signals in form of light.
- It works on the principal of optics for a light ray travelling from one medium to another.
- If angle of incidence (I) is less than **Critical angle (C·A)** $I < C·A$ then refraction occurs and light ray bends closer to the surface of ~~denseser medium~~ into lesser density.

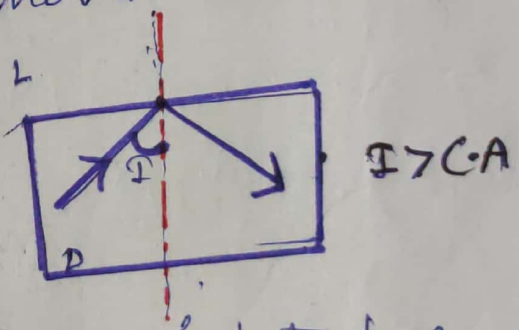


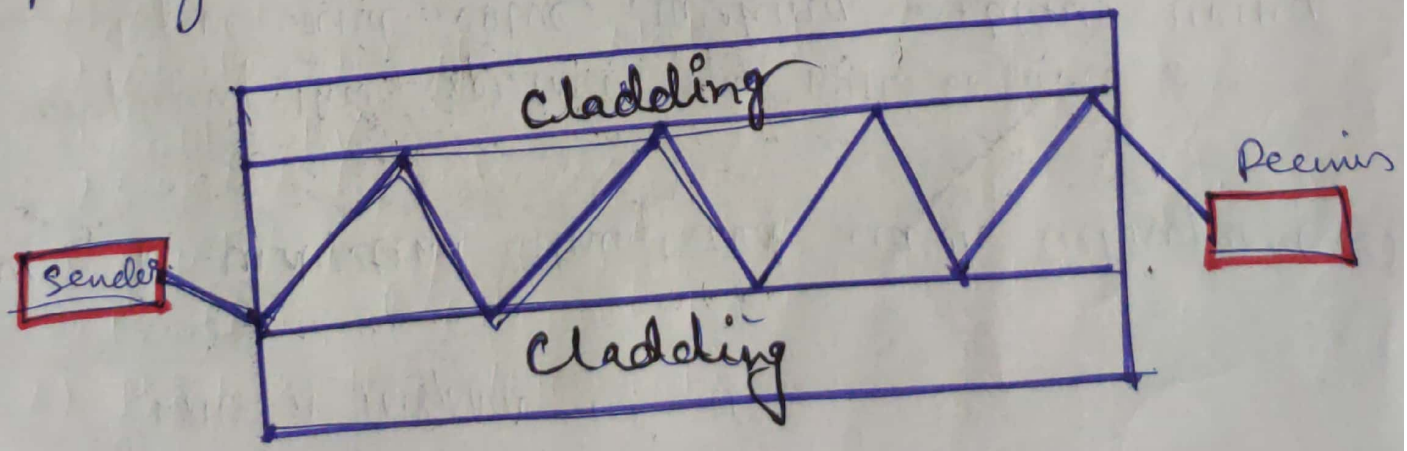
- If $I > C·A$; Reflection occurs and light ray ~~bends~~ moves back into the denser medium.



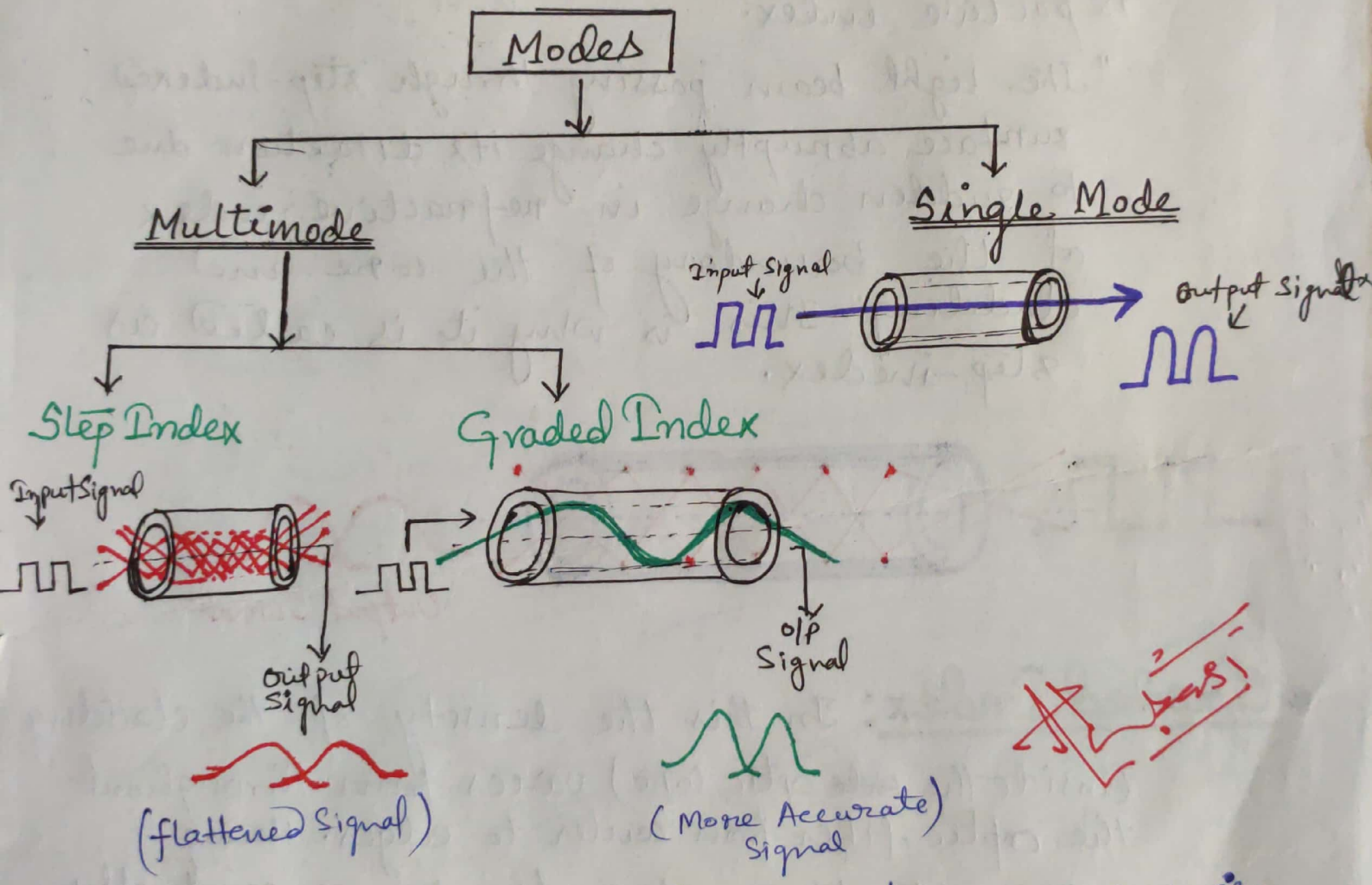
If $I = C·A$

Light Ray bend along the ~~surface~~ interface or surface





* Propagation Modes: It refers to the number of paths followed by light rays inside a fiber optic cable. It can be categorized as follow-



a) Multimode: Multiple light beams from a source are rendered inside the core which pass through it following different paths with different velocities. The density of the core remains constant from the center to the edges. It supports multiple several modes of propagation simultaneously.

b) Single Mode:

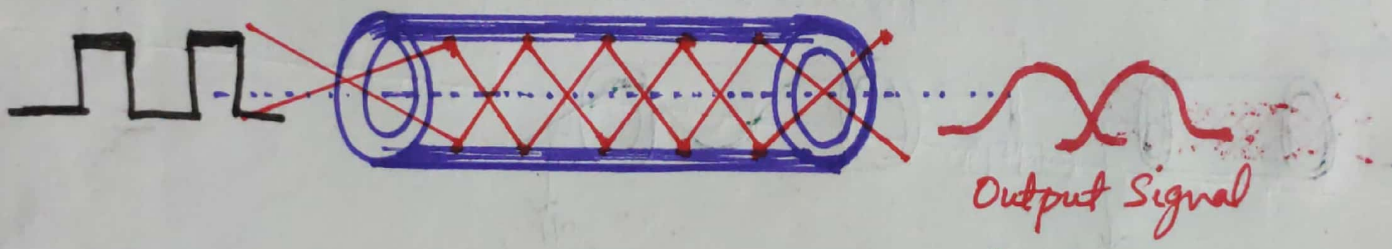
Single mode uses step-index fiber and highest intensity light beam from source, limiting it to a very small range of angles close to all horizontal line. It has very small diameter and has lower density inner cladding. All beams passing through it are almost horizontal

Lecture-10(2) Cont...

Computer Network

***Step Index:** In this the inner core of the fiber ~~opti~~ optic wire is cladded with a material in such a way that the density remains same from center to edge with a lower refractive index.

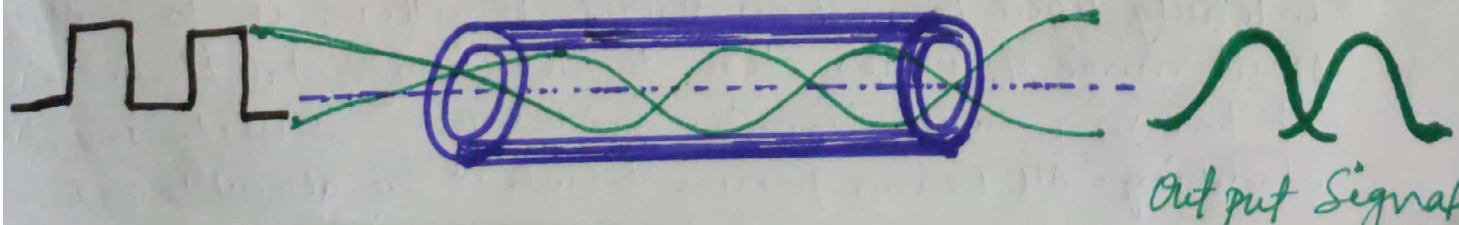
"The light beam passing through step-indexed surface abruptly change it's direction due to sudden change in refractive index at the boundary of the core and cladding". This is why it is called as step-index.



***Graded Index:** In this the density of the cladding (inside the ~~code~~ optic core) varies ~~from~~ throughout the optic fiber from center to edges. ~~Hence~~

"The refractive index also changes gradually from center to edges along the varying ~~desi~~ density of core cladding. Hence the incident light beams changes its direction gradually and hence more accurate signals are likely to reach at destination.

The density is ~~at its na~~ highest at the center and decreases gradually to its lower ends.

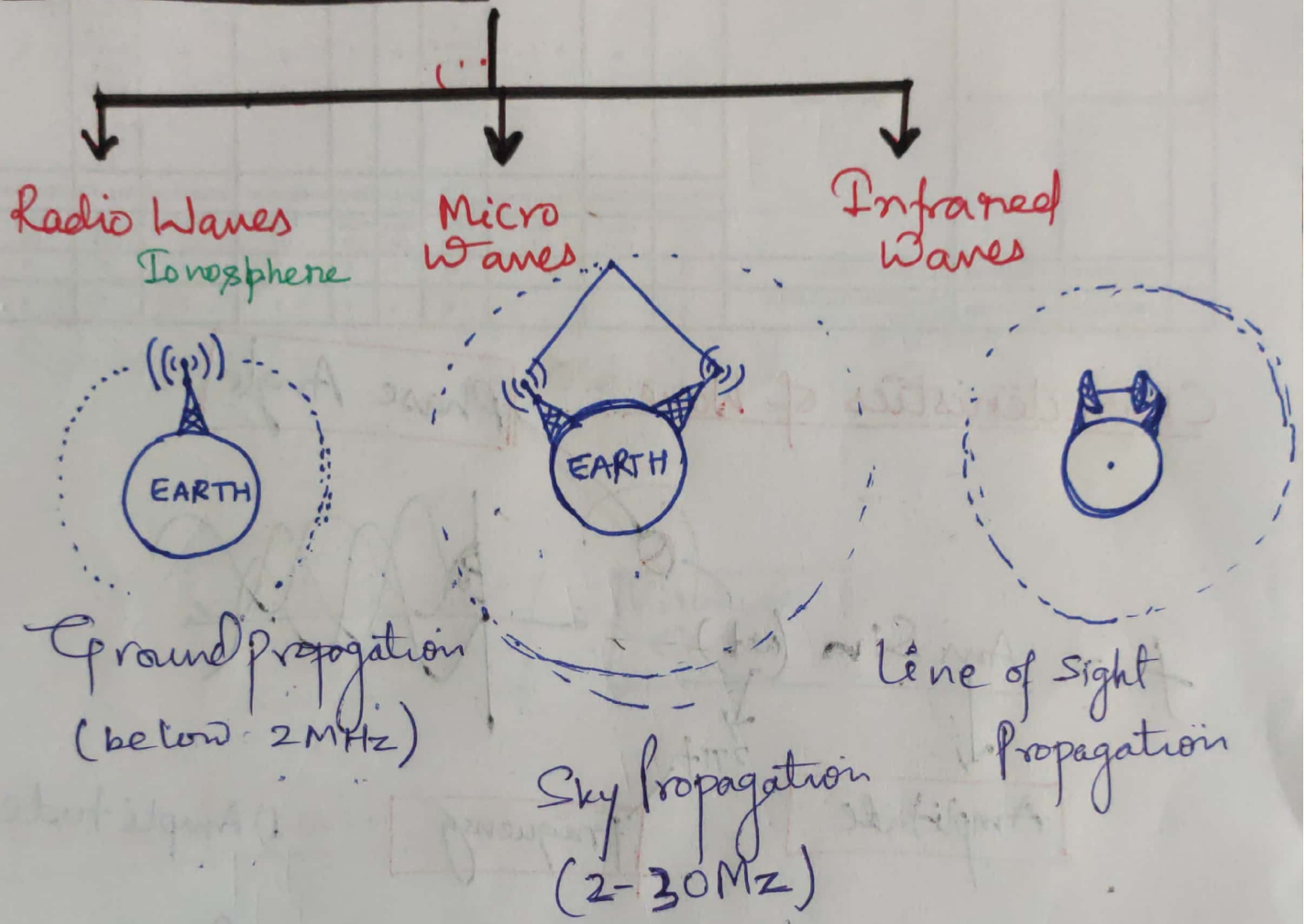


LECTURE-11 ● Computer Network

19. Sep. 20

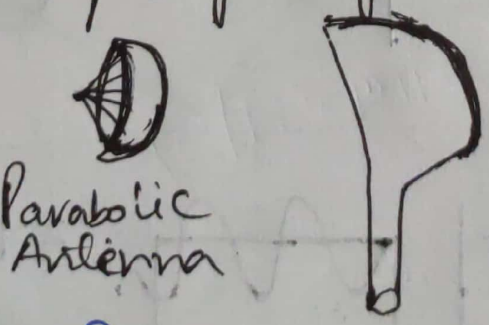
COMPUTER NETWORK

* UnGuided Media:



1) **Radio Waves:** Frequency range 3KHz — 1GHz

2) **Micro Waves:** Frequency Rang 1GHz — 300GHz



3) **Infared Wave:** Freq. Range 300GHz — 4THz

Short Range Commuc".

Can not Penetrate Wall

Used in Bluetooth (IrDA)

Data ~~Rate~~ Rate: 75 Kbps to 4Mbps.

Characteristics of Wave

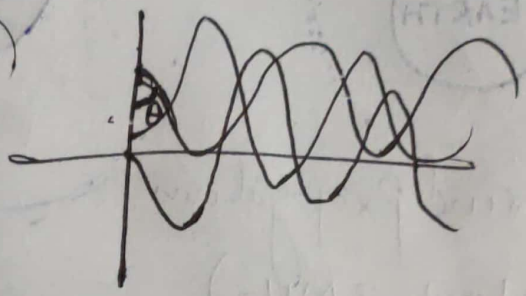
Phase Angle

$f = A_m \sin(\omega t)$

$\omega t \rightarrow 2\pi f$

Amplitude

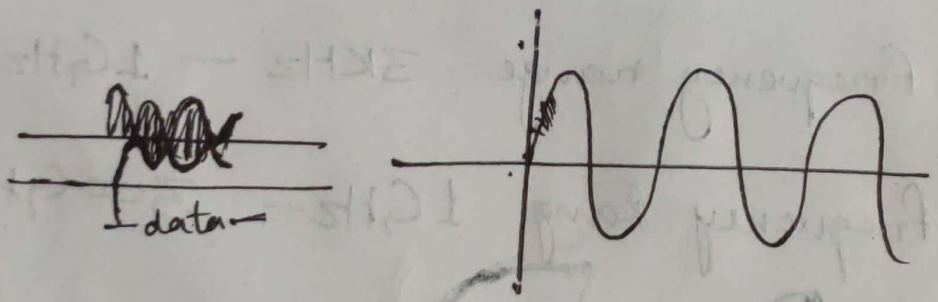
Frequency



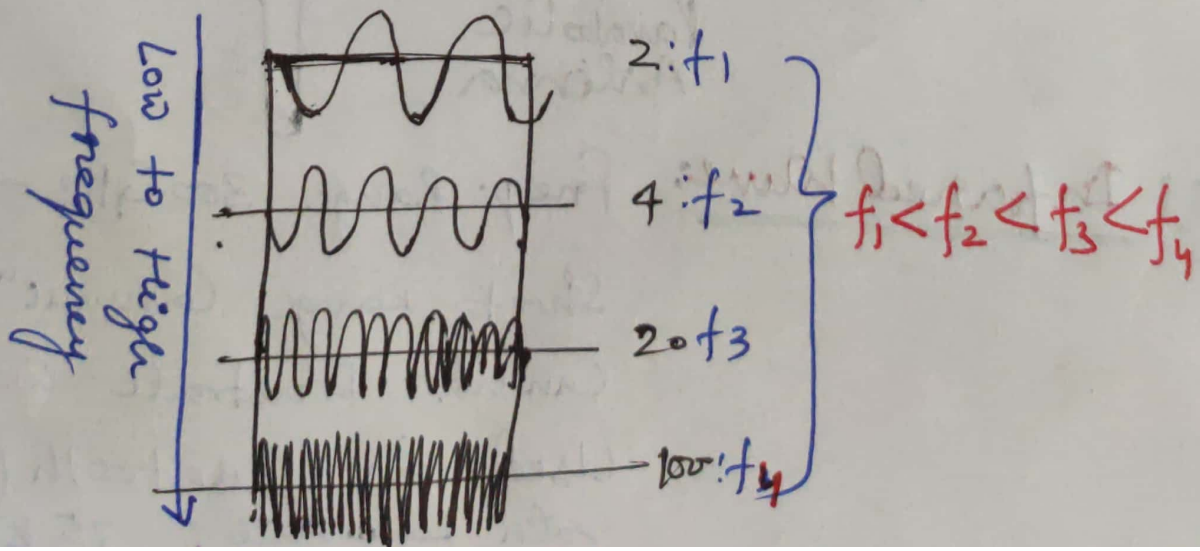
1) Amplitude (Am)

2) Frequency (F)

3) Phase Angle (θ)



1)

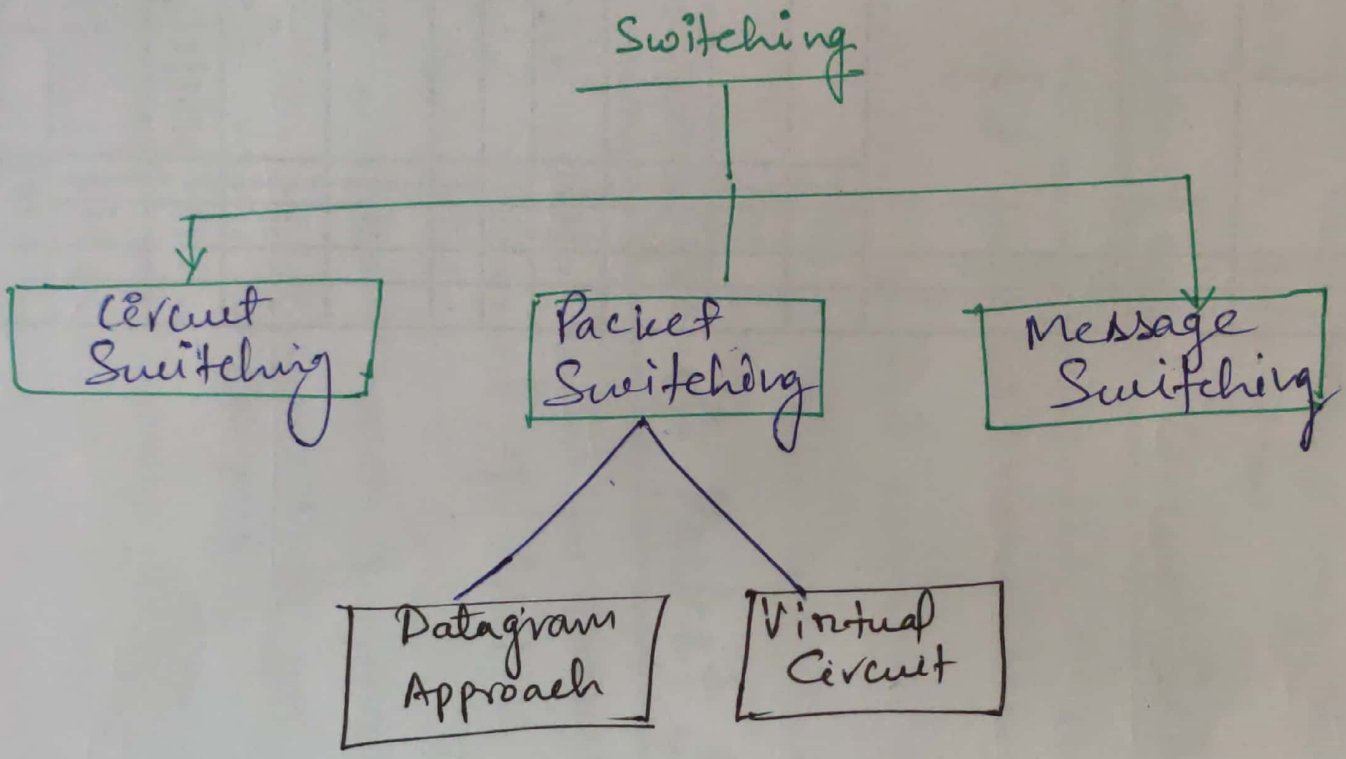


Switching:

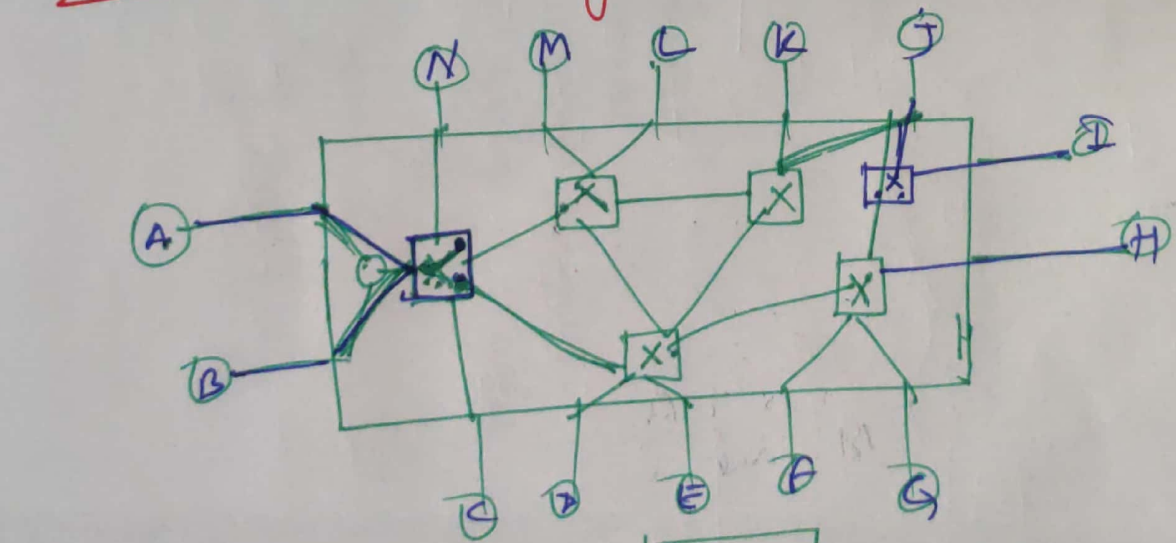
19.09.20

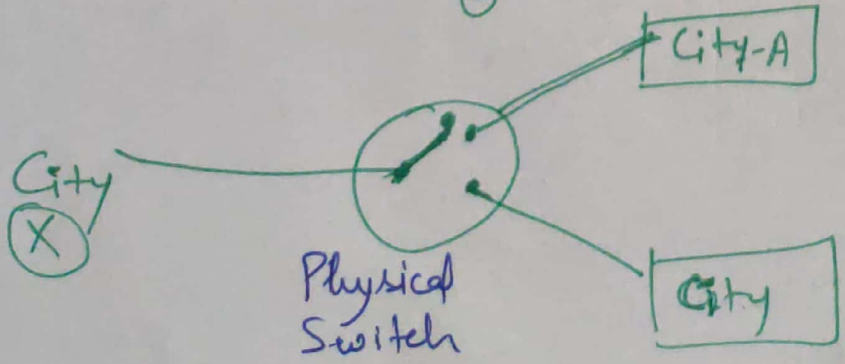
COMPUTER NETWORK

Switching Modes:



① Circuit Switching:





Switching Methods

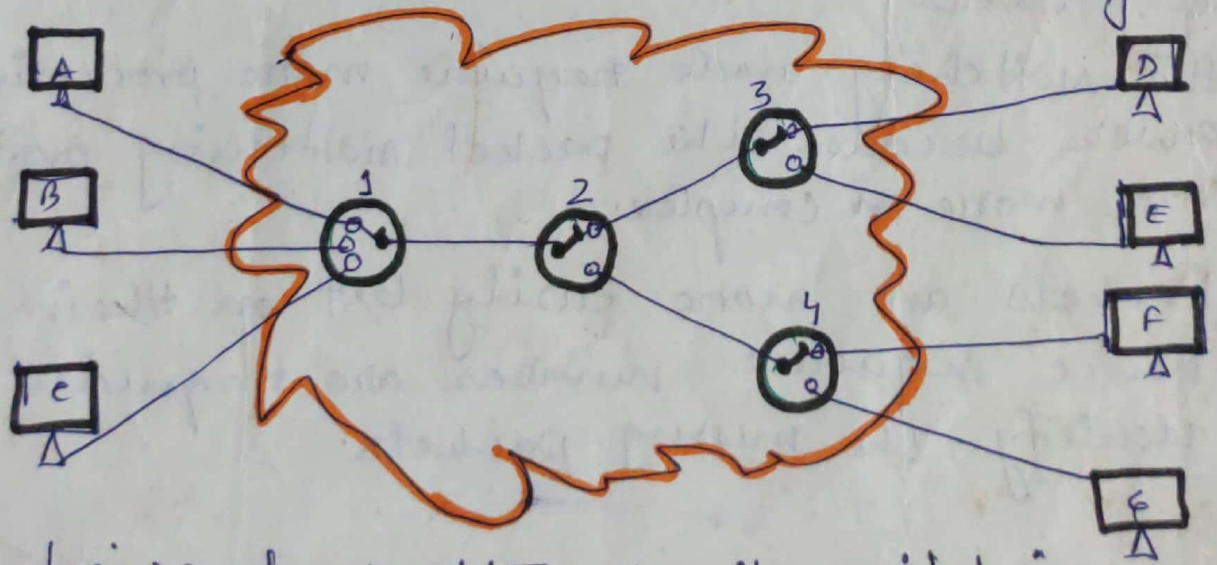
Switching is the technique that determines that how the connections among the nodes are established and how data movement is handled.
There are three switching techneque

a) Circuit Switching
b) Message " "
c) Packet " "

1) Circuit Switching (Telephon N/Ws):-

In circuit switching communicating devices are connection oriented. The end-to-end connections are established for a duration and a dedicated link is established for that duration.

Hence, the transfer mode of a n/w that involves setting up a dedicated end to end connections is called circuit switching.



The figure shows the circuit switching as in the by telephone n/w a circuit switched connections are et established.

Advantages of Circuit Switched N/w

① Due to a dedicated link establishment, a guaranteed data transmission is possible

② Ensures, the privacy and also prevents delay in data flow.

Disadvantages Circuit Switching:

① Due to being dedicated, a channel could not to be used for other nodes even if the channel is free.

② Dedicated channel requires more band width.

③ It takes long time to establish connections.

Disadvantages of Packet Switching

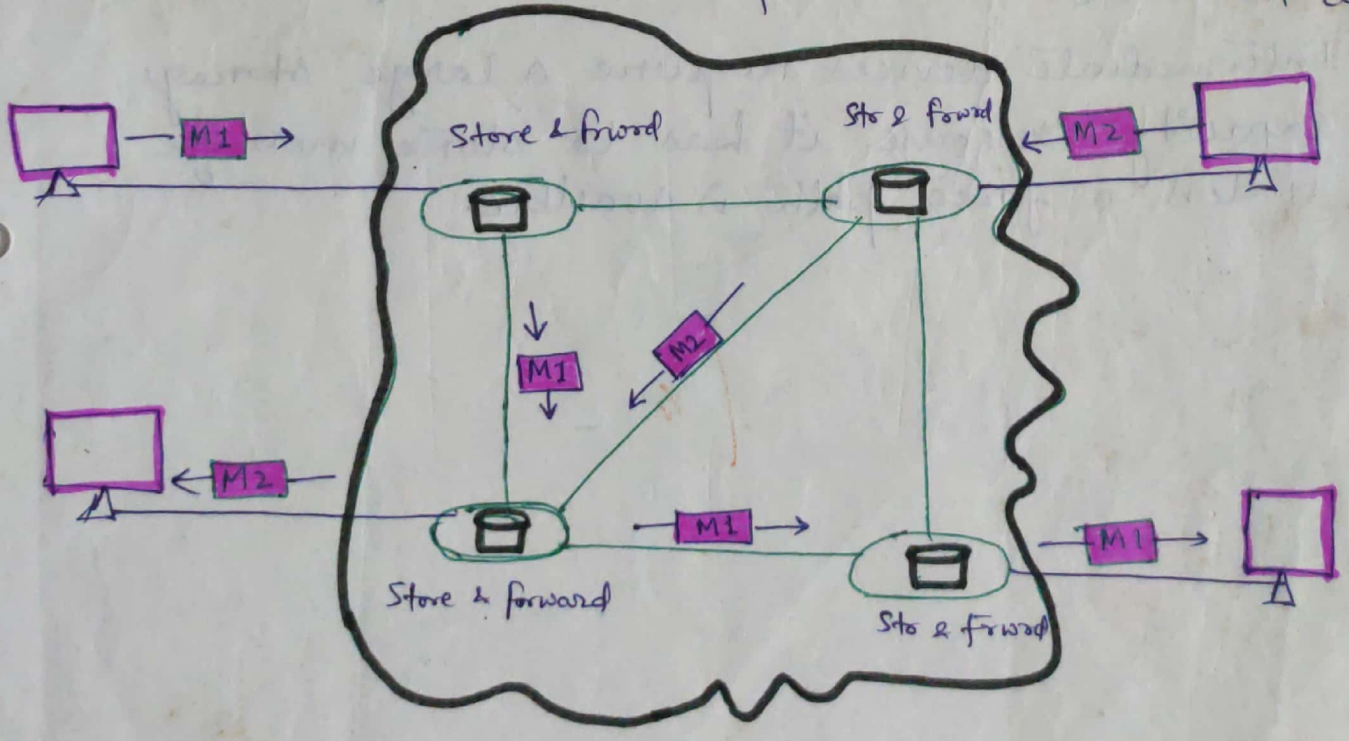
① Switching nodes for packet switching require large amount of RAM to handle large quantities of packets.

② The switching node require more processing power because the packet switching protocols are more complex.

③ Packets are more easily lost on their route hence sequence number are required to identify the missing packets.

(2) Message Switching (Telegraph Network):-

In message switched n/w nodes are connected to the stations, called as switching station.
At this switching station, an operator takes the decision of routing the message based on the destination address information.
Whenever a message arrives at the station, the operator either forward the message to the destination if the channel is free or hold & store the message until the channel becomes free.
In this, no dedicated link is established.
Each message is treated as an independent unit and includes its own destination and source address.
Each inter-mediate devices (stations) recieves the message and store it, until the next device is ready to recieve it and then forward it to the next device



Message Switching

Advantages of Message Switched N/W

1. Provides efficient traffic management by assigning priorities to the messages to be switched.
2. Reduces n/w traffic congestion because it is able to store message untill a comm channel is free.
3. Network devices are allowed to share the data channel.
4. Provides asynchronous comm" across time zone.

Disadvantages of Message Switched N/W:

1. It can not be used for real-time application such as voice and vedio because storing and forwarding of message causes delay.
2. Intermediate devices require a large storage capacity because it has to store message unless a free path is availble.

Lecture - 11 Cont....

3) Packet Switching (Internet & Cellular N/W) :-

In packet switching, messages are broken into packets, each of which includes a header with source, destination and intermediate nodes address information. ~~Independent~~

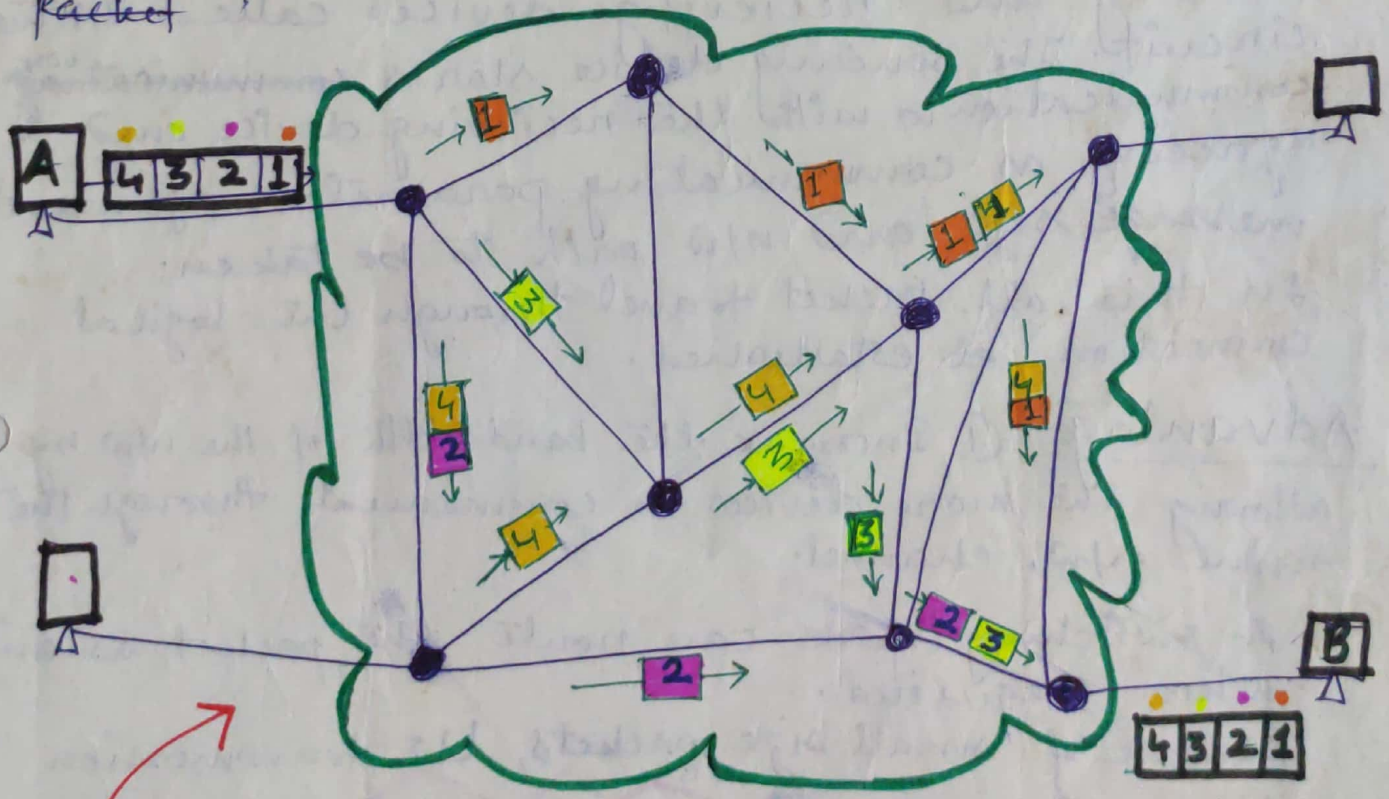
Individual packets take different routes to reach at destination, this gives two advantage -

a) Bandwidth is reduced by splitting data into different routes in a busy circuit.

b) If certain link in n/w goes down, the transmission, the remaining packets can be sent through another route.

A packet is restricted to a maximum length so - as to be stored in intermediate devices.

~~Packet~~



Packet switching could be done in two way -

a) Datagram Packet Switching

b) Virtual Circuit Packet switching.

Lecture - 11 Cont....

a) Datagram Packet Switching

In this method a message is devided into a stream of packets.
Each packet is separately addressed and treated as an independent unit with its own control instructions. Each intermidiate nodes determines the packet's next routes segment. Before the transmission starts, the sequence of packets and their destinations are established by the exchange of control information b/w sending & receiving ~~temet~~ terminal of n/w.

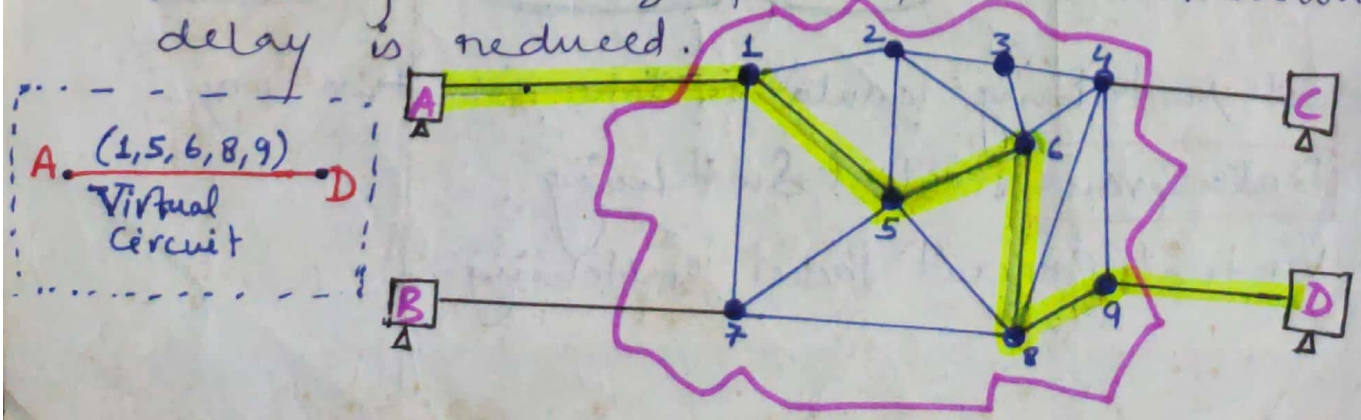
b) Virtual Circuit Packet Switching:

It established a logical connection b/w the sending and recieving devices called virtual circuit. The sending device starts ~~communication~~ communication with the recieving device and agreeing as communicating parameters eg: maximum message size, and n/w path to be taken.
In this all packet travel through the logical connection et established.

Advantage ① Increase the band width of the n/w by allowing the more devices to communicate through the same n/w, channel.

② A switching node can route the packet as and when required.

③ Because of small size packets, the transmission delay is reduced.



- **Rule Based Management:** It is required to define the set of rules for the secured communication among different devices in the network. It also monitors IT events through secure rules driven system in the network.

- **Firewall Rules**: It defines the secured rules for communicating with different firewalls in the network. Firewall rules defines the different range of security policies in order to provide the access to the network only to the set of authorised users on the network.

ii. Securing Network Application

There are many ways to define the security for different applications on the network. Security plays a major role across all the layers of Open Systems Interconnection (OSI) model of the network. OSI model helps for easy communication across different hosts in the network. OSI model provides a flexible interface for sending, sharing, and storing the information on the hosts in the network. The OSI model is shown in the figure 2.2.8:

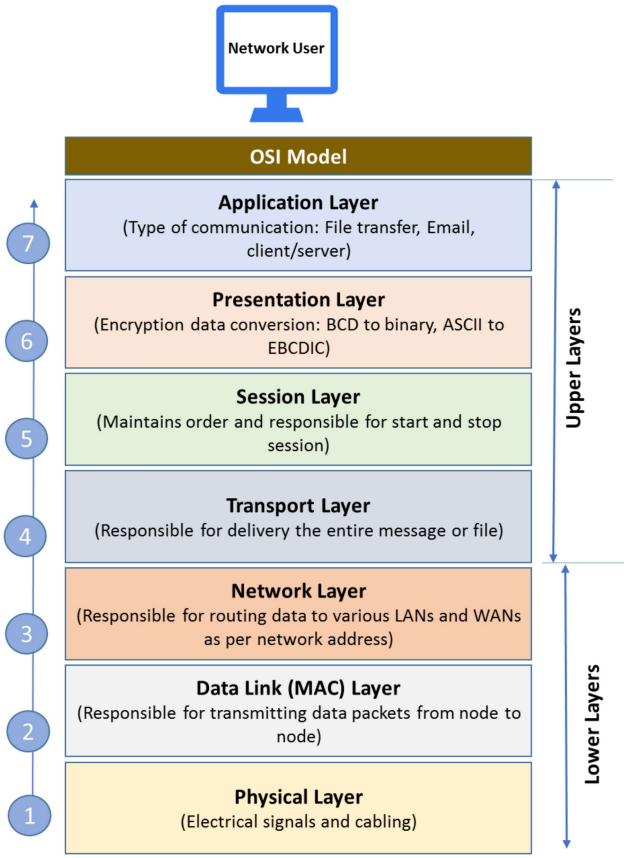


Figure 2.2.8: OSI Seven Layer Model

At the application layer, basic security is provided across various end users applications on the network. In presentation layer, security is provided in defining the format of the information on the network.

At the physical layer, the security is provided for basic communication across different hosts in the network. Similarly, security plays a major role across all the other layers of the OSI model.

Security plays an important role within the context of seven layer OSI model as shown in the table 2.2.1:

Layer Number	Layer Name	Description	Function
Layer 7	Application Layer	This layer provides the interface to the users. The users can perform multiple tasks such as file transfer, email, etc.	Provide services for user applications
Layer 6	Presentation Layer	Transforms the data from different devices to the recognizable format (Read and write).	It is used for translation, compression, and encryption.
Layer 5	Session Layer	Establishes and manages the connection to other devices.	Allows devices to establish and manage sessions.
Layer 4	Transport Layer	It controls end to end transmission and error checking. This ensures the complete data transfer by checking whether small pieces of data called fragments are arrived.	Provide connection, establishment, management, and termination as well as acknowledgements and retransmissions.

Layer 3	Network Layer	This layer act as network/logical addressing and routing between two different networks.	Makes logical addressing, fragmentation, and reassembly available.
Layer 2	Data Link Layer	As the name indicates, it is a two party communication layer acting as Ethernet. It ensures that computer abstract address (IP address) is associated with physical computer for the communication inside the same network.	Performs physical addressing, data framing, error detection, and handling.
Layer 1	Physical Layer	It handles actual electrical and physical transmission of the data over a network medium. In general terms, it is a hardware means used for sending and receiving the data over medium.	Involved with encoding and signalling, data transmission, and reception

Table 2.2.1 OSI Reference Model

Network Security Strategies:

It is most important and difficult task to develop network security strategies that protect all parts of the complicated network with minimum effect on the use and performance of the network. Challenges such as a complexity and porous nature (minute loop holes) of the modern networks that include public serves for e-commerce, extranet connections and remote access services are faced by the Security design. In order to handle all the difficulties,