Chapter 4

Computer Networking

4.1 Data Communication Model

Introduction: At present, the computer has emerged as an essential service so many computers interconnect and share information between each other and the exchange of data between each room exits has increased phenomenally in the power of the compute. is Networking. The network is basically a group of all the elements that are used to connect computers and exchange data between multiple computers. The basic purpose of networking is to increase productivity.

Properties of Networking: While building a network the following basic qualities are kept in mind:

1. Price: This category comes with useful elements, their adjustment and maintenance.

2. Security: All elements and statistics are protected in this category.

3. Speed: The speed at which the data is exchanged so that the network gets quality comes in this category

4. Positioning: In this category all the elements of the network are interconnected in physical condition.

5. Scalability: In this category how the network accepts new change is kept in mind.

Data Communication

The exchange of data by any medium (wire or wireless) between the two devices used in the network comes in this category. The direct communication of data is with its exchanges rather than the generation of data and the effect of the exchange of data depends on three factors.

1. Delivery - Mechanism to exchange data by keeping in mind the right target i.e. the data is correctly achieved by goal only.

2. Purity - If the medium makes any changes in the data then it is unusable.

3. Timeliness - It is important only if the mechanism exchanges data at the right time.

Information System

Figure 4.1: Information System

Each section of this picture is a part of the communication system. Each part has its own meaning and its utility.

1. Origin - The tool / Application that produces data.

2. Transmitter - The medium does not accept the datato send it to the target in the form it produces, so the transmitter is the device that prepares the data to be sent to the target.

3. Sender System - When two devices exchange data between each other the communication system between them is called the sender system.

4. Recipient - Recipient is the device that receives data from the sender system before moving on to the target.

5. Goal: The data on the last device which crosses the sender system from the originating device is called the target.

Part of the data communication system - the data communication system has 5 major parts-

1. Message - Message is the data or information that we want to transmit on the given medium. The message can be of various forms such as text, image, video

2. The sender - This is the device that sends the message. It can be a computer, telephone device or camera etc.

3. Receiver - This is the device that receives the message at the end.

4. Media - From the source the message reaches its goal by using media. This is the path which leads to the goal from the origin through the medium. Medium can be an optical fiber, coaxial wire, twisted pair or radio waves.

5. Protocol - Protocol is a set of rules that govern data transmission. It gives an agreement between two instruments (Source and Destination).

Definition of Network

The network is a group of some electronic devices that are connected to some wires or wireless. The work of this medium should carry information from one end to the other. This medium allows all the consumers of this network to share these devices with each other. These devices which are used in the network are called nodes. The number of nodes in a network can be as per requirement. To be qualified and effective for a network it should meet many criteria mainly the following-

(1) Error free work - Job supplement means an exchange of information without error. It involves the time taken in the decision taken by the goal of reaching the goal of information and after it. The editing of a network depends on the following:

a. Consumers number - If there are more consumers in the network then their impact falls on the speed of exchange of information in the network.

b. Communication - This means that the speed of transmitting data is at speed. It is measured in the Kbps / Mbps/ Gbps.

c. Types of medium - It is meant to be used in the exchange of data through the medium of work. The quality of communication of data depends on the medium used.

d. Types of equipment- Equipment used in the network affect both speed and efficiency of data exchange. A high-performance computer works effectively when editing the work.

e. Software - software that operates in the network of devices that operate on the network also affects the quality of the work of the network.

(2) Reconciliation - Reconciliation means predicting the accuracy of time and data to be re-reacted by the goal. For example, we can assume that a network printer

of a network predicted 3 seconds to print a page but it takes 30 seconds which means that there is no harmony with the target in my network.

(3) Trustworthiness - A standard of the usefulness of the reliability Network.

(4) Recovery / Restoration - How soon after a network gets spoiled its utility reaches its real state, its usefulness depends on it.

(5) Security - Protecting against the use of our network's devices, software and data in unauthorized use is the only security. Wire protection is also done in this category.

4.2 Network Topology

The style of connecting computers with each other is called topology. Choosing topology style is an important step in the process of networking. Before choosing a topology it is necessary to consider many aspects. Details of some of these aspects are presented below-

(1) Cost- To reduce the cost of a network, it is necessary that we try to keep the costs of its construction low. To do this, it is necessary to ensure the medium of changing the information signals. The length of the transmission on which the transmission is to be done can also be changed as required.

(2) Flexibility- Because the number of nodes cannot be ascertained as the network's expansion is not pre-determined. For this reason, our chosen topology should be such that there is a capacity to expand.

(3) Reliability- There can be two types of fault in a network. Deterioration of one of the first nodes, the second, the whole network is getting worse. We should look at the fact that when one node gets spoiled, it will not affect the rest of the network.

Topology can be of three types, they are:

4.2.1 Bus Topology - All computers in bus topology are connected to the same cable. Every node (computer) is connected to two other nodes, one can send the same computer message at a time in this genre.

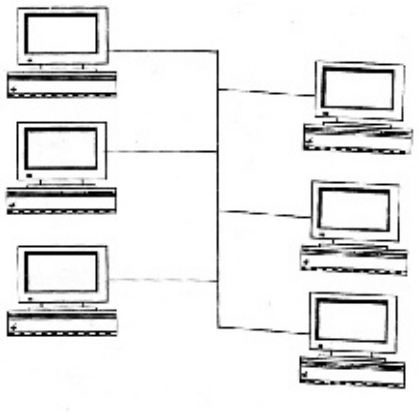


Figure 4.2 BUS Topology System

Benefits of Bus Topology

1. This technique is simple, easy to understand and easy to use.

2. In this, less cable is require to connect computers. So, it falls cheap.

3. It can be easily added to many computers.

Disadvantages of Bus Topology

1. When computers are unable to establish coordination of each other, all computers start transmissions simultaneously. This causes the network to slow down.

2. When the cable breaks two computers cannot interconnect.

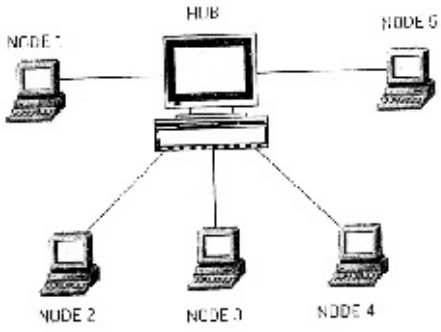
4.2.2 Star Topology: Computer is connected to a hub or switch in this topology. The hub or switch is in the center of the network and sends the signals of one node to all the nodes.

Benefits of Star Topology

1. It's easy to add new computers. The computer is connected to the hub by the cable and in the network.

2. It can be easily detected by hubs or switches.

3. Turning off the work of a computer does not have any effect on the rest of the network.



चित्र 11

Figure 4.3 Star Topology

Disadvantages of Star Topology

1. When the hub or switch goes down the entire network stops working.

2. Star Topology is expensive because every computer is connected to a cable separated by the hub or switch located in the center.

4.2.3 Tree topology: In this topology, computers are added in such a way that they are the branches of tree. The node located at the top is called root. Root is connected to zero or more child nodes (breastpunct thumbs).

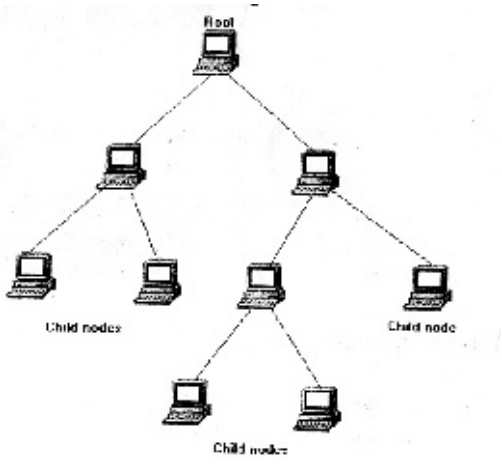


Figure 4.4 Tree Topology

The root node is the father of the child node. Every child node also has many child nodes. In this way, the parent node of every node consists of only the parent node

of the root node. In this type of topology, there is only one path from one node to the other node.

Benefits of Tree Topology

1. It is easy to add new computer to child node in this topology.

2. It does not require a centered hub.

Disadvantages of Tree Topology

1. Adding a computer to a root node is not easy.

2. Adding or removing the computer to the root node can be interrupted by the network.

4.3 Concept of LAN ,WAN, MAN

Networks are broadly divided into three types:

4.3.1 Local Area Network - This network is spread within a building or within a few kilometers area. It is used for the exchange of information technology resources by various computers of any office or factory.

LANs are usually spread in smaller areas such as in a department or a building. The LANs are small so it is easy to handle them. Generally there are some flaws from short circuits and unwanted signals. LAN connects all nodes from the same cable. Telephone cables are used for transmission so they are cheap.

Features of LAN

1. The most important feature of LAN is its speed. Generally, its data transmission speeds are between 10 to 100 mbps. Currently it is 1 Gbps and more.

2. LAN is a flexible network, without disturbing all networks the computer can be added and removed.

3. Since LAN is limited in the area, we can take several types of topology work in it.

4.3.2 Metropolitan Area Network - Metropolitan means the city. This network is spread over a very large area such as the city or town. MAN is a major form of

LAN, It also uses the same technique as LAN. Creating this is more complex than LAN. It can be spread around up to 60 kilometres. It connects branches and business houses in different areas of the same city. Examples - Cable TVs of cities Network.

Features of MAN

1. The entire network is operated and controlled by a centralized machine.

2. MANs main goal is to use software and hardware resources together.

3. MAN can transmit both data and sound.

4.3.3 Wide Area Network (WAN) - In comparison to other networks, the WAN works in a very large area, it can be spread throughout the country or even the peninsula. All the computers in the countries or peninsula in the WANare connected to each other. They can also exchange computer data and give a centrally controlled transmission. WAN can be from transmission, wired media (telephone line, fiber optics) or wireless medium (microwave). In all three types of networks, it is spread over the largest area. Adding two WAN network is very complicated. They may down due to short circuit, wire breakdown or other circuit.

Figure 4.5 WAN System

Features of the WAN

1. The WAN uses several network devices for transmission such as router, switch, and gateway.

2. WAN uses two types of switching method for data transmission.

   a. packet switching

   b. circuit switching

3. Their data transmission speed is slower than other networks.

4.4 Standardization and protocols

In the electronic devices there is a need for a group of rules for communicating that acts as the reason of communication between the sender and the recipient. The protocols ensure the correct communication between the sender and the recipient. The sender and recipient of no protocol will not be able to understand the computing accurately. There are many topics in which the protocols are used.

Protocol: In the computer network, there is a lot of system requirements for transmission of the entities, it is necessary to agree with these protocols. Groups of rules that govern data computation are called protocols. The following element of the protocol is-

1. Syntax - Tells the format of data.

2. Semantics - These are related to every part of a bit how it has been interpreted.

3. Timing - When the data has been sent and at what speed

Regardless of any technique or system as per rules the regulation is known as a standard.

The need for Standards: The standers create a competitive and open market for equipment makers and make tools useful for working around the globe so that no company can make its arbitrariness.

Standardization Committees

1) ISO (International Organization for Standardization)

2) ANSI (American National Standards Institute)

3) IEEE (Institute of Electrical and Electronics Engineers)

4) ITU (International Telecommunication Union)

4.5 Transmission

Transmission is the transfer of data between two or more devices under which data is sent and received between one or more devices.

Methods of Data Transmission

Data on transmission medium can be sent in two ways - asynchronous and synchronous

1.Asynchronous Data Transmission - Asynchronous transmission is also called start-stop transmission. In Asynchronous Transmission Start Stop Bit between each letter. The sender can always send a letter which the receiver receives. As long as the line's hardware is ready to send the data, the asynchronous communication line remains open. To tell about the data being sent, a series of bits is sent to the receiver device because the line remains open. After sending the entire data, the recipient of the data is informed that the data has been exhausted. After this the stop bit is sent so that the line can be broken. The interval between the two letters in the asynchronous transmission is undefined, i.e., to computer destination, a line of letters can be sent or the data can be sent at irregular intervals.

Figure 4.6 Asynchronous Data Transmission

The main advantage of this is that the computer does not need storage because transmission is literally done. One of the disadvantages of its transmission is that the line between sending two letters remains open.

2. Synchronous Data Transmission - There are two channals in Synchronous Communication to send a data and to keep all the links together for the start. To start the two computers together, the clock hardware is used when the computer is ready to send the data, then it sends a mixture of bit towards the receiver which is called the sync character because the first letter is bad therefore the second letter is sent along with it so that it can be ensured that all links can be started together.

A block of synchronous transmission letter is formed. Every block give header and trailer information by which the computer receiving it matches the clock to the sender's computer. The header is the information for identifying the sender and receiving computer. After the header, there is a group of letters which are the actual information and in the end of the block it is trailer. The trailer sends information about the end of the message. After this there is a check letter which helps in finding the defects during transmission.

The advantage of synchronous transmission is its efficiency. It eliminates the need for a start stop bit with every letter. It provides high data transmission speed compared to asynchronous. The interval between sending the block is very low and the block is sent at maximum line speed. The only drawback of synchronous transmission is that the storage device needs buffer memory for storage which collects the blocks of the line.

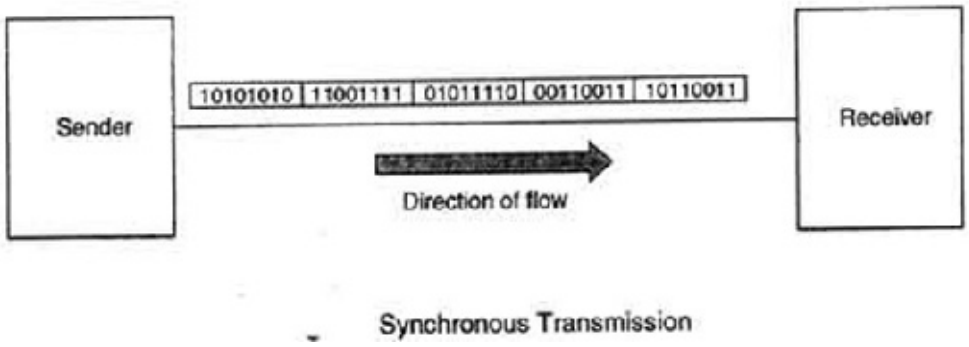


Figure 4.7 Synchronous Data Transmission

Data Transmission Methods

Data transmission methods are

(1) Simplex

(2) Half duplex

(3) Full duplex

Simplex : In simplex transmission method data communicates on one side. Example of Simplex is Television Communication. In this, the main transmitter sends the signal but does not expect the answer. The recipient cannot respond to the transmitter. The example of Simplex translation is the keyboard because it is connected to the computer and can give only data to the computer. In one-sided transmission it also requires a message that can tell that the recipient has obtained the data. Simplex transmission is not used in the work because a back path is required to send self, control and error signals.

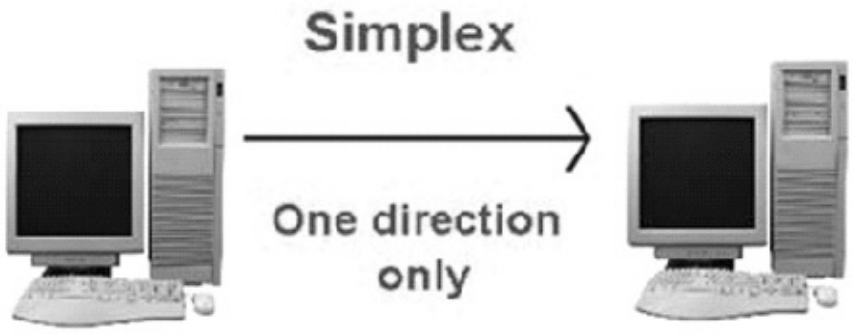


Figure 4.8 Simplex data Transmission

Half Duplex: In Half Duplex Method, both units do communication through the same medium but only one unit can transmit data at a time, when one unit is sending the data and the other is receiving the data so that Half duplex line sends and receives data in an alternate manner. It requires two cables. This is a very common way. The transmission is become sound. It can speak the same person at a time in that it is supposed to serve as the unit of the computer can transmission of data and computer sends a message of acceptance. In Half Duplex, if both devices try to send and receive data together, packets collide.

Figure 4.9 Half-Duplex Data Transmission

Full duplex: In the full duplex, the information mission flows in both directions at the same time. In full duplex method, the direction of the translation is changed as well as the line is diverted.

In such a case, the speed of the line in a computer is very fast. Using the full duplex method we can improve the efficiency of the translation. In Full Duplex Communication, both devices can send and receive data in both directions simultaneously. Its main example is telephone system.

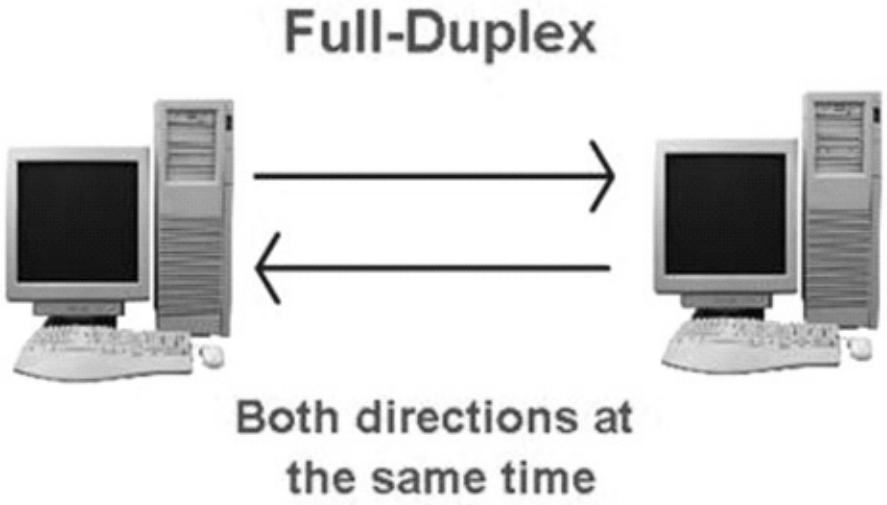


Figure 4.10 Full Duplex Data Transmission

Parallel Transmission: In this transmission more than two bits can transmit from source to destination at a time by using multiple cables.

4.6 Networking Signals

Signal is the electrical electronics and optical representation of Data, to which can be sent to the communications medium. Data transmission, Digital translation or Digital communication is point-to-point and point to multi physical transfer on channel. For example, the sound signal that convert from a microphone or converts to a microphone converts

There are two types of networking signals

(1) Analog Signals

(2) Digital Signals

Analog signals: Analog signal is a continuous signal that changes according to time. The voltage, current and frequency changes in the electronics signal are changed to present. Most signals remain in the form of analog signals, which are later converted to digital signals because analog signals sending devices are expensive. The IC circuit is

used to convert analog to digital. Later these signals have to be received in analog so they are converted from digital to analog. While converting signals and sending them some errors are added that spoil the main signal, they are called impairments. As the signal moves forward on the media, its ability or energy slowly starts to decrease, in such an anal signal we use the amplifier to increase.

Figure 4.11 Analog signals

Digital Signals: A digital signal is an electronic signal that is converted to bit patterns. Every point of the digital signal is the discrete value. Digital Signals are represented by zero or one. Like analog signals, even with digital signals, there are errors during transmission due to which the form of real signals changes. And as the signal progresses over the media, its energy gets reduced.At least no matter how much the energy of any signal should be so that the receiver can understand the pattern between them, otherwise the receiver will not be able to detect the correct information. To correct the reduced energy, the digital signals uses repeates. HDMI technology is used to translate audio and video simultaneously, which is an example of digital signals.

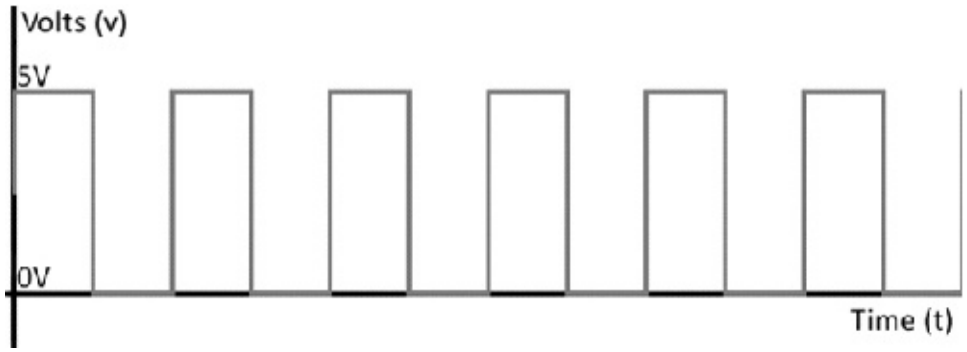


Figure 4.12 Digital Signals

4.7 Transmission Media in Networks

Transmission medium is the path on which transmitters and receivers exchange signals or transmit data to each other. The transmission media determines the physical path between two devices Transmission medium can be divided into two parts.

(1) Guided Transmission Media

(2) Unguided Transmission Media

Guided Transmission Media: Guided media is the medium in which the signals run according to the physical path or not confused with the path. The media's capacities in the directed media are related to its length and how it is connected and depends on it.

Examples: Twisted pair cable, coaxial cable and optical fiber cable

Twisted Pair Cable: Two cables are wrapped in each other in this technology. The two wires are wrapped in each other, reducing the electrical interference of each other. And having a couple wrapped in each other reduces the electric interference of the other couple. Twisted Pairs can only transmit digital and analog signals. The twisted pair cable is used for local telephone transmission and for digital data transmission between the main computer and the network computer in a short distance of up to 1 kilometer, the speed of data transmission can be 9600 bits per second up to 100 meters.

Figure 4.13 Twisted Pair Cable

Twisted pair cable is of two types

(1) Unshielded Twisted Pair (UTP): This is the most popular twisted pair cables and it is also becoming popular in cabling of local area network. UTP is generally used only in the form of telephone system and in many office buildings already. In this kind of cable there is possibility of a cross-talk in the workplace.

Figure 4.14 Unshielded twisted pair cable

The main problem of the UTP cable is the mixing of the signals of a wire which is called cross talk. Shielding is used to reduce cross-talk.

(2) STP: The STP uses high-quality tuned wire jackets that are more secure than the UTP's jacket. The STP is wrapped around the wires and around the wires with the call, making it very effective to make STP brilliant. By which transmitting data is protected against heavy crimes, therefore, STP transmits long distances of data in more speed than UTP and is more secure.

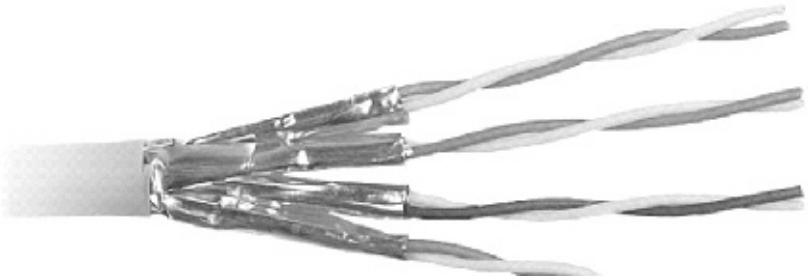


Figure 4.15 Shielded twisted pair cable

Coaxial Cable: There is a hard copper coil called core which is now wrapped with insulator. It is covered with unstained clusters of fine wire.

There is a protective plastic shell on top of these clusters. Symbols are exchanged by the core of copper. The outer armor is made from clustered wires.

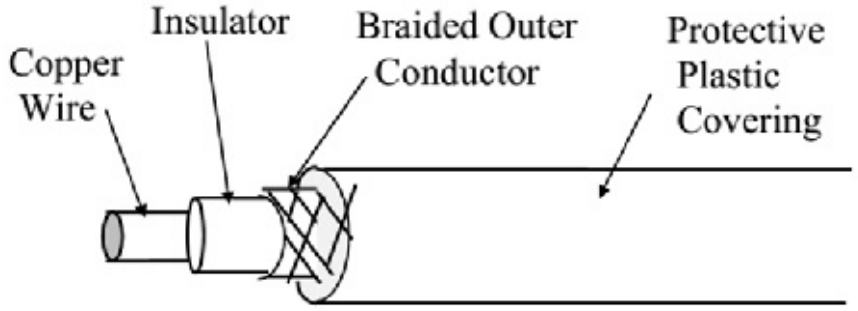


Figure 4.16 Coaxial Cable

Coaxial cable is commonly used for television networks. Coaxial cable can transmit data at a faster distance than a twisted cable. It is cheaper than fiber optic and can be used easily. There are two types of coaxial cable.

(1) Thicknet: This cable is used only in the TV network. It is thick and cannot be

easily folded, so it is difficult to use.

(2) Thinnet: It is mostly used in networking. It is only flexible and cheap and can be use easily.

Fiber Optic Cable: This is the most innovative technology of without wire. It is the most excellent in handling security and data. It only transmits the light waves in place of electrical signals. It is the safest to send data because the data cannot be stolen in this cable. Inner part of the cable are made of plastic or glass in which the transmission of light occurs. up of inner part, which sends in the hinterland after hitting the light is up a plastic flower on top of the glass layer sends.

The sender is connected to a data transmission device that converts the electrical signals into light waves. These light waves are transmitted by fiber optic cable, the second data transmission device transmits these light waves into the widest signals before the receiving computer. Later this fundamental signal is sent to the receiving computer. Fiber optical cables are more empensive than coaxial cable. It tranmit data by 60 megabytes to two gigabytes per second.

Fiber optic is more suitable for more long distance transmission of data but this is the most expensive, speed and transmission medium of without wire.

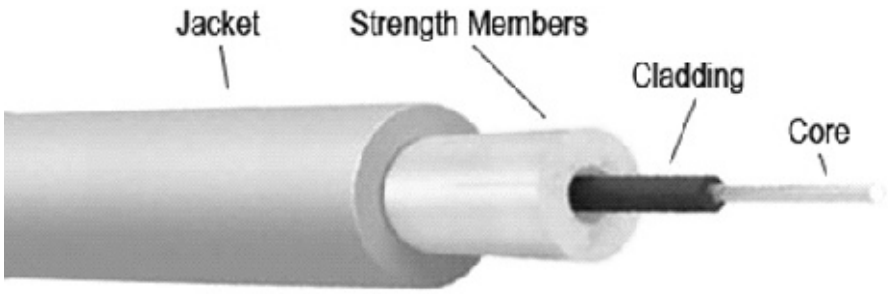


Figure 4.17 Fiber Optic Cable

Unguided Transmission Media: Unguided transmission media is the medium in which radio waves are used and the signals do not move according to the physical path and it is used where it is not possible to reach

Radio transmission medium: Radio waves can easily be generated. It can reach at long distances and it can easily cross the buildings so they are taken more for the work of data transmission. After the transmission radio waves can more in all directions, so the sender and the recipient are not required to be in the same line. In the past radio communication was used in telegrams. Transmissions of countries were used in the work of this radio transmission, on low transmission speed and low frequency (Fre-

quency) but now the transmission of data transmission at fast transmission on VHF (High High Frequency) and UHF (Ultra High Frequency) use the frequencies in many ways.

30 KHZ	Low Frequency	Long Distance Telegraph
3 MHZ	Medium Frequency	Used for sending medium-range non-wire signals.
30 MHZ	High Frequency	Used for sending long-range signals.
300 MHZ	Very High Frequency	Used for F. M. (FM) transmission and short-range mobile transmission
3 GHZ	Ultra-High Frequency	In television broadcast
30 GHZ	Super High Frequency	Use in Radar and Microwave Transmission

Microwave Transmission Media: These signals are also sent and received without the help of cable like TV and radio signals. Microwave signals are broadcasted by antenna mounted on buildings. The sender antenna and the recipient antenna are placed in the same line as the microwave signal only proceeds in one direction. To set the sender antenna and the recipient antenna in the same line is called line of power transmission. Microwave stations located on the ground are set in a type which imposed that they can exchange information with each other only if they can exchange information only when one these microwave stations are placed on the roof of buildings or on the mountain, hence the transmission path remains free. Stations need to be in the same line for microwave transmission.

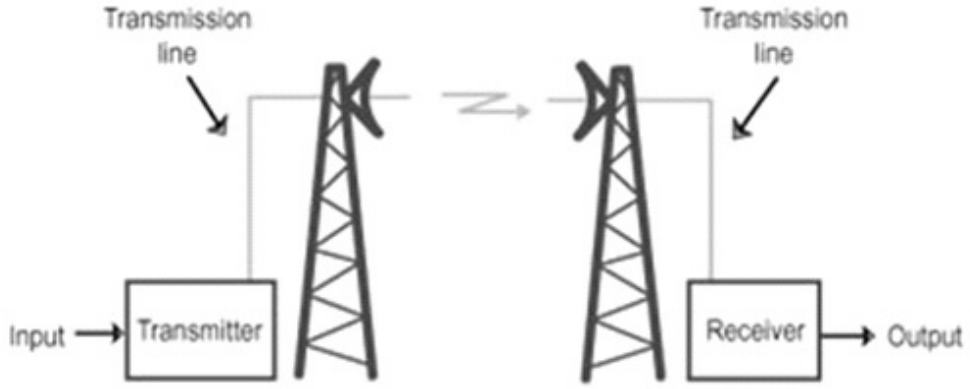


Fig. 4.18 Microwave Communication

Microwave systems use the repeater stations to diagnose the problem of the line off site. The distance of the microwave transmission is limited, so after every 25-30 kilometers the repeaters are placed. The sender station sends the microwave signals that the repeaters receive, than repeaters give them power so that they can reach the distance and signal after providing power Programmed again is transmitted. Microwave transmission cheaper fiber optic cable so microwave signals are used for the transmission of high-speed local and long distance .

Infrared Transmission Media: It is used for short range transmisson. Infrared transmission is cheap, easily used and there is no legal obstacle in using them as it works within the building. There should be no barrier between the sender and the recipient. Infrared medium uses infrared light for the transmission of signals. Light emitting diode (LED) transmits light signals and photo diodes receive light signals. Because infrared signals work very fast, so their data transmission speeds are very fast.

Examples of infrared transmission are remote of TV. Examples: In a large room, many computers with equipment to obtain infrared transmission are equipped with local network such as compute infrared can connect with.

Figure 4.19 Infrared Communication

Satellite Transmission: First time, transmission in satellite was used in 1960 when NASA launched Eco satellite. Satellite transmission can happen only when both antennas in a line. The main difference in satellite transmission and microwave transmission is that an antenna is mounted on the satellite, which is located approximately 3600 kilometers above the equator, the Geo synchronous orbit. This planet remains stable compared to Earth and remains at a point relative to the Earth, due to this, transmissions can be done by satellite system in mobile devices and all the locations can be reached.

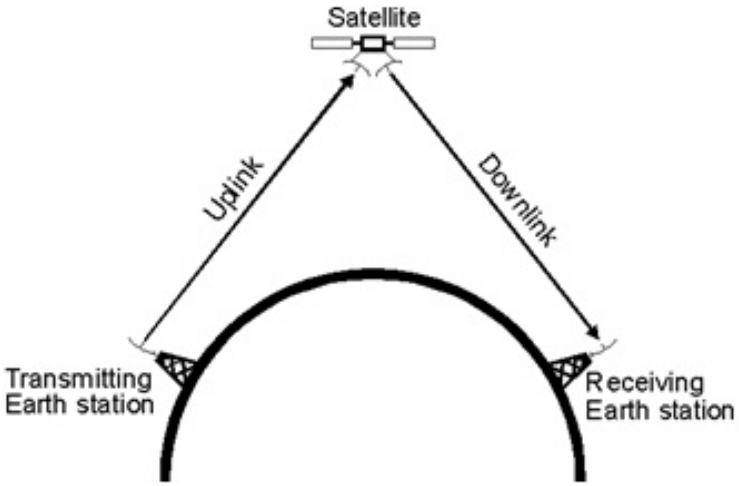


Fig. 4.20 Satellite Communication

In satellite transmission 6 GHZ signals is transmitted by the transmitter in the space. The signal becomes impaired due to long distances. By making this signal powerful by a transponder on the planet and sending it back to the earth at 4 GHz frequency receiver receivesthese signals on the earth. Installing satellites in the classroom is very expensive.

Satellite Transmission Features

1. Life cycle of every satellite takes between 7 to 10 years.

2. The stations located on earth are at a distance from the user. The signals have to be fixed by the high speed transmission medium.

3. Anyone can tap the satellite transmission.

4. In many situations, satellites cannot work because run by solar energy. In the state of the solar eclipse and in the middle of the sun, due to which the satellite ceases to meet solar energy. If the capacity decreases, then they stop working.

5. The shape that sends the satellite and the return frequency of the signs on the earth may be of C band (4/6 GHz) or K4 (11/4 GHZ). The same frequency requires large antenna and blocking stations due to rain and environment have to face.

4.8 OSI & TCP / IP Model

Before knowing about the OSI and the TCP / IP model we also need to know how the Internet came.

If we talk about history, then the history of the Internet begins with the Department of Defense United States. While there were already computers in their different places, there was no exchange of information between them and the information that was exchanged was sent in an external storage, so the Department of Defense took the initiative that the computers of different places can be added together, they named this project as DARPA.

The department of defense and various other supportive departments formed research and some protocols in organizations which could exchange information by connecting computers. The whole process gave the name of the DOD model, which had four layers. After it changed its name to ARPANET and ARPANET presented a model called TCP / IP Model In addition to this, there were 4 floats like DOD, whose names are -

1 Application layer

2 Transport Layers

3. Internet Layer

4. Network Access Layer

The concept of the layer was given to spread the work of network communication in different parts.

Along with Arpanet, another organization, ISO (International Organization for Standardization) presented a model named OSI model, was a model of 7 layers. After the conversation, it was given the status of reference model and the TCP / IP model was given the protocol model.

The TCP / IP model is applicable only in computer networks and if the information is to be read or read about its different layers, then the OSI model is kept in mind..

OSI Model	TCP/IP Model
Application Layer	
Presentation Layer	Application Layer
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet layer
Data Link Layer	
	Network Access layer
Physical Layer	

OSI model facility

1. The big picture of the network can be understood.
2. It is possible to see hardware and software working together.
3. It is easy to know what new technology has developed in it.
4. Easy to troubleshoot problems of different networks.
5. Can be used to compare basic functional relationships on different networks.

Information about various Layers of OSI Model:(Top to Down)

1. Application layer: This is the top level. Various methods are used to manipulate data (information) in this layer. The result for the user is the transfer of disturbing files also used in this layer. Mail services, directory services, network resources etc. are provided by the application layer.

2. Presentation Layer: The presentation layer takes care that the data should be change in such a way that the information of the receiver is understood and able to use the data. This layer plays the role of translator.

3. Session Layer: This layer works as synchronization of interactions between two devices. In order to avoid any harm to the data, the presentation layer properly synchronizes data from the presentation layer on the other side.

4. Transport Layer: This is primarily the most important layer, whose main task is to transfer the data from one computer to another computer responsibly. This layer decides that the transmission of data will be on parallel path or on single path. The main functions of this layer are multiplexing, segmentation and addressing. This layer breaks the data into small pieces.

By which the data can be transmitted correctly is called the Protocol Data Unit (PDU), The Protocol Data Unit on the Transport Layer has been given the name of Segment. The Transport Layer also works along with addressing all these, which helps in recognizing the applications in the network. Port numbers are used as addressing on the Transport Layer, which ranges from 0 to 65535.

If the data sent by the transport layer does not reach the recipient correctly, then it is the responsibility of the transport layer to resend that data and ensure that the data has reached the correct type and shape correctly.

5. Network Layer: Network Layer transforms the packet into the segments connected to the transport layer by adding information to the packet. The main function of the network layer is to send the data from one network to the other network, which is called routing. The table which is used by the network layer is called routing table, from which it determines which way would be better to send data if there is no way right for any reason is not the router selects one way of your writing table.

Network layer routing also gives addressing which we call IP addresses.

6. Data Link Layer: Data Link Layer Network layer transforms the packet from network layer to its frame by converting it into a frame that is a bits of bits. Data link layer also detects errors and also works for correction along with this, the Data Link Layer does two important functions and the following are:

1. How to use the medium

2. Assign the MAC Address

7. Physical Layer: Physical Layer transforms frames from data link layer into physical signals. It is also responsible for turning on the layer link, maintaining it smoothly and closing it.

In the computer networks, the data is generated from the application layer and processed from different layers and accesses the physical layer, it is later converted into signals. These signals move with the media to reach another device. Here the device returns these signals changes to the required information. This information comes back from the other layers of the application layer, which the person working or the user gets,

the application of data is taken from the layer to the physical layer called encapsulation and moving data from the physical layer to the application layer is called dencapsulation.

Every layer in the network fulfills its work responsibly.

4.9 Advancements of Networking

When two or more computers are added to share information and use of resources, then it becomes the network. A local area network, sometimes too far beyond the capacity of the transmission medium it has to be done that this network equipment helps local area network to reach long distances. This network device can be used for transmission of two different networks. Can also add common network equipment is as follows: -

Modem: Translation can happen to anyone from analog and digital when digital data is to be operated from the telephone line, then the digital data has to be converted into analog data because the analog data is transmitted faster Occurs. The sender's technique here that wants to convert digital messages to analog messages is called Modulation, the message recipient receives the inverse work, i.e. the analog signals are replaced by the demodulation technique digital signature.

Modem changes the digital signals of the computer to analog singles so that their translation can be transmitted from the telephone line to the model's signals in the sender's digital signals, thus with the help of Modern, two different computers can be translated by phone line. Modem's data transmission speed bits are measured in seconds.

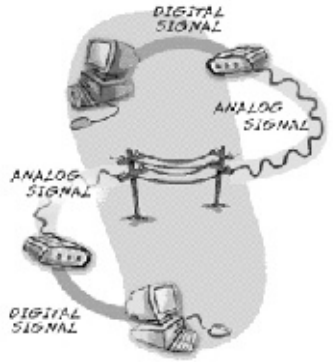


Figure 4.21 Modem Communication

Hub: Hub is a tool by which many computer in a network can be physically added. In this device first information is collected and later it is transmitted to computers so it is said interface unit. Only a few bits of data can be collected, so its transmission through more speed. It is a device that gets data first makes them powerful and lets them

transmit to the other computer because HUB make the data powerful so it also makes the signals unencumbered with the data powerful. It is a powerful wiring center which can be used printers, scanners, computer to connects with LAN. One device can only transmit data by hub at a time. Hub is a point by which the problem can be diagnosed by detecting it and its data transmission speed is 10 megabits per second. HUB are of two types -

1. **PASSIVE HUB:** This is a simple hardware tool. It can get data signals from multiple cables in the network.

2. **ACTIVE HUB:** It is a complex hardware tool that can test and control the information given by all different networks.

Switch (SWITCH): After seeing the address of the receipt of the frame, the switch starts sending frames to their destination. Do not wait for the entire frame to arrive before send it. It removes the errors of signals of data packets when data packets come in, the receiver is detected from their header and then they are sent to the receiver. In the frame the bits are applied in a predetermined order in which bits are detected for destination detection, fault control, receiver data, and information about the end of the frame.

Depending on how many computers can be added to a switch, it is known at its speed and depending on how many ports it has in it. Switches are the fastest and give different bandwidth for each device. The switches increase the efficiency of the network by reducing the additional traffic, and also ensure that all the devices can be transmitted at the same time. The switch keeps separate small buffer memory for all those devices connected. When it receives the data packet, it saves it in the buffer then after seeing its address, it converts it to its destination. If the location from which the data package has arrived and its address is the same, then the switch removes the data package. And does not transmit them, thus reducing the transmission of unnecessary data packets, it reduces data traffic and in other words the switch is a sensible hub .

Router:

This device is used to transmit data between two networks. When any network is built after connecting two or more small network than router makes a table of all routes/paths which is used to identify route between two networks. Router uses best path to sent packets.

If any path goes down it sends packet via another route.

Router not only sends data it also chose best path. They send information to their neighbours which sent to his neighbours. It also works as firewall which stop un-

wanted packets.

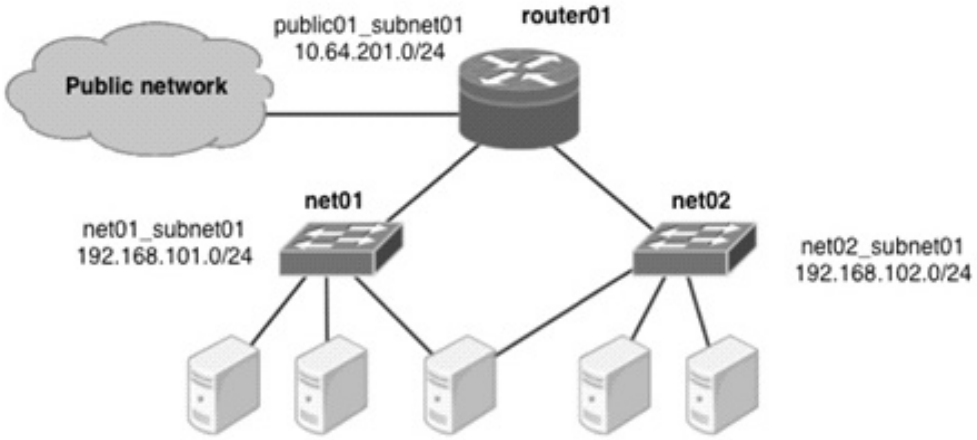


Figure 4.22 Router

GATEWAY: This tool connects to uneven network or some networks want information about how they can be streamlined after data arrives. When we connect two or more networks with two different operating systems, then the gateway are required. The address of the gateway messages and the necessary protocols change, they send them from one network to another.

The gateway transmits the group of instructions from the sender network to the instructions of the receiver network. The gateway usually has software in the router, the gateway can understand the instructions to all the networks connected to it, and it can change them from one to the other. The requests of the computers connected to the server are changed into instructions conveying the message of the server to the receiver the computer changes to the understanding of computers.

4.10 Internet Protocol (IP)

IP addressing is an important function of the network layer which can make transmission possible even if it is in any network of its device or another network. IP (Version 4) and IP (Version 6) provide graded addressing for carrying data through both packets. Design, implementation and an effective IP plan will ensure the network will work effectively and efficiently.

It is also important to know that computers only work in Binary which is displayed by Zero (0) or One (1). The computer user / operator change the language given to it in the binary.

For example, the binary code for A written by ASCII standard is 01000001.

It is not necessary to know how words change in binary at this time, we need to

know the use of binary for IP address.

IP (Version 4): IP (Version 4) is a binary address of 32 bit. Packets senders and recipients on this network layer include this unique information. As a result, packet get its 32-bit sender and 32 bit recipient's address. Changing binary to decimal is based on mathematical positional notation. Positional notation, that is a digit gives different value according to the location. In the positional notation, the number is called the radix. Radix is 10 in decimal system.

We write the 32-bit binary address in the Dotted Decimals format because humans cannot read and remember the binary properly and the computer does all its work in binary.

This 32-bit binary address is shown in a group of 8-bit or octet, and the group of each 8 bit remains separate from a dot (dot).

For example, 11000000 10101000 00001010 00001010 can write binary address in dotted decimals 192.168.10.10. Binary number system have Radix 2, so the number is either 0 or 1. Posts in these 8-bit binary / binary numbers represent these quantities:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

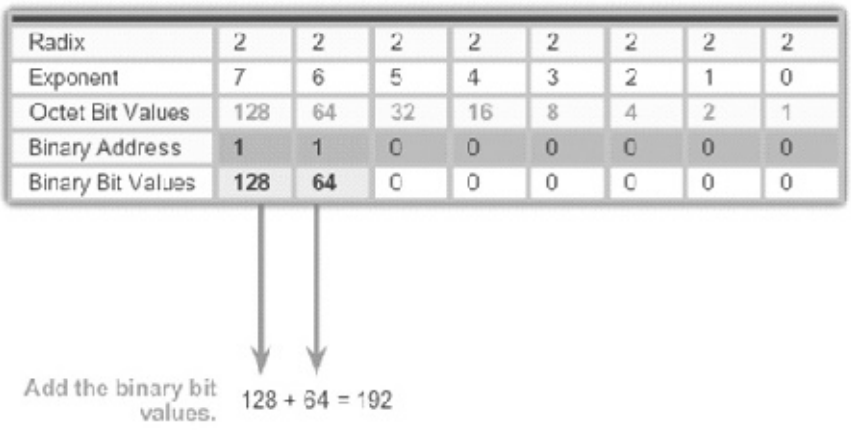


Figure 4.23 Internet Protocal

Every octet is made of 8 bits in which the bit is either 0 or 1. The quantity of 4 bits or 8 bits is in a series of 0 to 255. The value of the location of each bit is directly

opposite direction i, 1, 2, 4, 8, 16, 32, 64and 132. If decimals are to be replaced by binary, then divide the given value according to the numbers mentioned above, in place of the number of those obtained from them, place 0 and 1 in place of others.

For example, if the 155 is to change binary I would have the following split

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
128			16	8		2	1
1	0	0	1	1	0	1	1

155's binary will be 10011011

If any binary change in decimals then they can change according to above. Binary values are the value of the bit I value, keeping it according to its position and add it to the end.

The IP address has two parts in which one part is related to its network and the host.

IP Addresses are divided into 5 classes

Class A

Class B

Class C

Class D (Multicasting)

Class E (Reserved for the future Development and Research)

The class of that IP is detected from the first octet of any IP. The range of IP ranges from 0 to 255, which is as per the classes.

Class A: 0-127

Class B: 128-191

Class C: 192-223

Class D: 224-239

Class E: 240-255

For example, class of 10.10.12.50 is A because its first octet is 10 which come in the range of class A.

The subnet mask determines how much of the IP address belongs to the network, and how much the host. According to each class, different subnet masks are defined as follows.

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

Class D:Not defined

Class E: Not defined

In class A the first octet is 255 which means values of 8 bits are 1, so the first octet of the IP address will be associated with the network, after which the remaining 24 bit will remain associated with the host. Similarly, the first and second octets of class B are 255, which mean values of 16 bits are 1, so the first and second octet of IP address will be associated with the network, after which the remaining 16 bit will remain associated with the host. Similarly, the first, second and third octets in class C are 255 means the values of 24 bits are 1, so the first, second and third octet of the IP address will be associated with the network, after which the remaining 8 bit will remain associated with the host.

IP (Version 6): Slowly as the Internet user started to grow, the address coming in the IP V4 started to end and the need started to increase so the IP (Version 6) was developed. The IP V6 does not have the concept of a class. This is the address of 128-bit which is written in Hexadecimal.

This is an example of the 2001: 0db8: 85a3: 0000: 0000: 8a2e: 0370: 7334 IP V6 address. This address can be further shortened leading zeros in a group can be removed. One or more consecutive groups of zero values can be replaced with a single empty group using two colon consecutively.

2001: db8: 85a3: 0: 0: 8a2e: 370: 7334

2001: db8: 85a3:: 8a2e: 370: 7334

4.11 MAC Address

MAC Address is a unique and physical address given to any network card for physical network for communication. The MAC address is used by IEEE Network technologies such as Ethernet and Wireless and works on the data link layer. The MAC address is given by the organization that creates any interface card and the read-only chip on the hardware is stored it and cannot be changed. MAC are made according to the standards of Institute of Electrical and Electronics Engineers (IEEE) and is the following - MAC-48, EUI-48 and EUI-64

The MAC address is also called a burn address or hardware address. MAC Address is the address of 48-bit which is arranged by 6 groups of 2 numbers of hexadecimal. These groups are separated from Hyphen (-). Mac address is usually divided into parts, the first 3 groups are given to an organization by the Institute of Electrical and Electronics Engineers (IEEE) and the last 3 groups are like serial numbers on the cards created by any organization, thus any MAC Address does not match any other MAC address.

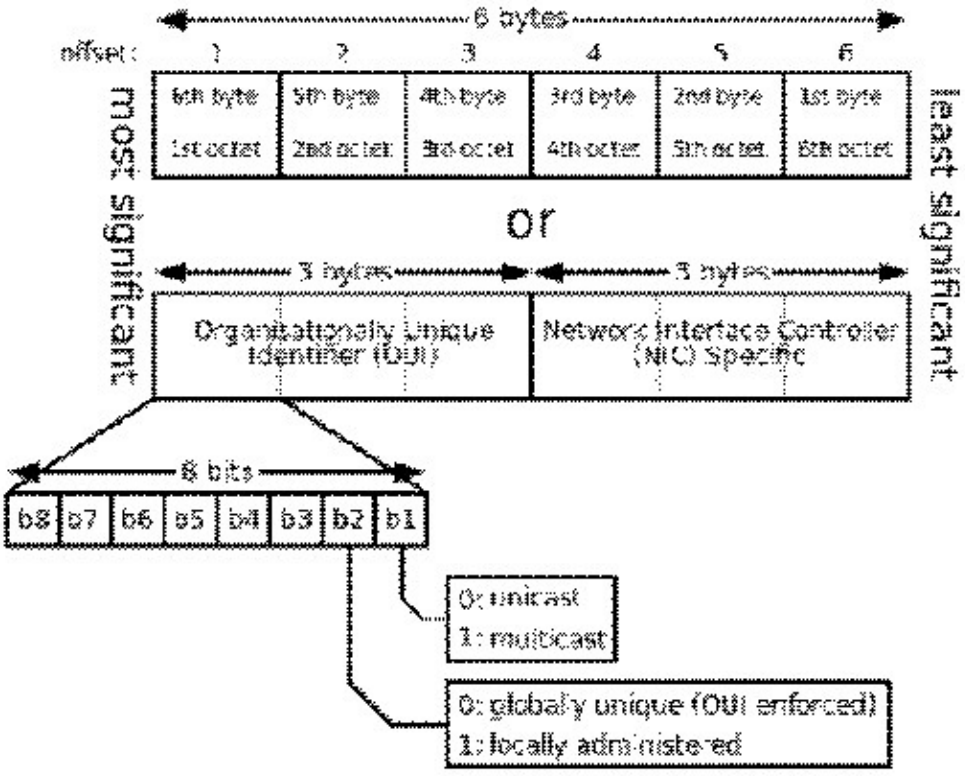


Figure 4.24 MAC Address

4.12 Subnetting

It is already known that the network runs well and smoothly with good planning, implementation and good management of IP. IPV4 have two types of hierarchy that are related to the host and the network. Any router sends any packet from one network to another network with the information related to the network. Once the network portion is detected, the host address only works for the address of the computer to which to send the packet. As the number of networks increases in organizations like this, the two types of taxation seem insignificant. It is now necessary to redistribute the network gradation. Which network can now divide three orders - Network, Subnetwork and Host data packets are transmitted rapidly by dividing the various modules of any network and it creates a cosmic network.

It is also known to us that the part of the IP is related to the network and which part is related to the host, and the subnet mask is done according to the classes and the subnet masks are already there.

Netting of any network: Every network has a valid series of host addresses. All the computers or devices or hosts present in the same network keep the same subnet mask and are the members of that network. IPV4 address has 32 binary bits that are related to the network and the host. The Subnetting is done by giving the host bits to the network. How many subnetworks of any network will be made depends on how many bits are given from the host by network or how many network networks have taken over the host.

For example, if 1 bit is taken then 2 subnetworks, 2 bit is taken then 4, 3 bit is taken then 8 subnetworks will be created. As host bits will be reduced, any network address will also be reduced. A network of class C consists of 24-bit network and 8 bit host if host is given 8 bits to 1-bit network, then the host will now be able to save 128 host addresses, which means that earlier this network was 256 hosts and this was a network. Now this network has broken into two pieces and hosts are now broken into pieces. There will be 128 - 128 host addresses in every subnetwork and now the network will be 25 bits than 24. Network bits can be written as slash (/) after any address such as 192.168.1.0/24.

"In the simple language it said, that the subnetting is transfer of bit from host network".

Any network is the first unique network addresses that represents any network and the final address is Broadcast Address which is used to send information to all the devices in any network. According to Manako, network address and Broadcast address cannot even be assigned to the device. The address of this can be assigned to

computers or other devices. According to this, 2 addresses cannot be taken from any network.

For example, if the host part of a network is 8 bit, then there will be a total of 256 host addresses, 2 of which cannot work, then only 254 addresses can be used. All these are calculated according to their class because in every class there are different types of bits hosted by class.

The question of subnetting can be asked in two ways - according to the network requirement and according to the host's requirements.

The question is according to what is required it is calculated according to how many bits are to be placed in the host part or how many bits have to be given to the network part. Calculate the number of which it is needed in the power of 2, giving or keeping the same bit according to it.

We will consider subnetting in some examples -

1. 192.168.1.0/24 Network subnetting in such a way that its four networks will be created

Network class:

Subnet mask of class:

How much is to keep or give:

How many networks were created?

How many host networks are left?

When submitting this network, we have to answer the questions written above.

Remedy: The class of the network is C, which is identified by the first octet of this address. The subnet Mask of Class C is 255.255.255.0 which we have already read. We will estimate how much bit to take or take, we need to create 4 subnetworks, and we need to give 2 bit network to 4, 2, 2. This network of sub-networking has 24 bit network and 8 bit host, now we have to give it to the network from 2 bit host, then the network will be 26 bit and the host will be 6 bit. Network address can now be written as follows 192.168.1.0.26.

Now 4 parts of this network or subnetwork are created and host address is equal to equal parts. The host part has 6 bit remaining, that means 2 to the power 6,

each network will have a total of 64 addresses, 2 of which cannot be used, 62 addresses can be assigned to computers or devices.

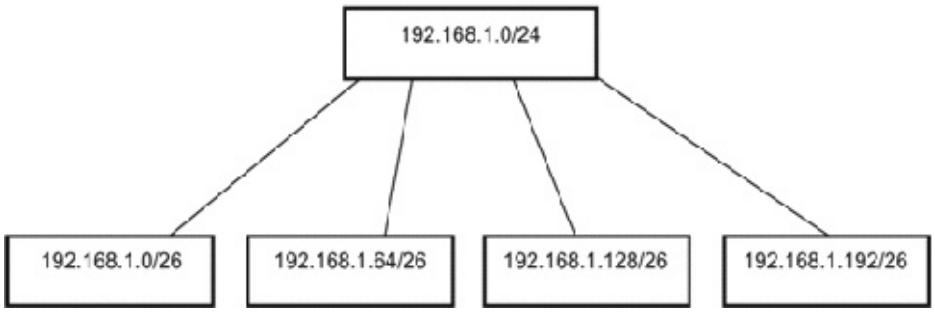


Figure 4.25 Subneting

4.13 Planing of IP address

An IP address plan is an important task that needs to be done in the right way. IP address is a very valuable resource in the network of any organization, which needs to be used as per the need. New computers or devices cannot be added if any network address is over.

In the conventional subnetting all the subnetworks are given the same number of addresses. It is good only when all the essentials of the networks are usually not done.

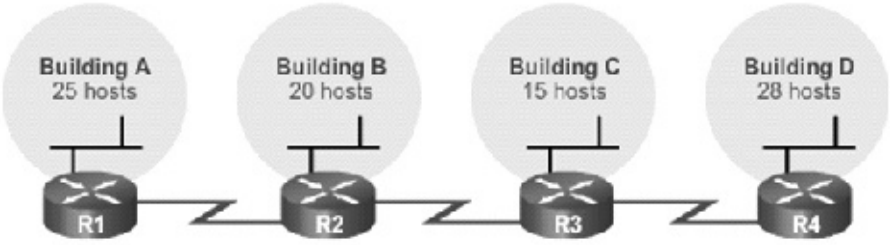


Figure 4.26 Networks with the need of a different host

According to Figure 4.26 a total of 7 networks are needed with 3 wide area networks (WAN) and 4 local area networks. According to conventional subnetting, if divided, the network will be required to deliver from the 3 bit host which will create total 8 networks and every network has a power of 5, 32 addresses and our need is met.

But by dividing this way many addresses are useless which will not be used. According to Figure 4.26, there are 3 wide area network in which 2 router is con-

nected, 2 addresses will be required but every interface of the router becomes a separate network, then 2 other address (network and broadcast), total 4 is required but 32 addresses are being given, resulting in 28 addresses being lost.

It can be saved from variable length subnet mask (VLSM) technology. VLSM technology helps to divide any network in an unequal manner. VLSM technology is similar to traditional subnetting, but in the past it is subnetting a network, and then subnetting the subnet network again, which gives network of uneven subnet masks and the absence of usage of the addresses ceases to an extent is there.

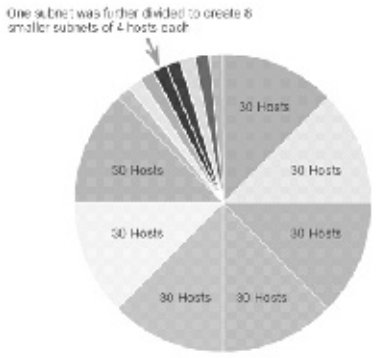


Fig. 4.27 Network subnetting by VLSM

4.14 Wireless

Wireless networks allow any device to bundle without any cable. Wireless LAN (W LAN) is a classified part of wireless technology that is usually used in homes, offices and campus. This technique works on radio waves for instead of wires. It can be added to an already-connected LAN network, so that the user can use the wireless facility anytime in that area. This technique is similar to Ethernet.

Wireless technology and standards: Productivity in today's time is no longer restricted to a certain place or work for a set time period people are now connected to the office at any time and place for the airport or home now employees can see their emails, voice messages, and new information anytime. Users now expect someone to be connected to the Internet without interrupting the connection.

Wireless has the following advantages -

1. Flexibility to do work, increase productivity, move forward and create a friendly environment as needed.

2. Any user can connect anytime to the internet. There is no need to be in any one area or place.

3. Reduction in the cost of productivity coming from wireless.

It has the following technology

1. Wireless Personal Area Networks (WPAN): This technique works only in the area of few feet. Bluetooth is an example. With the help of Bluetooth, the user who has the mobile can always send the data to each other.

2. Wireless LANs (WLANs): This technique works only in the area of some 100 meters. This can be done separately from the internet at home, office and campus.

3. Wireless Wide-Area Networks (WWANs): This technique works in a very long range area. This technique is connected to home, city, and country. Satellite and mobile communications are examples of this.

All wireless devices work in the range of radio waves of electromagnetic spectrum. Regulation and allocation of radio frequency is the responsibility of the International Telecommunication Union (ITU). Variations of different frequencies and bands are allocated for various purposes. This frequency comes mostly after payment, while some frequency is free, such as Industrial, Scientific and Medical (ISM) and the National information infrastructure (NII) frequency bands.

WLAN (Wireless LAN) works at 2.4 GHz of ISM band and 5 GHz of NII. Wireless Communication works in the magnetic spectrum of 300 GHz from 3 HZ of radio waves.

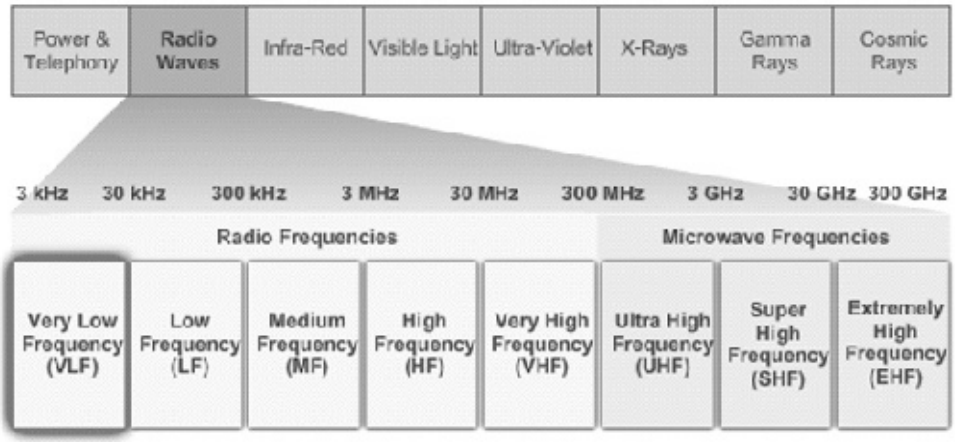


Fig. 4.28 Magnetic spectrum

Wireless lenses near these devices have transmitters and receivers to work on select frequencies which are low -

2.4 GHz (802.11b / g / n / ad)

5 GHz (802.11a / n / ac / ad)

60 GHz (802.11ad)

4.15 Standards of Wireless

IEEE 802.11: The WLAN standard defines how the unrecognized ISM frequency band (RF) is used for the mac layer of the physical layer and wireless link in the frequency band.

Various implementation of IEEE 802.11 standard has been developed over the years. The following are highlighted on these standards: -

802.11: This was developed in 1997 and obsolete. This technique works at 2.4 GHz and provides a speed of 2 Mbps normally LAN used to work on 100 mbps while it worked on 2 Mbps and an antenna that used to be the sender and recipient of the equipment used in it.

IEEE 802.11a: It was released in 1999. It works on a low crowd frequency of 5 GHz and speeds up to 54 Mbps. It works on more frequencies so its area is reduced and it lessens the walls.

IEEE 802.11b: It was released in 1999. It works on the frequency of 2.4 GHz and provides speed of 11 Mbps.

IEEE 802.11g: It was released in 1993. It works on the frequency of 2.4 GHz and speeds up to 54 Mbps. This previous technology is compatible with IEEE 802.11b.

IEEE 802.11n: It was released in 2009. This works on both frequencies. 2.4 and 5 GHz. This technique speeds 150 to 600 Mbps. It has more than one antenna on the device coming to work which has MIMO (Multi in Multi Out) technology so that they transmit extra data transmission. It supports up to 4 antennas. This is compatible with previous technologies 802.11a / b / g.

IEEE 802.11ac: It was released in 2013. It works on the frequency of 5 GHz and gives speeds of up to 450 Mbps to 1.3 Gbps. This is compatible with previous technologies 802.11a / n.

IEEE 802.11ad: It was released in 2014 and is also called WiGig. It works on the frequency of 2.4, 5 and 60 GHz. And can speed up to 7 Gbps so this is the fastest wireless technology.

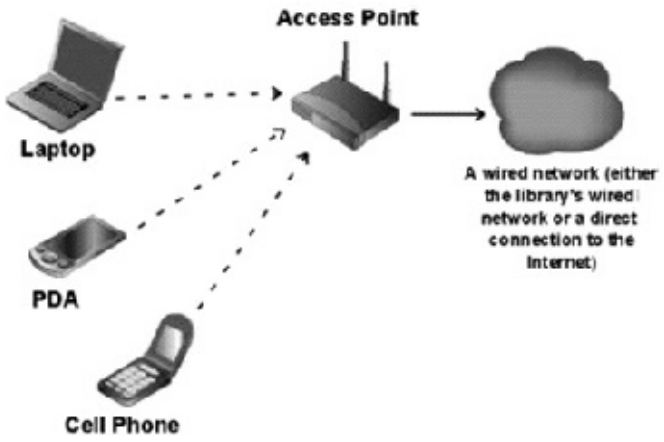


Figure 4.29 Wireless Network

Wireless Security: It is difficult to secure a network connected to a wireless network. Security is an important priority for anyone who is using network administration.

The wireless network was related to the intelligence information as far as the network is approaching or remains open. An attacker may not have to physically enter the workplace to gain access to a WLAN. Therefore it is very important to protect the wireless network.

Wireless attacks can occur as follows -

Wireless intruders

Rogue apps

Interception of data

DoS attacks

Ways to Protect Wireless (Securing WLANs)

Security is always a matter of concern as the range of network limit varies. Wireless signals can travel through the concrete medium of the roof, wall, outside of the house or office. Wireless without any security is equal to leaving any Ethernet network in open use.

The following security arrangements to provide wireless security -

SSID cloaking: In this, the beacon frames left by the wireless device are discontinued so that the wireless network is not visible in any device. The device to connect to the wireless network can be added only after complete information of the wireless so no network can detect it.

MAC address filtering: In the wireless router, you can create a list of physical MAC Address so that any computer or device can be switched off to accommodate that network.

Both of the above methods can be broken so that the wireless network is required to encrypt and authenticate, therefore 802.11 standard has two types of methods which are low -

Open system authentication: Any customer or user can easily connect to it where security does not matter much. This kind of safety cafe, as the hotel offers free internet access in places, where security is not kept safe.

Shared key authentication: In order to encrypt the communication between the computer and the router, a key or password is inserted in the router without which any customer or user can connect without informing. The following security arrangements are for encrypting or hiding data.

WEP (Wired Equivalent Privacy): This is the first generation of authentication. It uses the key as a password. This takes the RC4 algorithm to work.

WPA: This uses the Temporal Key Integrity Protocol (TKIP) encryption algorithm for strong security.

WPA2: This is a way of providing security to the wireless network according to the industry standard; it takes AES (Advance Encryption Standard) instead of TKIP, which is a powerful way.

4.16 Congestion Control

Congestion control is the technique and method which fixes before the crowd of packets in the network meaning it does not happen or it fixes it after it is done. It is of two types

1. Open loop Congestion Control (Prevention)

2. Close Loop Congestion Control (Removal)

Open Loop Congestion Control: In different ways different strategies are used to prevent congestion. In this technique the congestion is either stopped by the sender or the recipient's place.

The following policies are used in this technique:

1. Retransmission Policy: In this policy if the sender feels that the packet sent by him has been destroyed on the way then that packet is re-sent but it can generate congestion. Good policy is required to stop this. In this a clock is used so that there is no congestion. The TCP protocol is already made in such a way that the possibility of congestion will be less.

2 Acknowledgment Policy: In this policy if the sender expects a confirmation of every packet sent, if any packet is not confirmed on receipt of the recipient, and then reduces the speed of sending the sender packets. This reduces the probability of congestion.

Close loop congestion control: After the conjunction of open loop congestion control it is rectified, various techniques are used by different protocols.

1. Backpressure: The node congestion that is in this technique stops receiving the data from the node before it which can increase the angle on the first node, but do the same as the first node is there. This is called node-node congestion control. This echnique is only used in the virtual circuit network

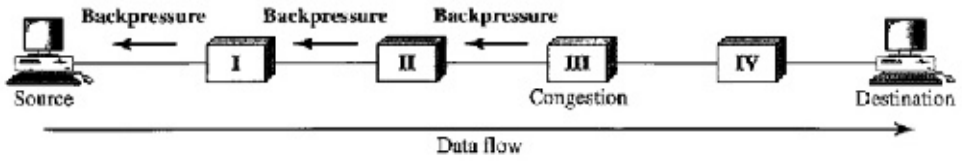


Figure 4.30 Backpressure Congestion Control

2 Choke Packet: In this technique a special type of packet choke packet is sent to the sender. It is almost similar to backpresure technology but sent to the node before it in Bekpresure, the information is sent directly to the sender and information is not sent to the middle node.

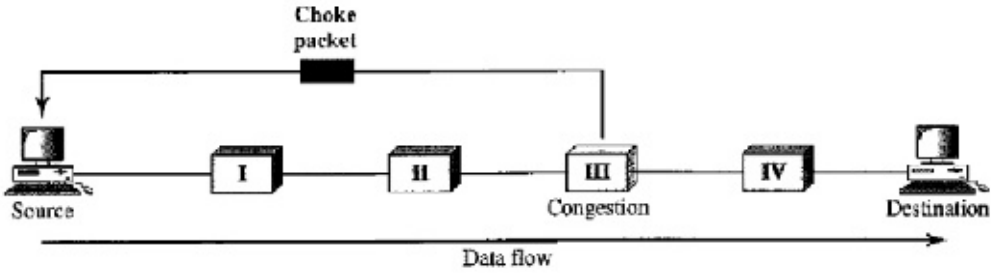


Figure 4.31 Choke packet congestion control

4.17 Quality of Service

The quality of service in computer networks means Resource Reservation for any type of communication. The quality of service is to given priority to high quality of any user, application and data flow. According to quality of service certain factors such as bit rate, delay, jitter and bit error rate should be according to quality.

Generally speaking the quality of service is meant to provide a high level of service.

Flow characteristics: There are mainly 4 types of flow characteristics

1. Reliability : Reliability is a feature. If the reliability is low then its direct intention is not to destroy the packet / acknowledgment which inspires retransmission.

2. Delay: The delay between the recipients from the sender can be tolerated to a certain extent in some year. But some applications such as telephony and audio conferencing cannot be delayed.

3. Jitter: The relation of jitter is delayed in the same packet related to the packets. If all the packets are reaching the distributor from the sender to the seller at the same time, not the jitter, but if the packets are reaching different delays, then the jitter is for the packets going to the network and not good for the user.

4. Bandwidth: The direct connection of bandwidth is at the speed of packets sent at one time. Separate different types of bandwidth are needed. If the bandwidth is more than or equal to the required bandwidth, the application will work properly otherwise the packets will start to be destroyed, which in turn will result in the packets that are not good for the network and computer users.

4.17.1 Techniques for improving the quality of service:

1. Scheduling

2. FIFO Queuing

3. Priority Queuing

4. Weighted Fair Queuing

4.18 DNS (Domain Name Service)

4.18.1 Introduction : DNS is a hierarchal distributed system which changes the domain name to IP. The computer does not understand the man made name and works in the binary while the human does not understand binary and works in own language so it becomes necessary that there is a system that can convert the names of human language into the address of the computer network address.

For example, IP 216.58.196.3 of www.google.co.in. It is possible from DNS.

4.18.2 History: In the days of internet, there were some computers in the world whose IP address was known to each other. Later, these computers were given the names of human or human languages which were converted to the IP from the computer's operating system File Hosts (Hosts.txt) in which the IP address was written in front of the computer's name.

But as the Internet promotion started, this work also started to become smile so now there was a need for a system to do this easily.

Paul Mocapetris created the Domain Name System in the University of California, Irvine in 1983 and wrote the first implementation at the request of John Postell from ISI.

4.18.3 Domain Name Space: Domain Name System is a tree-like data structure. This tree structure is divided into several joints which start with a root or dot (.). The root domain or dot (.) is divided into several categories called top level domains.

For example com, org, net

Under the top level domain, there are secondary level domains in the pedestal structure that the user can choose their own requirements. A domain name occurs in all categories if a domain name is not in a category it can be taken from another category. Secondary level domains are divided into subdomains which the user can do according to their wish.

mail.google.com

Here is the mail subdomain, Google is the secondary level domain name and com dot top level domains, and all of this is divided by dot (.)

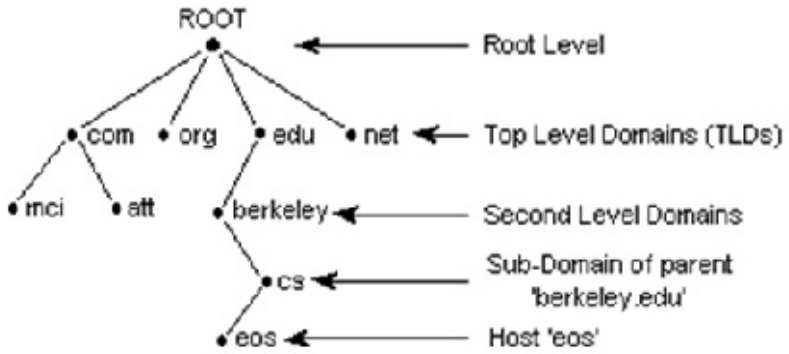


Figure 4.32 Domain Name System

Each DNS server stores information about any domain in the zone file. Any server has the following resource record (Resource Record).

1. NS record: This record keeps information on any domain's authority.

2. A record: This record keeps the details of the IP of any domain.

3. CNAME record: This record keeps information about the domain name of any domain, its other name.

4. MX records: It keeps information about its mail record.

Every computer or network device is inserted into the DNS entry so that it can locate the IP from the domain name. If no computer or network device has the entry of DNS, it will not be able to locate or contact any other computer or device by the domain name. The following is the method of IP address of any computer or network device.

Any computer contacts the DNS server in its DNS entry for any other computer, and asks its own question (domain's IP) if that DNS server has the address of that domain then it answers.

If that server does not respond to that domain, then it asks for itself or the latter of the DNS server.

If any server does not respond then the root server is asked.

4.19 Email System

Email is the most popular service of internet services. In the early days of the internet only small and text messages could be sent by email. But now a days email is a very complex system. With the help of mail, text, images, video can also be sent. Email information can be sent simultaneously to more than one recipient.

Email service: Email has the following services:

1. It can be easily used.

2. Information can be sent to any corner of the world in a few seconds, so it works very fast.

3. When someone has to answer an email it keep up with the information already coming.

4. If a user is not able to use his email or is out of work he can use the email sending technique in which the user who has email will automatically go to the mail, whatever information the first store is.

5. Older postal system used paper while email uses electronic data so it is environmentally friendly.

6. Email can be read and respond to any device such as computer, laptop, mobile, tablet.

Architecture of Email : Before understanding the architecture of email it is necessary to understand some of the key elements.

1. **Mail User Agent:** This is an application or program that lets the user write and send mail.

2. **Mail Transfer Agent:** This is usually a server that serves to send email to each other.

3. **Mail Delivery Agent:** This is the mail server's technology in which the address of the receiver of the mail is given to him in the inbox.

4. **Post Office Protocol :** This is the protocol to receive mail from the server or the user's application or program from the server.

5. **SMTP (Simple Mail Transfer Protocol):** It comes with a user's program or application to send email to server and server to another server.

6. **Internet Message Access Protocol:** This is a new way of achieving a new one which uses some modern technology.

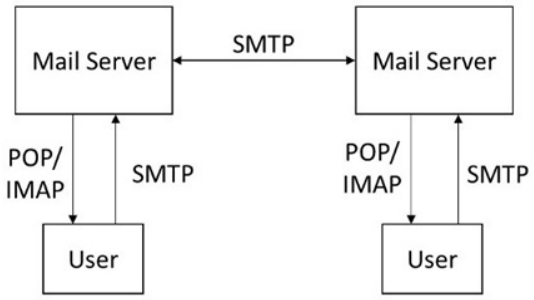


Figure 4.33 Mail system

We will try to understand the architecture of the email from Figure 4.33. as written below -

7. Writes a user with any user program or application or adds an image that is called attachment. When writing an email some important information such as the address of the recipient, addresses the subject of the email which is called the email header.

8. Now this created message is sent with the help of SMTP protocol to the email server whose service is taking the user.

9. Now the server matches the address of the recipient's domain to the domain of the email header sent by the sender. If the recipient's domain matches the domain of the server then the server finds the user's name in its database. After getting the name the server enters the mail in the Inbox's Inbox while working as a mail delivery agent, which is read by receiving it via the POP / IMAP protocol.

10. If recipient and recipient's domain is not available then the server sends that email to its related server via SMTP protocol. Now the second server also uses the above method to put email in the inbox of the user.

Difference between POP / IMAP: Both POP / IMAP protocols are used to bring email from the server to the user. But there are some technical differences which are below: -

1. As soon as the user application or program opens the user name and password, then the POP protocol downloads the entire email to the server from the server / client (Client) while POP works in two types, either one of the email the copy keeps the server or after download it destroys the copy. POP downloads the

entire email with an attachment.

2. IMAP is more powerful and complicated protocol than POP and gives more features to the user.

3. IMAP only downloads the email header instead of downloading the entire email so that the user knows that the mail has come from and what is his subject.

4. If the user can download an email without any email in his inbox, he can find it.

5. Do not download the entire mail saves bandwidth.

6. Users can create new folders according to their convenience.

Important points

1. The style of connecting computers is called topology.

2. Network can be broadly divided into three types - LAN, MAN, WAN

3. Broadcasting medium is the path on which the sender and recipient exchange information.

4. Fiber optic medium transmission is the fastest path.

5. Protocol is a set of rules.

6. All the tools in the star topology are connected to a central device.

7. OSI is a reference model and TCP / IP is protocol model.

8. In a simple mode the data can go in the same direction, the recipient can't send data back to the sender.

9. Microwave signals are broadcasted by antenna mounted on buildings.

10. OSI models carry 7 layers and 4 layers in TCP / IP.

11. Coaxial cable used in the television.

12. An analog signal is used to send the sound.

13. Computer does its work in binary.

14. Router is used to send packets from one network to another.

15. IPV4 is 32 bit binary address and IPV6 is the address of 128 bit.

16. The IP address of the network layer is the addressing scheme.

17. MAC address is a physical address which does not change. It will be on read only chip on the hardware.

18. Subnetting is done to split a large network into smaller networks.

19. Modem changes analog signals into digital signals and digital signals into analog signals.

20. In Network, hub is a powerful wiring center.

21. The gateway transmits the group of instructions from the sender network into the instructions of the recipient network.

22. 32bit binary address in IPV4 is shown in a group of 8 bits or octets, and each 8 bit group remains separate from a dot (dot).

23. IPV4 has 5 classes. These are A,B,C,D and E

24. Wireless network allows any device to interact without any connection. Wireless LAN (W LAN) is a classified part of wireless technology that is usually used in homes, offices and campus.

25. Conjunction control is the technique and method which fixes the crowd of packets in the network even before it does not mean it does not happen or it fixes it after it is done.

26. The quality of service is to give priority to high quality of any user, application and data flow.

Exercises

Objective Type Questions

1. Which one is the transmission medium?

   (A) Modem (B) Multiplexer

   (C) Hub (D) Coaxial Cable

2. The oldest and more usable transmission line is?

   (A) Coaxial Cable (B) Fiber Optic

   (C) Twisted Pair (D) None of the above

3. What is WAN?

(A) Wire Area Network (B) Local Area Network

(C) Wide Area Network (D) Wire Accessible Network

4. How much layers the OSI model have?

(A) 4 (B) 2

(C) 7 (d) 5

5. Which tool sends packets from one network to another?

(A) Router (B) Hub

(C) Switch (D) Gateway

6. What kind of transmissions does the wave go in all directions?

(A) Radio link (B) Microwave

(C) Infrared (D) Satellite

7. Which layer of TCP / IP model works as transportation?

(A) Application (B) Transport

(C) Network Access (D) Internet

8. Which device do we use to increase the power of analog signal?

(A) Amplifier (B) Transmitter

(C) Repeater (D) Transponder

9. Which of the following equipment is used in the telephone line?

(A) Router (B) Modem

(C) Switch (D) Hub

10. Which of the following can also work as a firewall?

(A) Router (B) Modem

(C) Switch (D) Hub

11. In which numbers system computers writed IP address?

(A) Binary (B) decimal

(C) Hexadecimal (D) None of these

12. How much bits in IPV6?

(A) 128 (B) 64

(C) 28 (D) 32

13. What does the class D of IP call?

(A) Broadcasting (B) multicasting

(S) Subnetting (D) routing

14. MAC address is associated with a layer?

(A) Internet (B) network

(C) Data Link (D) Applications

15. Which technology is working at the shortest distance?

(A) 3G (B) Wireless

(C) Bluetooth (D) satellite

Very Short Type Questions

1. Write the names of two types of signals.
2. Write the names of two types of twisted pair cable.
3. Write the full name of OSI and TCP / IP.
4. Write the name of the topology that works in the network.
5. Write the names of the two devices that are working on the network.
6. The IP is related to which layer.
7. What kind of address is the MAC address?
8. Write the name of the security system that works in wireless.
9. Which technology is used to reduce the congestion of packets in the network?
10. Why is the quality of service required?
11. What is the use of DNS?
12. Write the full name of SMTP.

Short Type Questions

1. What are the different types of wired transmission?

2. Write about two types of signals?

3. Why is planning of IP address is required?

4. Why we do subnetting.

5. Explain the MAC address.

6. Explain the choke packet system.

7. What is the jitter in the network?

8. Explain the mail transfer agent.

9. Why is DNS required?

Essay Type Qestions

1. Write the details of OSI Model in short.

2. Explain the data transmission.

3. Explain the transmission media.

4. What is satellite transmission? Explain.

5. Explain the IP in detail.

6. Explain modem's methodology with Diagram.

7. Explain subnetting with examples.

8. What is Congestion Control? Explain in detail.

9. Explain the process of sending email.

Answer Key

1. D 2.C 3. C 4. C 5. A 6. A 7. B 8. A 9.B 10. A

11. A 12. A 13. B 14. C 15. C