What is data?

Facts and statistics collected together for reference or analysis is called data. It refers to the quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.
Data can exist in a variety of forms; as numbers or text on pieces of paper, as bits and bytes stored in electronic memory, or as facts stored in a person's mind. Strictly speaking, data is the plural of *datum*, a single piece of information. In practice, however, people use *data* as both the singular and plural form of the word.

Information is organized or classified data which has some meaningful values for the receiver. Information is the processed data on which decisions and actions are based. For e.g. the history of temperature readings all over the world for the past 100 years is data. If this data is organized and analyzed to find that global temperature is rising, then that is information. **Data processing** is the re-structuring or re-ordering of data by people or machine to increase their usefulness and add values for particular purpose. Data processing consists of basic steps input, processing and output.

Differences between data and information

The major differences between data and information are:

1. Data is the input language for a computer and information is the output language for human
2. Data is unprocessed facts or mere figures but information is processed data which has been made sense of
3. Data does not depend on information but information depends on data and without it, information cannot be processed
4. Data is not specific but information is specific enough to generate meaning
5. Data is the raw material that is collected but information is a detailed meaning generated from the data.

Data Representation

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

Text

In data communications, text is represented as a bit pattern, a sequence of bits (O's or1'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. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

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.

There are 10 digits i.e. 1, 2, 3, 4, 5, 6, 7, 8, 9 available in decimal number system. It is known as Base 10 system. The value of a digit in a number depends upon its position in the number e.g. the number 546 in this system is represented as $(546)_{10}$
$546 = (4*10^2) + (8*10^1) + (6*10^0)$

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 I-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11. There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of three primary colors: red, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

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. In Chapters 4 and 5, we learn how to change sound or music to a digital or an analog signal.

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, as we will see in Chapters 4 and 5.

What does Data Communications (DC) mean?

Data communication refers to the exchange of data between a source and a receiver. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area. Some devices/technologies used in data communications are known as data communication equipment (DCE) and data terminal equipment (DTE). DCE is used at the sending node, and DTE is used at the receiving node.

The meanings of source and receiver are very simple. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver.

Data communications incorporates several techniques and technologies with the primary objective of enabling any form of electronic communication. These technologies include telecommunications, computer networking and radio/satellite communication. Data communication usually requires existence of a transportation or communication medium between the nodes wanting to communicate with each other, such as copper wire, fiber optic cables or wireless signals.
For example, a common example of data communications is a computer connected to the Internet via a Wi-Fi connection, which uses a wireless medium to send and receive data from one or more remote servers.

Datum mean the facts information statistics or the like derived by calculation or experimentation. The facts and information so gathered are processed in accordance with defined systems of procedure. Data can exist in a variety of forms such as numbers, text, bits and bytes. The Figure is an illustration of a simple data communication system.

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 30-ms. if some of the packets arrive with 3D-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

Communication System

Communication is the process of establishing connection or link between two points for information exchange. OR Communication is simply the basic process of exchanging information. The electronics equipment which are used for communication purpose, are called communication equipment. Different communication equipment when assembled together forms a **communication system**.

Typical example of communication system are line telephony and line telegraphy, radio telephony and radio telegraphy, radio broadcasting, point-to-point communication and mobile communication, computer communication, radar communication, television broadcasting, radio telemetry, radio aids to navigation, radio aids to aircraft landing etc.

The Communication Process

In the most fundamental sense, communication involves the transmission of information from one point to another through a succession of process as listed below:

1. The generation of a thought pattern or image in the mind of an originator.
2. The description of that image, with a certain measure of precision, by a set of oral visual symbols.

3. The encoding of these symbols in a form that is suitable for transmission over a physical medium of interest.
4. The transmission of the encoded symbols to the desired destination.
5. The decoding and reproduction of the original symbols.
6. The recreation of the original thought pattern or image, with a definable degradation in quality, in the mind of recipient.

Block Diagram of Digital Communication System

The **basics components or elements** of data communication system are as follows:

1. Message
2. Sender
3. Receiver
4. Medium or Communication Channel
5. Encoder and Decoder
6. Protocol

Communication Channel

1. **Message**: - The message is the information or data that is to be communicated. It may consist of text, numbers, pictures, sounds, videos or any combination of these.
2. **Sender**: - A device that is used for sending messages (or data) is called *sender*. It is also called *transmitter* or *source*. The sender can be a computer, telephone, or a video camera etc. Usually, a computer is used as sender in data communication system.
3. **Receiver**: - A device that is used for receiving messages is called *receiver*. It is also known as *sink*. The receiver can be a computer, telephone set, printer, or a fax machine etc. Usually, a computer is also used as receiver in data communication system.

4. **Medium**: - The path through which data is transmitted (or sent) from one location to another is called *transmission medium*. It is also called *communication channel*. It may be a wire, or fiber optic cable, or telephone line etc. If the sender and receiver are within a building, a wire is used as the medium. If they are located at different locations, the medium may be telephone line, fiber optics, and microwave or satellite system.

5. **Encoder and Decoder**: - In communication systems, computers are used for senders and receivers. A computer works with digital signals. The communication channels usually use analog signals. The encoder and decoder are used in communication systems to convert signals from one from to another.

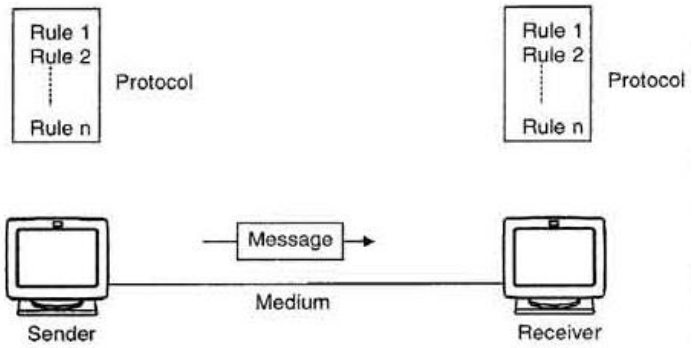
   Encoder: - The encoder is an electronic device. It receives data from sender in the form of digital signals. It converts digital signals into a form that can be transmitted through transmission medium.

   Decoder: - The decoder is an electronic device. It receives data from transmission medium. It converts encoded signals (i.e. analog signals) into digital form.

6. **Protocol:** - It is a set of rules that governs the data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

Protocol performs the following functions:

1. **Data sequencing**. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.
2. **Data routing**. Data routing defines the most efficient path between the source and destination.
3. **Data formatting**. Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.
4. **Flow control**. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.
5. **Error control**. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.
6. **Precedence and order of transmission**. These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.
7. **Connection establishment and termination**. These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.



8. **Data security**. Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

9. **Log information.** Several communications Software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

What does Computer Network mean?

The generic term "**network**" refers to a group of entities (objects, people, etc.) which are connected to one another. A network, therefore, allows material or immaterial elements to be circulated among all of these entities, based on well-defined rules.

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.
A **computer network** is a set of connected computers. Computers on a network are called **nodes**. The connection between computers can be done via cabling, most commonly the Ethernet cable, or wirelessly through radio waves. Connected computers can share resources, like access to the Internet, printers, file servers, and others. A network is a multipurpose connection, which allows a single computer to do more.

Computer networking is the practice of interfacing two or more computing devices with each other for the purpose of sharing data. Computer networks are built with a combination of hardware and software components.

Network: A group of computers and peripheral devices connected to each other. Note that the smallest possible network is two computers connected together.
Networking: Implementing tools and tasks for linking computers so that they can share resources over the network.
Depending on what kind of entity is involved, the term used will differ:

Transportation network: A combination of infrastructure and vehicles used for transporting people and goods between different geographic areas.
Telephone network: Infrastructure for transporting voice signals from one telephone station to another.
Neural network: A group of brain cells connected to each other
Criminal network: A group of con artists in cahoots (wherever there's one con artist, there's usually another!)
Computer network: A group of computers linked to each other with physical lines, exchanging information as digital data (binary values, i.e. values encoded as a signal which may represent either 0 or 1)

Characteristics of a computer network

- Share Resources from one computer to another
- Create files and store them in one computer, access those files from the other computer(s) connected over the network
- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over network.
- Facilitate communication via email, video conferencing, instant messaging, etc.
- Allow for the sharing of software or operating programs on remote systems.

Why do we need computer networks?

Computer networks help users on the network to share the resources and in communication. Can you imagine a world now without emails, online newspapers, blogs, chat and the other services offered by the internet?
Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities.

The following are the important **uses and benefits** of a computer network.

1. **File sharing:** Networking of computers helps the network users to share data files.
2. **Hardware sharing:** Users can share devices such as printers, scanners, CD-ROM drives, hard drives etc. Without computer networks, device sharing is not possible.
3. **Application sharing:** Applications can be shared over the network, and this allows implementing client/server applications
4. **User communication:** Networks allow users to communicate using e-mail, newsgroups, and video conferencing etc.
5. **Network gaming:** A lot of network games are available, which allow multi-users to play from different locations.
6. **Voice over IP (VoIP)**: Voice over Internet Protocol (IP) is a revolutionary change in telecommunication which allows to send telephone calls (voice data) using standard Internet Protocol (IP) rather than by traditional PSTN.

Disadvantages of computer Network

Security Concerns

One of the major drawbacks of computer networks is the security issues that are involved. If a computer is a standalone computer, physical access becomes necessary for any kind of data theft. However, if a computer is on a network, a hacker can get unauthorized access by using different tools. In case of big organizations; variety of network security software needs to be used to prevent theft of any confidential and classified data.

Virus and Malware

If even one computer on a network gets affected by a virus; there is a possible threat for the other systems getting affected too. Viruses can spread on a network easily, because of the inter-connectivity of workstations. Moreover, multiple systems with common resources are the perfect breeding ground for viruses that multiply. Similarly, if malware gets accidentally installed on the central server, all clients in the network that are connected to that server will get affected automatically.

Lack of Robustness

If the main file server of a computer network breaks down, the entire system becomes useless. If there is a central linking server or a bridging device in the network, and it fails, the entire network will come to a standstill. In case of big networks, the file server should be a powerful computer, which often makes setting up and maintaining the system doubly expensive.

Needs an Efficient Handler

The technical skills and know-how required to operate and administer a computer network is considerably high. Any user with just the basic skills cannot do this job. Also, the responsibility that comes with such a job is high, since allotting username-passwords and permissions to users in the network are also the network administrator's duties. Similarly, network connection and configuration is also a tedious task, and cannot be done by an average user who does not have advanced knowledge of computers and/or networking.

Lack of Independence

Since most networks have a centralized server and dependent clients, the client users lack any freedom whatsoever. Centralized decision making can sometimes hinder how a client user wants to use own computer. Computer networks have had a profound effect on the way we communicate with each other today, and have made our life easier. From the World Wide Web to your local office LAN, computers have become indispensable in daily life, and networks have become a norm in most businesses. If networks are designed and configured keeping in mind its pros and cons, they are the best piece of facility you could ever have.

Describes why and how computer networks support successful work of an Enterprise.

Information and communication are two of the most important strategic issues for the success of every enterprise. While today nearly every organization uses a substantial number of computers and communication tools (telephones, fax, and personal handheld devices), they are often still isolated.

To overcome these obstacles in an effective usage of information technology, computer networks are necessary. They are a new kind (one might call it paradigm) of organization of computer systems produced by the need to merge computers and communications. At the same time they are the means to converge the two areas; the unnecessary distinction between tools to process and store information and tools to collect and transport information can disappear. Computer networks can manage to put down the barriers between information held on several (not only computer) systems. Only with the help of computer networks can a borderless communication and information environment be built.
Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities. Because of these optimal information and communication possibilities, computer networks may increase the organizational learning rate, which many authors declare as the only fundamental advantage in competition.
Besides this major reason why any organization should not fail to have a computer network, there are other reasons as well:

- cost reduction by sharing hard- and software resources
- high reliability by having multiple sources of supply
- cost reduction by downsizing to microcomputer-based networks instead of using mainframes
- greater flexibility because of possibility to connect devices from various vendors

Because of the importance of this technology, decisions of purchase, structure, and operation of computer networks cannot be left to technical staff. Management as well has a critical need for understanding the technology of computer networks.

Network Topology

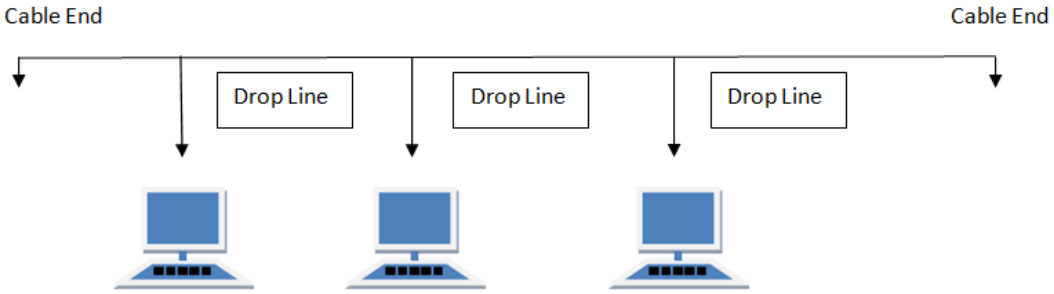
In communication networks, a topology is a usually schematic description of the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology. It defines the shape of communication network. There are five common types of network Topologies.

1. Bus Topology
2. Ring Topology
3. Star Topology
4. Tree Topology
5. Mesh Topology

1. Bus Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.
In linear bus topology, all computers are connected by a single length of cabling with a terminator at each end. The bus topology is the simplest and most widely used network design.

Bus networks are the most common LANs. They have no switches, and in their simplest form, no repeaters, but simply share a common linear communication medium. Each station requires a tap (hardware for attachment to the medium), which must be capable of delivering the signal to all stations in the bus.



Features of Bus Topology

- It transmits data only in one direction.
- Every device is connected to a single cable

Advantages of Bus Topology

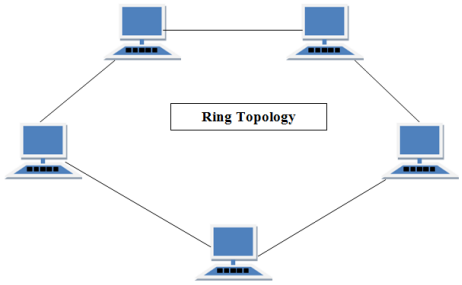
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

2. Ring Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbor for each device.
In ring topology the computers are arranged in a circle. Data travels around the ring in one direction, with each devise on the ring acting as a repeater. Ring Networks typically use a Token Passing Protocol. The layout is similar to linear bus, except that the nodes are connected in a circle using cable segments. In this layout, each node is connected to only two others. Each node passes information along to the next, until it reaches at its intended destination.
The ring topology is usually found in peer-to-peer (PCs connected in pairs) networks, in which each machine manages both information processing and distribution of data files.



Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

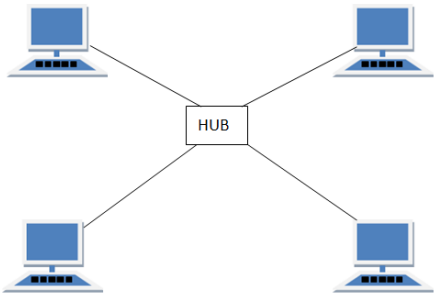
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

3. Star Topology

In Star Topology, all the cables run from the computers to a central location, where they are connected by a hub. Hub is a device used to extend a network so that additional work stations can be attached.
In Star topology each node is connected to single centrally located server, using its own dedicated segment of cable. A star topology is a LAN architecture in which endpoints on the network are connected to a common central hub, or switch, by dedicated links. In this topology each node is connected to a centralized switch by a dedicated physical link. The switch provides a path between any two devices wishing to communicate, either physically in a circuit switch or logically in a packet switch.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fiber or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

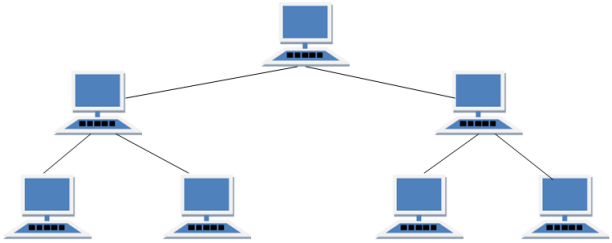
Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

4. Tree Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

This is a network topology containing zero or more nodes/computers linked together in a hierarchical fashion. The topmost node is called the root. The root may have zero or more child nodes, connected by edges (links); the root is the parent root to its children. Each node can have in turn zero or more nodes of its own. Nodes sharing the same parents are called siblings. Every node in the tree has exactly one parent node (except root which has no parents), and all nodes in the tree are descendants of the root node. These relationships ensure that there is one and only one path from one node to any other node in the tree. Tree topology LAN architecture is identical to BUS topology network, except that branches with multiple nodes are possible in this case. The advantages and disadvantages of Tree topology are same as that of Bus Topology.



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

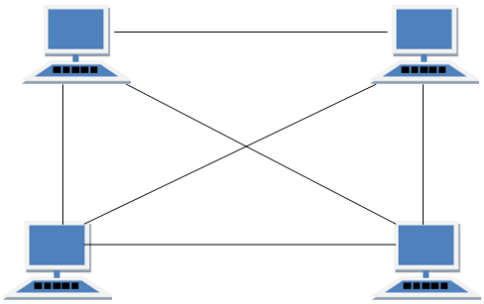
1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

5. Mesh Topology

In this topology, two or more nodes are connected together in an arbitrary fashion. Any two nodes in a Mesh or Graph may or may not be connected by a link. Not all the nodes need to be connected in a graph, but if the path can be traced between any two nodes, the graph is a connected one.

A Mesh Topology is a Mixture of BUS topology, STAR Topology, Ring and Tree Topology, with no restriction of connection among all the nodes in a network.

The mesh network topology employs either of two schemes, called full mesh and partial mesh. In the full mesh topology, each workstation is connected directly to each of the others. In the partial mesh topology, some workstations are connected to all the others, and some are connected only to those other nodes with which they exchange the most data.



Types of Mesh Topology

1. **Partial Mesh Topology:** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology:** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

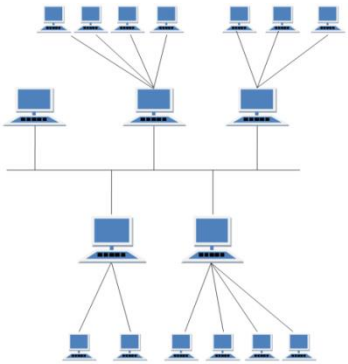
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

Hybrid Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

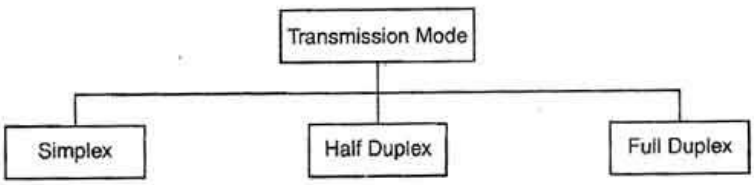
Transmission Modes in Computer Networks

The way in which data is transmitted from one place to another is called data transmission mode. It is also called the data communication mode. It is indicates the direction of flow of information. Sometimes, data transmission modes are also called directional modes.

Types of Data Transmission Modes

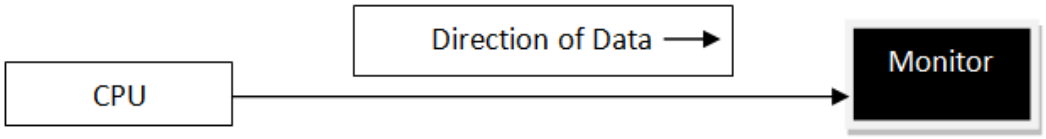
Different types of data transmission modes are as follows:

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



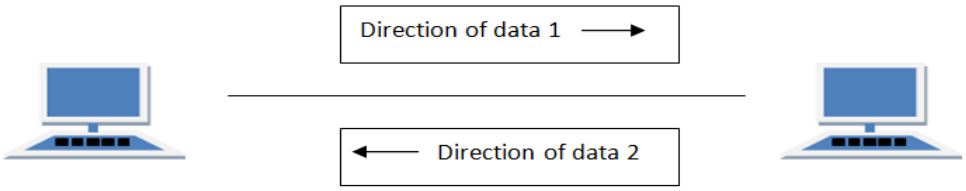
1. Simplex Mode

In simplex mode, data can flow in only one direction. In this mode, a sender can only send data and cannot receive it. Similarly, a receiver can only receive data but cannot send it. Data sent from computer to printer is an example of simplex mode.
In simplex mode, it is not possible to confirm successful transmission of data. It is also not possible to request the sender to re-transmit information. This mode is not widely used. However, this mode is used in business field at certain point-of-sale terminals. Examples of simplex Mode is loudspeaker, television broadcasting, television and remote, keyboard and monitor etc.



2. Half-Duplex Mode

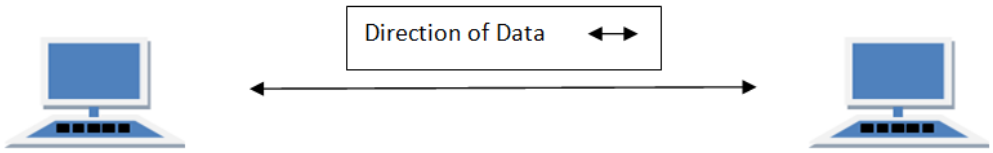
A half-duplex system can transmit data in both directions, but only in one direction at a time that mean half duplex modes support two-way traffic but in only one direction at a time. The interactive transmission of data within a time sharing system may be best suited to half-duplex lines. Both the connected devices can transmit and receive but not simultaneously. When one device is sending the other can only receive and vice-versa. Data is transmitted in one direction at a time, for example a walkie-talkie.
This is generally used for relatively low-speed transmission, usually involving two-wire, analog circuits. Due to switching of communication direction, data transmission in this mode requires more time and processes than under full duplex mode. Examples of half-duplex application include line printers, polling of buffers, and modem communications (many modems can support full duplex also).



3. Full-Duplex Mode

In full duplex system we can send data in both directions as it is bidirectional. Data can be sent in both directions simultaneously. We can send as well as we receive the data. Full-duplex method is used to transmit the data over a serial communication link. Two wires needed to send data over a serial communication link layer. Full-duplex transmission, the channel capacity is shared by both communicating devices at all times.

Example of Full Duplex is a Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



Different types of Networks

There are many ways in which different networks can be classified, such as their size, capabilities and the geographical distance they cover. Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the internet itself, covering the whole geographical world.

1. Local Area Network (LAN)

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.
LAN can be wired, wireless, or in both forms at once.

2. Metropolitan Area Network (MAN)

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. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.
This is a network which is larger than a LAN but smaller than a WAN, and incorporates elements of both. It typically spans a town or city and is owned by a single person or company, such as a local council or a large company.

3. Wide Area Network (WAN)

WAN networks connect computers together over large physical distances, remotely connecting them over one huge network and allowing them to communicate even when far apart. The Internet is a WAN, and connects computers all around the world together.

LANs connect to WANs, such as the internet, using routers to transfer data and information quickly and securely. WANs are usually too large to be controlled by one administrator, and so usually have collective ownership, or in the case of the internet, are publicly owned.
WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET).

Intranet, Extranet and Internet – What do they mean?

- **Intranet**

Intranet is a computer network system in which a specific organizational systems share information, computing services and operational systems with each other by using an Internet (IP) technology. This term basically refers to the network of a specific organization. You can also say it a private network.
An intranet is a private computer network that uses Internet Protocol technologies to securely share any part of an organization's information or operational systems within that organization.
In its simplest form, an Intranet can be set up on a networked PC without any PC on the network having access via the Intranet network to the Internet.

- **Extranet**

The term Extranet is linked with Intranet. Extranet is a kind of computer network that allows the outside users to access the Intranet of organization. This network system is basically used for business to business (B2B) purposes. This system basically allows the outside users of an organization, like partners, suppliers, vendors and other stakeholders to remain in touch with the activities of organization.
Extranet is the next stage in the intranet. It has also very restricted users but as compared to intranet it has a more opened environment. When the usage of the internet remains restricted to the internal environment of an organization only it is called as intranet but when the customers and other outsiders like the stakeholders of an organization also join this system then this system becomes the extranet.
After setting the extranet, the users can then send private messages by using the public network system through the most enhanced encryption and security technologies.

- **Internet**

The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer.
This is *the world-wide network* of computers accessible to anyone who knows their Internet Protocol (IP) address. It is a global network of millions of private, public and organizational network. It carries a massive range of informational resources and data in form of HTTP (Hypertext Markup language) documents and applications through World Wide Web (WWW).
Nothing is impossible today. All kinds of verbal communication, social networking, online shopping and financial services are being performed through Internet. The extranet and intranet also rely on the internet.

Network Devices

- **Hub**

A hub works in the physical layer of the OSI model. It is basically a non-intelligent device, and has no decision making capability. What a Hub basically does is take the input data from one of the ports and broadcast the information to all the other ports connected to the network.

So, there is a lack of security in the Hub. The Network Hubs are outdated and are out of the market.

- **Repeaters**

A repeater is a device similar to the Hub, but has additional features. It also works in the Physical layer. The repeaters are used in places where amplification of input signal is necessary. But, the kind of amplification done by the repeater is different from the regular amplification by amplifiers. The regular amplifies everything fed into it. That means, if the input signal has noise induced into it, both the desired signal and noise signal are together amplified. But, in the case of a repeater, it regenerates the input signal, and amplifies only the desirable signal. Hence, the noise component of the signal is eliminated.
The repeaters are necessary since, during the transmission of the signals over long distances, the signal has attenuation, delay distortions and noise, which lead in loss of data. Hence, in order to prevent this, the regenerative repeaters are used.

- **Switches**

A switch is an intelligent device that works in the data link layer. The term intelligent refers to the decision making capacity of the Switch. Since it works in the Data link layer, it has knowledge of the MAC addresses of the ports in the network.
If data has to be sent from Computer A to Computer B, then, the data is transferred to the Computer B only, and not to any other computers connected on the network. Hence, it establishes a link between the sender and the receiver based on the MAC addresses. This also means that when data is being sent from A to B, Computer C can establish a link with Computer D and communication can take place between them. So, simultaneous data transfer is possible in a switch.
It is also to be noted that a switch is a secure device, because it sends information only to the desired destinations, and also certain security features such as firewalls can be implemented in the Switches.

- **Bridge**

A bridge is also a device which works in the Data Link Layer, but is more primitive when compared to a switch. Initial bridges were used to connect only 2 LAN's, but the most recent ones perform similar operation as the switches. It also works on the principle of transfer of information using the MAC addresses of the ports.
It can be noted is that the normal ADSL modem can be connected via bridging also. The only difference is that, when bridging is used, each time the device has to be connected to the internet; it has to dial to the internet and establish a connection. Also, a bridge alone cannot be used to connect to the internet, because, the bridge works in the Data Link Layer, and has no knowledge of the IP Addresses, which are used in the Internet.

- **Router**

The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is a device that forwards data packets along networks. A router is

connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.
A router may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Typically, a packet may travel through a number of network points with routers before arriving at its destination. Routing is a function associated with the Network layer (layer 3) in the standard model of network programming, the Open Systems Interconnection (OSI) model.
Static routers: These must have their routing tables configured manually with all network addresses and paths in the internetwork.
Dynamic routers: These automatically create their routing tables by listening to network traffic.

- **Gateway**

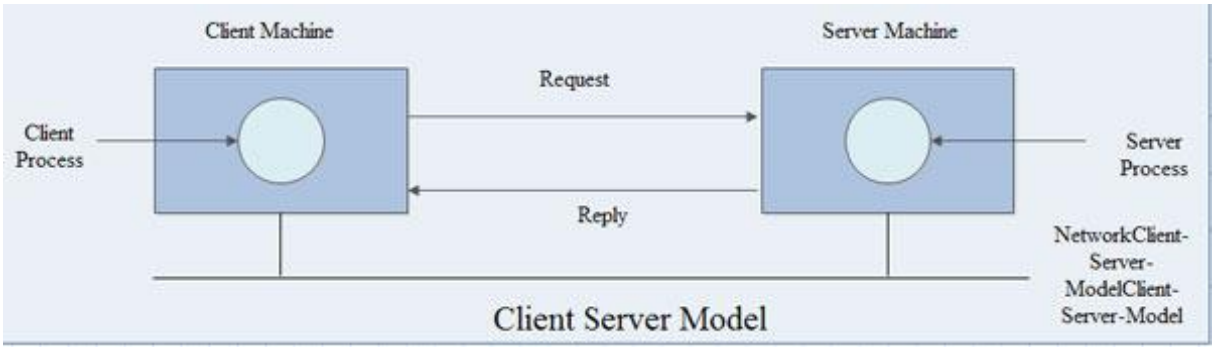
A gateway is a device used to connect networks using different protocols. Gateways operate at the network layer of the OSI model. In order to communicate with a host on another network, an IP host must be configured with a route to the destination network. If a configuration route is not found, the host uses the gateway (default IP router) to transmit the traffic to the destination host. The default t gateway is where the IP sends packets that are destined for remote networks. If no default gateway is specified, communication is limited to the local network. Gateway receive data from a network using one type of protocol stack, removes that protocol stack and repackages it with the protocol stack that the other network can use.
A gateway is a network point that acts as an entrance to another network. E-mail gateways-for example, a gateway that receives Simple Mail Transfer Protocol (SMTP) e-mail, translates it into a standard X.400 format, and forwards it to its destination.

Networking Models

- **Client-Server Model**

A **client-server** network is designed for end-users, called clients, to access resources such as files, songs, video collections, or some other service from a central computer called a server. A server's sole purpose is to do what its name implies - serve its clients!
The type of computing system, in which one powerful workstation serves the requests of other systems, is an example of client server technology.

Once the server has fulfilled the client's request, the connection is terminated. Your Web browser is a client program that has requested a service from a server; in fact, the service and resource the server provided is the delivery of this Web page.



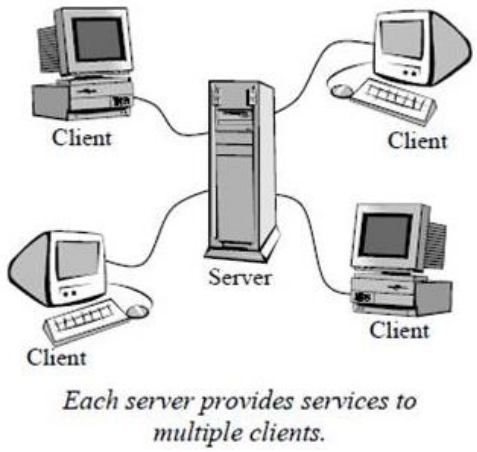


Fig: Client-Server Networking Model

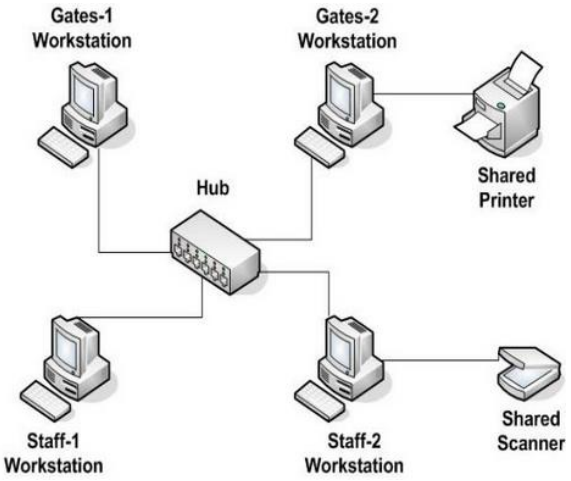


Fig: Peer-to-Peer Networking Model

- It is also known as centralized computing.
- In this type of system, multiple computers are joined to one powerful mainframe computer.
- The server or mainframe computer has huge storage and processing capabilities.
- The computers that are connected to the mainframe or server are called Clients or Nodes.
- These nodes are *not* connected to each other; they are only connected to server.

- **Peer-to-Peer Network Model (P2P)**

In its simplest form, a peer-to-peer (P2P) network is created when two or more PCs are connected and share resources without going through a separate server computer.
Peer-to-peer networks are quite common in small offices that do not use a dedicated file server. All client versions of Windows, Mac and Linux can function as nodes in a peer-to-peer network and allow their files to be shared.
It is easy to install and so is the configuration of computers on this network. P2P is more reliable as central dependency is eliminated. Failure of one peer doesn't affect the functioning of other peers. In case of Client –Server network, if server goes down whole network gets affected. The over-all cost of building and maintaining this type of network is comparatively very less.
In this network, the whole system is decentralized thus it is difficult to administer. Security in this system is very less viruses, spywares, Trojans, etc. Malwares can easily transmit over this P-2-P architecture.
Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session. Unlike the client/server model, in which the client makes a service request and the server fulfills the request, the P2P network model allows each node to function as both a client and server.

- **Active Networking Model**

Active Networks, unlike the traditional networks are not just passive carrier of bits but instead provides the capability for the user to inject customized programs into the networks. The network nodes would interpret these programs and perform desired operation on the data flowing through the network.

Active Networks is a relatively new concept, where a network is not just a passive carrier of bits but a more general computation model. Active Network may be simplistically viewed as a set of 'Active Nodes' that perform customized operations on the data flowing through them. It also consists of active hardware, capable of routing or switching as well as executing code within active packets. These programmable networks have opened many new doors for possible applications that were unimaginable with traditional data networks.

- **Distributed computing**

- If one computer can forcibly start, stop or control another computers are not autonomous. A system with one control unit and many slaves, or a large computer with remote printers and terminals is not called a computer network; it is called a **Distributed System**.
- Distributed computing means that the task is divided among multiple computers.
- Distributed computing interconnects one or more personal computers or Workstations.
- In distributed computing, the nodes are capable of processing their own data and rely on network for services other than data processing.
- It allows various services like network sharing, hardware sharing and file sharing.

Protocols and Standards in Computer Networking

A protocol is a set of rules which define:

- How to establish communication between the machines
- The format of any data which is to be exchanged between the machines
- How errors in the data will be detected
- How errors will be corrected
- Methods of compressing the data to transmit it faster and more efficiently
- How the connection between the machines is to be terminated

Network standards are also ground rules that are set by commissions so that hardware is compatible among similar computers and assures interoperability. This is done to ensure that backwards compatibility and compatibility from vendor to vendor. It is necessary to have standards because if each company had its own protocol standards and didn't allow it to talk with other protocols there would be a lack of communication from different machines and would result in one company being hugely successful and the other running out of business due to lack of being able to communicate with other machines.

- **Connection Oriented Protocols**

These protocols require that a logical connection be established between two devices before transferring data. This is generally accomplished by following a specific set of rules that specify how a connection should be initiated, negotiated, managed and eventually terminated. Usually one device begins by sending a request to open a connection, and the other responds. They pass control information to determine if and how the connection should be set up. If this is successful, data is sent between the devices. When they are finished, the connection is broken.

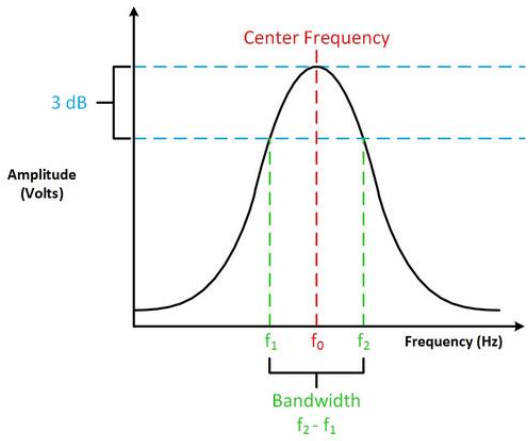
The process is much like a telephone call, where a virtual circuit is established--the caller must know the person's telephone number and the phone must be answered--before the message can be delivered. TCP is an example of a connection-oriented protocol.

- **Connection less Protocols**

Connectionless protocols, in contrast, allow data to be exchanged without setting up a link between processes. These protocols do not establish a connection between devices. As soon as a device has data to send to another, it just sends it. Each unit of data, with all the necessary information to route it to the intended destination, is transferred independent of other data packets and can travel over different paths to reach the final destination. Some data packets might be lost in transmission or might arrive out of sequence to other data packets.
UDP is a connectionless protocol. It is known as a datagram protocol because it is analogous to sending a letter where you don't acknowledge receipt.

What is bandwidth?

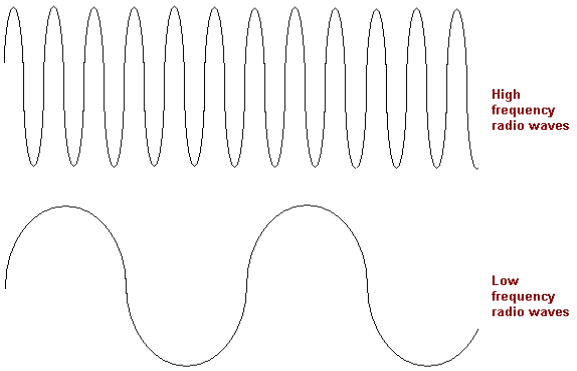
Bandwidth refers to the *range* of component frequencies that is contained in a signal. If the minimum and maximum components of frequencies that occur in a modulated signal are f_{min} and f_{max}, then the bandwidth is given by $f_{max} - f_{min}$.



When the bandwidth is larger, a larger number of frequencies can be represented by a signal. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz). For instance, AM radio signals which have a bandwidth of 9-10 kHz fail to transmit higher frequencies of sound that FM radios, having bandwidths of 100-200 kHz, can transmit without a problem.

Frequency

For an oscillating or varying current, frequency is the number of complete cycles per second in alternating current direction. The standard unit of frequency is the hertz (Hz).
If a current completes one cycle per second, then the frequency is 1 Hz.



Bandwidth and data rate

Bandwidth and data rate belongs to the world of Internet connections, basically from web hosting, and used to determine the amount of data being transferred (bit) in a given time, normally in a second. In network communication and system, both have different meaning and purposes, which makes them different from each other. Scroll down for the brief introduction of bandwidth and data rate so that next time you can choose the best option for your web hosting and network system.

Bandwidth

In communications, bandwidth is the difference between highest and lowest of the frequency range used for signaling. It is measured in Hertz (Hz). Bandwidth has the same meaning also in electronics, signal processing, and optics.

If talk about computing then it means how much amount or bits of data can be transferred in a time period, normally in one second. For example, if the bandwidth of an Internet connection is 1 MB then it means it can transfer the 1 MB amount of data within one second. It is measured in hertz, bps, kbps and mbps. Mbps, kbps or bps are used for digital devices while hertz is used for analog devices.

- **Signal Bandwidth** – the bandwidth of the transmitted signal or the range of frequencies present in the signal, as constrained by the transmitter.
- **Channel Bandwidth** – the range of signal bandwidths allowed by a communication channel without significant loss of energy (attenuation).
- **Channel Capacity** or **Maximum Data rate** – the maximum rate (in bps) at which data can be transmitted over a given communication link, or channel.

Bandwidth is a wider term, which is basically associated with the computer networking and digital technologies and measures the bit rate of communication resources available or consumed. It was used firstly in analog tools for submission of radio transmission and electromagnetic signals. If talk about computing then it means how much amount or bits of data can be transferred in a time period, normally in one second. For example, if the bandwidth of an Internet connection is 1 MB then it means it can transfer the 1 MB amount of data within one second. It is measured in hertz, bps, kbps and mbps. Mbps, kbps or bps are used for digital devices while hertz is used for analog devices.

Data Rate

Data rate is the term associated with the rate of data transferred between two or more computing and telecommunication devices or systems. It describes how much binary digits or bits can be transferred in a given time, normally in one second. Mostly data transferred rate is measured in Mbps. Data rate depends upon the bandwidth of Internet connection. If the bandwidth rate is high, data rate will be also high and vice versa.

Difference

After summarizing the discussion, following differences arises between bandwidth and data rate.

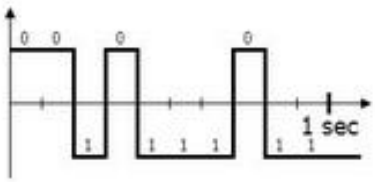
- Hz, bps, kbps and Mbps are used for the measurement of bandwidth while in data rate; Mbps is used as a basic measurement unit.
- In a network connection, bandwidth is always higher than data rate because data rate depends upon how much bandwidth is available for transmission.
- In case of website hosting, increase in visitor strengths increases the bandwidth speed of server while on the other hand data transfer rate decreases.
- Bandwidth is a wider term than data rate. Bandwidth is associated with how much amount of speed is available to you and data rate is associated with transfer of data.

Bit Rate and Baud Rate

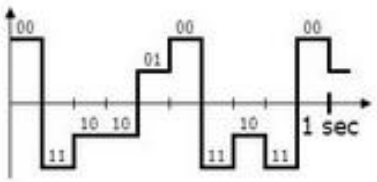
Bit rate is measured as number of data bits transmitted / second in communication channel. Baud rate is measured as number of times a signal state is changed in a communication channel. One change of state can transmit one bit or less than one bit which depends on modulation technique used. The bit and baud rate have the connection:

bps = baud / second x the number of bits / per baud

Bit rate and baud rate are not always the same. The bit rate is the number of bits transmitted per second, whereas, the baud rate is the number of signal units transmitted per second and one signal unit is able to represent one or more bits. Therefore, baud rate is always less than or equal to the bit rate but never greater.
Because symbols are comprised of bits, the baud rate will equal the bit rate only when there is just one bit per symbol.



Baud = 10
Bit rate = 10 bps



Baud = 10
Bit rate = 20 bps

Baud → *How many times a signal changes per second*
Bit rate → *how many bits can be sent per time unit. (Usually per second)*
Bitrate is controlled by baud and number of signal levels

Example 1

What is the bit rate and baud rate for an analogue signal that carries 3 bits in each signal unit if 2000 signal units are sent per second?
Answer: Baud rate = 2000 baud per second, Bit rate = 2000 x 3 = 6000 bps

Example 2

What is the baud rate for an analogue signal if the bit rate of the signal is 2000 and each signal unit carries 4 bits?
Answer: Baud rate = 2000 / 4 = 500 baud

Transmission Impairments

Transmission impairments refer to a condition that causes information to be lost in a signal.
With any communications system, it must be recognized that the received signal will differ from the transmitted signal due to various transmission impairments. For analog signals, these impairments introduce various random modifications that degrade the signal quality. For digital signals, bit errors are introduced: A binary 1 is trans- – formed into a binary 0 and vice versa.

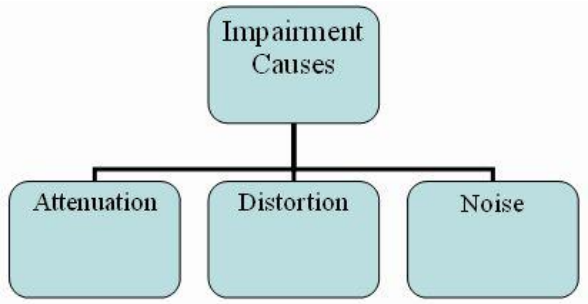


Fig -1: Causes of impairment

Attenuation:

Attenuation means a loss of energy. The strength of a signal falls off with distance over any transmission medium. For guided media, this reduction in strength, or attenuation, is generally logarithmic and is thus typically expressed as a constant number of decibels per unit distance. In fig. shows the effect of attenuation and amplification.

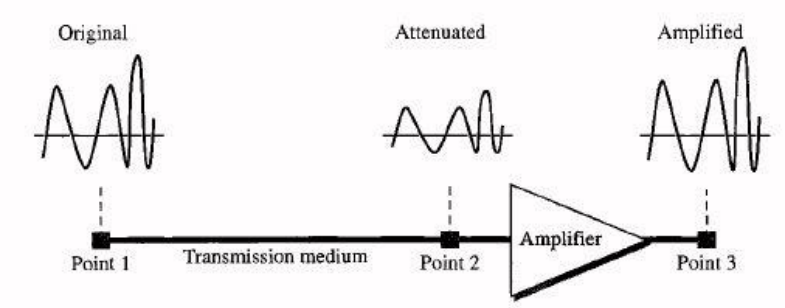


Fig-2: Attenuation

For unguided media, attenuation is a more complex function of distance and of the makeup of the atmosphere. Attenuation introduces three considerations for the transmission engineer. First, a received signal must have sufficient strength so that the electronic circuitry in the receiver can detect and interpret the signal. Second, the signal must maintain a level sufficiently higher than noise to be received without error. Third, attenuation is an increasing function of frequency.

Distortion:

Distortion means that the signal changes its form or shape. Delay distortion is a phenomenon peculiar to guided transmission media. The distortion is caused by the fact that the velocity of propagation of a signal through a guided medium varies with frequency. For a band limited signal, the velocity tends to be highest near the center frequency and lower toward the two edges of the band.

Thus, various frequency components of a signal will arrive at the receiver at different times. This effect is referred to as delay distortion, as the received signal is distorted due to variable delay in its components. The distortion effect is as shown in fig.

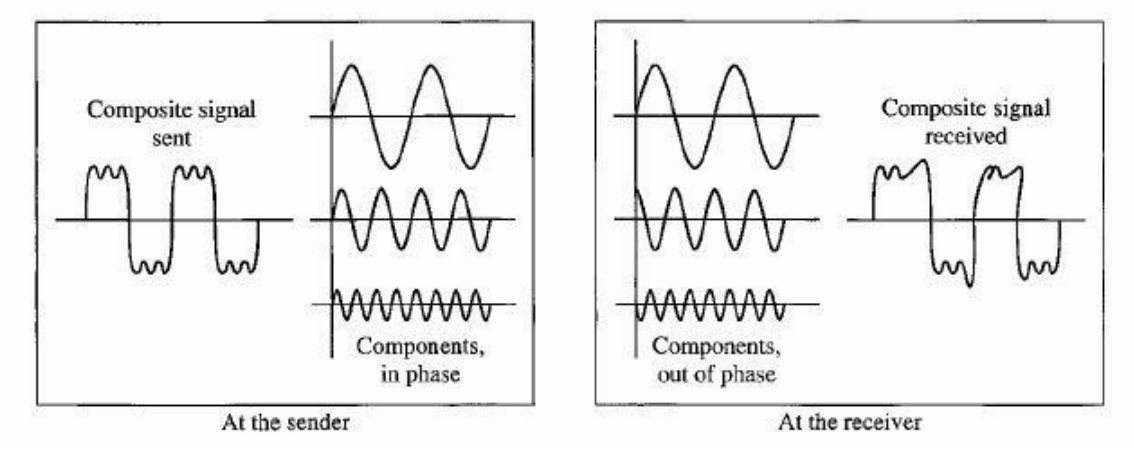


Fig-3: Distortion

Delay distortion is particularly critical for digital data. Consider that a sequence of bits is being transmitted, using either analog or digital signals. Because of delay distortion, some of the signal components of one bit position will spill over into other bit positions, causing inter symbol interference, which is a major limitation to maximum bit rate over a transmission control. Equalizing techniques can also be used for delay distortion.

Noise:

Noise is refers to any unwanted signal. For any data transmission event, the received signal will consist of the transmitted signal, modified by the various distortions imposed by the transmission system, plus additional unwanted signals that are inserted somewhere between transmission and reception; the latter, undesired signals are referred to as noise-a major limiting factor in communications system performance.

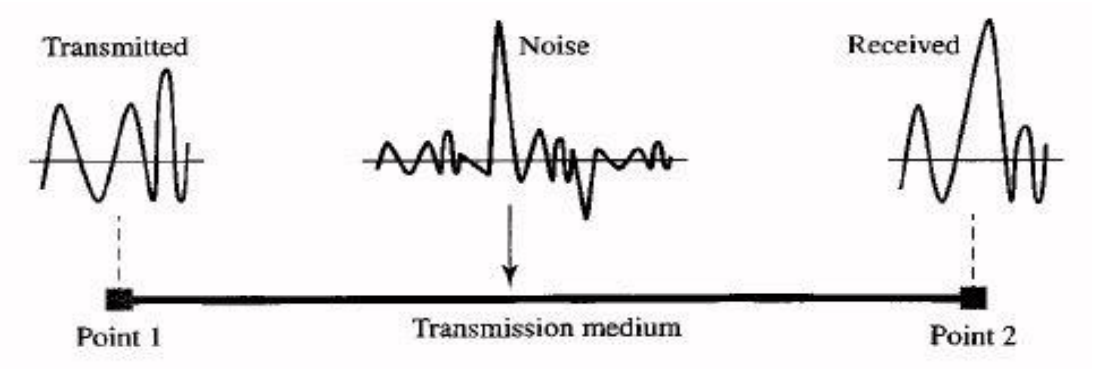
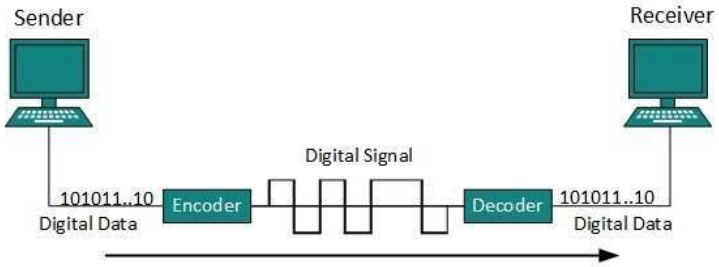


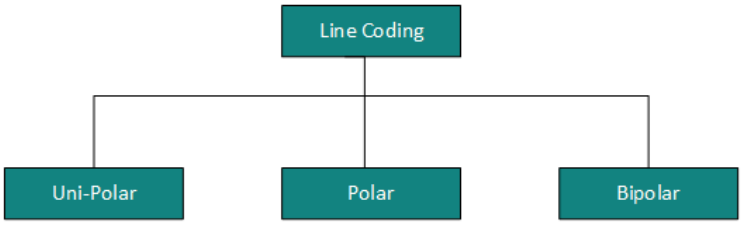
Fig-4: Noise

Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format. It is represented (stored) internally as series of 1s and 0s.

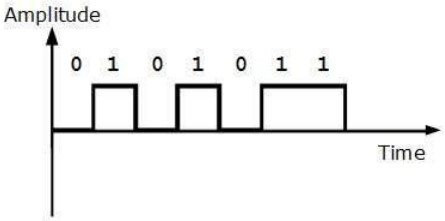


Digital signal is denoted by discreet signal, which represents digital data. There are three types of line coding schemes available:



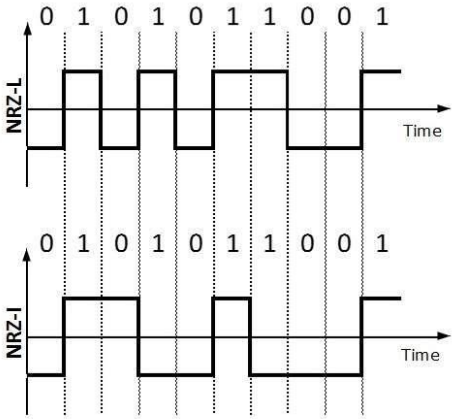
Uni-polar Encoding

Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.



Polar Encoding

Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:



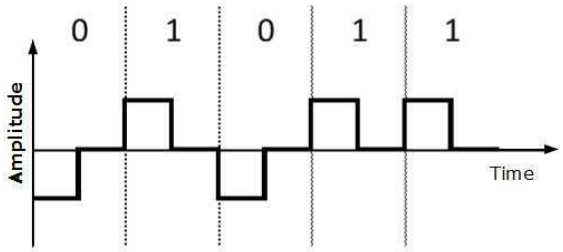
1. **Polar Non-Return to Zero (Polar NRZ)**

   It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.
   NRZ scheme has two variants: NRZ-L and NRZ-I.

   NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I change voltage when a 1 is encountered.

2. **Return to Zero (RZ)**

   Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver's clock are not synchronized.



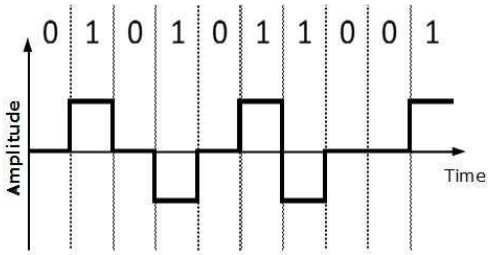
   RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

3. **Manchester**
   This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

4. **Differential Manchester**
   This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



Block Coding

To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding.
Block coding is represented by slash notation, mB/nB. Means, m-bit block is substituted with n-bit block where n > m. Block coding involves three steps:

- Division,
- Substitution
- Combination.
- After block coding is done, it is line coded for transmission.

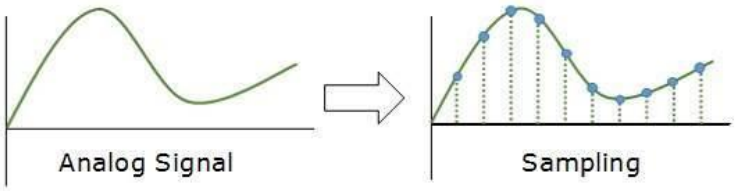
Analog-to-Digital Conversion

Microphones create analog voice and camera creates analog videos, which are treated is analog data. To transmit this analog data over digital signals, we need analog to digital conversion.
Analog data is a continuous stream of data in the wave form whereas digital data is discrete. To convert analog wave into digital data, we use Pulse Code Modulation (PCM).

PCM is one of the most commonly used methods to convert analog data into digital form. It involves three steps:

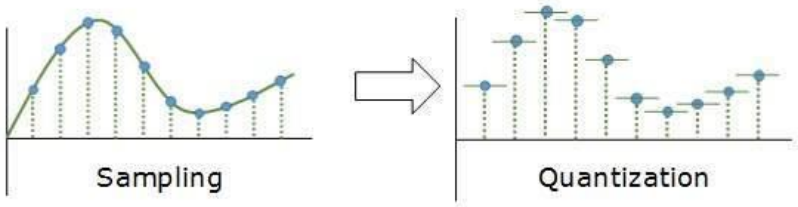
- Sampling
- Quantization
- Encoding.

Sampling



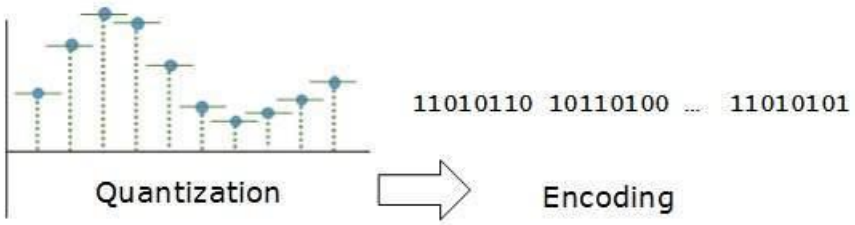
The analog signal is sampled every T interval. Most important factor in sampling is the rate at which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.

Quantization



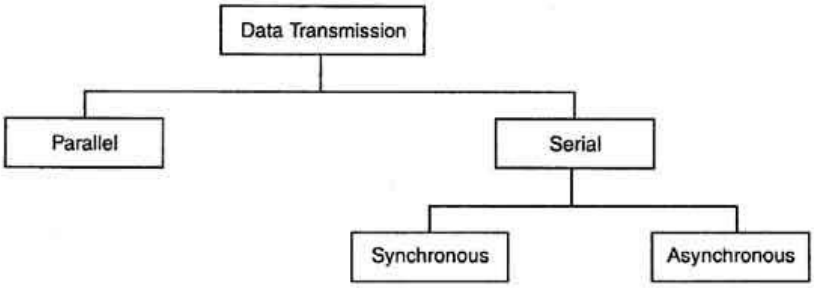
Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

Encoding



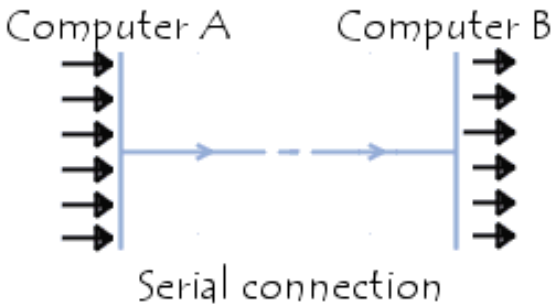
In encoding, each approximated value is then converted into binary format.

Serial and Parallel Transmission



1. Serial Transmission

In a serial connection, the data are sent one bit at a time over the transmission channel. However, since most processors process data in parallel, the transmitter needs to transform incoming parallel data into serial data and the receiver needs to do the opposite.



When transferring data between two physically separate devices, especially if the separation is more than a few kilometers, for reasons of cost, it is more economical to use a single pair of lines. Data is transmitted as a single bit at a time using a fixed time interval for each bit. This mode of transmission is known as *bit-serial* transmission.

- In serial transmission, the various bits of data are transmitted serially one after the other.
- It requires only one communication line rather than *n* lines to transmit data from sender to receiver.
- Thus all the bits of data are transmitted on single line in serial fashion.
- In serial transmission, only single bit is sent with each clock pulse.
- As shown in fig., suppose an 8-bit data 11001010 is to be sent from source to destination. Then least significant bit (LSB) *i,e.* 0 will be transmitted first followed by other bits. The most significant bit (MSB) *i.e.* 1 will be transmitted in the end via single communication line.
- The internal circuitry of computer transmits data in parallel fashion. So in order to change this parallel data into serial data, conversion devices are used.
- These conversion devices convert the parallel data into serial data at the sender side so that it can be transmitted over single line.
- On receiver side, serial data received is again converted to parallel form so that the interval circuitry of computer can accept it.

Advantage of Serial transmission

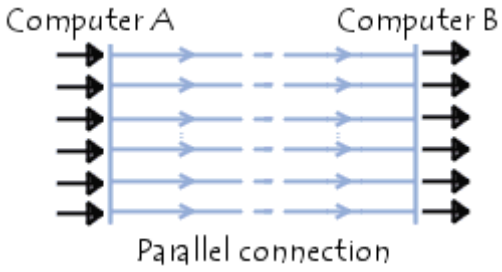
Use of single communication line reduces the transmission line cost by the factor of *n* as compared to parallel transmission.

Disadvantages of Serial transmission

1. Use of conversion devices at source and destination end may lead to increase in overall transmission cost.
2. This method is slower as compared to parallel transmission as bits are transmitted serially one after the other.

2. Parallel Transmission

Parallel connection means simultaneous transmission of N bits. These bits are sent simultaneously over N different channels (a channel being, for example, a wire, a cable or any other physical medium). The parallel connection on PC-type computers generally requires 10 wires.



Within a computing or communication device, the distances between different subunits are too short. Thus, it is normal practice to transfer data between subunits using a separate wire to carry each bit of data. There are multiple wires connecting each sub-unit and data is exchanged using a *parallel transfer* mode. This mode of operation results in minimal delays in transferring each word.

- In parallel transmission, all the bits of data are transmitted simultaneously on separate communication lines.
- In order to transmit *n* bits, *n* wires or lines are used. Thus each bit has its own line.
- All n bits of one group are transmitted with each clock pulse from one device to another *i.e.* multiple bits are sent with each clock pulse.
- Parallel transmission is used for short distance communication.
- As shown in the fig, eight separate wires are used to transmit 8 bit data from sender to receiver.

Advantage of parallel transmission

It is speedy way of transmitting data as multiple bits are transmitted simultaneously with a single clock pulse.

Disadvantage of parallel transmission

It is costly method of data transmission as it requires *n* lines to transmit *n* bits at the same time.

Comparison of Serial and Parallel Transmission

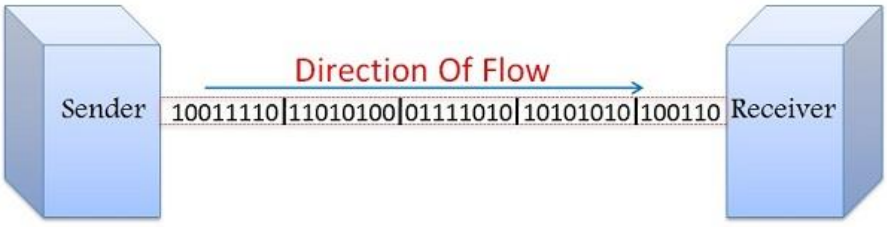
Sr. No.	Factor	Serial	Parallel
1.	Number of bits transmitted at one clock pulse	One bit	*n* bits
2.	No. of lines required to transmit *n* bits	One line	*n* lines
3.	Speed of data transfer	Slow	Fast
4.	Cost of transmission	Low as one line is required	Higher as *n* lines are required.
5.	Application	Long distance communication between two computers	Short distance communication. like computer to printer.

Synchronous and Asynchronous Transmission

There are two types of serial transmission-synchronous and asynchronous both these transmissions use '**Bit synchronization**'
Bit Synchronization is a function that is required to determine when the beginning and end of the data transmission occurs. Bit synchronization helps the receiving computer to know when data begin and end during a transmission. Therefore bit synchronization provides timing control.

Synchronous Transmission

In Synchronous Transmission, data flows in a full duplex mode in the form of blocks or frames. Synchronization between the sender and receiver is necessary so that the sender know where the new byte starts (since there is no gap between the data).



Synchronous Transmission is efficient, reliable and is used for transferring a large amount of data. It provides real-time communication between connected devices. Chat Rooms, Video Conferencing, telephonic conversations, as well as face to face interactions, are some of the examples of Synchronous Transmission.

- Synchronous transmission does not use start and stop bits.
- In this method bit stream is combined into longer frames that may contain multiple bytes.

- There is no gap between the various bytes in the data stream.
- In the absence of start & stop bits, bit synchronization is established between sender & receiver by *'timing'* the transmission of each bit.
- Since the various bytes are placed on the link without any gap, it is the responsibility of receiver to separate the bit stream into bytes so as to reconstruct the original information.
- In order to receive the data error free, the receiver and sender operates at the same clock frequency.

Advantage of Synchronous transmission

This method is faster as compared to asynchronous as there are no extra bits (start bit & stop bit) and also there is no gap between the individual data bytes.

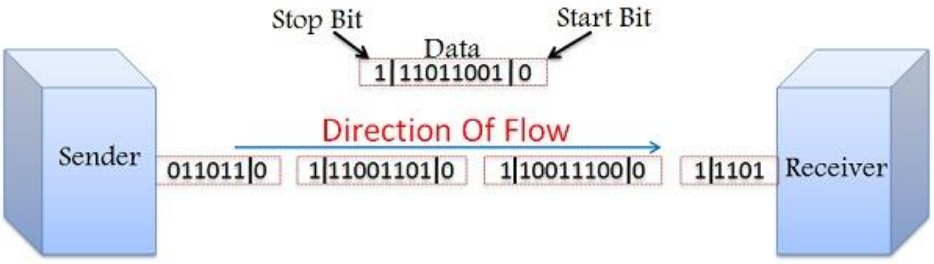
Disadvantages of Synchronous transmission

- It is costly as compared to asynchronous method. It requires local buffer storage at the two ends of line to assemble blocks and it also requires accurately synchronized clocks at both ends. This leads to increase in the cost.
- The sender and receiver have to operate at the same clock frequency. This requires proper synchronization which makes the system complicated.

Asynchronous Transmission

In asynchronous transmission data flows in a half-duplex mode; 1 byte or a character at a time. It transmits the data in a continuous stream of bytes. In general, the size of a character sent is 8 bits to which a parity bit is added i.e. a start and a stop bit that gives the total of 10 bits. It does not require a clock for synchronization; rather it uses the parity bits to tell the receiver how to interpret the data.

It is simple, fast, and economical and does not require a 2-way communication. Letters, emails, forums, televisions and radios are some of the examples of Asynchronous Transmission.



- Asynchronous transmission sends only one character at a time where a character is either a letter of the alphabet or number or control character *i.e.* it sends one byte of data at a time.
- Bit synchronization between two devices is made possible using start bit and stop bit.
- Start bit indicates the beginning of data *i.e.* alerts the receiver to the arrival of new group of bits. A start bit usually 0 is added to the beginning of each byte.
- Stop bit indicates the end of data *i.e.* to let the receiver know that byte is finished, one or more additional bits are appended to the end of the byte. These bits, usually 1s are called stop bits.
- Addition of start and stop increase the number of data bits. Hence more bandwidth is consumed in asynchronous transmission.

- There is idle time between the transmissions of different data bytes. This idle time is also known as Gap
- The gap or idle time can be of varying intervals. This mechanism is called Asynchronous, because at byte level sender and receiver need not to be synchronized. But within each byte, receiver must be synchronized with the incoming bit stream.

Advantages of Asynchronous transmission

1. This method of data transmission is cheaper in cost as compared to synchronous *e.g.* If lines are short, asynchronous transmission is better, because line cost would be low and idle time will not be expensive.
2. In this approach each individual character is complete in itself; therefore if character is corrupted during transmission, its successor and predecessor character will not be affected.
3. It is possible to transmit signals from sources having different bit rates.
4. The transmission can start as soon as data byte to be transmitted becomes available.
5. Moreover, this mode of data transmission in easy to implement.

Disadvantages of asynchronous transmission

1. This method is less efficient and slower than synchronous transmission due to the overhead of extra bits and insertion of gaps into bit stream.
2. Successful transmission inevitably depends on the recognition of the start bits. These bits can be missed or corrupted.

Comparison Chart

Basis for Comparison	**Synchronous Transmission**	**Asynchronous Transmission**
Meaning	Sends data in the form of blocks or frames	Sends 1 byte or character at a time
Transmission Speed	Fast	Slow
Cost	Expensive	Economical
Time Interval	Constant	Random
Gap between the data	Absent	Present
Examples	Chat Rooms, Video Conferencing, Telephonic Conversations, etc.	Letters, emails, forums, etc.

Differences between Synchronous and Asynchronous Transmission

- In Synchronous Transmission data is transferred in the form of frames on the other hand in Asynchronous Transmission data is transmitted 1 byte at a time.
- Synchronous Transmission requires a clock signal between the sender and receiver so as to inform the receiver about the new byte. Whereas, in Asynchronous Transmission sender and receiver does not require a clock signal as the data sent here has a parity bit attached to it which indicates the start of the new byte.
- Data transfer rate of Asynchronous Transmission is slower than that of Synchronous Transmission.

- Asynchronous Transmission is simple and economic whereas, Synchronous Transmission is complex and expensive.
- Synchronous Transmission is efficient and has lower overhead as compared to the Asynchronous Transmission.

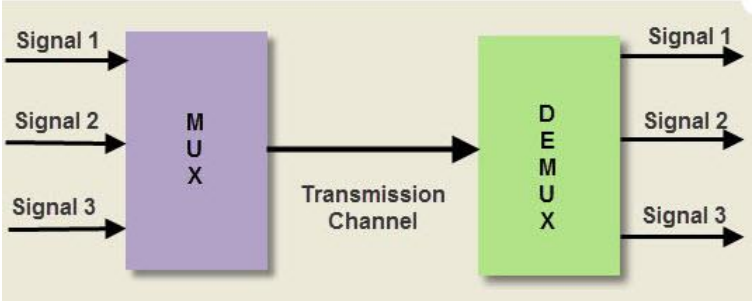
Conclusion

Both Synchronous and Asynchronous Transmission have their advantages and disadvantages. Asynchronous is simple, economical and used for transmitting a small amount of data whereas, Synchronous Transmission is used for transferring the bulk of data as it is efficient and has less overhead. Hence, we conclude that both Synchronous and Asynchronous Transmission are necessary for data.

Multiplexing

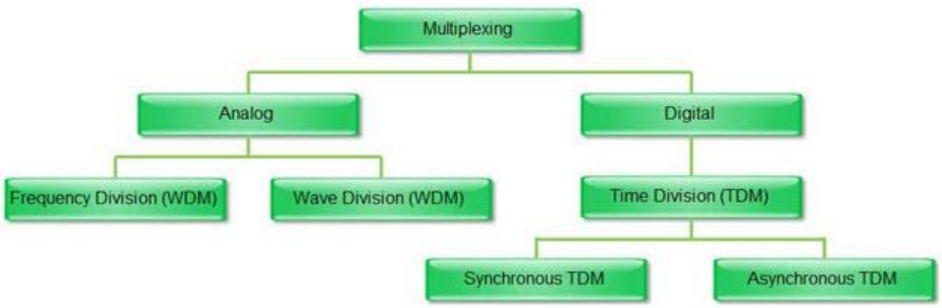
Multiplexing is a popular networking technique that integrates multiple analog and digital signals into a signal transmitted over a shared medium. Multiplexers are used to convert multiple signals into one signal.

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. Whenever the transmission capacity of a medium linking two devices is greater than the transmission needs of the devices, the link can be shared in order to maximize the utilization of the link, such as one cable can carry a hundred channels of TV.



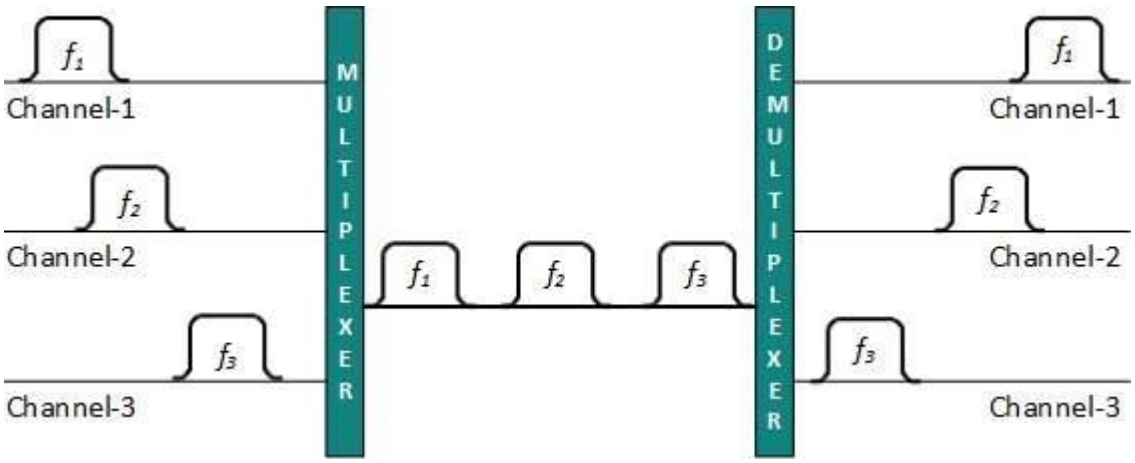
De-multiplex (DEMUX) is the reverse of the multiplex (MUX) process – combining multiple unrelated analog or digital signal streams into one signal over a single shared medium, such as a single conductor of copper wire or fiber optic cable. Thus, de-multiplex is reconverting a signal containing multiple analog or digital signal streams back into the original separate and unrelated signals.

Types of Multiplexer



Frequency Division Multiplexing

Frequency-Division Multiplexing (FDM**)** is a scheme in which numerous signals are combined for transmission on a single communications line or channel. It is analog technique. Each signal is assigned a different frequency (sub channel) within the main channel.
Frequency division multiplexing is applied when the bandwidth of the link is greater than the combined bandwidth of the signals to be transmitted.



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.

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.
Time-division multiplexing is primarily applied to digital signals as well as analog signals, wherein several low speed channels are multiplexed into high-speed channels for transmission. Based on the time, each low-speed channel is allocated to a specific position, where it works in synchronized mode. At both the ends, i.e., the multiplexer and de-multiplexer are timely synchronized and simultaneously switched to the next channel.

a. TDM is the digital multiplexing technique.
b. In TDM, the channel/link is not divided on the basis of frequency but on the basis of time.
c. Total time available in the channel is divided between several users.
d. Each user is allotted a particular a time interval called time slot or time slice during which the data is transmitted by that user.
e. Thus each sending device takes control of entire bandwidth of the channel for fixed amount of time.
f. In TDM the data rate capacity of the transmission medium should be greater than the data rate required by sending or receiving devices.

g. In TDM all the signals to be transmitted are not transmitted simultaneously. Instead, they are transmitted one-by-one.
h. Thus each signal will be transmitted for a very short time. One cycle or frame is said to be complete when all the signals are transmitted once on the transmission channel.
i. The TDM system can be used to multiplex analog or digital signals; however it is more suitable for the digital signal multiplexing.
j. The TDM signal in the form of frames is transmitted on the common communication medium.

Types of TDM

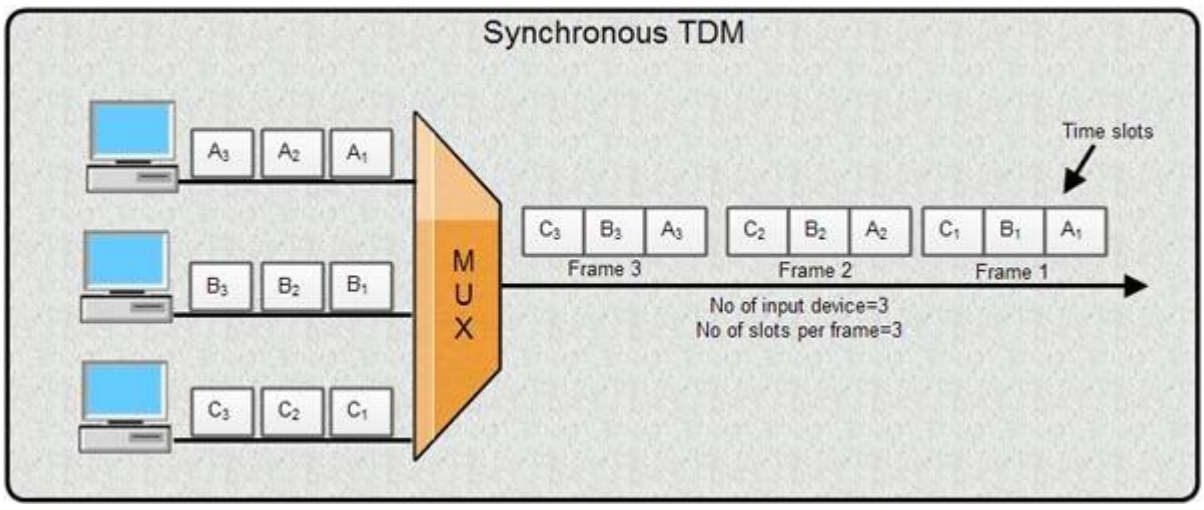
1. Synchronous TDM
2. Asynchronous TDM

Synchronous Time Division Multiplexing

Synchronous time division multiplexing can be used for both analog and digital signals. In synchronous TDM, the connection of input is connected to a frame. If there are 'n' connections, then a frame is divided into 'n' time slots – and, for each unit, one slot is allocated – one for each input line. In this synchronous TDM sampling, the rate is same for all the signals, and this sampling requires a common clock signal at both the sender and receiver end. In synchronous TDM, the multiplexer allocates the same slot to each device at all times.

1. In synchronous TDM, each device is given same **time slot** to transmit the data over the link, irrespective of the fact that the device has any data to transmit or not. Hence the name Synchronous TDM. Synchronous TDM requires that the total speed of various input lines should not exceed the capacity of path.
2. Each device places its data onto the link when its **time slot** arrives *i.e.* each device is given the possession of line turn by turn.

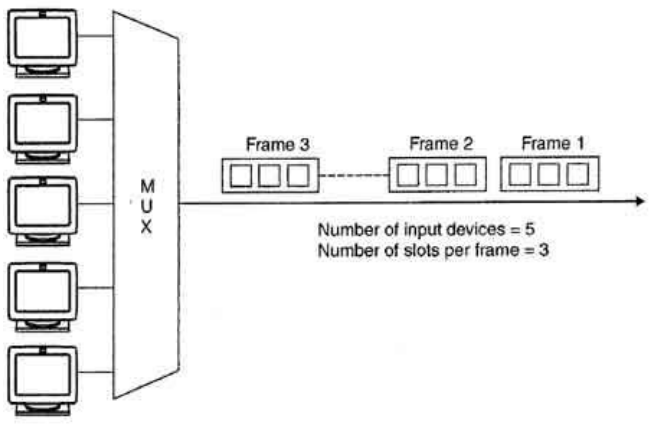
3. If any device does not have data to send then its time slot remains empty.
4. The various time slots are organized into **frames** and each frame consists of one or more time slots dedicated to each sending device.
5. If there are *n* sending devices, there will be *n* slots in frame *i.e.* one slot for each device.



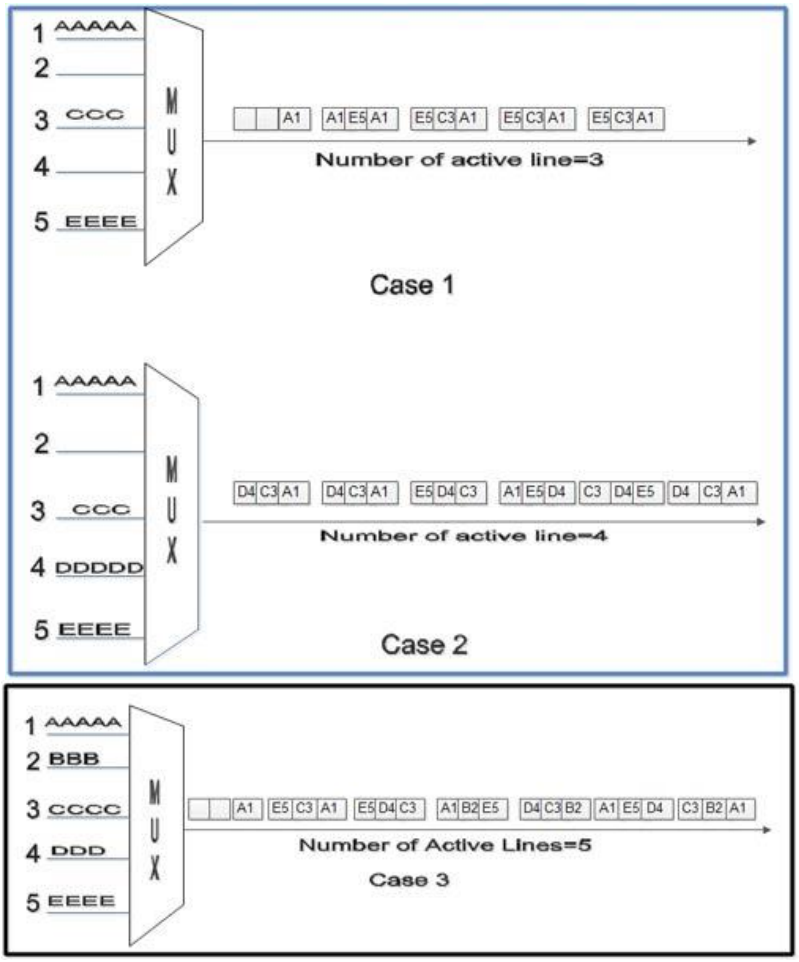
Asynchronous Time Division Multiplexing

In asynchronous time-division multiplexing, the sampling rate is different for different signals, and it doesn't require a common clock. If the devices have nothing to transmit, then their time slot is allocated to another device. Designing of a multiplexer or de-multiplexer is difficult and the bandwidth is less for time-division multiplexing. This type of time-division multiplexing is used in asynchronous transfer mode networks.
Asynchronous TDM is a more flexible method of TDM. With Asynchronous TDM the length of time allocated is not fixed for each device but time is given to devices that have data to transmit.

1. It is also known as statistical time division multiplexing.
2. Asynchronous TDM is called so because is this type of multiplexing, time slots are not fixed *i.e.* the slots are flexible.
3. Here, the total speed of input lines can be greater than the capacity of the path.
4. In synchronous TDM, if we have *n* input lines then there are *n* slots in one frame. But in asynchronous it is not so.
5. In asynchronous TDM, if we have *n* input lines then the frame contains not more than *m* slots, with *m* less than *n (m < n).*
6. In asynchronous TDM, the number of time slots in a frame is based on a statistical analysis of number of input lines.
7. In this system slots are not predefined, the slots are allocated to any of the device that has data to send.
8. The multiplexer scans the various input lines, accepts the data from the lines that have data to send, fills the frame and then sends the frame across the link.
9. If there are not enough data to fill all the slots in a frame, then the frames are transmitted partially filled.
10. Asynchronous Time Division Multiplexing is depicted in fig. Here we have five input lines and three slots per frame.
11. In Case 1, only three out of five input lines place data onto the link *i.e.* number of input lines and number of slots per frame are same.
12. In Case 2, four out of five input lines are active. Here number of input line is one more than the number of slots per frame.
13. In Case 3, all five input lines are active.
14. In all these cases, multiplexer scans the various lines in order and fills the frames and transmits them across the channel.



Asynchronous TDM

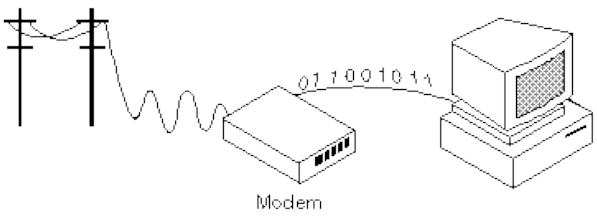


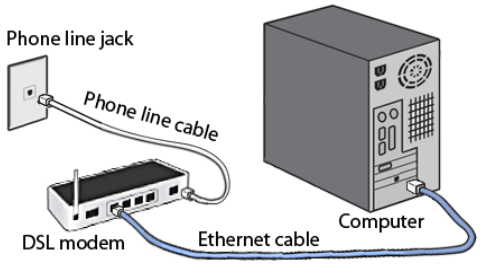
Advantages of TDM

1. Full available channel bandwidth can be utilized for each channel.
2. Intermodulation distortion is absent.
3. TDM circuitry is not very complex.
4. The problem of crosstalk is not severe.

Modem

The word "**modem**" stands for "**mo**dulator-**dem**odulator". A modem's purpose is to convert digital information to analog signals (modulation), and to convert analog signals back into useful digital information (demodulation).





A modem is a network device that both modulates and demodulates analog carrier signals (called sine waves) for encoding and decoding digital information for processing. Modems accomplish both of these tasks simultaneously and, for this reason, the term modem is a combination of "modulate" and "demodulate."

Modulation

Modulation is a technique in which message signal is transmitted to the receiver with the help of carrier signal. **Or** Modulation is the process of superimposing the information contents of a modulating signal on a carrier signal (which is of high frequency) by varying the characteristic of carrier signal according to the modulating signal.
Electronic communication includes TV, radio, Internet etc. Here we need to transmit the information bearing signal from one place to another. To do this we need to strengthen the signal so that the signal travels for long distances. This is what is called **Modulation**.

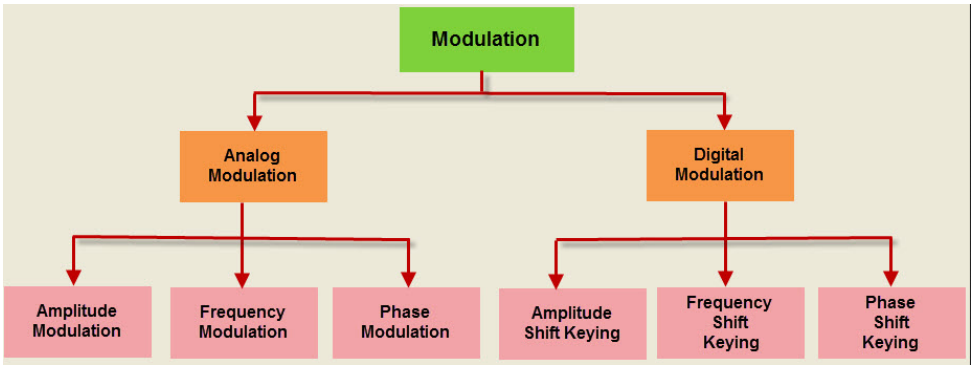
Information is referred as baseband or **modulating signal**. The waveform which is used to convert the information in the physically transmitted form is called **carrier**. The device which performs modulation operation is called **modulator** and the resulting waveform or output of modulator is called as modulated signal. The device which performs inverse of modulation is called **demodulator** and the operation is named as **demodulation**. The device which does both modulation and demodulation is called **MODEM**. Modulation can be applied on Direct current, alternating current and optical signal.

Advantages of Modulation:

- With the help of modulation, we can increase the quality of reception.
- We can also decrease the height of the antenna.
- Avoid mixing of different frequency signals and increase the range of communication i.e. without modulation, we can transmit the message up to 100 meters and with modulation, we can transmit the message up to 150 meters.
- Allow the flexibility for adjusting the bandwidth.

Modulation is nothing but, a carrier signal that varies in accordance with the message signal. Modulation technique is used to change the signal characteristics. Basically, the modulation is of following two types:

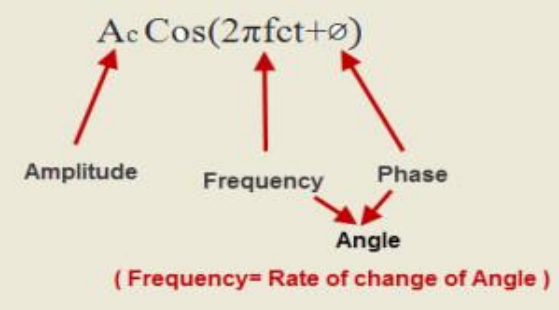
1. Analog Modulation
2. Digital modulation



Analog Modulation

In analog modulation, analog signal (sinusoidal signal) is used as a carrier signal that modulates the message signal or data signal. The general function Sinusoidal wave's is shown in the figure below, in which, three parameters can be altered to get modulation – they are amplitude, frequency and phase; so, the types of analog modulation are:

1. Amplitude Modulation (AM)
2. Frequency Modulation (FM)
3. Phase Modulation (PM)

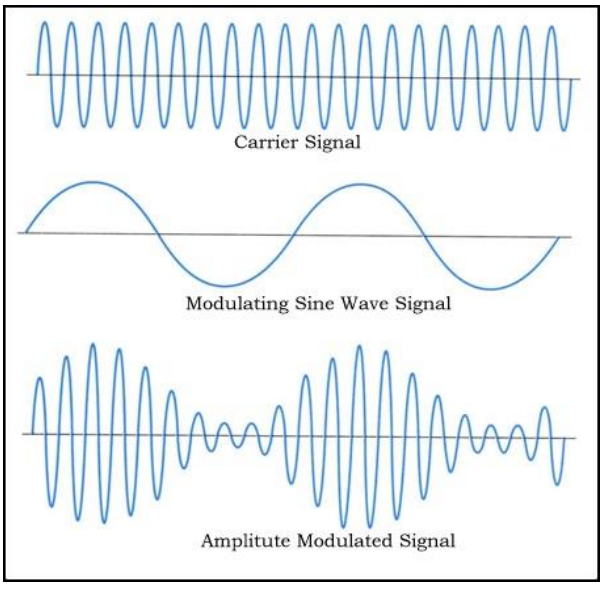


Amplitude Modulation

Amplitude modulation was developed in the beginning of the 20th century. It was the earliest modulation technique used to transmit voice by radio. In this modulation, the amplitude of the carrier signal varies in accordance with the message signal, and other factors like phase and frequency remain constant.

When compared to frequency modulation, the Amplitude modulation is weak, but still it is used for transmitting messages. Bandwidth of amplitude modulation should be twice the frequency of modulating signal or message signal.

In AM radio broadcasting, the modulating signal or message signal is 15 kHz. Hence the AM modulated signal which is used for broadcasting should be 30 kHz.



Advantages of Amplitude Modulation:

- Because of amplitude modulation wavelength, AM signals can propagate longer distances.
- For amplitude modulation, we use simple and low cost circuit; we don't need any special equipment and complex circuits that are used in frequency modulation.

- The Amplitude modulation receiver will be wider when compared to the FM receiver. Because, atmospheric propagation is good for amplitude modulated signals.
- Bandwidths limit is also big advantage for Amplitude modulation, which doesn't have in frequency modulation.
- Transmitter and receiver are simple in Amplitude modulation. When we take a demodulation unit of AM receiver, it consists of RC filter and a diode which will demodulate the message signal or modulating signal from modulated AM signal, which is unlike in Frequency modulation.
- Zero crossing in Amplitude modulation is equidistant.

Disadvantages of Amplitude Modulation

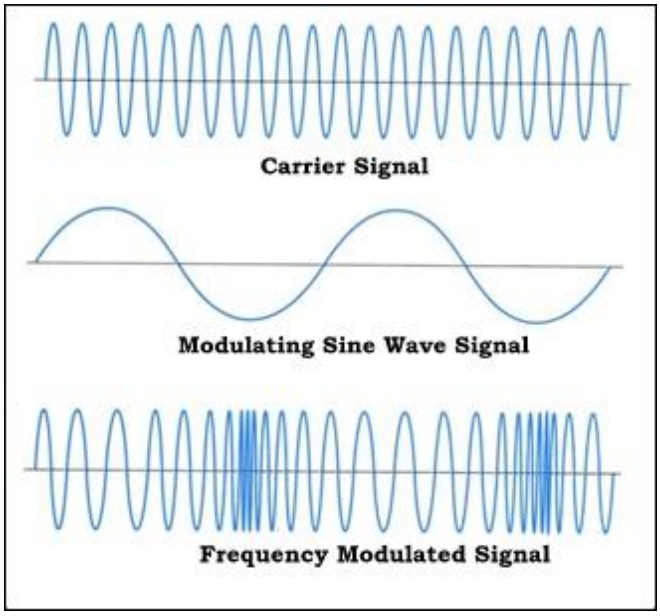
- Adding of noise for amplitude modulated signal will be more when compared to frequency modulated signals. Data loss is also more in amplitude modulation due to noise addition. Demodulators cannot reproduce the exact message signal or modulating signal due to noise.
- More power is required during modulation because Amplitude modulated signal frequency should be double than modulating signal or message signal frequency. Due to this reason more power is required for amplitude modulation.
- Noise addition and signal interferences are less for frequency modulation. That is why Amplitude modulation is not used for broadcasting songs or music.

Applications of Amplitude Modulation

- Used to carry message signals in early telephone lines.
- Used to transmit Morse code using radio and other communication systems.
- Used in Navy and Aviation for communications as AM signals can travel longer distances.
- Widely used in amateur radio.

Frequency Modulation

The process of carrier signal frequency is varied according to the message signal or modulation signal frequency by keeping the amplitude constant is called frequency modulation. Frequency modulation is used in different applications like radar, radio and telemetry, seismic prospecting etc.
This type of modulation is commonly used for broadcasting music and speech, magnetic tape recording systems, two way radio systems and video transmission systems. When noise occurs naturally in radio systems, frequency modulation with sufficient bandwidth provides an advantage in cancelling the noise.



Advantages of Frequency Modulation

- Frequency modulation has more noise resistivity when compared to other modulation techniques.
- The frequency modulation is having greater resistance to rapid signal strength variation, which we will use in FM radios even while we are travelling and frequency modulation is also mainly used in mobile communication purposes.
- For transmitting messages in frequency modulation, it does not require special equipment like linear amplifiers.
- Transmission rate is good for frequency modulation when compared to other modulation that is frequency modulation can transmit around 1200 to 2400 bits per second.
- Frequency modulation has a special effect called capture effect in which high frequency signal will capture the channel and discard the low frequency or weak signals from interference.

Disadvantages of Frequency Modulation

- In the transmission section, we don't need any special equipment but in the reception, we need more complicated demodulators for demodulating the carrier signal from message or modulating signal.
- Frequency modulation cannot be used to find out the speed and velocity of a moving object. Static interferences are more when compared to phase modulation. Outside interference is one of the biggest disadvantages in the frequency modulation. There may be mixing because of nearby radio stations, pagers, construction walkie-talkies etc.
- To limit the bandwidth in the frequency modulation, we use some filter which will again introduce some distortions in the signal.
- Transmitters and receiver should be in same channel and one free channel must be there between the systems.

Applications of Frequency Modulation (FM)

- Frequency modulation is used in radio's which is very common in our daily life.
- Frequency modulation is used in audio frequencies to synthesize sound.
- For recording the video signals by VCR systems, frequency modulation is used for intermediate frequencies.
- Used in applications of magnetic tape storage.

Phase Modulation

In this type of modulation, the phase of the carrier signal varies in accordance with the message signal. When the phase of the signal is changed, then it affects the frequency. So, for this reason, this modulation is also comes under the frequency modulation.

In the phase modulation, we vary the carrier signal in accordance with the phase of the modulating signal or message signal by keeping the frequency constant. If the amplitude of message or modulating signal is huge then the phase shift will also be greater.
Generally, phase modulation is used for transmitting waves. It is an essential part of many digital transmission coding schemes that underlie a wide range of technologies like GSM, WiFi, and satellite television.

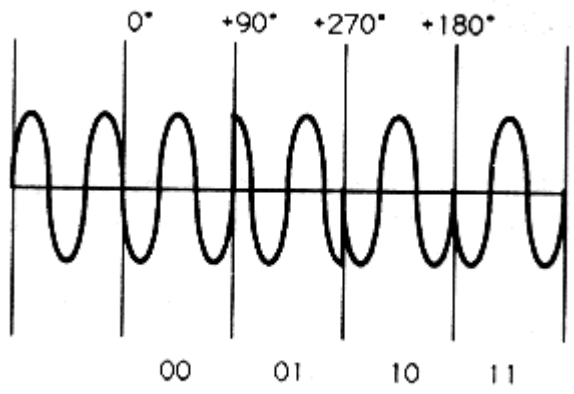
Advantages and Disadvantages of Phase Modulation

- The main advantage of phase modulation is that it has less interference from static, which is why we use this type of modulation in finding out the speed or velocity of a moving object. In frequency modulation, we cannot find out the velocity of moving object.

- The main disadvantage is phase ambiguity comes if we increase the phase modulation index, and data loss is more and we need special equipment like frequency multiplier for increasing the phase modulation index.

Applications of Phase Modulation

- Phase modulation application is not different from frequency modulation. Phase modulation is also used in communication systems.
- It may be used in binary phase shift keying.



PHASE MODULATION USING FOUR PHASES

Digital Modulation

For a better quality and efficient communication, digital modulation technique is employed. The main advantages of the digital modulation over analog modulation include available bandwidth, high noise immunity and permissible power. In digital modulation, a message signal is converted from analog to digital message, and then modulated by using a carrier wave. The carrier wave is switched on and off to create pulses such that the signal is modulated. Similar to the analog, in this system, the type of the digital modulation is decided by the variation of the carrier wave parameters like amplitude, phase and frequency.
The most important digital modulation techniques are based on keying such as Amplitude Shift Keying, Frequency Shift Keying, Phase Shift Keying,

Pulse Modulation

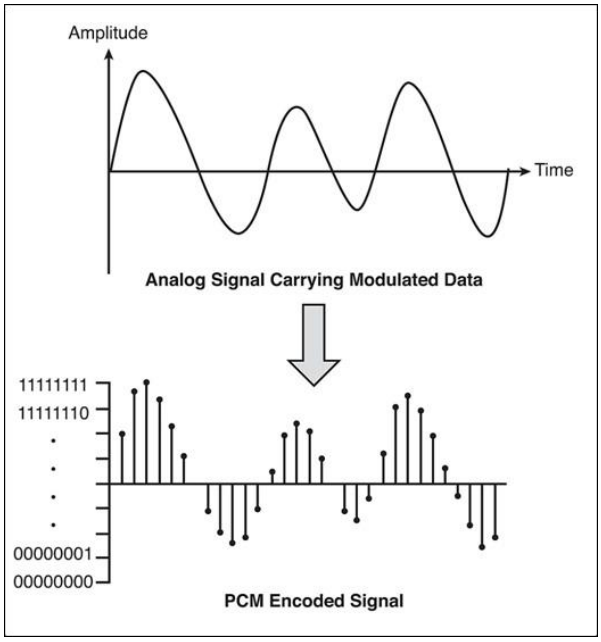
The Pulse wave modulation is a process of sampling of the continuous wave at periodic intervals and transmitting a very short pulse of radio frequency carrier for each sample, with the pulse characteristics being varied in some manner proportional to the signal amplitude at the sampling instant.

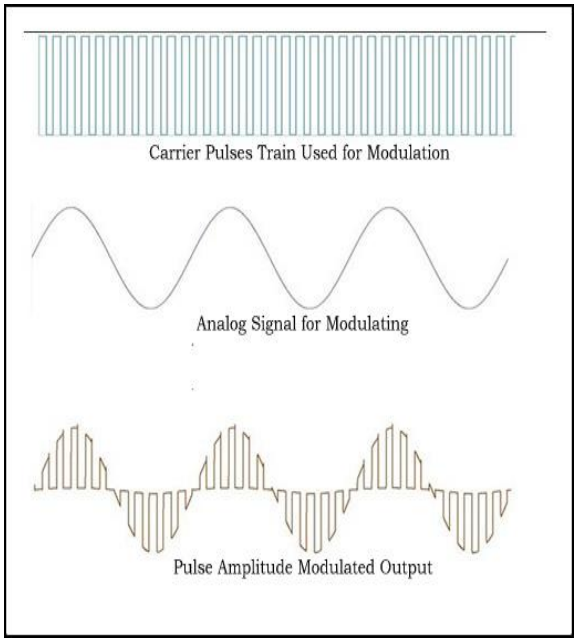
In the **pulse code modulation (PCM)**, Analog Signal is reconstructed to digital signal for ease of transmission by using the analog signal samples. In technical terms, PCM will transmit the analog in a digital form, whose signal is sampled at regular intervals of time and quantized at same quantum levels to digital code.

In **pulse amplitude modulation (PAM)**, the amplitude of regular interval of periodic pulses or electromagnetic pulses is varied in proposition to the sample of modulating signal or message signal. This is an analog type of modulation.

In the **pulse position modulation (PPM)**, the position of each pulse in a signal by taking the reference signal is varied according to the sample value of message or modulating signal instantaneously. In the pulse position modulation, width and amplitude is kept constant.

In **pulse width modulation (PWM)** or pulse duration modulation, the width of the pulse carrier is varied in accordance with the sample values of message signal or modulating signal or modulating voltage. In pulse width modulation, the amplitude is made constant and width of pulse and position of pulse is made proportional to the amplitude of the signal.





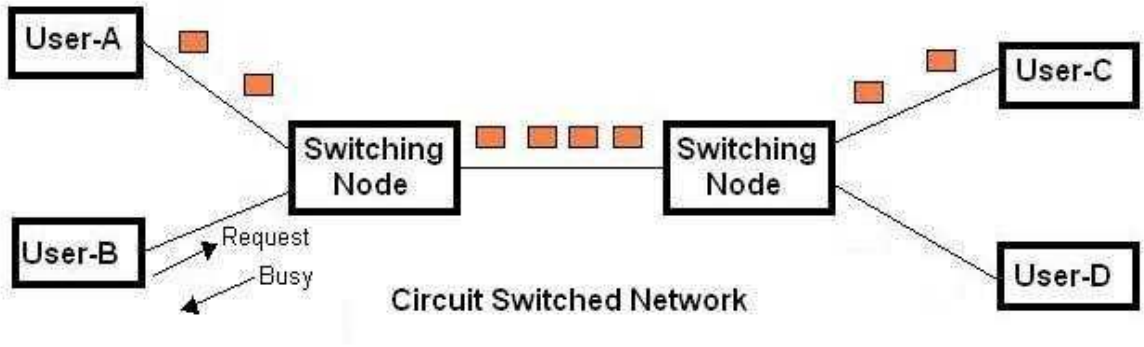
Switching

Switching is process to forward packets coming in from one port to a port leading towards the destination. In large networks there might be multiple paths linking sender and receiver. Information may be switched as it travels through various communication channels.

There are basically three types of switching methods are made available. Out of three methods, circuit switching and packet switching are commonly used but the message switching has been opposed out in the general communication procedure but is still used in the networking application.

1. Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There 'is a need of pre-specified route from which data will travels and no other data is permitted .In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.
Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases: Establish the circuit, Transfer the data, Disconnect the circuit.
Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

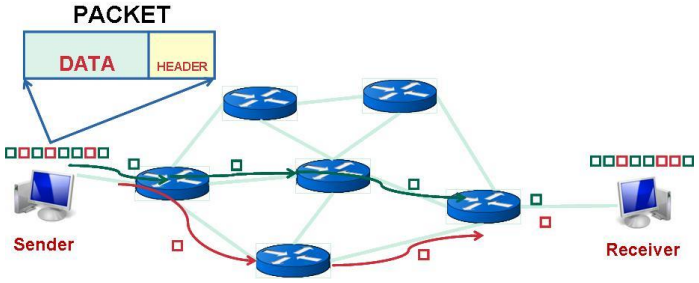


Advantages of circuit switching

Packet switching has to distinct advantages.
1. A damaged packet can be resent - only the damaged part is sent, no need to resent an entire file.
2. It allows multiplexing; different users, or different processes from the same user, can communicate at the same time.

2. Packet Switching

The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently. It is easier for intermediate networking devices to store small size packets and they do not take many resources either on carrier path or in the internal memory of switches.
Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.



Advantage of Packet Switching

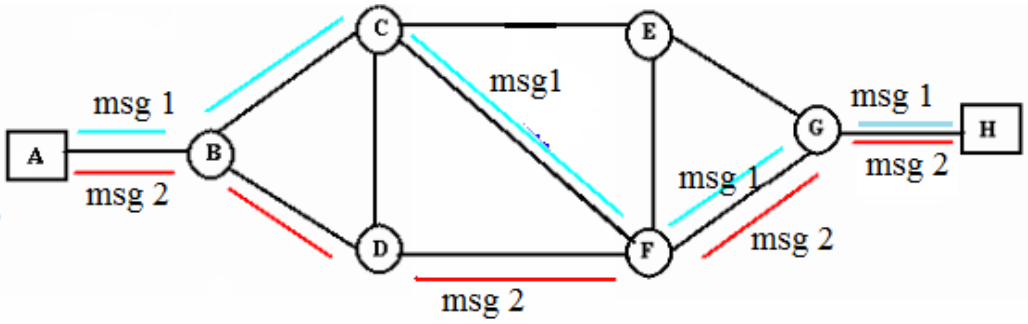
- More efficient use of overall network bandwidth due to flexibility in routing
- Packet switching networks are often cheaper to build as less equipment is needed.
- Another benefit of packet switching is known as "pipelining".

3. Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.
A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.
This technique was considered substitute to circuit switching. Message switching is replaced by packet switching.

Message switching has the following **drawbacks:**

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.



Diag of Circuit switching

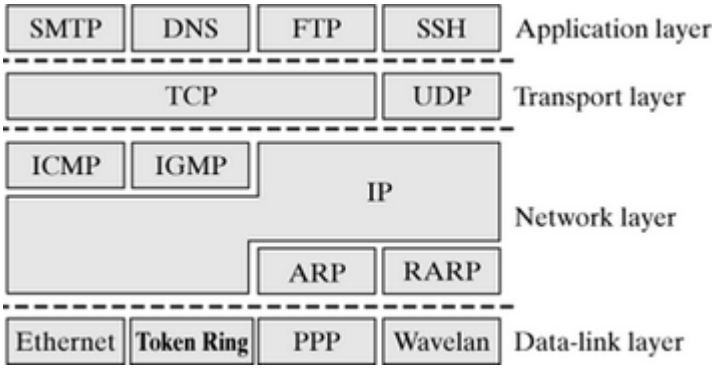
Circuit Switching vs. Packet Switching

Circuit Switching	Packet Switching
Physical path exist between source and destination	No physical path
All packets use same path	Packets travel independently
Reserve the entire bandwidth in advance	Does not reserve
Bandwidth Wastage	No Bandwidth wastage
No store and forward transmission	Support store and forward transmission

Internet protocol Stack

A protocol stack refers to a group of protocols that are running concurrently that are employed for the implementation of network protocol suite.

The protocols in a stack determine the interconnectivity rules for a layered network model such as in the OSI or TCP/IP models. To become a stack the protocols must be interoperable being able to connect both vertically between the layers of the network and horizontally between the end-points of each transmission segment.
The protocol stack is used to allow the combination of different protocols that each set the boundaries for a number of network activities.

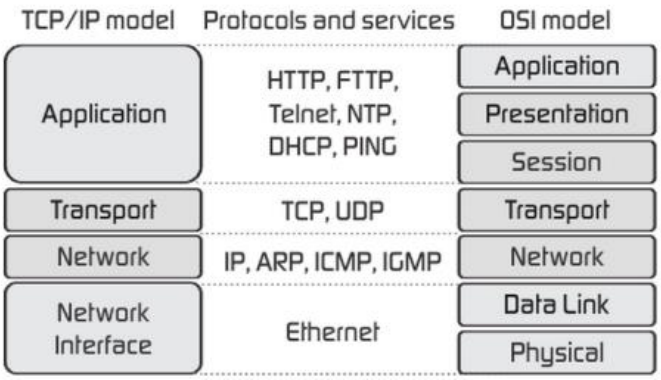


Note
IGMP - Internet Group Management Protocol
ICMP – Internet Control Message Protocol
RARP – Reverse Address Resolution Protocol
ARP – Address Resolution protocol
SMTP – Simple Mail Transport Protocol
TCP – Transport Control Protocol
UDP – User Datagram Protocol

Layered Architecture

The layer architecture is basically grouping different components according to their purpose and structuring different layers so that the higher layers use the services provided by the lower layers. Layered architecture is a technique used in designing computer software, hardware, and communications in which system or network components are isolated in layers so that changes can be made in one layer without affecting the others.
The layered architecture has the following **benefits**.

1. The implementation of higher level system components is simplified by the usage of lower level system component.
2. Lower level system components are independent of functionalities and modification in higher level system components.
3. Testing of lower level system is possible, before the higher system levels are put in use.



E.g. OSI Layer/TCP IP layer in Networking

Network Entities and Layers

In the Open Systems Interconnection (OSI) model of network communication, an entity is an active element within a subsystem that communicates with other entities using a defined protocol. A **network element** is usually defined as a manageable logical entity uniting one or more physical devices. This allows distributed devices to be managed in a unified way using one management system.

OSI Layer	Layer Name	Devices
4-7	Transport, Session, Presentation,Application	**Multi-Layer Swtich**
3	Network	Routers, **Layer 3 Switch**
2	Data Link	**Switches**, Bridges, NIC's
1	Physical	**Hub or Layer 1 switch**

The OSI Reference Model

OSI (Open Systems Interconnection) is reference model for how applications can communicate over a network. A reference model is a conceptual framework for understanding relationships. The purpose of the OSI reference model is to guide vendors and developers so the digital communication products and software programs they create will interoperate, and to facilitate clear comparisons among communications tools.
The OSI reference model architecture divides network communication into seven layers. The seven layers of function are provided by a combination of applications, operating systems, network card device drivers and networking hardware that enable a system to put a signal on a network cable or out over Wi-Fi or other wireless protocol). Each layer covers different network activities, equipment, or protocols. The OSI layers may be summarized by:

1. **Physical Layer**: The physical layer is the actual cable, fibers, cards, switches, and other mechanical and electrical equipment that make up a network. This is the layer that transforms digital data into signals that can be sent down a wire to transmit data. These signals are often electrical but, as in the case of fiber optics, they can also be non-electrical signals such as optics or any other type of pulse that can be digitally encoded. It activates, maintain and deactivate the physical connection. Voltages and data rates needed for transmission is defined in the physical layer. It converts the digital bits into electrical signal.

2. **Data Link Layer:** Data link layer synchronizes the information which is to be transmitted over the data. Error controlling is easily done. The encoded data are then passed to physical. Error detection bits are used by the data link on layer. It also corrects the errors. Outgoing messages are assembled into frames. Then the system waits for the acknowledgements to be received after the transmission. It is reliable to send message. This layer has two sub-layers, the Logical Link Control Layer and the Media Access Control Layer.

3. **The Network Layer:** It routes the signal through different channels to the other end. It acts as a network controller. It decides by which route data should take. It divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels. This layer also determines the route from the source to the destination computer. It determines which path the data should take based on network conditions, priority of service, and other factors. It also manages traffic problems on the network, such as switching and routing of packets and controlling the congestion of data.

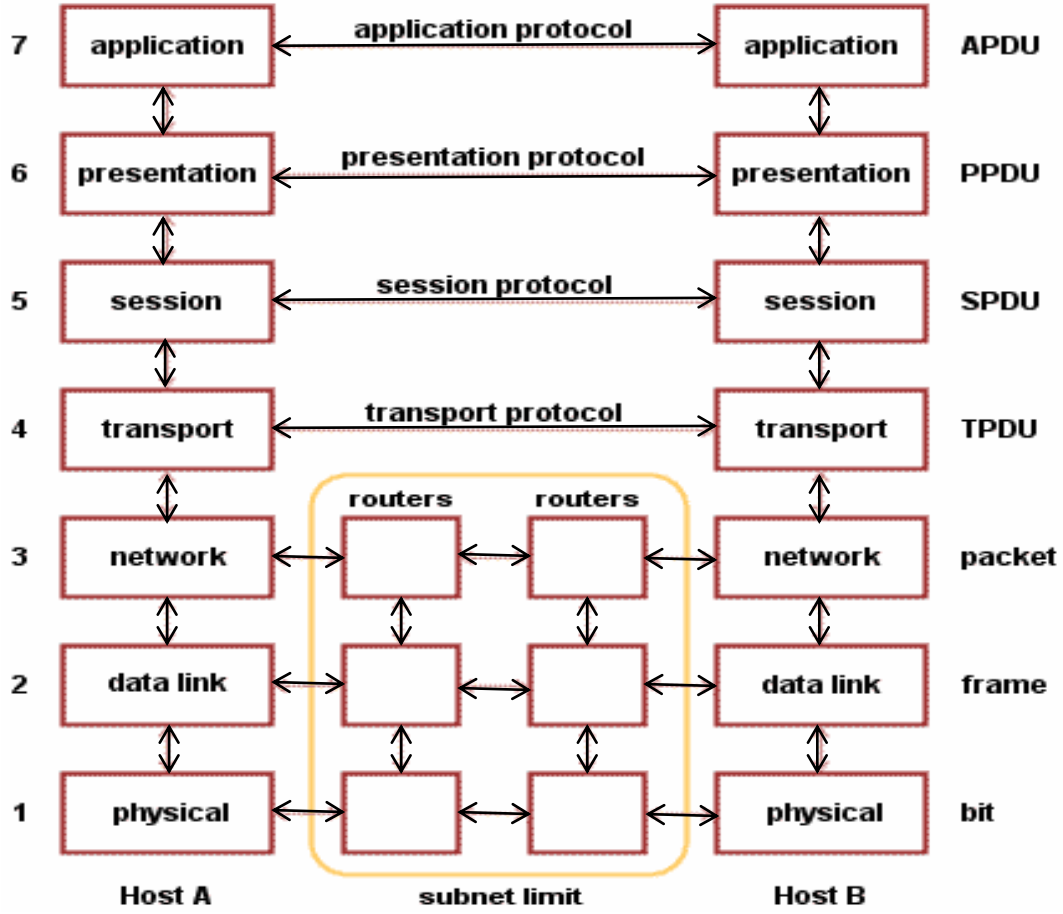


Fig: ISO-OSI Reference Model

4. **The Transport Layer:** The transport layer is responsible for streaming data across the network. It decides if data transmission should be on parallel path or single path.
   The network layer and the transport layer work together like a postal system. The network layer addresses the data, much like a person addresses an envelope. Then, the transport layer acts as the sender's local postal branch, sorting and grouping all similarly addressed data into larger shipments bound for other local branches, where they will then be delivered.
   Functions such as multiplexing, segmenting or splitting on the data done by layer four that is transport layer. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer. Ex. SPX, TCP, UDP.

5. **The session Layer:** Session layer manages and synchronize the conversation between two different applications. Transfer of data from one destination to another session layer streams

of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided. This layer sets up, coordinates and terminates conversations. Services include authentication and reconnection after an interruption.

6. **The Presentation Layer:** Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data. The presentation layer is where received data is converted into a format that the application it is destined for can understand. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role translator.

7. **Application Layer:** It is the top layer. It supports application and end-user processes. Everything at this layer is application-specific. Manipulation of data (information) in various ways is done in this layer. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc. are services provided by application layer. Layer 7 Application examples include WWW browsers, NFS, SNMP, Telnet, HTTP, FTP, etc.

Advantages of OSI model

- It is standard legalized by International Standards Organization (ISO).
- All OSI layers providing error checking and handling.
- Provides connection-oriented and connectionless model.
- OSI protocols are well hidden and can be replaced easily as the technology changes.
- Emphasis on providing reliable data transfer service.

Disadvantages of OSI model

- OSI is complex and costly
- Not so widespread as TCP/ IP

The TCP/IP Reference Model

TCP/IP that is transmission control protocol and the internet protocol was developed by Department of Defense's Project Research Agency (ARPA, later DARPA) under the project of network interconnection.

Originally it was created to connect military networks together, later it was used by government agencies and universities. It is robust to failures and flexible to diverse networks. Most widely used protocol for interconnecting computers and it is the protocol of the internet. The following were seen as major design goals:

- ability to connect multiple networks together seamlessly
- ability for connections to remain intact as long as the source and destination machines were functioning
- to be built on flexible architecture

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

TCP/IP Layers	TCP/IP Prototocols				
Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Transport Layer	TCP		UDP		
Network Layer	IP		ARP	ICMP	IGMP
Network Interface Layer	Ethernet		Token Ring	Other Link-Layer Protocols	

1. Link Layer (or Host-To-Network Layer)

The network interface layer, also called ***the link layer or the data-link layer or Host to Network Layer***, is the interface to the actual network hardware. This is the lowest layer in TCP/IP model. The host has to connect to network using some protocol, so that it can send IP packets over it. This protocol varies from host to host and network to network.

2. Internet Layer

The function of this layer is to allow the host to insert packets into network and then make them travel independently to the destination. However, the order of receiving the packet can be different from the sequence they were sent. The internetwork layer, also called the **internet layer or the network layer, provides the "virtual network"** image of an internet this layer shields the higher levels from the physical network architecture below it. Internet Protocol (IP) is the most important protocol in this layer.

3. Transport Layer

It does the same functions as that of transport layer in OSI model. Here are the key points regarding transport layer:

- It decides if data transmission should be on parallel path or single path.
- Functions such as multiplexing, segmenting or splitting on the data done by layer four that is transport layer.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
- Functions of the transport layer are same as the OSI model.
- Transport layer also arrange the packets sent in sequence.

4. Application Layer

This layer is same as that of the OSI model and performs the following functions:

- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.

- The functions such as LOGIN or password checking are also performed by the application layer.
- **TELNET, FTP, SMTP, DN, HTTP, NNTP** are the protocols employed in this layer.

Merits of TCP/IP

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model.

S.N.	OSI (Open System Interconnection)	TCP/IP Model
1	OSI provides layer functioning and also defines functions of all the layers.	TCP/IP model is more based on protocols and protocols are not flexible with other layers.
2	In OSI model the transport layer guarantees the delivery of packets.	In TCP/IP model the transport layer does not guarantees delivery of packets.
3	Follows horizontal approach	Follows vertical approach.
4	OSI model has a separate presentation layer	TCP/IP does not have a separate presentation layer
5	OSI is a general model.	TCP/IP model cannot be used in any other application.
6	Network layer of OSI model provide both connection oriented and connectionless service.	The Network layer in TCP/IP model provides connectionless service.
7	OSI model has a problem of fitting the protocols in the model	TCP/IP model does not fit any protocol
8	Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
9	OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.
10	It has 7 layers	It has 4 layers

How OSI reference model follows Horizontal approach and TCP/IP reference model follows vertical approach? Explain.

First, recall that every layer in the model, except the bottom (physical) layer, is really a program or algorithm running on a computer. There is no way for, say, a Web browser and a Web server to actually connect together directly—they are just software programs, after all. Instead, the software running at various layers communicates logically. That is to say, through the use of software and procedures, a process running at layer 5 on one machine can accomplish logical communication with a similar process running at layer 5 on another machine. In this way OSI reference model is called a Horizontal Approach.
Since machines are only physically connected at layer 1, this means that in order for a protocol at layer 5 to function, the data on the sending machine must "pass down" the data through the layers between layer 5 and layer 1. The data is then transmitted over the physical connection to layer 1 of the other machine, and "passed up" the protocol stack of the receiving machine to layer 5. This is how the two machines are logically linked at layer 5, even though they have no physical connection at that layer.

Vertical communication is done up and down the protocol stack every time anything is sent across the network, and of course, whenever anything is received. This occurs because the higher levels are implemented as logical functions, in software; there is no actual physical connection. The higher layers package data and send it down to the lower layers for it to be sent across the network. At the very lowest level, the data is sent over the network. On the receiving end, the process is reversed, with the data traveling back up to the higher layers on the receiving device. This mechanism is implemented in TCP/IP and so called vertical approach.

Thus, with the exception of the actual physical connection at layer 1, all horizontal communication also requires vertical communication—down the stack on one machine, and then back up the stack on the other.

X.25 Network Protocol

X.25 is a standard suite of protocols used for packet switching across computer networks. The X.25 protocols works at the physical, data link, and network layers (Layers 1 to 3) of the OSI model.
X.25 supports multiple simultaneous conversations by multiplexing packets and using virtual communication channels.
X.25 was originally designed more than 25 years ago to carry voice over analog telephone lines (dialup networks). Typical applications of X.25 today include automatic teller machine networks and credit card verification networks.

Frame Relay

Originally, frame relay was designed for use across the Integrated Services Digital Network (ISDN) interface. However, today, most interfaces use this technology to improve performance. It follows the principle of packet-switched technology, which allows sharing the network medium and the available bandwidth to end to end stations.

Frame relay puts data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the endpoints, which speeds up overall data transmission.

In the U.S., Frame Relay is quite popular because it is relatively inexpensive. However, it is being replaced in some areas by faster technologies, such as ATM.
Frame relay provides a minimal service in which it is used as a low-cost carrier to replace the networks of leased lines used to connect ATM machines, POS terminals, and other devices to mainframes for client-server applications.

NGN and MPLS

MPLS is an acronym for Multiprotocol Label Switching. A NGN is a Next Generation Network.
The MPLS environment, which has been gaining increased attention, was born out of Cisco's tag switching. MPLS was originally proposed by the IETF (Internet Engineering Task Force) in 1997, with the core specifications being finalized in 2000.
MPLS was created to address the weaknesses in traditional IP networks. MPLS is another type of network entirely: MPLS is a service-enabling technology. As such, it is capable of carrying both IP and non-IP payloads. It uses what is called "label switching" to transport cells or packets over any data link layer throughout the network. The simple idea behind MPLS is to label each packet as it enters a network; the routing across the network is then routed from a label forwarding table.

Physical Layer and its Design Issues

Introduction

The lowest layer of the OSI Reference Model is layer 1, the *physical layer*. The physical layer is special compared to the other layers of the model, because it is the only one where data is physically moved across the network interface. The following are the main responsibilities or design issues of the physical layer in the OSI Reference Model:

- **Definition of Hardware Specifications:** The details of operation of cables, connectors, wireless radio transceivers, network interface cards and other hardware devices are generally a function of the physical layer (although also partially the data link layer).
- **Encoding and Signaling:** The physical layer is responsible for various encoding and signaling functions that transform the data from bits that reside within a computer or other device into signals that can be sent over the network.
- **Data Transmission and Reception:** After encoding the data appropriately, the physical layer actually transmits the data, and of course, receives it. Note that this applies equally to wired and wireless networks, even if there is no tangible cable in a wireless network.
- **Topology and Physical Network Design:** The physical layer is also considered the domain of many hardware-related network design issues, such as LAN and WAN topology.

Transmission Media

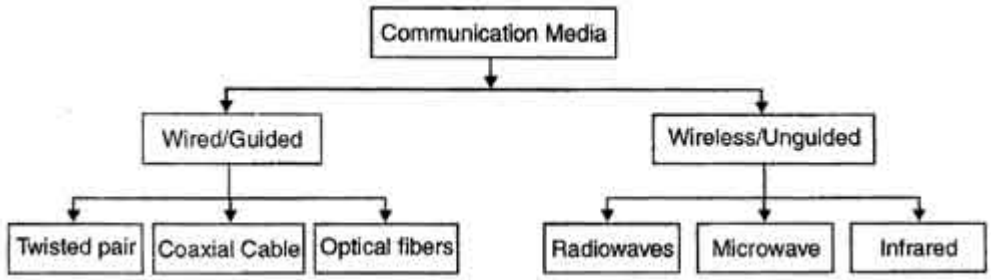
Transmission media is a pathway that carries the information from sender to receiver. We use different types of cables or waves to transmit data. Data is transmitted normally through electrical or electromagnetic signals.

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.**

Types of Transmission Media

Transmission media is broadly classified into two groups.

1. Wired or Guided Media or Bound Transmission Media
2. Wireless or Unguided Media or Unbound Transmission Media



1. Wired or Guided or Bounded Transmission Media

Bound Transmission Media in Communication Networks are the cables that are tangible or have physical existence and are limited by the physical geography. It Consist of physical connection between source and destination via a wire or a cable. These connections are bounded to a channel to follow. There are three basic types of guided media: Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost etc.

- Twisted pair cable
- Co-axial cable
- Fiber-optic cable

a) Twisted pair cable

The most popular network cabling is twisted pair. It is light weight, easy to install, inexpensive and support many different types of network. It also supports the speed of 100 MPs. Twisted pair cabling is made of pairs of solid or stranded copper twisted along each other.
The twisting reduces the electrical noise and the error rate of the data transmission.

i. Unshielded Twisted Pair Cable (UTP Cable)

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own color plastic insulator. Identification is the reason behind colored plastic insulation.
It consists of two insulating copper wires. The wires are twisted together in a helical form to reduce electrical interference from similar pair.

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- Higher grades of UTP are used in LAN technologies like Ethernet
- Bandwidth is low when compared with Coaxial Cable

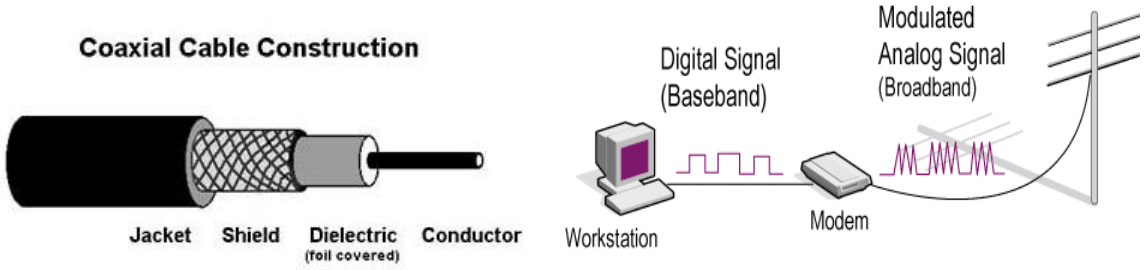
ii. Shielded Twisted Pair Cable (STP Cable)

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk.
It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk
- Heavy

b) Coaxial Cable

Coaxial cables are a type of cable that is used by cable TV and that is common for data communications. Coax cables have concentric layers of electrical conductors and insulating material. This construction ensures that signals are enclosed within the cable and prevents electrical noise from interfering with the signal.
Data is transmitted through the center wire, while the outer braided layer serves as a line to ground. Both of these conductors are parallel and share the same axis. This is why the wire is called coaxial.
Coaxial cable includes shield for improved performance and therefore is expensive. In general, coaxial cable enables longer distance transmission at higher data rates than twisted pair cable but this is more expensive.



There are two types of coaxial cables

i. Baseband Coaxial Cable: In Baseband, data is sent as digital signals through the media as a single channel that uses the entire bandwidth of the media. Baseband communication is bi-directional, which means that the same channel can be used to send and receive signals. In Baseband, frequency-division multiplexing is not possible.

The signal on baseband cable must be amplified at a specified distances. It is used for local area networks.

ii. Broadband Coaxial Cable: Broadband sends information in the form of an analog signal. Each transmission is assigned to a portion of the bandwidth; hence multiple transmissions are possible at the same time. Broadband communication is unidirectional, so in order to send and receive, two pathways are needed. This can be accomplished either by assigning a frequency for sending and assigning a frequency for receiving along the same cable or by using two cables, one for sending and one for receiving. In broadband frequency-division multiplexing is possible.

Advantages of Coaxial Cable

1. It can be used for both analog and digital transmission.
2. It offers higher bandwidth as compared to twisted pair cable and can span longer distances.
3. Because of better shielding in coaxial cable, loss of signal or attenuation is less.
4. Better shielding also offers good noise immunity.
5. It is relatively inexpensive as compared to optical fibers.
6. It has lower error rates as compared to twisted pair.
7. It is not as easy to tap as twisted pair because copper wire is contained in plastic jacket.

Limitations

1. High Installation Cost
2. High Maintenance Cost
3. More Expensive than twisted pair cables

c) Fiber-Optics Cable

Fiber Optics, also called optical fibers, is microscopic strands of very pure glass with about the same diameter of a human hair. Thousands of these optical fibers are arranged in bundles in optical cables and are used to transmit light signals over long distances. The bundles are protected by a jacket, which is the cable's outer covering. The light propagates along the fiber by the process of total internal reflection.

Fiber optics is a technology in which signals are converted from electrical into optical signals, transmitted through a thin glass fiber, and re-converted into electrical signals. The basic optical fiber consists of two concentric layers differing in optical properties, and a protective outer coating.

Core: the inner light-carrying member.
Cladding: the middle layer, which serves to confine the light to the core.
Buffer: the outer layer which serves as a "shock absorber" to protect the core and cladding from damage.

The light propagates along the fiber by the process of total internal reflection. The light is contained within the glass core and cladding by careful design of their refractive indices. The loss along the fiber is low and the signal is not subject to electromagnetic interference which plagues other methods of signal transmission, such as radio or copper wire links.

Single-mode and **multi-mode** are the two types of optical fibers. The single-mode, used for long distances, has small cores and transmits infrared laser light. The multi-mode, normally used for short distances, has large cores and transmits infrared light.

In the simplest optical fiber, the relatively large core has uniform optical properties. Termed a step-index multimode fiber, this fiber supports thousands of modes and offers the highest dispersion - and hence the lowest bandwidth.

By varying the optical properties of the core, the graded-index multimode fiber reduces dispersion and increases bandwidth. Grading makes light following longer paths travel slightly faster than light following a shorter path.

The most popular fiber for networking is the 62.5/125 multimode fiber. The numbers mean that the core diameter is 62.5 micrometer and the cladding is 125 micrometer. During transit, light pulses lose some of their energy. Attenuation for a fiber is specified in decibels per kilometer (dB/km). For commercially available fibers, attenuation ranges approximately from 0.5dB/km for single mode fibers to 1000 dB/km for large-core plastic fibers.

2. Wireless or Unguided or Unbounded Transmission Media

In Unguided or Unbounded transmission the source and destination does not have any physical connection between them. Data is sent through air which does not make it bound to a channel this known as unbounded. It is also known as Wireless media as no wires are involved in this communication. The three types of unbound transmission media are: **Radio wave, Micro wave, Infrared.**

a. **Radio wave:** Radio waves are Omni directional i.e. they travel in all the directions from the source. Because of this property, transmitter and receiver need not to be aligned. Radio waves can penetrate buildings easily, so they are widely used for communication both indoors outdoors. Radio waves can operate on a single or multiple frequency bands**.** Radio waves are widely used for AM and FM radio, television, cordless telephone, cellular phones etc.

b. **Microwave:** Microwaves have been used in data communications for a long time. They have a higher frequency than radio waves and therefore can handle larger amounts of data.
Microwave transmission is line of sight transmission. The transmit station must be in visible contact with the receive station. This sets a limit on the distance between stations depending on the local geography. Typically the line of sight due to the Earth's curvature is only 50 km to the horizon! Repeater stations must be placed so the data signal can hop, skip and jump across the country. An example of microwave technology is Bluetooth.

   i. **Terrestrial microwave:** The wireless signals can be transmitted few miles. The antennas used are parabolic and need to be pointing to each other. Low gigahertz is used in this type of communication. Signals from one antenna can be repeated to another antenna in order for the data to reach from source to destination.

   ii. **Satellite microwave:** This type of communication requires sending the relay station in space, thus to be prevented from atmosphere. The signals from Satellite are used across the world. These satellites are placed in space with the use of Rockets and Space shuttles. Being place above a very high distance from the equator, and is place in such a way that the rotation of each and the satellite matches thus always maintain a point of sight and thus looks stationary when seen from the earth.

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- Cost of launching satellite is very expensive

Difference between Satellite System and Terrestrial System

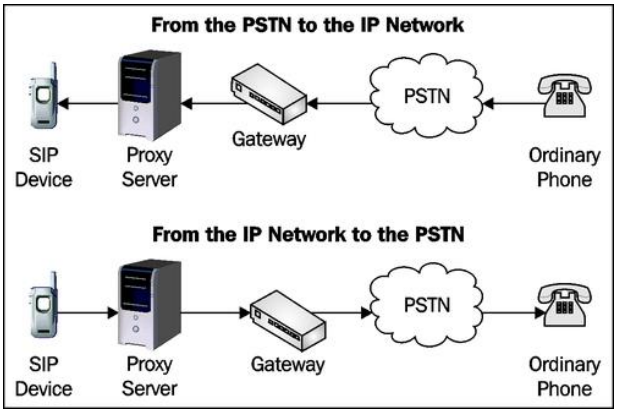
There are a number of differences between satellite based and terrestrial wireless communications that affect design.

- Coverage area of a satellite based system is greater than that of a terrestrial based wireless communication system. A GEO satellite with one single antenna can cover about $1/4^{th}$ of the earth.
- Satellite communications link will have more degradations compare to terrestrial communication link but quality of transmission is usually quite good.
- In a satellite link delay from earth to satellite to earth is about 240ms while in terrestrial link it will be far less. But transmission cost in a satellite system is independent of the distance within the area of coverage of the satellite antenna, while in terrestrial system it varies based on the distance.
- In a satellite based system satellite EIRP and bandwidth is very vital parameters which need to be carefully designed at the initial stage of both satellite and earth station point of view.
- Very high bandwidths and very high data rates are achievable in a satellite based communication system.

c. **Infrared:** Infrared offers a great unbound photonic solution. Like fiber-optic cabling, infrared communications use light, so they are not bound by the limitations of electricity.
Infrared is electromagnetic energy at a wavelength or wavelengths somewhat longer than those of red light. IR wireless is used for short- and medium-range communications and control. The key component of an infrared system is an infrared LED (Light Emitting Diode) to emit the light and a photo-diode in the television or equipment to receive the light. IR works only up to about 10 meters but that is fine for the type of applications it is mainly used for. It will only work line-of-sight.
IR wireless technology is used in intrusion detectors; home-entertainment control units; robot control systems; medium-range, line-of-sight laser communications; cordless microphones, headsets, modems, and printers and other peripherals. The range of the Device depends on the intensity of the infrared on the receiving transistor.

Public Switched Telephone Network (PSTN)

The **public switched telephone network** (**PSTN**) is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephone operators, providing infrastructure and services for public telecommunication. The PSTN consists of telephone lines, fiber optic cables and microwave transmission links.
The PSTN began in the United States in 1878 with a manual mechanical switchboard that connected different parties and allowed them



to carry on a conversation. Today, the PSTN is a network of computers and other electronic equipment that converts speech into digital data and provides a multitude of sophisticated phone features, data services, and mobile wireless access. Public switched telephone networks are communication systems that are available to the public to allow users to interconnect communication devices.

Today, as smartphones and mobile devices continue to proliferate, wireless telecom networks are taking up market share and PSTN landline technology is diminishing. In some places, less industrialized communities have skipped directly from underserved or insufficient public switched telephone network architecture directly to the use of cell phones and mobile devices.
PSTN has also been known to stand for "pretty standard telephone network," a tongue-in-check expression referring to its slow speed.
The PSTN provides traditional Plain Old Telephone Service (POTS), also known as "landline phone" service, to residences and many other establishments. Parts of the PSTN are also utilized for DSL, VoIP and other Internet-based network technologies. Thanks to the PSTN, homes and businesses can make both local and long distance telephone calls. Callers can speak and be heard by one another because communication is bidirectional.

ISDN (Integrated Service Digital Network)

ISDN Stands for "Integrated Services Digital Network." ISDN is a telecommunications technology that enables the transmission of digital data over standard phone lines. It can be used for voice calls as well as data transfers.

The first ISDN standard was defined in 1988 by the CCITT organization, which is now the ITU-T (International Telegraph and Telephone Consultative Committee). However, it wasn't until the 1990s that the service became widely used. Since the introduction of ISDN, several variants have been standardized.

There are two different types, or lines, of ISDN internet service. The first is a basic rate ISDN line. Called a Basic Rate Interface (BRI), this line has two data, or bearer, channels that operate at 64 kb/sec. Two or more ISDN-BRI lines can be combined as well; yielding speeds of 256 kb/sec. combining these lines is common for video conferencing use or for transmitting data at higher speeds. The second type of ISDN line is called a primary rate line, or Primary Rate Interface (PRI). This line had 23 bearer channels and has a total speed of 1,544 kb/sec. It is used mostly for telephone communication rather than data transmission.
ISDN was a common high-end Internet service in the 1990s and early 2000s and was offered by many ISPs as faster alternative to dial-up Internet access. Many businesses and organizations used ISDN service for both Internet access and network connections between locations. In the mid-2000s, DSL and cable serviced began to replace ISDN connections because of their faster speed and lower cost. Today, ISDN is still used in some network connections, but it is rarely used for Internet access.

PSTN vs. ISDN

1. PSTN lines are analog while ISDN lines are digital.
2. When comparing the two networks, the PSTN lines are used for small companies and ISDN are used for bigger companies.
3. The ISDN provides 128 kb/s, which is really good for the Internet. PSTN has a disadvantage that it does not make the most possible use of the broadband.

4. While PSTN does not allow two simultaneous connections, it is allowed in ISDN service.
5. When using ISDN, one can make faster calls than when using the PSTN.

DSL & ADSL

DSL (Digital Subscriber Line) is the generic term for services that provide internet connections using digital data connections between a modem and a phone line. What's great about DSL, is that even when the phone line is in use, there is no interruption, and you can still experience a high speed internet connection even when you are making calls. The only issue is, that when you are close to the central office of the company with which you are subscribed, you will have faster internet, but when you are far from their central office, although you are within their scope, you will have a slower internet connection.

There are different types of DSL. There's SDSL, VDSL, and ADSL. ADSL stands for Asymmetric Digital Subscriber Line. This type of service means that the speed of data sent is known as upstream, and the data received is known as downstream, and the speeds are not always guaranteed to be the same. They have different speeds that change from time to time. The most requested service is the ADSL service. In regards to ADSL, the internet service providers offer options for higher bandwidth, in upstream, downstream or both. The only thing is, they naturally charge higher rates for higher speeds.

ADSL uses a special ADSL modem and a micro-filter in the subscriber's telephone line. This is what allows the ADSL service and telephone service to be used at the same time. The word 'asymmetric' in ADSL actually means that the downstream is faster than the upstream. ADSL supports a downstream rate of 1.5 to 9 Mbps, and an upstream rate of 16 to 640 Kbps.
When you use ADSL, your PC will always be connected to the internet, as long as the power is on, and once you 'turn on' your computer, your PC will automatically have an internet connection, unless you manually disconnect. Unlike dial-ups, ADSL can serve various computers within a house for multiple members simultaneously.

Summary:

The simple difference between DSL and ADSL is that DSL is the generic term for Digital Subscriber Line services, and ADSL, or Asymmetric Digital Subscriber Line, is just one of its types. There are other types of DSL, such as SDSL and VDSL.

VoIP

Voice over Internet Protocol, or VoIP, is a technology by which telephone calls are placed over the Internet rather than over the standard Public Switched Telephone Network (PSTN), also known as the land line network.

Advantages to VoIP

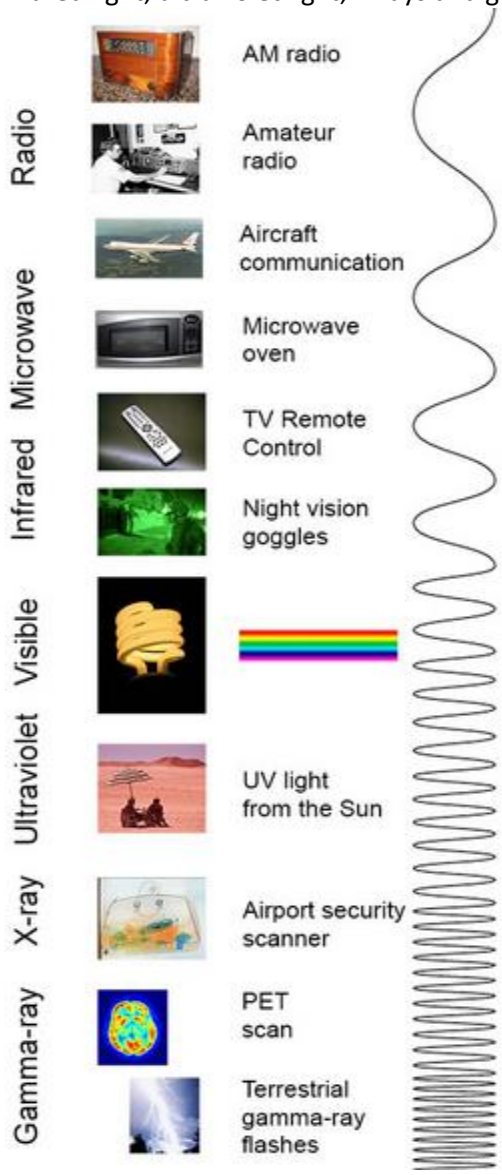
There are several advantages to using a VoIP service:

- Making international calls with a VoIP service is often much cheaper than calling from a traditional land line telephone. Often, calls are just a few cents per minute. Check with your VoIP service for specific dialing rates before placing a call.

- You can often purchase an international number. If you live in the United States, but most of your family or business contacts live in the UK, a VoIP service would enable you to purchase a local number in the UK, making it very inexpensive or even free for others to call you.

Electromagnetic Spectrum

The electromagnetic (EM) spectrum is the range of all types of EM radiation. Radiation is energy that travels and spreads out as it goes – the visible light that comes from a lamp in your house and the radio waves that come from a radio station are two types of electromagnetic radiation.
The other types of EM radiation that make up the electromagnetic spectrum are microwaves, infrared light, ultraviolet light, X-rays and gamma-rays.



Radio: our radio captures radio waves emitted by radio stations, bringing our favorite tunes. Radio waves are also emitted by stars and gases in space.

Microwave: Microwave radiation will cook our popcorn in just a few minutes, but is also used by astronomers to learn about the structure of nearby galaxies.

Infrared: Night vision goggles pick up the infrared light emitted by our skin and objects with heat. In space, infrared light helps us map the dust between stars.

Visible: Our eyes detect visible light. Fireflies, light bulbs, and stars all emit visible light.

Ultraviolet: Ultraviolet radiation is emitted by the Sun and is the reason skin tans and burns. "Hot" objects in space emit UV radiation as well.

X-ray: A dentist uses X-rays to image our teeth, and airport security uses them to see through our bag. Hot gases in the Universe also emit X-rays.

Gamma ray: Doctors use gamma-ray imaging to see inside our body. The biggest gamma-ray generator of all is the Universe.

Line of Sight

Line of sight (LoS) is a type of propagation that can transmit and receive data only where transmit and receive stations are in view of each other without any sort of an obstacle between them. FM radio, microwave and satellite transmission are examples of line-of-sight communication.

Long-distance data communication is more effective through wireless networks but geographical obstacles and the curvature of the earth bring limitations to line-of-sight transmission. However, these issues can generally be mitigated through planning, calculations and the use of additional technologies.

Introduction to Wireless LAN and IEEE 802.11

- The IEEE 802 Standard comprises a family of networking standards that cover the physical layer specifications of technologies from Ethernet to wireless.
- A wireless LAN (**WLAN or WiFi**) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure.
- The widespread acceptance of WLANs depends on industry standardization to ensure product compatibility and reliability among the various manufacturers.
- The 802.11 specification [**IEEE Std 802.11**] as a standard for wireless LANS was ratified by the Institute of Electrical and Electronics Engineers (**IEEE**) in the year 1997.
- This version of 802.11 provides for 1 Mbps and 2 Mbps data rates and a set of fundamental signaling methods and other services.
- Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels the ISO-OSI model, the physical layer and link layer.
- The major motivation and benefit from **Wireless_LANs** is increased mobility. Untethered from conventional network connections, network users can move about almost without restriction and access LANs from nearly anywhere.

Data Link Layer

What is DLL (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.
The Data Link Layer is the second layer in the OSI model, above the Physical Layer, which ensures that the error free data is transferred between the adjacent nodes in the network. It breaks the datagrams passed down by above layers and converts them into frames ready for transfer.

Data link layer has two sub-layers:

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

Functionality of Data-link Layer

Data link layer does many tasks on behalf of upper layer. These are some services provided by data link layer.

1. **Framing**
   Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

2. **Addressing**
   Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

3. **Synchronization**
   When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

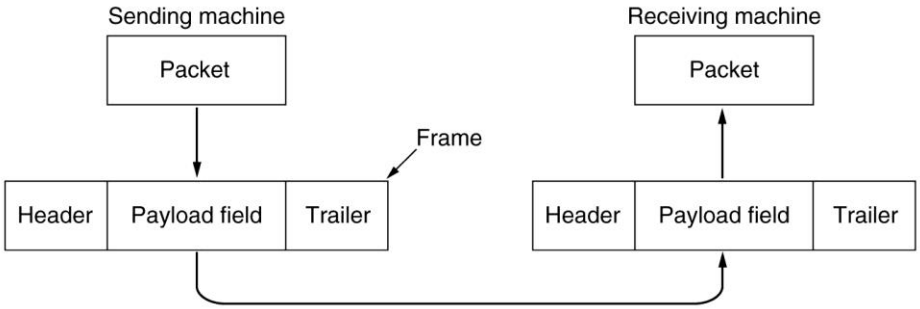
4. **Error Control**
   Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

5. **Flow Control**
   Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machines to exchange data on same speed.

6. **Multi-Access**
   When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

What is framing?

In networking, a frame is a unit of data. A frame works to help identify data packets used in networking and telecommunications structures. One way to define frames in networking is that the frame is a primary data unit within Level 2, or the data link layer of the OSI model. By contrast, Level 3, or the networking layer of the OSI model uses the packet as a primary data unit.



Since the physical layer merely accepts and transmits a stream of bits without any regard to meaning or structure, it is up to the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. If these bit patterns can accidentally occur in data, special care must be taken to make sure these patterns are not incorrectly interpreted as frame delimiters. The four framing methods that are widely used are:

1. Character count
2. Starting and ending characters, with character stuffing
3. Starting and ending flags, with bit stuffing
4. Physical layer coding violations

What is the difference between a packet and a frame?

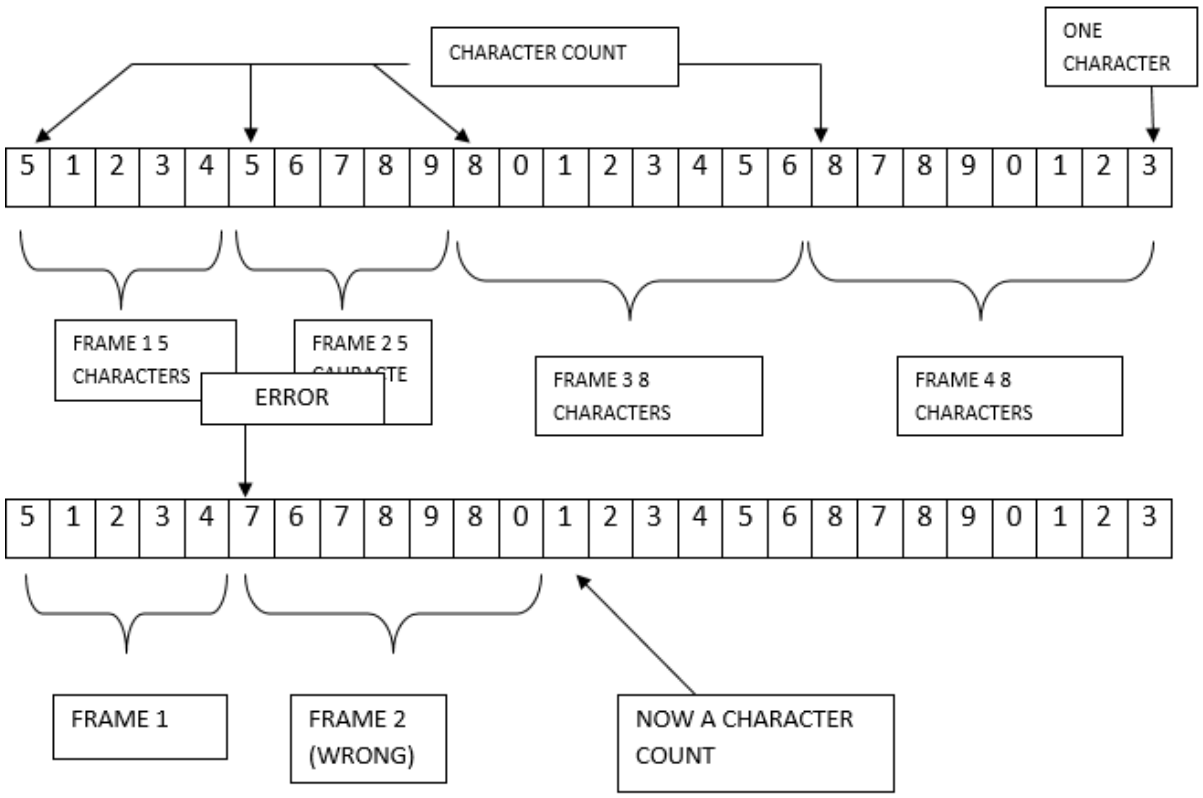
A packet refers to the encapsulated unit created at the network layer of the OSI model. One of the most commonly encountered packets is the IP packet, which contains control information such as the source and destination IP addresses, differentiated services flags and so on. Thus, a packet typically contains logical address information.
A frame, on the other hand, refers to the encapsulated unit created at the data link layer. One of the most commonly encountered frames is the Ethernet frame, which contains information such as source and destination MAC addresses etc. Thus a frame typically contains physical address information.

It is worth noting that a packet is encapsulated within a frame and hence the packet would always form the data part of the frame. For a transmitting host, data is first encapsulated within the packet, which is further encapsulated in a frame. This is then sent out over the physical layer as a bit stream. For a receiving host, the physical bit stream is picked up, translated into a frame and the frame headers are stripped off (de-capsulated), thereby retrieving the packet, which is then further de-capsulated to retrieve higher layer information.

1. Character Count

Character count method uses a field in the header to count the number of characters in the frame. When the data link layer at the destination sees the character count, it knows how many characters follow and therefore comes to know the end of the frame.

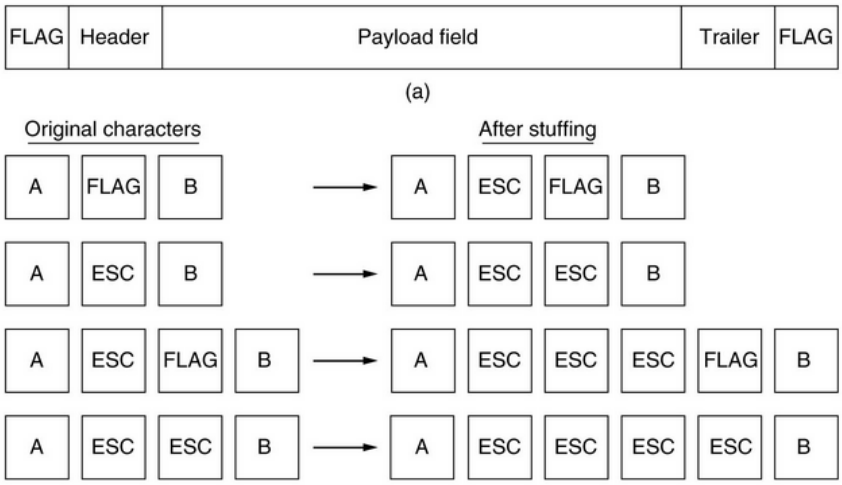
A character stream (a) without errors. (b) With one error:



Count can be garbled by a transmission error is the trouble with this algorithm. For example, if the character count of 5 in the second frame of figure (b) becomes a 7, the destination will be out of synchronization and will be unable to find the beginning of the next frame. Even if the checksum is incorrect so the destination knows that the frame is bad, it still has no way of telling where the next frame starts. Retransmission does not help either, since the destination does not know how many characters to skip over to get to the start of the retransmission. Because of which Character count method is not very frequently used.

2. Starting and ending characters, with character stuffing

This method is also called byte stuffing. In the second method, each frame starts with the ASCII character sequence DLE STX and ends with the sequence DLE ETX.(where DLE is Data Link Escape, STX is Start of TeXt and ETX is End of TeXt.) This method overcomes the drawbacks of the character count method. If the destination ever loses synchronization, it only has to look for DLE STX and DLE ETX characters. If however, binary data is being transmitted then there exists a possibility of the characters DLE STX and DLE ETX occurring in the data. Since this can interfere with the framing, a technique called character stuffing is used.
The sender's data link layer inserts an ASCII DLE character just before the DLE character in the data. The receiver's data link layer removes this DLE before this data is given to the network layer. However character stuffing is closely associated with 8-bit characters and this is a major hurdle in transmitting arbitrary sized characters.



3. Starting and ending flags, with bit stuffing

The third method allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character. At the start and end of each frame is a flag byte consisting of the special bit pattern 01111110. Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a zero bit into the outgoing bit stream. This technique is called bit stuffing.
When the receiver sees five consecutive 1s in the incoming data stream, followed by a zero bit, it automatically de-stuffs the 0 bit. The boundary between two frames can be determined by locating the flag pattern.

Bit stuffing
(a) The original data.
(b) The data as they appear on the line.
(c) The data as they are stored in receiver's memory after de-stuffing.

4. Physical layer coding violations

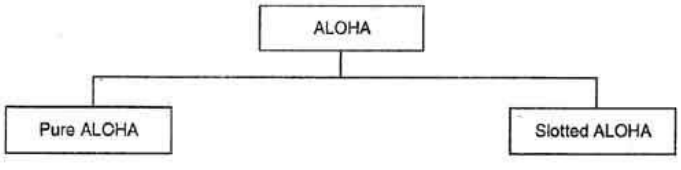
The final framing method is physical layer coding violations and is applicable to networks in which the encoding on the physical medium contains some redundancy. In such cases normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair. The combinations of low-low and high-high which are not used for data may be used for marking frame boundaries.

ALOHA

A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.
ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.
Aloha means "Hello". Aloha is a multiple access protocol at the data link layer and proposes how multiple terminals access the medium without interference or collision. In 1972 Roberts developed a protocol that would increase the capacity of aloha two fold. The Slotted Aloha protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.

There are two different types of ALOHA:

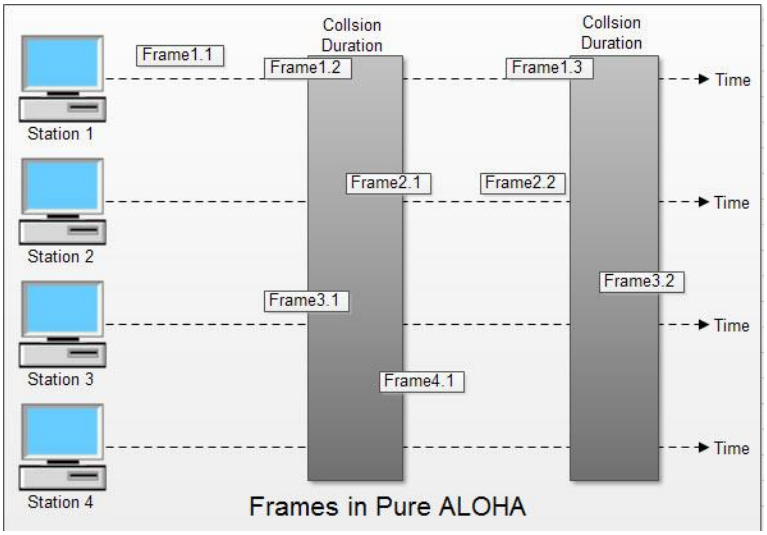
(i) Pure ALOHA
(ii) Slotted ALOHA



Types of ALOHA

(i) Pure ALOHA

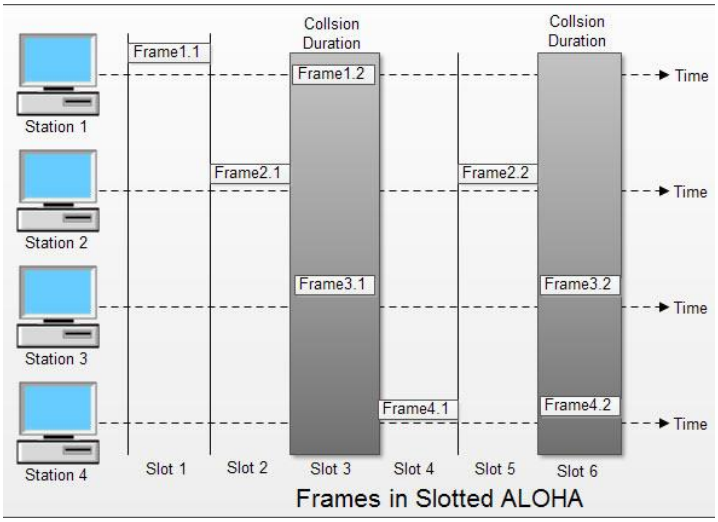
- **In** pure ALOHA, the stations transmit frames whenever they have data to send.
- When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
- If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.



- Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.
- Figure shows an example of frame collisions in pure ALOHA.
- In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.
- Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

(ii) Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.
- In slotted ALOHA, if any station



is not able to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.

- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

HDLC (High level Data link Control) Protocol

A high-level data link control (HDLC) is a protocol that is a bit-oriented synchronous data link layer. HDLC ensures the error-free transmission of data to the proper destinations and controls the data transmission speed.
HDLCs can provide both connection-oriented and connectionless services.
A high-level data link control defines rules for transmitting data between network points. Data in an HDLC is organized into units called frames and is sent across networks to specified destinations. HDLC also manages the pace at which data is transmitted. HDLC is commonly used in the open systems interconnection (OSI) model's layer 2.
HDLC frames are transmitted over synchronous links or asynchronous links, which do not mark the start and end of frames. This is done using a frame delimiter or flag, which contains unique sequence of bits that are not visible inside a frame.

There are three types of HDLC frames:

- Information frames/User data (I-frames)
- Supervisory frames/Control data (S-frames)
- Unnumbered frames (U-frames)

On **synchronous** links, this is done with bit stuffing. Any time that 5 consecutive 1-bits appear in the transmitted data, the data is paused and a 0-bit is transmitted. This ensures that no more than 5 consecutive 1-bits will be sent.

When using **asynchronous** serial communication such as standard RS-232 serial ports, bits are sent in groups of 8, and bit-stuffing is inconvenient. Instead they use "control-octet transparency", also called "byte stuffing" or "octet stuffing". The frame boundary octet is 01111110, (7E in hexadecimal notation). A "control escape octet", has the bit sequence '01111101', (7D hexadecimal).

The common fields within an HDLC frame are:

- Flag
- Address
- Control information
- Frame check sequence

The contents of an HDLC frame are shown in the following table:

Flag	Address	Control	Information	FCS	Flag
8 bits	8 or more bits	8 or 16 bits	Variable length, n * 8 bits	16 or 32 bits	8 bits

The HDLC protocol is used by a variety of standards implemented in the protocol stacks of X.25, V.42 and ISDN and many other protocol stacks.

Modes of operation

1. **The best-effort or datagram service**

   In this mode, the packets are carried in a UI frame, and a best-effort delivery is performed (i.e. there is no guarantee that the packet carried by the frame will be delivered.) The link layer does not provide error recovery of lost frames. This mode is used for point-to-point links carrying a network protocol which itself uses datagram packets

2. **The Asynchronous Balanced Mode (ABM)**

   This provides a reliable data point-to-point data link service and may be used to provide a service which supports either a datagram or reliable network protocol. In this mode, the packets are carried in numbered I-frames, which are acknowledged by the receiver using numbered supervisory frames. Error recovery (e.g. checkpoint or go-back-n error recovery) is employed to ensure a well-ordered and reliable flow of frames.

Error Detection and Correction

In networking, error detection refers to the techniques used to detect noise or other impairments introduced into data while it is transmitted from source to destination. Error detection ensures reliable delivery of data across vulnerable networks. Error detection minimizes the probability of passing incorrect frames to the destination, known as undetected error probability.

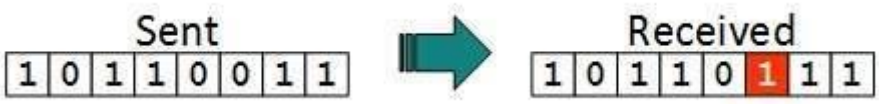
There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing. Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

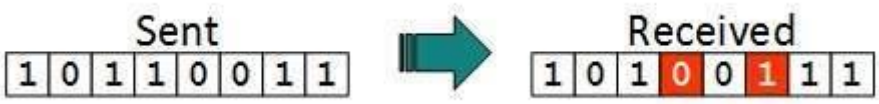
Types of Errors

There may be three types of errors:

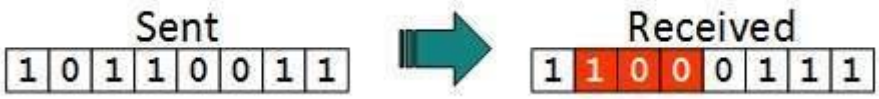
1. **Single bit error:** In a frame, there is only one bit, anywhere though, which is corrupt.



2. **Multiple bits error:** Frame is received with more than one bits in corrupted state.



3. **Burst error:** Frame contains more than1 consecutive bits corrupted.



Error control mechanism may involve two possible ways:

1. Error detection
2. Error correction

Error Detection

Error detection is the process of detecting the error during the transmission between the sender and the receiver. Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

Types of error detection

1. Parity checking
2. Cyclic Redundancy Check (CRC)
3. Checksum

1. Parity Checking

Parity adds a single bit that indicates whether the number of "1" bits in the preceding data is even or odd. If a single bit is changed in transmission, the message will change parity and the error can be detected at this point. Parity checking is not very robust, since if the number of bits changed is even, the check bit will be invalid and the error will not be detected.

- Single bit parity
- Two dimension parity

- **Even parity** -- Even parity means the number of 1's in the given word including the parity bit should be even (2,4,6,....).
- **Odd parity** -- Odd parity means the number of 1's in the given word including the parity bit should be odd (1,3,5,....).

The parity bit can be set to 0 and 1 depending on the type of the parity required.

For even parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is even. Shown in fig. (a).

For odd parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is odd as shown in fig. (b).

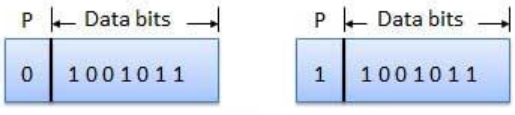


Fig. (a)

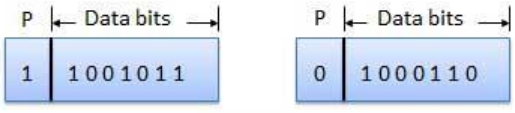


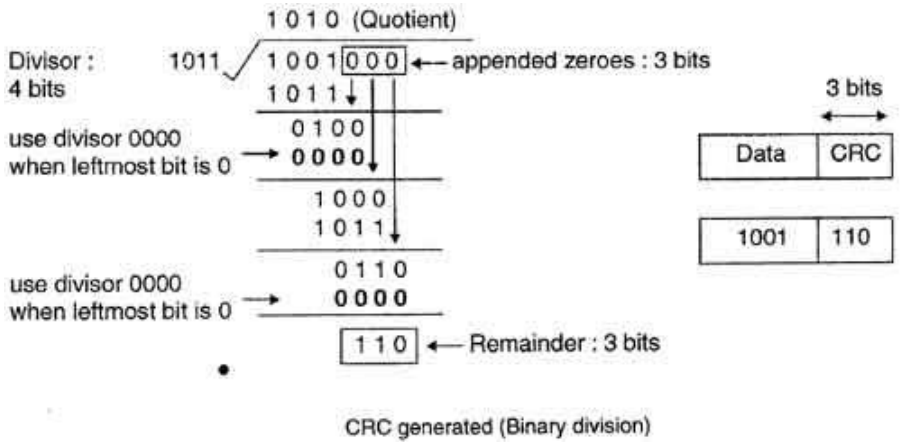
Fig. (b)

The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added
The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

Moreover, parity does not indicate which bit contained the error, even when it can detect it. The data must be discarded entirely, and re-transmitted from scratch. On a noisy transmission medium a successful transmission could take a long time, or even never occur. Parity does have the advantage, however, that it's about the best possible code that uses only a single bit of space

2. Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a code-word. The sender transmits data bits as code-words.
At the other end, the receiver performs division operation on code-words using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.



CRC generated (Binary division)

For CRC following some of Peterson & Brown's notation here . . .

- ***k*** is the length of the message we want to send, *i.e.,* the number of information bits.
- ***n*** is the total length of the message we will end up sending the information bits followed by the check bits. Peterson and Brown call this a *code polynomial*.
- ***n-k*** is the number of check bits. It is also the degree of the generating polynomial. The basic (mathematical) idea is that we're going to pick the n-k check digits in such a way that the code polynomial is divisible by the generating polynomial. Then we send the data, and at the other end we look to see whether it's still divisible by the generating polynomial; if it's not then we know we have an error, if it is, we hope there was no error.

Instead of the divisor, dividend (message), quotient, and remainder (as described in the previous section) being viewed as positive integers, they are viewed as polynomials with binary coefficients. This is done by treating each number as a bit-string whose bits are the coefficients of a polynomial.

For example, the ordinary number 23 (decimal) is 10111 binary and so it corresponds to the polynomial:

1*x^4 + 0*x^3 + 1*x^2 + 1*x^1 + 1*x^0

Or, more simply:

X^4 + x^2 + x^1 + 1

Using this technique, the message, and the divisor can be represented as polynomials and we can do all our arithmetic calculation.

Sequential steps in CRC are as follows.

Sender follows following steps.

- Data unit is composite by number of 0s, which is one less than the divisor.
- Then it is divided by the predefined divisor using binary division technique. The remainder is called CRC. CRC is appended to the data unit and is sent to the receiver.

Receiver follows following steps.

- When data unit arrives followed by the CRC it is divided by the same divisor which was used to find the CRC (remainder).
- If the remainder result in this division process is zero then it is error free data, otherwise it is corrupted

Practice question

1. Given a data word 1010011110 and the divisor 10111,
   A. Show the generation of codeword at the sender site (using binary division)
   B. Show the checking of codeword at the receiver site(assume no error)
2. Given the message M = 1010001101, determine the CRC using the generator polynomial $P = X^5 + X^4 + X^2 + 1$.

3. Checksum

Check sum is the third method for error detection mechanism. Checksum is used in the upper layers, while Parity checking and CRC is used in the physical layer. Checksum is also on the concept of redundancy.

In the checksum mechanism two operations to perform:

a. Checksum generator

Sender uses checksum generator mechanism. First data unit is divided into equal segments of n bits. Then all segments are added together using 1's complement. Then it complements ones again. It becomes Checksum and sends along with data unit.
Ex:
If 16 bits 10001010 00100011 is to be sent to receiver.
So the checksum is added to the data unit and sends to the receiver. Final data unit is 10001010 00100011 01010010.

b. Checksum checker

Receiver receives the data unit and divides into segments of equal size of segments. All segments are added using 1's complement. The result is completed once again. If the result is zero, data will be accepted, otherwise data will be rejected.
Ex:
The final data is nonzero then it is rejected.

Error Correction

In the digital world, error correction can be done in two ways:

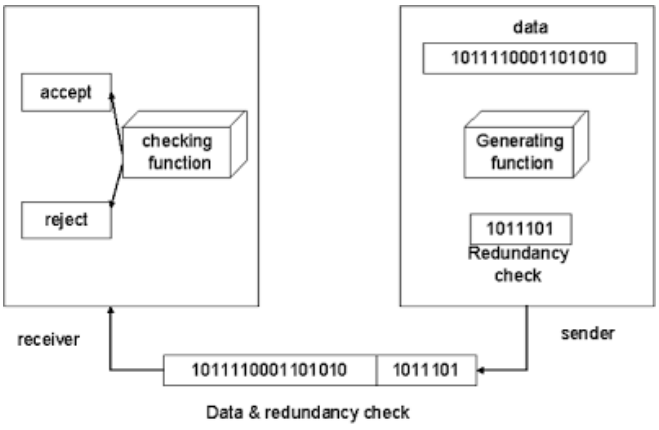
- **Backward Error Correction**: When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit. In many cases, the request is implicit; the receiver sends an acknowledgement (ACK) of correctly received data, and the transmitter re-sends anything not acknowledged within a reasonable period of time. This mechanism is also called **Automatic Repeat Request (ARQ).**

- **Forward Error Correction**: When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive; for example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

Hamming Code

Hamming code is a set of error-correction codes that can be used to detect and correct bit errors that can occur when computer data is moved or stored. Hamming code is named for R. W. Hamming of Bell Labs.
The hamming code can be applied to data units of any length and uses the relationship between data and redundancy bits. Like other error-correction code, Hamming code makes use of the concept of parity and parity bit s, which are bits that are added to data so that the validity of the data can be checked when it is read or after it has been received in a data transmission. Using more than one parity bit, an error-correction code can not only identify a single bit error in the data unit, but also its location in the data unit.



The Hamming Distance is a number used to denote the difference between two binary strings. It is a small portion of a broader set of formulas used in information analysis.

Calculating the Hamming Code

The key to the Hamming Code is the use of extra parity bits to allow the identification of a single error. Create the code word as follows:

1. Mark all bit positions that are powers of two as parity bits. (Positions 1, 2, 4, 8, 16, 32, 64, etc.)
2. All other bit positions are for the data to be encoded. (Positions 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, etc.)
3. Each parity bit calculates the parity for some of the bits in the code word. The position of the parity bit determines the sequence of bits that it alternately checks and skips.
   Position 1: check 1 bit, skip 1 bit, check 1 bit, skip 1 bit, etc. (1,3,5,7,9,11,13,15,...)
   Position 2: check 2 bits, skip 2 bits, check 2 bits, skip 2 bits, etc. (2,3,6,7,10,11,14,15,...)
   Position 4: check 4 bits, skip 4 bits, check 4 bits, skip 4 bits, etc. (4,5,6,7,12,13,14,15,20,21,22,23,...)
   Position 8: check 8 bits, skip 8 bits, check 8 bits, skip 8 bits, etc. (8-15,24-31,40-47,...)
   Position 16: check 16 bits, skip 16 bits, check 16 bits, skip 16 bits, etc. (16-31,48-63,80-95,...)
   Position 32: check 32 bits, skip 32 bits, check 32 bits, skip 32 bits, etc. (32-63,96-127,160-191,...)
   etc.
4. Set a parity bit to 1 if the total number of ones in the positions it checks is odd. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

Here is an example:

A byte of data: 10011010
Create the data word, leaving spaces for the parity bits: _ _ 1 _ 0 0 1 _ 1 0 1 0
Calculate the parity for each parity bit (a ? represents the bit position being set):

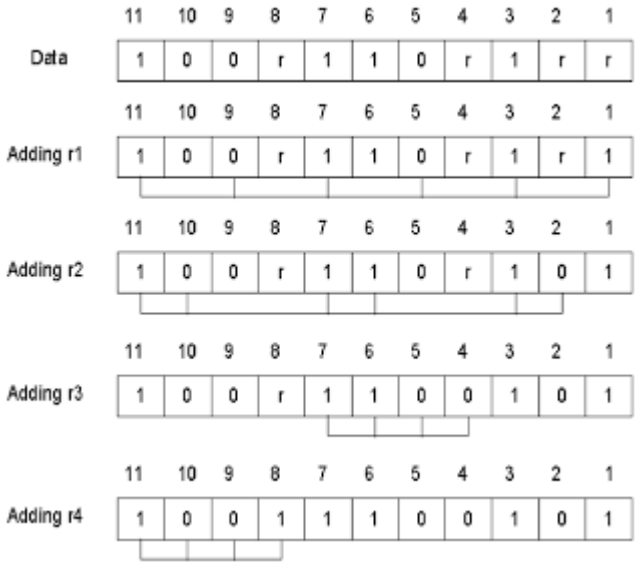
- Position 1 checks bits 1,3,5,7,9,11:
  ? _ **1** _ **0** 0 **1** _ **1** 0 **1** 0. Even parity so set position 1 to a 0: **0** _ **1** _ **0** 0 **1** _ **1** 0 **1** 0
- Position 2 checks bits 2,3,6,7,10,11:
  0 **?** **1** _ 0 **0** **1** _ 1 **0** **1** 0. Odd parity so set position 2 to a 1: 0 **1** **1** _ 0 **0** **1** _ 1 **0** **1** 0
- Position 4 checks bits 4,5,6,7,12:
  0 1 1 **?** **0** **0** **1** _ 1 0 1 **0**. Odd parity so set position 4 to a 1: 0 1 1 **1** **0** **0** **1** _ 1 0 1 **0**
- Position 8 checks bits 8,9,10,11,12:
  0 1 1 1 0 0 1 **?** **1** **0** **1** **0**. Even parity so set position 8 to a 0: 0 1 1 1 0 0 1 **0** **1** **0** **1** **0**
- Code word: 011100101010.

Error Detection and Correction

Example:

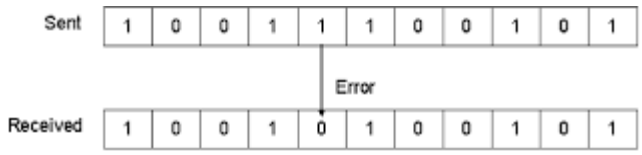
At the sender:

Data to be sent: 1001101
Redundancy bit calculation is shown below.



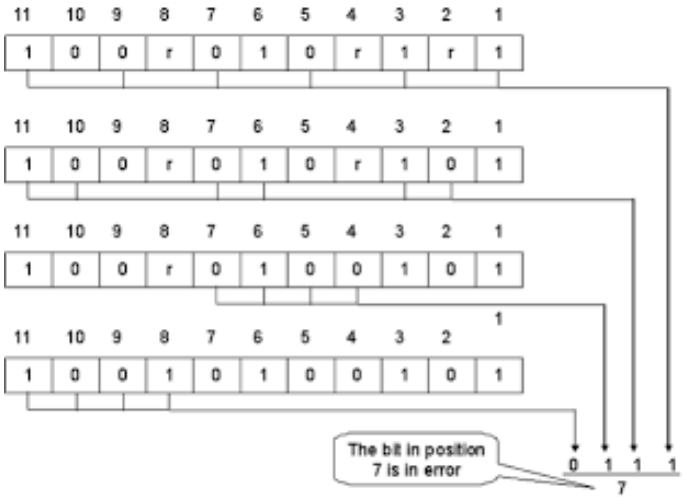
Data sent with redundancy bits: 10011100101

During transmission:



At the receiver:

The receiver takes the transmission and recalculates four new r values using the same set of bits used by the sender plus the relevant parity (r) bit for each set. Then it assembles the new parity values into a binary number in order of r position (r8, r4, r2, r1).
Once the bit is identified, the receiver can reverse its value and correct the error.



Flow Control

Flow control is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted. Flow Control is one important design issue for the Data Link Layer that controls the flow of data between sender and receiver.
In Communication, there is communication medium between sender and receiver. When Sender sends data to receiver than there can be problem in below case: Sender sends data at higher rate and receiver is too sluggish to support that data rate.
To solve the above problem, **FLOW CONTROL** is introduced in Data Link Layer. It also works on several higher layers. The main concept of Flow Control is to introduce **EFFICIENCY** in Computer Networks.

Networks of any size have many different devices connected and each device has unique data transmission parameters. For instance, a router is built to manage the routing of data whereas a desktop, at the receiving end of that data, has far less sending/receiving abilities.
These differences sending/receiving abilities may lead to conflict if the sender starts transmitting data faster than the receiving node's ability. To counteract this problem, flow control is used. This technique manages the flow of data between nodes, keeping the sending/receiving capabilities of both nodes as the primary concern.

Xon-Xoff is an example of a flow control protocol that sync the sender with the receiver. It transmits an off signal when the receiver no longer has space in its buffer and transmits on signal when the receiver can resume taking data. Xon-Xoff works on asynchronous serial connections.

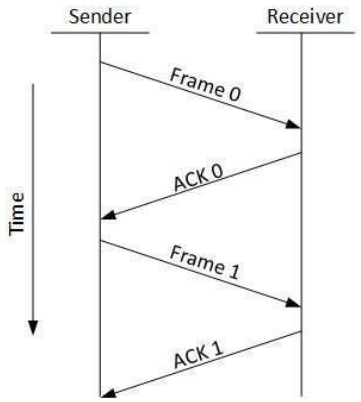
Consider a situation in which the sender transmits frames faster than the receiver can accept them. If the sender keeps pumping out frames at high rate, at some point the receiver will be completely swamped and will start losing some frames. To prevent this situation two approaches are used they are:

a. **Feedback based Flow control:** In this approach the receiver sends back information to the sender giving it permission to send more or at least telling the sender how the receiver is doing. This method is used in data link layer.
b. **Rate based flow control:** In this approach the protocol has a built in mechanism that limits the rate at which sender may transmits data, without using feedback from the receiver. The protocol contains well defined rules about when a sender may transmit the next frame. These rules often prohibit frames from being sent until the receiver has granted permission, either implicitly or explicitly for ex: when a connection is setup the receiver might say "you may send me a frame, but after they have been sent, don't send anymore, until I have told you to continue". This method is used in network layer.

While using feedback based flow control, two types of mechanisms can be deployed to control the flow:

1. Stop and Wait

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



2. Sliding Window

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Error Control

Network is responsible for transmission of data from one device to another device. The end to end transfer of data from a transmitting application to a receiving application involves many steps, each subject to error. With the error control process, we can be confident that the transmitted and received data are identical. Data can be corrupted during transmission. For reliable communication, error must be detected and corrected.

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss. In such case, both sender and receiver are equipped with some protocols which help them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

Requirements for error control mechanism:

1. **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.

2. **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.
3. **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.

4. **Retransmission:** - The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

Key Differences between Flow Control and Error Control

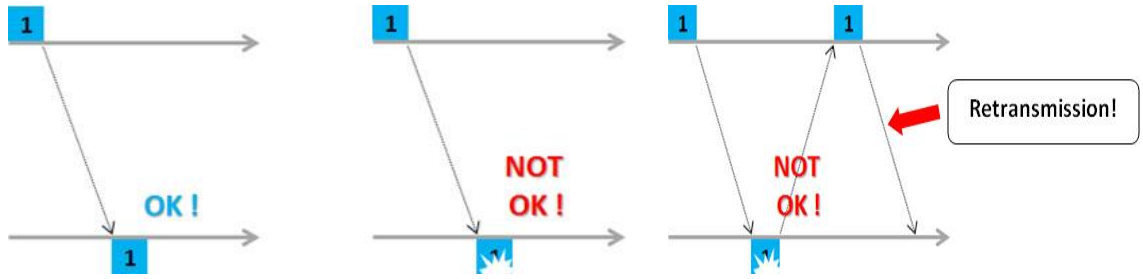
1. Flow control is to monitor the proper transmission of data from sender to receiver. On the other hand, Error Control monitors the error-free delivery of data from sender to receiver.
2. Flow control can be achieved by the Feedback-based flow control and rate-based flow control approach whereas, to detect the error the approaches used are Parity checking,

Cyclic Redundancy Code (CRC) and checksum and to correct the error the approaches used are Hamming code, Binary Convolution codes, Reed-Solomon code, Low-Density Parity Check codes.

3. Flow control prevents the receiver's buffer from overrunning and also prevents the loss of data. On the other hand, Error control detects and corrects error occurred in the data.

Retransmission Strategies

If the information arrived properly (complete), then receiver is ready to receive (and process) new data. If the information arrived with some problem, corrupted, the receiver must request that the transmitter sent the packet again. This mechanism is simply called Retransmission.

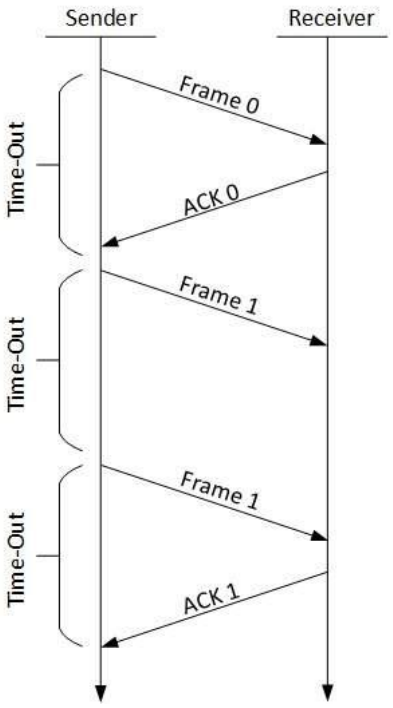


There are three types of techniques available which Data-link layer may deploy to control the errors by **Automatic Repeat Requests (ARQ)**:

- **Stop-and-wait ARQ**

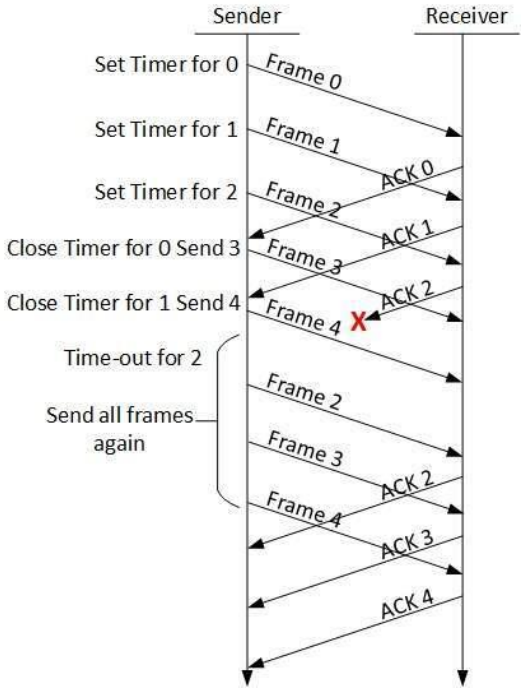
The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.



- **Go-Back-N ARQ**

Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.

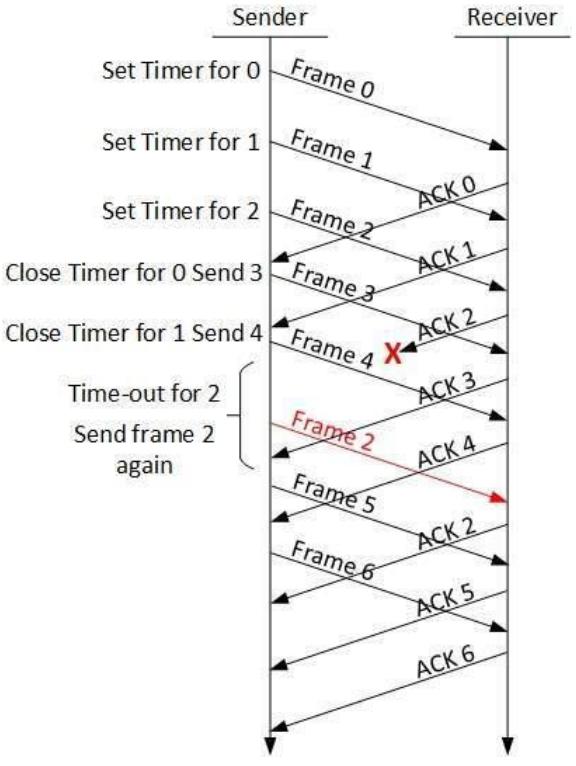


The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not received any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

- **Selective Repeat ARQ**

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

The sender in this case, sends only packet for which NACK is received.

- **Pipelining**

  The transport protocols that rely on pipelining allow the sender to transmit **W** unacknowledged segments before being forced to wait for an acknowledgement from the receiving entity. This is implemented by using a sliding window. The sliding window is the set of consecutive sequence numbers that the sender can use when transmitting segments without being forced to wait for an acknowledgement.
  Sender does not wait for each frame to be ACK'ed. Rather it sends many frames with the assumption that they will arrive. It must still get back ACKs for each frame.

Sliding Windows Protocol

Sliding window is a technique for controlling transmitted data packets between two network computers where reliable and sequential delivery of data packets is required, such as when using the Data Link Layer (OSI model) or Transmission Control Protocol (TCP). In the sliding window technique, each data packet (for most data link layers) and byte (in TCP) includes a unique consecutive sequence number, which is used by the receiving computer to place data in the correct order. The objective of the sliding window technique is to use the sequence numbers to avoid duplicate data and to request missing data.
Sliding window is also known as **windowing**.
If the application in the receiving computer processes the data packets at a slower rate than the sending computer is sending them, the acknowledgment signal from the receiving computer will tell the sending computer to decrease the number of packets in the window size in the next transmission, or to temporarily stop transmission to free the buffer. If, on the other hand, the receiving application can process the data packets faster than the sending computer is sending them, the acknowledgment signal will tell the sending computer to increase the number of packets in the next transmission.
Piggybacking- In two way communication, whenever a data frame is received, the receiver waits and does not send the control frame (acknowledgement) back to the sender immediately. The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.
"This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking."

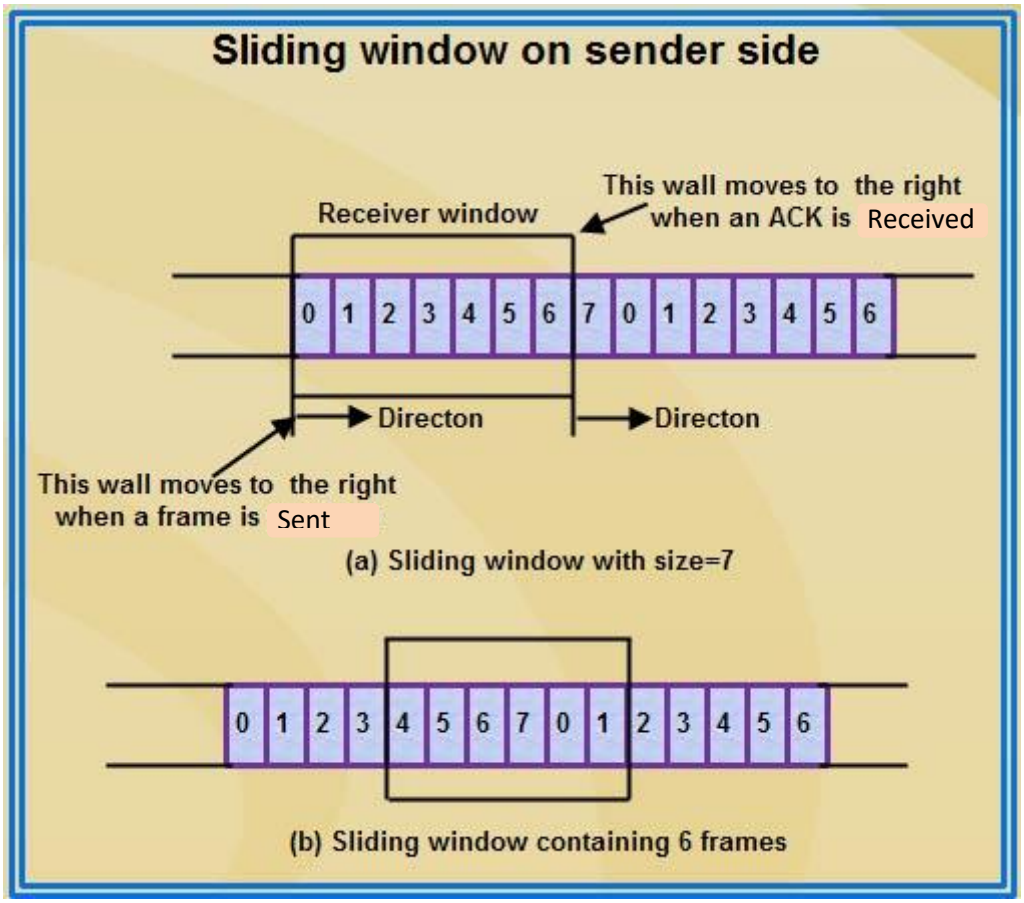
Summary

- Sliding window refers to an imaginary boxes that hold the frames on both sender and receiver side.
- It provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment.
- Frames may be acknowledged by receiver at any point even when window is not full on receiver side.
- Frames may be transmitted by source even when window is not yet full on sender side.
- The windows have a specific size in which the frames are numbered modulo- n, which means they are numbered from 0 to n-l. For e.g. if n = 8, the frames are numbered 0, 1,2,3,4,5,6, 7, 0, 1,2,3,4,5,6, 7, 0, 1, ...
- The size of window is n-1. For e.g. In this case it is 7. Therefore, a maximum of n-l frames may be sent before an acknowledgment.

- When the receiver sends an ACK, it includes the number of next frame it expects to receive. For example in order to acknowledge the group of frames ending in frame 4, the receiver sends an ACK containing the number 5. When sender sees an ACK with number 5, it comes to know that all the frames up to number 4 have been received.

Sliding Window on Sender Side

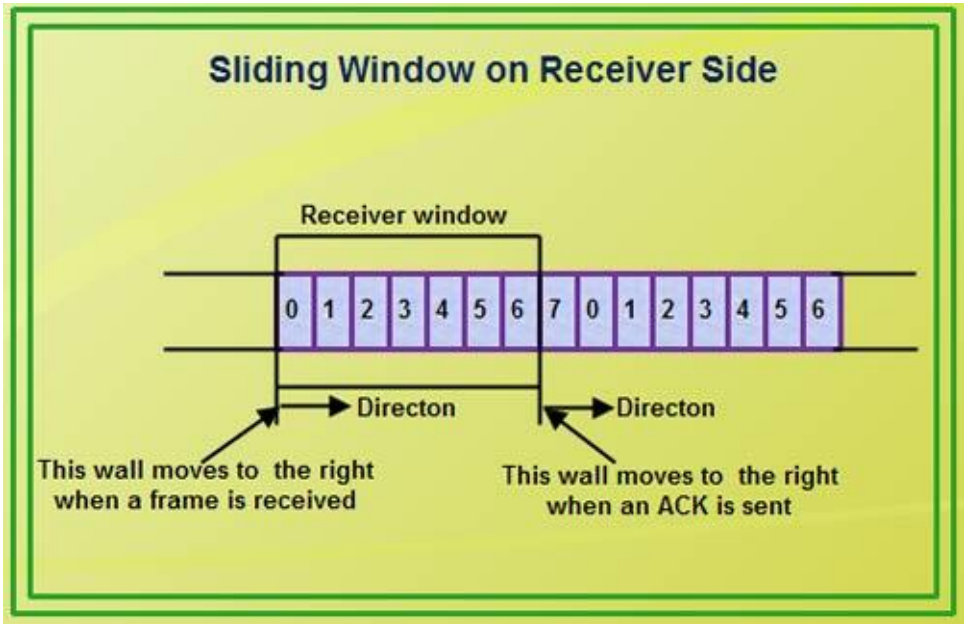
- At the beginning of a transmission, the sender's window contains n-l frames.
- As the frames are sent by source, the left boundary of the window moves inward, shrinking the size of window. This means if window size is w, if four frames are sent by source after the last acknowledgment, then the number of frames left in window is w-4.



- When the receiver sends an ACK, the source's window expand i.e. (right boundary moves outward) to allow in a number of new frames equal to the number of frames acknowledged by that ACK.
- For example, Let the window size is 7 (see diagram (a)), if frames 0 through 3 have been sent and no acknowledgment has been received, then the sender's window contains three frames - 4, 5, 6.
- Now, if an ACK numbered 3 is received by source, it means three frames (0, 1, 2) have been received by receiver and are undamaged.
- The sender's window will now expand to include the next three frames in its buffer. At this point the sender's window will contain six frames (4, 5, 6, 7, 0, and 1). (See diagram (b)).

Sliding Window on Receiver Side

- At the beginning of transmission, the receiver's window contains n-1 spaces for frame but not the frames.
- As the new frames come in, the size of window shrinks.
- Therefore the receiver window represents not the number of frames received but the number of frames that may still be received without an acknowledgment ACK must be sent.
- Given a window of size w, if three frames are received without an ACK being returned, the number of spaces in a window is w-3.
- As soon as acknowledgment is sent, window expands to include the number of frames equal to the number of frames acknowledged.
- For example, let the size of receiver's window is 7 as shown in diagram. It means window contains spaces for 7 frames.



- With the arrival of the first frame, the receiving window shrinks, moving the boundary from space 0 to 1. Now, window has shrunk by one, so the receiver may accept six more frame before it is required to send an ACK.
- If frames 0 through 3 have arrived but have DOC been acknowledged, the window will contain three frame spaces.

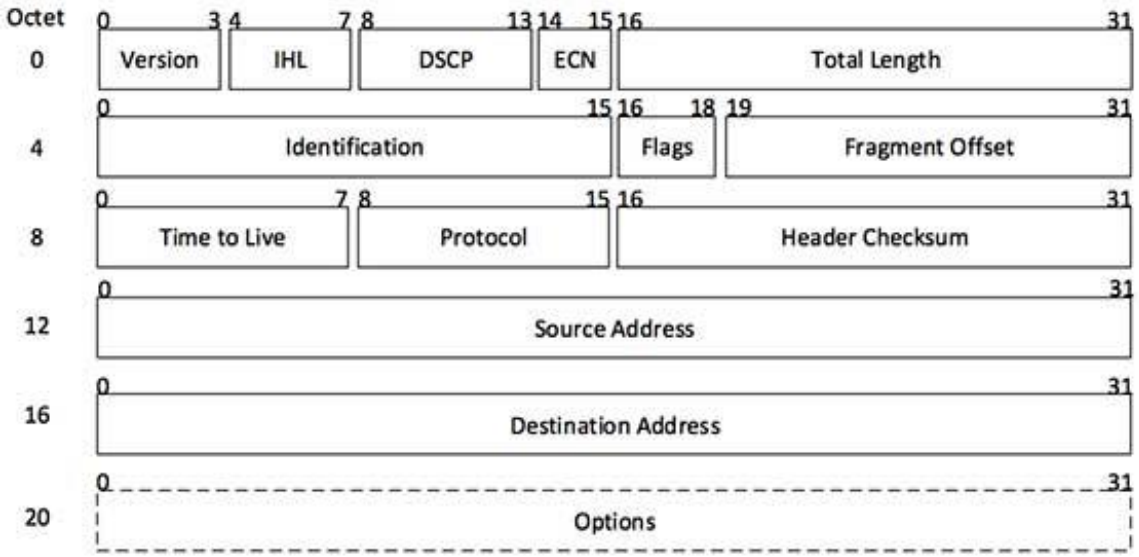
- As receiver sends an ACK, the window of the receiver expands to include as many new placeholders as newly acknowledged frames.
- The window expands to include a number of new frame spaces equal to the number of the most recently acknowledged frame minus the number of previously acknowledged frame. For *e.g.,* If window size is 7 and if prior ACK was for frame 2 & the current ACK is for frame 5 the window expands by three (5-2).
- Therefore, the sliding window of sender shrinks from left when frames of data are sending. The sliding window of the sender expands to right when acknowledgments are received.
- The sliding window of the receiver shrinks from left when frames of data are received. The sliding window of the receiver expands to the right when acknowledgement is sent

IPV4 Frame Format

The Internet Protocol specifies the technical format of packets and the addressing scheme for workstations to communicate over a data network. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication network. IP usually works in combination with the Transmission Control Protocol (TCP), which establishes a virtual connection between a source and a destination or with UDP.

Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol (IP) used to facilitate communication over a network through an addressing system. It is currently the most popular Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^{32} addresses (slightly over 4 billion addresses). Each device connecting to the Internet requires an IP address. That means that each device including cell phones, office phones, game consoles and computers each need their own IP address in order to connect and communicate over the Internet.

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.



[Image: IP Header]

(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.

IP header includes much relevant information including Version Number, which, in this context, is 4. Other details are as follows:

1. **Version:** Identifies the version of IP used to generate the datagram. For IPv4, this is of course the number 4. The purpose of this field is to ensure compatibility between devices that may be running different versions of IP.
2. ***Internet Header Length (IHL):*** Specifies the length of the IP header, in 32-bit words. This includes the length of any options fields and padding. The normal value of this field when no options are used is 5 (5 32-bit words = 5*4 = 20 bytes). Contrast to the longer *Total Length* field below.

3. ***Type of Service (TOS):*** A field designed to carry information to provide quality of service features, such as prioritized delivery, for IP datagrams. It was never widely used as originally defined, and its meaning has been subsequently redefined for use by a technique called *Differentiated Services (DS)*. **DSCP:** Differentiated Services Code Point; this is Type of Service. **ECN:** Explicit Congestion Notification; It carries information about the congestion seen in the route.
4. **Total Length:** Length of entire IP Packet (including IP header and IP Payload). Since this field is 16 bits wide, the maximum length of an IP datagram is 65,535 bytes, though most are much smaller.

5. **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.
6. **Flags:** As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
7. **Fragment Offset:** This offset tells the exact position of the fragment in the original IP Packet.
8. **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.

9. **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
10. **Header Checksum:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
11. **Source Address:** 32-bit address of the Sender (or source) of the packet.

12. **Destination Address:** 32-bit address of the Receiver (or destination) of the packet.
13. **Options:** This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

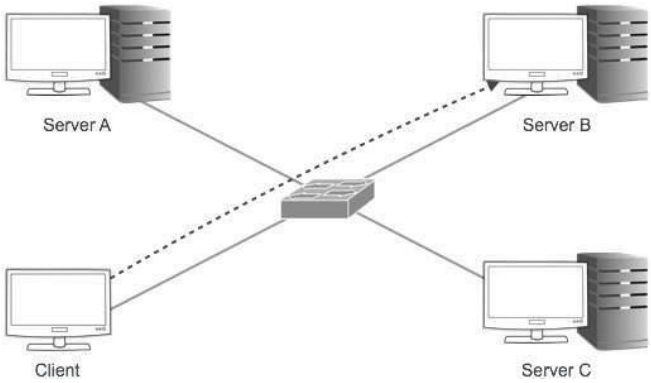
IPV4 Addressing

IPv4 supports three different types of addressing modes:

1. **Unicast Addressing Mode**

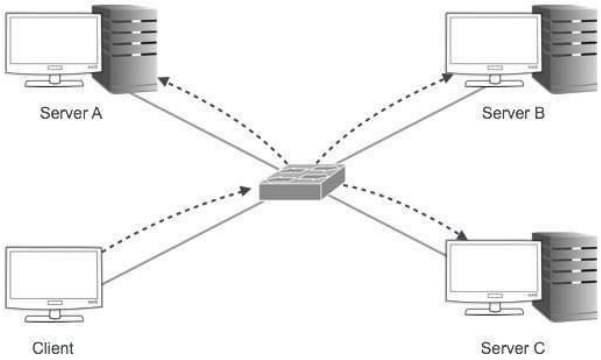
   In this mode, data is sent only to one destined host. The Destination Address field contains 32-bit IP address of the destination host. Here the client sends data to the targeted server.

   The IPv4 unicast address identifies an interface's location on the network in the same way a street address identifies a house on a city block. Just as a street address must identify a unique residence, an IPv4 unicast address must be globally unique to the network and have a uniform format.



2. **Broadcast Addressing Mode**

   In this mode, the packet is addressed to all the hosts in a network segment. The Destination Address field contains a special broadcast address, i.e. **255.255.255.255**. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers.



   The following are the different types of IPv4 broadcast addresses:

   a) **Network broadcast**. Formed by setting all the host bits to 1 for a classful address prefix. An example of a network broadcast address for the classful network ID 131.107.0.0/16 is 131.107.255.255. Network broadcasts are used to send packets to all interfaces of a classful network. IPv4 routers do not forward network broadcast packets.

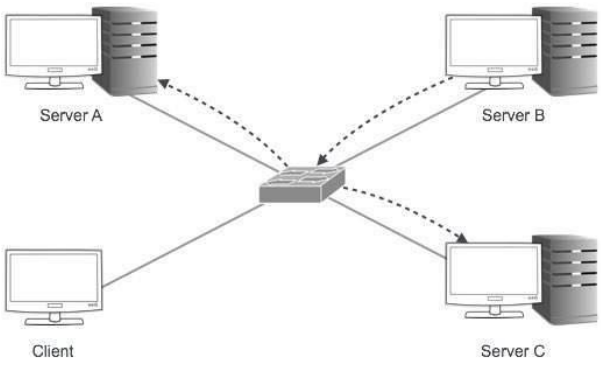
b) **Subnet broadcast**. Formed by setting all the host bits to 1 for a classless address prefix. An example of a network broadcast address for the classless network ID 131.107.26.0/24 is 131.107.26.255. Subnet broadcasts are used to send packets to all hosts of a classless network. IPv4 routers do not forward subnet broadcast packets. For a classful address prefix, there is no subnet broadcast address, only a network broadcast address. For a classless address prefix, there is no network broadcast address, only a subnet broadcast address.

c) **All-subnets-directed broadcast.** Formed by setting all the original classful network ID host bits to 1 for a classless address prefix. A packet addressed to the all-subnets-directed broadcast was defined to reach all hosts on all of the subnets of a subnetted class-based network ID. An example of an all-subnets-directed broadcast address for the subnetted network ID 131.107.26.0/24 is 131.107.255.255. The all-subnets-directed broadcast is the network broadcast address of the original classful network ID. IPv4 routers can forward all-subnets directed broadcast packets, however the use of the all-subnets-directed broadcast address is deprecated in RFC 1812.

d) **Limited broadcast.** Formed by setting all 32 bits of the IPv4 address to 1 (255.255.255.255). The limited broadcast address is used for one-to-everyone delivery on the local subnet when the local network ID is unknown. IPv4 nodes typically only use the limited broadcast address during an automated configuration process such as Boot Protocol (BOOTP) or DHCP. For example, with DHCP, a DHCP client must use the limited broadcast address for all traffic sent until the DHCP server acknowledges the use of the offered IPv4 address configuration. IPv4 routers do not forward limited broadcast packets.

3. Multicast Addressing Mode

This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.



Here a server sends packets which are entertained by more than one server. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

IPV4 Address

For IP version 4, each TCP/IP host is identified by a logical IP address. The IP address is a Network layer address and has no dependence on the Data-Link layer address (such as a MAC address of a network adapter). A unique IP address is required for each host and network component that

communicates using TCP/IP and can be assigned manually or by using Dynamic Host Configuration Protocol (DHCP).
The IP address identifies a system's location on the network in the same way a street address identifies a house on a city block. Just as a street address must identify a unique residence, an IP address must be globally unique to the internetwork and have a uniform format.

Each IP address includes a network ID and a host ID.

- **The network ID** (also known as a network address) identifies the systems that are located on the same physical network bounded by IP routers. All systems on the same physical network must have the same network ID. The network ID must be unique to the internetwork.
- **The host ID** (also known as a host address) identifies a workstation, server, router, or other TCP/IP host within a network. The host address must be unique to the network ID.

IPv4 Address Syntax

An IP address consists of 32 bits. Instead of expressing IPv4 addresses 32 bits at a time using binary notation (Base2), it is standard practice to segment the 32 bits of an IPv4 address into four 8-bit fields called *octets*. Each octet is converted to a decimal number (base 10) from 0–255 and separated by a period (a dot). This format is called *dotted decimal notation*. The following table provides an example of an IP address in binary and dotted decimal formats.

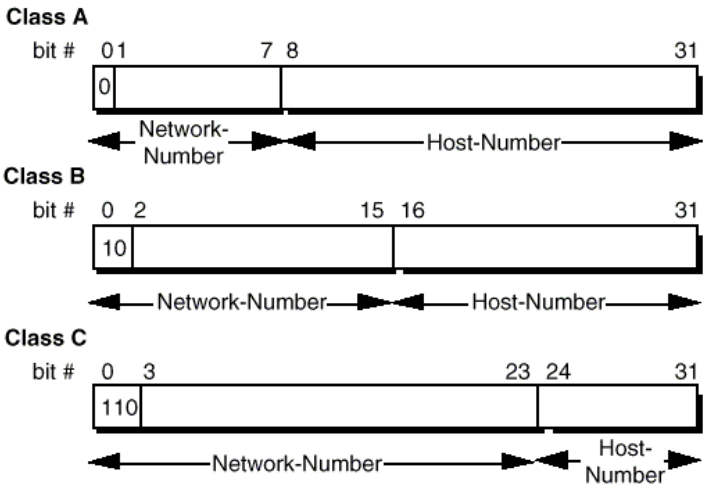
Binary Format	Dotted Decimal Notation
11000000 10101000 00000011 00011000	192.168.3.24

For example, the IPv4 address of 11000000101010000000001100011000 is:

- Segmented into 8-bit blocks: 11000000 10101000 00000011 00011000.
- Each block is converted to decimal: 192 168 3 24
- The adjacent octets are separated by a period: 192.168.3.24.

Classful Network

A classful network is a network addressing architecture used in the Internet from 1981 until the introduction of Classless Inter-Domain Routing in 1993. The method divides the address space for Internet Protocol Version 4 (IPv4) into five address classes by address range. Classes A, B, C are networks of three different network sizes, i.e. number of hosts for unicast addresses. Class D is for multicast. The class E address range is reserved for future or experimental purposes.



1. Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

00000001 – 01111111
1 – 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.
Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).
Class A network IDs were assigned to networks with a very large number of hosts. Out of a total of 128 possible classes A networks, there are 126 networks and 16,777,214 hosts per network.

2. Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – 10111111
128 – 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.
Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH
Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses. Class B network IDs were assigned to medium to large-sized networks.

3. Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is:

11000000 – 11011111
192 – 223

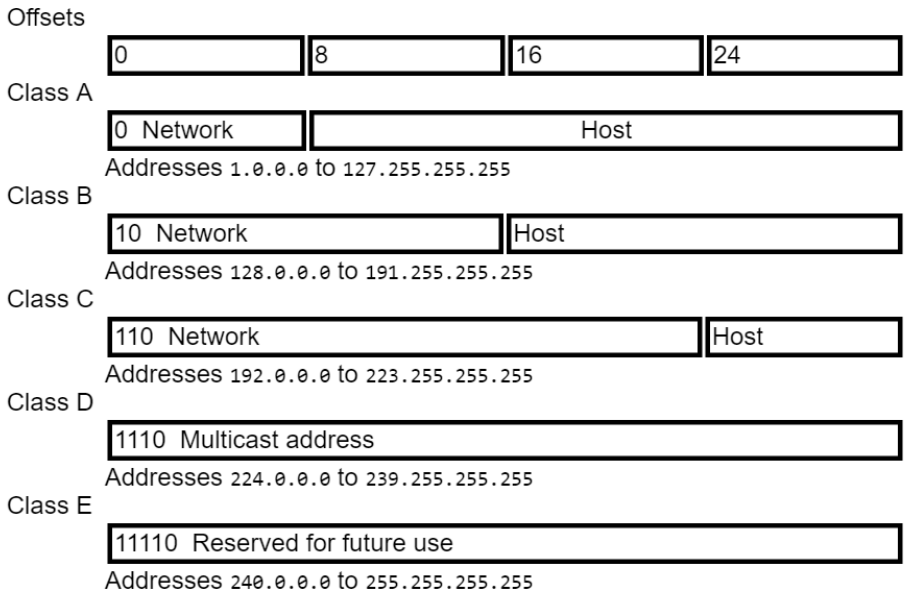
Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.
Class C gives 2097152 (2^{21}) Network addresses and 254 (2^8-2) Host addresses.
Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH
Class C addresses were assigned to small networks.

4. Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

11100000 – 11101111
224 – 239

Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.



5. Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development purposes.

Public IP Address

Public IP address is assigned to every computer that connects to the Internet where each IP is unique. In this case, there cannot exist two computers with the same public IP address all over the Internet. This addressing scheme makes it possible for the computers to "find each other" online and

exchange information. User has no control over the IP address (public) that is assigned to the computer. The public IP address is assigned to the computer by the Internet Service Provider as soon as the computer is connected to the Internet gateway.
A public IP address can be either **static** or **dynamic**. A static public IP address does not change and is used primarily for hosting web pages or services on the Internet. On the other hand, a dynamic public IP address is chosen from a pool of available addresses and changes each time one connects to the Internet.

Private IP Address

An IP address is considered private if the IP number falls within one of the IP address ranges reserved for private networks such as a Local Area Network (LAN). The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks (local networks):

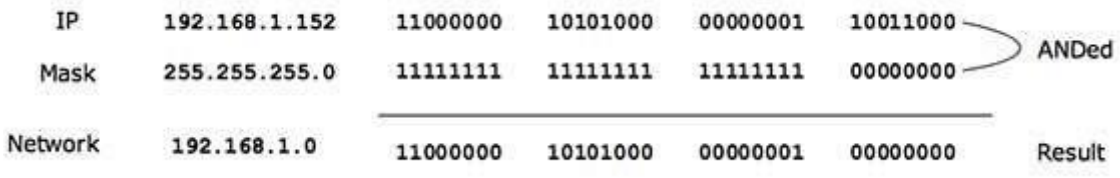
10.0.0.0 - 10.255.255.255 (Total Addresses: 16,777,216)
172.16.0.0 - 172.31.255.255 (Total Addresses: 1,048,576)
192.168.0.0 - 192.168.255.255 (Total Addresses: 65,536)

Private IP addresses are used for numbering the computers in a private network including home, school and business LANs in airports and hotels which makes it possible for the computers in the network to communicate with each other.
Say for example, if a **network X** consists of 10 computers, each of them can be given an IP starting from **192.168.1.1** to **192.168.1.10**. Unlike the public IP, the administrator of the private network is free to assign an IP address of his own choice (provided the IP number falls in the private IP address range as mentioned above).

Subnet mask

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address. For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then.

This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.



Address Class	Bits for Subnet Mask	Subnet Mask	Network Prefix
Class A	11111111 00000000 00000000 00000000	255.0.0.0	/8
Class B	11111111 11111111 00000000 00000000	255.255.0.0	/16
Class C	11111111 11111111 11111111 00000000	255.255.255.255	/32

CIDR (Classless Inter Domain Routing)

CIDR stands for *Classless Inter-Domain Routing* (occasionally, Classless Internet Domain Routing). CIDR was developed in the 1990s as a standard scheme for routing network traffic across the Internet.
Before CIDR technology was developed, Internet routers managed network traffic based on the *class* of IP addresses. In this system, the value of an IP address determines its subnetwork for the purposes of routing.
CIDR is an alternative to traditional IP subnetting that organizes IP addresses into subnetworks independent of the value of the addresses themselves. CIDR is also known as *supernetting* as it effectively allows multiple subnets to be grouped together for network routing.

CIDR reduced the problem of wasted address space by providing a new and more flexible way to specify network addresses in routers. CIDR lets one routing table entry represent an aggregation of networks that exist in the forward path that don't need to be specified on that particular gateway. This is much like how the public telephone system uses area codes to channel calls toward a certain part of the network. This aggregation of networks in a single address is sometimes referred to as a *supernet*.

CIDR specifies an IP address range using a combination of an IP address and its associated network mask. CIDR notation uses the following format –

xxx.xxx.xxx.xxx/n - Where n is the number of (leftmost) '1' bits in the mask. For example, 192.168.12.0/27

IPV4 - subnetting

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

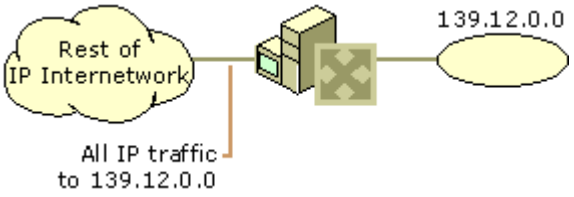


Fig (a): Before subnetting

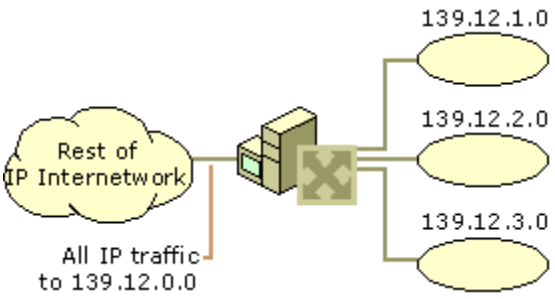


Fig (b): After subnetting

Subnetting allows us to create multiple logical networks that exist within a single Class A, B, or C network. If we do not subnet, we are only able to use one network from your Class A, B, or C network, which is unrealistic.

Class A Subnets

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.
For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (2^1=2) with (2^{23}-2) 8388606 Hosts per Subnet. The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets.

In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

Class B Subnetting

By default, using Classful Networking, 14 bits are used as Network bits providing (2^{14}) 16384 Networks and (2^{16}-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting.

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

Class C Subnetting

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

Examples

Sample Exercise 1

Now that you have an understanding of subnetting, put this knowledge to use. In this example, you are given two address / mask combinations, written with the prefix/length notation, which have

been assigned to two devices. Your task is to determine if these devices are on the same subnet or different subnets. You can use the address and mask of each device in order to determine to which subnet each address belongs.

DeviceA: 172.16.17.30/20
DeviceB: 172.16.28.15/20

Determine the Subnet for Device A:

```
172.16.17.30  -   10101100.00010000.00010001.00011110
255.255.240.0 -   11111111.11111111.11110000.00000000
                  -----------------| sub|------------
subnet =          10101100.00010000.00010000.00000000 = 172.16.16.0
```

Looking at the address bits that have a corresponding mask bit set to one, and setting all the other address bits to zero (this is equivalent to performing a logical "AND" between the mask and address), shows you to which subnet this address belongs. In this case, Device A belongs to subnet 172.16.16.0.

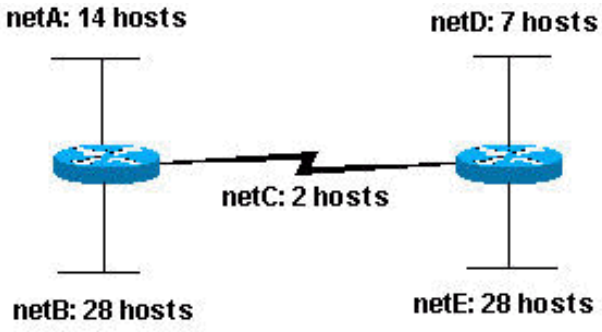
Determine the Subnet for Device B:

```
172.16.28.15  -   10101100.00010000.00011100.00001111
255.255.240.0 -   11111111.11111111.11110000.00000000
                  -----------------| sub|------------
subnet =          10101100.00010000.00010000.00000000 = 172.16.16.0
```

From these determinations, Device A and Device B have addresses that are part of the same subnet.

Sample Exercise 2

Given the Class C network of 204.15.5.0/24, subnet the network in order to create the network in figure with the host requirements shown



Looking at the network shown in Figure, we can see that we are required to create five subnets. The largest subnet must support 28 host addresses. Is this possible with a Class C network? And if so, then how?

We can start by looking at the subnet requirement. In order to create the five needed subnets we would need to use three bits from the Class C host bits. Two bits would only allow us, four subnets (2^2).

Since we need three subnet bits, that leaves us with five bits for the host portion of the address. How many hosts does this support? $2^5 = 32$ (30 usable). This meets the requirement.

Therefore we have determined that it is possible to create this network with a Class C network. An example of how we can assign the subnetworks is:

```
Net A: 204.15.5.0/27      host address range 1 to 30
Net B: 204.15.5.32/27     host address range 33 to 62
Net C: 204.15.5.64/27     host address range 65 to 94
Net D: 204.15.5.96/27     host address range 97 to 126
Net E: 204.15.5.128/27    host address range 129 to 158
```

Advantage of Subnetting

- Subnetting breaks large network in smaller networks and smaller networks are easier to manage.
- Subnetting reduces network traffic by removing collision and broadcast traffic, that overall improve performance.
- Subnetting allows us to apply network security polices at the interconnection between subnets.
- Subnetting allows us to save money by reducing requirement for IP range

IPv4 – VLSM (Variable Length Subnet Masking)

Variable Length Subnet Masking (VLSM) is a way of further subnetting a subnet. Using Variable Length Subnet Masking (VLSM) we can allocate IPv4 addresses to the subnets by the exact need. Variable Length Subnet Masking (VLSM) allows us to use more than one subnet mask within the same network address space.

Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 10 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum wastage of IP addresses.

For example, an administrator have 192.168.1.0/24 network. He has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

Step – 1

Make a list of Subnets possible.

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Step - 2

Sort the requirements of IPs in descending order (Highest to Lowest).
Sales 100
Purchase 50
Accounts 25
Management 5

Step – 3

Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

Step - 4

Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

Step – 5

Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

Step - 6

Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP addresses. So this can be assigned to Management. The last octet of the subnet mask will contain 11111000.
By using VLSM, the administrators can subnet the IP subnet in such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which were not possible if the administrator has used CIDR.

Sample Exercise 3

Address (Host or Network)	**Netmask** (i.e. 24)	**Netmask** for sub/supernet (optional)
200.100.10.0	24	27

```
Address:   200.100.10.0          11001000.01100100.00001010 .00000000
Netmask:   255.255.255.0 = 24    11111111.11111111.11111111 .00000000
Wildcard:  0.0.0.255             00000000.00000000.00000000 .11111111
=>
Network:   200.100.10.0/24       11001000.01100100.00001010 .00000000 (Class C)
Broadcast: 200.100.10.255        11001000.01100100.00001010 .11111111
HostMin:   200.100.10.1          11001000.01100100.00001010 .00000001
```

```
HostMax:   200.100.10.254        11001000.01100100.00001010 .11111110
Hosts/Net: 254
```

Subnets

```
Netmask:   255.255.255.224 = 27  11111111.11111111.11111111.111 00000
Wildcard:  0.0.0.31              00000000.00000000.00000000.000 11111

Network:   200.100.10.0/27       11001000.01100100.00001010.000 00000 (Class C)
Broadcast: 200.100.10.31         11001000.01100100.00001010.000 11111
HostMin:   200.100.10.1          11001000.01100100.00001010.000 00001
HostMax:   200.100.10.30         11001000.01100100.00001010.000 11110
Hosts/Net: 30

Network:   200.100.10.32/27      11001000.01100100.00001010.001 00000 (Class C)
Broadcast: 200.100.10.63         11001000.01100100.00001010.001 11111
HostMin:   200.100.10.33         11001000.01100100.00001010.001 00001
HostMax:   200.100.10.62         11001000.01100100.00001010.001 11110
Hosts/Net: 30

Network:   200.100.10.64/27      11001000.01100100.00001010.010 00000 (Class C)
Broadcast: 200.100.10.95         11001000.01100100.00001010.010 11111
HostMin:   200.100.10.65         11001000.01100100.00001010.010 00001
HostMax:   200.100.10.94         11001000.01100100.00001010.010 11110
Hosts/Net: 30

Network:   200.100.10.96/27      11001000.01100100.00001010.011 00000 (Class C)
Broadcast: 200.100.10.127        11001000.01100100.00001010.011 11111
HostMin:   200.100.10.97         11001000.01100100.00001010.011 00001
HostMax:   200.100.10.126        11001000.01100100.00001010.011 11110
Hosts/Net: 30

Network:   200.100.10.128/27     11001000.01100100.00001010.100 00000 (Class C)
Broadcast: 200.100.10.159        11001000.01100100.00001010.100 11111
HostMin:   200.100.10.129        11001000.01100100.00001010.100 00001
HostMax:   200.100.10.158        11001000.01100100.00001010.100 11110
Hosts/Net: 30

Network:   200.100.10.160/27     11001000.01100100.00001010.101 00000 (Class C)
Broadcast: 200.100.10.191        11001000.01100100.00001010.101 11111
HostMin:   200.100.10.161        11001000.01100100.00001010.101 00001
HostMax:   200.100.10.190        11001000.01100100.00001010.101 11110
Hosts/Net: 30

Network:   200.100.10.192/27     11001000.01100100.00001010.110 00000 (Class C)
Broadcast: 200.100.10.223        11001000.01100100.00001010.110 11111
HostMin:   200.100.10.193        11001000.01100100.00001010.110 00001
HostMax:   200.100.10.222        11001000.01100100.00001010.110 11110
Hosts/Net: 30

Network:   200.100.10.224/27     11001000.01100100.00001010.111 00000 (Class C)
Broadcast: 200.100.10.255        11001000.01100100.00001010.111 11111
HostMin:   200.100.10.225        11001000.01100100.00001010.111 00001
HostMax:   200.100.10.254        11001000.01100100.00001010.111 11110
Hosts/Net: 30



Subnets:   8
Hosts:     240
```

Sample Exercise 4

Address (Host or Network)	**Netmask** (i.e. 24)	**Netmask** for sub/supernet (optional)
192.168.16.0	18	20

```
Address:   192.168.16.0          11000000.10101000.00 010000.00000000
Netmask:   255.255.192.0 = 18    11111111.11111111.11 000000.00000000
Wildcard:  0.0.63.255            00000000.00000000.00 111111.11111111
=>
Network:   192.168.0.0/18        11000000.10101000.00 000000.00000000 (Class C)
Broadcast: 192.168.63.255        11000000.10101000.00 111111.11111111
HostMin:   192.168.0.1           11000000.10101000.00 000000.00000001
HostMax:   192.168.63.254        11000000.10101000.00 111111.11111110
Hosts/Net: 16382                 (Private Internet)
```

Subnets

```
Netmask:   255.255.240.0 = 20    11111111.11111111.1111 0000.00000000
Wildcard:  0.0.15.255            00000000.00000000.0000 1111.11111111

Network:   192.168.0.0/20        11000000.10101000.0000 0000.00000000 (Class C)
Broadcast: 192.168.15.255        11000000.10101000.0000 1111.11111111
HostMin:   192.168.0.1           11000000.10101000.0000 0000.00000001
HostMax:   192.168.15.254        11000000.10101000.0000 1111.11111110
Hosts/Net: 4094                  (Private Internet)

Network:   192.168.16.0/20       11000000.10101000.0001 0000.00000000 (Class C)
Broadcast: 192.168.31.255        11000000.10101000.0001 1111.11111111
HostMin:   192.168.16.1          11000000.10101000.0001 0000.00000001
HostMax:   192.168.31.254        11000000.10101000.0001 1111.11111110
Hosts/Net: 4094                  (Private Internet)

Network:   192.168.32.0/20       11000000.10101000.0010 0000.00000000 (Class C)
Broadcast: 192.168.47.255        11000000.10101000.0010 1111.11111111
HostMin:   192.168.32.1          11000000.10101000.0010 0000.00000001
HostMax:   192.168.47.254        11000000.10101000.0010 1111.11111110
Hosts/Net: 4094                  (Private Internet)

Network:   192.168.48.0/20       11000000.10101000.0011 0000.00000000 (Class C)
Broadcast: 192.168.63.255        11000000.10101000.0011 1111.11111111
HostMin:   192.168.48.1          11000000.10101000.0011 0000.00000001
HostMax:   192.168.63.254        11000000.10101000.0011 1111.11111110
Hosts/Net: 4094                  (Private Internet)


Subnets:   4
Hosts:     16376
```

Sample Exercise 5

Calculate the number of sub network and total no of host in a sub network for IP address 192.18.18.0/27. Also calculate the subnet mask, network address, Broadcast addresses and usable host range in each sub network.

Solution

The given IP- address is: 192.18.18.0/27
Therefore the subnet mask is: 11111111.11111111.11111111.11100000
That is: 255.255.255.224

Number of Host bits used in Network (N) = 3
Remaining Host bits (H) = 5

Total Subnets = $2^N = 2^3 = 8$
Total Hosts = $2^H = 2^5 = 32$
Valid Hosts per subnet = 32-2 = 30
Total no. of valid host over all subnet = 30 x 8 = 240
Block Size = 256 – Subnet mask = 256 – 224 = 32

The Subnet-ID, Host- IPs and Broadcast addresses of each subnet is calculated below.

S.N.	Subnet-ID	Host IP Range	Broadcast Address
1	192.18.18.0	192.18.18.1 →192.18.18.30	192.18.18.31
2	192.18.18.32	192.18.18.33 →192.18.18.62	192.18.18.63
3	192.18.18.64	192.18.18.63 →192.18.18.94	192.18.18.95
4	192.18.18.96	192.18.18.95 →192.18.18.126	192.18.18.127
5	192.18.18.128	192.18.18.129 →192.18.18.158	192.18.18.159
6	192.18.18.160	192.18.18.161 →192.18.18.190	192.18.18.191
7	192.18.18.192	192.18.18.193 →192.18.18.222	192.18.18.223
8	192.18.18.224	192.18.18.225 →192.18.18.254	192.18.18.255

Key terms to remember

- ✓ A subnet is a smaller portion of large network treated as its own separate network. To create subnet we borrow bits from host portion and assign them as network bits. This mean more networks, fewer hosts.
- ✓ If the network bits on two addresses do not match, then the two packets are intended for two separate networks.
- ✓ On a 32 bits IP address at least eight bits must belong to the network portion and at least 2 bits must belong to the host portion.
- ✓ Each IP address has a predefined IP class and that cannot be changed.
- ✓ Each class has a predefined default subnet mask that tell us the octets, which are already part of the network portion, as well as how many bits we have available to work with.
- ✓ Whatever network class is it, we cannot change those bits that are already assigned.
- ✓ We cannot assign the network ID and the broadcast address to a host.
- ✓ Regardless how many bits are left in the host field, network ID and the broadcast address must be reserved.
- ✓ Subnet bits start at the left and go to the right, without skipping bits.

Static and Dynamic IP Addresses

IP addresses may be either statically allocated or dynamically allocated by a service provider. A dynamic IP address has the following characteristics:

- ✓ A single IP address is allocated when the user connects to the internet.
- ✓ The service provider will normally change the IP address periodically - between every 12 and 24 hours is typical, significantly longer periods are increasingly common.

- ✓ Dynamic IP addresses can be used for outgoing (client-server) activities such as Web browsing, collecting email and similar activities.
- ✓ Dynamic IP addresses cannot be used (well there are 'kludges' that allow this) to host Web sites and email services that require a fixed IP defined in a DNS.

Static (Fixed) IP address(es) have the following characteristics:

- ✓ One or more fixed IP address(es) are permanently assigned to a user (and will normally incur a cost).
- ✓ Static IP addresses do not change (unless you change your service provider).
- ✓ Static IP addresses can be used for outgoing (client-server) activities such as Web browsing, collecting email and similar activities.
- ✓ Static IP addresses can be used to host Web sites and email services that require a fixed IP defined in a DNS.
- ✓ A limited number of static addresses can be used in conjunction with NAT to map many PRIVATE to PUBLIC addresses.

Internet Protocol Version 6 (IPv6)

IPv6 (Internet Protocol version 6) is a set of specifications from the Internet Engineering Task Force (IETF) that's essentially an upgrade of IP version 4 (IPv4). The basics of IPv6 are similar to those of IPv4 -- devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations.

The most obvious improvement in IPv6 over IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses. IPv6 also supports auto-configuration to help correct most of the shortcomings in version 4, and it has integrated security and mobility features.

IPv6 features include:

- ✓ Supports source and destination addresses that are 128 bits (16 bytes) long.
- ✓ No more NAT (Network Address Translation)
- ✓ Auto-configuration
- ✓ No more private address collisions
- ✓ Better multicast routing
- ✓ Simpler header format, Simplified, more efficient routing
- ✓ Built-in authentication and privacy support
- ✓ Flexible options and extensions
- ✓ Requires IPSec support.
- ✓ Uses Flow Label field to identify packet flow for QoS handling by router.
- ✓ Allows the host to send fragments packets but not routers.
- ✓ Doesn't include a checksum in the header.
- ✓ Uses a link-local scope all-nodes multicast address.
- ✓ Does not require manual configuration or DHCP.
- ✓ Uses host address (AAAA) resource records in DNS to map host names to IPv6 addresses.
- ✓ Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.

- ✓ Supports a 1280-byte packet size (without fragmentation).
- ✓ Uses Multicast Listener Discovery (MLD) messages to manage membership in local subnet groups.
- ✓ Uses ICMPv6 Router Solicitation and Router Advertisement messages to determine the IP address of the best default gateway.

IPv6 Address Structure

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbol.

For example, the below is 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001 0000000000000000 0011001000110100 1101111111100001
0000000001100011 0000000000000000 0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ':' symbol:

2001:0000:3238:DFE1:0063:0000:0000:FEFB

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. These rules are:

Rule: 1 Discard leading Zero(es):

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):
2001:0000:3238:DFE1:63:0000:0000:FEFB

Rule: 2 If two of more blocks contains consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

2001:0000:3238:DFE1:63::FEFB

Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address they can be shrink down to single zero, such as (2nd block):

2001:0:3238:DFE1:63::FEFB

Transition from IPv4 to IPv6

An **IPv6 transition mechanism** is a technology that facilitates the transitioning of the Internet from the Internet Protocol version 4 (IPv4) infrastructure in use since 1981 to the successor addressing and routing system of Internet Protocol Version 6 (IPv6). As IPv4 and IPv6 networks are not directly interoperable, transition technologies are designed to permit hosts on either network type to communicate with any other host.

Special methods are defined to handle interoperability, including:

- ➢ **"Dual Stack" Devices:** Routers and some other devices may be programmed with both IPv4 and IPv6 implementations to allow them to communicate with both types of hosts.

- **IPv4/IPv6 Translation:** "Dual stack" devices may be designed to accept requests from IPv6 hosts, convert them to IPv4 datagrams, send the datagrams to the IPv4 destination and then process the return datagrams similarly.
- **IPv4 Tunneling of IPv6:** IPv6 devices that don't have a path between them consisting entirely of IPv6-capable routers may be able to communicate by encapsulating IPv6 datagrams within IPv4. In essence, they would be using IPv6 on top of IPv4; two network layers. The encapsulated IPv4 datagrams would travel across conventional IPv4 routers.

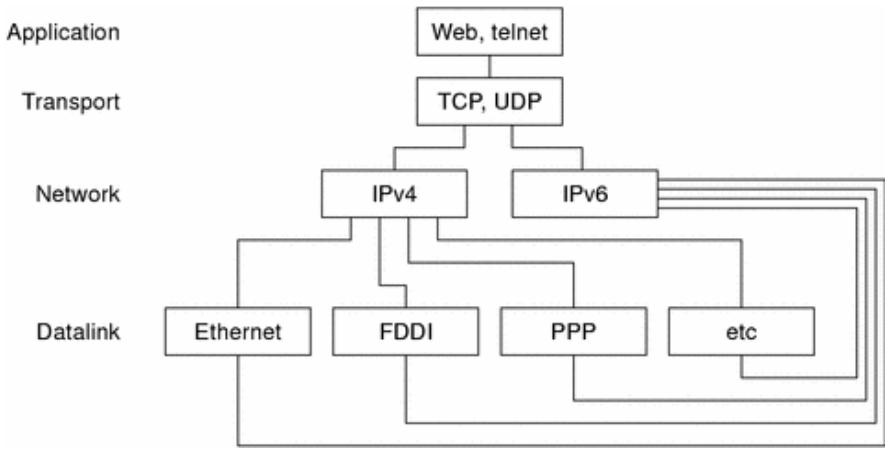
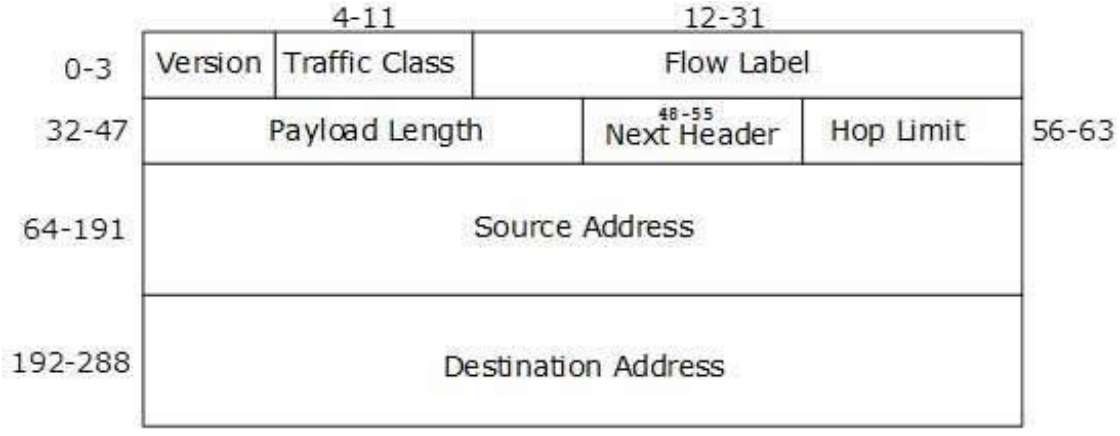


Figure 4–1 Dual-Stack Protocols

In the dual-stack method, subsets of both hosts and routers are upgraded to support IPv6, in addition to IPv4. The dual-stack approach ensures that the upgraded nodes can always interoperate with IPv4-only nodes by using IPv4.

IPv6 Header

The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.



[Figure: IPv6 Fixed Header]

IPv6 fixed header is 40 bytes long and contains the following information.

S.N.	Field & Description
1	**Version (4-bits):** It represents the version of Internet Protocol, i.e. 0110.
2	Traffic Class (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	**Flow Label (20-bits):** This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4	**Payload Length (16-bits):** This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5	**Next Header (8-bits):** This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
6	**Hop Limit (8-bits):** This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7	**Source Address (128-bits)**: This field indicates the address of originator of the packet.
8	**Destination Address (128-bits):** This field provides the address of intended recipient of the packet.

Special IPV6 Addresses

IPv6 Address	Meaning
::/128	Unspecified Address
::/0	Default Route
::1/128	Loopback Address

- As shown in the table above 0:0:0:0:0:0:0:0/128 address does not specify to anything and is said to be an unspecified address. After simplifying, all 0s are compacted to ::/128.
- In IPv4, address 0.0.0.0 with netmask 0.0.0.0 represents default route. The same concept is also applie to IPv6, address 0:0:0:0:0:0:0:0 with netmask all 0s represents default route. After applying IPv6 simplying rule this address is compressed to ::/0.
- Loopback addresses in IPv4 are represented by 127.0.0.1 to 127.255.255.255 series. But in IPv6, only 0:0:0:0:0:0:0:1/128 address represents Loopback address. After simplying loopback address, it can be represented as ::1/128.

IPv6 Addressing Modes

In computer networking, addressing mode refers to the mechanism how we address a host on the network. IPv6 offers several types of modes by which a single host can be addressed, more than one host can be addressed at once or the host at closest distance can be addressed. IPv6 addresses are broadly classified into three categories:

1. **Unicast addresses:** A Unicast address acts as an identifier for a single interface. An IPv6 packet sent to a Unicast address is delivered to the interface identified by that address.
2. **Multicast addresses:** A Multicast address acts as an identifier for a group/set of interfaces that may belong to the different nodes. An IPv6 packet delivered to a Multicast address is delivered to the multiple interfaces.
3. **Anycast addresses:** Anycast addresses act as identifiers for a set of interfaces that may belong to the different nodes. An IPv6 packet destined for an Anycast address is delivered to one of the interfaces identified by the address.

IPv6 Extension Headers

In IPv6, the Fixed Header contains only information which is necessary and avoiding information which is either not required or is rarely used. All such information is put between the Fixed Header and Upper layer header in the form of Extension Headers. Each Extension Header is identified by a distinct value.
When Extension Headers are used, IPv6 Fixed Header's Next Header field points to the first Extension Header. If there is one more Extension Header, then first Extension Header's 'Next-Header' field point to the second one, and so on. The last Extension Header's 'Next-Header' field point to Upper Layer Header. Thus all headers from one point to the next one in a linked list manner.
If the Next Header field contains value 59, it indicates that there's no header after this header, not even Upper Layer Header.

The following Extension Headers must be supported as per RFC 2460:

Extension Header	Next Header Value	Description
Hop-by-Hop Options header	0	read by all devices in transit network
Routing header	43	contains methods to support making routing decision
Fragment header	44	contains parameters of datagram fragmentation
Destination Options header	60	read by destination devices
Authentication header	51	information regarding authenticity
Encapsulating Security Payload header	50	encryption information

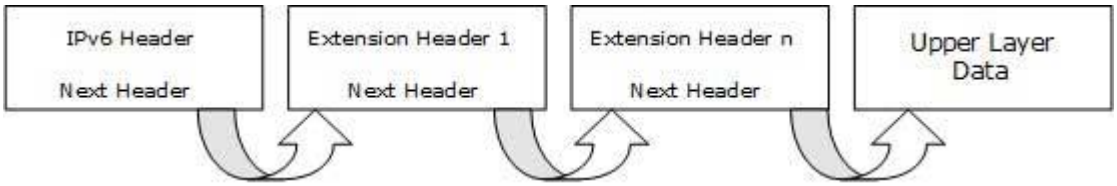
The sequence of Extension Headers should be:

IPv6 header
Hop-by-Hop Options header
Destination Options header[1]
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header[2]
Upper-layer header

These headers:

1. Should be processed by First and subsequent destinations.
2. Should be processed by Final Destination.

Extension Headers are arranged one after another in a Linked list manner, as depicted in the diagram below:



[*Figure: Extension Headers Connected Format*]

Why not IPv5?

Till date, Internet Protocol has been recognized has IPv4 only. Versions 0 to 3 were used while the protocol was itself under development and experimental process. So, we can assume lots of background activities remain active before putting a protocol into production.
Similarly, protocol version 5 was used while experimenting with stream protocol for internet. It is known to us as Internet Stream Protocol which used Internet Protocol number 5 to encapsulate its datagram. Though it was never brought into public use, but it was already used.
Here is a table of IP version and their use:

Decimal	Keyword	Version
0-1		Reserved
2-3		Unassigned
4	IP	Internet Protocol
5	ST	ST Datagram mode
6	IPv6	Internet Protocol version 6
7	TP/IX	TP/IX: The Next Internet
8	PIP	The P Internet Protocol
9	TUBA	TUBA
10-14		Unassigned
15		Reserved

Differences between IPv4 and IPv6

The following table lists the important differences between IPv4 and IPv6.

IPv4	IPv6
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals.
IPsec support is only optional.	Inbuilt IPsec support.
Fragmentation is done by sender and forwarding routers.	Fragmentation is done only by sender.

No packet flow identification.	Packet flow identification is available within the IPv6 header using the Flow Label field.
Checksum field is available in IPv4 header	No checksum field in IPv6 header.
Options fields are available in IPv4 header.	No option fields, but IPv6 Extension headers are available.
Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.	Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).
Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
Broadcast messages are available.	Broadcast messages are not available.
Manual configuration (Static) of IPv4 addresses or DHCP (Dynamic configuration) is required to configure IPv4 addresses.	Auto-configuration of addresses is available.
IPv4 is subdivided into classes <A-E>.	IPv6 is classless. IPv6 uses a prefix and an Identifier ID known as IPv4 network
IPv4 address uses a subnet mask.	IPv6 uses prefix length.

Internet Multicasting

IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. It is often employed for streaming media applications on the Internet and private networks. The method is the IP-specific version of the general concept of multicast networking. It uses especially reserved multicast address blocks in IPv4 and IPv6. Every IP datagram whose destination address starts with "1110" is an IP Multicast datagram.

Multicasting is similar to broadcasting, but only transmits information to specific users. The simple way to send data to multiple users simultaneously is to transmit individual copies of the data to each user. However, this is highly inefficient, since multiple copies of the same data are sent from the source through one or more networks. Multicasting enables a single transmission to be split up among multiple users, significantly reducing the required bandwidth.

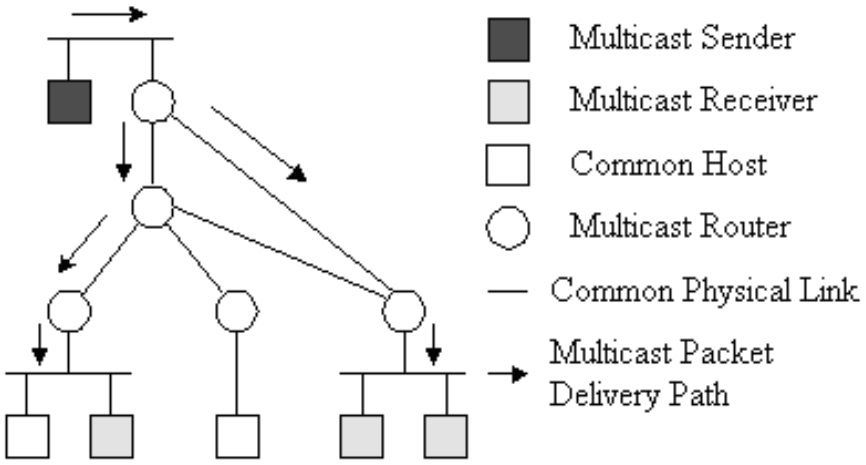


Fig: Illustration of Multicast Delivery

Multicasting has several different applications. It is commonly used for streaming media over the Internet, such as live TV and Internet radio. It also supports video conferencing and webcasts. Multicasting can also be used to send other types of data over the Internet, such as news, stock quotes, and even digital copies of software. Whatever the applications, multicasting helps to reduce Internet bandwidth usage by providing an efficient way of sending data to multiple users.

IP multicasting works by combining two other protocols with the Internet protocol. One is the Internet Group Management Protocol (IGMP), which allows users or client systems use to request access to a stream. The other is Protocol Independent Multicast (PIM), which is used by network routers to create multicast trees. When a router receives a request to join a stream via IGMP, it uses PIM to route the data stream to the appropriate system.

Mobile IP

Mobile IP (or **MIP**) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. Mobile IP communication protocol refers to the forwarding of Internet traffic with a fixed IP address even outside the home network. It allows users having wireless or mobile devices to use the Internet remotely.

In IP networks, routing is based on stationary IP addresses, similar to how a postal letter is delivered to the fixed address on the envelope. A device on a network is reachable through normal IP routing by the IP address it is assigned on the network. The problem occurs when a device roams away from its home network and is no longer reachable using normal IP routing. This results in the active sessions of the device being terminated. Mobile IP was created to enable users to keep the same IP address while traveling to a different network (which may even be on a different wireless operator), thus ensuring that a roaming individual could continue communication without sessions or connections being dropped.

The following figure illustrates the general Mobile IP topology.

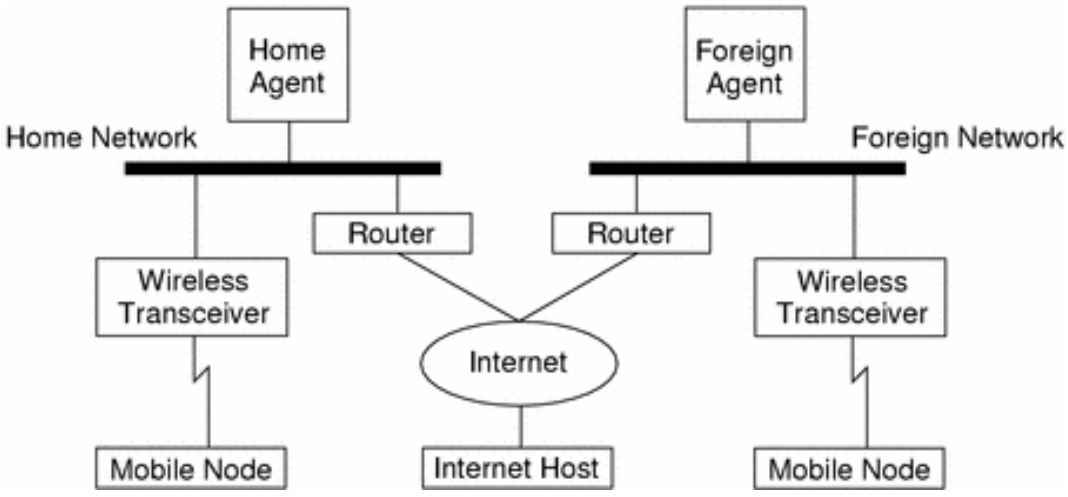


Figure: Mobile IP Topology

Mobile IP introduces the following new functional entities (components):

1. **Mobile Node (MN)**–Host or router that changes its point of attachment from one network to another.
2. **Home Agent (HA)**–Router on a mobile node's home network that intercepts datagrams destined for the mobile node, and delivers them through the care-of address. The home agent also maintains current location information for the mobile node.
3. **Foreign Agent (FA)**–Router on a mobile node's visited network that provides routing services to the mobile node while the mobile node is registered.

Following scenario shows how a datagram moves from one point to another within the Mobile IP framework.

1. The Internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process).
2. If the mobile node is on its home network, the datagram is delivered through the normal IP process to the mobile node. Otherwise, the home agent picks up the datagram.
3. If the mobile node is on a foreign network, the home agent forwards the datagram to the foreign agent.
4. The foreign agent delivers the datagram to the mobile node. Datagrams from the mobile node to the Internet host are sent using normal IP routing procedures. If the mobile node

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 subnets may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnets 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. 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 Design Issues

1. Store-and-Forward Packet Switching

- The major components of the system are the carrier's equipment (routers connected by transmission lines), shown inside the shaded oval, and the customers' equipment, shown outside the oval.

- Host H1 is directly connected to one of the carrier's routers, A, by a leased line. In contrast, H2 is on a LAN with a router, F, owned and operated by the customer. This router also has a leased line to the carrier's equipment.
- We have shown F as being outside the oval because it does not belong to the carrier, but in terms of construction, software, and protocols, it is probably no different from the carrier's routers.

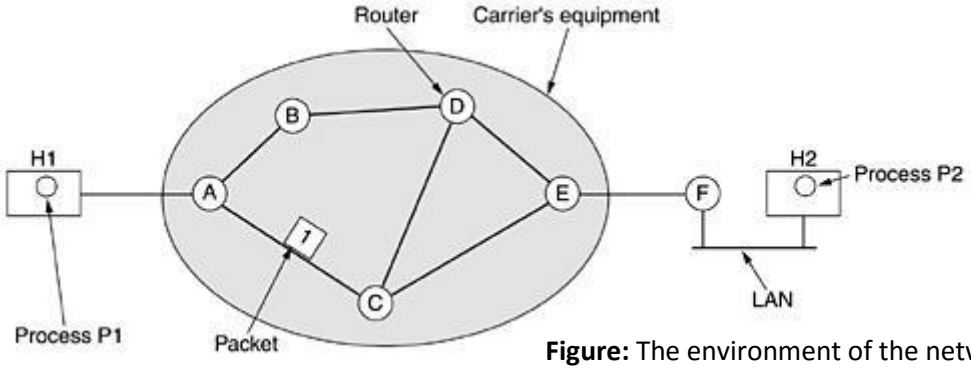


Figure: The environment of the network layer

- This equipment is used as follows. A host with a packet to send transmits it to the nearest router, either on its own LAN or over a point-to-point link to the carrier. The packet is stored there until it has fully arrived so the checksum can be verified.
- Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store-and-forward packet switching.

2. Services Provided to the Transport Layer

The network layer provides services to the transport layer at the network layer/transport layer interface. An important question is what kind of services the network layer provides to the transport layer. The network layer services have been designed with the following goals in mind.

1. The services should be independent of the router technology.
2. The transport layer should be shielded from the number, type, and topology of the routers present.
3. The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

Given these goals, the designers of the network layer have a lot of freedom in writing detailed specifications of the services to be offered to the transport layer. This freedom often degenerates into a raging battle between two warring factions. The other camp argues that the subnet should provide a reliable, connection-oriented service. They claim that 100 years of successful experience with the worldwide telephone system is an excellent guide. In this view, quality of service is the dominant factor, and without connections in the subnet, quality of service is very difficult to achieve, especially for real-time traffic such as voice and video.

These two camps are best exemplified by the Internet and ATM. The Internet offers connectionless network-layer service; ATM networks offer connection-oriented network-layer service. However, it is interesting to note that as quality-of-service guarantees are becoming more and more important, the Internet is evolving.

3. Implementation of Connectionless Service

Two different organizations are possible, depending on the type of service offered. If connectionless service is offered, packets are injected into the subnet individually and routed independently of each other. No advance setup is needed.

In this context, the packets are frequently called **datagrams** (in analogy with telegrams) and the subnet is called a datagram subnet. If connection-oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent. This connection is called a VC (virtual circuit), in analogy with the physical circuits set up by the telephone system, and the subnet is called a virtual-circuit subnet.

Let us now see how a datagram subnet works. Suppose that the process P1 in Figure has a long message for P2. It hands the message to the transport layer with instructions to deliver it to process P2 on host H2.

The transport layer code runs on H1, typically within the operating system. It prepends a transport header to the front of the message and hands the result to the network layer, probably just another procedure within the operating system.

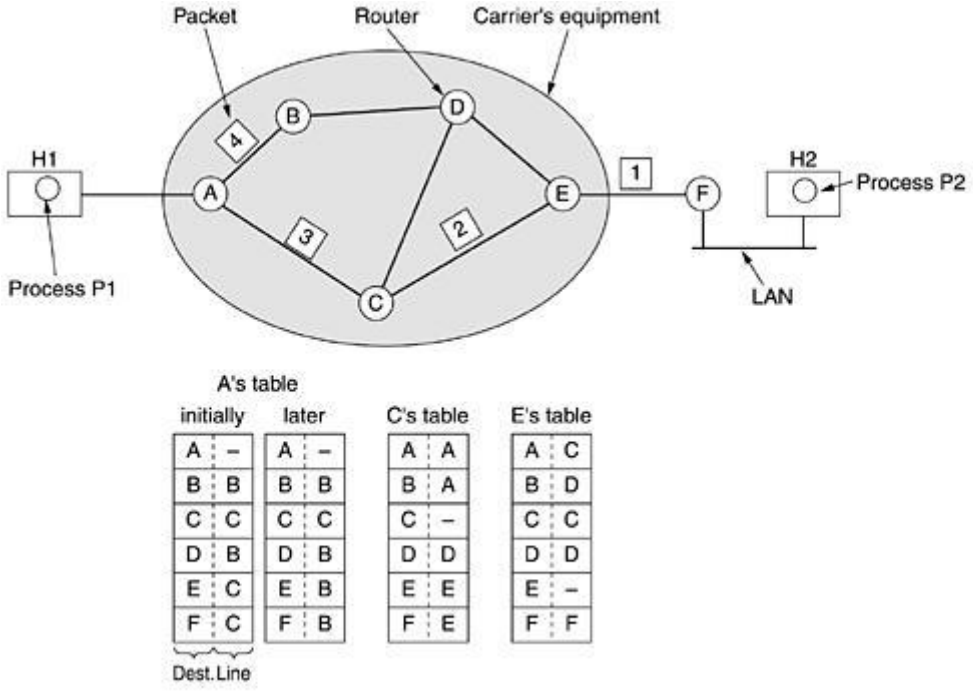


Figure: Routing within a datagram subnet

- Let us now see how a datagram subnet works. Suppose that the process P1 in Fig. 3-2 has a long message for P2. It hands the message to the transport layer with instructions to deliver it to process P2 on host H2.

- The transport layer code runs on H1, typically within the operating system. It prepends a transport header to the front of the message and hands the result to the network layer, probably just another procedure within the operating system.

- Let us assume that the message is four times longer than the maximum packet size, so the network layer has to break it into four packets, 1, 2, 3, and 4 and sends each of them in turn to router A using some point-to-point protocol, for example, PPP.
- At this point the carrier takes over. Every router has an internal table telling it where to send packets for each possible destination. Each table entry is a pair consisting of a destination and the outgoing line to use for that destination.
- Only directly-connected lines can be used. For example, in Fig. 5-2, A has only two outgoing lines—to B and C—so every incoming packet must be sent to one of these routers, even if the ultimate destination is some other router. A's initial routing table is shown in the figure under the label ''initially.''
- However, something different happened to packet 4. When it got to A it was sent to router B, even though it is also destined for F. For some reason, A decided to send packet 4 via a different route than that of the first three.
- Perhaps it learned of a traffic jam somewhere along the ACE path and updated its routing table, as shown under the label ''later.'' The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.

4. Implementation of connection oriented service

For connection-oriented service, we need a virtual-circuit subnet. The idea behind virtual circuits is to avoid having to choose a new route for every packet sent.
Instead, when a connection is established, a route from the source machine to the destination machine is chosen as part of the connection setup and stored in tables inside the routers. That route is used for all traffic flowing over the connection, exactly the same way that the telephone system works.
When the connection is released, the virtual circuit is also terminated. With connection-oriented service, each packet carries an identifier telling which virtual circuit it belongs to.
As an example, consider the situation of Figure. Here, host H1 has established connection 1 with host H2.

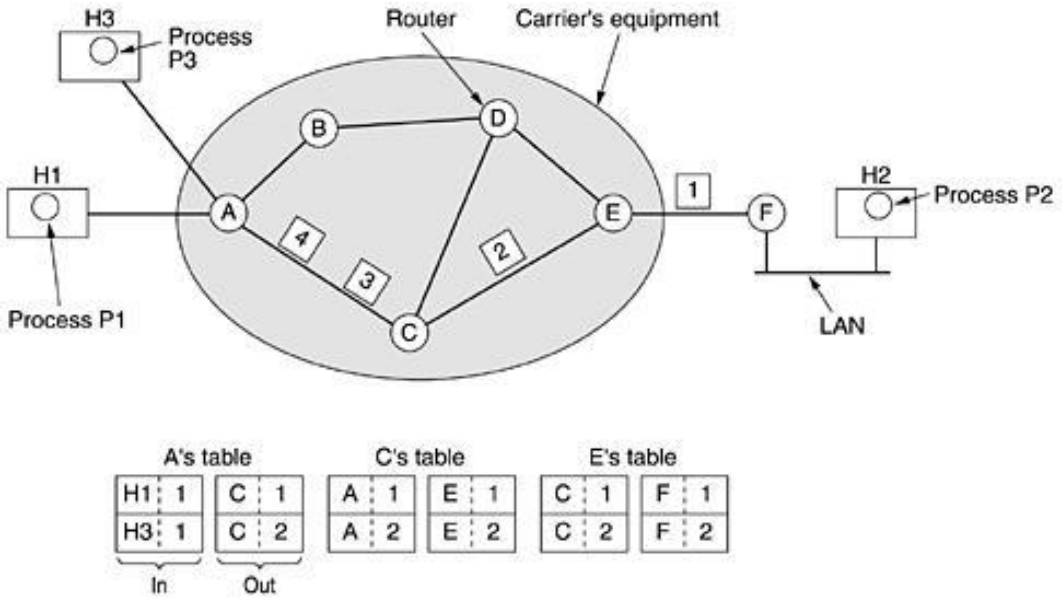


Figure: Routing within a virtual circuit subnet

It is remembered as the first entry in each of the routing tables. The first line of A's table says that if a packet bearing connection identifier 1 comes in from H1, it is to be sent to router C and given connection identifier 1. Similarly, the first entry at C routes the packet to E, also with connection identifier 1.

Now let us consider what happens if H3 also wants to establish a connection to H2. It chooses connection identifier 1 and tells the subnet to establish the virtual circuit. This leads to the second row in the tables.

Note that we have a conflict here because although A can easily distinguish connection 1 packets from H1 from connection 1 packets from H3, C cannot do this. For this reason, A assigns a different connection identifier to the outgoing traffic for the second connection.

Avoiding conflicts of this kind is why routers need the ability to replace connection identifiers in outgoing packets. In some contexts, this is called label switching.

5. Comparison of Virtual-Circuit and Datagram subnets

Inside the subnet, several trade-offs exist between virtual circuits and datagrams. One trade-off is between router memory space and bandwidth. Virtual circuits allow packets to contain circuit numbers instead of full destination addresses.

If the packets tend to be fairly short, a full destination address in every packet may represent a significant amount of overhead and hence, wasted bandwidth. The price paid for using virtual circuits internally is the table space within the routers.

Depending upon the relative cost of communication circuits versus router memory, one or the other may be cheaper. Another trade-off is setup time versus address parsing time. Using virtual circuits requires a setup phase, which takes time and consumes resources.

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

On the other hand, permanent virtual circuits, which are set up manually and last for months or years, may be useful here. Virtual circuits also have a vulnerability problem. If a router crashes and loses its memory, even if it comes back up a second later, all the virtual circuits passing through it will have to be aborted. In contrast, if a datagram router goes down, only those users

Whose packets were queued in the router at the time will suffer, and maybe not even all those, depending upon whether they have already been acknowledged.
The loss of a communication line is fatal to virtual circuits using it but can be easily compensated for if datagrams are used. Datagrams also allow the routers to balance the traffic throughout the subnet, since routes can be changed partway through a long sequence of packet transmissions.

Routing

Routing is the process of selecting best paths in a network. A simple definition of routing is "learning how to get from here to there". The main function of the network layer is routing packets from source to machine to the destination machine.
The algorithms that choose the routes and the data structures that they use are a major area of network layer design. The **routing algorithm** is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on. If the subnet uses datagrams internally, this decision must be made a new for every arriving data packet since the best route may have changed since last time. If the subnet uses virtual circuits internally, the routing decision is made only when a new virtual circuit is being set up. Thereafter, data packets just follow the previously established route. The latter case is sometimes called **session routing** because a route remains in force for an entire user session.
One can think of a router as having two processes inside it. One of the handles each packet as it arrives, looking up the outgoing line to use for it in the routing tables. This process is **forwarding.** The other process is responsible for filling in and updating the routing tables. That is where the routing algorithm comes into play.

Regardless of whether routes are chosen independently for each packet or only when new connections are established certain properties are desirable in a routing algorithm: **correctness, simplicity, robustness, stability, fairness and optimality.**

Correctness and simplicity hardly require comment but the need for robustness may be less obvious at first. Once a major network comes on the air, it may be expected to run continuously for years without system wide failures. Stability is also an important goal for the routing algorithm. There exist routing algorithms that never converge to equilibrium, no matter how long they run. A stable algorithm reaches equilibrium and stays there.
Routing algorithm can be grouped into two major classes: Non-adaptive and adaptive.

Non-adaptive algorithms do not base their routing decision on measurements or estimates of the current traffic and topology.
Adaptive algorithms, in contrast, change their routing decisions to reflect changes in the topology, and usually the traffic as well.

Static Routing

A static routing table is created, maintained, and updated by a network administrator, manually. A static route to every network must be configured on every router for full connectivity. This provides a granular level of control over routing and is completely manageable on smaller networks.
However, static routing is not fault-tolerant, as any change to the routing infrastructure (such as a link going down, or a new network added) requires manual intervention. Routers operating in a purely static environment cannot seamlessly choose a better route if a link becomes unavailable, because no information is intelligently shared between routers.

Advantages of Static Routing

- Minimal CPU/Memory overhead
- No bandwidth overhead (updates are not shared between routers)
- Granular control on how traffic is routed

Disadvantages of Static Routing

- Infrastructure changes must be manually adjusted
- No “dynamic” fault tolerance if a link goes down
- Impractical on large network

Dynamic Routing

Dynamic routing protocols are the applications which discover network destinations dynamically. Routers will communicate the adjacent routers which informs the network to which each router is connected. Dynamic routing protocols are supported by software applications running on the routing device (the router) which dynamically learn network destinations and how to get to them and also advertise those destinations to other routers. This advertisement function allows all the routers to learn about all the destination networks that exist and how to use those networks.
Router using dynamic routing will 'learn' the routes to all networks that are directly connected to the device. Next, the router will learn routes from other routers that run the same routing protocol.

Advantages of Dynamic Routing

- Simpler to configure on larger networks
- Will dynamically choose a different (or better) route if a link goes down
- Ability to load balance between multiple links

Disadvantages of Dynamic Routing

- Updates are shared between routers, thus consuming bandwidth
- Routing protocols put additional load on router CPU/RAM
- The choice of the “best route” is in the hands of the routing protocol, and not the network administrator

Routing Algorithm

The main function of the network layer is routing packets from the source machine to the destination machine. In most subnets, packets will require multiple hops to make the journey. The only notable exception is for broadcast networks, but even here routing is an issue if the source and destination are not on the same network.

The algorithms that choose the routes and the data structures that they use are a major area of network layer design. The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.
If the subnet uses datagrams internally, this decision must be made a new for every arriving data packet since the best route may have changed since last time. If the subnet uses virtual circuits internally, routing decisions are made only when a new virtual circuit is being set up.

Shortest Path Routing Algorithm

Links between routers have a cost associated with them. In general it could be a function of distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, router processing speed, etc.
The shortest path algorithm just finds the least expensive path through the network, based on the cost function.

Dijkstra's Shortest Path Algorithm

Dijkstra's algorithm solves the simple source shortest paths problem on a weighted, directed graph.
G = (V, E) for the case in which all weights are non-negative.
The algorithm repeatedly selects the vertex v belong s to v-s with the minimum shortest path estimate add

ALGORITHM

- Take a weighted, directed graph and take number of vertices.
- Next take the weights between the states.
- Start with the source vertex and identify the shortest path.
- Repeat the above process for all the vertices repetitively until the destination is reached.
- Display the shortest path from the source to destination.

Dijkstra's shortest path routing algorithm is presented below in pseudocode:

Given a network $G = (N, E)$, with a positive cost D_{ij} for all edges $(i, j \in N)$, start node S and a set P of permanently labeled nodes, the shortest path from start node S to every other node j is found as follows:

Initially $P = \{S\}$, $D_S = 0$, and $D_j = d_{Sj}$ for $j \overset{j \neq S}{\in} N$.

Step 1: (Find the closest node.) Find $i \notin P$ such that

$$D_i = \min_{j \notin P} D_j$$

Set $P = P \cup \{i\}$. If P contains all nodes then stop; the algorithm is complete.

Step 2: (Updating of labels.) For all $j \notin P$ set

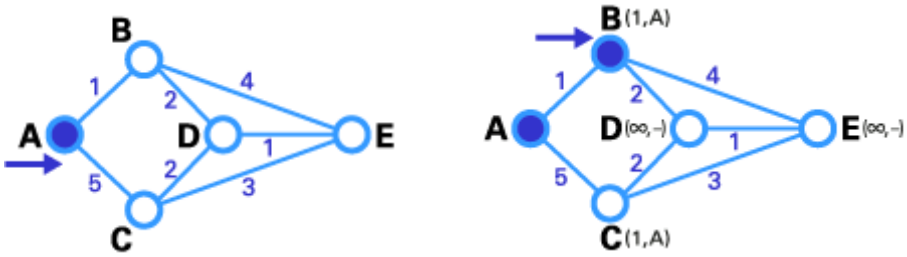
$$D_j = \min[D_j, D_i + d_{ij}]$$

Example

Here we want to find the best route between A and E (see below). You can see that there are six possible routes between A and E (ABE, ACE, ABDE, ACDE, ABDCE, ACDBE), and it's obvious that ABDE is the best route because its weight is the lowest. But life is not always so easy, and there are some complicated cases in which we have to use algorithms to find the best route.

Step 1: As you see in the first image, the source node (A) has been chosen as T-node, and so its label is permanent (we show permanent nodes with filled circles and T-nodes with the --> symbol).

Step 2: In the next step, you see that the status record set of tentative nodes directly linked to T-node (B, C) has been changed. Also, since B has less weight, it has been chosen as T-node and its label has changed to permanent (see below second figure).



Step 3: In step 3, like in step 2, the status record set of tentative nodes that have a direct link to T-node (D, E), has been changed. Also, since D has less weight, it has been chosen as T-node and its label has changed to permanent.

Step 4: In step 4, we don't have any tentative nodes, so we just identify the next T-node. Since E has the least weight, it has been chosen as T-node.

Lastly, E is the destination, so we stop her

Distance Vector Routing

- Modern computer networks generally use dynamic routing algorithms rather than the static ones described above because static algorithms do not take the current network load into account.
- Two dynamic algorithms in particular, distance vector routing and link state routing, are the most popular. In this section we will look at the former algorithm. In the following section we will study the latter algorithm.
- Distance vector routing algorithms operate by having each router maintain a table (i.e, a vector) giving the best known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbors.
- The distance vector routing algorithm is sometimes called by other names, most commonly the distributed Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm, after the researchers who developed it.
- It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP. In distance vector routing, each router maintains a routing table indexed by, and containing one entry for, each router in the subnet.
- This entry contains two parts: the preferred outgoing line to use for that destination and an estimate of the time or distance to that destination. The metric used might be number of hops, time delay in milliseconds, total number of packets queued along the path, or something similar.
- This updating process is illustrated in Fig. Part (a) shows a subnet. The first four columns of part (b) show the delay vectors received from the neighbors of router J. A claims to have a 12-msec

delay to B, a 25-msec delay to C, a 40-msec delay to D, etc. Suppose that J has measured or estimated its delay to its neighbors, A, I, H, and K as 8, 10, 12, and 6 msec, respectively.

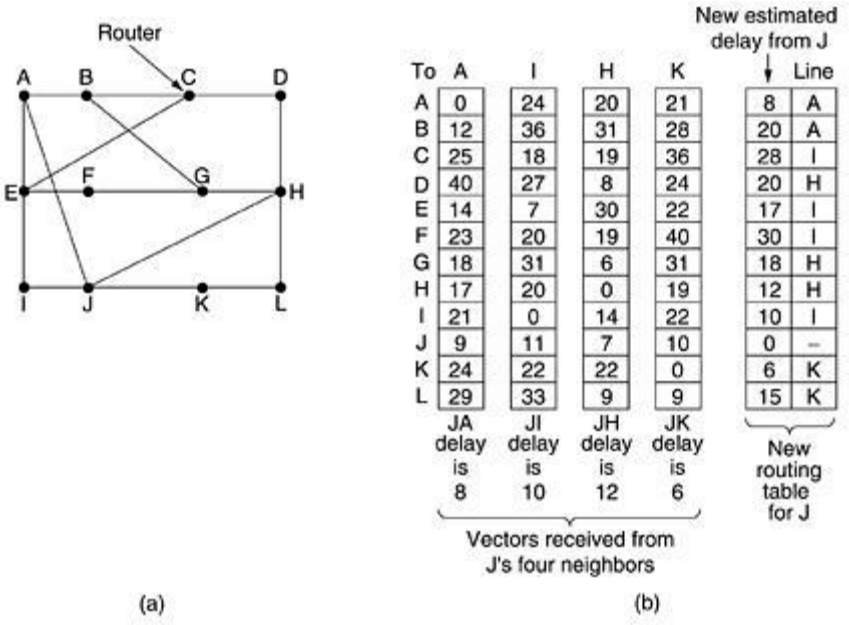


Figure: (a) A subnet. (b) Input from A, I, H, K, and the new routing table for J

- Consider how J computes its new route to router G. It knows that it can get to A in 8 msec, and A claims to be able to get to G in 18 msec, so J knows it can count on a delay of 26 msec to G if it forwards packets bound for G to A.
- Similarly, it computes the delay to G via I, H, and K as 41 (31 + 10), 18 (6 + 12), and 37 (31 + 6) msec, respectively. The best of these values is 18, so it makes an entry in its routing table that the delay to G is 18 msec and that the route to use is via H.

Flooding

- Another static algorithm is flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on. Flooding obviously generates vast numbers of duplicate packets, in fact, an infinite number unless some measures are taken to damp the process.
- One such measure is to have a hop counter contained in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero. Ideally, the hop counter should be initialized to the length of the path from source to destination.

- If the sender does not know how long the path is, it can initialize the counter to the worst case, namely, the full diameter of the subnet. An alternative technique for damming the flood is to keep track of which packets have been flooded, to avoid sending them out a second time.
- Achieve this goal is to have the source router put a sequence number in each packet it receives from its hosts. Each router then needs a list per source router telling which sequence numbers originating at that source have already been seen. If an incoming packet is on the list, it is not flooded.

- To prevent the list from growing without bound, each list should be augmented by a counter, k, meaning that all sequence numbers through k have been seen. When a packet comes in, it is easy to check if the packet is a duplicate; if so, it is discarded. Furthermore, the full list below k is not needed, since k effectively summarizes it.

Link State Routing

- Distance vector routing was used in the ARPANET until 1979, when it was replaced by link state routing. Two primary problems caused its demise. First, since the delay metric was queue length, it did not take line bandwidth into account when choosing routes.
- Initially, all the lines were 56 kbps, so line bandwidth was not an issue, but after some lines had been upgraded to 230 kbps and others to 1.544 Mbps, not taking bandwidth into account was a major problem.
- It would have been possible to change the delay metric to factor in line bandwidth, but a second problem also existed, the algorithm often took too long to converge. For these reasons, it was replaced by an entirely new algorithm, now called link state routing.
- The idea behind link state routing is simple and can be stated as five parts. Each router must do the following:
    1. Discover its neighbors and learn their network addresses.
    2. Measure the delay or cost to each of its neighbors.
    3. Construct a packet telling all it has just learned.
    4. Send this packet to all other routers.
    5. Compute the shortest path to every other router.

- In effect, the complete topology and all delays are experimentally measured and distributed to every router. Then Dijkstra's algorithm can be run to find the shortest path to every other router.

Flow based Routing

The static algorithm we have discussed till now doesn't take the capacity of the network into account. Flow based routing considers the flow in the network; mean consider the amount of traffic in the network before deciding on which outgoing line to place the packet. The basic idea behind the algorithm, is that any given line, if the capacity and average flow are known, it is possible to compute the mean packet delay on that li ne from queuing theory. The routing problem thus reduces to finding the routing algorithm that produces the minimum average delay for the subnet.

A flow router evaluates traffic flows in real time, based on an ID, route, and time of receipt and rate of flow, to keep streaming traffic moving as quickly as possible. Flow routing is a network routing technology that takes variations in the flow of data into account to increase routing efficiency.

Congestion Control

When too many packets are sent to a subnet more than its capacity, the Situation that arises is called **congestion.**

Reasons for Congestion:

1. If input packets coming from 3 or 4 lines, requires only one particular output line.

2. If routers are supplied with infinite amount of memory, packets take longtime to reach to the front of queue where duplicates are generated as they are timed out.
3. Slow processors cause congestion.
4. Low bandwidth lines also cause congestion.
5. Congestion feeds upon itself and cause congestion.

Congestion Control Algorithms

These algorithms control congestion. These are mainly divided into two groups:

1. Open Loop Solutions.
2. Closed Loop Solutions.
2.

Open Loop Solutions attempt to solve the problems by good design to make sure it does not occur in the first place. Once the system is up and running, mid-course corrections are not made.

Closed Loop Solutions are based on the concepts of a feedback loop. It has 3 parts.

- Monitor the system to detest when and where congestion occurs.
- Pass this information to places where action can be taken.
- Adjust system operation to correct the problem.

These closed loop algorithms are further divided into two categories:

Implicit feedback: The source reduces the congestion existence by making local observations.
Explicit feedback: Packets are sent back from the point of congestion to warn source

Open Loop Solutions:

- Congestion Prevention Policies
- Traffic Shaping
- Flow Specifications

1. Congestion prevention policies

Congestion is prevented using appropriate policies at various levels.

Layer	Policies
Transport	Retransmission policy Out-of-order caching policy Acknowledgement policy Flow control policy Timeout Determination
Network	Virtual circuits versus data gram inside the subnet Packet queuing service policy Packet discard policy Routing algorithm Packet lifetime Management
Data Link	Retransmission policy Out-of-order catching policy Acknowledgement policy Flow control policy

Retransmission policy: Deals with how fast a sender times out and what it transmits upon time out.
Out-of–order Catching policy: If receivers routinely discard all out-of-order packets, (packets arrived without order) they have to be retransmitted.
Acknowledgement policy: If each packet is acknowledged immediately, acknowledged packets generate extra traffic. This policy deals with piggybacking.
Flow Control policy: A tight flow control scheme (ex: a small window) reduces the data rate and thus helps fight congestion.
Timeout Determination: It is harder as transit time across the network is less predictable than transit time over a wire between two routers.
Virtual Circuits *vs.* Data grams: This affects congestion as many algorithms work only with virtual circuits.
Packets queuing and Service policy: Relates to whether routers have one queue per input line, one queue per output line or both.
Packet Discard policy: Tells which packet is dropped when there is no space.
Routing Algorithm: With this, Traffic is spreader over all the lines.
Packet lifetime management: Deals with how long a packet may live before being discarded.

2. Traffic Shaping

It is the process of forcing the packets to be transmitted at a more predictable rate. This approach is widely used in ATM Networks to manage congestion. When a virtual circuit is set up, the user and the subnet agree on a certain traffic pattern for that circuit. Monitoring a traffic flow based on agreement made is called "**Traffic Policing**".

Traffic shaping can be implemented with any of the two techniques:

- Leaky Bucket Algorithm
- Token Bucket Algorithm

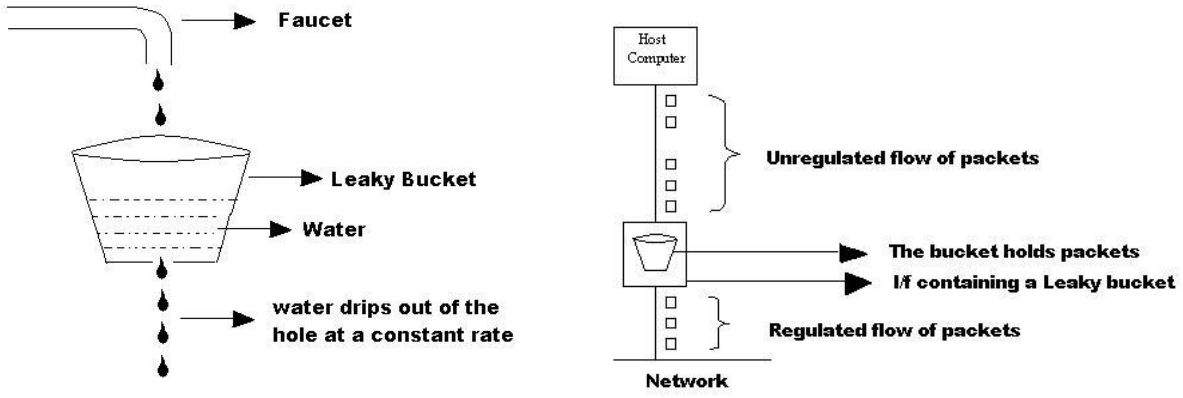
The Leaky Bucket Algorithm

The leaky bucket algorithm is a method of temporarily storing a variable number of requests and organizing them into a set-rate output of packets in an asynchronous transfer mode (ATM) network. The leaky bucket is used to implement traffic policing and traffic shaping in Ethernet and cellular data networks. The algorithm can also be used to control metered-bandwidth Internet connections to prevent going over the allotted bandwidth for a month, thereby avoiding extra charges.

Imagine a bucket with a small hole in the bottom. No matter, at what rate water enters the bucket, the outflow is at a constant rate, 'p', when there is any water in the bucket and 'r', when the bucket is empty. Also, once the bucket is full, any additional water entering it spills over the sides and is lost. The same idea can be applied to packets.

Conceptually, each host is connected to the network by an interface containing a leaky bucket, i.e., a finite internal queue. If a packet arrives at the queue when it is full, it is discarded. In other words, if one or more processes within the host try to send a packet when the maximum number is already queued, the new packet is unceremoniously discarded. This arrangement can be built into the h/w

inter face or simulated by the host operating system. It was first proposed by **TURNER** and is called the **"LEAKY BUCKET ALGORITHM".**

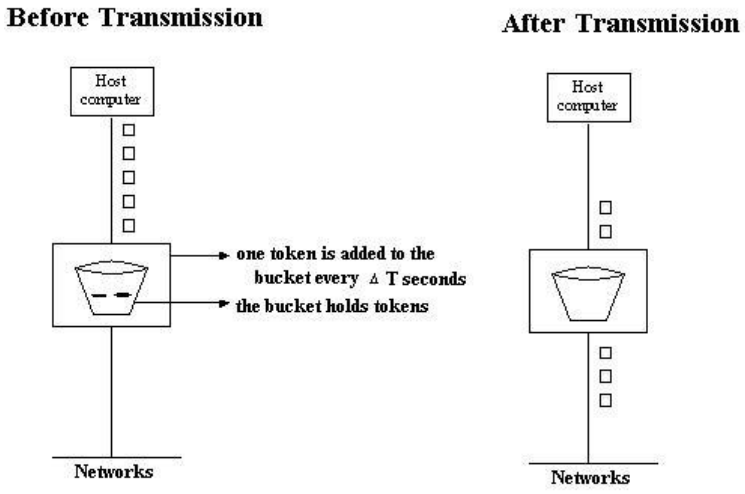


The host is allowed to put one packet per clock tick onto the network, which turns an uneven flow of packets from the user processes inside the host into an even flow of packets onto the network, smoothing out bursts and greatly reducing the chances of congestion.

The Token Bucket Algorithm

The **token bucket** is an algorithm used in packet switched computer networks and telecommunications networks. It can be used to check that data transmissions, in the form of packets, conform to defined limits on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow). It can also be used as a scheduling algorithm to determine the timing of transmissions that will comply with the limits set for the bandwidth and burstiness.

The algorithm that allows the output to speedup when large bursts arrive and one that never loses data is the TOKEN BUCKET ALGORITHM. In this algorithm, the leaky bucket holds tokens, generated by a clock at the rate of one token every ΔT sec. This algorithm allows to save up permission by hosts, up to the maximum size of the bucket, 'n' i.e., bursts of up to 'n' packets can be sent at once, allowing some burstiness in output stream and giving faster response to sudden bursts of input.



In the above circuit, we see a bucket holding 3 tokens, with 5 packets waiting to be transmitted. For a packet to be transmitted, it must be capture and destroy one token. In the above example, 3 out of 5 packets have gotten through by capturing the 3 tokens in the bucket, but the other 2 are struck waiting for 2 more tokens to be generated. The implementation of the token bucket algorithm is just a variable that counts tokens. The counter is incremented by 1, every ΔT and decremented by 1, when a packet is sent. When the counter hits '0', no packets may be sent.

The major advantage of the token bucket algorithm is that it throws away tokens instead of packets, when the bucket fills up.

Token bucket vs. Leaky bucket

S.N.	*Token Bucket*	*Leaky Bucket*
1	Token Dependent	Token independent
2	If bucket is full token are discarded, but not the packet	If bucket is full, packet or data is discarded.
3	Packets can only transmitted when there are enough token	Packets are transmitted continuously
4	It allows large bursts to be sent faster after that constant rate	It sends the packet at constant rate
5	It saves token to send large bursts	It does not save token

Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

Short for **Carrier Sense Multiple Access/Collision Detection**, **CSMA/CD** is a Media Access Control (MAC) protocol. It defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision. The CSMA/CD rules define how long the device should wait if a collision occurs. The medium is often used by multiple data nodes, so each data node receives transmissions from each of the other nodes on the medium.

CSMA/CD (carrier sense multiple access/collision detection) CD (collision detection) defines what happens when two devices sense a clear channel, then attempt to transmit at the same time. A collision occurs, and both devices stop transmission, wait for a random amount of time, and then retransmit. This is the technique used to access the 802.3 Ethernet network channel. This method handles collisions as they occur, but if the bus is constantly busy, collisions can occur so often that performance drops drastically. It is estimated that network traffic must be less than 40 percent of the bus capacity for the network to operate efficiently.

The following procedure is used to resolve a detected collision. The procedure is complete when retransmission is initiated or the retransmission is aborted due to numerous collisions.

1. Continue transmission (with a jam signal instead of frame header/data/CRC) until minimum packet time is reached to ensure that all receivers detect the collision.
2. Increment retransmission counter.
3. Was the maximum number of transmission attempts reached? If so, abort transmission.
4. Calculate and wait random back-off period based on number of collisions.
5. Re-enter main procedure at stage 1.

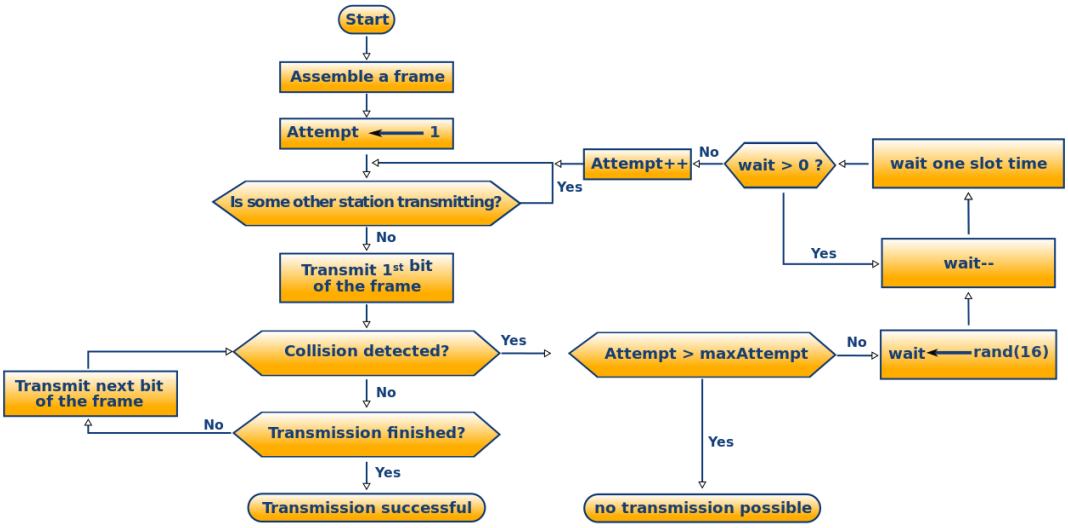


Fig: Simplified Algorithm of CSMA/CD

There are several CSMA access modes: 1-persistent, P-persistent, and O-persistent. 1-persistent is used in CSMA/CD systems, like Ethernet. This mode waits for the medium to be idle, and then transmits data. P-persistent is used in **CSMA/CA (Collision Avoidance)** systems, like Wi-Fi. This mode waits for the medium to be idle, and then transmits data with a probability p. If the data node does not transmit the data (a probability of 1 - p), the sender waits for the medium to be idle again and transmit the data with the same probability p. O-persistent is used by CobraNet, LonWorks, and the controller area network. This mode assigns a transmission order to each data node. When the medium becomes idle, the data node next in line can transmit data.

Transport Layer

In the Open Systems Interconnection (OSI) communications model, the Transport layer ensures the reliable arrival of messages and provides error checking mechanisms and data flow controls. The Transport layer provides services for both "connection-mode" transmissions and for "connectionless-mode" transmissions. For connection-mode transmissions, a transmission may be sent or arrive in the form of packets that need to be reconstructed into a complete message at the other end.

The transport layer is the layer in the open system interconnection (OSI) model responsible for end-to-end communication over a network. It provides logical communication between application processes running on different hosts within a layered architecture of protocols and other network components. The transport layer is also responsible for the management of error correction, providing quality and reliability to the end user. This layer enables the host to send and receive error corrected data, packets or messages over a network and is the network component that allows multiplexing.

TCP (Transmission Control Protocol)

Transmission control protocol (TCP) is a network communication protocol designed to send data packets over the Internet. TCP is a transport layer protocol in the OSI layer and is used to create a

connection between remote computers by transporting and ensuring the delivery of messages over supporting networks and the Internet.
Transmission Control Protocol is one of the most used protocols in digital network communications and is part of the Internet protocol suite, commonly known as the TCP/IP suite. Primarily, TCP ensures end-to-end delivery of data between distinct nodes. TCP works in collaboration with Internet Protocol, which defines the logical location of the remote node, whereas TCP transports and ensures that the data is delivered to the correct destination.

Before transmitting data, TCP creates a connection between the source and destination node and keeps it live until the communication is active. TCP breaks large data into smaller packets and also ensures that the data integrity is intact once it is reassembled at the destination node.

UDP (User Datagram Protocol)

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.

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- 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.

Here are few applications where UDP is used to transmit data:

- Domain Name Services
- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

SCTP (Stream Control Transmission Protocol)

SCTP (Stream Control Transmission Protocol) is a protocol for transmitting multiple streams of data at the same time between two end points that have established a connection in a network. Sometimes referred to as "next generation TCP" (Transmission Control Protocol) - or TCPng, SCTP is designed to make it easier to support a telephone connection over the Internet (and specifically to support the telephone system's Signaling System 7 - SS7 - on an Internet connection). A telephone connection requires that signaling information (which controls the connection) be sent along with voice and other data at the same time. SCTP also is intended to make it easier to manage connections over a wireless network and to manage the transmission of multimedia data. SCTP is a standard protocol (RFC 2960) developed by the Internet Engineering Task Force (IETF).

In computer networking, the **Stream Control Transmission Protocol** (**SCTP**) is a transport-layer protocol, serving in a similar role to the popular protocols TCP and UDP. SCTP provides some of the same service features of both: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP; it differs from these in providing multi-homing and redundant paths to increase resilience and reliability. Unlike TCP, SCTP ensures the complete concurrent transmission of several streams of data (in units called messages) between connected end points. SCTP also supports multihoming, which means that a connected end point can have alternate IP addresses associated with it in order to route around network failure or changing conditions.

Port

In computer networking, a **port** is an endpoint of communication in an operating system. While the term is also used for hardware devices, in software it is a logical construct that identifies a specific process or a type of service. A port is always associated with an IP address of a host and the protocol type of the communication, and thus completes the destination or origination address of a communications session. A port is identified for each address and protocol by a 16-bit number, commonly known as the **port number**.

On computer and telecommunication devices, a *port* (noun) is generally a specific place for being physically connected to some other device, usually with a socket and plug of some kind. Typically, a personal computer is provided with one or more serial ports and usually one parallel port. The serial port supports sequential, one bit-at-a-time transmission to peripheral devices such as scanners and the parallel port supports multiple-bit-at-a-time transmission to devices such as printers.

Sockets

A network socket is one endpoint in a communication flow between two programs running over a network. Sockets are created and used with a set of programming requests or "function calls" sometimes called the sockets application programming interface (API). The most common sockets API is the Berkeley UNIX C interface for sockets. Sockets can also be used for communication between processes within the same computer.

Sockets can also be used for "connection-oriented" transactions with a somewhat different sequence of C language system calls or functions. The Secure Sockets Layer (SSL) is a computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.

Sockets allow communication between two different processes on the same or different machines. To be more precise, it's a way to talk to other computers using standard UNIX file descriptors. In UNIX, every I/O action is done by writing or reading a file descriptor.

A file descriptor is just an integer associated with an open file and it can be a network connection, a text file, a terminal, or something else. To a programmer, a socket looks and behaves much like a low-level file descriptor. This is because commands such as read () and write () work with sockets in the same way they do with files and pipes. A **socket address** is the combination of an IP address and a port number, much like one end of a telephone connection is the combination of a phone number and a particular extension.

DNS (Domain Name System)

Domain Name System (DNS) enables you to use hierarchical, friendly names to easily locate computers and other resources on an IP network. DNS is a distributed database that contains mappings of DNS domain names to data. It is also a protocol for Transmission Control Protocol/Internet Protocol (TCP/IP) networks, defined by the Requests for Comments (RFCs) that pertain to DNS. DNS defines the following:

- Mechanism for querying and updating the database.
- Mechanism for replicating the information in the database among servers.
- Schema for the database.

The domain name system, more commonly known as "DNS" is the networking system in place that allows us to resolve human-friendly names to unique addresses. A domain name is the human-friendly name that we are used to associating with an internet resource. For instance, "google.com" is a domain name. Some people will say that the "Google" portion is the domain, but we can generally refer to the combined form as the domain name. The URL "google.com" is associated with the servers owned by Google Inc. The domain name system allows us to reach the Google servers when we type "google.com" into our browsers.

A top-level domain, or TLD, is the most general part of the domain. The top-level domain is the furthest portion to the right (as separated by a dot). Common top-level domains are "com", "net", "org", "gov", "edu", and "io". Top-level domains are at the top of the hierarchy in terms of domain names. Certain parties are given management control over top-level domains by ICANN (Internet Corporation for Assigned Names and Numbers). These parties can then distribute domain names under the TLD, usually through a domain registrar.

A fully qualified domain name, often called FQDN, is what we call an absolute domain name. Domains in the DNS system can be given relative to one another, and as such, can be somewhat ambiguous. A FQDN is an absolute name that specifies its location in relation to the absolute root of the domain name system.
A name server is a computer designated to translate domain names into IP addresses. These servers do most of the work in the DNS system. Since the total number of domain translations is too much for any one server, each server may redirect request to other name servers or delegate responsibility for a subset of subdomains they are responsible for.

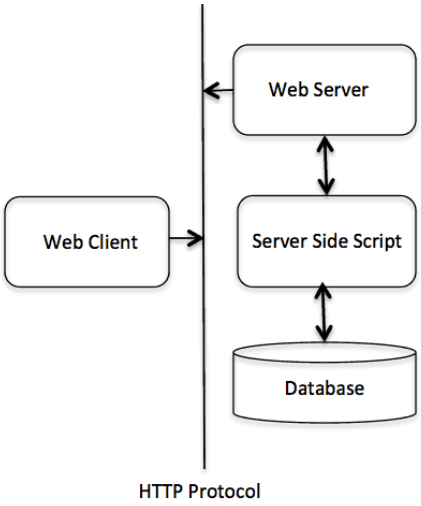
HTTP (Hype Text Transport Protocol)

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e. internet) since 1990. HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.

There are three basic features that make HTTP a simple but powerful protocol:

- **HTTP is connectionless:** The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client disconnects from the server and waits for a response. The server processes the request and re-establishes the connection with the client to send a response back.

- **HTTP is media independent:** It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content. It is required for the client as well as the server to specify the content type using appropriate MIME-type.
- **HTTP is stateless:** As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.



The following diagram shows a very basic architecture of a web application and depicts where HTTP sits:

The HTTP protocol is a request/response protocol based on the client/server based architecture where web browsers, robots and search engines, etc. act like HTTP clients and the Web server acts as a server.

Client
The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection.

Server
The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta-information, and possible entity-body content.

SMTP (Simple Mail Transport Protocol)

The purpose of the Simple Mail Transfer Protocol (**SMTP**) is to manage the transfer of electronic mail (**e-mail**) from one computer mail system to another. It does not accept mail from local users, nor does it distribute mail to the intended recipients. This task is handled by the local mail system. Since SMTP only interacts with the local mail system it does not see mail which is local to the system. Only when mail is to be sent to or received from another machine will SMTP come into play.
There is usually an I/O queue at the interface between the Local Mail System and the Client/Server ports. The Client is concerned with the sending of mail to another system, whilst the server is concerned with receiving mail.

The local system maintains a mailbox for each user on the system. The name of this mailbox is unique and consists of two parts:

The Local Port

This is simply the name of the user and must be unique to the local host.

The Global Port

This part is the name of the host and must be unique to the Internet.

PROXY

A proxy server is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service. The proxy server may exist in the same machine as a firewall server or it may be on a separate server, which forwards requests through the firewall.
An advantage of a proxy server is that its cache can serve all users. If one or more Internet sites are frequently requested, these are likely to be in the proxy's cache, which will improve user response time. A proxy can also log its interactions, which can be helpful for troubleshooting.
Proxy servers work as a intermediary between the two ends of a client/server network connection. Proxy servers interface with network applications, most commonly Web browsers and servers. Inside corporate networks, proxy servers are installed on specially-designated internal (intranet) devices. Some Internet Service Providers (ISPs) also utilize proxy servers as part of providing online services to their customers. Finally, a category of third-party hosted Web sites called Web proxy servers is available to end users on the Internet for their Web browsing sessions.

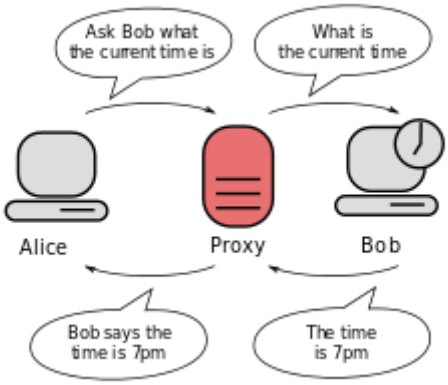
Key Features of Proxy Servers

Proxy servers traditionally provide three main functions:

1. firewall and network data filtering support
2. network connection sharing
3. data caching

A proxy server may reside on the user's local computer, or at various points between the user's computer and destination servers on the Internet.

- A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a *tunneling proxy*.
- A forward proxy is an Internet-facing proxy used to
- Retrieve from a wide range of sources (in most cases anywhere on the Internet).
- A reverse proxy is usually an internal-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching.



FTP (File Transport Protocol)

FTP stands for "file transfer protocol." FTP powers one of the fundamental Internet functions and is the prescribed method for the transfer of files between computers. It is also the easiest and most secure way to exchange files over the Internet. An FTP address looks a lot like an HTTP or web site address except it uses the prefix ftp:// instead of http://.
The most common use of FTP is to download files. FTP is vital to the MP3 music sharing, most online auctions and game enthusiasts. The ability to transfer files quickly and reliably is essential for everyone creating and maintaining a web page.
Typically, a computer with an FTP address is dedicated to receive an FTP connection. A computer dedicated to receiving an FTP connection is referred to as an FTP server or FTP site.

- Most web hosting services provide FTP access to their customers to allow them to upload the contents of their web sites.
- Companies often have FTP servers that allow users to send and receive files.
- Most universities have FTP servers that allow their students to download course materials and upload assignments for submission.
- Use FTP to transfer files among users, especially if the files are too large to attach to an email.
- Use FTP to browse through a collection of downloadable files on a public software archive.

Examples of Client –Server Networking Tools

A client is a piece of computer hardware or software that accesses a service made available by a server. The server is often (but not always) on another computer system, in which case the client accesses the service by way of a network. For example, web browsers are clients that connect to web servers and retrieve web pages for display. Email clients retrieve email from mail servers.
Over the years, Microsoft has given us a staggering number of tools to help with server administration. Since there are so many tools available, I decided to talk about some of important and popular tools.

1. **PowerShell**

   Microsoft's Server products have evolved to the point that we can perform almost any administrative action from the command line by using PowerShell. Most of the newer Microsoft Server products include management tools that are actually built on top of PowerShell. This means that any management tasks that can be performed through the GUI can also be performed from the command line or performed through a PowerShell Script.

2. **Best Practices Analyzer**

   The Best Practices Analyzer isn't really a single tool, but rather a series of tools designed to analyze our server deployments and ensure that they adhere to Microsoft's recommended best practices. Microsoft provides versions of the Best Practices analyzer for Exchange, SQL, Small Business Server, and other Microsoft server products.

3. **Security Configuration Wizard**

   The Security Configuration Wizard is designed to help us to reduce the attack surface of our servers. It analyzes the way in which your servers are configured and then recommends how we

can change various aspects of the configuration to make them more secure. The Security Configuration Wizard is included with Windows Server 2008 and Windows Server 2008 R2.

4. ADSI Edit

ADSI Edit allows us to manually edit the Active Directory database. Whenever someone asks us about ADSI Edit, we can usually compare it to the registry editor. The registry editor allows us to manually change various configuration parameters within a system, but if we use it incorrectly, we can destroy Windows. ADSI Edit is similar: It gives us free rein over Active Directory, but if we make a mistake, we can destroy it.

5. Microsoft File Server Migration Wizard

As time goes on, server hardware continues to improve. Some organizations are finding that they can decrease management costs by consolidating their aging file servers. The Microsoft File Server Migration Wizard, which is included in the File Server Migration Toolkit, helps organizations merge the contents of aging file servers into DFS root.

6. Server Core Configurator

So far, all the tools I've talked about are provided by Microsoft. However, there is one third-party tool I want to mention. Server Core Configurator is an open source tool written by Guy Teverovsky.

Any time you perform a server core installation of Windows Server 2008, you must perform certain post installation tasks before the server is ready to use. Microsoft offers some PowerShell scripts, but performing the initial configuration process from a command line can be tedious. The Server Core Configurator simplifies the provisioning process by providing a simple GUI we can use for the initial configuration.

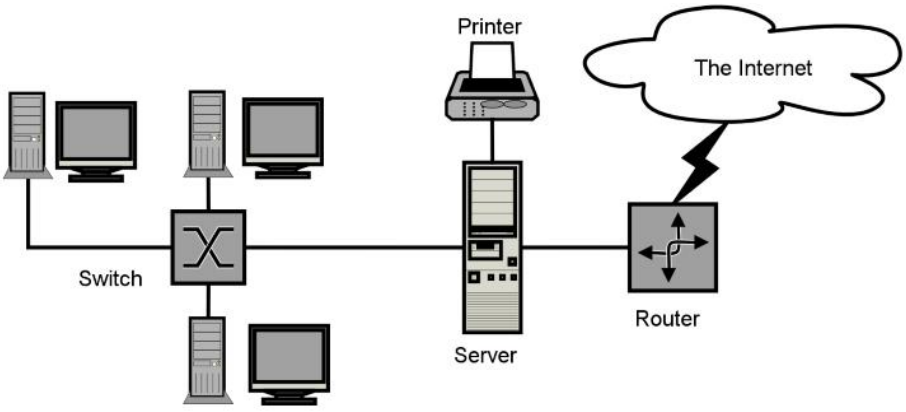
7. Microsoft Application Compatibility Manager

The Microsoft Application Compatibility Manager is part of the Application Compatibility Toolkit. It's designed to ease the transition from one version of Windows to the next by compiling an inventory of the applications running on your desktops and determining whether each one is compatible with the new version of Windows.

Note: Among these tools there are lots of open source tools, windows based tools and Third party's networking tools which can play an important role for client-server networking.

Cloud Networking

In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. It goes back to the days of flowcharts and presentations that would represent the gigantic server-farm infrastructure of the Internet as nothing but a puffy, white cumulus cloud, accepting connections and doling out information as it floats.



Cloud computing, often referred to as simply “the cloud,” is the delivery of on-demand computing resources—everything from applications to data centers—over the Internet on a pay-for-use basis. Cloud computing is a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to handle applications. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine.

In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "*the Internet*," so the phrase *cloud computing* means "a type of Internet-based computing," where different services — such as servers, storage and applications — are delivered to an organization's computers and devices through the Internet. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive online computer games.
To do this, cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing cores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

The Internet has its roots in the 1960s, but it wasn't until the early 1990s that it had any relevance for businesses. The World Wide Web was born in 1991, and in 1993 a web browser called Mosaic was released that allowed users to view web pages that included graphics as well as text. This heralded the first company web sites – and not surprisingly, most of these belonged to companies involved in computing and technology. As Internet connections got faster and more reliable, a new type of company called an Application Service Provider or ASP started to appear. ASPs took existing business applications and ran them for their customers. The ASP would buy the computing hardware and keeping the application running, and the customer would pay a monthly fee to access it over the Internet. But it wasn't until right at the end of the 1990s that cloud computing as we know it today appeared. That's when salesforce.com introduced its own multi-tenant application which was specifically designed:

- to run "in the cloud";
- to be accessed over the Internet from a web browser;
- To be used by large numbers of customers simultaneously at low cost.

Cloud computing promises several attractive benefits for businesses and end users. Three of the main benefits of cloud computing includes:

- Self-service provisioning: End users can spin up computing resources for almost any type of workload on-demand.
- Elasticity: Companies can scale up as computing needs increase and then scale down again as demands decrease.
- Pay per use: Computing resources are measured at a granular level, allowing users to pay only for the resources and workloads they use.

Cloud computing services can be private, public or hybrid. Private cloud services are delivered from a business' data center to internal users. This model offers versatility and convenience, while preserving management, control and security. Internal customers may or may not be billed for services through IT chargeback.

Network Visualization

Networks are critical to modern society, and a thorough understanding of how they behave is crucial to their efficient operation. Fortunately, data on networks is plentiful; by visualizing this data, it is possible to greatly improve our understanding. Our focus is on visualizing the data associated with a network and not on simply visualizing the structure of the network itself.
We are currently in the midst of a networking revolution. Data communications networks such as the Internet now connect millions of computers; cellular phones have become commonplace, and personal communications networks are in the developmental stages. In parallel with the ever increasing network sizes has been a concomitant increase in the collection of network measurement data. Understanding this data is of crucial importance as we move to a modern, information-rich society.

Unfortunately, tools for analyzing network data have not kept pace with the data volumes. More network measurement data is available today than ever before, yet it is useless until it is understood. Traditional network analysis software and graphs cannot cope with the size of today's networks and their data collection capabilities.
A network consists of nodes, links, and possibly spatial information. Statistics, which may be raw data or data summaries and may vary over time, are associated with the nodes and the links. The link statistics may be directed, as in call flow of a circuit-switched network, or undirected, as in the network's capacity. The network may have a natural spatial layout as does a geographical trade-flow network, or may be abstract as in a personal communications network. Network data may categorical, such as the type of node or link, or quantitative such as a link's capacity. The data may be static, such as a network's capacity, or time varying, such as the network flow in several time periods.
There are many more benefits to visualization. Here are just a few:

- The bandwidth of data you can transfer in a picture is much bigger than having a human look at log files or textual data.
- Relationships become very apparent. Sometimes they are completely hidden without visualization.
- Interactive visualizations benefit from dynamic queries which are an incredible tool to explore data.
- Visualization inspires. You look at a picture or a graph and suddenly you realize what is really going on.

- It's a great tool to communicate information in a very compact and often easy to understand way.
- It definitely reduces analysis and response times. Sifting through thousands of line of logs is definitely slower than looking at a few graphs of the same data.

Network virtualization

Network virtualization refers to the management and monitoring of an entire computer network as a single administrative entity from a single software-based administrator's console. Network virtualization also may include storage virtualization, which involves managing all storage as a single resource. Network virtualization is designed to allow network optimization of data transfer rates, flexibility, scalability, reliability and security. It automates many network administrative tasks, which actually disguise a network's true complexity. All network servers and services are considered one pool of resources, which may be used without regard to the physical components.

Network virtualization is especially useful for networks experiencing a rapid, large and unpredictable increase in usage.
The intended result of network virtualization is improved network productivity and efficiency, as well as job satisfaction for the network administrator.
Network virtualization is categorized as either **external virtualization**, combining many networks or parts of networks into a virtual unit, or **internal virtualization**, providing network-like functionality to software containers on a single network server.

Wireless network virtualization can have a very broad scope ranging from spectrum sharing, infrastructure virtualization, to air interface virtualization. Similar to wired network virtualization, in which physical infrastructure owned by one or more providers can be shared among multiple service providers, wireless network virtualization needs the physical wireless infrastructure and radio resources to be abstracted and isolated to a number of virtual resources, which then can be offered to different service providers.

Network virtualization lends itself to cost savings, efficiency, security and flexibility -- four key benefits for any client. Besides this basic efficiency benefit, there are several other compelling benefits to virtualization:

- **Hardware cost:** You can typically save a lot of money by reducing hardware costs when you use virtualization.
- **Energy costs:** Many organizations have found that going Virtual has reduced their overall electricity consumption for server computers by 80 percent. This savings is a direct result of using less computer hardware to do more work.
- **Recoverability:** One of the biggest benefits of virtualization is not the cost savings, but the ability to quickly recover from hardware failures.
- **Disaster recovery:** Besides the benefit of recoverability when hardware failures occur, an even bigger benefit of virtualization comes into play in a true disaster recovery situation.

Network Security

Network security is an over-arching term that describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources.

This means that a well-implemented network security blocks viruses, malware, hackers, etc. from accessing or altering secure information. Network Security is an organization's strategy and provisions for ensuring the security of its assets and of all network traffic. Network security is manifested in an implementation of security hardware, and software

The first layer of network security is enforced through a username/password mechanism, which only allows access to authenticated users with customized privileges. When a user is authenticated and granted specific system access, the configured firewall enforces network policies, that is, accessible user services.

However, firewalls do not always detect and stop viruses or harmful malware, which may lead to data loss. Antivirus software or an intrusion prevention system (IPS) is implemented to prevent the virus and/or harmful malware from entering the network. Network security is sometimes confused with information security, which has a different scope and relates to data integrity of all forms, print or electronic.

Why is Network security important?

In today's era, almost every single organization uses a computer and has a computer network to send, receive and store information. Whether it's sending emails, storing documents, or serving information through a web server, it is very important to focus on security, especially if your network contains sensitive, confidential and personal information.
Network security affects many organizations, whether they are large, small, or government organizations. If network security is breached an intruder can do all sorts of harm. That is why people need to be aware of and to be educated about network security and how to secure their computer and network. Systems are required to be updated regularly as new security flaws are discovered. Without being up to date, it makes it easy for a *hacker* to gain unauthorized access to the system.

Because hacker tools have become more and more sophisticated, super-intelligence is no longer a requirement to hack someone's computer or server. Of course, there are individuals that have developed sophisticated skills and know how to breach into a user's privacy in several ways, but these types of individuals are less common than in the past.
Today, most malicious users do not possess a high level of programming skills and instead make use of tools available on the Internet. There are several stages that an attacker has to pass through to successfully carry out an attack.

Security Attacks

We can group network attacks by the skills possessed by the attacker. Based on these criteria we can divide attacks in two categories:

1. **Unstructured** – attacks made by unskilled hackers. Individuals behind these attacks use hacking tools available on the Internet and are often not aware of the environment they are attacking. These threats should not be neglected because they can expose precious information to malicious users.
2. **Structured** – attacks made by individuals who possess advanced computing skills. Such hackers are experts in exploiting system vulnerabilities. By gaining enough information about a company's network, these individuals can create custom hacking tools to breach

network security. Most structured attacks are done by individuals with good programming skills and a good understanding of operating systems, networking and so on.

Social engineering is another type of network attack. Malicious users take advantage of human's credibility and often gain important information directly from their victims. They often call or send fraudulent emails to their victims pretending to be some other person entirely.

Phishing is a method that is pretty easy to implement by hackers. This paragraph from Wikipedia describes phishing attacks: "**Phishing** is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes indirectly, money) by masquerading as a trustworthy entity in an electronic communication". Entire sites are known to be duplicated by hackers in an attempt to steal precious information from users.

In today's data networks there are many different types of attacks and each one requires special skills that hackers must poses in order to successfully crack into someone's privacy:

Eavesdropping – is one of the common types of attacks. A malicious user can gain critical information from "listening" to network traffic. Because most communications are sent unencrypted, there are many cases in which traffic is susceptible to interception. The traffic can be analyzed using sniffing tools (also known as snooping) to read information as it is sent into the network. Wireless networks are more susceptible to interception than wired ones. Eavesdropping can be prevented by using encryption algorithms.

Dos and DDoS attacks (Denial of Service and Distributed Denial of Service attacks) – these attacks take advantage of network traffic to create abnormal behavior to network services or applications. Servers are often targeted and flooded with data until they become unreachable. Core network equipment can be blocked and thus prevent normal traffic from flowing into the network. Distributed denials of service attacks are more dangerous because attacks are made from multiple sources.

Password attacks – these attacks are based on cracking user or equipment passwords. They are one of the most feared network attacks because once a user is compromised; the whole network can be damaged, especially if we are talking about a domain user or network administrator.
Dictionary attacks use patterns to guess passwords in multiple attempts. Critical information can be gained by using a compromised username. This is one of the main reasons companies use strong passwords that are changed frequently.

Compromised-Key attack – by obtaining the private key of a sender, an attacker can decipher secured network traffic. This kind of attack is often hard to be carried out successfully because it requires good computing resources and skills.

Man-in-the-Middle attack – as the name implies, this attack is based on intercepting and modifying information between two transmitting nodes. A hacker can modify network routes to redirect traffic to its machine before it is carried out to the destination.

IP address spoofing – in this scenario hackers use spoofed IPs to impersonate a legitimate machine. The attacker can then modify packets making them look like legitimate traffic to the receiving network device.

Application-layer attacks – these attacks are based on cracking applications that run on servers or workstations. These types of attacks are common because there are many different applications that run on machines and are susceptible to attacks. Hackers use viruses, Trojans and worms to infect devices and gain important information.

Exploit attacks – these are usually made by individuals who possess strong computing skills and can take advantage of software bugs or misconfigurations. By having enough information of specific software, hackers can "exploit" a particular problem and use it to gain access to private data.

Passive Attack

A passive attack can be split into two types. The first type of passive attack is to simply **monitor the transmission** between two parties and to capture information that is sent and received. The attacker does not intend to interrupt the service, or cause an effect, but to only read the information. The second type of attack is a **traffic analysis**. If information is encrypted, it will be more difficult to read the information being sent and received, but the attacker simply observers the information, and tries to make sense out of it; or to simply determine the identity and location of the two communicating parties.
A passive attack is usually harder to detect as there is little impact to the information communicated.

Active Attack

On the other hand, an active attack aim is to cause disruption, and it is usually easily recognized. Unlike a passive attack, an active attack modifies information or interrupts a service. There are four types of an active attack:

- **Masquerade** – To pretend to be someone else. This could be logging in with a different user account to gain extra privileges. For example, a user of a system steals the System Administrators username and password to be able to pretend that they are them
- **Reply** – To capture information to send it, or a copy it elsewhere
- **Modification** – To alter the information being sent or received
- **Denial of service** – To cause a disruption to the network

Even though a passive attack doesn't sound harmful, it is just as bad as an activate attack, if not worse.

Security Services

Security services are a service that provides a system with a specific kind of protection. The X.800 OSI Security Architecture defines 6 major security service categories, that once a system satisfies these 6 categories, the system is X.800 compliant.

- **Confidentiality** – Protects data from being read or accessed by unauthorized personnel
- **Authentication** – Ensures that no one can impersonate someone to be legitimately authorized to access services they should not access.
- **Integrity** – Ensures data cannot be alternated and messages that are sent and received have not been read, duplicated, modified or replayed to another party.

- **Non-repudiation** – Prevents the sender or receiver from denying the transmission of a sent or received message. The sender and receiver are to be able prove that they sent or did not send or received a message
- **Access control** – Limits and control access to certain system applications to certain users Availability – Ensures the service is only available to legitimated users and not available to users who do not have access to the application

Security Mechanism

Security mechanisms are ways to detect, prevent, or recover from a security attack. It is important for systems to have implemented as many security mechanisms as possible as required for their system.

Specific Security Mechanisms

- Encipherment – Encrypting and decrypting communication
- Digital signatures – An electronic signature to assure the genuineness of a digital document
- Access controls – To only allows people with permission to access something
- Data integrity – Ensure data is in full and unchanged
- Authentication exchange – The exchange of communication that takes place when authorizing someone
- Traffic padding – Determining what is legitimate data and what is false data
- Routing Control – Sending information through a specific line or path
- Notarization – Official documentation of procedures

Pervasive Security Mechanisms

- Trusted functionality – How well you trust the information
- Security labels – Label information with a particular security attribute
- Event detection – Logging events that take place
- Security audit trails – Checking security to ensure that measures are being followed and intrusions have not occurred
- Security recovering – Recovering from a security issue

Wireless LAN Security

Wireless local area network security (WLAN security) is a security system designed to protect networks from the security breaches to which wireless transmissions are susceptible. This type of security is necessary because WLAN signals have no physical boundary limitations, and are prone to illegitimate access over network resources, resulting in the vulnerability of private and confidential data. Network operations and availability can also be compromised in case of a WLAN security breech. To address these issues, various authentications, encryption, invisibility and other administrative controlling techniques are used in WLANs. Business and corporate WLANs in particular require adequate security measures to detect, prevent and block piggy backers, eavesdroppers and other intruders.

Security has remained a major concern in WLANs around the globe. While wireless networks provide convenience and flexibility, they also increase network vulnerability. Security threats such as unauthorized access, denial of service attacks, IP and MAC spoofing, session hijacking and

eavesdropping can all be problems for WLANs. To counter these threats, various standard authentication and encryption techniques are combined with other access control mechanisms. These protocols, devices and techniques collectively secure the WLAN a level that equals and even exceeds wired LAN security.

Some of the technologies employed in WLAN security include:

- **Wired Equivalent Privacy (WEP):** An old encryption standard used to overcome security threats. WEP provides security to WLAN by encrypting the information transmitted over the air so that only the receivers with the correct encryption key can decrypt the information.
  Short for ***W**ired **E**quivalent **P**rivacy*, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicalities of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

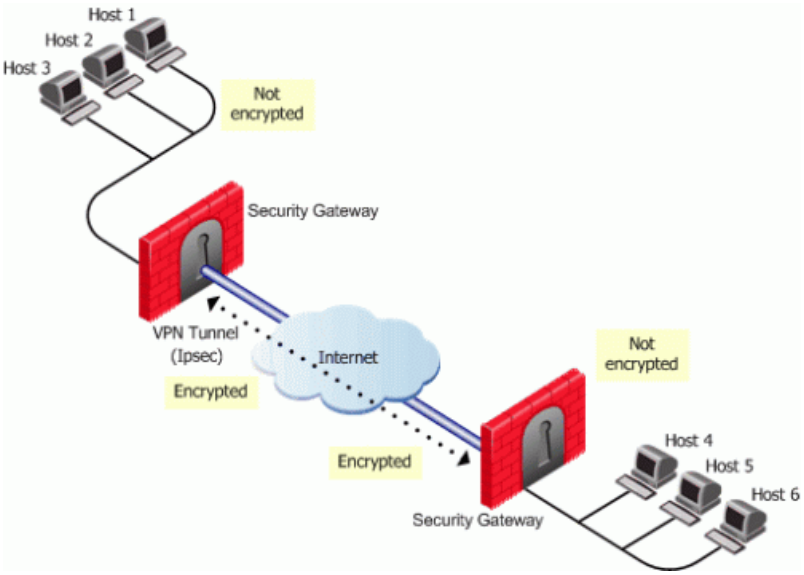
- **WPA/WPA2 (WI-FI Protected Access):** Improved on WEP by introducing Temporal Key Integrity Protocol (TKIP). While still using RC4 encryption, TKIP uses a temporal encryption key that is regularly renewed, making it more difficult to steal. In addition, data integrity was improved through the use of a more robust hashing mechanism. Short for ***W**i-Fi **P**rotected **A**ccess*, a Wi-Fi standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP (i.e., as a software upgrade to existing hardware), but the technology includes two improvements over WEP:

- **Wireless Intrusion Prevention Systems/Intrusion Detection Systems:** Intrusion detection and prevention focuses on radio frequency (RF) levels. This involves radio scanning to detect rogue access points or ad hoc networks to regulate network access. Advanced implementations are able to visually represent the network area along with potential threats, and have automatic classification capabilities so that threats can be easily identified.

VPN (Virtual Private Network)

Virtual Private Network (VPN) is the technology that you can use to access the office or home network remotely and securely over the Internet, so that the communication data is protected from sniffing or hijacking by hackers. Typically, private networks are not accessible from the Internet or other public networks, because firewalls will block all unrequested traffic. To remotely access a private network over Internet, we need to use technology like Virtual Private Network (VPN).

When the VPN connection is established between 2 parties (between a VPN client and VPN gateway or between 2 VPN gateways), a secured virtual tunnel will be created with capability to encrypt the data (so no hacker can see the data content), preserve data integrity (no data change during transmission) and ensure the communication only happen between that 2 authenticated parties.



In the Figure, host 1 and host 6 need to communicate. The connection passes in the clear between host 1 and the local Security Gateway. From the source and destination addresses of the packet, the Security Gateway determines that this should be an encrypted connection. If this is the first time the connection is made, the local Security Gateway initiates an IKE negotiation with the peer Security Gateway in front of host 6. During the negotiation, both Security Gateways authenticate each other, and agree on encryption methods and keys. After a successful IKE negotiation, a VPN tunnel is created.

After a VPN tunnel has been established:

- A packet leaves the source host and reaches the Security Gateway.
- The Security Gateway encrypts the packet.
- The packet goes down the VPN tunnel to the second Security Gateway. In actual fact, the packets are standard IP packets passing through the Internet. However, because the packets are encrypted, they can be considered as passing through a private "virtual" tunnel.
- The second Security Gateway decrypts the packet.
- The packet is delivered in the clear to the destination host. From the hosts' perspectives, they are connecting directly.

VPN Security

VPN protocols are designed to secure our data over public (unsafe) networks. Security is ensured using:

- **Data Confidentiality** – data is encrypted which makes it unreadable to those on the public network.
- **Data Integrity** – data is digitally signed, so that the recipient can recognize that the data has been changed during transmission. This doesn't encrypt the data, but uses a hash value of the data to determine if the content was altered. The hash value of any data will stay the same as long as the content of the data is not changed.
- **Replay Protection** – ensures that the same data can't be sent more than once. In a replay attack, an attacker captures and then resends the data, such as our login information in an

attempt to access the server. Through the use of sequencing, VPN protocols make sure that the data is not replayed.

- **Data Origin Authentication** – uses authentication techniques to ensure the origin of the transmitted and received data. It makes sure that the transmitter and a receiver is trusted.

Advantages of VPNs

VPNs promise two main advantages over competing approaches -- cost savings, and scalability (that is really just a different form of cost savings).

The Low Cost of a VPN

One way a VPN lowers costs is by eliminating the need for expensive long-distance leased lines. With VPNs, an organization needs only a relatively short dedicated connection to the service provider.

Another way VPNs reduce costs is by lessening the need for long-distance telephone charges for remote access.

Scalability

The cost to an organization of building a dedicated private network may be reasonable at first but increases exponentially as the organization grows. A company with two branch offices, for example, can deploy just one dedicated line to connect the two locations, but 4 branch offices require 6 lines to directly connect them to each other, 6 branch offices need 15 lines, and so on. Internet based VPNs avoid this scalability problem by simply tapping into the the public lines and network capability readily available.

Disadvantages of VPNs

Despite their popularity, VPNs are not perfect and limitations exist as is true for any technology. Organizations should consider issues like the below when deploying and using virtual private networks in their operations:

1. VPNs require an in-depth understanding of public network security issues and proper deployment of precautions.
2. The availability and performance of an organization's wide-area VPN (over the Internet in particular) depends on factors largely outside of their control.
3. VPN technologies from different vendors may not work well together due to immature standards.
4. VPNs need to accommodate protocols other than IP and existing ("legacy") internal network technology.

Cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Cryptography is derived from the Greek words: kryptos, "hidden", and graphein, "to write" - or "hidden writing". People who study and develop cryptography are called **cryptographers**. The study of how to *circumvent* the use of cryptography for unintended recipients is called **cryptanalysis**, or code-breaking. Cryptography and cryptanalysis are sometimes grouped together under the umbrella term **cryptology**.

Modern cryptography concerns itself with the following four objectives:

1. **Confidentiality** (the information cannot be understood by anyone for whom it was unintended)
2. **Integrity** (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3. **Non-repudiation** (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4. **Authentication** (the sender and receiver can confirm each other's identity and the origin/destination of the information)

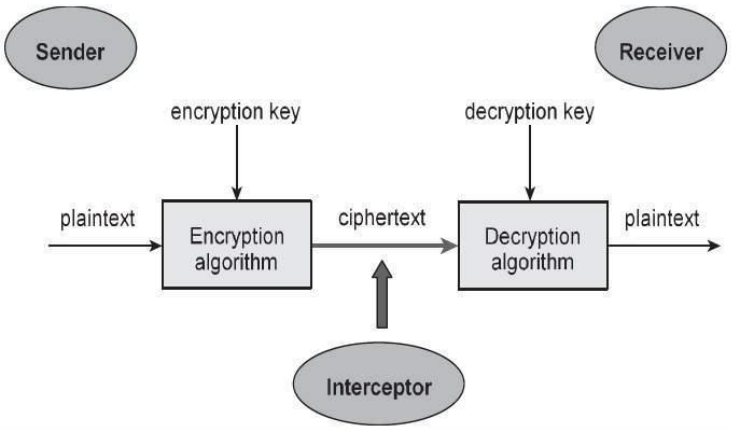
Encryption

Encryption is the process of taking a readable plain text document or image and scrambling that document or image to an extent that it is no longer readable. The intent of encryption is hiding and to protect the contents of that file from improper disclosure.

The various components of a basic cryptosystem are as follows −

- **Plaintext.** It is the data to be protected during transmission.
- **Encryption Algorithm**. It is a mathematical process that produces a cipher text for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a cipher text.
- **Cipher text**. It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The cipher text is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
- **Decryption Algorithm.** It is a mathematical process, that produces a unique plaintext for any given cipher text and decryption key. It is a cryptographic algorithm that takes a cipher text and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the cipher text.
- **Decryption Key**. It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher text in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a key space. An interceptor (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the cipher text and may know the decryption algorithm. He, however, must never know the decryption key.



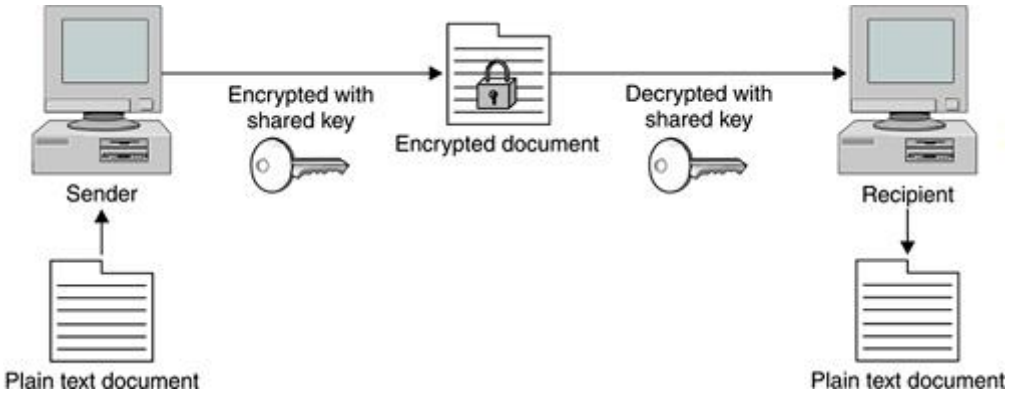
Types of Encryption

There are two types of encryptions schemes as listed below:

- Symmetric Key encryption
- Public Key encryption

Symmetric Key Encryption

An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message is called Symmetric key encryption.



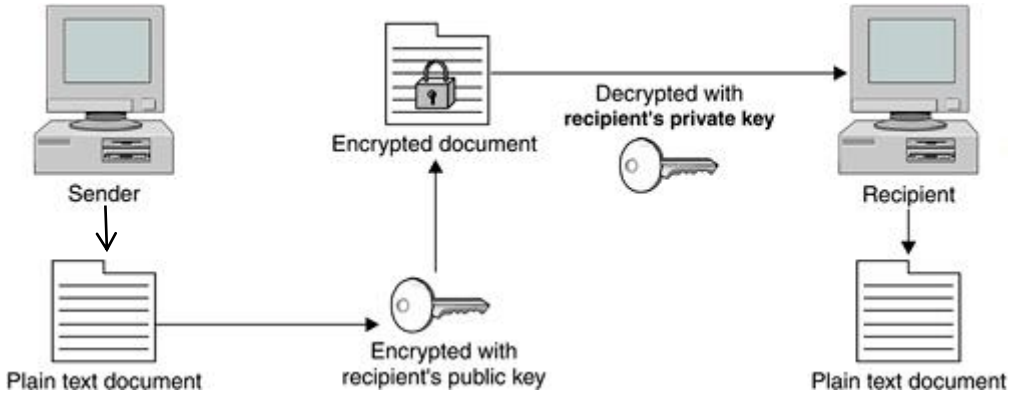
Symmetric key encryption algorithm uses same cryptographic keys for both encryption and decryption of cipher text. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Symmetric encryption is also known as private-key encryption and secure-key encryption.

The salient features of cryptosystem based on symmetric key encryption are −

- Persons using symmetric key encryption must share a common key prior to exchange of information.
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of n people, to enable two-party communication between any two persons, the number of keys required for group is $n \times (n – 1)/2$.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

Asymmetric Key Encryption (Public Key Encryption)

Asymmetric cryptography uses encryption that splits the key into two smaller keys. One of the keys is made public and one is kept private. You encrypt a message with the recipient's public key. The recipient can then decrypt it with their private key. And they can do the same for you, encrypting a message with your public key so you can decrypt it with your private key.



Asymmetric cryptography is usually implemented by the use of one-way functions. In mathematic terms, these are functions that are easy to compute in one direction but very difficult to compute in reverse. This is what allows you to publish your public key, which is derived from your private key. It is very difficult to work backwards and determine the private key.

The most important properties of public key encryption scheme are –

- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- Each receiver possesses a unique decryption key, generally referred to as his private key.
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the cipher text and the encryption (public) key.
- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

IPSec

Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. IPSec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPSec is based on standards developed by the Internet Engineering Task Force (IETF) IPSec working group.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at the Transport Layer (TLS) and the Application layer (SSH). Hence, only IPsec protects all application traffic over an IP network. Applications can be automatically secured by IPsec at the IP layer.

IPSec protects IP packets by authenticating the packets, by encrypting the packets, or by doing both. IPsec is performed inside the IP module, well below the application layer. Therefore, an Internet

application can take advantage of IPsec while not having to configure itself to use IPsec. When used properly, IPsec is an effective tool in securing network traffic.

IPsec protection involves five main components:

- **Security protocols –** The IP datagram protection mechanisms. The authentication header (AH) signs IP packets and ensures integrity. The content of the datagram is not encrypted, but the receiver is assured that the packet contents have not been altered.
- **Security associations database (SADB) –** The database that associates a security protocol with an IP destination address and an indexing number. The indexing number is called the security parameter index (SPI).
- **Key management –** The generation and distribution of keys for the cryptographic algorithms and for the SPI.
- **Security mechanisms –** The authentication and encryption algorithms that protect the data in the IP datagrams.
- **Security policy database (SPD) –** The database that specifies the level of protection to apply to a packet. The SPD filters IP traffic to determine how the packets should be processed.

Web Security

Web application security is a branch of Information Security that deals specifically with security of websites, web applications and web services. At a high level, Web application security draws on the principles of application security but applies them specifically to Internet and Web systems.

"Web security" is relative and has two components, one internal and one public. Your relative security is high if you have few network resources of financial value, your company and site aren't controversial in any way, your network is set up with tight permissions, your web server is patched up to date with all settings done correctly, your applications on the web server are all patched and updated, and your web site code is done to high standards.

Your web security is relatively lower if your company has financial assets like credit card or identity information, if your web site content is controversial, your servers, applications and site code are complex or old and are maintained by an underfunded or outsourced IT department. All IT departments are budget challenged and tight staffing often creates deferred maintenance issues that play into the hands of any who want to challenge your web security.

It's well known that poorly written software creates security issues. The number of bugs that could create web security issues is directly proportional to the size and complexity of your web applications and web server. Basically, all complex programs either have bugs or at the very, least weaknesses. On top of that, web servers are inherently complex programs. Web sites are themselves complex and intentionally invite ever greater interaction with the public. And so the opportunities for security holes are many and growing.

The world's most secure web server is the one that is turned off. Simple, bare-bones web servers that have few open ports and few services on those ports are the next best thing. Any system with multiple open ports, multiple services and multiple scripting languages is vulnerable simply because it has so many points of entry to watch.
As you know there are a lot of people out there who call themselves hackers. You can also easily guess that they are not all equally skilled. As a matter of fact, the vast majority of them are simply

copycats. They read about a KNOWN technique that was devised by someone else and they use it to break into a site that is interesting to them, often just to see if they can do it. Naturally once they have done that they will take advantage of the site weakness to do malicious harm, plant something or steal something.
A very small number of hackers are actually capable of discovering a new way to overcome web security obstacles. Given the work being done by tens of thousands of programmers worldwide to improve security, it is not easy to discover a brand new method of attack.

There are two roads to accomplish excellent security. On one you would assign all of the resources needed to maintain constant alert to new security issues. You would ensure that all patches and updates are done at once, have all of your existing applications reviewed for correct security, ensure that only security knowledgeable programmers do work on your site and have their work checked carefully by security professionals. You would also maintain a tight firewall, antivirus protection and run IPS/IDS.
Your other option: use a web scanning solution to test your existing equipment, applications and web site code to see if a KNOWN vulnerability actually exists. While firewalls, antivirus and IPS/IDS are all worthwhile, it is simple logic to also lock the front door. It is far more effective to repair half dozen actual risks than it is to leave them in place and try to build higher and higher walls around them. Network and web site vulnerability scanning is the most efficient security investment of all.

Communication Security

Communications security (COMSEC) ensures the security of telecommunications confidentiality and integrity - two information assurance (IA) pillars. Generally, COMSEC may refer to the security of any information that is transmitted, transferred or communicated.
COMSEC is used to protect both classified and unclassified traffic on military communications networks, including voice, video, and data. It is used for both analog and digital applications, and both wired and wireless links.
Communications security includes: crypto security, transmission security, emission security, and physical security of communications security materials and information.

a) **Crypto-security -** The component of communications security that results from the provision of technically sound cryptosystems and their proper use.
b) **Transmission-security** - The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.
c) **Emission security -** The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.
d) **Physical security -** The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.

Network Management

As networks become more complex, in terms of device population, topology and distances, it has been getting more and more important for network administrators to have some easy and convenient way for controlling all pieces of the whole network. Basic features of a network

management system include device information retrieval and device remote control. Former often takes shape of gathering device operation statistics, while latter can be seen in device remote configuration facilities.
For any information to be exchanged between entities, some agreement on information format and transmission procedure needs to be settled beforehand. This is what is conventionally called a **Protocol**. Large networks now days, may host thousands of different devices. To benefit network manager's interoperability and simplicity, any device on the network should carry out most common and important management operations in a well-known, unified way. Therefore, an important feature of a network management system would be a **Convention on management information naming and presentation**.

Sometimes, management operations should be performed on large number of managed devices. For a network manager to complete such a management round in a reasonably short period of time, an important feature of network management software would be **Performance**.
Some of network devices may run on severely limited resources what invokes another property of a proper network management facility: **Low resource consumption**.
In practice, the latter requirement translates into low CPU cycles and memory footprint for management software aboard device being managed.
As networking becomes a more crucial part of our daily lives, security issues have become more apparent. As a side note, even Internet technologies, having military roots, did not pay much attention to security initially. So, the last key feature of network management appears to be **Security**.
Data passed back and forth through the course of management operations should be at least authentic and sometimes hidden from possible observers. All these problems were approached many times through about three decades of networking history. Some solutions collapsed over time for one reason or another, while others, such as Simple Network Management Protocol (SNMP), evolve into an industry standard.

SNMP (Simple Network Management Protocol)

SNMP stands for Simple Network Management Protocol.
It was created in 1988. The purpose of its creation was to manage a growing number of network elements in a computer network. Slowly, this protocol started becoming popular and it forms the basis of network management today. Through SNMP one can retrieve information about network devices like routers, printers, hubs or even normal computers. The information that can be retrieved through SNMP is endless. Some examples of the type of information that can be retrieved through SNMP are:

- System up time
- CPU usage level
- Disk usage level
- Network settings etc.

Not only information can be retrieved but also these network devices can be configured with new values through SNMP Despite being simple in its design and approach, it's the sheer power of this protocol that makes its popular network management protocol today.

A computer network system that uses SNMP for network management consists of the three fundamental components:

- **The SNMP manager**: It is software that usually runs on the machine of network administrator or any human manager managing the computer network.
- **The SNMP agent**: It is software that usually runs on the network node that is to be monitored. This node could be a printer, router etc.
- **The SNMP MIB**: MIB stands for Management information base. This component makes sure that the data exchange between the manager and the agent remains structured.

So we can easily say that the SNMP manager acts as an interface between human network manager and the network node being managed. Similarly, the SNMP agent acts as an interface between the SNMP manager and the network node being monitored.

The Internet Network Management Framework

Contrary to what the name SNMP (Simple Network Management Protocol) might suggest, network management in the Internet is much more than just a protocol for moving management data between a management entity and its agents, and has grown to be more complex than the word "simple" might suggest. The current Internet Standard Management Framework traces its roots back to the Simple Gateway Monitoring Protocol, SGMP [RFC 1028]. That was designed by a group of university network researchers, users, and manager; their experience with SGMP allowed them to design, implement, and deploy SNMP in just a few months.

The framework consists of four parts:

1. **Definitions of *network management objects* known as MIB objects**
   In the Internet network management framework, management information is represented a collection of managed objects that together form a virtual information store, known as the Management Information Base (MIB). A MIB object might be a counter, such as the number of IP datagrams discarded at a router due to errors in an IP datagram header or the number of carrier sense errors in an Ethernet interface, descriptive information such as the server software running on a DNS server; status information such as whether a particular device is functioning correctly or not, or protocol-specific information such as a routing path to a destination.

   MIB objects thus define the management information maintained by a managed node. Related MIB objects are gathered into so-called MIB modules. In our human organization analogy, the MIB defines the information conveyed between the branch office and the main office.

2. ***A data definition language,* known as SMI (Structure of Management Information**)
   This defines the data types, an object model, and rules for writing and revising management information; MIB objects are specified in this data definition language. In our human organizational analogy, the SMI is used to define the details of the format of the information to be exchanged.

3. **A *protocol, SNMP***
   For conveying information and commands between a managing entity and an agent executing on behalf of that entity within a managed network device

4. ***Security and administration capabilities***
   The addition of these capabilities represents the major enhancement in SNMPv3 over SNMPv2.

Some Important Short Questions (Interview Questions)

1. **What protocol is used by DNS name servers?**
   DNS uses UDP for communication between servers. It is a better choice than TCP because of the improved speed a connectionless protocol offers. Of course, transmission reliability suffers with UDP.

2. **What is the difference between interior and exterior neighbor gateways?**
   Interior gateways connect LANs of one organization, whereas exterior gateways connect the organization to the outside world.

3. **What is the HELLO protocol used for?**
   The HELLO protocol uses time instead of distance to determine optimal routing. It is an alternative to the Routing Information Protocol.

4. **What are the advantages and disadvantages of the three types of routing tables?**
   The three types of routing tables are fixed, dynamic, and fixed central. The fixed table must be manually modified every time there is a change. A dynamic table changes its information based on network traffic, reducing the amount of manual maintenance. A fixed central table lets a manager modify only one table, which is then read by other devices. The fixed central table reduces the need to update each machine's table, as with the fixed table. Usually a dynamic table causes the fewest problems for a network administrator, although the table's contents can change without the administrator being aware of the change.

5. **What is source route?**
   It is a sequence of IP addresses identifying the route a datagram must follow. A source route may optionally be included in an IP datagram header.

6. **What is RIP (Routing Information Protocol)?**
   It is a simple protocol used to exchange information between the routers.

7. **What is SLIP (Serial Line Interface Protocol)?**
   It is a very simple protocol used for transmission of IP datagrams across a serial line.

8. **What is Proxy ARP?**
   It is using a router to answer ARP requests. This will be done when the originating host believes that a destination is local, when in fact is lies beyond router.

9. **What is OSPF?**
   It is an Internet routing protocol that scales well, can route traffic along multiple paths, and uses knowledge of the Internet's topology to make accurate routing decisions.

10. **What is Kerberos?**
    It is an authentication service developed at the Massachusetts Institute of Technology. Kerberos uses encryption to prevent intruders from discovering passwords and gaining unauthorized access to the files.

11. **What are 10Base2, 10Base5 and 10BaseT Ethernet LANs?**
    10Base2—An Ethernet term meaning a maximum transfer rate of 10 Megabits per second that uses baseband signaling, with a contiguous cable segment length of 100 meters and a maximum of 2 segments.
    10Base5—An Ethernet term meaning a maximum transfer rate of 10 Megabits per second that uses baseband signaling, with 5 continuous segments not exceeding 100 meters per segment.

10BaseT—An Ethernet term meaning a maximum transfer rate of 10 Megabits per second that uses baseband signaling and twisted pair cabling.

12. **What is the difference between an unspecified passive open and a fully specified passive open, an unspecified passive open has the server waiting for a connection request from a client?**
    A fully specified passive open has the server waiting for a connection from a specific client.

13. **Explain the function of Transmission Control Block?**
    A TCB is a complex data structure that contains a considerable amount of information about each connection.

14. **What is a Management Information Base (MIB)?**
    A Management Information Base is part of every SNMP-managed device. Each SNMP agent has the MIB database that contains information about the device's status, its performance, connections, and configuration. The MIB is queried by SNMP.

15. **What is anonymous FTP and why would you use it?**
    Anonymous FTP enables users to connect to a host without using a valid login and password. Usually, anonymous FTP uses a login called anonymous or guest, with the password usually requesting the user's ID for tracking purposes only. Anonymous FTP is used to enable a large number of users to access files on the host without having to go to the trouble of setting up logins for them all. Anonymous FTP systems usually have strict controls over the areas an anonymous user can access.

16. **What is a pseudo tty?**
    A pseudo tty or false terminal enables external machines to connect through Telnet or rlogin. Without a pseudo tty, no connection can take place.

17. **What does the Mount protocol do?**
    The Mount protocol returns a file handle and the name of the file system in which a requested file resides. The message is sent to the client from the server after reception of a client's request.

18. **What is External Data Representation?**
    External Data Representation is a method of encoding data within an RPC message, used to ensure that the data is not system-dependent.

19. **BOOTP helps a diskless workstation boot. How does it get a message to the network looking for its IP address and the location of its operating system?**
    Boot files BOOTP sends a UDP message with a sub-network broadcast address and waits for a reply from a server that gives it the IP address. The same message might contain the name of the machine that has the boot files on it. If the boot image location is not specified, the workstation sends another UDP message to query the server.

20. **What is a DNS resource record?**
    A resource record is an entry in a name server's database. There are several types of resource records used, including name-to-address resolution information. Resource records are maintained as ASCII files.

21. **What is Mail Gateway?**
    It is a system that performs a protocol translation between different electronic mail delivery protocols.

22. **What is wide-mouth frog?**
    Wide-mouth frog is the simplest known key distribution center (KDC) authentication protocol.

23. What are Digrams and Trigrams?

The most common two letter combinations are called as digrams. e.g. th, in, er, re and an. The most common three letter combinations are called as trigrams. e.g. the, ing, and, and ion.

24. What is silly window syndrome?

It is a problem that can ruin TCP performance. This problem occurs when data are passed to the sending TCP entity in large blocks, but an interactive application on the receiving side reads 1 byte at a time.

25. What is region?

When hierarchical routing is used, the routers are divided into what we call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.

26. What is multicast routing?

Sending a message to a group is called multicasting, and its routing algorithm is called multicast routing.

27. What is traffic shaping?

One of the main causes of congestion is that traffic is often busy. If hosts could be made to transmit at a uniform rate, congestion would be less common. Another open loop method to help manage congestion is forcing the packet to be transmitted at a more predictable rate. This is called traffic shaping.

28. What is packet filter?

Packet filter is a standard router equipped with some extra functionality. The extra functionality allows every incoming or outgoing packet to be inspected. Packets meeting some criterion are forwarded normally. Those that fail the test are dropped.

29. What is virtual path?

Along any transmission path from a given source to a given destination, a group of virtual circuits can be grouped together into what is called path.

30. What is virtual channel?

Virtual channel is normally a connection from one source to one destination, although multicast connections are also permitted. The other name for virtual channel is virtual circuit.

31. What is logical link control?

One of two sub-layers of the data link layer of the OSI reference model, as defined by the IEEE 802 standard; this sub-layer is responsible for maintaining the link between computers when they are sending data across the physical network connection.

32. Why should you care about the OSI Reference Model?

It provides a framework for discussing network operations and design.

33. What is the difference between routable and non- routable protocols?

Routable protocols can work with a router and can be used to build large networks. Non-Routable protocols are designed to work on small, local networks and cannot be used with a router.

34. What is MAU?

In token-ring, hub is called Multi-station Access Unit (MAU).

35. Explain 5-4-3 rule?

In a Ethernet network, between any two points on the network, there can be no more than five network segments or four repeaters, and of those five segments only three of segments can be populated.

36. What is the difference between TFTP and FTP application layer protocols?

The **Trivial File Transfer Protocol (TFTP)** allows a local host to obtain files from a remote host but does not provide reliability or security. It uses the fundamental packet delivery services offered by UDP.

The **File Transfer Protocol (FTP)** is the standard mechanism provided by TCP / IP for copying a file from one host to another. It uses the services offered by TCP and so is reliable and secure. It establishes two connections (virtual circuits) between the hosts, one for data transfer and another for control information.

37. What is the range of addresses in the classes of internet addresses?

Class A 0.0.0.0 - 127.255.255.255
Class B 128.0.0.0 - 191.255.255.255
Class C 192.0.0.0 - 223.255.255.255
Class D 224.0.0.0 - 239.255.255.255
Class E 240.0.0.0 - 247.255.255.255

38. What is the minimum and maximum length of the header in the TCP segment and IP datagram?

The header should have a minimum length of 20 bytes and can have a maximum length of 60 bytes.

39. What is difference between ARP and RARP?

The address resolution protocol (ARP) is used to associate the 32 bit IP address with the 48 bit physical address, used by a host or a router to find the physical address of another host on its network by sending a ARP query packet that includes the IP address of the receiver. The reverse address resolution protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.

40. What is ICMP?

ICMP is Internet Control Message Protocol, a network layer protocol of the TCP/IP suite used by hosts and gateways to send notification of datagram problems back to the sender. It uses the echo test / reply to test whether a destination is reachable and responding. It also handles both control and error messages.

41. What are the data units at different layers of the TCP / IP protocol suite?

The data unit created at the application layer is called a message, at the transport layer the data unit created is called either a segment or an user datagram, at the network layer the data unit created is called the **datagram**, at the data link layer the datagram is encapsulated in to a frame and finally transmitted as signals along the transmission media.

42. What is Project 802?

It is a project started by IEEE to set standards that enable intercommunication between equipment from a variety of manufacturers. It is a way for specifying functions of the physical layer, the data link layer and to some extent the network layer to allow for interconnectivity of major LAN protocols. It consists of the following:

802.1 is an internetworking standard for compatibility of different LANs and MANs across protocols.
802.2 Logical link control (LLC) is the upper sublayer of the data link layer which is non-architecture-specific, that is remains the same for all IEEE-defined LANs. Media access control (MAC) is the lower sublayer of the data link layer that contains some distinct modules each carrying proprietary information specific to the LAN product being used.
The modules are Ethernet LAN (**802.3**), Token ring LAN (**802.4**), Token bus LAN (**802.5**).
802.6 Is distributed queue dual bus (DQDB) designed to be used in MANs?

43. What is Bandwidth?

Every line has an upper limit and a lower limit on the frequency of signals it can carry. This limited range is called the bandwidth.

44. Difference between bit rate and baud rate.

Bit rate is the number of bits transmitted during one second whereas baud rate refers to the number of signal units per second that are required to represent those bits.

Baud rate = bit rate / N where N is no-of-bits represented by each signal shift.

45. What is MAC address?

The address for a device as it is identified at the Media Access Control (MAC) layer in the network architecture. MAC address is usually stored in ROM on the network adapter card and is unique.

46. What is attenuation?

The degeneration of a signal over distance on a network cable is called attenuation.

47. What is cladding?

A layer of a glass that surrounds the center fiber glass inside a fiber-optic cable is called cladding.

48. What is RAID?

A method for providing fault tolerance by using multiple hard disk drives is called RAID.

49. What are NETBIOS and NETBEUI?

NETBIOS is a programming interface that allows I/O requests to be sent to and received from a remote computer and it hides the networking hardware from applications. NETBEUI is NetBIOS extended user interface. These are the transport protocols designed by Microsoft and IBM for the use on small subnets.

50. What is redirector?

Redirector is software that intercepts file or prints I/O requests and translates them into network requests. This comes under presentation layer.

51. What is passive topology?

When the computers on the network simply listen and receive the signal, they are referred to as ***passive*** because they don't amplify the signal in any way. Example for passive topology is linear bus.

52. What are the important topologies for networks?

BUS topology: In this each computer is directly connected to primary network cable in a single line.
Advantages: Inexpensive, easy to install, simple to understand, easy to extend.
STAR topology: In this all computers are connected using a central hub.
Advantages: Can be inexpensive, easy to install and reconfigure and easy to trouble shoot physical problems.
RING topology: In this all computers are connected in loop.
Advantages: All computers have equal access to network media, installation can be simple, and signal does not degrade as much as in other topologies because each computer regenerates it.

53. What are major types of networks and explain.

1. Server-based network
2. Peer-to-peer network

Peer-to-peer network, computers can act as both servers sharing resources and as clients using the resources.

Server-based networks provide centralized control of network resources and rely on server computers to provide security and network administration.

54. What is Protocol Data Unit?

The data unit in the LLC level is called the **protocol data unit (PDU)**. The PDU contains of four fields a destination service access point (DSAP), a source service access point (SSAP), a control field and an information field. DSAP, SSAP are addresses used by the LLC to identify the protocol stacks on the

receiving and sending machines that are generating and using the data. The control field specifies whether the PDU frame is an information frame (I - frame) or a supervisory frame (S - frame) or a unnumbered frame (U - frame).

55. What is difference between baseband and broadband transmission?

In a baseband transmission, the entire bandwidth of the cable is consumed by a single signal. In broadband transmission, signals are sent on multiple frequencies, allowing multiple signals to be sent simultaneously.

56. What are the possible ways of data exchange?

(i) Simplex (ii) Half-duplex (iii) Full-duplex

57. What are the types of Transmission media?

Signals are usually transmitted over some transmission media that are broadly classified in to two categories.

Guided Media: These are wired transmission medium which includes twisted-pair, coaxial cable and fiber-optic cable. A signal traveling along any of these media is directed and is contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic that accept and transport signals in the form of electrical current. Optical fiber is a glass or plastic cable that accepts and transports signals in the form of light.

Unguided Media: This is the wireless media that transport electromagnetic waves without using a physical conductor. Signals are broadcast either through air. This is done through radio communication, satellite communication and cellular telephony.

58. What is point-to-point protocol?

A communications protocol used to connect computers to remote networking services including Internet service providers.

59. What are the two types of transmission technology available?

(i) Broadcast and (ii) point-to-point

60. Difference between the communication and transmission.

Transmission is a physical movement of information and concern issues like bit polarity, synchronization, clock etc. Communication means the meaning full exchange of information between two communication media.

61. Define IP?

Internetwork protocol (IP) is the transmission mechanism used by TCP/IP protocol. It is an unreliable and connectionless datagram protocol. It provides no error checking and tracking.

62. What do you mean by client server model?

In client server model, the client runs a program to request a service and the server runs a program to provide the service. These two programs communicate with each other. One server program can provide services to many client programs.

63. What is the information that a computer attached to a TCP/IP internet must possesses?

Each computer attached to TCP/IP must possesses the following information

- Its IP address
- Its subnet mask
- The IP address of the router.
- The IP address of the name server.

64. What is domain name system (DNS)?

Domain Name System (DNS) is a client server application that identifies each host on the internet with a unique user friendly name.

65. What is TELNET?

TELNET is a client –server application that allows a user to log on to a remote machine, giving the user access to the remote system. TELNET is an abbreviation of terminal Network.

66. What do you mean by local login and remote login?

When a user logs into a local time-sharing system, it is called **local login**. When a user wants to access an application program or utility located on a remote machine, he or she performs **remote login**.

67. What is Network Virtual Terminal?

A universal interface provided by TELNET is called **Network Virtual Terminal (NVT)** character set. Via this interface TELNET translates characters (data or command) that come from local terminal into NVT form and delivers them to the network.

68. What do you mean by Simple Mail Transfer Protocol?

The TCP/IP protocol that supports electronic mail on the internet is called Simple Mail Transfer Protocol. SMTP provides for mail exchange between users on the same or different computer and supports Sending a single message to one or more recipient Sending message that include text, voice, video, or graphics. Sending message to users on network outside the internet

69. What is Hypertext Transfer Protocol (HTTP) ?

It is the main protocol used to access data on the World Wide Web .the protocol transfers data in the form of plain text, hypertext, audio, video, and so on. It is so called because its efficiency allows its use in a hypertext environment where there are rapid jumps from one document to another.

70. What is URL?

It is a standard for specifying any kind of information on the World Wide Web.

71. What is World Wide Web?

World Wide Web is a repository of information spread all over the world and linked together. It is a unique combination of flexibility, portability, and user-friendly features.

The World Wide Web today is a distributed client-server service, in which a client using a browser can access a service using a server. The service provided is distributed over many locations called web sites.

72. What is HTML?

Hypertext Markup Language (HTML) is a language for creating static web pages

73. What do you mean by data communication?

It is the exchange of data between two devices via some form of transmission medium such as wire cable. The communicating system must be part of a communication system made up of a combination of hardware and software.

The effectiveness of a data communication system depends on three fundamental characteristics: delivery, accuracy and timeliness.

74. What is simplex?

It is the mode of communication between two devices in which flow of data is unidirectional. i.e. one can transmit and other can receive.

E.g. keyboard and monitor.

75. What is half-duplex?

It is the mode of communication between two devices in which flow of data is bi-directional but not at the same time. I.e. each station can transmit and receive but not at the same time.

E.g. walkie-talkies are half-duplex system.

76. What is full duplex?

It is the mode of communication between two devices in which flow of data is bi-directional and it occurs simultaneously. Here signals going in either direction share the capacity of the link.

E.g. telephone

77. What is a network?

It is a set of devices connected by communication links. A node can be a computer or any other device capable of sending and/or receiving data generated by other nodes on the network.

78. What is distributed processing?

It is a strategy in which services provided by the network reside at multiple sites.

79. What is point to point connection?

It provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between the two devices

E.g. when we change the TV channels by remote control we establish a point to point connection between remote control and TV control system.

80. What is multipoint connection?

In multipoint connection more than two specific devices share a single link. Here the capacity of the channel is shared either separately or temporally.

81. What is Beaconing?

The process that allows a network to self-repair networks problems is called beaconing. The stations on the network notify the other stations on the ring when they are not receiving the transmissions. Beaconing is used in Token ring and FDDI networks.

82. What is terminal emulation, in which layer it comes?

Telnet is also called as terminal emulation. It belongs to application layer.

83. What is frame relay, in which layer it comes?

Frame relay is a packet switching technology. It will operate in the data link layer.

84. What do you meant by "triple X" in Networks?

The function of **PAD (Packet Assembler Disassembler)** is described in a document known as X.3. The standard protocol has been defined between the terminal and the PAD, called ***X.28***; another standard

protocol exists between hte PAD and the network, called X.29. Together, these three recommendations are often called "triple X".

85. What is SAP?

Series of interface points that allow other computers to communicate with the other layers of network protocol stack.

86. What is subnet?

A generic term for section of a large networks usually separated by a bridge or router.

87. What is Brouter?

Hybrid devices that combine the features of both bridges and routers is called Brouter.\

88. How Gateway is different from Routers?

A gateway operates at the upper levels of the OSI model and translates information between two completely different network architectures or data formats.

89. What are the different types of networking / internetworking devices?

Repeater: Also called a ***regenerator***, it is an electronic device that operates only at physical layer. It receives the signal in the network before it becomes weak, regenerates the original bit pattern and puts the refreshed copy back in to the link.

Bridges: These operate both in the physical and data link layers of LANs of same type. They divide a larger network in to smaller segments. They contain logic that allow them to keep the traffic for each segment separate and thus are repeaters that relay a frame only the side of the segment containing the intended recipient and control congestion.

Routers: They relay packets among multiple interconnected networks (i.e. LANs of different type). They operate in the physical, data link and network layers. They contain software that enables them to determine which of the several possible paths the best for a particular transmission is.

Gateways: They relay packets among networks that have different protocols (e.g. between a LAN and a WAN). They accept a packet formatted for one protocol and convert it to a packet formatted for another protocol before forwarding it. They operate in all seven layers of the OSI model.

90. What is mesh network?

A network in which there are multiple networks links between computers to provide multiple paths for data to travel.

91. What is Crosstalk?

A type of signal interference caused by signals transmitted on one pair of wires bleeding over into the other pairs. Crosstalk can cause network signals to degrade, eventually rendering them unviable.

92. What is ipconfig?

IPconfig is a utility program that is commonly used to identify the addresses information of a computer on a network. It can show the physical address as well as the IP address.

93. What is the difference between a straight-through and crossover cable?

A straight-through cable is used to connect computers to a switch, hub or router. A crossover cable is used to connect two similar devices together, such as a PC to PC or Hub to hub.

94. What is client/server?

Client/server is a type of network wherein one or more computers act as servers. Servers provide a centralized repository of resources such as printers and files. Clients refers to workstation that access the server.

95. What do mean by tunnel mode?

This is a mode of data exchange wherein two communicating computers do not use IPSec themselves. Instead, the gateway that is connecting their LANs to the transit network creates a virtual tunnel that uses the IPSec protocol to secure all communication that passes through it.

96. What is sneakernet?

sneakernet is believed to be the earliest form of networking wherein data is physically transported using removable media, such as disk, tapes.

97. What is one basic requirement for establishing VLANs?

A VLAN is required because at switch level there is only one broadcast domain, it means whenever new user is connected to switch this information is spread throughout the network. VLAN on switch helps to create separate broadcast domain at switch level. It is used for security purpose.

98. What is IPv6?

IPv6, or Internet Protocol version 6, was developed to replace IPv4. At present, IPv4 is being used to control internet traffic, but is expected to get saturated in the near future. IPv6 was designed to overcome this limitation.

99. What is RSA algorithm?

RSA is short for Rivest-Shamir-Adleman algorithm. It is the most commonly used public key encryption algorithm in use today.

100. What is piggybacking?

Piggybacking is a bi-directional data transmission technique in the network layer (OSI model). It makes the most of the sent data frames from receiver to emitter, adding the confirmation that the data frame sent by the sender was received successfully (ACK acknowledge). This practically means that, instead of sending an acknowledgement in an individual frame it is piggy-backed on the data frame.

101. What is difference between baseband and broadband transmission?

In a baseband transmission, the entire bandwidth of the cable is consumed by a single signal. In broadband transmission, signals are sent on multiple frequencies, allowing multiple signals to be sent simultaneously.

"Computers are good at following instructions, but not at reading your mind."

— Donald Knuth

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards."

— Gene Spafford

"Man is a slow, sloppy, and brilliant thinker; computers are fast, accurate, and stupid."

— John Pfeiffer

Lab Guide

Network Cabling and LAN Setup

What is RJ45 Connector?

A registered jack (RJ) is a standardized physical network interface for connecting telecommunications or data equipment. The physical connectors that registered jacks use are mainly of the modular connector and 50-pin miniature ribbon connector types. The most common twisted-pair connector is an 8-position, 8-contact (8P8C) modular plug and jack commonly referred to as an RJ45 connector.

- An 8-pin/8-position plug or jack is commonly used to connect computers onto Ethernet-based local area networks (LAN).
- Two wiring schemes–T568A and T568B–are used to terminate the twisted-pair cable onto the connector interface.

Difference between RJ45 and RJ11

RJ45 and RJ11 are two commonly used jacks, but people often mixed them together because of their similar appearances. The biggest difference between them is that they are used for different applications. RJ45 is applied to networking while RJ11 is applied to telephone sets. Another difference is the number of wires in their connectors. From the previous introduction, we know that RJ45 connector has eight wires. But unlike RJ45, RJ11 has only four wires so that its size is also smaller than RJ45 connector.

RJ45 Network Interface Cards

Network interface card, or the network controller, is used to provide an electrical interface for the computer to the network and completely complies with the Ethernet standards. A proper termination is needed for connecting the LAN (local area network) media and the proper motherboard. Typically, cat 6 cable is terminated with an RJ45 modular plug, so its network interface card must have an RJ45 modular jack that matches with the patch cable.

The Major Categories of Ethernet Cables

	Cable Type	Maximum Data Transmission Speed	Maximum Bandwidth
Category 3	UTP	10 Mbps	16 MHz
Category 5	UTP	10/100 Mbps	100 MHz
Category 5 e	UTP	1000 Mbps	100 MHz
Category 6	UTP or STP	1000 Mbps	250 MHz
Category 6 a	STP	10,000 Mbps	500 MHz
Category 7	SSTP	10,000 Mbps	600 MHz

Crossover and Straight through Cable

If you have only two computers (desktop PCs or laptops) and both computers have either built-in or additional Ethernet network adapters, you can connect both computers directly using a crossover cable. Crossover cable is an Ethernet cable (Cat 5, Cat 5e or Cat 6) that has pins 1, 2, 3, 6 on one end crossed to pins 3, 6, 1, 2 on the other end respectively. Like standard (straight-through) Ethernet cable, crossover cable is also terminated with RJ-45 connectors.

Please note, if one of your computers has an auto-crossover (a.k.a. auto-switching or auto-MDI/MDIX) Ethernet port, you can connect them using either crossover or straight-through cable. Most Gigabit Ethernet (10/100/1000BaseT) adapters have auto MDI/MDIX function. Therefore, if you have it installed in one computer, you can connect it with other computer using a standard Ethernet cable.

The direct Ethernet connection works like an Ethernet network that is equipped with Ethernet hardware, i.e. hub, switch, or router. It can be used to share files, folders, drives, printers, and peripherals. It can also be used to share an Internet connection or play a networked game.

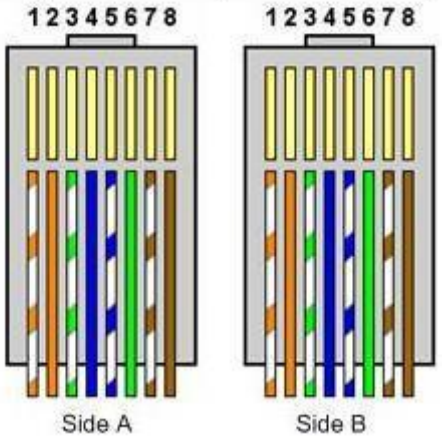
Most consumer Ethernet adapters in use today are Fast Ethernet (10/100BaseT) with autosensing which means the direct Ethernet connection can switch from/to 10 Mbps or 100 Mbps link speed depending on line condition. Therefore, a direct connection between two computers using Ethernet crossover cable is faster than using either serial or parallel cable. Moreover, Ethernet cable can reach longer distance (up to 100 meters) without repeater and you don't need to buy additional software to configure the direct connection.

Straight Cable

You usually use straight cable to connect different type of devices. This type of cable will be used most of the time and can be used to:

1) Connect a computer to a switch/hub's normal port.
2) Connect a computer to a cable/DSL modem's LAN port.
3) Connect a router's WAN port to a cable/DSL modem's LAN port.
4) Connect a router's LAN port to a switch/hub's uplink port. (normally used for expanding network)
5) Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.

Pin ID	Side A	Side B
1	Orange-white	Orange-white
2	Orange	Orange
3	Green-white	Green-white
4	Blue	Blue
5	Blue-white	Blue-white
6	Green	Green
7	Brown-white	Brown-white
8	Brown	Brown



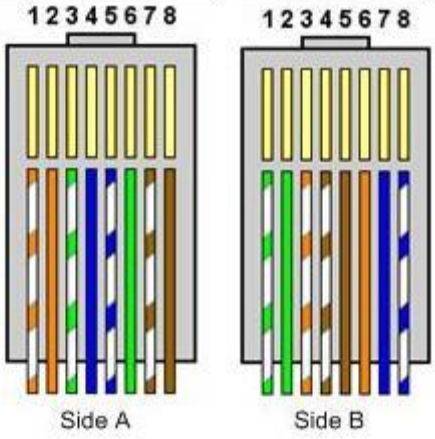
If you need to check how straight cable looks like, it's easy. Both sides (side A and side B) of cable have wire arrangement with same color. Check out different types of straight cable that are available in the market here.

Crossover Cable

Sometimes you will use crossover cable, it's usually used to connect same type of devices. A crossover cable can be used to:

1) Connect 2 computers directly.
2) Connect a router's LAN port to a switch/hub's normal port. (normally used for expanding network)
3) Connect 2 switches/hubs by using normal port in both switches/hubs.

Pin ID	side A	side B
1	Orange-white	green-white
2	Orange	green
3	green-white	orange-white
4	blue	brown-white
5	blue-white	Brown
6	green	orange
7	brown-white	Blue
8	brown	blue-white



In you need to check how crossover cable looks like, both side (side A and side B) of cable have wire arrangement with following different color.

Summary

	Hub	Switch	Router	Workstation
Hub	Crossover	Crossover	Straight	Straight
Switch	Crossover	Crossover	Straight	Straight
Router	Straight	Straight	Crossover	Crossover
Workstation	Straight	Straight	Crossover	Crossover

Basic Commands and Tools used for Networking in Windows

If you're planning on pursuing a field in networking or just looking to expand your networking knowledge; you must know some basic networking terms. Tools like ping, traceroute, lookup, whois, finger, netstat, ipconfig, and port scanners are available on nearly every operating system you can get your hands on. They're used for everything from troubleshooting a connection to looking up information. There are some things you can only do from the command line, even on Windows. Some of these tools don't have graphical equivalents, while others are just plain faster to use than their graphical interfaces.

1. Ping

The PING utility tests connectivity between two hosts. PING uses a special protocol called the Internet Control Message Protocol (ICMP) to determine whether the remote machine (website, server, etc.) can receive the test packet and reply.
Also a great way to verify whether you have TCP/IP installed and your Network Card is working.
We'll start by Pinging the loopback address (127.0.0.1) to verify that TCP/IP is installed and configured correctly on the local computer.
Type: **PING 127.0.0.1**
These packets ask the remote destination to reply. If the remote destination is configured to reply, it will respond with packets of its own. You'll be able to see how long the round-trip time is between your computer and the destination. You'll see a "request timed out" message if packet loss is occurring, and you'll see an error message if your computer can't communicate with the remote host at all.
This tool can help you troubleshoot Internet connection problems, but bear in mind that many servers and devices are configured not to reply to pings.

2. Tracert

Tracert is very similar to Ping, except that Tracert identifies pathways taken along each hop, rather than the time it takes for each packet to return (ping).
If I have trouble connecting to a remote host I will use Tracert to see where that connection fails. Any information sent from a source computer must travel through many computers / servers / routers (they're all the same thing, essentially) before it reaches a destination.
It may not be your computer but something that is down along the way. It can also tell you if communication is slow because a link has gone down between you and the destination.
For example, run **tracert google.com** and you'll see the path your packet takes to reach Google. If you're having issues connecting to a website, tracert can show you where the problem is occurring.

3. ARP

The ARP utility helps diagnose problems associated with the Address Resolution Protocol (ARP).
TCP/IP hosts use ARP to determine the physical (MAC) address that corresponds with a specific IP address. Type **arp** with the **– a** option to display IP addresses that have been resolved to MAC addresses recently.

4. ipconfig/ifconfig

The ipconfig command is used on Windows, while the ifconfig command is used on Linux, Mac OS X, and other Unix-like operating systems. These commands allow you to configure your network interfaces and view information about them.

For example, you can use the ipconfig /all command on Windows to view your entire configured network interfaces, their IP addresses, DNS servers, and other information. Or, you can use the ipconfig /flushdns command to flush your DNS cache, forcing Windows to get new addresses from its DNS servers every time you contact a new hostname. Other commands can force your computer to release its IP address and get a new one from its DHCP server. This utility can quickly display your computer's IP address or help you troubleshoot problems.
ipconfig /all will give you more detailed information.

Through **ipconfig /all** we can find DNS severs, if we have DHCP enabled, MAC Address, along with other helpful information. Other IPConfig tools that are helpful include **ipconfig /release** and **ipconfig /renew**. But before I get into this let's discuss how we actually get an IP Address.

5. Nbtstat

Nbtstat (NetBios over TCP/IP) enables you to check information about NetBios names.
It helps us view the NetBios name cache (nbtstat -c) which shows the NetBios names and the corresponding IP address that has been resolved (nbtstat -r) by a particular host as well as the names that have been registered by the local system (nbtstat –n).

6. NSLookup

NSLookup provides a command-line utility for diagnosing DNS problems. In its most basic usage, NSLookup returns the IP address with the matching host name.
The nslookup command will look up the IP addresses associated with a domain name. For example, you can run **nslookup howtogeek.com** to see the IP address of How-To Geek's server.

7. Whois

The whois command looks up the registration record associated with a domain name. This can show you more information about who registered and owns a domain name, including their contact information.
This command isn't included with Windows itself, but Microsoft's Windows Sysinternals provides a Whois tool you can download. This information is also available from many websites that can perform whois lookups for you.

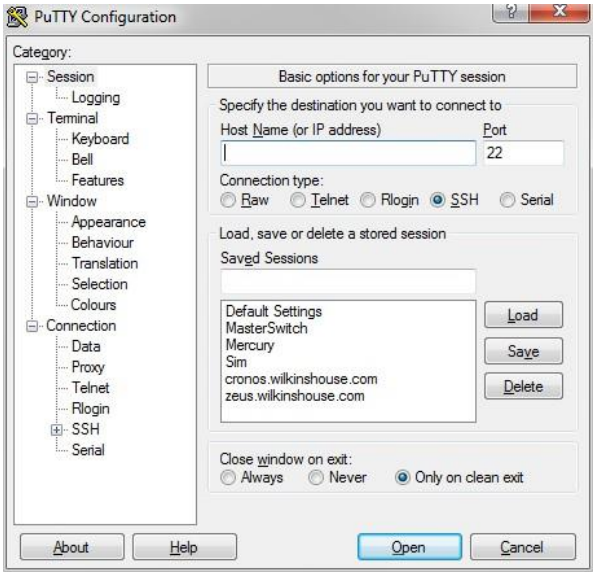
8. netstat

netstat stands for network statistics. This command displays incoming and outgoing network connections as well as other network information. It's available on Windows, Mac, and Linux — each version has its own command-line options you can tweak to see different types of information.

The netstat utility can show you the open connections on your computer, which programs are making which connections, how much data is being transmitted, and other information.

9. PuTTY/Tera Term

When connecting to a variety of different types of equipment, a telnet, SSH or serial client is required; when this is required both the puTTY and Tera Term programs are able to provide these functionalities. The selection of one over the other is strictly a personal preference. Figures 6 and 7 below show both puTTY and Tera Term being used to connect to a host via SSH.



10. Subnet and IP Calculator

One of the most important tools in the belt of a junior network engineer is an IP network calculator. These can be used to unsure a correct IP address selection and with this a correct IP address configuration. While this type of tool is used by senior level network engineers, much of the information obtained from the tool becomes simpler to calculate the longer and more experience you have in the field. Two of the more commonly used free IP calculators include Wildpackets (Bitcricket) Network Calculator and Solarwinds Advanced Subnet Calculator.

11. Telnet

Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

In the Windows Features window, check the Telnet Client option, press OK and wait for it to be installed. When done, press Close. There is no need to restart your computer.

Team Viewer

TeamViewer is a proprietary computer software package for remote control, desktop sharing, online meetings, web conferencing and file transfer between computers.
The TeamViewer software application allows for remote control, desktop sharing and file transfer between computers. TeamViewer is compatible with multiple platforms, including Windows, Mac OS X, Linux, iOS, and Android. TeamViewer allows a user to access another computer remotely using a web browser.
TeamViewer was founded in Uhingen, Germany in 2005. It is designed to work either by installing it on a computer or running a "Quick Support" version that does not require installation. While installation is not required, TeamViewer does need to be running on the computers for remote access and control to work. The software uses RSA key exchange and AES (256-bit) session encoding to provide a secure connection.

These are major benefits

- Easy to use, no configuration necessary
- All-In-One solution for on-demand remote support, remote access, and more
- Unlimited remote computers
- Easy file transfer, remote printing, Wake-on-LAN, and many other features at no extra cost, multi-platform software for Windows, Mac, and Linux
- The highest security standards
- Excellent customer support

Traffic Analyzer

Network traffic analysis is the process of recording, reviewing and analyzing network traffic for the purpose of performance, security and/or general network operations and management.
A network analyzer (also called a protocol analyzer or packet analyzer) is a combination of hardware and programming, or in some cases a stand-alone hardware device, that can be installed in a computer or network to enhance protection against malicious activity. Network analyzers can supplement firewalls, anti-virus programs, and spyware detection programs.

Network analyzers can:

1. Provide detailed statistics for current and recent activity on thenetwork.
2. Test anti-malware programs and pinpoint potential vulnerabilities
3. Detect unusual levels of network traffic.
4. Detect unusual packet characteristics.
5. Identify packet sources or destinations.
6. Configure alarms for defined threats.
7. Search for specific data strings in packets.
8. Monitor bandwidth utilization as a function of time.
9. Create application-specific plug-ins.
10. Display all statistics on a user-friendly control panel.

Network analyzers are not intended to replace firewalls, anti-virus programs, or spyware detection programs. However, the use of a network analyzer in addition to other countermeasures can minimize the probability that an attack will occur, and can facilitate rapid response in the event an attack begins.

C CODE FOR BIT STUFFING

```
#include<stdio.h>
#include<conio.h>
void ins(char,int);
void del(int);
char fr[50];
main()
{
int i,cnt=0;
clrscr();
printf("Enter the frame:\t");
gets(fr);
for(i=0;i<strlen(fr);i++)
{
if(fr[i]!='0'&&fr[i]!='1')
{
printf("ivalid input\n press any key to exit");
getch();
exit(0);
}
}
/*Stuffing the given bit*/
for(i=0;i<strlen(fr);i++)
{
if(cnt==5)
{
cnt=0;
ins('0',i);
}
if(fr[i]=='1'){cnt+=1;}else{cnt=0;}
}
printf("\n\nStuffed Frame is \t%s\n\n",fr);
getch();
/*Destuffing of aframe*/
cnt=0;
for(i=0;i<strlen(fr);i++)
{
if(cnt==5)
{
cnt=0;
del(i);
}
if(fr[i]=='1'){cnt+=1;}else{cnt=0;}
}
printf("Destuffed Frame is \t%s",fr);
getch();
return 0;
}
void ins(char in,int p)
{
char dup[50];
int i;
strcpy(dup,fr);
fr[p]=in;
for(i=p+1;i<strlen(fr)+1;i++)
{
fr[i]=dup[i-1];
}
}
void del(int q)
{
int i;
for(i=q;i<strlen(fr);i++)
{
fr[i]=fr[i+1];
}
}
```

PROGRAM FOR CYCLIC REDUNDENCY CHECK

```
#include<stdio.h>
#include<conio.h>
int gen[4],genl,frl,rem[4];
void main()
{
int i,j,fr[8],dupfr[11],recfr[11],tlen,flag;
clrscr();
frl=8; genl=4;
printf("enter frame:");
for(i=0;i<frl;i++)
{
scanf("%d",&fr[i]);
dupfr[i]=fr[i];
}
printf("enter generator:");
for(i=0;i<genl;i++)
scanf("%d",&gen[i]);
tlen=frl+genl-1;
```

```
for(i=frl;i<tlen;i++)
{
dupfr[i]=0;
}
remainder(dupfr);
for(i=0;i<frl;i++)
{
recfr[i]=fr[i];
}
for(i=frl,j=1;j<genl;i++,j++)
{
recfr[i]=rem[j];
}
remainder(recfr);
flag=0;
for(i=0;i<4;i++)
{
if(rem[i]!=0)
flag++;
}
if(flag==0)
{
printf("frame received correctly");
}
else
{
printf("the received frame is wrong");
}
getch();
}
remainder(int fr[])
{
int k,k1,i,j;
for(k=0;k<frl;k++)
{
if(fr[k]==1)
{
k1=k;
for(i=0,j=k;i<genl;i++,j++)
{
rem[i]=fr[j]^gen[i];
}
for(i=0;i<genl;i++)
{
fr[k1]=rem[i];
k1++;
}
}
}
}
```

C CODE FOR DISTANCE VECTOR ROUTING

```
#include<stdio.h>
#include<conio.h>
#include<string.h>
main()
{
char c1[]={'A','I','H','K','\0'};
char
c2[]={'A','B','C','D','E','F','G','H','I','J','K','L'};
int doj[]={8,10,12,6};
int i,j,min,delay[5][12],res,k=0,l=0,pre[5];
clrscr();
for(i=0;i<4;i++)
{
for(j=0;j<12;j++)
{
printf("\nenter delay from %c to
%c",c1[i],c2[i]);
scanf("%d",&delay[i][j]);
}
}
min=1000;
for(j=0;j<12;j++)
{
for(i=0;i<4;i++)
{
res=delay[i][j]+doj[i];
if(res<min)
{
min=res;
k=i;
}
}
delay[4][j]=min;
pre[l++]=k;
min=1000;
}
clrscr();
for(i=0;i<12;i++)
```

```
{
if(i==9)
delay[4][j]=0;
printf("\nDelay from j to %c is
%d",c2[i],delay[4][j]);
if(i!=9)
printf("\t by the mode %c",c1[pre[i]]);
else
printf("\t by the node");
}
getch();
}
```

C CODE FOR SHORTEST PATH ROUTING (Dijkstra's Algorithm)

```
 #include<stdio.h>
#include<string.h>
main()
{
int
n,ds[30][30],s,d,pr[30],ln[30],st[30],pt[30],i,j,u
,mn=10000;
clrscr();
printf("\n enter the no of nodes");
scanf("%d",&n);
for(i=0;i<n;i++)
{
for(j=0;j<n;j++)
{
printf("\nenter the weight from node %d to
%d ",(i+1),(j+1));
scanf("%d",&ds[i][j]);
}
st[i]=0;
ln[i]=10000;
pr[i]=-1;
}
printf("enter the source and destination
nodes ");
scanf("%d %d",&s,&d);
s--;
d--;
u=s;
ln[u]=0;
pr[u]=-1;
st[u]=2;
do
{
for(i=0;i<n;i++)
{
if(ds[u][i]!=0 && st[i]!=2)
{
st[i]=1;
if((ln[u]+ds[u][i])<ln[i])
{
pr[i]=u;
ln[i]=ln[u]+ds[u][i];
}
}
}
mn=10000;
for(i=0;i<n;i++)
if(st[i]==1 && ln[i]<mn )
{
mn=ln[i];
u=i;
}
}while(u!=d);
i=0;
u=d;
do
{
pt[i]=u;
i++;
u=pr[u];
}while(u>=0);
pt[i]='\0';
s++;
d++;
printf("\n the shortest from %d to %d is
%d",s,d,ln[d-1]);
printf("\npath is ");
for(u=i-1;u>=0;u--)
printf("\t %d ",(pt[u]+1));
getch();
}
```

C Program for Character Count

```
#include<stdio.h>
#include<string.h>
char input[10][20];
int get_input();
void make_frames(int);
int count_chars(int s);
void main()
{
        int no_of_words=get_input();
        make_frames(no_of_words);
}
int get_input()
{
        int answer;
        int i=0;
        do{
        printf("\nEnter the Word:");
        scanf("%s",input[i]);
        fflush(stdin);
printf("\nDo you want to continue:
(y: 1/n: 0)?:");
        scanf("%d",&answer);
        i++;
        }while(answer!=0);
        return i;
}
void make_frames(int num_words)
{
        int i=0;
printf("\nThe Transmitted Data is:\n\t")
for(;i<num_words;i++)
printf("%d%s",(count_chars(i)+1),input[i]);
printf("\n\n");
}
int count_chars(int index)
{
        int i=0;
        while(input[index][i]!='\0')
                i++;
        return i;
}
```

"If you can't explain it simply, you don't understand it well enough."

– Albert Einstein