

# **APPLICATION LAYER**

# Name Space:-

- Control over names and IP addresses.
- A name space that maps each address to a unique name can be organized in two ways:

**i) Flat Name Space :-** A name in this space is a sequence of characters without structure. The main disadvantage of a flat name space is that it cannot be used in a large system such as the Internet

**ii) Hierarchical Name Space:-** Made up of several parts.

1<sup>st</sup> part-nature of the organization

2<sup>nd</sup> part-name of an organization

3<sup>rd</sup> part-define departments in

the organization, and so on..

# Domain Name Space (DNS)

## Domain Name System (DNS)

- Hierarchical Name Space
- Domain Servers
- How does DNS Work in Internet
- Domain Name Resolution
- Messages Used in DNS
- Dynamic DNS (DDNS)

# Domain Name Space

- As we already know, each host machine on the Internet is assigned an IP address. The 32-bit IP address is represented in the numerical form, e.g., 202.12.32.22. However, it is very difficult for a user to remember the address of a machine in terms of an IP address. Therefore, the IP addresses have been denoted as a set of characters in English

e.g:-for the other name, of IP address 68.142.226.32 is yahoo.com.

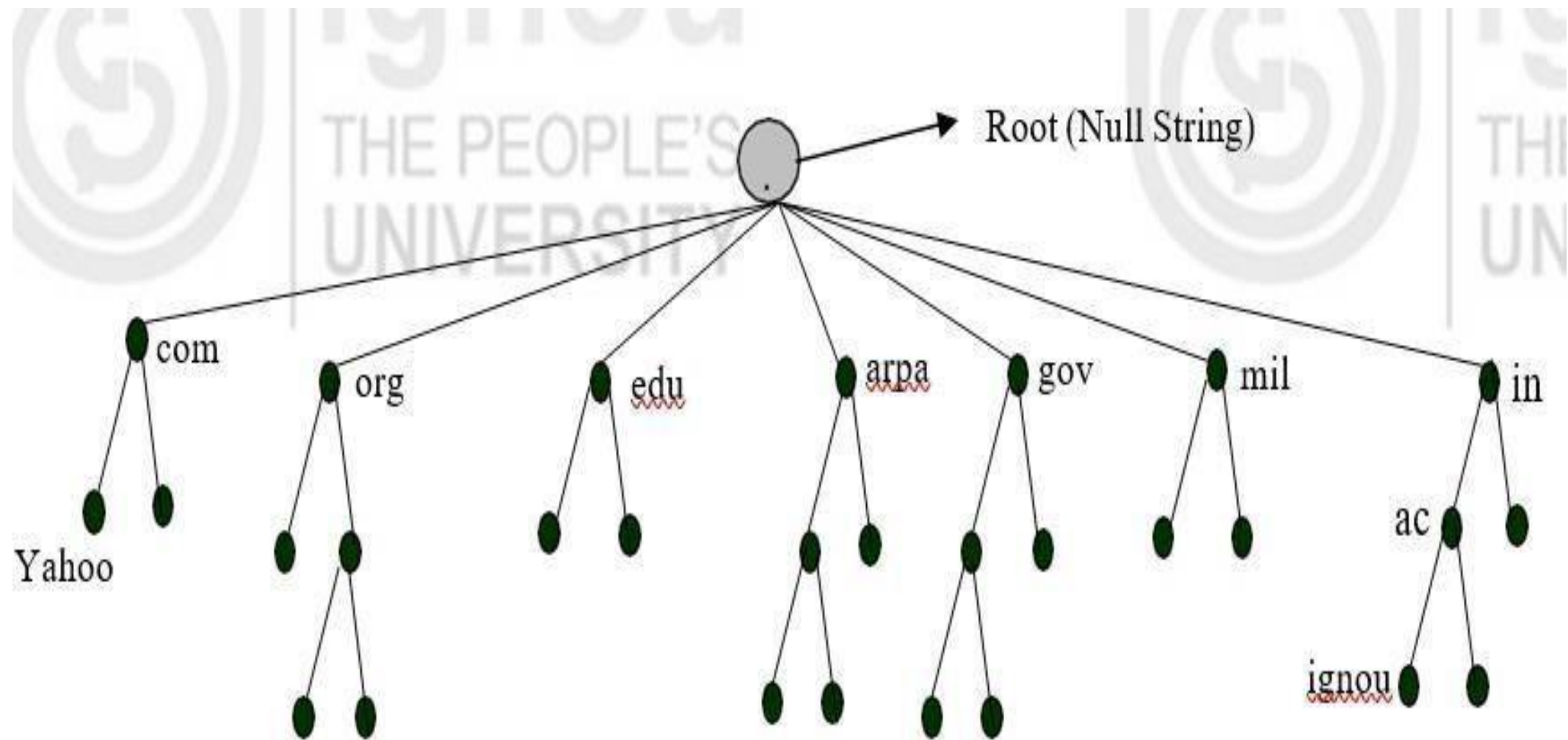


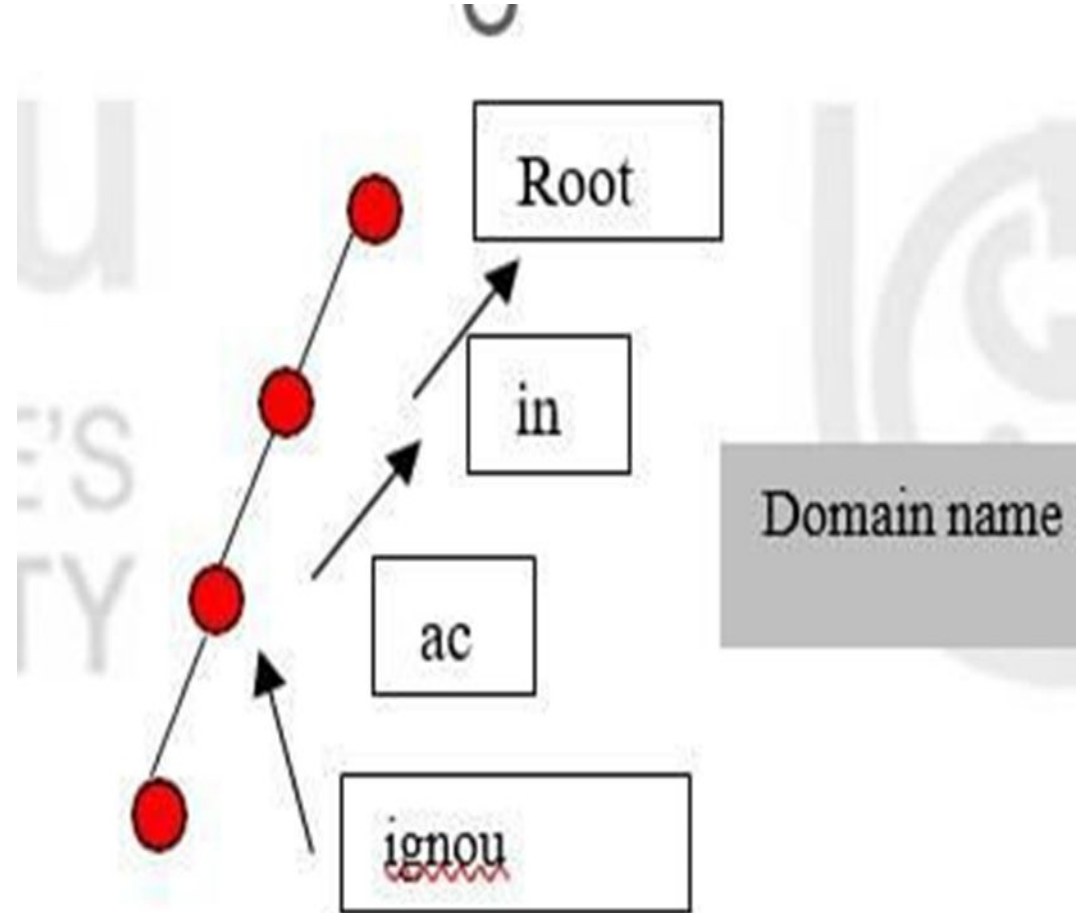
Figure 1: Hierarchical Name Space for DNS

- Levels:- maximum levels of tree 128.
- Label:-Each node in the tree has a label, which is a string with a maximum of 63 characters.
  - root label is a null string
  - children node have different labels,
- Domain name:-Each node in the tree has a domain name. A full domain name is a sequence of labels separated by dots (.). The domain names are always read from the node up to the root.

The last label is the label of the root (null).

Example:-

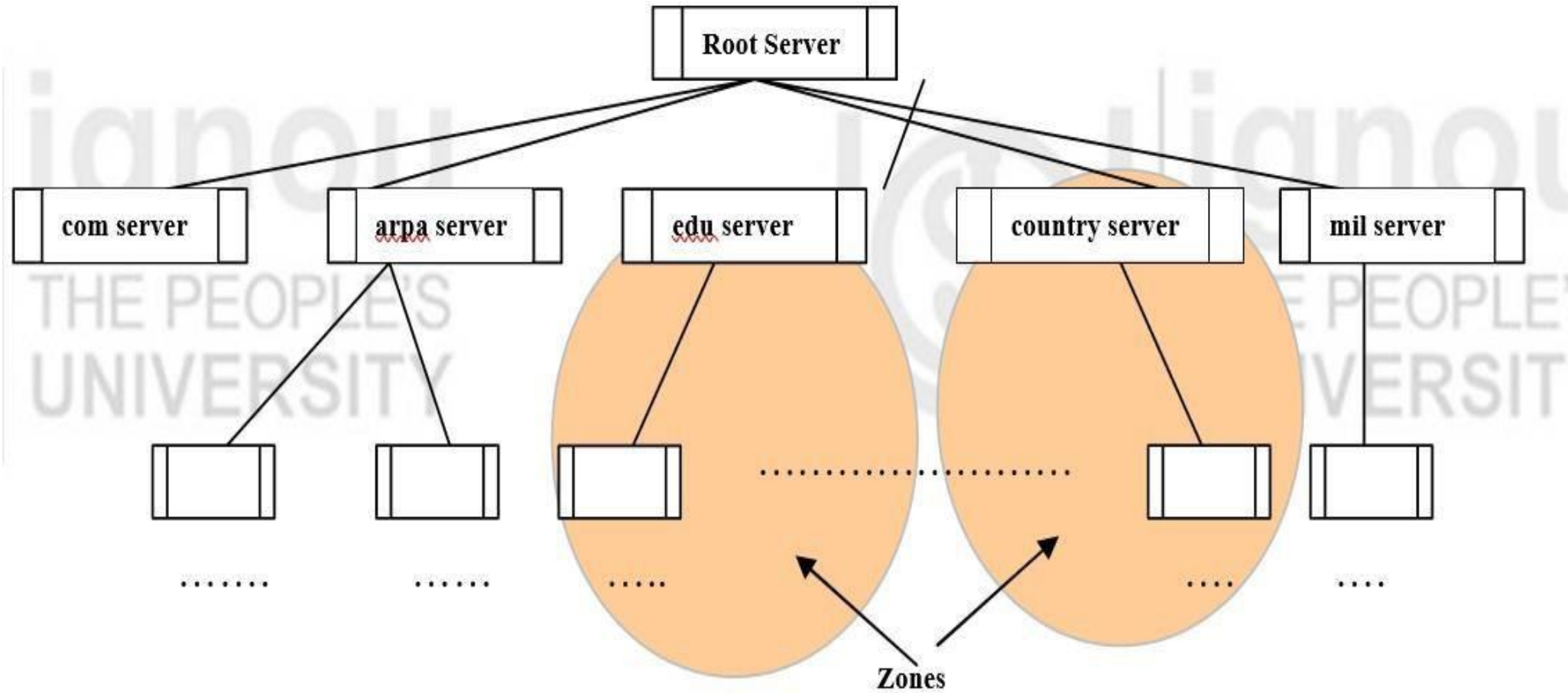
- Domain name is lbrce.ac.in



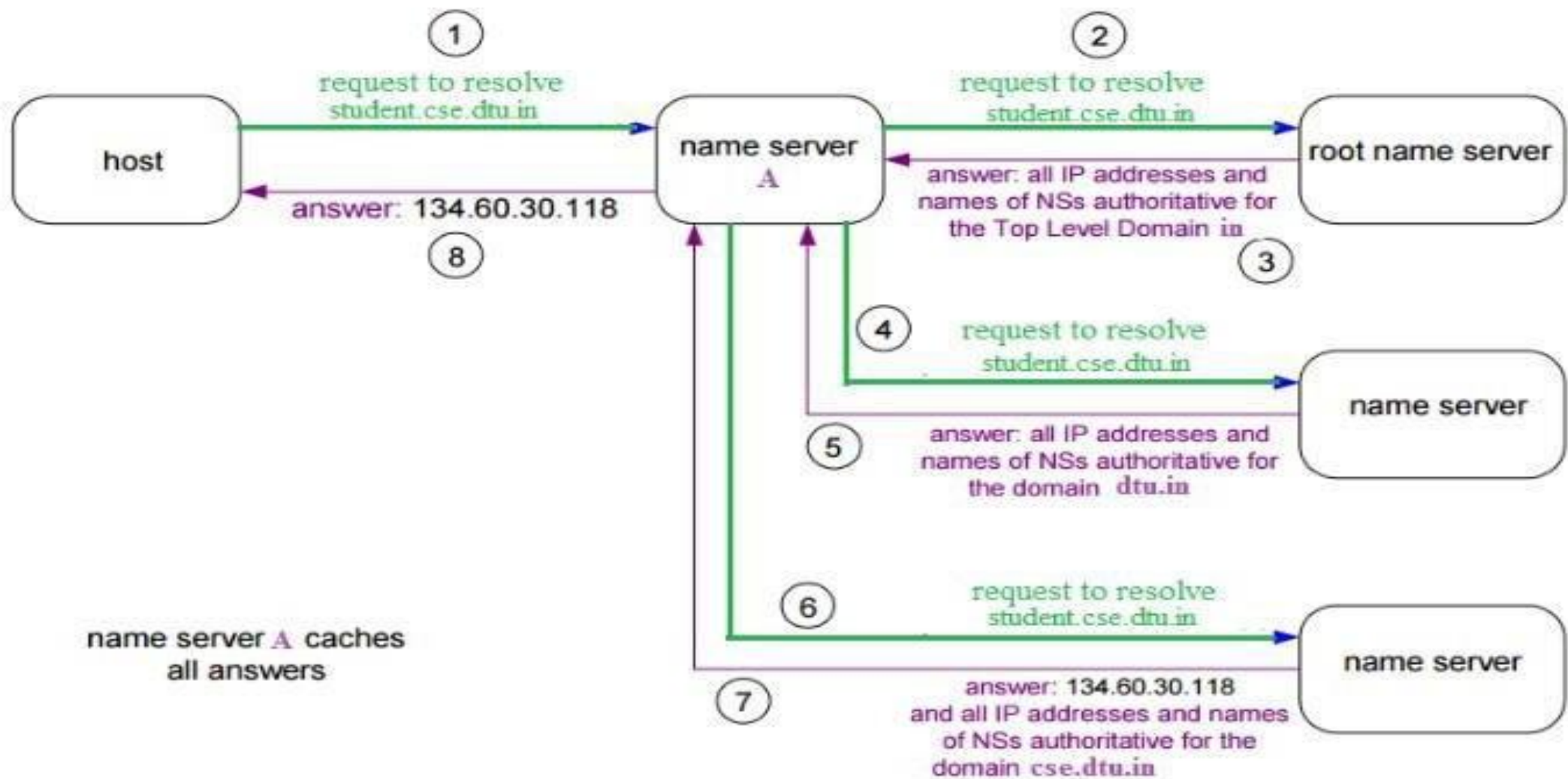
# Domain name server:-

- Domain name information has been distributed among various servers known as Domain Servers.
- The server is responsible or has an authority over a specific region called a zone i.e., the DNS database is divided into zones.
- The servers in their respective zones are responsible for answering queries for their zones and are called name servers.
- There are multiple name servers for a zone. There is usually one primary name server and one or more secondary name servers. A name server may be authoritative for more than one zone.





**Figure 3: Name Servers**



# How does DNS Work in Internet?

- The hierarchical system of domain names in Internet has been broadly classified into three categories:
  1. Generic domain names
  2. Country based domain names
  3. Inverse domains

# Generic domain names :-

Table 1: Generic Domain Names

Domain Name	Meaning
Com	Commercial <u>organisations</u>
Gov	Government institutions
Org	Non-profit <u>organisations</u>
Mil	Military groups
Edu	Educational institutions
Net	Major network support centers
Int	International <u>organisations</u>

## 2. Country based domain names:-

International 2- character country codes (e.g., zw for Zimbabwe). These are called the country domains. Many countries have their own second-level domains.

3. Inverse domains: if we want to know what is the domain name of the website. IP to

domain name mapping. So DNS can provide both the mapping for example to find the IP addresses of google.com then we have to type `nslookup www.google.com`.

## Domain Name Resolution:-

- The concept of mapping a domain name to an IP address and vice-versa is known as resolution process.

- The resolution process is basically a client server platform.

- the DNS calls a client program called resolver.

- The steps followed in the resolution are below:

- 1)The user program issues a request such as the `gethostbyname( )` system call.

- 2)The resolver formulates a query to the name server.

- 3)The name server checks to see if the answer is in its local authoritative database or cache, and if so, returns it to the client. Otherwise, it will query other available name server(s), starting down from the root of the DNS tree or as high up the tree as possible.

- 4)The user program will finally be given a corresponding IP address (or host name, depending on the query) or an error if the query could not be answered.

# Messages used in DNS:-

- As DNS follows the client server paradigm, it has two types of messages: Query and Response.

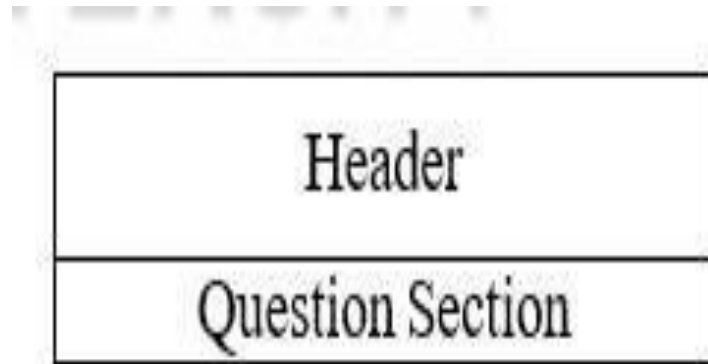


Figure 5: Query Message

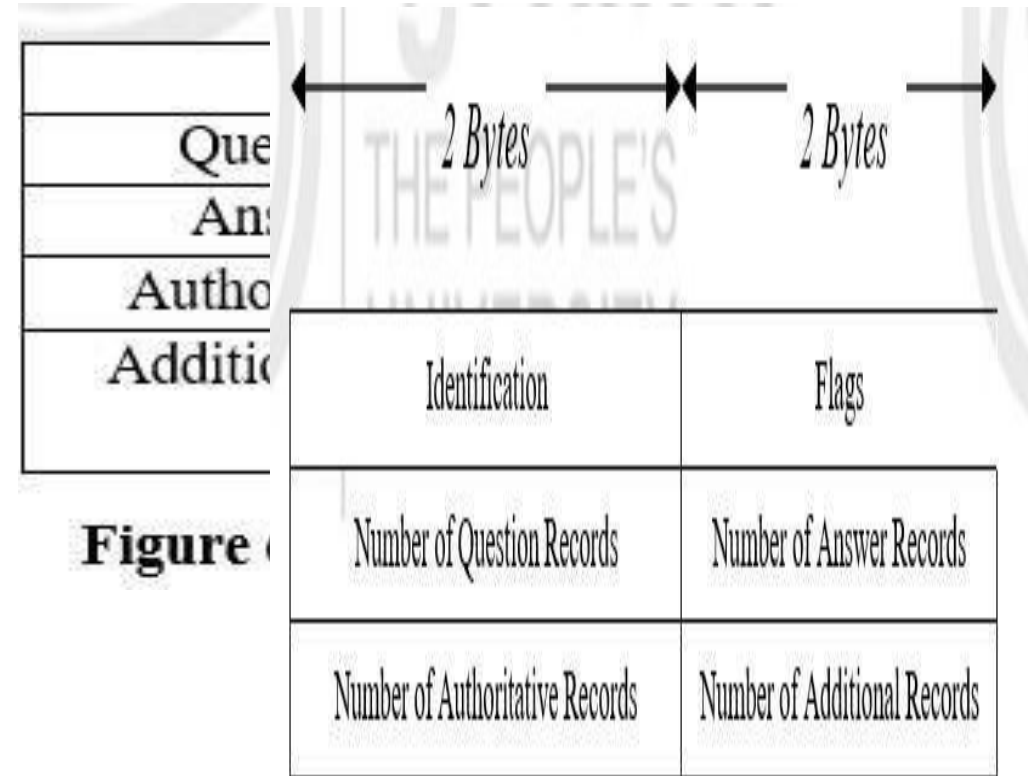


Figure 6: Header format for Query/Response

Figure 7: Header format for Query/Response

- **Message header:-**
- **Identification** used by the source of the message in order to match the response of the query.

- **Flags** contains various fields that define the kind of message i.e., recursive, iterative, authoritative, nonauthoritative etc.
- **Number of Question Records** contains the total number of queries asked by the resolver in the Question Section.
- **Number of Answer Records** contains the total number of answers specified in the Answer Section.
- **Number of Authoritative Records** contains the total number of Authoritative records in the Authoritative Section.
- **Number of Additional Records** contains the total number of Additional records in the Additional Section.



# Dynamic DNS (DDNS):-

- DDNS, most commonly known as Dynamic DNS, is an automatic method of refreshing a name server. It can dynamically update DNS records without the need for human interaction. It is extremely useful for updating A and AAAA records when the host has changed its IP address.
- DDNS is a service that automatically and periodically updates your DNS's A (IPv4) or AAAA (IPv6) records when your IP address changes. These IP changes are made by your Internet provider.
- When DNS (Domain Name System) was designed, nobody expected that there would be so many address changes such as adding a new

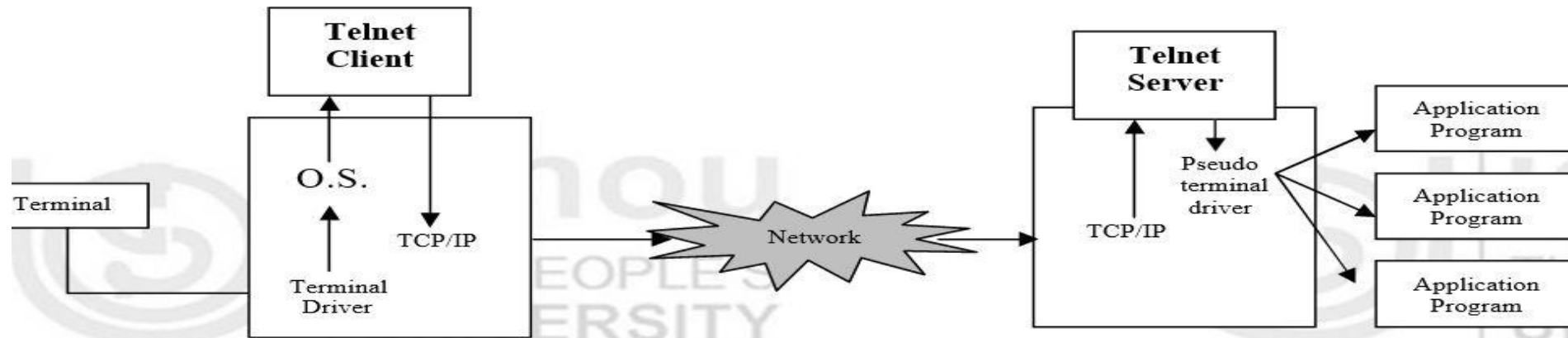
host, removing a host, or changing an IP address. When there is a change, the change must be made to the DNS master file which needs a lot of manual updating and it must be updated dynamically.

-

TELNET

# TELNET:-

- TELNET is a widely known application protocol that provides remote execution capability.
- TELNET is a popular client server application program.
- TELNET is an abbreviation for ***TErминаl NETwork***.
- TELNET is a standard application protocol that provides an interface, through which a program on a host i.e., *TELNET client* can access the resources of another host i.e., *TELNET server*.
- TELNET provides an environment such that the client acts as a local terminal connected to the server as shown in *Figure 13*. Basically, TELNET is a utility whereby a user first logs into a remote machine and thereafter the user can access the files / programs located remotely.



**Figure 13: TELNET**

The working of TELNET is as follows: The user types on the host machine /terminal that runs a driver known as terminal driver (a module of the operating system). It basically receives the keystrokes typed by the user on the terminal and passes the corresponding characters to the operating system. The operating system in turn sends these characters to the TELNET client. As discussed in SMTP, the language/format acceptable to the terminal might be different from the format allowed by TELNET. Therefore, the characters received by the TELNET client from the terminal driver are converted into a generic character set known as Network Virtual Terminal (NVT) characters. The transformed form of characters is sent to the TCP/IP protocol stack of the local machine.

**ELECTRONIC MAIL**

# ELECTRONIC MAIL

- Architecture
  - First Scenario
  - Second Scenario
  - Third Scenario
  - Fourth Scenario
- User Agent
  - Services Provided by a User Agent
  - Handling Mailboxes
  - User Agent Types
  - Sending Mail
  - Receiving Mail
  - Addresses
  - Mailing List
- MIME
- message transfer agent-SMTP
- message access agent -  
POP and IMAP

# ELECTRONIC MAIL

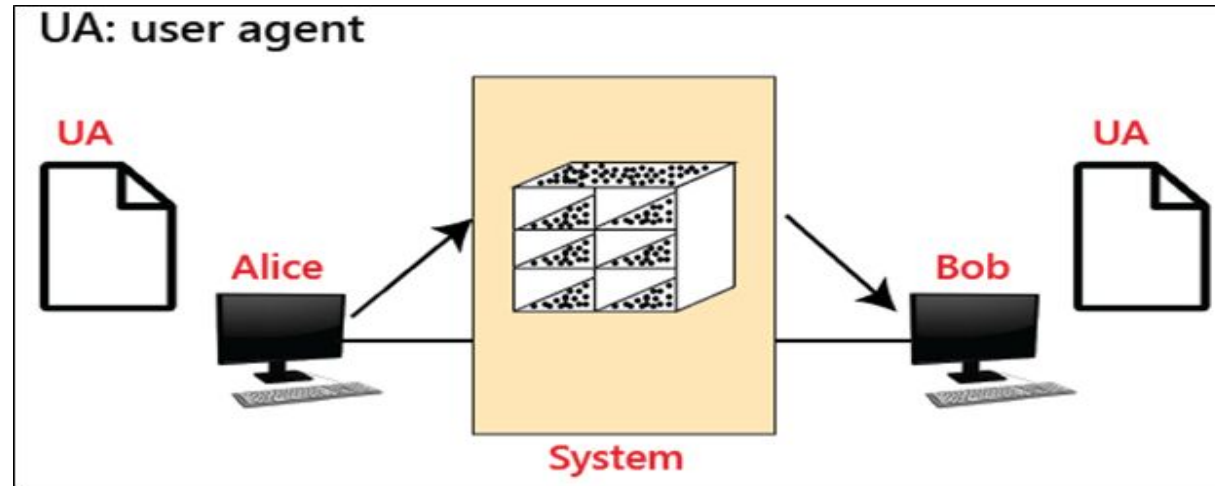
- One of the most popular Internet services is electronic mail (e-mail).
- Today, electronic mail is much more complex. It allows a message to include text, audio, and video.
- It also allows one message to be sent to one or more recipients.

## Architecture:-

The architecture of e-mail, we give four scenarios. We begin with the simplest situation and add complexity as we proceed. The fourth scenario is the most common in the exchange of email.

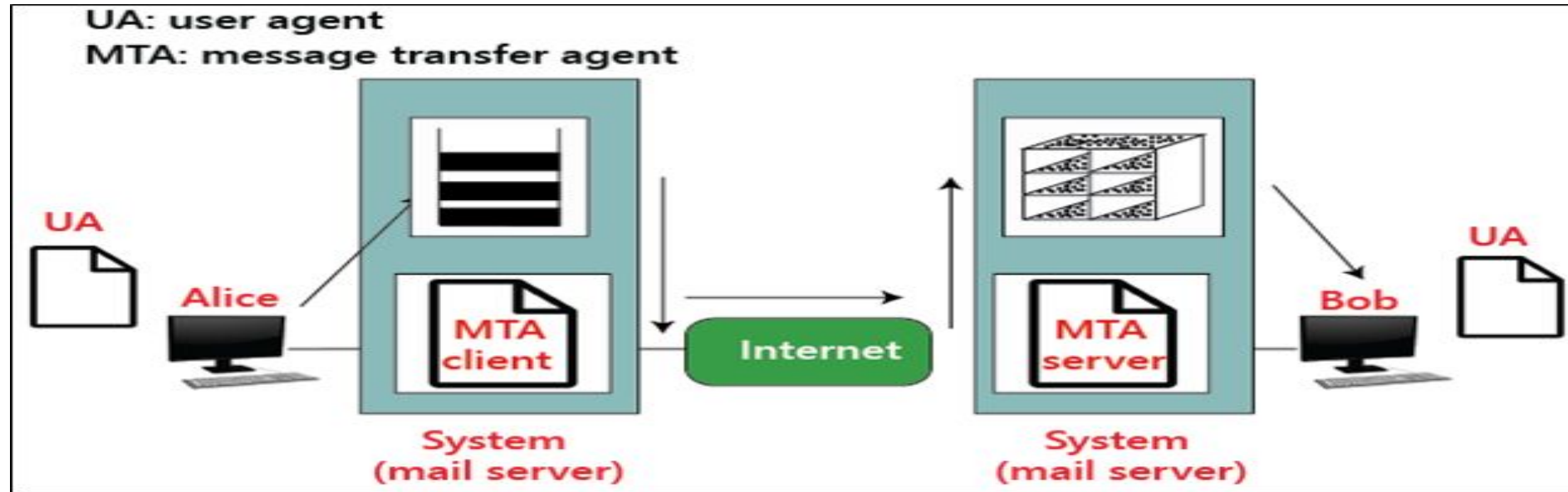


- **First Scenario:-** In the first scenario of e-mail, the sender and receiver use the same system, and that is directly connected to the server. This scenario requires only two user agent (UA).



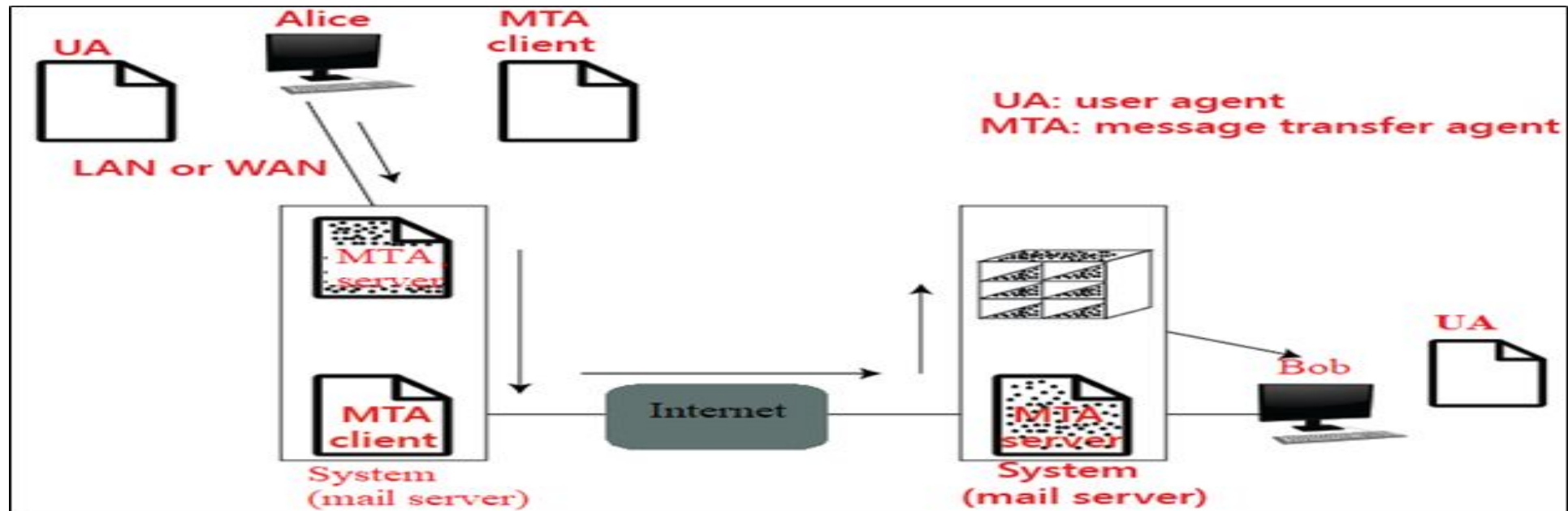
- For example, let takes two user agents (Alice and Bob), that is shown in the figure. When Alice sends the mail to Bob, then Alice runs the user agent (UA) program to prepare the e-mail. After that, this e-mail is stored in the mailbox of Bob.

- **Second Scenario:-** In the second scenario of e-mail, the sender and receiver are used the two different systems. The e-mail is sent through the internet in this scenario. This scenario requires two user agents (UAs) and a pair of message transfer agents (MTAs).



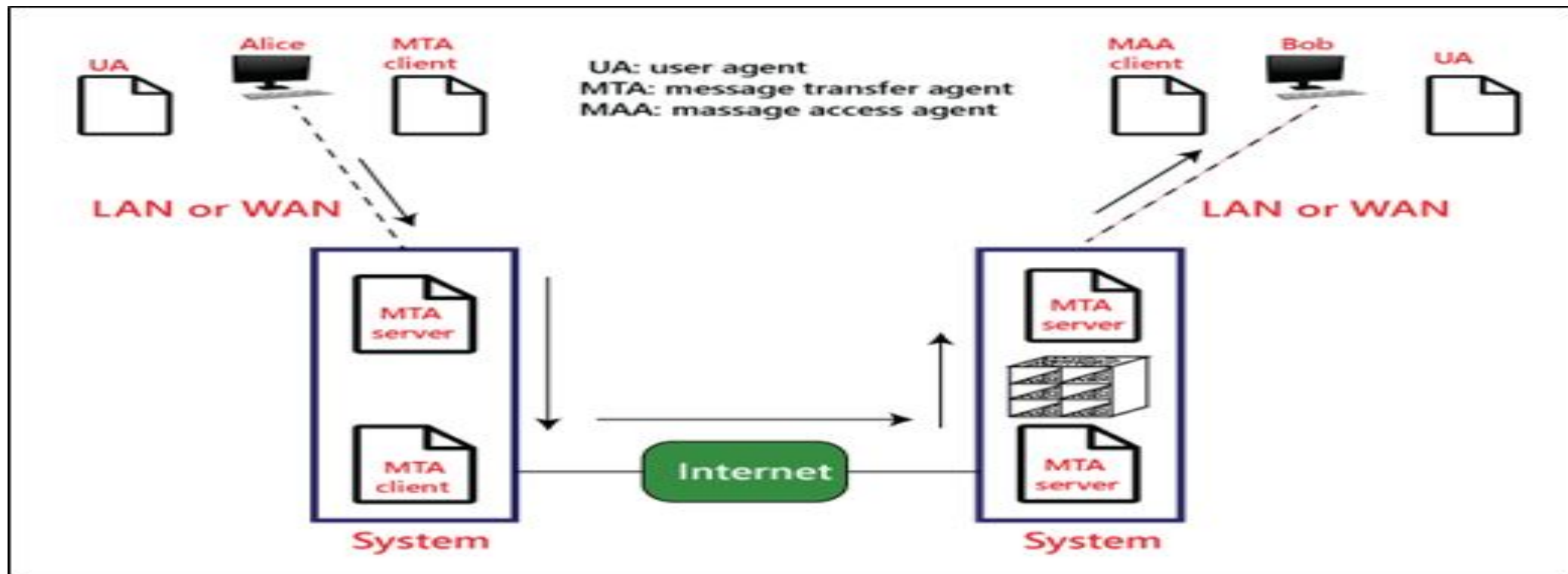
- For example, let takes two user agents (Alice and Bob), which is shown in the figure. When Alice sends the mail to Bob, then Alice runs the user agent (UA) and message transfer agents (MTAs) program to prepare the e-mail through the internet. After that, this e-mail is stored in the mailbox of Bob.

- **Third Scenario:-** In the third scenario of e-mail, the sender is connected to the server through a LAN and WAN. This scenario requires two user agents (UAs) and two pairs of message transfer agents (MTAs).



- Fourth Scenario:-

In the fourth scenario of e-mail, the sender and receiver are connected to the server through a LAN and WAN. This scenario requires two user agents (UAs), two pairs of message transfer agents (MTAs), and a pair of message access agents (MAAs).



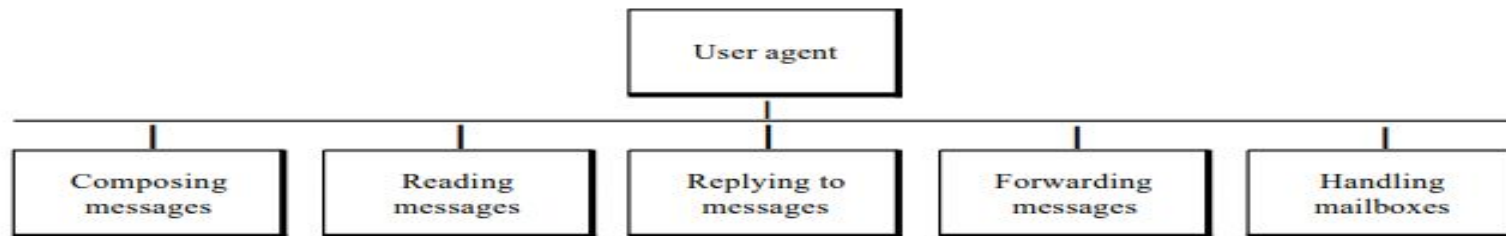
# User Agent:-

- The first component of an electronic mail system is the user agent (VA). It provides
- service to the user to make the process of sending and receiving a message easier
- *Services Provided by a User Agent:-*

---

Figure 26.11 *Services of user agent*

---



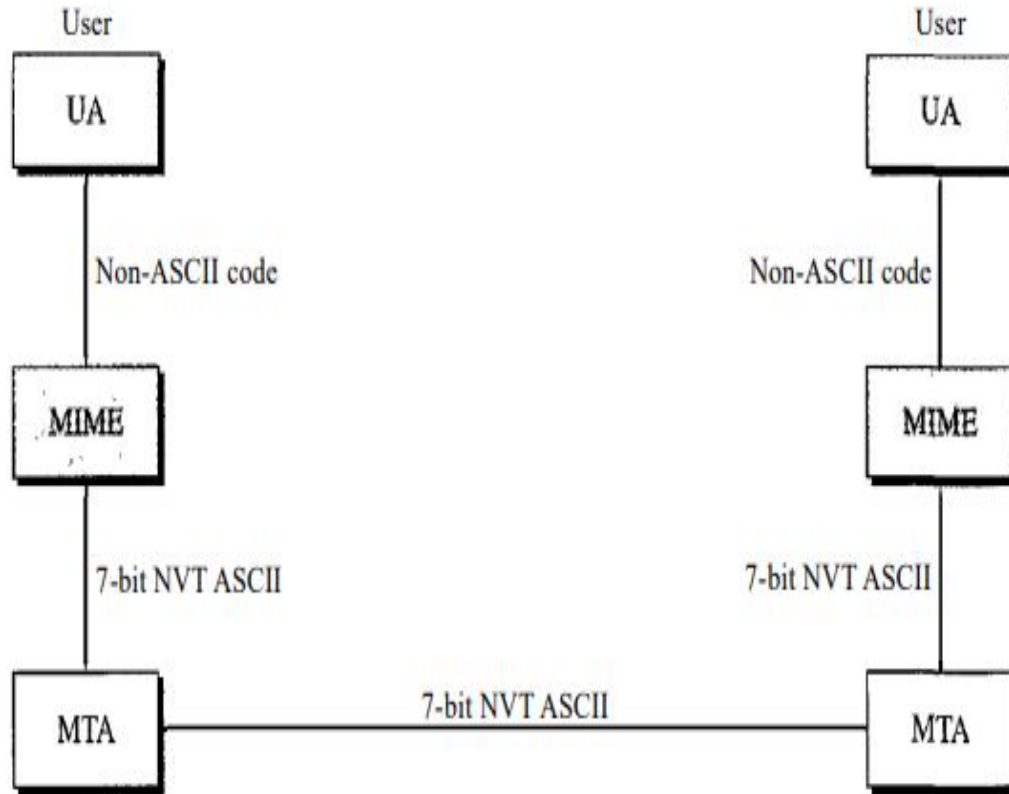
- *Handling Mailboxes* :-A user agent normally creates two mailboxes: an inbox and an outbox. Each box is a file with a special format that can be handled by the user agent.
- *User Agent Types*:-There are two types of user agents: command-driven and GUI-based
  - command-driven
  - GUI-based
- *Sending Mail* :-To send mail, the user, through the UA, creates mail that looks very similar to postal mail. It has an envelope and a message
- *Receiving Mail* :-The user agent is triggered by the user (or a timer). If a user has mail, the VA informs the user with a notice. If the user is ready to read the mail, a list is displayed in which each line contains a summary of the information about a particular message in the mailbox. The summary usually includes the sender mail address, the subject, and the time the mail was sent or received.

- *Addresses* :-To deliver mail, a mail handling system must use an addressing system with unique addresses. In the Internet, the address consists of two parts: a local part and a domain name, separated by an @ sign
- *Mailing List*:- Electronic mail allows one name, an alias, to represent several different e-mail addresses; this is called a mailing list.

## *MIME* :-

- Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail. MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers them to the client MTA to be sent through the Internet. The message at the receiving side is transformed back to the original data.

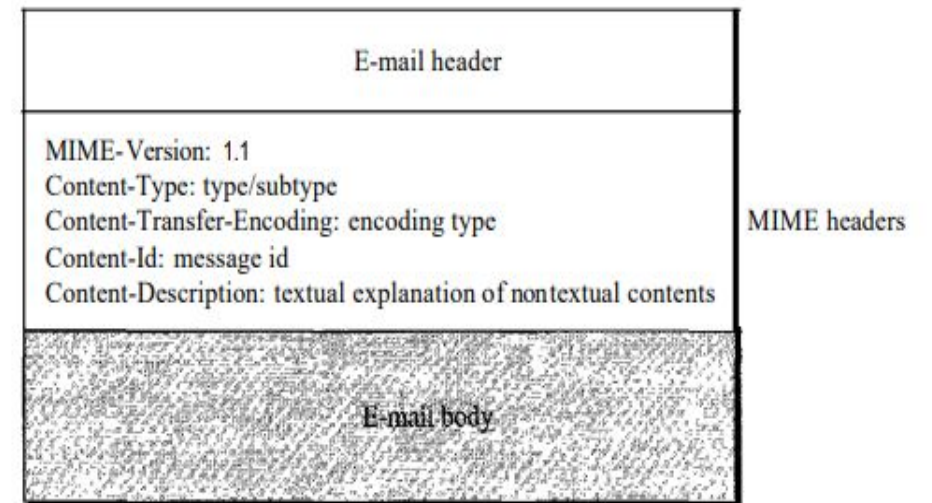
Figure 26.14 *MIME*



MIME defines five headers that can be added to the original e-mail header section to define the transformation parameters:

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

Figure 26.15 *MIME header*





- MIME-Version :-This header defines the version of MIME used. The current version is 1.1.

**MIME-Version: 1.1**

- Content-Type :-This header defines the type of data used in the body of the message. The content type and the content subtype are separated by a slash. Depending on the subtype, the header may contain other parameters

**Content-Type: <type /subtype; parameters>**

- Content-Transfer-Encoding :-This header defines the method used to encode the messages into Os and Is for transport

**Content-Transfer-Encoding: <type>**

- Content-Id :-This header uniquely identifies the whole message in a multiple-message environment.

**Content-Id:** id=<content-id>

- Content-Description This header defines whether the body is image, audio, or video.

**Content-Description:** <description>

Table 26.6 Content-transfer-encoding

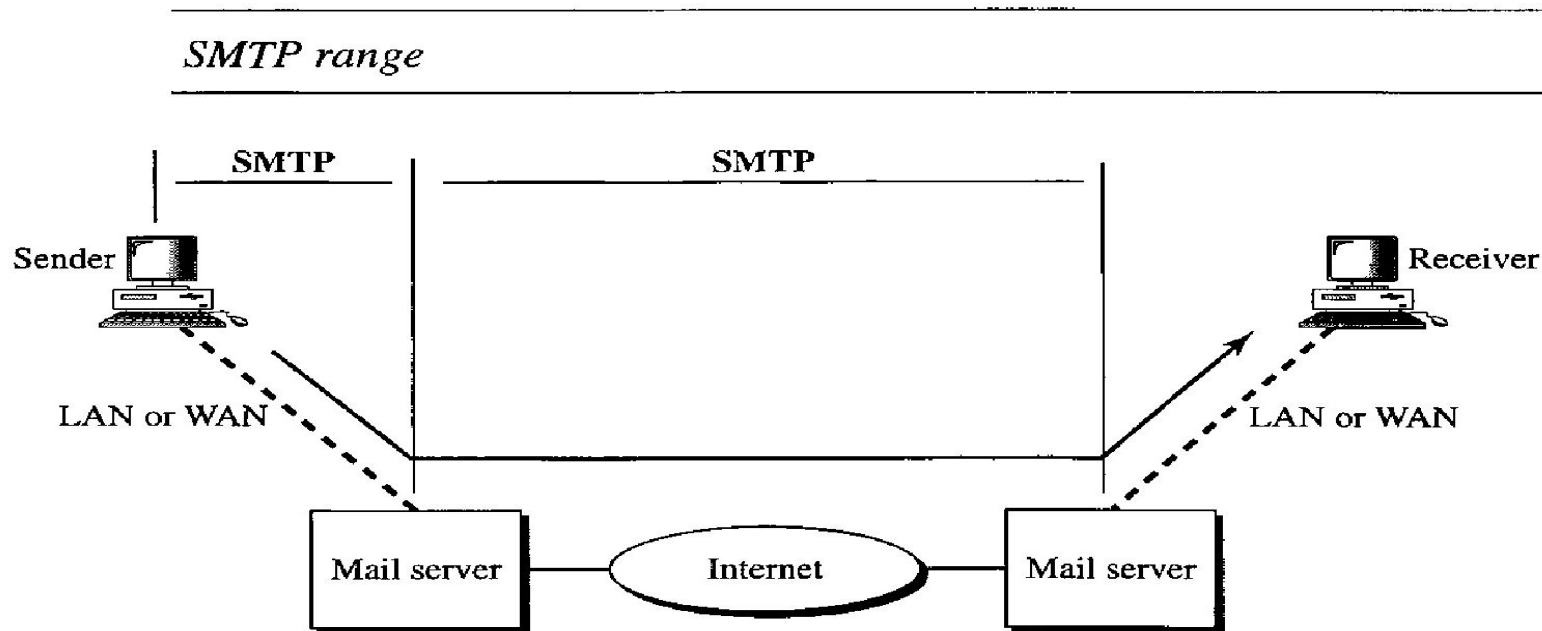
Type	Description
7-bit	NVT ASCII characters and short lines
8-bit	Non-ASCII characters and short lines
Binary	Non-ASCII characters with unlimited-length lines
Base-64	6-bit blocks of data encoded into 8-bit ASCII characters
Quoted-printable	Non-ASCII characters encoded as an equals sign followed by an ASCII code

Table 26.5 Data types and subtypes in MIME

Type	Subtype	Description
Text	Plain	Unformatted
	HTML	HTML format (see Chapter 27)
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to mixed subtypes, but the default is message/RFC822
	Alternative	Parts are different versions of the same message
Message	RFC822	Body is an encapsulated message
	Partial	Body is a fragment of a bigger message
	External-Body	Body is a reference to another message
Image	IPEG	Image is in IPEG format
	GIF	Image is in GIF format
Video	MPEG	Video is in MPEG format
Audio	Basic	Single-channel encoding of voice at 8 kHz
Application	PostScript	Adobe PostScript
	Octet-stream	General binary data (8-bit bytes)

## Message Transfer Agent: SMTP:-

- The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol (SMTP).
- Two pairs of MTA client/server programs are used in the most common situation (fourth scenario)



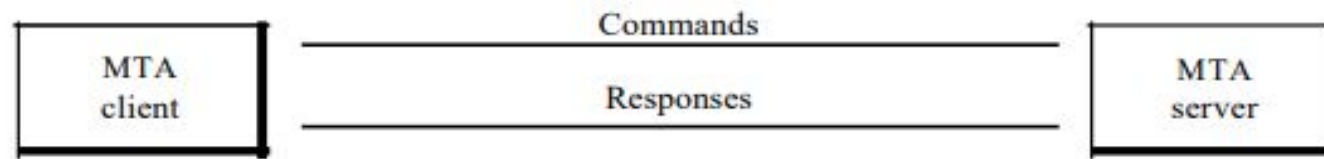
- SMTP is used two times, between the sender and the sender's mail server and between the two mail servers.
- SMTP is based on end-to-end delivery .
- SMTP is the Application Level protocol that handles message services over TCP/IP networks.
- SMTP uses TCP Well Known port 25.

- *Commands and Responses* :-SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.

---

Figure 26.17 *Commands and responses*

---



- **Commands:-**  
Commands are sent from the client to the server.
- *Mail Transfer Phases:-* The process of transferring a mail message occurs in three phases: connection establishment, mail transfer, and connection termination



Table 26.7 *Commands*

<i>Keyword</i>	<i>Argument(s)</i>
HELO	Sender's host name
MAIL FROM	Sender of the message
RCPTTO	Intended recipient of the message
DATA	Body of the mail
QUIT	
RSET	
VRFY	Name of recipient to be verified
NOOP	
TURN	
EXPN	Mailing list to be expanded
HELP	Command name

Table 26.7 *Commands (continued)*

<i>Keyword</i>	<i>Argument(s)</i>
SEND FROM	Intended recipient of the message
SMOLFROM	Intended recipient of the message
SMALFROM	Intended recipient of the message

Table 26.8 *Responses*

<i>Code</i>	<i>Description</i>
<b>Positive Completion Reply</b>	
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
<b>Positive Intermediate Reply</b>	
354	Start mail input
<b>Transient Negative Completion Reply</b>	
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted: insufficient storage
<b>Permanent Negative Completion Reply</b>	
500	Syntax error; unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mailbox unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

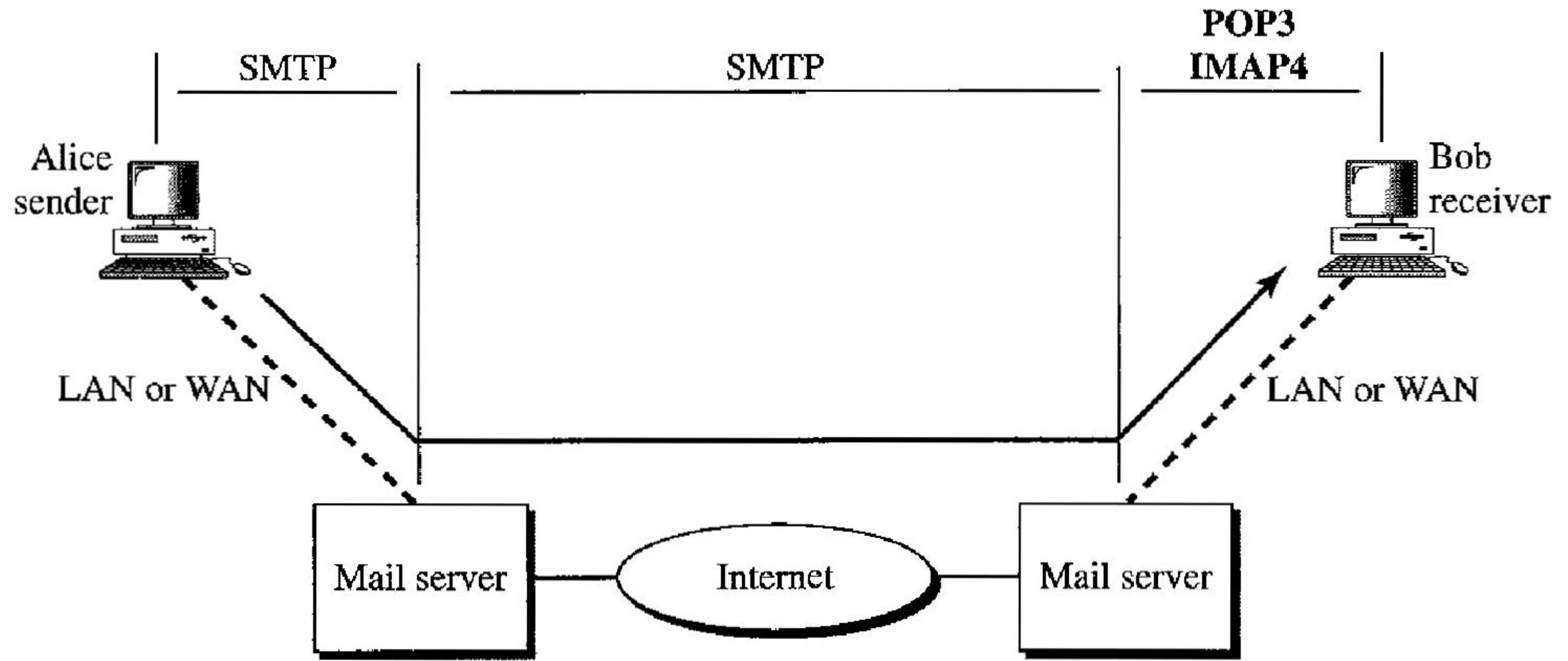
# Message Access Agent: POP and IMAP:-

- The first and the second stages of mail delivery use SMTP. However, SMTP is not involved in the third stage because SMTP is a push protocol; it pushes the message from the client to the server.
- On the other hand, the third stage needs a pull protocol; the client must pull messages from the server. The direction of the bulk data is from the server to the client. The third stage uses a message access agent.
- Currently two message access protocols are available: **Post Office Protocol, version 3 (POP3)** and **Internet Mail Access Protocol, version 4 (IMAP4)**. Figure below shows the position of these two protocols in the most common situation Post Office Protocol, version 3 (POP3) is simple and limited in functionality. The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server.

---

## *POP3 and IMAP4*

---





## •POP3(Post Office Protocol version 3):-

- Mail access starts with the client when the user needs to download e-mail from the mailbox on the mail server. The client opens a connection to the server on TCP port 110. It then sends its user name and password to access the mailbox. The user can then list and retrieve the mail messages, one by one. Figure below shows an example of downloading using POP3.
- POP3 has two modes: the delete mode and the keep mode.

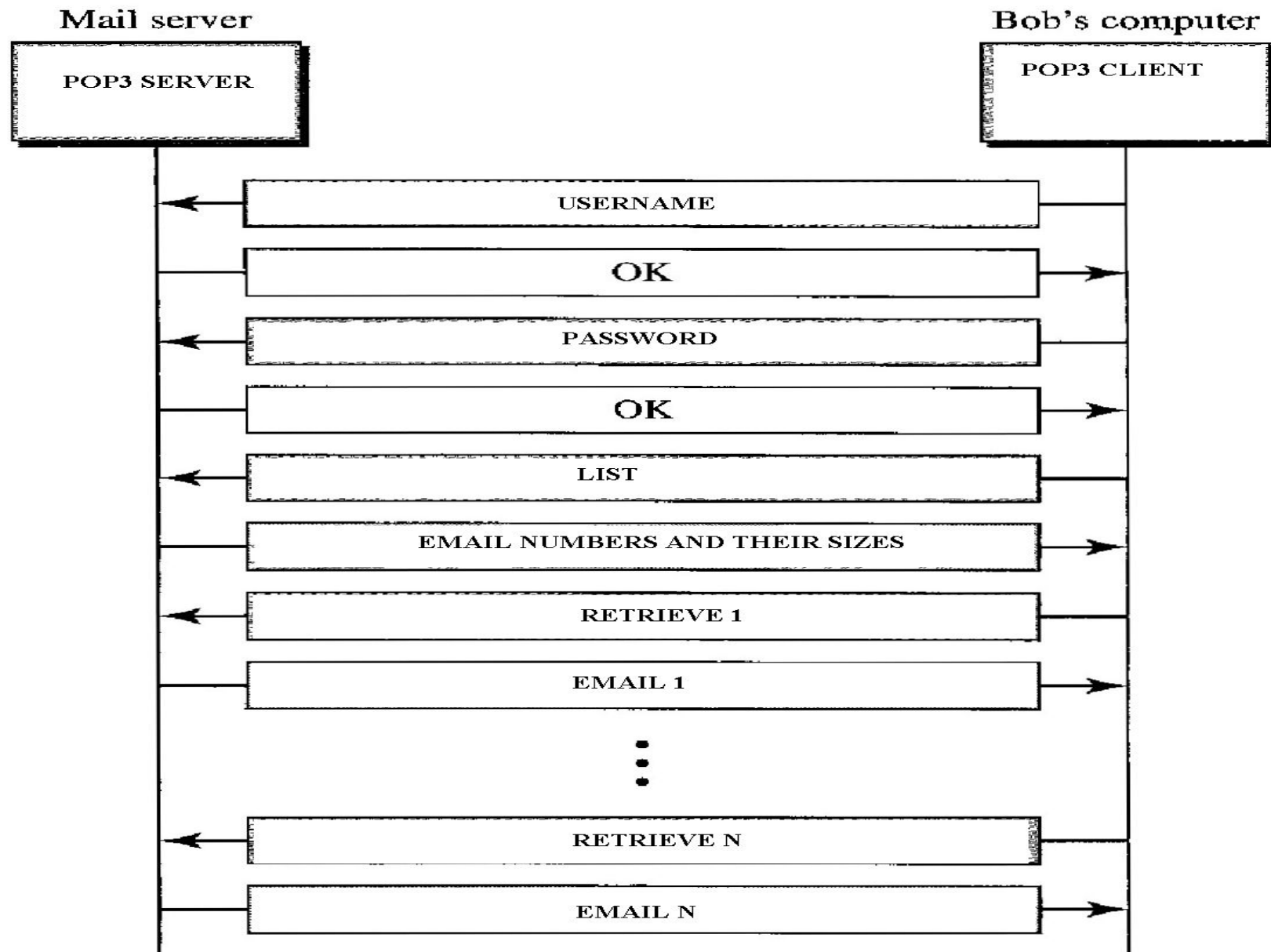
### **Delete mode:-**

- The mail is deleted from the mailbox after each retrieval.
- The delete mode is normally used when the user is working at her permanent computer and can save and organize the received mail after reading or replying.

### **Keep mode:-**

- The mail remains in the mailbox after retrieval.
- The keep mode is normally used when the user accesses her mail away from her primary computer (e.g., a laptop). The mail is read but kept in the system for later retrieval and organizing.

## *The exchange of commands and responses in POP3*



## IMAP Protocol:-

- IMAP-4 is more powerful and more complex.
- Once the TCP connection is established between the IMAP client and IMAP server, the IMAP server listens to the port 143 by default, but this port number can also be changed.
- By default, there are two ports used by IMAP:
  - Port 143: It is a non-encrypted IMAP port.
  - Port 993: This port is used when IMAP client wants to connect through IMAP securely.

IMAP4 provides the following extra functions:

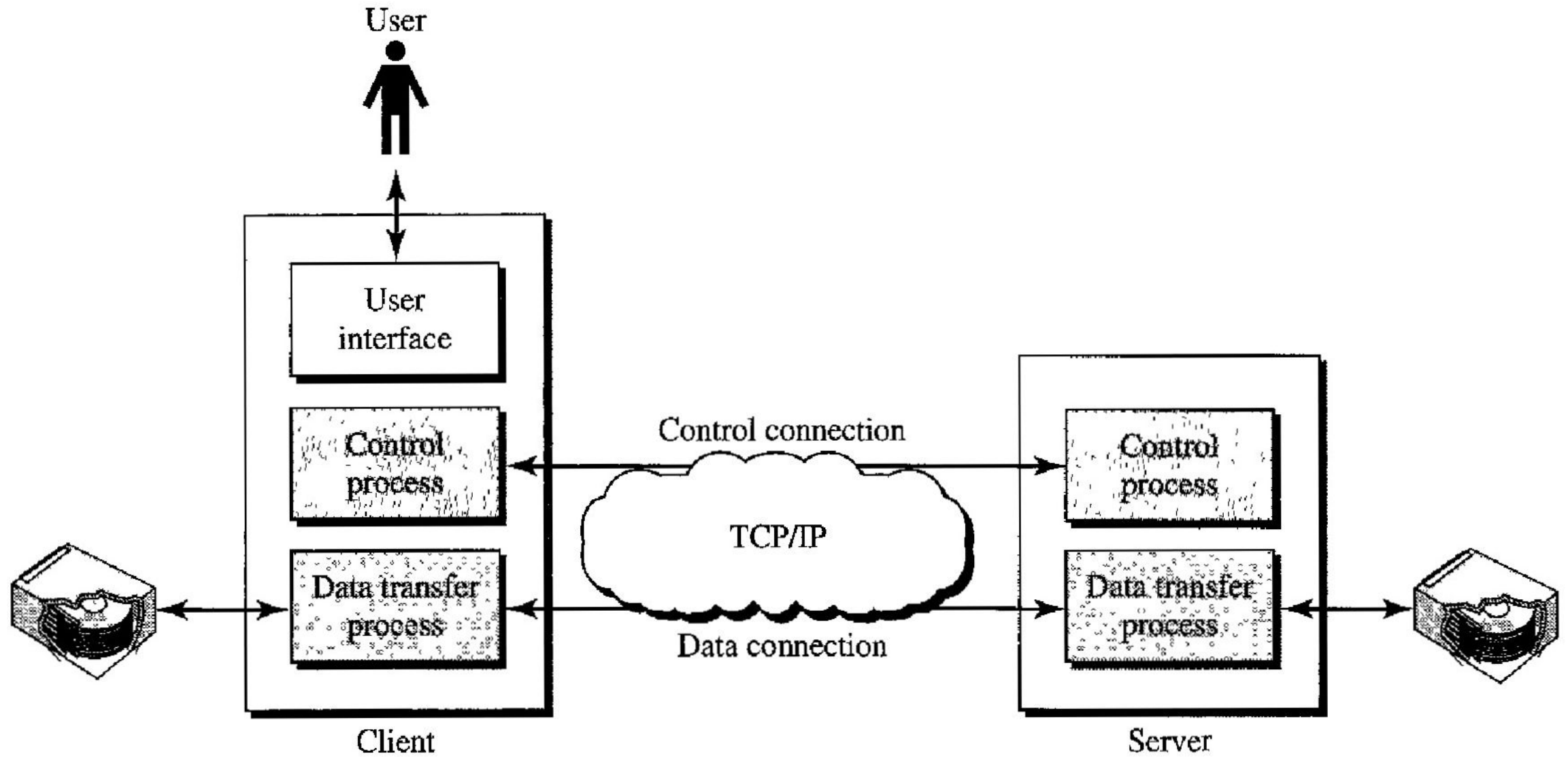
- A user can **check** the e-mail header prior to downloading.
- A user can **search** the contents of the e-mail for a specific string of characters prior to downloading.
- A user can **partially download** e-mail.
- This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.
- A user can **create, delete, or rename** mailboxes on the mail server.
- A user can **create a hierarchy** of mailboxes in a folder for e-mail storage

# FILE TRANSFER

# FILE TRANSFER:-

- Transferring files from one computer to another is one of the most common tasks expected from a networking or internetworking environment. One popular protocol involved in transferring files: File Transfer Protocol (FTP).
- File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another.
- Two systems may have different ways to represent text and data.
- Two systems may have different directory structures. All these problems have been solved by FTP in a very simple and elegant approach.
- FTP differs from other client/server applications in that it establishes two connections between the hosts.
- One connection is used for data transfer, the other for control information (commands and responses).
- We need to transfer only a line of command or a line of response at a time
- However, the difference in complexity is at the FTP level, not TCP.
- For TCP, both connections are treated the same.

# FTP



- **The FTP client** has three components: user interface, client control process, and the client data transfer process.
- **The FTP server** has two components: the server control process and the server data transfer process.
  - The control connection is made between the control processes.
  - The data connection is made between the data transfer processes.
- **control connection**:- For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of a control connection. The control connection is initiated on port number 21.
- **data connection**:-For sending the actual file, FTP makes use of a data connection. A data connection is initiated on port number 20.



# Anonymous FTP:-

- To use FTP, a user needs an account (user name) and a password on the remote server. Some sites have a set of files available for public access, to enable anonymous FTP.
- To access these files, a user does not need to have an account or password. Instead, the user can use anonymous as the user name and guest as the password.
- User access to the system is very limited. Some sites allow anonymous users only a subset of commands.
- For example, most sites allow the user to copy some files, but do not allow navigation through the directories.

# WWW(World Wide Web )

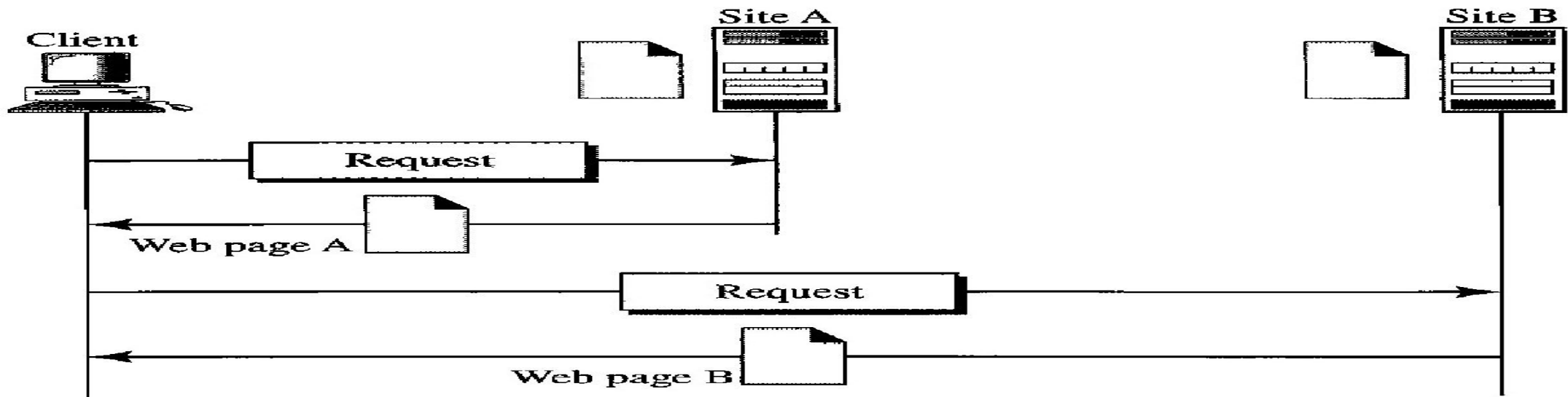
- Defination
- Client
- Server
- URL
- Cookies

- The World Wide Web (WWW) is a repository of information linked together from points all over the world.
- The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet.
- The WWW project was initiated by CERN (European Laboratory for Particle Physics) to create a system to handle distributed resources necessary for scientific research.
- The WWW today is a distributed client/server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called sites.

---

### *Architecture of WWW*

---



## Client (Browser)

- A variety of vendors offer commercial browsers that interpret and display a Web document, and all use nearly the same architecture.
- Each browser usually consists of three parts: a controller, client protocol, and interpreters.
- The controller receives input from the keyboard or the mouse and uses the client programs to access the document
- The client protocol can be one of the protocols described previously such as FTP or HTTP.
- The interpreter can be HTML, Java, or JavaScript, depending on the type of document.

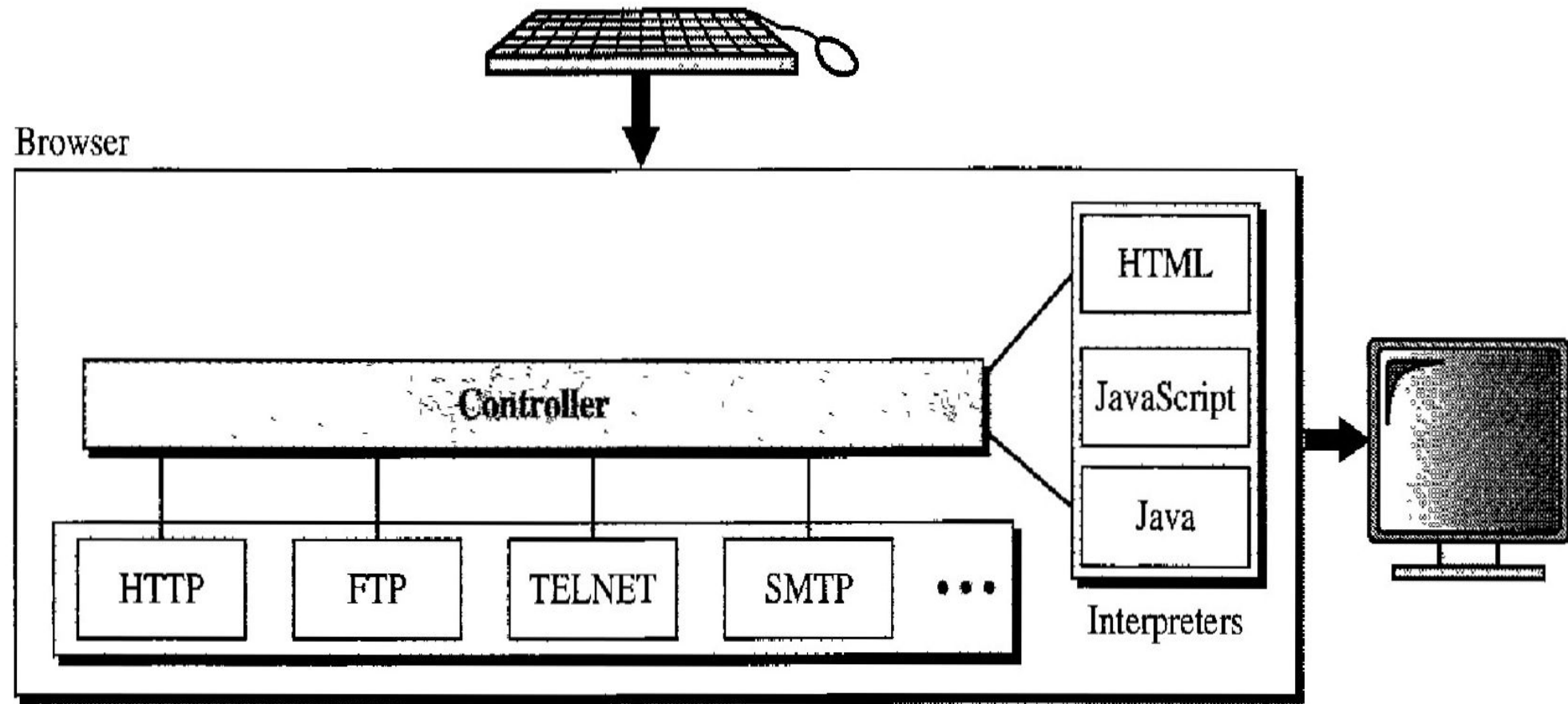
## Server

- The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client.
- To improve efficiency, servers normally store requested files in a cache in memory; memory is faster to access than disk.
- A server can also become more efficient through multithreading or multiprocessing.
- In this case, a server can answer more than one request at a time.

---

*Browser*

---



# *Uniform Resource Locator:-*

- A client that wants to access a Web page needs the address.
- The uniform resource locator (URL) is a standard for specifying any kind of information on the Internet.
- The URL defines four things: **protocol, host computer, port, and path** .
  - ***The protocol*** :-is the client/server program used to retrieve the document . Many different protocols can retrieve a document; among them are FTP or HTTP. The most common today is HTTP.
  - ***The host*** :-Web pages are usually stored in computers, and computers are given alias names that usually begin with the characters "www".
  - ***port***:- It is inserted between the host and the path, and it is separated from the host by a colon.
  - ***Path*** :-The pathname of the file where the information is located. Note that the path can itself contain slashes that, in the UNIX operating system, separate the directories from the subdirectories and files.

## URL

Uniform Resource Locator

Method

://

Host

:

Port

/

Path

# Cookies:-

- The World Wide Web was originally designed as a stateless entity. A client sends a request; a server responds. Their relationship is over. The original design of WWW, retrieving publicly available documents, exactly fits this purpose.

## **Creation and Storage of Cookies:-**

- When a server receives a request from a client, it stores information about the client in a file or a string.
- The information may include the domain name of the client, the contents of the cookie (information the server has gathered about the client such as name, registration number, and so on), a timestamp, and other information-depending on the implementation.
- The server includes the cookie in the response that it sends to the client.
- When the client receives the response, the browser stores the cookie in the cookie directory, which is sorted by the domain server name.



# HTTP

Defination

HTTP Transaction

Features

Advantages

Disadvantages

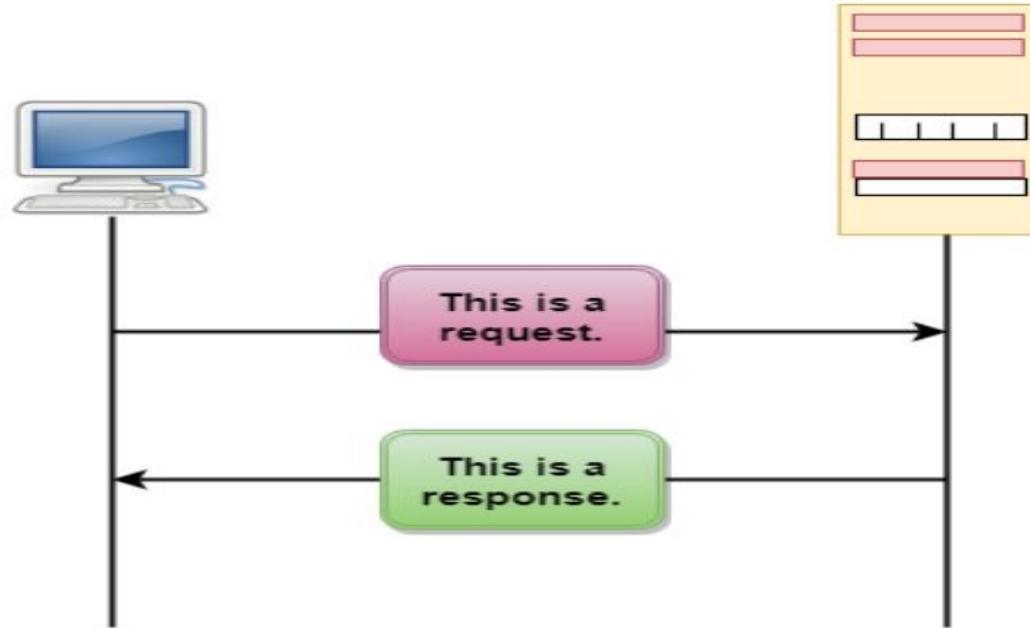
HTTP Connections

- The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web.
- HTTP functions as a combination of FTP and SMTP.
  - Similar to FTP because it transfers files and uses the services of TCP . However, it is much simpler than FTP because it uses only one TCP connection . There is no separate control connection; only data are transferred between the client and the server.
  - HTTP is like SMTP because the data transferred between the client and the server look like SMTP messages. In addition, the format of the messages is controlled by MIME-like headers . SMTP messages are stored and forwarded, but HTTP messages are delivered immediately.
- Unlike SMTP, the HTTP messages are not destined to be read by humans; they are read and interpreted by the HTTP server and HTTP client (browser).
- The commands from the client to the server are embedded in a **request message**.
- The contents of the requested file or other information are embedded in a **response message**.
- **HTTP uses the services of TCP on well-known port 80.**

# HTTP Transaction:-

- The HTTP transaction between the client and server. Although HTTP uses the services of TCP, HTTP itself is a stateless protocol.
- The client initializes the transaction by sending a request message. The server replies by sending a response.

## HTTP Transactions

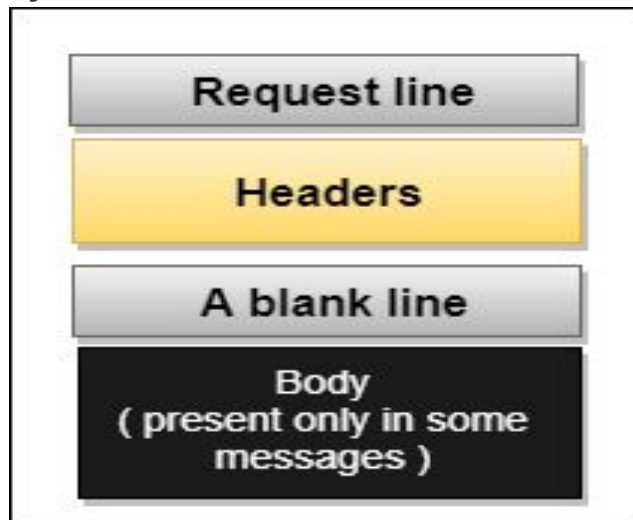


# Messages:-

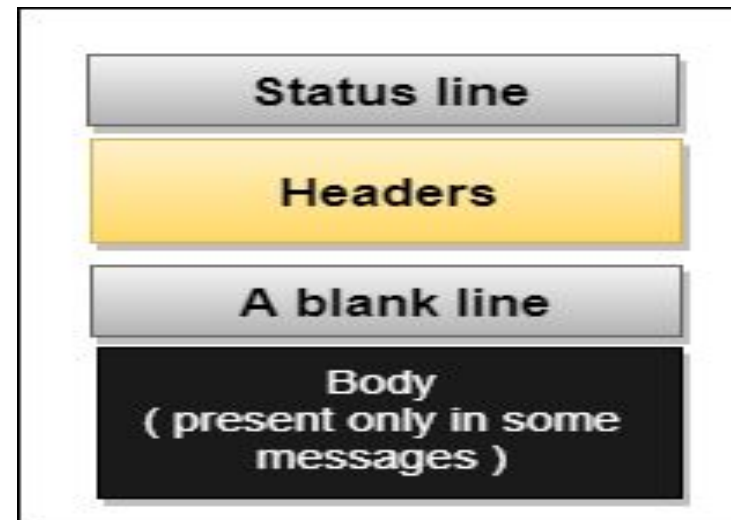
- HTTP messages are of two types: request and response. Both the message types follow the same message format.

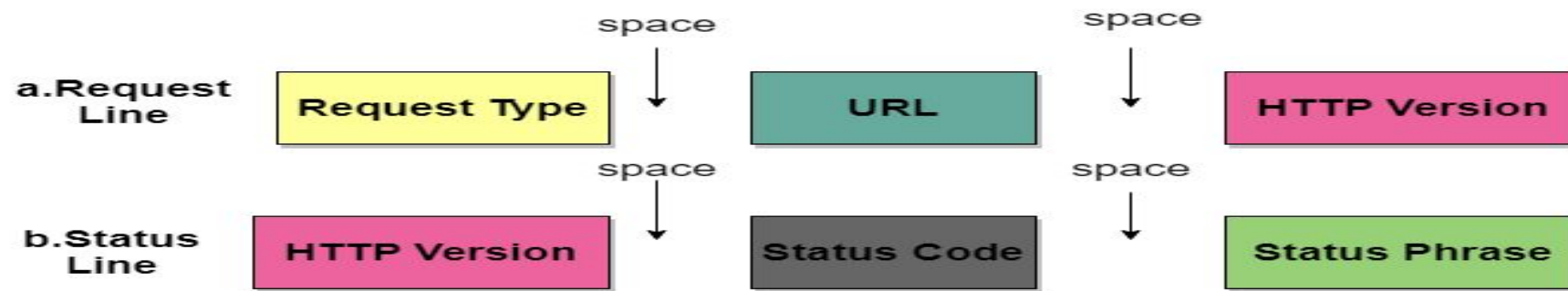


**Request Message:** The request message is sent by the client that consists of a request line, headers, and sometimes a body.



**Response Message:** The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.





- The first line in the Request message is known as the request line.
- The first line in the Response message is known as the Status line.
  - URL:-URL is a Uniform Resource locator and it is mainly a standard way of specifying any kind of information on the Internet.
  - HTTP Version:-The current version of the HTTP is 1.1.
  - Status Code:-The status code is the field of the response message. The status code consists of three digits.
  - Status Phrase:-This field is also used in the response message and it is used to explain the status code in the form of text.

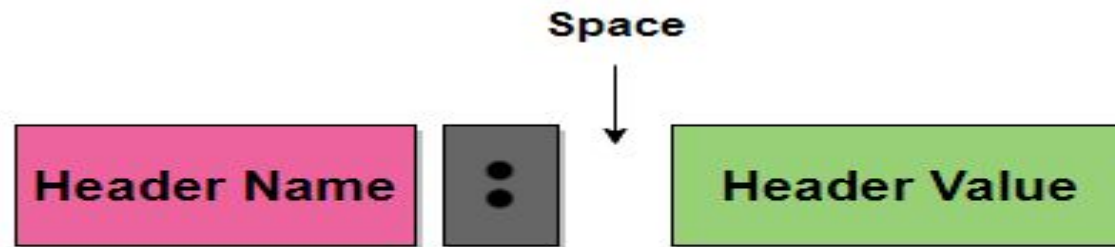
# Request Type

- This field is used in the request line. There are several request types that are defined and these are mentioned in the table given below:

Name of Method	Actions
GET	This method is used to request a document from the server.
HEAD	This method mainly requests information about a document and not the document itself
POST	This method sends some information from the client to the server.
PUT	This method sends a document from the server to the client.
TRACE	This method echoes the incoming request.
CONNECT	This method means reserved
OPTION	In order to inquire about the available options.

# Header:-

- The header is used to exchange the additional information between the client and the server. The header mainly consists of one or more header lines. Each header line has a header name, a colon, space, and a header value.
- The header line is further categorized into four:
  - *General Header* :-It provides general information about the message and it can be present in both request and response.
  - *Request Header* :-It is only present in the request message and is used to specify the configuration of the client.
  - *Response Header* :-This header is only present in the response header and mainly specifies the configuration of the server and also the special information about the request.
  - *Entity Header* :-It is used to provide information about the body of the document.



## Features of HTTP:-

The HTTP offers various features and these are as follows:

- **HTTP is simple** The HTTP protocol is designed to be plain and human-readable.
- **HTTP is stateless** Hypertext transfer protocol(HTTP) is a stateless protocol, which simply means that there is no connection among two requests that are being consecutively carried out on the same connection. Also, both the client and the server know each other only during the current requests and thus the core of the HTTP is itself a stateless one, On the other hand, the HTTP cookies provide in making use of stateful sessions.
- **HTTP is extensible** The HTTP can be integrated easily with the new functionality by providing a simple agreement between the client and the server.
- **HTTP is connectionless** As the HTTP request is initiated by the browser (HTTP client) and as per the request information by the user, after that the server processes the request of the client and then responds back to the client.



## **Advantages of HTTP:-**

1. There is no runtime support required to run properly.
2. As it is connectionless so there is no overhead in order to create and maintain the state and information of the session.
3. HTTP is usable over the firewalls and global application is possible.
4. HTTP is platform-independent.
5. HTTP reports the errors without closing the TCP connection.
6. Offers Reduced Network congestions.

## **Disadvantages of HTTP:-**

1. HTTP is too verbose.
2. It can be only used for point-to-point connections.
3. This protocol does not have push capabilities.
4. This protocol does not offer reliable exchange without the retry logic.

# HTTP Connections:-

## Persistent Connection

- TCP connection opened to server.
- Multiple objects can sent over single TCP connection between client and server.
- TCP connection closed

## Nonpersistent Connection

- TCP connection opened.
- At most one object sent over TCP connection .
- TCP connection closed

# SNMP Protocol

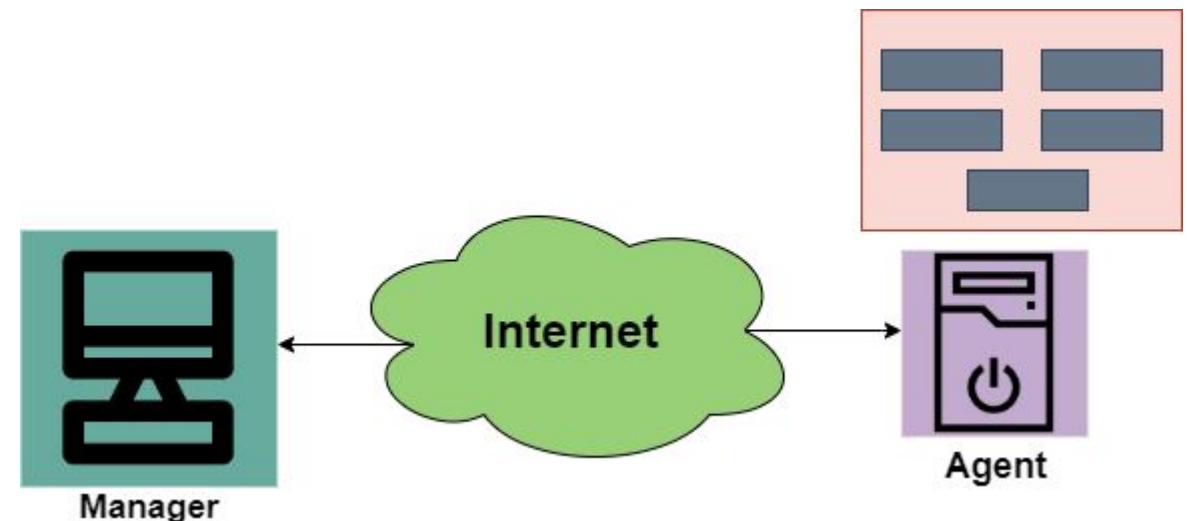
- SNMP mainly stands for Simple Network Management protocol.
- It is basically a framework that is used for managing the devices on the internet by using the TCP/IP protocol suite.
- Basically, SNMP provides a set of fundamental operations in order to monitor and maintain the Internet.
- It is an application 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.

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:

1. Collects response from the agents.
2. To acknowledge asynchronous events from the agents.
3. To set variables in the agent.
4. Queries the Agent

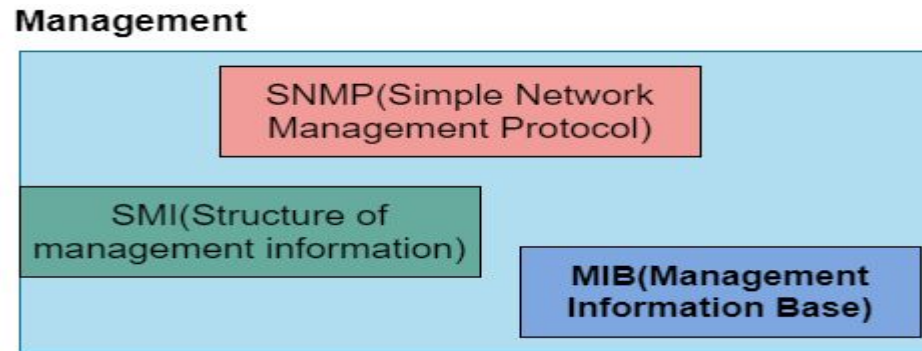
## **SNMP Agent:-**

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.

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.

**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.



**SNMP:-**It mainly defines the format of the packet that needs to be sent from the manager to the agent or vice-versa.

**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).

**MIB:-**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.

# SNMP messages:-

Different variables are:

**GetRequest** – SNMP manager sends this message to request data from the SNMP agent.

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

**GetBulkRequest** – This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.

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

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

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

**InformRequest** – It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.



## **SNMP versions –**

There are 3 versions of SNMP:

### **1. SNMPv1 –**

It uses community strings for authentication and uses UDP only.

### **2. SNMPv2c –**

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, the conclusion is the higher the version of SNMP, the more secure it will be.

# Advantages of SNMP Protocol

Given below are some of the benefits of using SNMP :

1. It is the standard network management protocol.
2. This protocol is independent of the operating system and programming language.
3. The functional design of this protocol is Portable.
4. The SNMP is basically a core set of operations and it remains the same on all managed devices. Thus SNMP supports extendibility.
5. SNMP is a universally accepted protocol.
6. It is a lightweight protocol.
7. This protocol allows distributed management access.

## **Disadvantages:-**

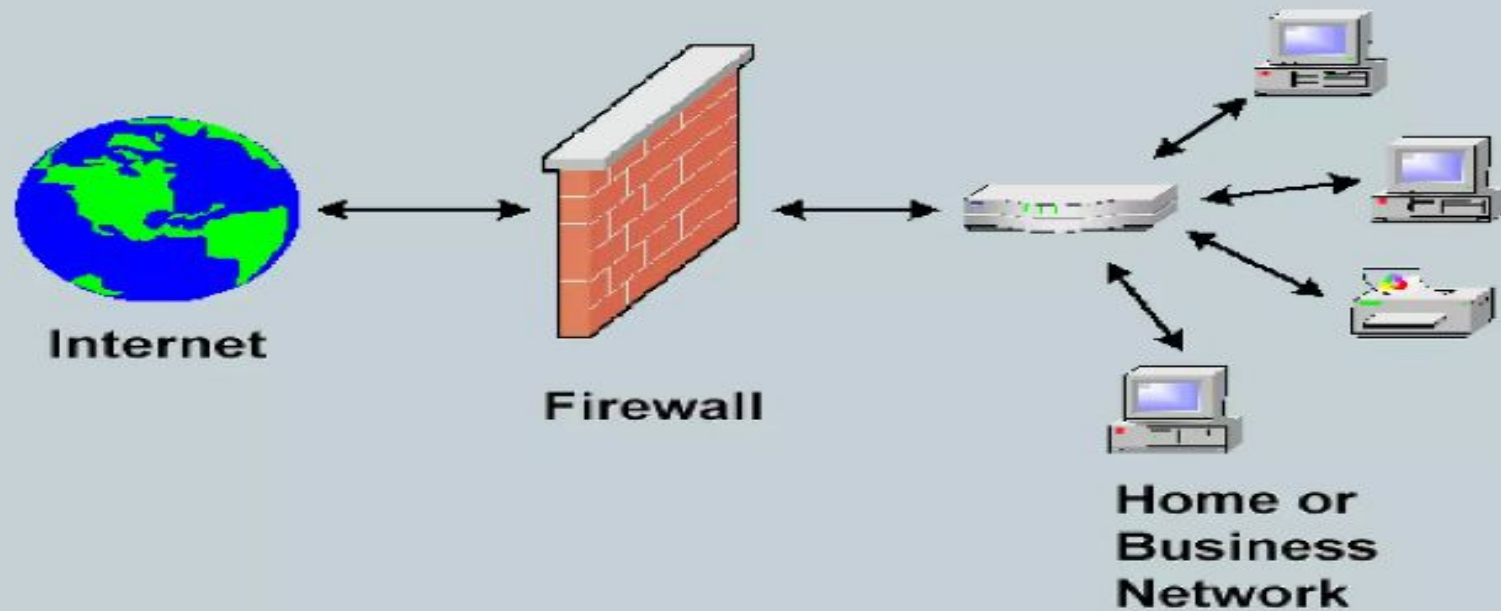
Some of the drawbacks of SNMP are as follows:


- 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.

# FIREWALLS

# What is a Firewall?

- A Firewall is simply a program or hardware device that filters the information coming through the internet connection into your private network or computer system.



- 
- **Hardware firewalls** are integrated into the router that sits between a computer and the Internet.
  - **Software firewalls** are installed on individual servers. They intercept each connection request and then determine whether the request is valid or not.

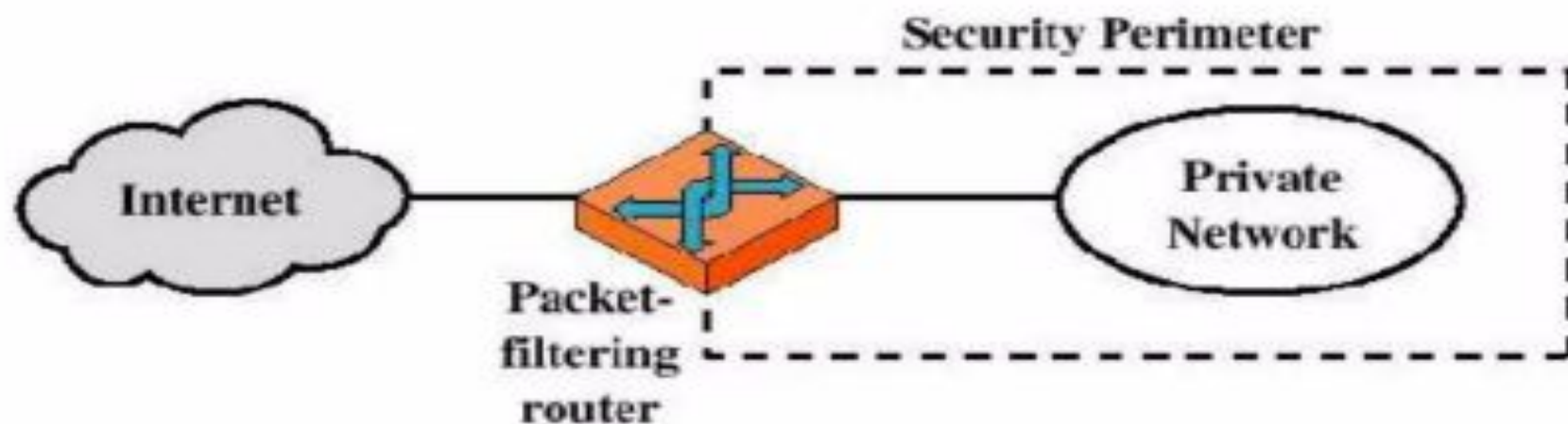
# History of Firewalls



- Firewall technology first began to emerge in the late 1980s. Internet was still a fairly new technology in terms of its global usage and connectivity.
- In 1988 an employee at the NASA Ames Research Center in California sent a memo by email to his colleagues that read, "We are currently under attack from an Internet VIRUS!"

# Types of firewalls

- Packet-filtering Router



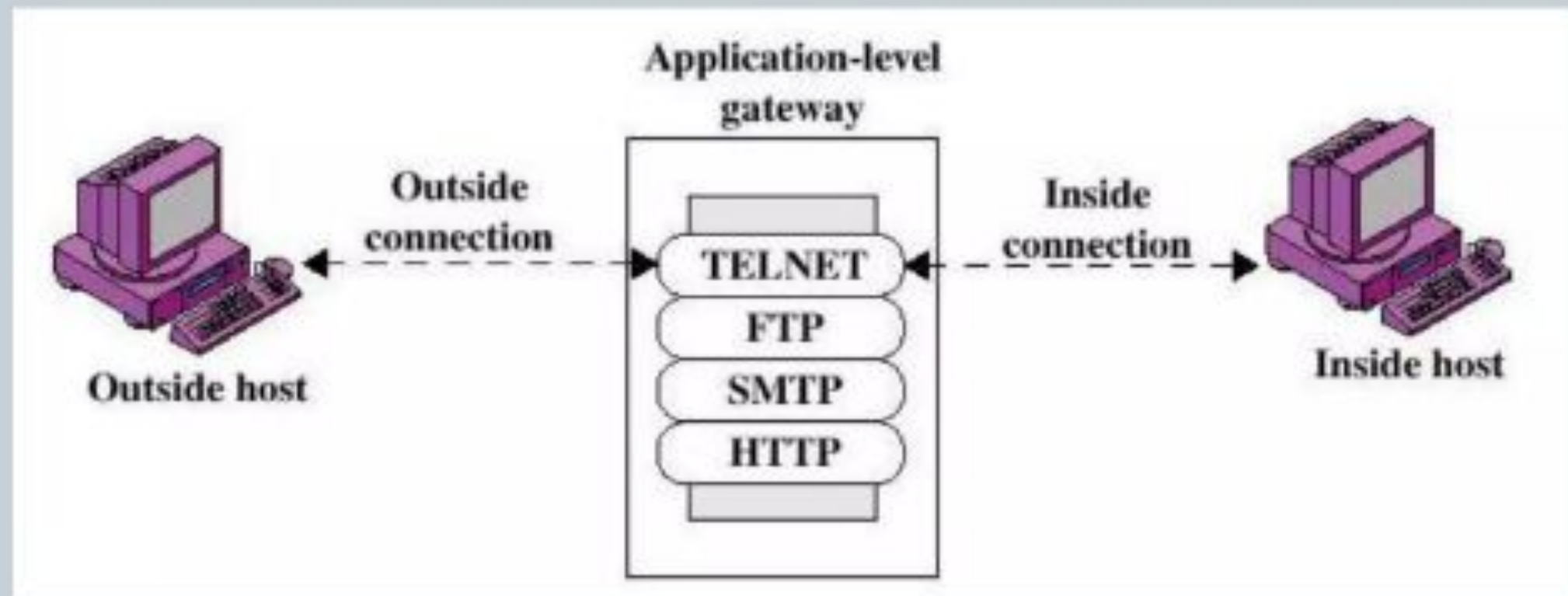


# Packet-filtering Router

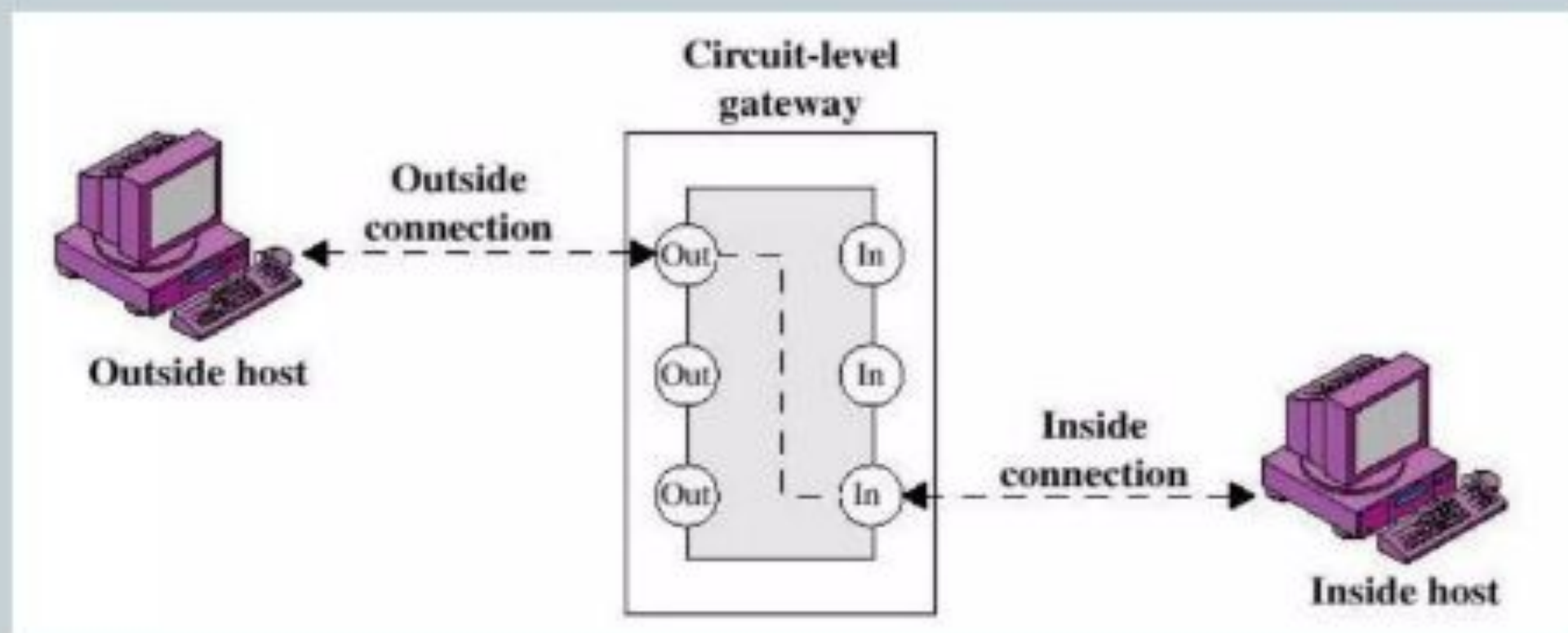


- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (discard or forward)

- Application-level Gateway



- **Circuit-level Gateway**



# Circuit-level Gateway



- Stand-alone system or
- Specialized function performed by an Application-level Gateway
- Sets up two TCP connections
- The gateway typically relays TCP segments from one connection to the other without examining the contents
- The security function consists of determining which connections will be allowed



# Advantages of firewall



- Concentration of security all modified software and logging is located on the firewall system as opposed to being distributed on many hosts;
- Protocol filtering, where the firewall filters protocols and services that are either not necessary or that cannot be adequately secured from exploitation;
- Information hiding, in which a firewall can ``hide" names of internal systems or electronic mail addresses, thereby revealing less information to outside hosts;
- Application gateways, where the firewall requires inside or outside users to connect first to the firewall before connecting further, thereby filtering the protocol;

# Disadvantages of firewall



- The most obvious being that certain types of network access may be hampered or even blocked for some hosts, including telnet, ftp, X Windows, NFS, NIS, etc.
- A second disadvantage with a firewall system is that it concentrates security in one spot as opposed to distributing it among systems, thus a compromise of the firewall could be disastrous to other less-protected systems on the subnet.

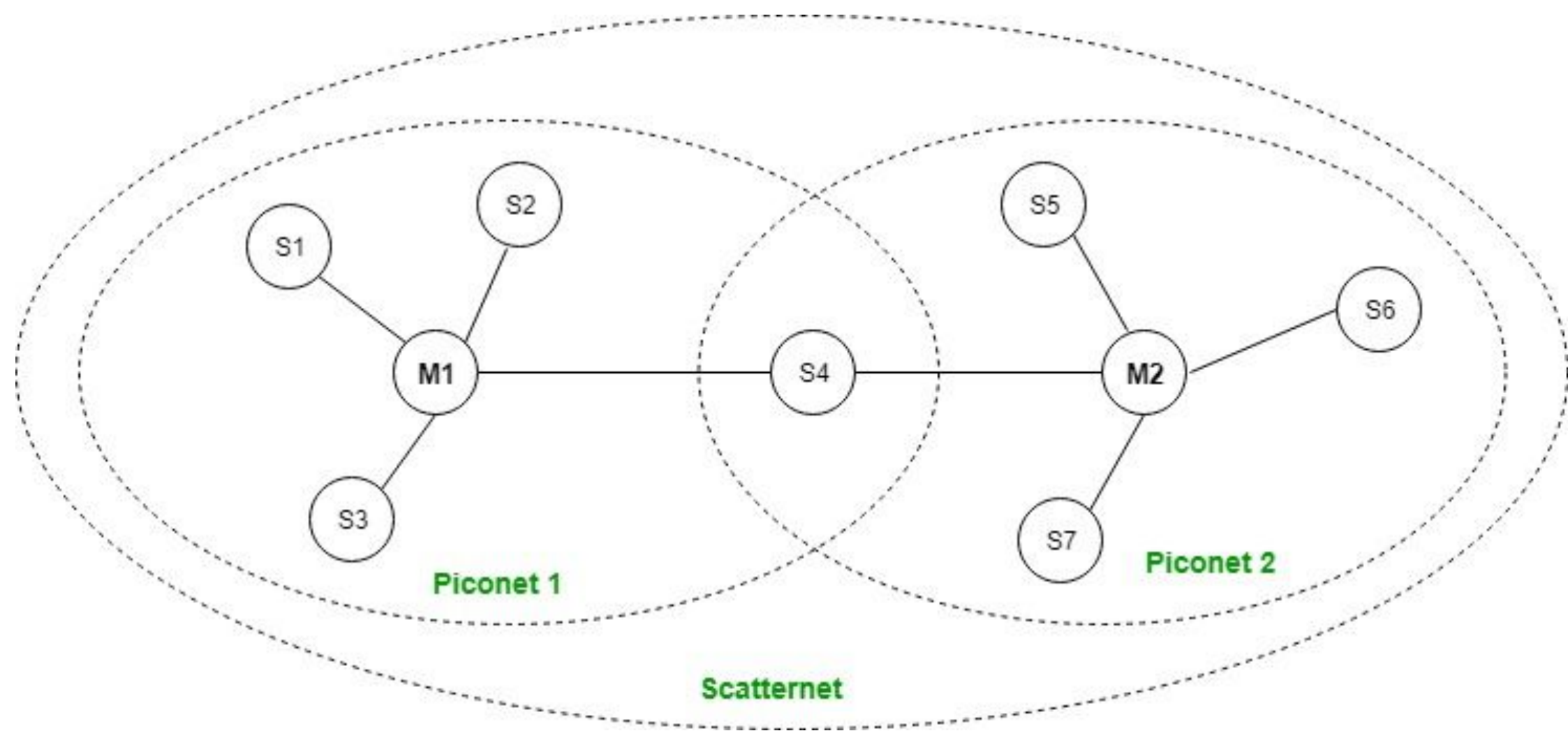
# Bluetooth :-

It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band from 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges up to 10 meters. It provides data rates up to 1 Mbps or 3 Mbps depending upon the version. The spreading technique that it uses is FHSS (Frequency-hopping spread spectrum). A Bluetooth network is called a **piconet** and a collection of interconnected piconets is called **scatternet**.

## Bluetooth Architecture:

The architecture of Bluetooth defines two types of networks:

1. Piconet
2. Scatternet





## Piconet:

Piconet is a type of Bluetooth network that contains **one primary node** called the master node and **seven active secondary nodes** called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has **255 parked nodes**, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

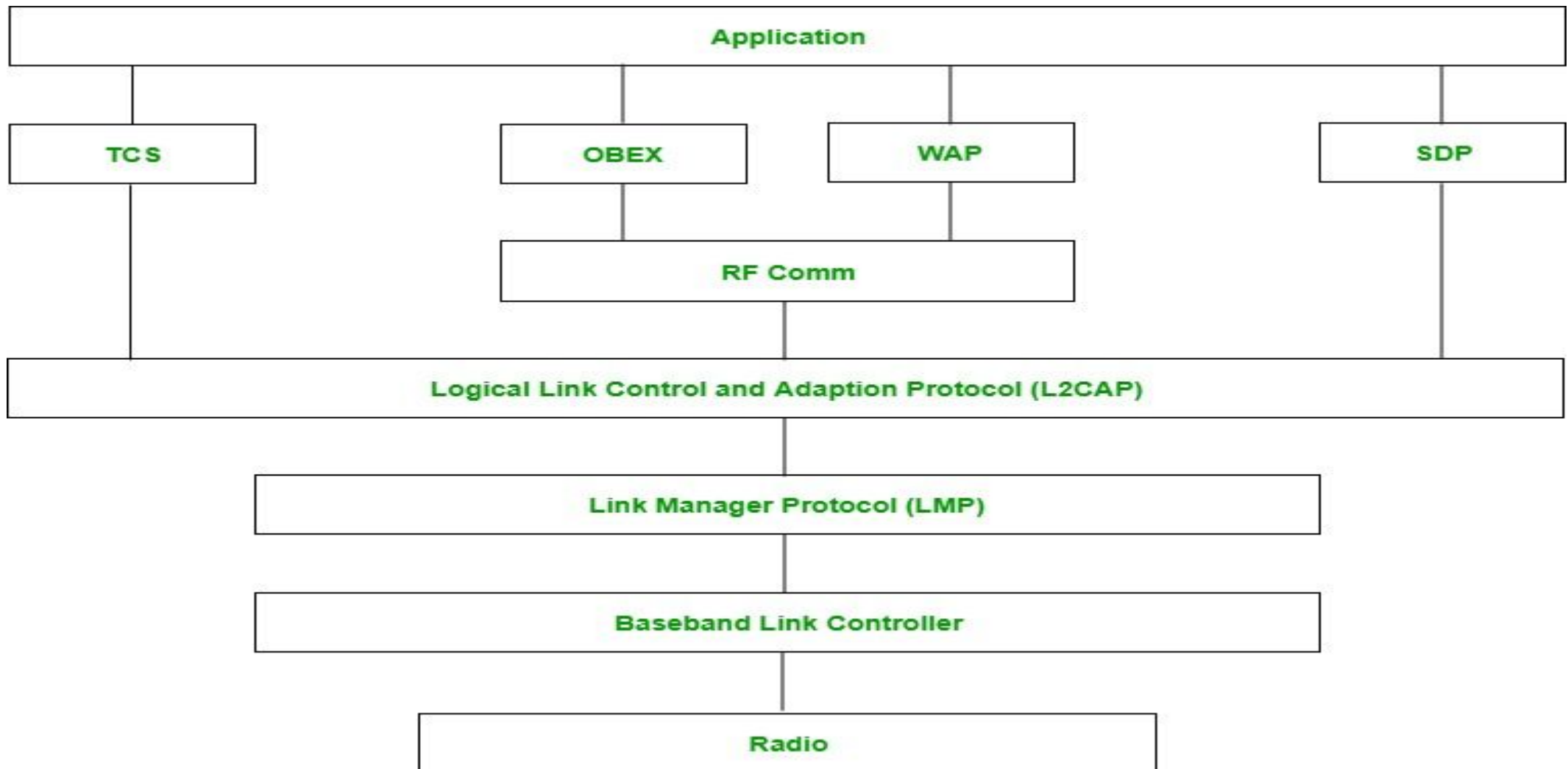
## Scatternet:

It is formed by using **various piconets**. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a slave. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.

Bluetooth Devices:- A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs

# Bluetooth Layers :-

Bluetooth uses several layers that do not exactly match those of the Internet model



1. **Radio (RF) layer:** It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of Bluetooth transceivers. It defines two types of physical links: connection-less and connection-oriented.
2. **Baseband Link layer:** The baseband is the digital engine of a Bluetooth system and is equivalent to the MAC sublayer in LANs. It performs the connection establishment within a piconet.
3. **Link Manager protocol layer:** It performs the management of the already established links which includes authentication and encryption processes. It is responsible for creating the links, monitoring their health, and terminating them gracefully upon command or failure.
4. **Logical Link Control and Adaption Protocol layer:** It is also known as the heart of the Bluetooth protocol stack. It allows the communication between upper and lower layers of the Bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs segmentation and multiplexing.
5. **SDP layer:** It is short for Service Discovery Protocol. It allows discovering the services available on another Bluetooth-enabled device.

1. **RF comm layer:** It is short for Radio Frontend Component. It provides a serial interface with WAP and OBEX. It also provides emulation of serial ports over the logical link control and adaption protocol(L2CAP). The protocol is based on the ETSI standard TS 07.10.
2. **OBEX:** It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.
3. **WAP:** It is short for Wireless Access Protocol. It is used for internet access.
4. **TCS:** It is short for Telephony Control Protocol. It provides telephony service. The basic function of this layer is call control (setup & release) and group management for gateway serving multiple devices.
5. **Application layer:** It enables the user to interact with the application.

## **Advantage:**

- Low cost.
- Easy to use.
- It can also penetrate through walls.
- It creates an Ad-hoc connection immediately without any wires.
- It is used for voice and data transfer.

## **Disadvantages:**

- It can be hacked and hence, less secure.
- It has a slow data transfer rate: of 3 Mbps.
- It has a small range: 10 meters.
- Bluetooth communication does not support routing.
- The issues of handoffs have not been addressed.



## **Applications:**

- Used in laptops, and in wireless PCs.
- In printers.
- In wireless headsets.
- Connecting digital camera wirelessly to a mobile phone.
- Data transfer from one cell phone to other cell phone or computer.