COMPUTER NETWORK
UNIT I

Unit 1: Introduction – Network Hardware – Network Software – Reference Models – OSI and TCP/IP Models – Example Networks: Internet, ATM, Ethernet and Wireless LANs – Physical Layer – Theoretical Basis for Data Communication – Guided Transmission Media.

INTRODUCTION:

COMPUTER NETWORK:

- **Computer network is a collection of electronic devices which are connected together via either wired or wireless medium to communicate the information among themselves.**

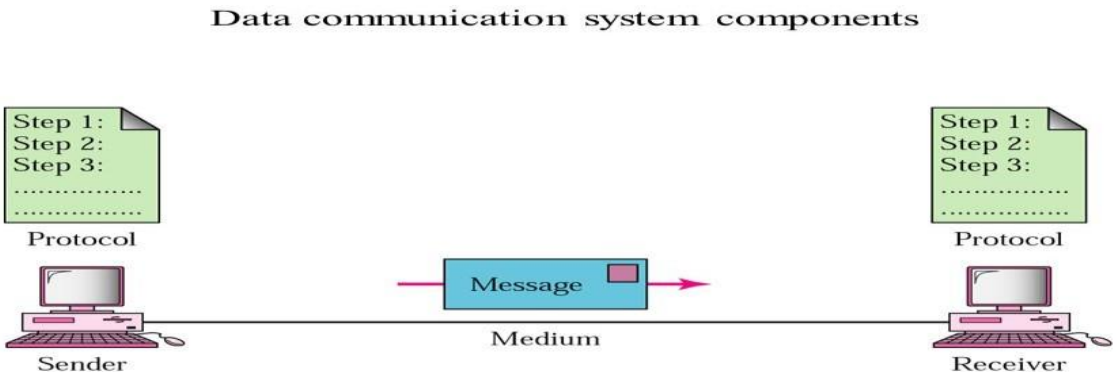
- **The devices are either desktop computers, laptops, digital notepads, mobile phones, printers, servers, Modems, switches and bridges.**

1.Introduction to Data communication:

- The word **data** refers to facts, concepts, and instructions presented in whatever form is agreed upon by the parties creating and using data.
- In computer information systems, data are represented by binary information units(or bits) produced in the form of **0's and 1's**.
- **DATA COMMUNICATION** is the exchange of data between two devices via some form of transmission medium (such as a wire cable).
- Data communication is considered local if the communicating devices are in the same building or restricted area.
- The effectiveness of a data communication system depends on three fundamental characteristics: **(2 marks)**

1. **Delivery:** The system must deliver data to the correct destination. Data must be received by user.
2. **Accuracy:** The system must deliver data accurately. Data that have been alteredin transmission and left uncorrected are unusable.
3. **Timeliness:** The system must deliver data in a timely manner without significantdelay.
4. Jitter: It refers as the variation in the arrival of the part of the data. In network the data are split into smaller groups and send them separately.

Components: (2 marks)



1. **Message**: Communication of a message or data will be transmitted from one device andwill be received in the destination or target device.
2. **Sender:** A data must has to be sent to a destination from a source. This source is called the sender.
3. **Receiver:** The destination of a transmitted data is the receiver which will receive the data.
4. **Transmission medium:** The transmission medium is the physical path for the data to travel to its destination after being sent by the Sender.
5. **Protocol:** A protocol is nothing but a set of rules that applies on the full data communication procedure. This is like an agreement between the two devices to successfully communicate witheach other.

Applications of Network:

There are a variety of fields in computer networks that are used in industries. Some of them are as follows:

1. **Internet and World Wide Web**

In computer networks, we have a global internet, also known as the World Wide Web, that offers us various features like access to websites, online services and retrieval of information. With the help of the World Wide Web, we can browse, and we can do search, and access web pages and multimedia content.

2. **Communication**

With the help of computer networks, communication is also easy because we can do email, instant messaging, voice and video calls and video conferencing, which helps us to communicate with each other effectively. People can use these features in their businesses and organizations to stay connected with each other.

3. **File Sharing and Data Transfer:**

Data transfer and file sharing are made possible by networks that connect different devices. This covers file sharing within a business setting, file sharing between personal devices, and downloading/uploading of content from the internet.

4. **Online gaming**

Multiplayer online games use computer networks to link players from all over the world, enabling online competitions and real-time gaming experiences.

5. **Remote Access and Control**

Networks enable users to access and control systems and devices from a distance. This is helpful when accessing home automation systems, managing servers, and providing remote IT support.

6. **Social media**

With the help of a computer network, we can use social media sites like Facebook, Twitter and Instagram to help people set up their profiles, and we can connect with others and share content on social media.

7. **Cloud Computing**

The provision of on-demand access to computing resources and services hosted in distant data centres relies on networks. Some example of cloud computing is software as a service (SaaS), platform as a service (PaaS) and infrastructure as service (IaaS).

8. **Online Banking and E-Commerce**

Online banking and e-commerce platforms, where customers conduct financial transactions and make online purchases, require secure computer networks.

9. **Enterprise Networks**

Computer networks, we have some networks that are only used in businesses and organizations so they can store data and share files and resources like printers, scanners, etc.

10. **Healthcare**

With the help of computer networks in the health industry, we can share patient records and store the records in the form of data that is easy and secure compared to the file method. Networks are also necessary for telemedicine and remote patient monitoring.

11. Education

Schools use networks to access online courses, virtual classrooms, and other online learning materials. Campuses of colleges and universities frequently have extensive computer networks.

12. Transportation and Logistics

The transportation sector uses Computer Networks to manage and track shipments, plan the best routes, and coordinate logistics activities.

13. Internet of Things (IoT) and Smart Homes

Through the Internet of Things (IoT), smart homes use networks to connect to and manage a variety of devices, including thermostats, security cameras, and smart appliances.

14. Scientific Research

To share data, work together on projects, and access high-performance computing resources for data analysis and scientific simulations, researchers use networks.

15. Government and Defense

With the help of computer networks, we can communicate, share data, and advance national defense. Government agencies and the military rely on secure networks.

Issues of Computer Network:

1. **Privacy issues**

Computer networks are a significant concern due to the potential for unauthorized access, data breaches, and misuse of personal information. Here are some key privacy issues in computer networks:

- **Unauthorized access to sensitive information such as personal data, financial information, and confidential business details.**
- **Can lead to identity theft, financial loss, and reputational damage.**
- **Encryption: Use strong encryption methods for data transmission and storage.**
- **Access Control: Implement robust access control mechanisms to limit who can access sensitive information.**
- **Regular Audits: Conduct regular security audits and vulnerability assessments.**
- **User Education: Educate users about safe online practices, phishing, and social engineering tactics.**
- **Update and Patch Systems: Keep software and systems up to date with the latest security patches.**

2. **Unauthorized access**

Computer networks refers to gaining entry into a system, network, or data without permission.

Hacking

- **Using technical skills to exploit vulnerabilities in software, hardware, or network configurations to gain unauthorized access.**

Phishing

- **Sending deceptive emails or messages to trick individuals into revealing their login credentials or other sensitive information.**

Strong Password Policies

- **Encourage the use of complex, unique passwords and implement regular password changes.**

3. **Ethical issues**
   - **Computer networks involve the principles and standards governing the conduct of individuals and organizations in their use of networked systems.**
   - **Protection of Data: Ensuring the security of data to prevent unauthorized access.**
   - **Education and Awareness: Promoting ethical awareness and education among users, developers, and IT professionals.**
   - **Identity Theft: The moral obligation to protect individuals from identity theft and fraud.**
4. **Political issues**
   - **Computer networks encompass a wide range of concerns related to governance, power dynamics, regulatory frameworks, and the impact of networked technologies on society and politics. Here are some of the key political issues in computer networks:**
   - **Fake News: The spread of false information online and its impact on public opinion and democratic processes.**
   - **Election Security: Political measures to protect electoral systems from cyber attacks and manipulation, including voter registration databases and electronic voting systems.**

NETWORK HARDWARE:

Network hardware is a set of physical or network devices that are essential for interaction and communication between hardware units operational on a computer network. These are dedicated hardware components that connect to each other and enable a network to function effectively and efficiently.

Criteria Of Network

- A network must be able to meet certain criteria are performance, reliability, andsecurity.
- **Performance**

  Performance can be measured in many ways, including **transit time and response time.**

Transit time is the amount of time required for a message to travel from one device to another.

Response time is the elapsed time between an inquiry and a response.

- **Reliability**
  - In addition to accuracy of delivery, network reliability is measured by thefrequency of failure,
  - The time it takes a link to recover from a failure.
- **Security**
  - Network security issues include protecting data from unauthorized access,
  - Protecting data from damage and development, and implementing policies
  - Procedures for recovery from breaches and data losses.
- **Throughput and Delay**
  - The throughput of the network is measures as amount of data transferred For specified period of time. The high transmission within the specified Period of time is called as high throughput.
- **Delay:**
  - The delay is measured as time difference between the transit time and actual time taken to transmit.

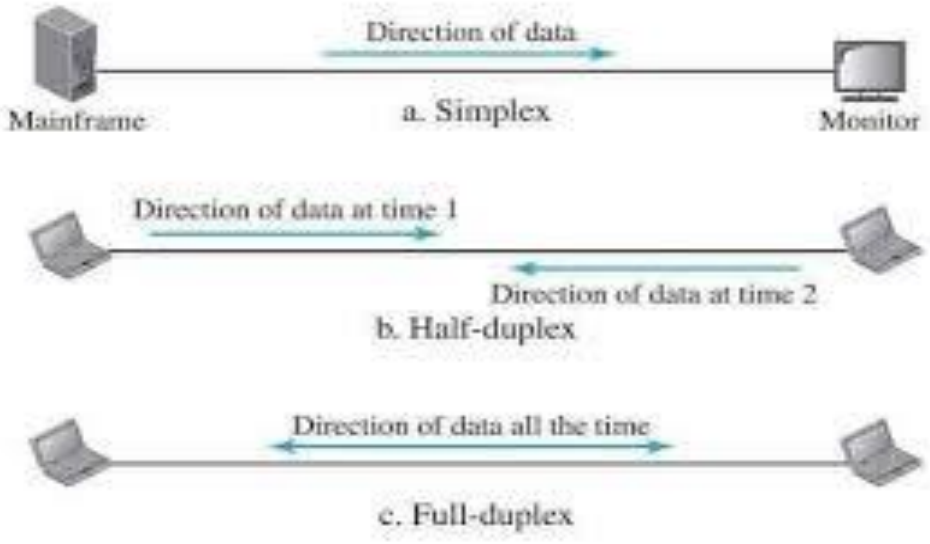
Transmission mode or data flow: (Unom-5marks)

- A given transmission on a communications channel between two machines can occur in several differentways.
- The transmission is characterized by:

✓ The direction of the exchanges

✓ The transmission mode: the number of bits sent simultaneously

✓ synchronization between the transmitter and receiver



Types of Transmission mode

- Simplex
- Half Duplex
- Full Duplex

Simplex

- **A simplex connection** is a connection in which the data flows in only one direction, from thetransmitter to the receiver.
- This type of connection is useful if the data do not need to flow in both directions
- (for example, from your computer to the printer or from the mouse to your computer...).

Half Duplex

- **A half-duplex connection** (sometimes called an *alternating connection* or *semi-duplex*) is a connection in which the data flows in one direction or the other, but not both at the same time.
- With this type of connection, each end of the connection transmits in turn.
- This type of connection makes it possible to have bidirectional communications using the fullcapacity of the line.

Full Duplex

- **A full-duplex connection** is a connection in which the data flow in both directionssimultaneously.
- Each end of the line can thus transmit and receive at the same time,
- transmission medium is used for both directions of transmission.

Type of Connection

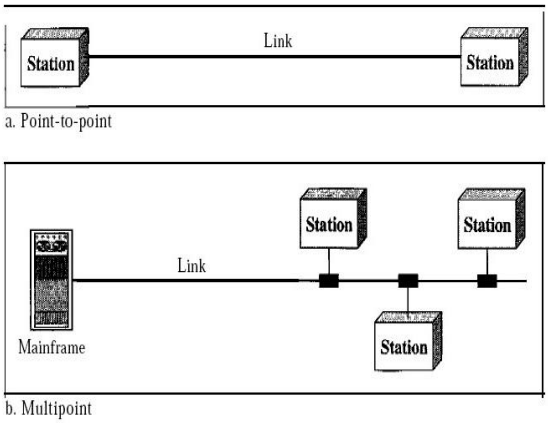
- A network is two or more devices connected through links.
- A link is a communications pathway that transfers data from one device to another.There are two possible types of connections:

point-to-point and multipoint.

Point-to-Point: A point-to-point connection provides a dedicated link between two devices. When you change television channels by infrared remote control, establishing apoint-to-point connection between the remote control and the television's control system.

Multipoint: A multipoint (also called multidrop) connection is one in which more thantwo specific devices share a single link In a multipoint environment, the capacity of thechannel is shared, either spatially or temporally.

Figure 1.3 *Types ofconnections: point-to-point and multipoint*



PROTOCOLS : 5 marks

- Protocol is a set of rules that governs communication.
- The key elements of protocol are syntax, semantics and timing.

  Syntax:

  Syntax refers the structure and format of the information data.

  Semantics:

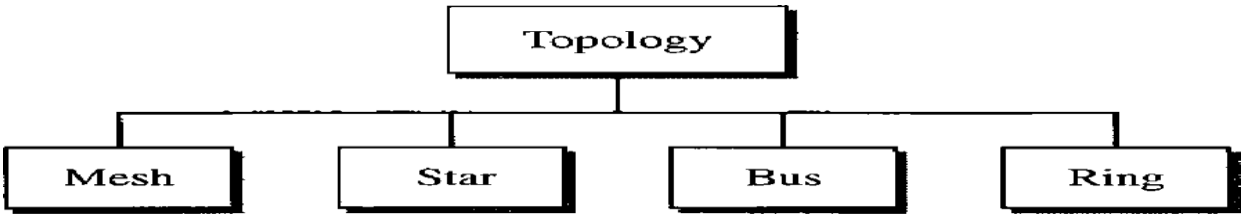
  Semantics refers to the meaning of each section of bits. It does an route identify theroute to be taken or the final destination of the message.

  Timing:

  Timing refers to two characteristics: when data should be sent and how fast it shouldbe sent.
- It dictates how to format, transmit and receive data
- Computer network devices -- from servers and routers to endpoints -- can communicate regardless of the differences in their underlying infrastructures,designs or standards.

Network Topology :(U-5marks)

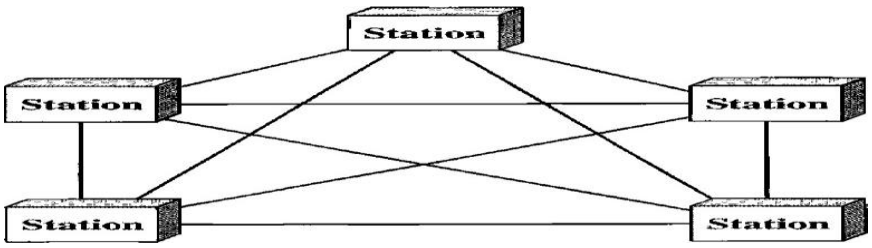
- The term ***physical topology*** refers to the way in which a network is laidout physically.
- 1 or more devices connect to a link; two or more links form a topology.



There are four basic topologies possible: **mesh, star, bus, and ring**

MESH TOPOLOGY:

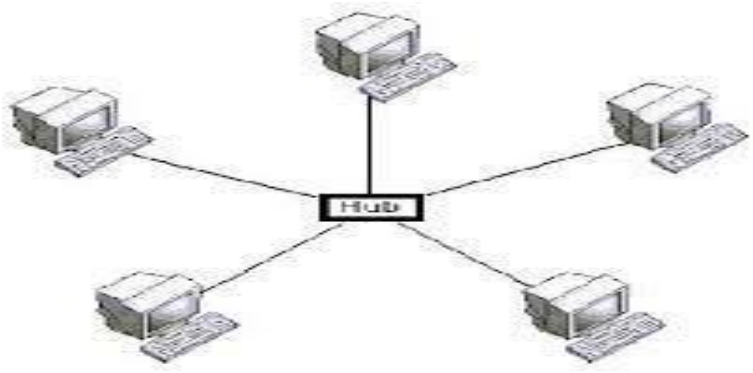
- A mesh offers several advantages over other network topologies.
- First, the use of dedicated links guarantees that each connection cancarry its own data load, thus eliminating
- The traffic problems that can occur when links must be shared bymultiple devices.
- Mesh has **n(n-1)/2 physical channels** to link n devices.
- There are **two techniques** to transmit data over the Mesh Topologyare:
- **Routing:** The nodes have a **routing logic**. Routing logic to direct the data toreach the destination using the **shortest distance**.



ADVANTAGES	DISADVANTAGES
Fully connected	Each connection can carry its own data load.
Robust	Robust
Not flexible	Fault is diagnosed easily, provides security and privacy.

STAR TOPOLOGY:

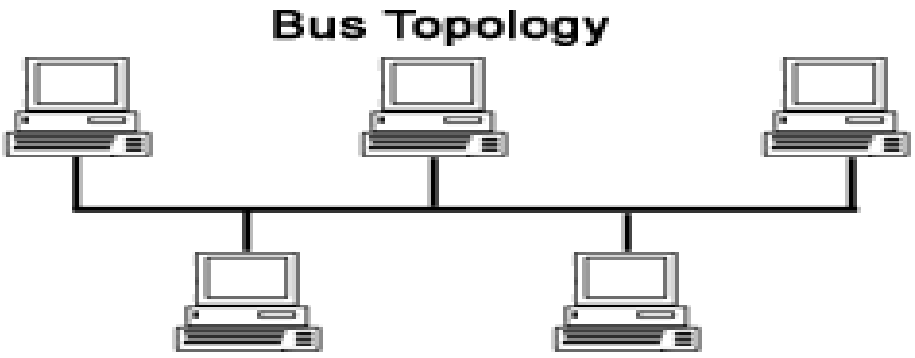
- All the computers are connected to a single hub through a cable.
- This hub is the central node and all others nodes are connected to the central node.
- It used with twisted pair, optical fiber or coaxial cable.



ADVANTAGES	DISADVANTAGES
Fast performance with few nodes and low network traffic	Performance is based on the hub
Hub can be upgraded easily	Expensive to use
Easy to troubleshoot	If the hub fails then the whole networkis stopped.
Easy to setup and modify	All the nodes depend on the hub.
Only the affected node has failed, rest of the nodes can work smoothly	Cost of installation is high

BUS TOPOLOGY*:*

- Every computer and network device is connected to single cable.
- When it has exactly two endpoints.
- It is also called **Linear Bus Topology**.



ADVANTAGES	DISADVANTAGES
It is cost effective	Cables fails then whole network fails
Easy to understand	If network traffic is heavy or nodes aremore, performance decreases
Used in small networks	Cable has a limited length
Easy to expand joining two cables Together	It is slower than the ring topology

RING TOPOLOGY:

- Each computer is connected to another computer, with the last one connectedto the first.
- Exactly two neighbors for each device.
- The transmission is unidirectional, but it can be made bidirectional by having2 connection between each node it is called **Dual Ring Topology.**
- Data transferred in a sequential manner that is bit by bit.

ADVANTAGES	DISADVANTAGES
Transmitting network is not affected by high traffic	Troubleshooting is difficult
Cheap to install and expand	Adding or deleting the computers disturbs the network activity
Easy identification of fault	Failure of one computer disturb the whole network

Types of Network :(U-5 marks)

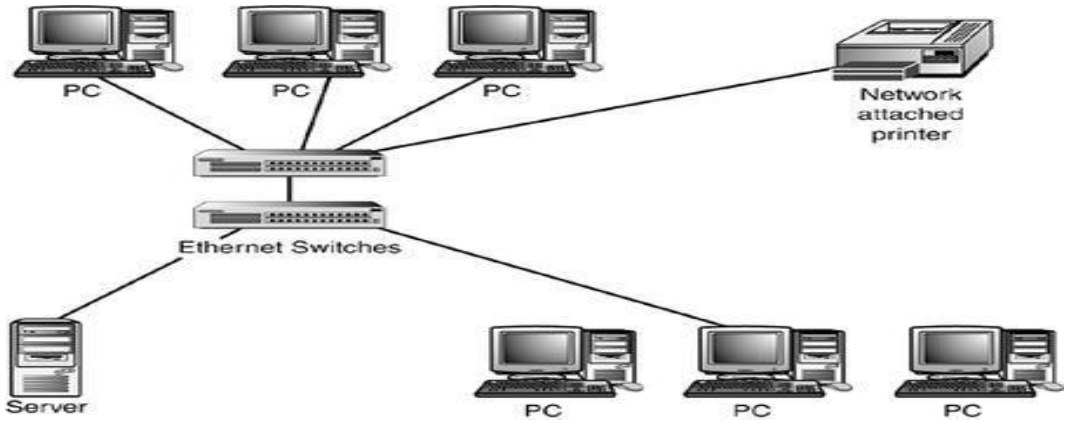
- One way to categorize the different types of computer network designs is by theirscope or scale.
- Common examples of area network types are:
  - ❖ LAN - Local Area Network
  - ❖ WAN - Wide Area Network
  - ❖ MAN - Metropolitan Area Network
  - ❖ PAN – Personal Area Network

1. PAN(Personal Area Network):

- ✓ Personal Area Network (PAN) is the computer network that connects computers/devices within the range of an individual person.
- ✓ As PAN provides a network range within a person's range typically within a range of 10 meters (33 feet) it is called a Personal Area Network.

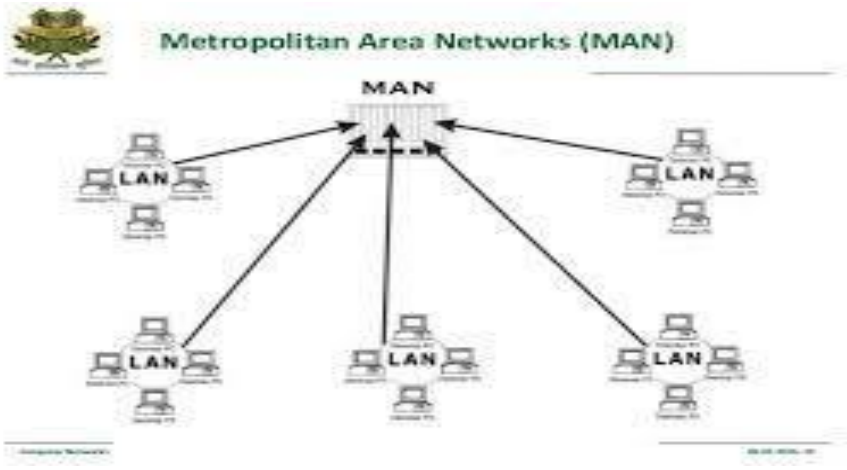
2. LAN(Local Area Network)

- Privately owned and links the devices in a single office, building, or campus.
- LAN can be as simple as two PCs.
- LAN are designed to allow resources to be shared between personal computers or workstation.
- The resources to be shared can include hardware, software or data.
- The most common LAN topologies are Bus, Ring and Star.
- LAN can be wired and ,wireless, or in both forms at once.
- LAN uses either Ethernet or Token-ring technology.



3. Metropolitan Area Network(MAN):

- **A** metropolitan area network is designed to extend over an entire city.
- A network spanning a physical area larger than a LAN but smaller than a WAN.
- It may be a single network such as a cable television network.
- A MAN may be wholly owned and operated by a private company.

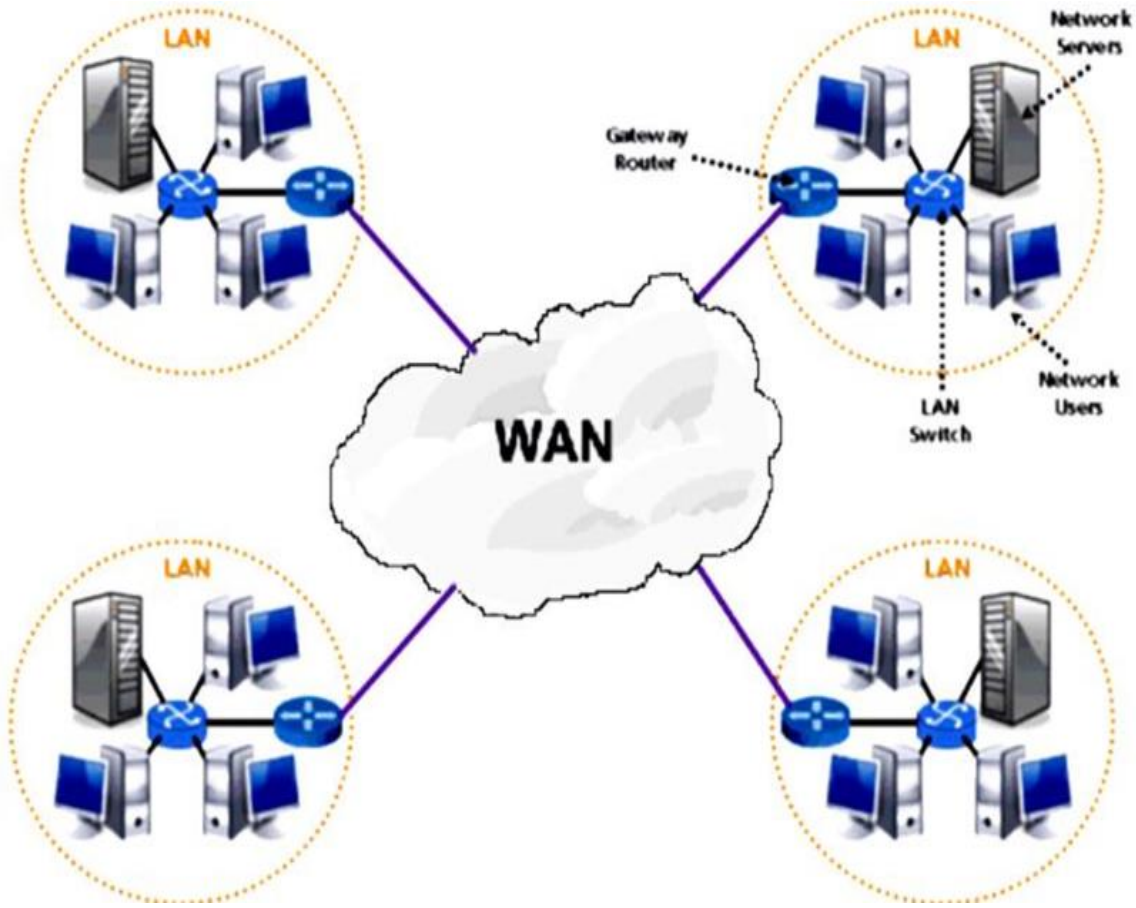


4. Wide Area Network:

- **A** wide area network provides long distance transmission of data, voice, image, and video information over large geographical areas that may comprise a country, a continent, or even the wholeworld.

- These networks provide connectivity to MANs and LANs.

- Since they are equipped with very high speed backbone, WANs use very expensive networkequipment.
    - WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM).



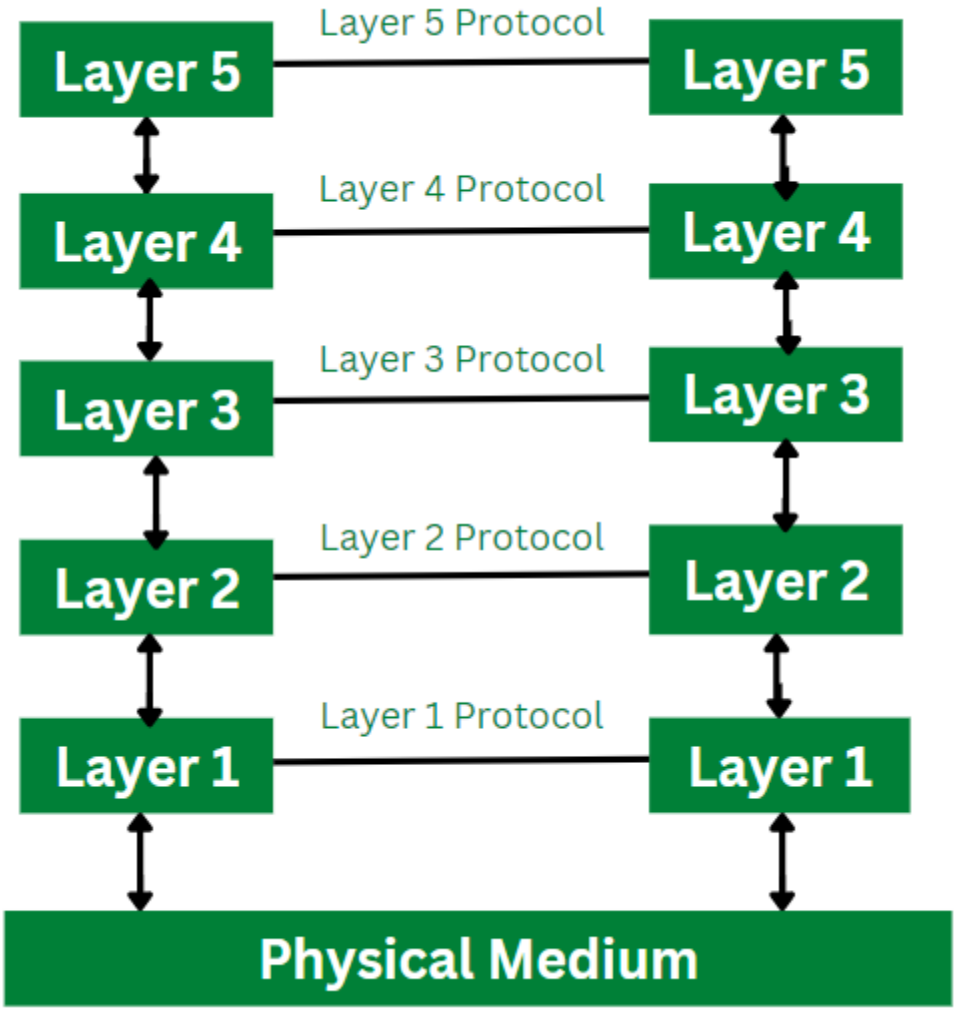
Network Software:

Network software is a broad term referring to a range of software applications designed to **enhance the functioning, management, and optimization of a computer network. This software facilitates communication among various interconnected devices, manages network operation, and monitors network performance.**

Layered Approach:

Every network consists of a specific number of functions, layers, and tasks to perform. Layered Architecture in a computer network is defined as a model where a whole network process is divided into various smaller sub-tasks. These divided sub-tasks are then assigned to a specific layer to perform only the dedicated tasks.

A single layer performs only a specific type of task.



Features of Layered Architecture

- **Use of Layered architecture in computer network provides with the feature of modularity and distinct interfaces.**
- **Layered architecture ensures independence between layers, by offering services to higher layers**

  from the lower layers and without specifying how these services are implemented.
- **Layered architecture segments as larger and unmanageable design into small sub tasks.**
- **In layer architecture every network has different number of functions, layers and content.**
- **In layered architecture, the physical route provides with communication which is available under the layer 1.**
- **In layered architecture, the implementation done by one layer can be modified by another layer.**

PROTOCOLS:

Protocol is a set of rules that governs communication.

- The key elements of protocol are syntax, semantics and timing.

Syntax:

Syntax refers the structure and format of the information data.

Semantics:

Semantics refers to the meaning of each section of bits. It does an route identify theroute to be taken or the final destination of the message.

Timing:

Timing refers to two characteristics: when data should be sent and how fast it shouldbe sent.

- It dictates how to format, transmit and receive data
- Computer network devices -- from servers and routers to endpoints -- can communicate regardless of the differences in their underlying infrastructures,designs or standards.

SERVICES:

- **Services are set of actions that a layer provides to the higher layer.**
- **These services are differed from each other to the layer to layer.**

Interfaces:

- **An interface is used to transmit data from the top layer to the lower layer.**
- **A layered design offers a clear interface, allowing for the transmission of only the most crucial information across levels.**
- **Additionally, it guarantees that the implementation of one layer may be easily modified by another.**

Standards and addresses:

In a layered approach to network architecture, different standards and addresses are associated with different layers.

- ✓ **International Organization for Standardization (ISO).**
- ✓ **International Telecommunication Union-Telecommunication Standards Sector(ITU-T).**
- ✓ **American National Standards Institute(ANSI).**
- ✓ **Institute of Electrical and Electronics Engineers(IEEE).**
- ✓ **Electric Industries Association(EIA).**

Addresses:

1. **Internetworking Protocol(IP) address:**

An IP address is a unique identifier assigned to a device or domain that connects to the Internet. Each IP address is a series of characters, such as '192.168.1.1'. Via DNS resolvers, which translate human-readable domain names into IP addresses, users are able to access websites without memorizing this complex series of characters.

2. **MAC (Media Access Control) Address**

A unique identifier assigned to network interfaces for communications on the physical network segment.

3. **Port Address:**

A port address (often just referred to as a port) is a numerical identifier used to distinguish between different services or processes on a single device. Ports allow multiple services to run simultaneously on a single IP address.

Connection Oriented Service:

- ✓ **Connection-Oriented Service is basically a technique that is typically used to transport and send data at session layer.**
- ✓ **The data streams or packets are transferred or delivered to receiver in a similar order in which they have seen transferred by sender.**
- ✓ **It is actually a data transfer method among two devices or computers in a different network that is designed and developed after telephone system.**
- ✓ **Whenever a network implements this service, it sends or transfers data or message from sender or source to receiver or destination in correct order and manner.**

Connectionless service:

- ✓ **A Connectionless Service is technique that is used in data communications to send or transfer data or message at Layer 4 i.e., Transport Layer of Open System Interconnection model.**
- ✓ **This service does not require session connection among sender or source and receiver or destination. Sender starts transferring or sending data or messages to destination.**
- ✓ **In other words, we can say that connectionless service simply means that node can transfer or send data packets or messages to its receiver even without session connection to receiver.**
- ✓ **Message is sent or transferred without prior arrangement. This usually works due to error handling protocols that allow and give permission for correction of errors just like requesting retransmission.**

Service Primitives:

Service Primitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Listen – server, Connect – client to server and then connection is established

Five service primitives for implementing a simple connection-oriented service.

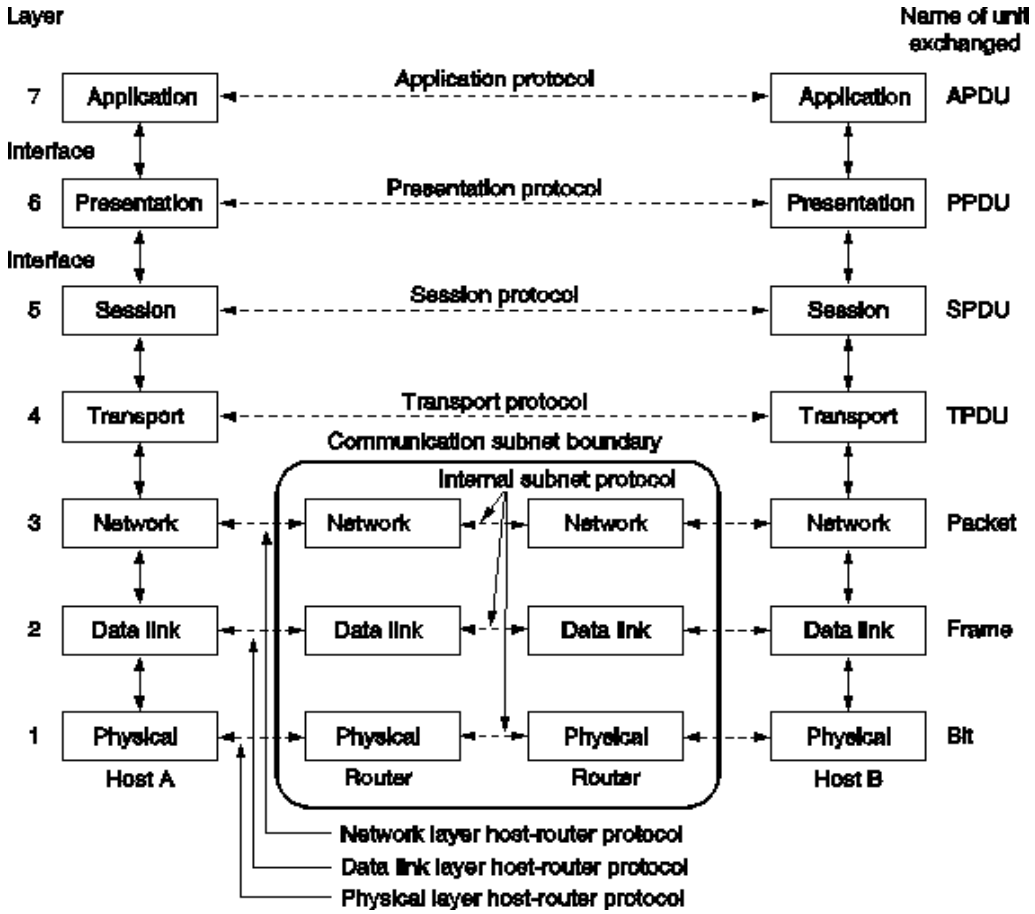
NETWORK MODELS:

OSI Reference Model:

- In 1947 the International Standards Organization (ISO) is a multinational body dedicated toworldwide agreement on International standards.
- **An ISO** standard that covers all aspects of network communications is the Open SystemInterconnection (OSI) model.
- The purpose of the OSI model is to show how to communication between different systemswithout requiring changes to the logic.
- OSI model is not a protocol.
- It is a model for understanding and designing a network architecture that is flexible, robust, andinteroperable.
- The OSI model is a layered framework for the design of network systems that allowscommunication between all types of computer systems.
- It consists of seven separate but related layers.
- Each of which define a part of the process of moving information across a network.

Layers of OSI model:

- **The** OSI model is composed of seven ordered layers.
- **The** processes of each machine that communicate at a given layer are called peer- to-peer processes.
- **Communication** between machines is a peer-to-peer process using the protocolsappropriate to a given layer.
- **Peer-to-peer** processes at the physical layer, communication is direct.
- **A sends a stream of bits to device B.**



Layer 1: Physical Layer

- Function: Transmission and reception of raw bit streams over a physical medium.
- Key Components: Cables, switches, hubs, network interface cards (NICs).
- Tasks:
- Data Encoding: Converts data bits into signals.
- Signaling: Determines the electrical, optical, or radio signals.
- Transmission Medium: Establishes how data is transferred physically (e.g., copper wires, fiber optics).
- Physical Topology: Describes the physical layout of devices in the network.

Layer 2: Data Link Layer

- Function: Ensures reliable node-to-node data transfer.
- Sub-layers:
- Logical Link Control (LLC): Manages frame synchronization, error checking, and flow control.
- Media Access Control (MAC): Controls how devices on the network gain access to the medium and permission to transmit data.
- Key Components: Switches, bridges.
- Tasks:
- Framing: Packages raw bits into frames.
- MAC Addressing: Provides hardware addresses for data transmission.
- Error Detection and Correction: Identifies and corrects errors that occur in the Physical layer.
- Flow Control: Manages the rate of data transmission between sender and receiver.

Layer 3: Network Layer

- Function: Determines the best path for data to travel from source to destination.
- Key Components: Routers, Layer 3 switches.
- Tasks:
- Logical Addressing: Utilizes IP addresses to identify devices on a network.
- Routing: Determines the optimal path to send data packets.
- Packet Forwarding: Moves packets from one network to another.
- Fragmentation and Reassembly: Breaks down packets if they are too large for transmission and reassembles them at the destination.

Layer 4: Transport Layer

- Function: Provides reliable data transfer between end systems.
- Key Protocols: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
- Tasks:
- Segmentation and Reassembly: Breaks down data into segments and reassembles them at the destination.
- Flow Control: Manages the pace at which data is sent.
- Error Detection and Recovery: Ensures complete and accurate data transfer.
- Multiplexing: Allows multiple communication sessions to be used simultaneously.

Layer 5: Session Layer

- Function: Manages and controls the connections (sessions) between computers.
- Key Protocols: NetBIOS, RPC (Remote Procedure Call), PPTP (Point-to-Point Tunneling Protocol).
- Tasks:
- Session Establishment: Initiates and manages sessions between applications.
- Session Maintenance: Keeps sessions alive during communication.
- Session Termination: Ends sessions when communication is complete.
- synchronization: Manages dialog control and synchronization.

Layer 6: Presentation Layer

- Function: Translates data between the application layer and the network.
- Key Protocols: SSL/TLS (Secure Sockets Layer/Transport Layer Security), MPEG, JPEG.
- Tasks:
- Data Translation: Converts data from one format to another.
- Data Encryption/Decryption: Secures data by converting it into a secure format and back again.
- Data Compression/Decompression: Reduces the size of data for efficient transmission and restores it to its original form at the destination.

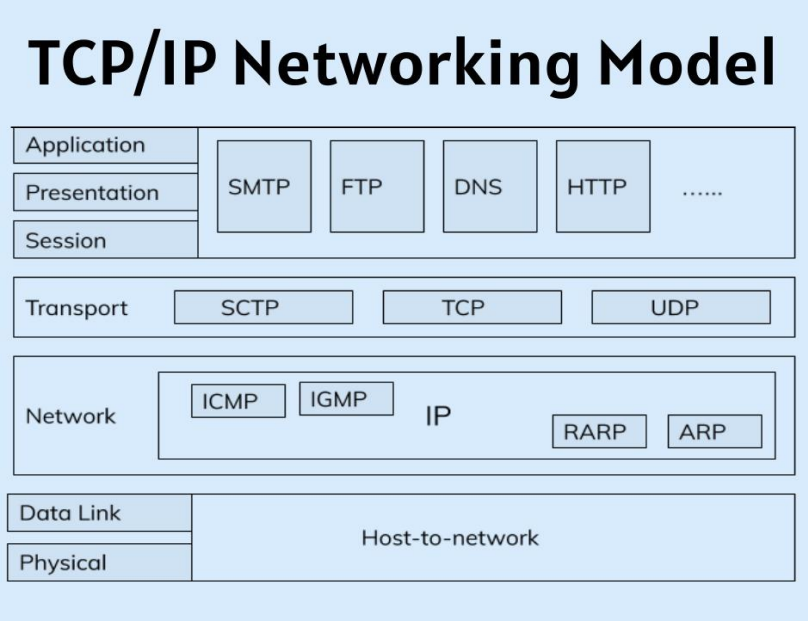
Layer 7: Application Layer

- Function: Provides network services directly to user applications.
- Key Protocols: HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System).
- Tasks:
- Network Services: Supports services like file transfer, email, and web browsing.
- Communication Initiation: Establishes initial communication sessions.

- Resource Sharing: Allows applications to share network resources.

TCP / IP PROTOCOL SUITE:

- The TCP/IP protocol suite is the backbone of modern networking, enabling communication across diverse and interconnected networks.
- Each layer of the TCP/IP model serves a specific function, from physical transmission .
- Application-specific data handling, ensuring reliable and efficient data exchange across the Internet.



1. Host-to-Network layer:

- In the TCP/IP protocol suite the physical and data link layers of OSI model.
- It is based on the transmission medium and it supports all kind of proprietary protocols Developed for this layer.
- Functionality:
- Choosing of transmission mode, synchronization of bits, error control, flow control and Physical addressing.

2. Internetwork Layer

- An 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.

Internetworking protocol(IP):

- It is a unreliable, connectionless protocol.
- It provides best-effort delivery of data to the receiver.
- Each and every machine is assigned by the IP address and referred by the layer.

Address Resolution Protocol: (ARP)

- It is used to fnd the MAC address of machine by known IP address.

Reverse Address Resolution Protocol:(RARP)

- It is used to fnd the IP address of machine by known MAC address.

Internet Control Message Protocol(ICMP):

- It is used to send the error reporting message by host and gateways to the sender.

Internet Group Message Protocol(IGMP):

3. Transport layer:

- It is used to transmit the group messages to recipients simultaneously.
- The Transport Layer in the TCP/IP model corresponds to Layer 4 of the OSI model.
- This layer is responsible for providing reliable data transfer between two devices on a network, ensuring that data is delivered accurately, in order, and without errors.
- It handles end-to-end communication and controls the flow of data between hosts.

UDP (User Datagram Protocol):

Connectionless: UDP does not establish a connection before sending data. Data is sent as individual packets called datagrams.

- TCP (Transmission Control Protocol)
- Is one of the core protocols of the Transport Layer in the TCP/IP model.
- It is a connection-oriented protocol that provides reliable, ordered, and error-checked delivery of data between applications running on devices across a network.
- TCP is widely used in the internet and most of the applications we use today rely on it.

SCTP (Stream Control Transmission Protocol):

- Reliable and Connection-Oriented: Like TCP, SCTP provides reliable, ordered delivery of data.

4. Application Layer

- 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.
- Following are the main protocols used in the application layer:
- HTTP: HTTP stands for **Hypertext transfer protocol**. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video.
- SMTP: SMTP stands for **Simple mail transfer protocol**. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

- FTP: FTP stands for **File Transfer Protocol**. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.
- DNS: DNS stands for **Domain Name Sys**tem. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses.
- 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.
- Following are the main protocols used in the application layer:
- HTTP: HTTP stands for **Hypertext transfer protocol**. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video.
- SMTP: SMTP stands for **Simple mail transfer protocol**. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- FTP: FTP stands for **File Transfer Protocol**. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.
- DNS: DNS stands for **Domain Name Sys**tem. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses.

EXAMPLE NETWORKS

THE INTERNET

- An internet is a collection of two or more networks interconnected each other to communicate the data.
- It has affected the way we do business as well as the way we spend our leisure time.
- Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet.
- The Internet is a communication system that has brought a wealth of information to our Finger tips and organized it for our use.

History of the Internet:

- **A network is a group of connected communicating devices such as computers and printers.**
- **An internet (note the lowercase letter i) is two or more networks that can communicate with each other.**
- **The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks. Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet.**
- **Millions of people are users. Yet this extraordinary communication system only came into being in 1969.**
- **In the mid-1960s, mainframe computers in research organizations were standalone devices.**
- **Computers from different manufacturers were unable to communicate with one another.**
- **The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.**
- **In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers.**
- **The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP).**

- **The IMPs, in tum, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host. By 1969, ARPANET was a reality.**
- **In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group.**

NSFNET:

- **The NSFNET is a loosely organized community of networks funded by the National Science Foundation to support the sharing of national scientific computing resources, data and information.**
- **NSFNET consists of a large number of industry and academic campus and experimental networks, many of which are interconnected by a smaller number of regional and consortium networks.**
- **The NSFNET Backbone Network is a primary means of interconnection between the regional networks and is the subject of this report.**

Internet Usage:

- **Email**
- **News groups**
- **File transfer**
- **Remote login**
- **Electronic commerce**
- **ICT based learning**

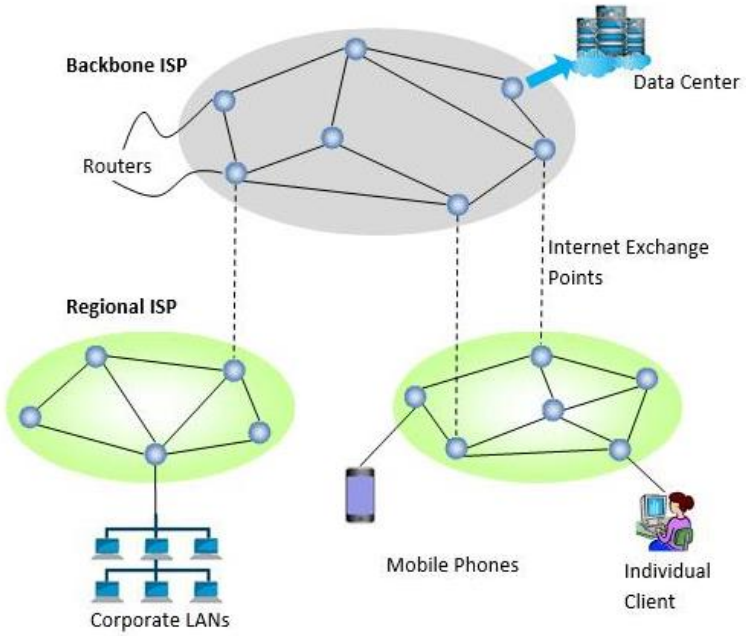
Architecture of Internet:

- **The architecture of the Internet is ever-changing due to continuous changes in the technologies as well as the nature of the service provided. The heterogeneity and vastness of the Internet make it difficult to describe every aspect of its architecture.**
- **The overall architecture can be described in three levels −**

  Backbone ISP (Internet Service Provider)

  Regional ISPs

  Clients



ISP: (Internet Service Providers):

- **Internet service provider (ISP), company that provides Internet connections and services to individuals and organizations. ISPs may also provide software packages (such as browsers), e-mail accounts, and a personal website or home page.**
- **ISPs can host websites for businesses and can also build the websites themselves.**

The ISPs are classified into four categories:

1. **International ISPs:**
   Top of the ISP hierarchies and connect the nations together.
2. **National ISPs:**
   Backbone networks are created and maintained by public and private sectors.
3. **Regional ISPs:**
   Smaller ISPs that are connected to one or more national ISPs.
4. **Local ISPs:**
   Provide direct service to users. Directly connected to regional or national ISPs.

Asynchronous Transfer Mode (ATM) :

Asynchronous Transfer Mode, network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with older technologies.

The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line.

ATM creates a fixed channel, or route, between two points whenever data transfer begins.

This differs from TCP/IP, in which messages are divided into packets and each packet can take

a different route from source to destination. This difference makes it easier to track and bill data usage across an ATM network, but it makes it less adaptable to sudden surges in network traffic.

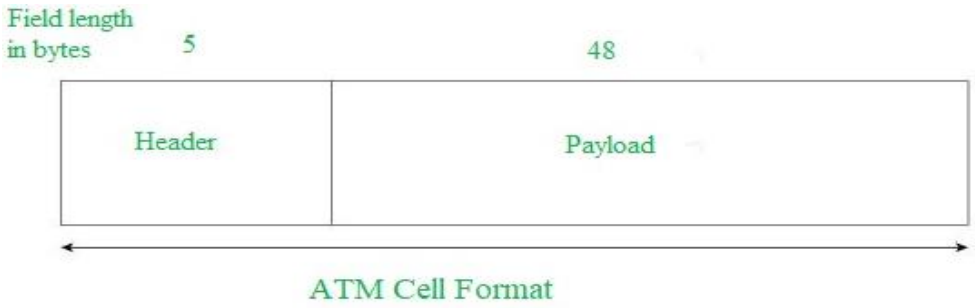
ATM (asynchronous transfer mode) is a dedicated-connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. Individually, a cell is processed asynchronously relative to other related cells and is queued before being multiplexed over the transmission path.

ATM creates fixed routes between two points before data transfer begins, which differs from TCP/IP, where data is divided into packets, each of which takes a different route to get to its destination. This makes it easier to bill data usage.

ATM Cells:

ATM Cell Format –

As information is transmitted in ATM in the form of fixed-size units called **cells**. As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload.



ATM Cell Format

Virtual circuits:

Asynchronous transfer mode (ATM), the data are transmitted through a fixed-size unit called cells. As we know, each cell has 53 bytes long. There are two types of Asynchronous transfer modes (ATM). These are as follows:

1. UNI header

This is used in the private connection in the Asynchronous transfer mode (ATM) network between ATM switches and ATM endpoints.

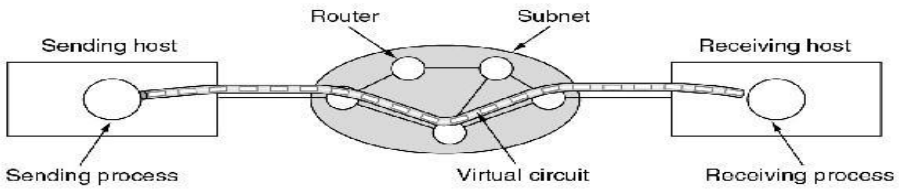
2. NNI header

It communicates between the Asynchronous Transfer Mode (ATM) switches.

ATM Virtual Circuits

VPI:

A virtual path identifier (VPI) is a data communication identifier that uniquely identifies a network path for an asynchronous transfer mode (ATM) cell packet to reach its destination node.



A virtual circuit.

VCI:

A VCI is a numerical value that uniquely identifies a virtual circuit within a network. It is used by network devices to direct incoming data packets to the appropriate virtual circuit for processing and delivery.

VIRTUAL CIRCUIT TYPES:

There are two main types of virtual circuits:

1. switched virtual circuits (SVCs) and
2. permanent virtual circuits (PVCs).

ATM REFERENCE MODEL:

1. **ATM Adaption Layer (AAL) –**
   It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and segments it into 48-byte cell payloads. AAL protocol excepts transmission from upper-layer services and helps them in mapping applications, e.g., voice, data to ATM cells.

2. **Physical Layer –**
   It manages the medium-dependent transmission and is divided into two parts physical medium-dependent sublayer and transmission convergence sublayer. The main functions are as follows:
   - It converts cells into a bit stream.
   - It controls the transmission and receipt of bits in the physical medium.
   - It can track the ATM cell boundaries.
   - Look for the packaging of cells into the appropriate type of frames.

3. **ATM-Layer** –
   It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.

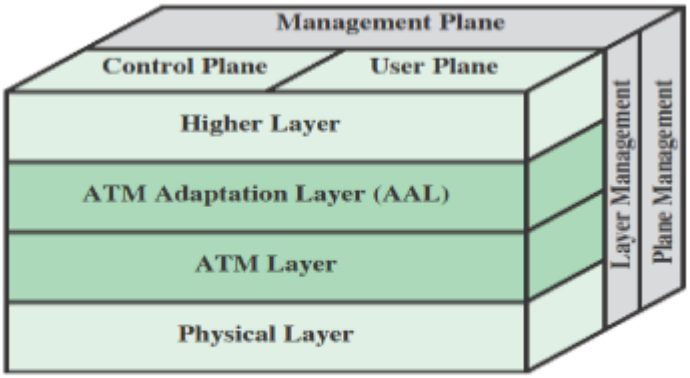


Figure 11.1 ATM Protocol Architecture

ADVANTAGES:

- ✓ **High Speed**
- ✓ **Scalability**
- ✓ **Flexible Bandwidth**
- ✓ **Consistent Latency**

Disadvantages:

- ✓ **Complexity**
- ✓ **Cost**
- ✓ **Cell Overhead**
- ✓ **Limited Support**

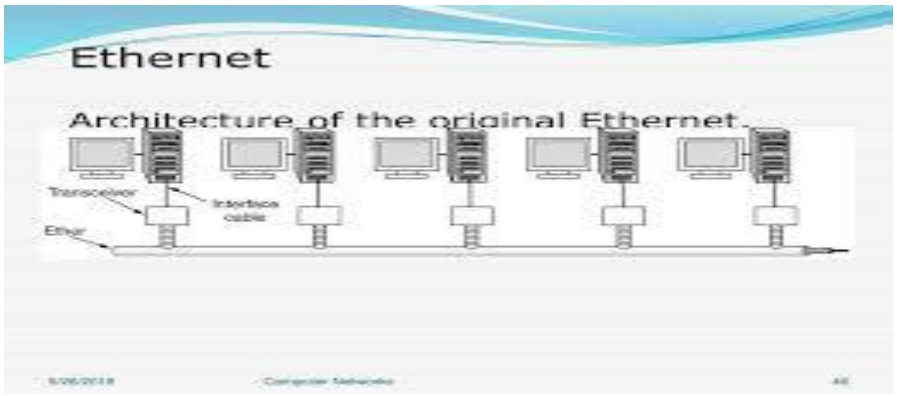
ETHERNET

A local Area Network (LAN) is a data communication network connecting various terminals or computers within a building or limited geographical area. The connection between the devices could be wired or wireless.

History of Ethernet

- ✓ Robert Metcalfe's invention of Ethernet in 1973 completely changed computer networking. With Ethernet Version 2's support for 10 Mbps and an initial data rate of 2.94 Mbps, it first gained popularity in 1982.
- ✓ Ethernet's adoption was accelerated by the IEEE 802.3 standardization in 1983. Local area networks (LANs) and the internet were able to expand quickly thanks to the rapid evolution and advancement of Ethernet, which over time reached speeds of 100 Mbps, 1 Gbps, 10 Gbps, and higher.
- ✓ It evolved into the standard technology for wired network connections, enabling dependable and quick data transmission for private residences, commercial buildings, and data centers all over the world.

- ✓ **ARCHITECTURE OF ETHERNET:**



- ✓ Classic Ethernet is simplest form of Ethernet. It comprises of an Ethernet medium composed of a long piece of coaxial cable.
- ✓ Stations can be connected to the coaxial cable using a card called the network interface (NI). The NIs are responsible for receiving and transmitting data through the network.
- ✓ Repeaters are used to make end-to-end joins between cable segments as well as re-generate the signals if they weaken.
- ✓ When a station is ready to transmit, it places its frame in the cable. This arrangement is called the broadcast bus.

TYPES OF ETHERNET:

1 .Fast Ethernet: This type of Ethernet network uses cables called twisted pair or CAT5. It can transfer data at a speed of around 100 Mbps (megabits per second). Fast Ethernet uses both fiber optic and twisted pair cables to enable communication.

2. Gigabit Ethernet: This is an upgrade from Fast Ethernet and is more common nowadays. It can transfer data at a speed of 1000 Mbps or 1 Gbps (gigabit per second). Gigabit Ethernet also uses fiber optic and twisted pair cables for communication.

3.10-Gigabit Ethernet: This is an advanced and high-speed network that can transmit data at a speed of 10 gigabits per second. It uses special cables like CAT6a or CAT7 twisted-pair cables and fiber optic cables.

4. **Switch-based Ethernet:** This network configuration includes a hub or a switch. In addition, a standard network cable is employed as opposed to a twisted pair cable. A network switch's primary role is to transfer information/data from one device to another on the same network.

Advantages of Ethernet:

- The fastest speed provide by Gigabit Ethernet is of 1Gbps. The speed ranges from more than 10 times Fast Ethernet.
- To form an Ethernet, we don't need much cost. It is relatively inexpensive. Total cost induced is less.
- In Ethernet, all the node have an equivalent privileges. It does not follow client-server architecture.
- It does not require any switches or hubs
- Maintenance and administration are simple.

Disadvantages of Ethernet:

- It offers a nondeterministic service.
- It doesn't hold good for real-time applications because it requires deterministic service.
- As priority packets cannot be set, it's not suitable for a client-server architecture.
- The receiver cannot able to send any knowledge after receiving the packets.
- If there's any problem in ethernet, it's difficult to troubleshoot what cable or node within the network causing an actual problem.

WIRELESS LAN'S:

WLAN stands for **Wireless Local Area Network.** WLAN is a local area network that uses radio communication to provide mobility to the network users while maintaining the connectivity to the wired network. A WLAN basically, extends a wired local area network. WLAN's are built by attaching a device called the access point(AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter which is similar in function to an ethernet adapter. It is also called a LAWN is a Local area wireless network.

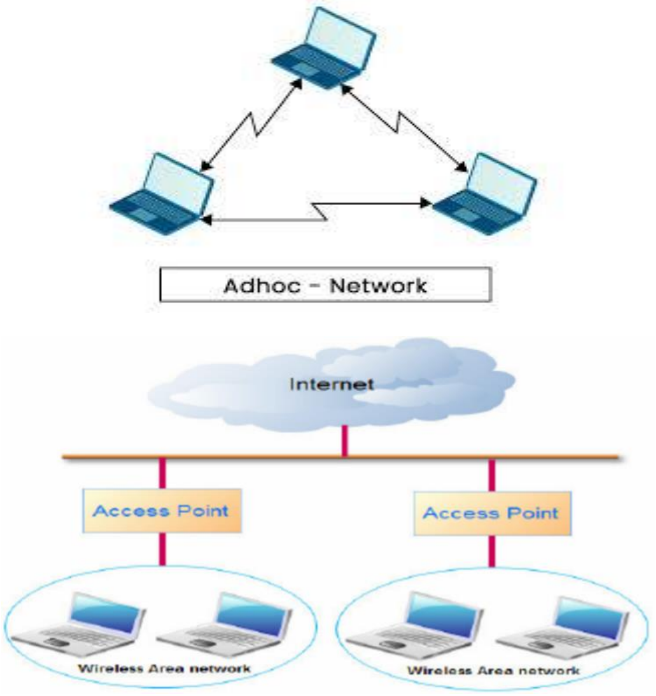
IEE 802.11:

WLAN gives users the mobility to move around within a local coverage area and still be connected to the network. Most latest brands are based on IEE 802.11 standards, which are the WI-FI brand name.

ARCHITECTURE:

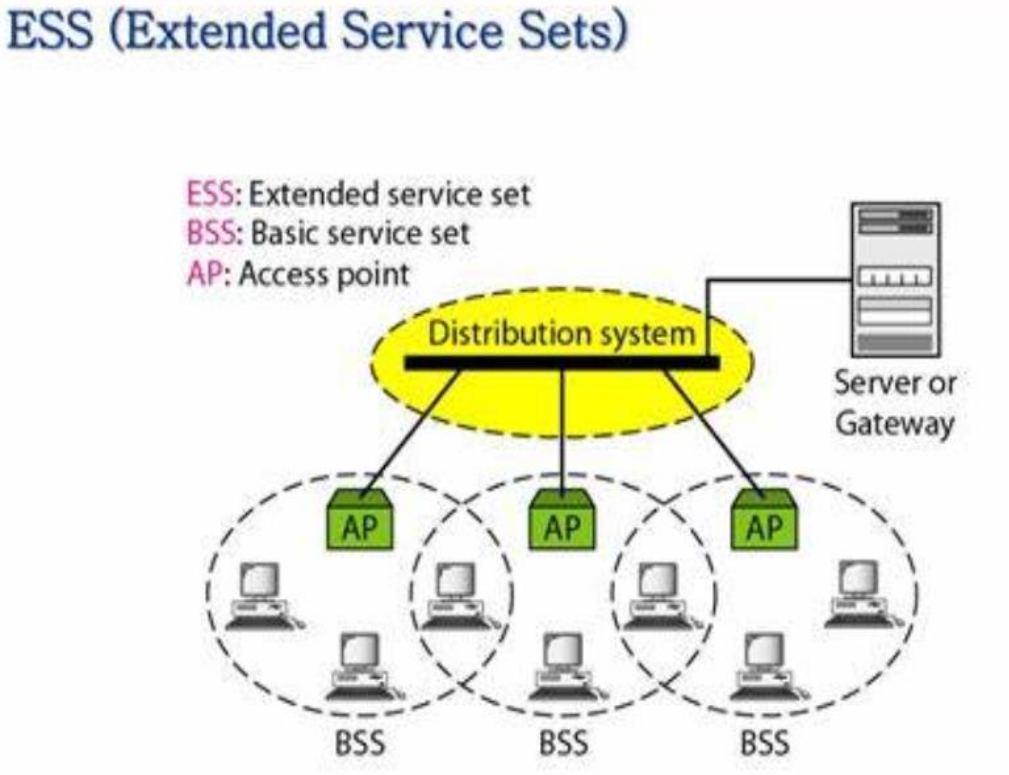
1. **Infrastructure:** In Infrastructure mode, all the endpoints are connected to a base station and communicate through that; and this can also enable internet access. A WLAN infrastructure can be set up with: a wireless router (base station) and an endpoint (computer, mobile phone, etc). An office or home WiFi connection is an example of Infrastructure mode.

2. **Ad Hoc:** In Ad Hoc mode WLAN connects devices without a base station, like a computer workstation. An Ad Hoc WLAN is easy to set up it provides peer-to-peer communication. It requires two or more endpoints with built-in radio transmission.

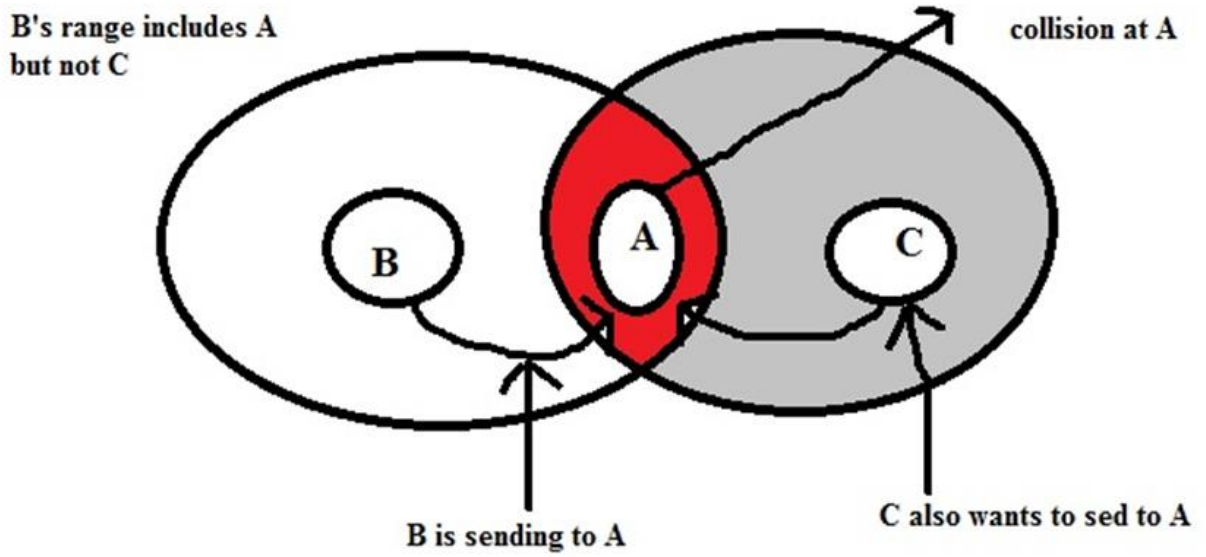


3. [Basic Service Set (BSS)](#) : Basic Service Set (BSS), as name suggests, is a group or set of all stations that communicate with each together. Here, stations are considered as computers or components connected to wired network.

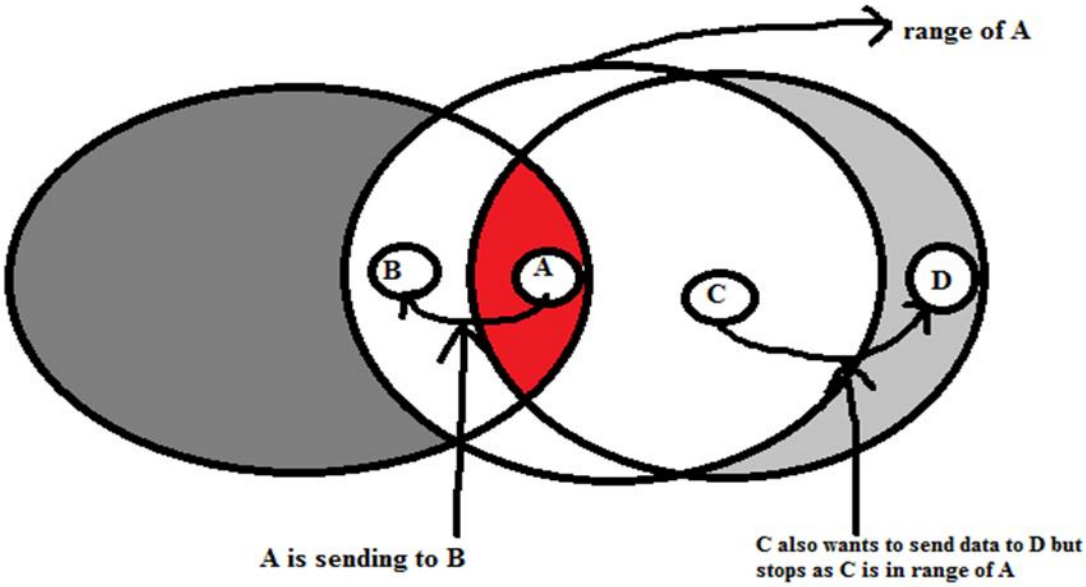
4.Extended Service Set (ESS) : Extended Service Set (ESS), as name suggests, is a group of BSSs or one or more interconnected BSS along with their wired network.



Hidden station problem: B is sending data to A, and after some time C also wants to send data to B. but C is not in the range of B and so it will be unaware of the transmission between B and A, and so C will send data to A and therefore there will be a collision.

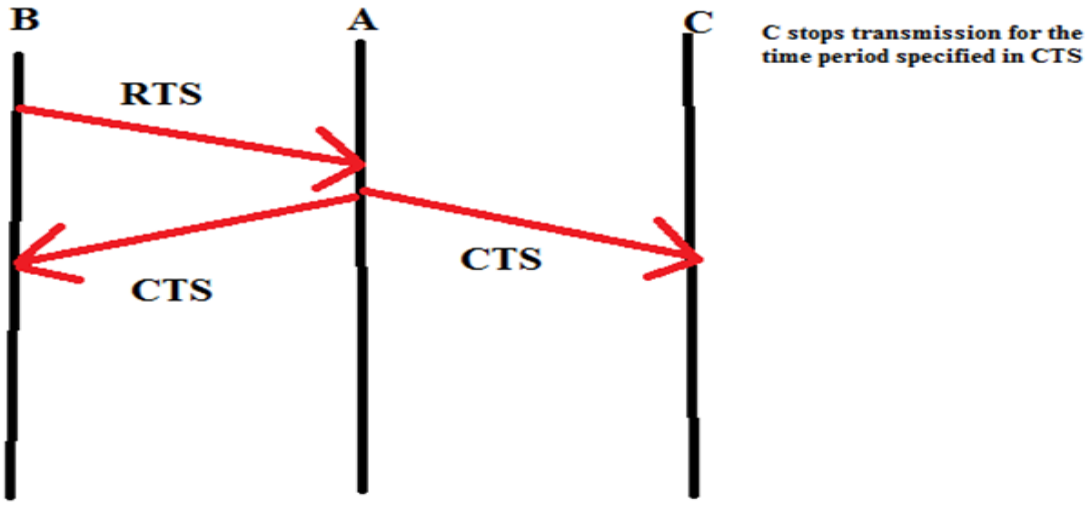


Exposed station problem: station A is sending data to B and C also wants to send data to D, but since C is in the transmission range of A, C will not send data to D. But the transmission between C and D will not affect the transmission between A and B.

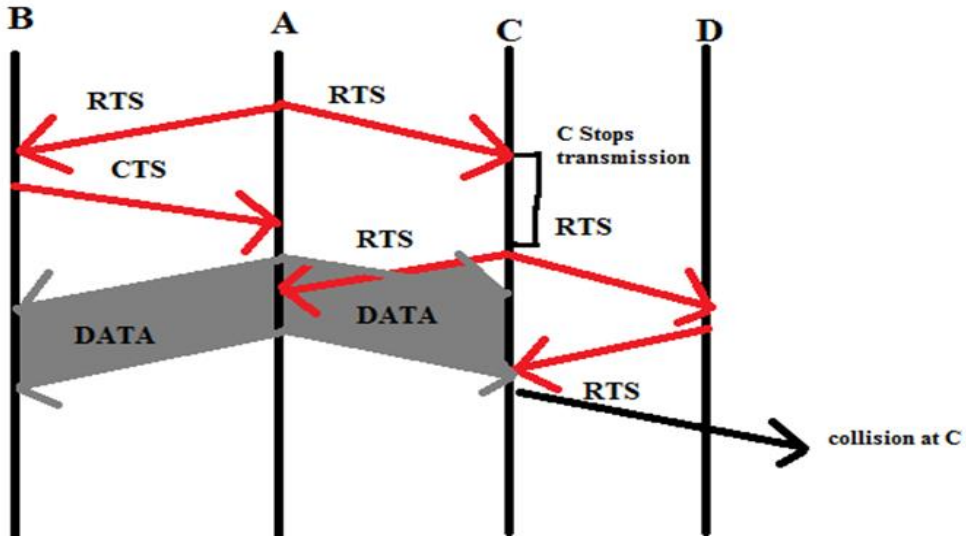


The hidden node can solve be solved by the use of handshaking. B before sending data to A, will first send request to send (RTS) to A. after that if A is ready to receive data from B then it will respond by sending Clear to send(CTS) to B, which will also be received by C since it will also in the transmission range of A. as a result of which C will stop transmission for the time period that is been specified in the CTS.

The use of handshaking is unable to prevent handshaking. C stops transmission for the time period specified in the RTS as it is in the range of A, but does not receive the CTS send by B. as a result of which it send RTS to D, and if D sent CTS to C then it collides with the data sent by A to B(also received by C).



USE OF HANDSHAKING TO PREVENT HIDDEN NODE PROBLEM



Advantages of Wireless **Local Area Network(**WLAN)

1. Installation speed and simplicity.
2. Installation flexibility.
3. Reduced cost of ownership.
4. Reliability.
5. Mobility.
6. Robustness.

Disadvantages of Wireless **Local Area Network** (WLAN)

1. Slower bandwidth.
2. Security for wireless LANs is the prime concern.
3. Less capacity.

4. Wireless networks cost four times more than wired network cards.
5. Wireless devices emit low levels of RF which can be harmful to our health.

PHYSICAL LAYER

Theoretical Basis for Data Communication

Fourier Analysis

Fourier showed that a periodic function $g(t)$ can be represented mathematically as aninfinite series of sines and cosines:

1. f is the function's *fundamental frequency*
2. $T = \frac{1}{f}$ is the function's *period*
3. a_n and b_n are the amplitudes of the nth *harmonics*

The series representation of $g(t)$ is called its *Fourier series* expansion.

In communications, we can always represent a data signal using a Fourier series by imagining that the signal repeats the same pattern forever.

Moreover, we can compute the coefficients a_n and b_n:

$$a_n = \frac{2}{T}\int_0^T g(t)\sin(2\pi n f\, t)dt$$

$$b_n = \frac{2}{T}\int_0^T g(t)\cos(2\pi n f\, t)dt$$

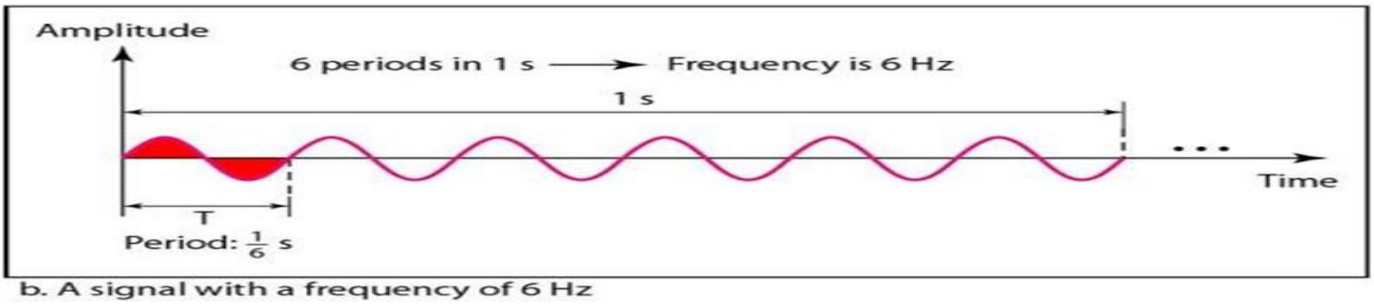
$$\frac{2}{}\int_{}^{T}$$

- Period and Frequency

Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle.

Frequency refers to the number of periods in 1 s. Note that period and frequency are just one characteristic defined in two ways. Period is the inverse of frequency, and frequency is the inverseof period, as the following formulas show.

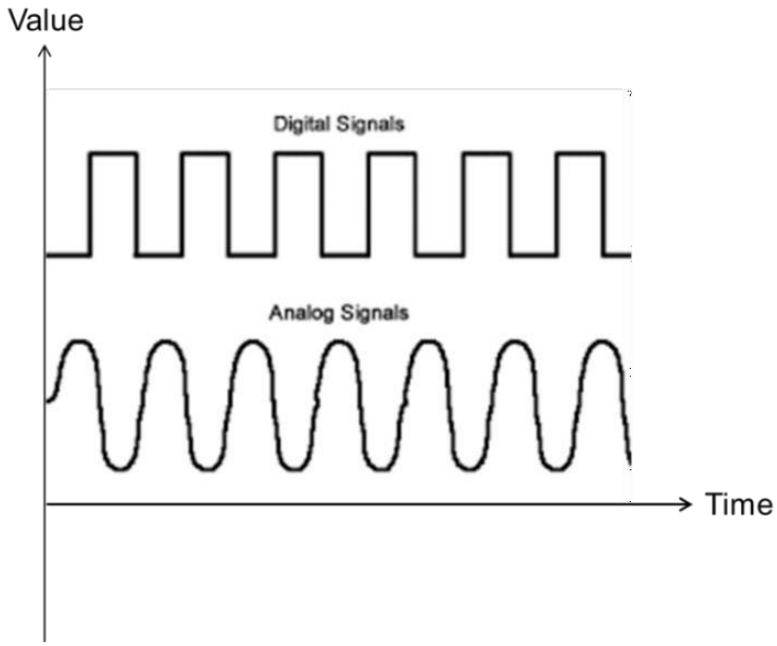
$$f = \frac{1}{T} \quad \text{and} \quad T = \frac{1}{f}$$



b. A signal with a frequency of 6 Hz

Analog and Digital Signals

Like the data they represent, signals can be either analog or digital. An ***analog signal*** *is a continuously varying electromagnetic wave that may be propagated over a variety of media* (i.e., has infinitely many levels of intensity over a period of time or can has infinite number of values in a range). As the wave moves from value **A** to value **B**, it passes through and includes an infinitenumber of values along its path. A ***digital signal***, on the other hand, *is a sequence of voltage pulsesthat may be transmitted over a wire medium* (i.e., can have only a limited number of defined values). Although each value can be any number, it is often as simple as 1 and O.



Types of analog signal:

Periodic Signals:

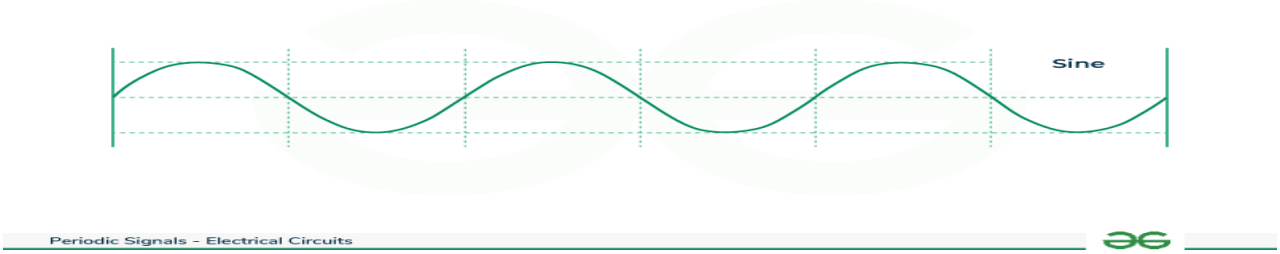
Periodic analog signals can be classified as simple or composite. A ***simple periodic analog*** signal,a **sine wave**, cannot be decomposed into simpler signals.

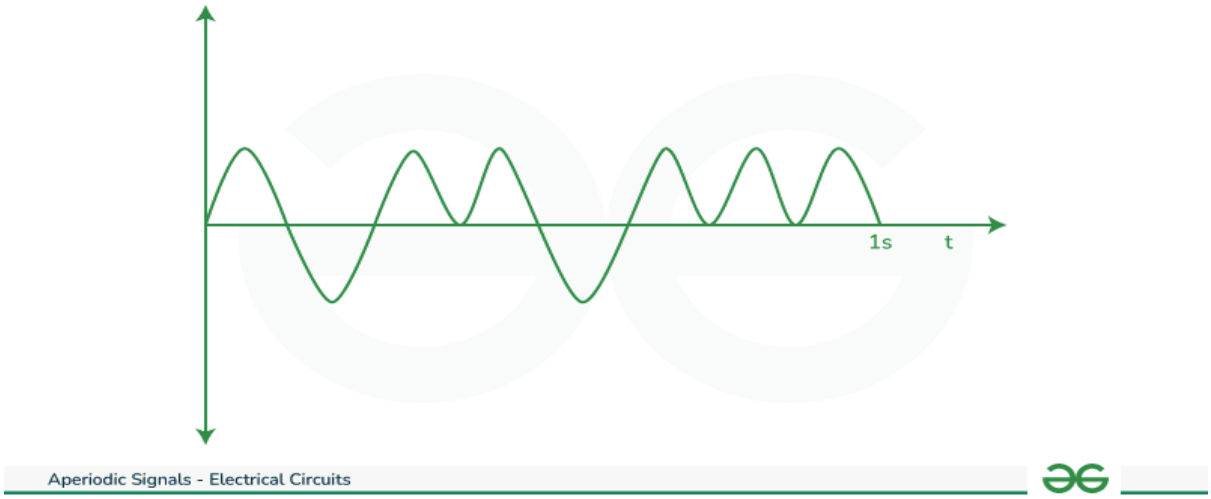
Aperiodic Signal:

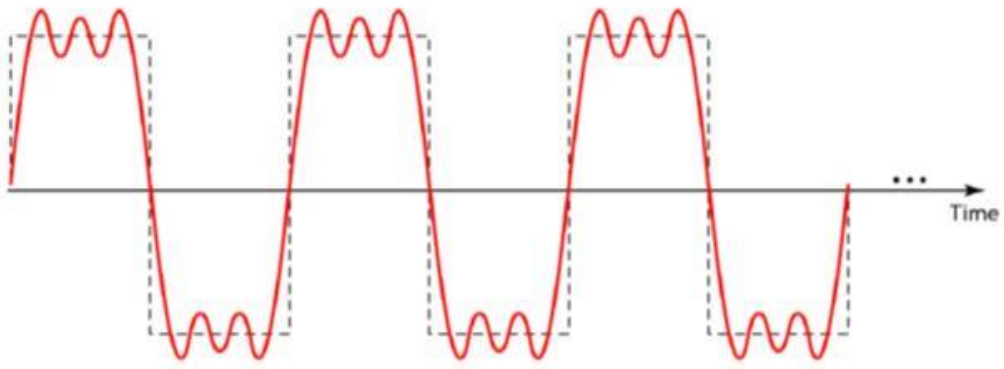
It does not repeat its pattern over a period.

Composite Signals:

A ***composite periodic analog*** signal is composed of multiple sine waves.







Baseband Signal:

A baseband signal or low pass signal is a signal that can include frequencies that are very near zero, by comparison with its highest frequency.

Passband signal:

A passband is the range of frequencies or wavelengths that can pass through a filter. For example, a radio receiver contains a bandpass filter to select the frequency of the desired radio signal out of all the radio waves picked up by its antenna.

Wavelength

The wavelength is the distance a simple signal can travel in one period.

$$Wavelength = propagatioon\ speed * periood = propagation\ speed/frequency$$

Bandwidth:

Bandwidth, or precisely network bandwidth, is the maximum rate at which data transfer occurs across any particular path of the network. Bandwidth is basically a measure of the amount of data that can be sent and received at any instance of time.

Data Transfer Rate:

The data transfer rate (DTR) is the amount of digital data that's moved from one place to another in a given time. The data transfer rate can be viewed as the speed of travel of a given amount of data from one place to another.

Bit Rate

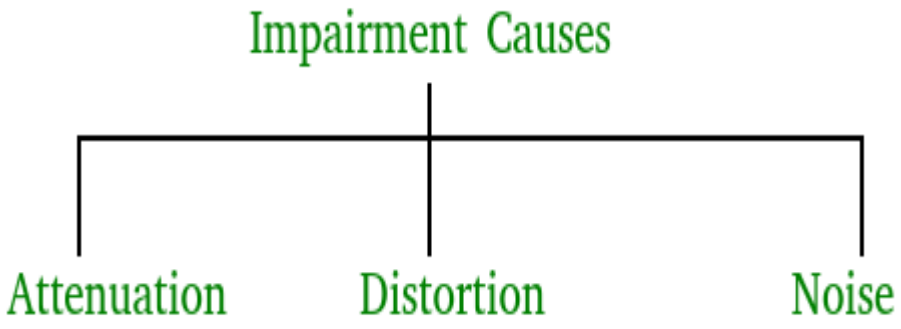
The bit rate is the number of bits sent in 1s, expressed in bits per second (bps).

BOTTLENECKS TO DATA TRANSMISSION

A network bottleneck occurs when data flow slows significantly because the network's capacity to handle the current volume of traffic has diminished or failed.

In communication system, analog signals travel through transmission media, which tends to deteriorate the quality of analog signal, which means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. The imperfection causes signal impairment. Below are the causes of the impairment.

Causes of impairment –



Distortion –

It means changes in the form or shape of the signal.

This is generally seen in composite signals made up with different frequencies. Each frequency component

has its own propagation speed travelling through a medium.

Attenuation – It means loss of energy. The strength of signal decreases with increasing distance which causes

loss of energy in overcoming resistance of medium. This is also known as attenuated signal.

Noise – The random or unwanted signal that mixes up with the original signal is called noise.

There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which

may corrupt the signal.

Delay or Latency:

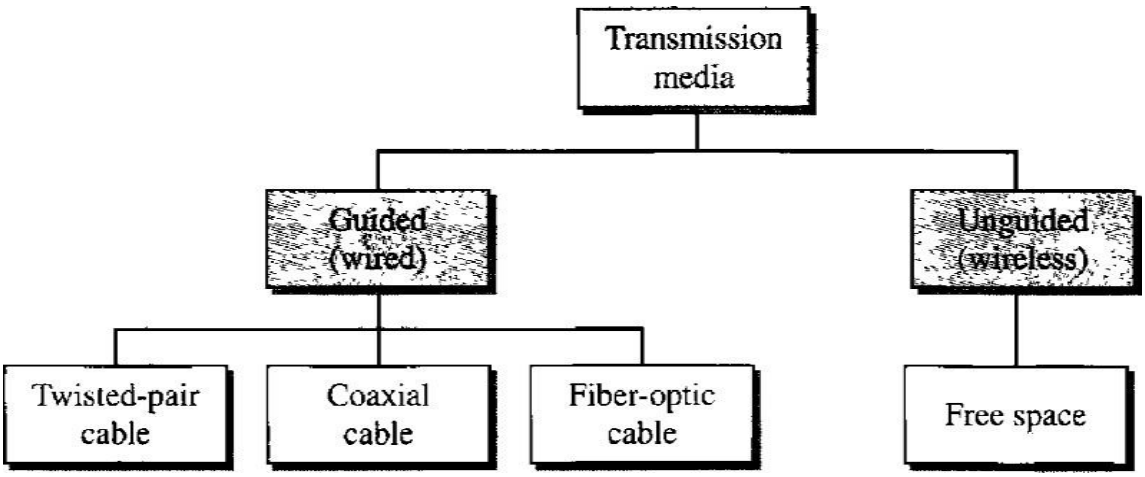
Network latency is the delay in network communication. It shows the time that data takes to transfer across
the network.

Networks with a longer delay or lag have high latency, while those with fast response times have low latency.

Guided Transmission Media

- Transmission media are actually located below the physical layer and are directly controlled bythe physical layer.
- A transmission **medium** can be broadly defined as anything that can carry informationFrom a source to a destination.
- 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 conversionof data from another form.
- Extending the range of the human voice became possible when the telephone wasinvented 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.
- Wireless communication started in 1895 when Hertz was able to send high frequencySignals.

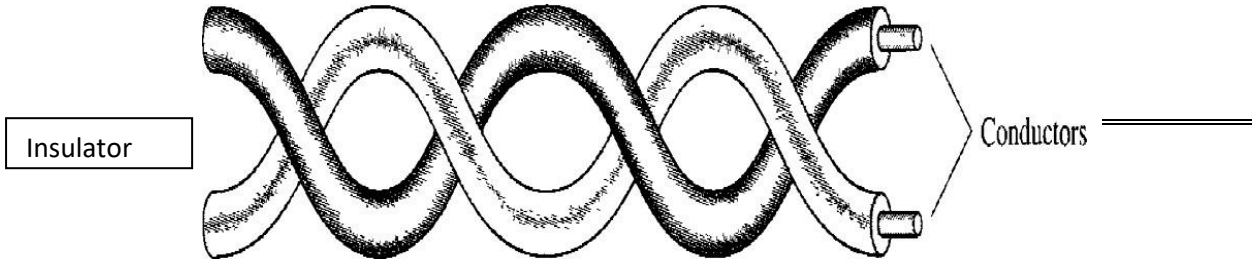
- It is divided into two broad categories:
  - **Guided media:** Guided media include twisted-pair cable, coaxial cable, andFiber-optic cable.
  - **Unguided media**: Unguided medium is free space.



GUIDED MEDIA:

- Guided media, which are those that provide a conduit 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 themedium.
- **Twisted-pair** and **coaxial cable** use metallic (copper) conductors that accept and transport signalsin the form of electric current.
- **Optical fiber** is a cable that accepts and transports signals in the form of light.

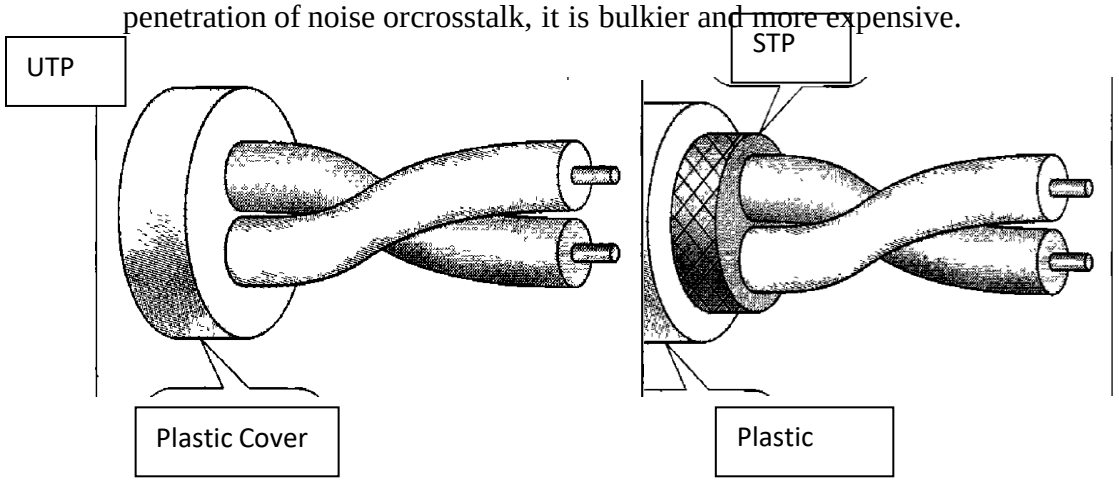
Twisted-Pair Cable:



- ❖ A twisted pair consists of two conductors (normally copper), each with its own plasticInsulation, twisted together.
- ❖ One of the wires is used to carry signals to the receiver, and the other is used onlyas 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 twist,ing the pairs, a balance is maintained.

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 orcrosstalk, it is bulkier and more expensive.



Applications

- ➢ Twisted-pair cables are used in telephone lines to provide voice and data channels.
- ➢ The local loop-the line that connects subscribers to the central telephone office---commonlyconsists of unshielded twisted-pair cables.

Advantages:

- ➢ Easy to install and maintain.
- ➢ Cheapest cable.
- ➢ Reduce the crosstalk.
- ➢ Preventing the electrical noise.

Disadvantages:

- ➢ Limited distance is covered.
- ➢ Difficult to connect the terminal block.

Coaxial Cable:

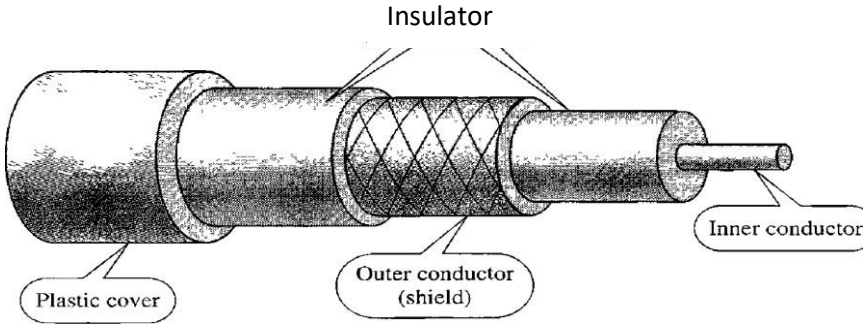
- Coaxial cable (or *coax)* carries signals of higher frequency ranges than those in twisted pair cable,in part because the two media are constructed quite differently.
- Instead of having two wires, coax has a central core conductor of solid or stranded wire (usuallycopper) enclosed in an insulating 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 bya plastic cover.
- **Coaxial cable standards**:

o Different coaxial cable designs are categorized by their radio government (RG) ratings.

o Each RG number denotes a unique set of physical specifications, including the wire , inner conductor, thickness and type of the inner insulator, the construction of the shield, and the size and typeof the outer casing.

Coaxial cable connectors:

o A number of connectors have been designed for use with coaxial cable.
o Few of the connector designs have become standardized.
o The most common of these is called a barrel connector.
o Coaxial connectors are familiar from cable TV and VCR hookups.
o Two other commonly used types of connectors are T-connectors and terminators.
o A T-connector (used in thin Ethernet) allows a secondary cable or cables to branch off from amain line.
o Terminators are required for bus topologies where one main cable acts as a backbone withbranches to several devices but does not itself terminate in a device.



Applications:

- ✓ Coaxial cable was widely used in analog telephone networks where a single coaxialnetwork could carry 10,000 voice signals.
- ✓ Cable TV networks
- ✓ Another common application of coaxial cable is in traditional Ethernet LANs.

Advantages:

- **Covers larger distance and high bandwidth.**
- **Shielded for cross talk and noise.**

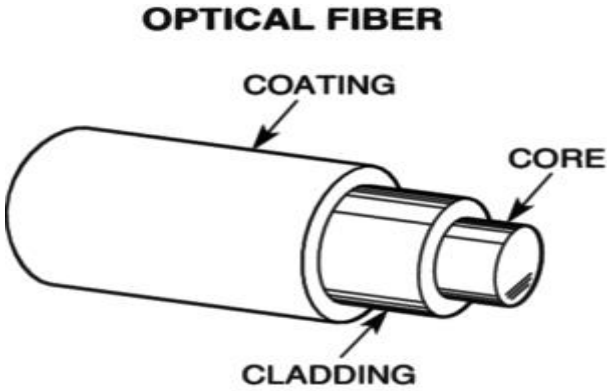
Disadvantages:

- **Heavy cable is used.**
- **High caused twisted pair cable is used.**
- **Higher attenuation.**

Fiber-Optic Cable:

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- To understand optical fiber, we first need to explore several aspects of the nature 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.

- **Nature of light:** light is a form of electromagnetic energy, travel at 300000 km/sec. This speeddecreases as the medium through which the light travels becomes denser.
- **REFRACTION**: light travel in a straight line as long as it is moving through a single uniform substance. If a ray of light travelling through one substance suddenly enters another substance, itsspeed, direction changes, this change is called refraction.
- **REFLECTION**: when the angle of incidence becomes greater than the critical angle, calledreflection.



Propagation Modes

- Current technology supports two modes for propagating light along optical channels.
- (**Multimode and Single mode**) for propagating light along optical channels, each requiringfiber with different physical characteristics.
- Multimode can be implemented in two forms:

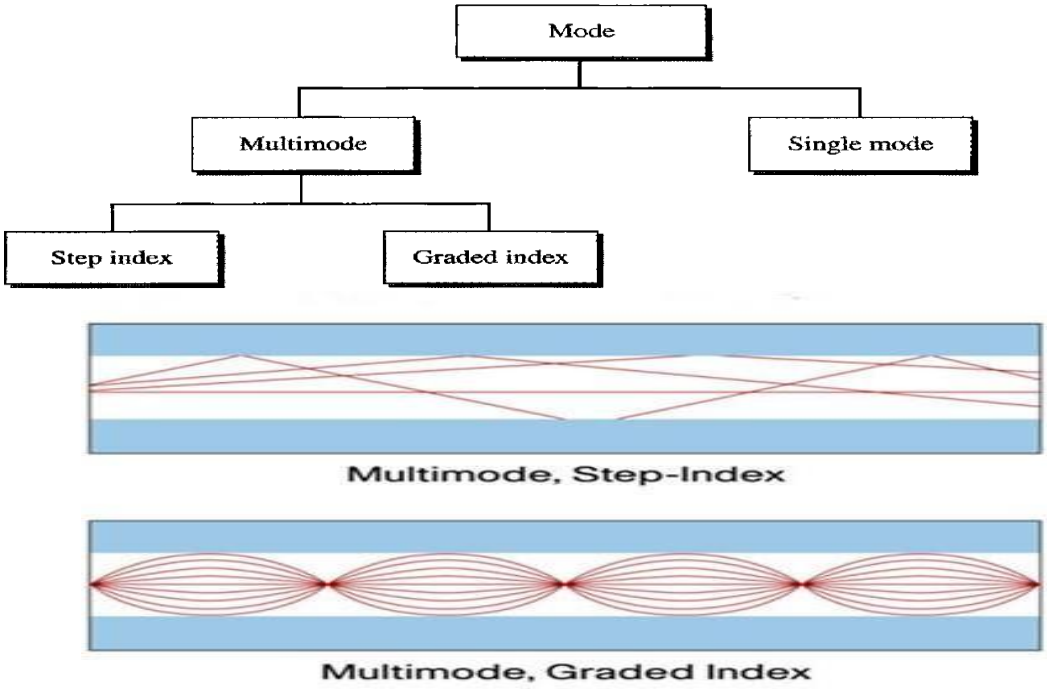
Light Probagation:

- ✓ **Light Propagation in Optical Fibers refers to the transmission of light through a fiber optic cable.**
- ✓ **In this process, light is sent through the core of the fiber optic cable and is transmitted over long distances with minimal attenuation or loss of signal.**
- ✓ **The light signal is typically generated by a laser or LED source and then sent through the fiber optic cable by means of internal reflection.**
- ✓ **The reflection takes place the light travels from more dense to less dense.**
  - **A beam of light moves through this constant density in a straight line until it reachesthe interface of the core and the cladding.**

1. Graded-index :

- Decreases distortion of the signal through the cable.
- A graded-index fiber is one with varying densities.
- Density is highest at the center of the core and decreases gradually to its lowest at the edges.

2. Step index fiber:



- The light path is straight line reflection on the core or straight at the center of the core.

- In optical fibers, a step-index fiber is a fiber where a uniform refractive index exists within the core and a sharply decreased refractive index exists in the core-cladding interface because of the lower refractive index in cladding.

Applications

- Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective.
- Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600Gbps.
- 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:

- Higher bandwidth.
  - ✓ Lower attenuation.
  - ✓ Light weight.

Disadvantages:

- Difficult to maintain.
- Higher Cost