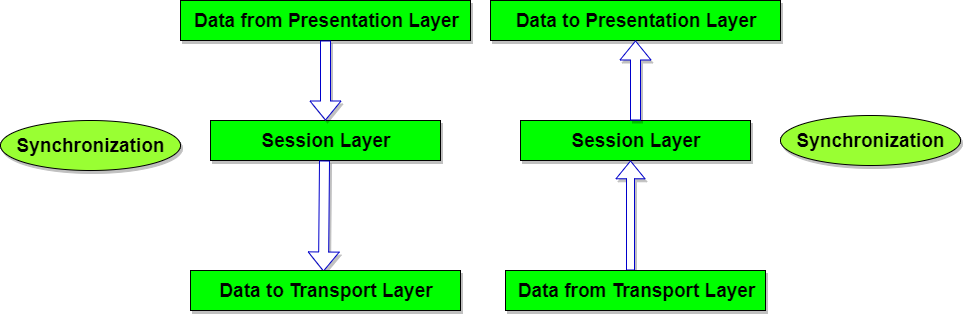
Session Layer - OSI Model

The Session Layer allows users on different machines to establish active communication sessions between them.

It's main aim is to establish, maintain and synchronize the interaction between communicating systems. Session layer manages and synchronize the conversation between two different applications. In 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.

Functions of Session Layer

1. **Dialog Control :**This layer allows two systems to start communication with each other in half-duplex or full-duplex.
2. **Token Management:**This layer prevents two parties from attempting the same critical operation at the same time.
3. **Synchronization :**This layer allows a process to add checkpoints which are considered as synchronization points into stream of data. Example: If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended. This ensures that 50 page unit is successfully received and acknowledged. This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.



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.
* To provide services such as **Token management** and **Synchronization**.

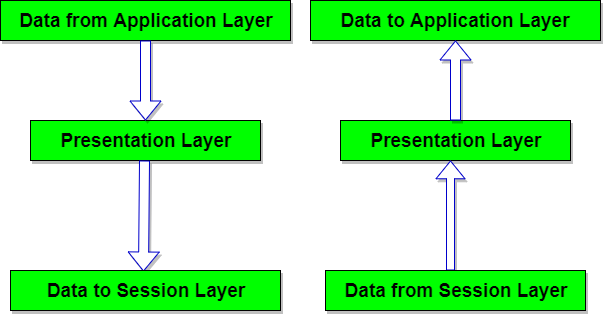
Presentation Layer - OSI Model

The primary goal of this layer is to take care of the **syntax** and **semantics** of the information exchanged between two communicating systems. 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. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role translator.

In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an **abstract** way. The presentation layer manages these **abstract data structures** and allows higher-level data structures(eg: banking records), to be defined and exchanged.

Functions of Presentation Layer

1. **Translation:** Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.
2. **Encryption:** It carries out encryption at the transmitter and decryption at the receiver.
3. **Compression:** It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of Data compression is to reduce the number of bits to be 0transmitted. It is important in transmitting multimedia such as audio, video, text etc.



Design Issues with Presentation Layer

* To manage and maintain the **Syntax** and **Semantics** of the information transmitted.
* **Encoding data** in a standard agreed upon way. Eg: String, double, date, etc.
* Perform **Standard Encoding** on wire.

The presentation layer (Layer 6) ensures that the message is presented to the upper layer in a standardized format. It deals with the syntax and the semantics of the messages.

The main functions of the presentation layer are as follows −

* It encodes the messages from the user dependent format to the common format and vice versa, for communication among dissimilar systems.
* It is responsible for data encryption and decryption of sensitive data before they are transmitted over common channels.
* It is also responsible for data compression. Data compression is done at the source to reduce the number of bits to be transmitted. It reduces the storage space and increases the file transfer rate. It is particularly useful for transmission of large multimedia files.

[**next →**](https://www.javatpoint.com/computer-network-client-and-server-model)[**← prev**](https://www.javatpoint.com/computer-network-transport-layer-protocols)

Application Layer

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers.

The Application layer includes the following functions:

* **Identifying communication partners:** The application layer identifies the availability of communication partners for an application with data to transmit.
* **Determining resource availability:** The application layer determines whether sufficient network resources are available for the requested communication.
* **Synchronizing communication:** All the communications occur between the applications requires cooperation which is managed by an application layer.

Services of Application Layers

* **Network Virtual terminal:** An application layer allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which in turn, talks to the host. The remote host thinks that it is communicating with one of its own terminals, so it allows the user to log on.
* **File Transfer, Access, and Management (FTAM):** An application allows a user to access files in a remote computer, to retrieve files from a computer and to manage files in a remote computer. FTAM defines a hierarchical virtual file in terms of file structure, file attributes and the kind of operations performed on the files and their attributes.
* **Addressing:** To obtain communication between client and server, there is a need for addressing. When a client made a request to the server, the request contains the server address and its own address. The server response to the client request, the request contains the destination address, i.e., client address. To achieve this kind of addressing, DNS is used.
* **Mail Services:** An application layer provides Email forwarding and storage.
* **Directory Services:** An application contains a distributed database that provides access for global information about various objects and services.

Authentication: It authenticates the sender or receiver's message or both.

Network Application Architecture

Application architecture is different from the network architecture. The network architecture is fixed and provides a set of services to applications. The application architecture, on the other hand, is designed by the application developer and defines how the application should be structured over the various end systems.

**Application architecture is of two types:**

* **Client-server architecture:** An application program running on the local machine sends a request to another application program is known as a client, and a program that serves a request is known as a server. For example, when a web server receives a request from the client host, it responds to the request to the client host.

**Characteristics Of Client-server architecture:**

* In Client-server architecture, clients do not directly communicate with each other. For example, in a web application, two browsers do not directly communicate with each other.
* A server is fixed, well-known address known as IP address because the server is always on while the client can always contact the server by sending a packet to the sender's IP address.

**Disadvantage Of Client-server architecture:**

It is a single-server based architecture which is incapable of holding all the requests from the clients. For example, a social networking site can become overwhelmed when there is only one server exists.

* **P2P (peer-to-peer) architecture:** It has no dedicated server in a data center. The peers are the computers which are not owned by the service provider. Most of the peers reside in the homes, offices, schools, and universities. The peers communicate with each other without passing the information through a dedicated server, this architecture is known as peer-to-peer architecture. The applications based on P2P architecture includes file sharing and internet telephony.

Features of P2P architecture

* **Self scalability:** In a file sharing system, although each peer generates a workload by requesting the files, each peer also adds a service capacity by distributing the files to the peer.
* **Cost-effective:** It is cost-effective as it does not require significant server infrastructure and server bandwidth.

Client and Server processes

* A network application consists of a pair of processes that send the messages to each other over a network.
* In P2P file-sharing system, a file is transferred from a process in one peer to a process in another peer. We label one of the two processes as the client and another process as the server.
* With P2P file sharing, the peer which is downloading the file is known as a client, and the peer which is uploading the file is known as a server. However, we have observed in some applications such as P2P file sharing; a process can be both as a client and server. Therefore, we can say that a process can both download and upload the files.

# Protocols in Application Layer

Last Updated: 29-07-2020

### Application Layer:-

The application layer is present at the top of the OSI model. It is the layer through which users interact. It provides services to the user.

### Application Layer protocol:-

#### 1. TELNET:

Telnet stands for the **TEL**ecomunications **NET**work. It helps in terminal emulation. It allows Telnet client to access the resources of the Telnet server. It is used for managing the files on the internet. It is used for initial set up of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.  
**Command**

telnet [\\RemoteServer]

\\RemoteServer : Specifies the name of the server to which you want to connect

#### 2. FTP:

FTP stands for file transfer protocol. It is the protocol that actually lets us transfer files.It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program.FTP promotes sharing of files via remote computers with reliable and efficient data transfer. Port number for FTP is 20 for data and 21 for control.

**Command**

ftp machinename

#### 3. TFTP:

The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it’s the protocol of choice if you know exactly what you want and where to find it. It’s a technology for transferring files between network devices and is a simplified version of FTP

**Command**

tftp [ options... ] [host [port]] [-c command]

#### 4. NFS:

It stands for network file system.It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the network.

**Command**

service nfs start

#### 5. SMTP:

It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called “store and forward,” SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. Port number for SMTP is 25.

**Command**

MAIL FROM:<mail@abc.com?

#### 6. LPD:

It stands for Line Printer Daemon.It is designed for printer sharing.It is the part that receives and processes the request. A “daemon” is a server or agent.

**Command**

lpd [ -d ] [ -l ] [ -D DebugOutputFile]

#### 7. X window:

It defines a protocol for the writing of graphical user interface–based client/server applications. The idea is to allow a program, called a client, to run on one computer. It is primarily used in networks of interconnected mainframes.

**Command**

Run xdm in runlevel 5

#### 8. SNMP:

It stands for Simple Network Management Protocol. It gathers data by polling the devices on  
the network from a management station at fixed or random intervals, requiring  
them to disclose certain information. It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defined values. Port number of SNMP is 161(TCP) and 162(UDP).  
**Command**

snmpget -mALL -v1 -cpublic snmp\_agent\_Ip\_address sysName.0

#### 9. DNS:

It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.abc.com might translate to 198.105.232.4.  
Port number for DNS is 53.  
**Command**

ipconfig /flushdns

#### 10. DHCP:

It stands for Dynamic Host Configuration Protocol (DHCP).It gives IP addresses to hosts.There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68.

**Command**

clear ip dhcp binding {address | \* }

[**next →**](https://www.javatpoint.com/computer-network-security)[**← prev**](https://www.javatpoint.com/simple-network-management-protocol)

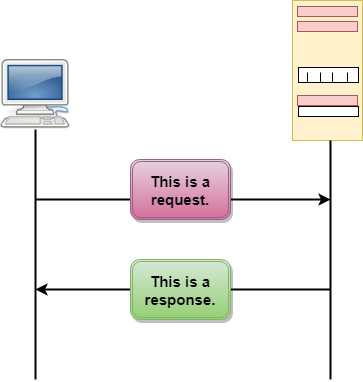
# HTTP

* 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.

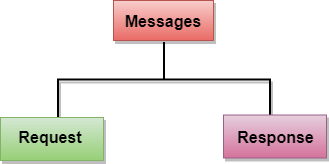
## HTTP Transactions



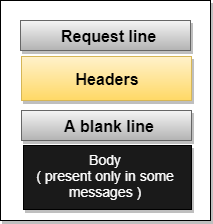
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

## Messages

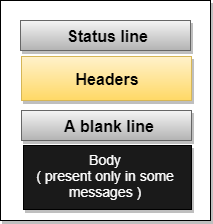
HTTP messages are of two types: request and response. Both the message types follow the same message format.



**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.



## Uniform Resource Locator (URL)

* A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
* The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
* The URL defines four parts: method, host computer, port, and path.



* **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
* **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
* **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
* **Path:** Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

Domain Name System (DNS) in Application Layer

Last Updated: 29-07-2020

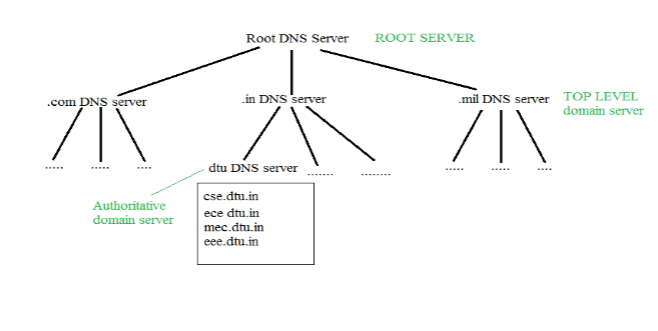
DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

**Requirement**

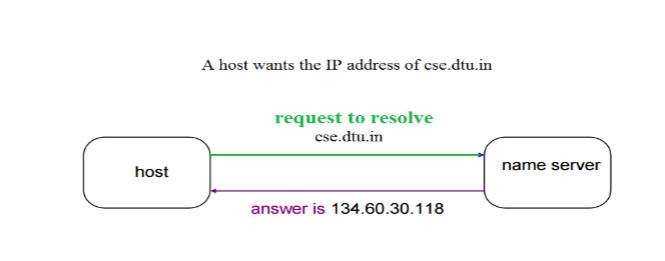
Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

**Domain :**  
There are various kinds of DOMAIN :

1. Generic domain : .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.
2. Country domain .in (india) .us .uk
3. Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping.So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.

**Organization of Domain**  
[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/gq/2017/02/DNS.png)  
It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately,  
there should not be a lot of delay for that to happen organization of database is very important.  
**DNS record** – Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.

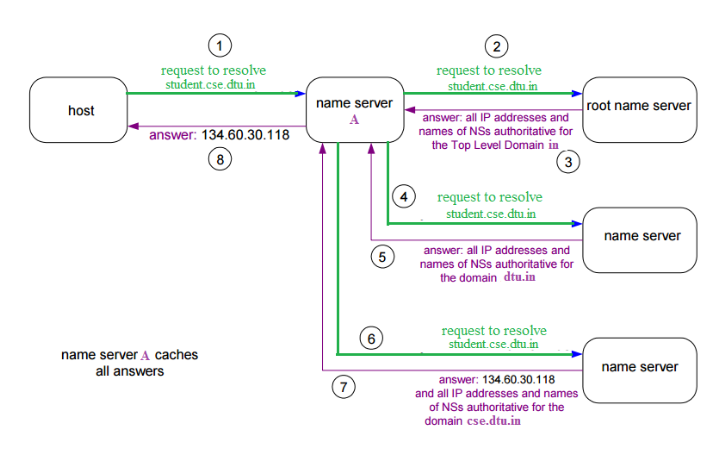
**Namespace** – Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –

**Name server** – It is an implementation of the resolution mechanism.. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.  
  
**Name to Address Resolution**  
[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/gq/2017/02/DNS_2.png)  
The host request the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.  
  
**Hierarchy of Name Servers**  
**Root name servers**– It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.

**Top level server** – It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.

**Authoritative name servers** This is organization’s DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.

**Domain Name Server**

[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/gq/2017/02/DNS_3.png)  
The client machine sends a request to the local name server, which , if root does not find the address in its database, sends a request to the root name server , which in turn, will route the query to an intermediate or authoritative name server. The root name server can also contain some hostName to IP address mappings . The intermediate name server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [**next →**](https://www.javatpoint.com/computer-network-ftp)[**← prev**](https://www.javatpoint.com/computer-network-client-and-server-model) DNS An application layer protocol defines how the application processes running on different systems, pass the messages to each other.   * DNS stands for Domain Name System. * DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address. * DNS is required for the functioning of the internet. * Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots. * DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses. * For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.   DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.  Computer Network DNS Generic Domains  * It defines the registered hosts according to their generic behavior. * Each node in a tree defines the domain name, which is an index to the DNS database. * It uses three-character labels, and these labels describe the organization type.  |  |  | | --- | --- | | **Label** | **Description** | | aero | Airlines and aerospace companies | | biz | Businesses or firms | | com | Commercial Organizations | | coop | Cooperative business Organizations | | edu | Educational institutions | | gov | Government institutions | | info | Information service providers | | int | International Organizations | | mil | Military groups | | museum | Museum & other nonprofit organizations | | name | Personal names | | net | Network Support centers | | org | Nonprofit Organizations | | pro | Professional individual Organizations |   Computer Network DNS Country Domain The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations. Inverse Domain The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name. Working of DNS  * DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client. * Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups. * DNS implements a distributed database to store the name of all the hosts available on the internet. * If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol. |

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.

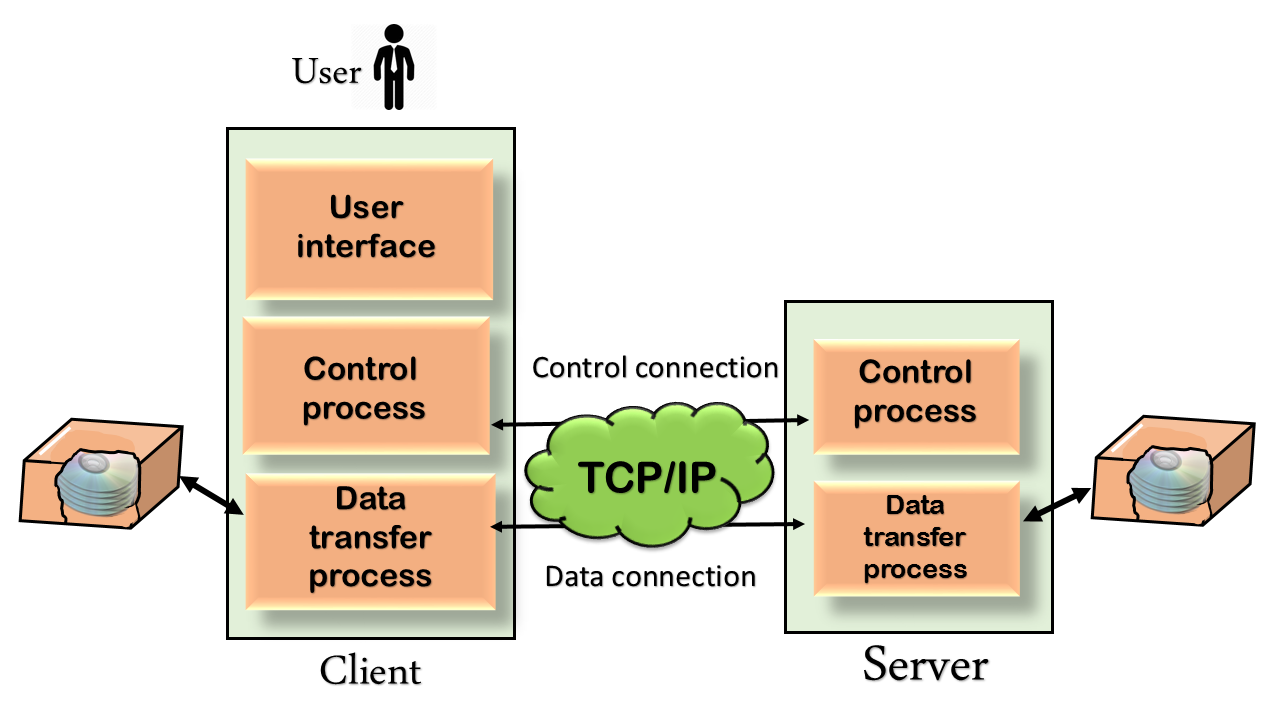
Objectives of FTP

* It provides the sharing of files.
* It is used to encourage the use of remote computers.
* It transfers the data more reliably and efficiently.

Why FTP?

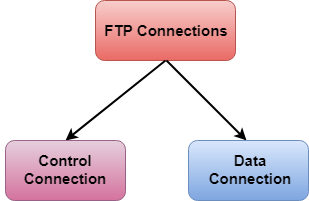
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

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 provides 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.

**Trivial File Transfer Protocol (TFTP)**

**Last Updated:** November 12, 2012

**Definition - What does *Trivial File Transfer Protocol (TFTP)* mean?**

Trivial File Transfer Protocol (TFTP) is a simple protocol used for transferring files. TFTP uses the User Datagram Protocol (UDP) to transport data from one end to another. TFTP is mostly used to read and write files/mail to or from a remote server.

File transfer is one of the most essential technologies for client/server and computer network infrastructures.  
  
Trivial File Transfer Protocol is very simple in design and has limited features as compared to File Transfer Protocol (FTP). TFTP provides no authentication and security while transferring files. As a result, it is usually used for transferring boot files or configuration files between machines in a local setup. Because of its simple design, it is rarely used interactively by users in a computer network. Its lack of security also makes it dangerous for use over the Internet.  
  
TFTP is very useful for boot computers and devices that do not have hard disk drives or storage devices because it can easily be implemented using a small amount of memory. This characteristic of TFTP makes it one of the core elements of network boot protocol, or preboot execution environment (PXE).  
  
Data transfer through TFTP is usually initiated through port 69. However, the data transfer ports are selected by the sender and receiver when the connection is initialized.

|  |  |  |
| --- | --- | --- |
| **S.NO** | **FTP** | **TFTP** |
| 1. | FTP stands for File Transfer Protocol. | TFTP stands for Trivial File Transfer Protocol. |
| 2. | The software of FTP is larger than TFTP. | While software of TFTP is smaller than FTP. |
| 3. | FTP works on two ports: 20 and 21. | While TFTP works on 69 Port number. |
| 4. | FTP services are provided by TCP. | While TFTP services are provided by UDP. |
| 5. | The complexity of FTP is higher than TFTP. | While the complexity of TFTP is less than FTP complexity. |
| 6. | There are many commands or messages in FTP. | There are only 5 messages in TFTP. |
| 7. | FTP need authentication for communication. | While TFTP does not need authentication for communication. |
| 8. | FTP is generally suited for uploading and downloading of files by remote users. | While TFTP is mainly used for transmission of configurations to and from network devices. |

Simple Mail Transfer Protocol (SMTP)

Last Updated: 23-04-2019

Email is emerging as one of the most valuable services on the internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver’s side.

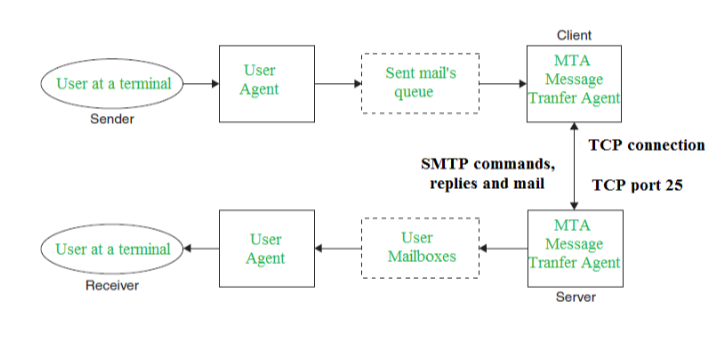
**SMTP Fundamentals**  
SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

**SMTP Protocol**

The SMTP model is of two type :

1. End-to- end method
2. Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method are used within an organization. A SMTP client who wants to send the mail will contact the destination’s host SMTP directly in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver’s SMTP.  
The client SMTP is the one which initiates the session let us call it as the client- SMTP and the server SMTP is the one which responds to the session request and let us call it as receiver-SMTP. The client- SMTP will start the session and the receiver-SMTP will respond to the request.  
  
**Model of SMTP system**

In the SMTP model user deals with the user agent (UA) for example Microsoft Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the MTA it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.  
[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/gq/2017/02/SMTP_1.png)

**Both the SMTP-client and MSTP-server should have 2 components:**

1. User agent (UA)
2. Local MTA

**Communication between sender and the receiver :**  
The senders, user agent prepare the message and send it to the MTA. The MTA functioning is to transfer the mail across the network to the receivers MTA. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.  
  
**SENDING EMAIL:**  
Mail is sent by a series of request and response messages between the client and a server. The message which is sent across consists of a header and the body. A null line is used to terminate the mail header. Everything which is after the null line is considered as the body of the message which is a sequence of ASCII characters. The message body contains the actual information read by the receipt.

**RECEIVING EMAIL:**  
The user agent at the server side checks the mailboxes at a particular time of intervals. If any information is received it informs the user about the mail. When the user tries to read the mail it displays a list of mails with a short description of each mail in the mailbox. By selecting any of the mail user can view its contents on the terminal.

[**next →**](https://www.javatpoint.com/udp-protocol)[**← prev**](https://www.javatpoint.com/http-vs-https)

# RIP Protocol

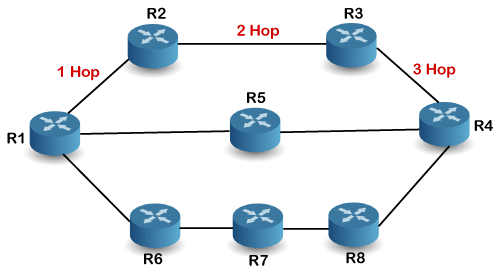
RIP stands for Routing Information Protocol. RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area. To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing table.

**Before understanding the structure of the packet, we first look at the following points:**

* RIP is based on the distance vector-based strategy, so we consider the entire structure as a graph where nodes are the routers, and the links are the networks.
* In a routing table, the first column is the destination, or we can say that it is a network address.
* The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.
* In RIP, infinity is defined as 16, which means that the RIP is useful for smaller networks or small autonomous systems. The maximum number of hops that RIP can contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.
* The next column contains the address of the router to which the packet is to be sent to reach the destination.

### How is hop count determined?

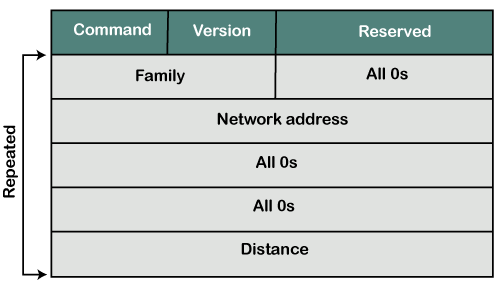
When the router sends the packet to the network segment, then it is counted as a single hop.



In the above figure, when the router 1 forwards the packet to the router 2 then it will count as 1 hop count. Similarly, when the router 2 forwards the packet to the router 3 then it will count as 2 hop count, and when the router 3 forwards the packet to router 4, it will count as 3 hop count. In the same way, [RIP](https://www.javatpoint.com/rip-full-form) can support maximum upto 15 hops, which means that the 16 routers can be configured in a RIP.

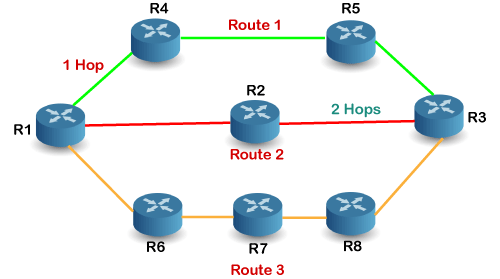
### RIP Message Format

Now, we look at the structure of the RIP message format. The message format is used to share information among different routers. The RIP contains the following fields in a message:



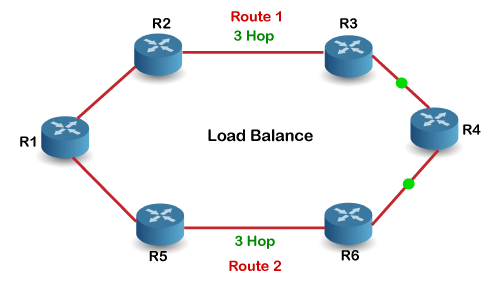
* Command: It is an 8-bit field that is used for request or reply. The value of the request is 1, and the value of the reply is 2.
* Version: Here, version means that which version of the protocol we are using. Suppose we are using the protocol of version1, then we put the 1 in this field.
* Reserved: This is a reserved field, so it is filled with zeroes.
* Family: It is a 16-bit field. As we are using the TCP/IP family, so we put 2 value in this field.
* Network Address: It is defined as 14 bytes field. If we use the IPv4 version, then we use 4 bytes, and the other 10 bytes are all zeroes.
* Distance: The distance field specifies the hop count, i.e., the number of hops used to reach the destination.

### How does the RIP work?



If there are 8 routers in a network where Router 1 wants to send the data to Router 3. If the network is configured with RIP, it will choose the route which has the least number of hops. There are three routes in the above network, i.e., Route 1, Route 2, and Route 3. The Route 2 contains the least number of hops, i.e., 2 where Route 1 contains 3 hops, and Route 3 contains 4 hops, so RIP will choose Route 2.

### Let's look at another example.

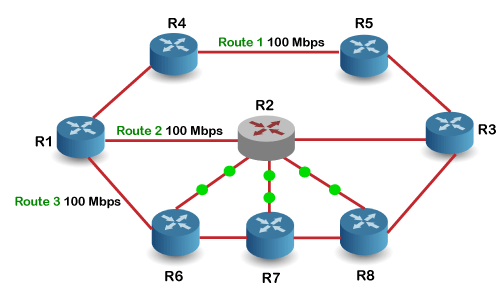


Suppose R1 wants to send the data to R4. There are two possible routes to send data from r1 to r2. As both the routes contain the same number of hops, i.e., 3, so RIP will send the data to both the routes simultaneously. This way, it manages the load balancing, and data reach the destination a bit faster.

### Disadvantages of RIP

**The following are the disadvantages of RIP:**

* In RIP, the route is chosen based on the hop count metric. If another route of better bandwidth is available, then that route would not be chosen. Let's understand this scenario through an example.



We can observe that Route 2 is chosen in the above figure as it has the least hop count. The Route 1 is free and data can be reached more faster; instead of this, data is sent to the Route 2 that makes the Route 2 slower due to the heavy traffic. This is one of the biggest disadvantages of RIP.

* The RIP is a classful routing protocol, so it does not support the VLSM (Variable Length Subnet Mask). The classful routing protocol is a protocol that does not include the subnet mask information in the routing updates.
* It broadcasts the routing updates to the entire network that creates a lot of traffic. In RIP, the routing table updates every 30 seconds. Whenever the updates occur, it sends the copy of the update to all the neighbors except the one that has caused the update. The sending of updates to all the neighbors creates a lot of traffic. This rule is known as a split-horizon rule.
* It faces a problem of Slow convergence. Whenever the router or link fails, then it often takes minutes to stabilize or take an alternative route; This problem is known as Slow convergence.
* RIP supports maximum 15 hops which means that the maximum 16 hops can be configured in a RIP
* The Administrative distance value is 120 (Ad value). If the Ad value is less, then the protocol is more reliable than the protocol with more Ad value.
* The RIP protocol has the highest Ad value, so it is not as reliable as the other routing protocols.

### How RIP updates its Routing table

The following timers are used to update the routing table:

* **RIP update timer : 30 sec**

The routers configured with RIP send their updates to all the neighboring routers every 30 seconds.

* **RIP Invalid timer : 180 sec**

The RIP invalid timer is 180 seconds, which means that if the router is disconnected from the network or some link goes down, then the neighbor router will wait for 180 seconds to take the update. If it does not receive the update within 180 seconds, then it will mark the particular route as not reachable.

* **RIP Flush timer : 240 sec**

The RIP flush timer is 240 second which is almost equal to 4 min means that if the router does not receive the update within 240 seconds then the neighbor route will remove that particular route from the routing table which is a very slow process as 4 minutes is a long time to wait.

### Advantages of RIP

**The following are the advantages of a RIP protocol:**

* It is easy to configure
* It has less complexity
* The CPU utilization is less.

[**next →**](https://www.javatpoint.com/cifs)[**← prev**](https://www.javatpoint.com/imap-protocol)

# POP Protocol

The POP protocol stands for Post Office Protocol. As we know that SMTP is used as a message transfer agent. When the message is sent, then SMPT is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent. The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.

### How is mail transmitted?

Suppose sender wants to send the mail to receiver. First mail is transmitted to the sender's mail server. Then, the mail is transmitted from the sender's mail server to the receiver's mail server over the internet. On receiving the mail at the receiver's mail server, the mail is then sent to the user. The whole process is done with the help of Email protocols. The transmission of mail from the sender to the sender's mail server and then to the receiver's mail server is done with the help of the [SMTP protocol](https://www.javatpoint.com/simple-mail-transfer-protocol). At the receiver's mail server, the POP or [IMAP protocol](https://www.javatpoint.com/imap-protocol) takes the data and transmits to the actual user.

Since SMTP is a push protocol so it pushes the message from the client to the server. As we can observe in the above figure that SMTP pushes the message from the client to the recipient's mail server. The third stage of email communication requires a pull protocol, and POP is a pull protocol. When the mail is transmitted from the recipient mail server to the client which means that the client is pulling the mail from the server.

### What is POP3?

The POP3 is a simple protocol and having very limited functionalities. In the case of the POP3 protocol, the POP3 client is installed on the recipient system while the POP3 server is installed on the recipient's mail server.

Advantages of POP3 protocol

**The following are the advantages of a POP3 protocol:**

* It allows the users to read the email offline. It requires an internet connection only at the time of downloading emails from the server. Once the mails are downloaded from the server, then all the downloaded mails reside on our PC or hard disk of our computer, which can be accessed without the internet. Therefore, we can say that the POP3 protocol does not require permanent internet connectivity.
* It provides easy and fast access to the emails as they are already stored on our PC.
* There is no limit on the size of the email which we receive or send.
* It requires less server storage space as all the mails are stored on the local machine.
* There is maximum size on the mailbox, but it is limited by the size of the hard disk.
* It is a simple protocol so it is one of the most popular protocols used today.
* It is easy to configure and use.

Disadvantages of POP3 protocol

**The following are the advantages of a POP3 protocol:**

* If the emails are downloaded from the server, then all the mails are deleted from the server by default. So, mails cannot be accessed from other machines unless they are configured to leave a copy of the mail on the server.
* Transferring the mail folder from the local machine to another machine can be difficult.
* Since all the attachments are stored on your local machine, there is a high risk of a virus attack if the virus scanner does not scan them. The virus attack can harm the computer.
* The email folder which is downloaded from the mail server can also become corrupted.
* The mails are stored on the local machine, so anyone who sits on your machine can access the email folder.

**Let's understand the working of the POP3 protocol.**

To establish the connection between the POP3 server and the POP3 client, the POP3 server asks for the user name to the POP3 client. If the username is found in the POP3 server, then it sends the ok message. It then asks for the password from the POP3 client; then the POP3 client sends the password to the POP3 server. If the password is matched, then the POP3 server sends the OK message, and the connection gets established. After the establishment of a connection, the client can see the list of mails on the POP3 mail server. In the list of mails, the user will get the email numbers and sizes from the server. Out of this list, the user can start the retrieval of mail.

Once the client retrieves all the emails from the server, all the emails from the server are deleted. Therefore, we can say that the emails are restricted to a particular machine, so it would not be possible to access the same mails on another machine. This situation can be overcome by configuring the email settings to leave a copy of mail on the mail server.

# Introduction to TELNET

[**TELNET**](https://practice.geeksforgeeks.org/problems/explain-telnet)stands for**TE**rmina**L NET**work. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard [**TCP/IP protocol**](https://www.geeksforgeeks.org/tcp-ip-in-computer-networking/) for virtual terminal service which is given by [**ISO**](https://www.geeksforgeeks.org/iso-full-form/). Computer which starts connection known as the**local computer**. Computer which is being connected to i.e. which accepts the connection known as **remote computer**. When the connection is established between local and remote computer. During telnet operation whatever that is performing on the remote computer will be displayed by local computer. Telnet operates on client/server principle. Local computer uses telnet client program and the remote computers uses telnet server program.

**TELNET Commands :**  
Commands of the telnet are identified by a prefix character, Interpret As Command (IAC) which is having code 255. IAC is followed by command and option codes. Basic format of the command is as shown in the following figure :



**Figure –** Telnet command format

Following are some of the important **TELNET commands** :

| **CHARACTER** | **DECIMAL** | **BINARY** | **MEANING** |
| --- | --- | --- | --- |
| WILL | 251 | 11111011 | 1. Offering to enable. 2. Accepting a request to enable. |
| WON’T | 252 | 11111100 | 1. Rejecting a request to enable. 2. Offering to disable. 3. Accepting a request to disable. |
| DO | 253 | 11111101` | 1. Approving a request to enable. 2. Requesting to enable. |
| DON’T | 254 | 11111110 | 1. Disapproving a request to enable. 2. Approving an offer to disable. 3. Requesting to disable. |

Following are some **common options**used with the telnet :

| **CODE** | **OPTION** | **MEANING** |
| --- | --- | --- |
| 0 | Binary | It interpret as 8-bit binary transmission. |
| 1 | Echo | It will echo the data that received on one side to the other side. |
| 3 | Suppress go ahead | It will suppress go ahead signal after data. |
| 5 | Status | It will request for the status of TELNET. |
| 6 | Timing mark | It define the timing marks. |
| 8 | Line width | It specifies the line width. |
| 9 | Page size | It specifies the number of lines in a page. |
| 24 | Terminal type | It set the terminal type. |
| 32 | Terminal speed | It set the terminal speed. |
| 34 | Line mode | It will change to the line mode. |

**Modes of Operation :**

Most telnet implementation operates in one of the following**three modes :**

Default mode

Character mode

Line mode

**Default Mode :**

* If there is no other modes are invoked then this mode is used.
* Echoing is performed in this mode by client.
* In this mode, user types a character and client enchoes the character on the screen but it does not send it until whole line is completed.

**Character Mode :**

* Each character typed in this mode is sent by client to server.
* Server in this type of mode is normally enchoes character back to be displayed on the client’s screen.

**Line Mode :**

* Line editing like echoing, character erasing etc is done from the client side.
* Client will send the whole line to the server.

# SSH Linux | Linux ssh command

In Linux, **ssh** is a protocol, which stands for S**ecure Shell** or S**ecure Socket Shell.** The secure shell is useful for security while connecting to a remote server. The **ssh command uses a ssh protocol**, which is a secure protocol, as the data transfer between the client and the host takes place in encrypted form. It transfers the input through the client to the host and returns the output transferred by the host. It executes through TCP/IP port 22.

The encrypted connection is also used to run the commands on a **Linux server**, **port** **forwarding**, **tunnelling**, and more.

Components of ssh command

The ssh command consists of three different types of components:

* **ssh command:** It instructs the machine to create a secure encrypted connection with the host system.
* **User name:** User name is the name of the Linux user, which is being accessed by the host machine.
* **Host:** A host is a machine that is being accessed by the user, such as a computer or a router. A domain name or an IP address also refers as Host.