NETWORK PROTOCOLS AND SECURITY

Dr.R.Revathi
Mr. Tushar Kanti De
Dr. A.V Praveen Krishna
Dr.Ch.Radhika Rani
Dr. Annapurana
Dr. P.Sunitha

Network Protocols and security

ISBN: XXXXXXXXXXXXXX

Printed @ KLEF

Dedication

Dedicated to our Mentors.

Phone: +919800965529
Email: vit.tushar@kluniversity.in

Preface

In today's interconnected world, computer networks have become the backbone of modern communication and information exchange. From local area networks (LANs) in our homes to vast global networks that span continents, network protocols play a critical role in facilitating seamless data transmission and ensuring the smooth functioning of digital ecosystems. However, with the increasing reliance on these networks for business, government, and personal use, the importance of network security has never been more paramount. This book delves into the fascinating world of network protocols and security, exploring the fundamental principles that govern data transmission, routing, and communication across various network architectures.

We aim to provide a comprehensive and in-depth understanding of how network protocols work and how they can be both leveraged and safeguarded to optimize network performance and protect against potential threats. This book focuses on network protocols, starting with the basics of data encapsulation and addressing. We explore various network models, including the OSI model and the TCP/IP model, to gain insight into the layered approach that governs communication in modern networks. Detailed discussions on popular network protocols like Ethernet, IP, TCP, and UDP lay the groundwork for comprehending the intricacies of data transfer and routing.

This book also delves into the realm of network security, where we shed light on the various challenges and risks that networks face in today's digital landscape. Understanding the significance of secure communication, we explore encryption, authentication, and public-key infrastructure (PKI) as essential components of robust network security. Further, we investigate common security threats, such as malware, DDoS attacks, and phishing, and delve into techniques to mitigate and prevent these risks. This book also brings together the worlds of network protocols and security, examining how both aspects interact and impact each other.. We envision this book to be a valuable resource for students, professionals, and enthusiasts seeking to deepen their knowledge of network protocols and security. Whether you are an aspiring network engineer, an IT administrator responsible for network management, or a security professional focused on safeguarding data, we hope this book equips you with the essential knowledge and tools to navigate the dynamic world of network protocols and security effectively.

Introduction

In today's interconnected world, computer networks serve as the backbone of modern communication and information exchange. From local area networks (LANs) within our homes to vast global networks spanning continents, these intricate systems, facilitate the seamless transmission of data, enabling us to access information, communicate with others, and conduct business efficiently. However, with the increasing reliance on networks, ensuring their security has become an indispensable aspect of the digital landscape.

This introduction delves into the fascinating realm of network protocols and security, providing a foundational understanding of their significance, functionalities, and interplay in modern networking environments. We explore how network protocols establish the rules and conventions that govern data exchange and communication between devices, while also unveiling the critical role of security measures in safeguarding sensitive information from unauthorized access and potential threats. This exploration centers on network protocols, laying the groundwork for comprehending how data is encapsulated, transmitted, and received across various network architectures.

We delve into the key concepts and principles that underpin network communication, including data packetization, addressing schemes, and the layered approach to network models. The Open Systems Interconnection (OSI) model and the Transmission Control Protocol/Internet Protocol (TCP/IP) model serve as our guides in understanding the hierarchical structure of networks and how each layer contributes to seamless data transmission. We explore popular network protocols such as Ethernet, IP, TCP, and UDP, revealing their specific roles in ensuring reliable, efficient, and secure data transfer.

Our journey focuses on network security, an integral aspect of modern computing as threats to network integrity continue to evolve in sophistication and scale. We uncover the various challenges and risks that networks face, ranging from unauthorized access and data breaches to malicious attacks and denial-of-service (DoS) incidents. Encryption emerges as a pivotal tool in securing sensitive information, ensuring that data remains confidential even in transit. We dive into encryption algorithms, digital signatures, and cryptographic protocols, understanding how they safeguard data integrity and authenticate communication participants.

Chapter-1

Introduction to Computer Networks

1.1 Introduction to Computer networks

A communication system for connecting computers/hosts. A computer network is a number of computers (also known as nodes) connected by some communication lines. Two computers connected to the network can communicate with each other through the other nodes if they are not directly connected. Some of the nodes in the network may not be computers at all but they are network devices (Like switches, routers etc.) to facilitate communication.

1.1.1 Introduction to the Networks

By themselves, computers are powerful tools. When they are connected in a network, they become even more powerful because the functions and tools that each computer provides can be shared with other computers.

Fig.1.1 Example of Communication Network.

Network is a small group of computers that share information, or they can be very complex, spanning large geographical areas that provide its users with unique capabilities, above and beyond what the individual machines and their software applications can provide. An example of a communication network is given in Fig.1.1.

The goal of any computer network is to allow multiple computers to communicate. The type of communication can be as varied as the type of conversations you might have throughout the course of a day. For example, the communication might be a download of an MP3 audio file for your MP3 player; using a web browser to check your instructor’s web page to see what assignments and tests might becoming up; checking the latest sports scores; using an instant- messaging service, such as Yahoo Messenger, to send text messages to a friend; or writing an e- mail and sending it to a business associate.

1.1.2 Uses of Computer Networks

a) Resource Sharing
b) Simultaneous Access
c) High Reliability Due To Alternative Sources Of Records
d) Cost Reduction
e) Provide Communication Medium

a) Resource Sharing

1. This is the main purpose of a computer network.
2. It defines creating all programs, peripherals and data feasible to anyone computer on the network to all other computers without considering the physical areas.
3. Thus a user at a considerable distance can share the resources or see computer data in a similar way that a local customer uses them.
4. Load sharing is also a job done by computer network.
5. If a job is needed, it can be implemented using various computers in a network by partitioning it, which reduces time consumption and loads, both things for a particular computer.

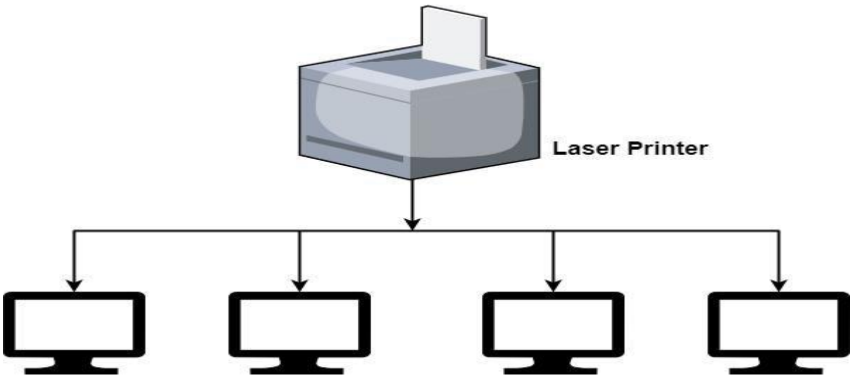


Fig.1.2 Recourse sharing in networks.

b) Simultaneous Access

1. Computer networks allow few users to create programs and data at the equivalent time.
2. An example is a company's quarterly sales document, which several managers need to view and update.
3. We can store the information on a network server, which is a central computer with a huge storage device and other resources that all users can share.
4. If the server stores files for users to access, it is generally known as a file server.
5. We can save an individual copy of a data file on the server, accessible to each employee in the organizations, as displayed in the figure.
6. Moreover, if one user changes the file, other users will see the difference when using it.

7. High Reliability due to Alternative Sources of Records
7. Reliability of networks is helpful to store critical information at more than one location.
8. If a computer fails or crashes, the data can be recovered from the network's other computers.
9. This way, the data is secured in a network. So, computer networks are more popular today.

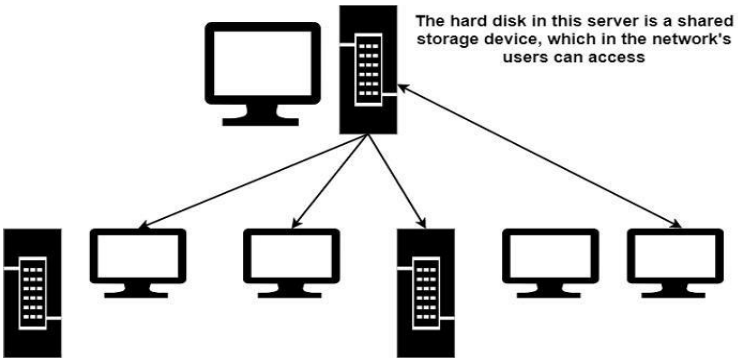

The hard disk in this server is a shared storage device, which in the network's users can access

Fig.1.3 Recourse sharing in networks.

c) Cost Reduction
1. The concept of resources sharing reduces the cost of establishment at each and every location.
2. Small computers can be used instead of mainframes except for servers which paved a way for developing simple devises for individual application at a lower cost.
3. Though mainframes are roughly ten times compared to microcomputers, the cost to performance ratio is much better for small/microcomputers than large/mainframe computers.

Provide Communication Medium

A computer network offers a dynamic communication medium between extensively distinct people. It is easy for two or more people living far apart to work on the same project by partitioning it using a network.

d) Uses of computer for people (A lay man answer)

1. Access to remote information
2. Person-to-person communication
3. Teleconferencing and video conferencing
4. Worldwide news groups
5. Interactive environment

1.1.3 Definition of Computer network

A computer network consists of two or more computers or other intelligent devices linked by communication media (e.g., *Cable* or Wireless Media) to achieve successful communication.

The four elements of computer networks are: Rules 2. Medium 3. Messages 4. Devices
The networks are divided into wired and wireless networks. The example for these are shown in the Fig.1.5 and Fig.1.6.

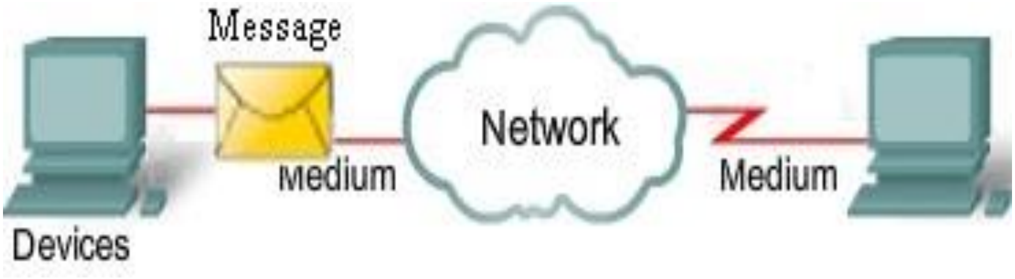


Fig.1.4 Four Elements of Computer networks.

Wired Network: A network in which computers and other devices are connected to the network via physical cables. Ex: Found in homes, schools, businesses, and government facilities.

Wireless: A network in which computers and other devices are connected to the network without physical cables; data is typically sent via radio waves. Ex : Found in homes, schools, and businesses, Wi-Fi hotspots found in coffeehouses, businesses, airports, hotels, and libraries.

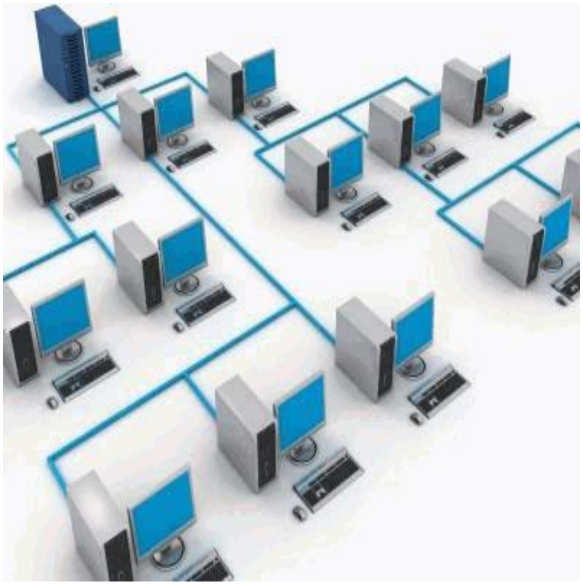


Fig.1.5 Wired networks.

Fig.1.6 Wireless networks.

1.1.4 Common Data network devices and their symbols
The common devices used in computer networks are

1. Desktop computer 2. Server 3. IP phone 4. LAN cable 5. LAN Switch 6. Router 7. Firewall 8. Wireless Router 9. Cloud 10. WAN media 11.Wireless media

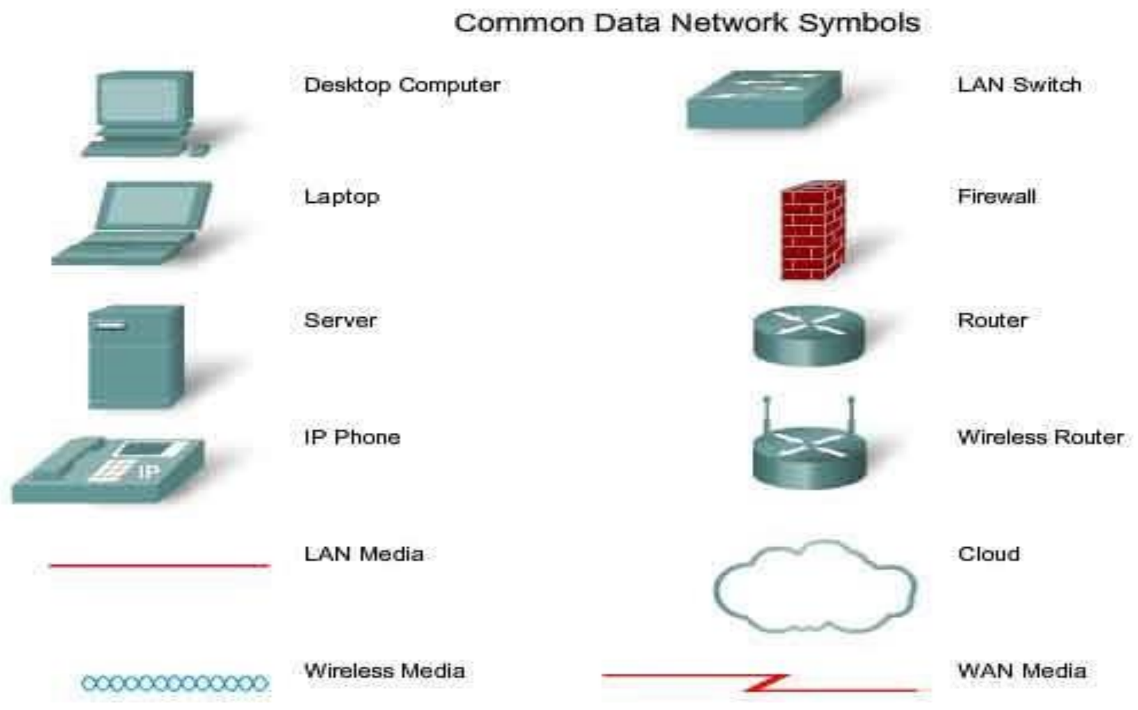


Fig.1.7 Symbols of common devices used in computer networks.

1.1.5 Common Data network connections

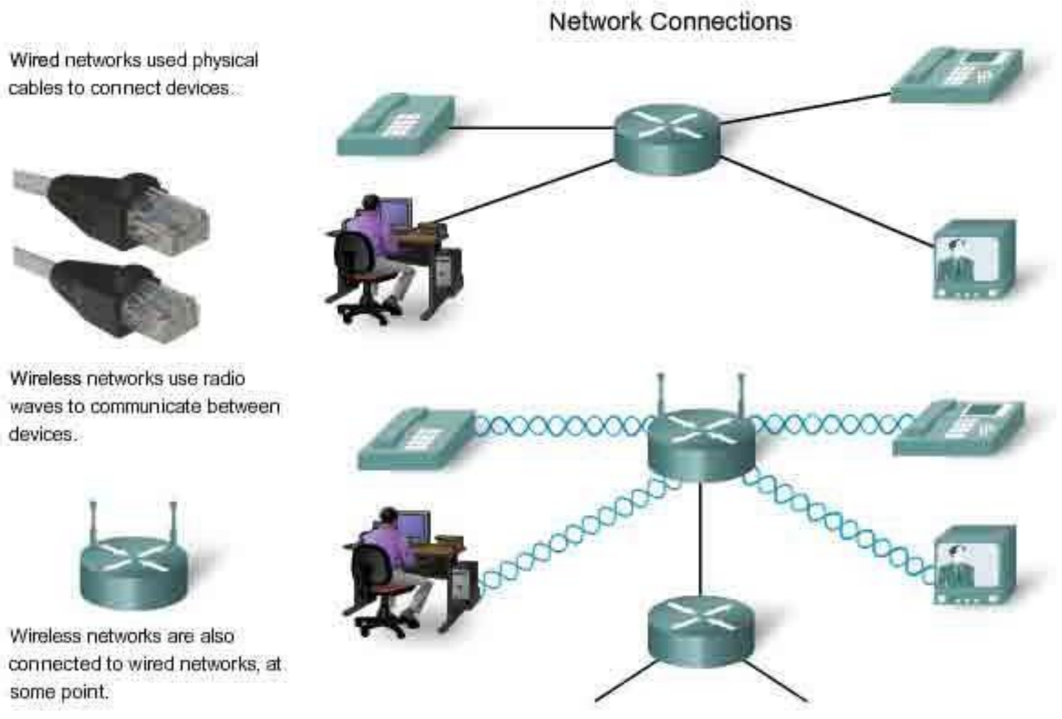

Network Connections
Wired networks used physical cables to connect devices.
Wireless networks use radio waves to communicate between devices.
Wireless networks are also connected to wired networks, at some point.

Fig.1.8 Symbols of common network connections.

1.1.6 Fault Tolerance

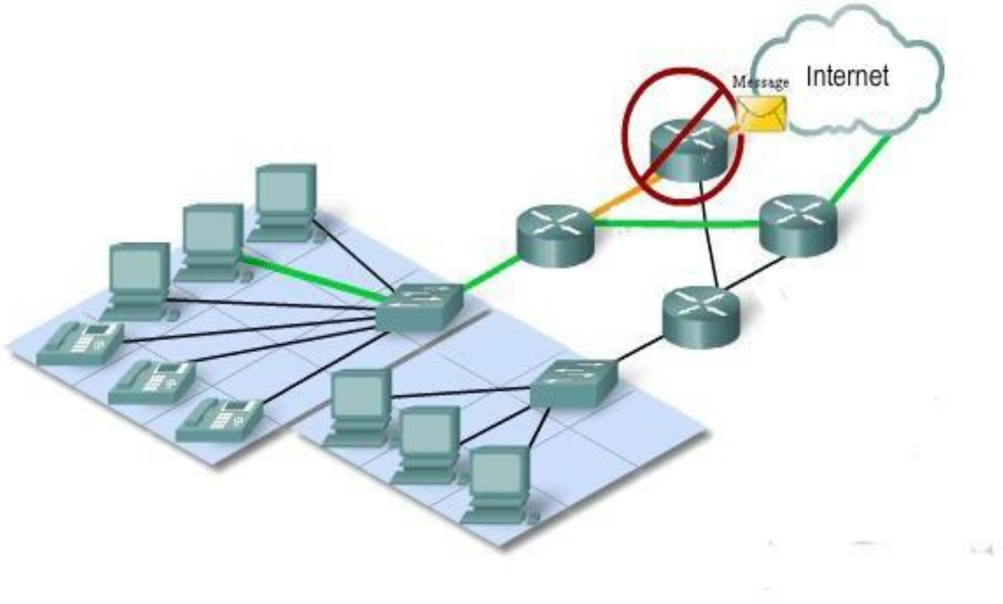


Fig.1.9 Fault Tolerance in networks.

The common feature in networks is to have redundant links which can be used in case if any line where network devices are not working. This is called fault tolerance in networks.

1.1.7 Network topologies

Network topology is defined as a geometrical structure in which devices are connected to each other. There are some defined geometric structures in networks. They are as follows.
1. Mesh 2. Ring 3. Bus 4. Star 5. Tree 6. Hybrid

a) Mesh topology

1. Devices are connected to all other devices through a dedicated point-to-point link.
2. If we have n number of devices we should have n(n-1) physical channels to link the devices.
3. Each device should have n-1 port to connect to each other.
4. Routing and flooding are the methods used to transmit the data in mesh networks.
5. Partial mesh topology and full mesh topology are used in computer networks.
6. In partial mesh topology some devices are connected to two or three devices.
7. In full mesh topology all are connected to each other.

Features of Mesh topology:
1. Fully lined 2. Robust 3. Not flexible

Advantages of Mesh topology:
1. Here the connection carry their unique load. 2. Robust 3. Faults can be identified easily.
4. Facilitates security and privacy.

Disadvantages of Mesh topology:

1. Installation and configuration are difficult.
2. Cabling cost is higher.
3. Bulk wiring is needed.

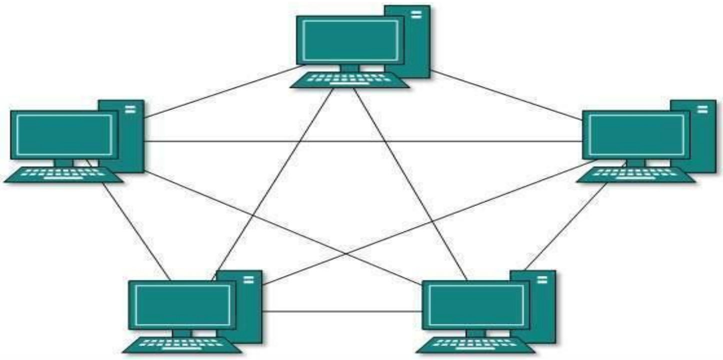


Fig.1.10 Mesh Network.

Applications of Mesh topology:
1. Military organizations 2. Emergency services 3. Backbone of several other topologies

b) Ring topology:

1. Each device is connected to its neighboring device.
2. The last device is connected to the first one.
3. All the devices have two neighbors.

Features of Ring topology:
1. Repeaters are used in large ring networks as the data has to travel all the nodes in the topology.
2. The transmission is unidirectional.
3. But bidirectional transmission is also possible if we have two connections.
4. Data is transmitted bit-by-bit in ring topology.

Advantages of Ring topology
1. Not effected by huge traffic and addition of new nodes
2. Cheaper to install and expand.

Applications:

1. Simple networks are required. 2. Networks having low data rates, 3. Used on LAN's or WAN's

c) Bus Topology: In this all the devices are connected with a single cable like a bus.
Features of Bus topology:
1. Connected to a single cable 2. Data is transferred in a single direction.

Advantages of Bus topology:

1. Cost effective as less amount of cable and ports are required.
2. Easy to understand an easy to expand the network.

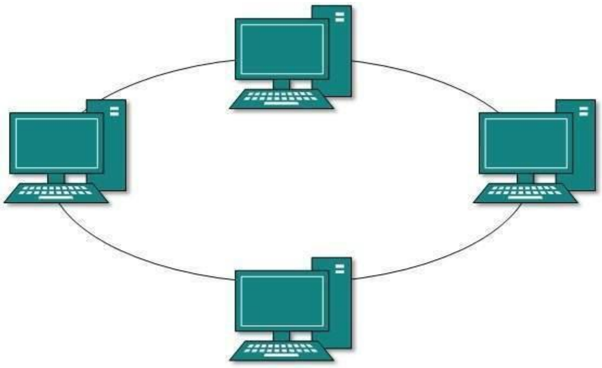


Fig.1.11 Ring Network.

Disadvantages of Bus topology

1. The whole network fails when cable fails.
2. Performance of the network is less when heavy traffic or more number of nodes are there.
3. Expansion of the network is difficult.

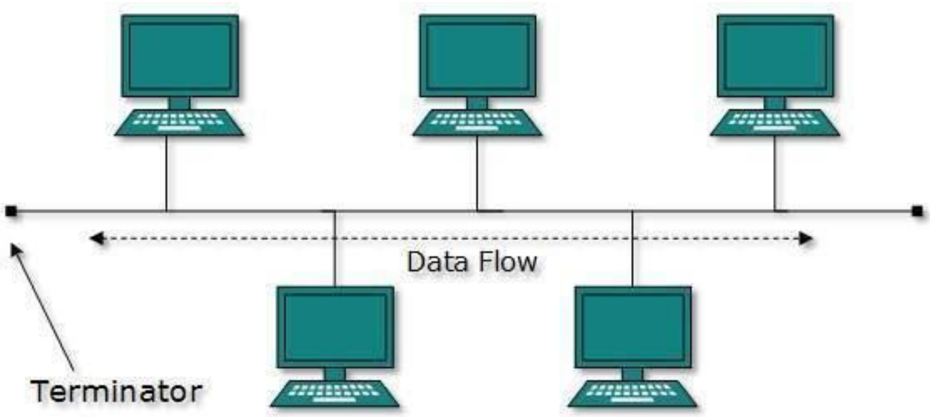


Fig.1.12 Bus Network.

Applications:

1. In computer mother boards.

d) Star Topology

1. Consists of dedicated link between each device and the central system.
2. The central device is called HUB.
3. Topology does not allow direct traffic between network devices.

Features of Star topology:

1. Each node has a unique connection to HUB.
2. HUB acts a repeater for data transmission.
3. Uses twisted pair cables, optical cables or coaxial cables.

Advantages of Star topology:
1. Speedy performance in smaller networks.
2. HUB can be upgraded easily.
3. Simpler to troubleshoot and easy to setup and modify.

Disadvantages of Star topology:
1. Expensive to install and Use.
2. If HUB crashes the whole network crashes.
3. Efficiency is dependent on its capacity.

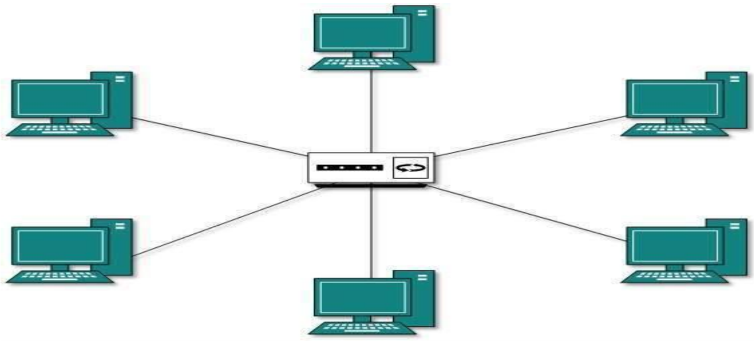


Fig.1.13 Star Network.

Applications of Star topology
1. Used on reservation counters. 2. Small business offices to access to files and applications.

e) Tree Topology

1. Root node and all other nodes are linked to it creating hierarchy.
2. Should have a minimum of three levels.

Features of tree topology:
1. Ideal if workstations are situated in groups.
2. Useful in WAN network.

Advantages of Tree Topology:
1. Extension of bus and star topologies. 2. Expansion of nodes is possible and easy.
3. Easily maintained 4. Fault detection is easy.

Disadvantages of Tree topology:

1. Heavily cabled 2. Costly 3. If additional nodes are introduced, maintenance if difficult.
4. Central hub fails the network fails.

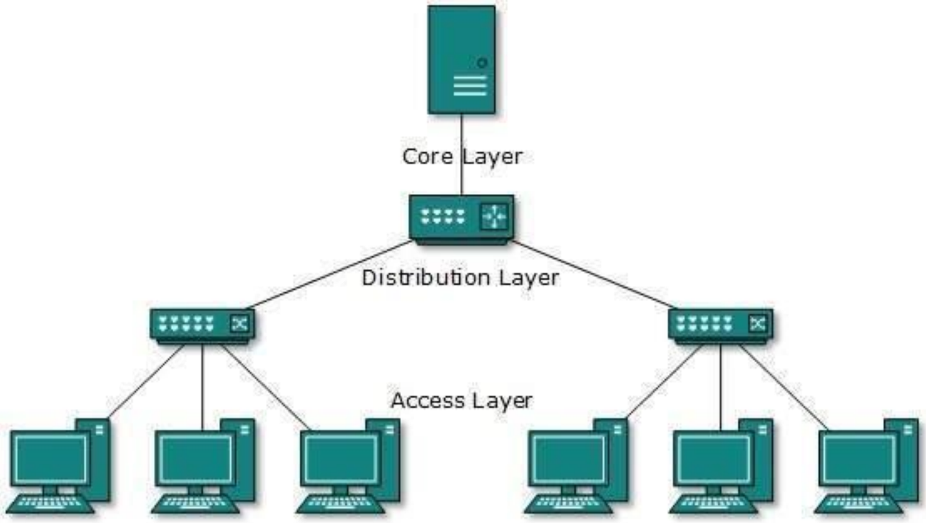


Fig.1.14 Tree Network.

Applications of Tree topology:
1. Used in small offices.

f) Hybrid topology

1. This is a combination of two different topologies. Advantages of Hybrid topology:
1. Reliable network because troubleshooting is easy
2. Cost effective, Flexible and scalable.

Disadvantages of Hybrid topology:
1. Complex in design 2. Costly.

1.2 Data transmission characteristics

Bandwidth: The amount of data that can be transferred at a given time. It is measured in bits per second. We have both analog and digital signals in data-communication. The bandwidth of the analog signal is the range of frequencies who are having a 3dB amplitude with respect to the resonant frequency. The bandwidth of the digital signal is defined as the number of bits that can be transmitted on a given link.

\\

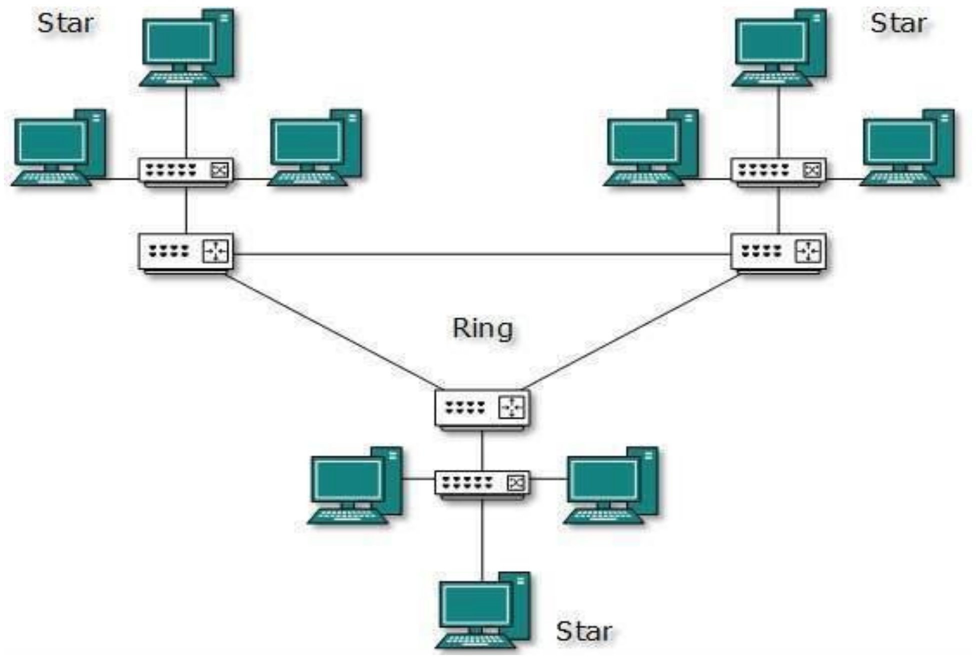


Fig.1.15 Hybrid Network.

We have two different types of data transmission. They are serial and parallel transmission. Serial transmission means sending a single bot at a time. It is a cost-effective communication at larger distances. Parallel transmission means sending a byte of information at a time or parallel transmission is defined as transmission structure that shares multiple data bits at a similar time over separate media. Parallel transmission can be used with a wired channel that uses multiple, separate wires.

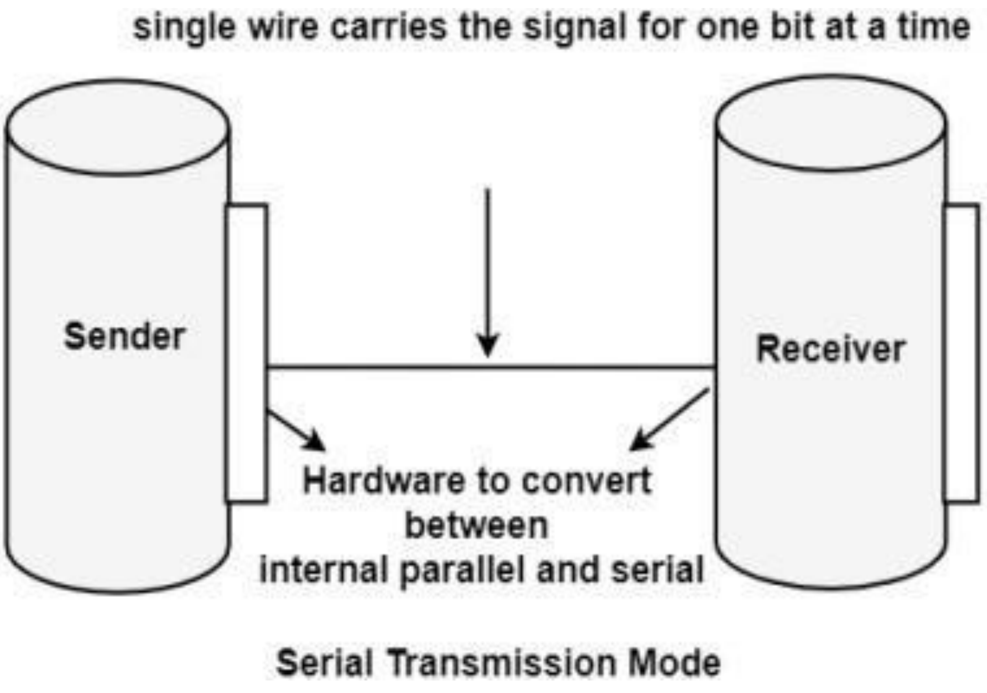

single wire carries the signal for one bit at a time
Sender
Receiver
Hardware to convert between internal parallel and serial
Serial Transmission Mode

Fig 1.16. Serial communication.

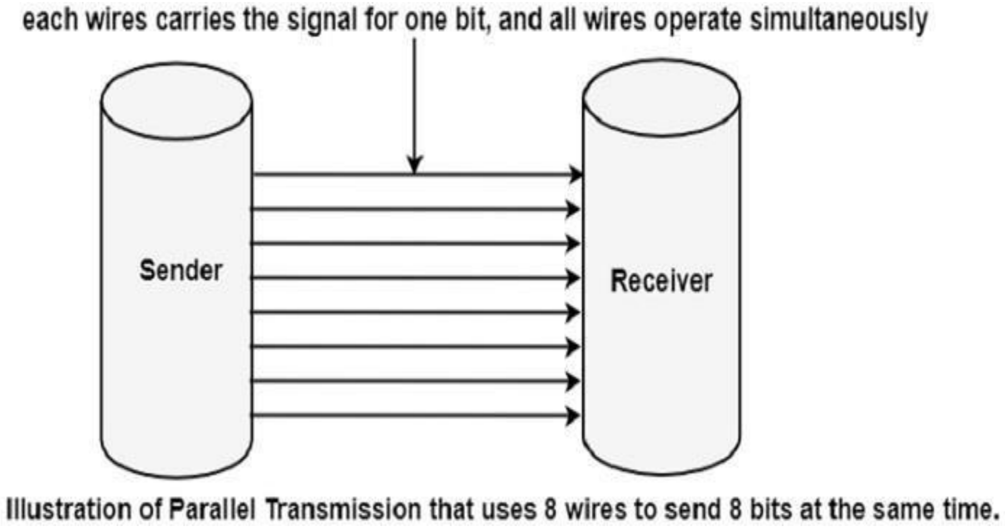

each wires carries the signal for one bit, and all wires operate simultaneously
Sender
Receiver
Illustration of Parallel Transmission that uses 8 wires to send 8 bits at the same time.

Fig 1.17. Parallel communication.

1.2.1 Transmission Timings

We have three different types of transmission timings in data communications. They are synchronous, asynchronous, and isochronous.

Synchronous transmission

Synchronous transmission means transferring data blocks at a continuous and consistent time. This type of communication is used when it is required to send large amounts of data very quickly for one location to another. Here the high speed is achieved by sending individual data blocks rather than individual characters. The data blocks are grouped and are preceded by an special character called as “syn”. These data blocks are spaced in regular intervals in time.

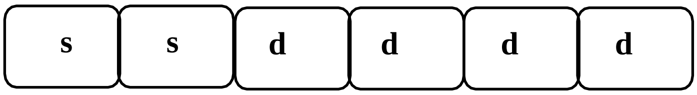


Fig 1.18. Synchronous transmission.

The “syn” characterizes decoded by the receiver at reception at receiver. Then, the connection is established, and data is transmitted. The data transmitted is divided into many parts according to the link requirements and transmitted in small parts. All these are reassembled at the receiver. The timing needed for synchronous connections is acquired from the devices located on the communication link. All the devices must be set to the same clocking signal which are on the communication link.

Characteristics of synchronous communication:

1. No gaps between characteristics are transmitted.

2. Timing information is given by the modem and other devices on the link.
3. "syn" characters precede the data blocks.
4. The "syn" characters used for timing purpose during data transmission.

Asynchronous transmission

Asynchronous transmission mode the data is sent in form of byte or character. The data is not sent sequentially. Here, the data words are identified by start and stop bits. They may be any special character also.

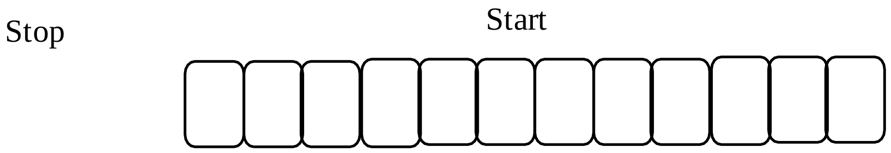


Fig 1.19. Asynchronous transmission.

The data blocks at the receiver are identified by the stop and start bits which are placed at the starting and ending of the data blocks. These additional bits provide the synchronization and timing information at the receiver. In asynchronous transmission the data is sent whenever the data is available. So, gaps are present in data transmission. These are marked by idle bits. These are represented by binary "1" that are set during the link inactive periods.

The following is a list of characteristics specific to asynchronous communication:

1. Each character is preceded by a start bit and followed by one or more stop bits.
2. Gaps or spaces between characters may exist.

Isochronous transmission

Isochronous Transfers are used for transmitting real-time information such as audio and video data and must be sent at a constant rate. USB isochronous data streams are allocated a dedicated portion of USB bandwidth to ensure that data can be delivered at the desired rate. An Isochronous pipe sends a new data packet in every frame, regardless of the success or failure of the last packet.

The maximum packet size for the isochronous endpoint data is:
1. 1023 or less bytes for full speed.
2. 1024 or less bytes for high-speed.

Isochronous Transfers have no error detection. Any error in electrical transmission is not corrected. Isochronous Transfers are also subject to timing jitters.

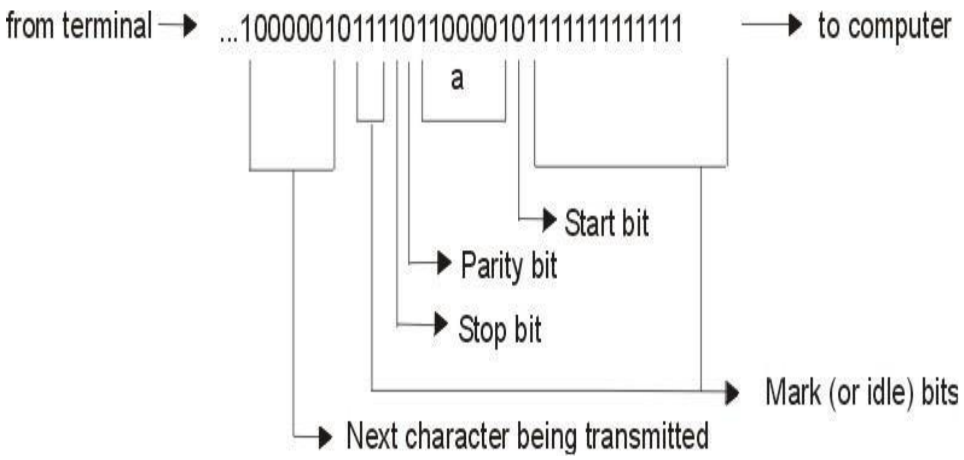


Fig 1.20. Asynchronous transmission with idle bits.

1.2.2 Transmission directions

Transmission direction is the way in the data I transmitted between devices. This is also known as transmission mode or communication mode. Each communication channel has direction in which the data is transmitted. So, these are also called transmission directions. These are defined in physical layer. There are three types of transmission directions. They are

1. Simplex
2. Half-duplex
3. Full-duplex.

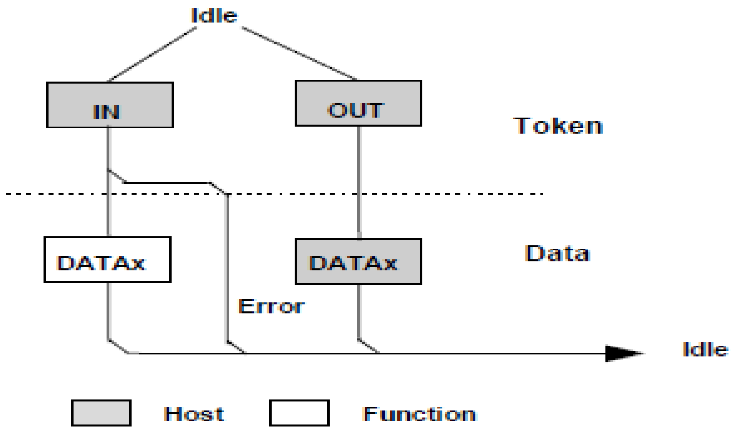


Fig 1.21. Isochronous transmission with idle bits.

Simplex transmission

Simplex transmission is a unidirectional mode of transmission. Data is transferred in one direction only. While sending the data devices cannot receive the data and vice-versa. Radio station, Keyboard, Monitor are some examples of simplex communication. In simplex mode of operation channel bandwidth is completely used. Intercommunication is not possible in simplex transmission.

Half-duplex transmission

In this mode devices can transfer in both directions. While, transmitting in one direction devices cannot transmit in other direction. In this transmission error detection is possible and the receiver requests the sender to retransmit the data. Walkie-talkie is an example of half-duplex transmission. In this mode the bandwidth is entirely used either in transmission or reception.

Full-duplex transmission

In this mode of transmission, the devices can transmit in both directions. Here two simplex connections are established between the devices. A telephone line is an example of full duplex communication. If there are no dedicated links between devices then bandwidth is equally divided between the devices.

1.2.3 Protocols and standards

1. In communication networks data is transmitted between two entities of different systems.
2. An Entity is anything which is capable of sending and receiving information or data.
3. The Entity can send or receive data if they agree to a set of rules called protocols.
4. A protocol defines what is communicated, how it is communicated and when it is communicated.
5. The key elements of the protocol are syntax, semantics, and timing.

Syntax:

Syntax refers to the structure or format of the data, meaning the order in which they are resented.

Ex: In a bit stream of data, a syntax defines which represents the sender’s data and which represents the receiver’s data, and which are the remaining bits represents the messages.

Semantics:

This refers to the meaning of each section of bits. i.e., meaning of each set of bits ans what is the action to be taken based on that.

To address and identify the route where the data must reach or the point in the destination timing is important: The two important factors in timing are.

1. When the data should be sent?
2. How fast data can be sent?

Standards: These are essential in creating and maintaining a open and competitive market of equipment manufacture and guarantying national and international inter-operability of data telecommunications technology and process. They provide guidelines for manufacturers, vendors, government agencies and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communication.

Standards are two categories.

1. De facto: Standards that have been approved by an organized body but have been adopted as standards through widespread use are de-facto standards
2. De Jury: Those have been legislated by an officially recognized body are de -jure.

1.3 Reference Models

Network models use a combination of hardware and software to send data from one location to another location. The tasks involved in communication data are grouped into imaginary layers and are named accordingly. The two important network models are

1. OSI Model (Open System Interconnection Model) -- Reference Model
2. TCP/IP Model (Transmission Control Protocol/Internet Protocol)

1.3.1 Open System Interconnection Model (OSI)

1. Established in – 1947
2. Developed by – International Standard organization.
3. Introduced in 1970
4. Has a set of protocols that allow any two systems to communicate with each other regardless of the underlying architecture.
5. It is a model to understand and design network architecture that is flexible, robust and interoperable.
6. This is layered framework and the design of the network systems that allows communication between all types of computer systems. It consists of 7 separate but related layers.
7. Each layer defines a specific process of moving information across a network.
8. Information travelling from one system to another will travel through many intermediate codes.
9. Here all the related functions are collected and made into discrete groups such that they become layers.
10. Each layer defines a family of functions distinct from those of other layers.
11. Thus, by defining and localizing functionality in this fashion the designers created a architecture that is comprehensive and flexible.
12. With in single machine each layer calls upon services of the layer just below it.
13. Communication is governed by an agreed –upon series of rules and conversions called protocols.
14. The process on each machine that communicates at a given layer is called peer to

peer process.

1.3.2 Organization of layers

1. The seven layers form 3 subgroups
2. Layer-1, Layer -2 and Layer -3 deal with the physical aspects of moving data from one device to another.
3. Layer – 5, Layer – 6 and Layer – 7 are thought of as user support layers. They allow interoperability among unrelated software systems.
4. Layer -4 links the two groups. It ensures what lower layers have transmitted is in the form that upper layer can use.
5. The process starts at upper layer 7 and moves down layer by layer.
6. Each layer adds a header or a trailer to the data unit. Commonly the tailer is added only at Layer 2.
7. When the formatted data unit passes through the physical layer it is converted to electromagnetic signal and is transmitted along the physical link.

1.3.3 Functions of each layer in OSI model

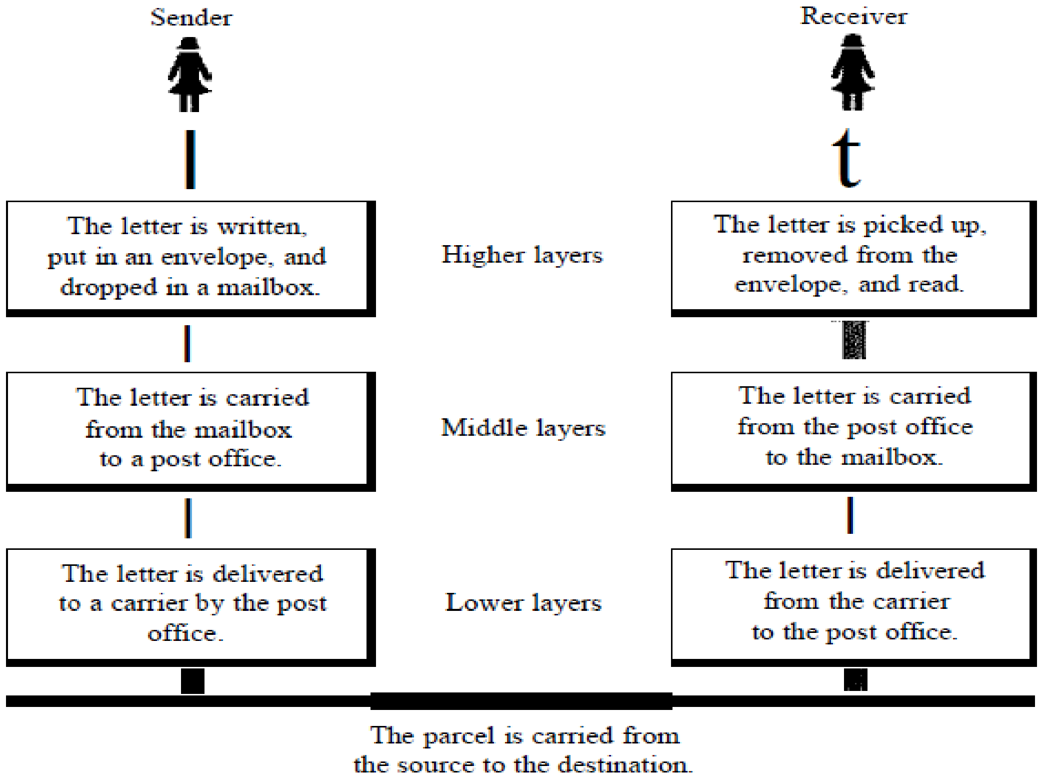
a) Function of Physical layer

1. Physical characteristics of interfaces and medium: Defines the characteristics of interfaces and transmission medium. Defines the type of transmission medium.
2. Representation of bits: Converts the bits into electrical signals and also defines the encoding to be used.
3. Data Rate: Defines the transmission the transmission rate or defines the duration of bits.
4. Synchronization of bits: Sender and receive should have the same bit rate and also are to be synchronized at bit level. In other words, sender and receiver clocks must be synchronized.
5. Line configuration: Physical layer is concerned with type of connections between the network devices.
6. Physical topology: Defines topology of the networks.
7. Transmission mode: Defines the transmission mode (Simplex. Half-duplex and full duplex).

b) Functions of Data Link Layer:

1. Framing: Divides the bits received from the network layer into manageable data units. These data units are called frames.
2. Physical addressing: Add the physical address of source and destination to each frame.
3. Flow control: Imposes a flow control mechanism to avoid overwhelming at the receiver.
4. Error Control: This layer adds reliability to the physical layer by detecting and retransmitting the damaged frames or lost frames. It also recognizes the lost frames and discards them.
5. Access Control: Link layer defines which device has control on link at which time. It

allows the devices to access the link efficiently without loss in transmission.



Sender

Receiver

The letter is written, put in an envelope, and dropped in a mailbox.

Higher layers

The letter is picked up, removed from the envelope, and read.

The letter is carried from the mailbox to a post office.

Middle layers

The letter is carried from the post office to the mailbox.

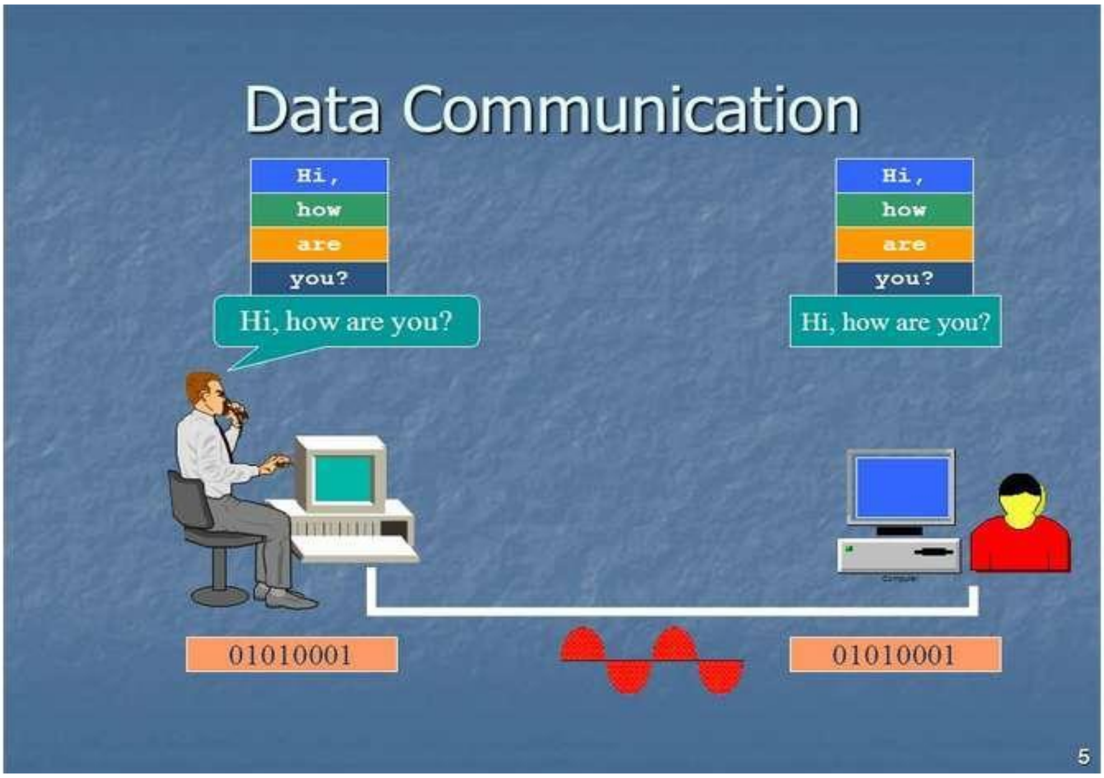
The letter is delivered to a carrier by the post office.

Lower layers

The letter is delivered from the carrier to the post office.

The parcel is carried from the source to the destination.

Fig 1.22. Tasks involved in sending a letter.



Data Communication

Fig 1.23. Communicating through electrical signals.

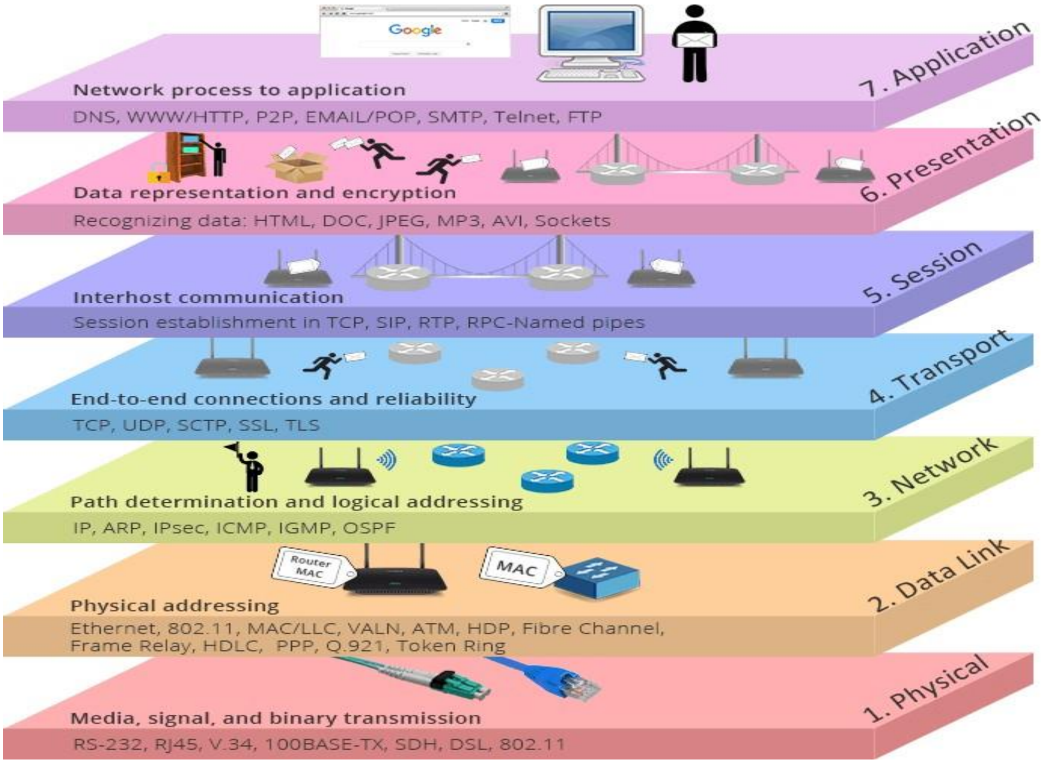

7 . Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

Fig 1.24. Seven Layers of OSI model.

Function of Network layer:

1. Responsible for source to destination delivery across multiple networks.
2. Adds logical address to all the packet coming from upper layers.
3. Routes the packet in a independent network or between different networks.

Functions of Transport Layer:

1. Service point addressing; Responsible for process-to-process delivery.
2. Segmentation and reassembly: Dividing the data from upper layer into transmittable segments containing a sequence number. These numbers enable receiver to reassemble the transmitted segments.
3. Connection control: Responsible for both connection oriented and connection less services.
4. Flow control: Works same as data link layer and is performed end to end rather across a single link.
5. Error Control: Works same as data link layer and is performed end to end rather across a single link.

Functions of Session Layer:

1. Dialog Control: Allows two systems into a dialog which can communicate between

them.

2. Synchronization: Adds check points to steam of data Functions of Presentation Layer:

1. Translation: Converts the data form application layer to a common format.
2. Encryption: Encrypts the data form application layer
3. Compression: Implements compression algorithms such that it occupies lesser data on the memory.

Functions Application layer: This layer enables the user whether the human or software to access the network. It provides interface and support for services such as electronic mail remote file access, database management and other types of distributed information services.

1.3.4 Peer to Peer Process:

1. Each layer calls upon the services provided by layers above and below it.
2. Communication is governed by an agreed-upon rules and conventions called protocols.
3. The processes which communicate at a given layer are called peer-to-peer process.

Interfaces between layer:

1. Allows each layer to data and network information.
2. Establishes a backup through each layer at receiver.
3. Defines what services to be provided to the layers above and below.

To better understand the peer to peer process please watch the video Peer to Peer Process https://www.youtube.com/watch?v=byrH3myfCcc

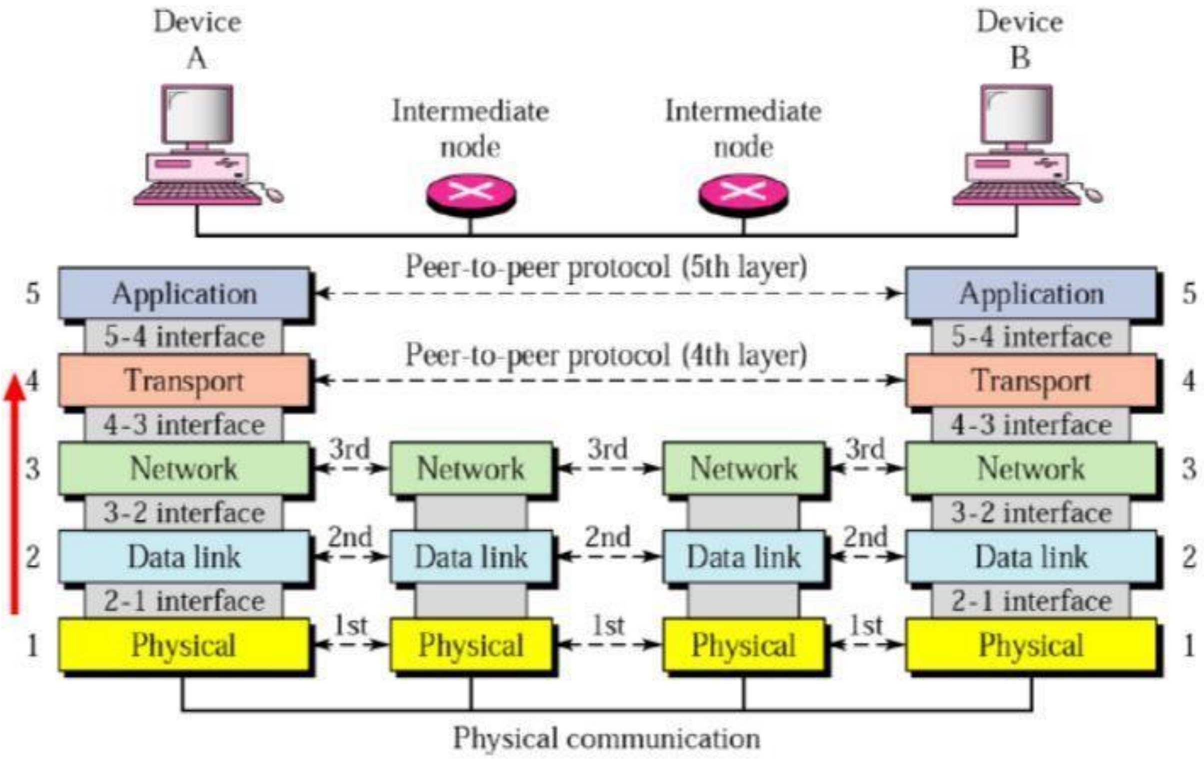
To better understand the OSI model please watch the video. https://www.youtube.com/watch?v=-6Uoku-M6oY

To better understand encapsulation and decapsulation please watch this video https://www.youtube.com/watch?v=AH-09WaUK-4

1.3.5 The TCP/IP Model

1. TCP/IP is a set of communication protocols used in internet and computer networks.
2. This provides end-to-end data communication specifying hw data should be packetized, addressed, transmitted, routed and received.
3. This functionality is divided into five abstract layers 1. Application layer 2. Transport layer

3. Network layer 4.Data link layer 5. Physical layer.
4. In this model the first three layers in the OSI model are combined as application layer



(Application, Presentation, Session)

Fig 1.25. Peer to Peer process.

https://www.youtube.com/watch?v=7rR8p6gsExY
Watch the video for better understanding of TCP/IP.

5. In the physical and data link layer use the protocols Ethernet, PPP, frame relay, Token ring, ATM. They support all the proprietary and standard protocols.
6. It assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination but with no grantees. ARP : Address resolution protocol RARP: Reverse Address resolution protocol ICMP: Internet control message protocol IGMP: Internet group message protocol.
7. In the transport layer TCP/IP uses the protocols TCP and UDP.
8. It is process- to process communication. UDP: User datagram protocol TCP: Transmission Control protocol
9. In the application layer it uses protocols such as SMTP, DNS, FTP etc...

Information at physical layer: bits

1. Information at data link layer: Frames
2. Information at Network layer: Packets

3. Information at Transport layer: Segments
4. Information at Application layer: Data.

Communication at data link layer: Host to Host
Communication at network layer: Hop to hop.
Communication at transport layer: Process to process

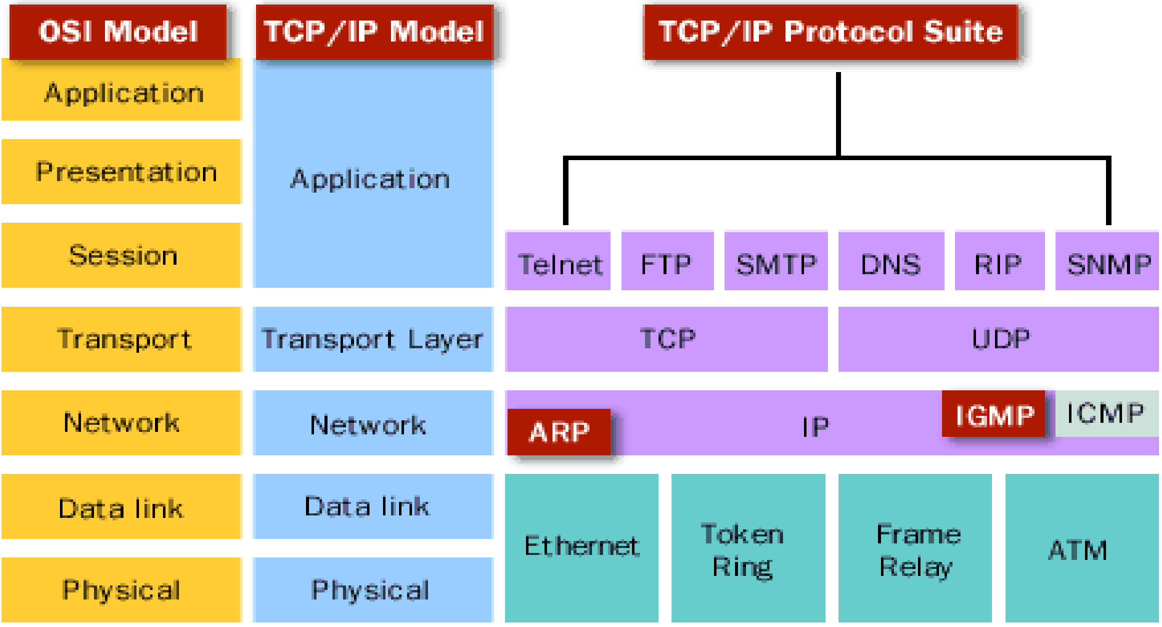


Fig 1.26. TCP/IP Model.

Summary

The International Standards Organization created a model called the Open Systems Interconnection, which allows diverse systems to communicate. The seven-layer OSI model provides guidelines for the development of universally compatible networking protocols. The physical, data link, and network layers are the network support layers. The session, presentation, and application layers are the user support layers. The transport layer links the network support layers and the user support layers. The physical layer coordinates the functions required to transmit a bit stream over a physical medium. The data link layer is responsible for delivering data units from one station to the next without errors. The network layer is responsible for the source-to-destination delivery of a packet across multiple network links. The transport layer is responsible for the process-to-process delivery of the entire message. The session layer establishes, maintains, and synchronizes the interactions between communicating devices.

The presentation layer ensures interoperability between communicating devices through transformation of data into a mutually agreed upon format. The application layer enables the users to access the network. TCP/IP is a five-layer hierarchical protocol suite developed before the OSI model. The TCP/IP application layer is equivalent to the combined session, presentation, and application layers of the OSI model. Four levels of addresses are used in an internet following the TCP/IP protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses. The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. The IP address uniquely defines a host on the Internet. The port address identifies a process on a host. A specific address is a user-friendly address.

Self-Assessment Questions:

1. What is the primary purpose of a computer network?

a) Sharing computer hardware components
b) Facilitating communication and data exchange
c) Running multiple operating systems on a single machine
d) Enabling virtual reality experiences

2. Which layer of the OSI model is responsible for data transmission between directly connected devices?

a) Physical Layer b) Data Link Layer c) Network Layer d) Transport Layer

3. What is a protocol in the context of computer networks?

a) A set of rules and conventions for communication
b) A specific brand of network hardware
c) A type of computer virus
d) A device used for wireless networking.

4. Which network topology connects all devices in a linear sequence?

a) Bus b) Star c) Ring d) Mesh

5. What is the primary advantage of a wireless network over a wired network?

a) Higher data transfer rates b) Greater security c) No physical cabling required d) Lower latency

6. Which protocol is used for reliable data delivery over an IP network?

a) TCP b) UDP c) ICMP d) HTTP

7. Which of the following is a hardware component of a computer network?

a) Network protocol b) Router c) TCP/IP d) DNS server

8. What is the main function of a network adapter (NIC)?

a) To manage network traffic
b) To provide internet access to devices
c) To connect devices from different networks
d) To connect devices to the network

9. Which software component is responsible for managing and controlling network devices?
a) Network adapter
b) Network protocol
c) Network operating system
d) Router

10. Which hardware component allows multiple devices to connect to a network wirelessly?
a) Switch
b) Hub
c) Modem
d) Wireless Access Point (WAP)

11. What is the primary function of a router in a computer network?
a) To connect devices within the same network
b) To connect devices from different networks
c) To manage network protocols
d) To control internet speed

12. Which software component provides a user interface for configuring and managing network devices?
a) Network adapter b) Network operating system c) Network protocol d) Router

13.What is the purpose of a network cable in a computer network?
a) To convert digital data into analog signals
b) To provide wireless connectivity
c) To transmit data between network devices
d) To filter network traffic.

14. Which hardware component is used to connect a network to the internet service provider (ISP)?
a) Router b) Switch c) Hub d) Modem

14. What is the primary function of a network operating system (NOS)?
a) To manage hardware components of the network
b) To provide internet access to devices
c) To enable communication and resource sharing among devices
d) To convert analog signals into digital data

15. Which software component is responsible for translating domain names to IP addresses?
a) DNS server b) DHCP server c) NOS d) Modem

15. Compare and contrast the OSI model and the TCP/IP model in terms of their origin's development and practical applications.

16. Explain how the voice and TCP/IP models are used in modern network troubleshooting and design.

17. What are some examples of network problems or scenarios that can be better understood and resolved by applying principles of the OSI or TCP/IP model.

18. How does the TCP/IP model differ from OSI model in terms of the number of layers and their names.

19. Explain the role of each layer in TCB/IP model such as the network, transport, Internet and application layers.

20. Describe the key protocols associated with TCP/IP model and which layer do they operate in.

21. What is the relationship between the TCP/IP model and OSI model how do they align in terms of their layers.

22. Discuss the advantages of the TCP bar IP model compared to the voice I model especially in the context of Internet and real-world network.

23. What are the seven layers of osi model and can you name them in the order from the physical layer to the application layer?

24. Describe the primary function of each layer in OSI model and provide an example of protocol or technology associated with each layer

Terminal Questions

1. Why is the computer network so important?
2. What is the difference between a host and an end system? List several different types of end systems. Is a web server an end system?
3. Why are standards important for protocols?
4. What are some of the physical media that the ethernet can run over?
5. What advantages does a circuit-switched network have over a packet-switched network?
6. What is peer-to-peer process?
7. Explain OSI model and its role in computer networks?
8. Identify the five components of a data communications system.
9. What are the advantages of distributed processing?
10. What are the three criteria necessary for an effective and efficient network?
11. What are the advantages of a multipoint connection over a point-to-point connection?
12. What are the two types of line configuration?

13. Categorize the four basic topologies in terms of line configuration.
14. What is the difference between half-duplex and full-duplex transmission modes?
15. Name the four basic network topologies, and cite an advantage of each type.
16. For *n* devices in a network, what is the number of cable links required for a mesh, ring, bus, and star topology?
17. What are some of the factors that determine whether a communication system is a LAN or WAN?

References of books, sites, links

Text Books

1 TCP/IP Protocol Suite, Behrouz A.Ferouzan, Fourth Edition

2 The DHCP Handbook, Ralph Droms, and Ted Lemon, Second Edition

3 Enabling Enterprise Multi homing With Cisco IOS Network Address Translation (NAT), Praveen Akkiraju, Cisco Consulting Engineering Kevin Delgadillo, Cisco IOS Product Marketing Yakov Rekhter, Cisco Fellow

4 PRO DNS and Bind, Ronald G.F.Aitchison,

5 Cisco certified Network Associate (200-120)

Web References

1 http://dkim.org/

2 Data and Computer Communications, William Stallings, Tenth Edition

3 https://notes.shichao.io/tcpv1/ch8/

4 David D. Clark (July 1982), IP Datagram Reassembly Algorithms .pdf (Type in Google)

5 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh945104(v=ws.11)

Chapter – 2
Physical Layer

2.1 Design issues of network layer

1. Reliability: Reliable data transmission is required.
2. Scalability: Networks to be flexible such that the process continues even when more devices are added and removes. Interoperability must be there between all the devices.
3. Addressing: Proper addressing mechanician must be maintained.
4. Error Control: All the layers agree upon a common error detection and correction methods while they are transmitted.
5. Flow Control: Proper flow control mechanisms must be maintained so that there is no loss of data due to different data rates of the devices.
6. Recourse allocation: Computer network provide services in the form of network resources to the end users. The main design issue is to allocate the and deallocate resources to all the process so that there is a minimal interface among hosts with optimal usage.
7. Statistical Multiplexing: Intelligently the bandwidth should be divided to each device.
8. Routing: Routing to optimal path should be done to reach the destination.
9. Security: The security mechanisms should be followed so that data reaches to the defined destination without and distortion.

2.2 Service Primitives:

1. Listen: Witing for incoming connection.
2. Connect: Means to establish a connection.
3. Receive: Waiting for incoming message.
4. Send: To transmit the data.
5. Disconnect: To terminate the connection.

2.3 Connection oriented and connection less services

Connection oriented	Connection less
Prior connection needs to be established	No need to establish prior connection
Recourses to allocated	Allocation of recourses not required
It ensures reliability of data	It is best effort service
No congestion takes place	Congestion takes place
Implements circuit switching	Implements packet switching
If data is lost there is a possibility of retransmission is there	Retransmission is not possible

Suitable for long and steady connection	Suitable for busty transmission
Connection is established through signalling	There is no concept of signalling
Packet reaches destination in sequential mode	Packet reaches destination in random mode
More delay in transmission, but once connection is established faster delivery is assured	There is no delay due to absence of connection established

2.4 Network architectures

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer. The two types of network architectures are used 1. Peer-To-Peer network 2. Client/Server network

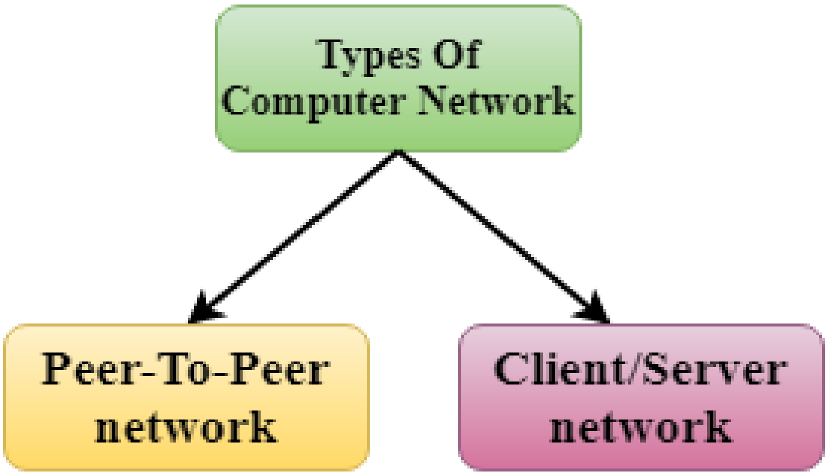


Fig.2.1. Types of Network architectures.

a) Peer-To-Peer network

1. Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
2. Peer-To-Peer network is useful for small environments, usually up to 10 computers.
3. Peer-To-Peer network has no dedicated server.
4. Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

Advantages Of Peer-To-Peer Network:

1. It is less costly as it does not contain any dedicated server.
2. If one computer stops working, but, other computers will not stop working.
3. It is easy to set up and maintain as each computer manages itself.
4. Disadvantages of Peer-To-Peer Network:

5. In the case of Peer-To-Peer network, it does not contain the centralized system.
6. Therefore, it cannot back up the data as the data is different in different locations.
7. It has a security issue as the device is managed itself.

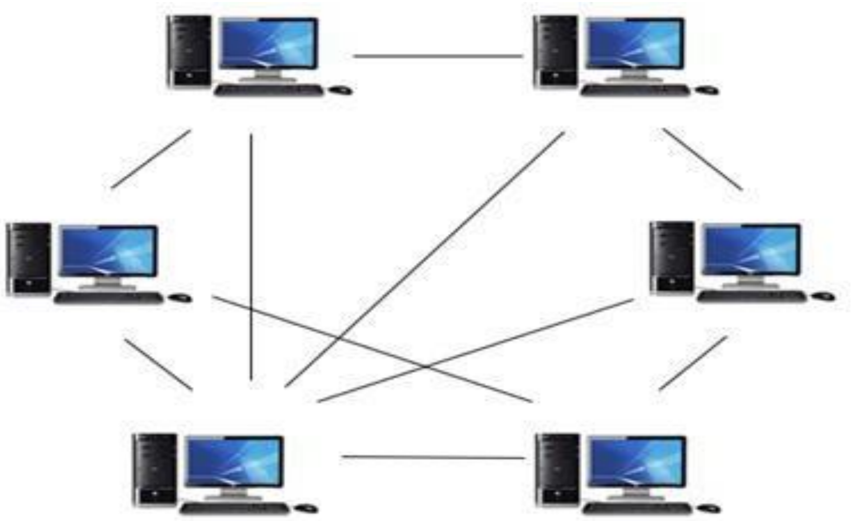


Fig.2.2. Example of Peer-to-Peer Network architectures.

b) Client/Server Network

1. Client/Server network is a network model designed for the end users called clients, to access resources such as songs, video, etc. from a central computer known as Server.
2. The central controller is known as a **server** while all other computers in the network are called **clients**.
3. A server performs all the major operations such as security and network management.
4. A server is responsible for managing all the resources such as files, directories, printer, etc.
5. All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for permission.
6. The server sends the response to client 1 to initiate its communication with the client 2.

2.5 Types of Networks

Different types of networks are distinguished based on their size (in terms of the number of machines), their data transfer speed, and their reach. There are usually said to be two categories of networks.

a) Local Area Network (LAN)

Local Area Network (LAN) is limited to a specific area, usually an office, and cannot extend beyond the boundaries of a single building. The first LANs were limited to arrange (from a central point to the most distant computer) of 185 meters (about 600feet) and no more than 30 computers. Today's technology allows a larger LAN, but practical administration limitations required to small, logical areas called workgroups. A work group is a collection of individuals who share the same files and databases over the LAN. Fig 0.2 gives an example of a local area network (LAN).

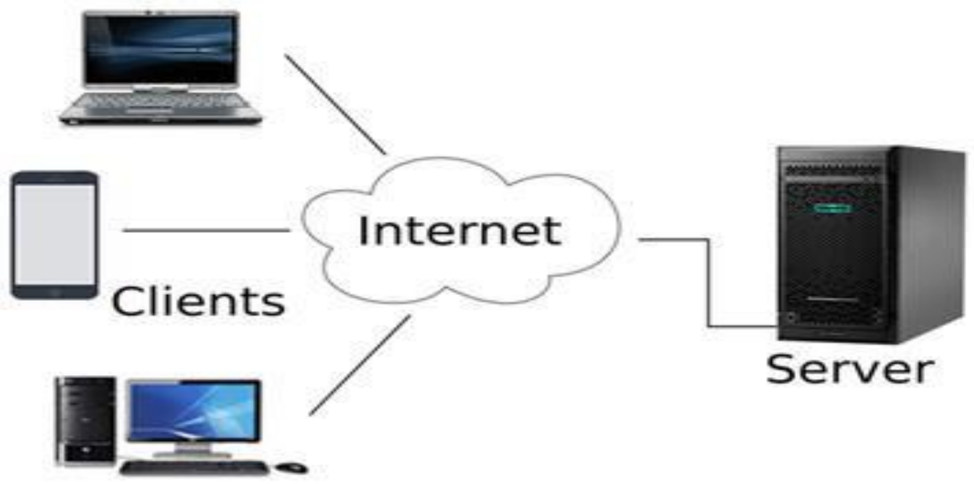


Fig.2.3. Example of Client-Server Network architectures.

b) Wide Area Network (WAN)

If you have ever connected to the Internet, you have used the largest WAN on the planet. A WAN is any network that crosses metropolitan, regional, or national boundaries. Most networking professionals define a WAN as any network that uses routers and public network links. The Internet fits both definitions. Fig 0.2 gives an example of a wide area network (WAN).

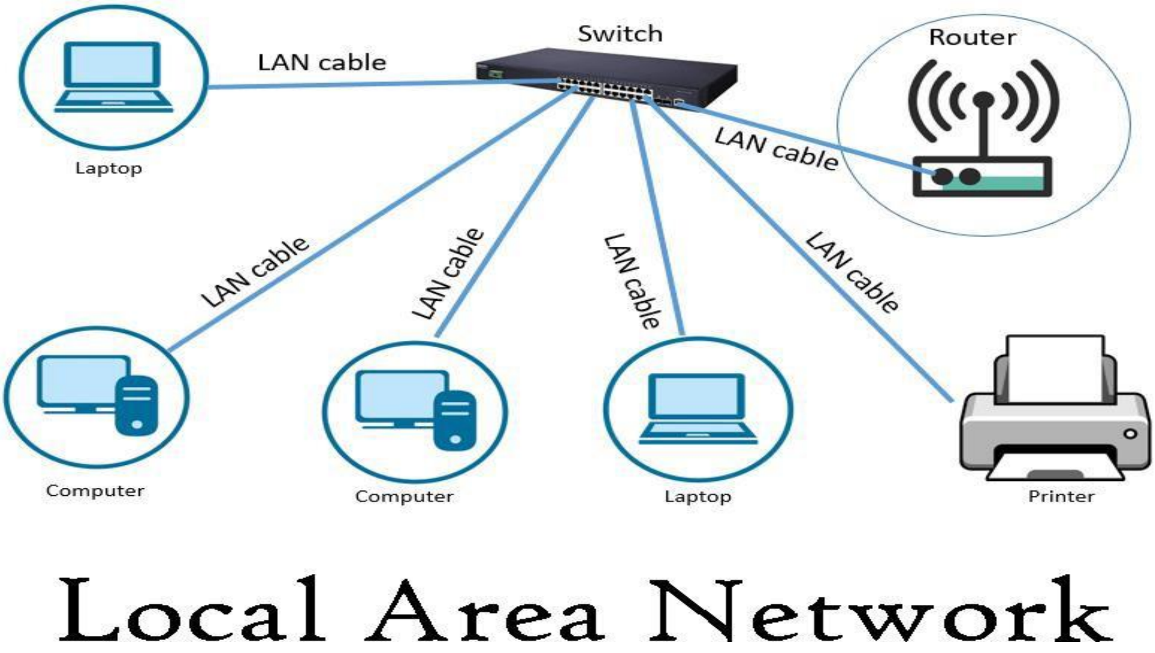


Fig.2.4. Local area network.

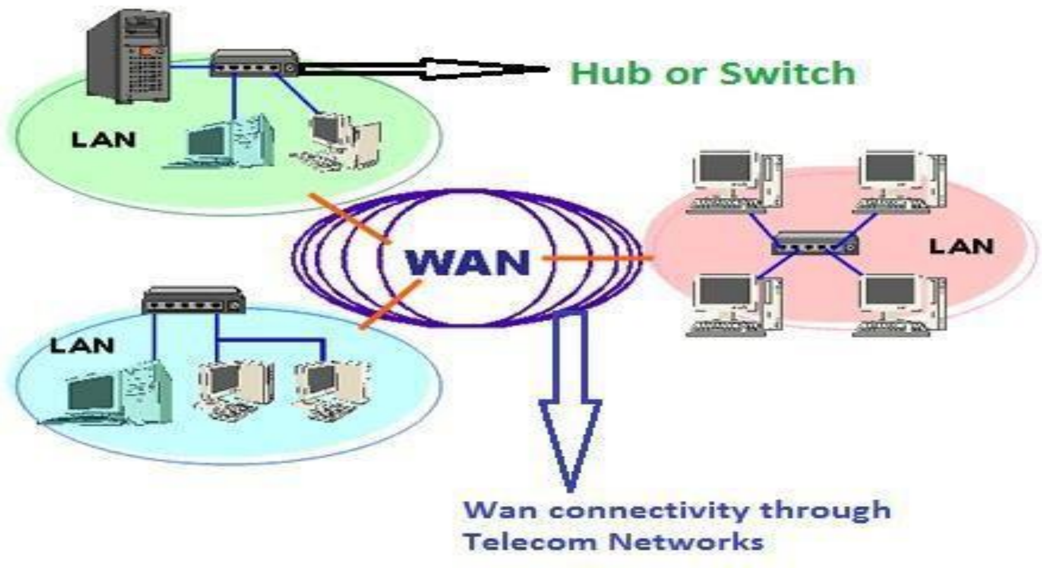


Fig.2.5. Wide area network.

Comparison between LAN and WAN

Tab 2.1 Comparison between LAN and WAN

	LAN	WAN
Stands for	Local Area Network	Wide area network
Covers	Local areas only offices, schools) (e.g., homes,	Large geographic areas (e.g., citi states, nations) es,
Definition	LAN (Local Area Network) is a computer network covering a small geographic area, like a home, office, schools, or group of buildings.	WAN (Wide Area Network) is a computer network that covers a broad area or any network whose communications links cross metropolitan, national boundaries over a long distance.
Speed	High speed (1000 Mbps)	Less speed (150 Mbps)
Data transfer rates	LANs have a high data transfer rate.	WANs have a lower data transfer rate compared to LANs.
Example	The network in an office building can be a LAN	The Internet is a good example of a WAN
Technology	Tend to use certain connectivity technologies, primarily Ethernet and Token Ring	WANs tend to use technologies like MPLS, ATM, Frame Relay and X.25 for connectivity over longer distances

Connection	One LAN can be connected to other LANs over any distance via telephone lines and radio waves.	Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.
Components	Layer 2 devices like switches,	Layers3 devices Routers, Switches
	bridges, Layer 1 devices like Hubs, Repeaters	Technology specific devices like ATM or Frame-relay Switches.
Fault Tolerance	LANs tend to have fewer problems associated with them, as there are smaller in number of systems to deal with.	WANs tend to be of fewer faults tolerance as they consist of large number of systems.
Data Transmission Error	Experiences fewer transmission errors data	Experiences more data transmission errors as compared to LAN
Ownership	Typically owned, controlled, and managed by a single person or organization.	WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management over long distances.
Set-up costs	If there is a need to set-up a couple of extra devices on the network, it is not very expensive to do that.	For WANs since networks in remote areas have to be connected the set-up costs are higher. However WANs using public networks can be setup very cheaply using just software (VPN etc).
Geographical Spread	Have a small geographical range and do not need any leased telecommunication lines	Have a large geographical range generally spreading across boundaries and need leased telecommunication lines
Maintenance costs	Because it covers a relatively small geographical area, LAN is easier to maintain at relatively low costs.	Maintaining WAN is difficult because of its wider geographical coverage and higher maintenance costs.
Bandwidth	High bandwidth is available for transmission.	Low bandwidth is available transmission.
Congestion	Less congestion	More congestion

c) Metropolitan Area Network (MAN)

1. Ownership of network is private or public.
2. Geographical area covered: Moderate.
3. Design and Maintenance is not easy.
4. Communication Medium: Coaxial cables, Optical fiber cables, PSTN, Wireless.
5. Band width of MAN is moderate.
6. Data rates(Speed):Moderate
7. It is used for small towns and cities.
8. Using Man multiple computers can simultaneously interact with each other.
9. It covers relatively large region such as cities, towns.
10. In Man congestion is more.
11. Fault tolerance: Less tolerant.

d) Personal Area Network (PAN)

1. Used for low data rate and short distance applications.
2. Data Rate in Pan is 250Kbps in ZigBee, From Kbps to 24 Mbps in blue tooth case .
3. It is used for Short range.
4. Pan has both star and mesh architectures.
5. Mainly used for low data rate applications in home automation, Bluetooth is used for data transfer between devices.
6. Pan is widely adopted in IoT (Internet of Things).

A personal area network (PAN) is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters. Bandwidth of PAN is less. PAN can be wired, such as USB or FireWire, or they can be wireless, such as infrared, ZigBee, Bluetooth and ultra-wide band, or UWB. Design and Maintenance of PAN is easy.

2.6 Guided transmission media

In communication channel is called the medium or transmission medium. It is of two types guided/wired media and unguided/wireless media. In guided transmission media we have three types 1. Guided/wired Twisted paired cable 2. Co-axial cable 3. Fiber-optic cable. In Unguided transmission media there are two types 1. Microwave links 2. Infrared. Factors which are considered to select the transmission media are

1. Transmission rate
2. Cost and ease of installation
3. Resistance to environmental conditions
4. Distances

Guided Transmission media

1. Twisted pair cable consists of two identical wires wrapped together in a double helix. Twisting of cables reduces crosstalk (leakage of signal from one to another). This reduces the noise. This also reduces external signal interference.
2. There are two types of twisted pair cables. They are Unshelled twisted pair cable (UTP) and shielded twisted pair cable (STP). The figure Fig 0.33 represents UTP and STP.

Advantages of twisted pairs
1. Simple
2. Flexible
3. Connected
4. Easy to install.
5. Low weight
6. Cheap

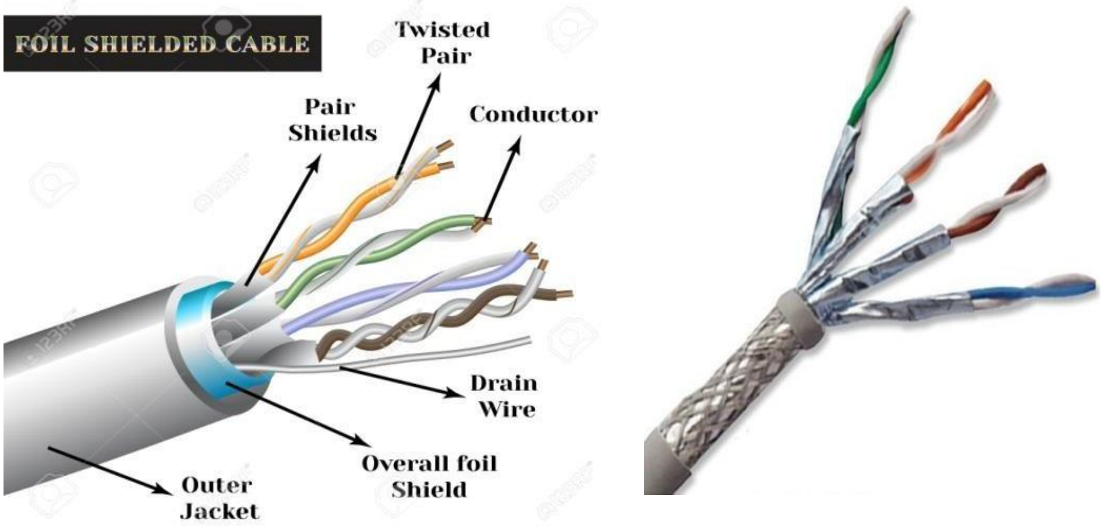


Fig.2.6. UTP and STP cables.

Disadvantages of twisted pairs

1. Attenuation over larger distances
2. We should use repeaters.
3. Low bandwidth
4. The data rates are 1Mbps (no conditions) and 10 Mbps (with conditions)

Coaxial cable

Consists of solid wire core (Concentric conductors) surrounded by one more foil/wire, each separated by plastic insulator. The plastic core is suitable for high speed communications widely used in television. There are two types of coaxial cables thicket and thinned. Coaxial cable is suitable for high-speed communication in wired communication. Fig 0.34 represents the thick and thin coaxial cables. Length of thicket cable is up to 500 meters long and thinnest is up to 185 meters.

Advantages of coaxial cable

1. Transmission characteristics are better than twisted pair
2. Broadband transmission
3. Shared cable network
4. High b/w 400mbps Disadvantages of coaxial cable

1. Expensive
2. Not compatible with twisted pair

Optical fiber

It consists of an inner glass core surrounded by a glass-like material which has layer refractive index. It consists of core and cladding. It works on the concept of total internal reflection. Core is a glass or a plastic through which light travels. Cladding is a covering of core and its function is it reflects light back to core.

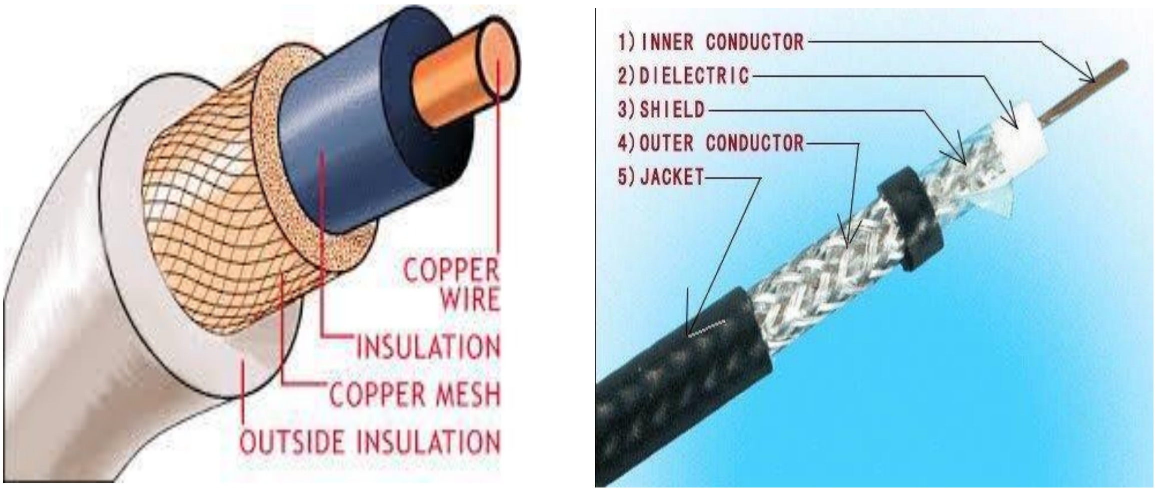


Fig.2.7. represents the thick and thin coaxial cables.

Protective coating is used to protect a hostile environment. There are two types of optical cable. They are single node and multi node. Single mode is used for 2 Kms and speed of 100Mbps data rate and multi-mode is used for 100 Kms and 2Gbps data rate. Fig 0.35(a) and (b) Represents the single mode and multi-mode optical file.

Advantages of Optical fibers

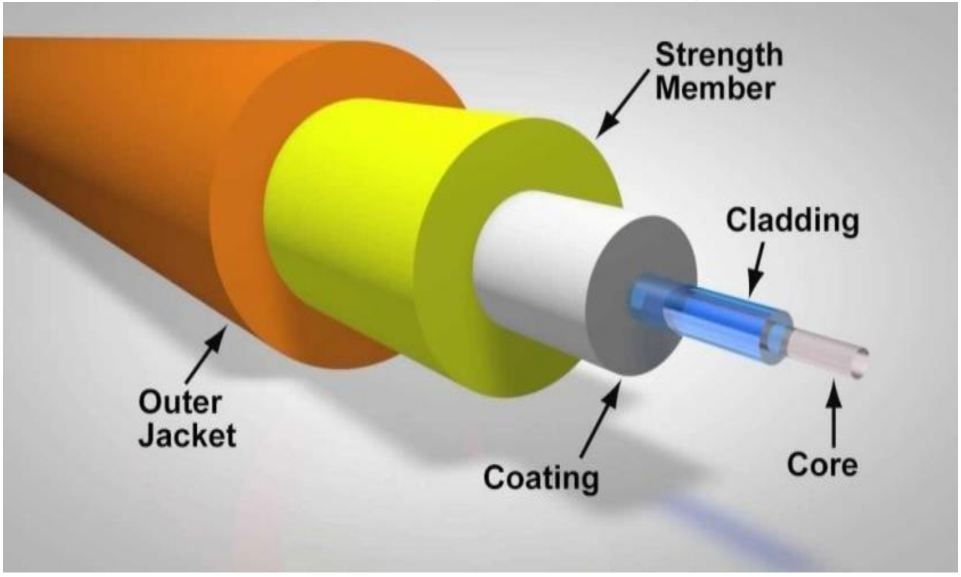
1. Immune to electrical and mechanical interference
2. Highly suitable for harsh environments.
3. Secure transmission
4. Broad band transmission

Disadvantages of optical fibers

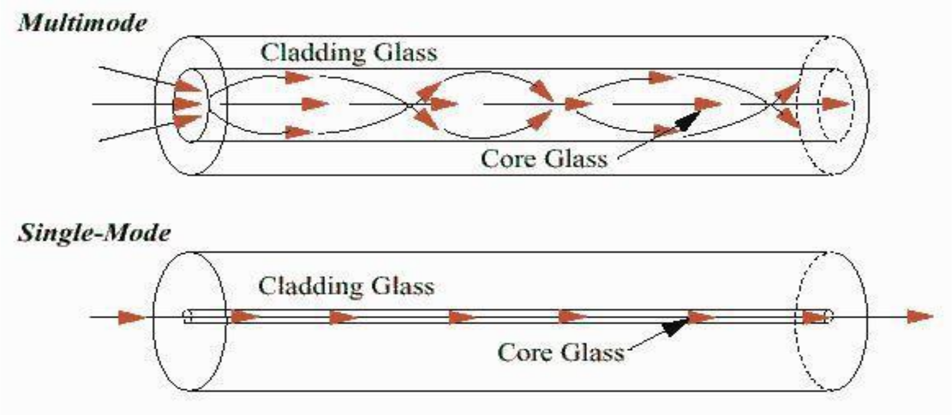
1. Installation problems
2. Connecting fibers is difficult.
3. Light is out if phase when there is a cut or bend.
4. More communication loss
5. Most expensive

2.7 Unguided Transmission Media

An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore, it is also known as wireless transmission. In unguided media, air is the medium through which the electromagnetic energy can flow easily. Unguided transmission is broadly classified into three categories. Fig 0.36 represents unguided transmission media.



(a)



(b)

Fig.2.8. (a) and (b) Represents the single mode and multi-mode optical file.

.

1) Radio waves
2) Microwaves
3) Infrared waves

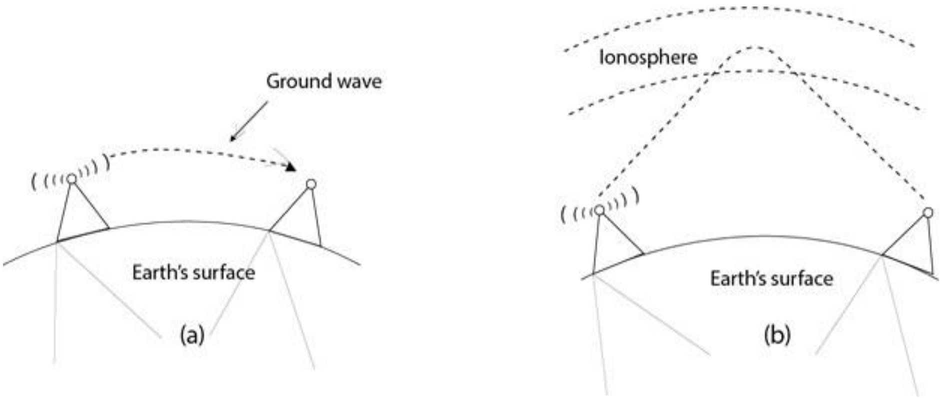


Fig.2.9. represents unguided transmission media.

Radio Waves

1. Radio waves are electromagnetic waves that are transmitted in all the directions of free space.
2. Radio waves are omni directional, i.e., the signals are propagated in all the directions.
3. The range in frequencies of radio waves is from 3Khz to 1Khz.
4. In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
5. An example of the radio wave is FM radio.

Applications Of Radio waves

1. A Radio wave is useful for multicasting when there is one sender and many receivers.
2. FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

1. Radio transmission is mainly used for wide area networks and mobile cellular phones.
2. Radio transmission provides a higher transmission rate.
3. Radio waves cover a large area, and they can penetrate the walls.

Microwaves

Microwaves are of two types:
1. Terrestrial microwave.
2. Satellite microwave communication.

Terrestrial Microwave Transmission

1. Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
2. Microwaves are electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
3. Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focused.
4. In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
5. It works on the line-of-sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave

1. Frequency range: The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
2. Bandwidth: It supports the bandwidth from 1 to 10 Mbps.
3. Short distance: It is inexpensive for short distances.
4. Long distance: It is expensive as it requires a higher tower for a longer distance.
5. Attenuation: Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

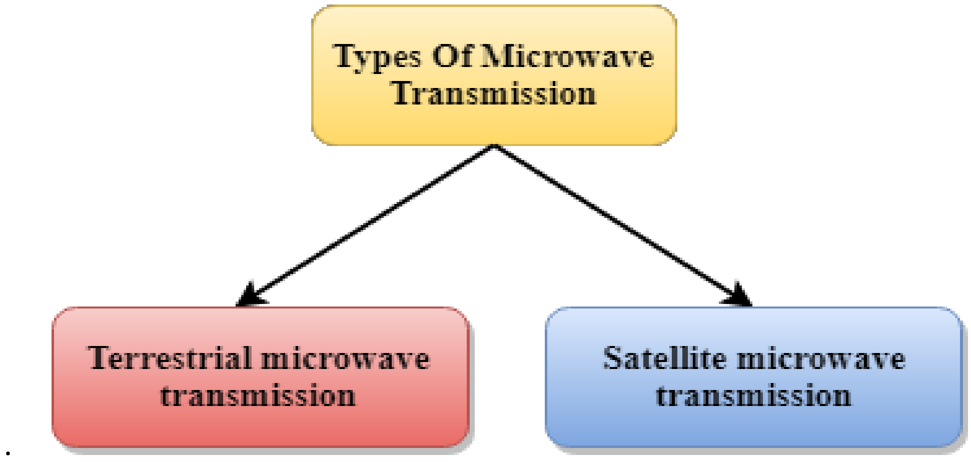

Types Of Microwave Transmission
Terrestrial microwave transmission
Satellite microwave transmission

Fig.2.10. Represents microwave transmission media.

Advantages Of Microwave

1. Eavesdropping: Eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
2. Out of phase signal: A signal can be moved out of phase by using microwave transmission.

3. Susceptible to weather condition: A microwave transmission is susceptible to eather condition. This means that any environmental change such as rain, wind can distort the signal.
4. Bandwidth limited: Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

1. A satellite is a physical object that revolves around the earth at a known height.
2. Satellite communication is more reliable nowadays as it offers more flexibility than cable and fiber optic systems.
3. We can communicate with any point on the globe by using satellite communication.

Advantages Of Satellite Microwave Communication

1. The coverage area of a satellite microwave is more than the terrestrial microwave.
2. The transmission cost of the satellite is independent of the distance from the center of the coverage area.
3. Satellite communication is used in mobile and wireless communication applications.
4. It is easy to install.
5. It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

1.Satellite designing and development requires more time and higher cost.

2.The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.

3. The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

1. Infrared transmission is a wireless technology used for communication over short ranges.

2.The frequency of the infrared in the range from 300 GHz to 400 THz.

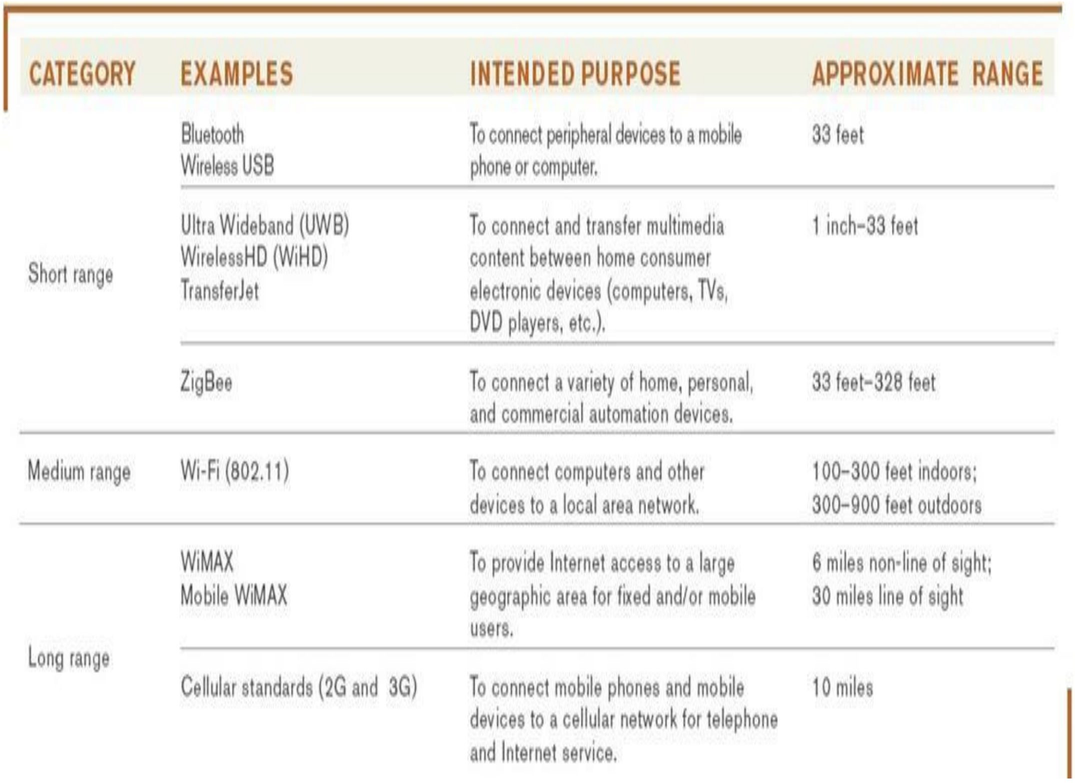
3.It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics of Infrared

1. It supports high bandwidth, and hence the data rate will be very high.
2. Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one

room cannot be interrupted by the nearby rooms.

3. Infrared communication provides better security with minimum interference.
4. Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.



CATEGORY	EXAMPLES	INTENDED PURPOSE	APPROXIMATE RANGE
Short range	Bluetooth Wireless USB	To connect peripheral devices to a mobile phone or computer.	33 feet
	Ultra Wideband (UWB) WirelessHD (WiHD) TransferJet	To connect and transfer multimedia content between home consumer electronic devices (computers, TVs, DVD players, etc.).	1 inch–33 feet
	ZigBee	To connect a variety of home, personal, and commercial automation devices.	33 feet–328 feet
Medium range	Wi-Fi (802.11)	To connect computers and other devices to a local area network.	100–300 feet indoors; 300–900 feet outdoors
Long range	WiMAX Mobile WiMAX	To provide Internet access to a large geographic area for fixed and/or mobile users.	6 miles non-line of sight; 30 miles line of sight
	Cellular standards (2G and 3G)	To connect mobile phones and mobile devices to a cellular network for telephone and Internet service.	10 miles

2.8 Switching, Modems and Multiplexing

2.8.1 Type of Connections or Switching

When multiple devices are connected then it is difficult to have a one-to-one connection between devices. The solution for this is to have different topologies which is costly and not affordable. Switching is one such solution which can be helpful in building in efficient networks.

These types of connections are of three types. They are 1. Circuit switched networks 2. Packet switched network 3. Broadcast network.

Circuit switched networks:

1. A network consists of a set of switches that are connected by the physical links commonly known as Circuit-Switched Network.
2. Whenever one device communicates with another device then a dedicated communication path is established between them over the network.
3. There is only a dedicated channel on each link used by each connection. Also, each link can be easily divided into n channels by using the TDM **or** FDM **technique.**
4. The Circuit Switching technique is mainly used in the public telephone Network **for**