Table of Contents

CHAPTER ONE

1. Data Communication and Computer Networking Basics

1.1 Introduction

Computer networks are the basis of communication in Computer Science and IT. They are used in a huge variety of ways and can include many different types of networks. A computer network is a set of computers that are connected together so that they can share information. The earliest examples of computer networks are from the 1960s, but they have come a long way in the half century since then.

A computer network comprises two or more computers that are connected either by cables (wired) or WiFi (wireless) with the purpose of transmitting, exchanging, or sharing data and resources. You build a computer network using hardware (e.g., routers, switches, access points, and cables) and software (e.g., operating systems or business applications).

Geographic location often defines a computer network. For example, a LAN (local area network) connects computers in a defined physical space, like an office building, whereas a WAN (widebarea network) can connect computers across continents. The internet is the largest example of WAN, connecting billions of computers worldwide.

You can further define a computer network by the protocols it uses to communicate, the physical arrangement of its components, how it controls traffic, and its purpose.

Computer networks enable communication for every business, entertainment, and research purpose. The internet, online search, email, audio and video sharing, online commerce, livestreaming, and social networks all exist because of computer networks.

1.1.1 History of Computer Networks

Computer networking as we know it today may be said to have gotten its start with the ARPANET development in the late 1960s and early 1970s. Prior to that time there were computer vendor" networks" designed primarily to connect terminals and remote job entry stations to a mainframe. But the notion of networking between computers viewing each other as equal peers to achieve "resource sharing" was fundamental to the ARPANET design [1]. The other strong emphasis of the ARPANET work was its reliance on the then novel technique of packet switching to efficiently share communication resources among" bursty" users, instead of the more traditional message or circuit switching. Although the term "network architecture" was not yet widely used, the initial ARPANET design did have a definite structure and introduced another key concept: protocol layering, or the idea that the total communications functions could be divided into several layers, each building upon the services of the one below. The original design had three major layers, a network layer, which included the network access and switch-to switch (IMP-to-IMP) protocols, a host-to-host layer (the Network Control Protocol or NCP), and

a “function-oriented protocol” layer, where specific applications such as file transfer, mail, speech, and remote terminal support were provided [2]. Similar ideas were being pursued in several other research projects around the world, including the Cyclades network in France [3], the National Physical Laboratory Network in England [4], and the Ethernet system [5] at Xerox PARC in the USA. Some of these projects focused more heavily on the potential for high-speed local networks such as the early 3-Mbps Ethernet. Satellite and radio channels for mobile users were also a topic of growing interest.

By 1973 it was clear to the networking vanguard that another protocol layer needed to be inserted into the protocol hierarchy to accommodate the interconnection of diverse types of individual networks.

The basis for the network interconnection approach developing in this community was to make use of a variety of individual networks each providing only a simple “best effort” or “datagram” transmission service. Reliable virtual circuit services would then be provided on an end-to-end basis with the TCP (or similar protocol) in the hosts. During the same time period, public data networks (PDNs) were emerging under the auspices of CCITT, aimed at providing more traditional virtual circuit types of network service via the newly defined X.25 protocol. The middle and late 1970s saw networking conferences dominated by heated debates over the relative merits of circuit versus packet switching and datagrams versus X.25 virtual circuits [8].

The computer vendors continued to offer their proprietary networks, gradually supporting the new X.25 service as links under their own protocols. Digital Equipment Corporation (DEC) was the notable exception, adopting the research community approach of peer-to-peer networking at an early date, and coming out with its own new suite of protocols (DECNET) [9]. By the late 1970s, a new major influence was emerging in the computer network community. The computer manufacturers realized that multivendor systems could no longer be avoided, and began to take action to satisfy the growing user demand for interoperability. Working through their traditional international body, the ISO, a new group (SC16) was created to develop standards in the networking area.

A computer network is a group of computers that has the potential to transmit, receive and exchange voice, data, and video traffic. A network connection can be set up with the help of either cable or wireless media. In modern times, computer networks are very important as information technology is increasing rapidly all over the world. The network and data communication are the essential factors to rise information technology in the world as technology’s advancement is on the system, including the gadgets. ARPANET began the networking long ago.

Review Questions

- What is computer network?
- What is Data communication means?

- Discus on History of Computer network?
- What is the Purpose of Computer network?

1.1.2 Network Basic Understanding

A system of interconnected computers and computerized peripherals such as printers is called computer network. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by either wired or wireless media.

Network Engineering: Networking engineering is a complicated task, which involves software, firmware, chip level engineering, hardware, and electric pulses. To ease network engineering, the whole networking concept is divided into multiple layers. Each layer is involved in some particular tasks and is independent of all other layers. But as a whole, almost all networking tasks depend on all of these layers. Layers share data between them and they depend on each other only to take input and send output.

Internet

A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet. The internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.

Internet enables its users to share and access enormous amount of information worldwide. It uses WWW, FTP, email services, audio and video streaming etc. At huge level, internet works on Client-Server model.

Internet uses very high-speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

1.1.3 Applications of Communication & Computer Network

Computer systems and peripherals are connected to form a network. They provide numerous advantages:

- Resource sharing such as printers and storage devices
- Exchange of information by means of e-Mails and FTP
- Information sharing by using Web or Internet
- Interaction with other users using dynamic web pages
- IP phones
- Video conferences
- Parallel computing
- Instant messaging

1.1.4 Characteristics of a Computer Network

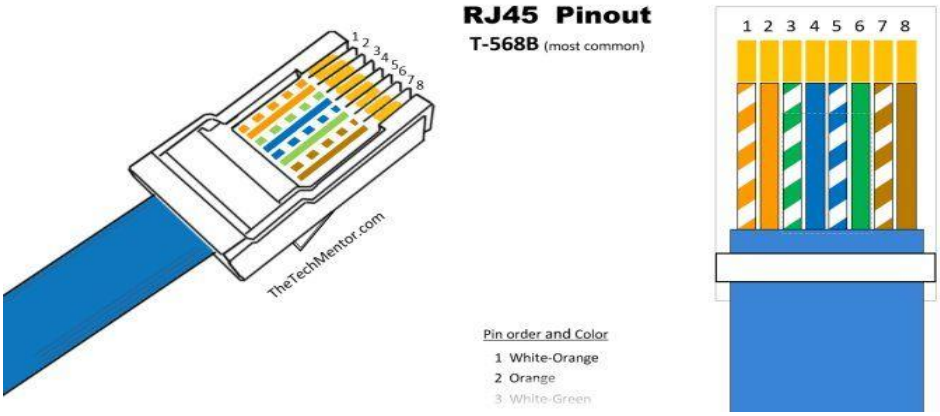
- ✓ Share resources from one computer to another.
- ✓ Create files and store them in one computer, access those files from the other computer(s) connected over the network.
- ✓ Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over the network.

Following is the list of hardware's required to set up a computer network.

- ✓ Network Cables
- ✓ Distributors
- ✓ Routers
- ✓ Internal Network Cards
- ✓ External Network Cards

A. Network Cables

Network cables are used to connect computers. The most commonly used cable is Category 5 cable RJ-45.



B. Distributors

A computer can be connected to another one via a serial port but if we need to connect many computers to produce a network, this serial connection will not work.

The solution is to use a central body to which other computers, printers, scanners, etc. can be connected and then this body will manage or distribute network traffic.

C. Router

A router is a type of device which acts as the central point among computers and other devices that are a part of the network. It is equipped with holes called ports. Computers and other devices

are connected to a router using network cables. Now-a-days router comes in wireless modes using which computers can be connected without any physical cable.

D. Network Card

Network card is a necessary component of a computer without which a computer cannot be connected over a network. It is also known as the network adapter or Network Interface Card (NIC). Most branded computers have network card pre-installed. Network cards are of two types: Internal and External Network Cards.

E. Internal Network Cards

Motherboard has a slot for internal network card where it is to be inserted. Internal network cards are of two types in which the first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA). Network cables are required to provide network access.

F. External Network Cards

External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard; however, no network cable is required to connect to the network.

G. Universal Serial Bus (USB)

USB card is easy to use and connects via USB port. Computers automatically detect USB card and can install the drivers required to support the USB network card automatically.

A system of interconnected computers and computerized peripherals such as printers is called computer network. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by either wired or wireless media.

1.1.5 Classification of Computer Networks

Computer networks are classified based on various factors. They include:

- ✓ Geographical span
- ✓ Inter-connectivity
- ✓ Administration
- ✓ Architecture

A. Geographical Span

Geographically a network can be seen in one of the following categories:

- ✓ It may be spanned across your table, among Bluetooth enabled devices, Ranging not more than few meters.

- ✓ It may be spanned across a whole building, including intermediate devices to connect all floors.
- ✓ It may be spanned across a whole city.
- ✓ It may be spanned across multiple cities or provinces.
- ✓ It may be one network covering whole world.

Personal Area Network

A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes.

For example, Piconet is Bluetooth-enabled Personal Area Network which may contain up to 8 devices connected together in a master-slave fashion.

Local Area Network

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization' offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million.

LAN provides a useful way of sharing the resources between end users. The resources such as printers; file servers, scanners, and internet are easily sharable among computers.

LANs are composed of inexpensive networking and routing equipment. It may contain local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally.

LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen. LAN can be wired, wireless, or in both forms at once.

Metropolitan Area Network

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).

Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.

Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.

Wide Area Network

As the name suggests, the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high-speed backbone, WANs use very expensive network equipment.

WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET). WAN may be managed by multiple administrations.

Internetwork

A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet. The internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.

Internet enables its users to share and access enormous amount of information worldwide. It uses WWW, FTP, email services, audio and video streaming etc. At huge level, internet works on Client-Server model.

Internet uses very high-speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page. The communication delay is very low.

Internet is serving many proposes and is involved in many aspects of life. Some of them are:

- ✓ Web sites
- ✓ E-mail
- ✓ Instant Messaging
- ✓ Blogging
- ✓ Social Media
- ✓ Marketing
- ✓ Networking
- ✓ Resource Sharing

- ✓ Audio and Video Streaming

B. Inter-Connectivity

Components of a network can be connected to each other differently in some fashion. By connectedness we mean either logically, physically, or both ways.

- ✓ Every single device can be connected to every other device on network, making the network mesh.
- ✓ All devices can be connected to a single medium but geographically disconnected, created bus like structure.
- ✓ Each device is connected to its left and right peers only, creating linear structure.
- ✓ All devices connected together with a single device, creating star like structure.
- ✓ All devices connected arbitrarily using all previous ways to connect each other, resulting in a hybrid structure.

C. Administration

From an administrator's point of view, a network can be private network which belongs a single autonomous system and cannot be accessed outside its physical or logical domain. A network can be public which is accessed by all.

D. Network Architecture

Computer networks can be discriminated into various types such as Client-Server, peer-to-peer or hybrid, depending upon its architecture.

- ✓ There can be one or more systems acting as Server. Other being Client, requests the Server to serve requests. Server takes and processes request on behalf of Clients.
- ✓ Two systems can be connected Point-to-Point, or in back-to-back fashion. They both reside at the same level and called peers.
- ✓ There can be hybrid network which involves network architecture of both the above types.

E. Network Applications

Computer systems and peripherals are connected to form a network. They provide numerous advantages:

- ✓ Resource sharing such as printers and storage devices
- ✓ Exchange of information by means of e-Mails and FTP
- ✓ Information sharing by using Web or Internet
- ✓ Interaction with other users using dynamic web pages
- ✓ IP phones
- ✓ Video conferences
- ✓ Parallel computing
- ✓ Instant messaging

Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the internet itself, covering the whole geographical world.

1.2 Data Communication

Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

Data communications and networking are changing the way we do business and the way we live. Business decisions have to be made ever more quickly, and the decision makers require immediate access to accurate information. Why wait a week for that report from Germany to arrive by mail when it could appear almost instantaneously through computer networks?

Businesses today rely on computer networks and internetworks. But before we ask how quickly we can get hooked up, we need to know how networks operate, what types of technologies are available, and which design best fills which set of needs.

The development of the personal computer brought about tremendous changes for Business, industry, science, and education. A similar revolution is occurring in data Communications and networking. Technological advances are making it possible for Communications links to carry more and faster signals. As a result, services are evolving to allow use of this expanded capacity. For example, established telephone services such as conference calling, call waiting, voice mail, and caller ID have been extended.

Research in data communications and networking has resulted in new technologies. One goal is to be able to exchange data such as text, audio, and video from all points in the world. We want to access the Internet to download and upload information quickly and accurately and at any time.

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term telecommunication, which includes telephony, telegraphy, and television, means communication at a distance (tele is Greek for “far”).

The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data

communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

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

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

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

Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

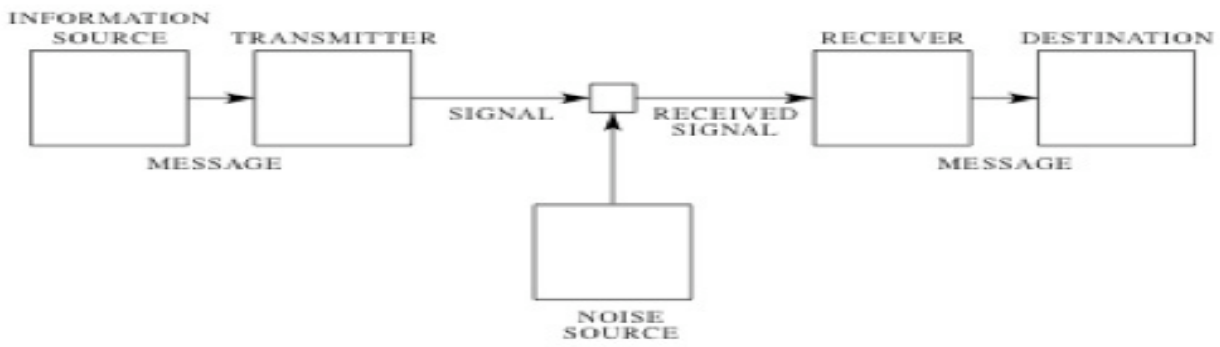
Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

1.2.1 Data Communications basics

Data Communications is the transfer of data or information between a source and a receiver. The source transmits the data and the receiver receives it. The actual generation of the information is not part of Data Communications nor is the resulting action of the information at the receiver.

Data Communication is interested in the transfer of data, the method of transfer and the preservation of the data during the transfer process.

The general Communication Model



- ✓ An information source, which produces a message.
- ✓ A transmitter, which encodes the message into signals
- ✓ A channel, to which signals are adapted for transmission
- ✓ A receiver, which 'decodes' (reconstructs) the message from the signal.
- ✓ A destination, where the message arrives.

Activity 2.1

- ➢ What is data transmission means and discuss in details
- ➢ Discuss on analog and digital signals
- ➢ How transmission impairment happens during data transmission?

1.2.2 Data Representation Technique

Data representation is defined as the methods used to represent information in computers. Different types of data can be stored in the computer system.

This includes numeric data, text, executable files, images, audio, video, etc. all these will look different to us as human.

1.2.2.1 Methods of Data Representation in Data Communication

1. Decimal Numbers
2. Binary Numbers
3. Hexadecimal Numbers
4. Text
5. Graphics

However, all types of information or data stored in the computer are represented as a sequence of 0s and 1s.

1. Decimal Numbers

As human we are used to writing numbers using digits 0 to 9. This is called base 10. This number system has been widely adopted, in large part because we have 10 fingers. However, other number systems still persist in modern society.

2. Binary Numbers

Any positive integer (whole number) can be represented by a sequence of 0s and 1s. Numbers in this form are said to be in base two, and are called binary numbers. Computers are based on the binary (base 2) number system because electrical wire can only be of two states (on or off).

3. Hexadecimal Numbers

Writing numbers in binary is tedious since this representation uses between 3 to 4 times as many digits as the decimal representation. The hexadecimal (base 16) number system is often used as

shorthand for binary. Base 16 is useful because 16 is a power of 2, and numbers have roughly as many digits as in the corresponding decimal representation.

Another name for hexadecimal numbers is alpha decimal because the numbers are written from 0 to 9 and A to F. where A is 10, B is 11 up to F that is 15.

4. **Text**

American Standard Code for Information Interchange (ASCII code) defines 128 different symbols. The symbols are all the characters found on a standard keyboard, plus a few extra. Unique numeric code (0 to 127) is assigned to each character. In ASCII, A is 65, B is 66, a is 97, b is 98, and so forth. When a file is saving as plain text, it is stored using ASCII.

ASCII format uses 1 byte per character 1 byte gives only 256 (128 standard and 128 non-standard) possible characters. The code value for any character can be converter to base 2, so any written message made up of ASCII characters can be converted to a string of 0s and 1s.

5. **Graphics**

Graphics on computer screen are consists of pixels. The pixels are tiny dots of color that collectively paint a graphic image on a computer screen. It is physical point in a raster image, or the smallest addressable element in an all-points addressable display device.

Hence it is the smallest controllable element of a picture represented on the screen. The address of a pixel corresponds to its physical coordinates.

LCD pixels are manufactured in two-dimensional grid, and are often represented using dots or squares, but CRT pixels correspond to their timing mechanism and sweep rates. The pixels are organized into many rows and columns on the screen.

1.2.3 Data Transmission formats

Data transmission is the process of sending digital or analog data over a communication medium to one or more computing, network, communication or electronic devices. It enables the transfer and communication of devices in a point-to-point, point-to-multipoint and multipoint-to multipoint environment.

Data transmission can be analog and digital but is mainly reserved for sending and receiving digital data. It works when a device or piece of equipment, such as a computer, intends to send a data object or file to one or multiple recipient devices, like a computer or server.

The digital data originates from the source device in the form of discrete signals or digital bit streams. These data streams/signals are placed over a communication medium, such as physical copper wires, wireless carriers and optical fiber, for delivery to the destination/recipient device. Moreover, each outward signal can be baseband or passband.

In addition to external communication, data transmission also may be internally carried to a device. For example, the random-access memory (RAM) or hard disk that sends data to a processor is also a form of data transmission.

1.2.4 Analog and Digital Transmission

A. Analog Transmission

Analog transmission is a method of conveying voice, data, image, signal, or video information. It uses a continuous signal varying in amplitude, phase, or another property that is in proportion to a specific characteristic of a variable.

An analog wave form (or signal) is characterized by being continuously variable along amplitude and frequency. In the case of telephony, for instance, when you speak into a handset, there are changes in the air pressure around your mouth. Those changes in air pressure fall onto the handset, where they are amplified and then converted into current, or voltage fluctuations. Those fluctuations in current are an analog of the actual voice pattern—hence the use of the term analog to describe these signals.

B. Digital Transmission

Data transmission (also known as digital transmission or digital communications) is a literal transfer of data over a point to point (or point to multipoint) transmission medium –such as copper wires, optical fibers, wireless communications media, or storage media. The data that is to be transferred is often represented as an electro-magnetic signal (such as a microwave).

Digital transmission transfers messages discretely. These messages are represented by a sequence of pulses via a line code. However, these messages can also be represented by a limited set of wave forms that always vary. Either way, they are represented using a digital modulation method.

Digital transmission is quite different from analog transmission. For one thing, the signal is much simpler. Rather than being a continuously variable wave form, it is a series of discrete pulses, representing one bit and zero bits. Each computer uses a coding scheme that defines what combinations of ones and zeros constitute all the characters in a character set (that is, lowercase letters, uppercase letters, punctuation marks, digits, keyboard control functions).

1.2.5 Transmission Impairments

The signal received may differ from the signal transmitted. The effect will degrade the signal quality for analog signals and introduce bit errors for digital signals. There are three types of transmission impairments: attenuation, delay distortion, and noise.

1. **Attenuation:** The impairment is caused by the strength of signals that degrades with distance over a transmission link. Three factors are related to the attenuation:

- ✓ The received signal should have sufficient strength to be intelligently interpreted by a receiver. An amplifier or a repeater is needed to boost the strength of the signal.
- ✓ A signal should be maintained at a level higher than the noise so that error will not be generated. Again, an amplifier or a repeater can be used.
- ✓ Attenuation is an increasing function of frequency, with more attenuation at higher frequency than at lower frequency. An equalizer can smooth out the effect of attenuation across frequency bands, and an amplifier can amplify high frequencies more than low frequencies.

2. **Delay distortion:** The velocity of propagation of a signal through a guided medium varies with frequencies; it is fast at the center of the frequency, but it falls off at the two edges of frequencies. Equalization techniques can be used to smooth out the delay distortion. Delay distortion is a major reason for the timing jitter problem, where the receiver clock deviates from the incoming signal in a random fashion so that an incoming signal might arrive earlier or late.
3. **Noise:** Impairment occurs when an unwanted signal is inserted between transmission and reception. There are four types of noises:
   - ✓ **Thermal noise:** This noise is a function of temperature and bandwidth. It cannot be eliminated. The thermal noise is proportional to the temperature and bandwidth as shown in the equation: thermal noise = K(constant) *temperature *bandwidth. Intermodulation noises this noise is caused by nonlinearity in the transmission system f 1; f2 frequencies could produce a signal at f1 + f2 or ABS (f1 – f2) and affect the frequencies at f1 + f2 or ABS (f1 – f2).
   - ✓ **Cross talk:** This type of noise is caused by electrical coupling in the nearby twisted pair or by unwanted signal picked by microwave antennas. For example, sometimes when you are on the telephone, you might hear someone else's conversation due to the cross-talk problem.
   - ✓ **Impulse noise:** Irregular pulses and short duration of relative high amplitude cause impulse noise. This noise is also caused by lightning and faults in the communication system. It is not an annoyance for analog data, but it is an annoyance for digital data. For example, 0.01 sec at 4800 bps causes 50 bits of distortion.

Activity 2.2

- ➢ Discuss and list some examples of half duplex transmission mode?
- ➢ Explain in details about parallel and serial data transmission mode?
- ➢ Discuss on the unguided transmission media using examples?
- ➢ Discus some common guided transmission medium with examples?

1.2.6 Data Transmission Mode

Data Transmission mode defines the direction of the flow of information between two communication devices. It is also called Data Communication or Directional Mode. It specifies the direction of the flow of information from one place to another in a computer network.

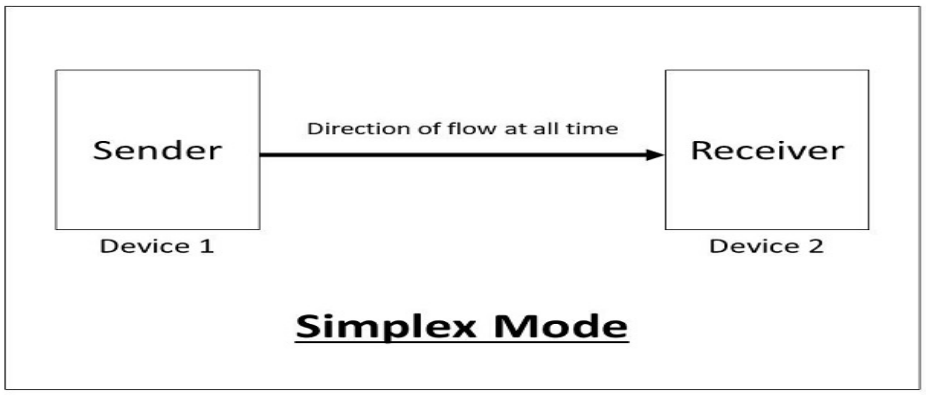
In the Open System Interconnection (OSI) Layer Model, the Physical Layer is dedicated to data transmission in the network. It mainly decides the direction of data in which the data needs to travel to reach the receiver system or node.

So, in this module, we will learn about different data transmission modes based on the direction of exchange, synchronization between the transmitter and receiver, and the number of bits sent simultaneously in a computer network.

According to the Direction of Exchange of Information:

1. **Simplex**

Simplex is the data transmission mode in which the data can flow only in one direction, i.e., the communication is unidirectional. In this mode, a sender can only send data but cannot receive it. Similarly, a receiver can only receive data but cannot send it.

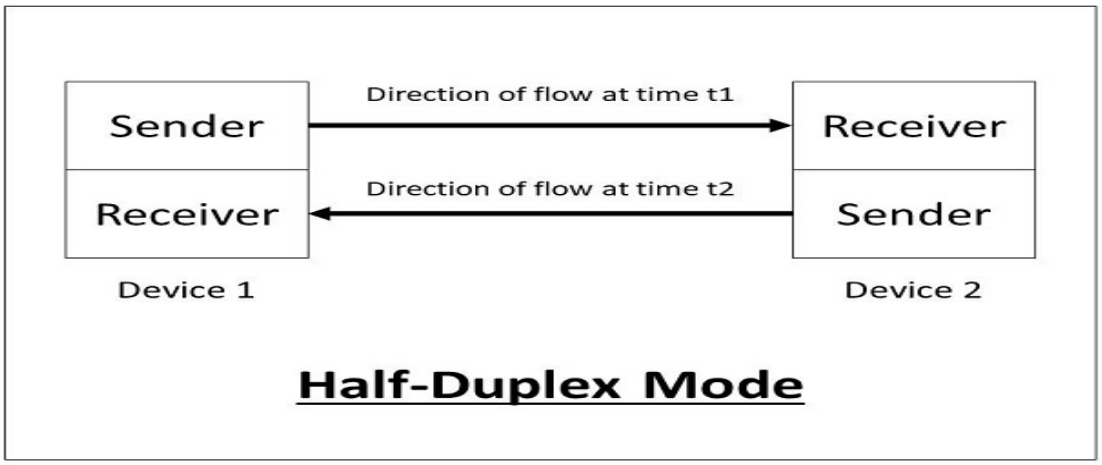


This transmission mode is not so popular because we cannot perform two-way communication between the sender and receiver in this mode. It is mainly used in the business field as in sales that do not require any corresponding reply. It is similar to a one-way street. For Example, Radio and TV transmission, keyboard, mouse, etc.

2. **Half-Duplex**

Half-Duplex is the data transmission mode in which the data can flow in both directions but in one direction at a time. It is also referred to as Semi-Duplex. In other words, each station can

both transmit and receive the data but not at the same time. When one device is sending the other can only receive and vice-versa.

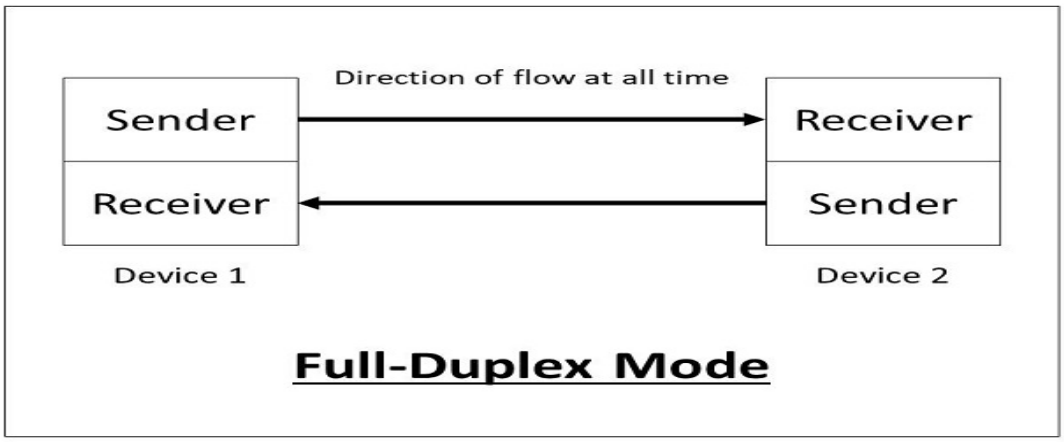


In this type of transmission mode, the entire capacity of the channel can be utilized for each direction. Transmission lines can carry data in both directions, but the data can be sent only in one direction at a time.

This type of data transmission mode can be used in cases where there is no need for communication in both directions at the same time. It can be used for error detection when the sender does not send or the receiver does not receive the data properly. In such cases, the data needs to be transmitted again by the receiver. For Example, Police radio, Internet Browsers, etc.

3. **Full-Duplex**

Full-Duplex is the data transmission mode in which the data can flow in both directions at the same time. It is bi-directional in nature. It is two-way communication in which both the stations can transmit and receive the data simultaneously.



Full-Duplex mode has double bandwidth as compared to the half-duplex. The capacity of the channel is divided between the two directions of communication. This mode is used when communication in both directions is required simultaneously. For Example, a Telephone Network, in which both the persons can talk and listen to each other simultaneously.

According to the synchronization between the transmitter and the receiver:

1. **Synchronous**

The Synchronous transmission mode is a mode of communication in which the bits are sent one after another without any start/stop bits or gaps between them. Actually, both the sender and receiver are paced by the same system clock. In this way, synchronization is achieved.

In a Synchronous mode of data transmission, bytes are transmitted as blocks in a continuous stream of bits. Since there is no start and stop bits in the message block. It is the responsibility of the receiver to group the bits correctly. The receiver counts the bits as they arrive and groups them in eight bits unit. The receiver continuously receives the information at the same rate that the transmitter has sent it. It also listens to the messages even if no bits are transmitted.

In synchronous mode, the bits are sent successively with no separation between each character, so it becomes necessary to insert some synchronization elements with the message, this is called “Character-Level Synchronization”.

For Example, if there are two bytes of data, say (10001101, 11001011) then it will be transmitted in the synchronous mode as follows:

For Example, communication in CPU and RAM

2. **Asynchronous**

The Asynchronous transmission mode is a mode of communication in which a start and the stop bit is introduced in the message during transmission. The start and stop bits ensure that the data is transmitted correctly from the sender to the receiver.

Generally, the start bit is ‘0’ and the end bit is ‘1’. Asynchronous here means ‘asynchronous at the byte level’, but the bits are still synchronized. The time duration between each character is the same and synchronized.

In an asynchronous mode of communication, data bits can be sent at any point in time. The messages are sent at irregular intervals and only one data byte can be sent at a time. This type of transmission mode is best suited for short-distance data transfer.

For Example, if there are two bytes of data, say (10001101, 11001011) then it will be transmitted in the asynchronous mode as follows:

For Example, Data input from a keyboard to the computer.

According to the number of bits sent simultaneously in the network:

1. **Serial**

The Serial data transmission mode is a mode in which the data bits are sent serially one after the other at a time over the transmission channel.

It needs a single transmission line for communication. The data bits are received in synchronization with one another. So, there is a challenge of synchronizing the transmitter and receiver.

In serial data transmission, the system takes several clock cycles to transmit the data stream. In this mode, the data integrity is maintained, as it transmits the data bits in a specific order, one after the other.

This type of transmission mode is best suited for long-distance data transfer, or the amount of data being sent is relatively small.

For Example, Data transmission between two computers using serial ports.

2. **Parallel**

The Parallel data transmission mode is a mode in which the data bits are sent parallelly at a time. In other words, there is a transmission of n-bits at the same time simultaneously.

Multiple transmission lines are used in such modes of transmission. So, multiple data bytes can be transmitted in a single system clock. This mode of transmission is used when a large amount of data has to be sent in a shorter duration of time. It is mostly used for short-distance communication.

For n-bits, we need n-transmission lines. So, the complexity of the network increases but the transmission speed is high. If two or more transmission lines are too close to each other, then there may be a chance of interference in the data, degrading the signal quality.

For Example, Data transmission between computer and printer.

Hence, after learning the various transmission modes, we can conclude that some points need to be considered when selecting a data transmission mode:

- ✓ Transmission Rate.
- ✓ The Distance that it covers.
- ✓ Cost and Ease of Installation.
- ✓ The resistance of environmental conditions.

This is all about the various transmission modes in a computer network.

1.2.7 Elements of Data Communication

For occurrence of data communication, communicating devices must be a part of communication system made up of a combination of hardware or software devices and programs.

Data Communication System Components:

There are mainly five components of a data communication system:

1. Message
2. Sender
3. Receiver
4. Transmission Medium
5. Set of rules (Protocol)

All above mentioned elements are described below:

Figure – Components of Data Communication System

1. **Message:**

This is most useful asset of a data communication system. The message simply refers to data or piece of information which is to be communicated. A message could be in any form, it may be in form of a text file, an audio file, a video file, etc.

2. **Sender:**

To transfer message from source to destination, someone must be there who will play role of a source. Sender plays part of a source in data communication system. It is simple a device that sends data message. The device could be in form of a computer, mobile, telephone, laptop, video camera, or a workstation, etc.

3. **Receiver:**

It is destination where finally message sent by source has arrived. It is a device that receives message. Same as sender, receiver can also be in form of a computer, telephone mobile, workstation, etc.

4. **Transmission Medium:**

In entire process of data communication, there must be something which could act as a bridge between sender and receiver, Transmission medium plays that part. It is physical path by which data or message travels from sender to receiver. Transmission medium could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves, etc.

5. **Set of rules (Protocol):**

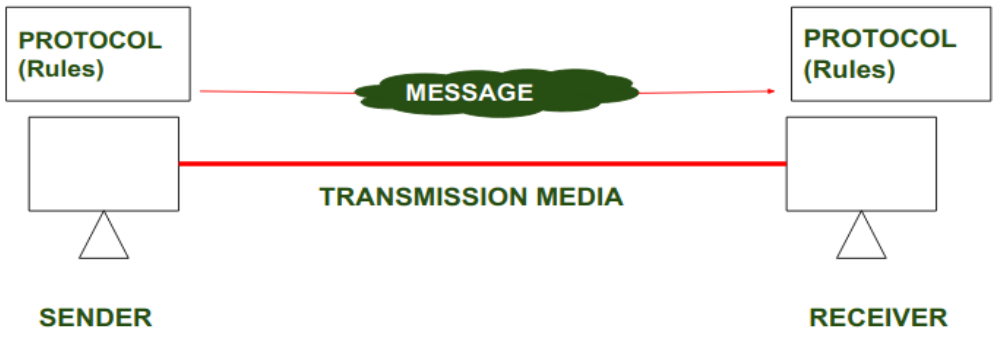
To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communicating devices. These are defined as protocol. In simple terms, the protocol is a set of rules that govern data communication. If two different devices are connected but there is no protocol among them, there would not be any kind of communication between those two devices. Thus, the protocol is necessary for data communication to take place.

A typical example of a data communication system is sending an e-mail. The user which sends email act as sender, message is data which user wants to send, receiver is one whom user wants to send message, there are many protocols involved in this entire process, one of them is Simple Mail Transfer Protocol (SMTP), both sender and receiver must have an internet connection which uses a wireless medium to send and receive email.

1.3 Protocol and Standard in Computer Networks

Protocol

In Order to make communication successful between devices, some rules and procedures should be agreed upon at the sending and receiving ends of the system. Such rules and procedures are called as Protocols. Different types of protocols are used for different types of communication.



In above diagrams Protocols are shown as set of rules. Such that Communication between Sender and Receiver is not possible without Protocol.

Standards

Standards are the set of rules for data communication that are needed for exchange of information among devices. It is important to follow Standards which are created by various Standard Organization like IEEE, ISO, ANSI etc.

Types of Standards:

Standards are of two types:

1. De Facto Standard.
2. De Jure Standard.

De Facto Standard: The meaning of the work" De Facto" is" By Fact" or "By Convention".

These are the standard s that have not been approved by any Organization, but have been adopted as Standards because of its widespread use. Also, sometimes these standards are often established by Manufacturers.

For example: Apple and Google are two companies which established their own rules on their products which are different. Also, they use some same standard rules for manufacturing for their products.

De Jure Standard: The meaning of the word "De Jure" is "By Law" or "By Regulations". Thus, these are the standards that have been approved by officially recognized body like ANSI, ISO, IEEE etc. These are the standard which are important to follow if it is required or needed.

For example: All the data communication standard protocols like SMTP, TCP, IP, UDP etc. are important to follow the same when we needed them.

1.4 Circuit Switching and Packet Switching

1.4.1 What is Circuit Switching?

Circuit switching is a communication method where a dedicated communication path, or circuit, is established between two devices before data transmission begins. The circuit remains dedicated to the communication for the duration of the session, and no other devices can use it while the session is in progress. Circuit switching is commonly used in voice communication and some types of data communication.

Advantages of Circuit Switching:

- ✓ **Guaranteed bandwidth:** Circuit switching provides a dedicated path for communication, ensuring that bandwidth is guaranteed for the duration of the call.
- ✓ **Low latency:** Circuit switching provides low latency because the path is predetermined, and there is no need to establish a connection for each packet.
- ✓ **Predictable performance:** Circuit switching provides predictable performance because the bandwidth is reserved, and there is no competition for resources.
- ✓ **Suitable for real-time communication:** Circuit switching is suitable for real-time communication, such as voice and video, because it provides low latency and predictable performance.

Disadvantages of Circuit Switching:

- ✓ **Inefficient use of bandwidth:** Circuit switching is inefficient because the bandwidth is reserved for the entire duration of the call, even when no data is being transmitted.
- ✓ **Limited scalability:** Circuit switching is limited in its scalability because the number of circuits that can be established is finite, which can limit the number of simultaneous calls that can be made.
- ✓ **High cost:** Circuit switching is expensive because it requires dedicated resources, such as hardware and bandwidth, for the duration of the call.

1.4.2 What is Packet Switching?

Packet switching is a communication method where data is divided into smaller units called packets and transmitted over the network. Each packet contains the source and destination addresses, as well as other information needed for routing. The packets may take different paths to reach their destination, and they may be transmitted out of order or delayed due to network congestion.

Advantages of Packet Switching:

- ✓ **Efficient use of bandwidth:** Packet switching is efficient because bandwidth is shared among multiple users, and resources are allocated only when data needs to be transmitted.
- ✓ **Flexible:** Packet switching is flexible and can handle a wide range of data rates and packet sizes.
- ✓ **Scalable:** Packet switching is highly scalable and can handle large amounts of traffic on a network.
- ✓ **Lower cost:** Packet switching is less expensive than circuit switching because resources are shared among multiple users.

Disadvantages of Packet Switching:

- ✓ **Higher latency:** Packet switching has higher latency than circuit switching because packets must be routed through multiple nodes, which can cause delay.
- ✓ **Limited QoS:** Packet switching provides limited QoS guarantees, meaning that different types of traffic may be treated equally.
- ✓ **Packet loss:** Packet switching can result in packet loss due to congestion on the network or errors in transmission.
- ✓ **Unsuitable for real-time communication:** Packet switching is not suitable for real-time communication, such as voice and video, because of the potential for latency and packet loss.

Similarities:

- ✓ Both methods involve the transmission of data over a network.
- ✓ Both methods use a physical layer of the OSI model for transmission of data.
- ✓ Both methods can be used to transmit voice, video, and data.
- ✓ Both methods can be used in the same network infrastructure.
- ✓ Both methods can be used for both wired and wireless networks.

Difference between Circuit Switching and Packet Switching:

Circuit Switching	**Packet Switching**
In-circuit switching has there are 3 phases: i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place.
In-circuit switching, each data unit knows the entire	In Packet switching, each data unit

Circuit Switching	Packet Switching
path address which is provided by the source.	just knows the final destination address intermediate path is decided by the routers.
In-Circuit switching, data is processed at the source system only	In Packet switching, data is processed at all intermediate nodes including the source system.
The delay between data units in circuit switching is uniform.	The delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because the path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources is more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source.	Transmission of the data is done not only by the source but also by the intermediate routers.
Congestion can occur during the connection establishment phase because there might be a case where a request is being made for a channel but the channel is already occupied.	Congestion can occur during the data transfer phase, a large number of packets comes in no time.
Circuit switching is not convenient for handling bilateral traffic.	Packet switching is suitable for handling bilateral traffic.

Circuit Switching	Packet Switching
In-Circuit switching, the charge depends on time and distance, not on traffic in the network.	In Packet switching, the charge is based on the number of bytes and connection time.
Recording of packets is never possible in circuit switching.	Recording of packets is possible in packet switching.
In-Circuit Switching there is a physical path between the source and the destination	In Packet Switching there is no physical path between the source and the destination
Circuit Switching does not support store and forward transmission	Packet Switching supports store and forward transmission
Call setup is required in circuit switching.	No call setup is required in packet switching.
In-circuit switching each packet follows the same route.	In packet switching packets can follow any route.
The circuit switching network is implemented at the physical layer.	Packet switching is implemented at the datalink layer and network layer
Circuit switching requires simple protocols for delivery.	Packet switching requires complex protocols for delivery.

Conclusion:

In conclusion, circuit switching and packet switching are two different methods used in communication networks to transfer data between two or more devices. Circuit switching establishes a dedicated communication path before data transmission begins, while packet switching divides the data into smaller units called packets and transmits them over the network. Understanding the differences between the two methods can help you choose the right network technology for your specific needs.

1.5 Computer Network

Network is a system of interconnected computers and computerized peripherals such as printers is called computer network. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by either wired or wireless media.

Computer network is a computer network is a system in which a number of independent computers are linked together to share data and peripherals, such as files and printers. In the modern world, computer networks have become almost indispensable. All major businesses and governmental and educational institutions make use of computer networks to such an extent that it is now difficult to imagine a world without them.

1.5.1 Computer Network and its Applications

Computer systems and peripherals are connected to form a network. They provide numerous advantages:

- Resource sharing such as printers and storage devices
- Exchange of information by means of e-Mails and FTP
- Information sharing by using Web or Internet
- Interaction with other users using dynamic web pages
- IP phones
- Video conferences
- Parallel computing
- Instant messaging

1.5.2 Types of Computer Network

Computer networks are classified based on various factors. They include:

- Geographical span
- Inter-connectivity
- Administration
- Architecture

A. Geographical Span

Geographically a network can be seen in one of the following categories:

- It may be spanned across your table, among Bluetooth enabled devices, Ranging not more than few meters.
- It may be spanned across a whole building, including intermediate devices to connect all floors.
- It may be spanned across a whole city.
- It may be spanned across multiple cities or provinces.
- It may be one network covering whole world.

B. Interconnectivity

Components of a network can be connected to each other differently in some fashion. By connectedness we mean either logically, physically, or both ways.

- Every single device can be connected to every other device on network, making the network mesh.
- All devices can be connected to a single medium but geographically disconnected, created bus-like structure.
- Each device is connected to its left and right peers only, creating linear structure.
- All devices connected together with a single device, creating star-like structure.
- All devices connected arbitrarily using all previous ways to connect each other, resulting in a hybrid structure.

C. Administration

From an administrator's point of view, a network can be private network which belongs a single autonomous system and cannot be accessed outside its physical or logical domain. A network can be public, which is accessed by all.

D. Network Architecture

Computer networks can be discriminated into various types such as Client-Server, peer-to-peer or hybrid, depending upon its architecture.

- here can be one or more systems acting as Server. Other being Client, requests the Server to serve requests. Server takes and processes request on behalf of Clients.
- Two systems can be connected Point-to-Point, or in back-to-back fashion. They both reside at the same level and called peers.
- There can be hybrid network which involves network architecture of both the above types.

Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the internet itself, covering the whole geographical world.

1. Personal Area Network

A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers, and TV remotes.

2. Local Area Network

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million.

LAN provides a useful way of sharing the resources between end users. The resources such as printers, file servers, scanners, and internet are easily sharable among computers.

LANs are composed of inexpensive networking and routing equipment. It may contain local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally.

LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen. LAN can be wired, wireless, or in both forms at once.

3. Metropolitan Area Network

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).

Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.

Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.

4. Wide Area Network

As the name suggests, the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high-speed backbone, WANs use very expensive network equipment.

WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET). WAN may be managed by multiple administration.

5. Internetwork

A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet. The internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.

Internet enables its users to share and access enormous amount of information worldwide. It uses WWW, FTP, email services, audio, and video streaming etc. At huge level, internet works on Client-Server model.

Internet uses very high-speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable. Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page. The communication delay is very low.

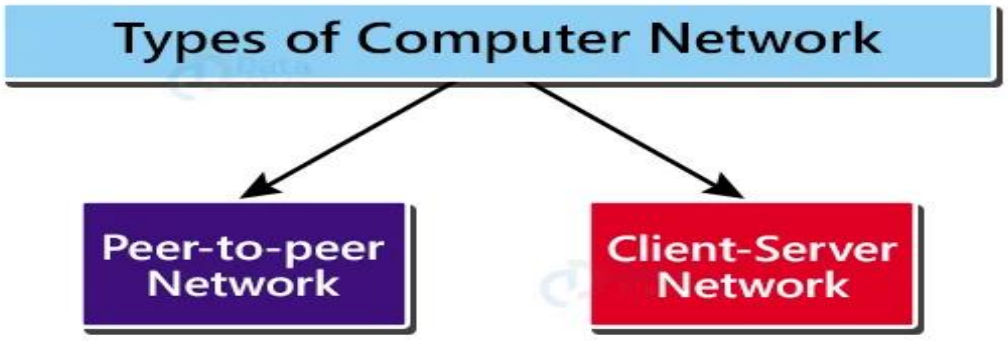
Internet is serving many proposes and is involved in many aspects of life. Some of them are:

- Web sites
- E-mail
- Instant Messaging
- Blogging
- Social Media
- Marketing
- Networking
- Resource Sharing
- Audio and Video Streaming

1.5.3 Network Architecture

The design and setup of a computer network is called Computer Network Architecture. It is the organization and arrangement of different network devices (i.e., the clients such as PCs, desktops, laptops, mobiles etc.) at both physical and logical levels in order to fulfil the needs of the end user/customer.

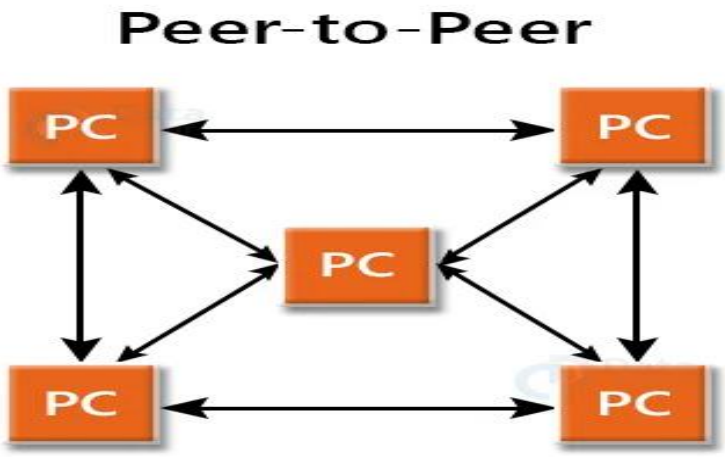
The two most well-known Computer Network Architectures are:



- Peer-to-peer Architecture
- Client-Server Architecture

Here is a brief, detailed look at each of the above-mentioned prominent architectures:

1. **Peer-to-Peer Architecture**



- The peers referred to here are the individual devices linked together directly, having equal responsibilities and equal powers without the presence of any central authority.
- Due to the absence of a central device in charge of tasks, this architecture is also known as decentralized architecture.
- Each computer has special rights for resource sharing; however, this might cause issues if the computer with the resource is unavailable.
- Useful in smaller environments with a smaller number of computers.

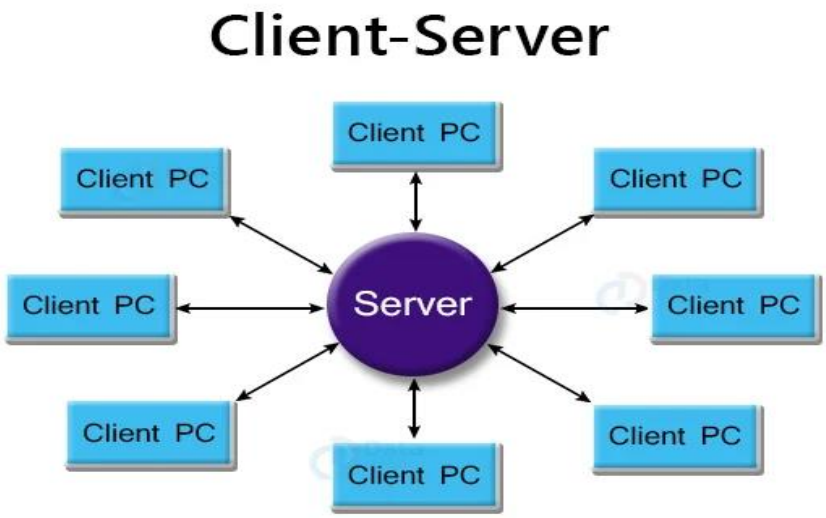
Advantages of Peer-to-Peer Network:

- ✓ No particular device is a client or a server, the tasks and responsibilities of servers are distributed among all the devices, which also act as clients.
- ✓ Very inexpensive to set up, as there is no requirement of a centralized server, and this also ensures that in case of any failure in the network, all unaffected devices continue to operate normally.
- ✓ It's simple to set up and maintain because each computer runs independently.

Disadvantages of Peer-to-Peer Network:

- ✓ No centralized system, thus difficult to keep a backup of the data in case of any fault.
- ✓ It has a security flaw because the computers are self-managed.
- ✓ With a growth in the number of machines on this network, performance, security, and access may all become big issues.

2. **Client-server Architecture**



- This is also known as centralized architecture, as one powerful central computer is in charge of serving all the requests from the client computers. This central computer is a server.
- The client computers connect to the server as and when they require the use of shared resources or shared data. All of the shared data is stored solely in the server, and not on any other computer.
- A server handles all of the key tasks, such as security and network administration.
- All of the clients interact with one another via a server.

Advantages of Client-Server Architecture:

- ✓ This type of architecture is much easier to scale since it is much more convenient to add more server computers than configure the network on each and every computer (as is the case in peer-to-peer architecture).
- ✓ Much faster network speeds.
- ✓ Because a single server manages the shared resources in a Client/Server network, there is improvement in security.
- ✓ Backing up data is easy because of the centralized system.
- ✓ The server provides a customized Network Operating System (NOS) to offer resources to a large number of users that want them.

Disadvantages of Client-Server Architecture:

- ✓ More prone to downtime because if the server fails, none of the client machines are able to get their requests served.
- ✓ Requirement of a dedicated network administrator to handle all of the resources.

- ✓ It is far more expensive than P2P. This is due to the requirement for a server with more RAM, as well as the necessity for several networking devices such as hubs, routers, switches, and so on.

There are some lesser-known computer architectures:

3. Centralized Computing Architecture

One powerful computer is utilized to service one or more low-powered computers in centralized computing architecture. The nodes under the centralized architecture are not linked; they are only connected to the server.

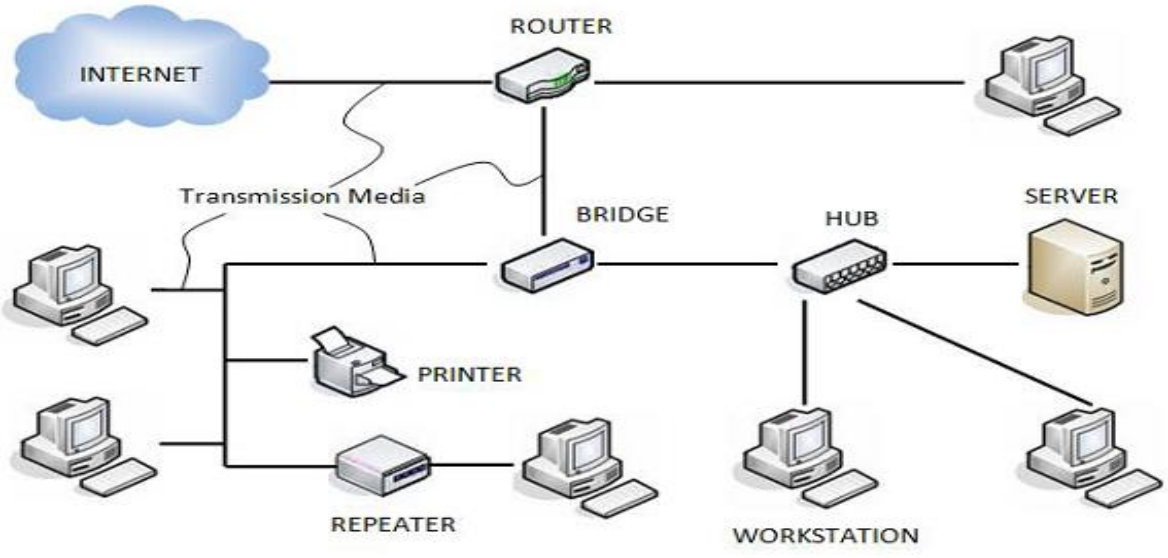
4. Distributed Computing Architecture

A distributed architecture connects one or more nodes, which are personal computers. It supports a variety of functions, including file sharing, hardware sharing, and network sharing. The nodes in the distributed architecture can manage their own data and rely on the network for administration rather than data processing.

1.5.4 Computer Network Components

Computer networks components comprise both physical parts as well as the software required for installing computer networks, both at organizations and at home. The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols.

The following figure shows a network along with its components:



COMPUTER NETWORK COMPONENTS

1.5.4.1 Hardware Components

Servers-Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.

Clients-Clients are computers that request and receive service from the servers to access and use the network resources.

Peers -Peers are computers that provide as well as receive services from other peers in a workgroup network.

Transmission Media − Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fiber optic cables etc.; or maybe unguided media like microwaves, infra-red waves etc.

Connecting Devices − Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:

- ✓ Routers
- ✓ Bridges
- ✓ Hubs
- ✓ Repeaters
- ✓ Gateways
- ✓ Switches

1.5.4.2 Software Components

Networking Operating System − Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.

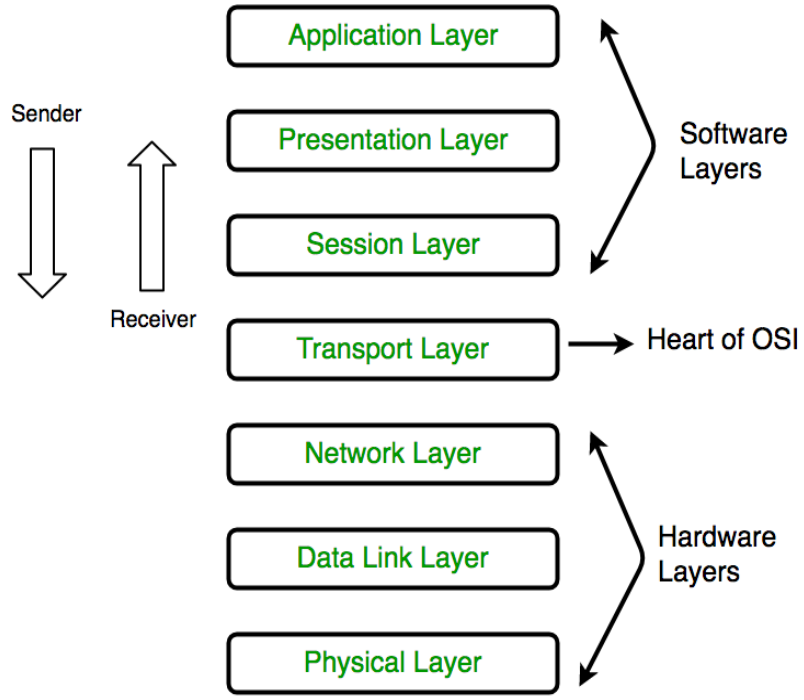
Protocol Suite − A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are −

1. **OSI Model (Open System Interconnections)**

The OSI Model is a logical and conceptual model that defines network communication used by systems open to interconnection and communication with other systems. The Open System Interconnection (OSI Model) also defines a logical network and effectively describes computer packet transfer by using various layers of protocols.

Open System Interconnect is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO). The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and

interoperable. The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. This model has seven layers:



- **Application Layer:** This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact with the user.
- **Presentation Layer:** This layer defines how data in the native format of remote host should be presented in the native format of host.
- **Session Layer:** This layer maintains sessions between remote hosts. For example, once user/password authentication is done, the remote host maintains this session for a while and does not ask for authentication again in that time span.
- **Transport Layer:** This layer is responsible for end-to-end delivery between hosts.
- **Network Layer:** This layer is responsible for address assignment and uniquely addressing hosts in a network.
- **Data Link Layer:** This layer is responsible for reading and writing data from and onto the line. Link errors are detected at this layer.
- **Physical Layer:** This layer defines the hardware, cabling, wiring, power output, pulse rate etc.

2. TCP / IP Model

The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is

equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCPIIP taking care of part of the duties of the session layer. So, in this book, we assume that the TCPIIP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the *application layer*.

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent.

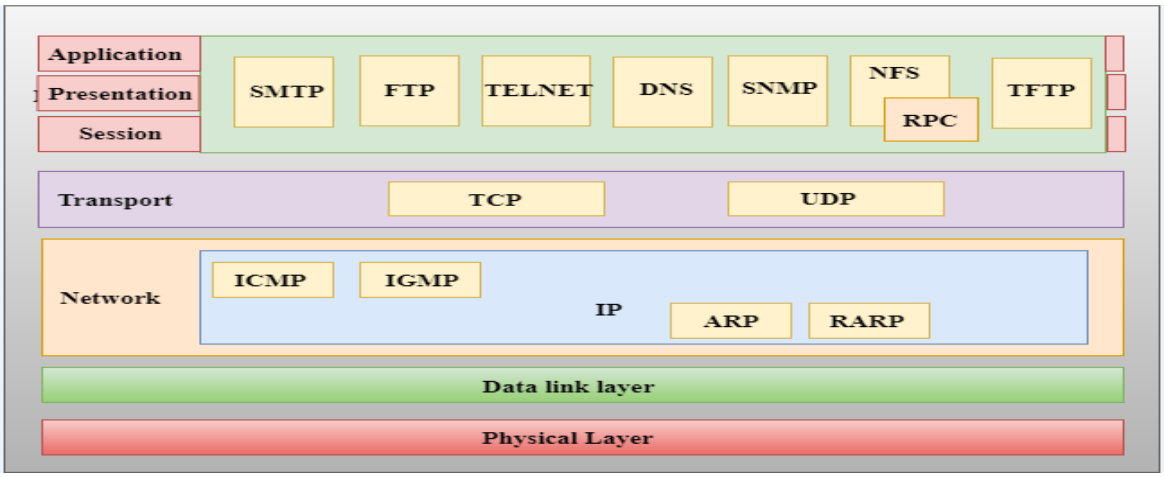
Whereas the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. The term hierarchical means that each upper-level protocol is supported by one or more lower-level protocols.

At the transport layer, TCP/IP defines three protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.

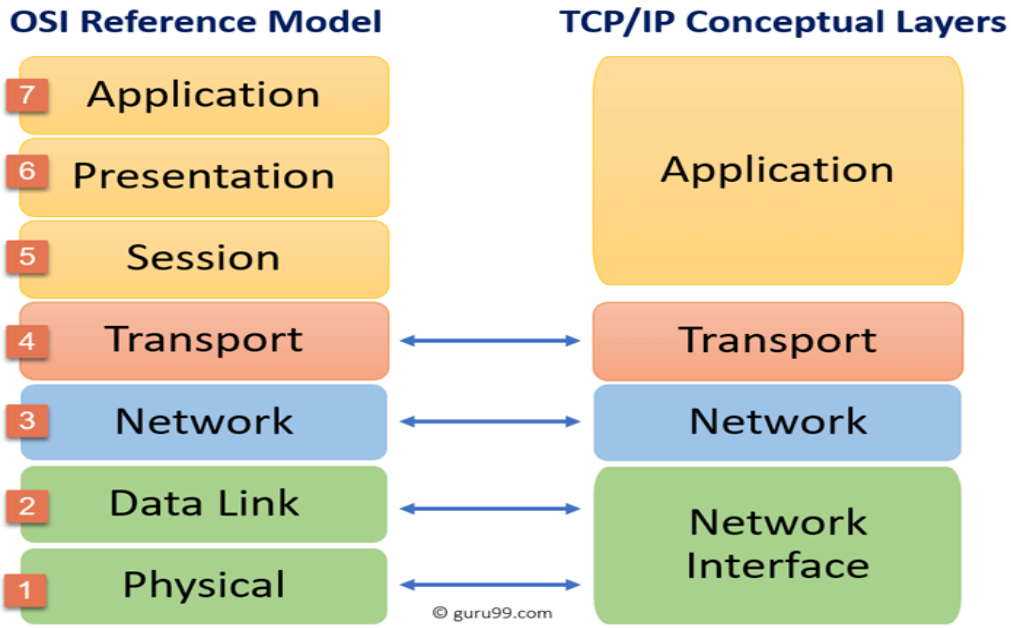
The functionality of the TCP IP model is divided into four layers, and each includes specific protocols.

TCP/IP is a layered server architecture system in which each layer is defined according to a specific function to perform. All these four TCP IP layers work collaboratively to transmit the data from one layer to another.

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Network Interface



Differences between OSI and TCP/IP models



Here, are some important differences between the OSI and TCP/IP model:

FUNCTION	TCP/IP MODEL	OSI MODEL
Definition	TCP/IP stands for Transmission control protocol/ Internet protocol	OSI stands for Open systems Interconnection
Developed by	It is developed by DOD (Department of Defence) project agency.	OSI model is developed by ISO (International standard organization).
Technology/ Platform	It comprises of a set of standard protocols which lead to development of the Internet. It is a communication medium which provides connection between hosts.	It is an independent standard and generic protocol used as a communication gateway between network and end user.
Features	▪ No guaranteed delivery of packets at transport layer. ▪ Based on horizontal approach. ▪ Session and presentation layers are not separate, both are included in application layer. ▪ Implemented model of OSI model. ▪ Network layer provides only connectionless service. ▪ Protocols can't be easily replaceable ▪ Comprises of four layers ▪ Services, protocols, and interfaces are not properly segregated but are protocol dependent ▪ Widely used model ▪ Not provide standardization of devices	▪ Transport layer provides guaranteed delivery of packets. ▪ Based on vertical approach. ▪ Session and presentation layers are separate ▪ It is a reference model on which various networks are built. ▪ Network layer provides connection oriented and connection less services (Both) ▪ In OSI model protocols are hidden and can be easily replaceable when technology changes occur ▪ It comprises of seven layers ▪ Services, protocols and interfaces are defined and it is protocol independent ▪ Limited usage of the model ▪ Standardization of devices like router, switches, load balancers and other hardware devices
networkinterview.com (An Initiative By ipwithease.com)		

1.5.5 Computer Network Topologies

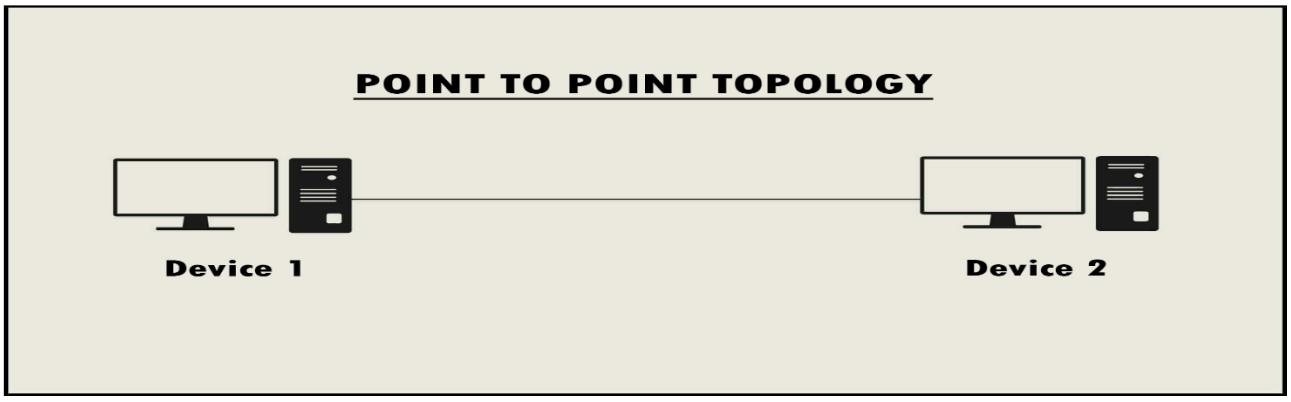
A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

The way a network is arranged can make or break network functionality, connectivity, and protection from downtime. The question of, "What is network topology?" can be answered with an explanation of the two categories in the network topology.

1. **Physical –** The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged. Setup, maintenance, and provisioning tasks require insight into the physical network.
2. **Logical –** The logical network topology is a higher-level idea of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network. Logical network topology includes any virtual and cloud resources. Effective network management and monitoring require a strong grasp of both the physical and logical topology of a network to ensure your network is efficient and healthy.

1.5.5.1 Point-to-Point

Point-to-point networks contains exactly two hosts such as computer, switches, routers, or servers connected back-to-back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice versa.

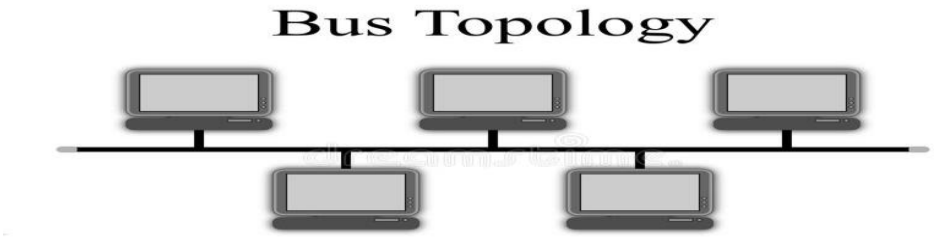


If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

1.5.5.2 Bus Topology

In case of Bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.



Advantages of Bus Topology

Bus topologies are a good, cost-effective choice for smaller networks because the layout is simple, allowing all devices to be connected via a single coaxial or RJ45 cable. If needed, more nodes can be easily added to the network by joining additional cables.

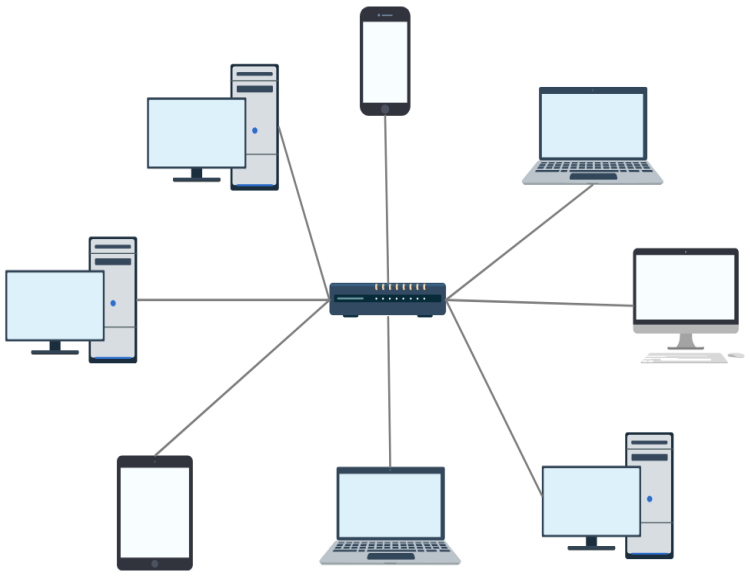
Disadvantages of Bus Topology

However, because bus topologies use a single cable to transmit data, they're somewhat vulnerable. If the cable experiences a failure, the whole network goes down, this can be time-consuming and expensive to restore, which can be less of an issue with smaller networks.

Bus topologies are best suited for small networks because there's only so much bandwidth, and every additional node will slow transmission speeds.

1.5.5.3 Star Topology

A star topology, the most common network topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable. Acting as a server, this central node manages data transmission—as information sent from any node on the network has to pass through the central one to reach its destination—and functions as a repeater, which helps prevent data loss.



Advantages of Star Topology

Star topologies are common since they allow you to conveniently manage your entire network from a single location. Because each of the nodes is independently connected to the central hub, should one go down, the rest of the network will continue functioning unaffected, making the star topology a stable and secure network layout?

Additionally, devices can be added, removed, and modified without taking the entire network offline.

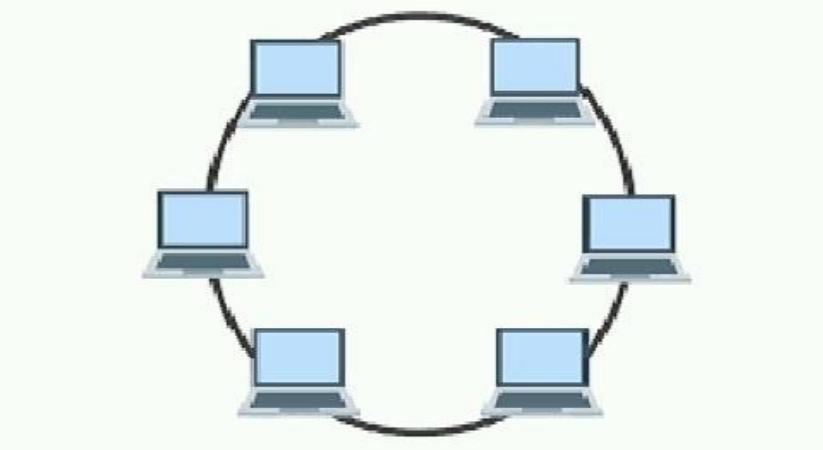
Disadvantages of Star Topology

On the flipside, if the central hub goes down, the rest of the network can't function. But if the central hub is properly managed and kept in good health, administrators shouldn't have too many issues.

The overall bandwidth and performance of the network are also limited by the central node's configurations and technical specifications, making star topologies expensive to set up and operate.

1.5.5.4 Ring Topology

Ring topology is where nodes are arranged in a circle (or ring). The data can travel through the ring network in either one direction or both directions, with each device having exactly two neighbors.



Advantage of Ring Topology

Since each device is only connected to the ones on either side, when data is transmitted, the packets also travel along the circle, moving through each of the intermediate nodes until they arrive at their destination. If a large network is arranged in a ring topology, repeaters can be used to ensure packets arrive correctly and without data loss.

Only one station on the network is permitted to send data at a time, which greatly reduces the risk of packet collisions, making ring topologies efficient at transmitting data without errors.

By and large, ring topologies are cost-effective and inexpensive to install, and the intricate point to point connectivity of the nodes makes it relatively easy to identify issues or misconfigurations on the network.

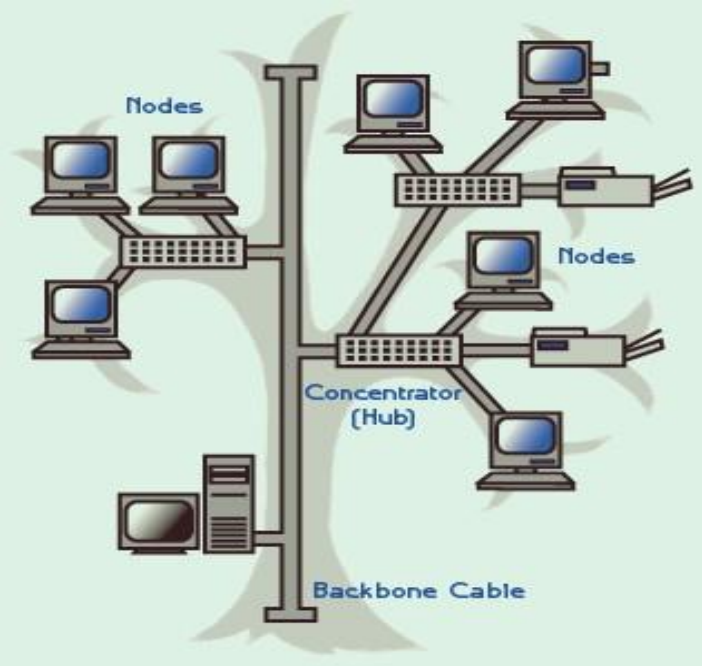
Disadvantage of Ring Topology

Even though it's popular, a ring topology is still vulnerable to failure without proper network management. Since the flow of data transmission moves unidirectional between nodes along each ring, if one node goes down, it can take the entire network with it. That's why it's imperative for each of the nodes to be monitored and kept in good health. Nevertheless, even if you're vigilant and attentive to node performance, your network can still be taken down by a transmission line failure.

Additionally, the entire network must be taken offline to reconfigure, add, or remove nodes. And while that's not the end of the world, scheduling downtime for the network can be inconvenient and costly.

1.5.5.5 Tree Topology

The tree topology structure gets its name from how the central node functions as a sort of trunk for the network, with nodes extending outward in a branch-like fashion. However, where each node in a star topology is directly connected to the central hub, a tree topology has a parent-child hierarchy to how the nodes are connected. Those connected to the central hub are connected linearly to other nodes, so two connected nodes only share one mutual connection. Because the tree topology structure is both extremely flexible and scalable, it's often used for wide area networks to support many spread-out devices.



Advantage of Tree Topology

Combining elements of the star and bus topologies allows for the easy addition of nodes and network expansion. Troubleshooting errors on the network is also a straightforward process, as each of the branches can be individually assessed for performance issues.

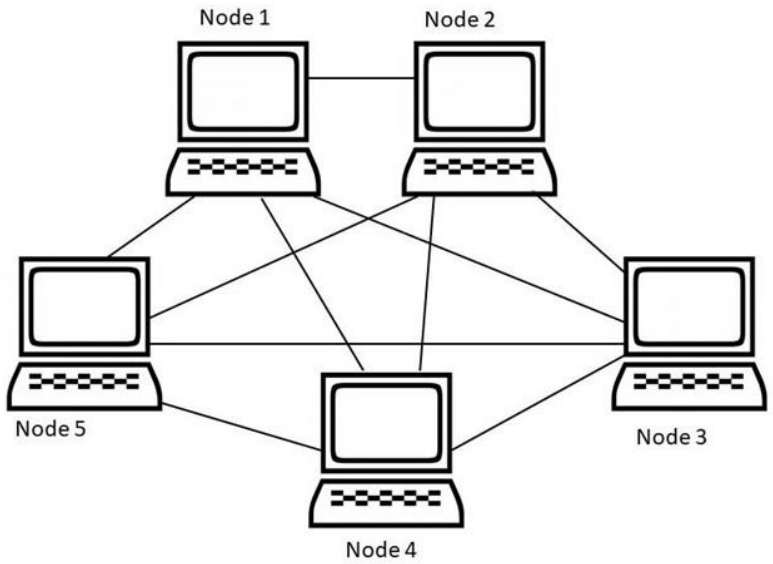
Disadvantage of Tree Topology

As with the star topology, the entire network depends on the health of the root node in a tree topology structure. Should the central hub fail, the various node branches will become disconnected, though connectivity within—but not between—branch systems will remain.

Because of the hierarchical complexity and linear structure of the network layout, adding more nodes to a tree topology can quickly make proper management an unwieldy, not to mention costly, experience. Tree topologies are expensive because of the sheer amount of cabling required to connect each device to the next within the hierarchical layout.

1.5.5.6 Mesh Topology

A mesh topology is an intricate and elaborate structure of point-to-point connections where the nodes are interconnected. Mesh networks can be full or partial mesh. Partial mesh topologies are mostly interconnected, with a few nodes with only two or three connections, while full-mesh topologies are surprise fully interconnected.



The web-like structure of mesh topologies offers two different methods of data transmission: routing and flooding. When data is routed, the nodes use logic to determine the shortest distance from the source to destination, and when data is flooded, the information is sent to all nodes within the network without the need for routing logic.

Advantages of Mesh Topology

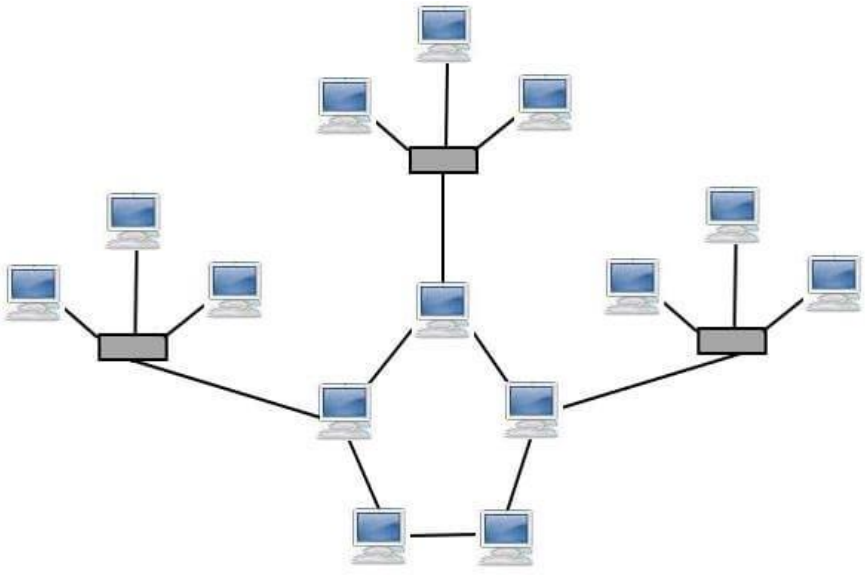
Mesh topologies are reliable and stable, and the complex degree of interconnectivity between nodes makes the network resistant to failure. For instance, no single device going down can bring the network offline.

Disadvantages of Mesh Topology

Mesh topologies are incredibly labor-intensive. Each interconnection between nodes requires a cable and configuration once deployed, so it can also be time-consuming to set up. As with other topology structures, the cost of cabling adds up fast, and to say mesh networks require a lot of cabling is an understatement.

1.5.5.7 Hybrid Topology

Hybrid topologies combine two or more different topology structures—the tree topology is a good example, integrating the bus and star layouts. Hybrid structures are most commonly found in larger companies where individual departments have personalized network topologies adapted to suit their needs and network usage.



Advantages of Hybrid Topology

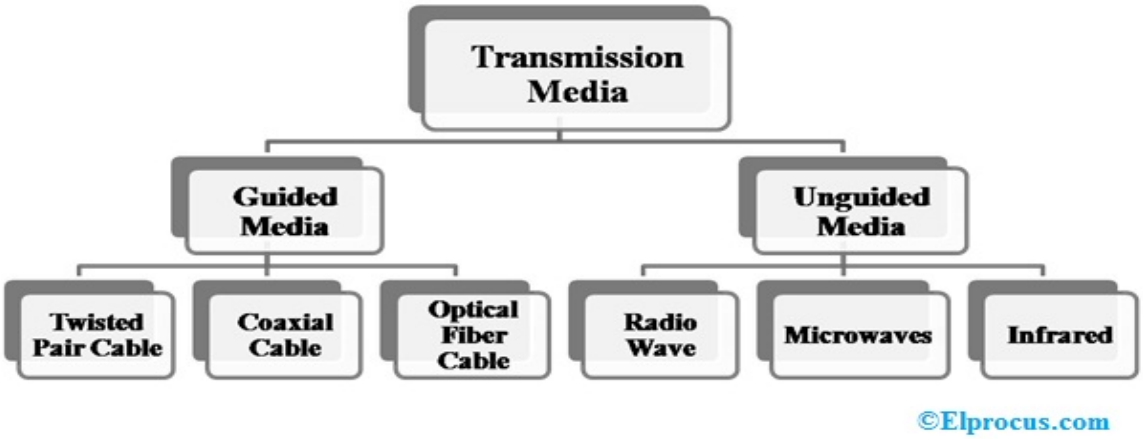
The main advantage of hybrid structures is the degree of flexibility they provide, as there are few limitations on the network structure itself that a hybrid setup can't accommodate.

Disadvantages of Hybrid Topology

However, each type of network topology comes with its own disadvantages, and as a network grows in complexity, so too does the experience and know-how required on the part of the admins to keep everything functioning optimally. There's also the monetary cost to consider when creating a hybrid network topology.

1.6 Transmission Media

Transmission media is broadly classified into two groups.



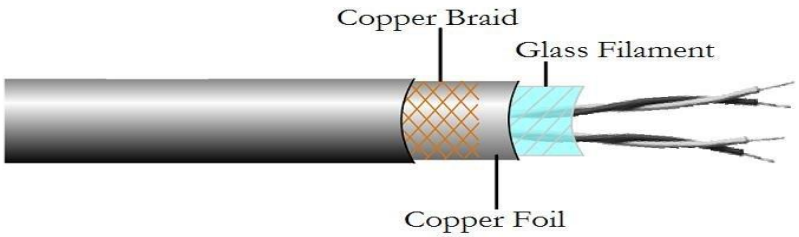
1.6.1 Guided Media

This kind of transmission media is also known as wired otherwise bounded media. In this type, the signals can be transmitted directly & restricted in a thin path through physical links. The main features of guided media mainly include secure, high-speed, and used in small distances. This kind of media is classified into three types which are discussed below.

1.6.1.1 Twisted Pair Cable

It includes two separately protected conductor wires. Normally, some pairs of cables are packaged jointly in a protective cover. Insulated copper wires arranged in regular spiral pattern.

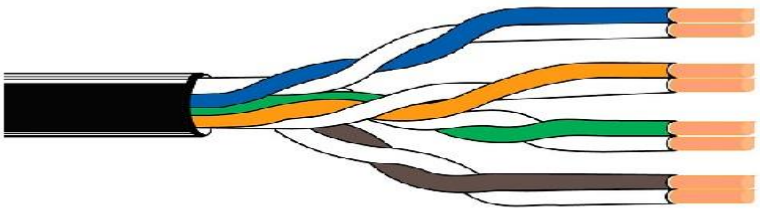
- ✓ The oldest, least expensive, and most commonly used media
- ✓ reduce susceptibility to interference than straight pair wires (two straight parallel wires tend to act as an antenna and pick up extraneous signals when compared to twisted pairs)
- ✓ Highly susceptible to electrical noise, interference, and 'tapping' of the signal as compared to the other guided media
- ✓ Usually used for multiplexing multiple telephone lines, also used for transmitting digital date for point-to-point links (e.g., the leased line for WSUNet)
- ✓ Arrangement of twisted pairs into group used for high-speed (10-100 Mbps) LAN.



This is the most frequently used type of transmission media and it is available in two types.

A. UTP (Unshielded Twisted Pair)

This UTP cable has the capacity to block interference. It doesn't depend on a physical guard and used in telephonic applications. The advantage of UTP is a low cost, very simple to install, and high speed. The disadvantages of UTP are liable to exterior interference, transmits in fewer distances, and less capacity.



Types of UTP

Category 3 Cable

- ✓ With 10 MHz bandwidth, used for telco voice and horizontal wiring for 10-Mbps
- ✓ 10Base-T Ethernet or 4-Mbps Token Ring.

Category 4 Cable

- ✓ With 20 MHz bandwidth, used for 16-Mbps Token Ring.

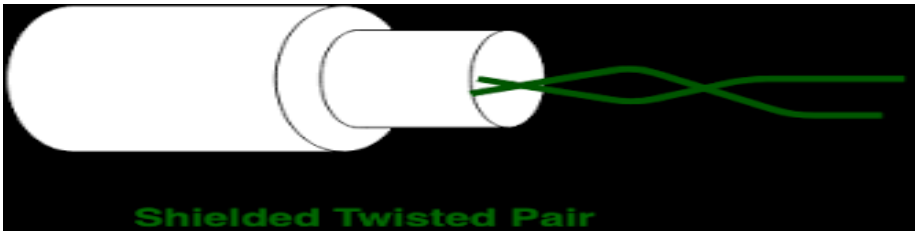
Category 5 Cable

- ✓ The single most popular flavor! With 100 MHz bandwidth, it can handle up to 100-Mbp

B. Shielded Twisted Pair

STP cable includes a particular jacket for blocking outside interference. It is used in rapid data rate Ethernet, in voice & data channels of telephone lines.

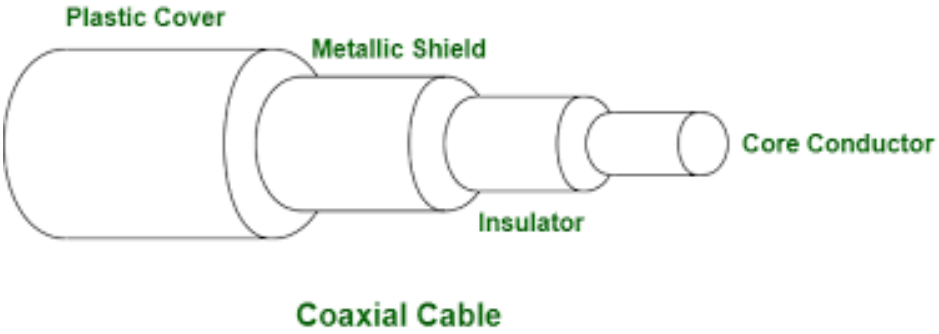
The main advantages of STP cable mainly include good speed, removes crosstalk. The main disadvantages are hard to manufacture as well as install, it is expensive and bulky.



1.6.1.2 Coaxial Cable

This cable contains an external plastic cover and it includes two parallel conductors where each conductor includes a separate protection cover. This cable is used to transmit data in two modes like baseband mode as well as broadband mode. This cable is widely used in cable TVs & analog TV networks.

The advantages of the coaxial cable include high bandwidth, noise immunity is good, low cost and simple to install. The disadvantage of this cable is, the failure of cable can disturb the whole network.



Coaxial Cable

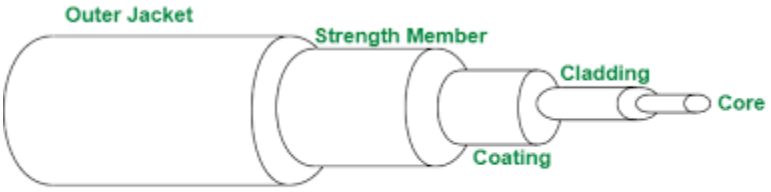
- ✓ Most versatile medium used in LANs, Cable TV, VCR-to-TV connections

- ✓ Noise immunity is better than twisted pair
- ✓ Less susceptible to interference and cross talk but there still is attenuation and thermal noise problem
- ✓ Can go up to 185m (10Base2) or 500m(10Base5) without the need for an amplifier/repeater

1.6.1.3 Optical Fiber Cable

This cable uses the notion of light reflected through a core that is made with plastic or glass. The core is enclosed with less thick plastic or glass and it is known as the cladding, used for large volume data transmission.

The main advantages of this cable include lightweight, capacity & bandwidth will be increased, signal attenuation is less, etc. The disadvantages are high cost, fragile, installation & maintenance is difficult and unidirectional.



OPTICAL FIBER CABLE

1.6.2 Unguided (wireless transmission)

In unguided media transmission and reception are achieved by means of an antenna. It is also known as unbounded otherwise wireless transmission media. It doesn't require any physical medium to transmit electromagnetic signals. The main features of this media are less secure; the signal can be transmitted through air, and applicable for large distances. There are three types of unguided media which are discussed below.

1.6.2.1 Radio waves

These waves are very easy to produce as well as penetrate through buildings. In this, the transmitting & receiving antennas no need to align. The frequency range of these waves ranges from 3 kHz to 1GHz. These waves are used in AM & Fm radios for transmission. These waves are classified into two types namely Terrestrial & Satellite.

1.6.2.2 Microwaves

It is a sightline transmission which means the transmitting & receiving antennas need to align correctly with each other. The distance which is covered through the signal can be directly proportional to the antenna's height. The frequency range of microwaves ranges from 1GHz to 300GHz. These are extensively used in TV distribution & mobile phone communication.

1.6.2.3 Infrared Waves

Infrared (IR) waves are used in extremely small distance communication as they cannot go through obstacles. So, it stops intrusion between systems. The range of frequency of these waves is 300GHz to 400THz. These waves are used in TV remotes, keyboards, wireless mouse, printer, etc.

- ✓ For short-range communication
- ✓ Remote controls for TVs, VCRs, and stereos
- ✓ Indoor wireless LANs

2 CHAPTER TWO
3 Application, Session and Presentation Layers

3.1 Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Application layer interacts with an application program, which is the highest level of OSI model.

The application layer is the OSI layer, which is closest to the end-user. It means OSI application layer allows users to interact with other software application.

Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model.

The functions of the Application Layers are

- ✓ Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- ✓ It allows users to log on to a remote host
- ✓ This layer provides various e-mail services
- ✓ This application offers distributed database sources and access for global information about various objects and services.

3.2 Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

The session layer is responsible for dialog control and synchronization.

Specific responsibilities of the session layer include the following:

- ✓ **Dialog control.** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.
- ✓ **Synchronization.** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent. Figure below illustrates the relationship of the session layer to the transport and presentation layers.

3.3 Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. Figure below shows the relationship between the presentation layer and the application and session layers.

The presentation layer is responsible for translation, compression, and encryption.

Specific responsibilities of the presentation layer include the following:

Translation: The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Encryption. To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

Compression: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video

3.4 Application, Session and Presentation Layers Protocols

The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at these layers.

3.4.1 Simple Mail Transfer Protocol (SMTP)

Governs the transmission of mail messages and attachments. SMTP is used in the case of outgoing messages. More powerful protocols such as POP3 and IMAP4 are needed and available to manage incoming messages.

- ✓ POP3(Post Office Protocol version 3) is the older protocol
- ✓ IMAP4(Internet Mail Access Protocol version 4) is the more advanced protocol

3.4.2 Telnet

Telnet is a protocol used to log on to remote hosts using the TCP/IP protocol suite. Using Telnet, a TCP connection is established and keystrokes on the user's machine act like keystrokes on the remotely connected machine. Often, Telnet is used to connect two dissimilar systems (such as PCs and UNIX machines).

Through Telnet, you can control a remote host over LANs and WANs such as the Internet. For example, network managers can use Telnet to log on to a router from a computer elsewhere on their LAN and modify the router's configuration.

3.4.3 File Transfer Protocol (FTP)

File Transfer Protocol (FTP) lets us transfer files, and it can accomplish this between any two machines using it. But accessing a host through FTP is only the first step. Users must then be subjected to an authentication login that's usually secured with passwords and usernames implemented by system administrators to restrict access.

FTP's functions are limited to listing and manipulating directories, typing file contents, and copying files between hosts.

3.4.4 Trivial File Transfer Protocol (TFTP)

Trivial File Transfer Protocol (TFTP) is stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it because it's fast and so easy to use! But TFTP doesn't offer the abundance of functions that FTP does because it has no directorybrowsing abilities, meaning that it can only send and receive files. There's no authentication as with FTP, so it's even more insecure, and few sites support it because of the inherent security risks.

A significant difference between FTP and TFTP is that TFTP relies on UDP at the Transport layer, but FTP uses TCP protocol.

3.4.5 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) collects and manipulates valuable network information. It gathers data from a network management station (NMS) at fixed or random intervals, requiring them to disclose certain information, or even asking for certain information from the device.

In addition, network devices can inform the NMS about problems as they occur so the network administrator is alerted.

3.4.6 Hypertext Transfer Protocol (HTTP)

It's used to manage communications between web browsers and web servers and opens the right resource when you click a link, wherever that resource may actually reside. In order for a browser to display a web page, it must find the exact server that has the right web page, plus the exact details that identify the information requested. The browser can understand what you need when you enter a Uniform Resource Locator (URL), which we usually refer to as a web address, e.g. http://www.lammle.com/forum and http://www.lammle.com/blog.

Each URL defines the protocol used to transfer data, the name of the server, and the particular web page on that server.

3.4.7 Hypertext Transfer Protocol Secure (HTTPS)

Hypertext Transfer Protocol Secure (HTTPS) is also known as Secure Hypertext Transfer Protocol. It uses Secure Sockets Layer (SSL). Sometimes you'll see it referred to as SHTTP or SHTTP, which were slightly different protocols, but since Microsoft supported HTTPS, it became the de facto standard for securing web communication. But no matter-as indicated, it's a secure version of HTTP that arms you with a whole bunch of security tools for keeping transactions between a web browser and a server secure.

3.4.8 Domain Name Service (DNS)

The Domain Name System (DNS) is a directory lookup service that provides a mapping between the name of a host on the Internet and its numerical address. Domain Name Service (DNS)- resolves hostnames- to IP addresses specifically, Internet names, such as www.au.edu.etBut you don't have to actually use DNS. You just type in the IP address of any device you want to communicate with and find the IP address of a URL by using the Ping program. For example, >ping www.cisco.com will return the IP address resolved by DNS.

3.4.9 Domain Name System (DNS)

Resolves domain names to IP addresses and vice versa. An IP address identifies hosts on a network and the Internet as well, but DNS was designed to make our lives easier. The IP address

would change and no one would know what the new one was. DNS allows you to use a domain name to specify an IP address.

Domain name

A domain name is represented by a series of character strings, called labels, separated by dots. Each label represents a level in the domain naming hierarchy. E.g., In the domain name www.google.com, com is the top-level domain (TLD), google is the second-level domain, and www is the third-level domain. Each second-level domain can contain multiple third level domains. E.g., In addition to www.google.com, Google also owns the following domains:

news.google.com, maps.google.com, and mail.google.com. The very last section of the domain is called its top-level domain (TLD) name.

3.4.10 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to hosts dynamically. It allows for easier administration and works well in small to very large network environments. Many types of hardware can be used as a DHCP server, including a Cisco router.

A DHCP address conflict occurs when two hosts use the same IP address. This sounds bad, and it is! A lot of information a DHCP server can provide to a host when the host is requesting an IP address from the DHCP server. Here's a list of the most common types of information a DHCP server can provide:

- ✓ IP address
- ✓ Subnet mask
- ✓ Domain name
- ✓ Default gateway (routers)
- ✓ DNS server address

This is the four-step process a client takes to receive an IP address from a DHCP server:

- ✓ The DHCP client broadcasts a DHCP Discover message looking for a DHCP server (Port 67).
- ✓ The DHCP server that received the DHCP Discover message sends a layer 2 unicast DHCP Offer message back to the host.
- ✓ The client then broadcasts to the server a DHCP Request message asking for the offered IP address and possibly other information.
- ✓ The server finalizes the exchange with a unicast DHCP Acknowledgment message...Etc.

4 CHAPTER THREE
5 Transport Layer

5.1 Definition

The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.

The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.

The transport layer protocols are implemented in the end systems but not in the network routers.

A computer network provides more than one protocol to the network applications. For example, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.

All transport layer protocols provide multiplexing/demultiplexing service. It also provides other services such as reliable data transfer, bandwidth guarantees, and delay guarantees.

Each of the applications in the application layer has the ability to send a message by using TCP or UDP. The application communicates by using either of these two protocols. Both TCP and UDP will then communicate with the internet protocol in the internet layer. The applications can read and write to the transport layer. Therefore, we can say that communication is a two-way process.

5.2 Multiplexing

The transport layer uses the multiplexing to improve transmission efficiency.

Multiplexing can occur in two ways:

Upward multiplexing: Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.

Downward multiplexing: Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.

5.3 Addressing

- ✓ According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the

session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.

- ✓ The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
- ✓ The transport layer protocols need to know which upper-layer protocols are communicating.

Important functions of Transport Layers

The transport layer is responsible for the delivery of a message from one process to another.

Other responsibilities of the transport layer include the following:

- ✓ **Service-point addressing:** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
- ✓ **Segmentation and reassembly:** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- ✓ **Connection control:** The transport layer can be either connectionless or connection-oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- ✓ **Flow control:** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- ✓ **Error control.** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

5.4 Protocols in Transport Layer

Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

5.4.1 User Datagram Protocol

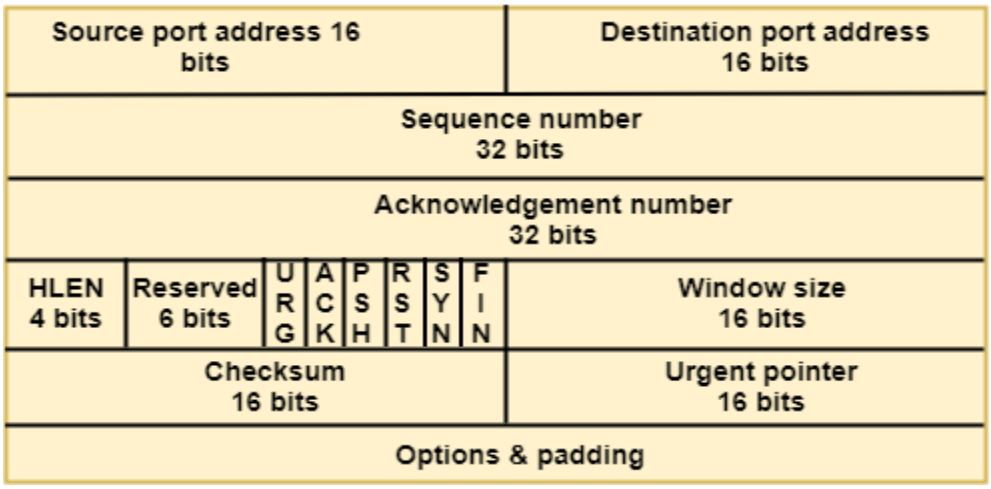
The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

5.4.2 Transmission Control Protocol

The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

TCP Segment Format



Were,

Source port address: It is used to define the address of the application program in a source computer. It is a 16-bit field.

Destination port address: It is used to define the address of the application program in a destination computer. It is a 16-bit field.

Sequence number: A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.

Acknowledgement number: A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.

Header Length (HLEN): It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.

Reserved: It is a six-bit field which is reserved for future use.

Control bits: Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

5.4.3 Stream Control Transmission Protocol

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

Differences between TCP & UDP

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retransmits the damaged frame.

6 CHAPTER FOUR

7 Network Layer Addressing and Routing

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Figure below shows the relationship of the network layer to the data link and transport layers.

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Other responsibilities of the network layer include the following:

Logical addressing. The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

Routing. When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

7.1 Network Addressing

Layer 3 network addressing is one of the major tasks of Network Layer. Network Addresses are always logical i.e. these are software based addresses which can be changed by appropriate configurations.

A network address always points to host / node / server or it can represent a whole network. Network address is always configured on network interface card and is generally mapped by system with the MAC address (hardware address or layer-2 address) of the machine for Layer-2 communication.

There are different kinds of network addresses in existence:

- ✓ IP
- ✓ IPX
- ✓ AppleTalk

We are discussing IP here as it is the only one, we use in practice these days.

IP addressing provides mechanism to differentiate between hosts and network. Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network. The host which needs to communicate outside its subnet, needs to know destination network address, where the packet/data is to be sent.

Hosts in different subnet need a mechanism to locate each other. This task can be done by DNS. DNS is a server which provides Layer-3 address of remote host mapped with its domain name or FQDN. When a host acquires the Layer-3 Address (IP Address) of the remote host, it forwards all its packet to its gateway. A gateway is a router equipped with all the information which leads to route packets to the destination host.

Routers take help of routing tables, which has the following information:

- ✓ Address of destination network
- ✓ Method to reach the network

Routers upon receiving a forwarding request, forwards packet to its next hop (adjacent router) towards the destination.

The next router on the path follows the same thing and eventually the data packet reaches its destination.

Network address can be of one of the following:

- ✓ Unicast (destined to one host)
- ✓ Multicast (destined to group)
- ✓ Broadcast (destined to all)
- ✓ Anycast (destined to nearest one)

A router never forwards broadcast traffic by default. Multicast traffic uses special treatment as it is most a video stream or audio with highest priority. Anycast is just similar to unicast, except that the packets are delivered to the nearest destination when multiple destinations are available.

7.2 Network Routing

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes. The software-based routers have limited functionality and limited scope.

A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination.

Routes can be statically configured or dynamically learnt. One route can be configured to be preferred over others.

7.2.1 Unicast routing

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.

7.2.2 Broadcast routing

By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

Broadcast routing can be done in two ways (algorithm):

- ✓ A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses.

All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting.

- ✓ This method consumes lots of bandwidth and router must destination address of each node.
- ✓ Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.

7.2.3 Multicast Routing

Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.

The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.

Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops.

7.2.4 Anycast Routing

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in routing topology.

Anycast routing is done with help of DNS server. Whenever an Anycast packet is received it is enquired with DNS to where to send it. DNS provides the IP address which is the nearest IP configured on it.

7.3 Network Layer Protocol

Every computer in a network has an IP address by which it can be uniquely identified and addressed. An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time and another IP at some different time.

7.3.1 Internetworking Protocol (IP)

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol-a best-effort delivery service.

The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP

does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

The limited functionality of IP should not be considered a weakness, however. IP provides bare-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency

7.3.2 Address Resolution Protocol (ARP)

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.

To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, "Who has this IP address?" Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

7.3.3 Internet Control Message Protocol (ICMP)

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP. ICMP contains dozens of diagnostics and error reporting messages.

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.

7.3.4 Internet Group Message Protocol

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

7.3.5 Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- ✓ **Class A:** It uses first octet for network addresses and last three octets for host addressing.
- ✓ **Class B:** It uses first two octets for network addresses and last two for host addressing.
- ✓ **Class C:** It uses first three octets for network addresses and last one for host addressing.
- ✓ **Class D:** It provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- ✓ **Class E:** It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.

7.3.6 Internet Protocol Version 6 (IPv6)

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6-equipped machines can roam around without the need of changing their IP addresses.

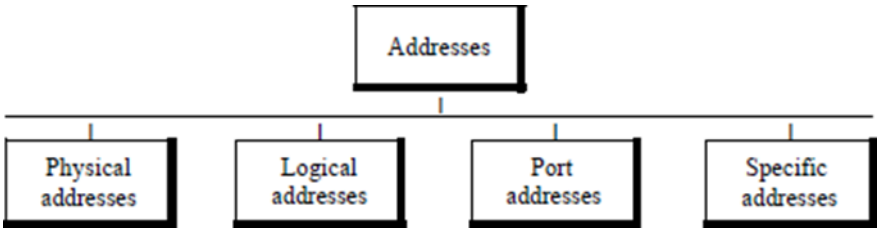
IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6-enabled networks to speak and roam around different networks easily on IPv4. These are:

- ✓ Dual stack implementation
- ✓ Tunneling

- ✓ NAT-PT

7.4 Internet Addressing

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses



Each address is related to a specific layer in the TCPIIP architecture

7.4.1 IP Address

7.4.1.1 IPv4

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet. An IPv4 address is 32 bits long.

IPv4 addresses are unique. They are unique in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have the same address at the same time. We will see later that, by using some strategies, an address may be assigned to a device for a time period and then taken away and assigned to another device.

On the other hand, if a device operating at the network layer has m connections to the Internet, it needs to have m addresses. We will see later that a router is such a device.

The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

7.4.1.2 Address Space

A protocol such as IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2N because each bit can have two different values (0 or 1) and N bits can have 2N values.

IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet.

Notations

There are two prevalent notations to show an IPv4 address: binary notation and dotted decimal notation.

Binary Notation

In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. The following is an example of an IPv4 address in binary notation:

01110101 10010101 00011101 00000010

Dotted-Decimal Notation

To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted decimal notation of the above address:

117.149.29.2

An IPv4 address in both binary and dotted-decimal notation. Note that because each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255.

Example 1

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

A. 10000001 00001011 00001011 11101111
B. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number (see Appendix B) and add dots for separation.

A. 129.11.11.239
B. 193.131.27.255

Example 2

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

A. 111.56.45.78
B. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent

A. 01101111 00111000 00101101 01001110
B. 11011101 00100010 00000111 01010010

7.4.2 Classful Addressing

IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing. Although this scheme is becoming obsolete, we briefly discuss it here to show the rationale behind classless addressing. In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.

In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

We can find the class of an address when given the address in binary notation or dotted-decimal notation. If the address is given in binary notation, the first few bits can immediately tell us the class of the address. If the address is given in decimal-dotted notation, the first byte defines the class. Both methods are shown in Figure below

7.4.2.1 Classes and Blocks

One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size as shown in Table

Class	*Number ofBlocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

In c1assful addressing, a large part of the available addresses were wasted.

Netid (Network Id) and Hostid

In classful addressing, an IP address in class A, B, or C is divided into ***netid*** and ***hostid.*** These parts are of varying lengths, depending on the class of the address. Note that the concept does not apply to classes D and E.

In class A, one byte defines the ***netid*** and three bytes define the ***hostid.*** In class B, two bytes define the netid and two bytes define the ***hostid.*** In class C, three bytes define the ***netid*** and one byte defines the ***hostid.***

7.4.2.2 Mask

Although the length of the ***netid*** and ***hostid*** (in bits) is predetermined in classful addressing, we can also use a mask (also called the default mask), a 32-bit number made of contiguous Is

followed by contiguous as. The masks for classes A, B, and C are shown in Table 19.2. The concept does not apply to classes D and E.

Table below Default masks for classful addressing

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	11111111 00000000 00000000 00000000	255.0.0.0	*18*
B	11111111 11111111 00000000 00000000	255.255.0.0	*116*
C	11111111 11111111 11111111 00000000	255.255.255.0	*124*

The mask can help us to find the **netid** and the **hostid**. For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the **netid**; the next 24 bits define the **hostid**.

The last column of Table 19.2 shows the mask in the form In where n can be 8, 16, or 24 in classful addressing. This notation is also called slash notation or Classless Interdomain Routing (CIDR) notation. The notation is used in classless addressing, which we will discuss later. We introduce it here because it can also be applied to classful addressing. We will show later that classful addressing is a special case of classless addressing.

7.4.2.3 Subnetting

During the era of classful addressing, subnetting was introduced. If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors. Subnetting increases the number of Is in the mask, as we will see later when we discuss classless addressing.

7.4.3 Classless Addressing

To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.

7.4.3.1 Address Blocks

In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity. For example, a household may be given only two addresses; a large organization may be given thousands of addresses. An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve. Restriction to simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1. The addresses in a block must be contiguous, one after another.

2. The number of addresses in a block must be a power of 2 (I, 2, 4, 8, ...).
3. The first address must be evenly divisible by the number of addresses.

7.5 Subnetting

7.5.1 Why subnetting?

Classes of IP addresses offer a range from 256 to 16.8 million hosts. Subnetting separates a network into multiple logically defined segments, or subnets. To efficiently manage a limited supply of IP addresses, all classes can be subdivided into smaller sub networks or subnets. This process is known as subnetting.

7.5.2 Subnetting Process

To create the sub network structure, host bits must be reassigned as network bits which is often referred to as borrowing bits. The starting point for this process is always the leftmost bit of the host. That is he one closest to the last network octet.

Subnet addresses include:

- ✓ The Class A, Class B, and Class C network portion,
- ✓ a subnet field and
- ✓ a host field.

The subnet field and the host field are created from the original host portion of the major IP address. This is done by assigning bits from the host portion to the original network portion of the address. Subnets have sub network ID (subnet ID) just as networks have network IDs. Subnet IDs are found by replacing all host fields with 0s.

7.5.3 Subnetting Advantage

The subnet field and the host field are created from the original host portion of the major IP address. This is done by assigning bits from the host portion to the original network portion of the address. Subnets have sub network ID (subnet ID) just as networks have network IDs. Subnet IDs are found by replacing all host fields with 0s.

7.5.4 Borrowing a bits

To determine the number of bits to be used, the network designer needs to calculate how many hosts the largest sub network requires and the number of sub networks needed Large number of subnets means fewer hosts and a large number of hosts means fewer subnets Total number of subnets is 2^bits borrowed Total number of hosts is 2^remaining host bits Example if three bits are borrowed from a class C address, total number of subnets is 8 (2^3) and total number of hosts is 32 (2^5)

Positional value of bits

Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1

Value is the position value of the bits borrowed.

Example

Q - What is the value of 01010110 in decimal?

A - 0 + 64 + 0 + 16 + 0 + 4 + 2 + 0 = 86

Usable subnets & Usable Hosts

Among the available subnets, it is not advised to use the following two subnets:

- ✓ The subnet with all 0's in the subnet field
- ✓ The subnet with all 1's in the subnet field

If subnet zero (all 0's in the subnet field) is used, it means that a network and a subnet have the same address. If the last subnet (all 1's in the subnet field) is used, it means that the network broadcast address and a subnet have the same address. Hence usable subnets will be 2^bits borrowed – 2. Example if three bits are borrowed from a class C address, total number of usable subnets is 6 (2^3 - 2) and total number of usable hosts is 30 (2^5 - 2)

7.5.5 Subnet Masks

For the subnet address scheme to work, every machine on the network must know which part of the host address will be used as the subnet address. This is accomplished by assigning a subnet mask to each machine. A subnet mask is a 32-bit value that allows the recipient of IP packets to distinguish the network portion of the IP address from the host portion of the IP address

A subnet mask is composed of 1s and 0s where:

- ✓ The 1s in the subnet mask represent the positions that refer to the network or subnet addresses
- ✓ The 0s in the subnet mask represent the positions that refer to the host address

7.5.5.1 Default subnet masks

Not all networks need subnets, meaning they use the default subnet mask. This is basically the same as saying that a network doesn't have a subnet address. Here is default subnet mask for Classes A, B, and C

- ✓ Class A - ***network. Node .node. node*** Subnet mask: 255.0.0.0
- ✓ Class B ***network. network. node. node*** Subnet mask:255.255.0.0
- ✓ Class C - ***network. network. network. node*** Subnet mask:255.255.255.0

These default subnet masks show the minimum number of 1's you can have in a subnet mask for each class.

7.5.5.2 Specifying subnets

- ✓ Example if three bits are borrowed from a class C address, the subnet mask is 255.255.255.224
- ✓ Subnets may also be represented, in a slash format.
- ✓ For example, /24 indicates that the total bits that were used for the network and sub network portion is 24
- ✓ The subnet mask 255.255.255.224 in slash format is /27. (224=11100000)

Number of bits borrowed from a class C address, positional value of each bit and resulting mask (in number and slash format).

Slash format	/25	/26	/27	/28	/29	/30	N/A	N/A
Mask	128	192	224	240	248	252	254	255
Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1

7.5.6 Subnetting Class C addresses

Example 1

Let us subnet the network address 192.168.10.0 with a subnet mask 255.255.255.192 or in slash format /26

- ✓ (192 is 11000000)

Q- How many usable subnets do we have?

A- Since 192 is 2 bits on (11000000), the answer would be 2^2 – 2 = 2

Q- How many usable hosts per subnet do we have?

A. We have 6 host bits off (11000000), so the answer would be 2^6 – 2 = 62 hosts

Q-What are the subnet IDs?

A-We vary the borrowed bits (00, 01, 10, 11).

So the subnets are 192.168.10.0, 192.168.10.64, 192.168.10.128, 192.168.10.192

Q - What are the valid or usable subnets.

A - The ones which do not have all 0's or all 1's in the subnet field, namely 192.168.10.64 and 192.168.10.128

Q - What's the broadcast address for the valid subnets?

A - The valid subnets start with 01 and 10. The broadcast address for these two addresses will have 01111111 and 10111111. Which are 127 and 191. So the broadcast addresses will be 192.168.10.127 and 192.168.10.191. As a shortcut you can follow this rule: The number right before the value of the next subnet is all host bits turned on and equals the broadcast address.

Q - What are the valid hosts?

A - These are the numbers between the subnet ID and broadcast address

The hosts for the first valid subnet are: 192.168.10.65, 192.168.10.66, ⋯, 192.168.10.126

The hosts for the second valid subnet are:192.168.10. 129, 192.168.10.130, ⋯, 192.168.10.190

Example 2

Now let us subnet the network address 192.168.10.0, this time with a subnet mask 255.255.255.224 or in slash format /27

Q - How many subnets do we have?

A - Since 224 is 3 bits on (11100000), the answer would be 2^3 – 2 = 6

Q - How many hosts per subnet do we have?

A - We have 6 host bits off (11100000), so the answer would be 2^5 – 2 = 30 hosts

Q - What are the subnet IDs?

A- We vary the borrowed bits (000, 001, 010, 011, 100, 101, 110, 111). So the subnets are 192.168.10.0, 192.168.10.32, 192.168.10.64, 192.168.10.96, 192.168.10.128, 192.168.10.160, 192.168.10.192, 192.168.10.224

Q - What are the valid or usable subnets?

A- 192.168.10.32, 192.168.10.64, 192.168.10.96, 192.168.10.128, 192.168.10.160, 192.168.10.192

Q - What's the broadcast address for the valid subnets?

A - The number right before the value of the next subnet is all host bits turned on and equals the broadcast address – 192.168.10.63, 192.168.10.95, 192.168.10.127, 192.168.10.159, 192.168.10.191, 192.168.10.223

Q - What are the valid hosts?

192.168.10.33 – 192.168.10.62	**192.168.10.129 – 192.168.10.161**
192.168.10.65 – 192.168.10.94	**192.168.10.161 – 192.168.10.193**
192.168.10.97 – 192.168.10.128	**192.168.10.193– 192.168.10.222**

Example 3

Subnet the network address 192.168.10.0, with a subnet mask 255.255.255.248 (/28)

Q - How many subnets do we have?

A - Since 248 is 4 bits on (11110000), 2^4 – 2 = 14

Q - How many hosts per subnet do we have?

A - We have 6 host bits off (11110000), 2^4 – 2 = 14

Q - What are the subnet IDs?

A - We vary the borrowed bits (0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111).

So the subnets ID's are:

192.168.10.0, 192.168.10.16, 192.168.10.32, 192.168.10.48, 192.168.10.64, 192.168.10.80, 192.168.10.96, 192.168.10.112, 192.168.10.128, 192.168.10.144, 192.168.10.160, 192.168.10.176, 192.168.10.192, 192.168.10.208, 192.168.10.224, 192.168.10.240

Q - What are the valid or usable subnets?

Q - What's the broadcast address for the valid subnets?
A- 192.168.10.31, 192.168.10.47, 192.168.10.63, 192.168.10.79, 192.168.10.95, 192.168.10.111, 192.168.10.127, 192.168.10.143, 192.168.10.159, 192.168.10.175, 192.168.10.191, 192.168.10.107, 192.168.10.223, 192.168.10.239
Q - What are the valid hosts?
192.168.10.17 – 192.168.10.30, 192.168.10.33 – 192.168.10.46, 192.168.10.49 – 192.168.10.62, 192.168.10.65–192.168.10.78, 192.168.10.81–192.168.10.94, 192.168.10.97–192.168.10.110, 192.168.10.113–192.168.10.126, 192.168.10.129–192.168.10.142, 192.168.10.145–192.168.10.158,192.168.10.161–192.168.10.174192.168.10.177–192.168.10.190, 192.168.10.193–192.168.10.106, 192.168.10.109–192.168.10.222, 192.168.10.225-192.168.10.238.

7.5.7 Calculating Class, A and B Network

The Class A and B sub netting procedure is identical to the process for Class C, except there may be significantly more bits involved.
Assigning 12 bits of a Class B address to the subnet field creates a subnet mask of 255.255.255.240 or /28.
All eight bits were assigned in the third octet resulting in 255, the total value of all eight bits. Four bits were assigned in the fourth octet resulting in 240.

Possible Class B subnet masks

255.255.128.0 (/17) 255.255.255.0 (/24)
255.255.192.0 (/18) 255.255.255.128 (/25)
255.255.224.0 (/19) 255.255.255.192 (/26)
255.255.240.0 (/20) 255.255.255.224 (/27)
255.255.248.0 (/21) 255.255.255.240 (/28)
255.255.252.0 (/22) 255.255.255.248 (/29)
255.255.254.0 (/23) 255.255.255.252 (/30)

7.5.7.1 Sub netting Class B addresses

Example 1

172.16.0.0 = Network address 255.255.192.0 = Subnet mask Q - How many Subnets?
A - 2^2 – 2 = 2.
Q - How many Hosts per subnet?
2^14 – 2 = 16,382. (6 bits in the third octet, and 8 in the fourth) Q - Subnet IDs of valid subnets?
A - 172.16.64.0 and 172.16.128.0
Q Broadcast address for each subnet and valid hosts?
A Below is the two subnets available and the address of each:

Subnet	172.16.64.0	172.16.128.0
First host	172.16.64.1	172.16.128.1
Last host	172.16.127.254	172.16.191.254
Broadcast	172.16.127.255	172.16.191.255

Example 2

172.16.0.0 = Network address 255.255.240.0 = Subnet mask Q How many Subnets?
A- 2^4 – 2 = 14
Q- How many Hosts per subnet? 2^12 – 2 = 4094
Q- Subnet IDs of valid subnets?
A- 172.16.16.0 and 172.16.32.0, …, 172.16.224.0
Q- Broadcast address for each subnet and valid hosts?
A- Below is the subnets available and the address of each:

Subnet	172.16.16.0	172.16.32.0	…
First host	172.16.16.1	172.16.32.1	…
Last host	172.16.31.254	172.16.47.254	…
Broadcast	172.16.31.255	172.16.47.255	…

Possible Class A subnet masks

255.128.0.0 (/9)	255.255.240.0 (/20)
255.192.0.0 (/10)	255.255.248.0 (/21)
255.224.0.0 (/11)	255.255.252.0 (/22)
255.240.0.0 (/12)	255.255.254.0 (/23)
255.248.0.0 (/13)	255.255.255.0 (/24)
255.252.0.0 (/14)	255.255.255.128 (/25)
255.254.0.0 (/15)	255.255.255.192 (/26)
255.255.0.0 (/16)	255.255.255.224 (/27)
255.255.128.0 (/17)	255.255.255.240 (/28)
255.255.192.0 (/18)	255.255.255.248 (/29)
255.255.224.0 (/19)	255.255.255.252 (/30)

7.5.7.2 Sub netting Class A addresses

Example 1

10.0.0.0 = Network address 255.255.0.0 (/16) = Subnet mask Q Subnets?
A 2^8 – 2 = 254
Q- Hosts?
A- 2^16 – 2 = 65,534
Q- Valid subnets?
A- 10.1.0.0, 10.2.0.0, 10.3.0.0, …, 10.254.0.0
Q- Broadcast address for each subnet and valid hosts?

Subnet	10.1.0.0	… 10.254.0.0
First host	10.1.0.1	… 10.254.0.1
Last host	10.1.255.254	… 10.254.255.254
Broadcast	10.1.255.255	… 10.254.255.255

Example 2

10.0.0.0 = Network address 255.255.240.0 (/20) = Subnet mask Q Subnets?
2^12 – 2 = 4094
Q-Hosts?

A- 2^12 – 2 = 4094
Q-Valid subnets?
A- Subnet 10.1.0.0, 10.1.16.0,…, 10.255.224.0
First host 10.1.0.1, 10.1.16.1,…, 10.255.224.1
Last host 10.1.15.254, 10.1.31.254,…, 10.255.239.254
Broadcast 10.1.15.255, 10.1.31.255,…, 10.255.239.255

8 CHAPTER FIVE
9 Data Link Layer and Physical Layer

9.1 Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur.

The physical layer is responsible for movements of individual bits from one hop (node) to the next.

9.2 Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). Figure below shows the relationship of the data link layer to the network and physical layers.

The data link layer is responsible for moving frames from one hop (node) to the next.

Other responsibilities of the data link layer include the following:

- ✓ **Framing:** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- ✓ **Physical addressing:** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
  - ✓ **Flow control:** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
  - ✓ **Error control:** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

- ✓ **Access control:** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

9.3 Ethernet

The standards at the layer 1 and 2 of the OSI model are defined as Ethernet standards. The different standards used in Ethernet define the different layer 1 and layer 2 protocols, however, the format of the frame does not change.

As we mentioned in the previous sections, the data link layer provides mechanisms for converting packets to frames while the physical layer converts frames to bits which are then transmitted over the physical media.