31/7/24

ASSIGNMENT 1

Unit-1 Introduction to Data communication

Q.1 Define the term : Data Communication.

—4 Data communication is the exchange of data between two or more devices through any transmission medium. This process involves the transfer of digital or analog data using methods such as wired cables, wireless signals or optical fibres. The primary goal ~~is~~ of data communication is to ensure that the transmitted data is accurately and reliably delivered from the source to the destination. Key elements of data communication include the sender, receiver, transmission medium, and communication protocols.

Q.2 Briefly describe the five components of data communication.

—4 The five components of data communication are:

i) Message

The actual data or information that is being communicated. This can be text, numbers, images, audio or video.

ii) Sender

The device or entity that initiates the communication by transmitting the

message. Examples include computers, mobile phone and sensors.

iii) Transmission Medium

The physical or wireless path through which the data travels from the sender to the receiver. Examples include twisted pair cables, coaxial cables, fibre optic cables and wireless signals. (radiowaves, microwaves).

iv) Receiver

The device or entity that receives the transmitted data. It interprets and processes the incoming information. The receiver can be another computer, a server, a printer or any device designed to accept data.

v) Protocol

A set of rules and conventions that govern how data is transmitted and received. Protocols ensure that the sender and receiver understand each other and can correctly encode, transmit and decode the data. Examples include TCP/IP, HTTP and FTP.

Q.3. What is a network? Describe network criteria.

→ A Network is a collection of interconnected devices and systems that communicate with each other to share resources, exchange data and enable various forms of electronic communication. They can be classified based on their size, type and scope, such as LAN, WAN and MAN.

→ For a network to be efficient and effective, it must meet several criteria :

i) Performance

- Throughput : The amount of data successfully transmitted over the network in a given time period.
- Latency : The time it takes for data to travel from the sender to the receiver, also known as delay.
- Bandwidth : The maximum rate at which data can be transferred over the network.
- Error Rate : The number of errors that occur in the transmitted data.

ii) Reliability

- Availability : The network's ability to be operational and accessible when needed.
- Fault Tolerance : The network's capability to continue functioning correctly even in

the event of component failures.

- Recovering Time: The time it takes for the network to recover from failures or disruptions.

iii) Scalability

The network's ability to grow and handle an increasing number of devices or higher amounts of traffic without degrading performance.

iv) Security

- Confidentiality: Ensuring that data is accessible only to authorized users.
- Integrity: Ensuring that data is not altered or tampered with during transmission.
- Availability: Protecting the network and its services from disruptions and ensuring they are accessible to legitimate users.

v) Cost

- Initial Setup Cost: The expense involved in establishing the network infrastructure, including hardware, software and installation.
- Maintenance Cost: The ongoing expenses for ~~maint~~ managing, supporting and upgrading the network.
- Operational Cost: The cost of running the

network, including power consumption, administration and support.

Q.4 What is network topology? Explain different network topologies with examples and compare them.

→ Network topology refers to the arrangement or layout of various elements (link, nodes) in a computer network. It describes how different devices (nodes) are connected and how data flows through the ~~data flows~~ network. They can be physical, depicting the actual layout of the cables and devices, or logical, representing the way data travels regardless of the physical design.

→ Different Network Topologies are :-

i) Bus Topology

All devices are connected to a single central cable, known as the bus or backbone. Data sent by one device is available to all other devices on the network. eg: Early Ethernet Networks.

Adv: Easy to install and extend. Requires less cable length than other topologies.

Disadv: Difficult to ~~understand~~ troubleshoot. A failure in the central bus can bring down the entire network. Limited by the length of the central cable.

ii) Star Topology

All devices are connected to a central hub or switch. The hub act as a repeater for data flow. eg: Most home and office networks using Ethernet.

- Advantages :-
  - Easy to Install and manage.
  - Failure of one device ~~an~~ does not affect the rest of the network.
  - Easy to detect faults and remove problematic devices.

- Disadvantages :-
  - Requires more cable than bus topology.
  - The hub or switch represents a single point of failure.

iii) Ring Topology.

Each device is connected to ~~it~~ two other devices, forming a circular pathway for signals. Data travels in one direction (or sometimes in both direction) throug the ring. eg: Some implementations of Token Ring networks.

Advantages

- Data packets travel at high speed.
- No data collisions due to the unidirectional flow.

- Disadvantages :-
  - Failure of a single device can disrupt the entire network.
  - Difficult to troubleshoot and reconfigure.

iv) Mesh Topology.

Every device is connected to every other device in the network. It can be a full mesh (where every device is directly connected to every other device) or a partial mesh (where only some devices have multiple connections). eg: Networks requiring high reliability, such as military communications.

- Advantages :-
  - High fault tolerance
  - Data can be rerouted in case of a link failure.

- Disadvantages :-
  - Expensive to implement due to the high number of connections.
  - Complex to configure and manage.

v) Tree Topology.

A combination of star and bus topologies. Groups of star-configured network are connected to a central bus backbone. eg: Hierarchical networks used in large organizations.

- Advantages :-
  - Scalable and easy to expand.
  - Hierarchical structure allows for better organization.

- Disadvantages :-
  - If the backbone fails, the entire network segment can fail
  - Requires more cable and can be more complex to configure.

vi) Hybrid ~~Tp~~ Topology.

A combination of two or more different topologies to form a more complex network. eg: A large corporate network combining star, ring and mesh topologies

- Advantages :-
  - Flexible and ~~Scalr~~ Scalable.
  - Can be designed to meet specific network requirements.

- Disadvantages :-
  - Complex to design and implement.
  - Can be expensive due to the combination of different topologies.

	Bus	Ring	Star	Mesh	Tree
Means	Every computer & network device is connected to single cable	Each computer is connected to another, with last one connected to the first	All the computers are connected to a single hub through a cable.	All the networks nodes are connected to each other	It has a root node and all other nodes are connected to it forming a hierarchy
Cost	Average	Cheap	High	High	High
Used in	Small Network	Expand Network	Small Network	Expand Network	Expand Network
Trouble Shoot	Easy; but cables fail then whole network fails	Difficult; Failure of one computer disturbs the whole network	Easy; If the hub fails then the whole network is down	Difficult; Installation and configuration is difficult	Easy; central root hub fails, network fails.

Q.5 Explain OSI model with its layer in detail.

—↓ The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and standardize the functions of a telecommunication or computing system. It ensures interoperability between different systems and technologies by providing a universal set of standards for data communication. It divides the

communication process into seven layers:

1. Physical Layer (layer-1)

Deals with the physical connection between devices, including the transmission and reception of raw ~~bitsre~~ bitstreams over a physical medium.

- Defines hardware specifications (electrical, ~~mechir~~ mechanical, procedural, etc)
- Handles bit synchronization, signal amplitude and data rate
- Transmits raw data bits (0s and 1s)

eg: Ethernet cables, fiber optics, radio frequencies

2. Data Link Layer (layer-2)

Provides node-to-node data transfer, error detection and correction and flow control.

- Framing: Encapsulating data packets into frames for transmission
- MAC (Media Access Control): Determines who can use the communication channel at a given time.
- Detects and corrects errors in data transmission.

eg: Ethernet, Wi-Fi, MAC addresses.

3. Network Layer (layer-3)

Manages device addressing, tracks the location of devices on the network and

determines the best way to move data. (End-to-End)
- Routing: Selecting optimal path for data packets.
- logical Addressing: Assigning unique IP addresses to devices.
- Packet Forwarding: Transmitting data packets across different networks.

eg: IP, routers.

4. Transport Layer (layer-4)

Ensures reliable data transfer between end systems with error recovery and flow control.
- Breaks down large data streams into smaller segments and reassembling them at the destination.
- Establishes, maintains and terminates connection
- Ensures data integrity.

eg: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

5. Session Layer (layer-5)

Manages sessions between applications, ensuring data is properly synchronized and organized.
- Establishes, manages and terminates session.
- Managing ~~dat~~ dialog control and synchronization
- Organizing data exchange and coordinating communication.

eg: NetBIOS, RPC (Remote Procedure Call)

6. Presentation Layer (layer - 6)

Translates data between the application and network layer, ensuring data is in a usable format.

- Converting data between different formats.
- Reducing the size of data to optimize transmission.
- Securing data for transmission and making it readable upon receipt.

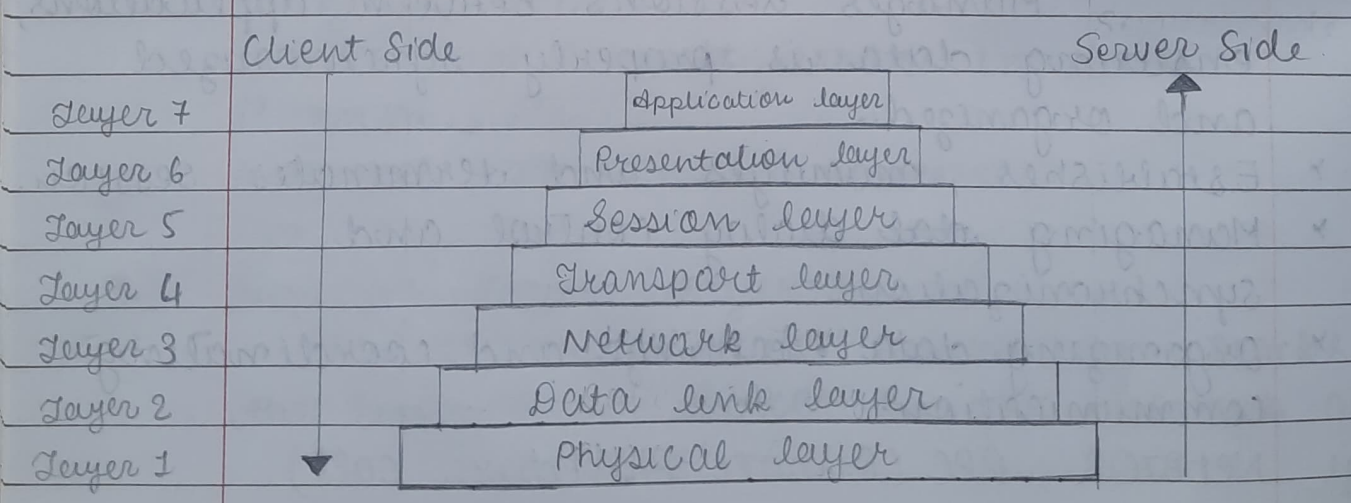
eg: JPEG, GIF, SSL/TLS encryption.

7. Application layer (layer - 7)

Provides network services directly to end-user applications, facilitating communication with the network.

- Enables application to communicate over the network.
- Implementing protocols that directly interact with user applications.
- Handles user interactions with network applications.

eg: HTTP, FTP, SMTP, DNS.



Q.6 Explain TCP/IP model with its layer in detail.

→ The TCP/IP (Transmission Control Protocol/ Internet Protocol) model is a conceptual framework used to standardize and guide the design and implementation of network communication protocols. It is the foundation of the internet and most modern networks. It has four layers :-

1. Network Access Layer (link / Data link layer)
Handles the physical transmission of data over a network. It encompasses the physical and data link layer of OSI model.
- Converting data into bits (digitization)
- Physical transmission of bits over the network medium (cables, wireless)
- Error detection and correction
- Media Access Control (MAC) to manage data transmission over shared media.
- Protocols : Ethernet, Wi-Fi, Bluetooth, Frame Relay & ATM.

2. Internet Layer (Network layer)
Manages the routing of data packets across the network. It determines the best path for data to travel from source to destination
- Responsible for addressing (IP addresses).
- Packet forwading and routing.

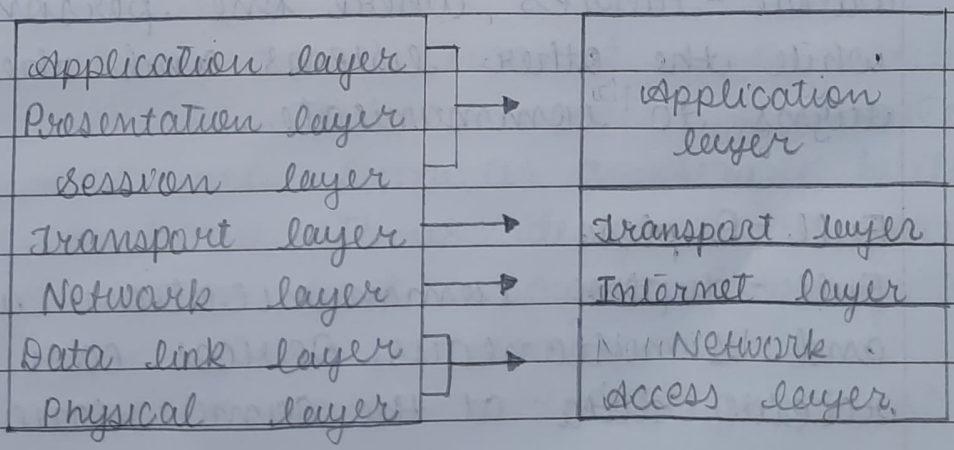
> Fragmentation and reassembly of packets.
- Protocols: IP, ICMP (Internet Control Message Protocol)

3. Transport Layer.
Ensures reliable data transmission between devices. It provides end-to-end communication services.
> Error control and flow control.
> Segmentation and reassembly of data.
> Connection-Oriented (TCP) or connectionless (UDP) services.
> Port addressing.
- Protocols: TCP, UDP.

4. Application Layer.
Provides protocols for specific data communication services on a process-to-process level. It's the closest layer to the user.
> Supports various applications and user services.
> Handles data format and encoding.
> Provides APIs for application development.
- Protocols: HTTP, FTP, SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), Telnet, SSH.

Q.7 Write down the difference between OSI model and TCP/IP model.

	OSI	TCP/IP
>	OSI refers to Open System Interconnection	TCP refers to Transmission control Protocol.
>	It has 7 layers	It has 4 layers.
>	It follows a vertical approach	It follows connectionless a horizontal approach.
>	Here, protocols are better covered and are easy to replace with the technology change	Protocols cannot be replaced easily here.
>	Strictly defined layer functionality	layer functionality can be combined.
>	Theoretical model for standardizing network communication	Practical and implementation - oriented model.



Q.8 Briefly describe following terms in content of data flow:

i) Simplex.

—↓ Simplex communication is unidirectional, meaning data flows in only one direction from the sender to the receiver. The receiver cannot send data back to the sender. In other words, the content is transmitted to a vast audience without requiring direct interaction or feedback.

eg: A traditional radio broadcast, where the radio station transmits signals and the listeners can only receive the signals without sending anything back.

ii) Half - Duplex.

—↓ Half - duplex communication is bidirectional but not simultaneous. Devices can both send and receive data, but not at the same time. When one device is transmitting, the other must wait until the transmission is complete before it can send data.

eg: Walkie - talkies, where one person talks while the other listens and they take turns to communicate.

iii) Full - Duplex.

—↓ Full - duplex communication is bidirectional and simultaneous. Devices can send and receive data at the same time without any

waiting, allowing for a continuous, two-way data flow. It doubles the capacity of the communication channel.

eg: Modern telephones, where both parties can speak and listen simultaneously, enabling a natural conversation flow.

Q.9 What is the physical topology of a network? Explain following physical topologies of network:

i) Mesh ii) Star iii) Bus iv) Ring v) Hybrid.

→ The physical topology of a network refers to the physical layout or arrangement of devices and cables in a network. It defines how different nodes (computers, printers, servers, etc) are interconnected and how data is physically transmitted through the network.

Pg-7

⇒ Types of topologies are same as Question-4.

Q.10 Describe the following types of network:

i) LAN

→ A LAN (Local Area Network) is a network that connects devices within a limited geographic area such as a single building, campus or home. It is designed to facilitate communication and resource sharing between devices in close proximity.

> Scope: limited to a small geographical area.

- Speed: High data transfer rates (typically from 100 Mbps to 10 Gbps).
- Ownership: Usually owned, controlled and managed by a single organization
- Eg: Office, home, school networks.
- Technology: Ethernet, Wi-Fi

iii) WAN

—> A WAN (Wide Area Network) covers a broad geographic area, often connecting multiple smaller networks such as LANs and MANs. WANs are used to connect devices across cities, countries or even continents.

- Scope: Extensive geographical area, spanning large distance.
- Speed: Varies significantly, Typically lower than LAN speeds due to scope.
- Ownership: Typically involves multiple organizations & service providers.
- Eg: The Internet, multinational ~~coorporate~~ corporate networks.
- Technology: MPLS (Multiprotocol Label Switching), leased lines, satellite links.

iii) MAN

—> A MAN (Metropolitan Area Network) spans a city or large campus, providing network coverage larger than a LAN but smaller than a WAN. It is designed to connect multiple LANs within a metropolitan area.

> Scope: Covers a city or a large metropolitan area.
> Speed: Intermediate between LAN and WAN, often ranging from 10 Mbps to 1 Gbps.
> Ownership: Can be owned by a single organization, a consortium or service providers.
> Eg: University campuses, municipal Wi-Fi networks, city-wide networks connecting government offices
> Technology: Fiber optics, Ethernet over fibre, wireless technologies.

Q.11 Explain different types of transmission media.
—4 Transmission media are the physical pathways that connect computers, other devices and people on a network. They can be classified into two broad categories :-

1. Guided (Wired) Media
(i) Twisted Pair Cable.
Consists of pairs of wires twisted together to reduce electromagnetic interference. There are two ~~more~~ types of TPC :
> Unshielded Twisted Pair (UTP) : Commonly used in Ethernet networks and telephone systems.
> Shielded Twisted Pair (STP) : Includes a shielding layer to provide additional protection against interference.

add:- ~> It is cost-effective, easy to install, flexible.
disa:- ~> It has limited bandwidth, & susceptible to electromagnetic interference and crosstalk.
eg: Cat 5, Cat 5e, Cat 6 cables.

(ii) Coaxial Cable.

Consists of a central conductor, insulating layer, metallic shield and outer protective layer (jacket)

Adv:- ~> Higher bandwith than TPC, better resistance to electromagnetic interference.

Dis:- ~> Bulkier and more difficult to install, more expensive than TPC.

eg: Cable television networks, early ethernet networks

(iii) Fiber Optical Cable.

Uses light to transmit data through strands of glass or plastic fibres.

> Single-Mode Fiber (SMF): Supports long-distance communication with a single light path.

> Multi-Mode Fiber (MMF): Supports shorter distances with multiple light paths.

Adv:- ~> Very high bandwith, immune to electromagnetic interference, long distance data transmission

Dis:- ~> Expensive, fragile and difficult to install.

Eg: Backbone network connections, long-distance tele communications.

2. Unguided (Wireless) Media

(i) Radio-Waves

Use radio frequencies to transmit data through the air. Applications are Wi-Fi, Bluetooth, AM/FM radio, television broadcasting.

Adv:- ~> Easy to set up, suitable for mobile devices.

Dis:- ~> limited range, susceptible to interference and security issues.

(ii) Microwaves

use higher frequency radio waves for point-to-point communication.

> Terrestrial : use ground-based dishes for line-of-sight communication.

> Satellite : use satellites for long-distance communication.

Adv:- ~> High bandwidth, long-distance communication

Dis:- ~> Requires line-of-sight, affected by weather.

(iii) Infrared

uses infrared light to transmit data over short distances. Applications are remote controls, short-range communication between devices.

Adv:- ~> High data rate, secure ~~(line-of-sight required)~~

Dis:- ~> Short range, requires direct line-of-sight, affected by environment factors. (sunlight).

Q.12 what is protocol? what are elements of protocol in content of data communication?

—> A protocol is a set of rules and conventions that define how data is transmitted and received over a network. They ensure that devices ~~are~~ can communicate effectively and accurately, regardless of their underlying hardware or software differences.

—4 Elements of a Protocol :-

i) Syntax : Defines the structure or format of data, it such as how data is packaged and organized, including the data's bit pattern, coding and format.

eg: Frame formats in Ethernet, header and trailer formats.

ii) Semantics : Determines the meaning of each piece of data within a message. It defines the control information and error handling procedures, specifying what actions are to be taken based on the data.

eg: Control information such as start and stop signals in data transmission.

iii) Timing : Specifies when data should be sent and received, including synchronization and flow control mechanisms. Also how fast the data should be sent.

eg: The timing of signals in a serial communication link, where specific bit rate (baud rates eg : 9600 baud) define the timing of bit transmission.

iv) Error Control : Includes ensuring the integrity of data during transmission by detecting and correcting errors.

eg: Checksums, Cyclic Redundancy Checks (CRC).

and Automatic Repeat Request (ARQ).

v) Security: Defines measures to protect data integrity, confidentiality and authenticity. It protects data during transmission from unauthorized access, tampering and ~~ev~~ eavesdropping.

eg: In HTTPS (HTTP Secure), security is provided through SSL/TLS (Secure Sockets layer/ Transport layer Security) protocols, which encrypt data between the client and server to protect against tampering and eavesdropping.