Computer Networks

Unit - I

Introduction and Physical layer

Introduction: Networks - Network Types - Protocol layering - TCP / IP Protocol suite - OSI model; Physical layer ; Performance; Socket programming; Transmission media.

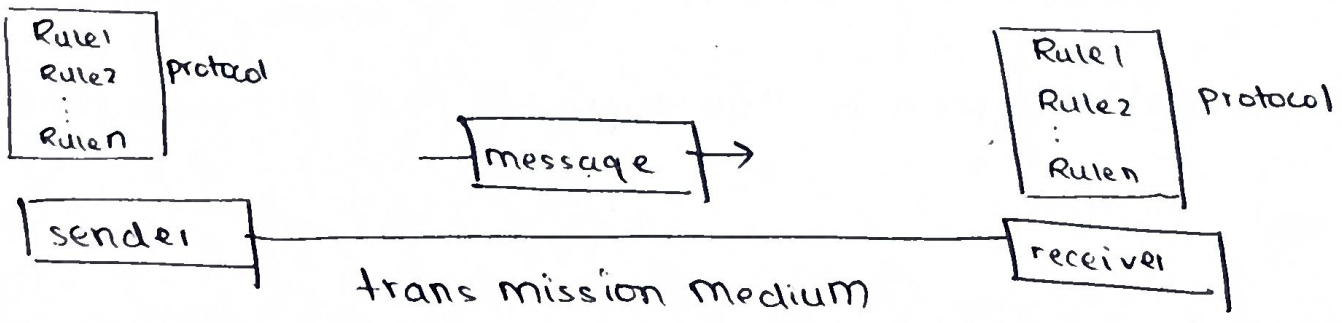
* Telecommunication

→ communication at a distance

→ data refers to information presented in whatever form is agreed by parties creating and using the data.

→ Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

* Components of a Data communications system



(i) message

(ii) sender

(iii) receiver

(iv) transmission medium

(v) protocol - a set of rules that govern data communications. an agreement between communicating devices.

* Effectiveness of Data Communication

(i) Delivery - The system must deliver data to the correct destination. Data must be received by the intended device & user & only by them.

(ii) Accuracy - The system must deliver the data accurately. Data that has been altered in transmission are unusable.

(iii) Timeliness - The system must deliver data in a timely manner. In the case of audio and video, timely delivery means delivering data as they are produced, in the same order that they are produced and without significant delay. (real-time transmission)

(iv) Jitter - the variation in packet arrival time. It is the uneven delay in the delivery of audio or video packets.

* Data Representation

→ Text
→ Audio
→ Images
→ Video
→ Numbers

* Data Flow

→ can be simplex, half-duplex or full-duplex

A. Simplex Mode

→ unidirectional data transfer.
→ only one of the 2 devices on a link can transmit, the other can receive

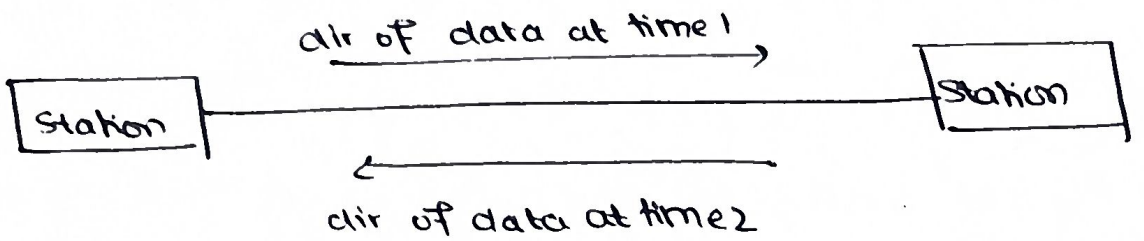
→ eg. keyboards, monitors
→ simplex mode uses entire channel capacity

Half-duplex

→ Each station can both transmit and receive, but not at the same time.

→ During transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.

→ eg. walkie-talkies and citizen band radios



Full-duplex

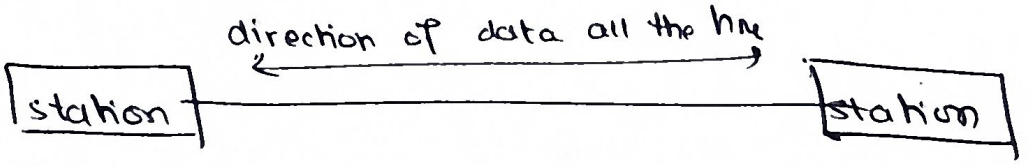
→ Both stations can transmit and receive simultaneously.

→ In this mode, signals going in one direction share the capacity of the link with signals going in the other direction. The sharing can occur in 2 ways:

(i) the link may have 2 physically separate transmission paths, one for sending and the other for receiving

(ii) the capacity of the channel is divided between signals traveling in both directions

eg. telephone line



* Networks

→ A network is an interconnection of a set of devices capable of communication.

→ set of devices = nodes, communication done w/ links

→ A node can be a computer, printer or any other device capable of sending and/or receiving data generated by other nodes on the network.

* Network Criteria

A. Performance

(i) transit time - time required for a message to travel from one device to another.

(ii) response time - elapsed time between an inquiry & a response.

(iii) throughput

(iv) delay

B. Reliability

measured by (i) the frequency of failure

(ii) the time it takes a link to recover from a failure

(iii) network robustness in a catastrophe

C. Security

→ protecting data from unauthorized access, damage

→ policies to recover from breach and data loss

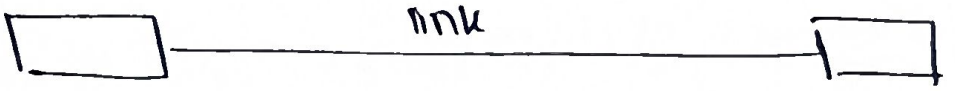
* Physical Structures

A. Type of Connections

(i) point-to-point → provides a dedicated link between two devices

→ entire capacity of the link is reserved for transmission between those 2 devices.

→ most PQP connections use an actual length of wire or cable to connect the two ends, but microwave or satellite links are also possible



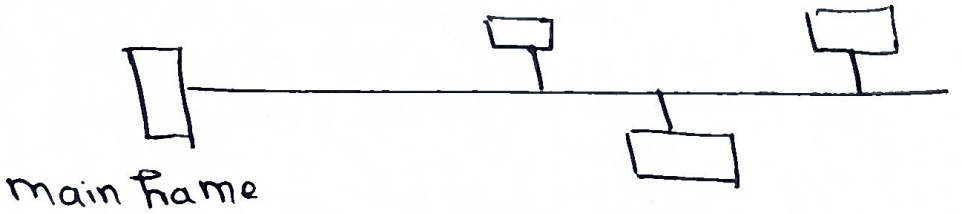
(ii) multipoint / multidrop connection

→ more than two specific devices share a single link

→ the capacity of the channel is shared, spatially or temporally.

→ If several devices can use the link simultaneously = spatially shared

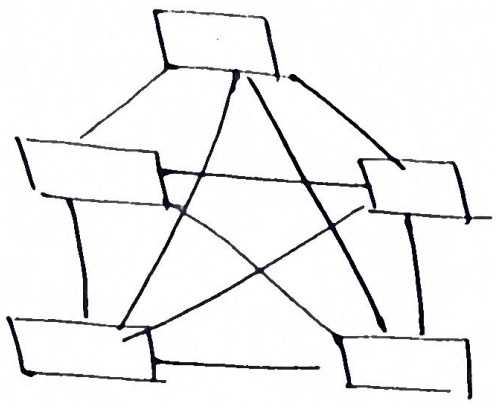
→ If users must take turns = time shared connection



* Topology

→ Geometric representation of the relationship of all link and nodes to one another.

A. Mesh Topology



→ Every device has a dedicated point-to-point link to every other device.

Total no. of links = $n(n-1)$

for duplex = $\frac{n(n-1)}{2}$

Advantages (i) dedicated link

(ii) less traffic

(iii) robust

(iv) privacy

(v) easy fault identification

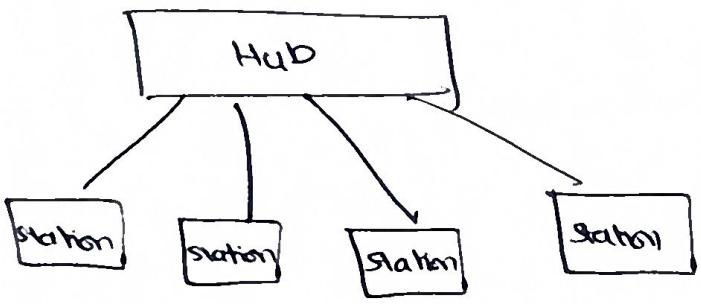
Disadvantage: (i) amount of cabling

(ii) hardware is expensive

Example: (i) backbone

(ii) telephone regional office connection at backbone.

B. Star Topology



Advantage - easy installation & configuration

less cabling & robust

less expensive

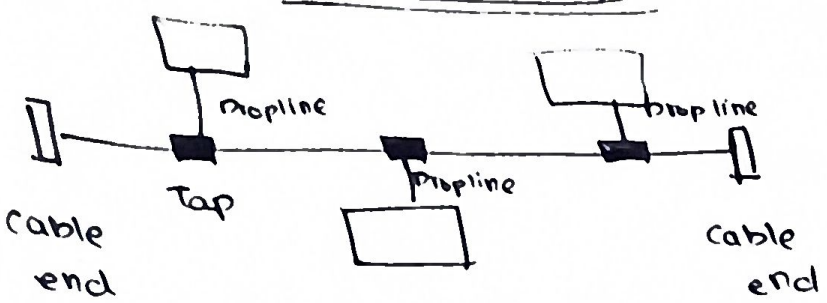
Disadvantage - single point failure.

→ Each device has a dedicated point to point link only to a central controller called a hub.

→ The devices are not directly linked to one another.

→ does not allow direct traffic between devices, controller acts as an exchange

C. Bus Topology



→ a multipoint topology, one long cable acts as backbone to link all the devices in a network

→ Nodes are connected to the bus cable by drop lines and taps.

→ A drop line is a connection running between the device and the main cable

→ A tap is a connector that splices into the main cable

→ As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker & weaker as it travels farther & farther. (Can have only limited no. of taps)

Advantage: (i) backbone cables - less cabling

(ii) less redundancy

Disadvantage: (i) Fault isolation

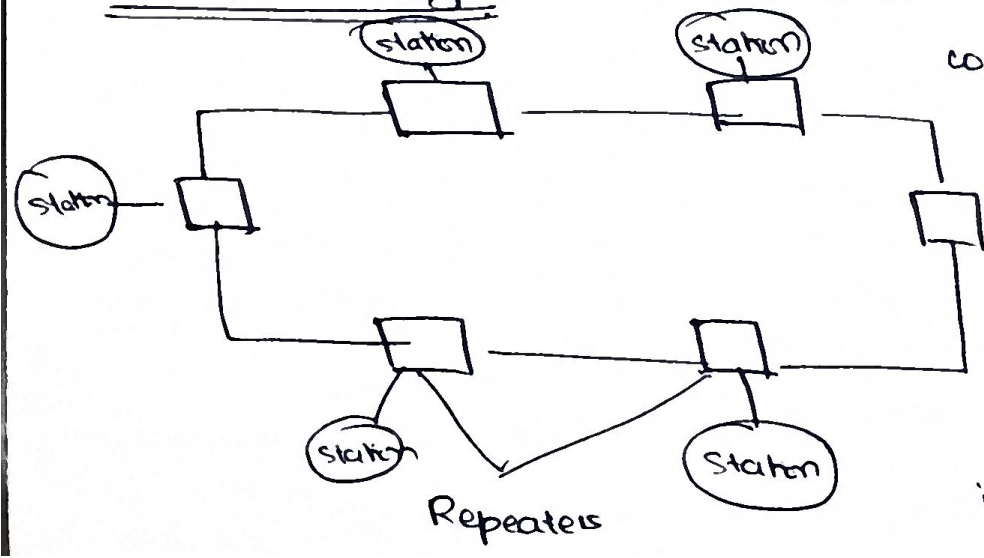
(ii) difficult reconnection

(iii) adding a new device is difficult

(iv) Fault stops transmission of others

Example: Ethernet LAN

D. Ring Topology



→ Each device has a dedicated point-to-point connection with only the two devices on either side of it.

→ A signal is passed along the ring in one direction, from device to device, until it reaches its application.

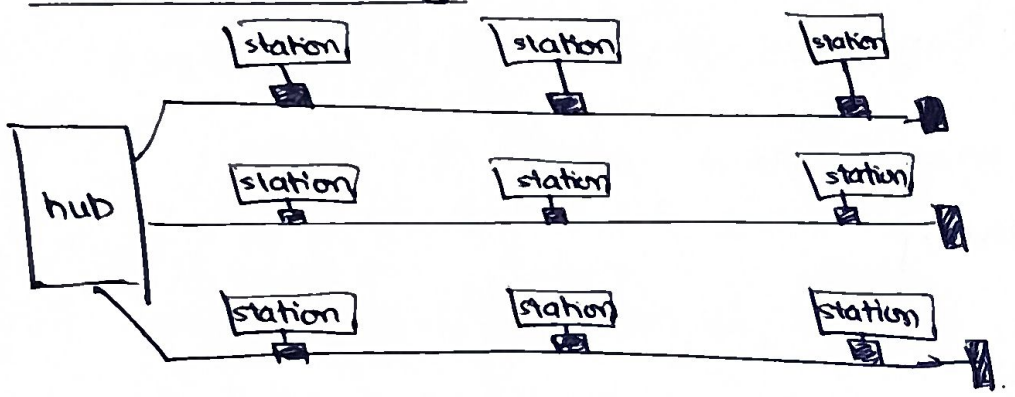
→ Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

Advantage: → Easy installation & configuration
→ Fault isolation is easy

Disadvantage: unidirectional traffic
single-break (use a dual ring / a switch)

Example: IBM introduced its LAN

* Hybrid Topology



a star backbone w/ three bus networks

* Network Types

(1) Local Area Network

→ privately owned and connects some hosts in a single office, building or campus
→ Each host in a LAN has an identifier, an address that uniquely defines the host in the LAN.
→ A packet sent by a host to another host carries both the source & destination host's addresses.
→ In the past - hosts connected through a common cable. intended recipients kept the packet, others dropped the packet.

→ Nowodays, LANs use a smart connecting switch, which identifies the destination address and sends it there alone.

(2) Wide Area Network

→ A WAN has a wider geographical span

→ While a LAN interconnects hosts, a WAN interconnects connecting devices such as switches, routers or modems

Types:

P2P WAN - connects 2 communicating devices through a transmission media (cable or air)

Switched WAN - a network with more than 2 ends.

- a combination of several P2P WANs connected by switches

* Switching → forwards data from a network to another network

2 types: (i) circuit switched

(ii) packet switched

A. Circuit Switched Network → a dedicated connection called a circuit is always available between the two end systems, the switch can only make it active or inactive.

→ Efficient only when it is at full capacity

B. Packet-Switched Networks → communication between 2 ends done in blocks of data called packets.

→ Switches store & forward data, since a packet is an independent entity.

→ A router in a packet switched network has a queue that can store and forward the packet.

* Internet → connects more than a network Rans / conns, comprises of thousands of interconnected networks.

→ At the top level, there are large networks called backbones, owned by communication companies such as Sprint, Verizon etc.

→ The backbone networks are connected through some complex switching systems, called peering points.

→ The provider networks are connected to backbone

→ The customer networks are networks at the edge of the Internet that actually use the services of the internet. They pay fees to the provider networks

→ Backbone and provider networks are also Internet Service Providers.

Read History P9 19

* Protocols

→ synonymous with rule.

→ consists of a set of rules that govern data communications

→ determines what is communicated, how it is communicated and when it is communicated.

→ They key elements are: syntax, semantics & timing

Syntax

→ structure or format of the data

→ indicates how to read the bits - field delineation

Semantics

→ interpret the meaning of the bits

→ knows which fields define what action

Timing

→ when data should be sent and what

→ speed at which data should be sent or received.

* Protocol Layering - TCP/IP and OSI model

* Protocol Layering

Protocol - the rules that both the sender and receiver and all intermediate devices need to be able to follow to communicate effectively.

→ When communication is simple, we may need only one simple protocol.

→ When the communication is complex, we may need to divide the task between different layers, for which a protocol is needed for each layer, called protocol layering.

* Advantages of Protocol layer.

→ enables one to divide a complex task into several smaller and simpler tasks

→ allows to separate services from implementation

→ Communication does not always use 2 end systems, there are intermediate systems that need only some layers, but not alll layers. If not for PL, we would have to make each intermediate system as complex as the end systems, which is expensive

*Principles of Protocol Layering

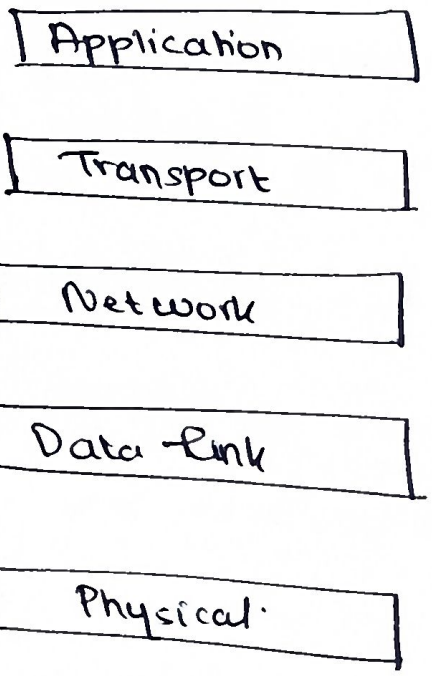
First Principle - The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.

Second Principle: The two objects under each layer at both sites shouldbe identical

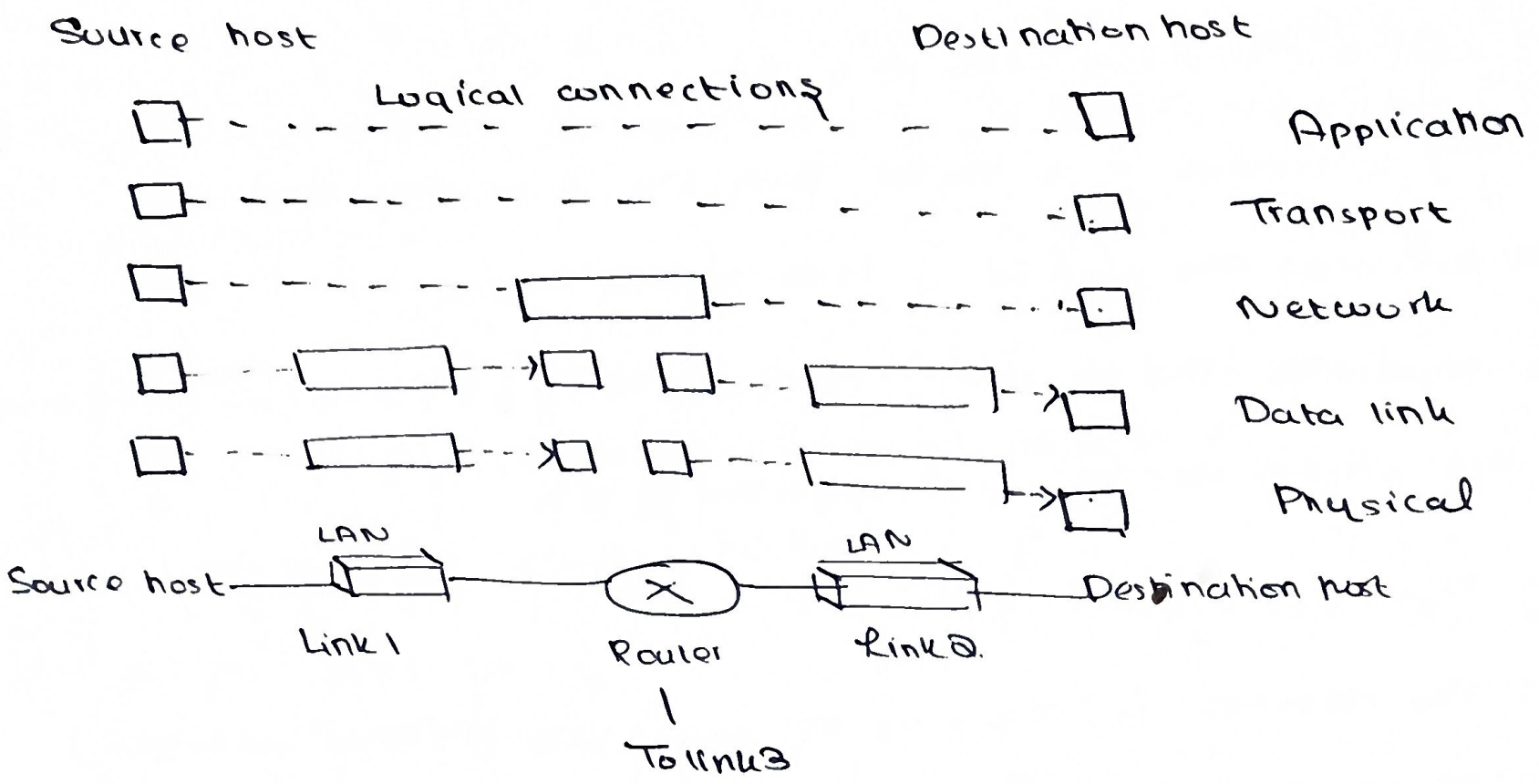
* TCP/ IP Protocol Suite

→ A hierarchical protocol made up of interactive modules, each of which provides a specific functionality.

Layers



Logical connections between layers of the TCP/IP Protocol suite



→ The duty of the data-link and physical layers is hop-to-hop, in which a hop is a router or host.

i.e the top three layer's domain of duty is the internet

→ Alternatively, in the top three layers, the data unit (packets) should not be changed by any router or link-layer switch.

→ In the bottom 2 layers, the packet created by the host is changed only by the router

L1, L2 → link
L3 - L5 → internet

Application → messages
Transport → segments / datagram
Network → datagrams
Data link → frames
Physical → bits

* Description of Each Layer

(1) Physical Layer

→ carries individual bits in a frame

→ bits received in a frame from the data link layer are transformed into signals in transmission media.

→ represents the physical characteristics of the interface and medium

→ also responsible for synchronization of bits

(2) Data link Layer.

→ The internet is made up of several links (LANs and WANs) connected by routers. There may be several overlapping sets of links that a datagram can travel from host to destination.

The data-link layer is responsible for taking the datagram and moving it across the best link.

→ DLL supports all standard & propietary protocols

→ DLL takes a datagram and encapsulates it in a packet called a frame.

→ also helps with error detection and correction

→ other utilities: flow control, access control, physical addressing

(3) Network Layer

→ responsible for creating a connection between the source and destination computer

→ communication at the network layer is host-to-host.

→ responsible for host to host communication and routing the packet through possible routes.

→ The NL in the Internet includes the main protocol - Internet Protocol (IP), that defines the format of the packet called a datagram

→ IP
(i) defines the format & structure of address in NL
(ii) routes packet from source to destination
(i) is a connectionless protocol
(iv) no error control
flow control
congestion control

→ NL includes unicast (one-to-one) and multicast (one-to-many) routing protocols. (Routing protocols do not take part in routing, but creates forwarding tables for routers to help with the routing process).

→ Auxiliary protocols in NL

(i) ICMP → Internet Control Message Protocol - helps IP report some problems while routing a packet.

(ii) IGMP → Internet Group Management Protocol - helps IP in multitasking

(iii) DHCP → Dynamic Host Configuration Protocol - helps IP get the NL address for a host

(iv) ARP → Address Resolution Protocol - helps IP find the link layer address of a host, when network-layer address is given.

(4) Transport Layer

→ Process to process delivery (end to end) of segments

→ TL at source host gets the message from the application layer, encapsulates it and sends it through the imaginary connection to the destination host.

→ TL gives services to the application layer.

→ There are a few transport-layer protocols in the Internet

(i) TCP - a connection-oriented protocol that establishes a logical connection between the TLs at two hosts

- → provides flow control, error control & congestion control
- → helps in segmentation and reassembly
- → uses service point addressing (portnos)

(ii) UDP - User Datagram Protocol

→ a connectionless protocol that transmits user datagrams w/o first creating a logical connection

→ does not provide flow, error or congestion control

(iii) SCTP - Stream Control Transmission Protocol

→ designed to respond to new applications that are emerging in the multimedia.

(5) Application Layer

→ the logical connection between 2 application layers is end to end.

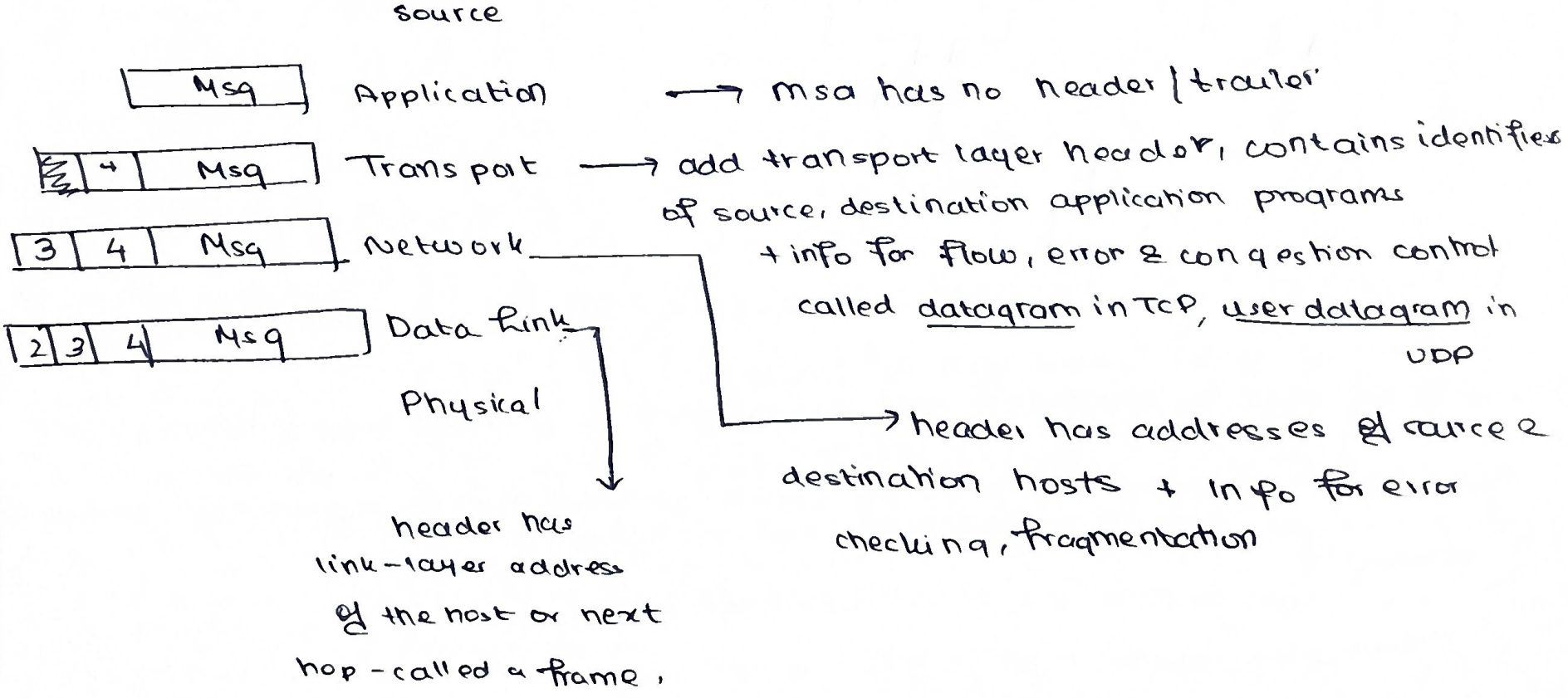
→ The application layer exchanges messages, comm is between processes (2 programs)

→ enables the user to access the network

→ provides user interface & support service such as

- email
- remote file access & transfer
- shared DB management
- network virtual terminal
- directory services

* Encapsulation / Decapsulation

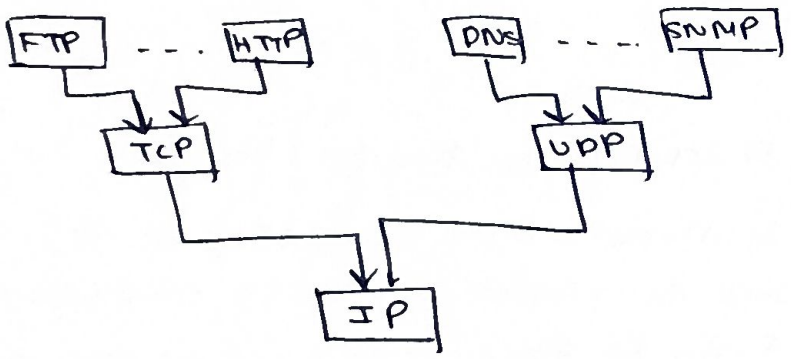


* Addressing

Application layer	names	
Transport layer	port numbers	→ define the application layer programs at the source & destination
Network layer	logical address	→ connection of device to the internet
Data-link layer	link-layer address	→ called MAC address, defines a host/router in a network.
Physical layer		

* Multiplexing and Demultiplexing

→ Multiplexing: a protocol at a layer can encapsulate a packet from several next higher-level protocols



multiplexing - reverse arrows ⇒ demultiplexing

→ To be able to multiplex and demultiplex, a protocol needs to have a field in its header to identify which protocol the encapsulated packets belong to.

Transport layer - UDP / TCP

Network layer - TCP & user datagram from UDP
IP can accept from ICMP, IGMP etc

Datalink layer → frame may carry payload from IP & other protocols like ARP.

The OSI Model

OSI - Open Systems Interconnection

→ An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

Purpose - how to facilitate communication between different systems w/o requiring changes to the logic of the underlying hardware and software.

→ The OSI model is not a protocol - but a model

→ Basis for creation of protocols in the OSI stack

→ The OSI model is a layered framework for the design of network systems that allows communications between all kinds of computer systems.

OSI Model

- Application
- Presentation
- Session
- Transport
- Network
- Data link
- Physical

} not in TCP — Application + presentation + session = application layer in TCP

Reasons for split-up

① → TCP/IP has more than one transport-layer protocol

→ Some functionalities of the session layer are available in some of the TL protocols

② → The application layer is not a single piece of software. Many applications can be developed at this layer.

* Lack of OSI Model's Success

→ completed after TCP/IP was already in place - changing would cost a lot

→ Some layers in the OSI model were never fully defined (Protocols for services in presentation & session layers not described + software not developed)

→ When OSI was implemented by an organization in a different application, it did not show high enough level of performance.

* Performance

① Bandwidth in Hertz

→ range of frequencies contained in a composite signal

eg. b/w of a subscriber telephone is 4kHz

② Bandwidth in Bits per second

→ no. of bits in a channel per second.

eg. b/w of a Fast Ethernet network is 100 Mbps

Relationship - An increase in bandwidth in hertz means an increase in bandwidth in bits per second

* Throughput

→ a measure of how fast we can actually send data through a network

B/w and throughput are not the same

B/w = potential measurement of a link
Th = actual measurement of how we can send data.

Example1 Network w/ a bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits what is the throughput of this network?

$$\text{Throughput} = \frac{12{,}000 * 10{,}000}{60} = 2{,}000 \times 1000 = 2 \times 10^6$$

$$= 2 \text{ Mbps}$$

* Latency / Delay

→ How long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source

Latency = propagation time + transmission time + queuing time + processing time

* Propagation Time – measures time required for a bit to travel from the source to the destination

$$\text{propagation time} = \frac{\text{distance}}{\text{propagation speed}}$$

propagation speed → 3×10^8 m/s

Example2 What is the propagation time if the distance between the 2 points is 12,000 km? propagation speed = 2.4×10^8 m/s

$$\text{Propagation time} = \frac{12{,}000 \times 1000}{2.4 \times 10^8} = 50\text{ms}$$

* Transmission Time - time taken between the first and last bit reaching the sender

$$\text{Transmission time} = \frac{\text{message size}}{\text{bandwidth}}$$

Example 3 What are the propagation times and transmission times for a 2.5 KB (kilobyte) message if the bandwidth of the network is 1 Gbps?

distance = 12,000 km

speed of light = 2.4×10^8 m/s

$$\text{Propagation time} = \frac{\text{distance}}{\text{propagation speed}} = \frac{12{,}000 \times 10^3}{2.4 \times 10^8}$$

$$= 50 \text{ ms}$$

$$\text{Transmission time} = \frac{\text{message size}}{\text{bandwidth}} = \frac{2.5 \times 10^3 \times 8}{10^9}$$

(to bits; $G = 10^9$)

$$= 0.02 \text{ ms}$$

Example 4 What are the propagation time and the transmission time for a 5 MB (megabyte) message if the bandwidth of the network is 1 Mbps?

distance = 12,000 km

speed = 2.4×10^8 m/s

Propagation time = $\frac{\text{distance}}{\text{propagation speed}}$

$= \frac{12,000 \times 10^3 * ^\circ}{2.4 \times 10^8} = 50ms$

Transmission time : $\frac{5 \times 10^6 \times 8}{10^6} = 40s = \frac{\text{message size}}{\text{bandwidth}}$

* Queuing Time

→ The time needed for each intermediate or end device to hold the message before it can be processed.

→ The queuing time is not a fixed factor, it changes with the load imposed on the network.

→ When there is heavy traffic on the network, the queuing time increases.

→ An intermediate device, such as a router, queues the arrived messages and processes them one by one.

→ If there are many messages, each message will have to wait.

* Bandwidth Delay Product

→ defines the no. of bits that can fill the link

BDP = bandwidth * delay

* Jitter

→ a problem encountered if different packets of data have different delays, and the application using the data at the receiver is time sensitive (audio and video data)

Example 5 If the bandwidth of the channel is 5 Kbps, how long does it take to send a frame of 100,000 bits out of this device?

$$\text{Time} = \frac{\text{no. of bits}}{\text{b/w}} = \frac{100000}{5000} = 20 \text{ seconds}$$

Example 6 If canal is the transmission time of a packet sent by a station if the length of the packet is 1 million bytes and the bandwidth of the channel is 200 kbps

$$\text{Time} = \frac{1,000,000 \times 8}{200 \times 10^3} = 40 \text{ seconds}$$

Example 7 What is the length of a bit in a channel with a propagation speed of 2×10^8 m/s if the channel bandwidth is

(a) 1 Mbps

(b) 10 Mbps

(c) 100 Mbps

$$(a) = \frac{\text{Propagation speed}}{\text{bandwidth}} = \frac{2 \times 10^8}{10^6} = 200\text{m}$$

$$= 200\text{m}$$

$$(b) = \frac{2 \times 10^8}{10 \times 10^6}$$

$$(c) = \frac{2 \times 10^8}{100 \times 10^6}$$

Example 8 How many bits can fit on a link with a 2ms delay if the bandwidth of the link is

a. 1Mbps
b. 10 Mbps
c. 100 Mbps

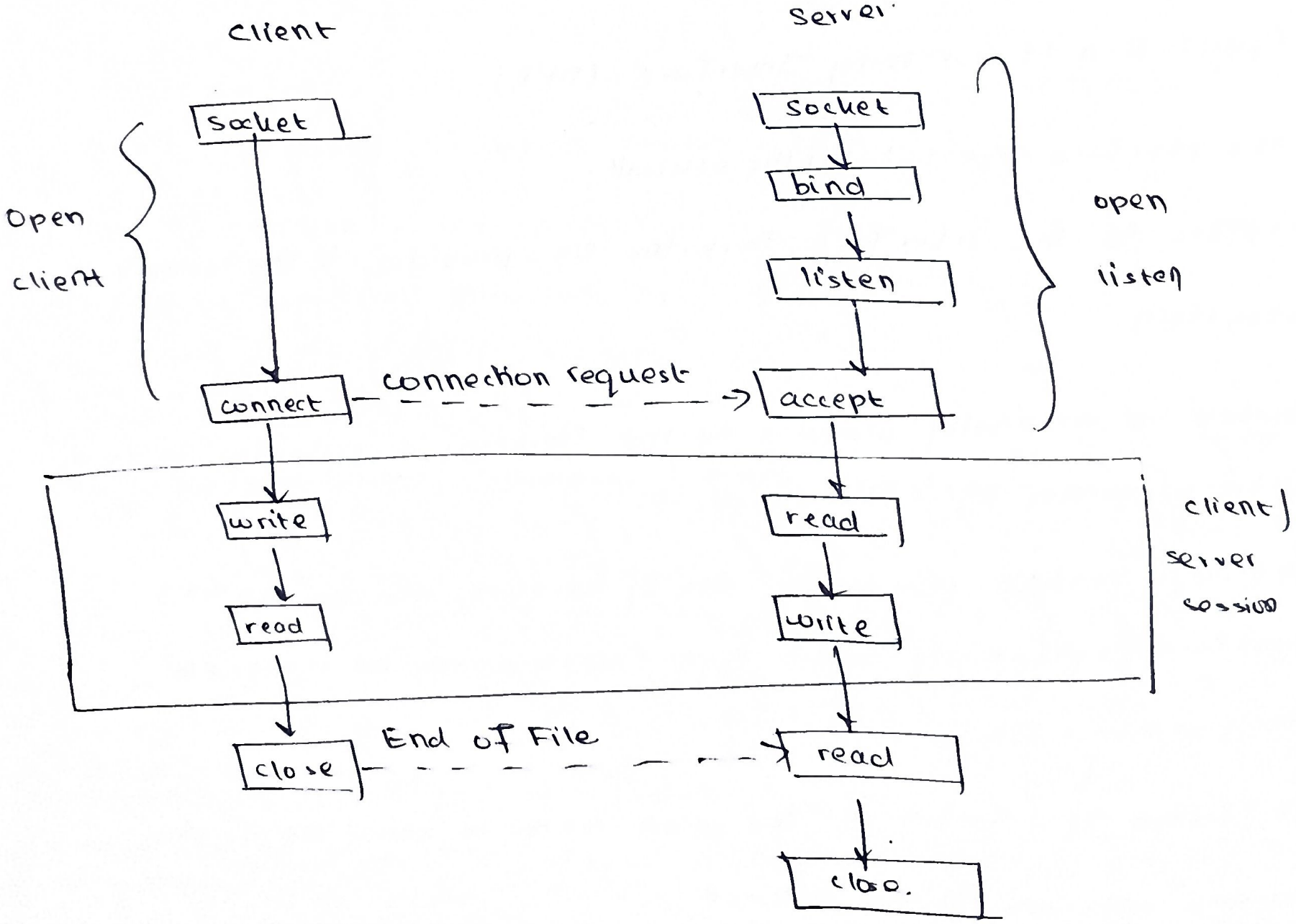
a. BDP = $2 \times 10^{-3} \times 1 \times 10^{6}$

= 2000bits

b. = $2 \times 10^{-3} \times 10 \times 10^{6}$

c. = $2 \times 10^{-3} \times 100 \times 10^{6}$

* Socket Programming



* Internet Architecture

→ defined by the IETF = Internet Engineering Task Force

→ has 3 main features:

(i) does not have strict layering. The application is free to bypass the defined transport layers and to directly use the IP.

(ii) has an hour glass - wide at the top, narrow in the middle & wide at the bottom. IP is the focal point in the architecture.

(iii) In order for a new protocol to be officially included in the architecture, there needs to be a protocol specification & at least one representative implementations of the specifications.

* Application Programming Interface (API)

→ the interface exported by the network.

→ refers to the interface that the OS provides to the networking subsystem

Sockets → originally provided by the Berkeley distribution of UNIX, now supported by virtually all OS

→ Each protocol provides a set of services, and the API provides a syntax by which those services can be invoked in this particular OS.

Definition of a socket → The point where a local application process attaches to the network

→ An interface between an application and the network

→ The interface defines operations for

(i) creating a socket

(ii) attaching a socket to the network

(iii) sending and receiving messages through the socket

(iv) closing the socket

* Socket Family

PF_INET – denotes the Internet family

PF_UNIX – denotes the UNIX pipe facility

PF_PACKET - denotes direct access to the network interface, i.e it bypasses the TCP/IP protocol stack

* Socket Types

- SOCK_STREAM – used to denote a byte stream

- SOCK_DGRAM – an alternative that denotes a message-oriented service, such as that provided by UDP

* Creating a socket

int sockfd = socket (address_family, type, protocol);

socket (PF_INET, SOCK_STREAM, 0)

implies TCP

* Client-server model with TCP

Server

→ is passively open

→ prepares to accept a connection, does not actually accept a connection

The server invokes:

(i) bind: int bind (socket, socket address, address length)

→ binds the newly created socket to the specified address, i.e the network address of the local participant

(ii) listen: int listen (int socket, int backlog)

→ defines how many connections can be pending on the specified socket.

(iii) accept: int accept (int socket, struct sockaddr *address, address length)

→ carries out the passive open

→ blocking operation

(i) does not return until a remote participant has established a connection

(ii) when it does, it returns a new socket that corresponds to the new established connection and the address argument that contains the remote participant's address.

Client

- application performs active open
- says who it wants to communicate with

The client invokes:

int connect (socket, address, address-length)

→ does not return until TCP has successfully established a connection at which the application is free to begin sending data.

→ The address contain the remote machine's address.

→ In practice, the client usually specifies only the remote participants address and lets the system fill in the local information

→ The server usually listens for messages on a well-known port.

→ A client does not care which port it uses for itself, the OS simply selects an unused one.

- Sending & Receiving messages

→ Once a connection is established, the application process invokes two operations

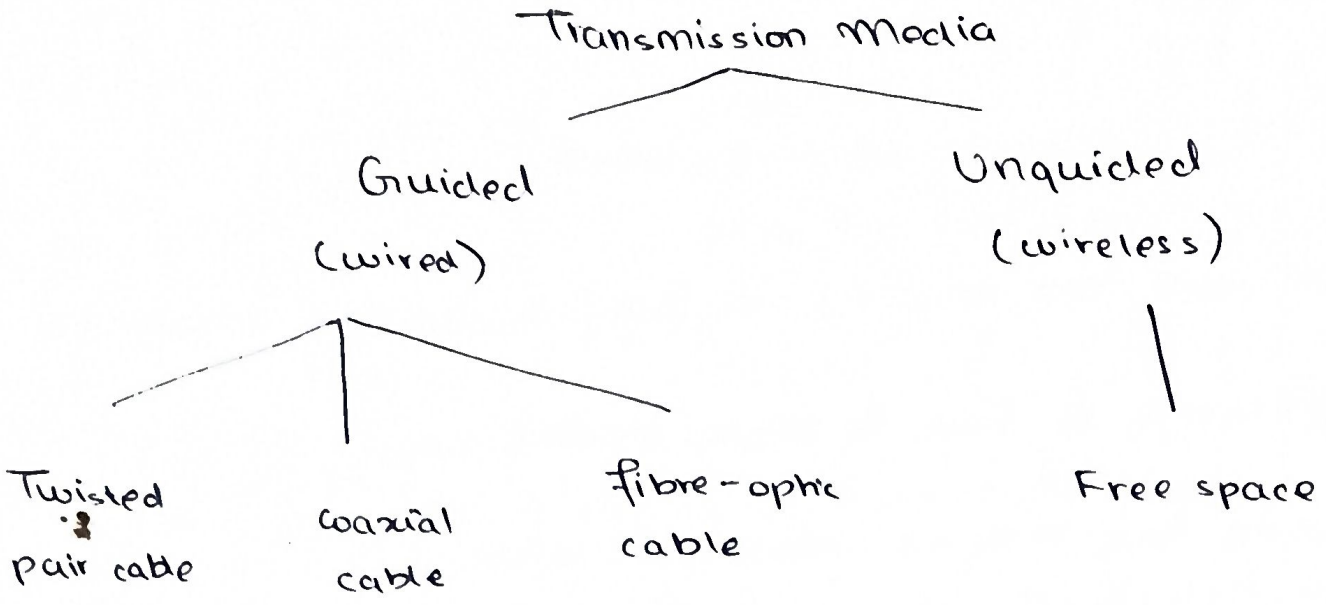
send (sock, msg, msg-len, flags)

recv (socket, buff, buff-len, flags)

* Transmission Media

→ anything that can be used to carry information from a source to a destination

eg. free space, metallic cable or a fibre-optic cable



* Guided media

→ provide a conduit from one device to another

→ includes twisted-pair cable, coaxial cable & fibre-optic cable

A. Twisted Pair Cable

→ one wire carrie signals, the other the ground reference

→ receiver uses the difference between the two

→ Interference and cross-talk affect both wires & create unwanted signals

→ By twisting the pairs, a balance is maintained

of 2 kinds - shielded and unshielded

↙

has a metal foil or braided mesh covering that encases each pair of insulated conductors

→ bulkier & expensive

Connectors

→ use a RJ45 (a keyed connector, meaning it can be inserted only in one way)

Performance

→ compare attenuation vs. frequency & distance

→ attenuation sharply increases w/ frequencies above 100kHz

Applications

→ used in telephone lines to provide voice and data channels

*3. Coaxial Cables

→ carries signals of higher frequencies than those in twisted pair cables.

→ Instead of 2 wires, coax has a central core conductor of solid or stranded wire, enclosed in an insulated sheath, which is, in turn, encased in an outer conductor.

→ The outer metallic wrapping serves as both a shield against noise and as the second conductor, which completes the circuit

Standards

categorized by their Radio Government (RG) ratings

Each RG number denotes a unique set of physical specifications

Connectors

use a BNC — Bayonet Neill- Concelman connector

BNC - cable to a device (TV)
BNC - T - for ethernet networks
BNC terminator - at end of cable to prevent reflection

Performance

→ higher attenuation - signal weakens rapidly and requires the frequent use of repeaters

Applications

→ In analog telephones

→ cable TV

→ traditional Ethernet LANs

c. Fibre-Optic Cable

→ made of glass or plastic and transmits signals in the form of light

→ If i (angle of incidence)

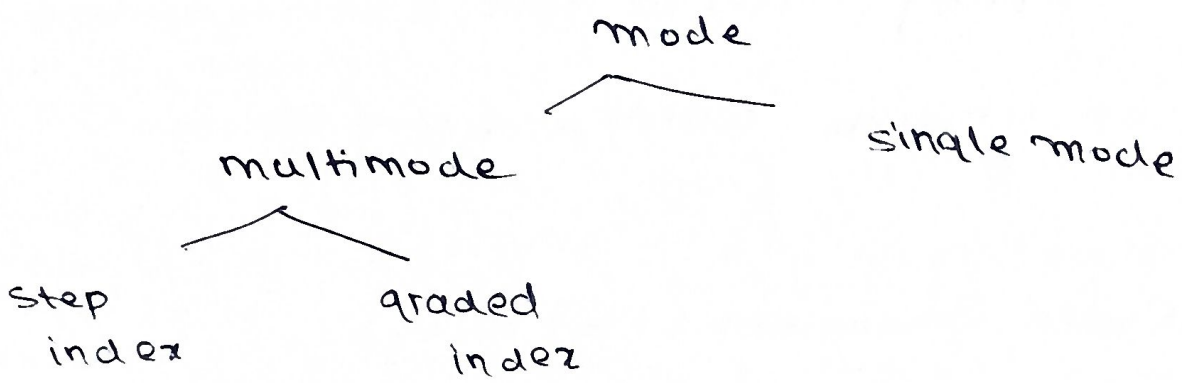
< critical angle - refraction to less dense medium

= critical - moves along surface

> critical angle - refracts into same medium

→ has a glass/plastic core surrounded by cladding

Propagation Modes



multimode - multiple beams from a light source move through the core in different paths.

→ density of core remains constant from the center to the edges

single-mode - uses a highly focused source of light

Fibre Sizes - on the ratio of the diameter of the core to the diameter of the cladding

Fibre optic Cable Connectors

(i) subscriber channel (SC) - for cableTV

(ii) straight-tip (ST) connector - to networking devices

MT-RJ (like an RJ-45)

Performance

→ much lesser attenuation

Applications

→ in backbone networks

→ cable tv companies

→ LANs

Advantages

→ higher bandwidth

→ less signal attenuation

→ immune to electromagnetic interference

→ corrosion resistant

→ light weight

Disadvantages

→ installation & maintenance

→ unidirectional light propagation

→ cost

* Unguided Media - Wireless

→ transport electromagnetic waves without using a physical conductor

→ can travel via ground, sky, line-of-sight propagation

- ground → lower portion of atmosphere
- sky → in ionosphere
- line-of-sight → in straight lines from antenna to antenna

A. Radio Waves

∿ between 3kHz & 1GHz

→ omnidirectional waves

→ ~~stop~~ susceptible to interference

→ sky mode radios can travel long distance

→ can penetrate walls

→ disadvantage: cannot isolated to within a building

→ used for multicast communications - radio, TV, paging systems

B. Microwaves

∿ = 1 – 300GHz

→ unidirectional, narrowly focused

→ must align antennas

→ line of sight propagation - hindered by earth's curvature, & other obstacles

→ often need repeaters

→ cannot penetrate walls

→ use of certain portions of the band requires permission from authorities.

→ used in cellular telephones, satellite networks, wireless LANs

Infrared Waves

ν = 300GHz - 400THz

→ for short-range communication - remote control

→ cannot penetrate walls

→ cannot be used outside a building - sun's rays contain Infrared waves.

Applications - keyboard, mice, printers

IrDA port allows a wireless keyboard to communicate with a PC.

* Disadvantages of Wireless Channels

→ subject to more errors

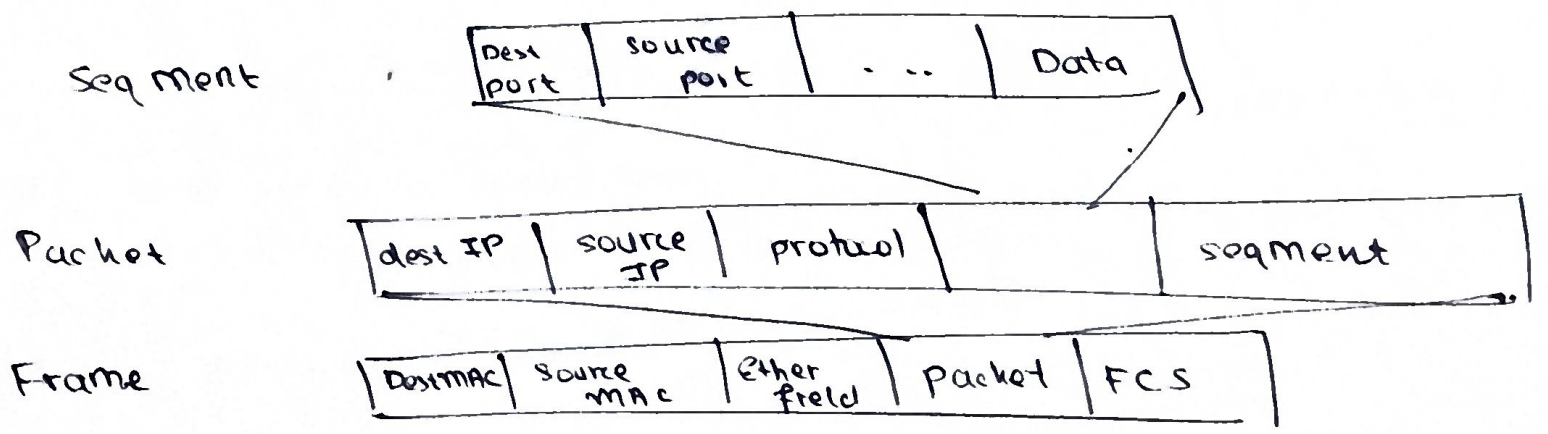
→ interference is a cause for errors, can be circumvented w/ a high SNR.

→ higher SNR => less capacity available for transmission

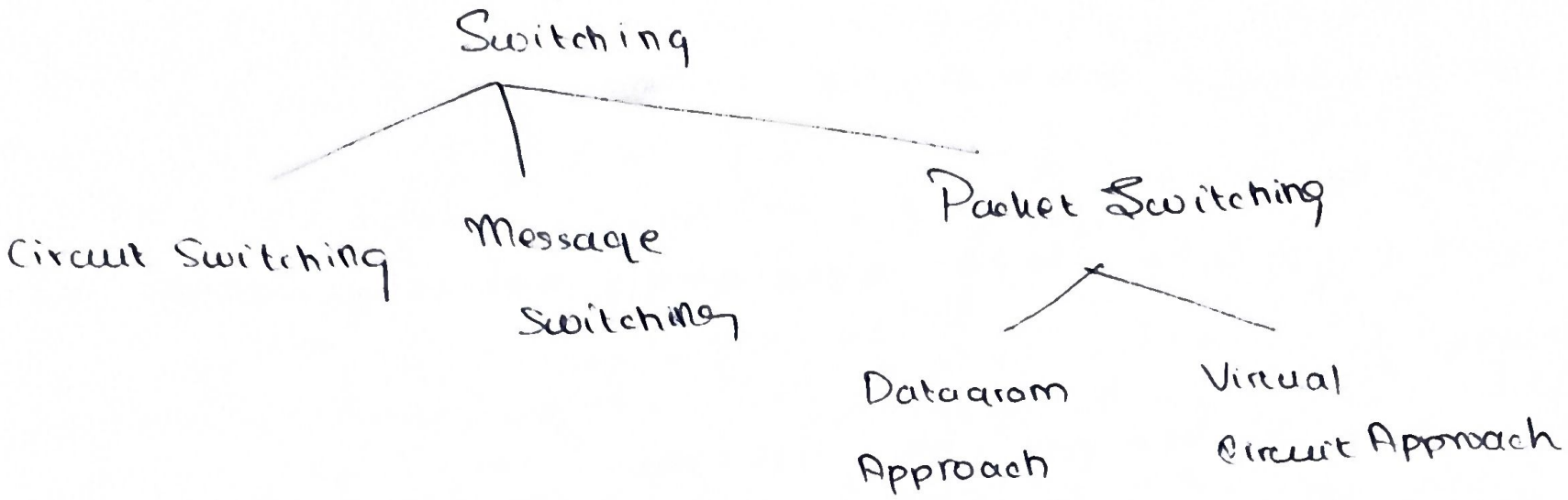
→ channel also subject to fading and no coverage holes.

---

* Protocol Data Unit (PDU)



* Switching? - The process of forwarding packets coming in from one port to another is called switching

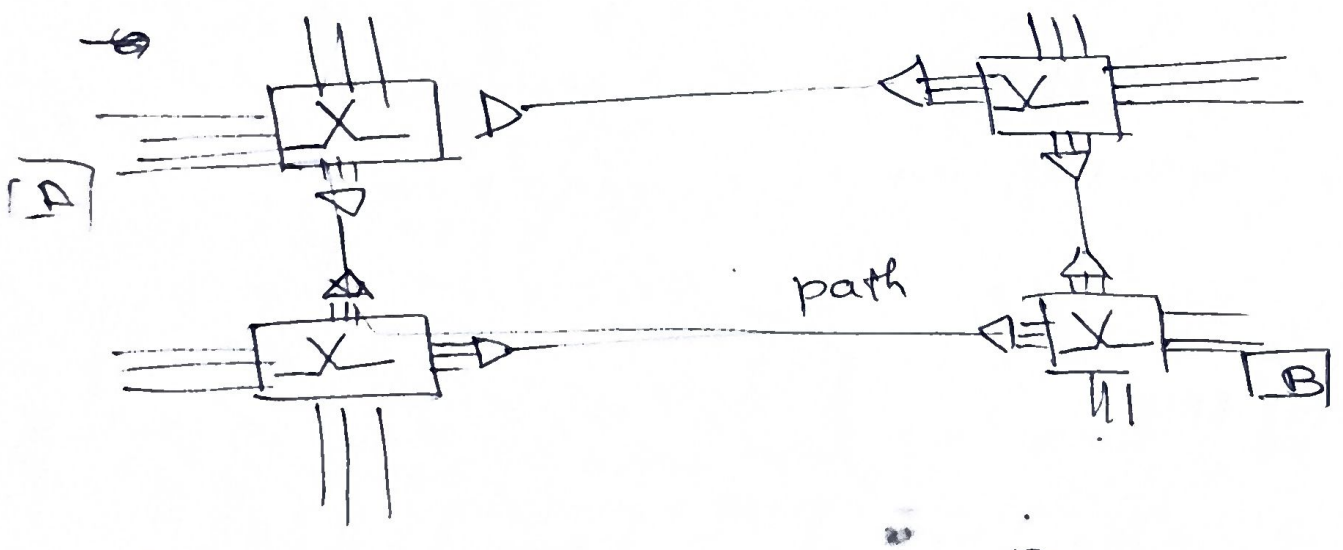


(A) Circuit Switching?

→ dedicated path between sender and receiver

→ has 3 phases connection establishment, data transfer, disconnection

→ each connection uses only one dedicated channel



Advantages

→ committed data transfer

→ no delay in data flow

Disadvantages

→ takes a long time to establish connection

→ more bandwidth

→ other data can't be transmitted even if the connection is dedicated.

(B) Message Switching

→ store and forward mechanism

→ message is transferred as a whole unit

→ not suitable for streaming media & real-time applications

→ can be used in telegraph & mail forwarding

Advantages

→ can store when a communication channel is not available,

helps reduce traffic

→ Can shared data channels,

can assign priorities

Disadvantages

→ cannot be used in real time applications because of delay

→ needs large storage capacity

(C) Packet Switching

→ Internet is a type of packet switching

→ msg. is broken into individual chunks called packet - each packet is sent individually

→ It has a source, dest IP & a seq. no.

→ The sequence number helps the receiver to

- reorder packet
- find missing packet
- send acknowledgements

Packet Switching

Data gram Approach

→ connectionless switching

→ each entity called a datagram

→ no fixed path

→ intermediate nodes takes decisions on forwarding

no congestion

flexible

Virtual Circuit

→ connection oriented switching

→ pre-planned route

→ path is fixed during logical connection

may have congestion

not flexible

Advantages

→ less delay

→ no need large storage

→ not hindered by link failure

→ allow simultaneous channel usage

→ better bandwidth usage

Disadvantages

→ complex protocols

→ routing delay

→ may cause errors