**UNIT -05**

**Application Layer Protocols**

5.1 DHCP – DHCP Client, DHCP server, DHCP scope

5.2 DNS – Resolution process, Resource Records, DNS protocol structure

5.3 HTTP – WWW architecture, HTTP: Request and Response Message

5.4 Email protocols – SMTP, POP3, IMAP4 & MIME

5.5 FTP, Telnet

DHCP

# Dynamic Host Configuration Protocol

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

DHCP port number for server is 67 and for the client is 68. It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses.

192.10.21.33

174.11.2.23 a

……...

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.

**DHCP Entities**

* **DHCP server:**

It automatically provides network information(IPaddress, subnet mask, gateway address) on lease. Once the duration is expired, that network information can be assigned to other machine.  It also maintains the data storage which stores the available IP addresses.

* **DHCP client:**

Any node which request an IP address allocation to a network is considered as DHCP client.

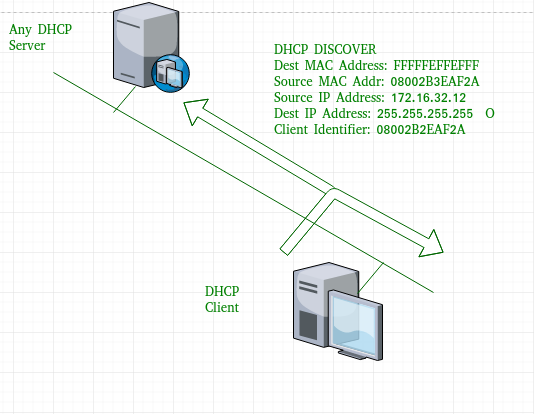
* **DHCP Relay Agent:**

In case, we have only one DHCP server for multiple LAN’s then this Agent which presents in every network forwards the DHCP request to DHCP server. So, using DHCP Relay Agent we can configure multiple LAN’s with single server.

In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process.

These messages are given as below:

1. **DHCP discover message –**  
   This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long



As shown in the figure, source MAC address (client PC) is 08002B2EAF2A, destination MAC address(server) is FFFFFFFFFFFF, source IP address is 0.0.0.0(because PC has no IP address till now) and destination IP address is 255.255.255.255 (IP address used for broadcasting). As the discover message is broadcast to find out the DHCP server or servers in the network therefore broadcast IP address and MAC address is used.

**DHCP offer message –**  
The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also a server ID is specified in the packet in order to identify the server.

the server has provided the offered IP address 192.16.32.51 and **lease time of 72 hours(after this time the entry of host will be erased from the server automatically) .** Also the client identifier is PC MAC address (08002B2EAF2A) for all the messages.

**DHCP request message –**  
When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratitutous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address .A Client ID is also added in this message.

**DHCP acknowledgement message –**  
In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.

**DHCP negative acknowledgement message –**  
Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it send DHCP Nak message to client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.

**DHCP decline –**  
If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server .When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.

1. **DHCP release –**  
   A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.
2. **DHCP inform –**  
   If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the dhcp inform message, DHCP server generates DHCP ack message with local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

**Note –** All the messages can be unicast also by dhcp relay agent if the server is present in different network.

**Advantages –** The advantages of using DHCP include:

* centralized management of IP addresses
* ease of adding new clients to a network
* reuse of IP addresses reducing the total number of IP addresses that are required
* simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client

The DHCP protocol gives the network administrator a method to configure the network from a centralised area.  
With the help of DHCP, easy handling of new users and reuse of IP address can be achieved.

**Disadvantages –** Disadvantage of using DHCP is:

* IP conflict can occur

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.

### DHCP does the following:

* DHCP manages the provision of all the nodes or devices added or dropped from the network.
* DHCP maintains the unique IP address of the host using a DHCP server.
* It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

## How DHCP works

DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

### The DHCP lease process works as follows:

* First of all, a client (network device) must be connected to the internet.
* DHCP clients request an IP address. Typically, client broadcasts a query for this information.
* DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.
* When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

## Benefits of DHCP

There are following benefits of DHCP:

Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

**Domain Name System (DNS) in Application Layer**

url

deepikajspmntc.gmail.com 192.36.12.15 10101010000000101010000

send mcafy20202gmail.com 14.3.2.6

www unipune.ac.in 45.23.6.1

jspmntcedu.in

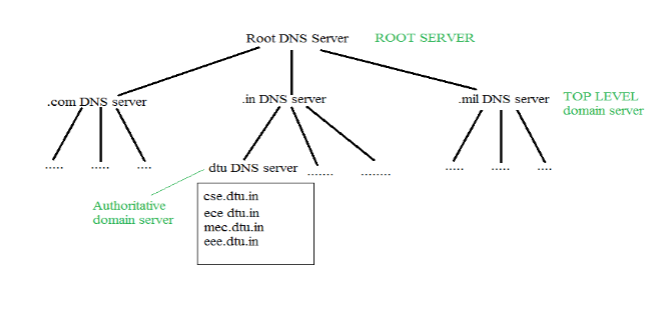
DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

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.

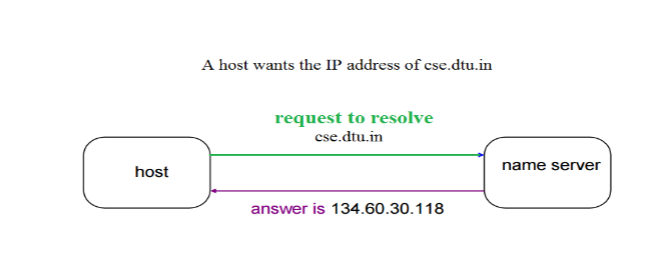


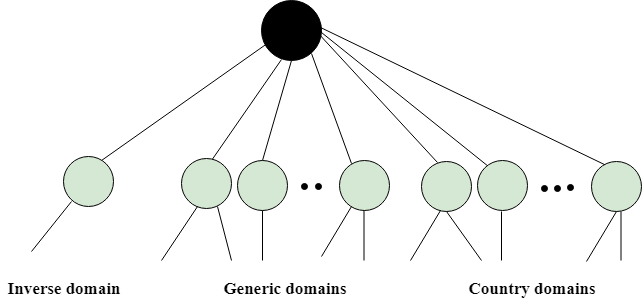
It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately,  
there should not be a lot of delay for that to happen organization of database is very important.  
DNS 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.

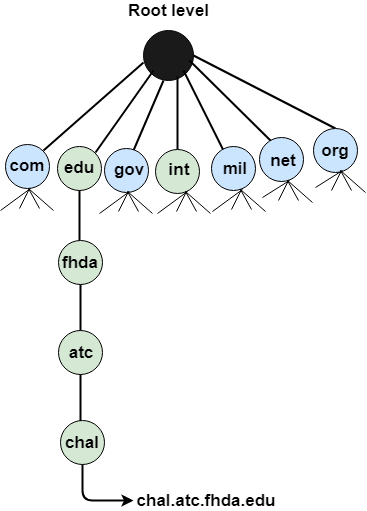
Name to Address Resolution

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.



## 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.



**Why does DNS use UDP and not TCP?**

# HTTP Tutorial



**HTTP** stands for **H**yper **T**ext **T**ransfer **P**rotocol

**WWW** is about communication between web **clients** and **servers**

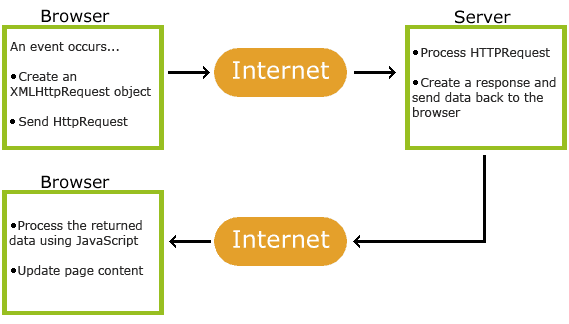
Communication between client computers and web servers is done by sending **HTTP Requests** and receiving **HTTP Responses**

## World Wide Web Communication

The World Wide Web is about communication between web **clients** and web **servers**.

**Clients** are often browsers (Chrome, Edge, Safari), but they can be any type of program or device.

**Servers** are most often computers in the cloud.



## HTTP Request / Response

Communication between clients and servers is done by **requests** and **responses**:

1. A client (a browser) sends an **HTTP request** to the web
2. A web server receives the request
3. The server runs an application to process the request
4. The server returns an **HTTP response** (output) to the browser
5. The client (the browser) receives the response

HTTP tutorial provides basic and advanced concepts of HTTP (Hyper Text Transfer Protocol). Our HTTP tutorial is developed for beginners and professionals.

## What is HTTP

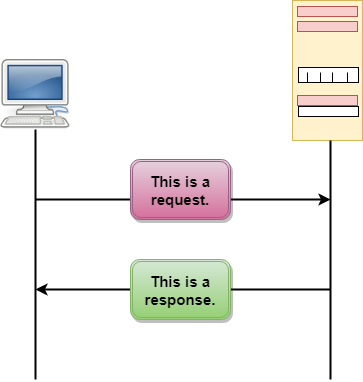
* HTTP stands for Hypertext Transfer Protocol.
* Hypertext Transfer Protocol is a set of rule which is used for transferring the files like, audio, video, graphic image, text and other multimedia files on the WWW (World Wide Web).
* HTTP is an application-level protocol. The communication usually takes place through TCP/IP sockets, but any reliable transport can also be used.
* The standard (default) port for HTTP connection is 80, but other port can also be used.
* The first version of HTTP was HTTP/0.9, which was introduced in 1991.
* The latest version of HTTP is HTTP/3, which was published in September 2019. It is an alternative to its processor HTTP/2.
* This latest version is already in use on the web with the help of UDP (User Datagram Protocol) instead of TCP (Transmission Control Protocol) for the underlying transport protocol.
* HTTP is used to make communication between a variety of hosts and clients. It supports a mixture of network configuration.
* HTTP is a protocol that is used to transfer the hypertext from the client end to the server end, but HTTP does not have any security.
* Whenever a user opens their Web Browser, that means the user indirectly uses HTTP.

## Three important things about HTTP

**Connectionless: HT**TP is connectionless. When the HTTP client opens the browser, the browser initiates an HTTP request. After making the request, the client disconnect from the server and wait for the response. When the response is ready, the server re-establish the connection again and delivers the response to the client, after which the client disconnects the connection. So both client and server know about each other during the current request and response only.

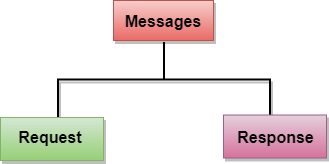
**Media Independent:**HTTP is media independent. HTTP can deliver any sort of data, as long as the two computers can read it.

**Stateless**: The HTTP is stateless. The client and server just know about each other just during the current request. If the connection is closed, and two computers want to connect again, they need to provide information to each other anew, and the connection is handled as the very first one.

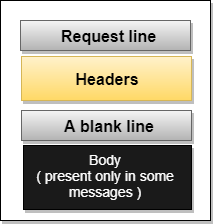


## Messages

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.

## 

## http://www.javapoints.com

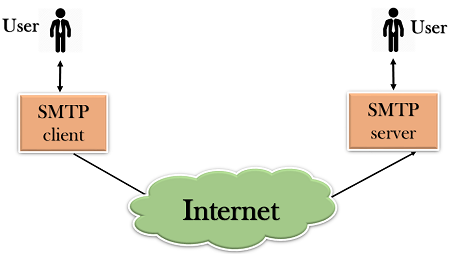
## What is HTTPS

* HTTPS stands for Hypertext Transfer Protocol Secure. HTTPS has a secure transfer.
* It was developed by Netscape.
* HTTPS is used to encrypt or decrypt user HTTP page or HTTP page requests that are returned by the webserver.
* HTTPS is first used in HTTP/1.1 and is defined in RFC 2616.
* In HTTPS, the standard port to transfer the information is 443.
* Using the HTTPS, sensitive information that we want to transfer from one user to another user can be done securely.
* HTTPS protocol uses HTTP on connection encrypted by SSL (Secure Socket Layer) or TLS (Transport Layer Security).
* HTTPS protects transmitted data from man-in-the-middle (MITM) attacks and eavesdropping.
* It is the default protocol for conduction financial transactions on the web.

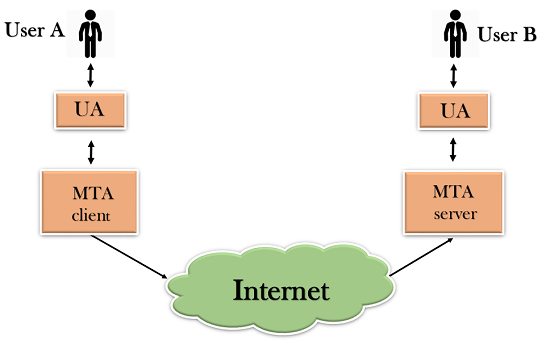
# SMTP

* SMTP stands for Simple Mail Transfer Protocol.
* SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.
* It is a program used for sending messages to other computer users based on e-mail addresses.
* It provides a mail exchange between users on the same or different computers, and it also supports:
  + It can send a single message to one or more recipients.
  + Sending message can include text, voice, video or graphics.
  + It can also send the messages on networks outside the internet.
* The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

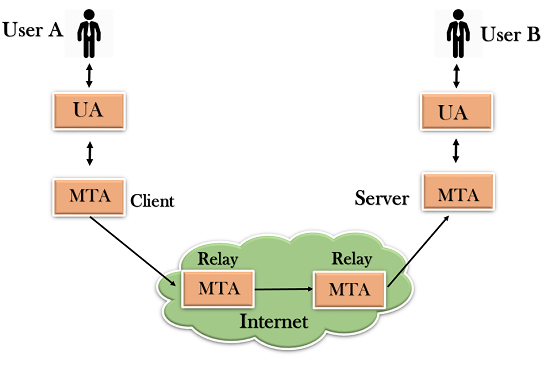
## Components of SMTP



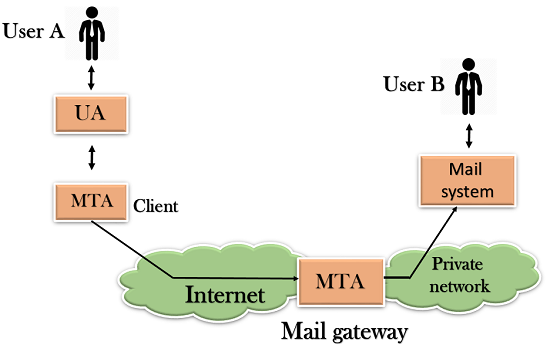
First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.



SMTP allows a more complex system by adding a relaying system. Instead of just having one MTA at sending side and one at receiving side, more MTAs can be added, acting either as a client or server to relay the email.



The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway. The mail gateway is a relay MTA that can be used to receive an email.



E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server. Here in this tutorial, we will discuss various protocols such as SMTP, POP, and IMAP.

## SMPTP

SMTP stands for Simple Mail Transfer Protocol. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Key Points:

* SMTP is application level protocol.
* SMTP is connection oriented protocol.
* SMTP is text based protocol.
* It handles exchange of messages between e-mail servers over TCP/IP network.
* Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
* When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
* These SMTP commands specify the sender’s and receiver’s e-mail address, along with the message to be send.
* The exchange of commands between servers is carried out without intervention of any user.
* In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

## IMAP

**IMAP** stands for **Internet Message Access Protocol.** It was first proposed in 1986. There exist five versions of IMAP as follows:

1. Original IMAP
2. IMAP2
3. IMAP3
4. IMAP2bis
5. IMAP4

**Key Points:**

* IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
* The e-mail is hold and maintained by the remote server.
* It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
* IMAP enables the users to search the e-mails.
* It allows concurrent access to multiple mailboxes on multiple mail servers.

## POP

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

**Key Points**

* POP is an application layer internet standard protocol.
* Since POP supports offline access to the messages, thus requires less internet usage time.
* POP does not allow search facility.
* In order to access the messaged, it is necessary to download them.
* It allows only one mailbox to be created on server.
* It is not suitable for accessing non mail data.
* POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.

## Comparison between POP and IMAP

|  |  |  |
| --- | --- | --- |
| S.N. | POP | IMAP |
| 1 | Generally used to support single client. | Designed to handle multiple clients. |
| 2 | Messages are accessed offline. | Messages are accessed online although it also supports offline mode. |
| 3 | POP does not allow search facility. | It offers ability to search emails. |
| 4 | All the messages have to be downloaded. | It allows selective transfer of messages to the client. |
| 5 | Only one mailbox can be created on the server. | Multiple mailboxes can be created on the server. |
| 6 | Not suitable for accessing non-mail data. | Suitable for accessing non-mail data i.e. attachment. |
| 7 | POP commands are generally abbreviated into codes of three or four letters. Eg. STAT. | IMAP commands are not abbreviated, they are full. Eg. STATUS. |
| 8 | It requires minimum use of server resources. | Clients are totally dependent on server. |
| 9 | Mails once downloaded cannot be accessed from some other location. | Allows mails to be accessed from multiple locations. |
| 10 | The e-mails are not downloaded automatically. | Users can view the headings and sender of e-mails and then decide to download. |
| 10 | POP requires less internet usage time. | IMAP requires more internet usage time. |

IME (Multipurpose Internet Mail Extension) media types were originally devised so that e-mails could include information other than plain text. MIME media types indicate the following things −

* How different parts of a message, such as text and attachments, are combined into the message.
* The way in which each part of the message is specified.
* The way different items are encoded for transmission so that even software that was designed to work only with ASCII text can process the message.

Now MIME types are not just for use with e-mail; they have been adopted by Web servers as a way to tell Web browsers what type of material was being sent to them so that they can cope with that kind of messages correctly.

[Text](https://www.tutorialspoint.com/html/mime_media_text.htm) [image](https://www.tutorialspoint.com/html/mime_media_image.htm) [multipart](https://www.tutorialspoint.com/html/mime_media_multipart.htm) [audio](https://www.tutorialspoint.com/html/mime_media_audio.htm) [video](https://www.tutorialspoint.com/html/mime_media_video.htm) [message](https://www.tutorialspoint.com/html/mime_media_message.htm) [model](https://www.tutorialspoint.com/html/mime_media_model.htm) [application](https://www.tutorialspoint.com/html/mime_media_application.htm)

# 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.

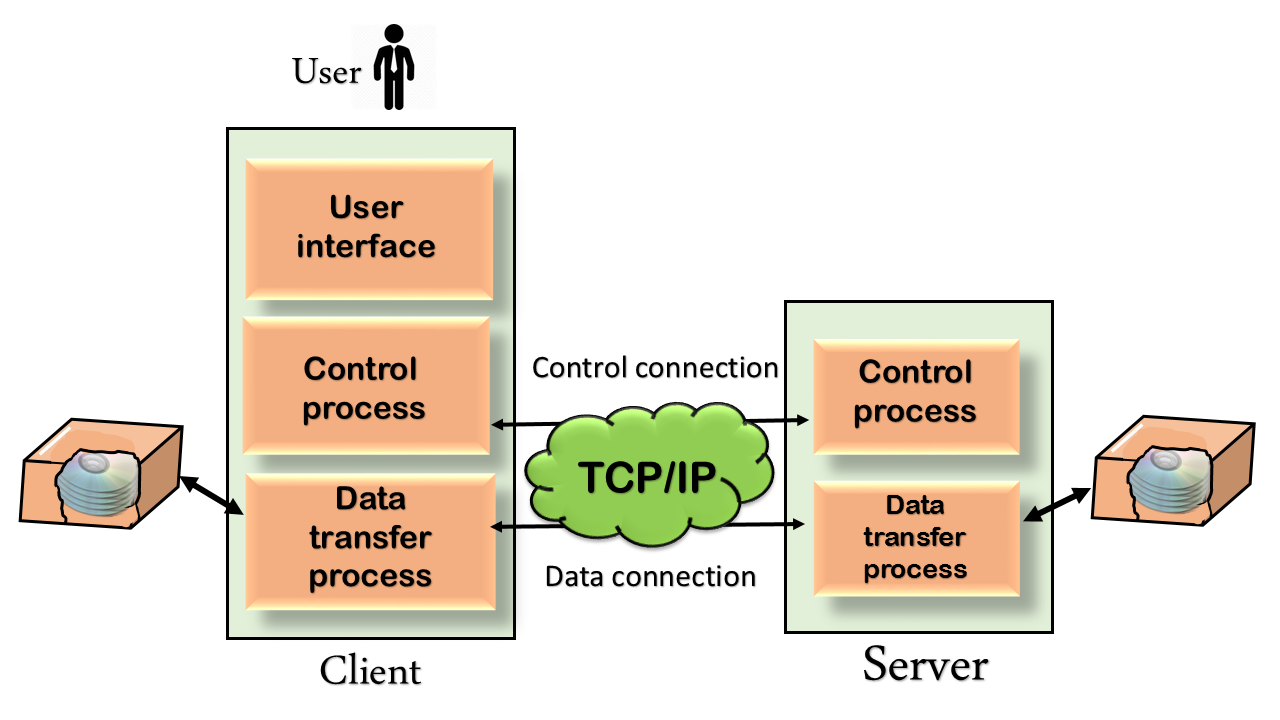
## Objectives of FTP

* 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?

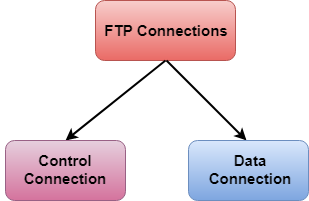
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. 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.

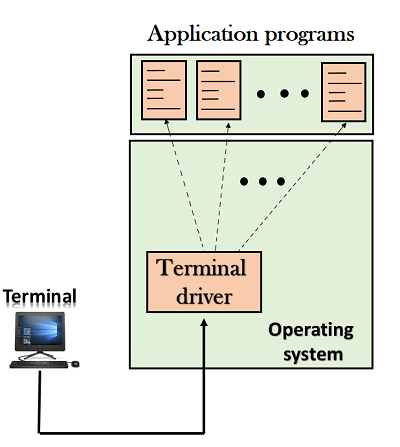
# Telnet

is a protocol that provides a command line interface for communication with a remote device or server.

* 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 transfers 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



### REMOTE Login

