

MODULE 1

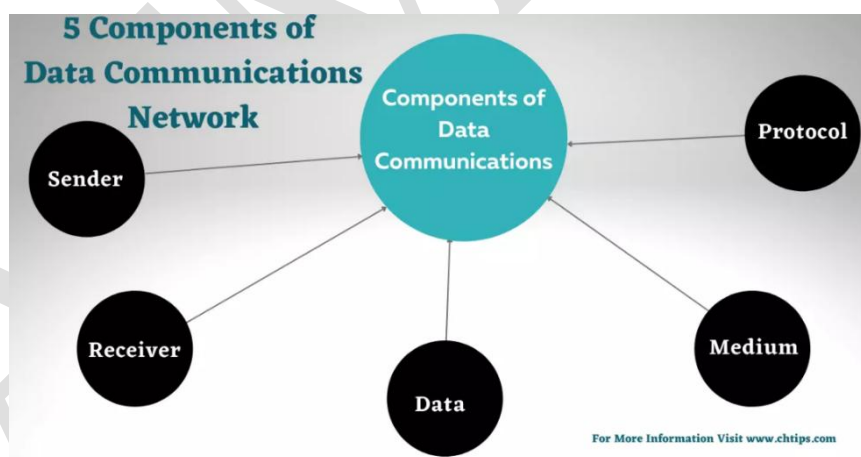
INTRODUCTION TO DATA COMMUNICATIONS AND NETWORKS

1. INTRODUCTION ON DATA COMMUNICATION

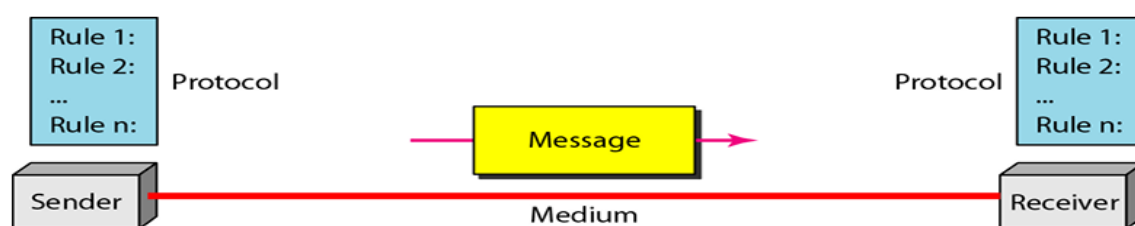
Definition: Data communication is the process of transferring data or information between two or more devices such as computers, mobile phones, or sensors, through a communication medium like cables, fiber optics, or wireless signals. In simple terms, it is the electronic exchange of data between a sender and a receiver using a set of established rules called protocols.

A data communication system consists of five essential components:

1. Sender (Source)
2. Message
3. Medium
4. Receiver (Destination)
5. Protocol



Components of Data Communication



Data Communication

1. Sender: (Source)

Definition: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

Example: If you send an email from your laptop, the laptop acts as the sender.

2. Message:

Definition: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

Example: When you send a WhatsApp voice note, the voice recording is the message.

3. Medium:

Definition: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

Example: In a Zoom call, your Wi-Fi connection is the medium.

4. Receiver: (Destination)

Definition: The receiver is the device that receives the message. It can be a computer, workstation etc.

Example: When your friend reads the email on their smartphone, the smartphone is the receiver.

5. Protocol:

Definition: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Example: Writing correct address, stamp, using envelope → otherwise the letter won't be delivered (similar to network protocols like IP address, TCP rules).

1.1.1 CHARACTERISTICS OF EFFECTIVE COMMUNICATION

The effectiveness of a data communications system depends on four fundamental characteristics are:

1. Delivery
2. Accuracy

3. Timeliness

4. Jitter

1. Delivery

Definition: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

Example: If you send an email to your friend, it must reach *your friend's email inbox* and not someone else's.

2. Accuracy

Definition: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

Example: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. Timeliness

Definition: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

Example: In online gaming or stock trading, if the data arrives late, it can affect the game result or financial decision.

4. Jitter

Definition: Jitter is the variation in the delay of received packets. In other words, the time gap between packets arriving at the destination should be consistent. If it keeps changing, the communication quality drops.

Example: In a video call, jitter causes the audio/video to break, lag, or go out of sync.

1.1.2 DATA FLOW

Communication between two devices can be **simplex, half-duplex, or full-duplex** as shown in Figure.

- **Simplex**

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit the other can only receive (Figure a).

Example: Keyboards and traditional monitors are examples of simplex devices.

- **Half-Duplex**

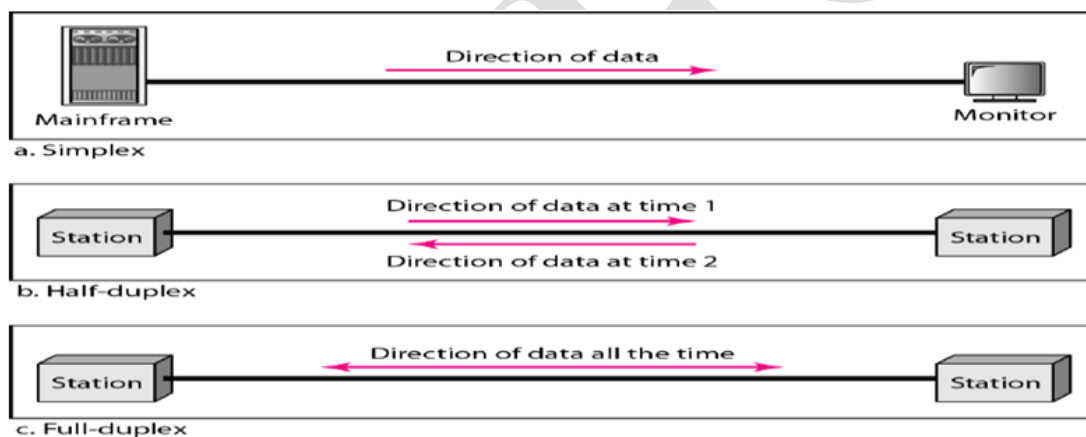
In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa (Figure b).

Example: Walkie-talkies and CB (citizens band) radios are both half duplex systems.

- **Full-Duplex**

In full-duplex, both stations can transmit and receive simultaneously (Figure c). One common example of full-duplex communication is the telephone network.

Example: When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time.



Data Flow

1.1.3 CONCLUSION OF DATA COMMUNICATION

In conclusion, data communication is the backbone of modern computing and networking, as it enables the exchange of information between devices, systems, and people across the world. By using components such as the sender, receiver, message, medium, and protocols, it ensures reliable and efficient transfer of data. Effective communication must meet key requirements like delivery, accuracy, timeliness, and minimal jitter to maintain quality, especially in real-time applications such as video conferencing, online gaming, and digital banking. Today, data communication is not only limited to computers but also extends to smartphones, IoT devices, satellites, and cloud services, making it essential for business, education, healthcare, and daily

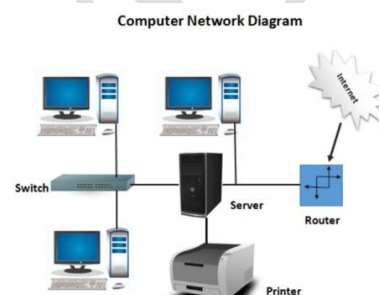
life. Without data communication, the global connectivity we experience through the internet and networks would not be possible.

1.2 COMPUTER NETWORKS

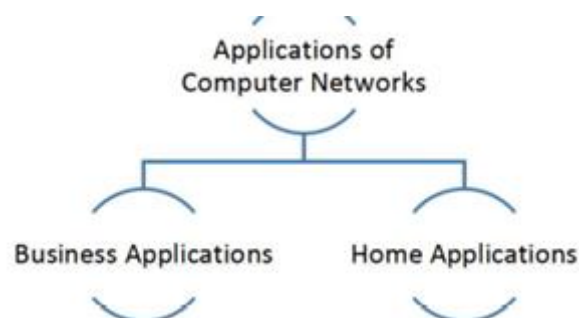
Definition: A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

“Computer network” to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used.

Networks come in many sizes, shapes and forms, as we will see later. They are usually connected together to make larger networks, with the Internet being the most well-known example of a network of networks.



1.2.1 APPLICATION OR USES OF COMPUTER NETWORKS



1. Business Applications

- To distribute information throughout the company (resource sharing). sharing physical resources such as printers, and tape backup systems, is sharing information.
- client-server model. It is widely used and forms the basis of much network usage.
- communication medium among employees, email (electronic mail), which employees generally use for a great deal of daily communication.
- Telephone calls between employees may be carried by the computer network instead of by the phone company. This technology is called IP telephony or Voice over IP (VoIP) when Internet technology is used.
- Desktop sharing lets remote workers see and interact with a graphical computer screen.
- doing business electronically, especially with customers and suppliers. This new model is called e-commerce (electronic commerce) and it has grown rapidly in recent years.

2 Home Applications

- Peer-to-peer communication
- Person-to-person communication
- Electronic commerce
- Entertainment (game playing,)

3. Mobile Users

- Text messaging or texting
- Smart phones,
- GPS (Global Positioning System)
- E-commerce
- NFC (Near Field Communication)

4 Social Issues

With the good comes the bad, as this new-found freedom brings with it many unsolved social, political, and ethical issues. Social networks, message boards, content sharing sites, and a host of other applications allow people to share their views with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

1.2.2 GOALS OF NETWORKING

1. Resource sharing (printers, files).
2. Communication (email, messaging).
3. Reliability (backup, fault tolerance).
4. Scalability (expansion with more devices).

1. Resource sharing (printers, files):

Definition: Resource sharing means multiple computers or users in a network can access and use hardware and software resources together.

Instead of each user having separate printers or storage, resources are shared to reduce cost and improve efficiency.

Example: A single printer in an office is shared by all employees through the network.

2. Communication

Definition: Reliability refers to the ability of a network to provide consistent service with backup and fault tolerance in case of failures.

It allows people to connect instantly, regardless of distance, using various services like email, chat, or video calls.

Example: Sending an email from India to the USA within seconds.

3. Reliability

Definition: Reliability refers to the ability of a network to provide consistent service with backup and fault tolerance in case of failures.

If one path or device fails, the system ensures data is not lost and continues working smoothly.

Example: Cloud storage automatically backs up files so users can recover them even if their computer crashes.

4. Scalability

Definition: Scalability is the capability of a network to expand easily by adding more devices or resources without affecting performance.

As organizations grow, their network can be upgraded without redesigning from scratch.

Example: Adding new computers to a company LAN without disturbing existing connections.

1.2.3 ADVANTAGES OF NETWORKING

1. Cost-effective resource sharing
2. Centralized data management.
3. Faster communication.
4. Supports distributed processing.

1. Cost-effective resource sharing

Explanation: Networking allows multiple users to share expensive resources such as printers, scanners, storage devices, and internet connections. Instead of buying separate resources for each user, they can all use the same resource over the network, reducing overall cost.

Example: In an office, one high-quality laser printer can be shared by all employees over the LAN instead of providing each person with a separate printer.

2. Centralized data management

Explanation: Networks allow data to be stored and managed in a central server, making it easier to update, back up, and secure. This ensures consistency of information and reduces duplication of work.

Example: In a university, student records are stored in a central database. Any authorized staff can access and update the records from their computers without maintaining separate copies.

3. Faster communication

Explanation: Networks enable quick and efficient communication between users through emails, instant messaging, file transfer, and video conferencing. This makes collaboration easier, even if people are far apart.

Example: Employees of a multinational company can use Microsoft Teams or Zoom to conduct meetings in real time without waiting for physical travel.

4. Supports distributed processing

Explanation: In a network, tasks can be divided among multiple computers (nodes) to balance the load and improve performance. This increases efficiency and reliability of work.

Example: In banking systems, customer transactions are processed across different branch servers but synchronized centrally, so no single computer is overloaded.

1.24 DISADVANTAGES OF NETWORKING

1. Security risks
2. Maintenance cost
3. Network congestion

1.Security Risks

Definition: Security risks mean the danger of unauthorized access, hacking, data theft, or virus attacks in a network. Since data and resources are shared, sensitive information can be misused if proper protection is not applied.

Example: A hacker stealing bank account details from an online banking network.

2. Maintenance Cost

Definition: Maintenance cost refers to the expense of setting up, managing, upgrading, and repairing a network. It includes the cost of hardware, software, and skilled IT staff needed to keep the network running.

Example: A company hiring network administrators and buying security software for smooth network operation.

3. Network Congestion

Definition: Network congestion happens when too many users or devices use the same network at the same time, causing slow speed, delays, or even network crashes.

Example: College Wi-Fi becoming very slow when all students stream videos during peak hours.

4.Unauthorized Access

Definition: When an outsider or someone without proper permission enters the network and uses its data or resources.

Real-time example:

- If a college Wi-Fi is password protected, but a student hacks it or guesses the password and uses it without permission, that is unauthorized access.
- Hackers stealing bank customer data through the internet is also unauthorized access.

5.Cost of Setup

Definition: Building and maintaining a computer network requires a lot of money (hardware, software, skilled technicians).

Real-time example:

- In a college, setting up a network with routers, switches, servers, and cabling for all classrooms is expensive. In companies like Infosys or hospitals, they spend huge money to install and maintain networks for smooth operations.

6.Network Fails

Definition: If the network stops working, users cannot access data, communicate, or use resources.

Real-time example:

- If the internet goes down in an ATM centre, customers cannot withdraw cash.
- In online classes, if the server or internet fails, students cannot attend lectures.
- If a hospital network crashes, doctors may not access patient records on time.

Network Devices [Basic Definitions just for Reference]

Devices used to connect computers, manage communication, and forward data.

1.Router

Explanation: A Router is a networking device that forwards data packets between computer networks. One or more packet-switched networks or subnetworks can be connected using a router. By sending data packets to their intended IP address, it manages traffic between different networks and permits several devices to share an Internet Connection.

- **Real-time Example:** The Wi-Fi router in your home that connects your laptop/mobile to the internet.
- **Technical Example:** Cisco Router used by ISPs to route internet traffic between cities.

2.Switch

Explanation: The Switch is a network device that is used to connect devices within a single network. It is responsible for filtering and forwarding the packets between LAN segments based on MAC address.

- **Real-time Example:** In a college lab, all computers are connected to a switch for faster communication.
- **Technical Example:** A 24-port Ethernet switch in a company LAN.

3. Hub

Explanation: A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through hub remains one. Hub does not have any routing table to store the data of ports and map destination addresses., the routing table is used to send/broadcast information across all the ports.

- **Real-time Example:** Used in very small networks where cost is a concern.
- **Technical Example:** A simple USB hub-like network hub in old LAN setups.

4. Modem

Explanation: A modem converts digital signals (computer data) into analog signals (telephone lines) and vice versa.

- **Real-time Example:** The broadband modem from BSNL/ACT/Jio in homes.
- **Technical Example:** DSL or Cable modem used by ISPs to provide internet.

Network Protocols

Rules that define how data is transmitted and received.

1. TCP/IP

Explanation: The TCP/IP model is a framework that is used to model the communication in a network. It is mainly a collection of network protocols and organization of these protocols in different layers for modelling the network.

- **Real-time Example:** Sending an email or browsing a website.
- **Technical Example:** TCP (port 80/443 for web), IP addressing (IPv4/IPv6).

2. HTTP

Explanation: HTTP (Hypertext Transfer Protocol) is a fundamental protocol of the Internet, enabling the transfer of data between a client and a server. It is the foundation of data communication for the World Wide Web.

- **Real-time Example:** When you open www.google.com, your browser uses HTTP/HTTPS.
- **Technical Example:** HTTP GET request when a webpage loads.

3. FTP

Explanation: It helps to transfer files from one computer to another by providing access to directories or folders on remote computers and allows software, data, and text files to be transferred between different kinds of computers. The end-user in the connection is known as localhost and the server which provides data is known as the remote host.

- **Real-time Example:** Web developers uploading website files to a hosting server.
- **Technical Example:** Using `ftp://` in FileZilla software to transfer files.

3. Network Security

Methods to protect data and networks.

1. Firewall

Explanation: A firewall is a network security device designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules. The primary purpose of a firewall is to establish a barrier between a trusted internal network and untrusted external networks.

- **Real-time Example:** Windows Firewall blocking unauthorized apps.
- **Technical Example:** Cisco ASA Firewall used by banks for network protection.

2. Encryption

Explanation: Encryption is a form of data security in which information is converted to ciphertext. Only authorized people who have the key can decipher the code and access the original plaintext information.

- **Real-time Example:** WhatsApp messages are end-to-end encrypted.
- **Technical Example:** AES-256 encryption used in VPNs.

3. Authentication

Explanation: **Authentication** is the process of verifying the identity of a user or information. User authentication is the process of verifying the identity of a user when that user logs in to a computer system.

- **Real-time Example:** Logging into Gmail using username + password.
- **Technical Example:** Multi-Factor Authentication (OTP + password).

Network Applications

Services that use networking.

1. Email

Explanation: Email stands for [Electronic Mail](#). It is a method to send messages from one computer to another computer through the Internet. It is mostly used in business, education, technical communication, and document interactions. It allows communicating with people all over the world without bothering them. In 1971, a test email was sent Ray Tomlinson to himself containing text.

- **Real-time Example:** Gmail, Outlook.
- **Technical Example:** Uses SMTP (sending), IMAP/POP3 (receiving).

2. File Sharing:

Explanation: File sharing is a productivity tool that enables a limited group of users to exchange data remotely. These can be shared with a single person, two people or even a whole company. File sharing allows users to share practically any type of file format including images, PowerPoint slides, text documents, audio and video files, and so on. When it comes to promoting cooperation and communication between people and organizations, file sharing is needed. It makes remote work possible and lessens the need for in-person meetings by letting users transfer files quickly and effortlessly between locations..

- **Real-time Example:** Google Drive or college LAN file sharing.
- **Technical Example:** Peer-to-peer file sharing (BitTorrent).

3. Video Conferencing

Explanation: Video conferencing is a technology that allows users in different locations to hold real-time face-to-face meetings, often at little to no cost. There are many ways to utilize video conferencing technology, such as company meetings, job training sessions, or addressing board members.

- **Real-time Example:** Zoom, Microsoft Teams, Google Meet.
- **Technical Example:** Uses RTP (Real-time Transport Protocol) for audio/video streaming.

1.2.6 NETWORK TOPOLOGY

Network topology refers to the arrangement of different elements like nodes, links, or devices in a computer network. Common types of network topology include bus, star, ring, mesh, and tree topologies, each with its advantages and disadvantages. In this article, we will discuss different types of network topology in detail.

There are two major categories of Network Topology i.e. **Physical Network topology and Logical Network Topology**. **Physical Network Topology** refers to the actual structure of the physical medium for the transmission of data. **Logical network Topology** refers to the transmission of data between devices present in the network irrespective of the way devices are connected. The structure of the network is important for the proper functioning of the network. one must choose the most suitable topology as per their requirement.

Types of Network Topology

Below mentioned are the types of Network Topology

1. **Point to Point Topology**
2. **Mesh Topology**
3. **Star Topology**
4. **Bus Topology**
5. **Ring Topology**
6. **Tree Topology**
7. **Hybrid Topology**

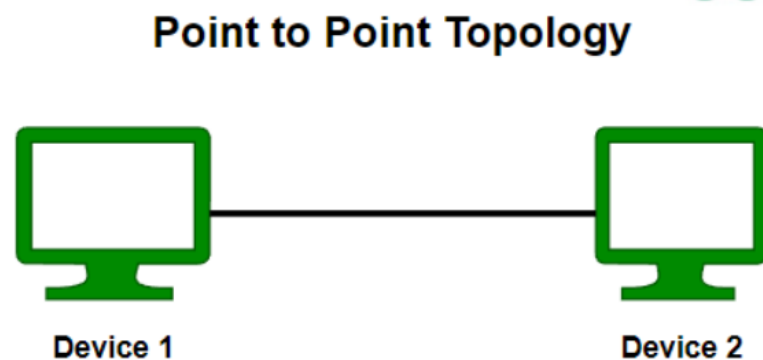
1. Point to Point Topology

Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.

□ Telephone Call

When you call a friend, it's a direct connection between your phone and your friend's phone.

□ Direct Cable Connection.



Point to Point Topology

Advantages of Point-to-Point (P2P) Connections

1. High Security

In P2P, data travels directly between two devices without passing through other nodes, reducing the chances of data interception or hacking. This makes it more secure than shared networks.

2. Low Latency

Since data takes the shortest possible path (direct link), there is less delay. This is useful for real-time applications like video calls, gaming.

3. Reliability

P2P uses a dedicated connection between two points. If the link is active, communication remains stable and less affected by network congestion.

4. Easy to Manage

With only two endpoints to monitor, setup, maintenance, and troubleshooting become easier compared to complex topologies with many nodes.

Disadvantages of Point-to-Point (P2P) Connections

1. Limited Scalability

Adding more devices means creating additional links for each pair, which becomes complex and impractical for large networks.

2. Higher Costs

Since each connection needs dedicated hardware (cables, ports, etc.), the cost of setup and maintenance is higher compared to shared networks.

3. Limited Flexibility

P2P links are made for a fixed purpose (connecting two points). Changing the network layout or adding new devices requires reconfiguration or new links.

4. Distance Limitations

The maximum length of the cable or wireless link is limited. For long distances, repeaters or amplifiers are needed, increasing cost and complexity.

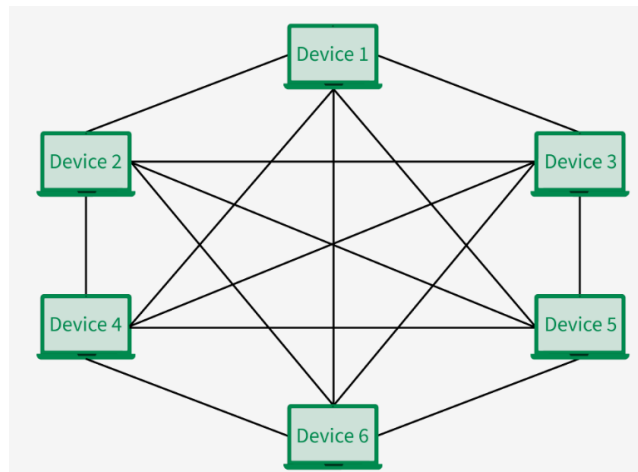
2. Mesh Topology

A mesh topology can be a full mesh topology or a partially connected mesh topology. In a full mesh topology, every computer in the network has a connection to each of the other computers in that network. The number of connections in this network can be calculated using the following formula (n is the number of computers in the network): $n(n-1)/2$.

In a partially connected mesh topology, at least two of the computers in the network have connections to multiple other computers in that network. It is an inexpensive way to implement redundancy in a network. In the event that one of the primary computers or connections in the network fails, the rest of the network continues to operate normally.

- **Example:**

- Conference call where everyone can directly talk to everyone.
- Modern internet backbone uses partial mesh for redundancy.



Mesh Topology

"Calculation of Connections in Full Mesh Topology"

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure , there are 6 devices connected to each other, hence the total number of ports required by each device is 5. The total number of ports required = $N * (N-1)$.
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is $N C 2$ i.e. $N(N-1)/2$. In Figure, there are 6 devices connected to each other, hence the total number of links required is $6*5/2 = 15$.

Advantages of a mesh topology:

- Can handle high amounts of traffic, because multiple devices can transmit data simultaneously.
- A failure of one device does not cause a break in the network or transmission of data.
- Adding additional devices does not disrupt data transmission between other devices.

Disadvantages of a mesh topology:

- The cost to implement is higher than other network topologies, making it a less desirable option.
- Building and maintaining the topology is difficult and time consuming.

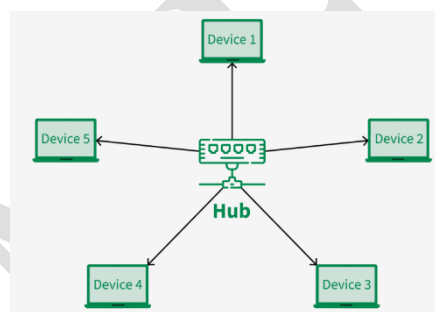
- The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.

3. Star Topology

A star network, star topology is one of the most common network setups. In this configuration, every node connects to a central network device, like a hub, switch, or computer.

Example:

- Computers in an office connected to one switch.
- Home Wi-Fi where all devices connect to one router.



Star Topology

Advantages of star topology

- Centralized management of the network, through the use of the central computer, hub, or switch.
- Easy to add another computer to the network. If one computer on the network fails, the rest of the network continues to function normally.
- The star topology is used in local-area networks (LANs), High-speed LANs often use a star topology with a central hub.

Disadvantages of star topology

- Can have a higher cost to implement, especially when using a switch or router as the central network device.
- The central network device determines the performance and number of nodes the network can handle.
- If the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network. This process is called “**Single Point of Failure**”.

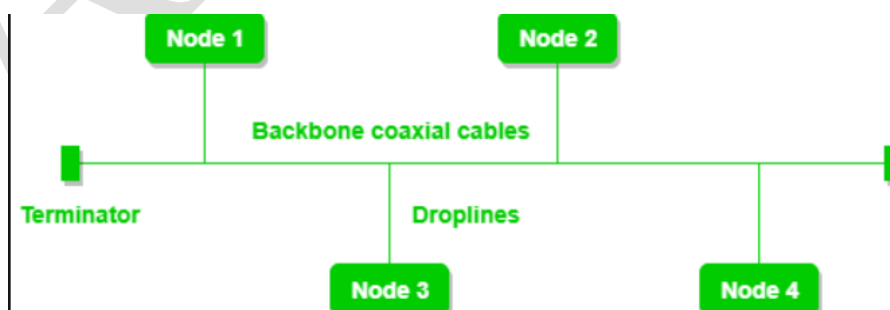
Example: A common example of star topology is a local area network (LAN) in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

4. Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable called **Coaxial Cable** (Backbone). A line topology, a bus topology is a network setup in which each computer and network device are connected to a single cable or backbone.

Example:

- Old Ethernet networks.
- School announcements over a single speaker wire — message goes to all classrooms.



Bus Topology

Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.

Disadvantages of Bus Topology

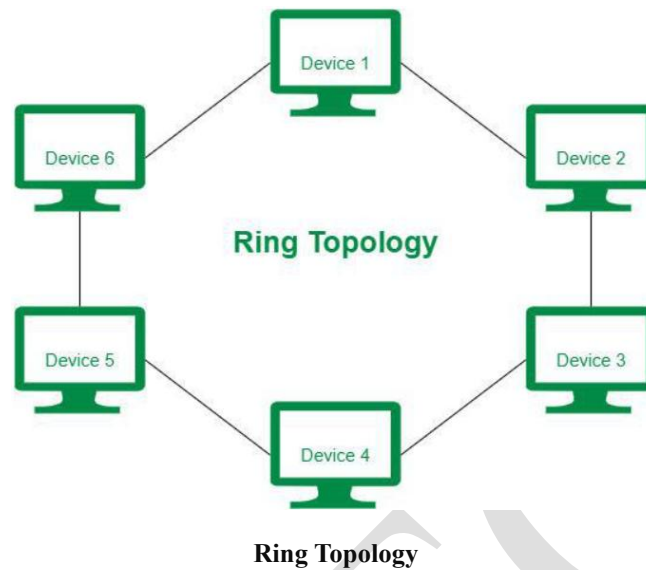
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the computer or terminator is removed or missing the cable used to be opened and close the connection data can be bounded back is called “**Single Reflection**”.
- If the network traffic is heavy, it increases collisions in the network.
- To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

Example: A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.

5. Ring Topology

A ring topology is a network configuration in which device connections create a circular data path. In a ring network, packets of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a **unidirectional** ring network. Others permit data to move in either direction, called **bidirectional**.

The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected. Ring topologies may be used in either local area networks (LANs) or wide area networks (WANs).



Advantages of ring topology

- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance of the network.

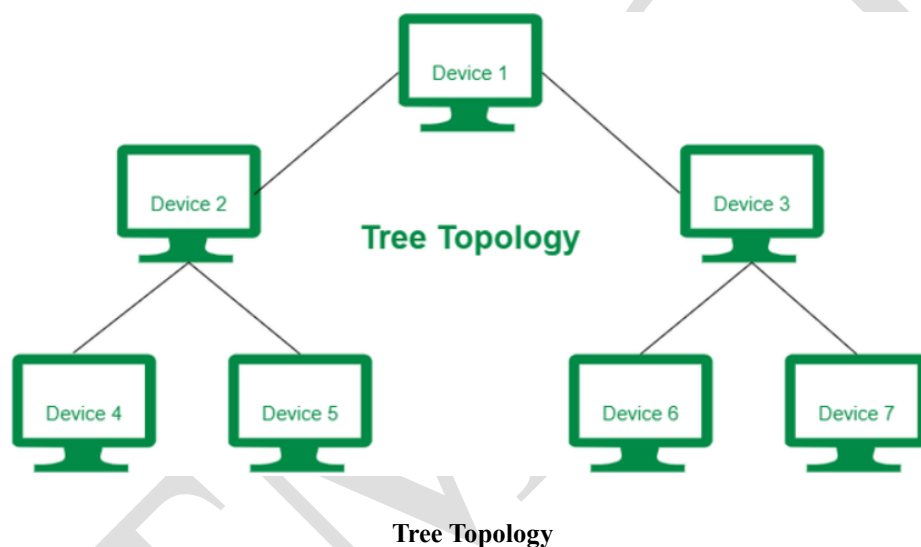
Disadvantages of ring topology

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.

6.Tree Topology

Tree topology is a hierarchical network topology in which nodes are connected in the form of a tree. It combines the characteristics of star topology and bus topology. The top-most node is called the **Root Node**, and all other nodes are connected as **Parent–Child Relationships**, forming multiple levels.

- ☐ The network starts from a root node (central node).
- ☐ Each node in the upper level can be connected to one or more nodes in the next level.
- ☐ Communication flows from top to bottom (downstream) or bottom to top (upstream).
- ☐ Data is transmitted from the root node to the corresponding child node.
- ☐ Each parent node controls the flow of data to its children.
- ☐ If a child wants to communicate with another child, data must first go through their common parent node.



Advantages

- **Hierarchical Structure:** Easy to expand by adding more nodes at different levels.
- **Scalability:** Supports large networks with multiple levels.
- **Fault Isolation:** A fault in one branch does not affect other branches.
- **Better Management:** Suits organizations with hierarchical workflows (e.g., schools, companies).

Disadvantages

- **Complex Installation:** Requires more cabling compared to bus topology.

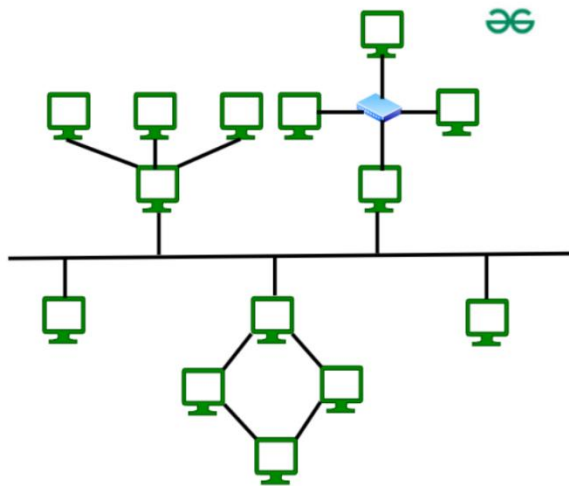
- **Dependency on Root Node:** If the root node fails, entire network may be affected.
- **Maintenance Cost:** Troubleshooting can be difficult in large tree networks.

7. Hybrid Topology

A Hybrid Topology is a network topology that combines two or more different types of topologies such as Star, Bus, Ring, Mesh etc., to form a single network. It is used when a single topology cannot fulfil all the requirements of an organization.

- ☐ Each part of the network follows its **respective topology rules** (e.g., star hub works like a star, bus works like a bus).
- ☐ The combined network allows communication between all nodes regardless of which sub-topology they belong to.
- ☐ The backbone (main connecting medium) plays a key role in connecting different topologies.

Example: A **star-ring hybrid** means several star networks are connected in a ring formation.



Hybrid Topology

Advantages of Hybrid Topology

- This topology is **very flexible**.
- The size of the network can be easily expanded by **adding new devices**.

Disadvantages of Hybrid Topology

- It is challenging to **design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive**.
- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices**.

Why is Network Topology Important?

Network Topology is important because it defines how devices are connected and how they communicate in the network. Here are some points that defines why network topology is important.

- **Network Performance:** Upon choosing the appropriate topology as per requirement, it helps in running the network easily and hence increases network performance.
- **Network Reliability:** Some topologies like Star, Mesh are reliable as if one connection fails, they provide an alternative for that connection, hence it works as a backup.
- **Network Expansion:** Choosing correct topology helps in easier expansion of Network as it helps in adding more devices to the network without disrupting the actual network.
- **Network Security:** Network Topology helps in understanding how devices are connected and hence provides a better security to the network.

Conclusion

In conclusion, network topologies play a crucial role in determining the efficiency and reliability of a computer network. Each topology, whether it's bus, star, ring, mesh, or tree, offers unique benefits and potential drawbacks. By understanding these different arrangements, network designers can choose the most appropriate topology to meet the specific needs of their systems, ensuring optimal performance and connectivity.

1.2.7 CLASSIFICATION OF NETWORKS

The types of networks are classified based upon the size, the area it covers and its physical architecture (**Geographical Boundaries**). The four primary network categories are PAN, LAN, WAN

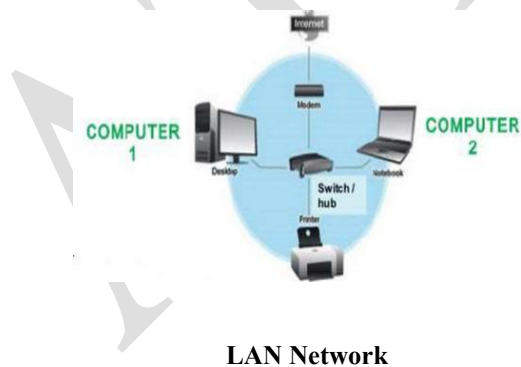
and MAN. Each network differs in their characteristics such as distance, transmission speed, cables and cost.

1. PAN (Personal Area Network)

- Pan devices communicate over the range of a person.
- Used for data transmission among devices such as computer, telephones, and personal digital assistants.
- The data cable is an example of PAN.
- This is also a Personal Area Network because that connection is for the users personal use only.
-

2. LAN (Local Area Network)

- LAN is network that connects computers and devices in a limited geographical area.
- The simplest form of LAN is to connect two computers together.
- LANs are inexpensive to install and also provide higher speeds.
- A network which consists of less than 500 interconnected devices across several buildings, is still recognized as a LAN.
- Data transfer rate is 10 to 100 mbps.
- **Example:** A computer lab in a school.



Advantage of LAN

- ☐ Easy to share devices such as printers, scanners etc.
- ☐ Easy to share data such as printers.

- ☐ Cost of LAN setup is low.

Disadvantages of LAN

- ☐ Power-a good LAN is Required to be all the time.
- ☐ Area covered is limited.
- ☐ Security – each computer and devices become another point of entry for undesirables.
- ☐ Example: IEEE 802.3 popularly called Ethernet.

3. MAN (Metropolitan Area Network)

- It is high speed network that connects local area networks in a metropolitan area.
- Is larger than a LAN, but smaller than a WAN.
- Is also used to mean the interconnection of several LANs by bridging them together. This network is also referred to as a campus network.
- **Example:** City or town handles the bulk of communication activity across that region.
- **Example:** Cable TV



MAN Network

Advantages of MAN

- ☐ Efficiency and shared access.
- ☐ All the computer-owning residents of the area have equal ability to go online.
- ☐ MAN can cover a wider area than a LAN.

Disadvantages of MAN

- ☐ It can be costly.
- ☐ Security problem.
- ☐ As the network consists of many computers over the span of a city, the connection can lag or become quite slow.

4.WAN (Wide Area Network)

WAN is a network that covers a larger geographic area (such as a city, country or world) using a communication channel that combines many types of media such as telephone lines, cables and radio waves.

Also called “enterprise networks” if they are privately owned by a large company.

To cover great distances, WANs may transmit data over leased high speed phone lines or wireless links such as satellites.

Types of WAN:

1. **Enterprise private network (EPN)**
2. **Virtual private network (VPN)**

1. **Enterprise private network (EPN):** An **enterprise private network** is a network build by an enterprise to interconnect various company sites, e.g.: production sites, head offices, remote offices, and shops in order to share computer resources.
2. **Virtual private network (VPN):** A virtual private network is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network instead of by physical wires.

Advantages of WAN

- ☐ **Increased efficiency:** WAN allows **centralized data storage** and **resource sharing** across different branches or locations. Employees can access the same data or applications from anywhere, avoiding duplication of work. This improves **productivity** and reduces time spent on transferring files manually.

Example: A company with offices in multiple cities can share a single database server. Employees in all locations can update records in real-time, which avoids delays and errors.

- ❑ **Easy of communication:** WAN connects computers and networks across **long distances** (cities, countries, even globally). It supports **emails, video calls, instant messaging, and collaborative tools** over the internet. This improves teamwork and decision-making even when teams are geographically apart.

Example: Video conferencing tools like Microsoft Teams or Zoom allow employees in India to attend meetings with colleagues in the US without traveling.

- ❑ **Lowered costs:** Instead of setting up separate servers, printers, or software for each location, WAN allows sharing of resources over the network. Reduces travel and postage costs because files, messages, and data can be sent digitally. Cloud-based WAN services reduce the need for expensive on-site infrastructure.

Example: An organization can use a single cloud server for HR, payroll, and ERP systems instead of buying separate hardware for each office, saving cost.

Disadvantages of WAN

- ❑ **Security problems:** Since WAN connects networks over **large geographical areas**, there is a higher risk of **unauthorized access, hacking, and data theft**. Data travels through public networks (like the Internet), which makes it vulnerable if not properly secured with **firewalls, encryption, and VPNs**.

Example: If a bank's WAN is not secured, hackers could intercept transactions or steal customer details.

- ❑ **Training costs:** WAN setup involves routers, firewalls, servers, and complex configurations. Employees and IT staff need proper training to operate and manage the network efficiently. This training takes time and money, increasing the organization's overall cost.

Example: A company switching to cloud-based WAN must train its network administrators on the new system before they can manage it.

- ❑ **Maintenance problems:** WAN covers **multiple locations**, so diagnosing and fixing issues can be **time-consuming**. Specialized network engineers are often needed, which increases

maintenance expenses. Downtime in WAN can disrupt communication across branches until the problem is solved.

Example: If a WAN link between two branch offices fails, the IT team may have to coordinate with Internet Service Providers (ISPs) to restore connectivity, which may take hours.

2 NETWORK MODEL

A network is a combination of hardware and software that sends data from one location to another. The hardware consists of the physical equipment that carries signals from one point of the network to another. The software consists of instruction sets that make possible the services that we expect from a network.

We can compare the task of networking to the task of solving a mathematics problem with a computer. The fundamental job of solving the problem with a computer is done by computer hardware. However, this is a very tedious task if only hardware is involved. We would need switches for every memory location to store and manipulate data. The task is much easier if software is available. At the highest level, a program can direct the problem-solving process; the details of how this is done by the actual hardware can be left to the layers of software that are called by the higher levels.

2.1 PROTOCOL LAYERING

In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices 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.

2.1.1 Scenarios

Let us develop two simple scenarios to better understand the need for protocol layering.

First Scenario

In the first scenario, communication is so simple that it can occur in only one layer.

Assume Maria and Ann are neighbours with a lot of common ideas. Communication between Maria and Ann takes place in one layer, face to face, in the same language, as shown in Figure 2.1



Figure 2.1 A Single-Layer Protocol

Even in this simple scenario, we can see that a set of rules needs to be followed

1. First, Maria and Ann know that they should greet each other when they meet.
2. Second, they know that they should confine their vocabulary to the level of their friendship. Third, each party knows that she should refrain from speaking when the other party is speaking.
3. Fourth, each party knows that the conversation should be a dialog, not a monolog: both should have the opportunity to talk about the issue.
4. Fifth, they should exchange some nice words when they leave.

We can see that the protocol used by Maria and Ann is different from the communication between a professor and the students in a lecture hall. The communication in the second case is mostly monolog; the professor talks most of the time unless a student has a question, a situation in which the protocol dictates that she should raise her hand and wait for permission to speak. In this case, the communication is normally very for-mal and limited to the subject being taught.

Second Scenario

- In the second scenario, we assume that Ann is offered a higher-level position in her company, but needs to move to another branch located in a city very far from Maria.
- The two friends still want to continue their communication and exchange ideas because they have come up with an innovative project to start a new business when they both retire.

- They decide to continue their conversation using regular mail through the post office. However, they do not want their ideas to be revealed by other people if the letters are intercepted.
- They agree on an encryption/decryption technique. The sender of the letter encrypts it to make it unreadable by an intruder; the receiver of the letter decrypts it to get the original letter.
- Now we can say that the communication between Maria and Ann takes place in three layers, as shown in Figure 2.2. We assume that Ann and Maria each have three machines (or robots) that can perform the task at each layer.

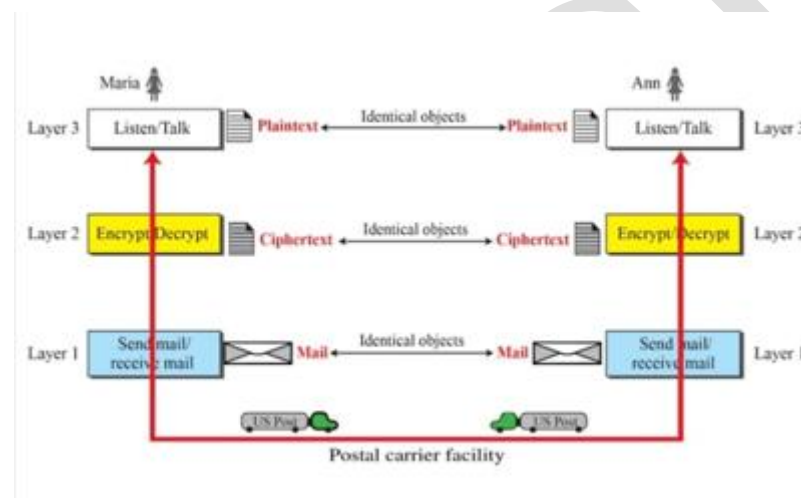


Figure 2.2 A three -Layer Protocol

- Let us assume that Maria sends the first letter to Ann. Maria talks to the machine at the third layer as though the machine is Ann and is listening to her.
- The third layer machine listens to what Maria says and creates the plaintext (a letter in English), which is passed to the second layer machine.
- The second layer machine takes the plaintext, encrypts it, and creates the ciphertext, which is passed to the first layer machine.
- The first layer machine, presumably a robot, takes the ciphertext, puts it in an envelope, adds the sender and receiver addresses, and mails it.

At Ann's side, the first layer machine picks up the letter from Ann's mail box, recognizing the letter from Maria by the sender address. The machine takes out the ciphertext from the envelope and delivers it to the second layer machine. The second layer machine decrypts the message, creates the plaintext, and passes the plaintext to the third-layer machine. The third layer machine takes the plaintext and reads it as though Maria is speaking.

Protocol layering enables us to divide a complex task into several smaller and simpler used only one machine to do job of all three machines. However, if Maria and Ann decide that the encryption/to change the whole machine. In the present situation, they need to change only the sec-decryption done by the machine is not enough to protect their secrecy, they would have on layer machine, the other two can remain the same.

This is referred to as modularity. Modularity in this case means independent layers. A layer (module) can be defined as a black box with inputs and outputs, without concern about how inputs are changed to outputs. If two machines provide the same outputs when given the same inputs, they can replace each other. For example, Ann and Maria can buy the second layer machine from two different manufacturers. As long as the two machines create the same cipher-text from the same plaintext and vice versa, they do the job.

Advantages:

1. 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, we don't care about how the layer is implemented.
2. Protocol layering which cannot be seen in our simple examples but reveals itself when we discuss protocol layering in the Internet, is that communication does not always use only two end systems, there are intermediate systems that need only some layers, but not all layers.
3. If we did not use protocol layering, we would have to make each intermediate system as complex as the end systems, which makes the whole system more expensive.

Example, Maria may decide not to buy the machine (robot) for the first layer, she can do the job herself. As long as Maria can do the tasks provided by the first layer, in both directions, the communication system works.

Disadvantage

Protocol layering One can argue that having a single layer makes the job easier. There is no need for each layer to provide a service to the upper layer and give service to the lower layer.

Example: Ann and Maria could find or build one machine that could do all three tasks. However, as mentioned above, if one day they found that their code was broken, each would have to replace the whole machine with a new one instead of just changing the machine in the second layer.

2.1.2 Principles of Protocol Layering

Let us discuss two 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. For example, the third layer task is to listen (in one direction) and talk (in the other direction). The second layer needs to be able to encrypt and decrypt. The first layer needs to send and receive mail

Second Principle

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. For example, the object under layer 3 at both sites should be a plaintext letter. The object under layer 2 at both sites should be a ciphertext letter. The object under layer 1 at both sites should be a piece of mail.

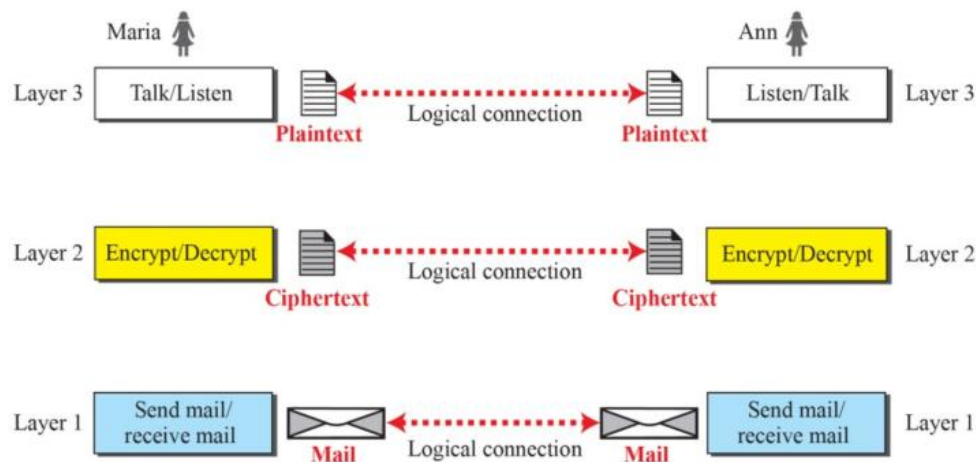


Figure 2.1.2 Logical Connection Between Peer Layer

2.2 TCP/IP PROTOCOL SUITE

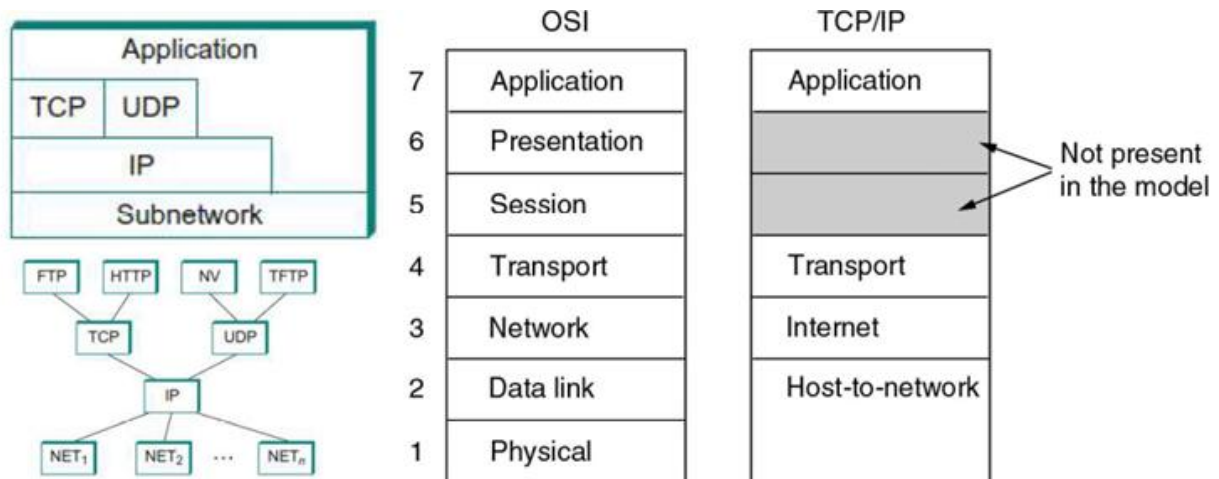


Figure 2.2 TCP/IP Protocol Suit

- It is the basic communication language or protocol of the Internet. TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. Protocols exist for a variety of different types of communication services between computers.
- The Transmission Control Protocol/Internetworking Protocol (TCP/IP) is a set of protocols, or protocol suite that defines how all the transmissions are exchanged across the Internet.
- At the transport layer TCP/IP defines two protocols: TCP and User Datagram Protocol (UDP).
- At the network layer the main protocol defined by TCP/IP is the Internetworking Protocol (IP).
- At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols.
- TCP or UDP creates a data unit that is called either a segment or a user datagram.
- The IP layer creates a data unit called a datagram.
- The movement of the datagram across the Internet is the responsibility of the TCP/IP protocol.

FUNCTIONS OF Each Layer of Interest Model (TCP/IP)

Layer	Primary function	Examples
Application	Do useful work with various network application programs.	HTTP, SMTP, POP, Ping, FTP
Transport	<i>Control</i> the flow of information between the application program running on the client and the application program running on the server	TCP (reliable), UDP (unreliable)
Internetwork Layer (IP)	Route packets <i>between</i> networks (inter-network)	IP
Subnetwork Layer (Network access Layer)	Move data <i>within</i> a local area network	Ethernet
	Define the physical characteristics of the communication hardware and medium	radio, twisted pair, fiber

The application layer is where real work gets done. Users typically interact with application programs to retrieve Web pages, transfer files, log on to remote systems, send and read e-mail, conduct teleconferences, etc. In other cases, the "user" might be a computer -- for example, a search engine "spider" automatically downloading pages to index.

Transport layer programs do what the name suggest -- they transport information between the application program on the client and the application program on the server. There are two major transport layer protocols.

1. Transmission control protocol (TCP) IS for applications that require a reliable connection between the client and server. TCP establishes a temporary connection between the client and server and controls the transmission of information. It checks for transmission errors, lost packets, and packets arriving out of order, and tries to automatically correct these without "bothering" the application program. It also does flow control slowing transmission if it is too fast for the receiver.
2. The user datagram protocol (UDP), is an unreliable transport protocol with no sessions and no flow control. Error checking is optional. UDP is faster than TCP, and is suitable for isochronous applications like voice over IP (VoIP) or streaming video where nothing can be done if an error is detected.

The Internetwork layer(IP) is responsible for routing packets between networks. The network layer protocol is called Internet protocol or IP for short. Again, as the name "inter-net" implies, IP moves information between networks. Since routing efficiency is critical, IP is simple and fast. The complexity of message integrity is left to TCP.

2.3 THE OSI MODEL (Open System Interconnection)

History of OSI MODEL

Although, when speaking of the Internet, everyone talks about the TCP/IP protocol suite, this suite is not the only suite of protocols defined. Established in 1947, the International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards.

Almost three-fourths of the countries in the world are represented in the ISO. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

ISO is the organization; OSI is the model. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

The OSI model was intended to be the basis for the creation of the protocols in the OSI stack.

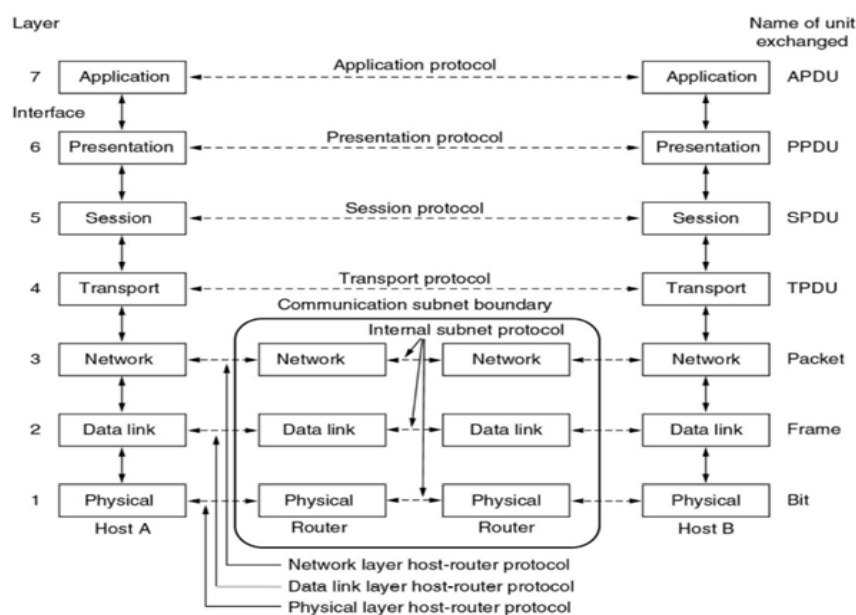


Figure 2.3.1 The OSI Model

This model group functions communication into seven logical layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

1. Physical Layer

- Deals with the transmission of Os and is over the physical media.
- Translation of bits into signal and Encode bits into signals.
- Carry data from the higher layers.
- It helps to transmit bits over a medium.
- Physical examples include Ethernet, FDDI, B8ZS, V.35, V.24, RJ45.
- The unit of communication at the physical layer is a **bit**.

2. Data link Layer

- To organize bits into frames and helps in providing hop-to-hop delivery.
- Create and detect frame boundaries.
- Handle errors by implementing an acknowledgement and retransmission scheme.
- Implement flow control.
- Supports points-to-point as well as broadcast communication.
- Supports simplex, half-duplex or full-duplex communication.
- The unit of communication at the data link layer is a **frame**.

3. Network Layer

- To move packets from source to destination to provide internetworking.
- Defines the most optimum path the packet should take from the source to the destination.
- Defines logical addressing so that any endpoint can be identified.
- Handles congestion in the network.
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.
- The unit of communication at the network layer is a **Packet**.

4. Transport Layer

- To provide reliable process-to-process message delivery and error recovery
- Purpose of this layer is to provide a reliable mechanism for the exchange of data between two processes in different computers.
- Ensures that the data units are delivered error free, data units are delivered in sequence, no loss or duplication of data units. Provides connectionless or connection-oriented service.
- The unit of communication at the transport layer is a **segment**, depending on the specific protocol used in this layer.

5. Session Layer

- To establish, manage and terminate sessions.
- Session layer provides mechanism for controlling the dialogue between the two end systems.
- It defines how to start, control and end conversations (called sessions) between applications.
- This layer requests for a logical connection to be established on an end-user's request.
- Session layer is also responsible for terminating the connection.
- The unit of communication at the application layer is a **Message or Data**.

6. Presentation Layer

- To translate, encrypt and compress data.
- Presentation layer defines the format in which the data is to be exchanged between the two communicating entities
- Also handles data compression and data encryption (cryptography).
- The unit of communication at the application layer is a **Message or Data**.

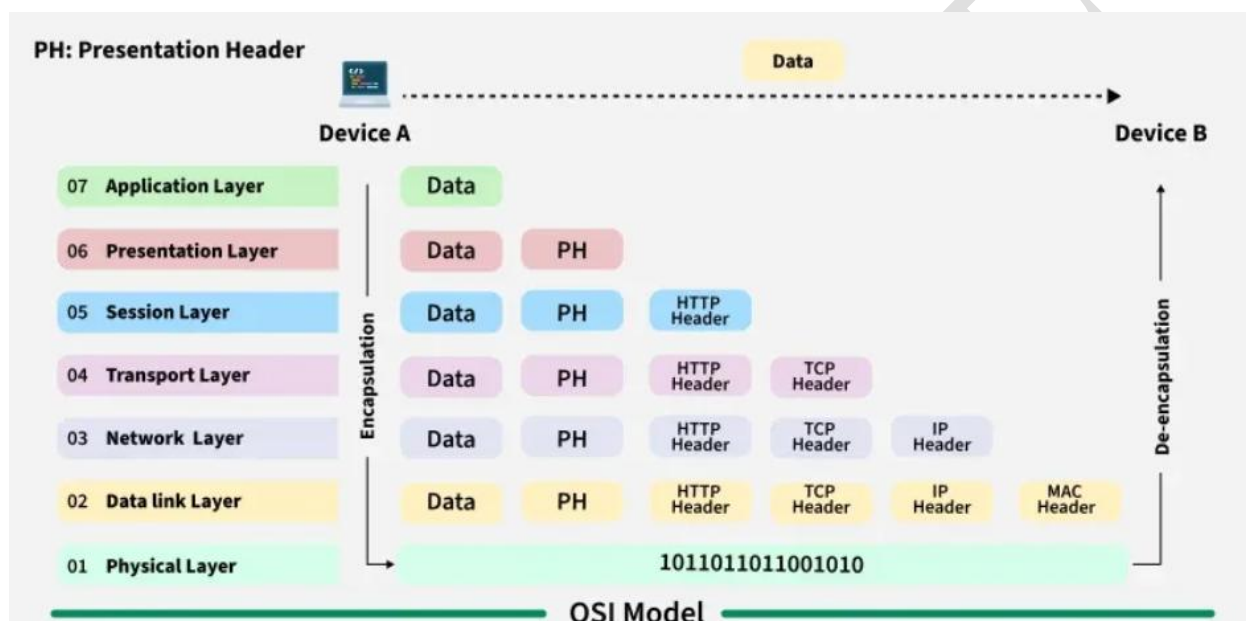
7. Application Layer

- To allow access to network resources
- Application layer interacts with application programs and is the highest level of OSI model.
- Application layer contains management functions to support distributed applications
- Examples of application layer are applications such as file transfer, electronic mail, remote login etc.

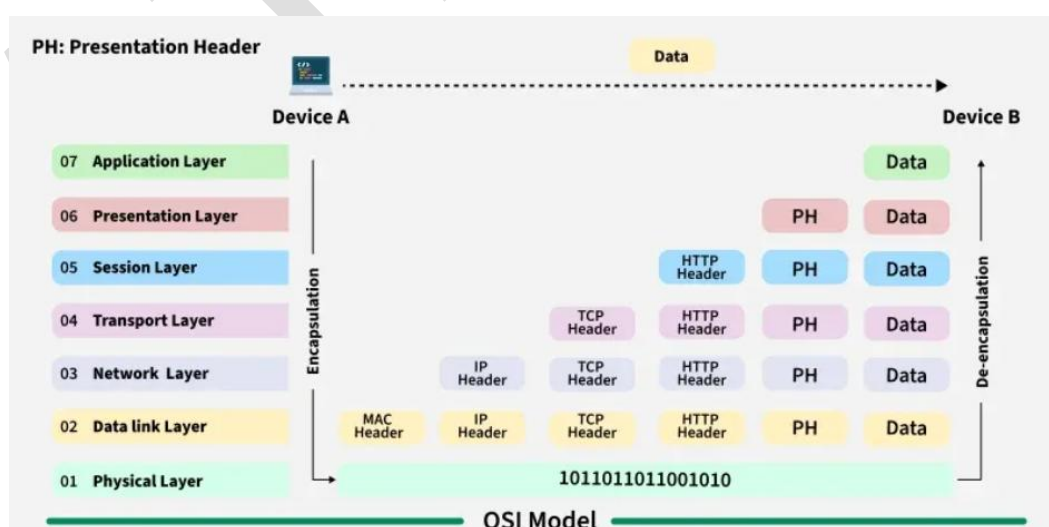
- The unit of communication at the application layer is a **Message or Data**.

2.3.1 Drawbacks of OSI model

- OSI was too loosely defined and proprietary standards were too entrenched.
- It's not even tangible.
- The OSI model doesn't do any functions in the networking process.



Encapsulation



De Encapsulation

2.3.2 COMPARISON OF OSI MODEL AND TCP/IP REFERENCE MODEL

OSI Model	TCP / IP
1) It has 7 layers	1) Has 4 layers
2) Transport layer guarantees delivery of packets	2) Transport layer does not guarantees delivery of packets
3) Separate presentation layer,	3) No session layer, 4) No presentation layer,
4) Separate session layer.	characteristics are provided by appln layer
5) Network layer provides both connectionless and oriented services.	5) Network layer provides only connection less services
6) It defines the services, interfaces and protocols very clearly and makes a clear distinction between them.	6) No clear distinguishes between service interface and protocols
7) The protocol is better hidden and can be easily replaced as the technology changes.	7) It is not easy to replace the protocols
8) OSI truly is a general model.	8) TCP/IP cannot be used for any other application
9) It has a problem of protocol filtering into a model	9) The model does not fit any protocol stack.

3 TRANSMISSION MEDIA

3.1 INTRODUCTION

Transmission media are actually located below the physical layer and directly controlled by the physical layer. We could say that transmission media belong to layer Transmission media are actually located below the physical layer and are directly con zero Figure 3.1 shows the position of transmission media in relation to the physical layer.

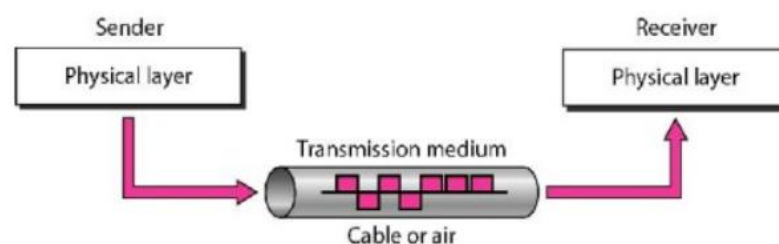


Figure 3.1 Transmission Medium and Physical Layer

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air. The air can also be used to convey the message in a smoke signal or semaphore. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane.

In data communications the definition of the information and the transmission medium is more specific. The transmission medium is usually **free space, metallic cable, or fiber-optic cable**. The information is usually a signal that is the result of a conversion of data from another form.

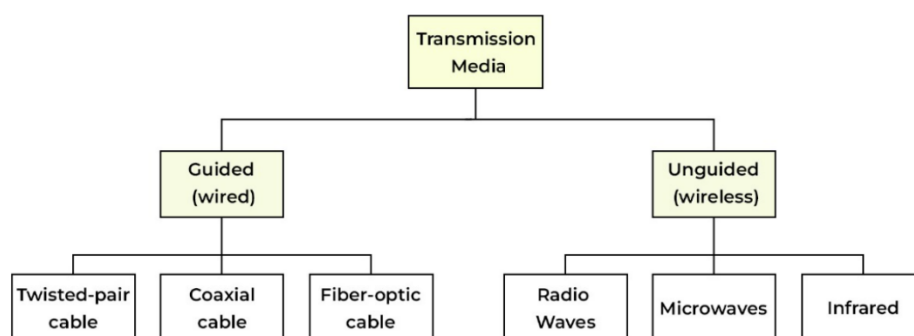
The use of long-distance communication using electric signals started with the invention of the telegraph by Morse in the 19th century. Communication by telegraph was slow and dependent on a metallic medium.

Extending the range of the human voice became possible when the telephone was invented in 1869. Telephone communication at that time also needed a metallic medium to carry the electric signals that were the result of a conversion from the human voice. The communication was, however, unreliable due to the poor quality of the wires. The lines were often noisy and the technology was unsophisticated.

These signals are transmitted from one device to another in the form of electromagnetic energy, which is propagated through transmission media.

Electromagnetic energy, a combination of electric and magnetic fields vibrating in relation to each other, includes power, radio waves, infrared light, visible light, ultraviolet light, and X, gamma, and cosmic rays. Each of these constitutes a portion of the **Electromagnetic Spectrum**.

7.2 CLASSIFICATION OF TRANSMISSION



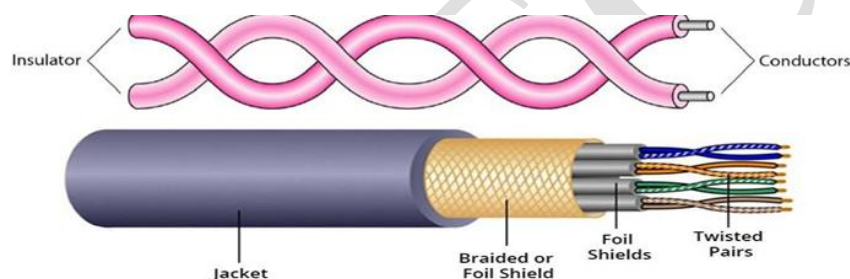
7.2 GUIDED MEDIA (WIRED)

- Guided media, which are those that provide a conduit (Channel) from one device to another, include **twisted-pair cable, coaxial cable, and Fiber-optic cable**.

- A signal traveling along any of these media is directed and contained by the physical limits of the medium.
- Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of **Electric Current**.
- Optical fiber is a cable that accepts and transports signals in the form of **Light**.
- Classification of Guided media are
 1. **Twisted-Pair Cable**
 2. **Coaxial Cable**
 3. **Fiber-Optic Cable**

7.2.1 Twisted – Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.



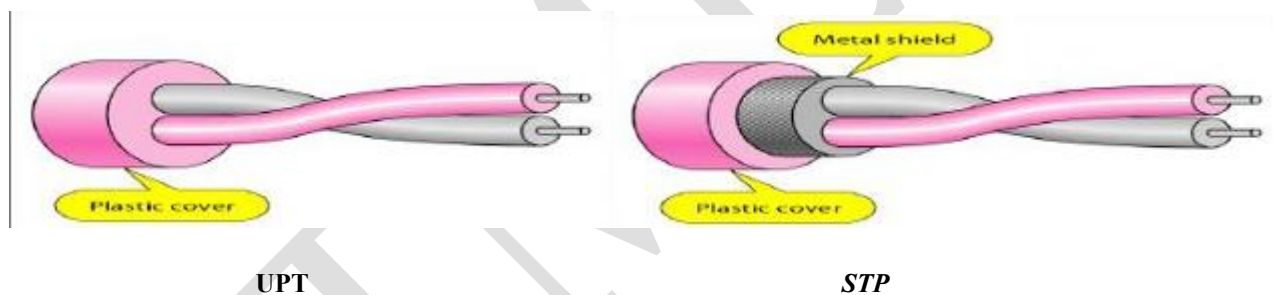
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.
- In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.
- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e.g., one is closer and the other is farther). This results in a difference at the receiver.
- By twisting the pairs, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther, in the next twist, the reverse is true.
- Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals.
- The unwanted signals are mostly cancelled out. From the above discussion, it is clear that the number of twists per unit of length (e.g., inch) has some effect on the quality of the cable.
- Then Further Twisted – Pair Cable is Classified into Two Types

1. Unshielded Twisted – Pair Cable

2. Shielded Twisted – Pair Cable

Unshielded Versus Shielded Twisted-Pair Cable

- The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP).
- IBM has also produced a version of twisted-pair cable for its use, called shielded twisted-pair (STP). STP cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors.
- Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.
- The difference between UTP and STP Our discussion focuses primarily on UTP because STP is seldom used outside of IBM.



Categories of Unshielded Twisted-Pair Cable

The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable for specific uses. Table shows these categories.

Categories of unshielded twisted-pair cables

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Ring & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring

Connectors

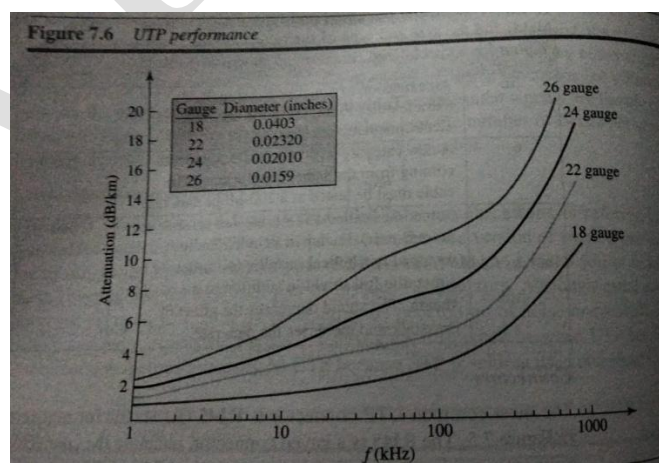
- The most common UTP connector is RJ45 (RJ stands for registered jack).
- The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.

Application

- Twisted-pair cables are used in telephone lines to provide voice and data channels.
- Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

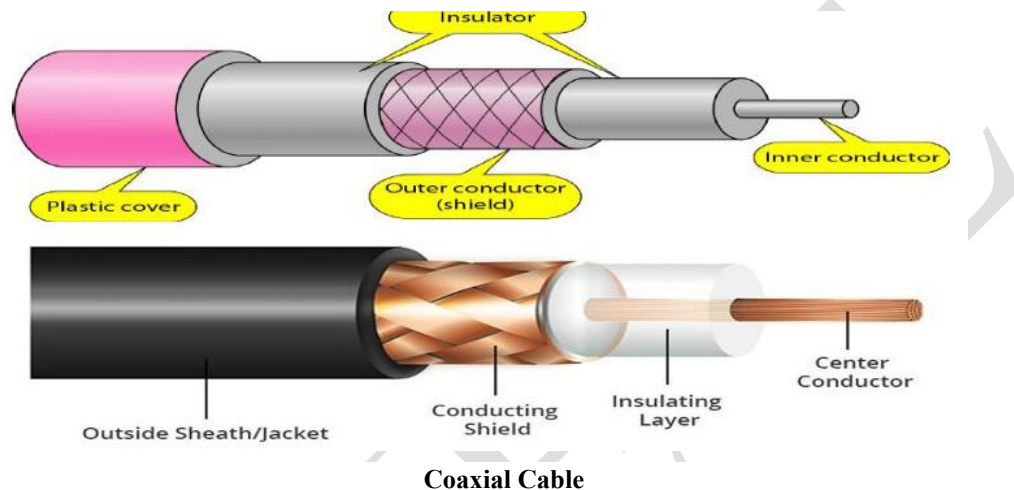
Performance

One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. A twisted-pair cable can pass a wide range of frequencies. However, Figure shows that with increasing frequency, the attenuation, measured in decibels per kilometer (dB/km), sharply increases with frequencies above 100 kHz. Note that gauge is a measure of the thickness of the wire.



7.2.2 Coaxial Cable

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



Applications

- Coaxial cable was widely used in analog telephone networks, digital telephone networks. Cable TV networks also use coaxial cables.
- Another common application of coaxial cable is in traditional Ethernet LANs.

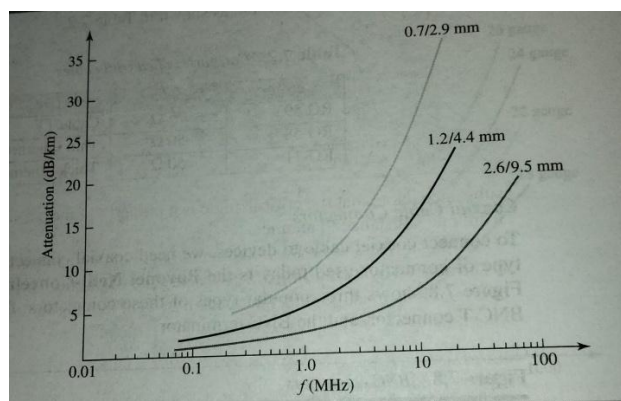
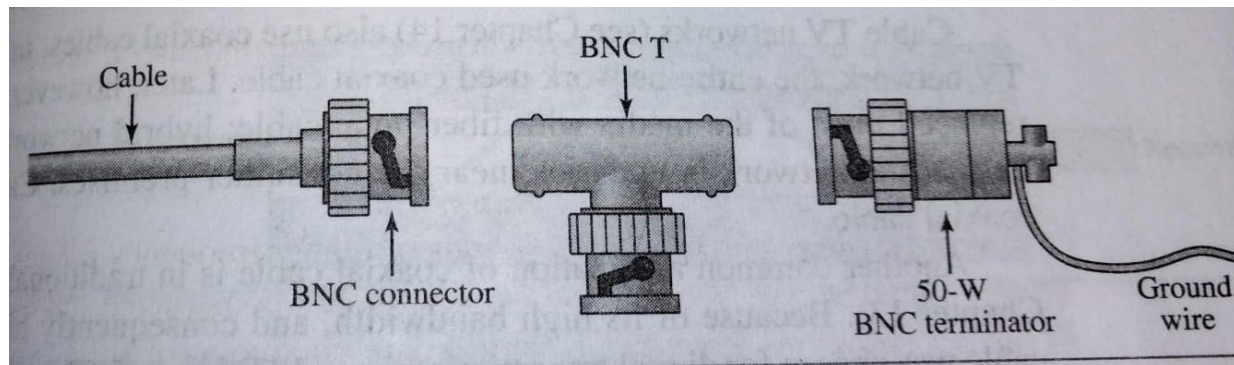
Coaxial Cable Standards

Coaxial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function, as shown in Table

Category	Impedance	Use
RG-59	75Ohm	Cable Tv
RG-58	50Ohm	Thin Ethernet
RG-11	50Ohm	Thick Ethernet

Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayonet Neill-Concelman (BNC) connector. Figure 7.8 shows three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator.

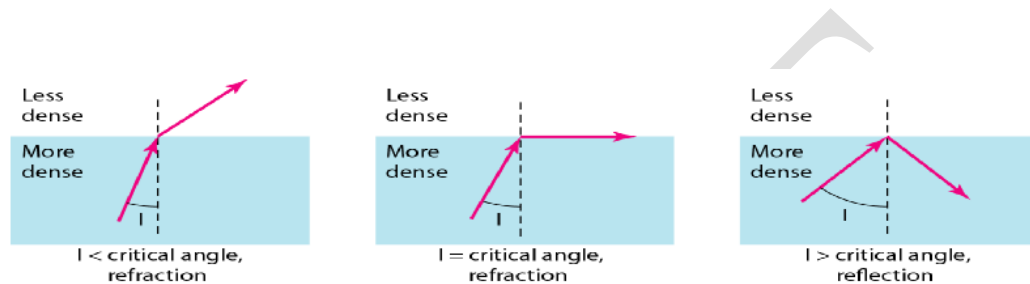


Cable TV networks (see Chapter 14) also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Later, however, cable TV providers replaced most of the media with fiber-optic cable, hybrid networks use coaxial cable only at the network boundaries, near the consumer premises. Cable TV uses RG-59 coaxial cable.

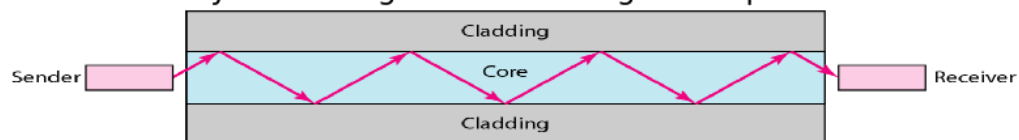
Another common application of coaxial cable is in traditional Ethernet LANs (see Chapter 13). Because of its high bandwidth, and consequently high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs. The 10Base-2, or Thin Ethernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10 Mbps with a range of 185 m. The 10Base5, or Thick Ethernet, uses RG-11 (thick coaxial cable) to transmit 10 Mbps with a range of 5000 m. Thick Ethernet has specialized connectors

7.2.3 Fiber-Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. Bending of light ray.



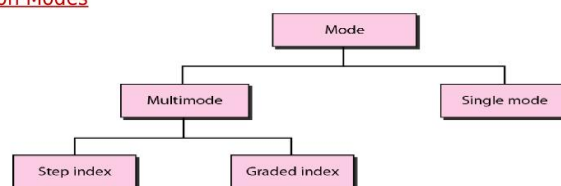
Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic.



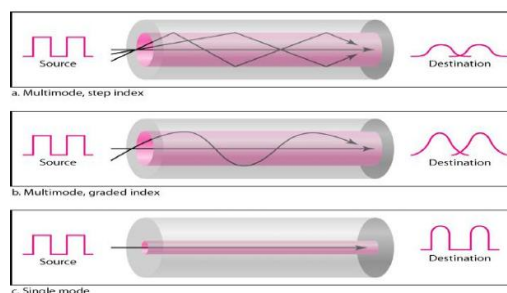
Propagation Modes

Core Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multi-mode can be implemented in two forms step-index or graded-index.

Propagation Modes



Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core, as shown in Figure.



Multimode

Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core.

In **multimode step-index fiber**, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. The term step index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber. A second type of fiber, called **multimode graded-index fiber**, decreases this distortion of the signal through the cable. The word index here refers to the index of refraction.

Single-Mode

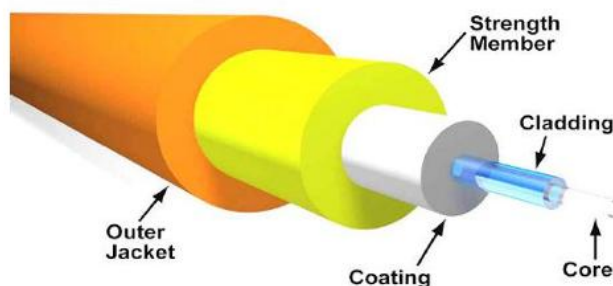
Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.

Fiber Types

Type	Core	Cladding	Mode
50/125	50.0	125	Multimode,graded index
62.5/125	62.5	125	Multimode,graded index
100/125	100.0	125	Multimode,graded index
7/125	7.0	125	Single mode

Fiber Construction

Fiber Construction



The subscriber channel (SC) connector, The straight-tip (ST) connector, MT-RJ (mechanical transfer registered jack) is a connector.

Applications

Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.

Advantages and Disadvantages of Optical Fiber

Advantages Fiber-optic cable has several advantages over metallic cable (twisted pair or coaxial).

1. Higher bandwidth.

2. Less signal attenuation Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted pair cable. **3 Immunity to electromagnetic interference.** Electromagnetic noise cannot affect fiber-optic cables.

3. Immunity to electromagnetic interference Electromagnetic noise cannot affect fiber-optic cables.

4. Resistance to corrosive materials. Glass is more resistant to corrosive materials than copper.

5 Light weight. Fiber-optic cables are much lighter than copper cables.

6 Greater immunity to tapping. Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages

There are some disadvantages in the use of optical fiber.

1. Installation and maintenance

2. Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

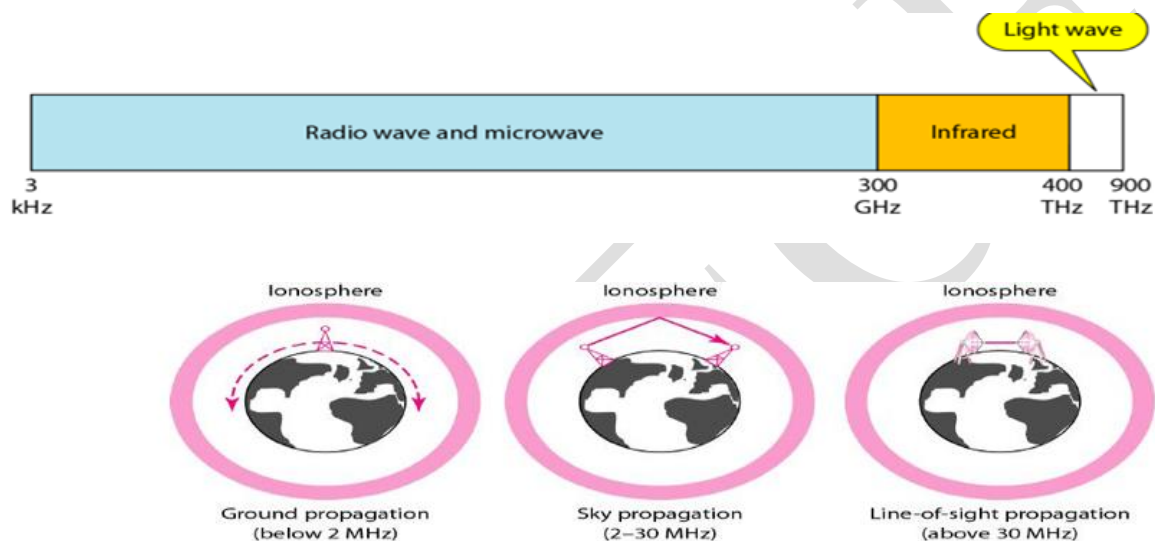
3 Cost The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

7.3 UNGUIDED MEDIA: WIRELESS

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them Figure 7.17.

The part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication. Unguided signals can travel from the source to the destination in several ways: **ground propagation**, **sky propagation**, and **line-of-sight propagation**, as shown in Figure.



In **ground propagation**, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal. The greater the power, the greater the distance.

In **sky propagation**, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances with lower output power.

In **line-of-sight propagation**, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

The section of the electromagnetic spectrum defined as radio waves and microwaves is divided into eight ranges, called bands, each regulated by government authorities. These bands are rated from very

low frequency (VLF) to extremely high frequency (EHF) Table 7.4 lists these bands, their ranges, propagation methods, and some applications.

Table 7.4 Bands

Band	Range	Propagation	Application
very low frequency (VLF)	3–30 kHz <i>kHz</i>	Ground	Long-range radio navigation
low frequency (LF)	30–300 kHz	Ground	Radio beacons and navigational locators

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

1. **Radio Waves**
2. **Microwaves**
3. **Infrared**

1. Radio Waves

Radio Waves Electromagnetic waves ranging in frequencies between **3 kHz and 1 GHz** are **normally called radio waves**. Radio waves are omni directional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna. The omni directional property has a disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

Omni directional Antenna

Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. Figure shows an omnidirectional antenna.

Applications

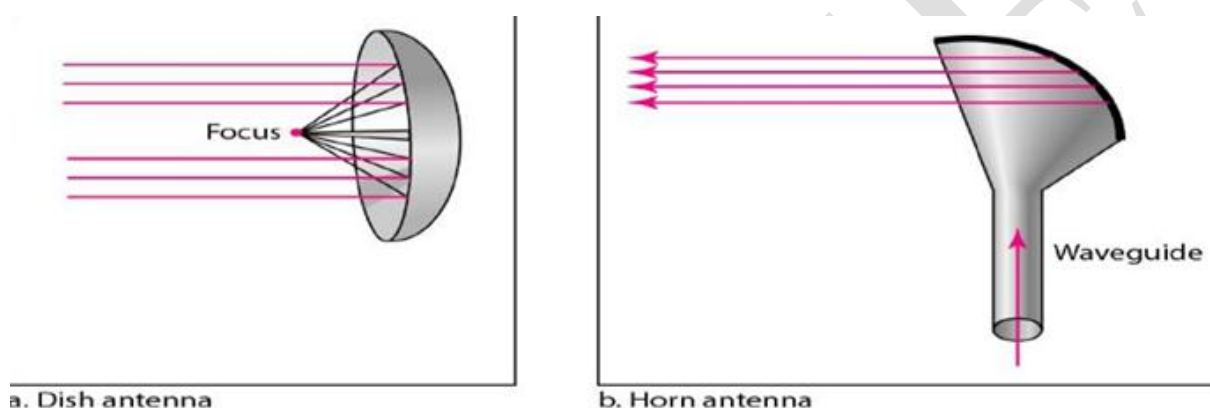
The Omni directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. **AM and FM radio, television, maritime radio, cordless phones, and paging** are examples of multicasting.

2. Microwaves

Electromagnetic waves having frequencies **between 1 and 300 GHz** are called **microwaves**. **Microwaves are unidirectional**. The sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

Unidirectional Antenna

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: **the parabolic dish and the horn Unidirectional Antenna**.



A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus.

The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

Outgoing transmissions are broadcast through a horn aimed at the dish. The micro-waves hit the dish and are deflected outward in a reversal of the receipt path.

A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem (resembling a handle) and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

Applications:

Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

3. Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication.

Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room.

When we use our infrared remote control, we do not interfere with the use of the remote by our neighbours. Infrared signals are useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications: Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.