

# UNIT-5

## APPLICATION LAYER

**Application Layer:** Responsibilities of Application Layer Domain Name Space, Distribution of Name Space, DNS in Internet, Generic Domain, Country Domain, Inverse Domain Resolution, Domain Name Space (DNS) Messages, Electronic mail, File Transfer Protocol.

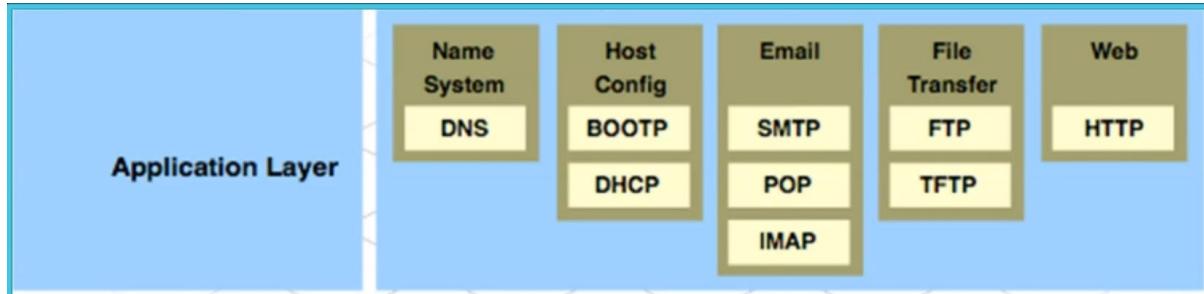
### **Application Layer in OSI Model**

The Application Layer of OSI (Open System Interconnection) model is the top layer in this model and takes care of network communication. The application layer provides the functionality to send and receive data from users. It acts as the interface between the user and the application. The application provides services like file transmission, mail service, and many more.

### **Functions or responsibilities of Application Layer**

- Application Layer provides a facility by which users can forward several emails and it also provides a storage facility.
- This layer allows users to access retrieve and manage files in a remote computer.
- It allows users to log on as a remote host.
- This layer provides access to global information about various services.
- This layer provides services which include: e-mail, transferring files, distributing results to the user, directory services, and network resources and so on.
- It provides protocols that allow software to send and receive information and present meaningful data to users.
- It handles issues such as network transparency, resource allocation and so on.
- This layer serves as a window for users and application processes to access network services.
- Application Layer is basically not a function, but it performs application layer functions.
- The application layer is actually an abstraction layer that specifies the shared protocols and interface methods used by hosts in a communication network.
- Application Layer helps us to identify communication partners, and synchronizing communication.
- This layer allows users to interact with other software applications.
- In this layer, data is in visual form, which makes users truly understand data rather than remembering or visualize the data in the binary format (0's or 1's).
- This application layer basically interacts with Operating System (OS) and thus further preserves the data in a suitable manner.
- This layer also receives and preserves data from its previous layer, which is Presentation Layer (which carries in itself the syntax and semantics of the information transmitted).
- The protocols which are used in this application layer depend upon what information users wish to send or receive.

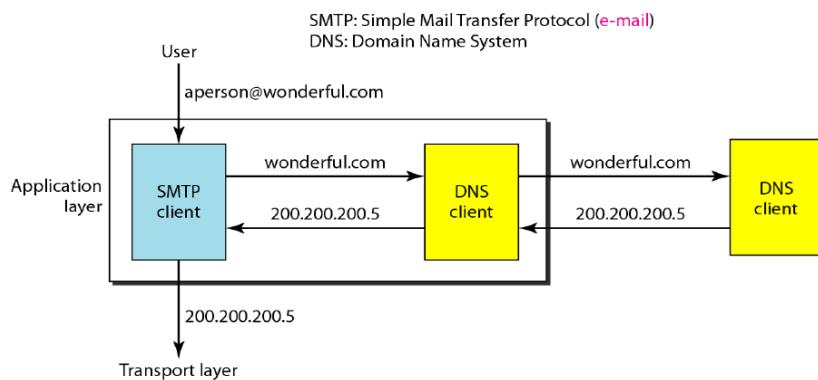
- This application layer, in general, performs host initialization followed by remote login to hosts.



## Domain Name Space

The Domain Name System (DNS) is like the internet's phone book. It helps us to find websites by translating easy-to-remember names (like `www.example.com`) into the numerical IP addresses (like `192.0.2.1`) that computers use to locate each other on the internet. Without DNS, we would have to remember long strings of numbers to visit our favourite websites. It is difficult to remember IP addresses by the people therefore a mapping is required to change the domain name to the IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

## Example



## Label

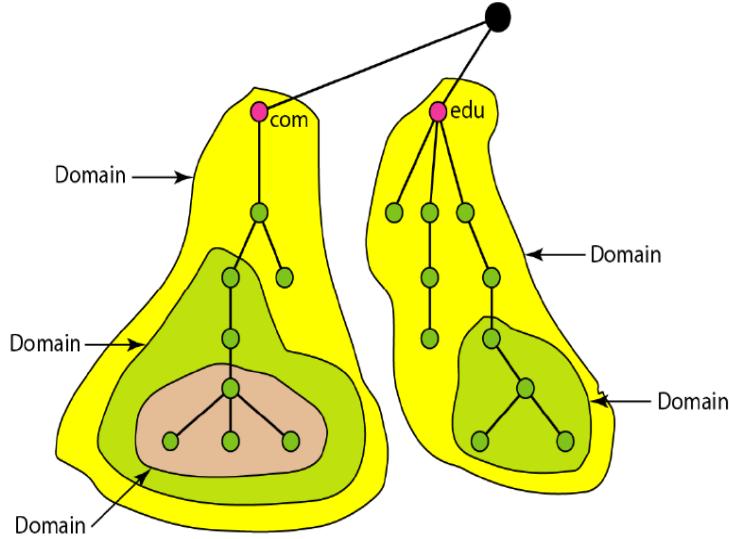
Each node in the tree has a label, which is a **string with a maximum of 63 characters**. The root label is an empty string. DNS requires that children of a node have different labels, which guarantees the uniqueness of the domain names.

## Domain Name

Each node in the tree has a domain name. A full domain name is a sequence of labels separated by dots (.). The domain names are always read from the node up to the root. The last label is the label of the root (null). This means that a full domain name always ends in a null label, which means the last character is a dot because the null string is nothing.

## Domain

A domain is a sub tree of the domain name space. The name of the domain is the domain name of the node at the top of the sub tree. Note that a domain may itself be divided into domains.



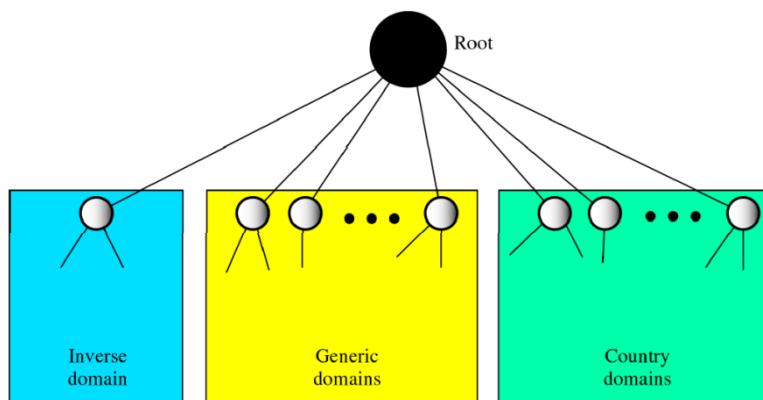
## DNS IN THE INTERNET

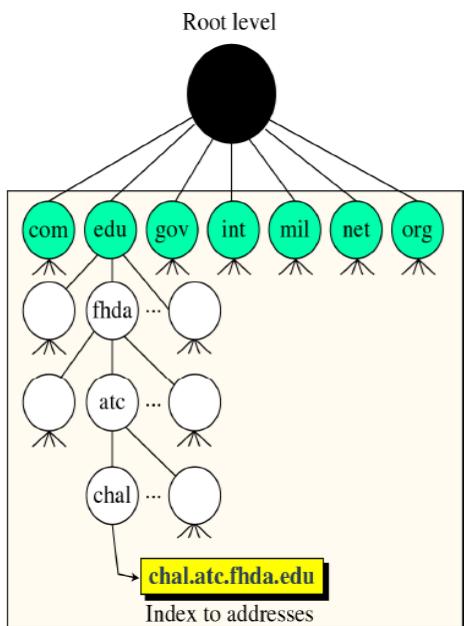
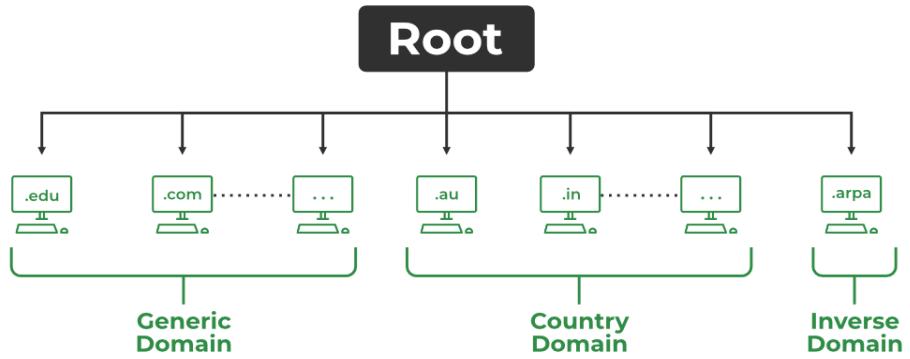
DNS is a protocol that can be used in different platforms. In the Internet, the domain name space (tree) is divided into three different sections: generic domains, country domains, and the inverse domain.

### Types of Domain

There are various kinds of domains:

- **Generic Domains:** .com (commercial), .edu(educational), .mil(military), .org(non-profit organization), .net(similar to commercial) all these are generic domains.
- **Country Domain:** .in (India) .us .uk
- **Inverse Domain:** if we want to know what is the domain name of the website. IP to domain name mapping.

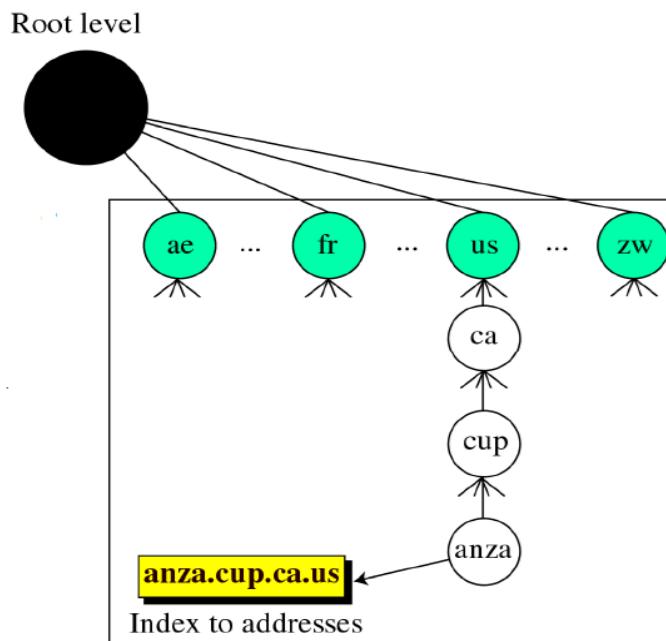




<i>Label</i>	<i>Description</i>
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

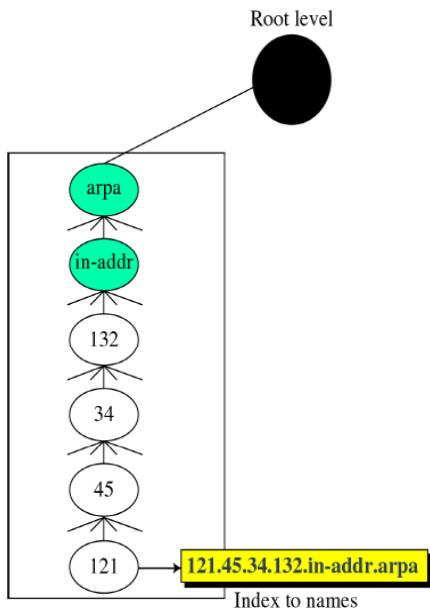
## Country Domain

The country domains section uses two-character country abbreviations (e.g., us for United States). Second labels can be organizational, or they can be more specific, national designations.



## Inverse Domain

The inverse domain is added to the domain name space with the first-level node called arpa (for historical reasons). The second level is also one single node named in-addr (for inverse address). The rest of the domain defines IP addresses.



## DNS Message Format

DNS allows you to interact with devices on the Internet without having to remember long strings of numbers. Changing of information between client and server is carried out by two types of DNS messages:

- Query message
- Response message.

The format is similar for both types of messages. The information is held up in up to five different sections of DNS message format. The query message is having two sections - header and question records.

The response message consists of five sections:

- Header
- Question
- Records
- Answer records
- Authoritative records
- Additional records

0	15 16	31
<b>Identification</b>	<b>Flags</b>	
<b>Number of questions</b>	<b>Number of answer RRs (All 0s in query message)</b>	
<b>Number of authority RRs (All 0s in query message)</b>	<b>Number of additional RRs (All 0s in query message)</b>	
<b>General DNS Message Format</b>		

Header  
 12 bytes

The above representation is showing the DNS Message format in which some fields are set to 0s for query messages.

- **Identification:** The identification field is made up of 16 bits which are used to match the response with the request sent from the client-side. The matching is carried out by this field as the server copies the 16-bit value of identification in the response message so the client device can match the queries with the corresponding response received from the server-side.
- **Flags:** It is 16 bits and is divided into the following Fields :

<b>QR</b>	<b>Opcode</b>	<b>AA</b>	<b>TC</b>	<b>RD</b>	<b>RA</b>	<b>zero</b>	<b>rCode</b>
<b>1</b>	<b>4</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>3</b>	<b>4</b>

Here is the description of each subfield of the Flags field:

- **QR (query/response):** It is a 1-bit subfield. If its value is 0, the message is of request type and if its value is 1, the message is of response type.
- **opcode:** It is a 4-bit subfield that defines the type of query carried by a message. This field value is repeated in the response. Following is the list of opcode values with a brief description:
  - If the value of the opcode subfield is **0** then it is a standard query.
  - The value **1** corresponds to an inverse of query that implies finding the domain name from the IP Address.
  - The value **2** refers to the server status request. The value **3** specifies the status reserved and therefore not used.
- **AA:** It is an Authoritative Answer. It is a 1-bit subfield that specifies the server is authoritative if the value is 1 otherwise it is non-authoritative for a 0 value.
- **TC:** It is Truncation. This is a 1-bit subfield that specifies if the length of the message exceeds the allowed length of 512 bytes, the message is truncated when using UDP services.
- **RD:** It is Recursion Desired. It is a 1-bit subfield that specifies if the value is set to 1 in the query message then the server needs to answer the query recursively. Its value is copied to the response message.
- **RA:** It is Recursion Available. It is a 1-bit subfield that specifies the availability of recursive response if the value is set to 1 in the response message.
- **Zero:** It is a 3-bit reserved subfield set to 0.
- **rCode:** It stands for Response Code. It is a 4-bit subfield used to denote whether the query was answered successfully or not. If not answered successfully then the status of error is provided in the response. Following is the list of values with their error status –
  - The value **0** of **rcode** indicates no error.
  - A value of **1** indicates that there is a problem with the format specification.
  - Value **2** indicates server failure.
  - Value **3** refers to the Name Error that implies the name given by the query does not exist in the domain.
  - Value of **4** indicates that the request type is not supported by the server.
  - The value **5** refers to the nonexecution of queries by the server due to policy reasons.
- **Number of Questions-** It is a 16-bit field to specify the count of questions in the Question Section of the message. It is present in both query and response messages.
- **A number of answer RRs-** It is a 16-bit field that specifies the count of answer records in the Answer section of the message. This section has a value of 0 in query messages.

The server answers the query received from the client. It is available only in response messages.

- **A number of authority RR**s- It is a 16-bit field that gives the count of the resource records in the Authoritative section of the message. This section has a value of 0 in query messages. It is available only in response messages. It gives information that comprises domain names about one or more authoritative servers.
- **A number of additional RR**s- It is a 16-bit field that holds additional records to keep additional information to help the resolver. This section has a value of 0 in query messages. It is available only in response messages.

## Electronic Mail

### Introduction:

**Electronic mail, commonly known as email, is a method of exchanging messages over the internet. Here are the basics of email:**

1. An email address: This is a unique identifier for each user, typically in the format of name@domain.com.
2. An email client: This is a software program used to send, receive and manage emails, such as Gmail, Outlook, or Apple Mail.
3. An email server: This is a computer system responsible for storing and forwarding emails to their intended recipients.

### To send an email:

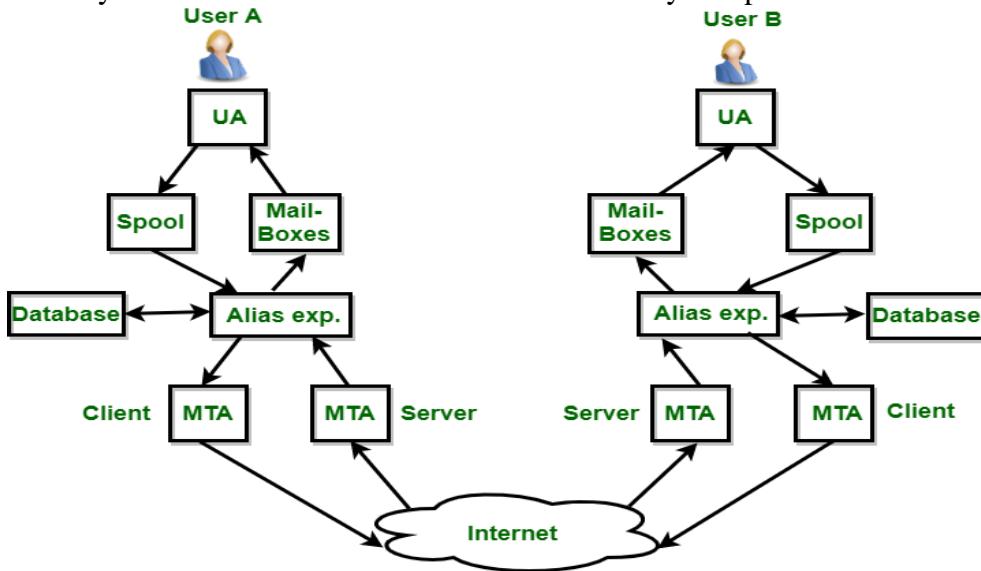
1. Compose a new message in your email client.
2. Enter the recipient's email address in the "To" field.
3. Add a subject line to summarize the content of the message.
4. Write the body of the message.
5. Attach any relevant files if needed.
6. Click "Send" to deliver the message to the recipient's email server.
7. Emails can also include features such as cc (carbon copy) and bcc (blind carbon copy) to send copies of the message to multiple recipients, and reply, reply all, and forward options to manage the conversation.

**Electronic Mail** (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a **message in formatted manner (mail)** to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called **sender** and person who receives mail is called **recipient**. It is just like postal mail service.

**Components of E-Mail System:** The basic components of an email system are: User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. **User Agent (UA):** The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.
2. **Message Transfer Agent (MTA):** MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfers mail to mailboxes of recipients if they are connected in the same

machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.



3. **Mailbox:** It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox. Access to mailbox is only to owner of mailbox.
4. **Spool file:** This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an **alias**, to represent several different e-mail addresses. It is known as **mailing list**, whenever users have to send a message, system checks recipient's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

#### **Services provided by E-mail system:**

- **Composition** – The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
- **Transfer** – Transfer means sending procedure of mail i.e. from the sender to recipient.
- **Reporting** – Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
- **Displaying** – It refers to present mail in form that is understand by the user.
- **Disposition** – This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

#### **Advantages of email:**

1. Convenient and fast communication with individuals or groups globally.
2. Easy to store and search for past messages.
3. Ability to send and receive attachments such as documents, images, and videos.
4. Cost-effective compared to traditional mail and fax.
5. Available 24/7.

### **Disadvantages of email:**

1. Risk of spam and phishing attacks.
2. Overwhelming amount of emails can lead to information overload.
3. Can lead to decreased face-to-face communication and loss of personal touch.
4. Potential for miscommunication due to lack of tone and body language in written messages.
5. Technical issues, such as server outages, can disrupt email service.
6. It is important to use email responsibly and effectively, for example, by keeping the subject line clear and concise, using proper etiquette, and protecting against security threats.

## **FILE TRANSFER PROTOCOL**

FTP or File Transfer Protocol is said to be one of the earliest and also the most common forms of transferring files on the internet. Located in the application layer of the OSI model FTP is a basic system that helps in transferring files between a client and a server. It is what makes the FTP unique that the system provides a reliable and efficient means of transferring files from one system to another even if they have different file structures and operating systems. Contrary to other protocols such as http that cover hypertexts and web resources in general ftp is dedicated to the management and the transfer of text, binary, or image files.

FTP is a standard communication protocol. There are various other protocols like HTTP which are used to transfer files between computers, but they lack clarity and focus as compared to FTP. Moreover, the systems involved in connection are heterogeneous, i.e. they differ in operating systems, directories, structures, character sets, etc the FTP shields the user from these differences and transfers data efficiently and reliably. FTP can transfer ASCII, EBCDIC, or image files. The ASCII is the default file share format, in this, each character is encoded by NVT ASCII. In ASCII or EBCDIC the destination must be ready to accept files in this mode. The image file format is the default format for transforming binary files.



### **Types of FTP**

**There are different ways through which a server and a client do a file transfer using FTP. Some of them are mentioned below:**

- **Anonymous FTP:** Anonymous FTP is enabled on some sites whose files are available for public access. A user can access these files without having any username or password. Instead, the username is set to anonymous, and the password is to the guest

by default. Here, user access is very limited. For example, the user can be allowed to copy the files but not to navigate through directories.

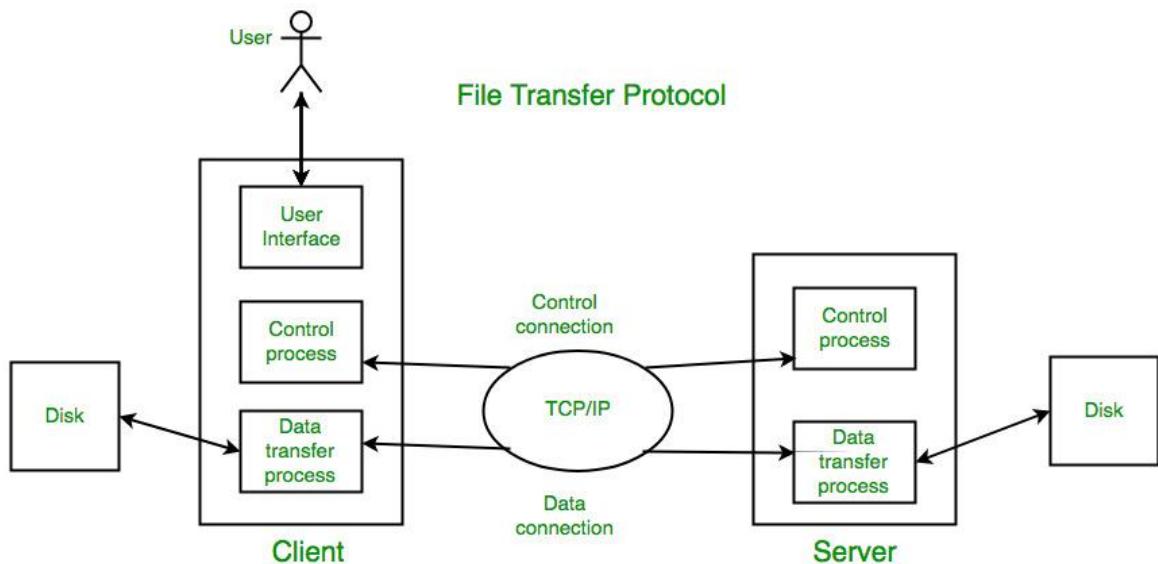
- **Password Protected FTP:** This type of FTP is similar to the previous one, but the change in it is the use of username and password.
- **FTP Secure (FTPS):** It is also called as FTP Secure Sockets Layer (FTP SSL). It is a more secure version of FTP data transfer. Whenever FTP connection is established, Transport Layer Security (TLS) is enabled.
- **FTP over Explicit SSL/TLS (FTPES):** FTPES helps by upgrading FTP Connection from port 21 to an encrypted connection.
- **Secure FTP (SFTP):** SFTP is not a FTP Protocol, but it is a subset of Secure Shell Protocol, as it works on port 22.

## How Does FTP Work?

FTP is a client server protocol that has two communication channel, command channel for conversation control and data channel for file content.

Here are steps mentioned in which FTP works:

- A user has to log in to FTP Server first there may be some servers where you can access to content without login, known as anonymous FTP.
- Client can start a conversation with server, upon requesting to download a file.
- The user can start different functions like upload, delete, rename, copy files, etc. on server.
- FTP can work on different modes like Active and Passive modes.



## Types of Connection in FTP

- Control Connection
- Data Connection

### Control Connection

For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of a control connection. The control connection is initiated on port number 21.

## **Data connection**

For sending the actual file FTP makes use of a data connection. A data connection is initiated on port number 20. FTP sends the control information out-of-band as it uses a separate control connection. Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples.

