Introduction to Computere Networeek —

A Networeek is a set of devices (nodes) connected by media links. A node can be a computere, printere or any other devices capable of sending and/or receiving data generated by other nodes on the Networeek.

Definition of Computere Networeek — Computere Networeek means an interconnected collection of autonomous computeres capable of having inter connections with each other.

Distributed system — If one computere can forcibly start, stop or control another, the computere are not autonomous. A system with one control unit and many slaves, are a large computere with remote printers and terminals is called a distributed systems.

Layered Architecture — computere n/w are generally organized as a series of layers or levels, each one built upon the one below. Every layere needs a mechanism for identifying senders and receivers.

Protocol — There are certain rules that must be followed to ensure proper communication.

- Node — It can be any network device (router, printer, camera)
- Host — It represents computer / work stations. (interface)
- Hub — Network device used to increase the reach-ability of signal re-generator it works in physical layer.

(a Switch without IP address is neither a node or a host)

Workstation — is a computer intended for individual use that is

faster than and more capable than a personal computer.

Types of Networks. —

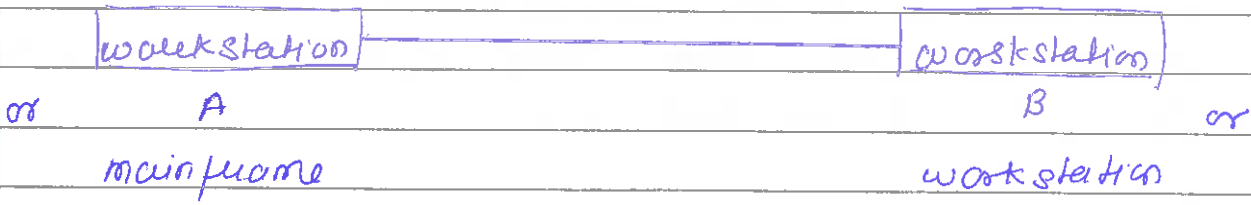
On the basis of transmission technology networks are classified into three categories.

1. Point-to-point 2. Multipoint 3. Broadcast n/w

Basic Concepts —

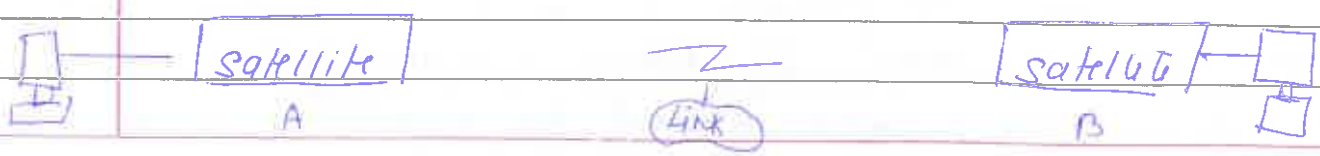
- Line configuration
- Topology
- Transmission mode
- categories of networks
- Internetwork

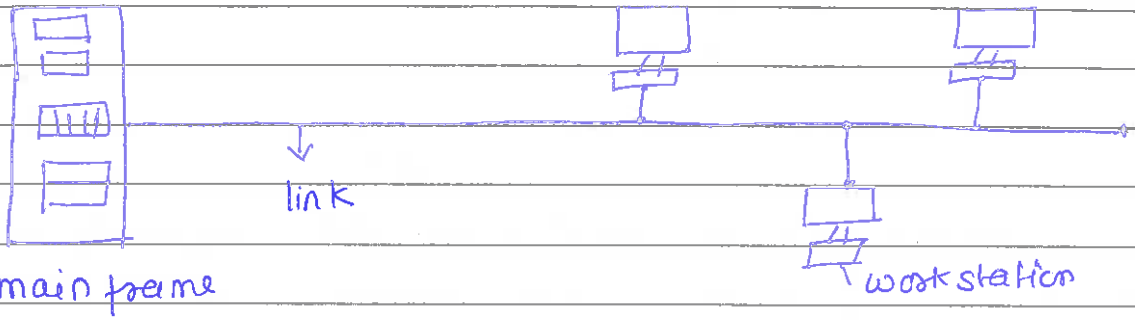
Line configuration — defines the attachment of communication devices to a link



point to-point line configuration

Point-to-point provides a dedication link between two devices. (use an actual length of wire or cable) or microwave or satellite links are also possible





Multipoint (also called multidrop) line configuration is one in which more than two specific devices share a single link. (capacity of the channel is shared, either spatially or temporary)

Topology :- defines the physical or logical arrangement of links in a network.

Mesh	point-to-point	(n-1) dev i/o ports	n(n-1)/2 device wise
Star	point-to-point	n i/o ports	n wire
Tree			
Ring	point-to-point	2n i/o ports	n wire
Bus – multipoint			

Q The lucky Ducky corporation has a fully connected mesh network consisting of eight devices. Calculate the total number of cable links needed and the number of ports for each device. (mesh / star / ring)

Transmission Mode – refers to the direction of information flow between two devices.

- Simplex — unidirectional — key → TV, Radio
- Half Duplex — direction of data at a time — walki-talkie, internet browser
- Full Duplex — Direction of data all the time — cell phone, two lane road

T
R
D
B
A

Categories of Network –
LAN / MAN / WAN

Internetworks – two or more n/ws are connected.

Q In satellite communication, up-link frequency and down-link frequency are different, why?

Ans Interference can be avoided

Q. In a broad sense, a railway track is an example of

Ans Half duplex

Q The topology with highest reliability is – Mesh.

Q. The method of communication in which transmission takes place in both directions; but only one direction at a time is called – Half duplex

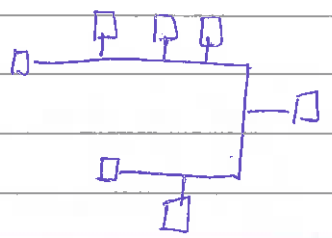
Q Security and privacy are less of an issue for devices in a which topology? Bus

Q A cable break in a which topology stops all x-missions
bus

Q. In a mesh topology, the relationship b/w one device and another is peer-to-peer

Q. A network that contains multiple hubs is most likely configured in a Tree

Q



Q Assume six devices are arranged in a mesh topology? How many cables are needed? How many ports are needed for each device?

Layered Architecture —

Established in 1947, the International standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the open system Interconnection model (OSI).

The purpose of the OSI model is to open communication between different systems without requiring changes to the logic of the underlying Hardware & Software. It is not a protocol, it is a model for understanding and designing a network architecture that is flexible, robust and interoperable.

T R U B A

Mnemonic —

Please Do Not Touch Steve's Pet Alligator

Peer-to-peer process — Between machines, layer x on one machine communicates with layer x another machine. This communication is governed by an agreed-upon series of rules + conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes.

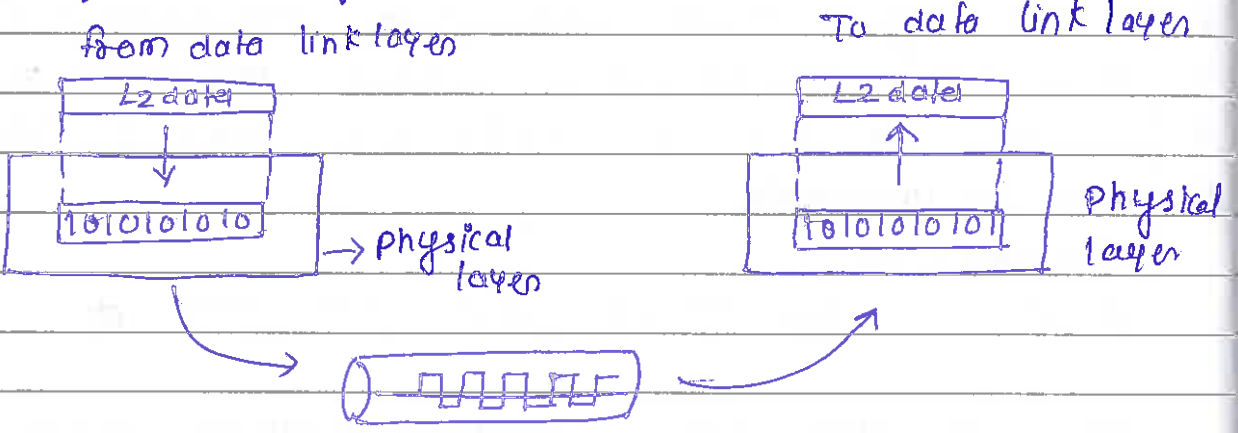
Interfaces between layers — Each interface defines what information ~~and~~ interfaces b/w & services a layer must provide for the layer above it.

Organizations of layers — Layers 1, Layers 2 and Layers 3 are the network support layers. They deal with the physical aspects of moving data from one device to another.

Layers 5, 6 and 7 can be thought of as the user support layers, they allow interoperability among unrelated Software systems.

Functions of the layers —

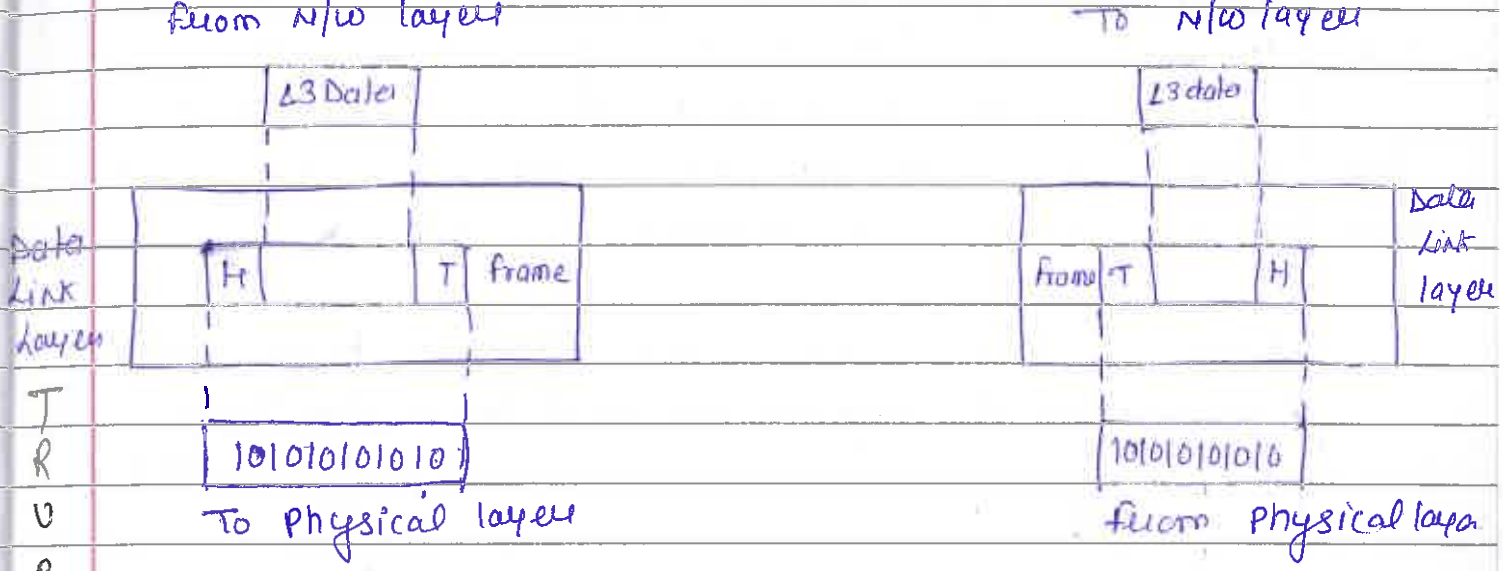
1. Physical layer — coordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical & electrical specifications of the interface & transmission medium.



1. It defines the characteristics of the interface b/w the devices and the transmission medium.
2. It consist data, in a stream of bits without any interpretation.
3. Data rate — the number of bits sent each second.
4. Synchronization — The sender & receiver must be synchronized at the bit level.
5. Line configuration
6. Physical Topology
7. Transmission mode.

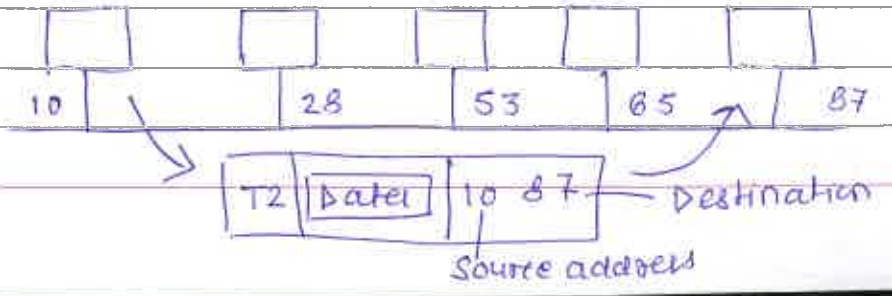
Data Link Layer — transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for node-to-node

delivery, it makes the physical layer appear error free to the upper layer.



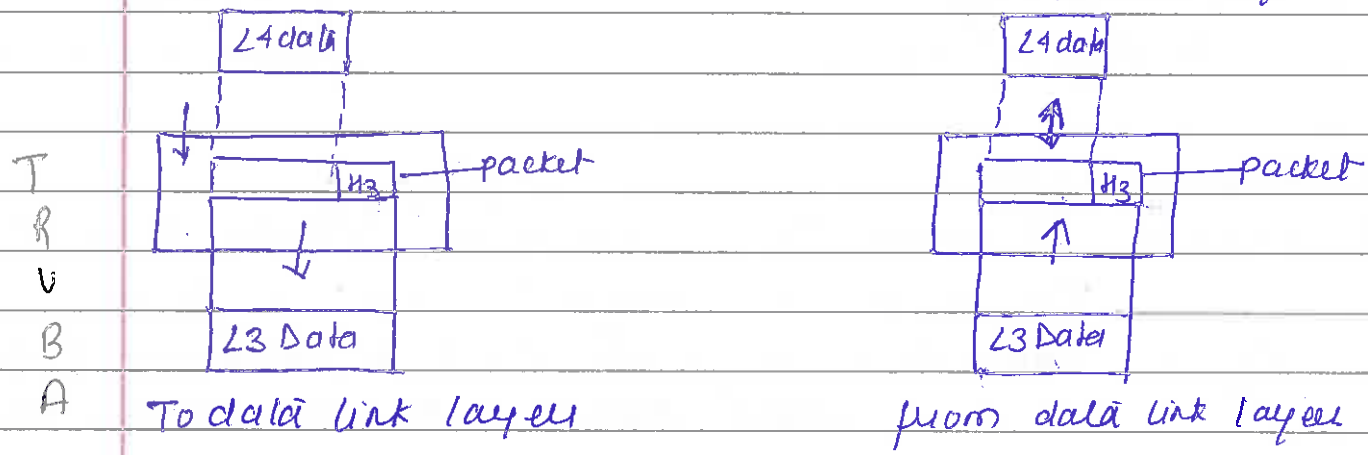
Responsibilities —

1. Framing - It (DLL) divides the stream of bit received from the n/w layer into manageable data units called frames.
2. Physical addressing - If frames are to be distributed to different systems on the n/w, the DLL adds a header to the frame to define the physical address of the sender and/or receiver of the frame.
3. Flow control - DLL imposes a flow control mechanism to prevent overwhelming the receiver.
4. Error control - It is normally achieved through a trailer added to the end of the frame.
5. Access control - When two or more devices are connected to the same link, DLL protocols are necessary to determine which device has control over the link at any given time.



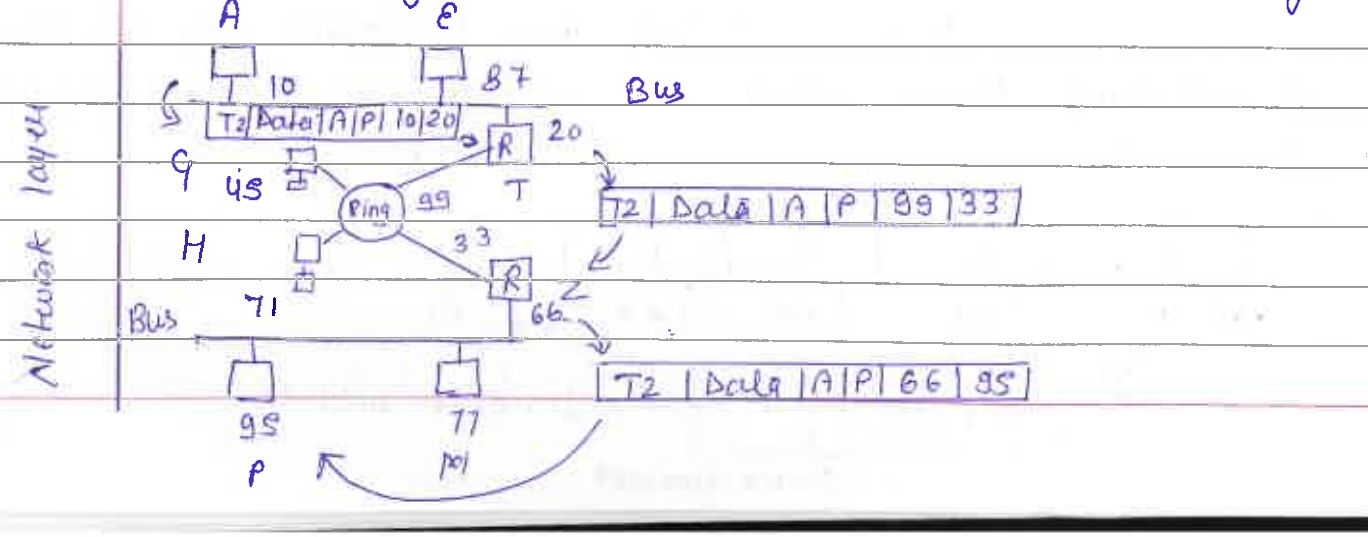
Network layer — It is responsible for the source-to-destination delivery of a packet possibly across multiple n/w (links). Whereas the data link layer oversees the delivery of the packet b/w two systems on the same n/w (links), the n/w layer ensures that each packet gets from its point of origin to its final destination.

Note — If two systems are connected to the same link, there is usually no need for a n/w layer.



Responsibilities —

1. Logical addressing — If a packet passes the n/w boundary, we need another addressing system to help distinguish the source & destination systems.
2. Routing — When independent n/w or links are connected together to create an internetwork or a large n/w.



Transport Layer:- It is responsible for source-to-destination delivery of the entire message. Whereas the network layer oversees end-to-end delivery of individual packet, it doesn't recognize b/w those packets.

A connection is a single logical path b/w the source and destination that is associated with all packets in a message
1. Connection Establishment
2. Data Transfer
3. Connection Release

Responsibility -

1. Service-point addressing - Computers often run several programs at the same time. For this reason, source-to-destination delivery means not only from one computer to the next but also a specific process (running prog^m) on one computer to a specific process (running prog^m) on the other. The transport layer header therefore must include a type of address called a service-point address or port address
   - N/w layer gets each packet to the correct computer
   - Transport layer gets the entire message to the correct process on that computer.

2. Segmentation and Reassembly - A message is divided into transmittable segment, each segment containing a sequence number. These sequence no. enables the transport layer to reassemble the message correctly upon arriving at the destination & to identify & replace packets that were lost in the transmission.

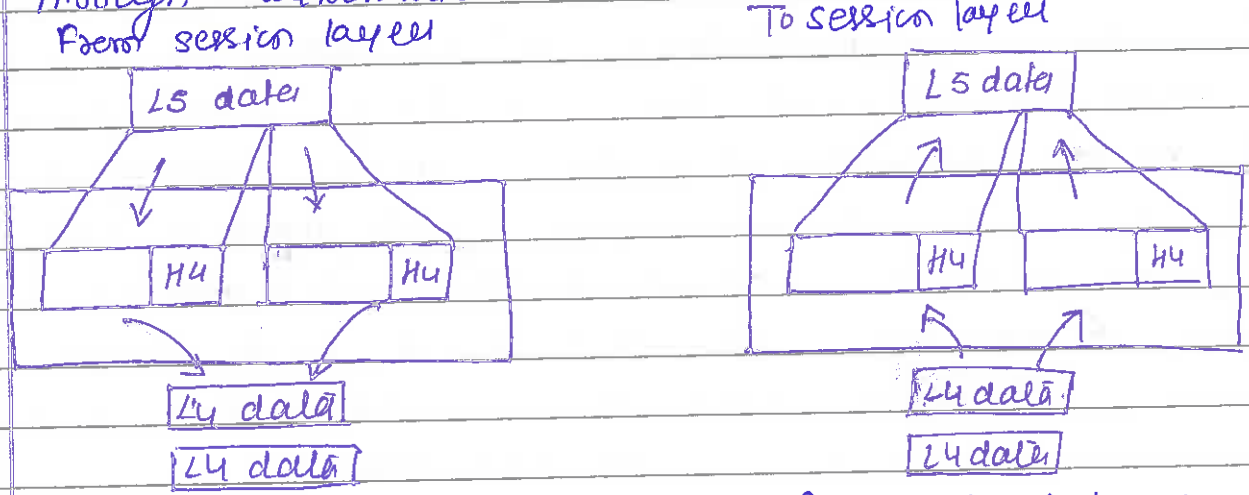
3. Connection control - Either connectionless or connection-oriented. Connection-less transport layer treat packet (each) as an independent packet.

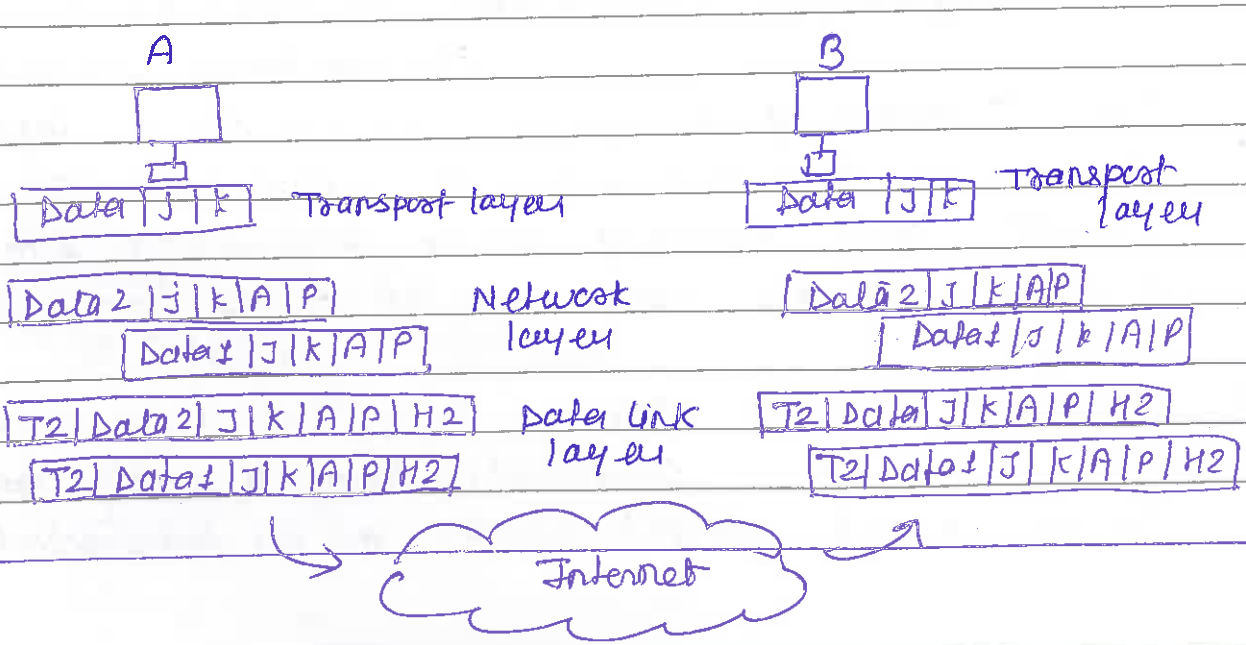
Connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets.

4. Flow control:- Like DLL, transport layer is responsible for flow control. It is performed end-to-end rather than across a single link.

5. Error control:- Error control at this layer is performed end-to-end rather than across a single link. (Sending transport layer make sure that my entire message arrives at the receiving transport layer without error (damage, loss or duplication)). It is usually achieved through retransmission.

TRUBA



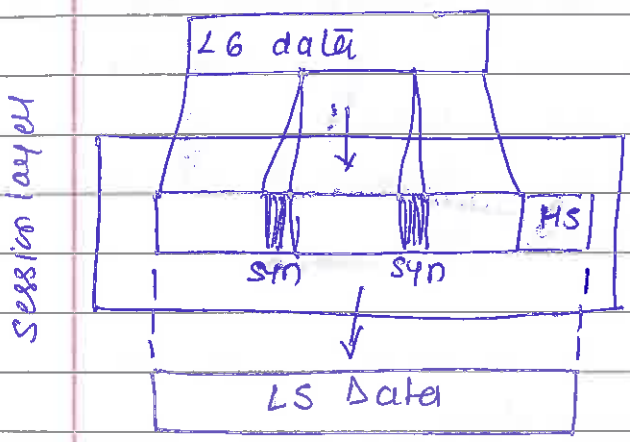


7. Session layer :— It is the n/w dialog controller. It establishes, maintains & synchronizes the interaction b/w communicating systems

Responsibilities —

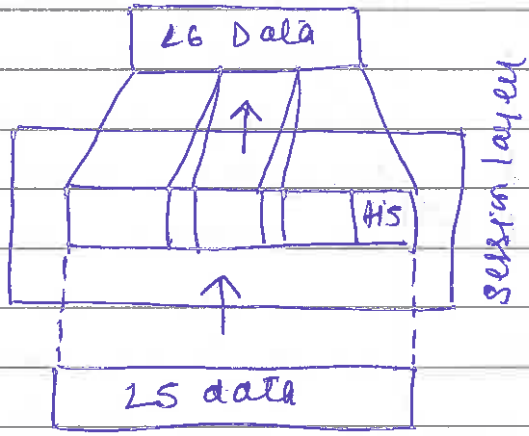
1. Dialog control - Session layer allows two systems to enter into a dialog. It allows the communication b/w processes to take place either in Half-duplex or full-duplex.
2. Synchronization - Session layer allows a process to add checkpoints into a stream of data.

From presentation layer



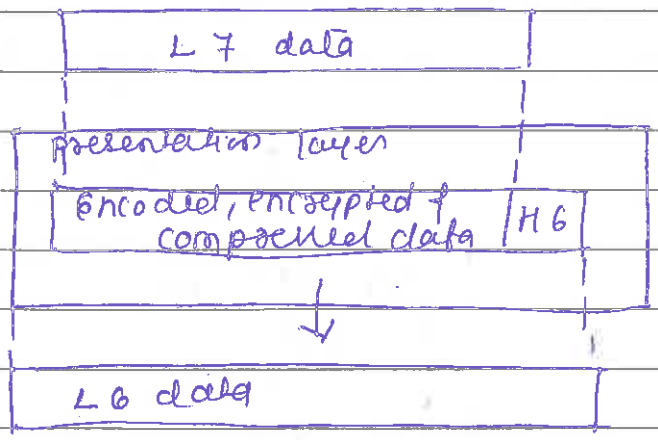
To Transport layer

To presentation layer

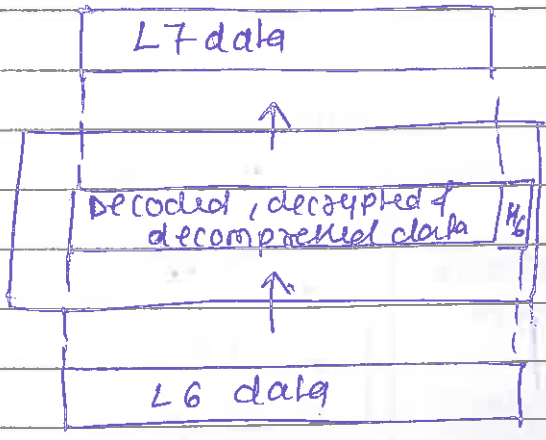


From Transport layer

6. Presentation layer :— It is concerned with the syntax & semantics of the information exchanged b/w two systems.



To session layer



From session layer.

Responsibilities —

1. Translation- The processes (running program) in two systems are usually exchanging in the form of character strings, numbers and so on. This layer is responsible for interoperability b/w these different encoding methods.

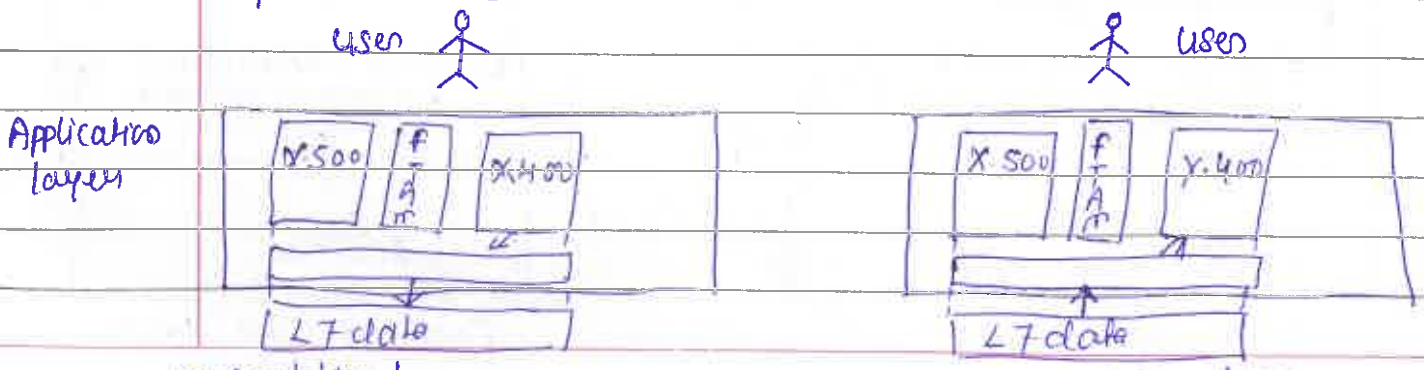
2. Encryption:- To carry sensitive information, a system must be able to assure privacy.

TRUBA

Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network.
Decryption reverses the original process to transform the message back to its original form.

3. Compression- Data compression reduces the number of bits to be transmitted.

7. Application layer:- enables the user, whether human or software, to access the network.
It provides user interfaces and support for services such as electronic-mail, remote file access & transfer, shared database management and other types of distributed information services.



1. Network Virtual Terminal - It is a software version of a physical terminal and allows a user to log on a remote host.

2. File transfer, access & management (FTAM) - This application allows a user to access files in a remote computer, to retrieve files from a remote computer; and to manage or control files in a remote computer.

3. Mail Services - provides the basis for e-mail forwarding & storage.

4. Directory Services - provides distributed database sources & access for global information about various objects & services.

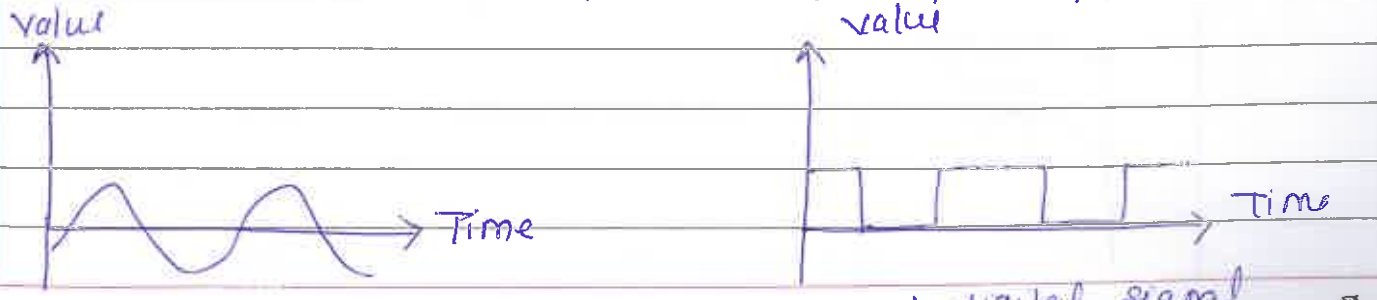
TRUBA

Signals :-

To be transmitted, information must be transformed into electromagnetic signals. (Informations can be in the form of data, voice, pictures & so on.)

Analog - refers to continous (a set of specific points of data & all possible points b/w). eg. Human Voice

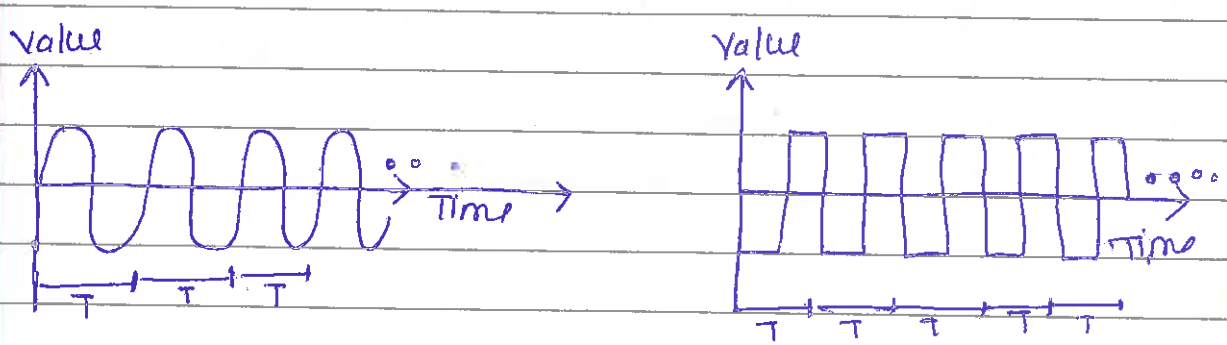
Digital - refers to discrete (a set of specific points of data with no other point in b/w). eg. Computer's data



a) Analog signal

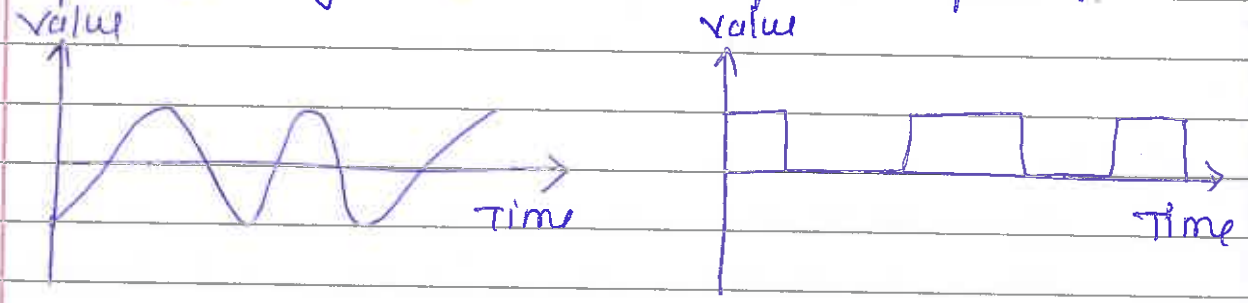
b) digital signal

Periodic Signals:- It consists of a continously repeated pattern. The period of a signal (T) is expressed in seconds. The completion of one full pattern is called a cycle.



a. Analog b. Digital

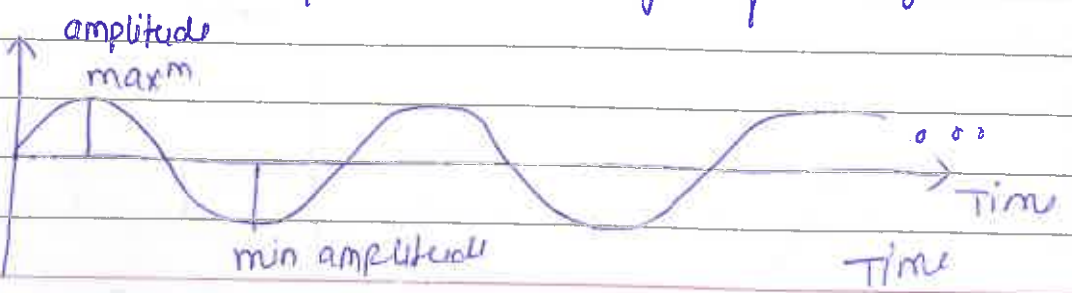
Aperiodic Signals - has no repetitive pattern



a. Analog Signal b. Digital signal

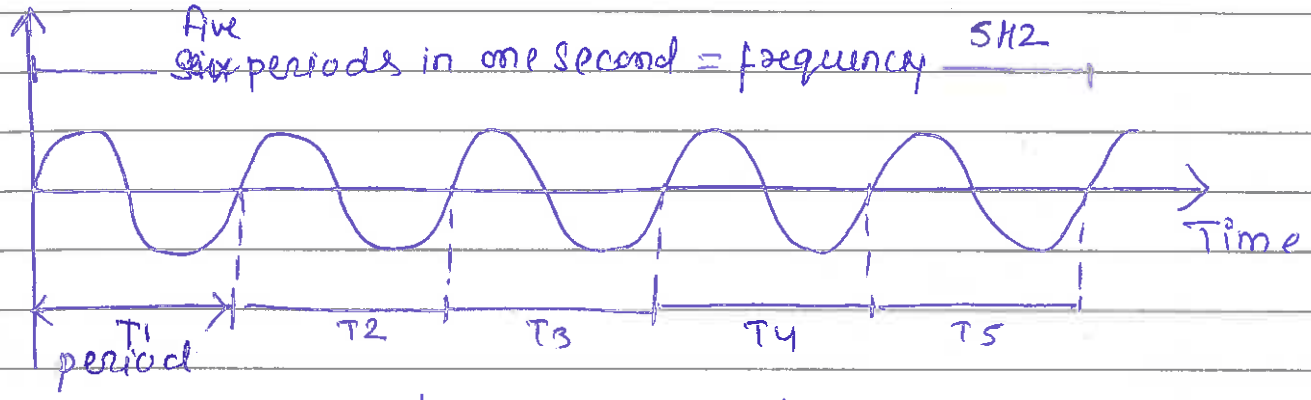
It can be decomposed into an infinite number of periodic Signals. "A sinewave is the simplest periodic signal"

Amplitude :- refers to the height of the signal.



Period :- refers to the amount of time, in seconds, a signal needs to complete one cycle.

Frequency :- refers to the number of periods in one second.

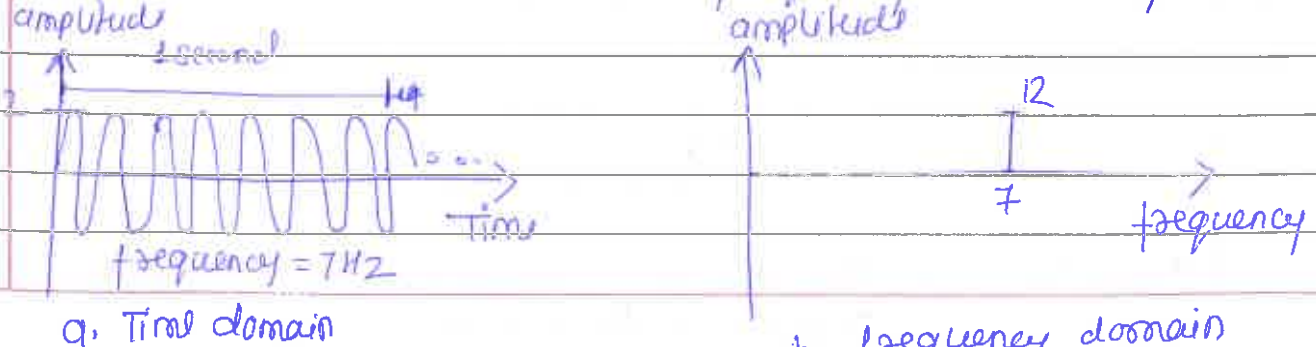


$$\text{period} = \frac{1}{\text{frequency}} \Rightarrow \frac{1}{5\ \text{Hz}}\ \text{sec}$$

Units of Period		units of frequency	
Unit	Equivalent	Unit	Equivalent
seconds (sec)	1 S	Hertz (Hz)	1 Hz
Milliseconds	10^{-3} S	kilo Hz	10^{3} Hz
Micro sec.	10^{-6} S	Mega Hz	10^{6} Hz
Nano sec.	10^{-9} S	Giga Hz	10^{9} Hz
Pico sec.	10^{-12} S	Tera Hz	10^{12} Hz

Time and frequency Domains :-

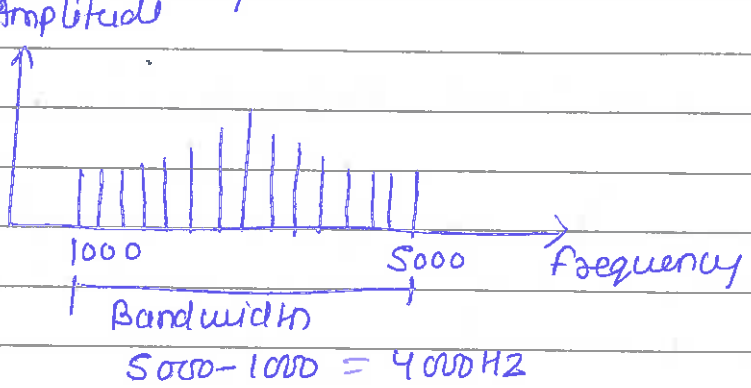
The time-domain plot shows changes in signal amplitude with respect to time, whereas to show the relationship b/w amplitude and frequency, we can use what is called a frequency-domain plot.



a. Time domain

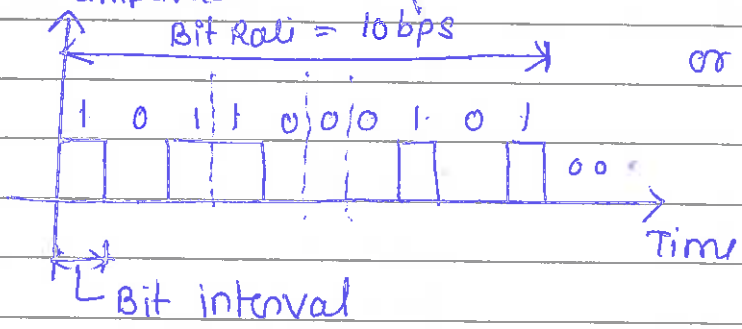
b. frequency domain

Bandwidth :- of a signal is the width of the frequency spectrum. In other words, bandwidth refers to the range of component frequencies, and frequency spectrum refers to the elements within that range.



Bandwidth = $frequency_{High} - frequency_{low}$

Digital Signals :-



Bit Interval :- is the time required to send one single bit

Bit Rate - is the number of bit intervals per second. This means that the bit rate is the number of bits sent in one second, usually expressed in bits per second (bps)

$$\text{Bit Rate} = 1/\text{Bit Interval}$$

Compiled By - Ms. Nandini Sharma
(Assistant Professor)

Transmission Media :- Signals travel from transmitter to receiver via a path. This path, called the medium, can be guided or unguided. A guided medium is contained within physical boundaries, while an unguided medium is boundless.

Transmission Media

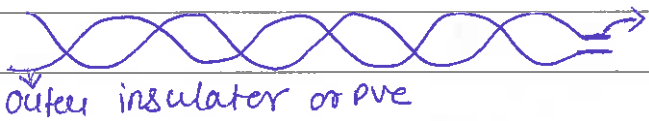
Guided | Unguided

Guided Media :- Guided media, which are those that provide a conduit from one device to another, include twisted pair cable, coaxial cable & fiber-optic cable.

Twisted-pair cable consists of two insulated copper wires twisted together. Twisting allows each wire to have approximately the same noise environment.

o Unshielded Twisted-pair (UTP) cable :- It is the most common type of telecommunication medium in use today. Its frequency range is suitable for transmitting both data & voice.

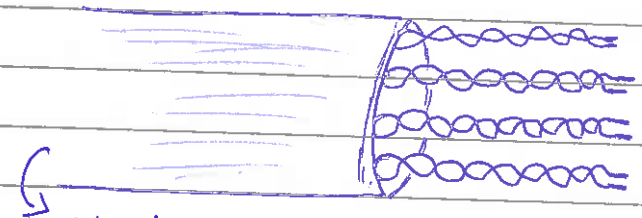
Frequency range from 100 Hz to 5 MHz.



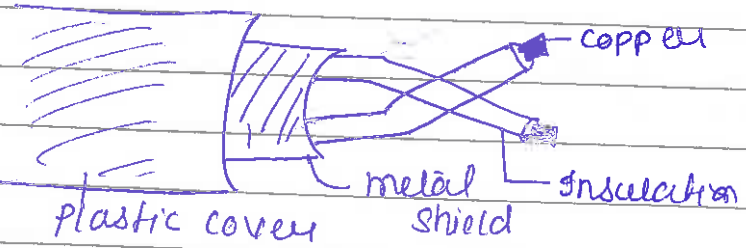
Twisted pair cable

Electronics Industries Association (EIA) has developed standards to grade UTP cables by quality. Categories are determined by cable quality, with 1 as the lowest and 5 as the highest.

- Category 1 :- The basic twisted-pair cabling used in telephone systems. This level of quality is fine for voice but inadequate for all but low-speed data communication.
- Category 2 :- The next higher grade, suitable for voice & for data transmission of upto 4 mbps.
- Category 3 :- Required to have at least three twists per foot & can be used for data transmission of upto 10 Mbps.
- Category 4 :- Must also have at least three twist per foot as well as other conditions to bring the possible transmission rate to 16 Mbps.
- Category 5 :- Used for data transmission upto 100 Mbps.



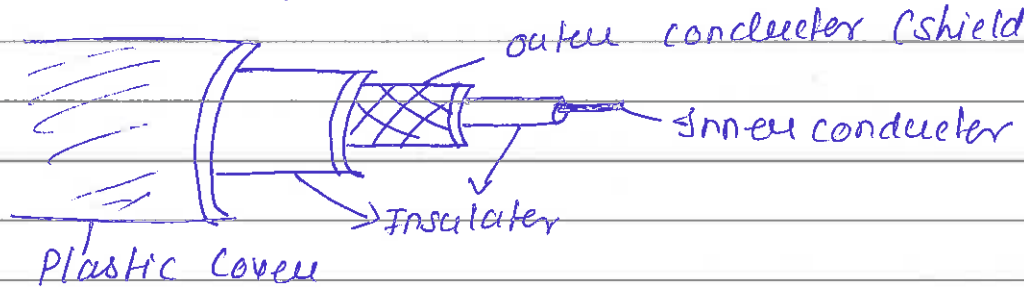
Shielded Twisted-pair (STP) :- cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors. The metal casing prevents the penetration of electromagnetic noise.



STP has the same quality considerations & uses the same connectors as UTP, but the shield must be connected to a ground.

Coaxial Cable:- or Coax carries signals of higher frequency ranges than twisted-pair cable. Instead of two wires, coax has a central core conductor of solid or stranded wire enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid or a combination of the two (also usually copper). The outer metallic wrapping serves both as a shield against noise & as the second conductor, which completes the circuit.

Frequency Range 100 KHz to 500 MHz



Coaxial cable.

Coaxial cable standards:- Different coaxial cable designs are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness & type of the inner insulator, the construction of the shield, & the size & the type of the outer casing.

RG-8, RG-9, RG-11 → used in thick ethernet
RG-58, RG-59 → used in thin ethernet
RG-59 → Used for TV

BNC → Beyonet Network connecter (Two types)
1. BNC-T connecters 2. BNC Terminaters

Fiber-optic cables carry data signals in the form of light. The signal is propagated along the inner core by Reflection. It composed of a glass or plastic inner core surrounded by cladding, all encased in an outside jacket.

Transmission is becoming increasingly popular due to its noise resistance, low attenuation & high bandwidth capabilities.

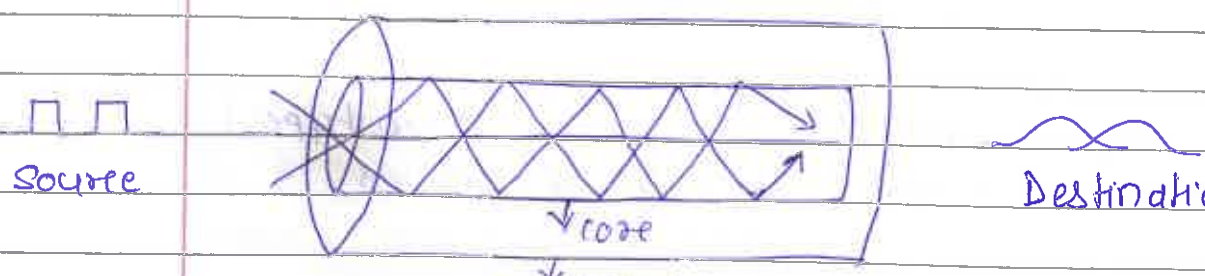
T
R
U
B
A

→ Mode — Single mode
Mode — Multimode — Step Index
Multimode — Graded-Index

Propagation Modes:-

1. Multimode:- multiple beams from a light source move through the core in different paths. How these beams move within cable depends on the structure of the core.

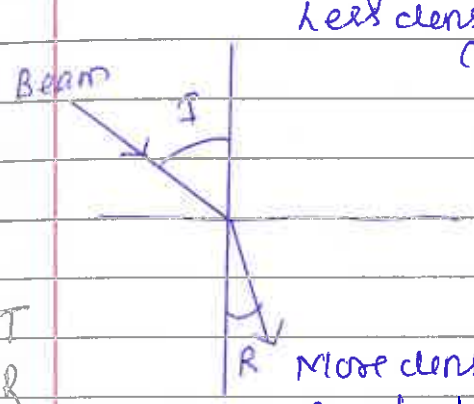
In multimode step-index fiber, the density of the core remains constant from the center of the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core & the cladding. At the interface, there is an abrupt change to a lower density that alters the angle of the beam's motion. The term step-index refers to the suddenness of this change.

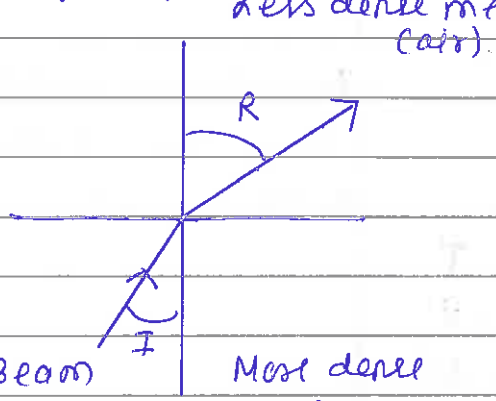


Multimode step-Index fiber

If a ray of light travelling through one substance suddenly enters another (more/less dense) substance, its speed changes abruptly, causing the ray to change direction. This change is refraction.

When light travels into a more dense medium, the angle of incidence is greater than the angle of refraction & vice versa





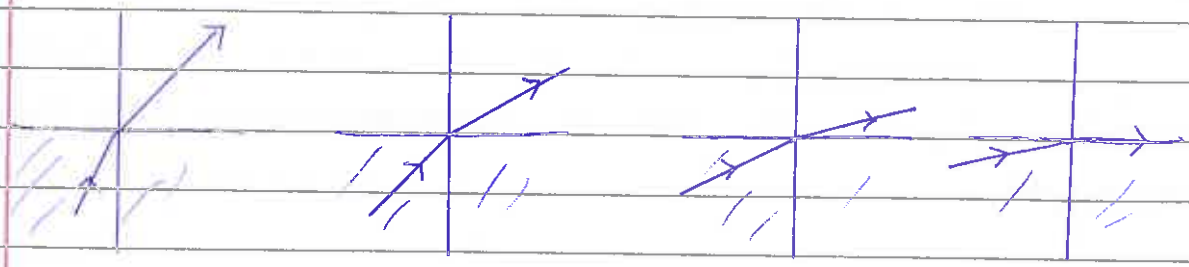
a. From less dense to more dense medium

b. From more less to less dense medium

Refraction

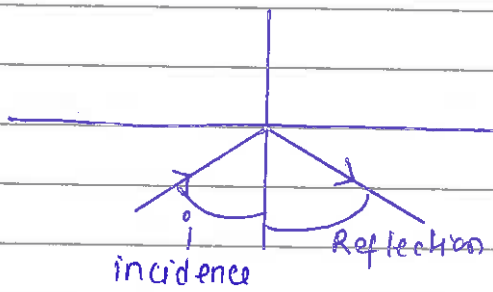
Critical Angle:- Once again we have a beam of light moving from a more dense into a less dense medium. In this example, however, we gradually increase the angle of incidence measured from the vertical. As the angle of incidence increases, so does the angle of refraction. It, too, moves away from the vertical & closer & closer to the horizontal.

At some point, in this process, the change in the incident angle results in a refracted angle of 90°, with the refracted beam now lying along the horizontal. The incident angle at this point is k/as the critical angle.



(a) (b) (c) (d)

Reflection:- When the angle of incidence becomes greater than the ~~refractive~~ critical angle, a new phenomenon occurs called ~~reflection~~.



Propagation Modes:- Contd....

Word index refers to the index of refraction.

A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core & decreases gradually to its lowest at the edge.

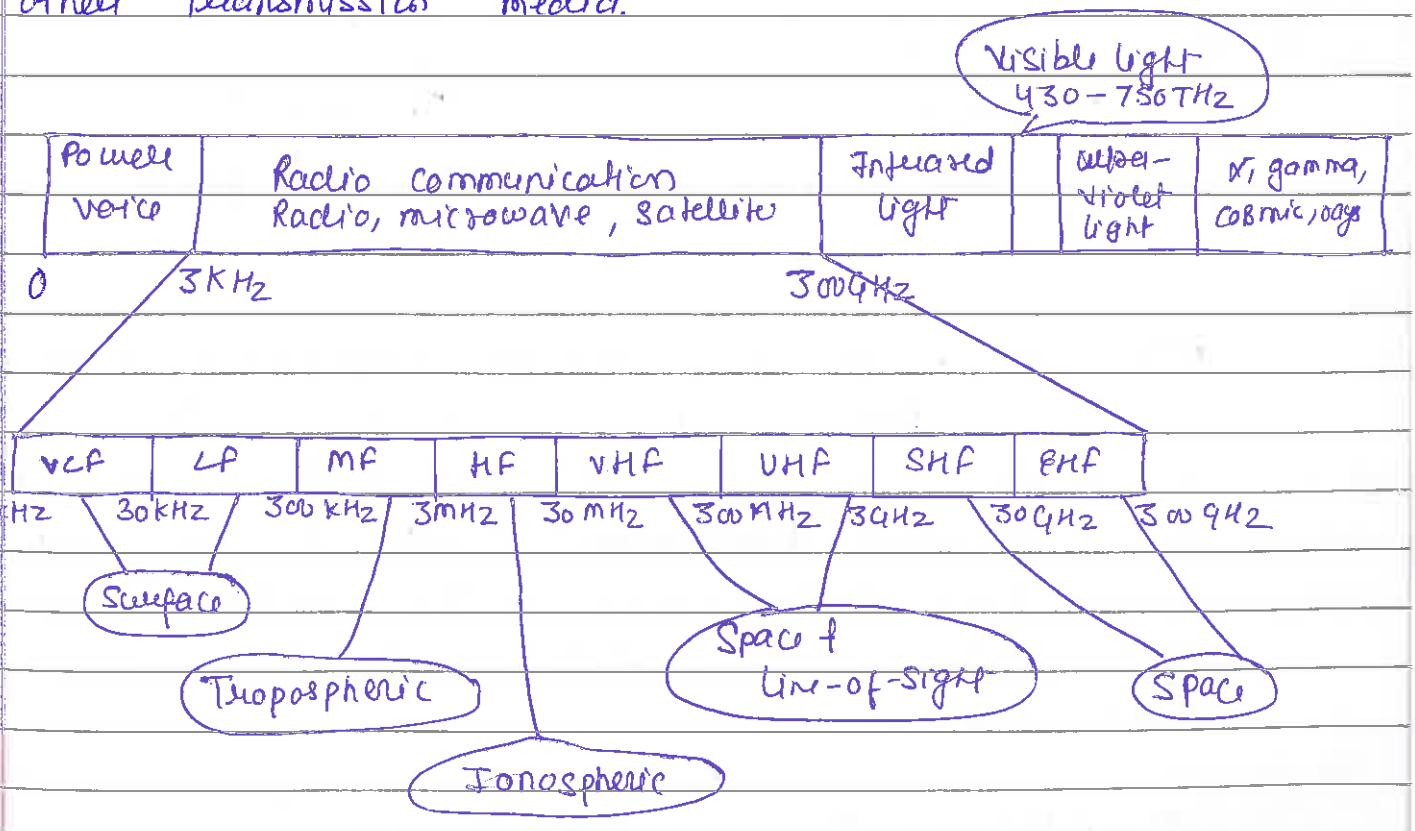
2. Single Mode:- It uses step-index fiber & a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.

Advantages of optical fiber -
- Noise resistency
- Less Signal attenuation
- Higher Bandwidth

Disadvantages of optical fiber -
- cost
- Installation / maintenance
- Fragility.

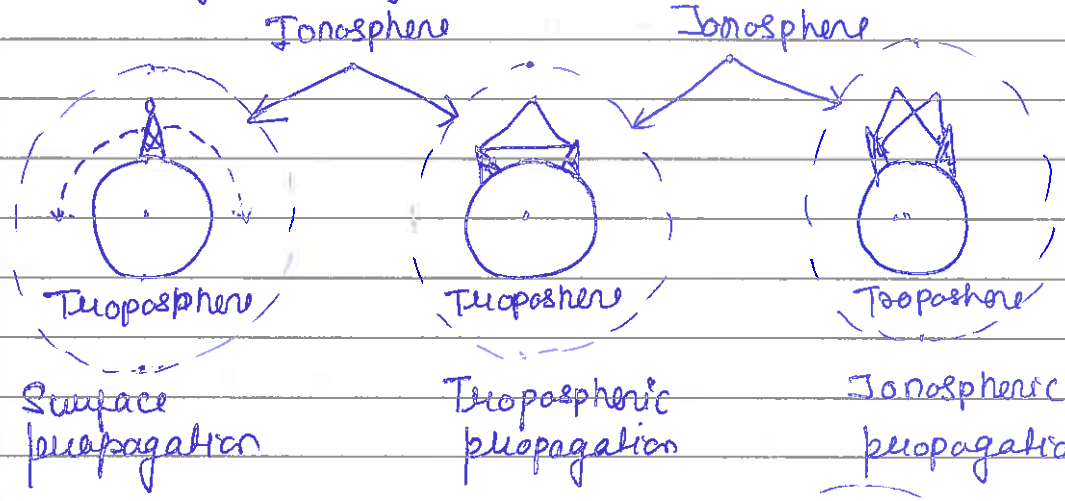
Unguided Media - unguided media or wireless communication, transport electromagnetic waves without using a physical conductor. Instead, signals are broadcast through air & thus are available to anyone who has a device capable of receiving them.

Electromagnetic Signals can travel through a vaccum, air or other transmission media.



VLF - Very Low Frequency
LF - Low frequency
MF - Middle frequency
HF - High frequency
VHF - Very high frequency
UHF - Ultra high frequency
SHF - Super high frequency
EHF - Extremely high frequency

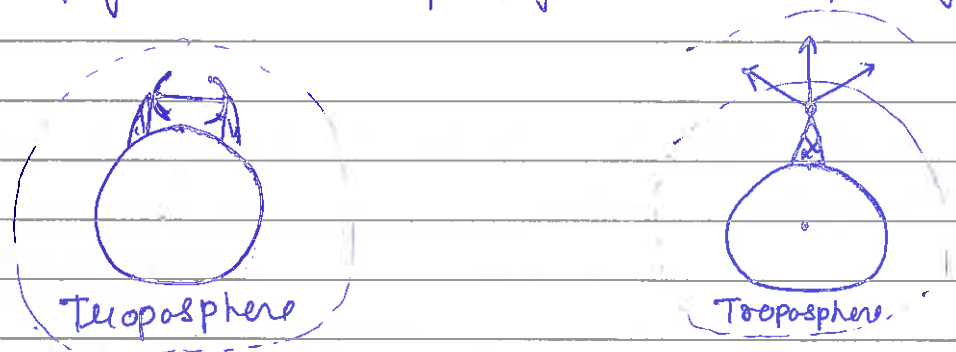
Types of propagation



Surface propagation

Tropospheric propagation

Ionospheric propagation



Line-of-Sight propagation

Space propagation

Microwaves - do not follow the curvature of the earth & therefore require line-of-sight transmission & reception equipment. One frequency is reserved for microwave transmission in one direction & the other for transmission in the other. (means that two frequency are necessary for two-way communication).

Compiled By - Miss. Nandini Sharma
(Assistant Professor)

Repeaters:— To increase the distance served by terrestrial microwave, a system of repeaters can be installed with each antenna.

Antennas — Two types of antennas are used for terrestrial microwave communications:— parabolic dish & horn.

Transmission Impairment:— Transmission are not perfect. The imperfections cause impairment in the signal sent through the medium. This means that the signal at the begining & end of the medium are not the same.

Impairment

- Attenuation
- Distortion
- Noise

Attenuation means loss of energy. When a signal, simple or complex, travels through a medium, it loses some of its energy so that it can overcome the resistance of the medium. That is why a wire carrying electrical signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

Decibel — To show that a signal has lost / gained strength, engineers use the concept of decibel. Decibel (dB) measures the relative strengths of two signals or a signal at two different points.

Note - that the dB is negative, if a signal is attenuated & positive if a signal is amplified.

$$dB = 10\log_{10}(P_2/P_1)$$

where P_1 & P_2 are the powers of a signal at points 1 & 2

Example 1

Imagine a signal travels through a transmission medium & its power is reduced to half. This means that $P_2 = (1/2)P_1$. In this case, the attenuation (loss of power) can be calculated as —

$$10\log_{10}(P_2/P_1) = 10\log_{10}(0.5\,P_1/P_1)$$
$$= -3\,dB.$$

TRUBA

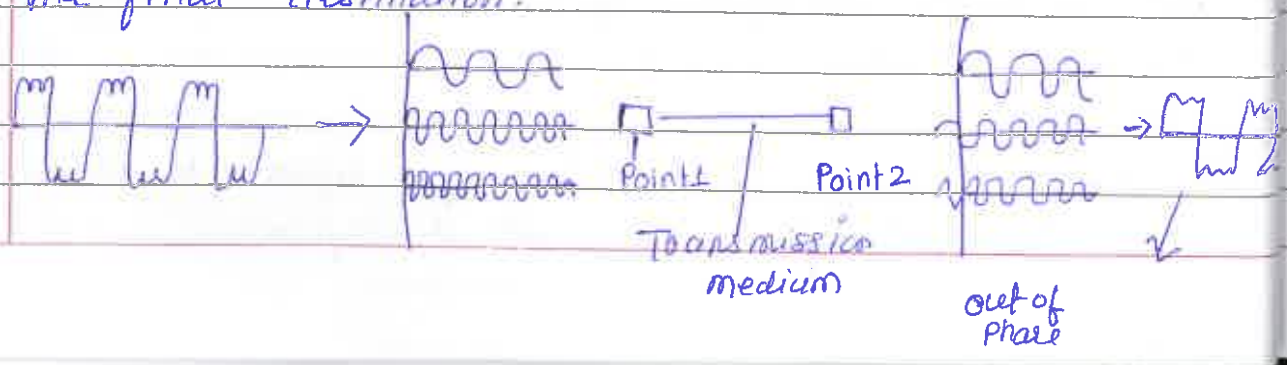
Example 2

Imagine a signal travels through an amplifier & its power is increased 10 times. This means that $P_2 = 10 \times P_1$. In this case the amplification can be calculated as —

$$10\log_{10}(P_2/P_1) = 10\log_{10}(10P_1/P_1)$$

$$= 10dB$$

Distortion:— It means that the signal changes its form or shape. Distortion occurs in a composite signal, made of different frequencies. Each signal component has its own propagation speed through a medium & therefore, its own delay in arriving at the final destination.



Noise — is another problem. Several types of noise such as thermal noise, induced noise, crosstalk, and impulse noise may corrupt the signal.

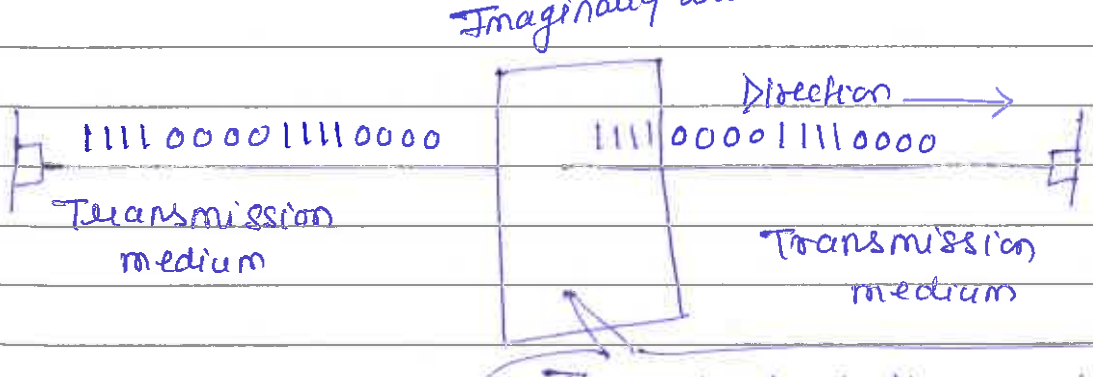
Thermal Noise is the random motion of electrons in a wire that creates an extra signal not originally sent by the transmitter.

Induced noise comes from sources such as motors and appliances.

Crosstalk is the effect of one wire on the other.

Performance — Transmission media are roads on which data travel. To measure the performance of transmission media, we can use three concepts — throughput, propagation speed & propagation time.

Throughput — is the measurement of how fast data can pass through a point. In other words, if we consider any point in the transmission medium as a wall through which bits pass, throughput is the number of bits that can pass this wall in one second.



Propagation Speed:- measures the distance a signal or a bit can travel through a medium in one second. The propagation speed of electromagnetic signals depends on the medium & the frequency of the signal.

Propagation Time:- It measures the time required for a signal to travel from one point of the transmission medium to another. The propagation time is calculated by dividing the distance by the propagation speed.

$$\text{Propagation time} = \frac{\text{Distance}}{\text{Propagation speed}}$$

T
R
U
B
A

Multiplexing:- is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

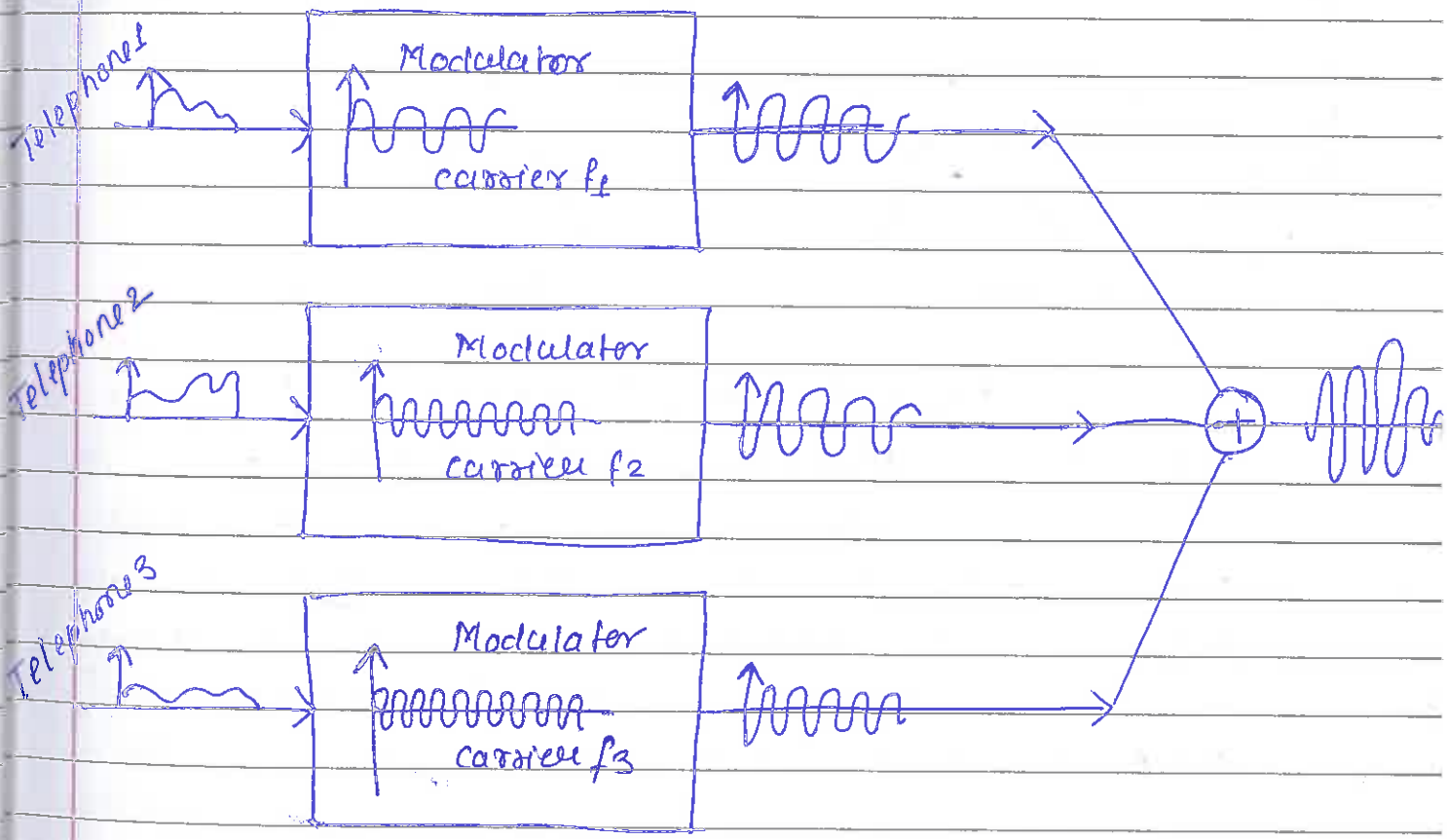
Many-to-one:- Multiplexer (MUX), which combines them into a ~~sig~~ single stream.

One-to-Many:- Demultiplexer (DEMUX), which separates the stream back into its component transmissions & direct them to their intended receiving devices.

- Path refers to the physical link
- channel refers to a portion of a path that carries a transmission between a given pair of devices.

Frequency-Division Multiplexing – It is an analog technique that can be applied when the bandwidth of a link is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulated different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link.

FDM is an analog process & we show it here using telephones as the input / output devices. Each telephone generates a signal of a similar frequency range. Inside the multiplexer, these similar signals are modulated onto different carrier frequencies. (Separate carrier frequencies used either AM/FM)



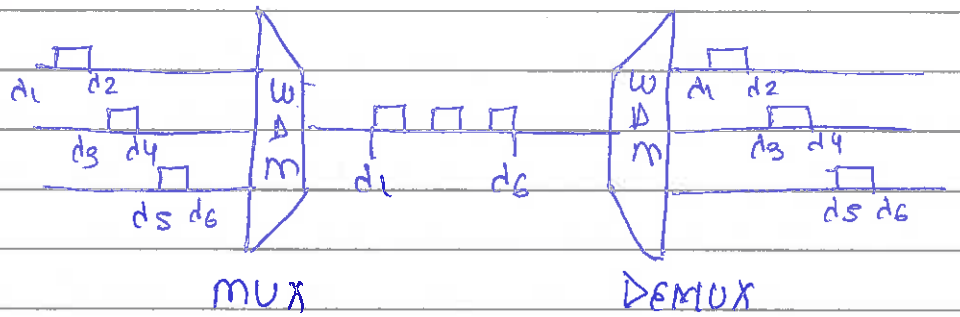
FDM multiplexing process, time domain

Compiled By –

Miss. Nandini Sharma
(Assistant Professor)

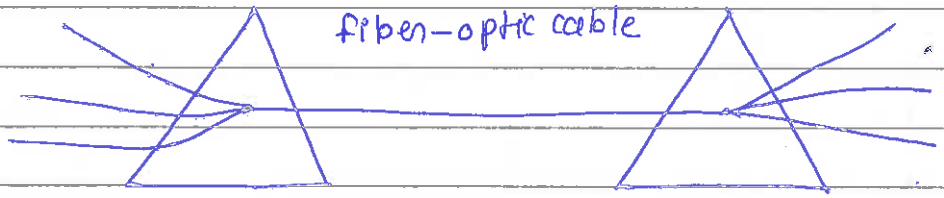
Wave-division multiplexing - It is conceptually the same as FDM, except that the multiplexing & demultiplexing involve light signals transmitted through fiber-optic channels.

Very narrow bands of light from different sources are combined to make a wider band of light.



MUX DEMUX

TRUBA



Multiplexer Demultiplexer

Prism in WDM mux & Demux

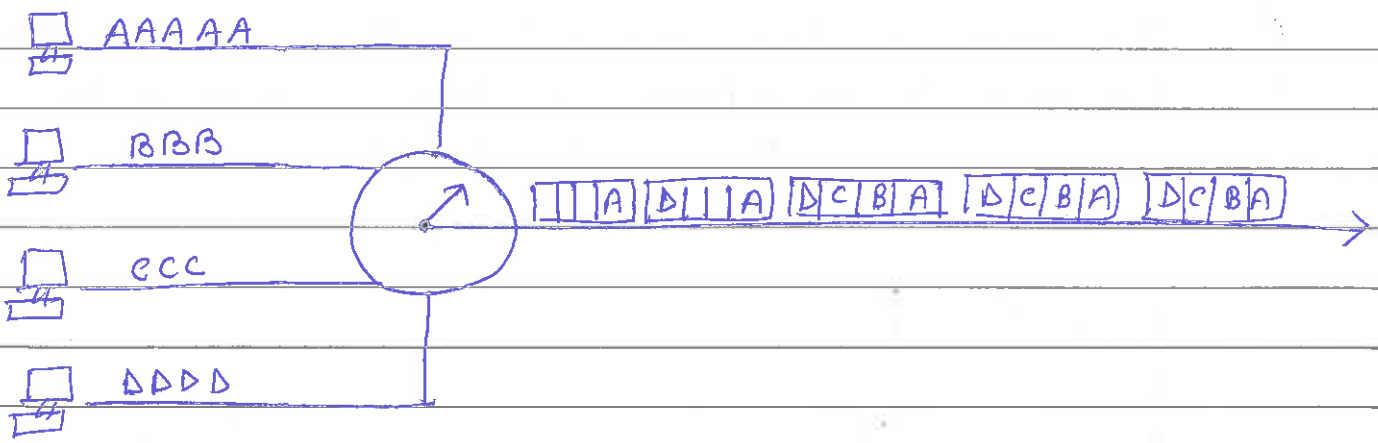
Time-Division Multiplexing :- It is a digital process that can be applied when the data rate capacity of the transmission medium is greater than the data rate required by the sending & receiving devices. In such a case, multiple transmissions can occupy a single link by subdividing them and inter-leaving the portions.

Note :- The same link is used as in FDM. However, the link is shared or sectioned by time rather than frequency.

TDM can be implemented in two ways —

Synchronous TDM — The term Synchronous has a different meaning from that used in other areas of telecommunications. Here Synchronous means that the multiplexer allocates exactly the same time slot to each device at all times, whether or not a device has anything to transmit.

Frames — Time slots are grouped into frames. A frame consists of one complete cycle of time slots, including one/more slots dedicated to each sending device.
In a system with n input lines, each frame has atleast n slots, with each slot allocated to carrying data from a specific input line.



Interleaving — The switch moves from device to device at a constant rate in a fixed order. This process is called interleaving.

Bit stuffing — In bit stuffing, the multiplexer adds extra bits to a device's source stream to force the speed relationship among the various devices into integer multiples of the other devices.

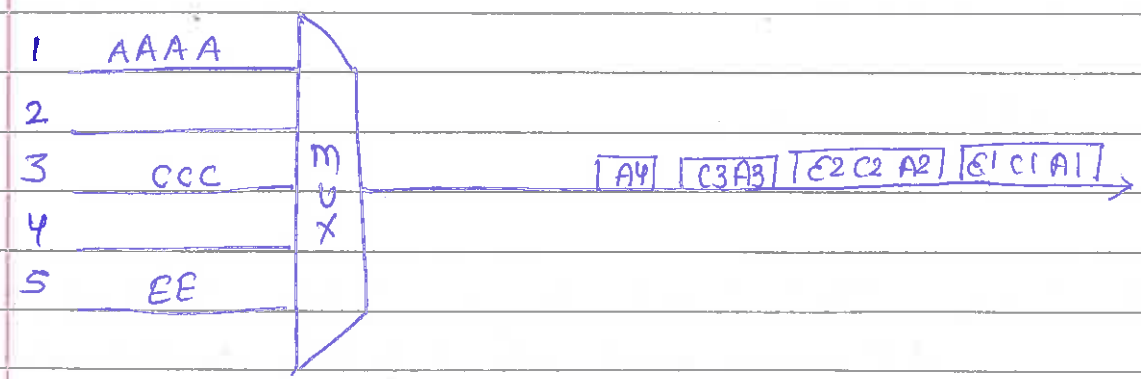
For example:- If we have one device with a bit rate of 2.75 times that of the other devices, we can add enough bits to raise the rate to 3 times that of the others. The extra bits are then discarded by the demultiplexer.

Asynchronous TDM:- Synchronous TDM doesn't guarantee that the full capacity of a link is used. For example,

Imagine that we have multiplexed the output of 20 identical computers onto a single line. Using Synchronous TDM, the speed of that line must be at least 20 times the speed of each input line. But what if only 10 computers are in use at a time? Half of the capacity of the line is wasted.

TRUBA

Asynchronous time-division multiplexing or statistical time-division multiplexing, is designed to avoid this type of waste. Here it means flexible.



only three lines sending data

Asynchronous of TDM frames

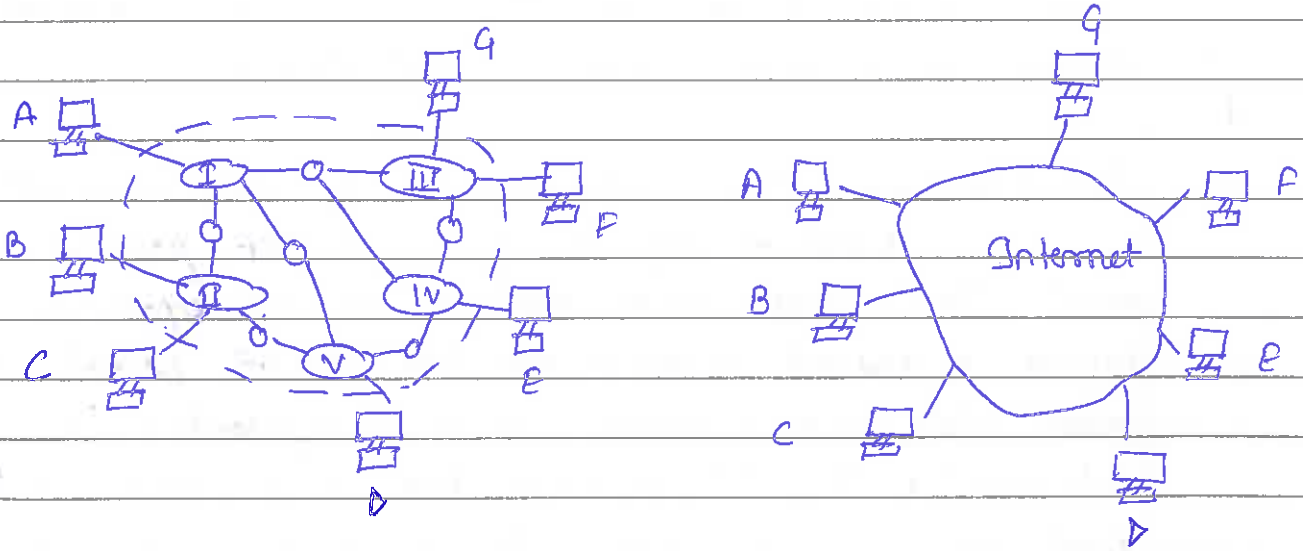
Compiled By:-

Miss. Nandini Sharma
(Asst. prof.)

TCP/IP protocol suite :- Transmission control protocol/ Internetworking protocol (TCP/IP) is a set of protocols, or a protocol suite, that defines how all transmissions are exchanged across the Internet.

In 1969, a project was funded by the Advanced Research Project Agency (ARPA), an arm of the U.S. department of defense. ARPA established a packet-switching network of computers linked by point-to-point leased lines called ARPANET that provided a basis for early research into networking. The conventions developed by ARPA to specify how individual computers could communicate across that network became TCP/IP.

TCP/IP was developed before the OSI model.



a. An actual internet b. An internet seen by TCP/IP

An internet under TCP/IP operates like a single network connecting many computers of any size & type. Internally, an internet is an inter-connection of independent physical n/ws linked together by internetworking devices. In figure, shows the topology of a possible internet.

TCP/IP protocol is made of five layers :- physical, data link layer, network, transport & application.

- The application layer in TCP/IP can be equated with the combination of session, presentation and application layers of the OSI model.
- At the transport layer, TCP/IP defines two protocol TCP & UDP.
- At the network layer, the main protocol defined by TCP/IP is Internetworking protocol (IP), although there are some other protocols that support data movement in this layer.
- At the physical and Data link layers, TCP/IP doesn't define any specific protocol. It supports all of the standard & proprietary protocols.

TRUBA

A network in a TCP/IP internetwork can be a local area network (LAN), a metropolitan area network (MAN) or a wide area network (WAN).

Encapsulation :- The encapsulation of data unit at different layers of the TCP/IP protocol suite. The data unit created at the application layer is called a message. TCP or UDP creates a data unit that is called either a segment / user datagram. The IP layer in turn will creat a data unit called a datagram. The movement of the data-gram across the internet is the responsibility of the TCP/IP.

However, to be able to move physically from one n/w to another, the datagram must be encapsulated in a frame in the data link layer of the underlying n/w & finally transmitted as signals along the transmission media.

Network Layer :- At the network layer or more accurately, the internetwork layer. TCP/IP, supports the internetwork protocal (IP). It contain ARP, RARP, ICMP, IGMP.

Internetwork Protocal :- It is an unreliable and connectionless datagram protocal, - a best-effort delivery service. The term best-effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

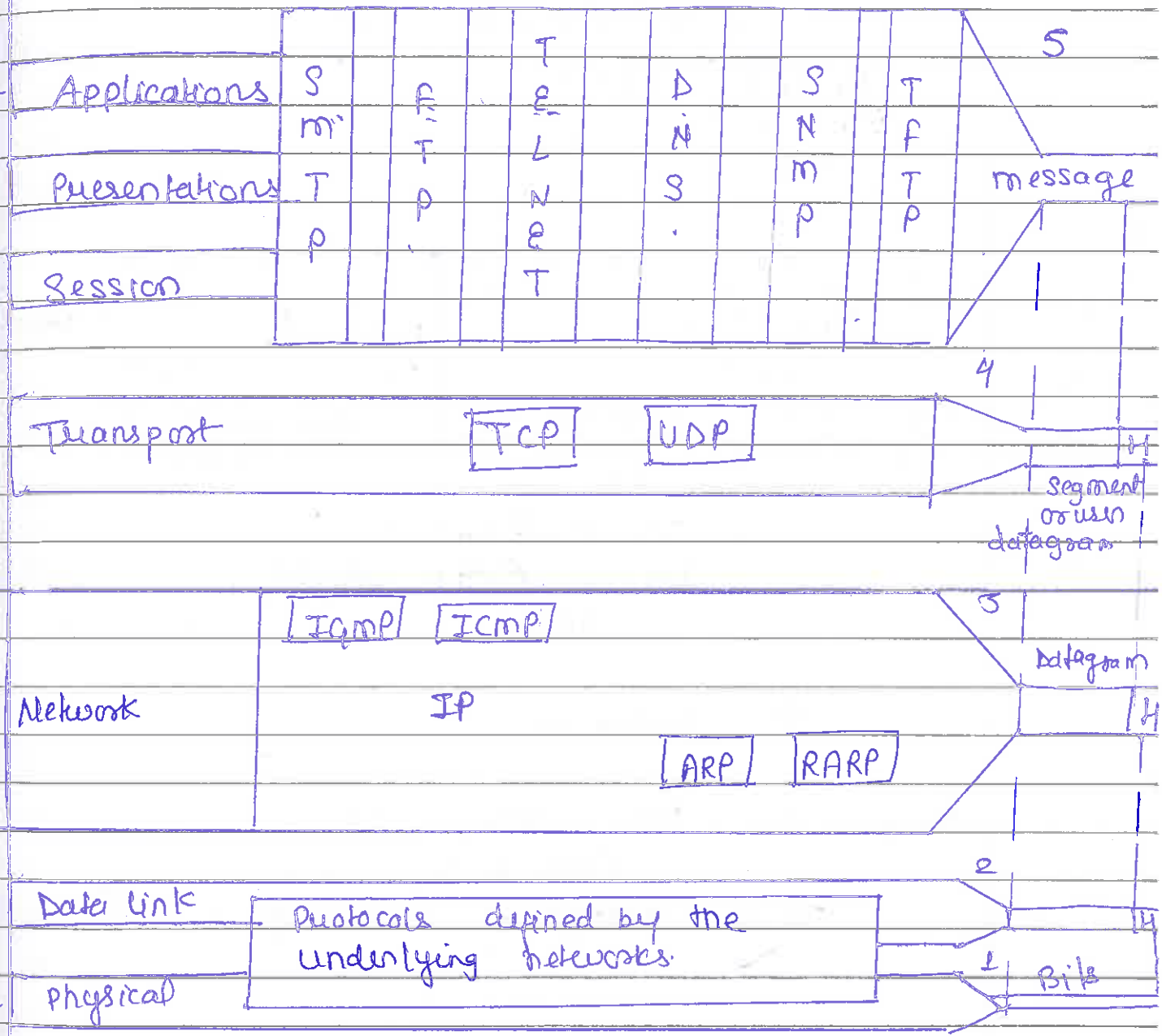
If reliability is important, IP must be paired with a reliable protocal such as TCP.

Example - Post office

The post office does its best to deliver the mail but doesn't always succeed. If an unregistered letter is lost, it is up to the sender / would be recipient to discover the loss & rectify the problem. The post office itself doesn't keep track of every letter & can't notify a sender of loss/damage. Stamped postcard included in a letter mailed through the post office. When the letter is delivered, the receiver mails the postcard back to the sender to indicate success. If the sender never receives the postcard, he/she assumes the letter was lost & sends out another copy.

IP transports data in packets called datagrams, each of which is transported separately. Datagrams may travel along different routes & may arrive out of sequence / duplicated.

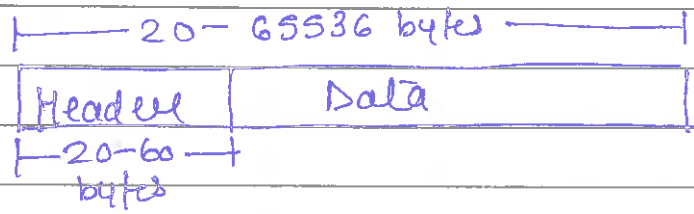
Note :- IP does not keep track of the routes & has no facility for reordering datagrams once they arrive. B/c it is connectionless service, IP does not create virtual circuit for delivery.



TCP/IP and OSI model

Compiled by — Miss. Nandini Sharma
(Assistant Professor)
Truba College of Sc. & Tech., Bhopal

IP datagram :-



Ver 4bits	HLEN 4bits	Service type 8 bits	Total length 16 bits
Identification (16 bits)		Flags 3 bits	Fragmentation offset 13 bits
Time to live 8 bits	protocol 8 bits		Header Checksum 16 bits
Source IP address			
Destination IP address			
option			

T
R
b.
B
A

IP Datagram

Compiled By - Miss. Nandini Sharma
(Assistant Professor)
Truba College of Sc. & Tech., Bhopal

Datagram :— Packets in the IP layer are called data-grams. A datagram is a variable-length packet (upto 65,536 bytes) consisting of two parts:— Header & data.

Version — The first field defines the version number of the IP. The current version is 4 (IPV4), with a binary value of 0100.

HLEN (Header length) — It defines the length of the header in multiples of four bytes. The four bits can represent a number 0 and 15, which, when multiplied by 4, gives a maximum 60 bytes.

Service type — defines how the datagram should be handled.

Total length — defines total length of the IP datagram. It is a two-byte field (16 bits) & can define upto 65536 bytes

Identification — used in fragmentation. A datagram, when passing through different networks, may be divided into fragments to match the networks, may be of frame size. Each fragment is identified with a sequence number in this field.

Flags — The bits in the flags field deal the fragmentation. (a datagram can be the first, middle or last)

Fragmentation offset — It is a pointer that shows the offset of the data in the original datagram

Time to live — the number of hops a datagram can travel before it is discarded.

Protocal – defines which upper-layer protocal data are encapsulated in the datagram

Header checksum – This is a 16-bit field used to check the integrity of the header, not the rest of the packet.

Source address :– identifies the original source of the datagram. (32 bit) -> internet address)

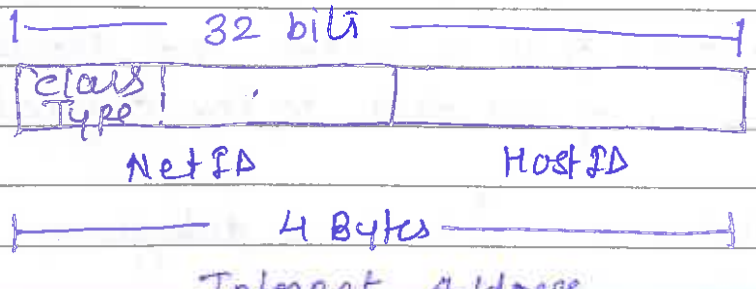
Destination address :– 32-bit internet address. It identifies the final destination.

T
R
U
B
A

Options – It gives more funtionality to the IP datagram. It can carry fields that control routing, timing management and alignment.

Addressing :– In addition to the physical address (contained on NICs) that identify individual devices, the internet requires an additional addressing convention :– an address that identifies the connection of a host to its network.

Each internet address consit of four bytes or 32 bits, defining three fields :– class, netid, Hostid



classes :- There are currently five different field-length patterns in use, each defining a class of address. The different classes are designed to cover the needs of different types of organizations.

For example, class A addresses are numerically the lowest. They use only one byte to identify class type & netid, and leave three bytes available for hostid numbers.

This division means that class A networks can accommodate far more hosts than can class B or class C n/ws, which provide two- and one-byte hostid fields, resp.

class D is reserved for multicast address.

Multicasting allows copies of a datagram to be passed to a select group of hosts rather than to an individual host. It is similar to broadcasting, but where broadcasting requires that a packet be passed to all possible destinatn, multicasting allows transmission to a selected subset.

class E is are reserved for future use.

byte 1	byte 2	byte 3	byte 4	
0 Net ID	Host ID	Host ID	Host Id	class A
10 Netid	Netid	Hostid	Hostid	class B
110 Netid	Netid	Netid	Hostid	class C
1110	Multicast	Address		class D
1111	Reserved For Future use			class E

|—— 32 bits ——|

IP address in decimal notations -

128. 11. 3. 31

10000000. 00001011 00000011 00011111

TRUBA

IP address in Binary notations -

128	64	32	16	8	4	2	1	
1	0	0	0	0	0	0	0	→ 128
0	0	0	0	1	0	1	1	→ 11
0	0	0	0	0	0	1	1	→ 3
0	0	0	1	1	1	1	1	→ 32

Class Ranges of Internet -

		From	To
difference	class A	0.0.0.0 (netid, Hostid)	127.255.255.255 (netid, Hostid)
128	class B	128.0.0.0 (netid, Hostid)	191.255.255.255 (netid, Hostid)
64	class C	192.0.0.0 (netid, Hostid)	223.255.255.255 (netid, Hostid)
32	class D	224.0.0.0 (Group address)	239.255.255.255 (Group address)
16	class E	240.0.0.0 (Undefined)	255.255.255.255 (Undefined)

Note :- To remember class IP range, start from class A zero then add 128 → get class B

initial range then add 64 in class B → 128+64 → 192
get class C → starting range → 192+32 → 224
get class D range of starting → 224+16 → 240
get class E range of starting. (This is shortcut method to memorize the range of class from A to E)

For example :— find the class of each address -

a. 4.23.145.90 → class A
b. 227.34.78.7 → class D
c. 246.7.3.8 → class E
d. 129.6.8.4 → class B
e. 198.76.9.23 → class C

For example — find the class of each address

a. 10011101 10001111 11111100 11001111
└ class B → check by class field

b. 110,11101 10001111 1111101 00001111
└ class C → checked by class field

c. 01011101 00011111 00000001 11110101
└ class A → checked by class field

d 11111101 10001010 00001111 00111111
└ class E → checked by class field.

Note — To identify class of binary and notations in two way

1. — checked by class field.
2. — To convert from binary to decimal notations & then check class by range in decimal.

Subnetting :- An IP address is 32 bit long. One portion of the address indicates a network (netid) & the other portion indicates the host (or router) on the network (hostid). This means that there is a sense of hierarchy in IP addressing.

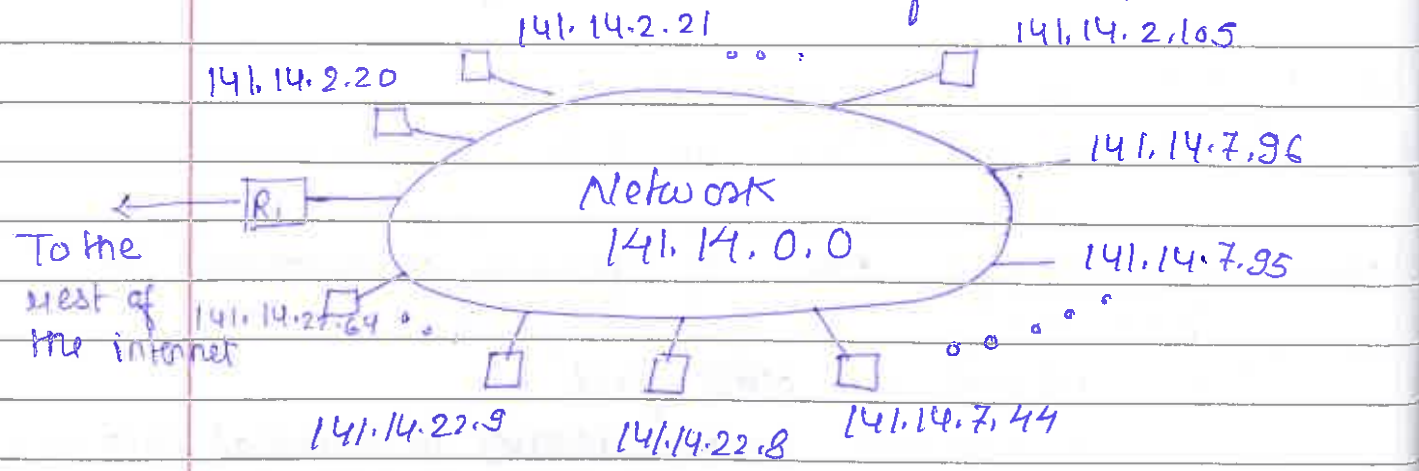
To reach a host on the Internet, we must first reach the network using the first portion of the address (netid). Then we must reach the host itself using the second portion (hostid).

In other words, classes A, B and C in IP addressing are designed with two levels of hierarchy.

However, in many cases, these two levels of hierarchy are not enough.

Example – Imagine an organizations with a class B address. The organization has two-level hierarchical addressing, but it cannot have more than one physical network.

A network with two levels of hierarchy (not subnetted)

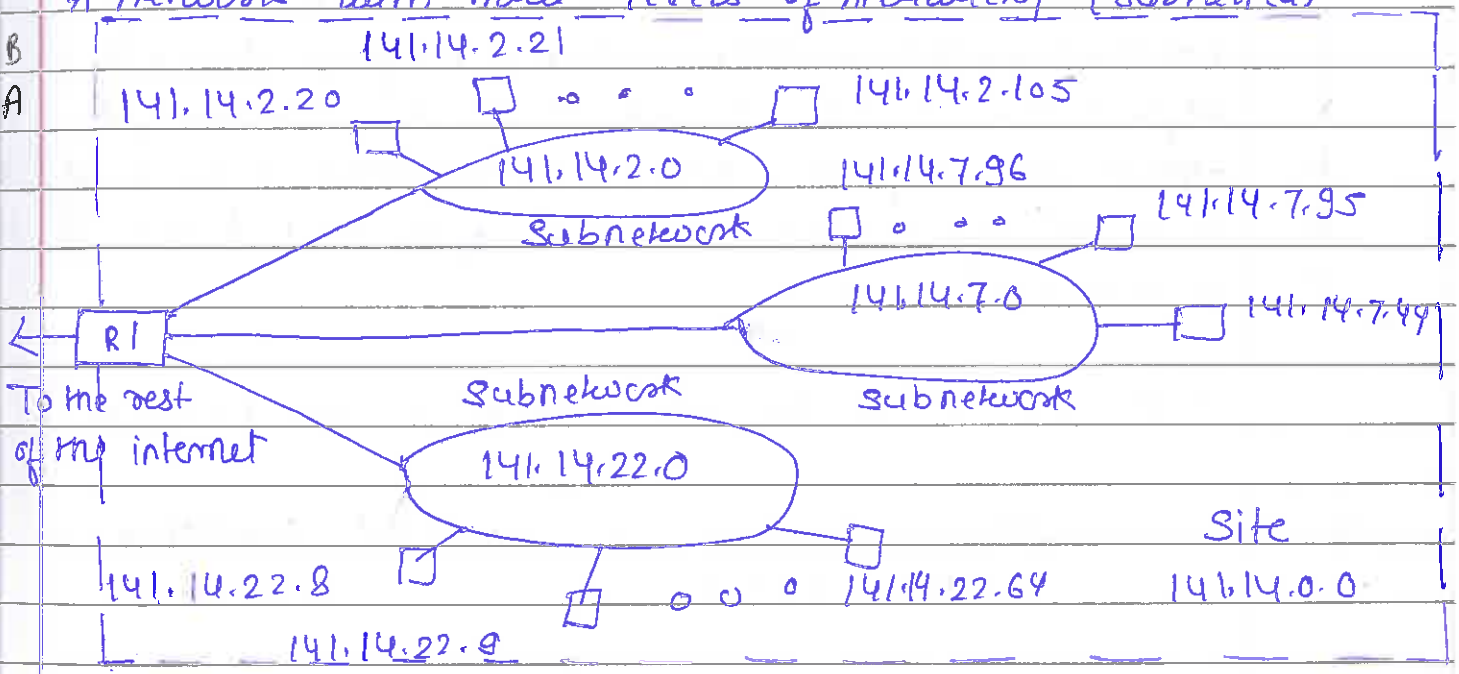


Compiled By – Ms. Nandini Sharma

With this scheme, the organization is limited to two levels of hierarchy. the hosts cannot be organized into groups, and all of the hosts are at same level. Organization has one network with many hosts.

One solution to this problem is Subnetting, the further division of a network into smaller networks called Subnetworks.

A network with three-levels of hierarchy (Subnetted)



In this example, the rest of the Internet is not aware that the network is divided into three physical subnetworks :- the three subnetworks still appear as a single network to the rest of the Internet. A packet destined for host 141.14.2.21 still reaches router R1, the destination address of the IP datagram is still a class B address where 141.14 defines the netid 2.21 defines the hostid.

However, when the packet arrives at router R1, the interpretation of the IP address changes. Router R1 knows that the

network 141.14 is physically divided into three subnetworks. It knows that the last two octets define two things :— Subnetid and hostid. Therefore, router R1 uses the first two octets (141.14) as the netid, the third octet (2) as the subnetid, and the fourth octet (21) as the hostid.

Three levels of Hierarchy :— Adding subnetworks creates an intermediate level of hierarchy in the IP addressing system. Now we have three levels — netid, subnetid & hostid. Netid is the first level, it defines the site. The second level is the subnetid, it defines the physical subnetwork. The hostid is the third level; it defines the connection of the host to the subnetwork.

TRUBA

Addresses in a network with & without subnetting

141.14.2.21 } without subnetting
NetID HostID

141.14.2.21 — hostid } with subnetting.
netid subnetid

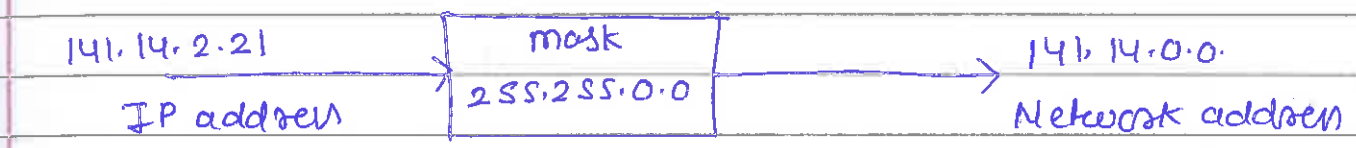
The routing of an IP datagram now involves three steps — delivery to the site, delivery to the subnetwork & delivery to the host.

Masking :— It is a process that extract the address of the physical network from an IP address. It can be done whether we have subnetting or not. If we have not subnetted the network, masking

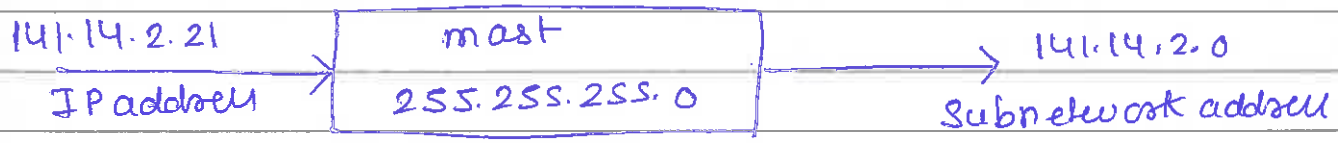
extract the network address from an IP address. If we have subnetted, masking extract the subnetwork address from an IP address.

Masks without subnetting :- To be compatible, routers use a mask even if there is no subnetting. The masks for networks that are not subnetted can be defined in below (example.)

Masking



a. Without subnetting



b. With subnetting

Example – Mask for unsubnetted networks

class	Mask	Address (example)	Network Address
A	255.0.0.0	15.32.56.7	15.32.0.0
B	255.255.0.0	135.67.13.9	135.67.13.0
C	255.255.255.0	201.34.12.72	201.34.12.64
D	N/A	N/A	N/A
E	N/A	N/A	N/A

Compiled By – Ms. Nandini Sharma

Masks with Subnetting :- When there is subnetting, the mask can vary, Some examples of masks used for subnetting.

Masks for Subnetted networks

Class	Mask	Address	N/w address
A	255.255.0.0	15.32.56.7	15.32.0.0
B	255.255.255.0	135.67.13.9	135.67.13.0
C	255.255.255.192	201.34.12.72	201.34.12.64
D	N/A	N/A	N/A
E	N/A	N/A	N/A

T
R
U
B
A

Finding the Subnetwork Address :-

To find the Subnetwork address, apply the mask to the IP address.

Boundary-level Masking :- If the masking is at the boundary level (the mask numbers are either 255 or 0), finding the subnetwork address is very easy. Follow two rules -

1. The bytes in the IP address that correspond to 255 in the mask will be repeated in the subnetwork address.
2. The bytes in the IP address that correspond to 0 in the mask will change to 0 in the subnetwork address.

Compiled By - Miss. Nandini Sharma
(Assistant Professor)

Example – How to get the Subnetwork address from an IP address:

IP address	45	23	21	8
Mask	255	255	0	0
Subnetwork address	45	23	0	0

Example – How to get the Subnetwork address from an IP address

IP address	173	23	21	8
Mask	255	255	255	0
Subnetwork address	173	23	21	0

Nonboundary-level masking – If the masking is not at the boundary level (the mask number are not just 255 or 0), finding the subnetwork address involves using the bit-wise AND operator, follow these rules –

1. The bytes in the IP address that correspond to 255 in the mask will be repeated in the subnetwork address.
2. The bytes in the IP address that correspond to 0 in the mask will change to 0 in the subnetwork address.
3. For other bytes, use the bit-wise AND operator.

Example – How to get the network address from an IP address.

IP address	45.	123.	21.	8	
Mask	255.	192.	0.	0	bitwise
Subnetwork address	45.	64.	0.	0.	

123	0 1 1 1 1 0 1 1	
192	1 1 0 0 0 0 0 0	'AND bit-wise
64	0 1 0 0 0 0 0 0	

Example - 213 . 23 . 47 . 37 IP address
255 . 255. 255. 240 mask
213 . 23 . 47 . 32 Subnetwork address

Other protocols in the network layer - TCP/IP support four other protocols in the network layer:- ARP, RARP, ICMP and IGMP

- ARP - associates an IP address with the physical address. Address resolution protocol, In TCP/IP, a protocol for obtaining the physical address of a node when the Internet address is known.

TRUBA

RARP - Reverse address resolution protocol - that allows a host to find its internet address given its physical address.

ICMP - is a mechanism used by hosts and routers to send notification of datagram problems back to the sender. (internet control message protocol).

IGMP - Internet group message protocol has been designed to help a multicast router identify the hosts in a LAN that are members of a multicast group. It is a companion to the IP protocol.

Compiled By - Nandini Sharma

Transport layer :- It is represented in TCP/IP by two protocols :- TCP / UDP.

Port address of a following protocols -

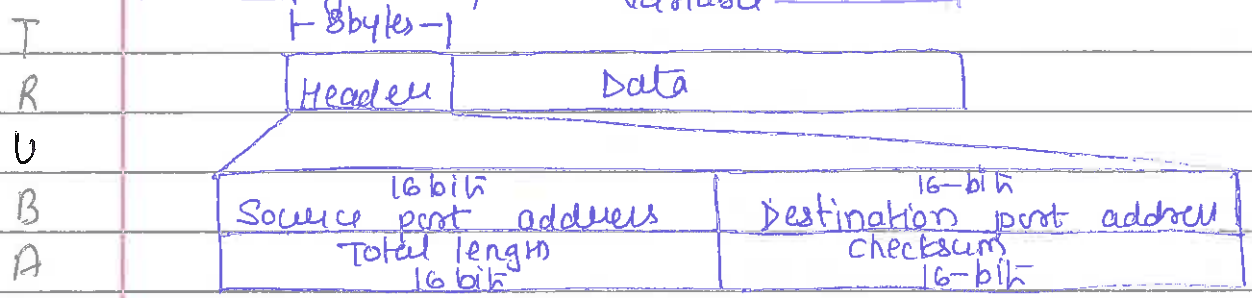
Port Number	Description
20	FTP- data
21	FTP - control
23	Telnet
25	SMTP
53	DNS
69	TFTP
79	Finger
80	HTTP
109	POP2
110	POP3
156	SQL Server
161	SNMP
443	HTTPs
458	Apple Quick Time
546	DHCP client
547	DHCP Server
569	MSN

Port numbers range from 0 to 65536, but only port numbers 0 to 1024 are reserved for priviliged services & designated as well-known ports. Above port number used by the server process as it's contact port.

UDP - User datagram protocal is the simplest of the two standard TCP/IP transport protocols. It is end-to-end transport level protocal that adds only port addresses,

checksum error control & length information to the data from the upper layer. The packet produced by the UDP is called a user datagram.

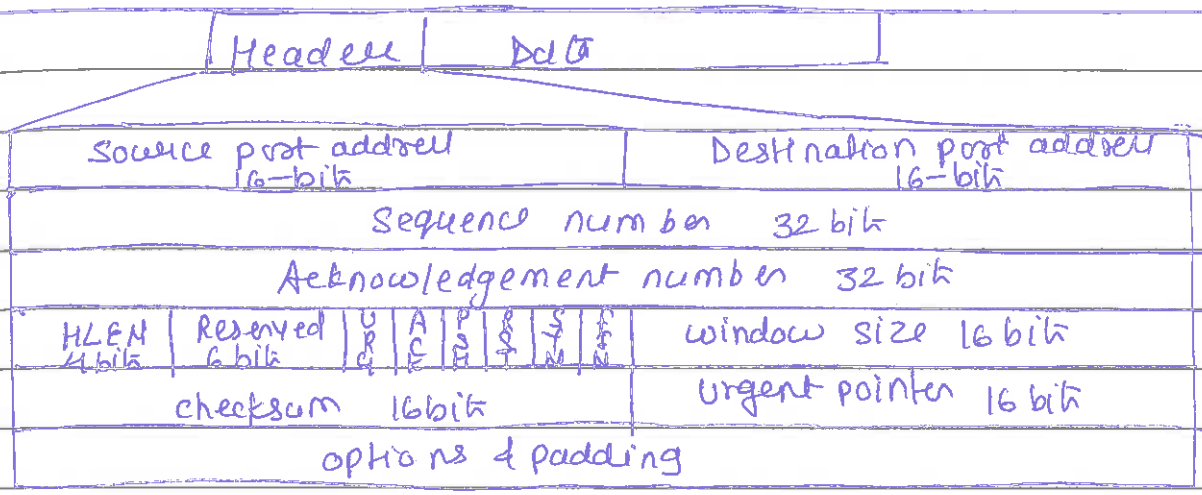
UDP datagram format -



- Source port address - The source port address is the address of the application program that has created the message.
- Destination port address - The destination port address is the address of the application program that will receive the message.
- Total length - The total length field defines the total length of the user datagram in bytes.
- checksum - The checksum is a 16-bit field used in error detection.

Transmission Control Protocol - It provides full transport layer services to applications.

TCP Segment

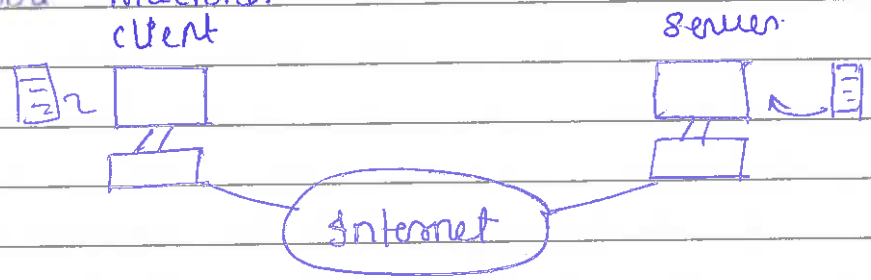


- Source port address – The source port address defines the application program in the source computer.
- Destination port address – The destination port address defines the application program in the destination computer.
- Sequence Number – A stream of data from the application program may be divided into two or more TCP segments. The sequence number field shows the position of the data in the original data stream.
- Acknowledgment Number – This number is valid only if the Ack bit in the control field is set. It defines the byte sequence number that is next expected.
- Header Length (HLEN) :– The four-bit HLEN field indicates the number of 32-bit words in the TCP header.
- Reserved – A six-bit field is reserved for future use.
- Control – Each bit of the six-bit control field functions individually & independently.
- Window Size – The window is a 16-bit field that defins the size of the sliding window.
- Checksum – The checksum is a 16-bit field used in error detection.
- Urgent pointer – The sender is informing the receiver that there are urgent data in the data portion of the segment.
- Options & padding – They are used to convey additional information to the receiver or for alignment purposes.

TCP/IP protocol suite I– Application layer

1. client-server model– The application programs using the Internet follow these client – server model strategies–

An application program, called the client, running on the local machine, request a server from another application program, called the server, running on the remote machine.



client - server model

2. Bootstrap protocol (BOOTP) – Each computer that is attached to a TCP/IP internet must know the following information.
   - Its IP address.
   - Its subnet mask.
   - The IP address of a router.
   - The IP address of a name server.

This information is usually stored in a configuration file & accessed by the computer during the bootstrap process. But what about a diskless workstation or a computer with a disk that is booted for the first time?

In the case of a diskless computer, the operating system & the networking s/w could be in read-only-memory (ROM)

BOOTP is a client-server protocol designed to provide the four previously mentioned pieces of information for a diskless computer or a computer that is booted for the first time. If we use BOOTP, we do not need RARP.

3. Dynamic Host configuration protocol (DHCP):- BOOTP is not a dynamic configuration protocol. When a client request is IP address, the BOOTP server searches a table that matches the physical address of the client with its IP address. This implies that the binding b/w the physical address & the IP address of the client should already exist. The binding is predetermined.

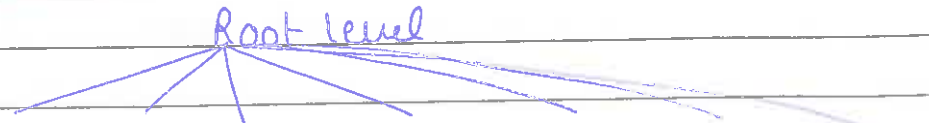
DHCP has been devised to provide dynamic configuration. It is an extension to BOOTP. It provides temporary IP addresses for a limited period of time.

4. Domain Name System:- To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet. However, people prefer to use names instead of addresses.

DNS is a protocol that can be used in different platforms. It is divided into three different sections:- generic domains, country domains & inverse domains.

Generic domains:- define registered hosts according to their generic behavior. Each node in the tree defines a domain, which is an index to the domain name space database.

It allow three-character labels.



↓

fhda

↓

atc

↓

chal

↳ chal . atc . fhda . edu

Index to address.

Generic domain labels -

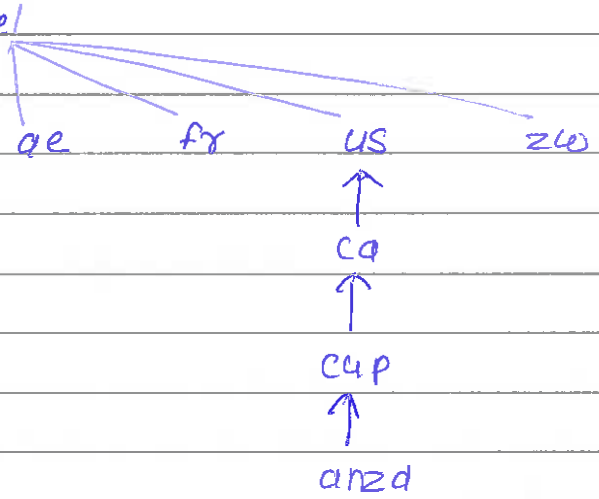
Label	Descriptions
com	commercial organizations
edu	Educational institutions
gov	Government institutions
int	International organizations
mil	Military groups
net	Network support centers
org	Non-profit organizations

proposed generic domain labels

Label	Descriptions
arts	cultural organizations
firm	Businesses or firms
info	Information service providers
nom	Personal nomenclatures
rec	Recreation / entertainment organizations
store	Business offering goods to purchase
web	web-related organizations

country Domains – follows the same format as the generic domains but uses two-character country abbreviations. in place of three character organizational abbreviations at the first level

country domains –

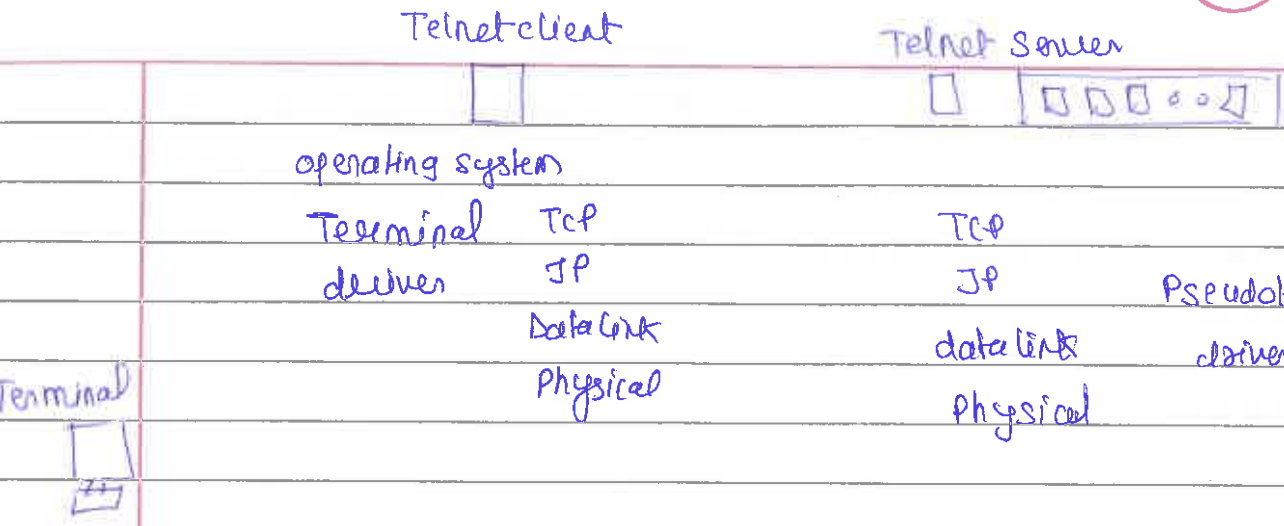


anza. cup. ca. us
Index to address.

Inverse domain – used to map an address to a name.

Example – when a Server has received a request from a client to do a task. whereas the Server has a file that contains a list of authorized clients, the server lists only the IP address of the client. To determine, if the client is on the authorize list, it can send a query to the DNS Server & ask for a mapping of address to name.

5. Telnet – is a general-purpose client-Server application program. It enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.

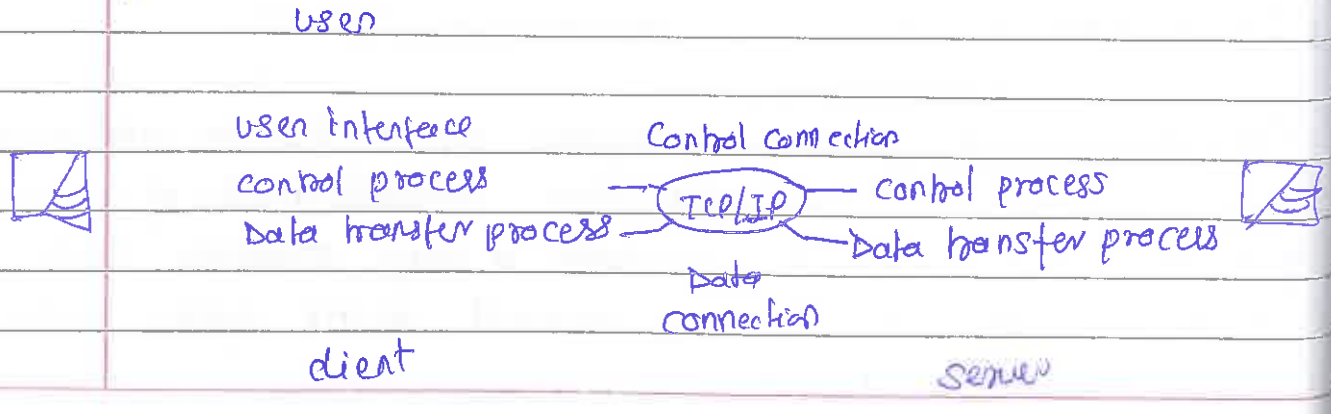


6. File Transfer protocol (FTP) :- is the standard mechanism provided by TCP/IP for copying a file from one host to another

T
R
U
B
A

Example:- Two systems may use different file name conventions, or may have different ways to represent text & data, or may have different directory structures. All of these problems have been solved by FTP in a very simple & elegant approach.

FTP differs from other client-server applications in that it establishes two connection between the hosts. one connection is used for data transfer, the other for control information (commands & responses)



FTP

Trivial File Transfer Protocal - There are occasions when we need to simply copy a file without the need for all of the functionalities of the FTP protocol. It is designed for these types of file transfer. It is so simple that the software package can fit into the read-only mem of a diskless workstation. It can be used at bootstrap time. It can read or write a file for the client.

Reading means copying a file from the servers site to the client site.

Writing means copying a file from the client site to the server site.

Example - when a diskless workstation or a router is booted, we need to download the bootstrap & configuration files. Here we do not need all the sophistication provided in FTP, just need a protocol that quickly copies the files.

7. Simple mail transfer protocal (SMTP) :- One of the most popular network services is electronic mail (e-mail). SMTP is a system for sending messages to other computers users based on e-mail addresses. It provides for mail exchange between users on the same / different computers & supports :-

- Sending a single message to one or more recipients.
- Sending messages that include text, voice, video or graphics
- Sending messages to users on networks outside the Internet.

SMTP client and server into two components :- UA & MTA or user agent & mail transfer agent.

Compiled By - Ms. Nandini Sharma

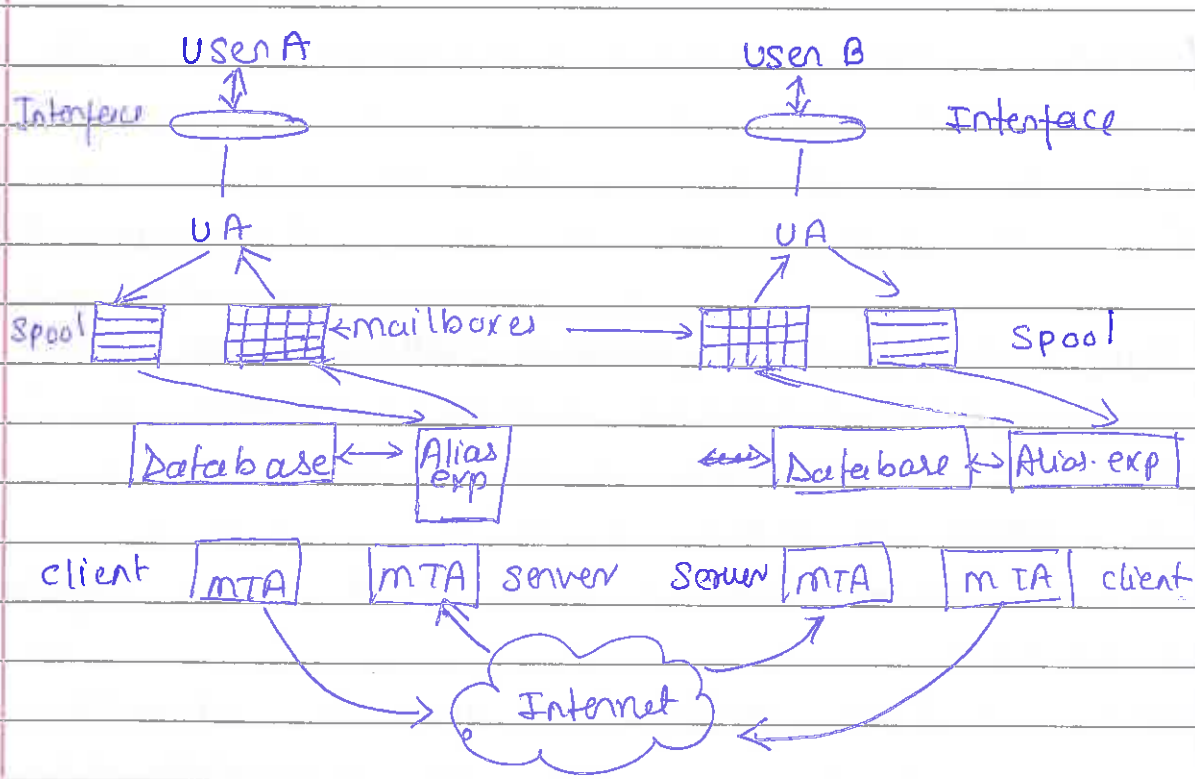
User Agent (UA) is normally a program used to send & receive mail.

Local part @ Domain name

Local part: address of the mailboxes on the local site

Domain name: The domain name of the destination

Mail transfer Agent:- The actual mail transfer is done through mail transfer agents (MTAs). To send mail, a system must have a client MTA, and to receive mail, a system must have a server MTA



The entire e-mail system.

Compiled By – Ms. Nandini Sharma
(Assistant Professor)
Truba College of Sc. & Tech., Bhopal

3. Multipurpose Internet mail Extensions — SMTP is a simple mail transfer protocol. SMTP can send messages only in NVT seven-bit ASCII format.

Example — It can't be used for languages that are not supported by 7-bit ASCII characters (such as French, German, Hebrew, Russian, chinese & japanese). Also, it can't be used to binary files or to send video or audio data.

MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME is not a mail protocol & can't replace SMTP, it is only an extension to SMTP.

9. Post office protocol (POP)3 — SMTP expects the destination host, the mail server receiving the mail, to be on-line all the time, otherwise, a TCP connection can't be established.

For this reason, it is not practical to establish an SMTP session with a desktop computer b/c desktop computers are usually powered down at the end of the day.

In many Organizations, mail is received by an SMTP server that is always on-line. This SMTP server provides a mail-drop service. The server receives the mail on behalf of every host in the organization. Workstations interact with the SMTP host to receive retrieve messages by using a client-server protocol such as Post-office-protocol (POP) version 3 (POP3).

SNMP — Simple Network management protocol is a framework for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring & maintaining an Internet.

SNMP uses the concept of manager & agent. That is, a manager, usually a host, controls & monitors a set of agents, usually routers.

SNMP is based on three basic ideas—

1. A manager checks an agent by requesting information that reflects the behavior of the agent.
2. A manager forces an agent to perform a task by resetting values in the agent database.
3. An agent contributes to the management process by warning the manager of an unusual situation

TRUBA

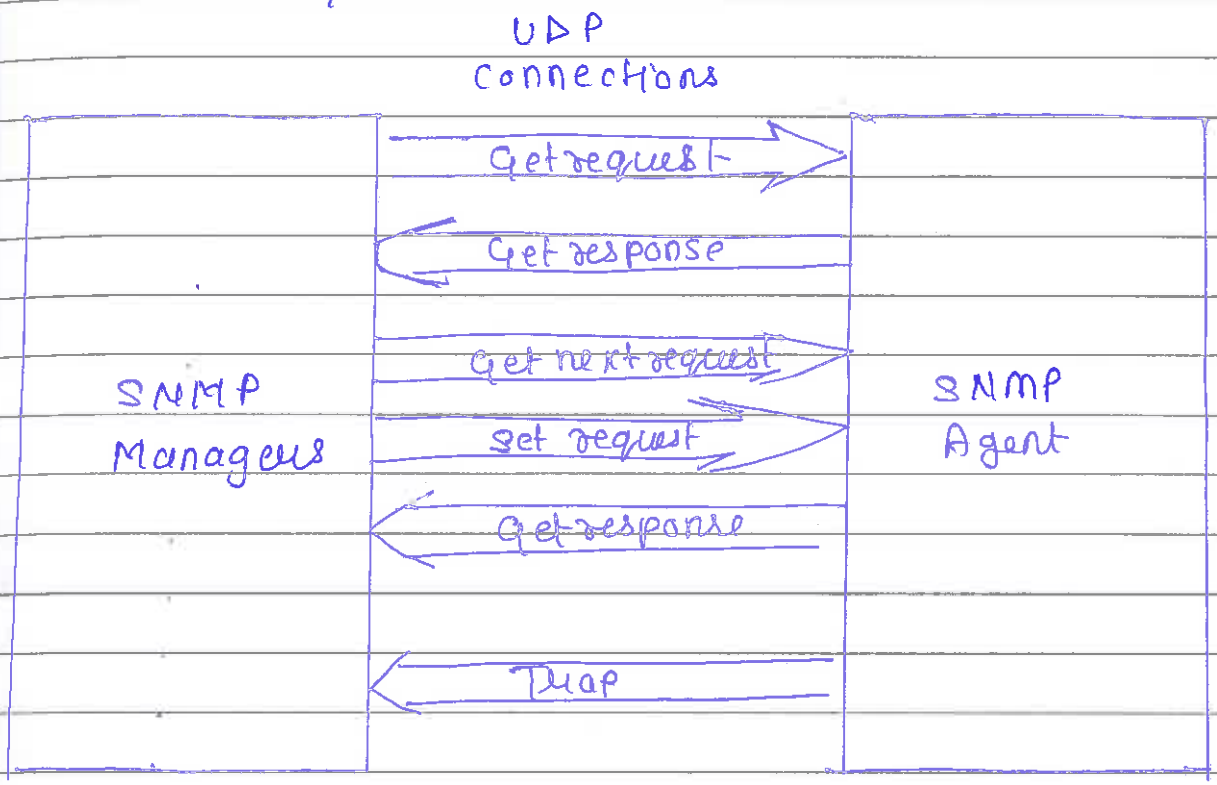
At the top level, management is accomplished with two other protocols:- Structure of management Information (SMI) & management information base (MIB).

SNMPv1— defines five messages—

- GetRequest — Sent from manager to agent to retrieve the value of a variable.
- GetNextRequest - Sent from manager to agent to retrieve the values of a variable. (The retrieved value is the value of the object following the defined object in the message)
- GetResponse- Sent from an agent to a manager in response to getrequest & getnextrequest.
- SetRequest - Sent from manager to the agent to set (store) a value in a variable.
- Trap1— is sent from the agent to the manager to report an event.

Example— If the agent is rebooted, it informs the manager & reports the time of rebooting.

SNMP Messages :-



References —

"Data Communications & Networking"
Author –
Behrouz A. Forouzan
2nd Edition Tata McGraw-Hill publishers

Prepared By :—

Miss. Nandini Sharma
Assistant Professor
Truba College of Sc. & Tech., Bhopal
CSE Dept.