COMPUTER NETWORKS

A computer network refers to the interconnection of computers using cables or wireless technologies. Computers may be connected to other terminals by telecommunication devices.

Benefits of using computer networks

1. They ensure that data is transmitted to various destinations efficiently.
2. Through the use of passwords and other data protection techniques, network ensures that the organizations data is protected from unauthorized access.
3. Since many organizations are now using client-server networks, networks ensure easy control of organizations activities.
4. Networks ensure sharing of resources such as data, hardware and software in an organization e.g. a printer can be locally installed on the server computer then it can be shared by the network administrator so that users or clients can access it from remote locations.
5. Networks ensure that the organizations operation overheads are minimized for example an organization that uses a client-server network, does not need to employ supervisors to monitor user activities since this is done by the events log file on the server.

Disadvantages of computer networks

1. The initial cost of setting up a network is high due to the high costs of server hardware and software.
2. Computer viruses spread fast in network environments compared to stand-alone environments.
3. Unless strict control measures are put in place, data can easily be hacked or accessed by unauthorized persons.
4. When the server fails, the network users will be forced to work offline and when the connectivity device fails the network will be completely disabled.

Factors to consider when evaluating computer networks

Throughput

This refers to the volume of data that can be transmitted by network media over a given period of time. A good network should support high volume of data transmission.

Cost

The organization should consider the overall cost of the network which includes the cost of planning, the cost of administration, the cost of cabling, the cost of network software and the cost of telecommunication devices that support connectivity. A good network should be cost effective.

Response time

This refers to how long it takes a network especially the central computer to respond to user requests. A good network should support fast response times.

Flexibility

It refers to the capability of network to support different structures or architecture and to allow for expansion with reference to technological changes and changes in clear requirements.

Reliability

It refers to the ability of a network to efficiently transmit messages from terminal to terminal. It also refers to the capability of network to work for a long period without failure.

Security

This is the capability of a network to protect the organizations data from unauthorized users. A good network should have inbuilt controls that prevent unauthorized access to its resources.

TYPES OF COMPUTER NETWORKS

The two major types of networks are Local area Networks and Wide area networks

Local Area Network (LANs)

LAN is a telecommunication System or a network that is capable of interconnecting a large number of computers, terminals and other peripheral devices within a limited geographical area. LANs supports local and remote accessibility to data. They majorly use wired transmission media hence they have high transmission speed.

A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or as many as thousands of users. The bandwidth in LAN is very high. Network bandwidth is a measure of the data transfer rate or capacity of a given network.

WAN (Wide Area Networks)

A wide area network (WAN) is a telecommunication network. It is a LAN of LANs or Network of Networks. WANs connect LANs that may be on opposite sides of a building, across the country or around the world. WANS are characterized by the slowest data communication rates and the largest distances. They are supported mostly by wireless technologies. WAN bandwidth is quite limited.

MAN (Metropolitan Area Networks)

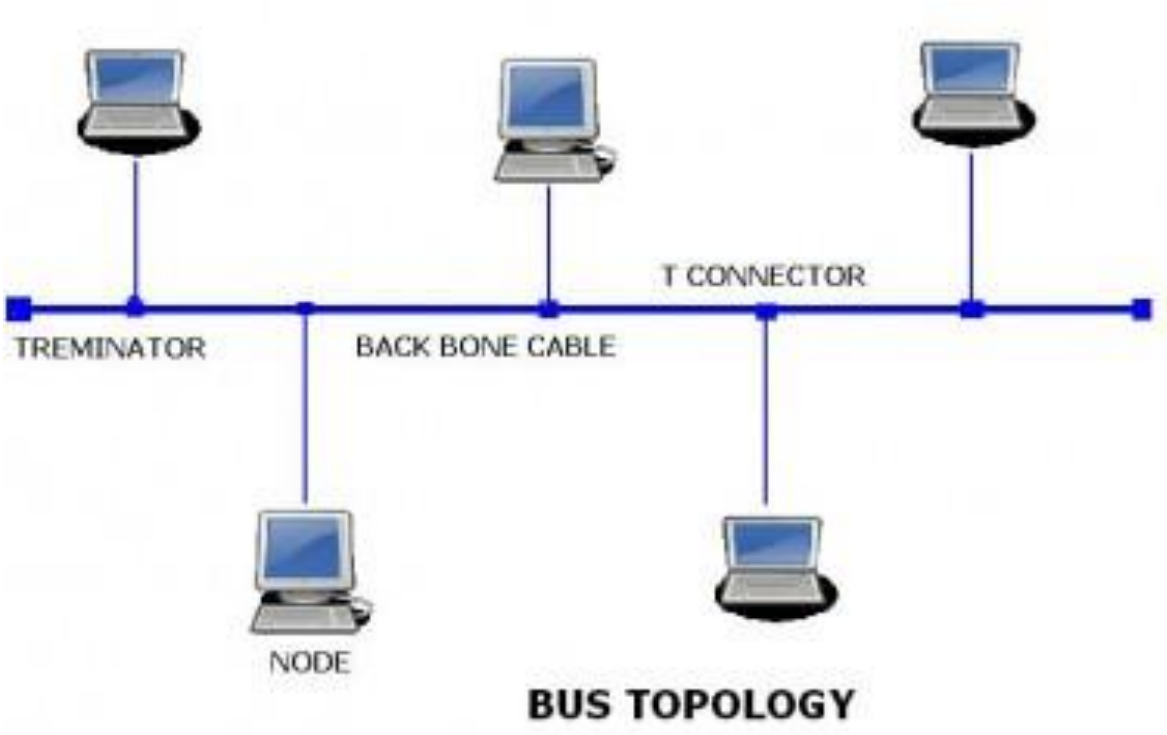
MAN is larger than a local area network and as its name implies covers the area of a single city. MANs rarely extend beyond 100 KM and frequently comprise a combination of different hardware and transmission media. It can be single network such as a cable TV network or it is a means of connecting a number of LANs into a larger network so that resources can be shared LAN to LAN as well as device to device.

LAN TOPOLOGIES

Physical topology refers to the arrangement of computers, cables and other components on a network. Logical topology describes the way data flows through the network components. Two networks have the same topology if the connection configuration is the same, although the networks may differ in physical interconnections, distances between nodes, transmission rates, and/or signal types.

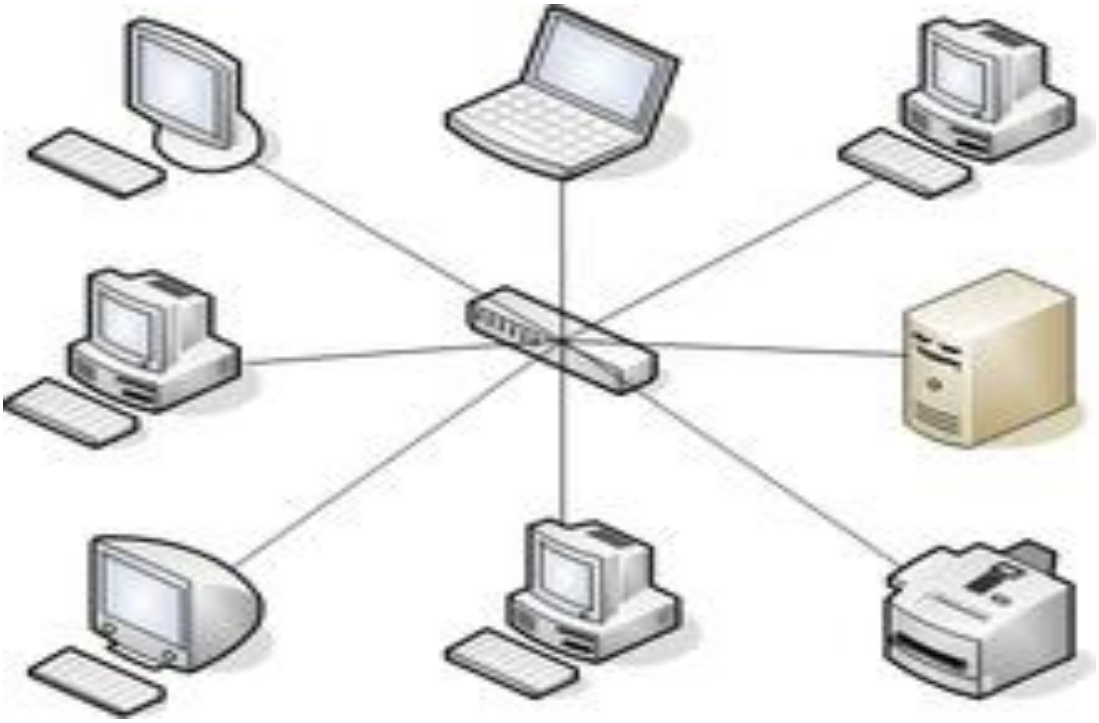
Bus topology

- In this topology all the network computers are connected using a single cable or bus that connects the computers in a straight line.
- Commonly referred to as **straight line topology**, it involves the transmission of a packet to all network nodes on the segment. Because of the way electrical signals are transmitted over this cable, the ends of the cable must be terminated by hardware devices called terminators to prevent signal bounce.
- If there is a break anywhere in the cable or if the ends of the cable are not terminated then, the signal will not flow to its designated point.
- The number of computers attached to the bus is directly proportional to network performance i.e. as the number of computer increase; the response time of network reduces.
- Bus networks are however, cheap and simple to install.



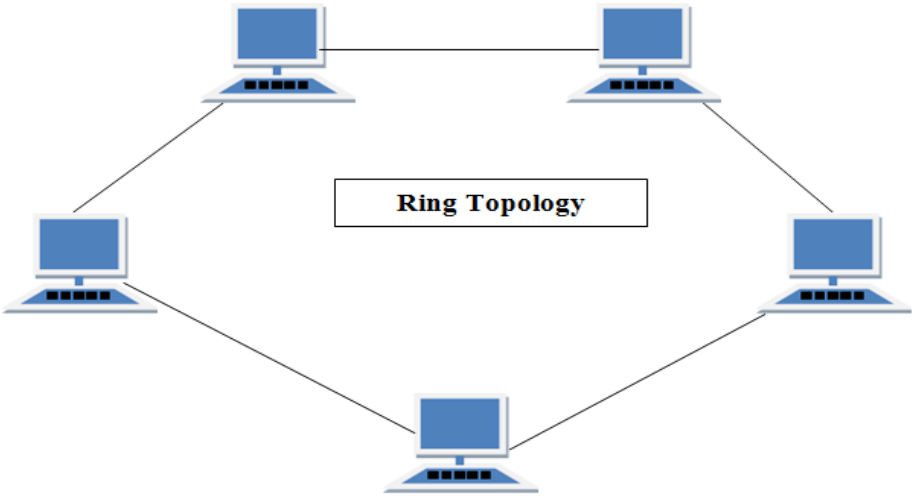
Star topology

- Star topology is the most common type of network topology that is used in homes and offices. In the Star topology there is a central connection point called the hub or switch.
- In contrast to the bus topology, the star topology allows each machine on the network to have a point to point connection to the central hub.
- A Star network topology is very easy to manage because of its simplicity in functionality.
  The problems can be easily located logically in a Star topology and therefore is easy to troubleshoot
- The Star topology is very simple in format so it is very easy to expand on the network.
- The Star topology is fully dependent on the hub or switch. If there are many nodes and the cable is long then the network may slow down.



Ring topology

- Computers are connected to a ring structure which is made of fiber optic cables and each packet is sent around the ring until it reaches its final destination (using broadcast method)
- It can handle high noise environment better than both the bus and star topologies.
- The impact of noise and EMI (Electromagnetic interference) is reduced.
- Ring topologies are relatively expensive to setup (due to cost of fiber optic cable) and only one computer at a time can send data.
- Ring topology is not dependent on a host computer.
- The need for complicated control software increases the cost of setting up the ring topology.

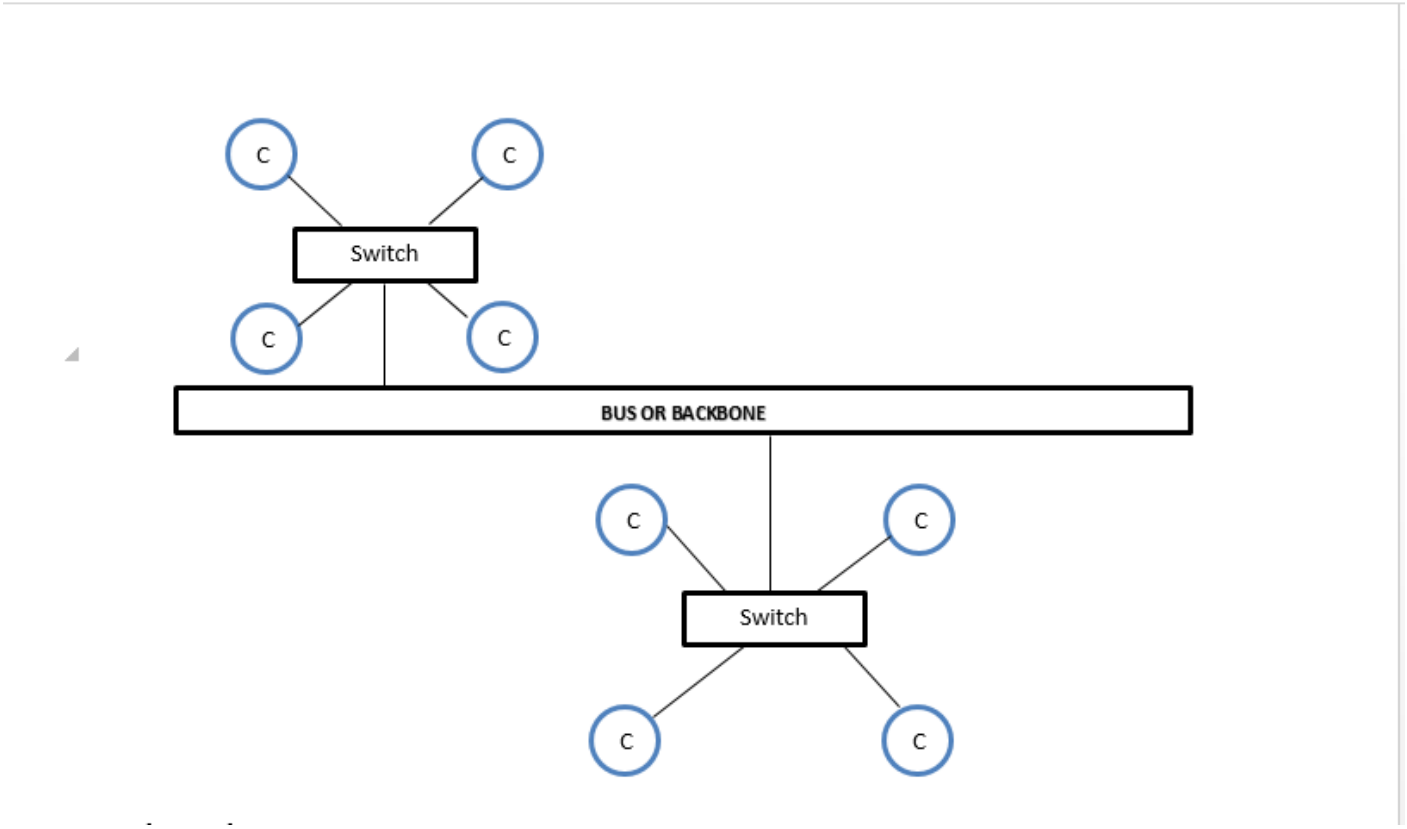


Hybrid topology

- It uses a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example, a tree network connected to a tree network is still a tree network topology. A hybrid topology is always produced when two

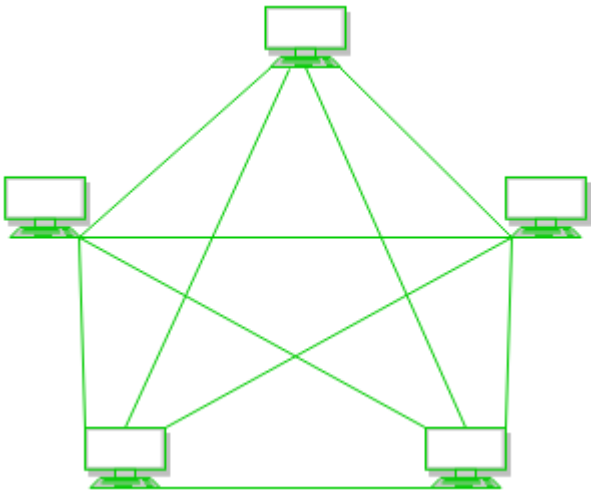
different basic network topologies are connected. Two common examples for Hybrid networks are *star-ring network* and *star bus network*

- ***A Star-ring network*** consists of two or more star topologies connected using a multi-station access unit (MAU) as a centralized hub.
- ***A Star-bus network*** consists of two or more star topologies connected using a bus trunk (the bus trunk serves as the network's backbone) as shown below



Mesh topology

- Mesh network or topology is a network where all the nodes are connected to each other and is a complete network.
- This topology incorporates a unique network design in which each computer on the network connects to every other, creating a point-to-point connection between every device on the network.
- The purpose of the mesh design is to provide a high level of redundancy. If one network cable fails, the data always has an alternative path to get to its destination.



REFERENCE MODELS IN COMMUNICATION NETWORKS

LAYERED NETWORK ARCHITECTURE

To reduce the design complexity, most of the networks are organized as a series of layers or levels, each one built upon one below it.

The basic idea of a layered architecture is to divide the design into small pieces. Each layer adds to the services provided by the lower layers in such a manner that the highest layer is provided a full set of services to manage communications and run the applications.

The benefits of the layered models are ***modularity*** and ***clear interfaces***, i.e. open architecture and comparability between the different providers' components. A basic principle is to ensure independence of layers by defining services provided by each layer to the next higher layer without defining how the services are to be performed. This permits changes in a layer without affecting other layers.

The basic elements of a layered model are **services, protocols and interfaces**.

A ***service*** is a set of actions that a layer offers to another (higher) layer.

Protocol is a set of rules that a layer uses to exchange information with a peer entity. These rules concern both the contents and the order of the messages used.

Interfaces support the sending of messages from one layer to another.

In an ***n-layer*** architecture, layer ***n*** on one machine carries on conversation with the layer ***n*** on other machine. The rules and conventions used in this conversation are collectively known as the ***layer-n protocol***. A protocol is an agreement between the communicating parties on how communication is to proceed.

REFERENCE MODELS.

A reference model is a conceptual framework for understanding relationships. Communication reference models aim to allow engineers to classify all of the necessary tasks of any network communication objective.

The most important reference models are

1. OSI reference model.
2. TCP/IP reference model.

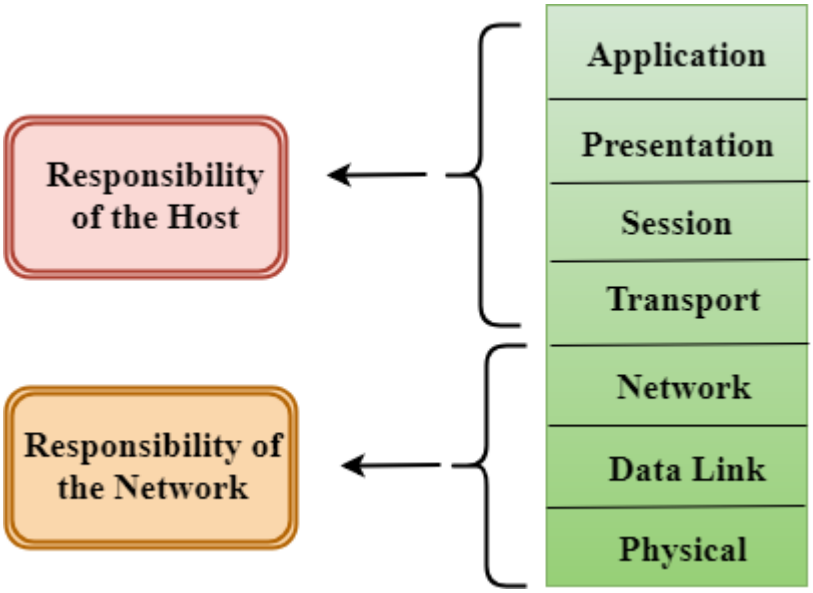
OSI Reference Model

There are many users who use computer network and are located all over the world. To ensure national and worldwide data communication ISO (International Organization of Standardization) developed this model. This is called a model for open system interconnection (OSI) and is normally called as OSI model.

The OSI model is divided into two layers namely the upper layers and lower layers.

The ***lower layers*** comprise of network, data link and physical layers while the ***upper layers*** comprises of the transport, session, presentation and application layers.

The seven layers of the OSI model are as shown below.



THE OSI MODEL

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other. To this effect, ISO has developed a standard.

ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system.

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Data link Layer
7. Physical Layer

Features of OSI Model

1. Big picture of communication over network is understandable through this OSI model.
2. It describes how hardware and software work together.
3. It facilitates the understanding of new technologies as they emerge.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

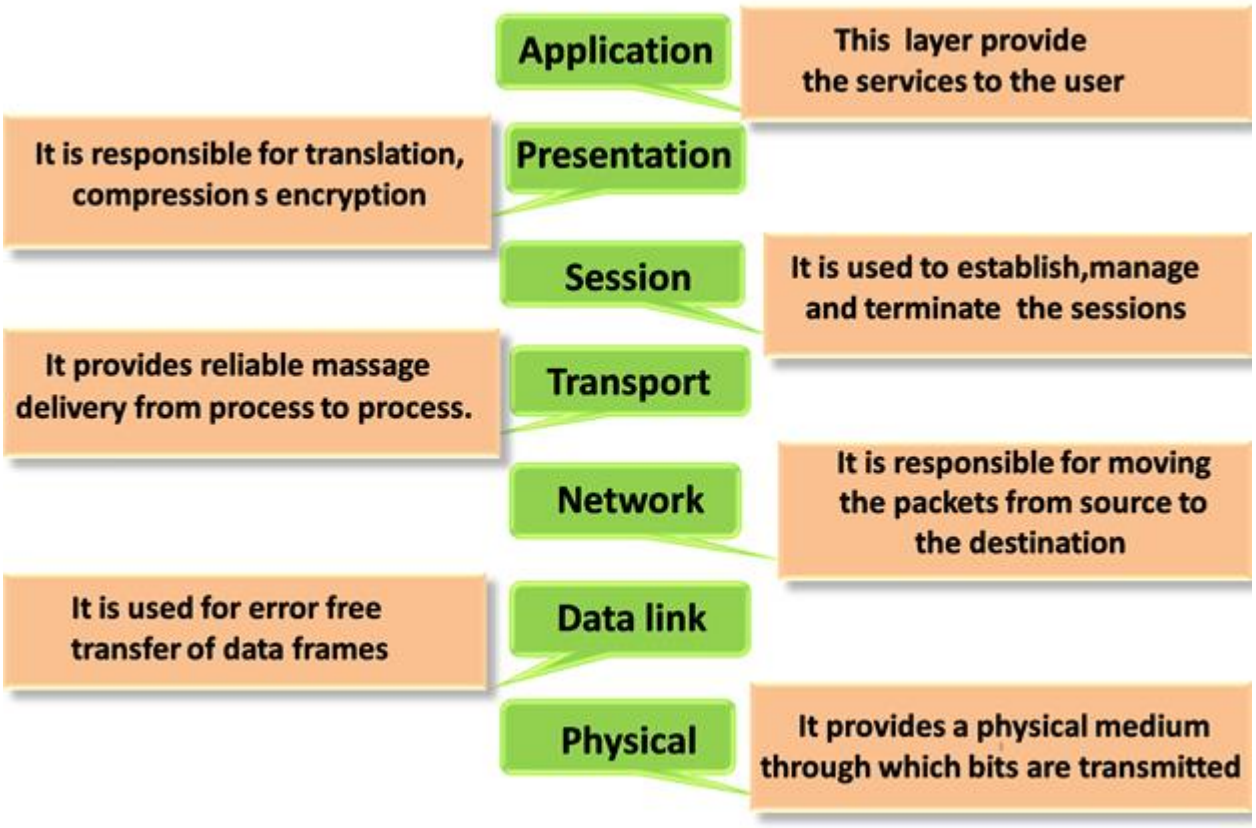
Principles of OSI Reference Model

The OSI reference model has 7 layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that architecture does not become difficult to move.

FUNCTIONS OF DIFFERENT LAYERS

Following are the functions performed by each layer of the OSI model.



OSI MODEL LAYER 1: THE PHYSICAL LAYER

- Physical Layer is the lowest layer of the OSI Model.
- It activates, maintains and deactivates the physical connection.
- It is responsible for transmission and reception of the unstructured raw data over network.
- Voltages and data rates needed for transmission is defined in the physical layer.
- It converts the digital/analog bits into electrical signal or optical signals.
- Data encoding is also done in this layer.

Design Issues with Physical Layer

The Physical Layer is concerned with transmitting raw bits over a communication channel.

The design issue has to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit and not as a 0 bit.

OSI MODEL LAYER 2: DATA LINK LAYER

- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- Data link layer synchronizes the information which is to be transmitted over the physical layer.
- The Data link layer is responsible for routing and forwarding the packets.
- This layer sends and expects acknowledgements for frames (A frame is a logical unit of data) received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.

- This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

Design Issues with Data Link Layer

- The issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism is often needed to let the transmitter know how much buffer space the receiver has at the moment.
- Broadcast networks have an additional issue in the data link layer: How to control access to the shared channel. A special sub-layer of the data link layer, the Medium Access Control (MAC) sub-layer, deals with this problem.

OSI MODEL LAYER 3: THE NETWORK LAYER

- Network Layer routes the signal through different channels from one node to the other.
- It acts as a network controller by managing the Subnet traffic.
- It decides by which route data should take.
- It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

Design Issues with Network Layer

- A key design issue is **determining how packets are routed from source to destination**. Routes can be based on static tables that are wired into the network and rarely changed. They can also be highly dynamic, being determined anew for each packet, to reflect the current network load.
- If **too many packets** are present in the subnet at the same time, they will get into one another's way, forming **bottlenecks**. The **control of such congestion** also belongs to the network layer.
- The **quality of service** provided (delay, transmit time, jitter, etc) is also a network layer issue.
- When a packet has to **travel from one network to another to get to its destination**, many problems can arise such as:
  1. The addressing used by the second network may be different from the first one.
  2. The second one may not accept the packet at all because it is too large.
  3. The protocols may differ, and so on.
- *It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.*

OSI MODEL LAYER 4: TRANSPORT LAYER

- Transport Layer decides if data transmission should be on parallel path or single path.
- It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
- Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the

destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

Design Issues with Transport Layer

- Accepting data from Session layer, split it into segments and send to the network layer.
- Isolating upper layers from the technological changes.
- Error control and flow control.

Transport layer protocols

Transmission Control Protocol (TCP)

- It is a standard protocol that allows the systems to communicate over the internet.
- It establishes and maintains a connection between hosts.
- When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

User Datagram Protocol (UDP)

- User Datagram Protocol is a transport layer protocol.
- It is an unreliable transport protocol because the receiver does not send any acknowledgment when the packet is received.

OSI MODEL LAYER 5: THE SESSION LAYER

- Session Layer manages and synchronize the conversation between two different applications.
- Transfer of data from source to destination 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.

Design Issues with Session Layer

- To allow machines to establish sessions between them in a seamless fashion.
- Provide enhanced services to the user.
- To manage dialog control by allowing two systems to start communication with each other in half-duplex or full-duplex modes.
- This layer prevents two parties from attempting the same critical operation at the same time.

OSI MODEL LAYER 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.
- While receiving the data, presentation layer transforms the data to be ready for the application layer.

- Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- It performs Data compression, Data encryption, Data conversion etc.

Design Issues with Presentation Layer

- To manage and maintain the Syntax and Semantics of the information transmitted.
- Encoding data in an agreed standard or format

OSI MODEL LAYER 7: APPLICATION LAYER

- Application Layer is the top most layer.
- This layer mainly holds application programs to act upon the received and to be sent data.
- An application layer serves as a window for users and application processes to access network services
- It handles issues such as network transparency and resource allocation

Merits of OSI reference model

1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

TCP/IP REFERENCE MODEL

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

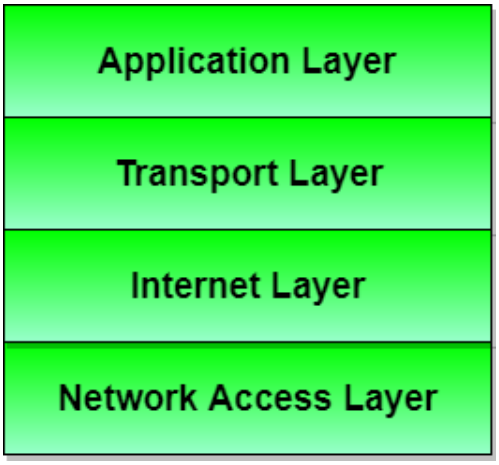
The features that stood out during the research, which led to making the TCP/IP reference model were:

1. Support for a flexible architecture. Adding more machines to a network was easy.
2. The network was robust, and connections remained intact until the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to (send data packets) another application running on different computer.

LAYERS OF TCP/IP REFERENCE MODEL

Below are the 4 layers that form the TCP/IP reference model



LAYER 1: NETWORK ACCESS LAYER

- It is the lowest layer that defines how the data should be sent physically through the network.
- Protocols are used to connect to the host, so that the packets can be sent over it.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

LAYER 2: INTERNET LAYER

- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- The order in which packets are received is different from the way they are sent.
- IP (Internet Protocol) is used in this layer.

The protocols used in this layer include:

1. IP Protocol

The Internet Protocol (IP) is a set of requirements for addressing and routing data on the Internet. IP can be used with several transport protocols, including TCP and UDP.

The responsibilities of this protocol include

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.

- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing**: When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

2. Address Resolution Protocol (ARP)

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

3. Internet Control Message Protocol (ICMP)

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

LAYER 3: TRANSPORT LAYER

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the internet layer.
- It decides if data transmission should be on parallel path or single path.
- Transport layer also arrange the packets to be sent in sequence.
- The two protocols used in the transport layer are User Datagram protocol and Transmission control protocol.

LAYER 4: APPLICATION LAYER

This layer allows the user to interact with the application.

Application layer protocols include:

1. **HTTP**: HTTP stands for Hypertext transfer protocol which allows us to access the data over the World Wide Web. It transfers the data in the form of plain text, audio or video.
2. **TELNET** is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
3. **FTP** (File Transfer Protocol) is a protocol that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
4. **SMTP** (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
5. **DNS** (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
6. **TCP (Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
7. **UDP (User-Datagram Protocol):** It is an unreliable connection-less protocol

Merits of TCP/IP model

1. It is operated independently.
2. It is scalable.
3. Supports Client/server architecture.
4. Supports a number of routing protocols.

Demerits of TCP/IP

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

COMPARISON OF OSI AND TCP/IP REFERENCE MODELS

The following are the **similarities** between OSI Reference Model and TCP/IP Reference Model.

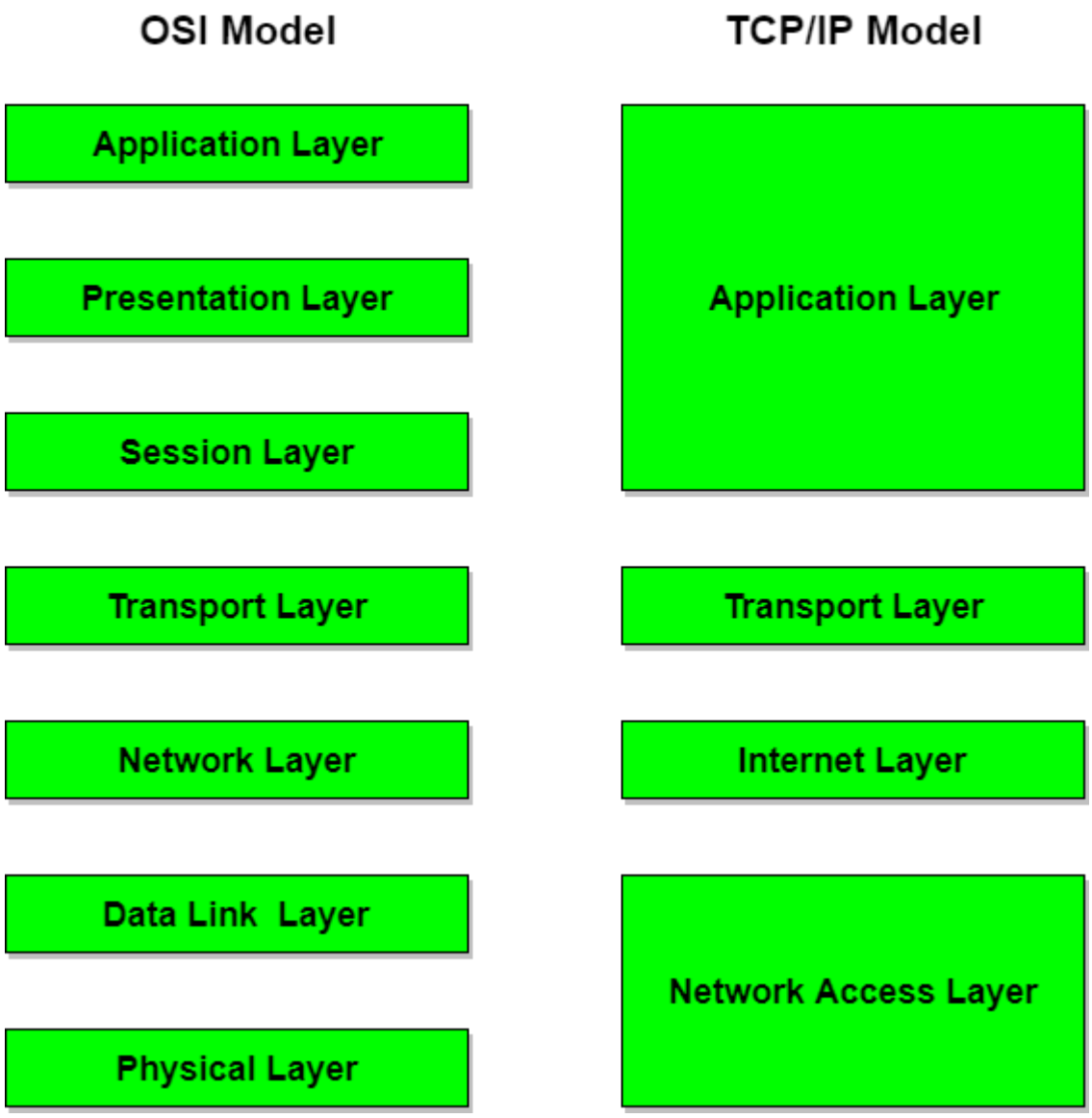
1. Both have layered architecture.
2. Layers provide similar functionalities.
3. Both are protocol stack.
4. Both are reference models.

DIFFERENCE BETWEEN OSI AND TCP/IP REFERENCE MODEL

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol

10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.

DIAGRAMMATIC COMPARISON BETWEEN OSI REFERENCE MODEL AND TCP/IP REFERENCE MODEL


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

NETWORK COMPONENTS

Hub

- It's a connectivity device (connectivity is the ability to link several communication hardware or terminals for communication purposes) that connects computers in a star network or topology (physical arrangement).
- Hubs contain multiple ports for connecting to network components. A single data packet sent through a hub goes to all connected computers.
- A hub is used to easily change and expand wiring systems and to enable central monitoring of network activity and traffic.

Repeater

This is a communication device that receives signals and re-transmits them at their original strength.
It regenerates the signals without amplifying or filtering them so as to increase the distance of transmission.
For a repeater to work, both segments connected to the repeater must use the same access method.

Switch

A switch is used to send a data packet directly from the source computer to the destination computer. *This provides for faster or greater rate of data transmission.*
A switch is similar to a hub but offers a more direct network connection between the source and destination computers.
When a switch receives a data packet, it creates a separate internal connection or segment between any two of its ports before forwarding the data packets to the appropriate port of the destination computer based on information in each pocket header.

Router

In moving data between different segments, routers examine a packet header to determine the best path for the packet to travel. They enable all users in a network to share a single connection to the internet or Wide Area Network. (WAN)
A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network. A router forwards the packet based on the information available in the routing table.
A router is used to send packets directly to a destination computer on another network or segment and to reduce stress on the network by controlling the data passing through it.

Bridge

This is a device that passes data packets between multiple network segments that use the same communication protocol and network architecture.
A packet is a logical grouping of information that includes a header, which contains the location information and user data
A bridge is used to expand the length of a segment and to reduce network traffic problems resulting from an excessive number of attached computers.

Gateway

It enables communication between different network architectures e.g. Ethernet and token ring architectures.
A gateway takes data from one network and repackages it so that each network can understand the repackaged. It therefore works like an interpreter because the format of an architecture e.g. Ethernet can be translated into a format that can be understood by token ring architecture.
A gateway is used to link two network system that are not designed using the same architecture and same set of communication rules.

Modem

It is an electronic device that makes possible the transmission of data to or from a computer via telephone or other communication lines. A modem is a communications device that can be either internal or external to your computer. It allows one computer to connect to another computer and transfer data over telephone lines.

It converts analog signals to digital signals and vice-versa

IP ADDRESSING

IP addressing

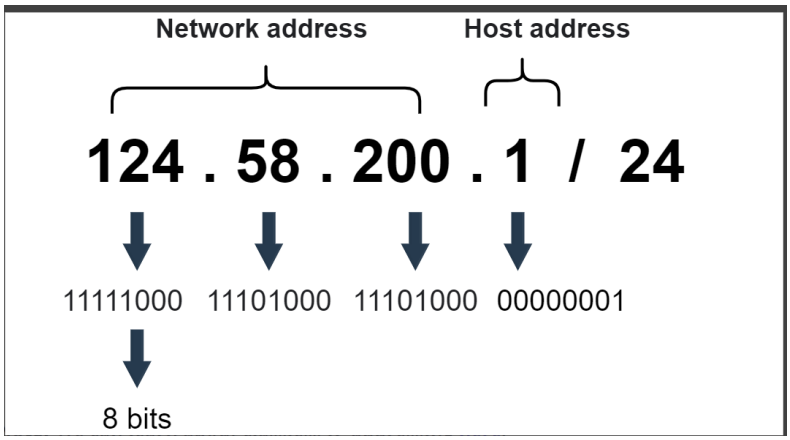
An Internet Protocol **(IP)** address is a unique identifier that assists in the recognition of different devices present over the network. Through **IP addressing**, we can send and receive data packets across the internet without trouble-free.

IP format

An IP address is a 32-bit numerical address separated by periods (.) (.) represented in dotted decimal notation. It is expressed in a set of four pairs, where each set ranges from 00 to 255255. Slash notation (/) (/) identifies the number of network bits reserved for the allocated IP address.

The parts of an IP address

The IP address has two parts: the **network address** and the **host address**. The network address is essential for the recognition of the network. In the host address part, we always reserve the first address for the network address, and the last address for the **broadcast address**. The broadcast address transmits data to all the hosts present in the network at once. The format of an IP address is as shown below



Subnetting

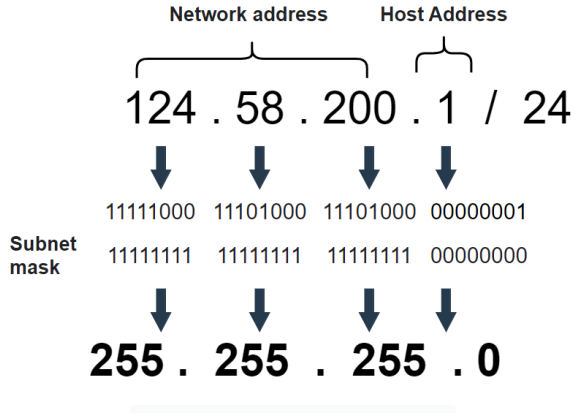
Subnetting is a process of partitioning a complex network into multiple smaller logical sub-networks, or subnets.

Subnet masks

A **subnet mask** is a 32-bit number that divides the existing IP into network and host addresses.

Example

To find the subnet mask of a particular IP address, let's set all network bits to 11s and the host bits to 00s. The given IP address has 24 bits reserved as a network address. So, its default subnet mask is 255.255.255.0.



Finding the subnet mask of an IP address

Note:

The IP address space for a network is globally allocated by the **Internet Assigned Numbers Authority (IANA)**. The network administrator is responsible for managing the IP addresses within the allocated address space.

The importance of subnetting

As networks grow larger and more complex day by day, traffic also requires fast and efficient routes. Subnetting provides a mechanism named **route aggregation** that limits the size of the routing table that each router has to maintain. This not only helps maintain efficient network speed, but also enhances performance.

Benefits

Some benefits of subnetting are listed below:

1. Subnetting splits broadcast domains, thus improving network speed and performance.
2. It reduces congestion and bottleneck problems.
3. It enhances network security, as devices don't access the whole network.

Introduction of Classful IP Addressing

An IP address is an address that has information about how to reach a specific host, especially outside the LAN. An IP address is a 32-bit unique address having an address space of 232.

Classful IP addressing is a way of organizing and managing IP addresses, which are used to identify devices on a network. Think of IP addresses like street addresses for houses; each device on a network needs its unique address to communicate with other devices. In this article, we are going to discuss Classful IP addresses, and their types in detail.

What is an IPV4 Address?

An IPv4 address is a unique number assigned to every device that connects to the internet or a computer network. It's like a home address for your computer, smartphone, or any other device, allowing it to communicate with other devices.

- **Format**: An IPv4 address is written as four numbers separated by periods, like this: 192.168.1.1. Each number can range from 0 to 255.
- The IPv4 address is divided into two parts: **Network ID** and **Host ID.**
- **Purpose**: The main purpose of an IPv4 address is to identify devices on a network and ensure that data sent from one device reaches the correct destination.
- **Example**: When you type a website address into your browser, your device uses the IPv4 address to find and connect to the server where the website is hosted.
- Host ID

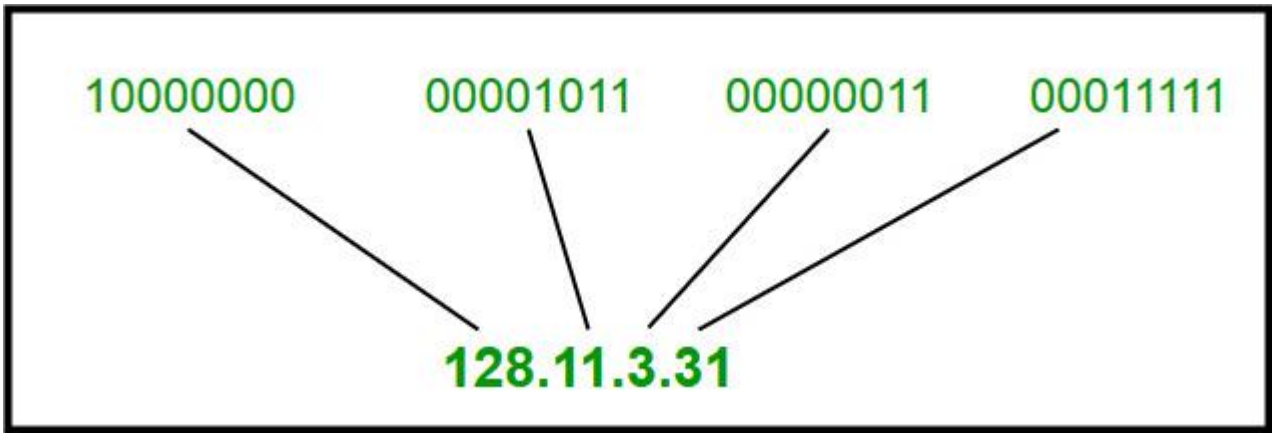
Think of an IPv4 address as a phone number for your device. Just as you dial a specific number to reach a particular person, devices use IPv4 addresses to connect and share information.

There are two notations in which the IP address is written, dotted decimal and hexadecimal notation.

Dotted Decimal Notation

Some points to be noted about dotted decimal notation:

- The value of any segment (byte) is between 0 and 255 (both included).
- No zeroes are preceding the value in any segment (054 is wrong, 54 is correct).



Dotted Decimal Notation

Hexadecimal Notation

Need For Classful Addressing

Initially in 1980's IP address was divided into two fixed part i.e., NID (Network ID) = 8bit, and HID (Host ID) = 24bit. So there are 28 that is 256 total network are created and 224 that is 16M Host per network.

There are one 256 Networks and even a small organization must buy 16M computer (Host) to purchase one network. That's why we need classfull addressing.

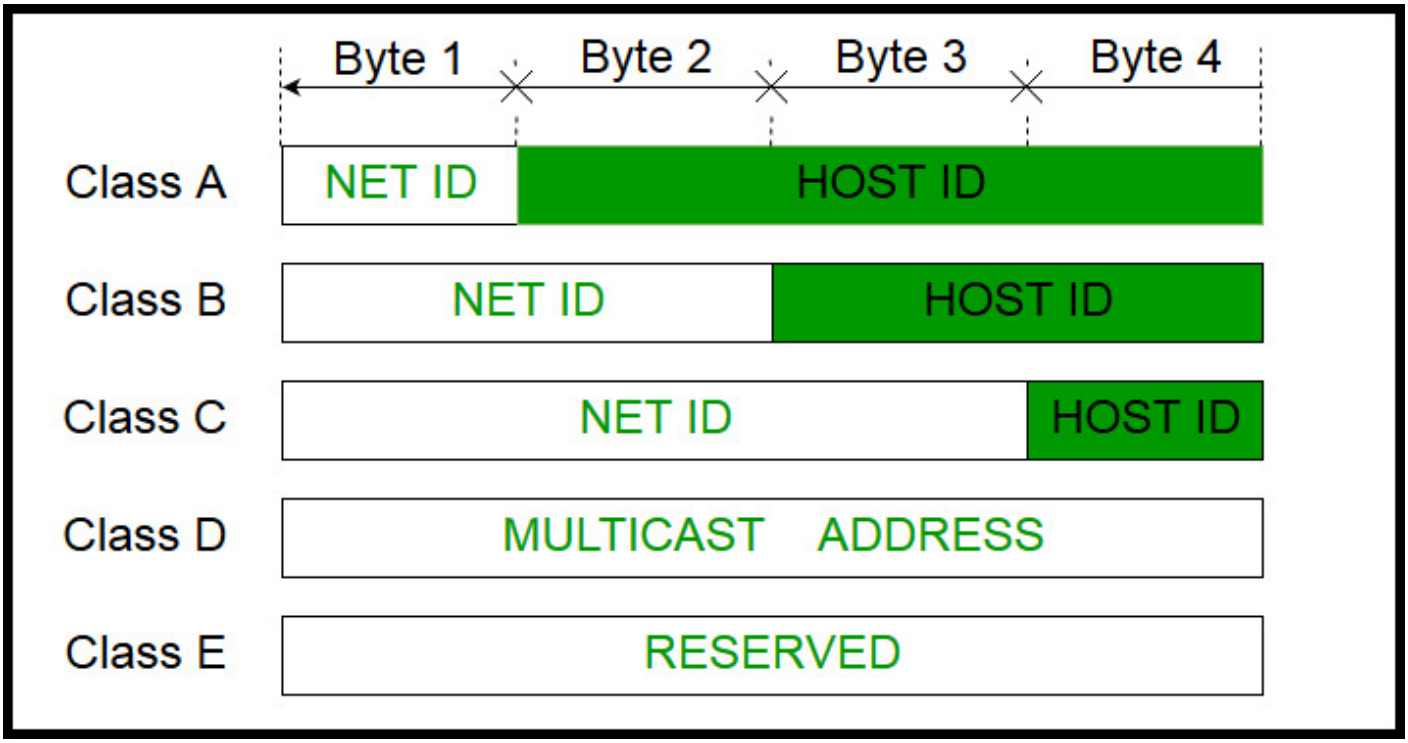
Classful Addressing

The 32-bit IP address is divided into five sub-classes. These are given below:

- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determines the classes of the IP address.

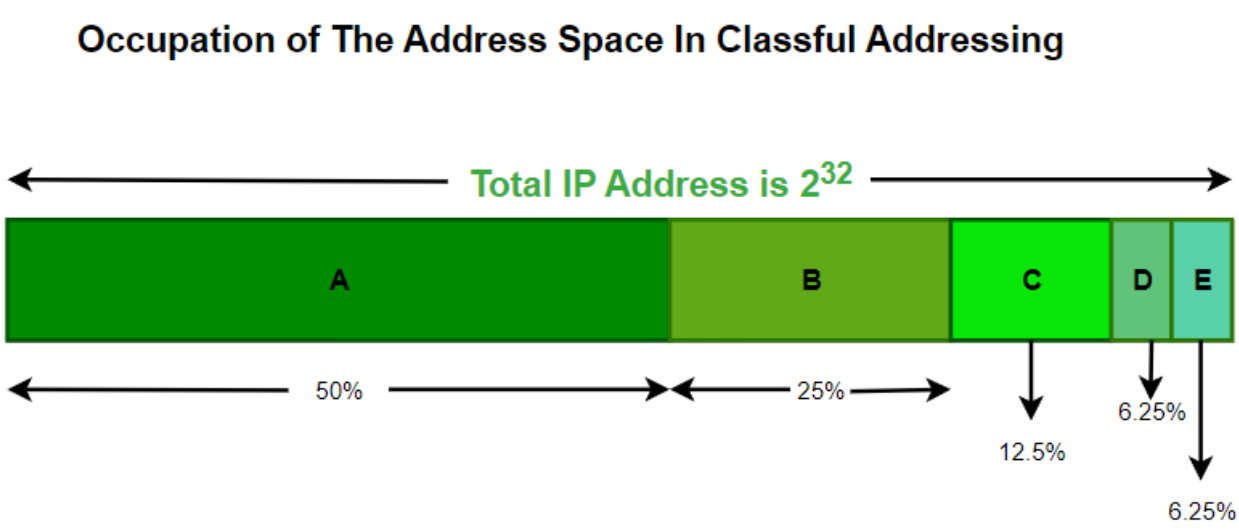
The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns an IP address to each device that is connected to its network.



Classful Addressing

Note:

- IP addresses are globally managed by Internet Assigned Numbers Authority (IANA) and Regional Internet Registries (RIR).
- While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.



Occupation of The Address Space In Classful Addressing

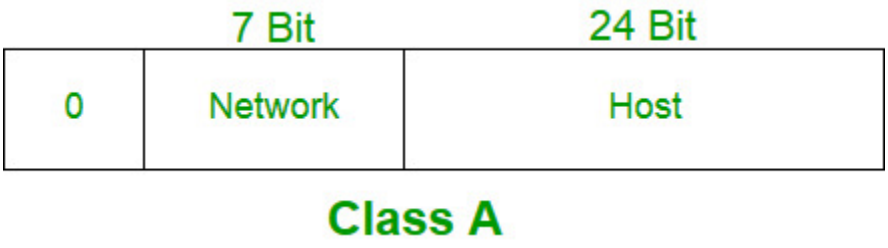
Class A

IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher-order bit of the first octet in class A is always set to 0. The remaining 7 bits in the first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for Class A is 255.x.x.x.

Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).



Class B

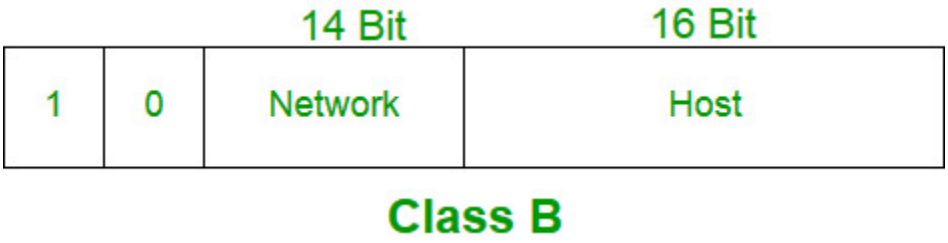
IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher-order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine the network ID. The 16 bits of host ID are used to determine the host in any network. The default subnet mask for class B is 255.255.x.x. Class B has a total of:

- 2^{14} = 16384 network address
- $2^{16} – 2$ = 65534 host address

Class B IP Addresses range from 128.0.x.x to 191.255.x.x.



Class B

Class C

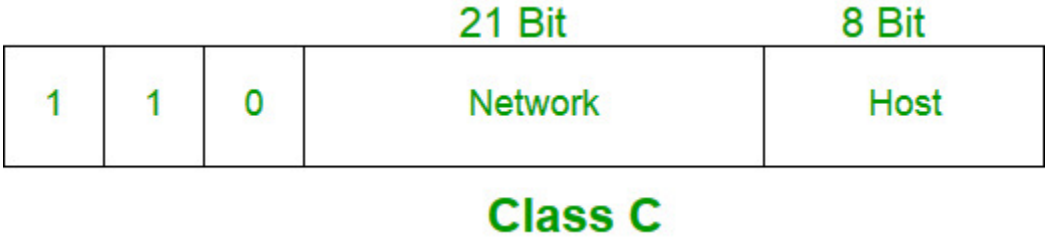
IP addresses belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher-order bits of the first octet of IP addresses of class C is always set to 110. The remaining 21 bits are used to determine the network ID. The 8 bits of host ID are used to determine the host in any network. The default subnet mask for class C is 255.255.255.x. Class C has a total of:

- 2^{21} = 2097152 network address
- $2^{8} – 2$ = 254 host address

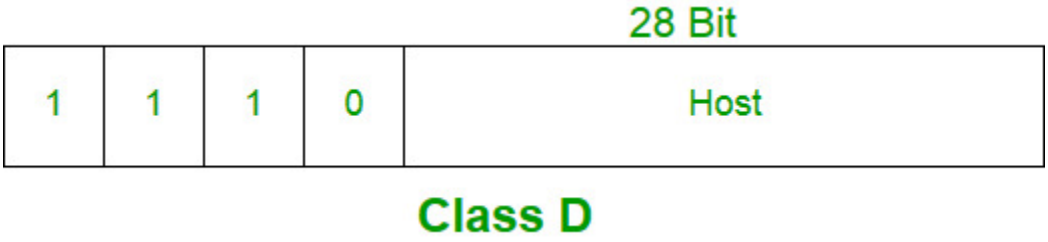
Class C IP addresses range from 192.0.0.x to 223.255.255.x.



Class D

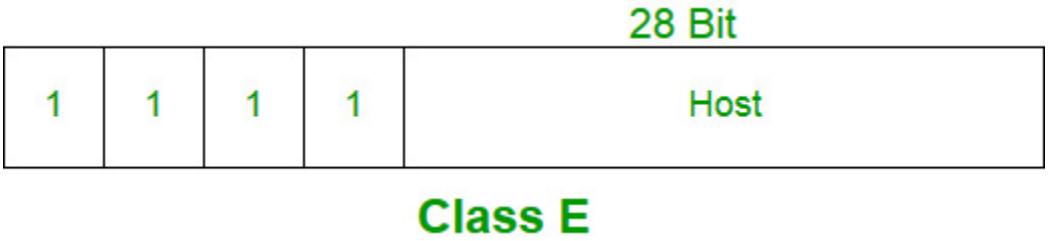
IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not possess any subnet mask. Class D has IP address range from 224.0.0.0 to 239.255.255.255



Class E

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.



Range of Special IP Addresses

169.254.0.0 – 169.254.0.16 : Link-local addresses
127.0.0.0 – 127.255.255.255 : Loop-back addresses
0.0.0.0 – 0.0.0.8: used to communicate within the current network.

Rules for Assigning Host ID

Host IDs are used to identify a host within a network. The host ID is assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- A host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for Assigning Network ID

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to the class A address and is reserved for internal loopback functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Summary of Classful Addressing

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

In the above table No. of networks for class A should be 127. (Network ID with all 0 s is not considered)

Problems With Classful Addressing

The problem with this classful addressing method is that millions of class A addresses are wasted, many of the class B addresses are wasted, whereas, the number of addresses available in class C is so small that it

cannot cater to the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993.

Conclusion

Classful IP addressing, with its categorization into classes like A, B, and C, was a fundamental method in early networking. It organized IP addresses based on network size but faced limitations in flexibility and efficient use of address space. The development of CIDR addressed these issues by allowing more precise control over subnetting and optimizing address allocation.

Classless Inter Domain Routing (CIDR)

Classless Inter-Domain Routing (CIDR) is a method of IP address allocation and IP routing that allows for more efficient use of IP addresses. CIDR is based on the idea that IP addresses can be allocated and routed based on their network prefix rather than their class, which was the traditional way of IP address allocation.

CIDR addresses are represented using a slash notation, which specifies the number of bits in the network prefix. For example, an IP address of 192.168.1.0 with a prefix length of 24 would be represented as 192.168.1.0/24. This notation indicates that the first 24 bits of the IP address are the network prefix and the remaining 8 bits are the host identifier.

Advantages of CIDR

1. Efficient use of IP addresses: CIDR allows for more efficient use of IP addresses, which is important as the pool of available IPv4 addresses continues to shrink.
2. Flexibility: CIDR allows for more flexible allocation of IP addresses, which can be important for organizations with complex network requirements.
3. Better routing: CIDR allows for more efficient routing of IP traffic, which can lead to better network performance. Reduced administrative overhead: CIDR reduces administrative overhead by allowing for easier management of IP addresses and routing.

Disadvantages of CIDR

1. Complexity: CIDR can be more complex to implement and manage than traditional class-based addressing, which can require additional training and expertise.
2. Compatibility issues: Some older network devices may not be compatible with CIDR, which can make it difficult to transition to a CIDR-based network.
3. Security concerns: CIDR can make it more difficult to implement security measures such as firewall rules and access control lists, which can increase security risks.

4. Overall, CIDR is a useful and efficient method of IP address allocation and routing, but it may not be suitable for all organizations or networks. It is important to weigh the advantages and disadvantages of CIDR and consider the specific needs and requirements of your network before implementing CIDR.