UNIT I

Basic Concepts: Components of data communication, distributed processing, standards and organizations. Line configuration, topology, Transmission mode, and categories of networks.

OSI and TCP/IP Models: Layers and their functions, comparison of models.

Digital Transmission: Interfaces and Modems: DTE-DCE Interface, Modems, Cable modems.

components of data communication network

1. Data
2. Sender
3. Receiver
4. Transmission Medium
5. Protocol

Data communication is the process of **transmitting data from a sender to a receiver through a transmission medium using a set of rules called protocols**.
The **five basic components** of data communication are:

---

1. Data (Message)

- **Data** is the information that needs to be transmitted from one device to another.
- It is the **actual content** being communicated.
- Data can be in different forms:
  - **Text**
  - **Audio**
  - **Video**
  - **Image**
  - **Combination of these forms**

Example: Sending a text message from one mobile phone to another.

---

2. Sender

- The **sender** is the device that **sends or transmits the data**.
- It is also called the **source**.
- Examples:
  - Computer
  - Mobile phone
  - Video camera
  - Server

Example: If you send a message from your mobile phone, your mobile phone is the **sender**.

3. Receiver

- The **receiver** is the device that **receives the transmitted data**.
- It is also called the **destination**.
- Examples:
  - Computer
  - Mobile phone
  - Server
  - Video camera

Example: If your friend receives the message on their mobile phone, their mobile phone is the **receiver**.

---

4. Transmission Medium

- A **transmission medium** is the **path through which data travels** from the sender to the receiver.
- It can be **wired or wireless**.
- Examples of wired media:
  - **Twisted-pair cable**
  - **Coaxial cable**
  - **Fiber-optic cable**
- Examples of wireless media:
  - **Radio waves**
  - **Microwaves**
  - **Infrared**

Example: In a wired network, an Ethernet cable can act as the **transmission medium**.

---

5. Protocol

- A **protocol** is a **set of rules** that controls communication between devices.
- It defines **how data is transmitted and received**.
- Protocols help devices understand and communicate with each other correctly.
- A protocol may define:
  - How data should be sent
  - How data should be received
  - How errors are handled
  - How successful delivery is confirmed
  - How communication is controlled

Example: TCP/IP is a widely used protocol suite for communication over computer networks.

Distributed Processing

- **Distributed processing** is a method in which a **large task or process is divided into smaller tasks**.
- These smaller tasks are processed by **multiple computers** instead of a single computer.
- Each computer handles a **specific part or subset of the overall task**.
- The computers communicate and **share data or resources** through a network.
- This reduces the workload on a single computer and can improve **performance and reliability**.

Example

- In a **banking system**, different computers may handle:
  - One computer → Customer information
  - Another computer → Account transactions
  - Another computer → ATM transactions
- Together, these computers perform the complete banking process.

In Simple Words

Distributed processing means dividing a task among multiple networked computers, where each computer performs a part of the task.

Standards and Organizations in Computer Networking

What are Networking Standards?

- **Networking standards** are a set of **rules and specifications** used in computer networks.
- They define how **devices, hardware, and software communicate** with each other.
- Standards allow products from **different vendors/manufacturers** to work together.

Why are Standards Needed?

- The **primary purpose** of networking standards is **interoperability**.
- They ensure that hardware and software from different vendors can **communicate and exchange data**.
- Without standards, connecting devices from different manufacturers would be **difficult or sometimes impossible**.

Advantages of Networking Standards

- **Interoperability**
  - Different devices and software can work together.
- **Vendor Independence**
  - Users are not forced to purchase products from a single vendor.
- **More Competition**
  - Multiple companies can develop compatible networking products.
- **Lower Cost**
  - Competition between vendors helps to **reduce prices**.
- **Easy Development**
  - Hardware and software can be developed **layer by layer** using standard rules.
- **Network Connectivity**
  - Different networks can be connected and can **share information easily**.

Example

- **TCP/IP** is a widely used networking standard/protocol suite.
- Devices from companies such as **Cisco, Dell, HP, and others** can communicate when they follow common networking standards.

Organizations Involved in Computer Networking Standards

Some important organizations are:

- **ISO** – International Organization for Standardization
- **IEEE** – Institute of Electrical and Electronics Engineers
- **ITU-T** – International Telecommunication Union – Telecommunication Standardization Sector
- **IETF** – Internet Engineering Task Force
- **W3C** – World Wide Web Consortium
- **ANSI** – American National Standards Institute
- **EIA** – Electronic Industries Alliance
- **TIA** – Telecommunications Industry Association

Important for Exams

- **ISO** → OSI Model
- **IEEE** → LAN/WLAN standards such as **Ethernet (802.3)** and **Wi-Fi (802.11)**
- **IETF** → Internet standards and **TCP/IP protocols**
- **ITU-T** → Telecommunication standards

- **W3C** → Web standards such as **HTML, CSS, and Web APIs**

Line Configuration in Computer Networks

- **Line configuration** refers to the way **two or more communication devices are connected to a communication link**.
- A **link** is the physical or wireless communication path through which data travels from one device to another.
- Line configuration describes **how devices are attached to and share the link**.

Types of Line Configuration

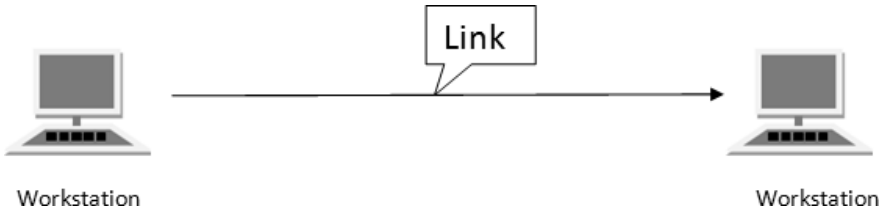
There are **two main types**:

1. **Point-to-Point**
2. **Multipoint (Multidrop)**

---

1. Point-to-Point

- A **point-to-point** line configuration provides a **dedicated link between exactly two devices**.
- The **entire capacity of the link** is reserved for communication between these two devices.
- No other device shares the link.
- It can use:
  - Twisted-pair cable
  - Coaxial cable
  - Fiber-optic cable
  - Microwave
  - Satellite communication



Example

- A direct connection between **two computers**.
- An **infrared remote control and a TV** can also be considered a point-to-point communication example.

Simple Representation

```
Device A ———————— Device B
```

2. Multipoint (Multidrop)

- A **multipoint** line configuration is one in which **more than two devices share a single link**.
- The capacity of the communication channel is **shared among multiple devices**.
- It is also called a **multidrop configuration**.

Simple Representation

```
        Device B
           |
Device A ——┼—— Device C
           |
        Device D
```

There are two ways in which the link can be shared:

A. Spatial Sharing

- Multiple devices **use the link at the same time**.
- The available channel capacity is divided among the devices.

Key Point:
Spatial sharing = Multiple devices share the link simultaneously.

B. Temporal (Time) Sharing

- Devices **take turns** using the communication link.
- Only one device uses the link at a particular time.

Key Point:
Temporal sharing = Devices share the link by taking turns.

Transmission Modes in Computer Networks

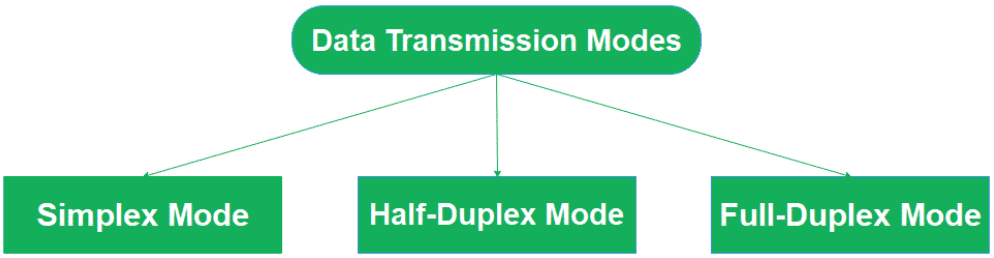
Introduction

- **Transmission mode** (also called **communication mode**) defines the **direction of data flow between two communicating devices**.
- It tells us **how data is transmitted between the sender and receiver** through a communication channel.
- A communication channel can be:
  - **Copper cables**
  - **Optical fiber**
  - **Wireless channels**
  - Other transmission media
- Data can be transmitted in the form of **electrical, optical, or electromagnetic signals**, depending on the transmission medium.
- Transmission modes are commonly classified based on the **direction of data flow**.

Types of Transmission Modes

There are **three main types** of transmission modes:

1. **Simplex**
2. **Half-Duplex**
3. **Full-Duplex**



---

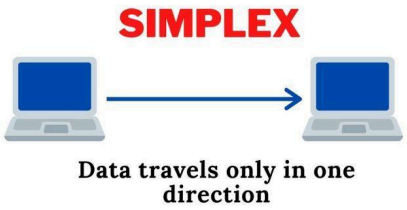
1. Simplex Mode

- Data flows in **only one direction**.
- One device always acts as the **sender**, and the other always acts as the **receiver**.
- The receiver **cannot send data back** to the sender through the same communication channel.

Example:

- Keyboard → Computer
- Television broadcasting → TV

```
Sender ──────────► Receiver
```



Key Point:
Simplex = One-way communication

---

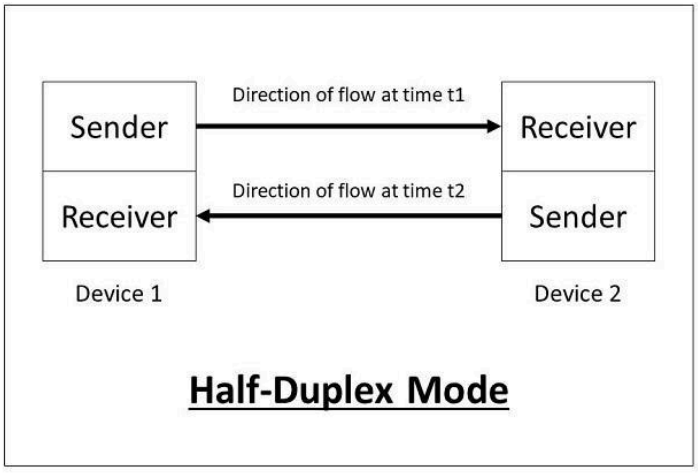
2. Half-Duplex Mode

- Data can flow in **both directions**, but **not at the same time**.
- Devices take **turns** sending and receiving data.
- When one device is transmitting, the other device must receive.

Example:

- Walkie-talkie

```
Device A ──────────► Device B
         ◄──────────
```



Key Point:
Half-Duplex = Two-way communication, but one direction at a time

---

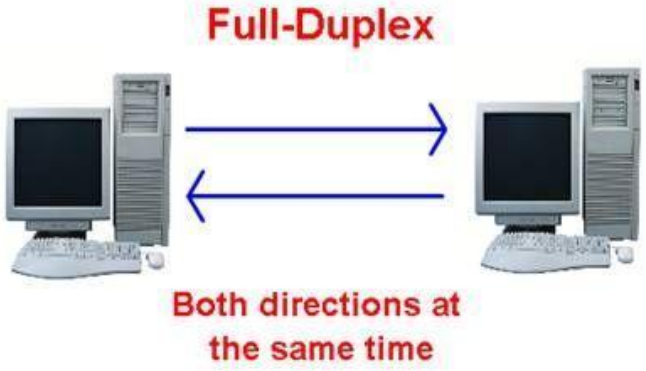
3. Full-Duplex Mode

- Data can flow in **both directions simultaneously**.
- Both devices can **send and receive data at the same time**.
- It provides more efficient communication than half-duplex.

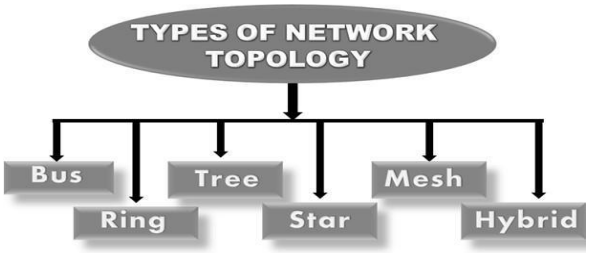
Example:

- Telephone/mobile phone conversation
- Video calls

```
Device A ◄──────────► Device B
         Simultaneously
```

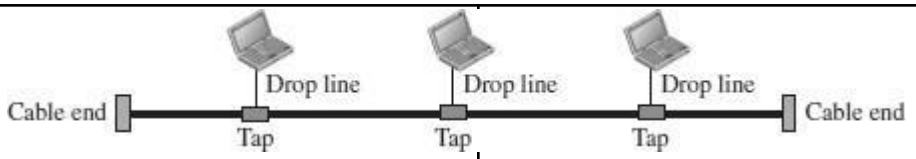


Key Point:
Full-Duplex = Two-way communication at the same time



BUS TOPOLOGY

- Bus topology is a network type in which every computer and network device is connected to single cable.
- The long single cable acts as a backbone to link all the devices in a network.
- When it has exactly two endpoints, then it is called **Linear Bus topology.**
- It transmits data only in one direction.



Advantages of Bus Topology

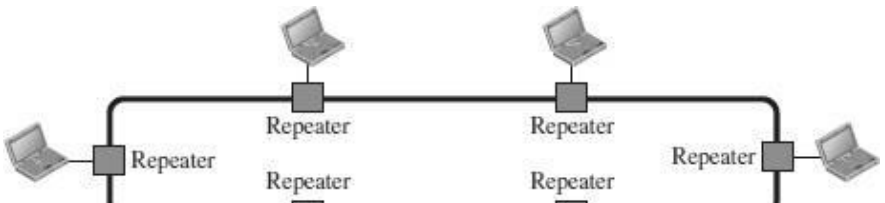
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more, the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

RING TOPOLOGY

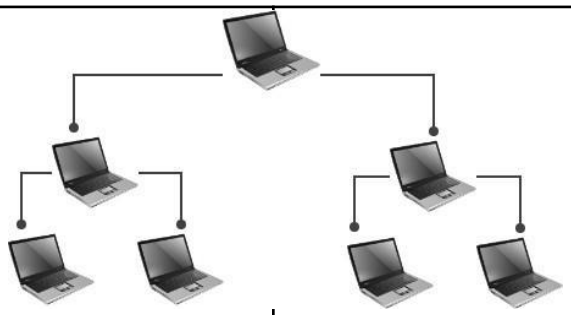
- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater.
- When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages of Ring Topology	***Disadvantages of Ring Topology***
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data. 2. Cheap to install and expand	1. Troubleshooting is difficult in ring topology. 2. Adding or deleting the computers disturbs the network activity. 3. Failure of one computer disturbs the whole network

TREE TOPOLOGY

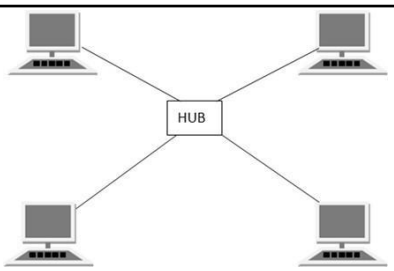
- It has a root node and all other nodes are connected to it forming a hierarchy.
- It is also called hierarchical topology.
- It should at least have three levels to the hierarchy.
- Tree topology is ideal if workstations are located in groups.
- They are used in Wide Area Network.



Advantages of Tree Topology	***Disadvantages of Tree Topology***
1. Extension of bus and star topologies. 2. Expansion of nodes is possible and easy. 3. Easily managed and maintained. 4. Error detection is easily done.	1. Heavily cabled. 2. Costly. 3. If more nodes are added maintenance is difficult. 4. Central hub fails, network fails.

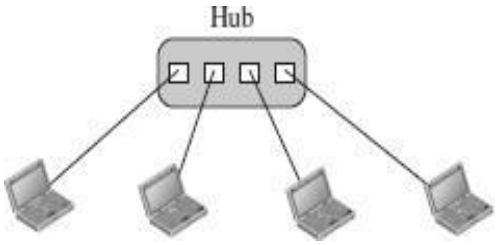
STAR TOPOLOGY

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- The devices are not directly linked to one another.
- The controller acts as an exchange.
- If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.



Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly

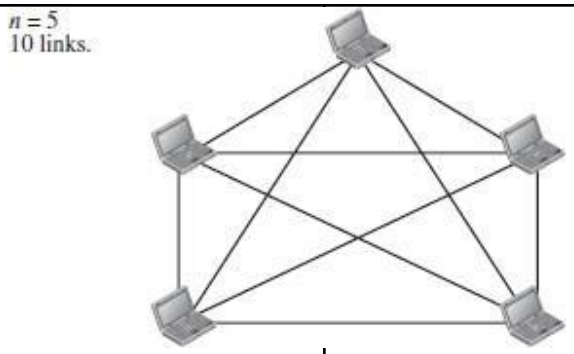


Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails, then the whole network is stopped.
4. Performance is based on the hub that is it depends on its capacity

MESH TOPOLOGY

- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The term dedicated means that the link carries traffic only between the two devices it connects.
- The number of physical links in a fully connected mesh network with *n* nodes is given by $n\ (n-1)\ /\ 2$.



Advantages of Mesh Topology

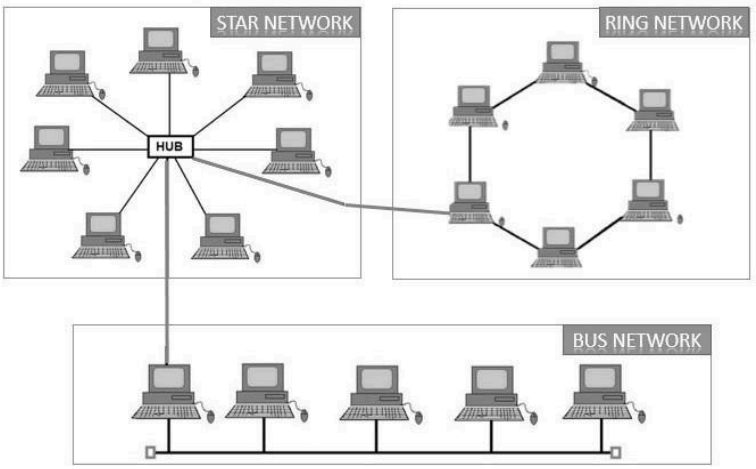
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

HYBRID TOPOLOGY

- Hybrid Topology is a combination of one or more basic topologies.
- For example if one department in an office uses ring topology, the other departments uses star and bus topology, then connecting these topologies will result in Hybrid Topology.
- Hybrid Topology inherits the advantages and disadvantages of the topologies included.



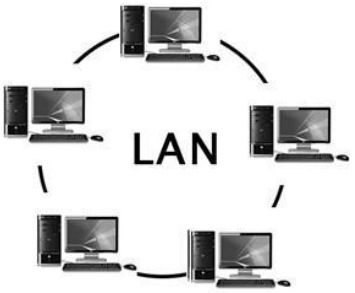
Advantages of Hybrid Topology	***Disadvantages of Hybrid Topology***
1. Reliable as Error detecting and trouble shooting is easy. 2. Effective. 3. Scalable as size can be increased easily. 4. Flexible.	1. Complex in design. 2. Costly

NETWORK TYPES

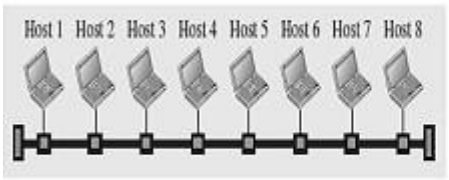
- A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
- A computer network can be categorized by their size.
- A computer network is mainly of three types:
    1. Local Area Network (LAN)
    2. Wide Area Network (WAN)
    3. Metropolitan Area Network (MAN)

LOCAL AREA NETWORK (LAN)

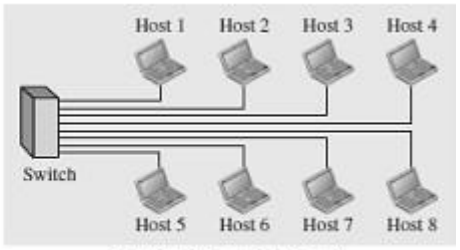
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.



- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- LAN can be connected using a common cable or a Switch.



a. LAN with a common cable (past)



b. LAN with a switch (today)

Advantages of LAN

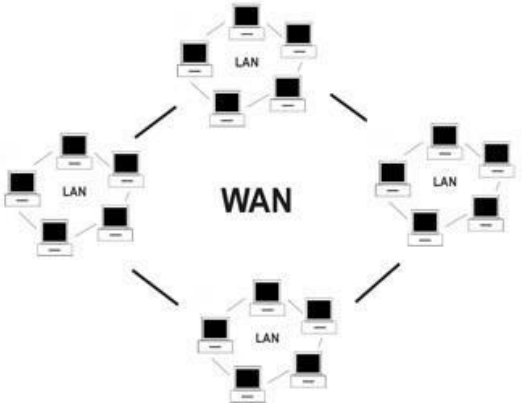
- Resource Sharing
- Software Applications Sharing.
- Easy and Cheap Communication
- Centralized Data.
- Data Security
- Internet Sharing

Disadvantages of LAN

- High Setup Cost
- Privacy Violations
- Data Security Threat
- LAN Maintenance Job
- Covers Limited Area

WIDE AREA NETWORK (WAN)

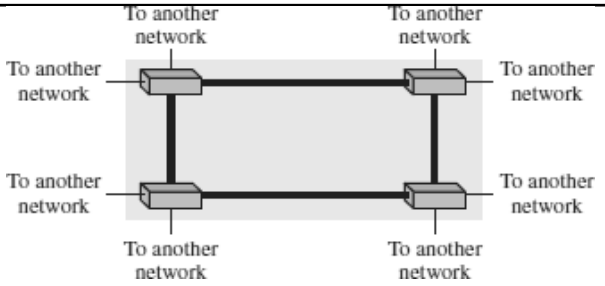
- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.



- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.
- WAN can be either a point-to-point WAN or Switched WAN.

Point-to-point WAN

Switched WAN



***Advantages of Wide Area Network*:**

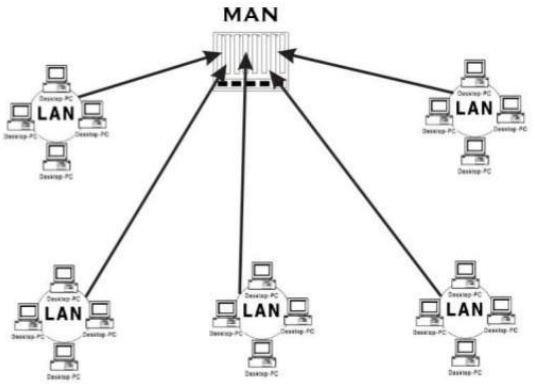
- Large Geographical area
- Centralized data
- Exchange messages
- Sharing of software and resources
- High bandwidth

***Disadvantages of Wide Area Network*:**

- Security issue
- Needs Firewall & antivirus software
- High Setup cost
- Troubleshooting problems

METROPOLITAN AREA NETWORK (MAN)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- It generally covers towns and cities (50 km)
- In MAN, various LANs are connected to each other through a telephone exchange line.
- Communication medium used for MAN are optical fibers, cables etc.
- It has a higher range than Local Area Network(LAN).It is adequate for distributed computing applications.



PROTOCOL LAYERING

- In networking, a protocol **defines the rules** that both the sender and receiver and all intermediate devices need to follow to be able **to communicate effectively**.
- A protocol provides a communication service that the process use to exchange messages.
- 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, in which case we need a protocol at each layer, or **protocol layering.**
- Protocol layering is that it allows us to separate the services from the implementation.
- A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer.
- Any modification in one layer will not affect the other layers.

Basic Elements of Layered Architecture

- **Service:** It is a set of actions that a layer provides to the higher layer.
- **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
- **Interface:** It is a way through which the message is transferred from one layer to another layer.

Features of Protocol Layering

1. **It decomposes the problem of building a network** into more manageable components.
2. **It provides a more modular design**.

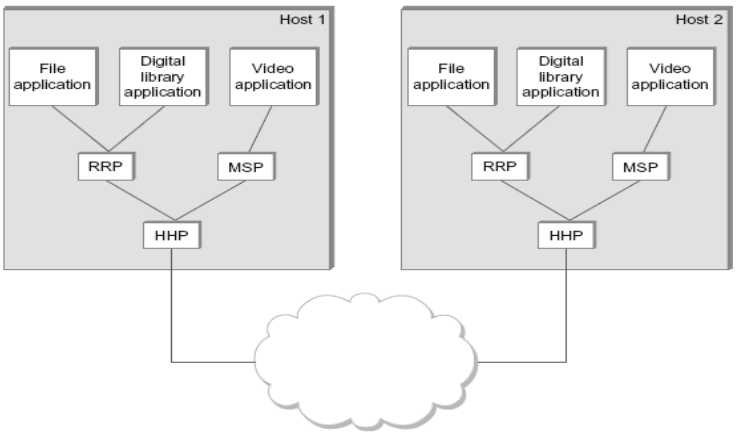
Principles of Protocol Layering

1. 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.
2. The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.

Protocol Graph

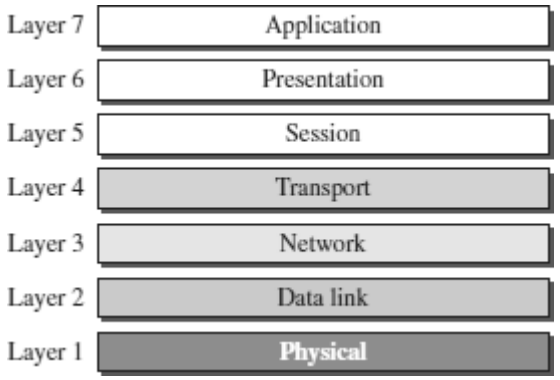
- The set of protocols that make up a network system is called a **protocol graph**.
- The nodes of the graph correspond to protocols, and the edges represent a dependence relation.
- For example, the Figure below illustrates a protocol graph consists of protocols ***RRP (Request/Reply Protocol)*** and ***MSP (Message Stream Protocol)*** implement

two different types of process-to-process channels, and both depend on the ***HHP (Host-to- Host Protocol)*** which provides a host-to-host connectivity service



OSI MODEL

- OSI stands for **Open System Interconnection.**
- It is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.



ORGANIZATION OF THE OSI LAYERS

The OSI model is divided into two layers: **upper layers and lower layers**.

UPPER LAYERS

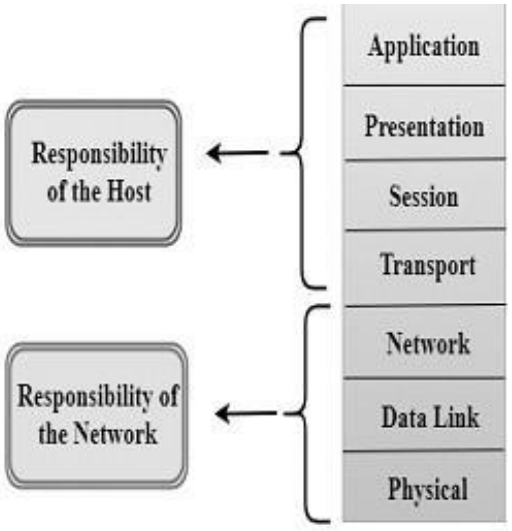
(Responsibility of the Host)

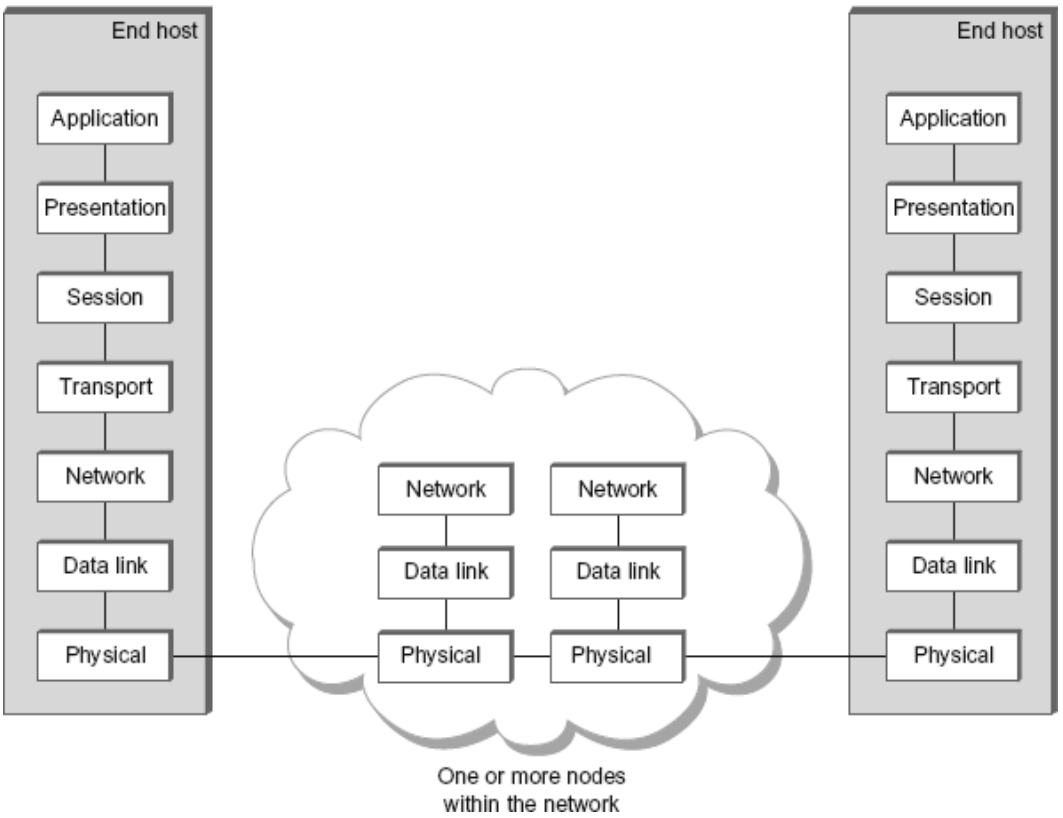
The upper layers of the OSI model mainly deals with the application related issues. They are implemented only in the software.

LOWER LAYERS

(Responsibility of the Network)

The lower layers of the OSI model deals with the data transport issues. They are implemented in hardware and software.





FUNCTIONS OF THE OSI LAYERS

1. PHYSICAL LAYER

The physical layer coordinates the functions required to **transmit a bit stream over a physical medium.**
The physical layer is concerned with the following functions:

- **Physical characteristics of interfaces and media -** The physical layer defines the characteristics of the interface between the devices and the transmission medium.
- **Representation of bits -** To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.
- **Signals:** It determines the type of the signal used for transmitting the information.
- **Data Rate or Transmission rate -** The number of bits sent each second –is also defined by the physical layer.
- **Synchronization of bits -** The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.
- **Line Configuration -** In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.
- **Physical Topology -** The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, bus, star or ring topology.

- **Transmission Mode -** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex or full-duplex.

2. DATA LINK LAYER

It is responsible for **transmitting frames from one node to the next node**.
The other responsibilities of this layer are

- **Framing -** Divides the stream of bits received into data units called frames.
- **Physical addressing** – If frames are to be distributed to different systems on the network , data link layer adds a header to the frame to define the sender and receiver.
- **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow ctrl mechanism.
- **Error control**- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Medium Access control** -Used to determine which device has control over the link at any given time.

3. NETWORK LAYER

This layer is responsible for the **delivery of packets from source to destination**.
It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
The other responsibilities of this layer are

- **Logical addressing** - If a packet passes the network boundary, we need another addressing system for source and destination called logical address. This addressing is used to identify the device on the internet.
- **Routing** – Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

4. TRANSPORT LAYER

It is responsible for **Process to Process** delivery. That is responsible for source-to-destination (end-to-end) delivery of the entire message, It also ensures whether the message arrives in order or not.
The other responsibilities of this layer are

- **Port addressing / Service Point addressing** - The header includes an address called port address / service point address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.

- **Connection control** - This can either be **connectionless or connection oriented.**
  - The connectionless treats each segment as an individual packet and delivers to the destination.
  - The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
- **Flow control** - The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error Control -** Error control is performed end-to-end rather than across the single link..

5. SESSION LAYER

This layer **establishes, manages and terminates connections between applications**.
The other responsibilities of this layer are

- **Dialog control** - Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization**- Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6. PRESENTATION LAYER

It is concerned with the **syntax and semantics of information exchanged between two systems.**
The other responsibilities of this layer are

- **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.
- **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.
- **Compression and expansion**-Compression reduces the number of bits contained in the information particularly in text, audio and video.

7. APPLICATION LAYER

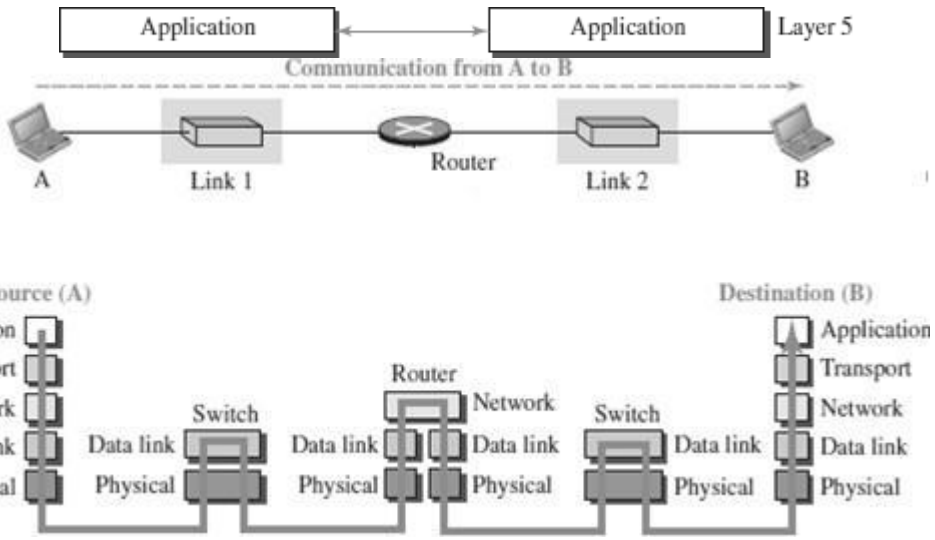
This layer **enables the user to access the network**. It handles issues such as network transparency, resource allocation, etc. This allows the user to log on to remote user.
The other responsibilities of this layer are

- **FTAM (File Transfer, Access, Management)** - Allows user to access files in a remote host.
- **Mail services** - Provides email forwarding and storage.

- **Directory services** - Provides database sources to access information about various sources and objects.

TCP / IP PROTOCOL SUITE

- The TCP/IP architecture is also called as Internet architecture.
- It is developed by the US Defense Advanced Research Project Agency (**DARPA**) for its packet switched network (**ARPANET**).
- TCP/IP is a protocol suite used in the Internet today.
- It is a 4-layer model. The layers of TCP/IP are
    1. **Application layer**
    2. **Transport Layer (TCP/UDP)**
    3. **Internet Layer**
    4. **Network Interface Layer**



APPLICATION LAYER

- An application layer incorporates the function of top three OSI layers. An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- Protocols such as FTP, HTTP, SMTP, POP3, etc running in the application layer provides service to other program running on top of application layer

TRANSPORT LAYER

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.
  - **UDP** – UDP provides connectionless service and end-to-end delivery of transmission. It is an unreliable protocol as it discovers the errors but not specify the error.
  - **TCP** – TCP provides a full transport layer services to applications. TCP is a reliable protocol as it detects the error and retransmits the damaged frames.

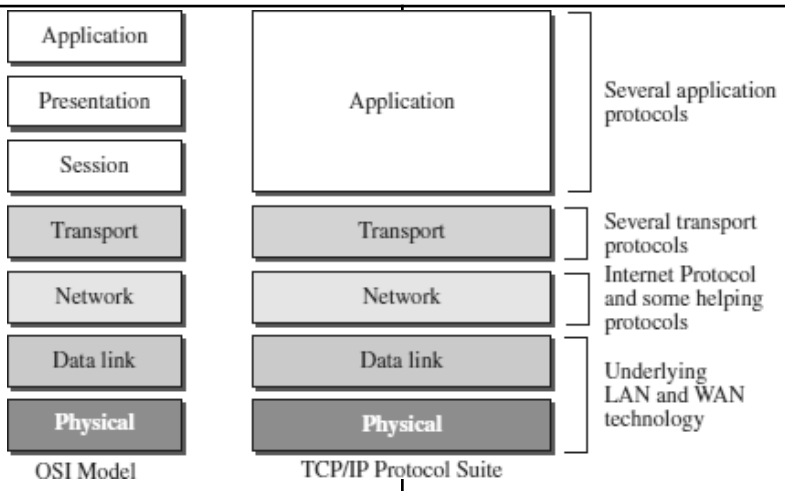
INTERNET LAYER

- The internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- Internet layer handle the transfer of information across multiple networks through router and gateway.
- IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

NETWORK INTERFACE LAYER

- The network interface layer is the lowest layer of the TCP/IP model.
- This layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.

COMPARISON - OSI MODEL AND TCP/IP MODEL



S.No	OSI MODEL	TCP/IP MODEL
1	Defined before advent of internet	Defined after the advent of Internet.
2	Service interface and protocols are clearly distinguished before	Service interface and protocols were not clearly distinguished before
3	Internetworking not supported	TCP/IP supports Internet working
4	Strict layering	Loosely layered
5	Protocol independent standard	Protocol Dependant standard
6	Less Credible	More Credible
7	All packets are reliably delivered	TCP reliably delivers packets, IP does not reliably deliver packets

Digital Transmission: Interfaces and Modems

1. Digital Transmission

- **Digital transmission** is the process of transmitting data in the form of **digital signals (bits: 0 and 1)**.
- It is used to transfer data between computers and other digital devices.
- For communication, digital devices may need an **interface** or a **modem**, depending on the type of communication channel.
- Important topics related to digital transmission include:
  - **DTE-DCE Interface**
  - **Modems**
  - **Cable Modems**

2. DTE-DCE Interface

DTE – Data Terminal Equipment

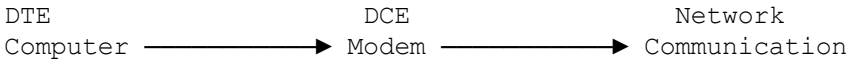
- **DTE** stands for **Data Terminal Equipment**.

- It is the device that **generates, receives, or processes data**.
- Examples:
  - Computer
  - Terminal
  - Router

DCE – Data Circuit-Terminating Equipment

- **DCE** stands for **Data Circuit-Terminating Equipment**.
- It provides the connection between the **DTE and the communication network**.
- It may perform functions such as **signal conversion, timing, and communication control**.
- Examples:
  - Modem
  - CSU/DSU

DTE-DCE Connection



- The **DTE** communicates with the **DCE**.
- The **DCE** connects the DTE to the communication network.
- A standard interface defines things such as:
  - **Mechanical characteristics** – connector and physical connection
  - **Electrical characteristics** – voltage and signal levels
  - **Functional characteristics** – purpose of each signal
  - **Procedural characteristics** – how communication takes place

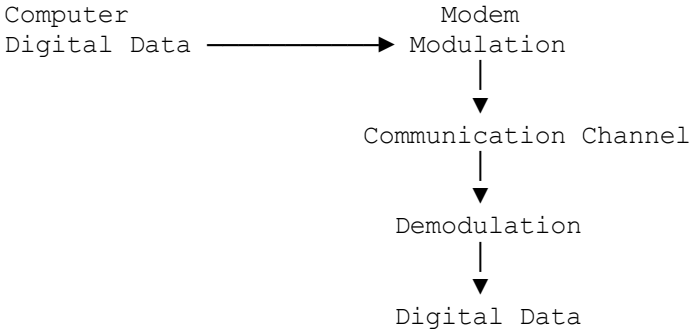
Key Point

DTE is the data-generating/processing device, while DCE connects it to the communication network.

3. Modem

- **Modem** stands for **Modulator-Demodulator**.
- It is a communication device used to convert signals so that digital data can be transmitted over a suitable communication medium.
- **Modulation** converts digital data into a signal suitable for transmission.
- **Demodulation** recovers the original digital data from the received signal.

Basic Working



Functions of a Modem

- Converts signals for transmission and reception.
- Performs **modulation and demodulation**.
- Enables digital devices to communicate over communication networks that require signal conversion.
- May also provide additional functions such as **error detection or correction**, depending on the modem type.

Example

- A computer sends digital data to a modem.
- The modem converts the data into a suitable transmission signal.
- The signal travels through the communication medium.
- The receiving modem converts it back into digital data.

Key Point

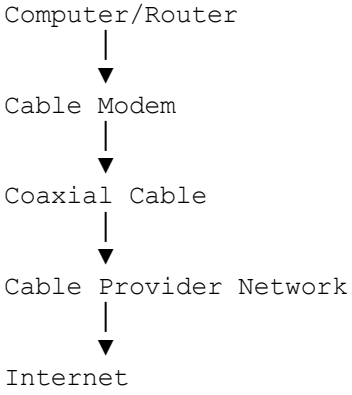
Modem = Modulator + Demodulator

---

4. Cable Modem

- A **cable modem** is a type of modem that provides **Internet/data communication over a cable television (CATV) network**.
- It uses **coaxial cable** in the cable network to transmit data.
- It allows users to access the Internet through a cable TV infrastructure.
- A cable modem usually connects:
    - **Computer/router ↔ Cable network**

Basic Structure



Features of Cable Modem

- Uses **cable TV infrastructure** for data communication.
- Provides **high-speed Internet access**.
- Usually provides an **always-on connection**.
- The connection can be shared among multiple users through a router.
- The available capacity of a cable network segment may be **shared among subscribers**, depending on the network design.