

Domain Name System

- ✓ Domain Name System is an Internet service that translates domain names into IP addresses.
- ✓ The DNS has a distributed database that resides on multiple machines on the Internet.
- ✓ DNS has some protocols that allow the client and servers to communicate with each other.

Name space

- ✓ The names assigned to the machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses.
- ✓ There are two types of name spaces: Flat name spaces and Hierarchical names.

Flat name spaces

- ✓ In a flat name space, a name is a sequence of characters without structure.
- ✓ A name in this space is assigned to an address.
- ✓ The names were convenient and short.
- ✓ A flat name space cannot be used in a large system such as the internet because it must be centrally controlled to avoid ambiguity and duplication.

Hierarchical Name Space

- ✓ In hierarchical name space, each name consists of several parts.
- ✓ First part defines the nature of the organization, second part defines the name of an organization, third part defines department of the organization, and so on.
- ✓ In hierarchical name space, the authority to assign and control the name spaces can be decentralized.
- ✓ Authority for names in each partition is passed to each designated agent.

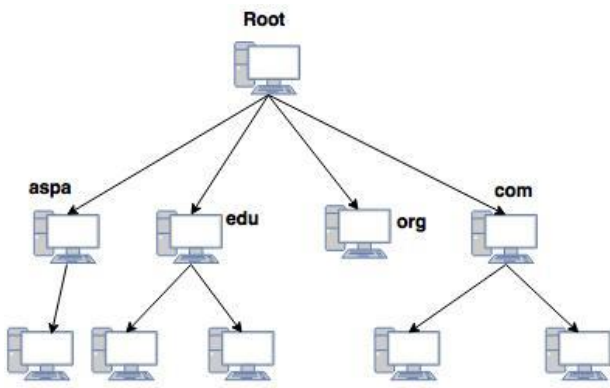
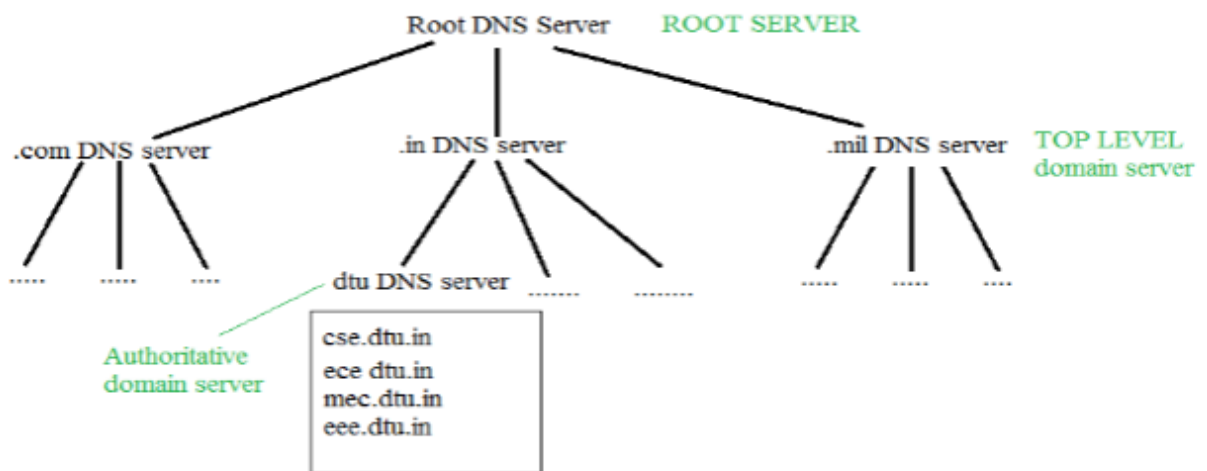


Fig: Hierarchy of DNS

DNS in the Internet

- DNS is a protocol that can be used in different platform.
- Domain Name Space is divided into different sections in the Internet: Generic domain, country domain and inverse domain.



1) Generic Domains

The generic domains define registered hosts according to their generic behavior.

2) Country Domains

- ✓ Country domain uses two character country abbreviations.

- ✓ Second labels can be more specific, national designation.
- ✓ **For example**, for Australia the country domain is “au”, Inida is .in, UK is .uk etc.

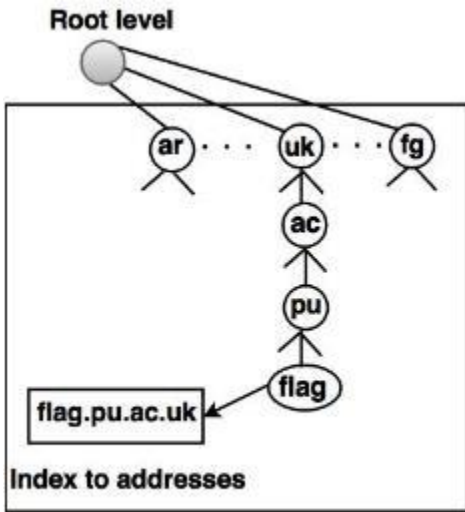


Fig: Country domains

3) Inverse Domains

- Inverse domain is used to map an address to a name.
- **For example**, a client send a request to the server for performing a particular task, server finds a list of authorized client. The list contains only IP addresses of the client.
- The server sends a query to the DNS server to map an address to a name to determine if the client is on the authorized list.
- This query is called an inverse query.
- This query is handled by first level node called arpa.

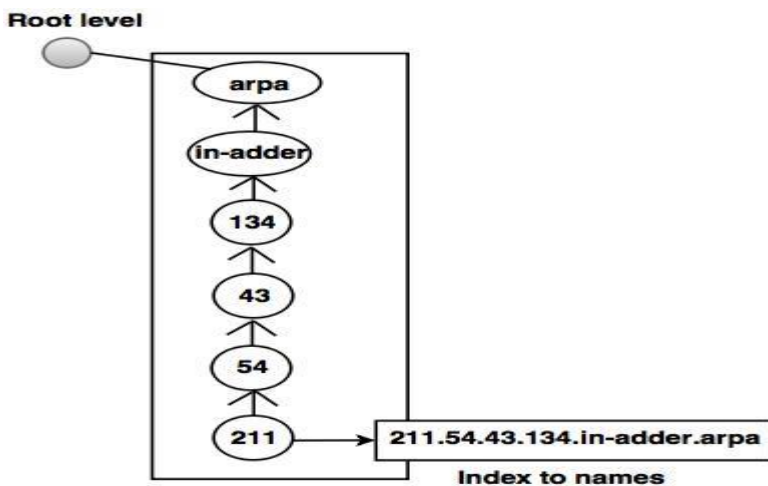


Fig. Inverse domain

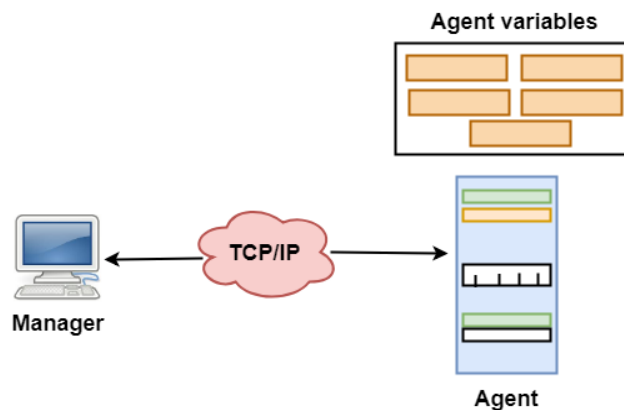
Simple Network Management Protocol (SNMP)

If an organization has 1000 of devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

Simple Network Management Protocol (SNMP) -

1. SNMP stands for **Simple Network Management Protocol**.
2. SNMP is an application layer protocol which uses UDP (**Connectionless**) port number 161/162
3. SNMP is a framework used for managing devices on the internet.
4. It provides a set of operations for monitoring and managing the internet.

SNMP Concept



- SNMP has two components Manager and agent MIB.
- The manager is a host that controls and monitors a set of agents such as routers.
- It is an application layer protocol in which a few manager stations can handle a set of agents.
- It is used in a heterogeneous (Different) network made of different LANs and WANs connected by routers or gateways.

SNMP components -

There are 3 components of SNMP:

1. SNMP Manager -

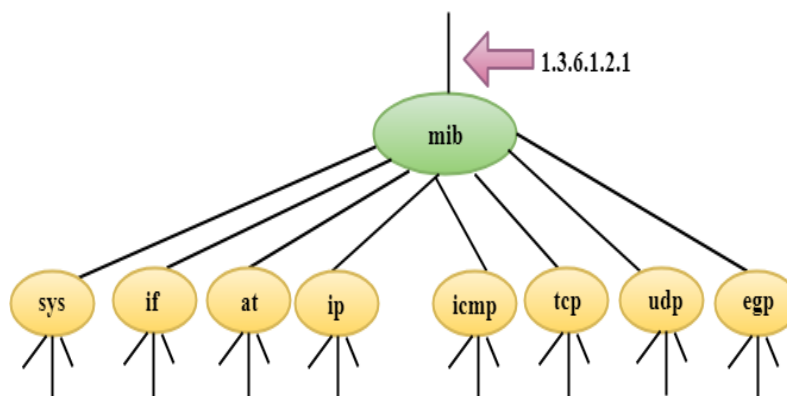
It is a centralised system used to monitor network. It is also known as Network Management Station (NMS)

2. SNMP agent -

It is a software management software module installed on a managed device. Managed devices can be network devices like router, switches, servers etc.

3. Management Information Base -

MIB consists of information of resources that are to be managed. These information is organised hierarchically. It consists of objects instances which are essentially variables.



SNMP messages -

Different variables are:

1. GetRequest -

SNMP manager sends this message to request data from SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.

2. GetNextRequest -

This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continuously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.

3. GetBulkRequest -

This message is used to retrieve large data at once by the SNMP manager from SNMP agent.

4. SetRequest -

It is used by SNMP manager to set the value of an object instance on the SNMP agent.

5. Response -

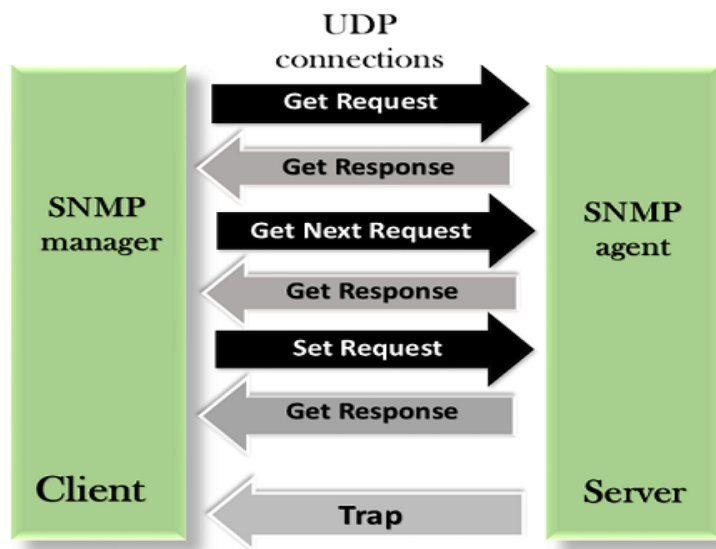
It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.

6. Trap -

These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.

7. InformRequest -

It was introduced in SNMPv2, used to identify if the trap message has been received by the manager or not.



SNMP security levels -

It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3.

There are 3 security levels namely:

1. noAuthNoPriv-

This (no authentication, no privacy) security level uses community string for no authentication and no encryption for privacy.

2. authNopriv -

This security level (authentication, no privacy) uses HMAC (Hashing for Message Authentication code) with Md5 (Message Digest Algorithm 5) for authentication and no encryption is used for privacy.

3. authPriv -

This security level (authentication, privacy) uses HMAC with Md5 or SHA (Secure Hash Algorithm) for authentication and encryption uses DES-56(Data Encryption Standard) algorithm.

SNMP versions -

There are 3 versions of SNMP:

1. SNMPv1 -

It uses community strings for authentication and use UDP only.

2. SNMPv2-

It uses community strings for authentication. It uses UDP but can be configured to use TCP.

3. SNMPv3 -

It uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, conclusion is the higher the version of SNMP, more secure it will be.

Electronic Mail

Electronic Mail (e-mail) is one of most widely used services of [Internet](#). This service allows an Internet user to send a **message in formatted manner (mail)** to the other Internet user in any part of world.

Components of E-Mail System :

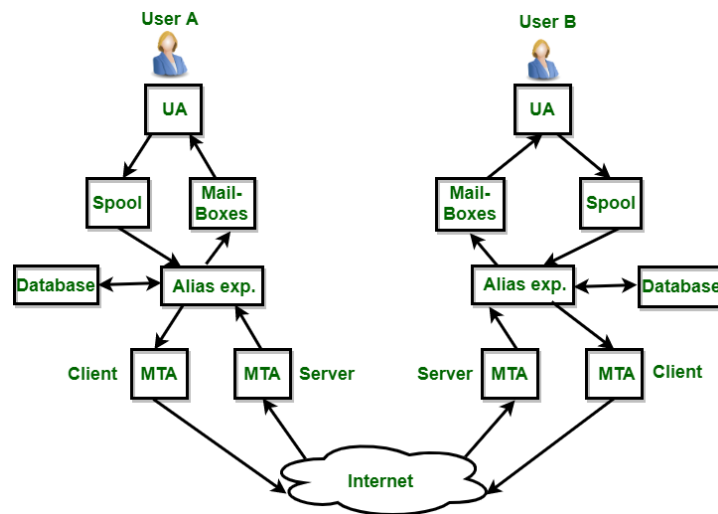
The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. User Agent (UA) :

The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.

2. Message Transfer Agent (MTA) :

MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by [Simple Mail Transfer Protocol](#).



1. Mailbox :

It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.

2. Spool file :

This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an **alias**, to represent several different e-mail addresses. It is known as **mailing list**, Whenever user have to sent a message, system checks recipients's name

against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

Services provided by E-mail system:

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

E-Mail Format

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

Format of E-mail :

An e-mail consists of three parts that are as follows :

1. Envelope
2. Header
3. Body

These are explained as following below.

1. Envelope :

The envelope part encapsulates the message. It contains all information that is required for sending any e-mail such as destination address, priority and security level. The envelope is used by MTAs for routing message.

2. Header :

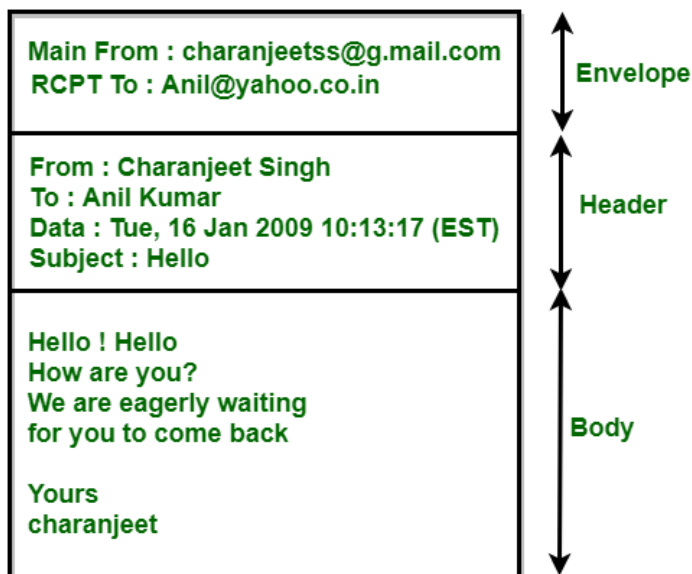
The header consists of a series of lines. Each header field consists of a single line of ASCII text specifying field name, colon and value. The main header fields related to message transport are :

1. **To:** It specifies the DNS address of the primary recipient(s).
2. **Cc :** It refers to carbon copy. It specifies address of secondary recipient(s).

3. **BCC:** It refers to blind carbon copy. It is very similar to Cc. The only difference between Cc and Bcc is that it allow user to send copy to the third party without primary and secondary recipient knowing about this.
4. **From :** It specifies name of person who wrote message.
5. **Sender :** It specifies e-mail address of person who has sent message.
6. **Received :** It refers to identity of sender's, data and also time message was received. It also contains the information which is used to find bugs in routing system.
7. **Return-Path:** It is added by the message transfer agent. This part is used to specify how to get back to the sender.

3. Body:- The body of a message contains text that is the actual content/message that needs to be sent, such as "Employees who are eligible for the new health care program should contact their supervisors by next Friday if they want to switch." The message body also may include signatures or automatically generated text that is inserted by the sender's email system.

The above-discussed field is represented in tabular form as follows :



Advantages and Disadvantages of E-mail

1. E-mails provides faster and easy mean of communication. One can send message to any person at any place of world by just clicking mouse.
2. Various folders and sub-folders can be created within inbox of mail, so it provide management of messages.
3. It is effective and cheap means of communication because single message can be send to multiple people at same time.
4. E-mails are very easy to filter. User according to his/her priority can prioritize e-mail by specifying subject of e-mail.
5. E-mail is not just only for textual message. One can send any kind of multimedia within mail.

Disadvantages of E-mail :

1. It is source of viruses. It is capable to harm one's computer and read out user's e-mail address book and send themselves to number of people around the world.
2. It can be source of various spams. These spam mails can fill up inbox and to deletion of these mail consumes lot of time.
3. It is informal method of communication. The documents those require signatures are not managed by e-mail.

Difference table between IMAP and POP3

Feature	IMAP	POP3
Stands for	IMAP stands for Internet Message Access Protocol.	It stands for Post Office Protocol 3.
Used for	IMAP is an advanced protocol that allows a user to check all the folders on the mail server and is used to retrieve the mails.	POP is a simple protocol compared to IMAP and used only for downloading the messages from our inbox to the local computer.
Port number	It listens on port number 143, and IMAPDS(IMAP with SSL) Listens on port 993.	It listens on port number 110, and POP3DS(POP3 with SSL) listens on port 995.
Accessibility	Using IMAP, the messages can be accessed using different devices.	Using POP3, mail can only be accessed using a single device at a time.
Readability	We can partially read the message before finishing the download.	We can only read the message once it is downloaded.
Change	In IMAP, a mail can be updated using email software or a web interface.	In POP3, mail can be updated using the local email software.
Update	IMAP allows the user to create, delete, or update the mailboxes on	POP3 does not allow the user to create, delete, or update the

	the mail server and also allows to create a hierarchy of mailboxes in the folder.	mailboxes on the mail server.
Mail organization	It allows the user to organize the mails on the server.	It does not allow to organize the mails on the server.
Download	In IMAP, the message header is previewed before downloading a message.	Using POP3, all the messages can be downloaded at once.
Email storage	Emails are stored on a single device once they are downloaded and removed from the server.	Emails are stored on the server and synced & can be accessed using multiple devices.

WEB

The **World Wide Web** abbreviated as WWW and commonly known as the web. The WWW was initiated by CERN (European laboratory for Nuclear Research) in 1989.

History:

It is a project created, by Timothy Berner's Lee in 1989, for researchers to work together effectively at CERN. is an organization, named World Wide Web Consortium (W3C), which was developed for further development in the web.

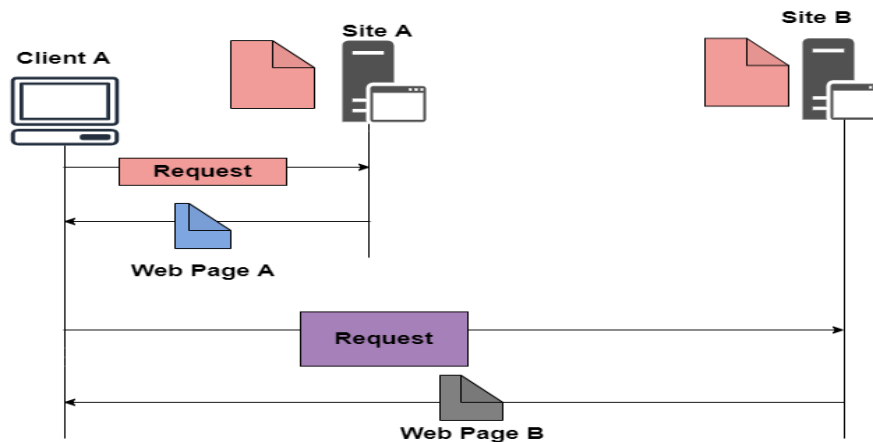
Components of Web: There are 3 components of web:

1. **Uniform Resource Locator (URL):** serves as system for resources on web.
2. **HyperText Transfer Protocol (HTTP):** specifies communication of browser and server.
3. **Hyper Text Markup Language (HTML):** defines structure, organisation and content of webpage.

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**.

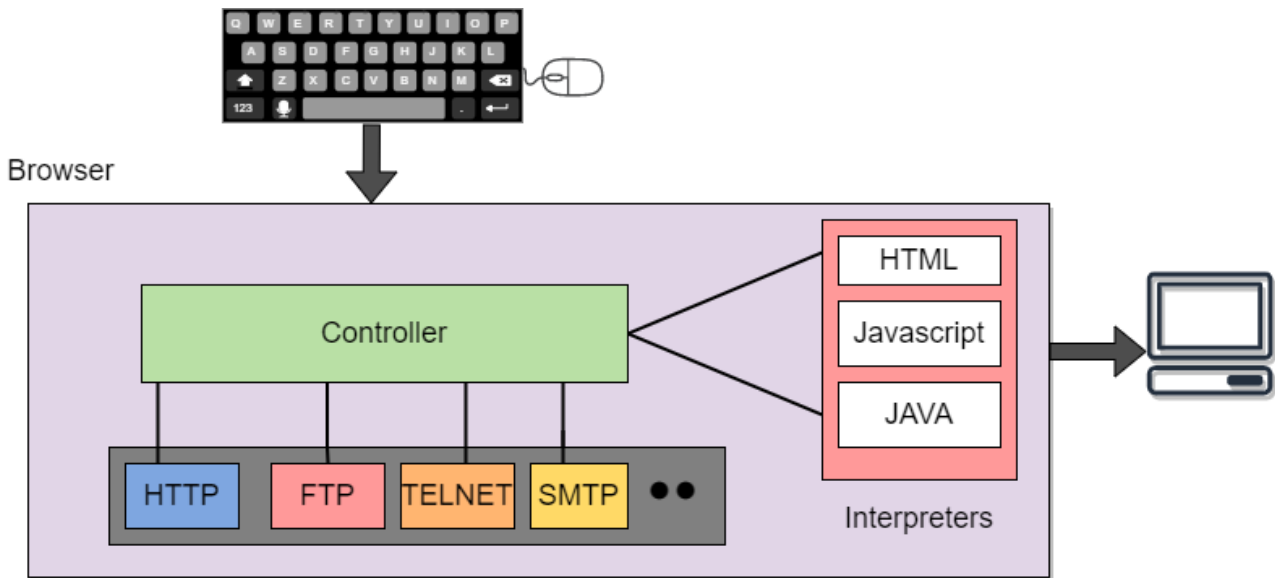
The reference generally contains the URL of site B. And the client is interested to take a look at this document too. Then after the client sends the request to the new site and then the new page is retrieved.

Now we will cover the components of WWW in detail.

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, 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

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

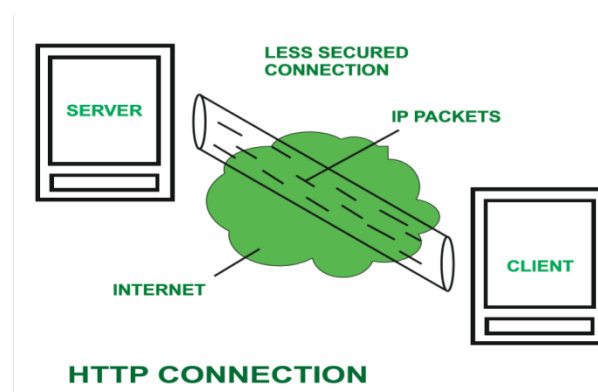
There are some drawbacks of the WWW and these are as follows;

- 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.

HTTP

- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.



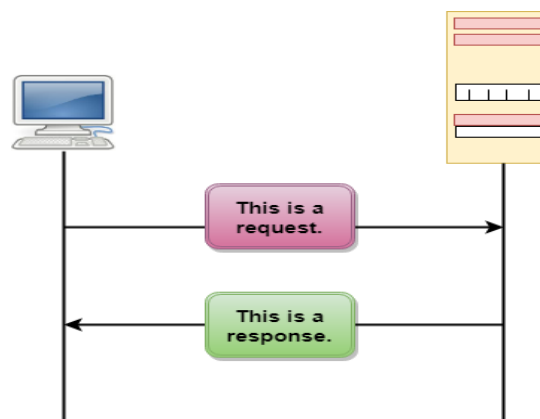
Features of HTTP:

- **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.

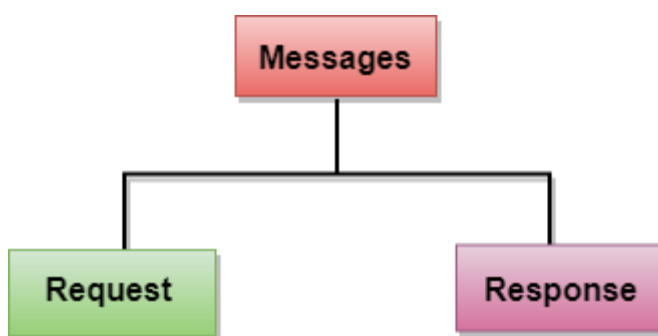
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

HTTP Transactions

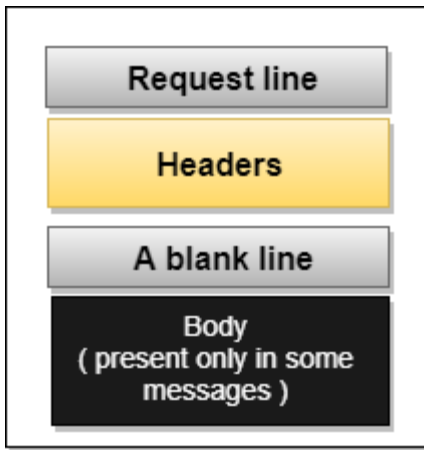


Messages

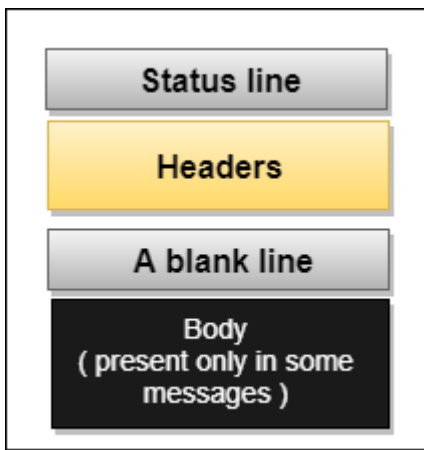
HTTP messages are of two types: request and response. Both the message types follow the same message format.



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.

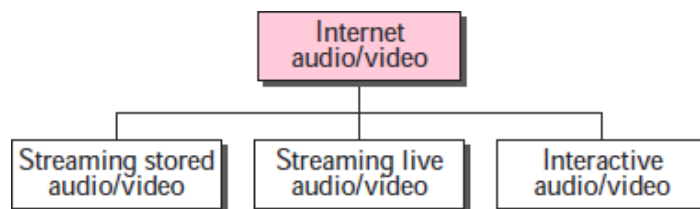


- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name 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.

Streaming audio and video

Streaming media is **video or audio content sent in compressed form over the Internet** and played immediately, rather than being saved to the hard drive.

We can divide audio and video services into three broad categories: **streaming stored audio/video**, **streaming live audio/video**, and **interactive audio/video**. Streaming means a user can listen (or watch) the file after the downloading has



started.

In the **first category**, streaming stored audio/video, **the files are compressed and stored on a server**. A client downloads the files through the Internet. This is sometimes referred to as **on-demand audio/video**.

In the **second category**, streaming live audio/video **refers to the broadcasting of radio and TV programs through the Internet**.

In the **third category**, interactive audio/video **refers to the use of the Internet for interactive audio/video applications**. A good example of this application is Internet telephony and Internet teleconferencing.

1. STREAMING STORED AUDIO/VIDEO

Downloading these types of files from a server can be different from downloading other types of files.

This is the class of application which allows the client to request for compressed audio or video files which are stored on the server. This application has three distinguishing factors follows:

I. **Stored Media:** The Multimedia content has been prerecorded and stored at the server. So , it is possible for the user to make following operations on the stored contents.

Pause

Rerwind

Fastworward

Index through

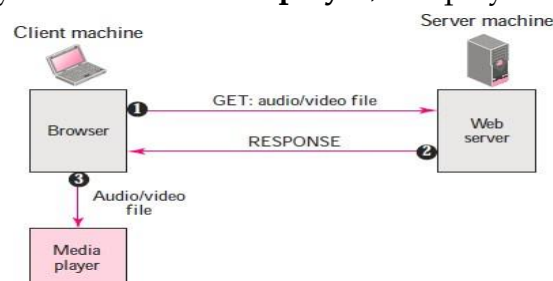
II. **Streaming:** In a streaming stored audio/video applications ,a client starts playout of the audio/video a few seconds after receiving the file from the server.

III. **Continuous playout:** Once the playout of the Multimedia content begins, it is necessary to proceed as per the original timings of recording. The requirement puts critical delay constraints on the data delivery.

Downloading these types of files from a server can be different from downloading other types of files.

First Approach: Using a Web Server

A compressed audio/video file can be downloaded as a text file. The **client (browser)** can use the services of **HTTP** and send a GET message to download the file. The **Web server** can send the compressed file to the browser. The browser can then use a help application, normally called a **media player**, to play the file. The file needs to

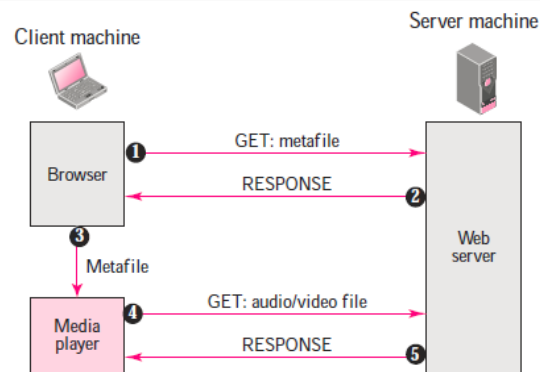


download completely before it can be played.

Second Approach: Using a Web Server with Metafile

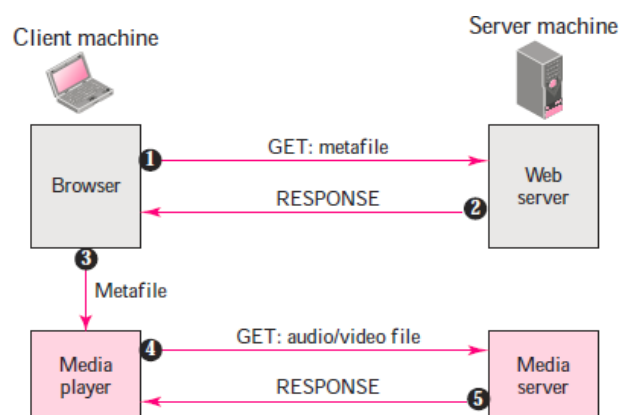
In another approach, the media player is directly connected to the Web server for downloading the audio/video file. The Web server stores two files: **the actual audio/video file** and a **metafile** that holds information about the audio/video file.

1. The HTTP client accesses the Web server using the GET message.
2. The information about the metafile comes in the response.
3. The metafile is passed to the media player.
4. The media player uses the URL in the metafile to access the audio/video file.
5. The Web server responds.



Third Approach: Using a Media Server

The **problem** with the **second approach** is that **the browser and the media player both use the services of HTTP**. HTTP is designed to run over TCP. This is appropriate for retrieving the metafile, but not for retrieving the audio/video file. **The reason is that TCP retransmits a lost or damaged segment, which is counter to the philosophy of streaming.** We need to dismiss TCP and its error control; we need to use UDP. However, HTTP, which accesses the Web server, and the Web server itself are designed for TCP; we need another server, a **media server**.

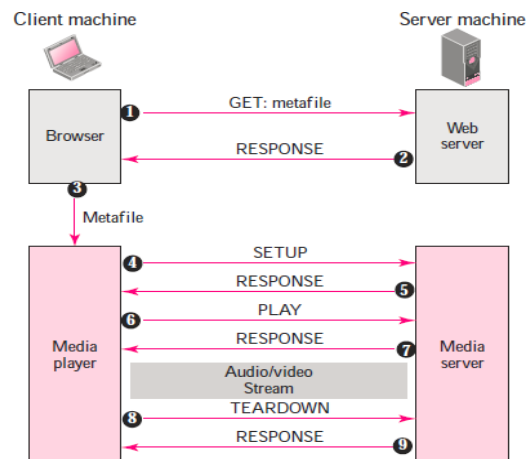


1. The HTTP client accesses the Web server using a GET message.
2. The information about the metafile comes in the response.

3. The metafile is passed to the media player.
4. The media player uses the URL in the metafile to access the media server to download the file. Downloading can take place by any protocol that uses UDP.
5. The media server responds.

Fourth Approach: Using a Media Server and RTSP

The **Real-Time Streaming Protocol (RTSP)** is a control protocol designed to add more functionalities to the streaming process. Using RTSP, we can control the playing of audio/video. Figure5 shows a media server and RTSP.



1. The HTTP client accesses the Web server using a GET message.
2. The information about the metafile comes in the response.
3. The metafile is passed to the media player.
4. The media player sends a SETUP message to create a connection with the media server.
5. The media server responds.
6. The media player sends a PLAY message to start playing (downloading).
7. The audio/video file is downloaded using another protocol that runs over UDP.
8. The connection is broken using the TEARDOWN message.
9. The media server responds.

2. STREAMING LIVE AUDIO/VIDEO

Streaming live audio/video is similar to the broadcasting of audio and video by radio and TV stations. Instead of broadcasting to the air, the stations broadcast through the Internet. There are **several similarities** between streaming stored audio/video and streaming live audio/video. **They are both sensitive to delay**; neither can accept retransmission. However, **there is a difference**. In the **first application**, the communication is **unicast and on-demand**. In the **second**, the communication is **multicast and live**. Live streaming is better suited to the multicast services of IP and the use of protocols such as UDP and RTP.

Examples: Internet Radio, Internet Television (ITV), Internet protocol television (IPTV)

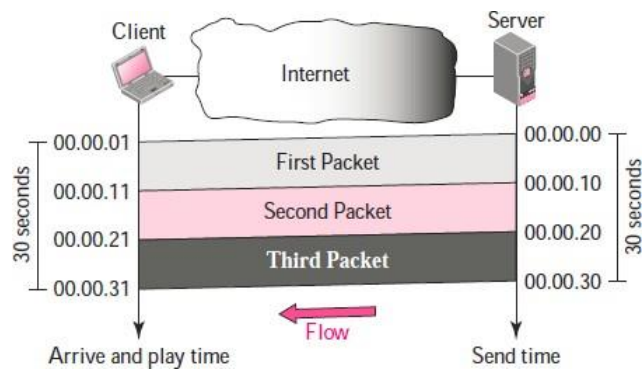
3. REAL-TIME INTERACTIVE AUDIO/VIDEO

In real-time interactive audio/video, **people communicate** with one another in **real time**. The **Internet phone** or **voice over IP** is an example of this type of application. **Video conferencing** is another example that allows people to communicate visually and orally.

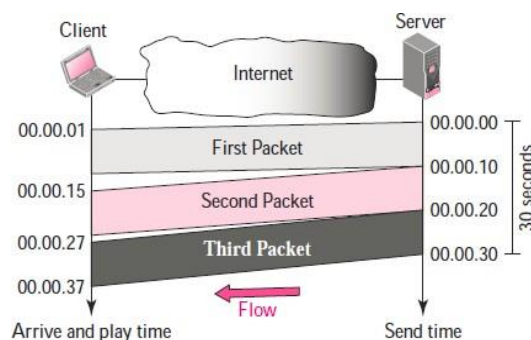
Before discussing the protocols used in this class of applications, we discuss some characteristics of real-time audio/video communication.

- **Time Relationship**

Real-time data on a packet-switched network **require the preservation of the time relationship between packets of a session.**



But what happens if the packets arrive with different delays? For example, the first packet arrives at 00:00:01 (1-s delay), the second arrives at 00:00:15 (5-s delay), and the third arrives at 00:00:27 (7-s delay). If the receiver starts playing the first packet at 00:00:01, it will finish at 00:00:11. However, the next packet has not yet arrived; it arrives 4 s later. There is a gap between the first and second packets and between the second and the third as the video is viewed at the remote site. This phenomenon is called **jitter**. **Jitter is introduced in real-time**



Data by the delay between packets.

- **Timestamp**

One solution to jitter is the use of a **timestamp**. If each packet has a timestamp that shows the time it was produced relative to the first (or previous) packet, then the receiver can add this time to the time at which it starts the playback. Imagine the first packet in the previous example has a timestamp of 0, the second has a timestamp of 10, and the third a timestamp of 20. If the receiver starts playing back the first packet at 00:00:08, the second will be played at 00:00:18, and the third at 00:00:28. There are no gaps between the packets.

