

Unit-3: Mobile Ad hoc network**3.1 Concepts and types of MANET (Mobile Ad hoc network)****3.1.1 VANET (Vehicular Ad hoc Network)****3.1.2 Smart phone Ad hoc Network (SPANC)****3.1.3 Flying Ad hoc network (FANET)****3.2 Concepts of OSI (Open Source Interconnection) layers****3.2.1 Types of layers****3.2.2 Introduction of OSI Layers and their purpose:**

Physical layer, Data link layer and Network Layer

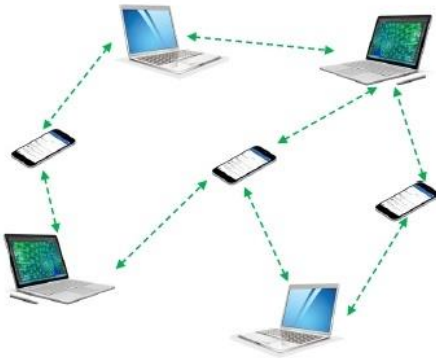
Transport layer and Session Layer.

3.3 Important protocols of Network layers**3.3.1 Concepts of Data packets and Datagram****3.3.2 Presentation layer protocols and their purpose:****3.3.2.1 SSL, HTTP, FTP, Telnet****3.3 Concepts of IP address****3.4 Difference between http and https**

What is ad-hoc network?

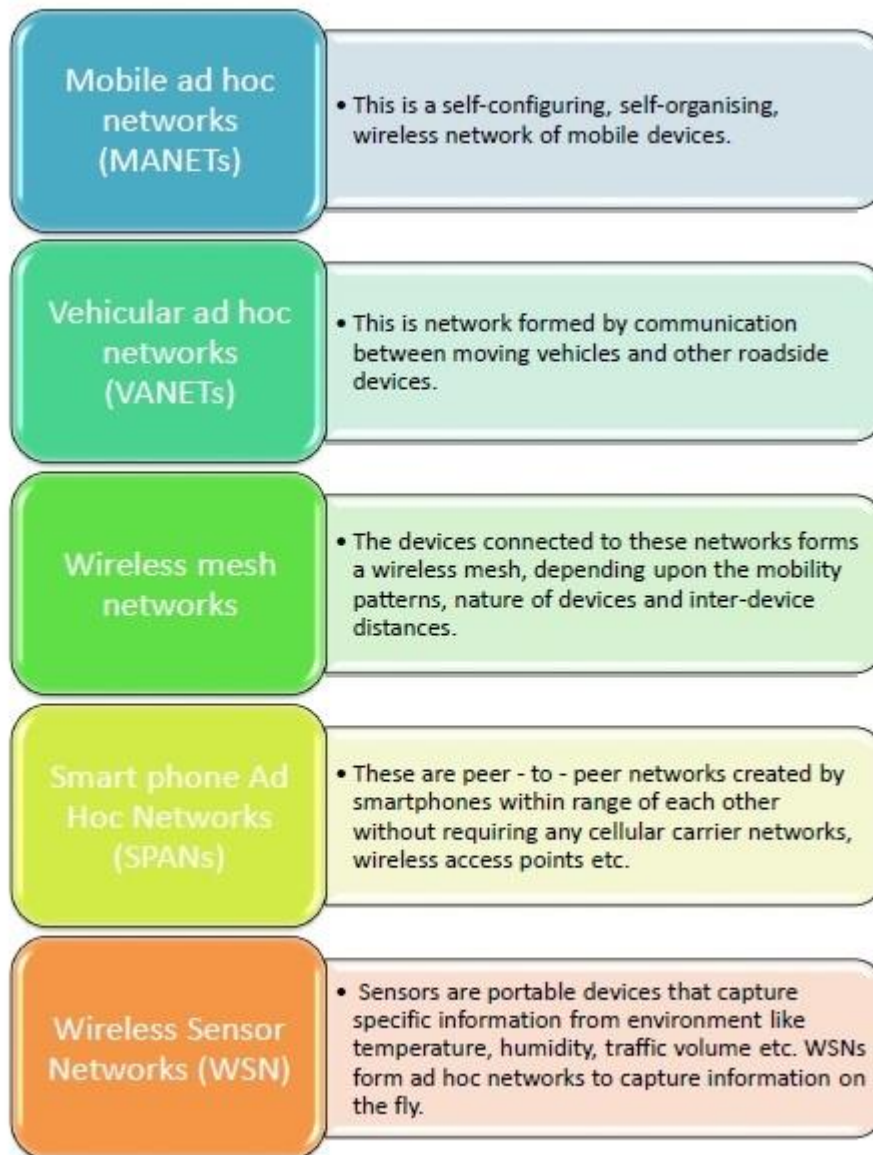
An ad hoc network is one that is when devices connect and communicate with each other. The term ad hoc is a Latin word that means "for this," implying improvised.

Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.



Classifications of Ad Hoc Networks

Ad hoc networks can be classified into several types depending upon the nature of their applications. The most prominent ad hoc networks that are commonly incorporated are illustrated in the diagram below –



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.

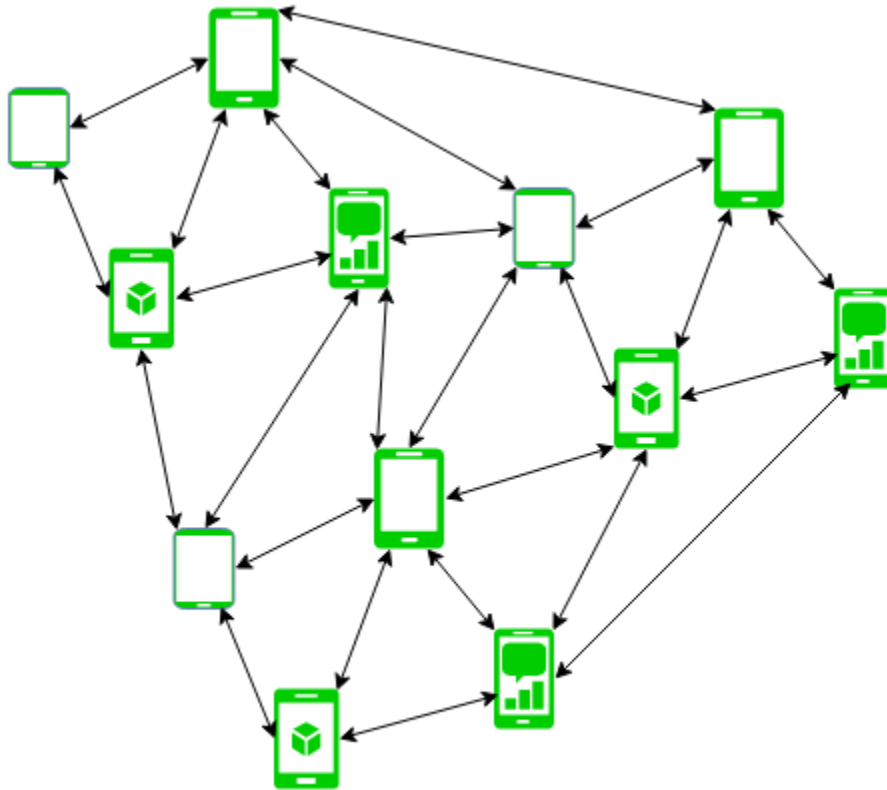


Figure - Mobile Ad Hoc Network

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 defense, 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. 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.

Pros and Cons of MANET –**Pros:**

- Separation from central network administration.
- Each node can play both the roles i.e. router and host showing autonomous nature.
- Self-configuring and self-healing nodes do not require human intervention.

Cons:

- Resources are limited due to various constraints like noise, interference conditions, etc.
- Lack of authorization facilities.
- More prone to attacks due to limited physical security.

Types of MANET –

Vehicular Ad hoc Network (VANETs) –
Enable effective communication with another vehicle or with the roadside equipments. Intelligent vehicular ad hoc networks (In VANETs) deals with another vehicle or with roadside equipments.

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.

Internet based Mobile Ad hoc Network (iMANETs) –
It supports internet protocols such as TCP/UDP and IP. To link mobile nodes and establish routes distributed and automatically.

Hub-Spoke MANET:
Multiple sub MANET's may be connected in hub-spoke VPN to create a geographically distributed MANET. Normal Ad-hoc routing algorithm does not apply directly.

Military or Tactical MANETs –
This is used by the military units. Emphasis on data rate, real-time demand, fast re-routing during mobility, security, radio range, etc.

Flying Ad hoc Network (FANETs) –
This is composed of unmanned aerial vehicles (commonly known as drones). Provides links to remote areas and mobility.

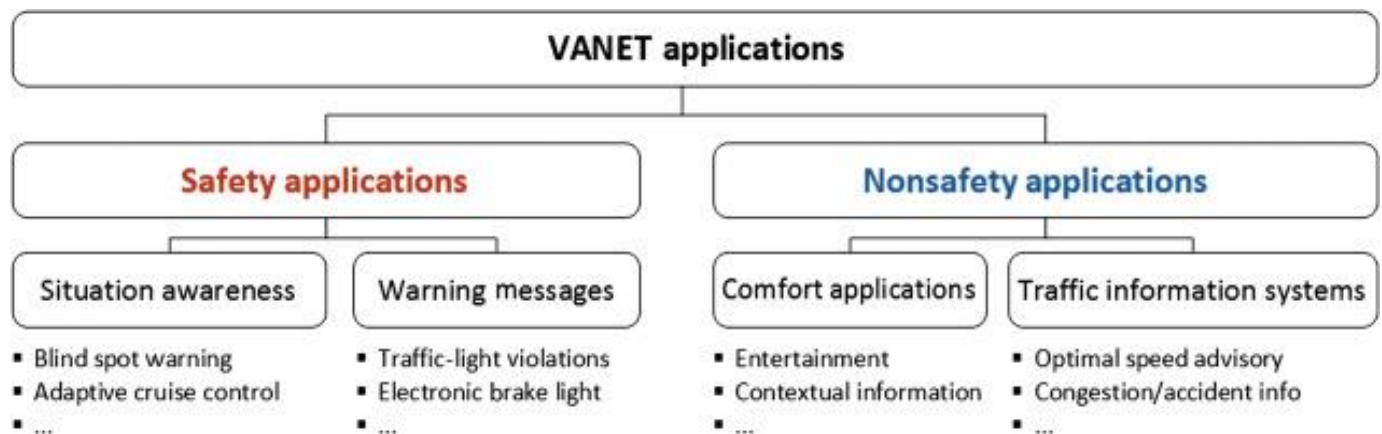
VANET in wireless network

A vehicular ad hoc network (VANET) consists of **groups of moving or stationary vehicles connected by a wireless network**. Until recently the main use of VANETs was to provide safety and comfort to drivers in vehicular environments.

VANET is similar to MANET in terms, that is also do not need any infrastructure for data transmission. VANET play important role in aspect of safe driving, intelligent navigation, emergency and entertainment applications .It can be defined as an intelligent component of transport system as vehicle are able to communicate with each other as well as roadside base station, which are located at critical points of the road. Example :-Intersection and Construction Sites.



VANET Application



Difference between MANET and VANET :

SR. No.	MANET	VANET
1	Production cost of MANET is cheap as compared to VANET	Much Expensive
2	Mobility of MANET is low as it make bit difficult for network enables the serving networks to locate a mobile subscriber's point.	High Mobility, as serving networks to locate a mobile subscriber's point is easy.
3	Change in network topology orientation is slow.	Frequent and very fast change of network topology,
4	Sparse node density.	Node density is frequent variables.
5	It ranges Upto 100 m.	500 m range available in VANET.
6	MANET node lifetime depends on power resources.	Depend on lifetime vehicle.
7	MANET have medium reliability.	High reliability of VANET.
8	Attribute Based addressing scheme.	Location Bases addressing scheme.
9	Position acquisition is obtained using Ultrasonic.	VANET maintain position acquisition by using GPS, RADAR.
10	Availability of Multi-hop Routing	Weakly available Multi-hop Routing.

Smart Phone Ad-hoc Networking (SPAN)

SPAN provides an Android framework for secure peer-to-peer communication between devices over a Wi-Fi mesh network. The result is a headless, infrastructure-less, self-healing network that dynamically links common smart phones and tablets together. SPAN can be used to share Internet connectivity between peers if and when it is available.

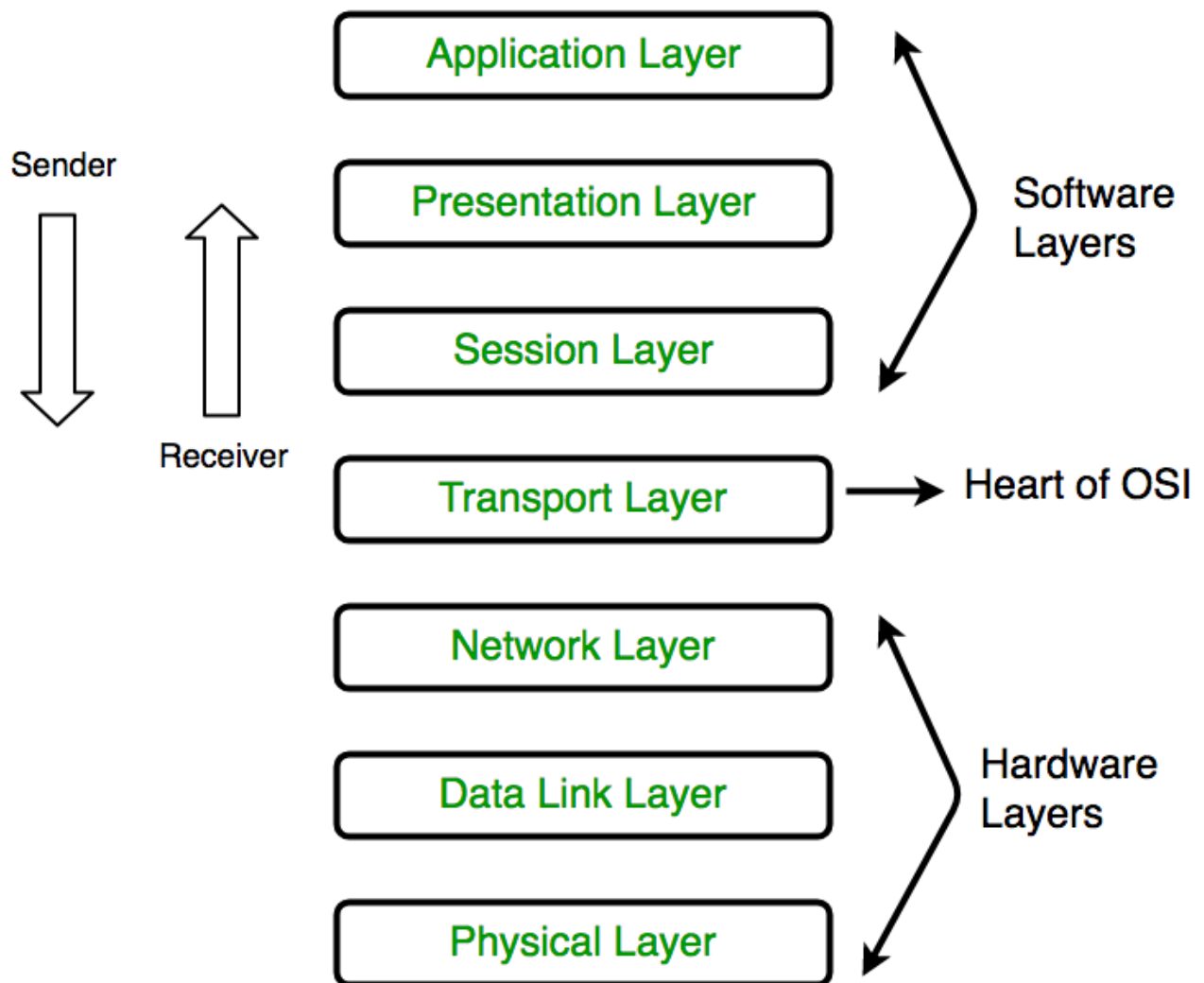
Flying ad hoc network (FANET)

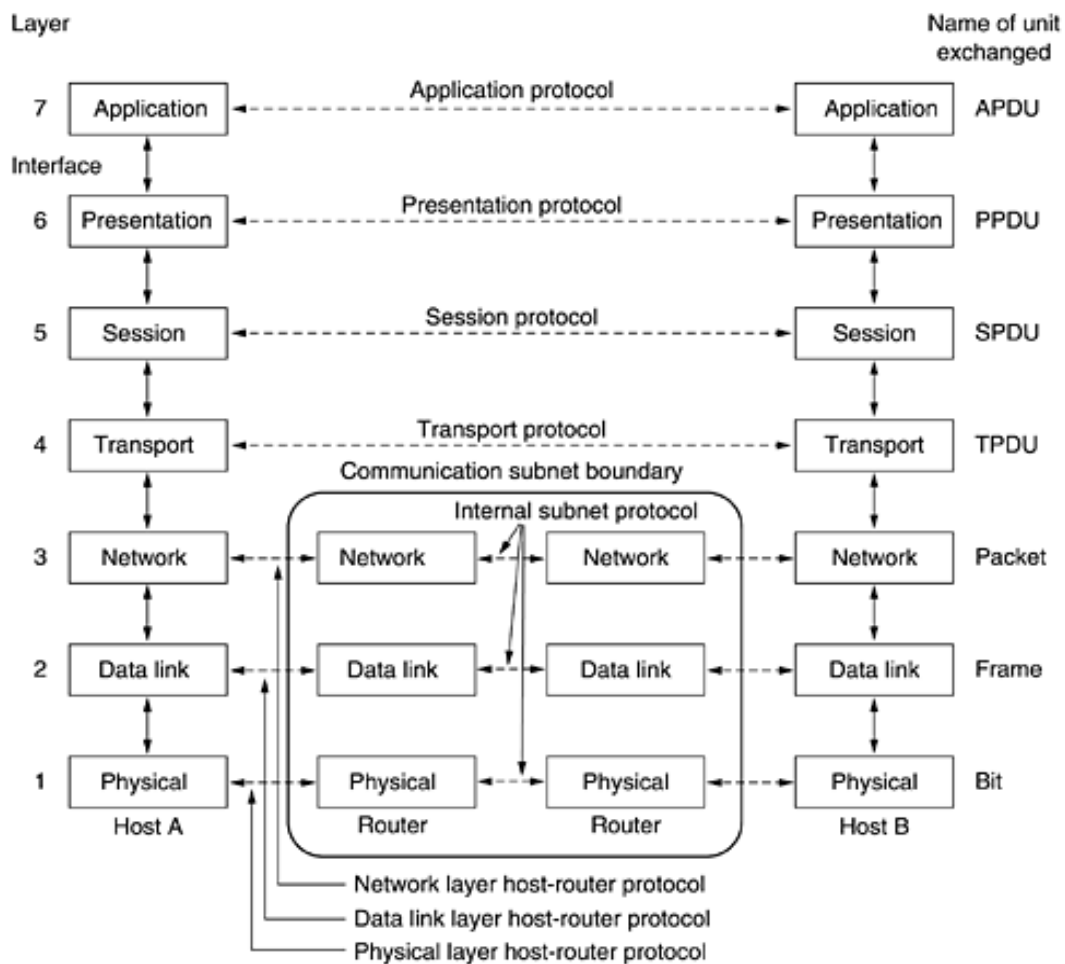
A Flying Ad hoc Networks (FANETs) is **such kind of network that consists of a group of small UAVs connected in ad-hoc manner, which are integrated into a team to achieve high level goals.**

Concepts of OSI Model (Open System Interconnection)

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – ‘**International Organization for Standardization**’, in the year 1984. It is 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work to transmit the data from one person to another across the globe.

Types of Layers

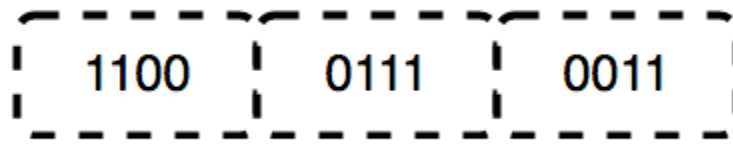




Introduction of OSI Layers and their Purpose

1. Physical Layer (Layer 1):

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits**. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are as follows:

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

* Hub, Repeater, Modem, Cables are Physical Layer devices.

** Network Layer, Data Link Layer, and Physical Layer are also known as Lower Layers or Hardware Layers.

2. Data Link Layer (DLL) (Layer 2) :

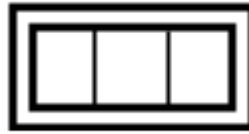
The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sublayers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of NIC (Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.



The functions of the Data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC address) of the sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

* *Packet in Data Link Layer is referred to as Frame.*

** *Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*

*** *Switch & Bridge are Data Link Layer devices.*

3. Network Layer (Layer 3) :

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

* *Segment in Network layer is referred to as Packet.*



**** Network layer is implemented by networking devices such as routers.**

4. Transport Layer (Layer 4) :

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

At sender's side: Transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

***Note:** The sender needs to know the port number associated with the receiver's application.*

Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

At receiver's side: Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are as follows:

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. **Service Point Addressing:** In order to deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

A. Connection-Oriented Service: It is a three-phase process that includes

- Connection Establishment
- Data Transfer
- Termination / disconnection

In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

B. Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

** Data in the Transport Layer is called as **Segments**.*

*** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*

*Transport Layer is called as **Heart of OSI model**.*

5. Session Layer (Layer 5) :

This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.

The functions of the session layer are :

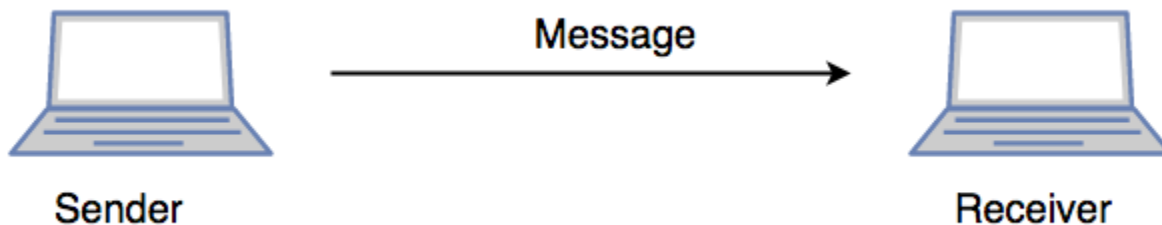
1. **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered synchronization points into the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

***All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as “Application Layer”.*

***Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers** or **Software Layers**.*

Scenario:

Let us consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0’s and 1’s) so that it can be transmitted.



6. Presentation Layer (Layer 6):

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The functions of the presentation layer are :

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.

***Application Layer is also called Desktop Layer.*



The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented on the Internet because of its late invention. The current model being used is the TCP/IP model.

No.	Layer Name	Responsibility	Information Form (Data Unit)	Device
7	Application Layer	Helps in identifying the client and synchronize communication	Message	-
6	Presentation Layer (Translation Layer)	Data from application layer is extracted and manipulated as required format for transmission	Message	-
5	Session Layer	Establishes connection, maintenance, authentication and ensure security	Message	Gateway
4	Transport Layer (HEART of OSI)	Take service from network layer and provide it to application layer	Segment	Firewall
3	Network Layer	Transmission of data from one host to other. Located in different network	Packet	Router
2	Data Link Layer	Node to node delivery of messages	Frame	Switch, Bridge
1	Physical Layer	Establishing physical connection between devices	Bits	Hub, Repeater, Modem, Cables

OSI model summarized (table form)

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.

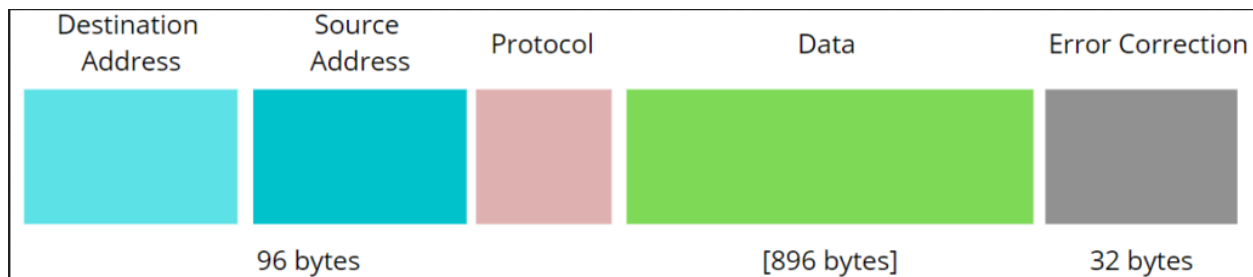
It makes it easier to retransmit lost pieces of data or interrupted ones. Packets are data units within the network layer in the OSI model.

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:

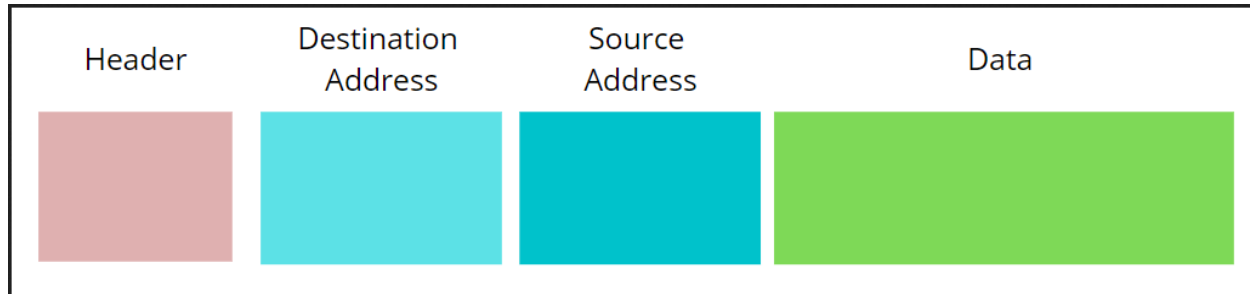


Datagram

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:



Presentation layer protocols and their purpose:

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 CipherSpec 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.

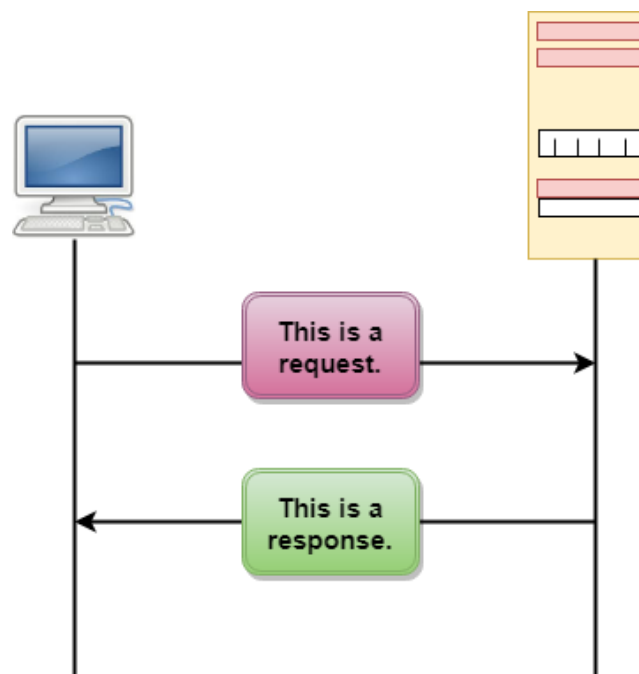
Features of HTTP:

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. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

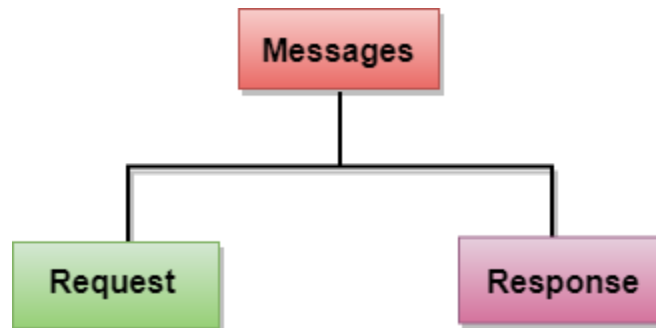
HTTP Transactions



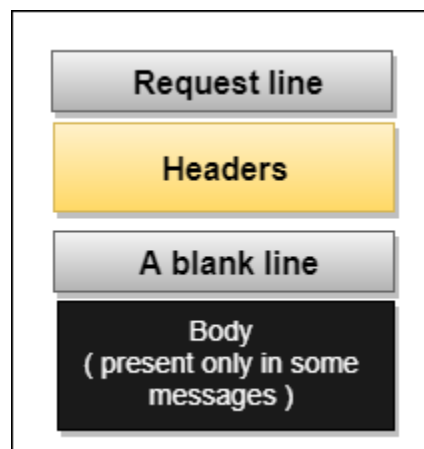
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Messages

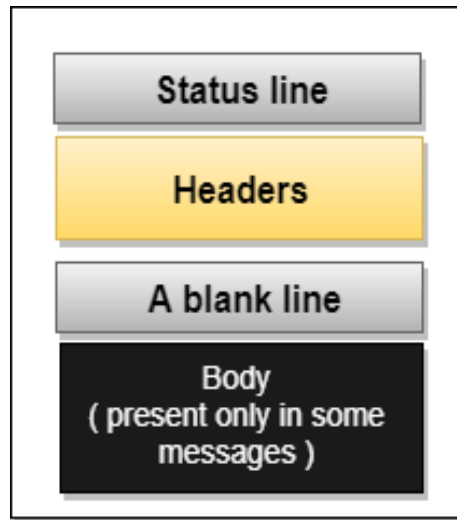
HTTP messages are of two types: request and response. Both the message types follow the same message format.



Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.



Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



FTP

FTP stands for File transfer protocol.

FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.

It is also used for downloading the files to computer from other servers.

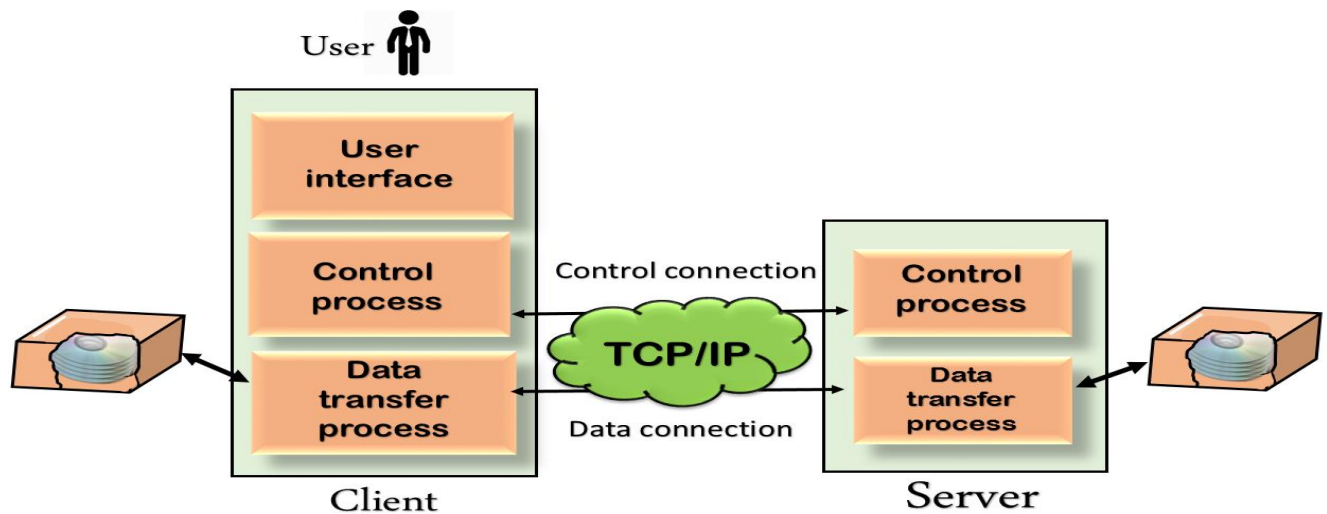
Objectives of FTP

It provides the sharing of files.

It is used to encourage the use of remote computers.

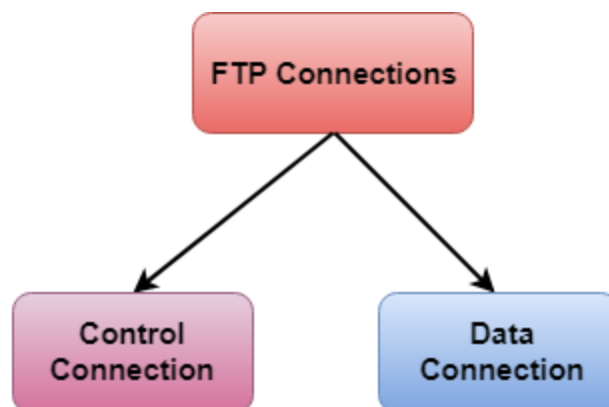
It transfers the data more reliably and efficiently.

Mechanism of FTP



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:



Control Connection: The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

Data Connection: The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.

It allows a user to connect to a remote host and upload or download the files.

It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.

The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

Speed: One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.

Efficient: It is more efficient as we do not need to complete all the operations to get the entire file.

Security: To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.

Back & forth movement: FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provide encryption.

FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.

Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.

It is not compatible with every system.

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.

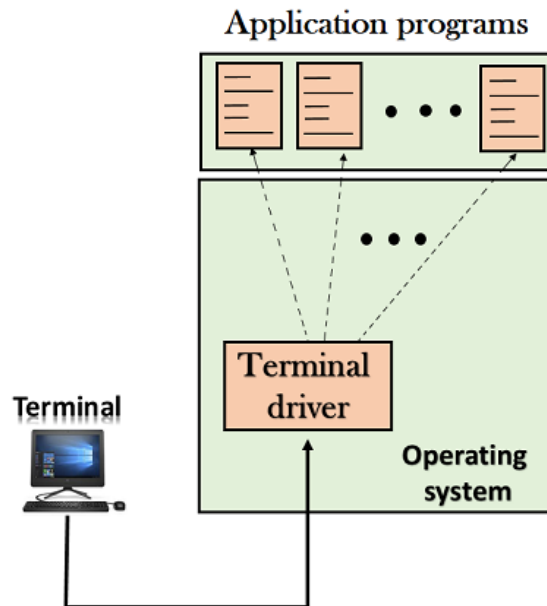
There are two types of login:

Local Login

When a user logs into a local computer, then it is known as local login.

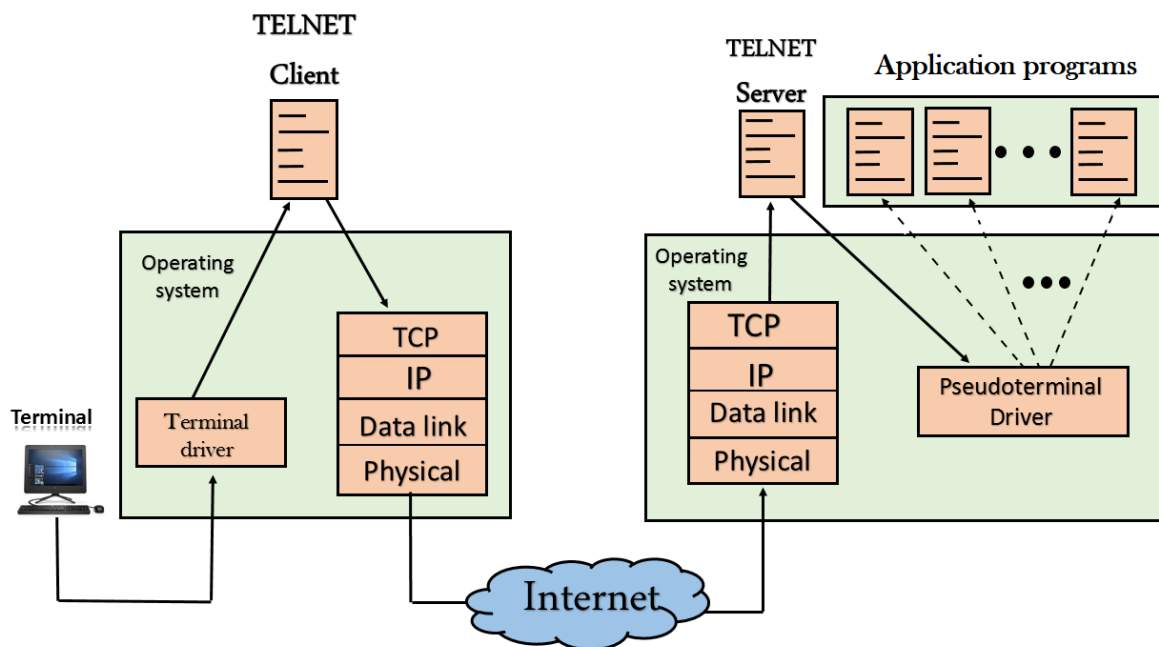
When the workstation running terminal emulator, the keystrokes entered by the user are accepted by the terminal driver. The terminal driver then passes these characters to the operating system which in turn, invokes the desired application program.

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.



How remote login occurs

At the local site

The user sends the keystrokes to the terminal driver, the characters are then sent to the TELNET client. The TELNET client which in turn, transforms the characters to a universal character set known as network virtual terminal characters and delivers them to the local TCP/IP stack

At the remote site

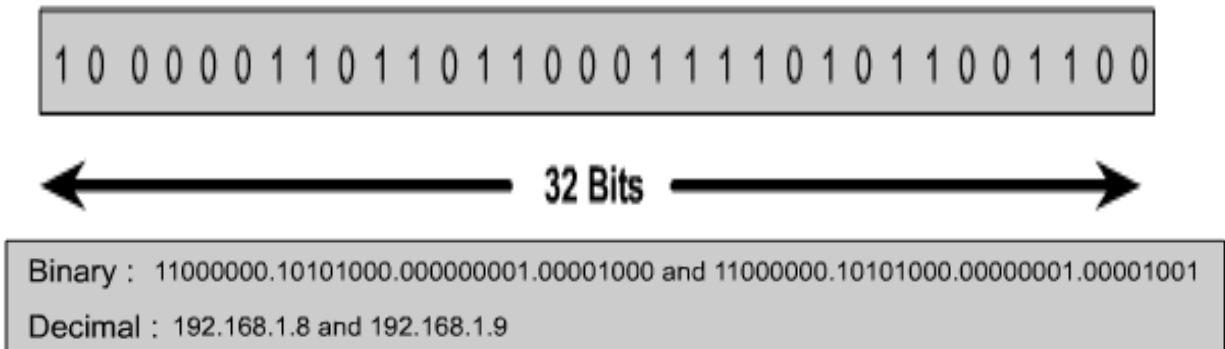
The commands in NVT (Network Virtual Terminal) forms are transmitted to the TCP/IP at the remote machine. Here, the characters are delivered to the operating system and then pass to the TELNET server. The TELNET server transforms the characters which can be understandable by a remote computer. However, the characters cannot be directly passed to the operating system as a remote operating system does not receive the characters from the TELNET server. Therefore it requires some piece of software that can accept the characters from the TELNET server. The operating system then passes these characters to the appropriate application program.

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.



Every IP address has two parts:

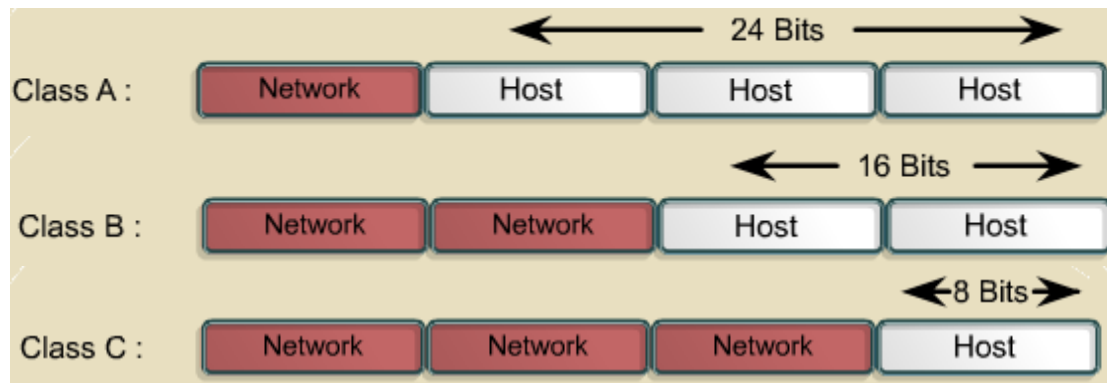
Network

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

An [IP](#) address is the identifier that enables your device to send or receive data packets across the internet. It holds information related to your location and therefore making devices available for two-way communication. The internet requires a process to distinguish between different networks, routers, and websites. Therefore, IP addresses provide the mechanism of doing so, and it forms an indispensable part in the working of the internet. You will notice that most of the IP addresses are essentially numerical. Still, as the world is witnessing a colossal growth of network users, the network developers had to add letters and some addresses as internet usage grows.

An IP address is represented by a series of numbers segregated by periods (.). They are expressed in the form of four pairs - an example address might be 255.255.255.255 wherein each set can range from 0 to 255.

[IP](#) addresses are not produced randomly. They are generated mathematically and are further assigned by the IANA (Internet Assigned Numbers Authority), a department of the ICANN.

ICANN stands for Internet Corporation for Assigned Names and Numbers. It is a non-profit corporation founded in the US back in 1998 with an aim to manage Internet security and enable it to be available by all.

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.