ARBA MINCH UNIVERSITY

ARBAMINCH INSTITUTE OF TECHNOLOGY

FACULTY OF COMPUTING AND SOFTWARE ENGINEERING

Lecture Manual

On

Data Communication and Computer Networks

(CoSc2032 & ITec2102)

B.SC. COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

Prepared By: Basha K.
Email: nimonabasha@gmail.com
Phone No.: +251 916273383 or 45854510

2022/23 G.C (2015 E.C)
Arba Minch, Ethiopia

Course Description and Objectives

This course will explore the various types of the data communication systems, networks and their applications. Concept & terminologies like computer networks, layer architecture (OSI & TCP/IP), network hardware, network software, standardization, network medium, and IP addressing will be explored. The practical aspect will deal with building small to medium level networks including Cabling, Configuring TCP/IP, Peer to Peer Networking, Sharing resources, Client Server Networking.

By the end of this course, you will be able to:

- Understand the concepts and principles of data communications and computer networks
- Understand data transmission and transmission media
- Understand Protocols and various networking components
- Understand TCP/IP & OSI Reference Model
- Understand LAN and WAN technologies
- Understand and implement IP addressing.
- Build small to medium level Computer networks

Table of Contents

CHAPTER ONE

BASICS OF DATA COMMUNICATIONS & COMPUTER NETWORKS

1. Introduction to Data Communications

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.

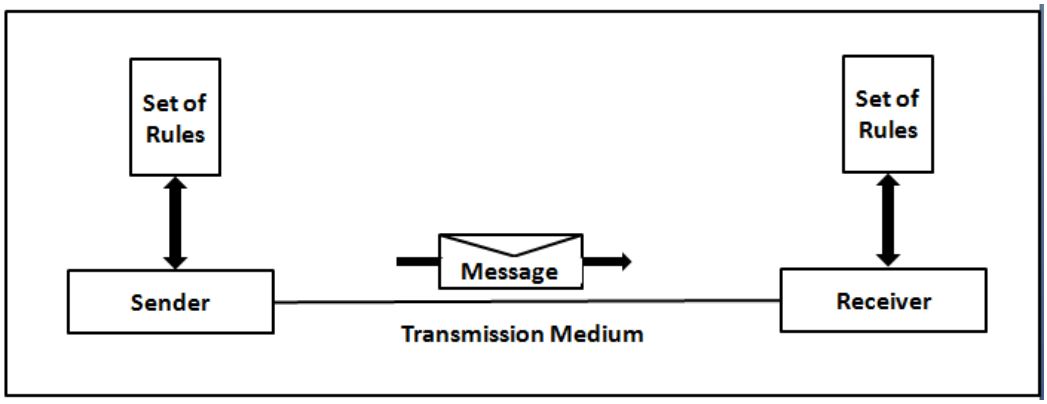
Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable or wirelessly. For data communications to occur, the communicating devices must be part of a **communication system** made up of a combination of **hardware** (physical equipment) and **software** (programs). The **effectiveness** of a data communications system depends on **four** fundamental characteristics: **delivery**, **accuracy**, **timeliness**, and **jitter**.

1. **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.
2. **Accuracy**. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **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.
4. **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.

1.1. Components of a Data Communications System

A data communications system has **five** components

1. **Message.** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender.** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver.** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium.** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media
5. **Protocol.** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking Afan-Oromo cannot be understood by a person who speaks only Japanese.



1.2. Data Representation Techniques

Information today comes in different forms such as text, numbers, images, audio, and video.

1.2.1. Text

In data communications, text is represented as a bit pattern, a sequence of bits (0's or 1's). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the

process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world.

1.2.2. Numbers

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

1.2.3. Images

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the *resolution*. For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image.

After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only black and- white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel.

1.2.4. Audio

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal. We learn how to change sound or music to a digital or an analog signal next chapter.

1.2.5. Video

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion. Again, we can change video to a digital or an analog signal.

1.3. Data Transmission Signals

When data is sent over physical medium, it needs to be first converted into electromagnetic signals. Data itself can be analog such as human voice, or digital such as file on the disk. Both analog and digital data can be represented in digital or analog signals.

1.3.1. Digital Signals

Digital signals are discrete in nature and represent sequence of voltage pulses. Digital signals are used within the circuitry of a computer system.

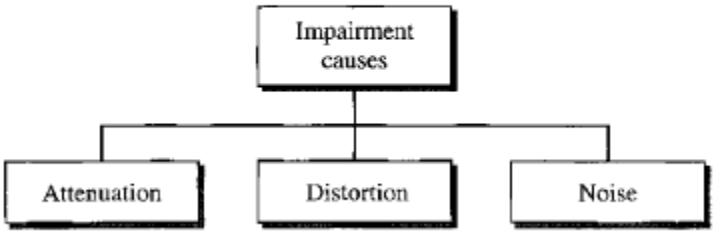
1.3.2. Analog Signals

Analog signals are in continuous wave form in nature and represented by continuous electromagnetic waves.

1.4. Transmission Impairment

When signals travel through the medium, they tend to deteriorate. Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. This may have many reasons as given:

Causes of impairment



1.4.1. Attenuation

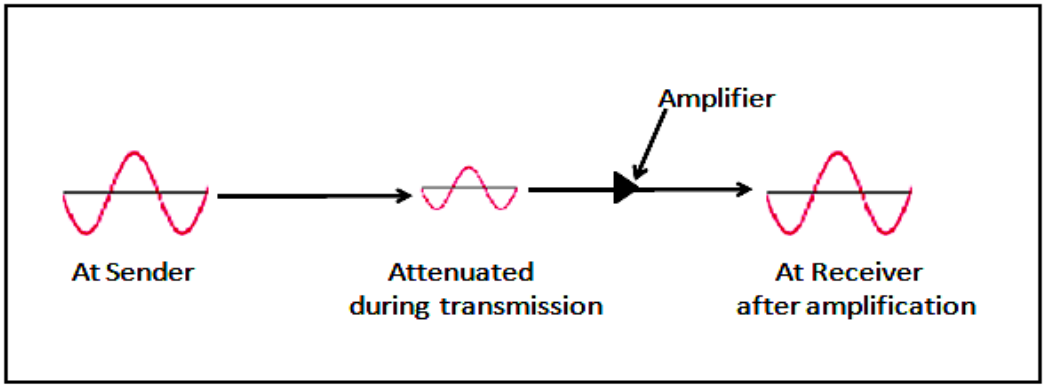
For the receiver to interpret the data accurately, the signal must be sufficiently strong. When the signal passes through the medium, it tends to get weaker. As it covers distance, it loses strength. Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium,

it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, **amplifiers** are used to amplify the signal. Attenuation is measured in terms of Decibels.

The decibel (dB) measures the relative strengths of two signals or one signal at two different points. Note that the decibel is negative if a signal is attenuated and positive if a signal is amplified.

$$dB=10\log_{10} P2/P1$$

Variables PI and P2 are the powers of a signal at points 1 and 2, respectively.



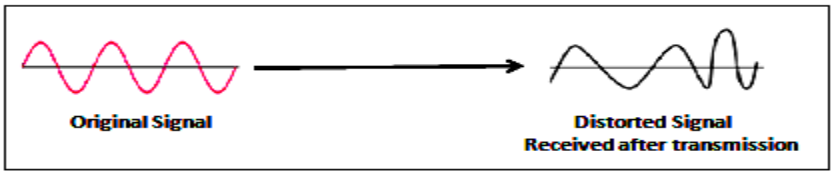
1.4.2. Dispersion

As signal travels through the media, it tends to spread and overlaps. The amount of dispersion depends upon the frequency used.

1.4.3. Delay distortion

Signals are sent over media with pre-defined speed and frequency. If the signal speed and frequency do not match, there are possibilities that signal reaches destination in arbitrary fashion. In digital media, this is very critical that some bits reach earlier than the previously sent ones. This happens when signal changes their shapes.

Distortion means that the signal changes its **form or shape**. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same



1.4.4. Noise

Random disturbance or fluctuation in analog or digital signal is said to be Noise in signal, which may distort the actual information being carried. Noise can be characterized in one of the following classes:

1.4.4.1. Thermal Noise

Heat agitates the electronic conductors of a medium which may introduce noise in the media. Up to a certain level, thermal noise is unavoidable. It is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter

1.4.4.2. Intermodulation

When multiple frequencies share a medium, their interference can cause noise in the medium. Intermodulation noise occurs if two different frequencies are sharing a medium and one of them has excessive strength or the component itself is not functioning properly, then the resultant frequency may not be delivered as expected.

1.4.4.3. Crosstalk

This sort of noise happens when a foreign signal enters into the media. This is because signal in one medium affects the signal of second medium. The effect of one wire on the other. One wire act as a sending antenna and the other as the receiving antenna

1.4.4.4. Impulse

This noise is introduced because of irregular disturbances such as lightening, electricity, short-circuit, or faulty components. Digital data is mostly affected by this sort of noise.

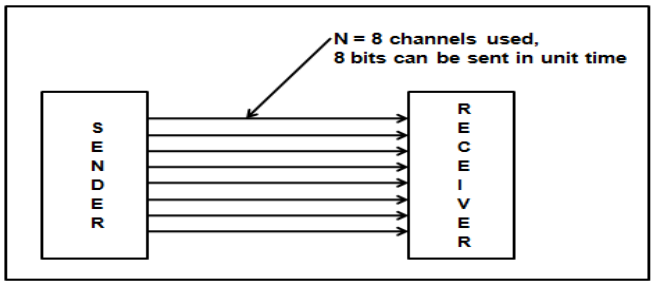
1.5. Digital Transmission Modes/format

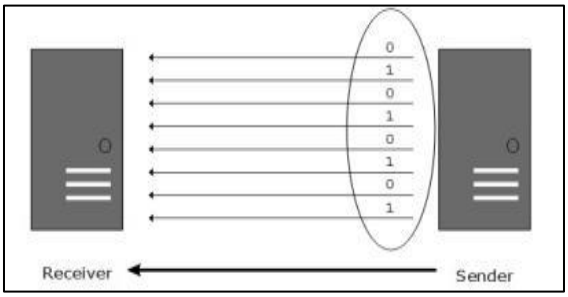
Data is transmitted between two digital devices on the network in the form of **bits (0&1)**. Transmission mode refers to the mode used for transmitting the data. The transmission medium may be capable of sending only a single bit in unit time or multiple bits in unit time. When a single bit is transmitted in unit time the transmission mode used is Serial Transmission and when multiple bits are sent in unit time the transmission mode used is called Parallel transmission.

1.5.1. Types of Transmission Modes:

There are **two** basic types of transmission modes **Serial** and Parallel as shown in the figure below. Serial transmission is further categorized into **Synchronous** and **Asynchronous** Serial transmission.

1) Parallel Transmission:





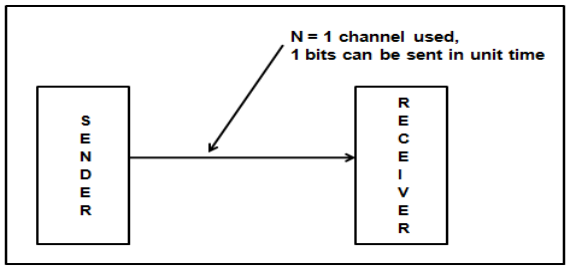
The binary bits are organized into groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bits at once on all lines. Because the data lines are equal to the number of bits in a group or data frame, a complete group of bits (data frame) is sent in one go.

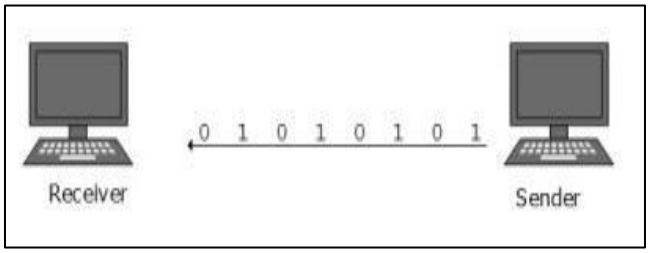
Advantage of Parallel transmission is high speed and **disadvantage** is the cost of wires, as it is equal to the number of bits sent in parallel, hence, it can be used for short distance communication only

- ♣ It involves simultaneous transmission of N bits over N different channels
- ♣ Parallel Transmission increases transmission speed by a factor of N over serial transmission
- ♣ **Example** of Parallel Transmission is the communication between CPU and the Projector

2) Serial Transmission

In Serial Transmission, as the name suggests data is transmitted serially, i.e., **bit by bit**, one bit at a time. Since only one bit has to be sent in unit time only a single channel is required. Bits are sent one after another in a queue manner.





Types of Serial Transmission:

Depending upon the **timing** of transmission of data there are two types of serial transmission as described below

2.1. Asynchronous Transmission

It is named so because there is **no importance of timing**. In asynchronous serial transmission the sender and receiver are not synchronized. The data is sent in group of 8 bits i.e. in bytes.

The sender can start data transmission at any time instant without informing the receiver. To avoid confusing the receiver while receiving the data, **start** and **stop** bits are inserted before and after every group of 8 bits as shown below.

The start bit is indicated by **0** and stop bit is indicated by**1**. The sender and receiver may not be synchronized as seen above but at the bit level they have to be synchronized i.e., the duration of one bit needs to be same for both sender and receiver for accurate data transmission. There may be **gaps** in between the data transmission indication that there is no data being transmitted from sender.

Ex. Assume a user typing at uneven speeds, at times there is no data being transmitted from Keyboard to the CPU.

Advantages

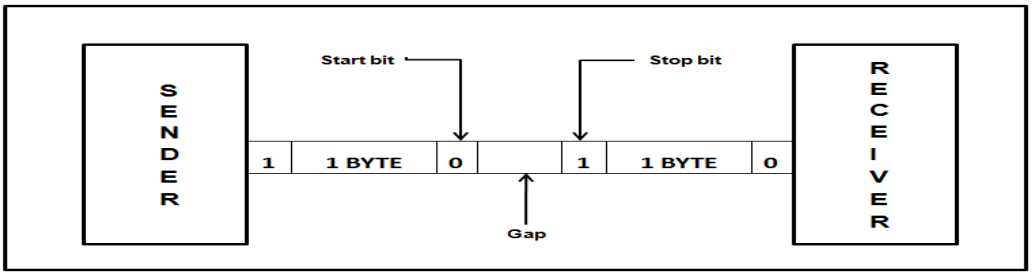
- ♣ Cheap and Effective implementation
- ♣ Can be used for low-speed communication

Disadvantages

- ♣ Insertion of start bits, stop bits and gaps make asynchronous transmission slow.

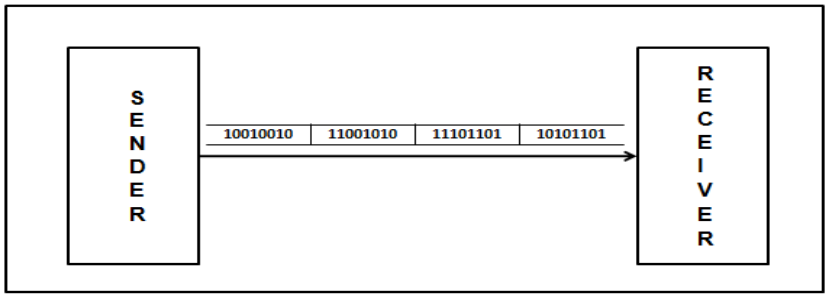
Application

- ♣ Keyboard



2.2. Synchronous Transmission

In Synchronous Serial Transmission, the sender and receiver are highly synchronized. No start, stop bits are used. Instead, a common master clock is used for reference. The sender simply sends stream of data bits in group of 8 bits to the receiver without any start or stop bit. It is the responsibility of the receiver to regroup the bits into units of 8 bits once they are received. When no data is being transmitted a sequence of 0‘s and 1‘s indicating **IDLE** is put on the transmission medium by the sender.



Advantage

- There are no start bits, stop bits or gaps between data units
- Since the above are absent data transmission is faster.
- Due to synchronization, there are no timing errors.

Comparison of serial and parallel transmission

Sr.no	Parameter	Parallel transmission	Serial transmission
1	Number of wire required to transmit N bits	N wire	1 wire
2	Number of bits transmitted simultaneously	N bits	1 bit
3	Speed of data transfer	False	Slow
4	Cost	Higher due to more number of conductor	Low, since only one wire is used
5	Application	Short distance communication such as computer to printer communication	Long distance computer to computer communication.

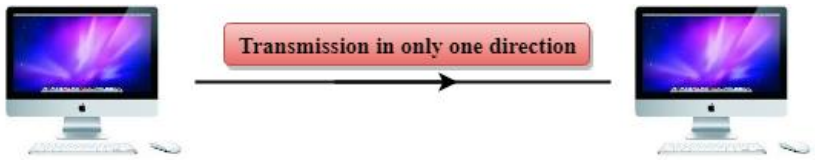
1.6. Modes of Data transmission/Data flow

Devices communicate with each other by sending and receiving data. The data can flow between the two devices in the following ways 1. **Simplex** 2. **Half Duplex** 3. **Full Duplex.**

1) **Simplex:**

In Simplex, communication is **unidirectional.** Only one of the devices sends the data and the other one only receives the data. The simplex mode can use the entire capacity of the channel to send data in one direction. Other example is **TV transmission**

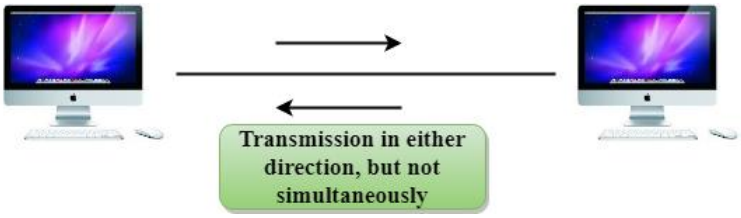
Example: in the below diagram: a cpu send data while a monitor only receives data.



2) Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Eg. **Military personnel Radio (**A walkie-talkie**)**

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

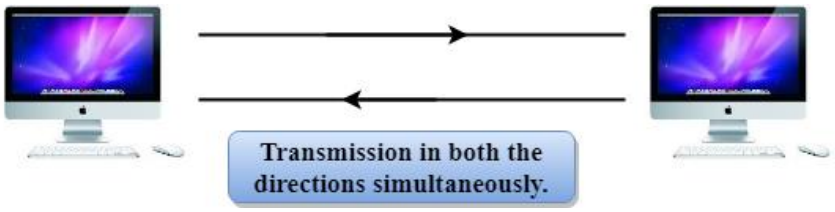


3) Full-Duplex

In full-duplex mode (also called **duplex**), both stations can transmit and receive **simultaneously**. The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions. One common example of full-duplex communication is the **telephone** network.

- ♣ When two people are communicating by a telephone line, both can talk and listen at the same time. Example: **mobile phones**

The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions. E.g Computer network.



1.7. Multiplexing

Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a **shared link**. Multiplexing divides the high-capacity medium into low-capacity logical medium which is then shared by different streams.

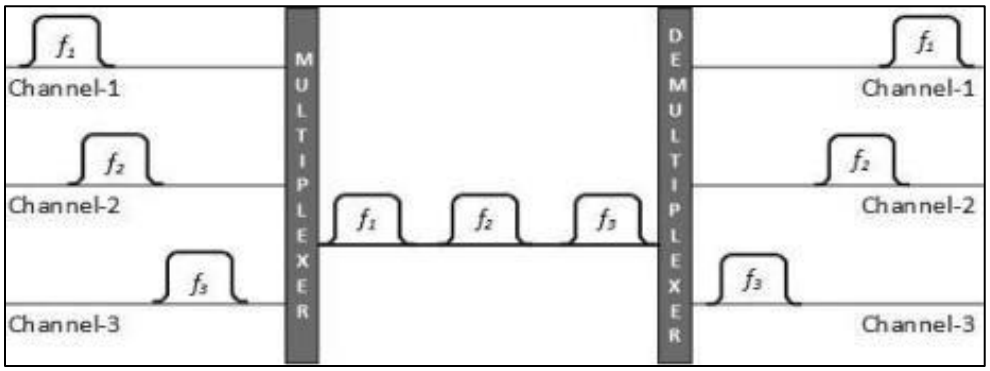
Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing.

When multiple senders try to send over a single medium, a device called **Multiplexer** divides the physical channel and allocates one to each. On the other end of communication, a **De-multiplexer** receives data from a single medium, identifies each, and sends to different receivers. There are different type of multiplexing technique

- Frequency Division Multiplexing
- Time Division Multiplexing
- Wavelength Division Multiplexing
- Code Division Multiplexing

1.7.1. Frequency Division Multiplexing

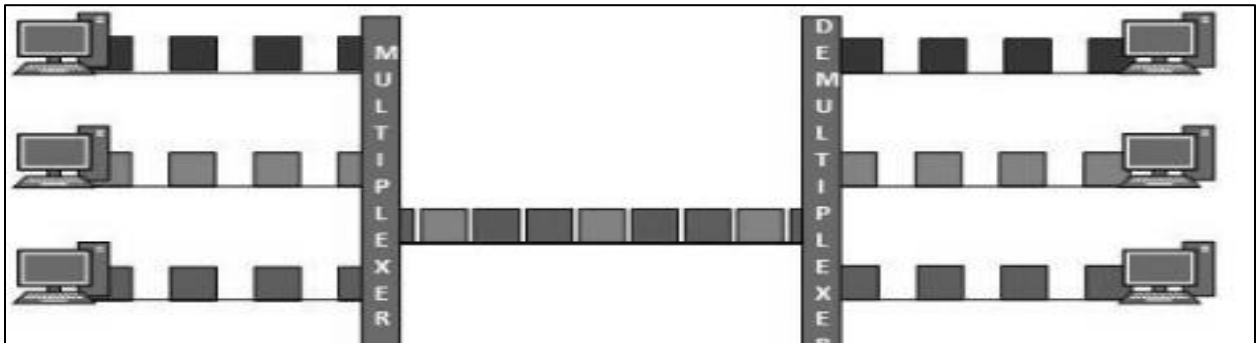
When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



1.7.2. Time Division Multiplexing

TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by **means of time slot**. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e., frame of an optimal size which can be transmitted in given time slot.

TDM works in synchronized mode. Both ends, i.e., Multiplexer and De-multiplexer are timely synchronized, and both switch to next channel simultaneously.



When channel A transmits its frame at one end, the De-multiplexer provides media to channel A on the other end. As soon as the channel A's time slot expires, this side switches to channel B. On the other end, the De-multiplexer works in a synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner.

1.7.3. Wavelength Division Multiplexing

Light has different wavelength (**colors**). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.

Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.

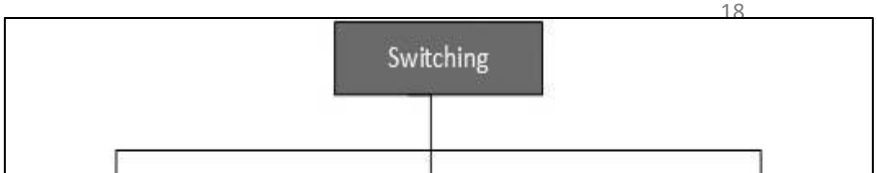
1.7.4. Code Division Multiplexing

Multiple data signals can be transmitted over a single frequency by using Code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a **unique code**. CDM uses orthogonal codes to spread signals.

Each station is assigned with a unique code, called **chip**. Signals travel with these codes independently, inside the whole bandwidth. The receiver knows in advance the chip code signal it has to receive.

1.8. Switching

Switching is a mechanism by which data/information sent from source towards destination which are not directly connected. Networks have interconnecting devices, which receives data from



directly connected sources, stores data, analyze it and then forwards to the next interconnecting device closest to the destination.

Switching can be categorized as:

CHAPTER TWO

2. COMPUTER NETWORKS

2.1. Introduction to Computer Networks

Network is a system of interconnected computers and computerized peripherals such as printers. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by either **wired** or **wireless** media. A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

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.

2.2. 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

2.3. Classification of Computer Network

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

- Geographical span
- Inter-connectivity
- Administration
- Architecture

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.

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.

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.

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.

2.4. Types Computer Network

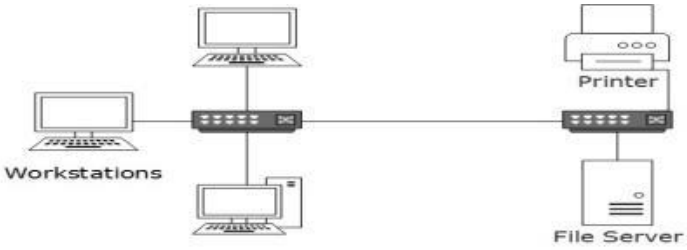
Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the internet itself, covering the whole geographical world.

A. 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.

B. 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.

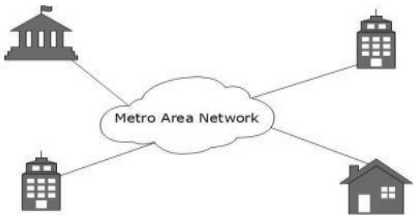


LANs are composed of inexpensive networking and routing equipment. It may contain local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally. LAN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

C. Metropolitan Area Network

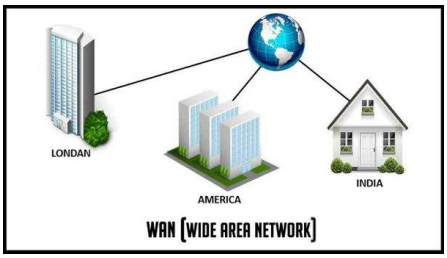
The Metropolitan Area Network (MAN) generally expands throughout a **city** such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI). Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.

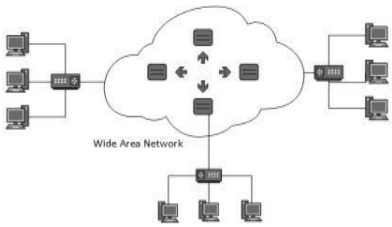


Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.

D. 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.



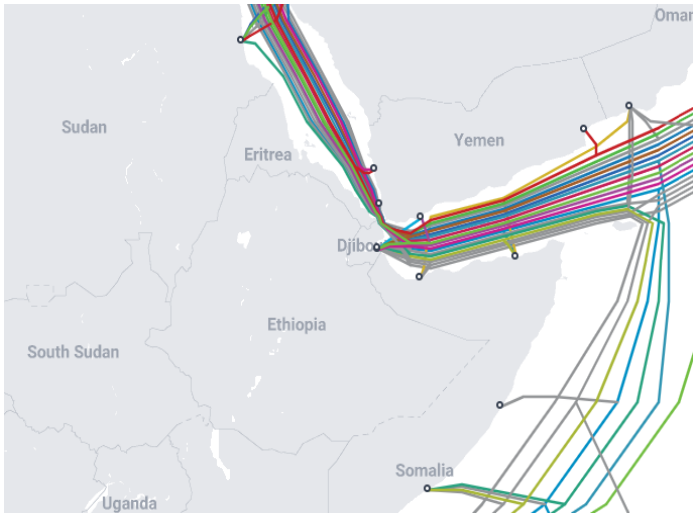


WAN may use advanced technologies such as **Asynchronous Transfer Mode** (ATM), **Frame Relay**, and Synchronous Optical Network (SONET). WAN may be managed by multiple administration.

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** (**subsea**) 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:

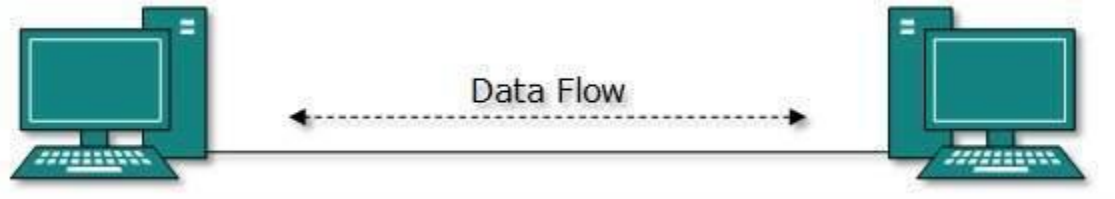
- Web sites
- Marketing
- E-mail
- Networking
- Instant Messaging
- Resource Sharing
- Blogging
- Audio and Video Streaming

2.5. 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.

2.5.1. Point-to-Point

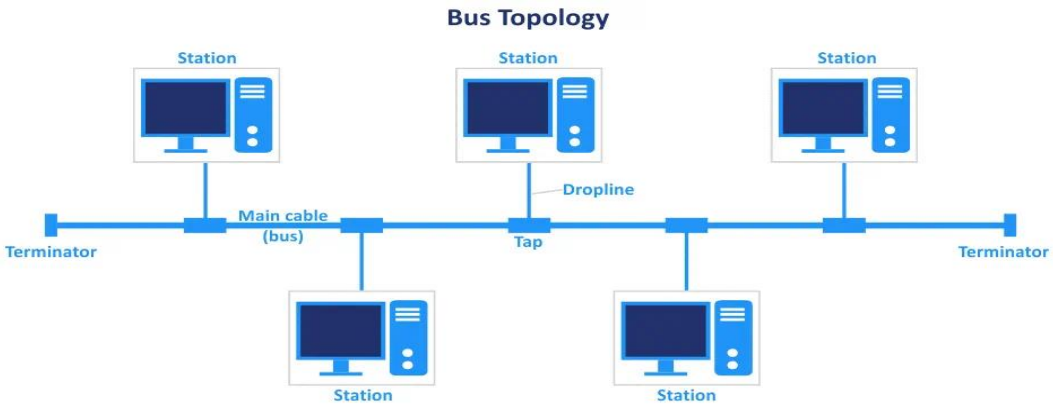
Point-to-point networks contains exactly two hosts such as computer, switches, routers, or servers connected back-to-back using a **single piece of cable**. Often, the receiving end of one host is connected to sending end of the other and vice versa.



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

2.5.2. 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.



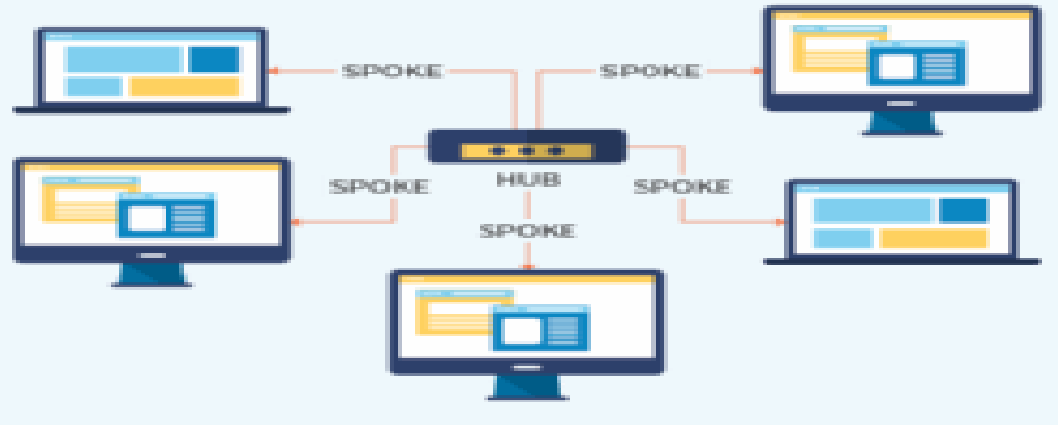
Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

2.5.3. Star Topology

All hosts in Star topology are connected to a **central device**, known as hub device, using a point-to-point connection. That is, there exists a point-to-point connection between hosts and hub. The hub device can be any of the following:

- Layer-1 device such as hub or repeater

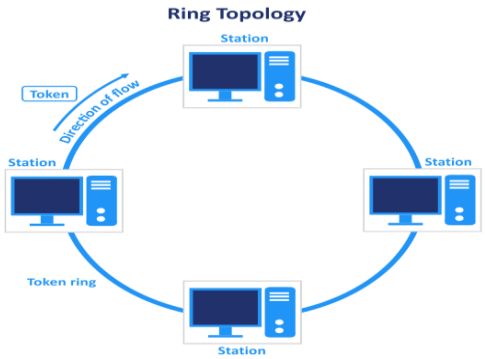
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway



As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts takes place through only the hub. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

2.5.4. Ring Topology

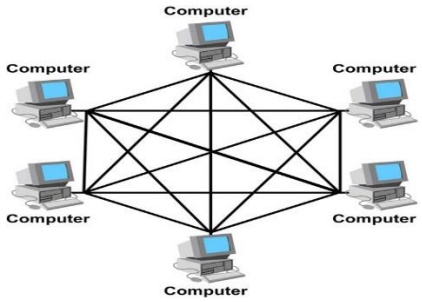
In ring topology, each host machine connects to exactly two other machines, creating a **circular** network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.



Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

2.5.5. Mesh Topology

In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection with few hosts only.

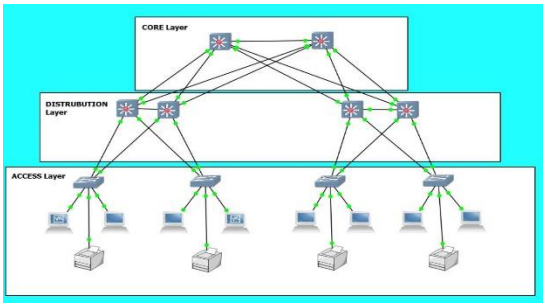


Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

1. **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. Thus, for every new host **n(n-1)/2** connections are required. It provides the most reliable network structure among all network topologies.
2. **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

2.5.6. Tree Topology

Also known as **Hierarchical** Topology, this is the **most common** form of network topology in use presently. This topology imitates as extended Star topology and inherits properties of Bus topology. This topology divides the network into multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is **access-layer** where computers are attached. The middle layer is known as **distribution layer**, which works as mediator between upper layer and lower layer. The highest layer is known as **core layer**, and is central point of the network, i.e. root of the tree from which all nodes fork.



All neighboring hosts have point-to-point connection between them. Similar to the Bus topology, if the root goes down, then the entire network suffers even though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment.

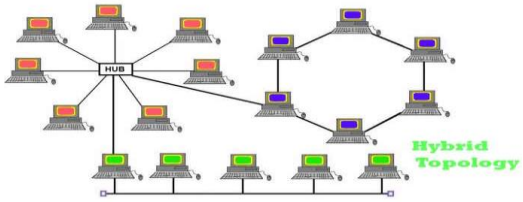
2.5.7. Daisy Chain

This topology connects all the hosts in a **linear** fashion. Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts. Means, if the end hosts in daisy chain are connected then it represents Ring topology.

Each link in daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediate host works as relay for its immediate hosts.

2.5.8. Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.

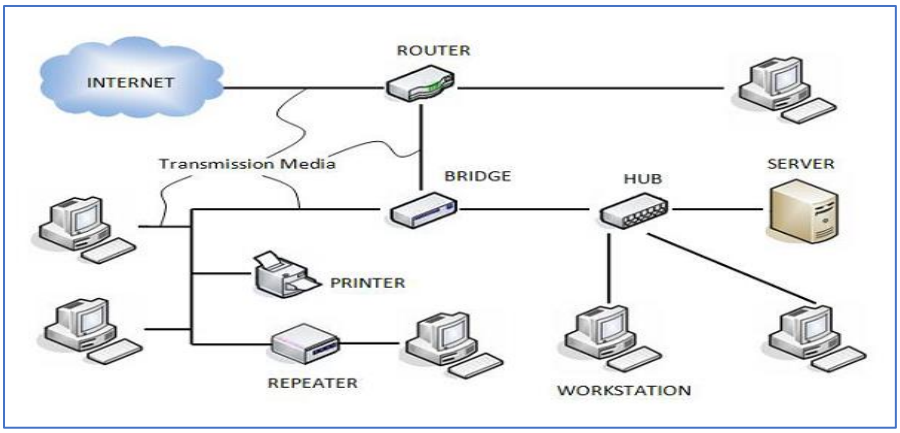


The above picture represents an arbitrarily hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology

2.5.9. 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 –



2.5.10.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
  - Hubs
  - Gateways
  - Bridges
  - Repeaters
  - Switches

2.5.11.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. It gives the server the capability to manage data, users, groups, security, applications, and other networking functions

- **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 −
    a. OSI Model (Open System Interconnections)
    b. TCP / IP Model

CHAPTER THREE

DATA COMMUNICATION AND TRANSMISSION MEDIAS

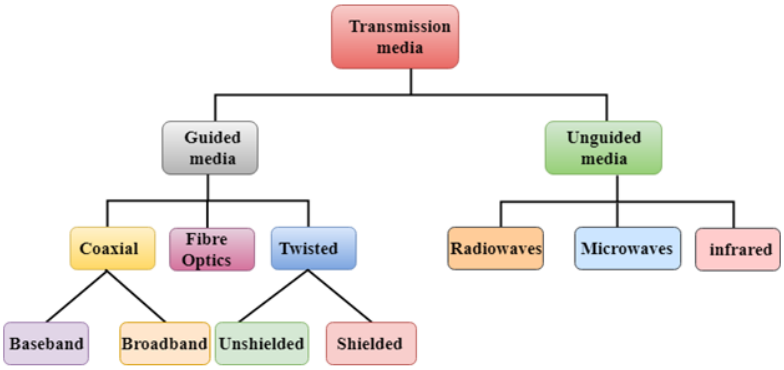
3. What is Transmission Media in data communications

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e., it is the channel through which data is sent from one place to

another. Data is transmitted normally through electrical or electromagnetic signals. An electrical signal is in the form of current. An electromagnetic signal is series of electromagnetic energy pulses at various frequencies. These signals can be transmitted through copper wires, optical fibers, atmosphere, water and vacuum Different Medias have different properties like bandwidth, delay, cost and ease of installation and maintenance. Transmission media is also called Communication channel.

3.1. Type of Transmission Media

Transmission Media is broadly classified into the following types:



Some factors need to be considered for designing the transmission media:

- **Bandwidth**: All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment**: When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference**: An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

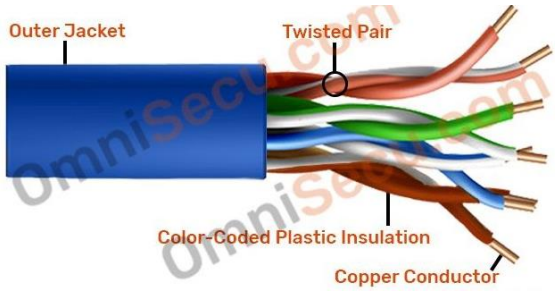
3.1.1. Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media. Bound transmission media are the cables that are tangible or have physical existence and are limited by the physical geography. Popular bound transmission media in use are twisted pair cable, co-axial cable and fiber optical cable. Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost etc.

3.1.1.1. Types Of Guided media:

I. Twisted pair:

Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz. A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair:

a) **Unshielded Twisted Pair**:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **CAT 1 Cables**: are usually used for telephone wiring. It transfers up to 1MBPS of data.
- **CAT2 Cables:** are the second-lowest grade UTP cables used for supporting digital voice and data communication. It transfers up to 4 MBPS of data.
- **CAT 3 Cables:** are third-grade unshielded twisted pair cables used for Token Ring and 10BASE-T Ethernet applications. It transfers up to 10 MBPS of data.
- **CAT 4 Cables:** have four pairs of UTP copper cables used for Token ring networks. It transfers up to 16 MBPS of data.
- **CAT 5 cables:** are used in structured cabling for Ethernet, Token ring, and Fast Ethernet connections. It transfers up to 100 MBPS data.
- **CAT 5e cables:** are very popular and used in Ethernet, Gigabit Ethernet, and Fast Ethernet connections. It transfers up to 1 GBPS data.
- **CAT 6 cables**: are high-grade UTP cables used for Gigabit Ethernet and 10 Ethernet (55m) connections. It transfers up to 10 GBPS data.
- **CAT 6a cables:** are also used for Gigabit Ethernet and 10 Ethernet (55m). It transfers up to 10 GBPS data.

- **CAT 7 cables:** are top graded UTP cables used for Gigabit Ethernet and 10 Ethernet (100m). It transfers nearly 10 GBPS data.

UTP Categories - Copper Cable				
UTP Category	**Data Rate**	**Max. Length**	**Cable Type**	**Application**
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Advantages Of Unshielded Twisted Pair:

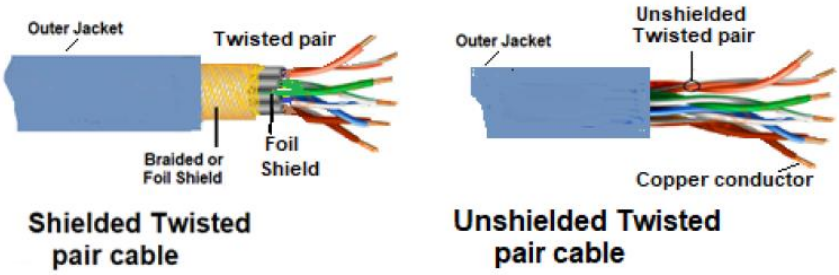
- ♣ It is cheap.
- ♣ Installation of the unshielded twisted pair is easy.
- ♣ It can be used for high-speed LAN.

Disadvantage:

- ♣ This cable can only be used for shorter distances because of attenuation.

b) Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.



Characteristics Of Shielded Twisted Pair:

- ♣ The cost of the shielded twisted pair cable is not very high and not very low.

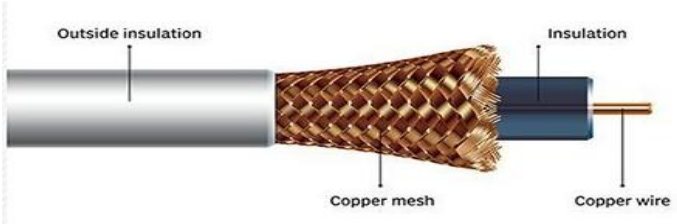
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

II. Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the EMI (Electromagnetic interference).



Coaxial cable is of two types:

- **Baseband transmission**: It is defined as the process of transmitting a single signal at high speed.
- **Broadband transmission**: It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.

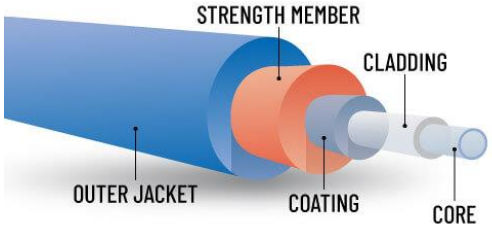
- ♣ It has better shielding as compared to twisted pair cable.
- ♣ It provides higher bandwidth.

Disadvantages Of Coaxial cable:

- ♣ It is more expensive as compared to twisted pair cable.
- ♣ If any fault occurs in the cable causes the failure in the entire network.

III. Fiber Optic

Fiber optic cable is a cable that uses electrical signals for communication. Is a cable that holds the optical fibers coated in plastic that are used to send the data by pulses of light. The plastic coating protects the optical fibers from heat, cold, electromagnetic interference from other types of wiring. Fiber optics provide faster data transmission than copper wires.



Basic elements of Fiber optic cable:

- **Core**: The optical fiber consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fiber. The more the area of the core, the lighter will be transmitted into the fiber.
- **Cladding**: The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fiber.
- **Jacket**: The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fiber strength, absorb shock and extra fiber protection.

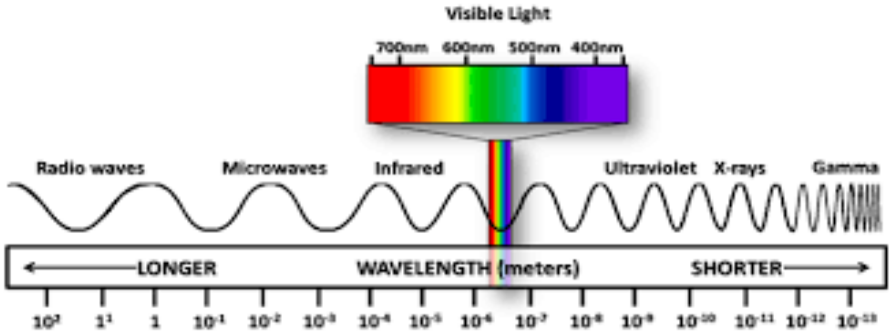
Following are the advantages of fiber optic cable over copper:

- **Greater Bandwidth**: The fiber optic cable provides more bandwidth as compared copper. Therefore, the fiber optic carries more data as compared to copper cable.
- **Faster speed**: Fiber optic cable carries the data in the form of light. This allows the fiber optic cable to carry the signals at a higher speed.
- **Longer distances**: The fiber optic cable carries the data at a longer distance as compared to copper cable.

- **Better reliability**: The fiber optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier**: Fiber optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

3.1.2. Unguided Transmission

An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore, it is also known as **wireless** transmission. In unguided media, **air** is the media through which the electromagnetic energy can flow easily.

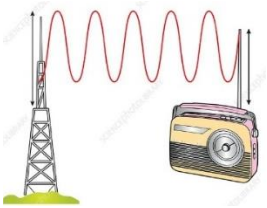


Unguided transmission is broadly classified into three categories:

a. Radio waves

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

- An example of the radio wave is **FM radio**.



Applications Of Radio waves:

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

Advantages Of Radio transmission:

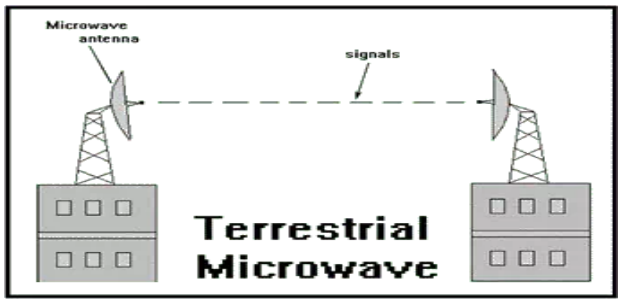
- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

b. Microwaves

Microwaves are of two types:

1. **Terrestrial microwave**
2. **Satellite microwave communication.**

Terrestrial Microwave Transmission



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

Characteristics of Microwave:

- **Frequency range**: The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth**: It supports the bandwidth from 1 to 10 Mbps.
- **Short distance**: It is inexpensive for short distance.
- **Long distance**: It is expensive as it requires a higher tower for a longer distance.

- **Attenuation**: Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

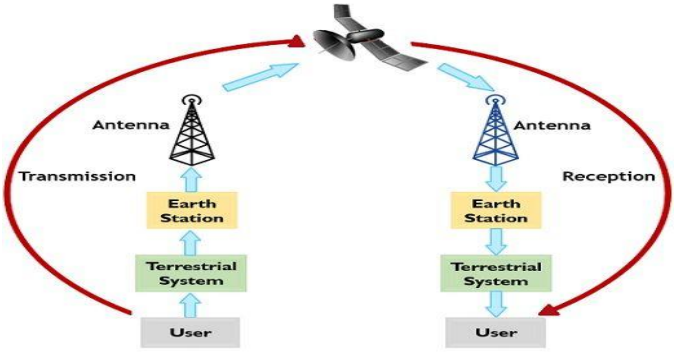
Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- **Eavesdropping**: An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal**: A signal can be moved out of phase by using microwave transmission.
- **Susceptible to weather condition**: A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- **Bandwidth limited**: Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication



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

How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

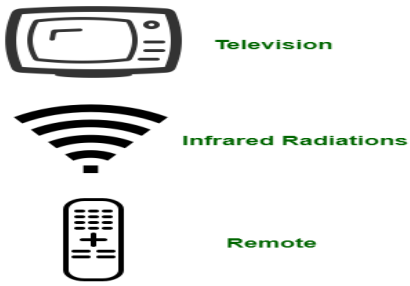
Advantages Of Satellite Microwave Communication:

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

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

c. Infrared



- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.

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

Characteristics Of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

CHAPTER FOUR

LAYERED MODELS

4. Introduction and Overview

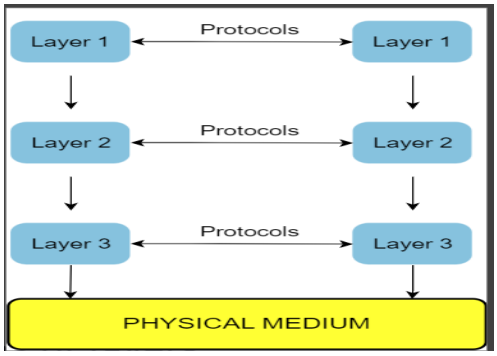
Network engineering is a complicated task, which involves software, firmware, chip level engineering, hardware, and electric pulses. To ease network engineering, the whole networking concept is divided into **multiple layers**. Each layer is involved in some particular tasks and is

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. In networking, layering means to break up the sending of messages into separate components and activities. Each component handles a different part of the communication. This can be referred to as the Transmission Control Protocol/Internet Protocol (TCP/IP) and OSI model.

For smooth data transmission, you need a very organized strategy because, in a network, many users transmit data simultaneously from one to another. An efficient approach is what allows users to send/receive data in an efficient and orderly manner. This strategy is implemented in computer networks, using different architecture and models and **layered architecture** is one of them.

4.1. Layering

The grouping of relevant communication functions into different hierarchical sets is known as layering. Every batch of operations is a separate layer. In layered architecture of Network Model, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work.



In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by the topmost layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and passes on to lower layer. If the task is initiated by lowermost layer, then the reverse path is taken.

4.2. Functions of layers

Each layer is responsible for the following functions:

- Perform a subset of different functions required for communication.

- Provide the services of its functions to the next higher layer in the hierarchy.
- Implementation of communication protocols with peer layers in another system.
- After implementing its operations, it relies on the next layer to perform additional functions.

4.3. Motivation of layering

There are many reasons to use layering in communication, but some of them include:

- Modularity
- Reusability and controllability

Modularity

It decomposes a significant problem into multiple small subproblems that can be managed easily. This gives you more flexibility in designing, modifying, and evolving the computer network. In simple words, it decreases complexity.

Reusability and controllability

It's a standard layering functionality; the lower layer can be shared with many upper layers, increasing the reusability and controllability because of the segmentation of functions. The layering can support incremental modifications easily.

4.4. Layered architecture

The architecture of computer networks uses a layering mechanism in which data transmitted from one defined layer to another for processing is a layered architecture.

There are three major fundamental components of layered architecture:

- **Service**: A collection of functions provided by a layer to a higher layer.
- **Protocol**: A set of rules to share data with the peer layer.
- **Interface**: This is a means of transmitting a message from one layer to another.

4.5. The application of layered architecture

Layered architecture is used for communication. There are two network models which use layering.

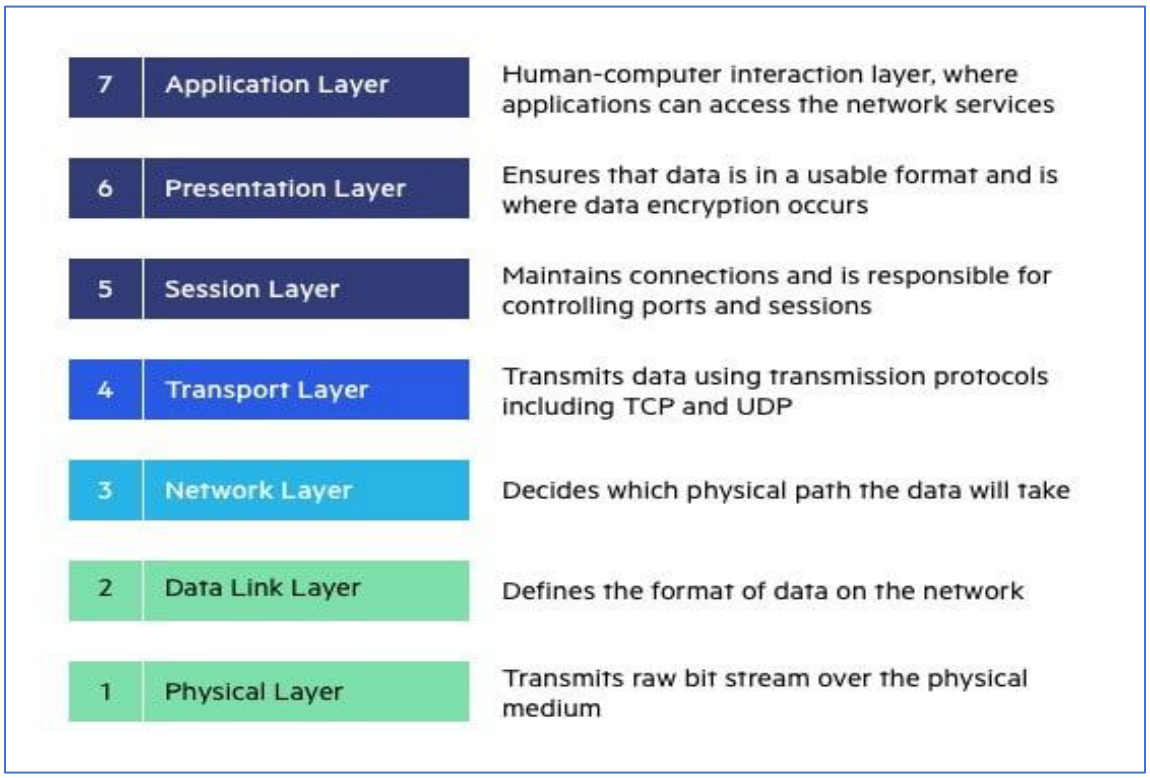
I. **OSI model**

II. **IP/TCP model**

4.5.1. OSI Model

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:



1. Application Layer:

The entire process begins at the end user's device. This can be a phone, laptop, server, etc. The application layer provides the interface for data exchange between the program and the user. For example, Facebook's web application/mobile application is the interface through which we like, share, comment, and perform various other activities. All these activities generate snippets of data that needs to be transmitted across the network.

Application layer functions

- **Transport access and management**

It allows a user to access, retrieve and manage files in a remote computer.

- **Mail services**

It provides the basis for email forwarding and storage facilities.

- **Virtual terminal (TELNET)**

For various reasons, it can be said that the standardization of terminals has completely failed. The OSI solution to this problem is to define a virtual terminal that is really just an abstract data

structure that takes the abstract state of the actual terminal. This abstract data structure can be operated by both the keyboard and the computer and reflects the current state of the data structure on the display. The computer can query this abstract data structure and change this abstract data structure so that the output appears on the screen.

- **Other functions**

In addition to the three functions above, there are some other functions: directory services, remote job entry, graphics, information communication and so on.

Application layer Protocol examples

There are several protocols which work for users in Application Layer. Application. layer protocols can be broadly divided into two categories:

- Protocols which are used by **users**. For example, **e-mail**.
- Protocols which **help** and support protocols used by users. For example, **DNS**.

Few of Application layer protocols are described below:

♣ **DNS (Domain Name System)**

The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Currently, the limit on domain name length is 63 characters, including **www**. And .com or other extensions. Domain names are also restricted to only a subset of ASCII characters, making many other languages unable to properly represent their names and words. Punycode-based IDNA systems, which map Unicode strings to valid DNS character sets, have been validated and adopted by some registries as a workaround. DNS uses **UDP port 53**.

♣ Post Office Protocol (POP)

The Post Office Protocol version 3 (**POP3**) is a simple mail retrieval protocol used by User Agents (client email software) to **retrieve mails from mail server**.

When a client needs to retrieve mails from server, it opens a connection with the server on **TCP port 110**. User can then access his mails and download them to the local computer. POP3 works in two modes. The most common mode, the delete mode, is to delete the emails from remote server after they are downloaded to local machines. The second mode, the keep mode, does not delete the email from mail server and gives the user an option to access mails later on mail server.

- **HTTP (Hypertext Transfer Protocol)**

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, and hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

HTTP is a **client and server-side** standard for request and response (TCP). The client is the end user, the server is the website. Using a web browser, web crawler, or other tools, the client initiates an HTTP request to the specified port on the server. The responding server stores (some) resources, such as HTML files and images. (We call it) This answering server is the origin server. There may be multiple middleware between the user agent and the origin server, such as agents, gateways, or tunnels. Although the TCP / IP protocol is the most popular application on the Internet, the HTTP protocol does not require that it be used and based on the layers it supports. In fact, HTTP can be implemented on any other Internet protocol, or on other networks. HTTP assumes only that the underlying protocol (provided by the underlying protocol) is reliable and that any protocol capable of providing this guarantee can be used by it.

Typically, a request is made by the HTTP client to establish a TCP connection to the server's designated port (**the default is port 80**).

- **FTP (File Transfer Protocol)**

The File Transfer Protocol (FTP) is the most widely used protocol for file transfer over the network. FTP uses TCP/IP for communication and it works on **TCP port 21**. FTP works on Client/Server Model where a client requests file from Server and server sends requested resource back to the client. FTP uses out-of-band controlling i.e., FTP uses TCP port 20 for exchanging controlling information and the actual data is sent over TCP port 21. The client requests the server for a file. When the server receives a request for a file, it opens a TCP connection for the client and transfers the file. After the transfer is complete, the server closes the connection. For a second file, client requests again and the server reopens a new TCP connection.

- **Simple Mail Transfer Protocol**

The Simple Mail Transfer Protocol (SMTP) is used **to transfer electronic mail** from one user to another. This task is done by means of email client software (User Agents) the user is using. User Agents help the user to type and format the email and store it until internet is available. When an email is submitted to send, the sending process is handled by Message Transfer Agent which is normally comes inbuilt in email client software.

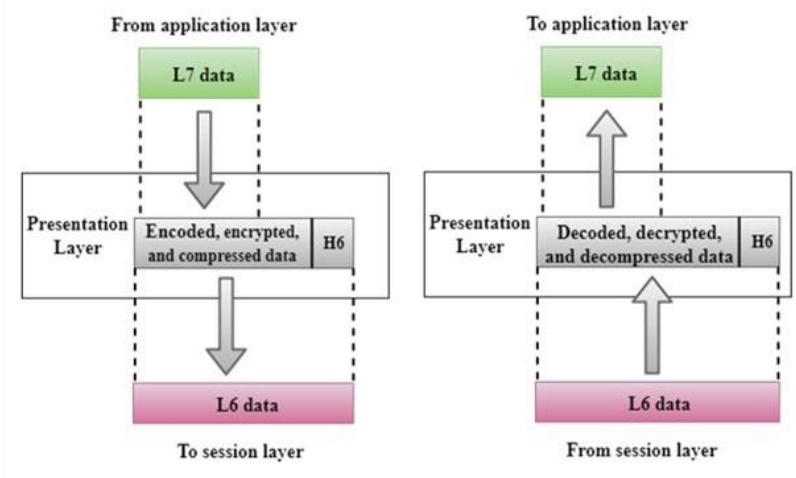
Message Transfer Agent uses SMTP to forward the email to another Message Transfer Agent (Server side). While SMTP is used by end user to only send the emails, the Servers normally use SMTP to send as well as receive emails. **SMTP uses TCP port number 25 and 587**. Client software uses Internet Message Access Protocol (**IMAP**) or **POP** protocols to **receive** emails.

2. Presentation Layer:

The presentation layer ensures the translation of characters from the original format in the host system to the format of the receiving system. This layer takes care of syntax and semantics of messages exchanged in between two communication systems. It also adds encryption and decryption features. Data compression is handled at this layer.

i. The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.

ii. The presentation layer at sending side receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer. At the receiving side, the presentation layer receives data from the session layer decompresses and decrypts the data as required and translates it back as per the encoding scheme used at the receiver.



iii. Translation

The sending and receiving devices may run on different platforms (hardware, software and operating system). Hence it is important that they understand the messages that are used for communicating. Hence a translation service may be required which is provided by the Presentation layers

iv. **Compression**

Data compressed at sender has to be decompressed at the receiving end, both performed by the Presentation layer.

v. Encryption

It is the process of transforming the original message to change its meaning before sending it. The reverse process called **decryption** has to be performed at the receiving end to recover the original message from the encrypted message.

Ex. **Secure socket Layer**

Presentation layer protocols

The following are the **presentation layer protocols**: **XDR, TLS, SSL and MIME**.

What is SSL, TLS and HTTPS?

What is an SSL Certificate?

SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. The two systems can be a server and a client (for example, a shopping website and browser) or server to server (for example, an application with personal identifiable information or with payroll information).

It does this by making sure that any data transferred between users and sites, or between two systems remain **impossible to read**. It uses **encryption algorithms** to scramble data in transit, preventing **hackers** from reading it as it is sent over the connection. This information could be anything sensitive or personal which can include credit card numbers and other financial information, names and addresses.

- **TLS** (Transport Layer Security) is just an updated, **more secure**, version of SSL. We still refer to our security certificates as SSL because it is a more commonly used term, but when you are buying SSL from DigiCert you are actually buying the most up to date TLS certificates with the option of ECC, **RSA** or **DSA** encryption.

- **HTTPS** (Hyper Text Transfer Protocol Secure) appears in the URL when a website is secured by an SSL certificate. The details of the certificate, including the issuing authority and the

corporate name of the website owner, can be viewed by clicking on the lock symbol on the browser bar.

3. Session Layer:

The inclusion of this layer enables maintaining sessions during browsing. This helps with implementing authentication, authorization, synchronization, and dialog control. Let us consider examples to appreciate the significance of the session layer.

- **Authentication**: Once a user logs in, he/she should remain logged in until he/she logs out. Obtaining the status of a user's authentication happens at this layer.
- **Authorization**: Access rights to specific parts of a website are given to super-users and admins.
- **Dialog Control**: Allows various systems running applications like WebEx to communicate. The challenge here is to send and receive data simultaneously, that is overcome by half-duplex or full-duplex protocols under the session layer.
- **Synchronization**: The digital experience relies on audio and video being synchronized. The session layer ensures the timestamps of the audio and video received are in the right order.

The protocols used are: **PPTP, SAP, L2TP and NetBIOS**

4. Transport Layer:

All modules and procedures pertaining to transportation of data or data stream are categorized into this layer. As all other layers, this layer communicates with its peer Transport layer of the remote host. Transport layer offers **peer-to-peer** and **end-to-end connection** between two processes on remote hosts. Transport layer takes data from upper layer (i.e., Application layer) and then breaks it into smaller size **segments**, **numbers** (sequence number) each byte, and hands over to lower layer (Network Layer) for delivery. The transport layer is the fourth layer in the OSI model and enables the following services:

- **Reliability**: This layer ensures that a packet sent is received without corruption. If not, the packet is **resent**. This may add a **delay**. But it is suitable for applications where data integrity is a must.
- **Flow-Control**: The rate of sending information is limited by the buffer size and the receiver capacity. The delays caused due to propagation, queueing, and transmission are taken into account by the flow-control algorithms. It avoids **overwhelming's**.

- **Congestion Control**: In routers, the entry of packets can be decided based on the current traffic.
- **Multiplexing and Demultiplexing**: Before the transport layer, the ports do not play a major role. The ports can be thought of as multiple inputs to the same network channel. The transport Layer enables multiplexing of various application inputs. On the receiving end, the transport layer sends the packets to corresponding ports. This action is similar to that of a demux.

End-to-End Communication

A process on one host identifies its peer host on remote network by means of **TSAPs**, also known as **Port numbers**. TSAPs are very well defined and a process which is trying to communicate with its peer knows this in advance. **For example**, when a DHCP client wants to communicate with remote DHCP server, it always requests on port number **67**. When a DNS client wants to communicate with remote DNS server, it always requests on **port number 53** (UDP)

The two main Transport layer protocols are:

1. Transmission Control Protocol (TCP)

The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is **most widely used protocol** for data transmission in communication network such as **internet**.

- It provides reliable communication between two hosts.
- Connection oriented protocol
- Reliable protocol
- Provide error and flow control

Features Of TCP protocol

- TCP is **reliable** protocol. That is, the receiver always sends either positive or negative **acknowledgement** about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the **same order** it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.

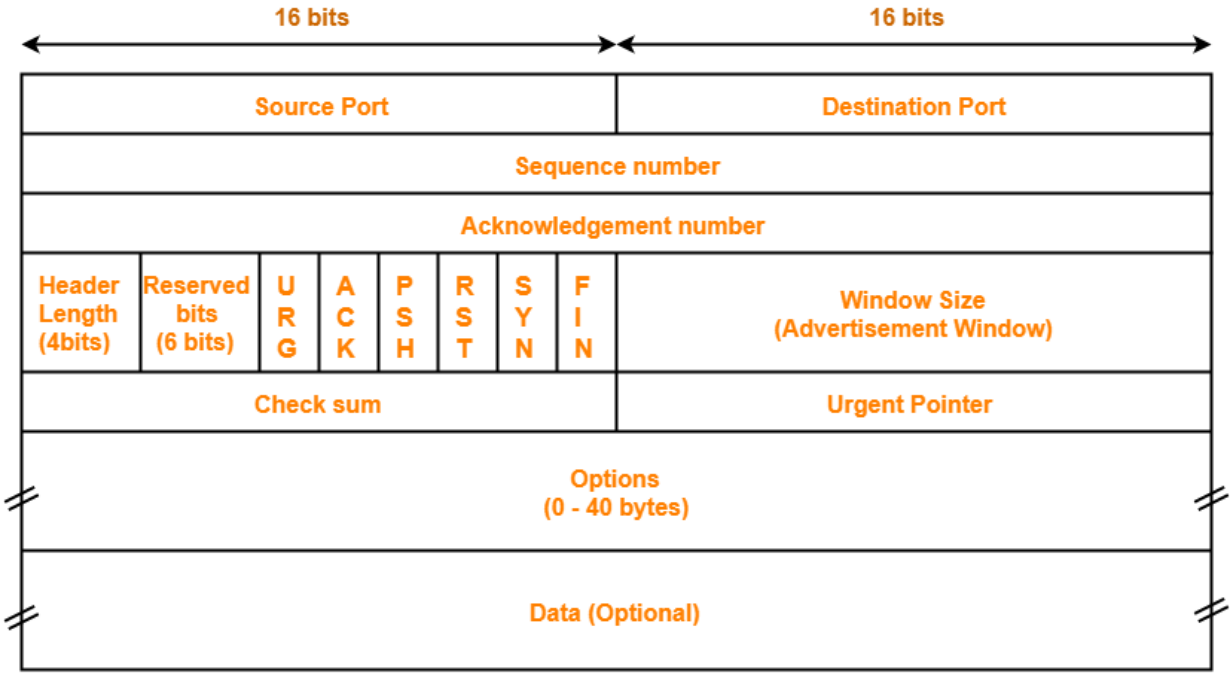
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e., it can perform roles of both receiver and sender

TCP Header

The length of TCP header is minimum 20 bytes and maximum 60 bytes.

TCP segment = TCP header + Data chunk

The following diagram represents the TCP header format-



TCP Header

Addressing in TCP

TCP communication between two remote hosts is done by means of **port numbers (Transport Service Access Point (TSAPs)).** Ports numbers can range from **0 – 65535** which are divided as:

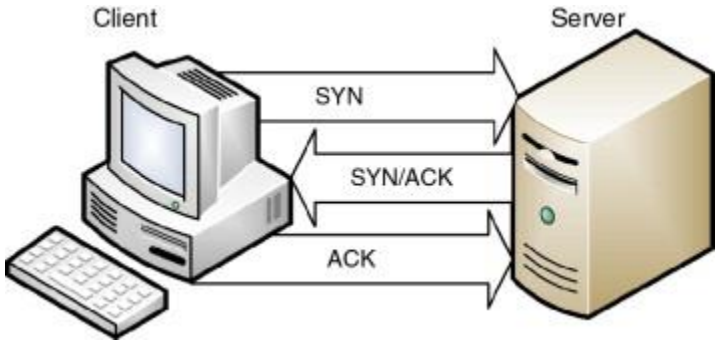
- System Ports (0 – 1023)
- User Ports (1024 – 49151)
- Private/Dynamic Ports (49152 – 65535)

Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. **Three-way handshaking** is used for connection management.

The TCP handshake

TCP uses a three-way handshake to establish a reliable connection. The connection is **full duplex**, and both sides **synchronize** (SYN) and **acknowledge** (ACK) each other. The exchange of these four flags is performed in three steps—**SYN**, **SYN-ACK**, and **ACK**—as shown in Figure



Establishment

Client initiates the connection and sends the segment with a **Sequence number**. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

Release

Either of server and client can send TCP segment with **FIN flag set to 1**. When the receiving end responds it back by **ACKnowledging FIN**, that direction of TCP communication is **closed and connection is released**.

Bandwidth Management

TCP uses the concept of **window size** to accommodate the need of Bandwidth management. Window size tells the sender at the remote end the number of data byte segments the receiver at this end can receive. TCP uses slow **start phase by using window size 1** and **increases the window size exponentially after each successful communication**.

- **For example,** the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received, the windows size is doubled to 4 and next the segment sent will be 4 data bytes long. When the acknowledgement of 4-byte data segment is received, the client sets windows size to 8 and so on.

If an acknowledgement is missed, i.e., data lost in transit network or it received NACK, then the window size is **reduced to half and slow start phase starts again**.

Error Control and Flow Control

TCP uses **port numbers** to know what application process it needs to handover the data segment. Along with that, it uses **sequence numbers to synchronize** itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.

If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the **TCP timestamp** value is compared to make a decision.

Multiplexing

The technique to combine two or more data streams in one session is called **Multiplexing**. When a TCP client initializes a connection with Server, it always refers to a well-defined port number which indicates the application process. The client itself uses a randomly generated port number from private port number pools.

Using TCP Multiplexing, a client can communicate with a number of different application process in a single session.

- For example, a client requests a web page which in turn contains different types of data (HTTP, SMTP, FTP etc.) the TCP session timeout is increased and the session is kept open for longer time so that the three-way handshake overhead can be avoided.

This enables the client system to **receive multiple connection over single virtual connection**. These virtual connections are not good for Servers if the timeout is too long.

Congestion Control

When large amount of data is fed to system which is **not capable of handling** it, congestion occurs. TCP controls congestion by means of **Window mechanism**. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:

- Additive increase, Multiplicative Decrease
- Slow Start
- Timeout React

Crash Recovery

TCP is very **reliable** protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e., when a host receives a packet, it is bound to ACK that packet having the next sequence number expected (if it is not the last segment).

When a TCP Server crashes mid-way communication and re-starts its process, it sends TPDU broadcast to all its hosts. The hosts can then send the last data segment which was never unacknowledged and carry onwards

2. User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be **an unreliable** transport protocol but it uses IP services which provides best effort delivery mechanism. In UDP, the receiver **does not generate an acknowledgement** of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol **unreliable** as well as **easier on processing**.

Requirement of UDP

A question may arise, why do we need an unreliable protocol to transport the data?

TCP proves to be an overhead for certain kinds of applications.

- The Connection Establishment Phase, Connection Termination Phase etc. of TCP are time consuming.
- To avoid this overhead, certain applications which require fast speed and less overhead use UDP.

We deploy UDP where the acknowledgement packets share significant amount of bandwidth along with the actual data.

- For example, in case of video streaming, thousands of packets are forwarded towards its users. Acknowledging all the packets is troublesome and may contain huge amount of bandwidth wastage.

The best delivery mechanism of underlying IP protocol ensures best efforts to deliver its packets, but even if some packets in video streaming get lost, the impact is not catastrophic and can be ignored easily. Loss of few packets in video and voice traffic sometimes goes unnoticed.

Features

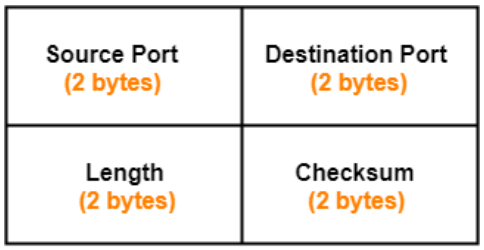
- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for **data flowing in one direction**. **Not fullduplex**
- UDP is simple and suitable for query-based communications.
- UDP is not connection oriented.

- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

UDP Header

UDP header is as simple as its function.

The following diagram represents the UDP Header Format-



UDP Header

Applications Using UDP-

Following applications use UDP-

- Applications which require one response for one request use UDP. Example- DNS.
- Routing Protocols like RIP and OSPF use UDP because they have very small amount of data to be transmitted.
- Trivial File Transfer Protocol (TFTP) uses UDP to send very small sized files.
- Broadcasting and multicasting applications use UDP.
- Streaming applications like multimedia, video conferencing etc. use UDP since they require speed over reliability.
- Real time applications like chatting and online games use UDP.
- Management protocols like SNMP (Simple Network Management Protocol) use UDP.
- Bootp / DHCP uses UDP.
- Other protocols that use UDP are- Kerberos, Network Time Protocol (NTP), Network News Protocol (NNP), Quote of the day protocol etc.

Disadvantages

- UDP delivers basic functions required for the end-to-end transmission of data.
- It does not use any sequencing and does not identify the damaged packet while reporting an error.

- UDP can identify that an error has happened, but UDP does not identify which packet has been lost.

3. Network Layer:

Layer-3 in the OSI model is called Network layer. Network layer manages options pertaining to host and network **addressing**, **managing sub-networks**, and **internetworking**. Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

Layer-3 Functionalities

Devices which work on Network Layer mainly focus on routing. Routing may include various tasks aimed to achieve a single goal. These can be:

- Addressing devices and networks.
- Populating routing tables or static routes.
- Queuing incoming and outgoing data and then forwarding them according to
- quality of service constraints set for those packets.
- Internetworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provides connection oriented and connection less mechanism.

Network Layer Features

With its standard functionalities, Layer 3 can provide various features as:

- Quality of service management
- Load balancing and link management
- Security
- Interrelation of different protocols and subnets with different schema.
- Different logical network design over the physical network design.
- L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

The Network Layer uses four basic processes…

1) Addressing end devices
2) Encapsulation
3) Routing
4) De-encapsulation

The network layer is one of the most important layers. It enables many features such as:

- **Address Assignment**: IP addresses are assigned to the host. There are two ways of assigning addresses: Static and Dynamic. Static addresses are assigned manually and do not change under any circumstances. Dynamic IP's, on the other hand, are assigned on an as-needed basis.
- **Routing**: Selecting the route can be done manually or automatically. Today, most of it is automatic. There are two predominant algorithms used for routing: Distance Vector Routing and Link State Routing.
- **Fragmentation**: Within the transport layer, there is a constraint on the maximum allowable size for data. Therefore, bits are segmented accordingly in the transport layer. Fragmentation is the same process applied to the segmented packets received from the transport layer. The aim is to accommodate datagrams received from the transport layer into frames.

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

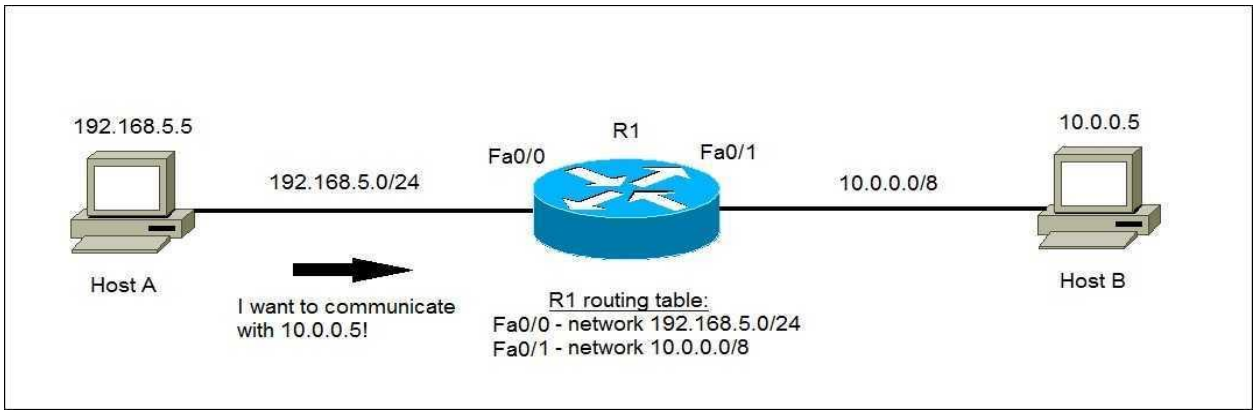
We are discussing IP here as it is the only one, we use in practice these days.

There are several network layer protocols in existence; however, only the following two are commonly implemented as show in the figure:

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)

Internet protocol is widely respected and deployed Network Layer protocol which helps to communicate end to end devices over the internet. It comes in two flavors. **IPv4** which has ruled the world for **decades but now is running out of address space**. **IPv6** is created to replace IPv4 and hopefully mitigates limitations of IPv4 too.

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.

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.

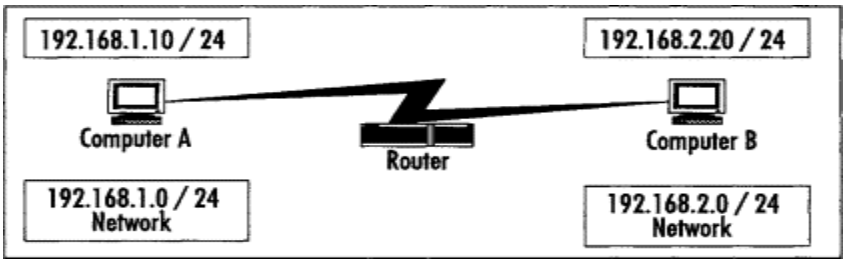
A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple paths existing to reach the same destination, router can make decision based on the following information:

- Hop Count
- Bandwidth
- Metric
- Prefix-length
- Delay

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

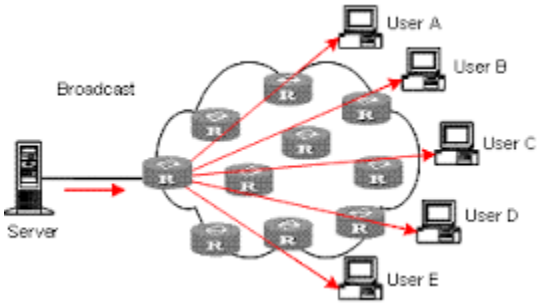
Unicast routing

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.



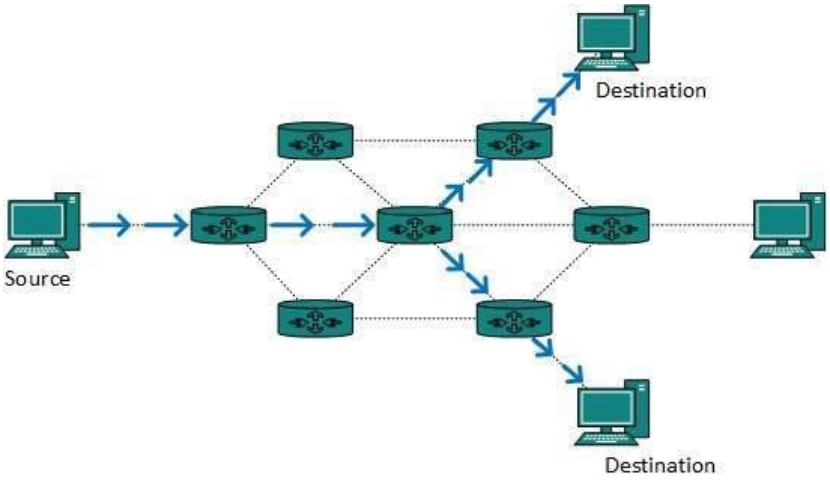
Broadcast routing

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.



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 loop

Unicast Routing Protocols

There are two kinds of routing protocols available to route unicast packets:

1) **Distance Vector Routing Protocol**

Distance Vector is simple routing protocol which takes routing decision on the **number of hops between source and destination**. A route with **a smaller** number of hops is considered as the best route. Every router advertises its set best routes to other routers. Ultimately, all routers build up their network topology based on the advertisements of their peer routers,

- for example, Routing Information Protocol (**RIP**).

2) **Link State Routing Protocol**

Link State protocol is slightly complicated protocol than Distance Vector. It takes into account the states of links of all the routers in a network. This technique helps routes build a common graph of the entire network. All routers then calculate their best path for routing purposes,

- for example, Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS).

Multicast Routing Protocols

Unicast routing protocols use graphs while Multicast routing protocols use trees, i.e. spanning tree to avoid loops. The optimal tree is called shortest path spanning tree.

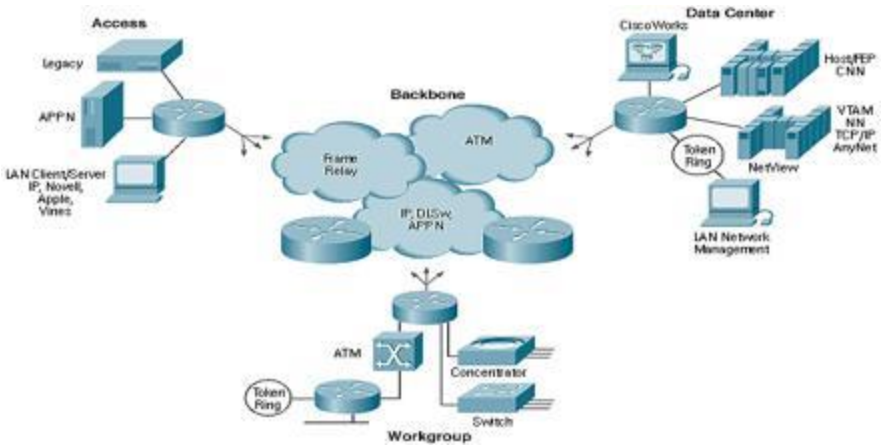
Internetworking

In real world scenario, networks under same administration are generally scattered geographically. There may exist requirement of **connecting two different networks** of same kind as well as of different kinds. Routing between two networks is called **internetworking**.

Networks can be considered different based on various parameters such as, **Protocol**, **topology**, **Layer-2 network** and **addressing scheme**.

In internetworking, routers have knowledge of each other's address and addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol.

- **Routing protocols** which are used within an organization or administration are called **Interior Gateway Protocols** or IGP. **RIP**, **OSPF** are examples of IGP. Routing between different organizations or administrations may have Exterior Gateway Protocol, and there is only one EGP i.e., Border Gateway Protocol



Packet Fragmentation

Most Ethernet segments have their maximum transmission unit (MTU) fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software **capabilities** which tell what amount of data that device can handle and what size of packet it can process.

- If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally.
- If the packet is larger, it is broken into smaller pieces and then forwarded. This is called **packet fragmentation**. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is **assembled** again.

If a packet with DF (do not fragment) bit set to 1 comes to a router which cannot handle the packet because of its length, the packet is dropped.

When a packet is received by a router has its MF (more fragments) bit set to 1, the router then knows that it is a fragmented packet and parts of the original packet is on the way.

If packet is fragmented too small, the overhead is increases. If the packet is fragmented too large, intermediate router may not be able to process it and it might get dropped.

Network Layer Protocols

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.

- **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.

- **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.

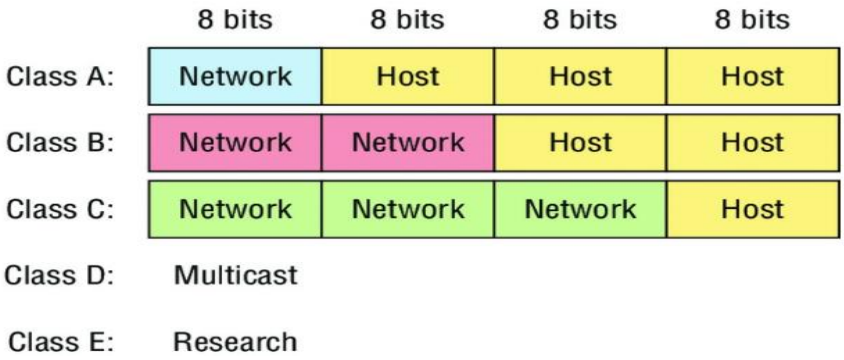
ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.

- **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.

❖ 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

6. Data Link Layer:

Data Link Layer is **second** layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between **two hosts** which are directly connected in some sense. This direct connection could be **point to point or broadcast**. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in **the form of electrical signals**, assembles them in a recognizable **frame format**, and hands over to upper layer.

Data link layer has two sub-layers:

- **Logical Link Control (LLC)**: It deals with protocols, flow-control, and error control
- **Media Access Control (MAC)**: It deals with actual control of media

1. ***Logical Link Control (LLC) or Data Link Control (DLC) Sublayer:*** LLC or DLC is the topmost layer of the data link layer. It deals with the communication between the lower layers and upper layers. This sublayer runs above the data link layer and provides flow control and error information. It is responsible for **assigning the frame sequence** number. It specifies the mechanism that can be used to address stations on a transmission medium and to control the data exchanged between the sender and the receiver.
2. ***Media Access Control (MAC) Sublayer:*** The bottom sublayer of the Data Link Layer is the Media Access Control. It is also known as Medium Access Control. It provides **multiplexing** and **flow control** for the transmission media. The main responsibility of this

sublayer is to encapsulate the frame, check for transmission errors, and then allow the frame to be forwarded to the upper layer. It determines who is permitted to access the media at any given time.

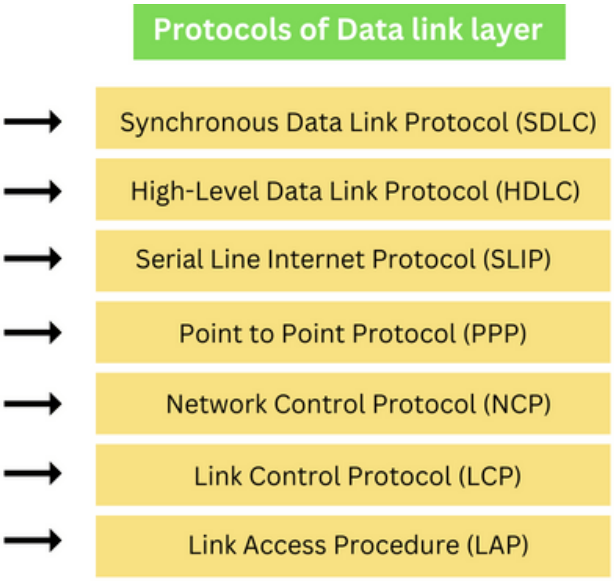
Functions of Data link layer:

1. ***Hop to Hop or Node to Node delivery of data:*** The responsibility of the Data Link Layer (DLL) is to provide hop-to-hop delivery of data. The data link layer determines the node to which the data should be sent first, then the following node the data should be sent to, and so on, till the information arrives at the destination system.
2. ***Framing:*** It is a process of encapsulating data packets obtained from the network layer into frames for transmission. Each frame consists of a header, a payload field, and a trailer. The header contains the frame start bits, the address of both the source and destination, the type of data, and quality control bits. The payload field contains the data packet. The trailer contains error detection bits, error correction bits, and frame stop bits.
3. ***Physical addressing:*** The Data Link Layer attaches the physical addresses of the receiver and sender to the header of each frame. To send information from source to destination, you must know what we are sending and where we are sending it.
4. ***Error control:*** During transmission, the frame can get corrupted by any cause. The error can be controlled in the data link layer in three phases of error control as follows:
    - ***Error detection:*** The error in the data frame is detected with the help of error detection bits present in the frame trailer.
    - ***Acknowledgment:*** After receiving the data frame, the receiver responds to inform the sender about the successful delivery of the data frame. This acknowledgment can be positive or negative. If the data frame is received successfully, it sends positive feedback to the sender; otherwise, it sends negative feedback to the sender.
    - ***Retransmission:*** If the receiver successfully receives the data frame, the sender sends the next set of data frames, but if the data frame does not reach the receiver successfully, the sender must resend the data frames.
5. ***Flow Control:*** The receiver should be able to receive the data frame at the same speed at which the sender is sending the data frame, i.e., both the sender and the receiver should work at the same speed. If the sender sends frames with high speed and the receiver receives frames with low speed, the sender will be overloaded, resulting in loss of data.

Data loss can be handled with the help of two mechanisms:

- ***Stop and wait:*** The sender should wait until the acknowledgment is received from the receiver for frame-1. The sender will wait for the response of the receiver, and then it will send the next data frame.
- ***Sliding Window:*** Here, instead of sending acknowledgment after each frame, the sender sends acknowledgment after some set of frames.

Protocols of Data link layer:



- ***Synchronous Data Link Protocol (SDLC):*** It is the first bit-oriented protocol and is widely used. It is a subset of the High-Level Data Link Protocol. IBM developed this protocol in 1975. It manages synchronous serially transmitted bits over a data link layer.
- ***High-Level Data Link Protocol (HDLC):*** It is a bit-oriented protocol for conveying data on point-to-multipoint and point-to-point links. The International Organization for Standardization (ISO) developed this protocol in 1979. It is based on Synchronous Data Link Protocol. It provides connectionless and connection-oriented services. It provides two transmission modes: Asynchronous Balanced Mode (ABM) and Normal Feedback Mode (NRM).
- ***Serial Line Internet Protocol (SLIP):*** It is a simple internet protocol through which the user is allowed to access the internet with the help of a computer modem. Rick Adams developed this protocol in 1984. It works with TCP/IP for communication over the router and serial port.

- ***Point to Point Protocol (PPP):*** It is a character-oriented or byte-oriented protocol. PPP is a WAN protocol that runs over an Internet link. It is used in broadband communication. It is used to transmit multiprotocol data between point-to-point devices. It provides transmission encryption, loop connection authentication, and compression of data.
- ***Network Control Protocol (NCP):*** This layer was implemented by ARPANET. It allows transferring data between two devices. It is a part of the point-to-point protocol. This network layer will carry the data packets from the origin to the goal.
- ***Link Control Protocol (LCP):*** This layer is also a component of the point-to-point protocol. It is mainly used for establishing and maintaining the link before sending data.
- ***Link Access Procedure (LAP):*** It is derived from the high-level data link protocol. It is used for framing and data transmission over point-to-point links. It has several Link Access Protocols, such as Multilink Procedure (MLP), Link Access Procedure for Modems (LAPM), Link Access Procedure for Half-Duplex (LAPX), and Link Access Procedure for Frame Relay (LAPF).

7.Physical Layer:

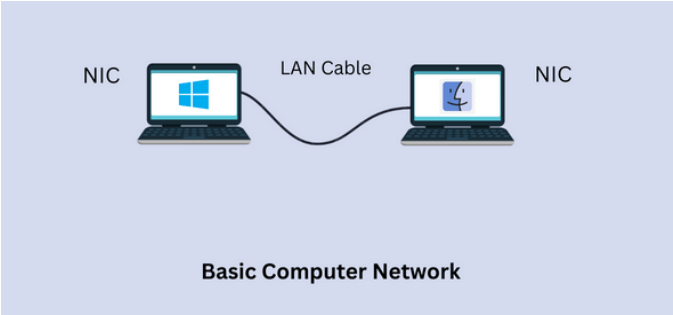
Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations. This layer defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.

Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data. The binary data is then sent over the wired or wireless media

This layer deals with electrical, mechanical, functional, and procedural characteristics of physical links. Network topology comes under this layer. One prominent aspect of the physical layer is **encoding**. Encoding refers to the representation of data. The objective of encoding is to ensure the maximum probability that the message, being transmitted is sent without any errors. There are different types of encoding available. They differ in the way the 0's and 1's is represented. Basic representation is -5V signal for 0 and +5V signal for 1. The probability of error is high, and therefore various other schemes are required.

The OSI model is the abbreviation for Open Systems Interconnection Model. It defines the transmission of data from one system to another in a computer network. For example, in the most elemental form, two systems are joined to each other using Local Area Network (LAN) cables and

share data with the help of a Network Interface Card (NIC) that allows communication over a network, but if one system is based on Microsoft Windows, and the other is based on macOS, so how would these computers communicate with each other. To successfully communicate between systems of distinct architectures, the International Organization for Standardization (ISO) presented the 7-layered OSI model in 1984.



The physical layer converts the data frame received from the data link layer into bits, i.e., in terms of ones and zeros. It maintains the data quality by implementing the required protocols on different network modes and maintaining the bit rate through data transfer using a wired or wireless medium.

Attributes of the physical layer:

The physical layer has several attributes that are implemented in the OSI model:

1. Signals: The data is first converted to a signal for efficient data transmission. There are two kinds of signals:

- ***Analog Signals:*** These signals are continuous waveforms in nature and are represented by continuous electromagnetic waves for the transmission of data.
    - ***Digital Signals:*** These signals are discrete in nature and represent network pulses and digital data from the upper layers.

2. Transmission media: Data is carried from source to destination with the help of transmission media. There are two sorts of transmission media:

- ***Wired Media:*** The connection is established with the help of cables. For example, fiber optic cables, coaxial cables, and twisted pair cables.
- ***Wireless Media:*** The connection is established using a wireless communication network. For example, Wi-Fi, Bluetooth, etc.

3. Data Flow: It describes the rate of data flow and the transmission time frame. The factors affecting the data flow are as follows:

- ***Encoding:*** Encoding data for transmission on the channel.

- ***Error-Rate:*** Receiving erroneous data due to noise in transmission.
- ***Bandwidth:*** The rate of transmission of data in the channel.

4. Transmission mode: It describes the direction of the data flow. Data can be transmitted in three sorts of transmission modes as follows:

- ***Simplex mode:*** This mode of communication is a one-way communication where a device can only send data. Examples are a mouse, keyboard, etc.
- ***Half-duplex mode:*** This mode of communication supports one-way communication, i.e., either data can be transmitted or received. An example is a walkie-talkie.
- ***Full-duplex mode:*** This mode of communication supports two-way communication, i.e., the device can send and receive data at the same time. An example is cellular communication.

5. Noise in transmission: Transmitted data can get corrupted or damaged during data transmission due to many reasons. Some of the reasons are mentioned below:

- ***Attenuation:*** It is a gradual deterioration of the network signal on the communication channel.
- ***Dispersion:*** In the case of Dispersion, the data is dispersed and overlapped during transmission, which leads to the loss of the original data.
- ***Data Delay:*** The transmitted data reaches the destination system outside the specified frame time.

4.5.2. Encapsulation:

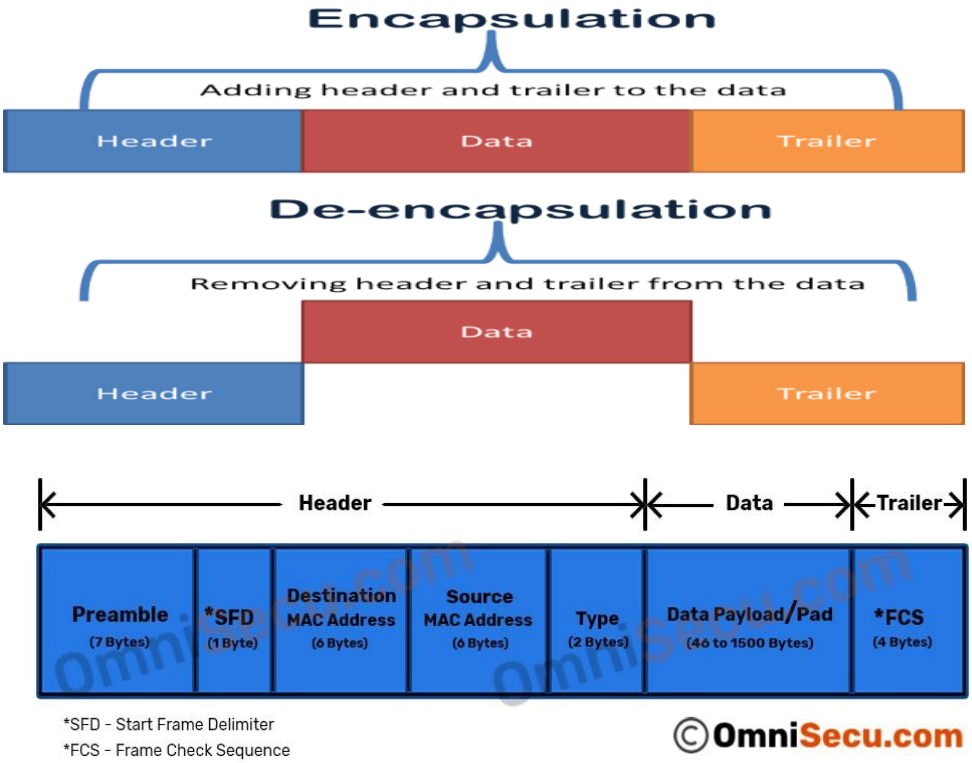
Encapsulation refers to attaching new information in the Application Layer data as it is passed onto next layers in the OSI and TCP/IP model. This additional information basically divided into two parts, Header and Trailer. These are elements attached in order to make the transmission smoother, on each layer a PDU (Protocol Data Unit) is generated.

Data Encapsulation is the process in which some extra information is added to the data item to add some features to it. We use either the OSI or the TCP/IP model in our network, and the data transmission takes place through various layers in these models. Data encapsulation adds the protocol information to the data so that data transmission can take place in a proper way. This information can either be added in the header or the footer of the data.

The data is encapsulated on the sender's side, starting from the application layer to the physical layer. Each layer takes the encapsulated data from the previous layer and adds some more

information to encapsulate it and some more functionalities with the data. These functionalities may include proper data sequencing, error detection and control, flow control, congestion control, routing information, etc

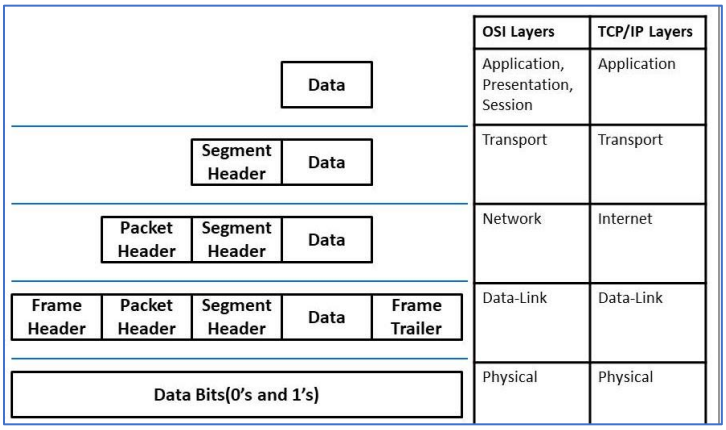
Decapsulation refers to the removal of all these additional information and extraction of originally existing data, and this process continues till the last layer i.e., the Application Layer. This process removes, fragments of distinct information in each layer as it approaches that layer. Here is the pictorial representation of the whole process.



Actually, we use different terms for the encapsulated form of the data that is described in the below-mentioned diagram

OSI Layers	TCP/IP Layers	Encapsulated Term
Application	Application	Data
Presentation		Data
Session		Data
Transport	Transport	Segment
Network	Internet	Packet
Data-Link	Data-Link	Frame
Physical	Physical	Bits

Now, we will see the whole process of encapsulation and de-encapsulation in the OSI and TCP/IP model step-by-step as mentioned in the below picture

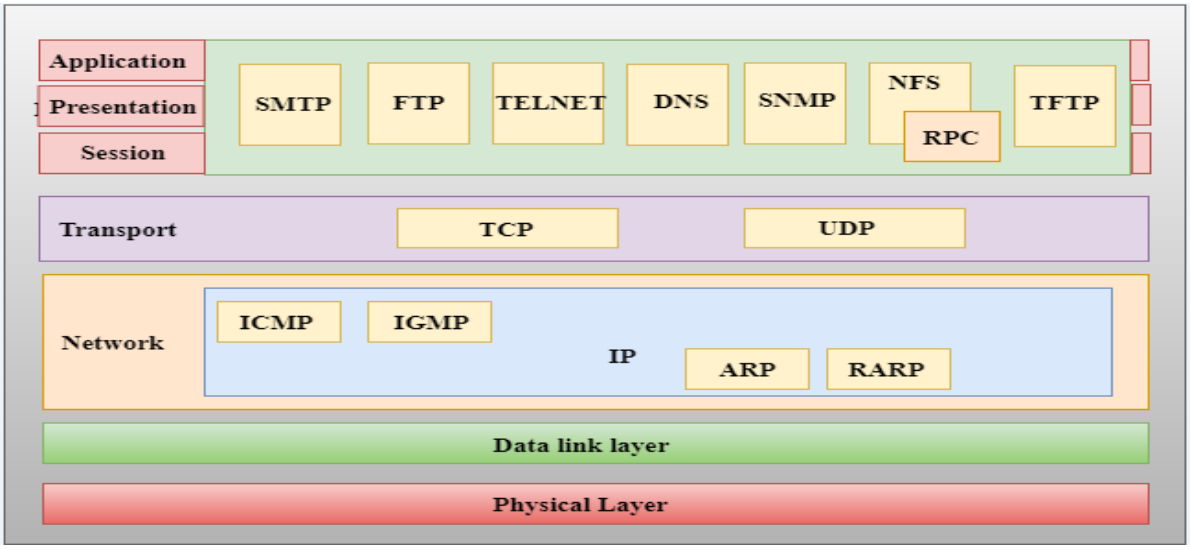


4.5.3. TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of **five layers**: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:



- **Network Access Layer**
  - A network layer is the lowest layer of the TCP/IP model.
  - A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
  - It defines how the data should be sent physically through the network.
  - This layer is mainly responsible for the transmission of the data between two devices on the same network.
  - The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
  - The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.
- **Internet Layer**
  - An internet layer is the second layer of the TCP/IP model.
  - An internet layer is also known as the network layer.
  - The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
    - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
    - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.

- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:
  - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
  - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

♣ **Transport Layer**

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

- **User Datagram Protocol (UDP)**
  - It provides connectionless service and end-to-end delivery of transmission.
  - It is an unreliable protocol as it discovers the errors but not specify the error.
  - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
  - **UDP consists of the following fields:**

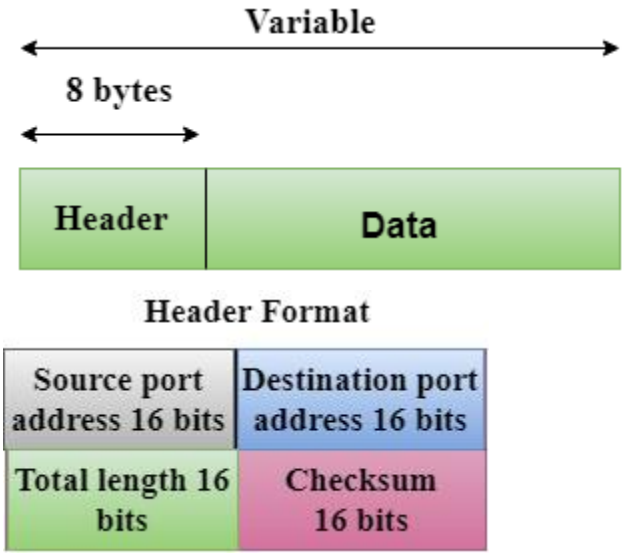
    Source port address: The source port address is the address of the application program that has created the message.

    Destination port address: The destination port address is the address of the application program that receives the message.

Total length: It defines the total number of bytes of the user datagram in bytes.

Checksum: The checksum is a 16-bit field used in error detection.

- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

♣ **Application Layer**

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.

- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer

CHAPTER 5

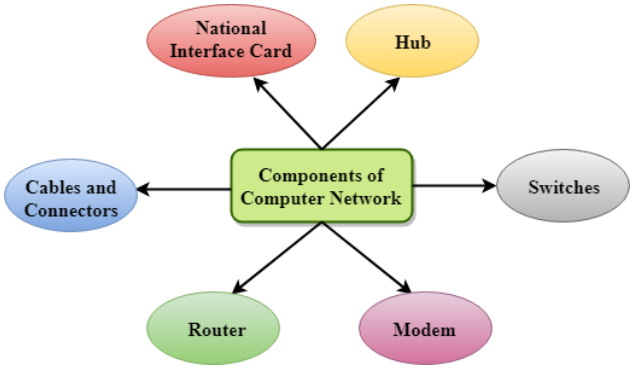
5. COMPONENTS OF COMPUTER NETWORK

5.1. What is a Computer Network?

Computer Network is a group of computers connected with each other through wires, optical fibers or optical links so that various devices can interact with each other through a network.

The aim of the computer network is the sharing of resources among various devices. In the case of computer network technology, there are several types of networks that vary from simple to complex level.

5.2. Components Of Computer Network:



Major components of a computer network are:

- **NIC (National interface card)**

NIC is a device that helps the computer to communicate with another device. The network interface card contains the hardware addresses, the data-link layer protocol use this address to identify the system on the network so that it transfers the data to the correct destination.

There are two types of NIC: wireless NIC and wired NIC.

- **Wireless NIC:** All the modern laptops use the wireless NIC. In Wireless NIC, a connection is made using the antenna that employs the **radio wave technology**.
- **Wired NIC:** Cables use the **wired NIC** to transfer the data over the medium.

- **Hub**

Hub is a central device that splits the network connection into multiple devices. When computer requests for information from a computer, it sends the request to the Hub. Hub distributes this request to all the interconnected computers.

- **Switches**

Switch is a networking device that groups all the devices over the network to transfer the data to another device. A switch is better than Hub as it does not broadcast the message over the network, i.e., it sends the message to the device for which it belongs to. Therefore, we can say that switch sends the message directly from source to the destination.

- **Cables and connectors**

Cable is a transmission media that transmits the communication signals. **There are three types of cables:**

- ✓ **Twisted pair cable:** It is a high-speed cable that transmits the data over **1Gbps** or more.
- ✓ **Coaxial cable:** Coaxial cable resembles like a TV installation cable. Coaxial cable is more expensive than twisted pair cable, but it provides the high data transmission speed.
- ✓ **Fiber optic cable:** Fiber optic cable is a high-speed cable that transmits the data using light beams. It provides high data transmission speed as compared to other cables. It is more expensive as compared to other cables, so it is installed at the government level.

- **Router**

Router is a device that connects the LAN to the internet. The router is mainly used to connect the distinct networks or connect the internet to multiple computers.

- **Modem**

Modem connects the computer to the internet over the existing telephone line. A modem is not integrated with the computer motherboard. A modem is a separate part on the PC slot found on the motherboard.

5.3. Uses Of Computer Network

- **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
- **Server-Client model:** Computer networking is used in the **server-client model**. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.

- **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.
- **E-commerce:** Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

5.4. Features Of Computer network

A list Of Computer network features is given below.

- Communication speed
- File sharing
- Back up and roll back is easy
- Software and Hardware sharing
- Security
- Scalability
- Reliability
- Communication speed

Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.

File sharing

File sharing is one of the major advantages of the computer network. Computer network provides us to share the files with each other.

Back up and roll back is easy

Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

Software and Hardware sharing

We can install the applications on the main server; therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.

Security

Network allows the security by ensuring that the user has the right to access the certain files and applications.

Scalability

Scalability means that we can add the new components on the network. Network must be scalable so that we can extend the network by adding new devices. But it decreases the speed of the connection and data of the transmission speed also decreases, this increases the chances of error occurring. This problem can be overcome by using the routing or switching devices.

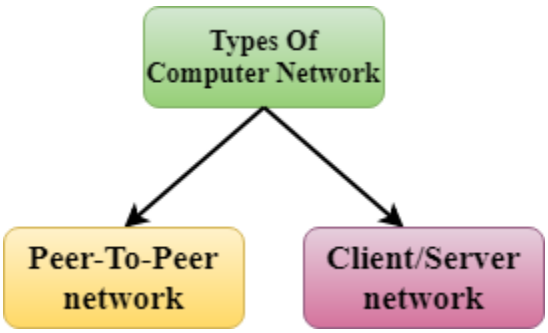
Reliability

Computer network can use the alternative source for the data communication in case of any hardware failure.

5.5. Computer Network Architecture

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

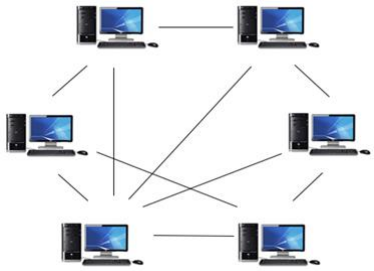
The two types of network architectures are used:



1) Peer-To-Peer network
2) Client/Server network

Peer-To-Peer network

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



Advantages Of Peer-To-Peer Network:

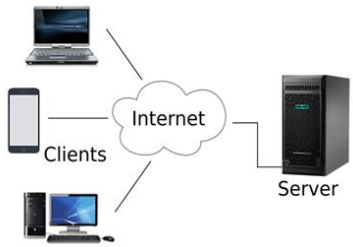
- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

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

Client/Server Network

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



Advantages Of Client/Server network:

- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages Of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

5.6. Internet Standards and RFCs

Internet Standards refer to all the documented requirements both in technology as well as methodology pertaining to the Internet. An internet standard (STD) is a specification that has been approved by the Internet Engineering Task Force (IETF). Such standard helps to promote a consistent and universal use of the internet world wide.

Internet Standardization Process

Working groups present their work of the Internet are published as **RFC** (Request for Comments). RFCs are the basis for Internet standards. Not all RFCs become Internet Standards! (There are >3000 RFCs and less than 70 Internet standards

A typical (but not only) way of standardization is:

- Internet Drafts
- RFC
- Proposed Standard
- Draft Standard (requires 2 working implementation)
- Internet Standard (declared by IAB)

The standardization process has **three steps**. The documentation laid down in a step is called the **maturity level**. There were previously three maturity levels but are merged to form only two maturity levels now which are:

- **Proposed Standard**: These are the standards that are ready for implementation. However, they can be revised according to circumstances of deployment.
- **Draft Standard**: When a Proposed Standard has been meticulously tested by at least two sites for at least 4 months, they are considered as Draft Standard. Draft Standard has been merged with Internet standard to form the future Internet standard.
- **Internet Standard**: These are technically matured standards that define the protocols and formats of messages. The fundamental standards are those which form the Internet Protocol (IP).

The organizations of Internet Standards

Who is Who on the Internet?

1. **Internet Engineering Task Force (IETF)**

IETF formulates, publishes and regulates Internet Standards, particularly those related to TCP/IP. The organization is open standard, with no formal memberships. Development of IETF standards is open to all. Any interested person can participate for their development. IETF documents are free and easily available over the Internet. IETF specifications are on individual protocols that may be used in different systems.

2. **Internet Society (ISOC)**

ISOC was founded in the US in 1992 as a non-profit organization to provide support on technical development of the Internet. It presently conducts a range of activities on standards education access, and policies.

3. **Internet Architecture Board (IAB)**

IAB is a committee of IETF and an advisory body of ISOC. The board comprises researchers and professionals for developing technical aspects of the Internet.

The responsibilities of IAB are −

- Supervise architectural standards of different networks and IP.
- Review issues related to Internet Standards.
- Provide guidance to IETF and ISOC.

4. **Internet Research Task Force (IRTF)**

IRTF is composed of a number of research groups whose overall objective is focused on the long-term development of the Internet. It is a parallel organization to IETF. The participants are individual contributors who have long-term memberships. The research groups work on Internet protocols, applications, technology and overall architecture.

5. World Wide Web Consortium (W3C)

It is the foremost international standards organization for the world wide web (www). It is a community of a large number of member organizations, who work together to develop web standards and improve web services. Some of the popular standards developed by W3C are HTML, HTTP, XML, CSS, etc.

CHAPTER SIX

6. INTERNET ADDRESSING

6.1. What is Internet Protocol (IP) addressing?

When devices communicate with each other over a local area network, or "LAN", or across the internet, the message transmitted is ultimately directed to the target device's network hardware address that is programmed into the device by the manufacturer. This hardware address, or "**MAC**" address, is physically encoded very much like an automobile's VIN number that includes information about the manufacturer and when the device was created along with a sequential number.

Unfortunately, MAC addresses are not helpful for routing communication messages outside of a small number of locally interconnected devices because they are randomly scattered around the world, i.e., a device with a MAC address of 10:20:30:40:50:60 could be in New York and another with a MAC address of 10:20:30:40:50:61 could be in Beijing.

To enable devices to find each other easily no matter where they are in the world, the creators of the Internet came up with a logical addressing scheme that made it much easier for devices to find each other, no matter where they were on the Internet. These logical, Internet Protocol, addresses are commonly referred to as "**IP addresses**".

6.1.1. IP addresses

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.

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.

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 2^N 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 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

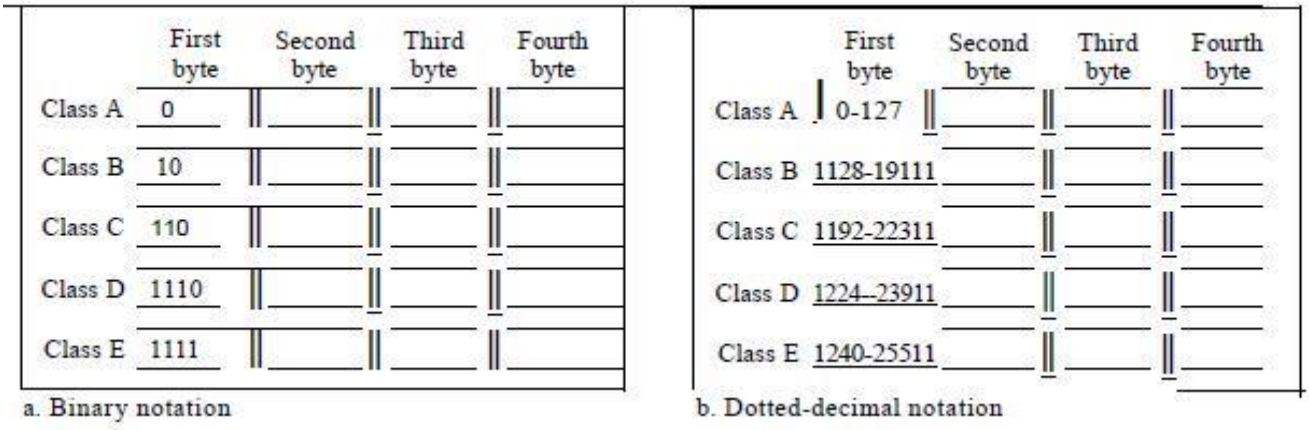
b. 11011101 00100010 00000111 01010010

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.



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 was 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.

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. 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 above Table 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.

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.

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.

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:

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

6.1.2. SUBNETTING

The need for sub netting

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.

The sub - netting 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.

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)*

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

Positional value of bits

Value is the position value of the bits borrowed.

Example

Q - What is the value of 01010110 in decimal?

- 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)

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

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.

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

Sub netting 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 (**11**000000), 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 (11**000000**), 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 (**111**00000), the answer would be 2^3 – 2 = 6

Q - How many hosts per subnet do we have?

A - We have 6 host bits off (111**00000**), 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.*1*68.10.96, 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

CHAPTER SEVEN

7. CONNECTING DEVICES (LAN and WAN Technologies)

7.1. Networking Technologies Definition

Networking technology allows for the exchange of data between large and small information systems used primarily by businesses and educational institutions. Network technicians, also known as network engineers or specialists, are responsible for the configuration, installation and troubleshooting of the technology used to transmit digital information, including audio, visual and data files. Through networking, end-users are able to transmit files, messages and other data through e-mail or various other channels, sharing information through Internet or Intranet connections, based on the needs of an organization.

The development of a network involves assessing the administrative and informational requirements of an organization and evaluating the costs for hardware, installation, training, security and account management. Once a network is deployed, networking technicians are usually responsible for ensuring the network remains operational and updated as needed. They usually provide technical support to company employees for any problems that may arise.

Networking technologies such as Ethernet, Token Ring and FDDI provide a data link layer function; that is, they allow a reliable connection between one node and another on the same network.

It is any technology (software and hardware) by which two or more computer systems are connected together and communicate information between them.

7.2. Type Network Technology

There are

1. LAN technology
2. WAN technology

7.2.1. LAN technology

LAN is a type of network which is used to connect devices within a limited area. LAN is limited to a building, church, school, or small geographical area.

Factors considered while selecting the LAN

- Cost efficiency,
- Installed base,

- Maintainability, and
- Performance

Types of LAN technologies:

- Ethernet
- Token Ring
- FDDI
- LocalTal

2.1.1.1. *Ethernet*

Ethernet is the technology that is commonly used in wired local area networks (LANs). Ethernet is a network protocol that controls how data is transmitted over a LAN and is referred to as the **IEEE 802.3 protocol**. The protocol has evolved and improved over time to transfer data at the speed of more than a gigabit per second. In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.

To set up a wired Ethernet LAN, you need the following:

- **Computers and devices to connect**: Ethernet connects any computer or other electronic device to its network as long as the device has an Ethernet adapter or network card.
- **Network interface cards in the devices**: A network interface card is either integrated into the motherboard of the computer or installed separately in the device. There are also USB versions of Ethernet cards, such as external dongles. An Ethernet card is known as a network card. It has ports where you connect cables. There may be two ports, one for an RJ-45 jack that connects unshielded twisted pair (UTP) cables and one for a coaxial jack on the network card. (Coaxial connections are extremely rare, though.)
- **A router, hub, switch, or gateway to connect devices**: A hub is a device that acts as a connecting point between devices on a network. It consists of several RJ-45 ports to which you plug the cables.
- **Cables**: UTP (Unshielded Twisted Pair) cables are commonly used in Ethernet LANs. This cable is similar to the kind used for landline telephone sets but fatter, with eight twisted pairs of wires of different colors inside. The end is crimped with an RJ-45 connector, which is a larger version of the RJ-11 jack that plugs into a landline phone.

Currently, these data rates are defined for operation over optical fibers and twisted-pair cables:

- **Fast Ethernet**

Fast Ethernet refers to an Ethernet network that can transfer data at a rate of 100 Mbit/s.

- **Gigabit Ethernet**

Gigabit Ethernet delivers a data rate of 1,000 Mbit/s (1 Gbit/s).

- **10 Gigabit Ethernet**

10 Gigabit Ethernet is the recent generation and delivers a data rate of 10 Gbit/s (10,000 Mbit/s). It is generally used for backbones in high-end applications requiring high data rates.

Multiple Access Control

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there are no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created (data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.

- **CSMA – Carrier Sense Multiple Access**

It ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However, there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes-

- **1-persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally (with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.

- **P-persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it sends with p probability. This repeat continues until the frame is sent. It is used in WIFI and packet radio systems.
- **O-persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

Two types

- **CSMA/CD –** Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected. For more details refer – Efficiency of CSMA/CD. used or wired networks
- **CSMA/CA –** Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal (its own) then the data is successfully sent but if there are two signals (its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However, it is not so in wired networks, so CSMA/CA is used in this case.

CSMA/CA avoids collision by:

1. **Interframe space –** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time, it again checks the medium for being idle. The IFS duration depends on the priority of station.
2. **Contention Window –** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
3. **Acknowledgement –** The sender re-transmits the data if acknowledgement is not received before time-out.

10BASE-2 Thin Ethernet

What Does 10BASE-2 Mean?

10Base2 is among the family of Ethernet network standards for local area networks (LAN) that uses a thinner version of coaxial cable to establish a network path or medium and operates at a speed of 10 Mbps to carry out baseband transmission.

10Base2 is also known as cheaper net, thin wire, thinnet and thin Ethernet.

- It uses a lighter and thinner coaxial cable
- 10 Base-2 uses an RG-58 coaxial cable
- Each node on the bus must be separated by a minimum of 0.5 meters
- The overall length of the bus must be less than 185 meters (606 feet)
- Used commonly for wired in a bus topology.

10 Base-5 – Thick Ethernet

- A single thicknet coaxial cable laid out a connecting all nodes together in a bus topology.
- Better in noise resistance and better for long distance up to 500 meters
- At each end of the coaxial cable is a terminator.
- Each node on the network physically connects to AUI (Adapter Unit Interface)-RJ-8
- But is inflexible
- Fault intolerant

10 Base-T – Unshielded Twisted Pair

- It utilizes Category 3 (or higher) Unshielded Twisted Pair (UTP) cable
- Used commonly in **star topology.**
- Used for short distance communication

10 Base-F

- It is a **version of Ethernet which runs over fiber optic cable.**
- In physical topology, it is very similar to 10 Base-T
- It supports distances up to 2000 meters (6600 feet).
- Used for wired in a star topology

2.1.1.2. Token Ring

- It is topology that used use token passing for synchronized access to the ring
- It implemented at layer two OSI model
- It unidirectional transmission and used single ring
- It is self-healing technology which means devices can insert without disturbing the network.

- Hardware must be designed to pass token even if attached computer is powered down

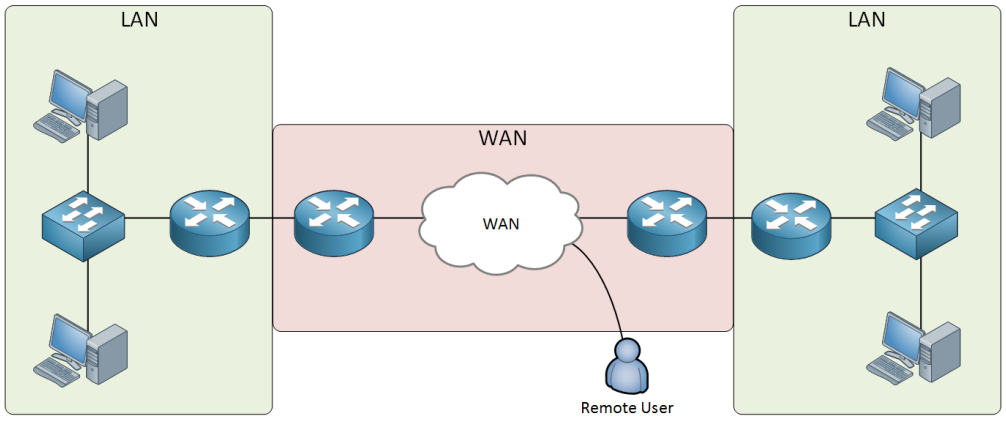
2.1.1.3. Fiber Distributed Data Interconnect (FDDI)

- Uses fiber optics between stations
- Up to 2km length between stations and 100km ring circumference
- Transmits data at 100Mbps and used for ring topology
- It uses double ring as follows and it and reliability than token ring
- Primary ring (outer ring) used for transfer while second ring for backup
- Is also self-healing technology
- So, FDDI is another ring technology

7.2.2. WAN Technologies

Our own networks are called LANs (Local Area Network). We own and operate these networks. It's called a "local" area network since all devices that make up the LAN are close to each other. Perhaps in one building or a few buildings close to each other (called a campus). When we need access to other remote networks, connect two LANs together or give others access to our LAN, we need a WAN (Wide Area Network). As the name implies, WANs cover large geographical areas. This could be a network between two cities or as large as the Internet.

WANs are operated by companies like phone/cable companies, service providers, or satellite companies. They build large networks that span entire cities or regions and lease the right to use their networks to their customers.



In its simplest form, a wide-area network (WAN) is a collection of local-area networks (LANs) or other networks that communicate with one another. A WAN is essentially a network of networks, with the Internet the world's largest WAN.

Today, there are several types of WANs, built for a variety of use cases that touch virtually every aspect of modern life.

WAN Service Types

WANs (Wide Area Network) has three common different types of services. These WAN Services are:

- Leased Lines
- Circuit-Switched Network
- Packet-Switched Network

WAN Protocols

There are several WAN Protocols that are used between different locations of different networks. These protocols are:

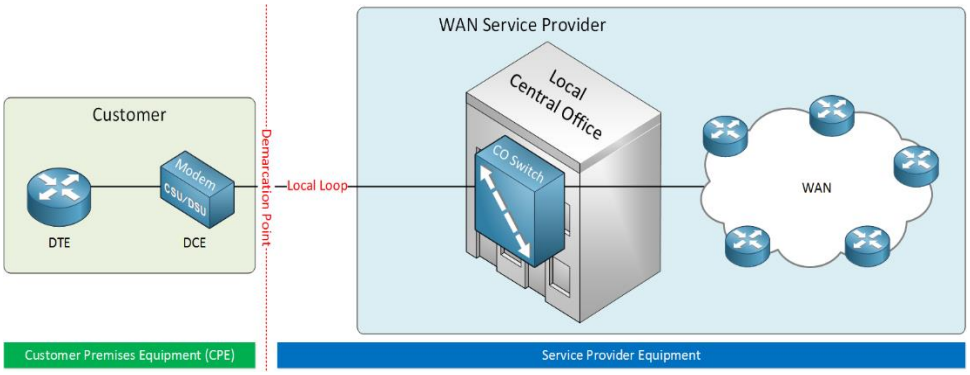
- HDLC
- PPP
- Frame Relay
- ATM

HDLC (High-Level Data Link Control) is a layer 2 WAN Encapsulation Protocol that is used on synchronous data links. It is the simplest WAN Protocol that can connect your remote offices over leased lines. It has both industry standard and Cisco proprietary version.

PPP (Point to Point Protocol) is also a WAN Encapsulation Protocol that is based on HDLC but we can say that PPP is the enhanced version of HDLC. There are many additional features in PPP like Authentication, Multilink support, Error Detection, Quality Check.

Frame Relay is another L2 Protocol. It is based on X.25 and provide Virtual Circuit based connections. Frame Relay was popular before, but nowadays it is rarely used.

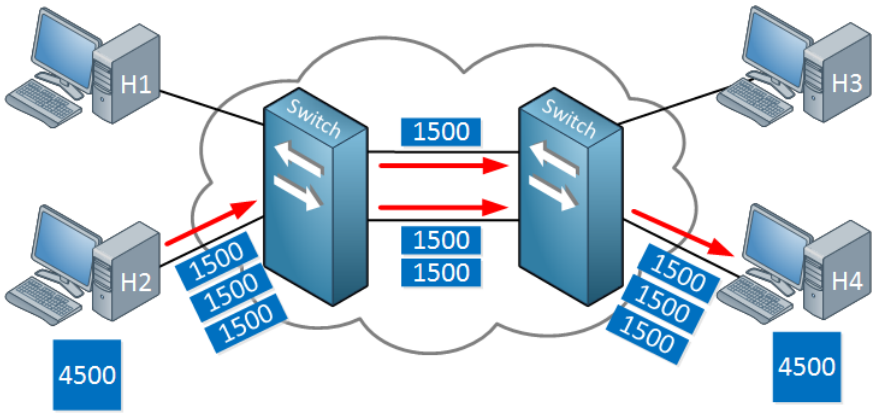
ATM (Asynchronous Transfer Mode) is a cell-based Layer 2 WAN Protocol. It is used with high-speed transmission media like T3, E3 and SONET.



Types of WAN technologies Summary

- **Packet switching**

Packet switching is a method of data transmission in which a message is broken into several parts, called **packets**, that are sent independently, in triplicate, over whatever route is optimum for each packet, and reassembled at the destination. Each packet contains a piece part, called the payload, and an identifying header that includes destination and reassembly information. The packets are sent in triplicate to check for packet corruption. Every packet is verified in a process that compares and confirms that at least two copies match. When verification fails, a request is made for the packet to be re-sent.



- **TCP/IP protocol suite**

TCP/IP is a protocol suite of foundational communication protocols used to interconnect network devices on today's Internet and other computer/device networks. TCP/IP stands for Transmission Control Protocol/Internet Protocol.

- **Router**

A router is a networking device typically used to interconnect LANs to form a wide area network (WAN) and as such is referred to as a WAN device. IP routers use IP addresses to determine where to forward packets. An IP address is a numeric label assigned to each connected network device.

- **Overlay network**

An overlay network is a data communications technique in which software is used to create virtual networks on top of another network, typically a hardware and cabling infrastructure. This is often done to support applications or security capabilities not available on the underlying network.

- **Packet over SONET/SDH (PoS)**

Packet over SONET is a communication protocol used primarily for WAN transport. It defines how point-to-point links communicate when using optical fiber and SONET (Synchronous Optical Network) or SDH (Synchronous Digital Hierarchy) communication protocols.

- **Multiprotocol Label Switching (MPLS)**

MPLS is a network routing-optimization technique. It directs data from one node to the next using short path labels rather than long network addresses, to avoid time-consuming table lookups.

- **ATM**

ATM (Asynchronous Transfer Mode) is a switching technique common in early data networks, which has been largely superseded by IP-based technologies. ATM uses asynchronous time-division multiplexing to encode data into small, fixed-sized cells. By contrast, today's IP-based Ethernet technology uses variable packet sizes for data.

- **Frame Relay**

Frame Relay is a technology for transmitting data between LANs or endpoints of a WAN. It specifies the physical and data-link layers of digital telecommunications channels using a packet switching methodology.

Frame Relay packages data in frames and sends it through a shared Frame Relay network. Each frame contains all necessary information for routing it to its destination. Frame Relay's original purpose was to transport data across telecom carriers' ISDN infrastructure, but it's used today in many other networking contexts.

CHAPTER EIGHT

8. COMPUTER NETWORK SECURITY BASICS

8.1. What is Network Security?

- Security is “the quality or state of being secure—to be free from danger” .
- The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent(unintended) unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use.
- Refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection.
- Is protecting information and information systems from unauthorized access, use, disclosure, disruption (interruption/disorder), modification or destruction (damage).

During initial days of internet, its use was limited to military and universities for research and development purpose. Later when all networks merged together and formed internet, the data used to travel through public transit network. Common people may send the data that can be highly sensitive such as their bank credentials, username and passwords, personal documents, online shopping details, or confidential documents. All security threats are intentional i.e., they occur only if intentionally triggered. Security threats can be divided into the following categories:

Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.

Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.

8.2. Benefits of Network Security

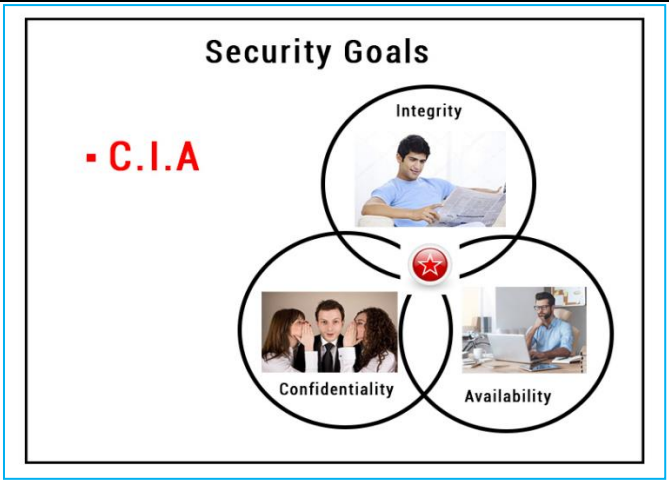
Network Security is vital in protecting client data and information, keeping shared data secure and ensuring reliable access and network performance as well as protection from cyber threats. A well-designed network security solution reduces overhead expenses and safeguards organizations from costly losses that occur from a data breach or other security incident. Ensuring legitimate access to systems, applications and data enables business operations and delivery of services and products to customers.

8.3. Top Network Security Tools

Some of the security tools, hardware, and software that are necessary to ensure that the network is, indeed, secure are listed below:

- Wireshark
- Nessus
- Snort
- Netcat
- Metasploit
- Aircrack
- BackTrack

8.4. CIA Triad in Cyber Security



In the CIA Triad, you may picture a man in a black suit solving crime and running behind criminals, we are not talking about that. Our CIA triad is a Fundamental cybersecurity model that acts as a foundation for developing security policies designed to protect data. Confidentiality, integrity, and availability are the three letters upon which CIA triad stands. The CIA Triad is a common prototype that constructs the basis for the development of security systems. They are used to find vulnerabilities and methods to create solutions.

1. **Confidentiality:**
    - Computer-related assets are accessed only by authorized parties.
    - Confidentiality is sometimes called secrecy or privacy
2. **Integrity:** assets can be modified only by authorized parties or only in authorized ways
3. **Availability:** assets are accessible to authorized parties at appropriate times

- **Threats:** Something that can potentially cause damage to information assets.
- **Vulnerabilities:** A weakness in the organization, computer system, or network that can be exploited by threat.
- **Control:** an action, device, procedure, or technique that remove or reduce a vulnerabilities

8.5. What is security threat

- Definition: Something that can potentially cause damage to information assets.
- A malicious attacker must have **three** things:
  i. **Method**: the skills, knowledge, tools, and other things with which to be able to pull off the attack.
  ii. **Opportunity**: the time and the access to accomplish the attack.
  iii. **Motive**: a reason to want to perform this attack against this system.

8.6. Types of Security Attacks

In an Information Security context there are 4 broad based categories of attacks:

1) Fabrication
2) Interception
3) Interruption
4) Modification

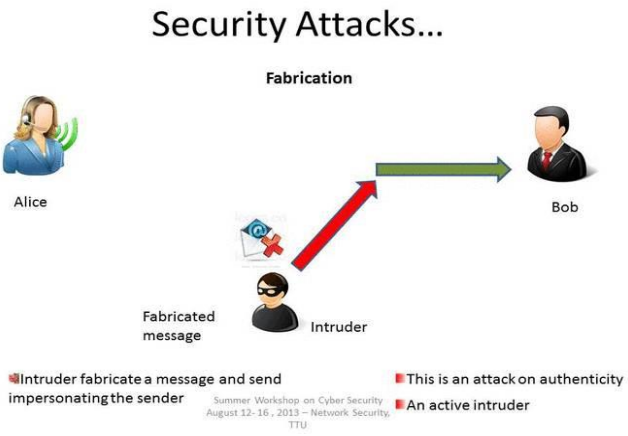
Fabrication

A fabrication attack creates **illegitimate** information, processes, communications or other data within a system. Often, fabricated data is inserted right alongside authentic data. When a known system is compromised, attackers may use fabrication techniques to gain trust, create a false trail, collect data for illicit use, spawn malicious or extraneous processes. In addition, fabricated data may reduce confidence in genuine data with the affected system.

- **Example**: the intruder may insert spurious transactions to a network communication system, or add records to an existing database
- **Its attach om authenticity**

Examples of Fabrication attacks include:

- SQL Injection
- Route Injection
- User / Credential Counterfeiting
- Log / Audit Trail Falsification
- Email Spoofing

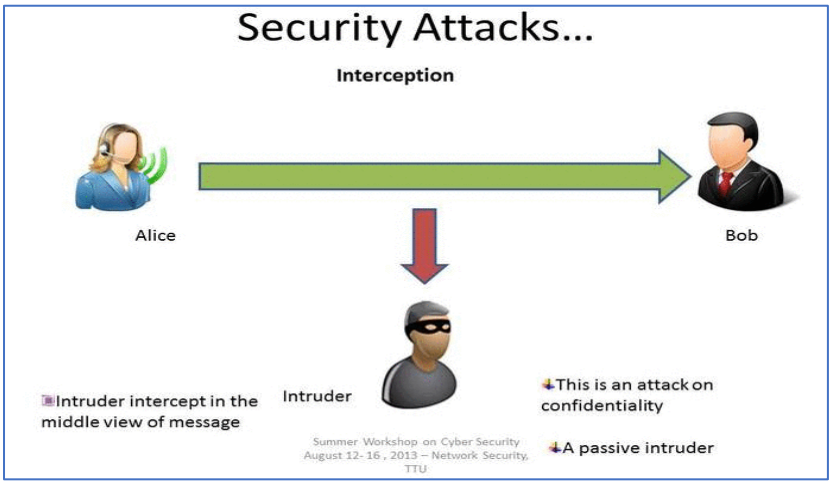


Mitigate the attack:

- Use of Authentication and authorization mechanisms
- Using Firewalls
- Use Digital Signatures - Digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

Interception

An interception is where an unauthorized individual **gains access** to confidential or private information. Interception attacks are attacks against network the **confidentiality** objective of the CIA Triad.



Examples of Interception attacks:

- Eavesdropping on communication.
- Wiretapping telecommunications networks.

- Illicit copying of files or programs.
- Obtaining copies of messages for later replay.
- Packet sniffing and key logging to capture data from a computer system or network.

Mitigate the attack:

- Using **Encryption** - SSL, VPN, 3DES, BPI+ are deployed to encrypts the flow of information from source to destination so that if someone is able to snoop in on the flow of traffic, all the person will see is ciphered text.
- Traffic Padding - It is a function that produces cipher text output continuously, even in the absence of plain text. A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted. When input plaintext is not present, the random data are encrypted and transmitted. This makes it impossible for an attacker to distinguish between tree data flow and noise and therefore impossible to deduce the amount of traffic.

Interruption

In an interruption attack, a network service is made degraded or unavailable for legitimate use. They are the attacks against the **availability** of the network.

Examples of Interruption attacks:

- Overloading a server host so that it cannot respond.
- Cutting a communication line.
- Blocking access to a service by overloading an intermediate network or network device.
- Redirecting requests to invalid destinations.
- Theft or destruction of software or hardware involved.

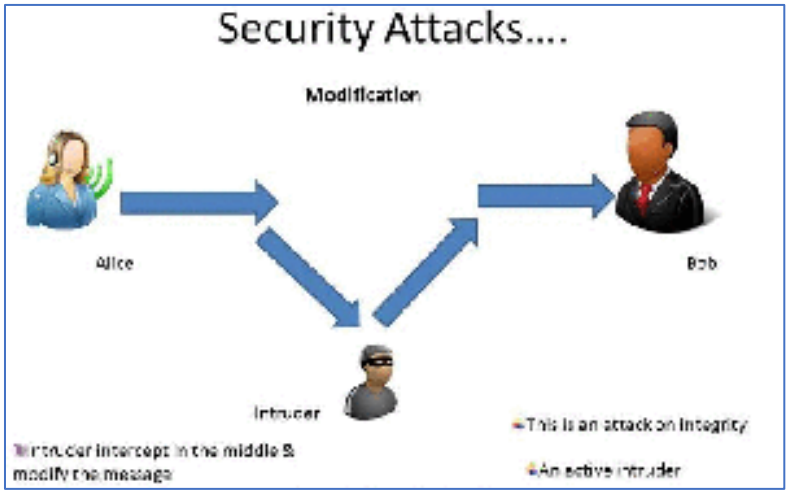
Mitigate the attack:

- Use **Firewalls** - Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. Modern stateful firewalls like Check Point FW1 NGX and Cisco PIX have a built-in capability to differentiate good traffic from **DoS** attack traffic.
- Keeping backups of system configuration data properly.
- Replication.

Modification

Modification is an attack against the integrity of the information. Basically, there is **three** types of modifications.

1) **Change**: Change existing information. The information is already existed but incorrect. Change attacks can be targeted at sensitive information or public information.
2) **Insertion**: When an insertion attack is made, information that did not previously exist is added. This attack may be mounted against historical information or information that is yet to be acted upon.
3) **Deletion**: Removal of existing information.



Examples of Modification attacks include:

- Modifying the contents of messages in the network.
- Changing information stored in data files.
- Altering programs so they perform differently.
- Reconfiguring system hardware or network topologies.

Mitigate the attack:

- Introduction of intrusion detection systems (**IDS**) which could look for different signatures which represent an attack.
- Using **Encryption** mechanisms
- Traffic padding
- Keeping backups
- Use messaging techniques such as checksums, sequence numbers, digests, authentication codes

8.7. Types of security controls

There are several types of security controls that can be implemented to protect hardware, software, networks, and data from actions and events that could cause loss or damage. For example:

- **Physical security controls** include such things as data center perimeter fencing, locks, guards, access control cards, biometric access control systems, surveillance cameras, and intrusion detection sensors.
- **Digital security controls** include such things as usernames and passwords, two-factor authentication, antivirus software, and firewalls.
- **Cybersecurity controls** include anything specifically designed to prevent attacks on data, including DDoS mitigation, and intrusion prevention systems.
- **Cloud security controls** include measures you take in cooperation with a cloud services provider to ensure the necessary protection for data and workloads. If your organization runs workloads on the cloud, you must meet their corporate or business policy security requirements and industry regulations.

8.8. What is Encryption?

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called **cryptography**.

In computing, unencrypted data is also known as **plaintext**, and encrypted data is called **ciphertext**. The formulas used to encode and decode messages are called **encryption algorithms, or ciphers.**

To be effective, a cipher includes a variable as part of the algorithm. The variable, which is called a **key**, is what makes a cipher's output unique. When an encrypted message is intercepted by an unauthorized entity, the intruder has to guess which cipher the sender used to encrypt the message,

as well as what keys were used as variables. The time and difficulty of guessing this information is what makes encryption such a valuable security tool.

Encryption has been a longstanding way for sensitive information to be protected. Historically, it was used by militaries and governments. In modern times, encryption is used to protect data stored on computers and storage devices, as well as data in transit over networks.

Why is encryption important?

Encryption plays an important role in securing many different types of information technology (IT) assets. It provides the following:

- **Confidentiality** encodes the message's content.
- **Authentication** verifies the origin of a message.
- **Integrity** proves the contents of a message have not been changed since it was sent.
- **Nonrepudiation** prevents senders from denying they sent the encrypted message.

How is encryption used?

Encryption is commonly used to protect data in transit and data at rest. Every time someone uses an ATM or buys something online with a smartphone, encryption is used to protect the information being relayed. Businesses are increasingly relying on encryption to protect applications and sensitive information from reputational damage when there is a data breach.

There are three major components to any encryption system:

- The data,
- The encryption engine and
- The key management.

In laptop encryption, all three components are running or stored in the same place: on the laptop. In application architectures, however, the three components usually run or are stored in separate places to reduce the chance that compromise of any single component could result in compromise of the entire system.

How does encryption work?

At the beginning of the encryption process,

- ✓ The sender must decide what cipher will best disguise the meaning of the message and what variable to use as a key to make the encoded message unique. The most widely used types of ciphers fall into two categories: **symmetric** and **asymmetric**.

8.9. Categories of Cryptography

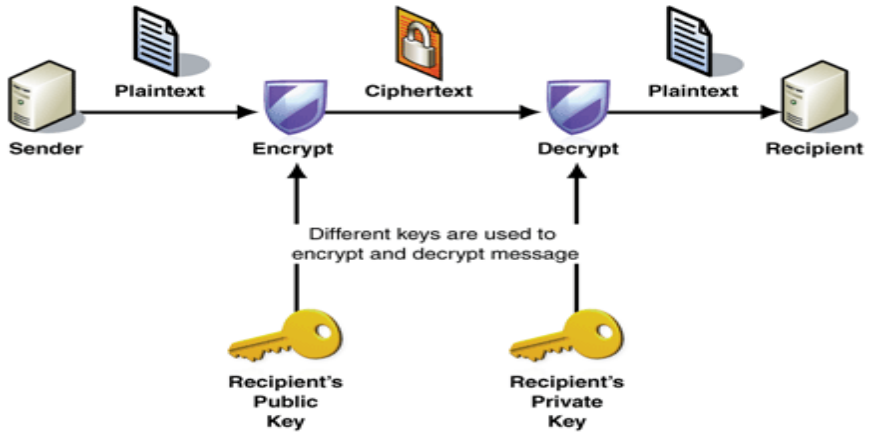
- **Symmetric ciphers**

Also referred to as **secret key encryption**, use a single key. The key is sometimes referred to as a **shared secret** because the sender or computing system doing the encryption must share the secret key with all entities authorized to decrypt the message. Symmetric key encryption is usually much faster than asymmetric encryption. The most widely used symmetric key cipher is the **Advanced Encryption Standard (AES)**, which was designed to protect government-classified information.

- **Asymmetric ciphers**

Also known as **public key encryption**, use **two** different -- but logically linked -- keys. This type of cryptography often uses **prime numbers** to create keys since it is computationally difficult to factor large prime numbers and reverse-engineer the encryption. The **Rivest-Shamir-Adleman (RSA)** encryption algorithm is currently the most widely used public key algorithm. With RSA, the public or the private key can be used to encrypt a message; whichever key is not used for encryption becomes the decryption key.

Today, many cryptographic processes use a symmetric algorithm to encrypt data and an asymmetric algorithm to securely exchange the secret key.



Encryption vs. decryption

Encryption, which encodes and disguises the message's content, is performed by the message sender. **Decryption**, which is the process of **decoding** an obscured message, is carried out by the message receiver.

8.10. Types of Authentication Protocols

When we develop software, our first and most important priority is **user authentication**. To authenticate the user there are several mechanisms by which we can authenticate the data that are given by the user.

Why is user authentication important?

Requiring users to provide and prove their **identity** adds a layer of security between adversaries and sensitive data. With authentication, IT teams can employ the least privileged access to limit what employees can see. The average employee, for example, doesn't need access to company financials, and accounts payable doesn't need to touch developer projects. When selecting an authentication type, companies must consider UX along with security. Some user authentication types are less secure than others, but too much friction during authentication can lead to poor employee practices.

1. Kerberos

Kerberos is a type of protocol that is used to authenticate users. It validates the client and server during networking with the help of a cryptographic key. It is designed to strongly authenticate the users during the reporting of the application. All the proposals of Kerberos are available at MIT. The main use of the Kerberos is in the product-based companies.

Advantages

1. The various operating systems are supported by the Kerberos.
2. In Kerberos, the authentication key is shared very efficiently in comparison to public sharing.

Disadvantages

1. The client and service can only authenticate themselves with the help of Kerberos.
2. When we use a soft or weak password, it always shows vulnerability.

2. Lightweight Directory Access Protocol (LDAP)

LDAP stands for Lightweight Directory Access Protocol. With the help of this protocol, we can determine the organization, individual, or any other devices during the networking over the internet. It is also called a Directory as a service. Lightweight Directory Access Protocol (LDAP) is the ground for Microsoft Building Activity Directory.

Advantages for Lightweight Directory Access Protocol (LDAP)

1. It is a type of automated protocol that is why it is very easier for the organization.
2. All the existing software is supported by Lightweight Directory Access Protocol (LDAP).

3. Multiple directories can be allowed in Lightweight Directory Access Protocol(LDAP)

Some disadvantages of LDAP

1. It requires the experience of deployment.
2. The directory servers are required to be LDAP-obedient for deployment.

3. OAuth2

OAuth2 is a type of authentication protocol for the framework. It provides permission to the users which are coming through the HTTP servers. When the user makes a request to access the resources, suddenly, an API call is created, and after that, the authentication token is generated.

Advantages of OAuth2

1. It is a very simple type of authentication protocol, and it is very easy to use.
2. It provides the code for server-side authentication.

Disadvantages for OAuth2

1. It is a little bit difficult to manage the different sets of codes.
2. When we connect it to an affected system, it also shows some serious effects.

4. SAML

SAML stands for **Security Assertion Markup Language**. It is based on an XML-based authentication protocol. It provides authorization between the service provider and the identity provider. It is also a product of the OASIS Security Service Technical Committee.

Advantages of SAML

1. The administrative cost is reduced for the end user with the help of SAML (Security Assertion Markup Language).
2. It provides a single window for authentication for all the services.

Disadvantages of SAML

1. It is fully dependent on the identity provider.
2. A single XML format manages all the data.

5. RADIUS

RADIUS stands for **Remote Authentication Dial-In User Service**. It is a type of network protocol that provides accounting, centralized authentication, and authorization. When the user makes a request to access all the resources, the RADIUS server creates a temporary credential to access all the resources. After this, the temporary credential is saved on the local database and provides access to the user.

Advantages of RADIUS

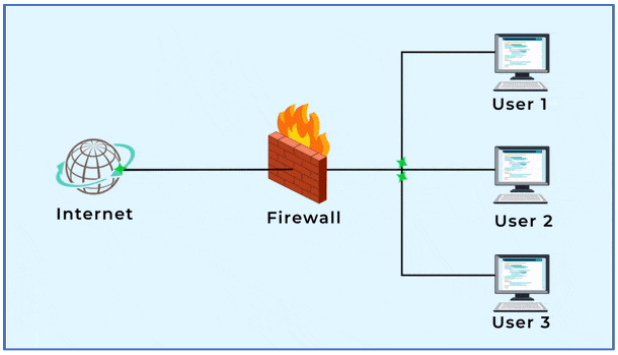
1. It has a feature to provide multiple accesses to the admin.
2. It also provides a unique id for every session of the user.

The disadvantage of RADIUS

1. The mechanism for initial implementation is very hard on hardware.
2. It has a variety of models that may require a special team which is cost-consuming.

8.11. What is a Firewall?

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.



Types of Firewalls

- **Packet filtering**

A small amount of data is analyzed and distributed according to the filter's standards.

- **Proxy service**

Network security system that protects while filtering messages at the application layer.

- **Stateful inspection**

Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.

- **Next Generation Firewall (NGFW)**

Deep packet inspection Firewall with application-level inspection.

What Firewalls Do?

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on **blocking malware and application-layer attacks**, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly

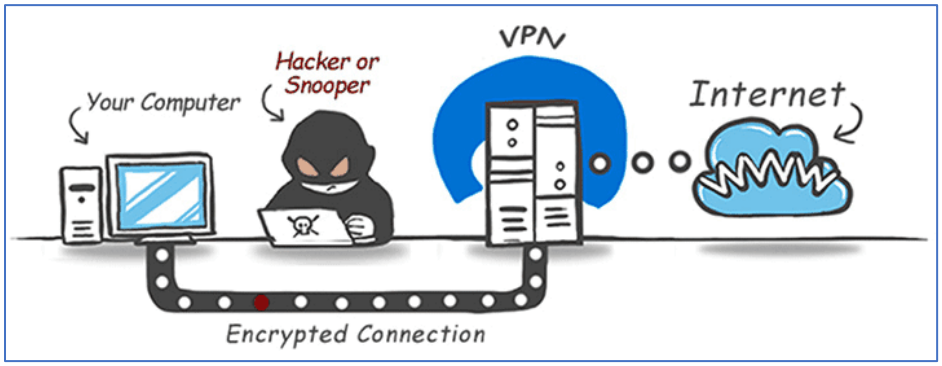
and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

Why Do We Need Firewalls?

Firewalls, especially Next Generation Firewalls, focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network. Firewalls can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down. By leveraging a firewall for your security infrastructure, you're setting up your network with specific policies to allow or block incoming and outgoing traffic.

8.12. VPN

Stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.



How does a VPN work?

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

What are the benefits of a VPN connection?

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can't decipher this data.

8.13. What is Transport Layer Security (TLS)?

Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is **encrypting** the communication between web applications and servers, such as **web browsers** loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP). In this article we will focus on the role of TLS in web application security.

What is the difference between TLS and SSL?

TLS evolved from a previous encryption protocol called **Secure Sockets Layer** (SSL), which was developed by Netscape. TLS version 1.0 actually began development as SSL version 3.1, but the name of the protocol was changed before publication in order to indicate that it was no longer associated with Netscape. Because of this history, the terms TLS and SSL are sometimes used interchangeably.

What is the difference between TLS and HTTPS?

HTTPS is an **implementation** of TLS encryption on top of the HTTP protocol, which is used by all websites as well as some other web services. Any website that uses HTTPS is therefore employing TLS encryption.

Why should businesses and web applications use the TLS protocol?

TLS encryption can help protect web applications from data breaches and other attacks. Today, TLS-protected HTTPS is a standard practice for websites. The Google Chrome browser gradually cracked down on non-HTTPS sites, and other browsers have followed suit. Everyday Internet users are more wary of websites that do not feature the HTTPS padlock icon.

What does TLS do?

There are three main components to what the TLS protocol accomplishes: Encryption, Authentication, and Integrity.

- **Encryption:** hides the data being transferred from third parties.

- **Authentication:** ensures that the parties exchanging information are who they claim to be.
- **Integrity:** verifies that the data has not been forged or tampered with

REVIEW QUESTION AND ANSWER

Use the following link

https://www.javatpoint.com/computer-network-mcq

https://www.javatpoint.com/computer-network-mcq-part2

https://www.javatpoint.com/networking-interview-questions