Application Layer Protocols

❖ 5.1 Application Layer Protocols

- The application layer is present at the top of the **OSI model.**
- It is the layer through which users interact.
- It provides services to the user. Application layer performs several kinds of functions which are requirement in any kind of application or communication process.

Application Layer Protocol in Computer Network

1. TELNET

- Telnet stands for the **TEL**etype **NET**work. It helps in terminal emulation. It allows Telnet clients to access the resources of the Telnet server. Port number of telnet is 23.

2. FTP

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

3. TFTP

- The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it.The Port number for TFTP is 69.

4. NFS

- It stands for a Network File System. It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. The Port number for NFS is 2049.

5. SMTP

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

6. LPD

- It stands for Line Printer Daemon. It is designed for printer sharing. It is the part that receives and processes the request. A "daemon" is a server or agent. The Port number for LPD is 515.

7. X window

- It defines a protocol for the writing of graphical user interface–based client/server applications. The idea is to allow a program, called a client, to run on one computer. It is primarily used in networks of interconnected mainframes. Port number for X window starts from 6000 and increases by 1 for each server.

8. SNMP

- It stands for Simple Network Management Protocol. The Port number of SNMP is 161(TCP) and 162(UDP).

9. DNS

- It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address The Port number for DNS is 53.

10. DHCP

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

11. HTTP/HTTPS

- HTTP stands for Hypertext Transfer Protocol and HTTPS is the more secured version of HTTP, that's why HTTPS stands for Hypertext Transfer Protocol Secure. This protocol is used to access data from the World Wide Web. The Hypertext is the well-organized documentation system that is used to link pages in the text document.
- HTTP is based on the client-server model.
- It uses TCP for establishing connections.
- HTTP is a stateless protocol, which means the server doesn't maintain any information about the previous request from the client.
- HTTP uses port number 80 for establishing the connection.

12. POP

- POP stands for Post Office Protocol and the latest version is known as POP3 (Post Office Protocol version 3). This is a simple protocol used by User agents for message retrieval from mail servers.
- POP protocol work with Port number 110.
- It uses TCP for establishing connections.
- POP works in dual mode- Delete mode, Keep Mode.
- In Delete mode, it deletes the message from the mail server once they are downloaded to the local system.
- In Keep mode, it doesn’t delete the message from the mail server and also facilitates the users to access the mails later from the mail server.

13. IRC

- IRC stands for Internet Relay Chat. It is a text-based instant messaging/chatting system. IRC is used for group or one-to-one communication. It also supports file, media, data sharing within the chat. It works upon the client-server model. Where users connect to IRC server or IRC network via some web/ standalone application program.
- It uses TCP or TLS for connection establishment.
- It makes use of port number 6667.

14. MIME

- MIME stands for Multipurpose Internet Mail Extension. This protocol is designed to extend the capabilities of the existing Internet email protocol like SMTP. MIME allows non-ASCII data to be sent via SMTP. It allows users to send/receive various kinds of files over the Internet like audio, video, programs, etc. MIME is not a standalone protocol it works in collaboration with other protocols to extend their capabilities.

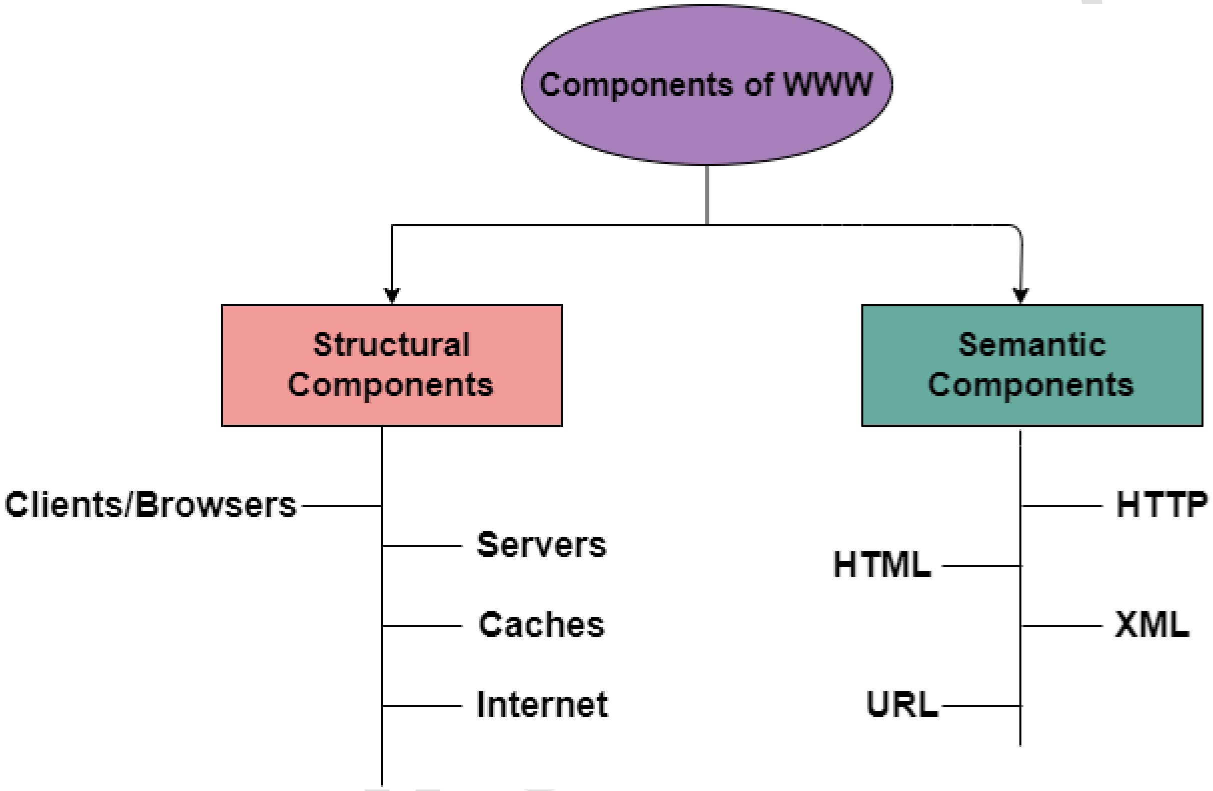
❖ 5.2 World Wide Web and HTTP

- 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.
- It was invented by Tim Berners-Lee.

Components of WWW

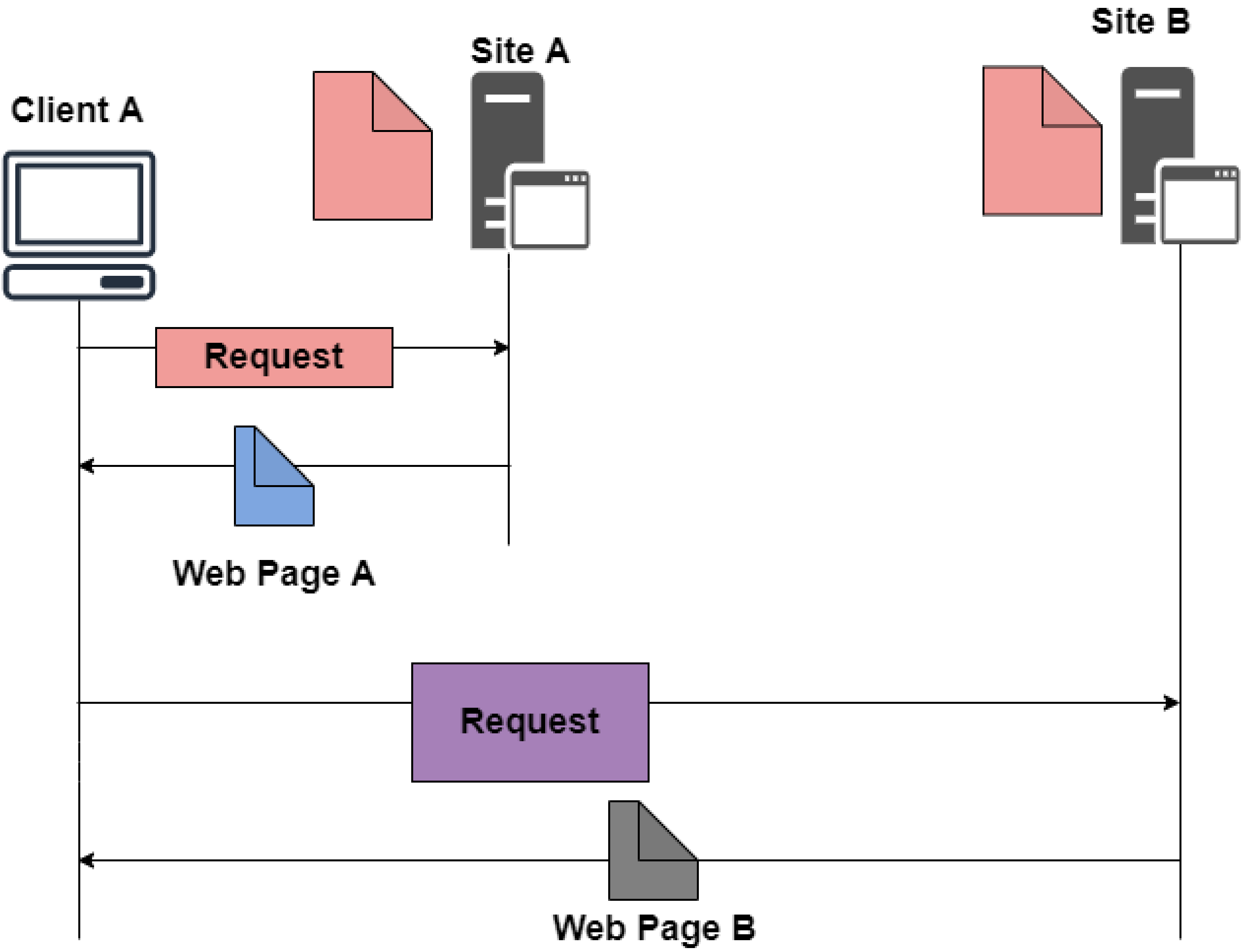
The Components of WWW mainly falls into two categories:

1. Structural Components
2. 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.

Components of WWW.

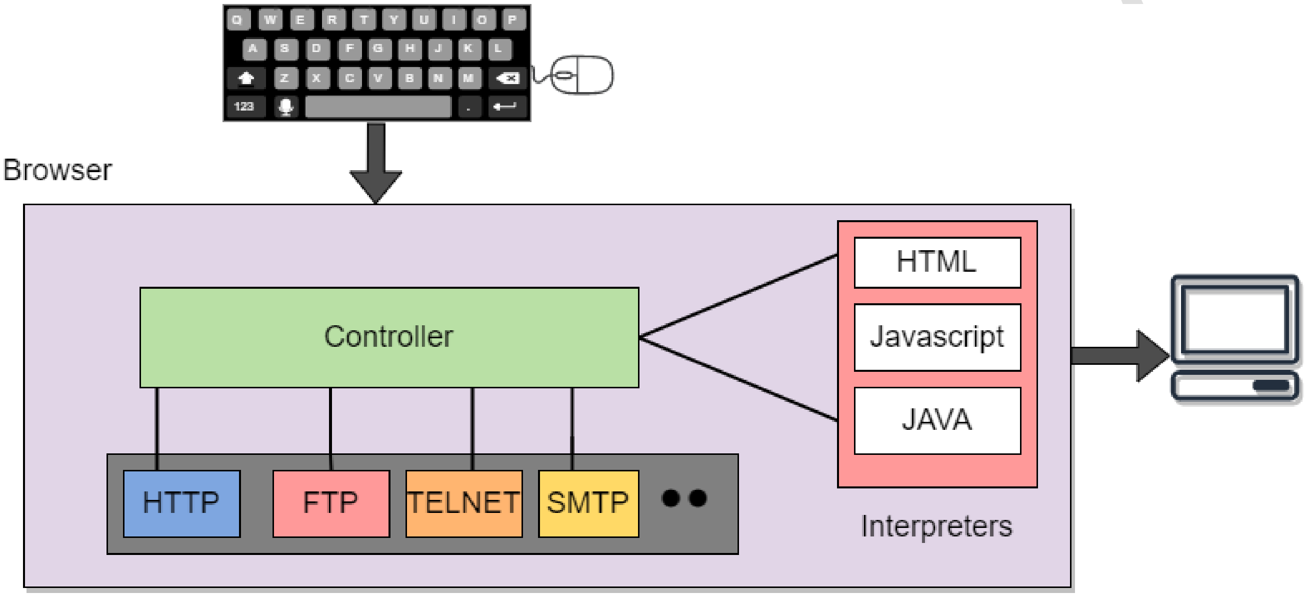
1. Client/Browser

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, and TELNET.



2. 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.

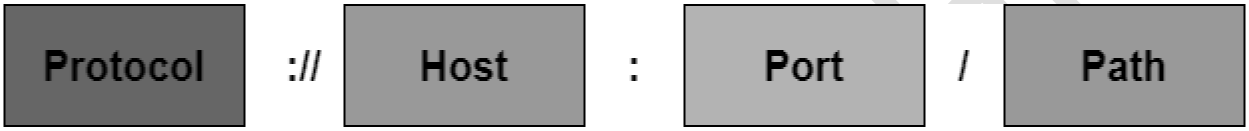
3. URL

URL is an abbreviation of **the Uniform Resource Locator.**

- It is basically a standard used for specifying any kind of information on the Internet.
- In order to access any page the client generally needs an address.
- To facilitate the access of the documents throughout the world HTTP generally makes use of Locators.

- **URL mainly defines the four things:**

- **Protocol**
  It is a client/server program that is mainly used to retrieve the document. A commonly used protocol is HTTP.
- **Host Computer**
  It is the computer on which the information is located. It is not mandatory because it is the name given to any computer that hosts the web page.
- **Port**
  The URL can optionally contain the port number of the server. If the port number is included then it is generally inserted in between the host and path and is generally separated from the host by the colon.
- **Path**
  It indicates the pathname of the file where the information is located.



4. HTML

HTML is an abbreviation of Hypertext Markup Language.

- It is generally used for creating web pages.
- It is mainly used to define the contents, structure, and organization of the web page.

5. XML

XML is an abbreviation of Extensible Markup Language. It mainly helps in order to define the common syntax in the semantic web.

Features of WWW

- 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

- 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

- 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.

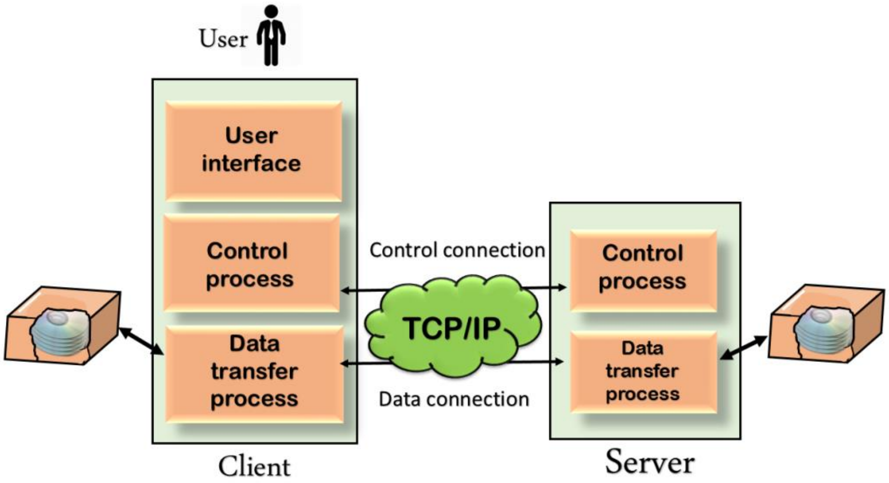
5.3 FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

Objectives of FTP

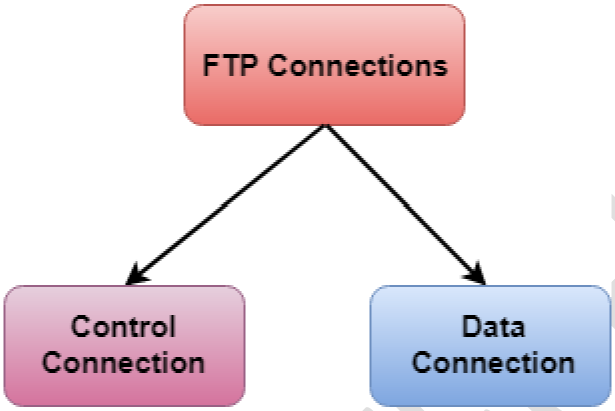
- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Mechanism of FTP



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

There are two types of connections in FTP:



- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

- Speed: One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- Efficient: It is more efficient as we do not need to complete all the operations to get the entire file.

- Security: To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- Back & forth movement: FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

❖ 5.4 Electronic Mail

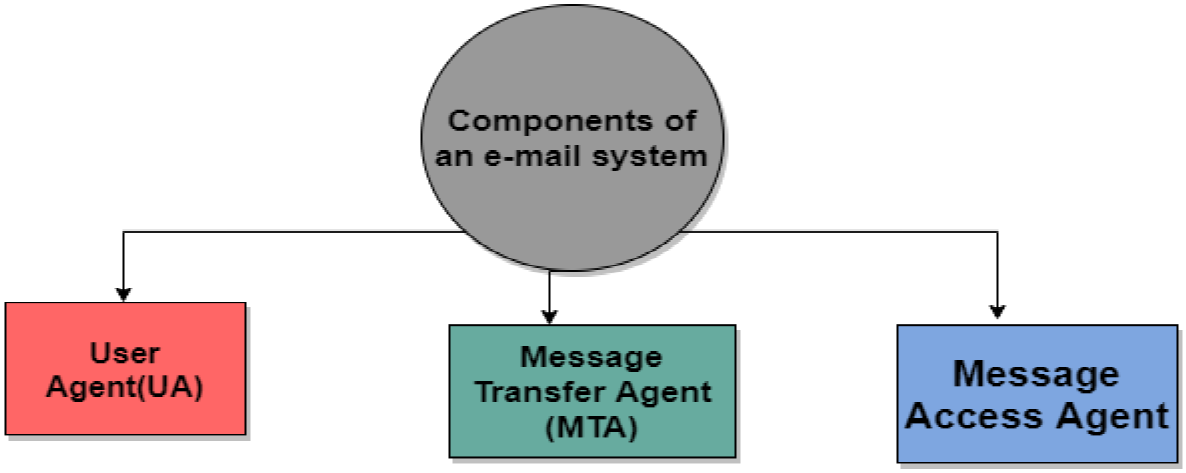
- Electronic mail, commonly known as email, is a method of exchanging messages over the internet.

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.

Components of E-mail System

The basic Components of an Email system are as follows:



1. User Agent (UA)

It is a program that is mainly used to send and receive an email. It is also known as an email reader. User-Agent is used to compose, send and receive emails.

- It is the first component of an Email.
- User-agent also handles the mailboxes.
- The User-agent mainly provides the services to the user in order to make the sending and receiving process of message easier.

Given below are some services provided by the User-Agent:

1.Reading the Message

2.Replying the Message

3.Composing the Message

4.Forwarding the Message.

5.Handling the Message.

2. Message Transfer Agent

The actual process of transferring the email is done through the Message Transfer Agent(MTA).

- In order to send an Email, a system must have an MTA client.
- In order to receive an email, a system must have an MTA server.
- The protocol that is mainly used to define the MTA client and MTA server on the internet is called SMTP (Simple Mail Transfer Protocol).
- The SMTP mainly defines how the commands and responses must be sent back and forth

3. Message Access Agent

In the first and second stages of email delivery, we make use of SMTP.

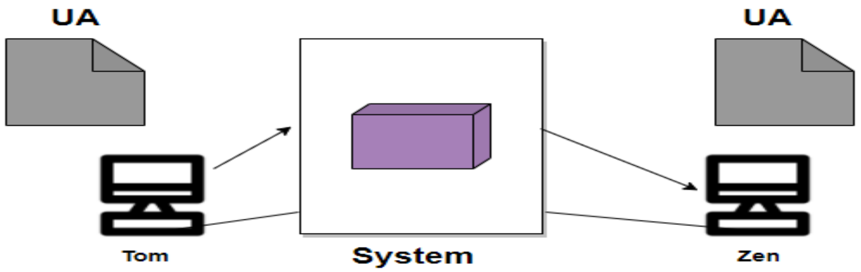
- SMTP is basically a Push protocol.
- The third stage of the email delivery mainly needs the pull protocol, and at this stage, the message access agent is used.
- The two protocols used to access messages are POP and IMAP4.

- **Architecture of Email**

Now its time to take a look at the architecture of e-mail with the help of four scenarios:

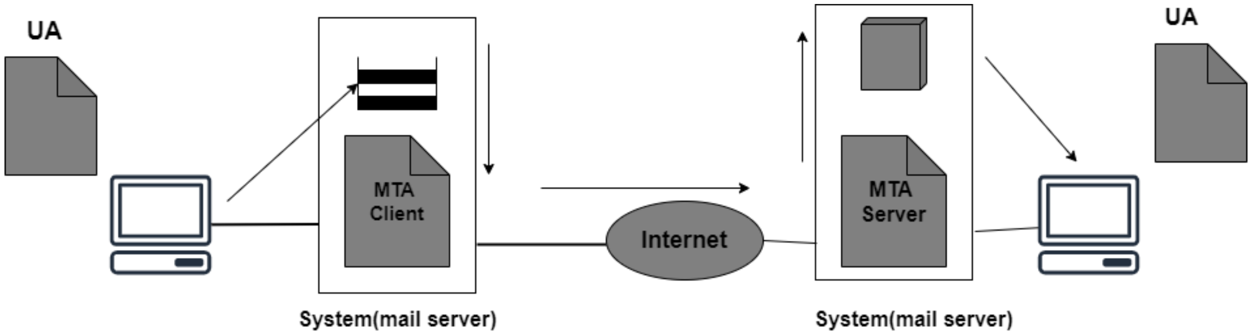
First Scenario

When the sender and the receiver of an E-mail are on the same system, then there is the need for only two user agents.



Second Scenario

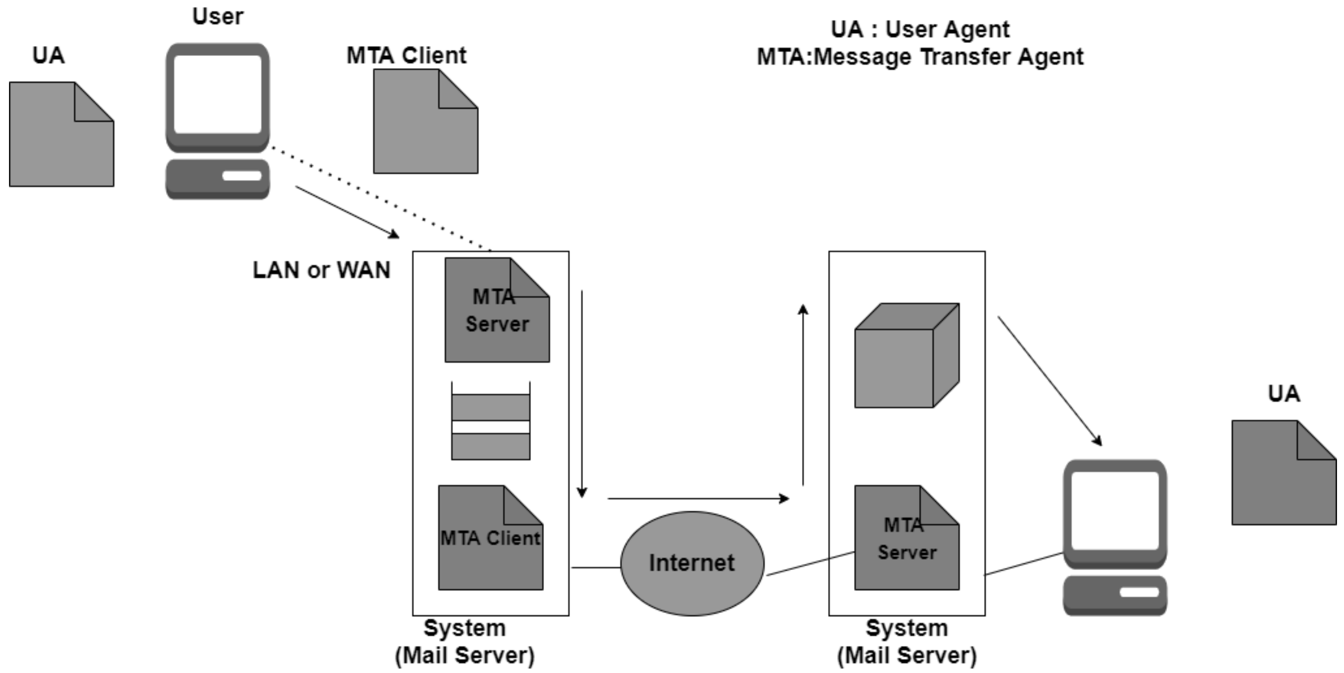
In this scenario, the sender and receiver of an e-mail are basically users on the two different systems. Also, the message needs to send over the Internet. In this case, we need to make use of User Agents and Message transfer agents (MTA).



Third Scenario

In this scenario, the sender is connected to the system via a point-to-point WAN it can be either a dial-up modem or a cable modem. While the receiver is directly connected to the system like it was connected in the second scenario.

Also in this case sender needs a User agent(UA) in order to prepare the message. After preparing the message the sender sends the message via a pair of MTA through LAN or WAN.



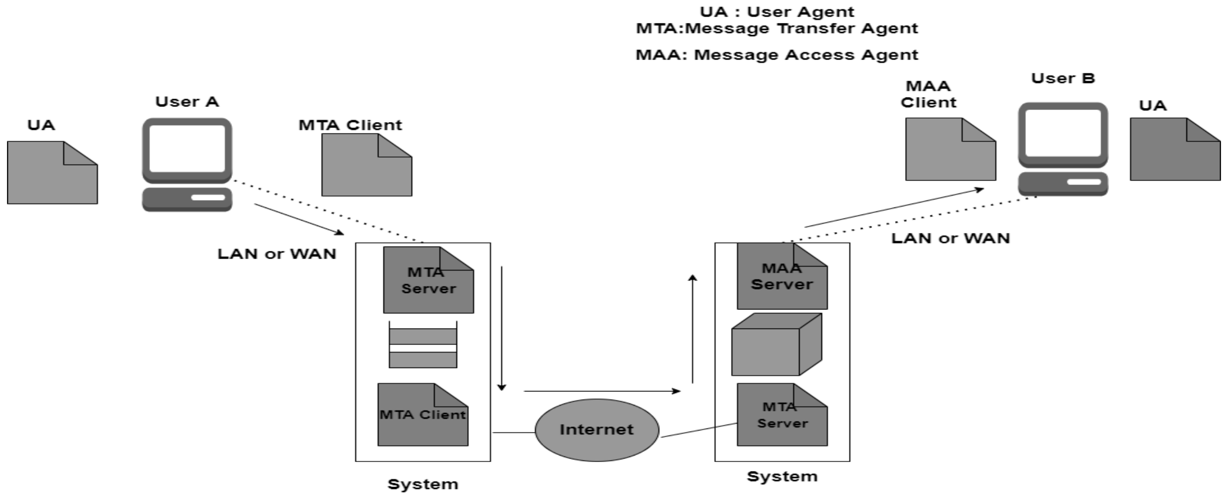
Fourth Scenario

In this scenario, the receiver is also connected to his mail server with the help of WAN or LAN.

When the message arrives the receiver needs to retrieve the message; thus there is a need for another set of client/server agents. The recipient makes use of MAA(Message access agent) client in order to retrieve the message.

In this, the client sends the request to the Mail Access agent(MAA) server and then makes a request for the transfer of messages.

This scenario is most commonly used today.



Structure of Email

The message mainly consists of two parts:

1.Header

2.Body

Header

The header part of the email generally contains the sender's address as well as the receiver's address and the subject of the message.

Body

The Body of the message contains the actual information that is meant for the receiver.

Email Address

In order to deliver the email, the mail handling system must make use of an addressing system with unique addresses.

The address consists of two parts:

- Local part
- Domain Name

Local Part

It is used to define the name of the special file, which is commonly called a user mailbox; it is the place where all the mails received for the user is stored for retrieval by the Message Access Agent.

Domain Name

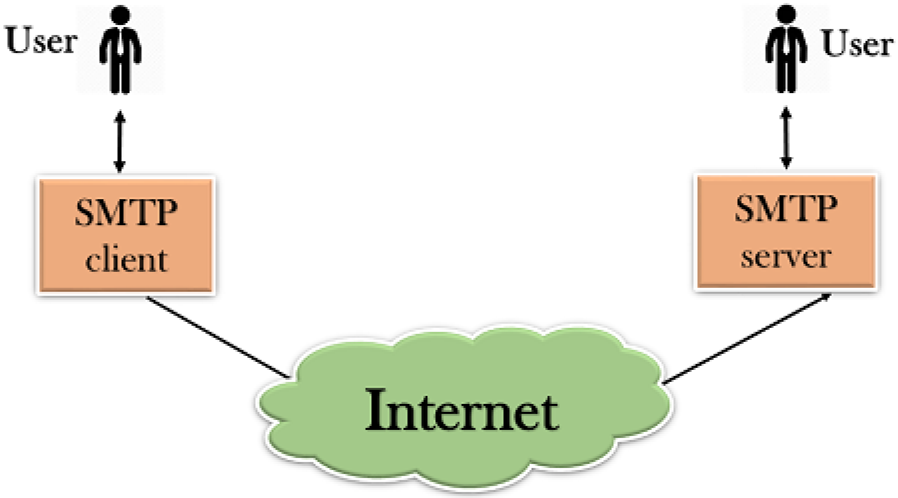
It is the second part of the address is Domain Name.

Both local part and domain name are separated with the help of @.

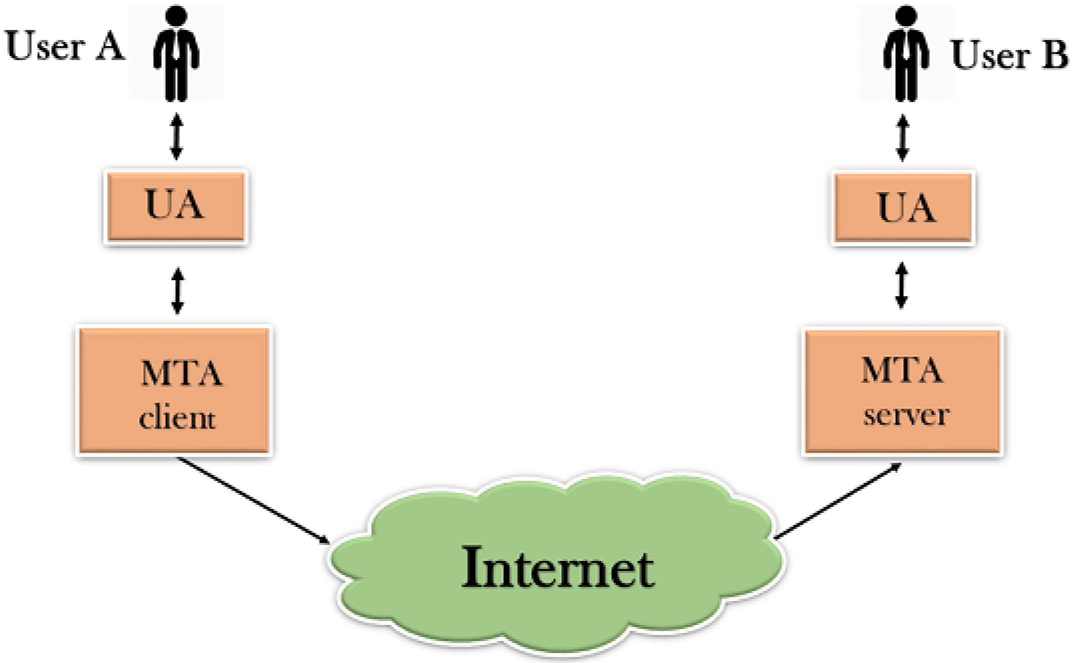
SMTP

- 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.

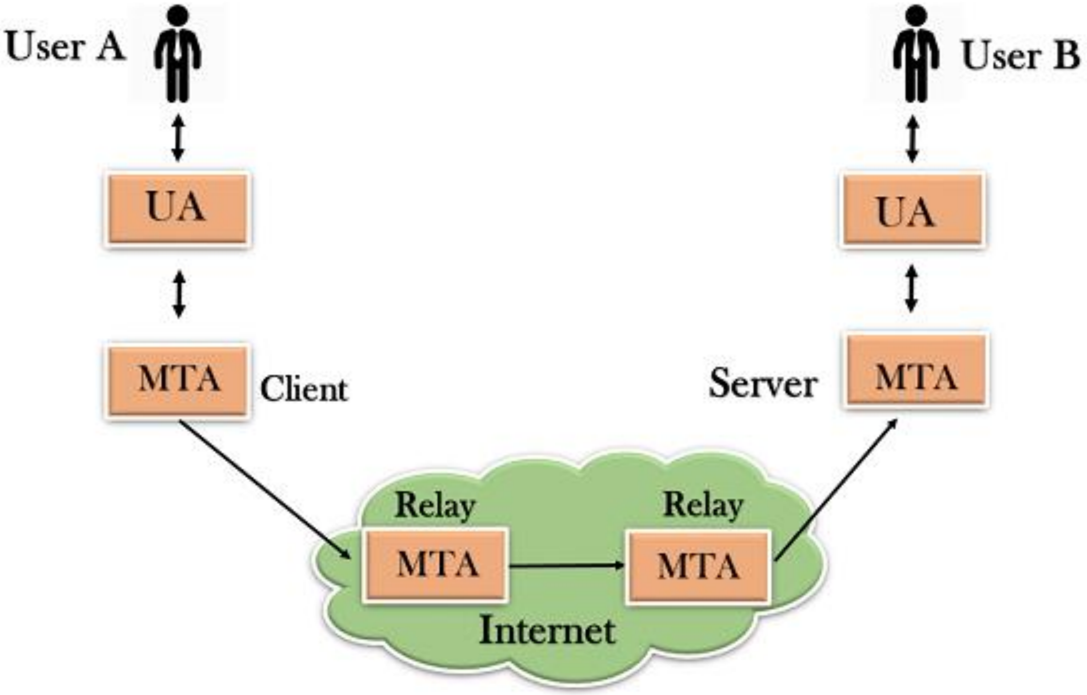
Components of SMTP



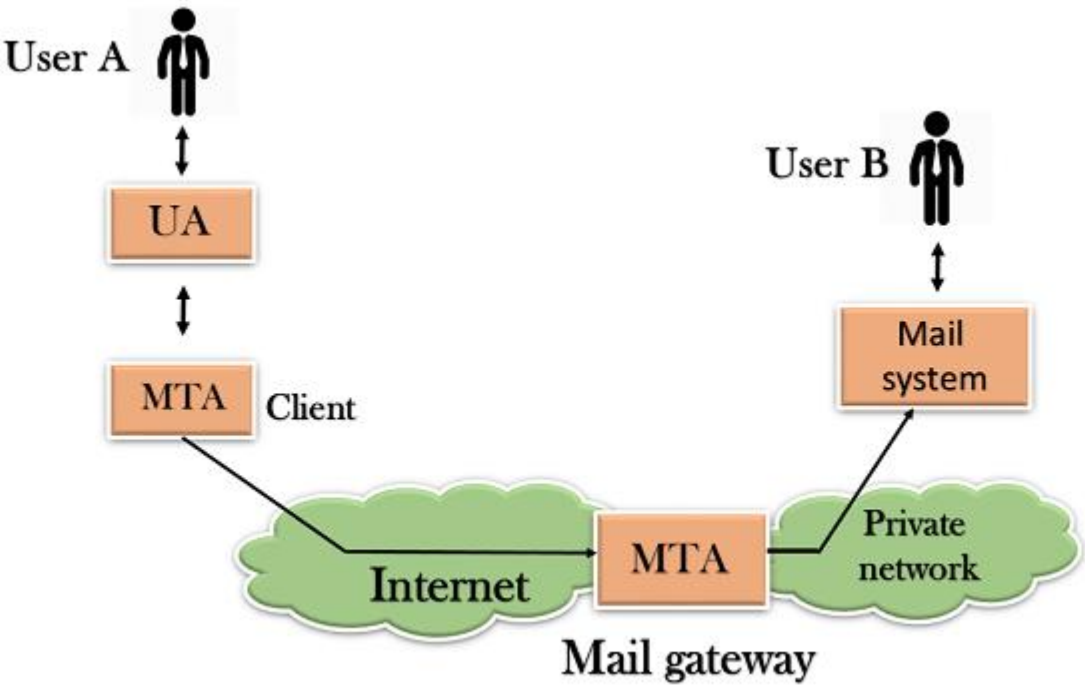
- First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.



- 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.



Working of SMTP

1. **Composition of Mail:** A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.
2. **Submission of Mail:** After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.
3. **Delivery of Mail:** E-mail addresses contain two parts: username of the recipient and domain name. For example, vivek@gmail.com, where "vivek" is the username of the recipient and "gmail.com" is the domain name.

   If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain. The MX record contains the domain name and IP address of the recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message.

4. **Receipt and Processing of Mail:** Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.
5. **Access and Retrieval of Mail:** The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

Advantages of SMTP

- If necessary, the users can have a dedicated server.
- It allows for bulk mailing.
- Low cost and wide coverage area.
- Offer choices for email tracking.
- Reliable and prompt email delivery.

Disadvantages of SMTP

- SMTP's common port can be blocked by several firewalls.
- SMTP security is a bigger problem.
- Its simplicity restricts how useful it can be.
- Just 7-bit ASCII characters can be used.
- If a message is longer than a certain length, SMTP servers may reject the entire message.

POP

- POP stands for **Point of Presence** (also known as **Post Office Protocol**).
- It is a point where many devices share a connection and can communicate with each other.
- We can say that it is a man-made demarcation point (a point where the public network of a company ends and the private network of the customer begins for eg. the point at which your broadband cable enters the house) between communicating entities.
- It basically consists of high-speed telecommunications equipment and technologies that help in bringing together people from all over the internet.
- An example of this would be the local access point that connects customers via their internet service provider (ISP) to the rest of the world. The size of an ISP can be calculated by seeing the number of POPs that the service provider has. The normal houses routers, modems, servers, switches, and other such devices that have to share data over networks all use POPs. Internet Service Providers have multiple POPs.

Characteristics of POP :

- Post Office Protocol is an open protocol, defined by Internet RFCs.
- It allows access to new mail from a spread of client platform types.
- It supports download and delete functions even when offline.
- It requires no mail gateways due to its native nature.

- POP can handle email access only while the emails are sent by SMTP.
- RFC 918 got published in 1984 which defined the Post Office Protocol (POP). The explanation of why POP came in the picture was to supply a neater way for a client computer to retrieve e-mail on an SMTP (Simple Mail Transfer Protocol) server so that it can be used locally. POP Version 2 got published in 1985.
- It improvised the capabilities of POP by defining a far impressive set of commands further as replies. RFC 1939 was published in 1996 and POP3 has not been improvised since that point.

Examples:

- **Carrier hotels :**
  These buildings are extremely secure with size averaging around 54, 000 square feet. These hotels offer hardware and software installation, updation and several other services.

- **Meet-me rooms :**
  Meet-Me Rooms (MMRs) are small space inside carrier hotels, averaging around 5, 000 square feet. These small rooms house interconnects networking equipment owned by many telecommunication companies.

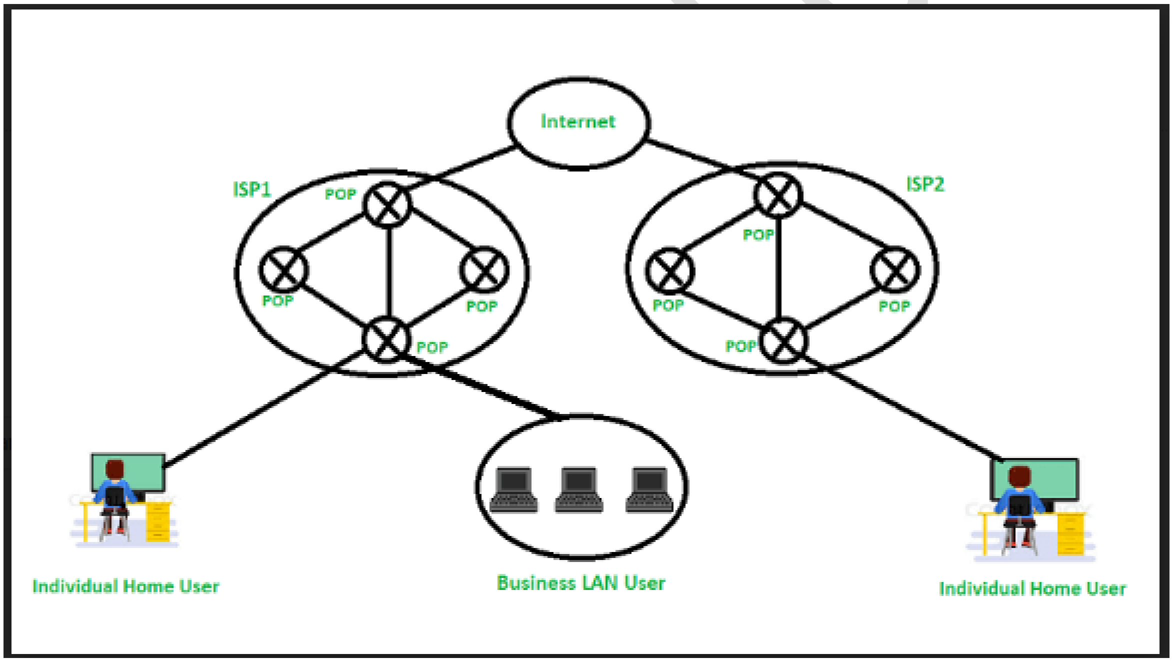


Figure – Post Office Protocol (POP)

Working:

1. **Base stations** – A central point of reference to an access point and bandwidth management to ensure evenly distribution of the connection speed of the customer.
2. **Client equipment** – utilized by customers to link with the base stations
3. **Network switches** – Used for proper distribution
4. **Routers** – Provides multiple paths for the data to be shared in the network
5. **Firewall** – Used for securing the network from threats (internal and external)

Advantages:

- The latest version of **Post Office Protocol (POP3)** is the most widely used protocol and is being supported by most email clients.
- It provides a convenient and standard way for users to access mailboxes and download messages.

POP3 has two modes:

- In **Delete mode**, the mail is deleted from the mailbox after each retrieval, in the keep mode, the mail remains in the mailbox after retrieval . The Delete mode is normally used when the user is working on a permanent computer and can save and organize the received mail after reading or replying.
- The **keep mode** is normally used when the user accesses mail away from the primary computer(eg, laptop). The mail is read but kept in the system for later retrieval and organization.

- The creation of the latest messages is impossible without being logged onto the web
- All messages get stored on the disc drive of your computer
- Easy to use and configure.
- As the attachments are already on your PC, opening them may be a quicker process
- There isn't any maximum size on your mailbox, except as determined by the scale of your disc drive

Disadvantages:

- Consumes large memory as all the messages are stored on the disc drive
- Opening attachments may be a fast process unless the attachment contains a virus
- Since all attachments get downloaded on your computer, there's a danger of a virus attack if they're not scanned by antivirus software
- as these scans are only 60% effective
- Emails cannot be opened by other machines unless they are configured to do so.
- Email folders can become corrupted and might even drift.
- It is not easy to export a local mail folder to another physical machine or another mail client.

IMAP

- **Internet Message Access Protocol** (IMAP) is an application layer protocol that operates as a contract for receiving emails from the mail server.
- It was designed by Mark Crispin in 1986 as a remote access mailbox protocol, the current version of IMAP is IMAP4.
- It is used as the most commonly used protocol for retrieving emails. This term is also known as Internet mail access protocol, Interactive mail access protocol, and Interim mail access protocol.

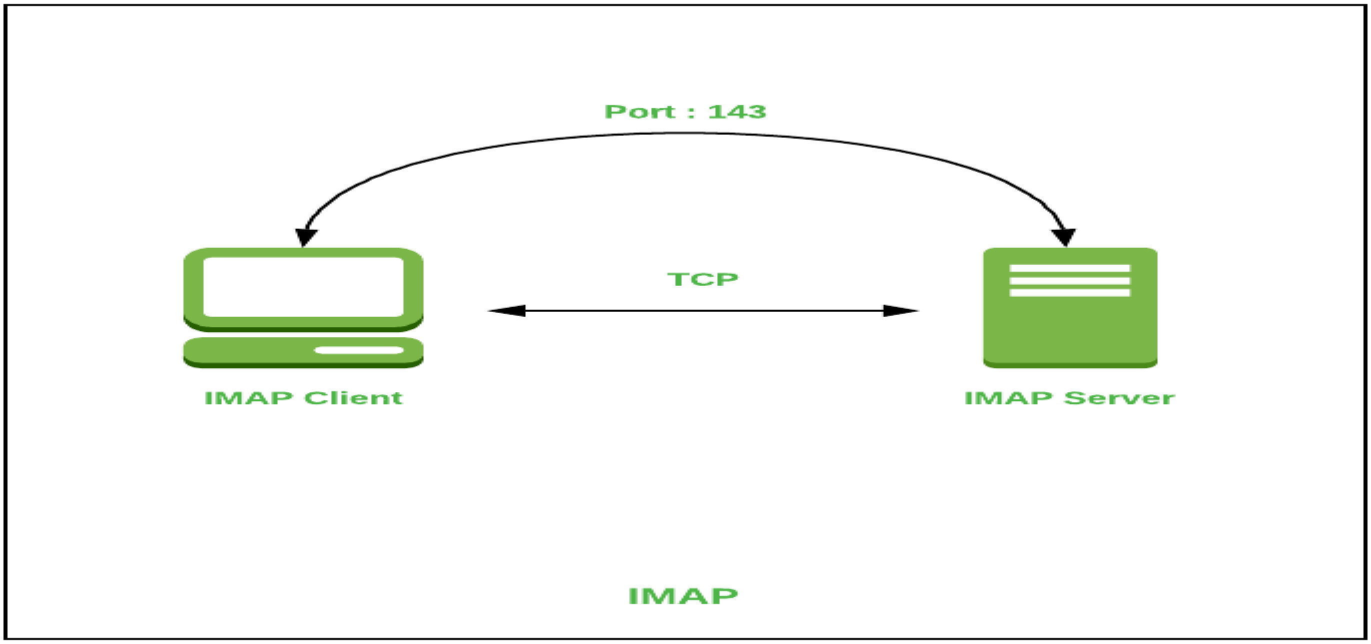
Features of IMAP :

- It is capable of managing multiple mailboxes and organizing them into various categories.
- Provides adding of message flags to keep track of which messages are being seen.
- It is capable of deciding whether to retrieve email from a mail server before downloading.
- It makes it easy to download media when multiple files are attached.

Working of IMAP :

- It is a combination of client and server process running on other computers that are connected through a network.
- This protocol resides over the TCP/IP protocol for communication.
- Once the communication is set up the server listens on port 143 by default which is non-encrypted.
- For the secure encrypted communication port, 993 is used.
- MAP follows Client-server Architecture and is the most commonly used email protocol.

Architecture of IMAP:



Advantages :

- It offers synchronization across all the maintained sessions by the user.
- It provides security over POP3 protocol as the email only exists on the IMAP server.
- Users have remote access to all the contents.
- It offers easy migration between the devices as it is synchronized by a centralized server.
- There is no need to physically allocate any storage to save contents.

Disadvantages :

- IMAP is complex to maintain.
- Emails of the user are only available when there is an internet connection.
- It is slower to load messages.
- Some emails don’t support IMAP which makes it difficult to manage.
- Many browser-based solutions are unavailable due to not support of IMAP.

- **Difference between POP3 and IMAP**

Key	POP3	IMAP
Full Form	POP3 stands for Post Office Protocol 3	IMAP stands for Internet Message Access Protocol.
Complexity	POP3 is simple and only mails can be downloaded from your inbox to local computer.	IMAP is complex and allows to see all the folders on the mail server.
Ports	POP3 listens on 110 and POP with SSL, POP3DS listens on 995 port.	IMAP listens on 143 and IMAP with SSL, IMAPDS listens on 993 port
Multiaccess	POP3 supports single device to access the mail at a time.	IMAP supports multiple devices which can access the mail at a time.
Download	In POP3, mail to be downloaded first then can be read.	In IMAP, mail can be partially read before complete download.
Mail Organize	Mails cannot be organized on mail server using POP3.	IMAP allows to organize mails on mail server.
Update Email	Mails cannot be created/updated/deleted on mail server using POP3.	IMAP allows to create/update/delete mails on mail server.
Search Content	Mail content cannot be searched on mail server using POP3. To search, mail to be downloaded first.	Mail content can be searched on mail server using IMAP.
Download	All message are downloaded at once.	Mail message header can be previewed before a message is

Key	POP3	IMAP
		to be downloaded.
Change	Using local email software, a mail can be updated.	A mail can be updated via a web interface or email software.

MIME

- MIME stands for **Multipurpose Internet Mail Extensions**.
- It is used to extend the capabilities of Internet e-mail protocols such as SMTP.
- The MIME protocol allows the users to exchange various types of digital content such as pictures, audio, video, and various types of documents and files in the e-mail.
- MIME was created in 1991 by a computer scientist named Nathan Borenstein at a company called Bell Communications.

Need of MIME Protocol

MIME protocol is used to transfer e-mail in the computer network for the following reasons:

1. The MIME protocol supports multiple languages in e-mail, such as Hindi, French, Japanese, Chinese, etc.
2. Simple protocols can reject mail that exceeds a certain size, but there is no word limit in MIME.
3. Images, audio, and video cannot be sent using simple e-mail protocols such as SMTP. These require MIME protocol.
4. Many times, emails are designed using code such as HTML and CSS, they are mainly used by companies for marketing their product. This type of code uses MIME to send email created from HTML and CSS.

MIME Header

MIME adds five additional fields to the header portion of the actual e-mail to extend the properties of the simple email protocol. These fields are as follows:

1. MIME Version
2. Content Type
3. Content Type Encoding
4. Content Id

5. Content description

1. MIME Version

It defines the version of the MIME protocol. This header usually has a parameter value 1.0, indicating that the message is formatted using MIME.

2. Content Type

It describes the type and subtype of information to be sent in the message. These messages can be of many types such as Text, Image, Audio, Video, and they also have many subtypes such that the subtype of the image can be png or jpeg. Similarly, the subtype of Video can be WEBM, MP4 etc.

3. Content Type Encoding

In this field, it is told which method has been used to convert mail information into ASCII or Binary number, such as 7-bit encoding, 8-bit encoding, etc.

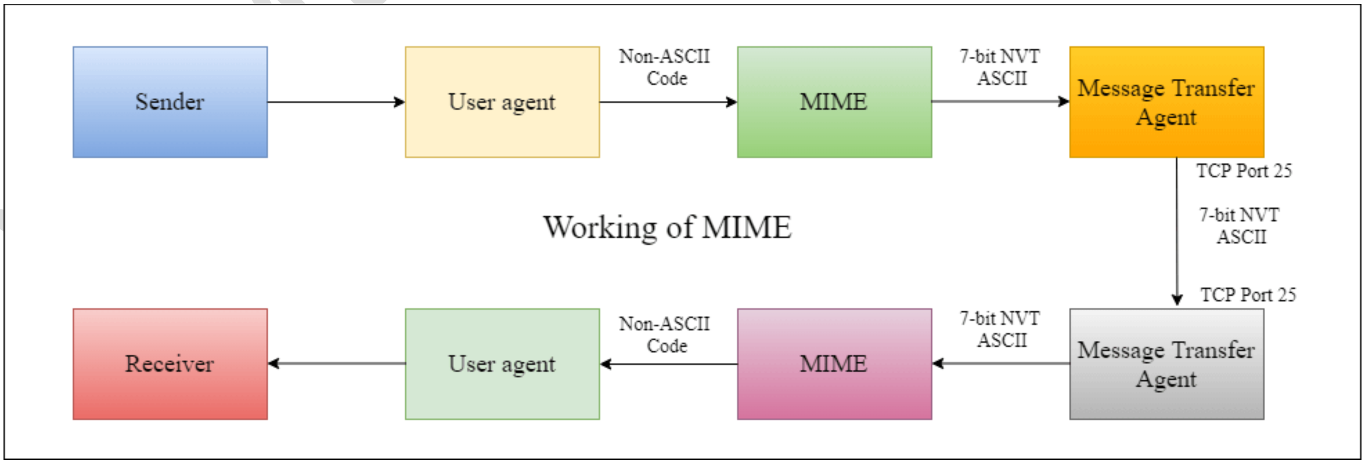
4. Content Id

In this field, a unique "Content Id" number is appended to all email messages so that they can be uniquely identified.

5. Content description

This field contains a brief description of the content within the email. This means that information about whatever is being sent in the mail is clearly in the "Content Description". This field also provides the information of name, creation date, and modification date of the file.

Working diagram of MIME Protocol



Features of MIME Protocol

1. It supports multiple attachments in a single e-mail.
2. It supports the non-ASCII characters.
3. It supports unlimited e-mail length.
4. It supports multiple languages.

Advantage of the MIME

The MIME protocol has the following advantages:

1. It is capable of sending various types of files in a message, such as text, audio, video files.
2. It also provides the facility to send and receive emails in different languages like Hindi, French, Japanese, Chinese etc.
3. It also provides the facility of connecting HTML and CSS to email, due to which people can design email as per their requirement and make it attractive and beautiful.
4. It is capable of sending the information contained in an email regardless of its length.
5. It assigns a unique id to all e-mails.

Web-Based Mail

- Webmail is a cloud-based service or Web-based email system that allows you to access and use your email from almost anywhere through an internet connection.
- Unlike Thunderbird or Microsoft Outlook, it does not need software installation.
- It is a kind of service, which is provided by certain companies and ISPs (Internet service providers).

Some popular webmail services

In modern times, many webmail services are available for users, which are not software-based. Below, a list contains some the free webmail services.

- **Gmail:** Gmail is a type of Webmail, a free Web-based e-mail service that allows users a gigabyte of storage for messages or other data.
- **Yahoo! Mail:** It is a web and cloud-based messaging solution that is launched by the American company Yahoo! on 8 October 1997.
- **com:** It is a free web-based e-mail service that allows you to send and receive e-mail on your computer.

Advantages of Webmail

1. Convenience

One of the most important advantages of webmail is convenience, which is beneficial at the time when you travel frequently and work from remote locations.

2. Cost

Usually, big providers provide basic webmail services free of cost. Also, some premium services are also offered by some providers.

3. Retain Your Address

Another benefit of webmail is that you do not need to change your old email address, even if you have changed Internet providers.

4. Large Storage

One of the biggest advantages of webmail is storage capacity.

Disadvantages of Webmail

1. Personal Name

You may be unable to create an address on webmail using the name you had in mind or your own name as it has a large customer base.

2. Ads

From advertisers, webmail providers have to get their revenue as you are using the service for free of cost.

3. More Spam

Because of spammers' large customer base, they tend to target webmail services more as compared to traditional providers

4. No Offline Working

Although broadband becomes more appropriate in terms of reliability, both are required to connect your device with the network to write, send messages, and as well as review messages.

Email Security:

- Basically**, Email security** refers to the steps where we protect the email messages and the information that they contain from unauthorized access, and damage.

- It involves ensuring the confidentiality, integrity, and availability of email messages, as well as safeguarding against phishing attacks, spam, viruses, and another form of malware.
- It can be achieved through a combination of technical and non-technical measures

Email Security Policies

An email security policy should include the following essential components:

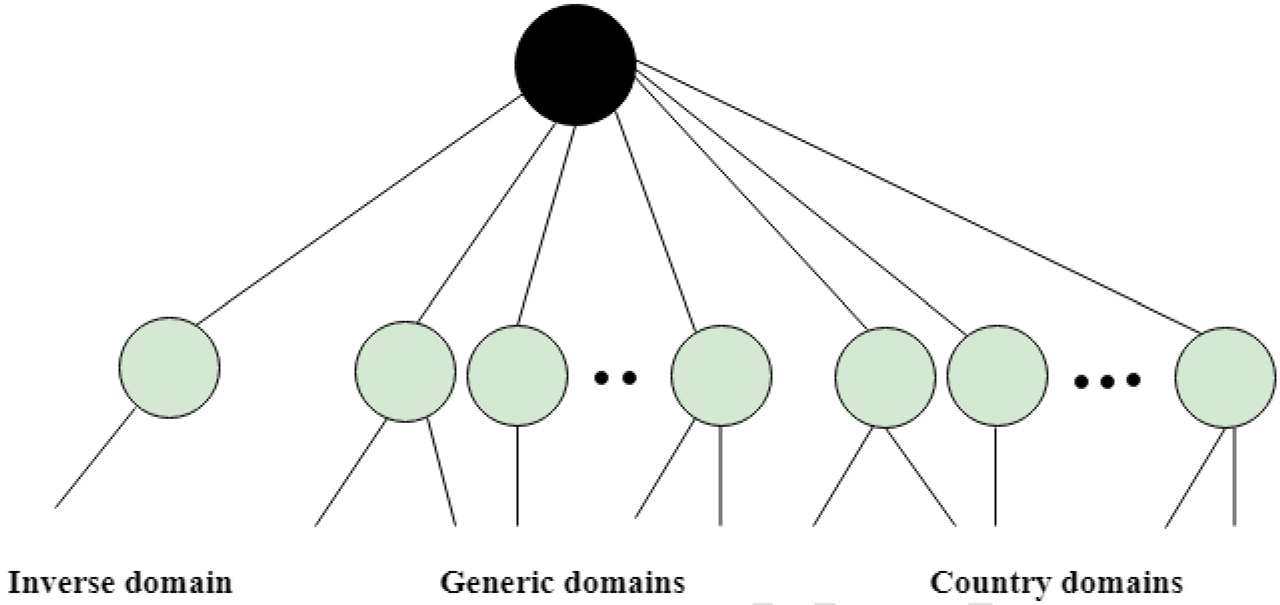
- **Appropriate Use:** The policy should outline what comprises acceptable email usage inside the organization, including who is permitted to use email, how to use it, and for what purpose email we have to use.
- **Password and Authentication:** The policy should require strong passwords and two-factor authentication to ensure that only authorized users can access email accounts.
- **Encryption**: To avoid unwanted access, the policy should mandate that sensitive material be encrypted before being sent through email.
- **Virus Protection: T**he policy shall outline the period and timing of email messages and attachment collection.
- **Retention and Detection**: The policy should outline how long email messages and their attachments ought to be kept available, as well as when they should continue to be removed.

5.5 Domain Name System

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for **Domain Name System.**
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

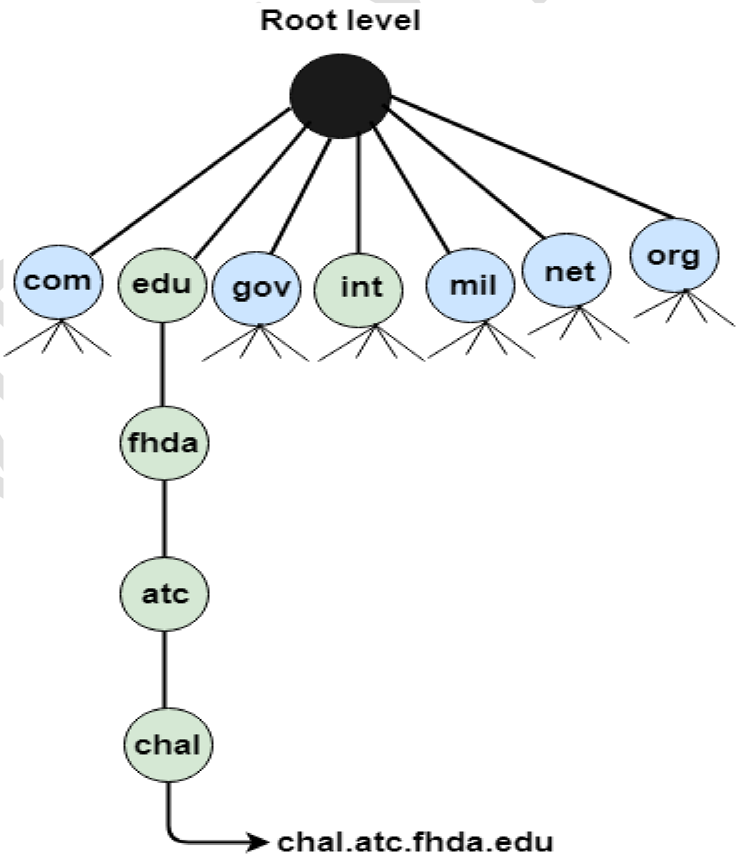


Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers

int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations



Country Domain

- The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

- The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. Server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

DNS Resource Records

There are several different types of DNS records, including −

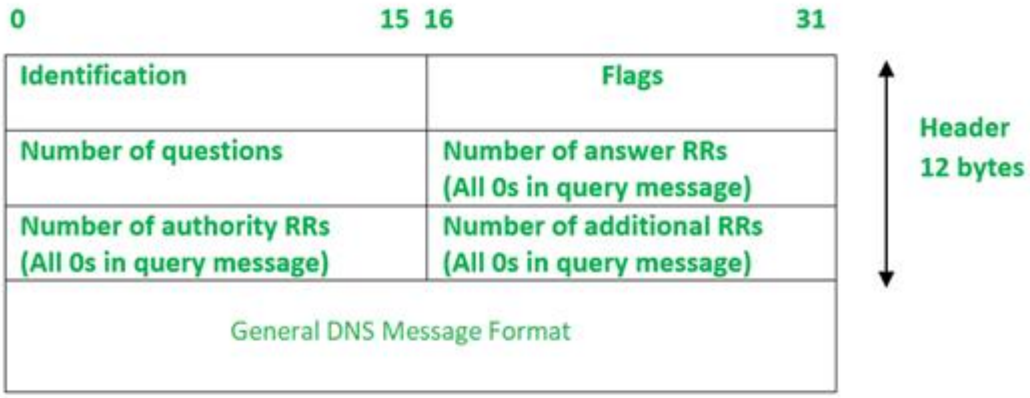
- **A record (Address Record)** − maps a domain or sub domain to an IP address.
- **MX record (Mail Exchange Record)** − routes email for a domain to the correct email server.
- **CNAME record (Canonical Name Record)** − creates an alias for a domain.
- **TXT record (Text Record)** − stores arbitrary text in a domain's DNS record.
- **PTR record (Pointer Record)** − maps an IP address to a domain name.
- **NS record (Name Server Record)** − specifies the name servers for a domain.
- **SOA record (Start of Authority Record)** − specifies the DNS server that is the authority for a specific domain.

- **SRV record (Service Record)** – specifies the hostname and port number for a specific service, such as a website or email server.
- **AAAA record (Quad-A Record)** – maps a domain or subdomain to an IPv6 address.
- **CAA record (Certification Authority Authorization Record)** – specifies which certificate authorities (CAs) are authorized to issue SSL/TLS certificates for a domain.

DNS message format

The response message consists of five sections:

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

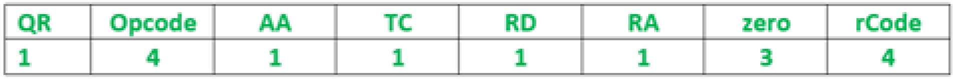


0 15	16 31
Identification	Flags
Number of questions	Number of answer RRs (All 0s in query message)
Number of authority RRs (All 0s in query message)	Number of additional RRs (All 0s in query message)

General DNS Message Format

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 :



QR	Opcode	AA	TC	RD	RA	zero	rCode
1	4	1	1	1	1	3	4

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 non execution 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 RRs-** 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 RRs**– 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.

DDNS

- The Domain Name Service (DNS) maps hostnames to IP addresses. Dynamic DNS (DDNS) services automatically update their records as IP addresses change to ensure that clients requesting the record for a hostname always receive the correct IP address.

Security of DNS

- DNS Security Extensions (DNSSEC) is a security protocol created to mitigate this problem. DNSSEC protects against attacks by digitally signing data to help ensure its validity. In order to ensure a secure lookup, the signing must happen at every level in the DNS lookup process

Types of Attacks:

1. **Denial of service (DoS):** An attack where the attacker renders a computer useless (inaccessible) to the user by making a resource unavailable or by flooding the system with traffic.
2. **Distributed denial of service (DDoS):** The attacker controls an overwhelming amount of computers (hundreds or thousands) in order to spread malware and flood the victim's computer with unnecessary and overloading traffic
3. **DNS spoofing (also known as DNS cache poisoning):** An attacker will drive the traffic away from real DNS servers and redirect them to a "pirate" server, unbeknownst to the users.
4. **Fast flux:** An attacker will typically spoof his IP address while performing an attack.
5. **Reflected attacks:** Attackers will send thousands of queries while spoofing their own IP address and using the victim's source address.
6. **Reflective amplification DoS:** When the size of the answer is considerably larger than the query itself