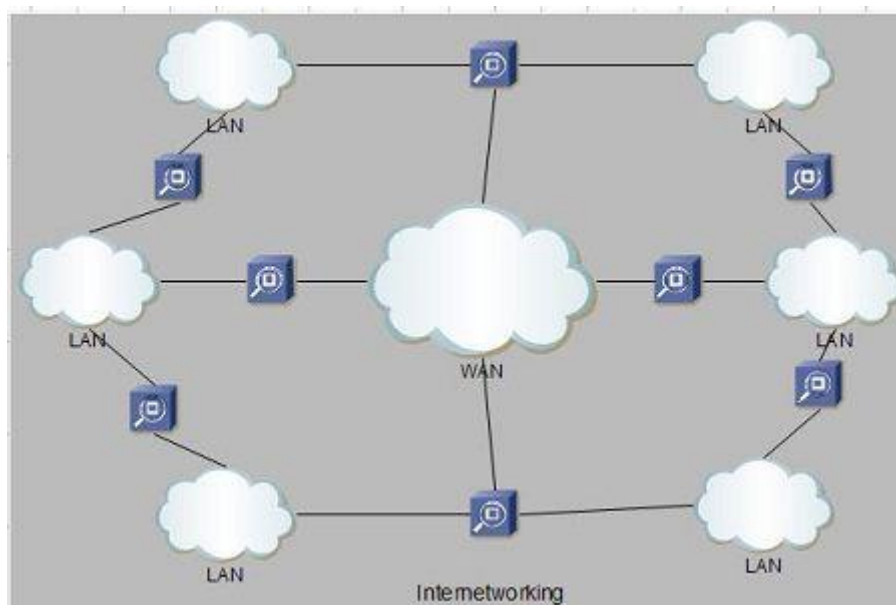


# Internetworking

Internetworking started as a way to connect disparate types of computer networking technology. Computer network term is used to describe two or more computers that are linked to each other. When two or more computer LANs or WANs or computer network segments are connected using devices such as a router and configure by logical addressing scheme with a protocol such as IP, then it is called as computer internetworking.

Internetworking is a term used by Cisco. Any interconnection among or between public, private, commercial, industrial, or governmental computer networks may also be defined as an internetwork or “Internetworking “.

In modern practice, the interconnected computer networks or Internetworking use the Internet Protocol. Two architectural models are commonly used to describe the protocols and methods used in internetworking. internetworking is Open



## Type of Internetworking

Internetworking is implemented in Layer 3 (Network Layer) of this model. The most notable example of internetworking is the Internet (capitalized). There are three variants of internetwork or Internetworking, depending on who administers and who participates in them:

- Extranet
- Intranet
- Internet

Intranets and extranets may or may not have connections to the Internet. If connected to the Internet, the intranet or extranet is normally protected from being accessed from the Internet without proper authorization. The Internet is not considered to be a part of the intranet or extranet, although it may serve as a portal for access to portions of an extranet.

### **Extranet**

An extranet is a network of internetwork or Internetworking that is limited in scope to a single organisation or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities. Technically, an extranet may also be categorized as a MAN, WAN, or other type of network, although, by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

### **Intranet**

An intranet is a set of interconnected networks or Internetworking, using the Internet Protocol and uses IP-based tools such as web browsers and ftp tools, that is under the control of a single administrative entity. That administrative entity closes the intranet to the rest of the world, and allows only specific users. Most commonly, an intranet is the internal network of a company or other enterprise. A large intranet will typically have its own web server to provide users with browsable information.

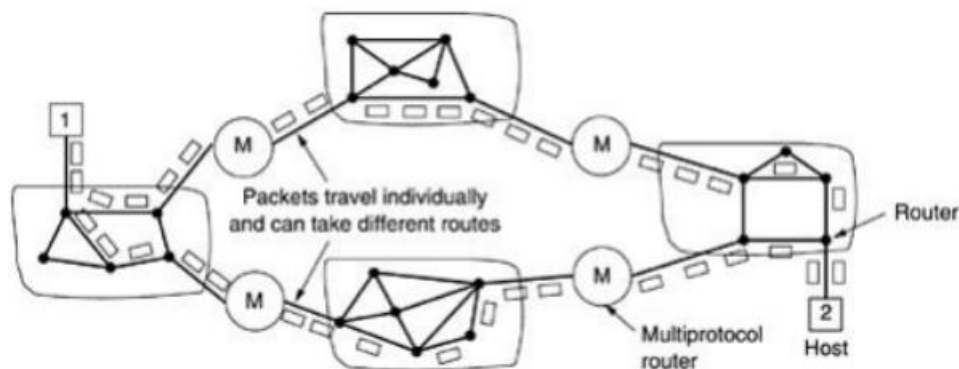
### **Internet**

A specific Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and private networks based upon the Advanced Research Projects Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defence also home to the World Wide Web (WWW) and referred to as the 'Internet' with a capital 'I' to distinguish it from other generic internetworks. Participants in the Internet, or their service providers, use IP Addresses obtained from address registries that control assignments.

# Connectionless Internetworking

The datagram model is shown in Fig. 9. In this model, the only service the network layer offers to the transport layer is the ability to inject datagrams into the subnet and hope for the best. There is no notion of a virtual circuit at all in the network layer, let alone a concatenation of them. This model does not require all packets belonging to one connection to traverse the same sequence of gateways. In Fig. 9 datagrams from host 1 to host 2 are shown taking different routes through the internetwork. A routing decision is made separately for each packet, possibly depending on the traffic at the moment the packet is sent. This strategy can use multiple routes and thus achieve a higher bandwidth than the concatenated virtual-circuit model. On the other hand, there is no guarantee that the packets arrive at the destination in order, assuming that they arrive at all.

The model of Fig. 9 is not quite as simple as it looks. For one thing, if each network has its own network layer protocol, it is not possible for a packet from one network to transit another one. One could imagine the multiprotocol routers actually trying to translate from one format to another, but unless the two formats are close relatives with the same information fields, such conversions will always be incomplete and often doomed to failure. For this reason, conversion is rarely attempted.



**Fig 9. A connectionless internet.**

A second, and more serious, problem is addressing. Imagine a simple case: a host on the Internet is trying to send an IP packet to a host on an adjoining SNA network. The IP and SNA addresses are different. One would need a mapping between IP and SNA addresses in both directions. Furthermore, the concept of what is addressable is different. In IP, hosts (actually, interface cards) have addresses. In SNA, entities other than hosts (e.g., hardware devices) can also have addresses. At best, someone would

have to maintain a database mapping everything to everything to the extent possible, but it would constantly be a source of trouble.

Another idea is to design a universal "internet" packet and have all routers recognize it. This approach is, in fact, what IP is—a packet designed to be carried through many networks. Of course, it may turn out that IPv4 (the current Internet protocol) drives all other formats out of the market, IPv6 (the future Internet protocol) does not catch on, and nothing new is ever invented, but history suggests otherwise. Getting everybody to agree to a single format is difficult when companies perceive it to their commercial advantage to have a proprietary format that they control.

## HTTP (HyperText Transfer Protocol)

- 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.

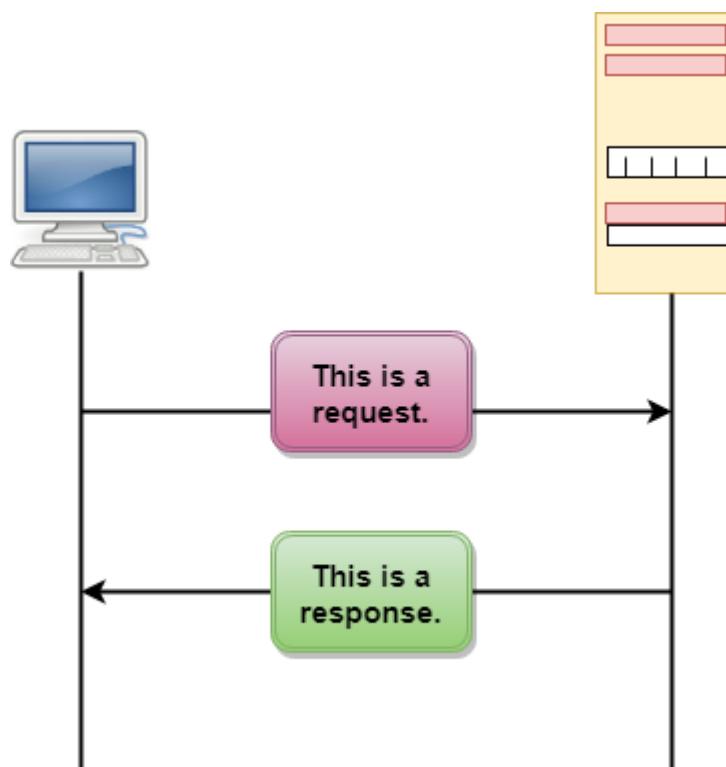
### Features of HTTP:

**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.

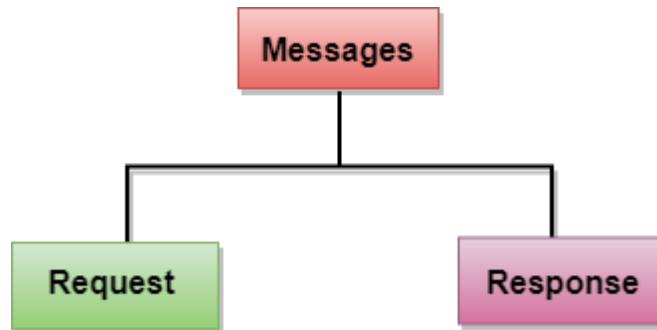
## HTTP Transactions



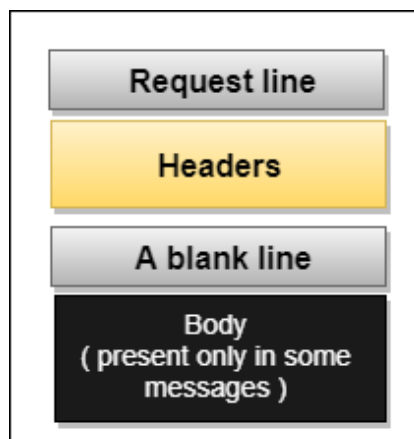
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

## Messages

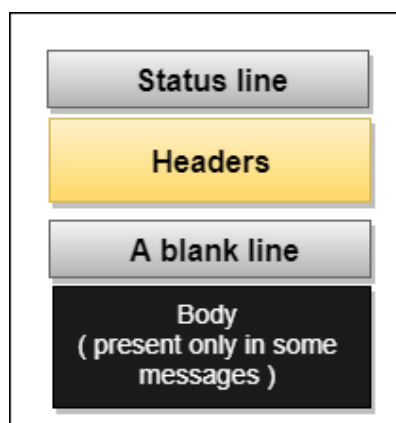
HTTP messages are of two types: request and response. Both the message types follow the same message format.



**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.

# World Wide Web

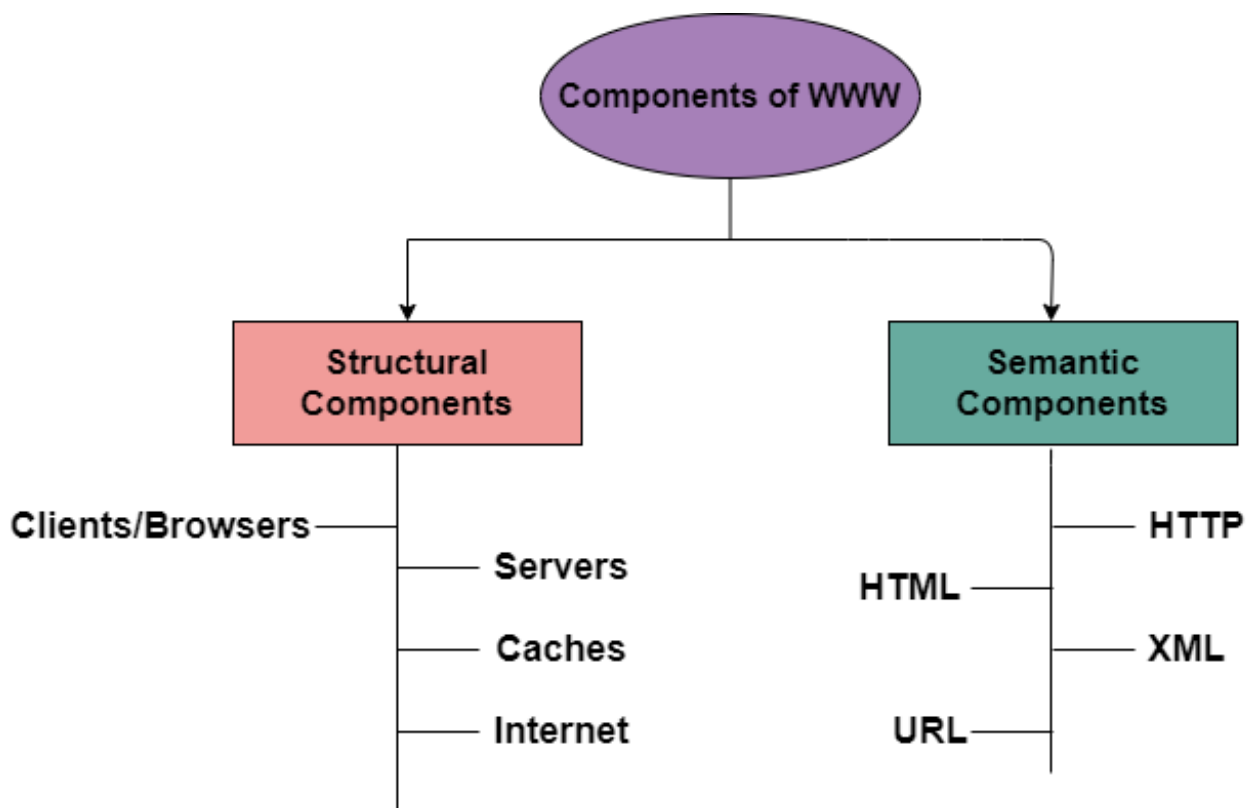
The World Wide Web or Web is basically a collection of information that is linked together from points all over the world. It is also abbreviated as WWW.

- World wide web provides flexibility, portability, and user-friendly features.
- It mainly consists of a worldwide collection of electronic documents (i.e, Web Pages).
- It is basically a way of exchanging information between computers on the Internet.
- The WWW is mainly the network of pages consists of images, text, and sounds on the Internet which can be simply viewed on the browser by using the browser software.

## Components of WWW

The Components of WWW mainly falls into two categories:

- Structural Components
- Semantic Components

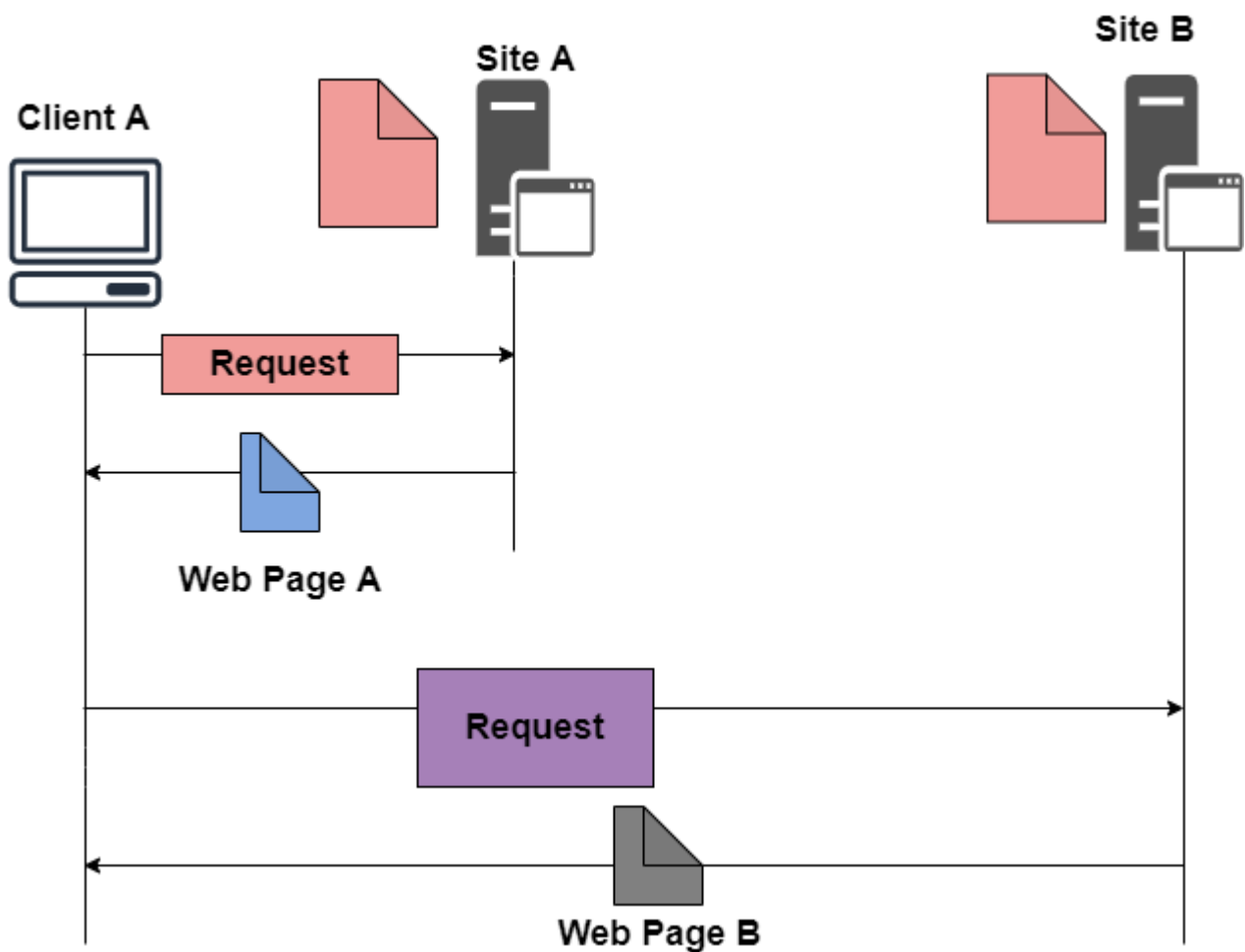




## Architecture of WWW

The WWW is mainly a distributed client/server service where a client using the browser can access the service using a server. The Service that is provided is distributed over many different locations commonly known as sites/websites.

- Each website holds one or more documents that are generally referred to as web pages.
- Where each web page contains a link to other pages on the same site or at other sites.
- These pages can be retrieved and viewed by using browsers.



In the above case, the client sends some information that belongs to site A. It generally sends a request through its browser (It is a program that is used to fetch the documents on the web).

and also, the request generally contains other information like the address of the site, web page (URL).

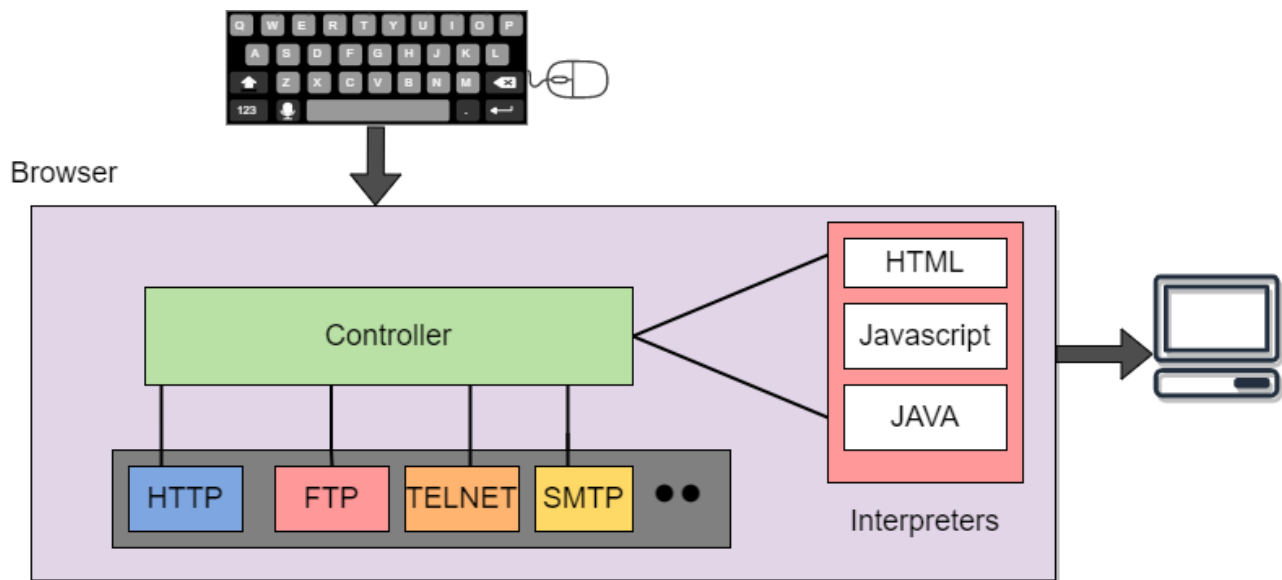
The server at site A finds the document then sends it to the client. after that when the user or say the client finds the reference to another document that includes the web page at site B.

The reference generally contains the URL of site B. And the client is interested to take a look at this document too. Then after the client sends the request to the new site and then the new page is retrieved.

### **Client/Browser**

The Client/Web browser is basically a program that is used to communicate with the webserver on the Internet.

- Each browser mainly comprises of three components and these are:
  - ❖ Controller
  - ❖ Interpreter
  - ❖ Client Protocols
- The Controller mainly receives the input from the input device, after that it uses the client programs in order to access the documents.
- After accessing the document, the controller makes use of an interpreter in order to display the document on the screen.
- An interpreter can be Java, HTML, JavaScript mainly depending upon the type of the document.
- The Client protocol can be FTP, HTTP, TELNET.



## Server

The computer that is mainly available for the network resources and in order to provide services to the other computer upon request is generally known as the server.

- The Web pages are mainly stored on the server.
- Whenever the request of the client arrives then the corresponding document is sent to the client.
- The connection between the client and the server is TCP.
- It can become more efficient through multithreading or multiprocessing. Because in this case, the server can answer more than one request at a time.

## Features of WWW

Given below are some of the features provided by the World Wide Web:

- Provides a system for Hypertext information
- Open standards and Open source
- Distributed.
- Mainly makes the use of Web Browser in order to provide a single interface for many services.
- Dynamic
- Interactive
- Cross-Platform

## **Advantages of WWW**

Given below are the benefits offered by WWW:

- It mainly provides all the information for Free.
- Provides rapid Interactive way of Communication.
- It is accessible from anywhere.
- It has become the Global source of media.
- It mainly facilitates the exchange of a huge volume of data.

## **Disadvantages of WWW**

There are some drawbacks of the WWW and these are as follows;

- It is difficult to prioritize and filter some information.
- There is no guarantee of finding what one person is looking for.
- There occurs some danger in case of overload of Information.
- There is no quality control over the available data.
- There is no regulation.

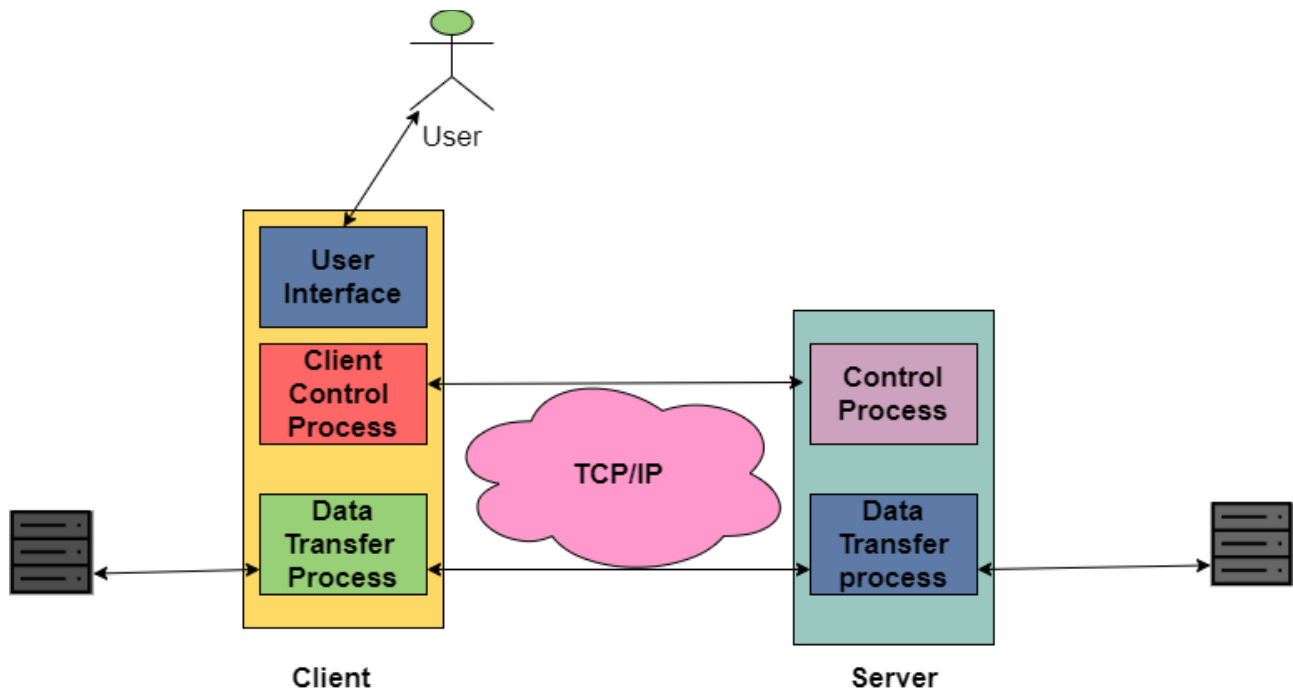
# FTP Protocol

FTP means File Transfer Protocol and it is the standard mechanism provided by the TCP/IP in order to copy a file from one host to another.

- File Transfer Protocol is a protocol present at the Application layer of the OSI Model.
- FTP is one of the easier, simpler, and secure ways to exchange files over the Internet.
- FTP is different from the other client/server applications as this protocol establishes two connections between the hosts.
  - where one connection is used for the data transfer and is known as a data connection.
  - while the other connection is used to control information like commands and responses and this connection is termed as control connection.
- FTP is more efficient as there is the separation of commands.
- The File Transfer Protocol makes the use of two protocols; Port 21 for the Control connection and Port 20 is used for Data connection.
- The control connection in FTP makes the use of very simple rules of communication, we just need to transfer a line of command or a line of response at a time.
- On the other hand, the data connection needs more complex rules; and the reason behind this is there are a variety of types of data that needs to be transferred.
- The transferring of files from the client computer to the server is termed as "uploading", while the transferring of data from the server to the client computer is termed as "downloading".
- The types of files transferred using the FTP are ASCII files, EBCDIC files, or image files.

## Working of FTP

Given below figure shows the basic model of file Transfer Protocol, where the client comprises of three components: User Interface, Client control process, and client data transfer process. On the other hand, the server comprises of two components mainly the server control process and the server data transfer process.



1. Also, the control connection is made between the control processes while the data connection is made between the data transfer processes.
2. The control Connection remains connected during the entire interactive session of FTP while the data connection is opened and then closed for each file transferred.
3. In simple terms when a user starts the FTP connection then the control connection opens, while it is open the data connection can be opened and closed multiple times if several files need to be transferred.

## Data Structure

Given below are three data structures supported by FTP:

### 1.File Structure

In the File data structure, the file is basically a continuous stream of bytes.

### 2.Record Structure

In the Record data structure, the file is simply divided into the form of records.

### 3. Page Structure

In the Page data structure, the file is divided into pages where each page has a page number and a page header. These pages can be stored and accessed either randomly or sequentially.

### FTP Clients

It is basically software that is designed to transfer the files back-and-forth between a computer and a server over the Internet. The FTP client needs to be installed on your computer and can only be used with the live connection to the Internet.

Some of the commonly used FTP clients are Dreamweaver, FireFTP, and Filezilla.

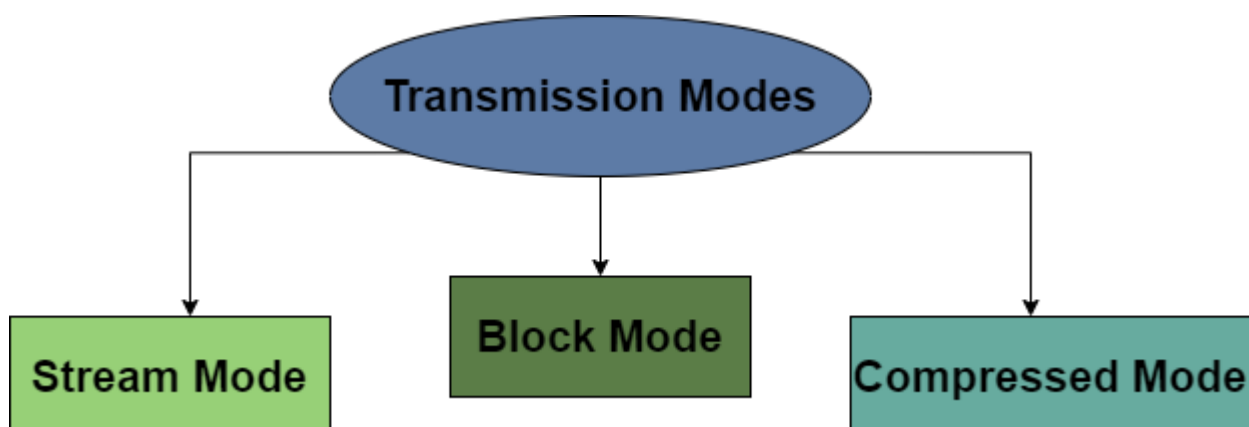
### Features of FTP

Following are the features offered by the File transfer protocol:

- FTP is mainly used to transfer one file at a time.
- Other actions performed by FTP are listing files, creating and deleting directories, deleting files, renaming files, and many more.
- FTP also hides the details of individual computer systems.
- FTP allows those files that have ownership and access restrictions.
- It is a connection-oriented protocol.
- FTP is a stateful protocol as in this the client establishes a control connection for the duration of an FTP session that typically spans multiple data transfers.

### Transmission Modes

FTP can transfer a file across the data connection using one of the three given modes:



## **1.Stream Mode**

Stream Mode is the default mode of transmission used by FTP. In this mode, the File is transmitted as a continuous stream of bytes to TCP.

If the data is simply in the form of the stream of bytes, then there is no need for End-of-File, closing of data connection by the sender is considered as EOF or end-of-file. If the data is divided into records (that is the record structure), each record has an I-byte of EOR (end-of-record).

## **2.Block Mode**

Block mode is used to deliver the data from FTP to TCP in the form of blocks of data. Each block of data is preceded by 3 bytes of the header where the first byte represents the block descriptor while the second and third byte represents the size of the block.

## **3.Compressed Mode**

In this mode, if the file to be transmitted is very big then the data can be compressed. This method is normally used in Run-length encoding. In the case of a text file, usually, spaces/blanks are removed. While in the case of the binary file, null characters are compressed.

## **Advantages of FTP**

Following are some of the benefits of using File Transfer protocol:

- Implementation of FTP is simple.
- FTP provides one of the fastest ways to transfer files from one computer to another.
- FTP is a standardized protocol and is widely used.
- File Transfer protocol is more efficient as there is no need to complete all the operations in order to get the entire file,

## **Disadvantages of FTP**

Let us take a look at the drawbacks of FTP:

- File Transfer Protocol is not a secure way to transfer the data.
- FTP does not allow the copy from server to server and also not allows removal operations for the recursive directory.
- Scripting the jobs is hard using the FTP protocol.

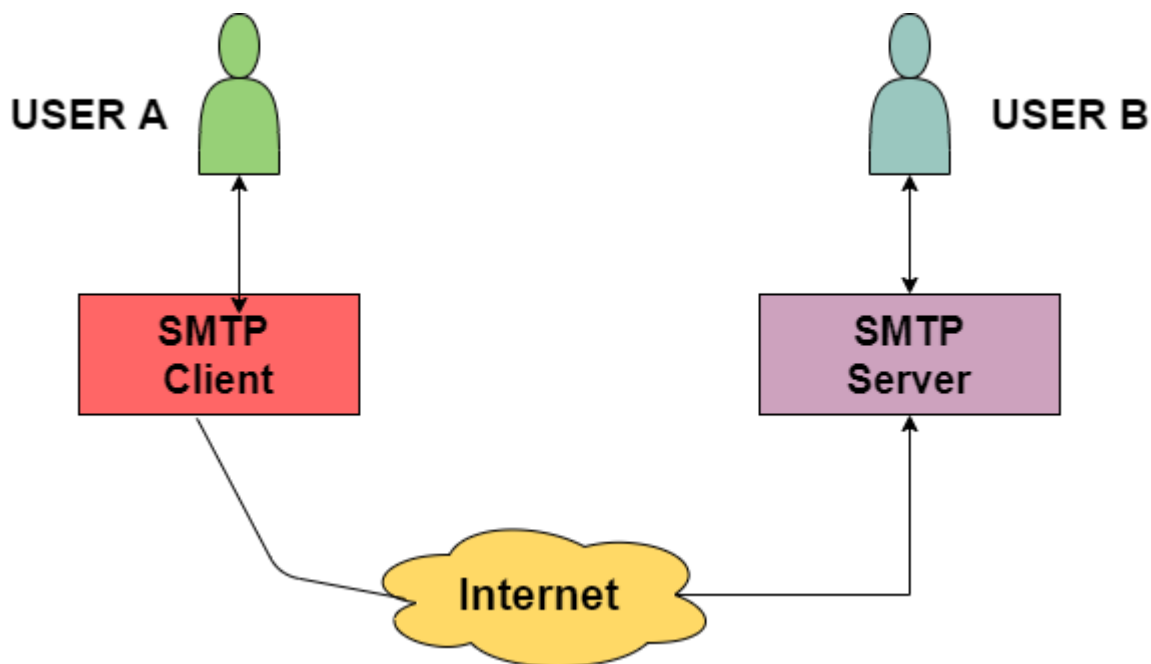


- The spoofing of the server can be done in order to send data to a random unknown port on any unauthorized computer

## **SMTP Protocol**

SMTP mainly stands for Simple Mail Transfer Protocol. Basically, the actual transfer of mail is done through the message transfer agents (MTA). Thus, in order to send the mail, the system must have the client MTA and in order to receive the mail, the system must have a server MTA.

- In order to define the MTA client and server on the Internet, there is a formal way and it is known as Simple Mail Transfer Protocol (SMTP).
- SMTP also makes the use of TCP/IP for sending and receiving e-mail.
- SMTP is based on the client/server model.
- The original standard port for SMTP is Port 25.
- Using this protocol, the client who wants to send the e-mail first opens a TCP connection to the SMTP server and then sends the e-mail across the TCP connection. It is important to note that the SMTP server is always in listening mode. As soon as it listens for the TCP connection from any client then the connection is Initiated on port 25 and after the successful connection, the client sends the e-mail/message immediately.



SMTP is used two times while sending an Email:

1. Between the Sender and Sender's mail server
2. Between the Sender's mail server and the Receiver's mail server

It is important to note that in order to receive or download the email,

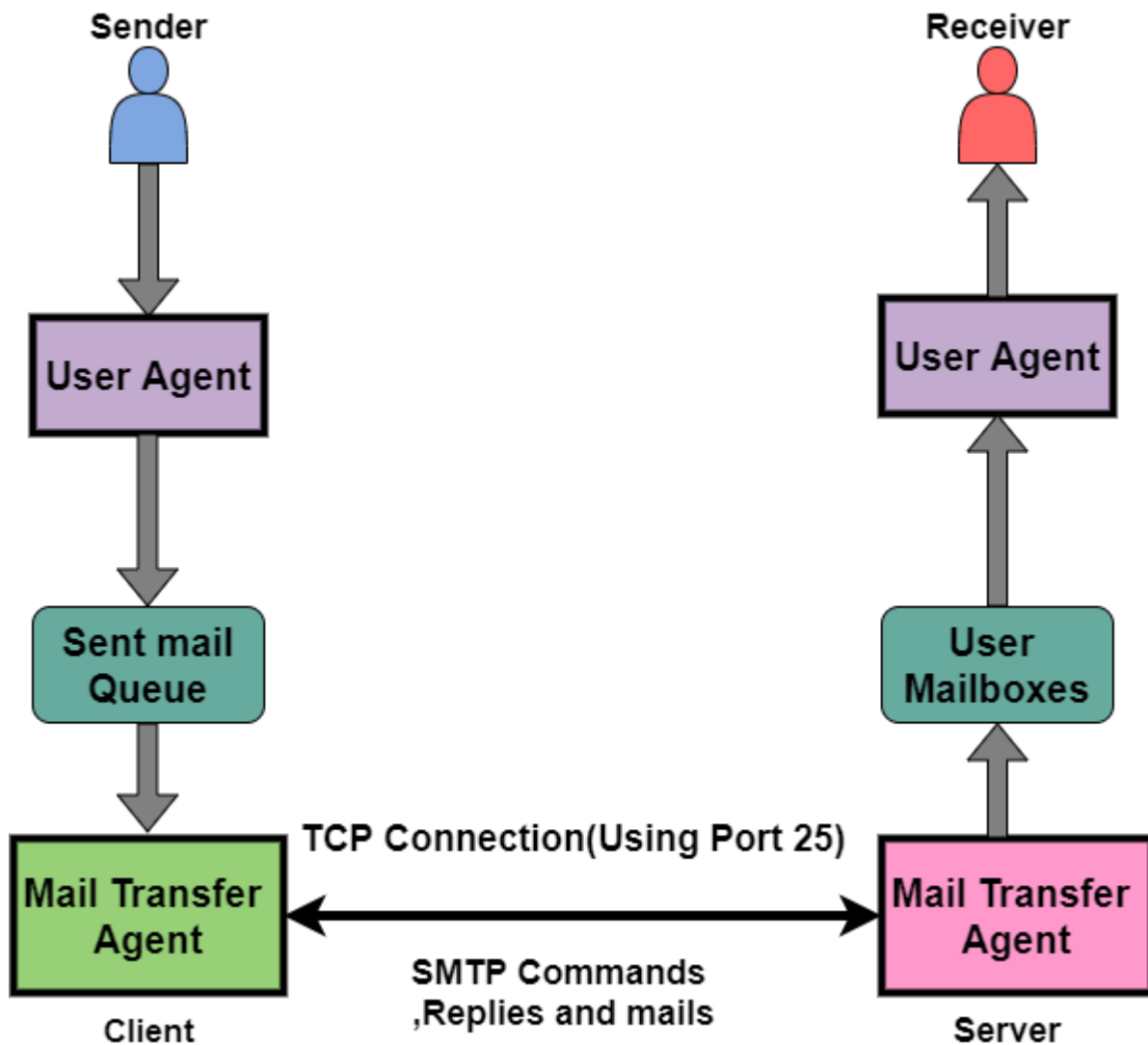
- There is a need for another protocol between the mail server of receiver and the receiver.
- Commonly used protocols are POP3 and IMAP. Thus, these two are mail access agents.

### Architecture of SMTP

All the users make use of User Agent (UA). The Mail Transfer Agent (MTA) mainly helps to exchange all the messages in between both sender and receiver using the TCP/IP. The system administrator has the authority to configure the set up of local MTA, thus the users who are sending the email do not need to deal with the MTA.

The MTA keeps the queue in the pool of messages, if the receiver is not available at that moment then MTA can schedule the repeat delivery of all the messages.

MTA (Mail User Agent) forwards the emails into mailboxes of the user's local system, and then the user agent (UA) can download those messages at any time.



The SMTP Client as well as the SMTP server both has two main components and these are:

- UA(User-Agent)
- MTA (Mail Transfer Agent)

Let us now take a look at communication between the sender and the receiver:

The user agent at the sender side prepares the message and then sent it to the MTA. The task of the MTA is to transfer the Email across the network to the Receiver MTA. Also, in order to send the Email, a system must have the client MTA and in order to receive the email, a system must have a server MTA.

## **Sending the Email**

An email is sent between the sender and receiver using a series of request and response messages. An Email mainly consists of two parts a header and body. The body part of an email indicates the main message area. It is the actual information that is to be read by the receiver. The header mainly contains the address of the sender and recipient and it also contains the subject of the email.

In order to terminate the header of the email, there is a NULL line, everything after the NULL line is considered as the body of the message.

## **Receiving the Email**

Mailboxes are checked by the user agent at the server side at a particular interval of time. In case if any information is received then it informs the receiver about the email.

At the time when the user tries to read the email then MTA mainly displays a list of emails with their short description in the mailbox. If the user selects any of the emails then can easily view the contents inside the email.

## **SMTP Protocol Method**

### **1. Store-and-Forward Method**

The store and forward method are used within an organization.

### **2. End-to-End Method**

Mainly the end-to-end method is used to communicate between the different organizations

An SMTP client is the one who wants to send the mail and will definitely contact the destination's host SMTP directly in the order to send the Email to the destination. Also, the session is initiated by the client SMPT.

On the other hand, the SMTP server will keep the mail to itself until it is successfully copied to the SMTP at the receiver. The server SMTP mainly responds to the session request.

Thus, the session is started by the client-SMTP and the server-SMTP will respond to the request of the sender.

## **Characteristics of SMTP**

Let us take a look at the characteristics of the SMTP:

- SMTP makes use of Port 25.
- It makes use of persistent TCP connections and thus can send multiple emails all at once.
- It is a stateless protocol.
- It is a connection-oriented protocol.
- It makes use of TCP at the transport layer.
- It is a push control protocol.

## **Advantages of SMTP**

Let us take a look at the advantages offered by the simple mail transfer protocol (SMTP):

- SMTP offers reliability in terms of the outgoing email messages.
- It is the simplest form of communication between various computers in a network via email.
- In those cases where a particular message was not delivered successfully then, the SMTP server always tries to re-send the same message until the transmission becomes successful.

## **Disadvantages of SMTP**

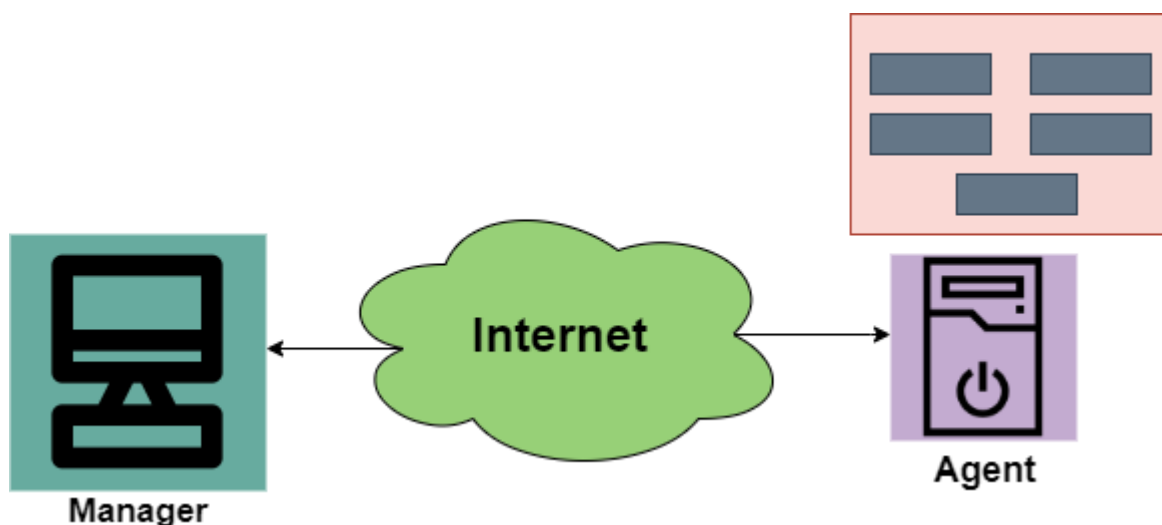
- SMTP does not provide good security.
- It is only limited to 7-bit ASCII characters.
- Beyond some specific length, email messages are rejected by SMTP servers.
- The usefulness of SMTP is limited by its simplicity.
- With the help of SMTP, the transmission of executable files and binary files is not possible until they get converted into text files.

# SNMP Protocol

SNMP mainly stands for Simple Network Management protocol.

- It is basically a framework that is used for managing the devices on the internet by using the TCP/IP protocol suite.
- Basically, SNMP provides a set of fundamental operations in order to monitor and maintain the Internet.
- It is an application layer protocol that was defined by the Internet engineering task force.
- This protocol is mainly used to monitor the network, detect the faults in the Network, and sometimes it is also used to configure the remote devices.

## Concept of SNMP



The SNMP protocol makes the use of Manager and Agent; where the manager is usually a host that controls and monitors the set of agents.

The SNMP is an application-level protocol and it consists of a few manager stations that mainly controls a set of agents. This protocol is mainly designed at the application level so that it can monitor the devices that are mainly made by different manufacturers and that are installed on different physical networks.

Thus, there are three components in the architecture of the SNMP:

- SNMP Manager
- SNMP Agent
- Management Information Base

### **SNMP Manager**

It is basically a centralized system and it is mainly used to monitor and manage devices that are connected with the network. SNMP manager is typically a computer and it is used to run one or more network management systems.

Given below are the main functions of SNMP Manager:

- Collects response from the agents.
- To acknowledge asynchronous events from the agents.
- To set variables in the agent.
- Queries the Agent

### **SNMP Agent**

SNMP Agent is basically a software program that is packaged within the network element. It is mainly installed on a managed device where managed devices can be switches, servers, routers, PC, etc.

Mainly the agents keep the information in the database also the manager has the access to the values present in the database.

Given below are the main responsibilities of the SNMP Agent:

- SNMP agents mainly collect the management information about its local environment
- The SNMP agent mainly signals an event to the manager.
- The SNMP agents also act as a proxy for some non-SNMP manageable network nodes.

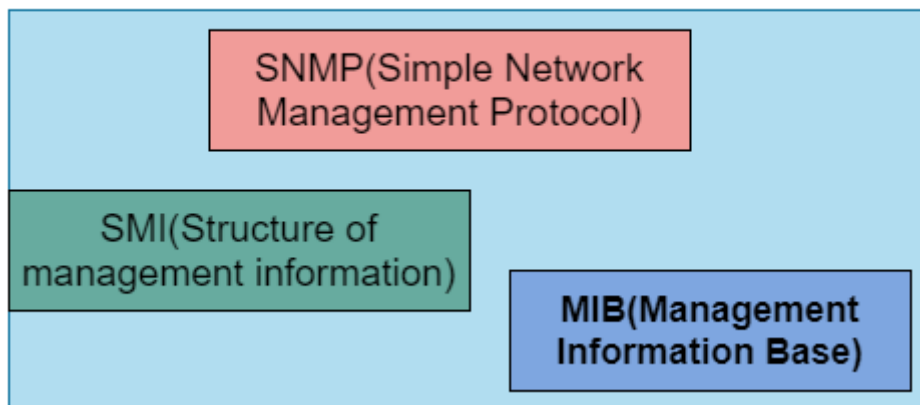
Thus, the management with SNMP is mainly based on these given ideas:

1. An SNMP manager checks the agent by requesting information that mainly reflects the behavior of the SNMP agent.
2. The SNMP manager also forces the agent to perform the task by resetting the values in the database of the agent.
3. Management process is also contributed by the agent just by warning the SNMP manager about an unusual situation.

## Management Components

In order to perform the Management tasks, the SNMP protocol makes the use of two other protocols and are SMI and MIB. We can also say that the Management on the Internet is done by the cooperation of three protocols and these are SNMP, MIB, SMI.

### Management



Let us discuss their roles one by one;

## Role of SNMP

The SNMP protocol performs some specific roles in Network Management;

- It mainly defines the format of the packet that needs to be sent from the manager to the agent or vice-versa.
- SNMP is also used to interpret the result and create the statistics.
- The packets that are exchanged between the manager and agent contains the name of the object(variable) and their status(values).



- The SNMP is also responsible for reading and changing these values.

## **Role of SMI**

In order to use the SNMP, there is a need for some rules and these rules are for naming the objects. Now it's time to take a look at the roles of SMI:

- SMI (Structure of Management Information) is mainly used to define the general rules for naming the objects.
- It is also used to define the type of objects that includes (range and length).
- This is also used to show how to encode the objects and values.
- The SMI does not define the number of objects that should be managed by an entity.
- It also does not define the association between the objects and their values.

## **Role of MIB**

In order to manage each entity, this protocol is mainly used to define the number of objects and then to name them according to the rules defined by the SMI and after that associate a type to each named object.

- MIB (Management Information Base) is mainly used to create a set of objects that are defined for each entity that is similar to the database.
- Thus, MIB mainly creates a collection of named objects, their types.

## **Advantages of SNMP Protocol**

Given below are some of the benefits of using SNMP:

- It is the standard network management protocol.
- This protocol is independent of the operating system and programming language.
- The functional design of this protocol is Portable.
- The SNMP is basically a core set of operations and it remains the same on all managed devices. Thus SNMP supports extendibility.

- SNMP is a universally accepted protocol.
- It is a lightweight protocol.
- This protocol allows distributed management access.

### **Disadvantages**

Some of the drawbacks of SNMP are as follows:

- This protocol leads to the reduction of the bandwidth of the network.
- Access control, authentication, and privacy of data are some largest security issues using this.
- SNMP deals with information that is neither detailed nor enough well organized.

## **MIME Protocol**

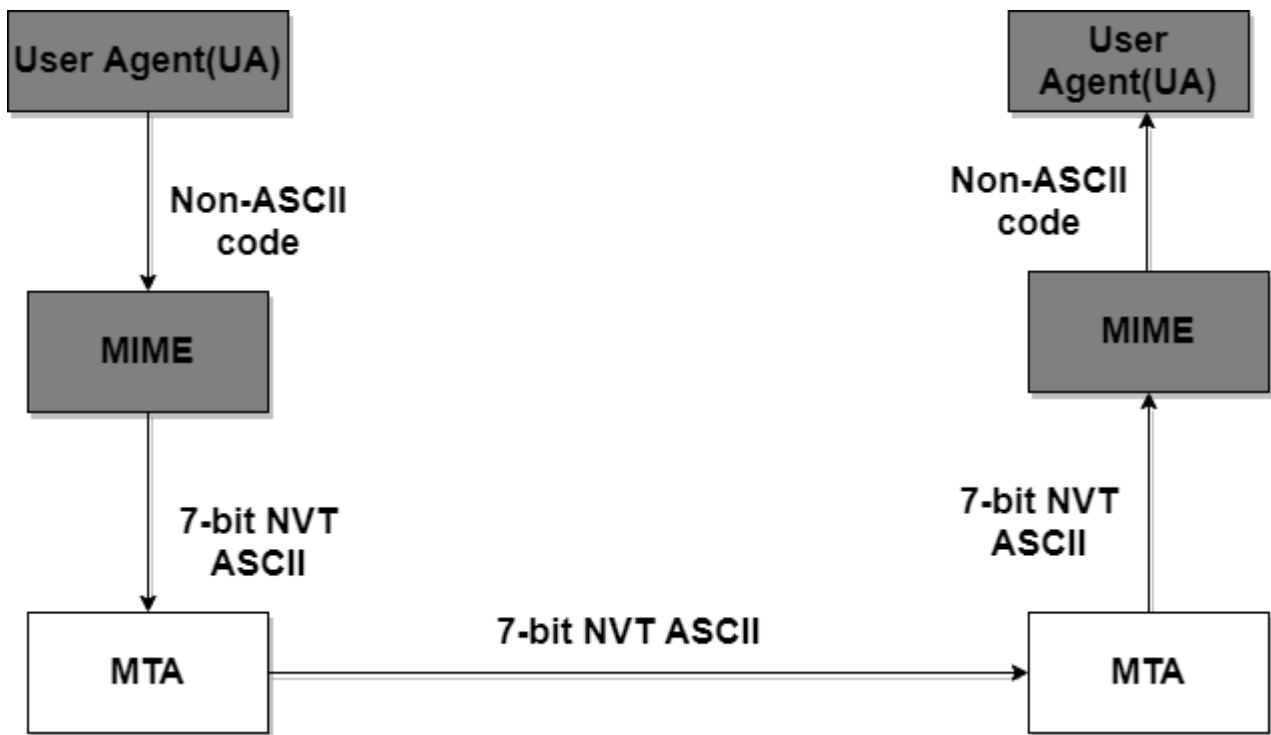
MIME is a short form of Multipurpose Internet Mail Extensions (MIME).

- It is mainly used to describe message content types.
- MIME is basically a supplementary protocol that mainly allows the non-ASCII data to be sent through E-mail.
- It basically transforms the non-ASCII data at the sender site NVT ASCII data and then delivers them to the client in order to be sent through the Internet.
- At the receiver side, the message is transformed back to the original data.
- MIME is basically a set of software functions that mainly transforms the Non-ASCII data to ASCII data and vice-versa,

Following are the different kinds of data files that can be exchanged on the Internet using MIME:

- Audio
- Images

- Text
- Video
- Other application-specific data (it can be pdf, Microsoft word document, etc).
- MIME is one of the applications of Email and it is not restricted only to the textual data.



Let us take an example where a user wants to send an Email through the user agent, and this email is in a non-ASCII format. So here we use the MIME protocol that mainly converts this non-ASCII format into the 7-bit NVT ASCII format.

The message is transferred via email system to the other side in the 7-bit NVT ASCII format and then again, the MIME protocol will convert it back into the Non-ASCII code. at the receiver side so that receiver can read it.

At the beginning of any email transfer basically, there is an insertion of the MIME header.

## **Features of MIME**

The features of the MIME protocol are as follows:

1. MIME supports the character set other than ASCII.
2. With the help of MIME, we can send multiple attachments in a single message.
3. MIME also provides support for different content types and multi-part messages.
4. It provides support of compound documents
5. It also provides support for non-textual content in the email message.

## **MIME Header**

The MIME header is mainly added to the original e-mail header section in order to define the transformation. Given below are five headers that are added to the original header:

1. MIME-Version
2. Content-Type
3. Content-Transfer-Encoding.
4. Content-Id
5. Content-Description

## **Advantages of MIME**

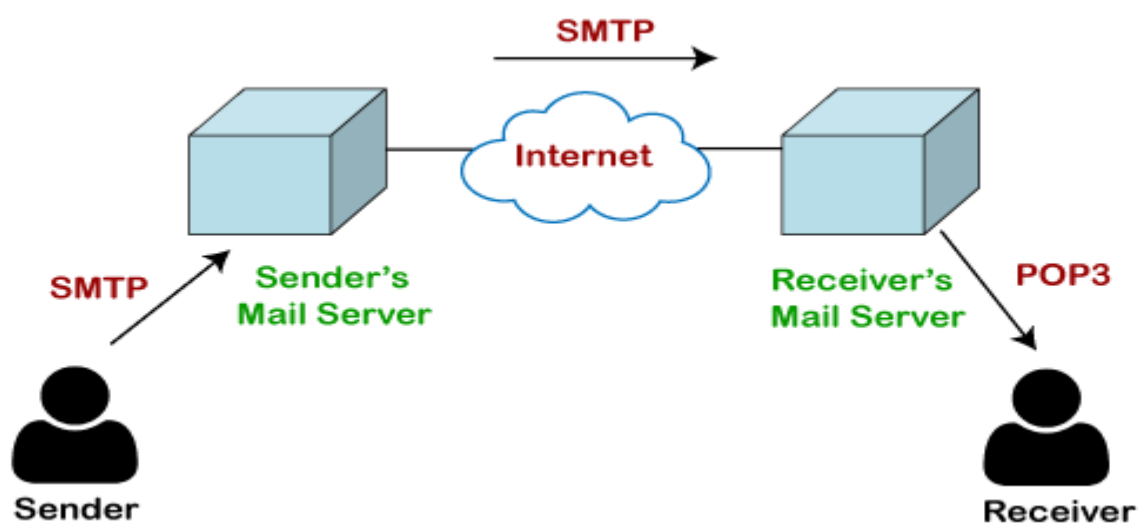
Some benefits of using MIME are as follows:

- Supports Interactive Multimedia.
- Supports the transfer of Multiple attachments.
- Supports different content types.
- Also supports text with different fonts and colors.

# 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 SMTP 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?



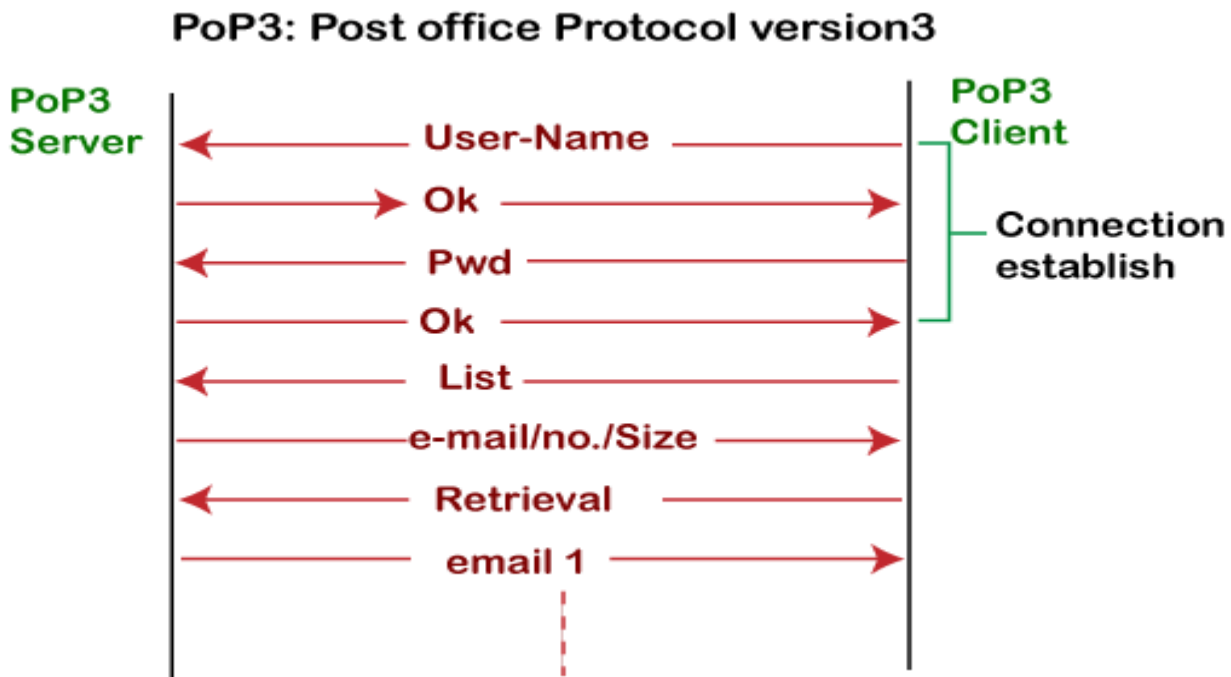
Suppose sender wants to send the mail to receiver. First mail is transmitted to the sender's mail server. Then, the mail is transmitted from the sender's mail server to the receiver's mail server over the internet. On receiving the mail at the receiver's mail server, the mail is then sent to the user. 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. At the receiver's mail server, the POP or 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.

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.

## 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.

# DNS Protocol

DNS is an abbreviation of Domain Name System or Domain Name Service. It is an application layer protocol.

Basically, a Domain name system is a supporting program that is used by other programs such as an E-mail.

The user of the email program knows the email address of the recipient; the Internet protocol needs the IP address.

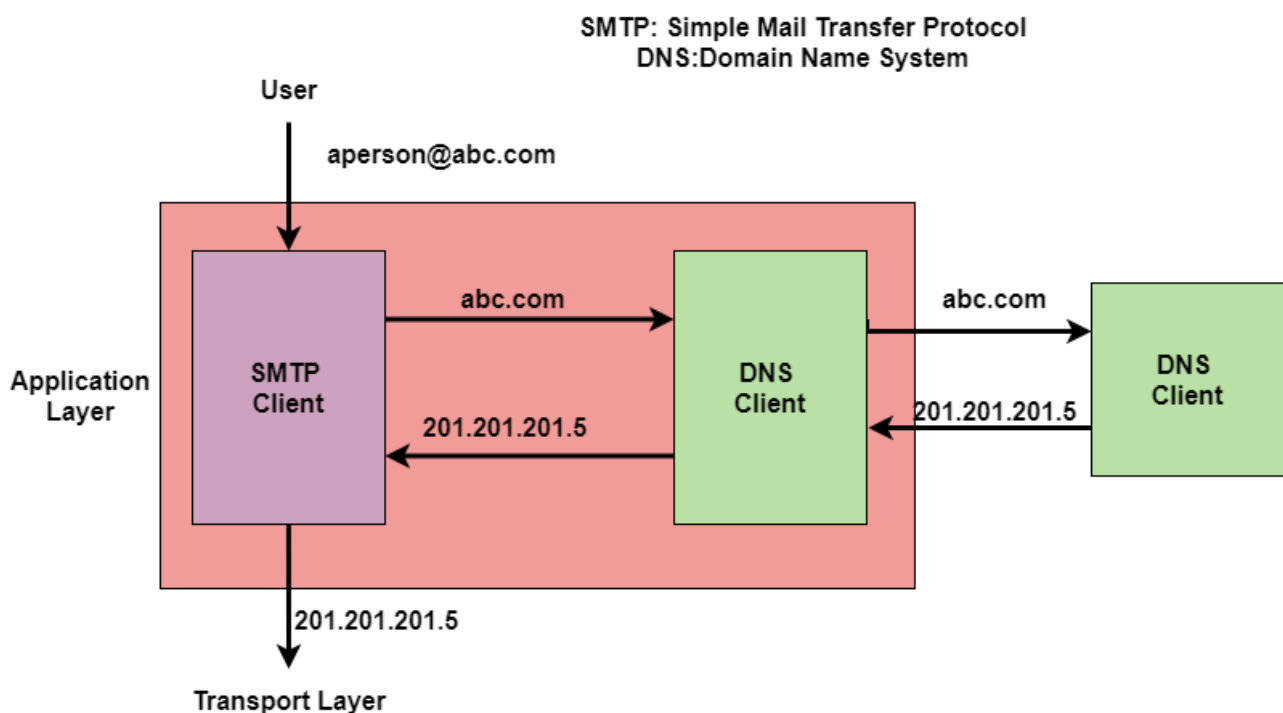
Mainly the DNS client program sends a request to the DNS server in order to map the e-mail address to the corresponding IP address.

In order to identify an entity, the TCP/IP protocols also make use of an IP address that uniquely identifies the connection of the host to the internet. But people usually prefer to use names instead of numeric addresses. Thus there is a need for the system that can map a name to an address or an address to a name.

Domain Name System is a system that can map a name to an address or an address to a name.

## Example

Given below is an example of using the Domain name system:





## **Name Space**

NameSpace basically maps each address to a unique name. The names assigned to the machines must be unique because addresses are unique.

It is further categorized into two:

- Flat Name Space
- Hierarchical Name Space

## **Flat Name Space**

In the Flat Name Space basically, a name is assigned to an address.

- A name in this space is basically a sequence of characters without any structure.
- Also, the names may or may not have a common section. In case if they have a common section then it has no meaning.
- One of the main disadvantages of this system is that it cannot be used in the case of large systems; because there is no central control and it will lead to ambiguity and duplication.

## **Hierarchical Name Space**

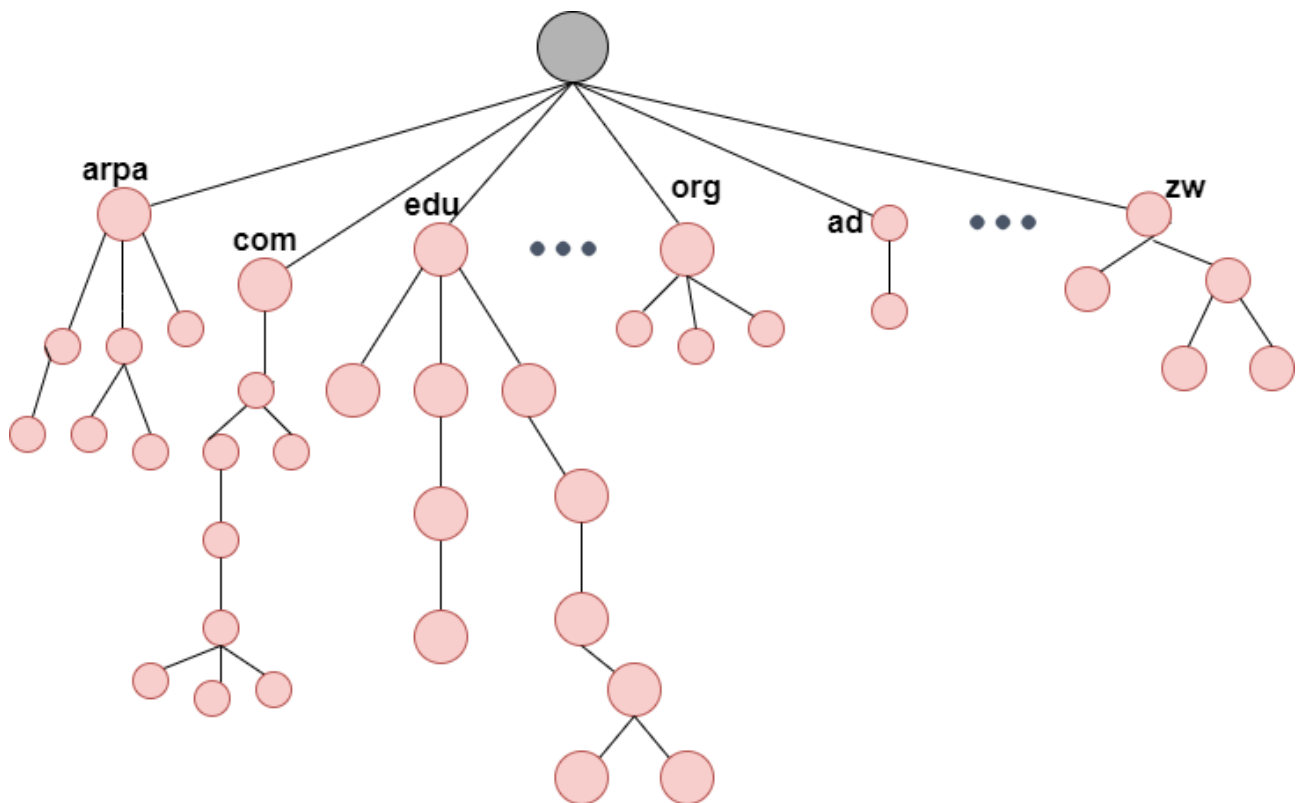
In Hierarchical Name Space each name consists of several parts.

- The first part mainly indicates the nature of the organization.
- The second part mainly indicates the name of the organization.
- The third part mainly defines the departments in the organization and so on.
- The central authority can assign the part of the name that indicates the name and nature of the organization and the responsibility of the rest of the name is given to the organization itself.
- An organization can also add suffixes (or prefixes) to the name in order to define the host or resources.

## Domain Name Space

When we use the hierarchical Name Space in that case we need to design the Domain Name Space. In this Design, the names are defined in the inverted-tree structure where the root lies at the top.

Also, the tree can have 128 levels and these are from Level 0(root) to Level 127.



### Label

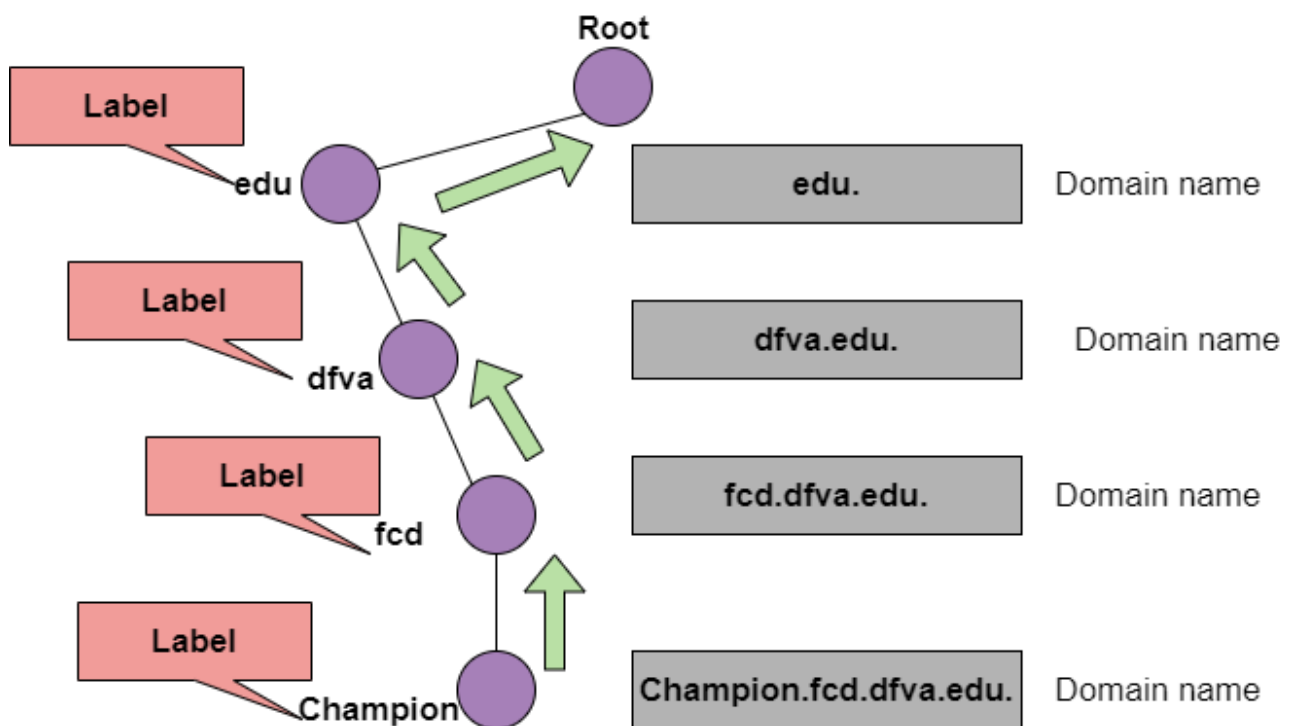
Each node of the tree must have a label. A Label is a string having a maximum of 63 characters.

- The root label is basically a null string(means an empty string).
- Domain Name Space requires that the children of the node that means branches from the same node should have different labels and this guarantees the uniqueness of the domain names.

## Domain Name

Each node of the tree has a domain name.

- A Full domain name is basically a sequence of labels that are usually separated by dots(.).
- The domain name is always read from the node up to the root.
- The last label is the label of the root that is always null.
- All this means that the full domain name always ends in the null label, which means that the last character is always a dot because the null string is nothing.



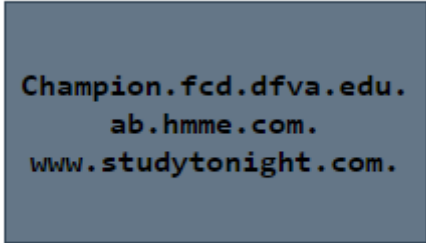
The figure shows the domain names and labels

**Domain Names are further categorized into two:**

### **1. Fully Qualified Domain Name**

- If the label is terminated by the null string then it is known as a fully qualified domain name. This domain name contains the full name of the host.
- FQDN mainly consists of two parts: hostname and domain name.
- The FQDN mainly contains all the labels from the most specific one to the most general one that helps to uniquely define the name of the host.
- Example: Champion.fcd.dfva.edu. in this the hostname is Champion.

Given below are some Fully Qualified Domain names;




```
Champion.fcd.dfva.edu.  
ab.hmme.com.  
www.studytonight.com.
```

### **2. Partially Qualified Domain Name**

If the label is not terminated by the null string, then it is known as Partially Qualified Domain Name.

This name starts from the node but does not reach the root.

It is mainly used when the name to be resolved belongs to the same site as the client and in this case, the resolver can supply the missing part that is known as a suffix in order to create an FQDN.



```
Champion.fcd.dfva.edu  
ab.hmme  
www
```

### **Domain**

A Domain is basically the subtree of the Domain Name Space. The name of the domain is usually the domain name of the node that is at the top of the subtree.

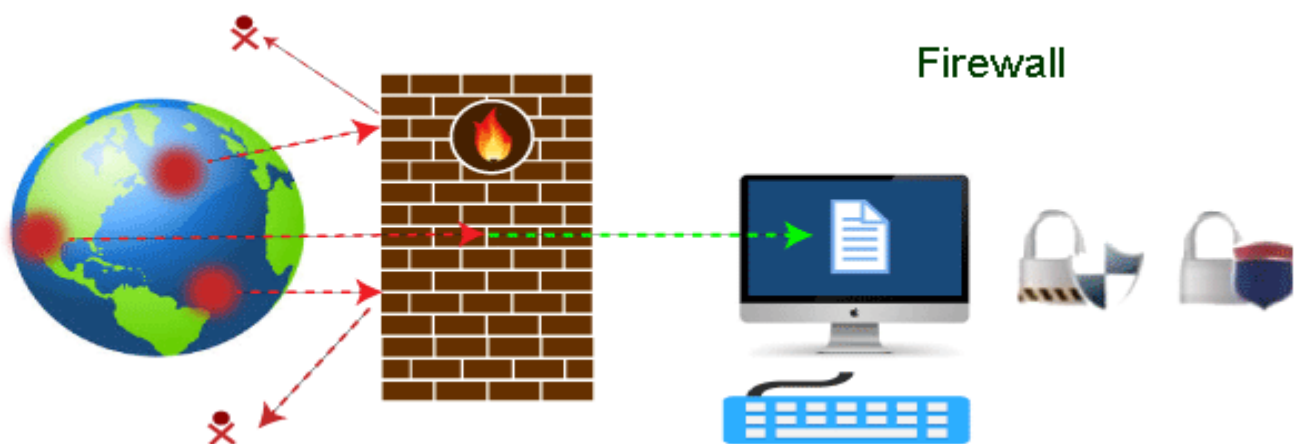
# Firewall

Nowadays, it is a big challenge to protect our sensitive data from unwanted and unauthorized sources. There are various tools and devices that can provide different security levels and help keep our private data secure. One such tool is a 'firewall' that prevents unauthorized access and keeps our computers and data safe and secure.

## What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



## Firewall: Hardware or Software

This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware and software, though it's best to have both.

Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

## **Why Firewall**

Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.

Firewalls are designed in such a way that they can react quickly to detect and counter-attacks throughout the network. They can work with rules configured to protect the network and perform quick assessments to find any suspicious activity. In short, we can point to the firewall as a traffic controller.

Some of the important risks of not having a firewall are:

## **Open Access**

If a computer is running without a firewall, it is giving open access to other networks. This means that it is accepting every kind of connection that comes through someone. In this case, it is not possible to detect threats or attacks coming through our network. Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.

## **Lost or Comprised Data**

Without a firewall, we are leaving our devices accessible to everyone. This means that anyone can access our device and have complete control over it, including the network. In this case, cybercriminals can easily delete our data or use our personal information for their benefit.

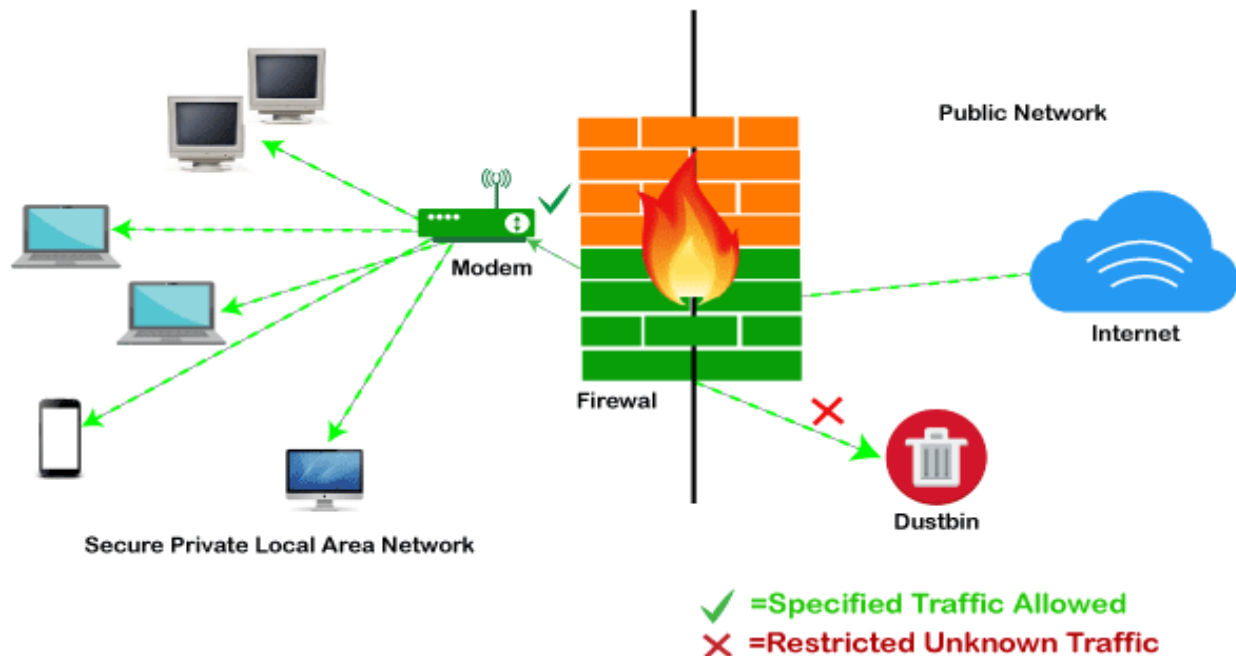
## **Network Crashes**

In the absence of a firewall, anyone could access our network and shut it down. It may lead us to invest our valuable time and money to get our network working again.

## **How does a firewall work?**

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.



## Functions of Firewall

As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.

Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller. Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.

Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control

- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

### **Limitations of Firewall**

When it comes to network security, firewalls are considered the first line of defense. But the question is whether these firewalls are strong enough to make our devices safe from cyber-attacks. The answer may be "no". The best practice is to use a firewall system when using the Internet. However, it is important to use other defense systems to help protect the network and data stored on the computer. Because cyber threats are continually evolving, a firewall should not be the only consideration for protecting the home network.

The importance of using firewalls as a security system is obvious; however, firewalls have some limitations:

- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering.
- Firewalls cannot stop or prevent attackers with modems from dialling in to or out of the internal network.
- Firewalls cannot secure the system which is already infected.

Therefore, it is recommended to keep all Internet-enabled devices updated. This includes the latest operating systems, web browsers, applications, and other security software (such as anti-virus). Besides, the security of wireless routers should be another practice. The process of protecting a router may include options such as repeatedly changing the router's name and password, reviewing security settings, and creating a guest network for visitors.

### **Types of Firewall**

Depending on their structure and functionality, there are different types of firewalls. The following is a list of some common types of firewalls:



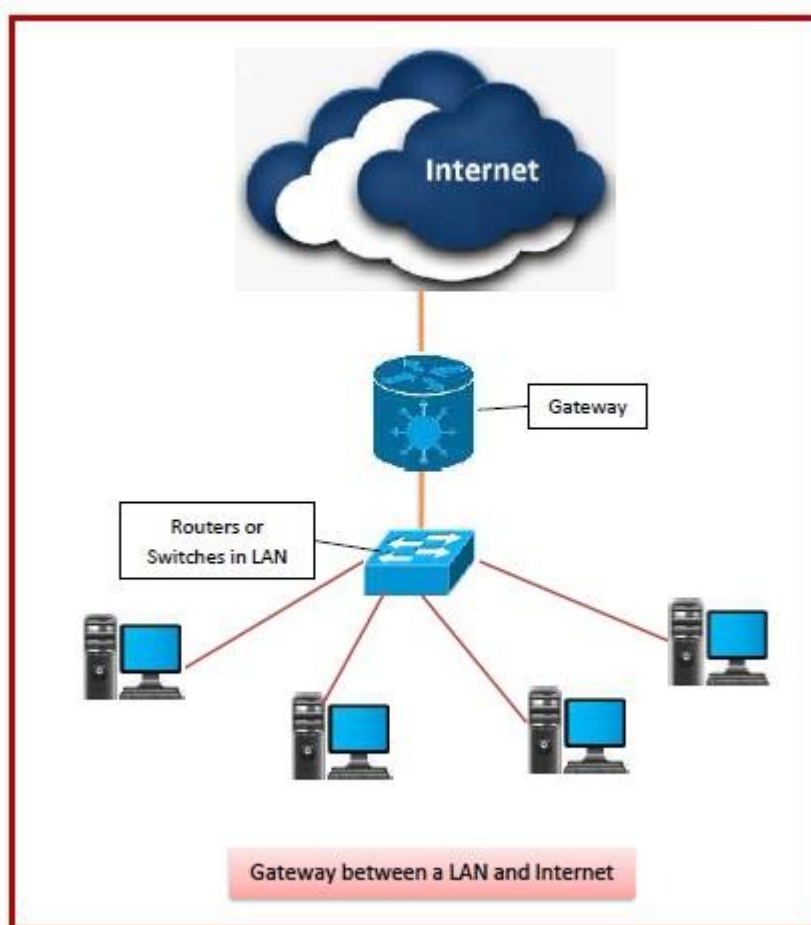
- Proxy Firewall
- Packet-filtering firewalls
- Stateful Multi-layer Inspection (SMLI) Firewall
- Unified threat management (UTM) firewall
- Next-generation firewall (NGFW)
- Network address translation (NAT) firewalls

## Difference between a Firewall and Anti-virus

Attributes	Firewall	Anti-virus
Definition	A firewall is defined as the system which analyzes and filters incoming or outgoing data packets based on pre-defined rules.	Anti-virus is defined as the special type of software that acts as a cyber-security mechanism. The primary function of Anti-virus is to monitor, detect, and remove any apprehensive or distrustful file or software from the device.
Structure	Firewalls can be hardware and software both. The router is an example of a physical firewall, and a simple firewall program on the system is an example of a software firewall.	Anti-virus can only be used as software. Anti-virus is a program that is installed on the device, just like the other programs.
Implementation	Because firewalls come in the form of hardware and software, a firewall can be implemented either way.	Because Anti-virus comes in the form of software, therefore, Anti-virus can be implemented only at the software level. There is no possibility of implementing Anti-virus at the hardware level.
Responsibility	A firewall is usually defined as a network controlling system. It means that firewalls are primarily responsible for monitoring and filtering network traffic.	Anti-viruses are primarily responsible for detecting and removing viruses from computer systems or other devices. These viruses can be in the form of infected files or software.
Scalability	Because the firewall supports both types of implementations, hardware, and software, therefore, it is more scalable than anti-virus.	Anti-viruses are generally considered less-scalable than firewalls. This is because anti-virus can only be implemented at the software level. They don't support hardware-level implementation.
Threats	A firewall is mainly used to prevent network related attacks. It mainly includes external network threats?for example- Routing attacks and IP Spoofing.	Anti-virus is mainly used to scan, find, and remove viruses, malware, and Trojans, which can harm system files and software and share personal information (such as login credentials, credit card details, etc.) with hackers.

# Gateway

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.



## Features of Gateways

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.

- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.
- When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.
- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.
- It uses packet switching technique to transmit data across the networks.

## **Types of Gateways**

On basis of direction of data flow, gateways are broadly divided into two categories –

**Unidirectional Gateways** – They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.

**Bidirectional Gateways** – They allow data to flow in both directions. They can be used as synchronization tools.