3.1 Concepts and types of MANET (Mobile Ad hoc network) Introduction of Mobile Ad hoc Network (MANET)

MANET stands for Mobile Adhoc Network also called a wireless Adhoc network or Adhoc

wireless network that usually has a routable networking environment on top of a Link

Layer ad hoc network.. They consist of a set of mobile nodes connected wirelessly in a self- configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently. Each node behaves as a router as they forward traffic to other specified nodes in the network.

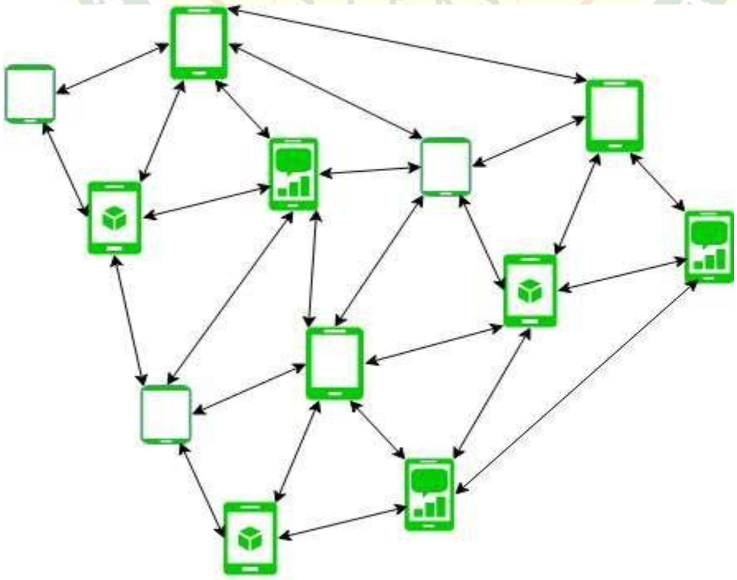


Figure - Mobile Ad Hoc Network

MANET may operate a standalone fashion or they can be part of larger internet. They form a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes.

The main challenge for the MANET is to equip each device to continuously maintain the information required to properly route traffic. MANETs consist of a peer-to-peer, self-forming, self-healing network MANET's circa 2000-2015 typically communicate at radio frequencies (30MHz-5GHz). This can be used in road safety, ranging from sensors for the environment, home, health, disaster rescue operations, air/land/navy defence, weapons, robots, etc.

Characteristics of MANET –

- Dynamic Topologies:

Network topology which is typically multihop may change randomly and rapidly with time, it can form unidirectional or bi-directional links.

- Bandwidth constrained, variable capacity links:

Wireless links usually have lower reliability, efficiency, stability, and capacity as compared to a wired network

- Autonomous Behavior:

Each node can act as a host and router, which shows its autonomous behavior.

- Energy Constrained Operation:

As some or all the nodes rely on batteries or other exhaustible means for their energy. Mobile nodes are characterized by less memory, power, and lightweight features.

- Limited Security:

Wireless networks are more prone to security threats. A centralized firewall is absent due to the distributed nature of the operation for security, routing, and host configuration.

- Less Human Intervention:

They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature.

Advantages:

Flexibility: MANETs are highly flexible, as they can be easily deployed in various environments and can be adapted to different applications and scenarios. This makes them ideal for use in emergency situations or military operations, where there may not be a pre- existing network infrastructure.

Scalability: MANETs can easily scale to accommodate a large number of nodes, making them suitable for large-scale deployments. They can also handle dynamic changes in network topology, such as the addition or removal of nodes.

Cost-effective: Since MANETs do not require any centralized infrastructure, they are often more cost-effective than traditional wired or wireless networks. They can also be used to extend the range of existing networks without the need for additional infrastructure.

Rapid Deployment: MANETs can be rapidly deployed in areas where infrastructure is not available, such as disaster zones or rural areas.

Disadvantages:

Security: MANETs are vulnerable to security threats, such as attacks by malicious nodes, eavesdropping, and data interception. Since the network is decentralized, there is no central authority to ensure the security of the network.

Reliability: MANETs are less reliable than traditional networks, as they are subject to interference, signal attenuation, and other environmental factors that can affect the quality of the connection.

Bandwidth: Since MANETs rely on wireless communication, bandwidth can be limited. This can lead to congestion and delays, particularly when multiple nodes are competing for the same channel.

Routing: Routing in MANETs can be complex, particularly when dealing with dynamic network topologies. This can result in inefficient routing and longer delays in data transmission.

Power Consumption: Since MANETs rely on battery-powered devices, power consumption can be a significant issue. Nodes may need to conserve power to extend the life of the battery, which can limit the amount of data that can be transmitted.

3.1.1 VANET (Vehicular Ad hoc Network)

Enable effective communication with another vehicle or with the roadside equipments. Intelligent vehicular ad hoc networks(InVANETs) deals with another vehicle or with roadside equipment. VANETs use wireless communication technologies, such as WIFI or cellular, to enable vehicles to communicate with each other and with infrastructure devices, such as traffic lights or road-side units.

Uses: VANETs can be used to support a wide range of applications, such as:

- Intelligent Transportation Systems (ITS): VANETs can be used to improve traffic flow and reduce congestion by providing real-time traffic information and routing advice to drivers.
- Road Safety: VANETs can be used to improve road safety by providing information about the location of other vehicles, road conditions, and potential hazards.
- Entertainment and infotainment: providing in-vehicle entertainment and internet access to the passengers
- Emergency Services: VANETs can be used to support emergency services by providing real-time information about accidents or other incidents on the road.
- Commercial Services: VANETs can be used for commercial services such as providing location-based advertisement and other location-based service to the driver or passengers.

VANETs are considered as one of the most critical application of the Internet of Things (IoT) technology and the 5G technology.

Advantages:

- Improves traffic flow and reduces congestion.
- Enhances road safety by providing real-time information about road conditions, potential hazards, and the location of other vehicles.
- Enables in-vehicle entertainment and internet access to passengers.

- Supports emergency services by providing real-time information about accidents or other incidents on the road.
- Provides location-based advertising and other services to the driver or passengers.

Disadvantages:

- Vulnerable to attacks and security breaches.
- Requires a large number of vehicles to form an effective network.
- Limited coverage area, as VANETs rely on wireless communication technologies such as Wi-Fi or cellular.

3.1.2 Smart phone Ad hoc Network (SPANC)

To create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. Here peers can join or leave the network without destroying it. ad-hoc network that utilizes smartphones as the primary nodes for communication. In SPANC, smartphones can act as both routers and hosts, creating a decentralized network without the need for a central infrastructure. This allows for increased flexibility and scalability in wireless communication, especially in emergency or disaster scenarios where traditional communication infrastructure may be unavailable.

Some examples of SPANC applications include disaster response, search and rescue, and urban crowd management.

Uses: Smart Phone Ad hoc Network (SPANC) can be used for a variety of applications, including:

- Emergency communication: In the event of a natural disaster or other emergency, SPANCs can be used to establish a communication network quickly, allowing people to contact emergency services or stay in touch with loved ones.
- Remote areas: SPANCs can be useful in remote areas where traditional wireless networks are not available, such as rural communities or wilderness areas.
- Event networking: SPANCs can be used to create a temporary network for events or gatherings, allowing attendees to communicate and share information.
- Military and emergency services: SPANCs can be used by military and emergency services to establish a quick and reliable communication network in the field.
- Content sharing: SPANCs can be used to share various types of content such as pictures and videos, as well as other forms of multimedia.
- Research and Development: SPANCs can be used in various research and development projects such as security, routing, and energy consumption.
- Crowdsourcing: SPANCs can be used to gather data from a large group of people, such as in a survey or study.
- Advertising and marketing: SPANCs can be used to deliver targeted advertising and marketing messages to a specific group of people.

Advantages:

- Enables communication without relying on traditional network infrastructure or wireless access points.
- Provides a decentralized network without the need for a central infrastructure.
- Useful in emergency or disaster scenarios where traditional communication infrastructure may be unavailable.
- Can be used to establish a communication network quickly in the event of a natural disaster or other emergency.

Disadvantages:

- Limited coverage area, as SPANCs rely on the range of smartphone Wi-Fi capabilities.
- Requires a large number of smartphones to form an effective network.
- Vulnerable to attacks and security breaches.

3.1.3 Flying Ad hoc network (FANET)

This is composed of unmanned aerial vehicles (commonly known as drones). Provides links to remote areas and mobility. Flying Ad-hoc Networks (FANETs) are a specialized type of mobile ad-hoc network that are designed specifically for use in aerial vehicles, such as drones, UAVs, and UGVs. They enable communication and coordination among a group of flying vehicles in a decentralized and self-organizing manner.

FANETs provide a flexible and reliable communication infrastructure for aerial vehicles, allowing for real-time data collection and transmission, as well as navigation and control. They can operate in a standalone mode or can be connected to other networks, such as satellite or cellular networks, to provide extended communication capabilities.

Uses: FANETs have several potential uses in various fields such as:

- Military and defense: FANETs can be used for reconnaissance, surveillance, and intelligence gathering, as well as for communication and coordination among military personnel and units.
- Emergency response: FANETs can be used to provide communication and coordination among emergency responders in the field, enabling effective response to natural disasters or other emergency situations.
- Civil aviation: FANETs can be used for air traffic management and control, as well as for communication and coordination among commercial and private aircraft.
- Environmental monitoring: FANETs can be used to collect and transmit data for environmental monitoring and research, such as for monitoring air and water quality, or for monitoring wildlife populations.
- Agriculture: FANETs can be used for precision agriculture, such as for monitoring crop health and for controlling crop-dusting drones.

- Search and Rescue: FANETs can be used to provide communication and coordination among search and rescue teams, enabling efficient and effective search and rescue operations.
- Infrastructure inspection: FANETs can be used for inspecting and monitoring large-scale infrastructure, such as bridges, buildings, and power lines.
- Media and Entertainment: FANETs can be used for live streaming and for capturing high-quality video and images for use in media and entertainment.

Advantages:

- Provides flexibility and mobility as the network can be set up and moved quickly.
- Suitable for disaster response, search and rescue operations, and remote sensing applications.
- Can cover large areas with minimal infrastructure requirements.
- Can operate in harsh environments where traditional communication infrastructure is not available.

Disadvantages:

- Limited endurance of the flying platforms.
- Communication range is affected by weather conditions.
- Lack of standardization in FANETs technology.
- Difficult to maintain and manage due to the dynamic nature of the network.

3.2 The OSI Model

- An Open Systems Interconnection (OSI) Model is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The purpose of the OSI Model is to show howto facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI Model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computersystems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

Seven layers of the OSI model

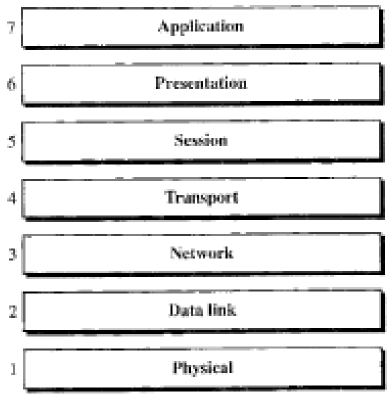
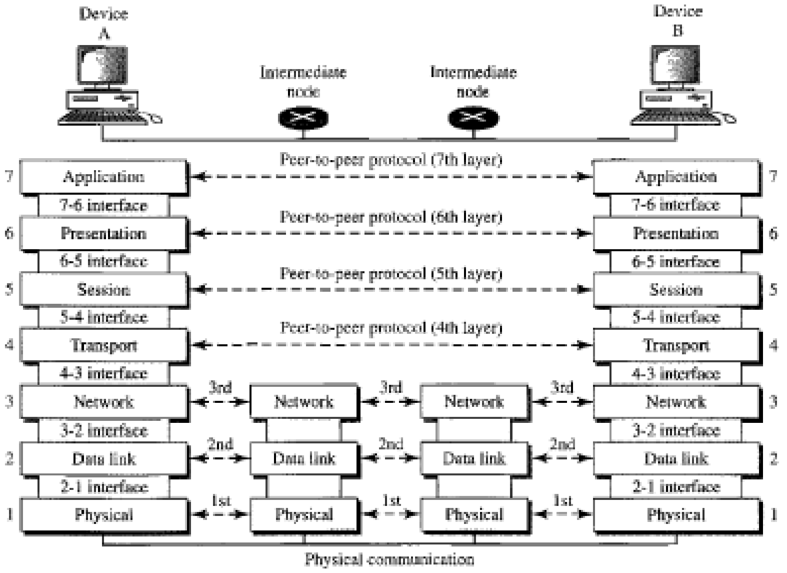
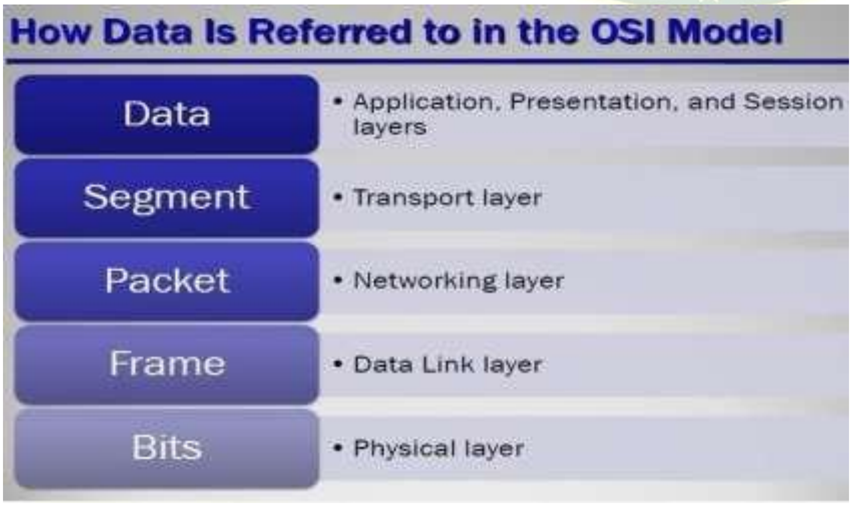


Figure 2.3 *The interaction between layers in the OSI model*

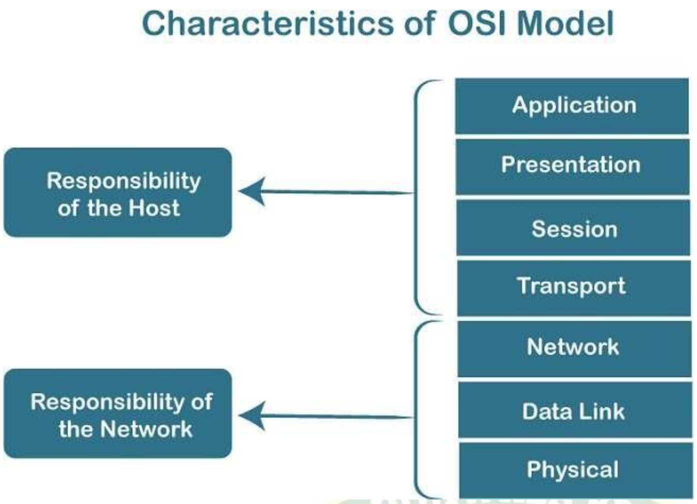




How Data Is Referred to in the OSI Model

Data	• Application, Presentation, and Session layers
Segment	• Transport layer
Packet	• Networking layer
Frame	• Data Link layer
Bits	• Physical layer

Characteristics of OSI Model:

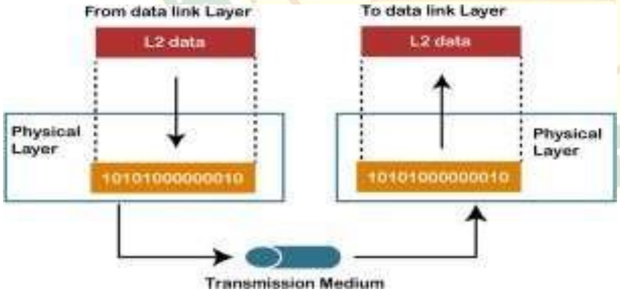

Characteristics of OSI Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
Responsibility of the Host
Responsibility of the Network

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

The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical m

1. **Physical Layer**:



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

The physical layer is also concerned with the following:

• Physical characteristics of interfaces and medium. The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

• Representation of bits. The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical oroptical. The physical layer defines the type of encoding.

• Data rate. The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

• Synchronization of bits. The sender and receiver not only must use the same bit rate but alsomust be synchronized at the bit level. In other words, the sender and the receiver clocks mustbe synchronized.

• Line configuration. The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link.In a multipoint configuration, a link is shared among several devices.

• Physical topology. The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every deviceis on a common link), or a hybrid topology (this is a combination of two or more topologies).

• Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send;the other can only receive. The simplex mode is a one-way communication. In the half-duplexmode, two devices can send and receive, but not at the same time. In a full-duplex (or simplyduplex) mode, two devices can send and receive at the same time.

2. Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

Other responsibilities of the data link layer include the following:

• Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

• Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is theaddress of the device that connects the network to the next one.

• Flow control. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

• Error control. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize

duplicate frames. Error control is normally achieved through a trailer added to the end of theframe.

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

3. Network Layer :

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination. If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.

Other responsibilities of the network layer include the following:

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

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

4. Transport Layer:

The transport layer is responsible for process-to-process delivery of the entire message. A processis an application program running on a host. Whereas the network layer oversees source-to- destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to- destination level.

Other responsibilities of the transport layer include the following:

• Service-point addressing. Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process(running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

• Segmentation and reassembly. A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

• Connection control. The transport layer can be either connectionless or connection oriented.A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before deliveringthe packets. After all the data are transferred, the connection is terminated.

• Flow control. Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

• Error control. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

5. Session Layer:

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

Specific responsibilities of the session layer include the following:

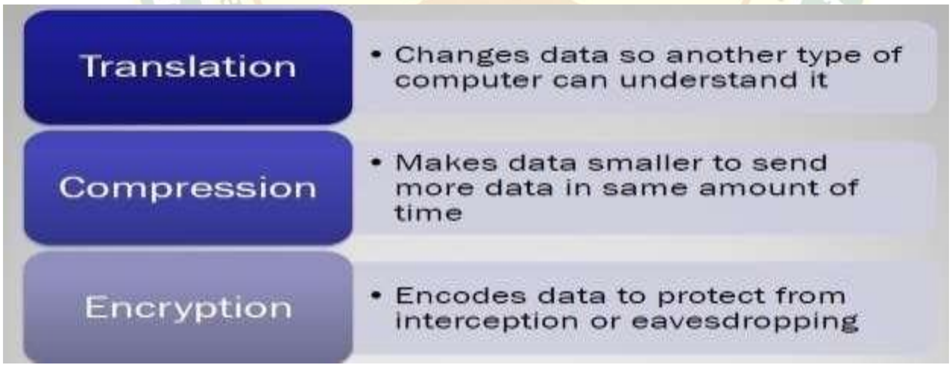
• Dialog control. The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half

duplex (one way at a time)or full-duplex (two ways at a time) mode.

• Synchronization. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

6. Presentation Layer:

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.



Translation

- Changes data so another type of computer can understand it

Compression

- Makes data smaller to send more data in same amount of time

Encryption

- Encodes data to protect from interception or eavesdropping

Specific responsibilities of the presentation layer include the following:

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

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

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

7. Application Layer :

The application layer enables the user, whether human or software, to access the network.

It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

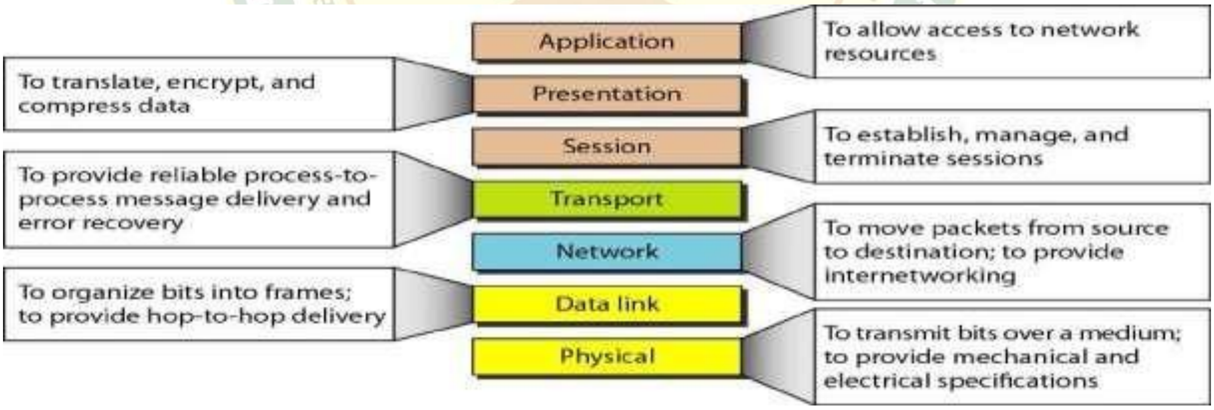
Specific services provided by the application layer include the following:

- Network virtual terminal. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.

- File transfer, access, and management. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for usein the local computer, and to manage or control files in a remote computer locally.

- Mail services. This application provides the basis for e-mail forwarding and storage.

- Directory services. This application provides distributed database sources and access for global information about various objects and services.


Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

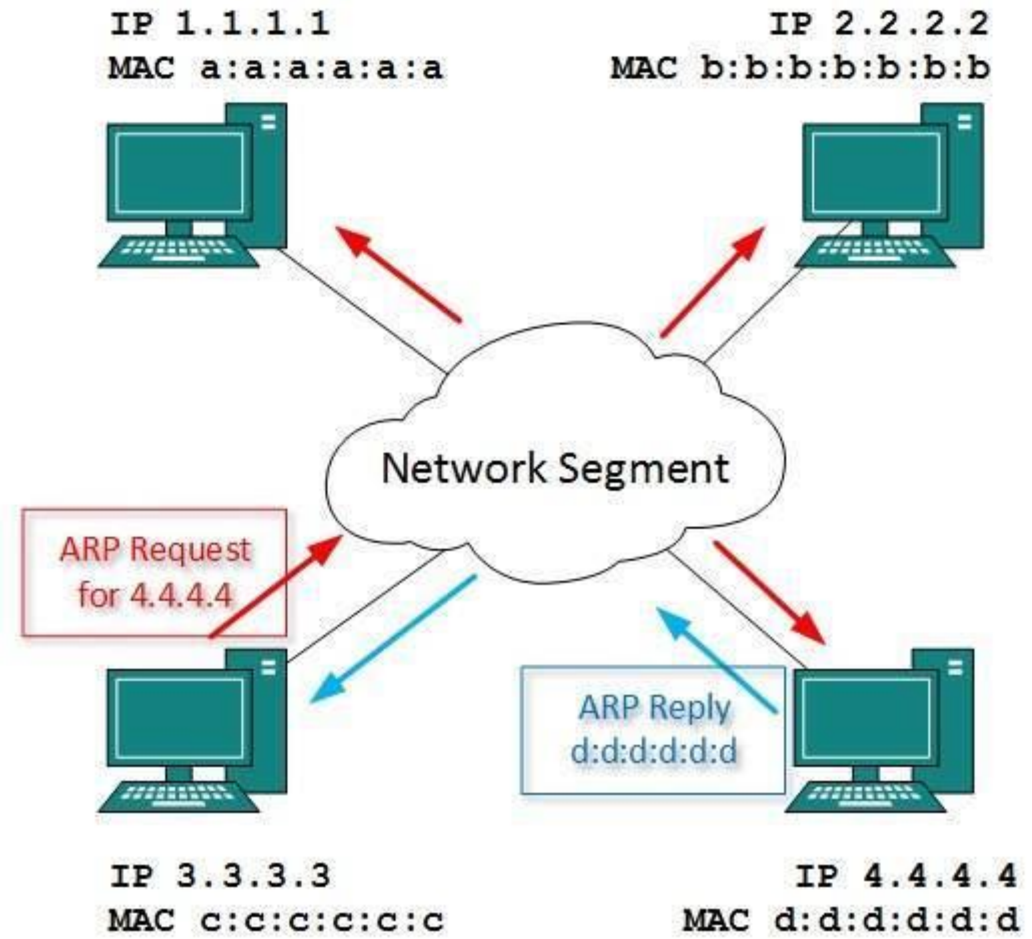
3.1 Important Protocols of Network Layers

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

Address Resolution Protocol (ARP)

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

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



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

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

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

Internet Control Message Protocol (ICMP)

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

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

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

Internet Protocol Version 4 (IPv4)

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

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

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

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

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

Internet Protocol Version 6 (IPv6)

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

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

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

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

- Dual stack implementation
- Tunnelling
- NAT-PT

3.3.1 Concept of Data packets and Datagram

Packet

• While communicating through networks it's important to send and receive files and information. The basic unit of communication between a source and a destination in a network is a packet.

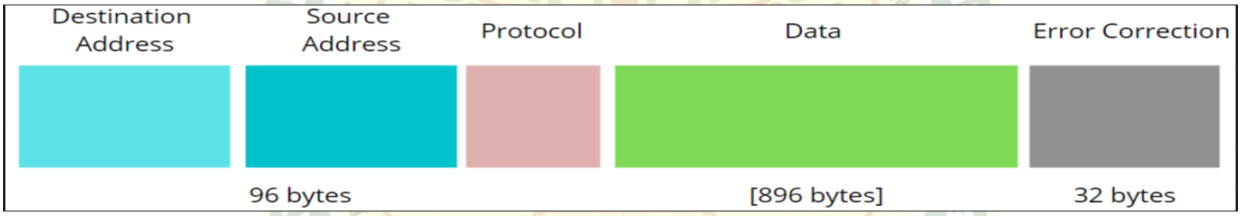
• It makes it easier to retransmit lost pieces of data or interrupted ones. Packets are data units within the network layer in the OSI model.

• Each packet contains a header with source and destination IP addresses a field for the protocol specification, the data, a trailer, protocol version, etc. The trailer field contains information about error corrections and other flags for the identification.

Let's consider the example of an email.

When the user clicks on the button 'send', the associated operation executes. The message will go through the OSI model layers until it reaches the network access layer where the packet should be created.

We format the data sent through an email into a packet, containing information about the used protocol, the error correction, IP addresses of the sender and the receiver (source and destination, respectively), as well as the email text:

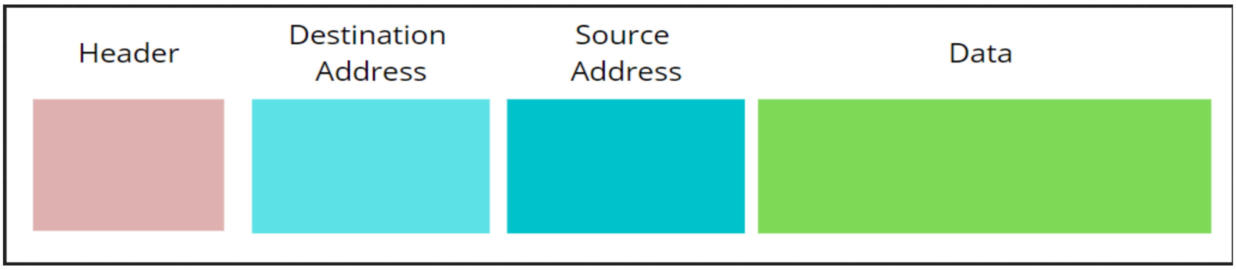


Datagram

• The datagram represents a data unit of transfer in networking. Data transmitted in a network is divided into smaller parts called datagram. In a datagram, we divide data frequently and transmitted from source to destination without a predefined route. We also can't guarantee the order of delivery to the receiver end.

• While TCP uses packets in connection-oriented protocols, datagrams are used in UDP, making them carry less information since they don't need to have a response message from the destination. The transport layer uses datagram as a unit of transfer data. A datagram comprises a header, IP addresses of destination and source, and the data.

• In the case we sent an email using the UDP protocol, there will be no packets but datagram. The information transmitted would be in the following figure:



3.3.2 Presentation Layer protocols and their purpose :

• Presentation layer is 6th layer in the OSI model, and its main objective is to present all messages to upper layer as a standardized format. It is also known as the "Translation layer".

• This layer takes care of syntax and semantics of messages exchanged in

between two communication systems. Presentation layer has responsible that receiver can understand all data.

Functions of Presentation Layer

Presentation layer performs various functions in the OSI model:

• Presentation layer helps to translate from American standard code for information interchange (ASCII) to the extended binary code decimal interchange code (EBCDIC).

• It deals with user interface as well as supporting for several services such as email and file transfer.

• It provides encoding mechanism for translating all messages from user dependent format with common format and vice – versa.

• It's main goal for data encryption and decryption of entire data before they are getting transmission over all common platforms.

• It provides data compression mechanism for source point to decrease the all bits which are transmitted. Due to this data compression system, user are able to transmit enlarge multimedia file at fastest file transfer rate.

• Due to use of Data Encryption and Decryption algorithm, presentation layer provides more network protection and confidentiality while transmission data over the entire network.

3.3.2.1 SSL, HTTP, FTP, Telnet

Secure Sockets Layer

Secure Sockets Layer (SSL) is a standard technique for transmitting documents securely across a network. SSL technology, created by Netscape, establishes a secure connection between a Web server and a browser, ensuring private and secure data transmission. SSL communicates using the Transport Control Protocol (TCP).

The term "socket" in SSL refers to the method of sending data via a network between a client and a server.

A Web server requires an SSL certificate to establish a secure SSL connection while using SSL for safe Internet transactions. SSL encrypts network connection segments atop the transport layer, a network connection component above the program layer.

SSL is based on an asymmetric cryptographic process in which a Web browser generates both a public and a private (secret) key. A certificate signing request is a data file that contains the public key (CSR). Only the recipient receives the private key.

Objectives of SSL

The goals of SSL are as follows −

• Data integrity − Information is safe from tampering. The SSL Record Protocol, SSL Handshake Protocol, SSL Change Cipher Spec Protocol, and SSL Alert Protocol maintain data privacy.

• Client-server authentication − The SSL protocol authenticates the client and server using standard cryptographic procedures.

• SSL is the forerunner of Transport Layer Security (TLS), a cryptographic technology for secure data transfer over the Internet.

HTTP

- HTTP stands for HyperText Transfer Protocol.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request.

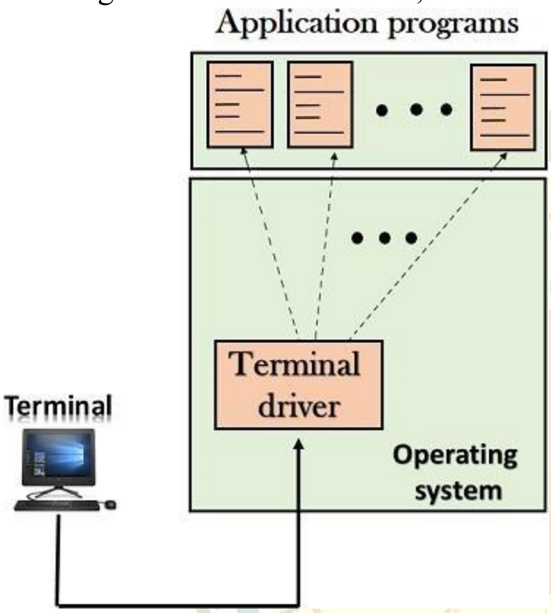
Telnet

- The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfer a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.
- The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer. A popular client- server program Telnet is used to meet such demands. Telnet is an abbreviation for Terminal Network.
- Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

There are two types of login:

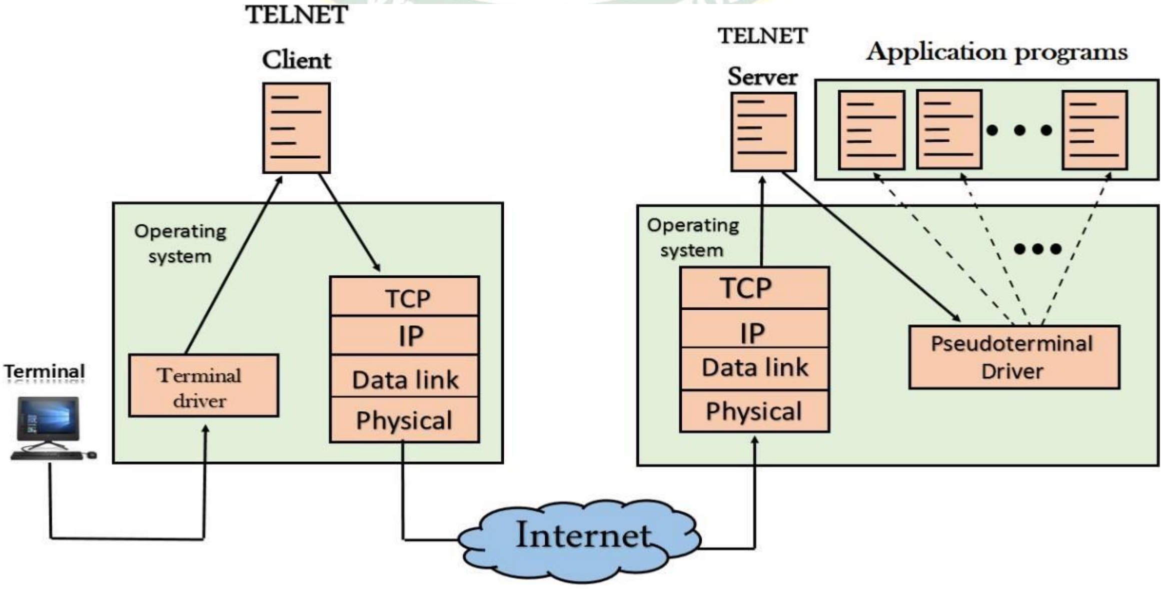
Local Login

- When a user logs into a local computer, then it is known as local login.
- When the workstation running terminal emulator, the keystrokes entered by the user are accepted by the terminal driver. The terminal driver then passes these characters to the operating system which in turn, invokes the desired application program.
- However, the operating system has special meaning to special characters. For example, in UNIX some combination of characters has special meanings such as control character with "z" means suspend. Such situations do not create any problem as the terminal driver knows the meaning of such characters. But, it can cause the problems in remote login.



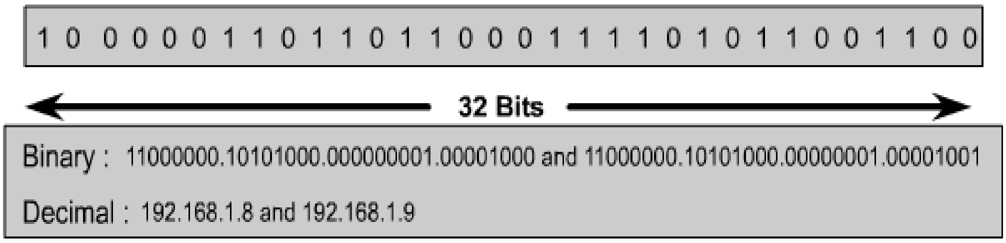
Remote login

- When the user wants to access an application program on a remote computer, then the user must perform remote login.



3.4 Concepts of IP Address

- An IP address is a 32-bit sequence of 1s and 0s.
- To make the IP address easier to use, the address is usually written as four decimal numbers separated by periods.
- This way of writing the address is called the dotted decimal format.



Binary : 11000000.10101000.000000001.00001000 and 11000000.10101000.0000001.00001001

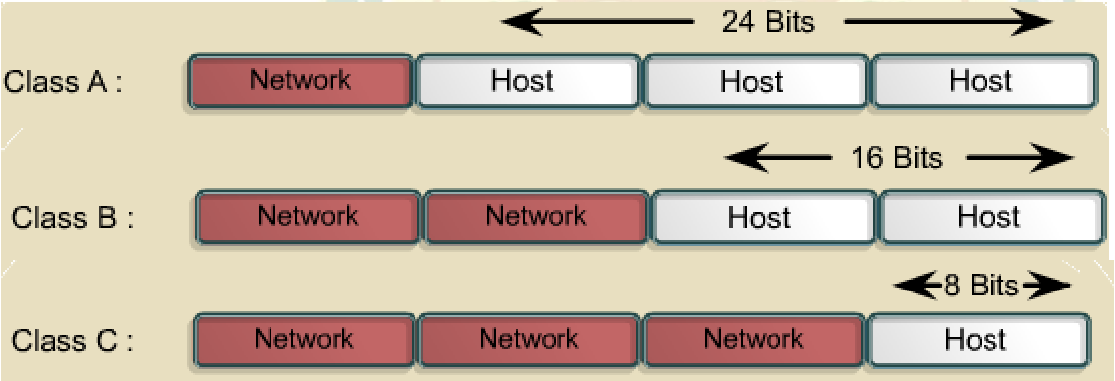
Decimal : 192.168.1.8 and 192.168.1.9

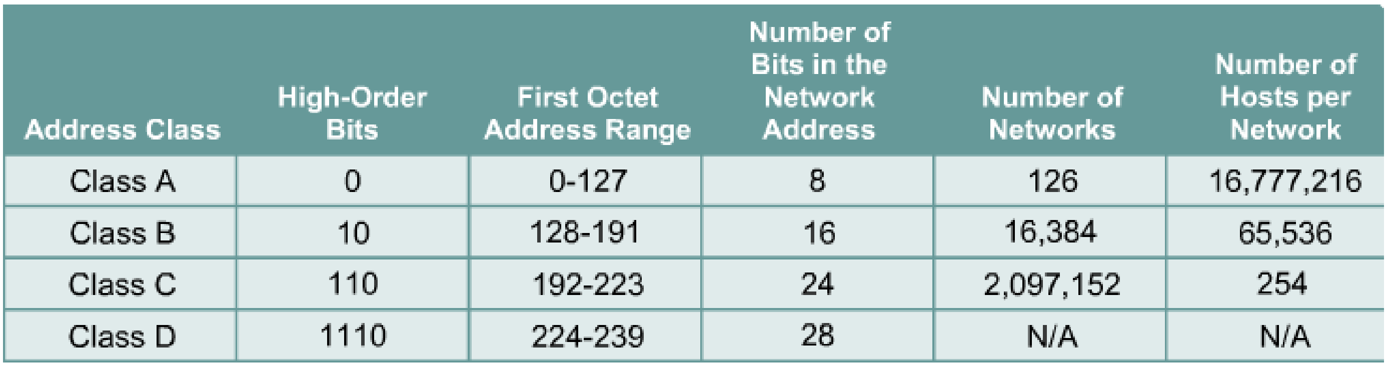
Every IP address has two parts:

Network

Host

- IP addresses are divided into classes A, B and C to define large, medium, and small networks.
- The Class D address class was created to enable multicasting. IETF reserves Class E addresses for its own research.





Address Class	High-Order Bits	First Octet Address Range	Number of Bits in the Network Address	Number of Networks	Number of Hosts per Network
Class A	0	0-127	8	126	16,777,216
Class B	10	128-191	16	16,384	65,536
Class C	110	192-223	24	2,097,152	254
Class D	1110	224-239	28	N/A	N/A

3.5 Difference between HTTP and HTTPs

HTTP	HTTPS
The full form of HTTP is the Hypertext Transfer Protocol.	The full form of HTTPS is Hypertext Transfer Protocol Secure.
It is written in the address bar as http://.	It is written in the address bar as https://.
The HTTP transmits the data over port number 80.	The HTTPS transmits the data over port number 443.
It is unsecured as the plain text is sent, which can be accessible by the hackers.	It is secure as it sends the encrypted data which hackers cannot understand.
It is mainly used for those websites that provide information like blog writing.	It is a secure protocol, so it is used for those websites that require to transmit the bank account details or credit card numbers.
It is an application layer protocol.	It is a transport layer protocol.
It does not use SSL.	It uses SSL that provides the encryption of the data.
Google does not give the preference to the HTTP websites.	Google gives preferences to the HTTPS as HTTPS websites are secure websites.
The page loading speed is fast.	The page loading speed is slow as compared to HTTP because of the additional feature that it supports, i.e., security.