## Application layer:

enables the user, whether human or software, to access the network.
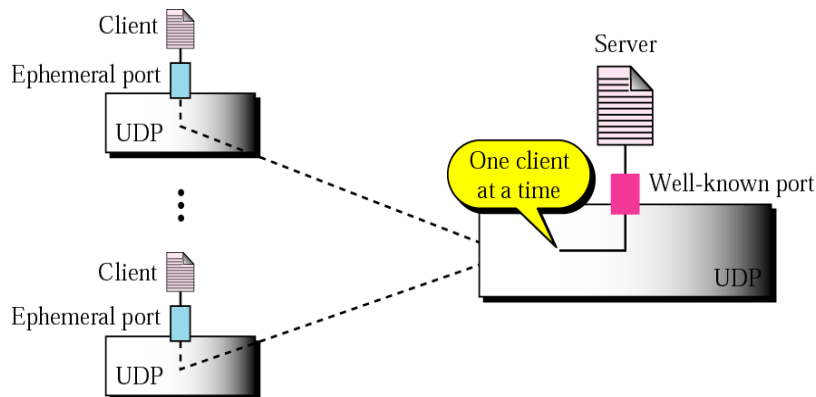- It provides user interfaces and support for services such as electronic mail, file access and transfer, access to system resources, surfing the world wide web, and network management.
- A user at a local site wants to receive a service from a computer at a remote site

Two approaches : client server & Peer to peer
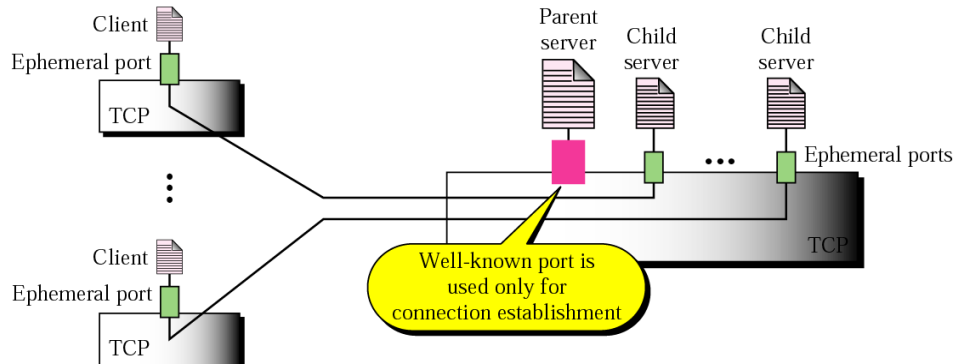
Client

Server

Client
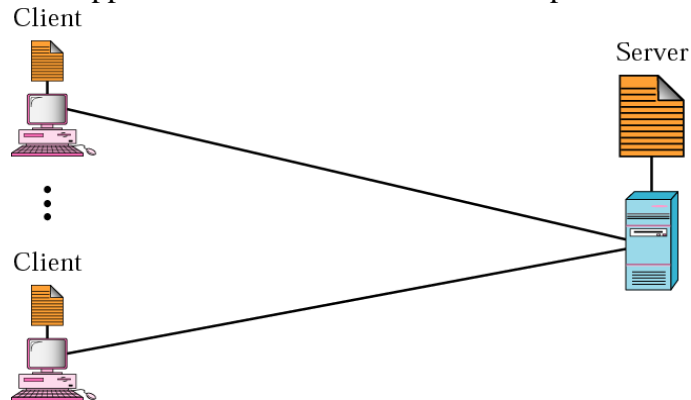
An *iterative* server can process only one request at a time; it receives a request, processes it, and sends the response to the requestor before it handles another request. A concurrent server, on the other hand, can process many requests at the same time and thus can share its time between many requests
- Connectionless iterative server

Client
Ephemeral port
UDP

Server

One client at a time
Well-known port
UDP

Client
Ephemeral port
UDP

- Connection-oriented concurrent server

Client
Ephemeral port
TCP

Parent server
Child server
Child server

Ephemeral ports

Well-known port is used only for connection establishment

TCP

Client
Ephemeral port
TCP

World Wide Web (WWW)

WWW project was initiated by CERN (European Laboratory for Particle Physics) to create a system to manage distributed resources necessary for scientific research

Architecture

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*. Each site holds one or more documents, referred to as Web pages. Each **Web page**, , can contain some links to other Web pages in the same or other sites. Thus, a Web page can be **simple** or **composite**. A simple Web page has no link to other Web pages; a composite Web page has one or more links to other Web pages. Each Web page is a file with a name and address.
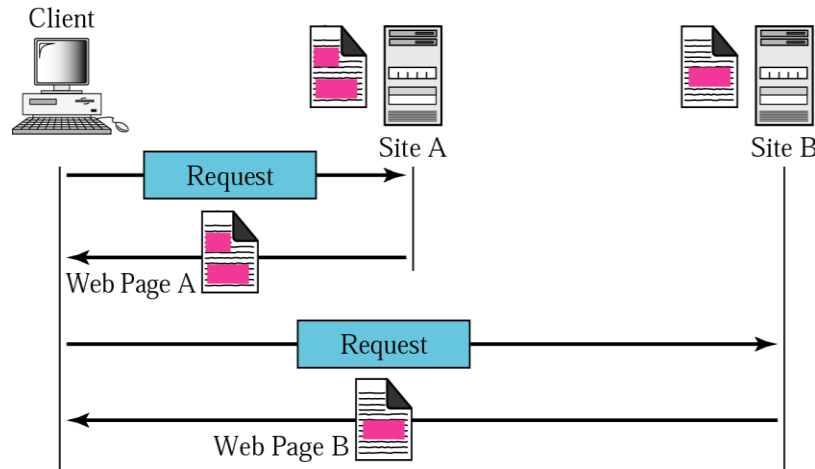
Each site holds one or more documents, referred to as Web pages. Each **Web page**, , can contain some links to other Web pages in the same or other sites. Thus, a Web page can be **simple** or **composite**. A simple Web page has no link to other Web pages; a composite Web page has one or more links to other Web pages. Each Web page is a file with a name and address.

Web pages are written using HTML and web pages are transferred from web site to client browser using HTTP.

Hypertext and Hypermedia

Hypertext :means creating documents that refer to other documents. In a hypertext document, a part of text can be defined as a link to another document. When a hypertext is viewed with a browser, the link can be clicked to retrieve the other document.

Hypermedia is a term applied to document that contains links to documents containing text , graphics, video, or audio.

Web Client (Browser)

Lot of vendors offer commercial **browsers** that interpret and display a Web document, and all of them use nearly the same architecture.

Eg (Internet Explorer, chrome, edge & Firefox)

Each browser usually consists of three parts: a controller, client protocol, and interpreters.
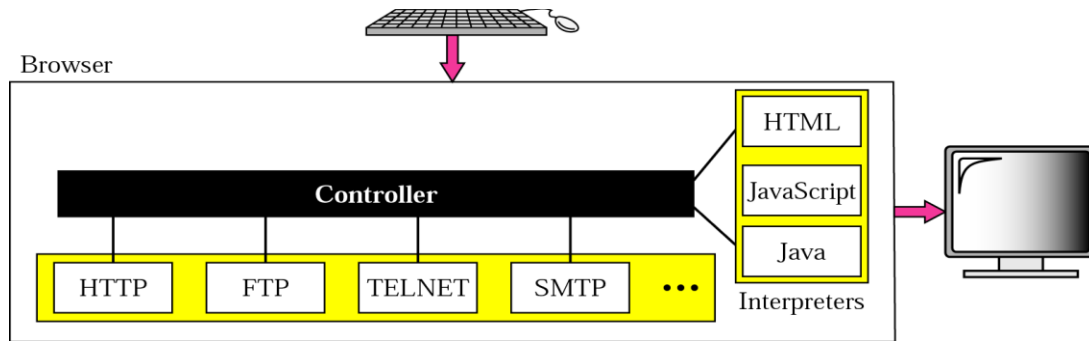
- The controller receives input from the keyboard or the mouse and uses the client programs to access the document.
- After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols described previously such as FTP, or TELNET, or HTTP .

The interpreter can be HTML, Java, or JavaScript, depending on the type of document

Web Server

The Web pages are stored at the server. Each time a client request arrives, the corresponding document is sent to the client.

Eg of Web servers : Apache HTTP ,Apache tomcat , Microsoft Internet Information Server (IIS) **,** lighttpd , Jagsaw , NGINX ,

URL

Uniform Resource Locator (URL)

A client that wants to access a Web page needs the file name and the address of that Web page. To facilitate the access of documents distributed throughout the world, HTTP uses **uniform resource locator (URL)**

URL is a standard locator 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 application program used to retrieve the document. Many different protocols can retrieve a document; among them are Gopher, FTP, HTTP, News, and TELNET. The most common today is HTTP.

The **host** is the domain name of the computer on which the information is located. Web pages are usually stored in computers, and computers are given domain name

aliases that usually begin with the characters "www". But This is not mandatory, as the host can have any domain name.

The URL can optionally contain the **port** number of the server

Path is the pathname of the file where the information is located. path can contain slashes which separate the directories from the subdirectories and files. In other words, the path defines the complete file name where the document is stored in the directory system.
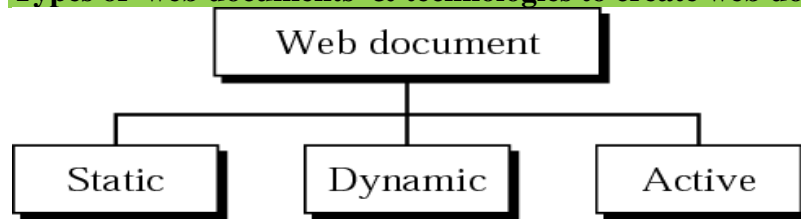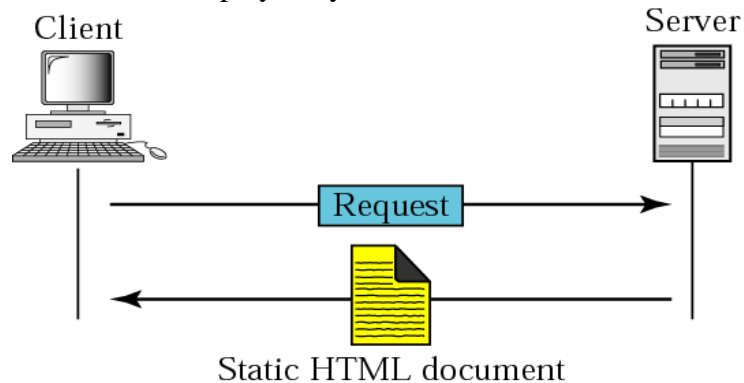
Type of webpage Need to be declared at the time of creation of webpage.

1. Static documents

are fixed-content documents that are created and stored in a server. The client can get a copy of the document only . We can can change document at server , client can't change it &
Document is displayed by client browser

Static documents are prepared using one of the several languages: Hypertext Markup Language (HTML), Extensible Markup Language (XML), Extensible Style Language (XSL), and Extended Hypertext Markup Language (XHTML)

2. Dynamic Documents

A **dynamic document** is created by a Web server whenever a client browser requests the document.

When a request arrives, the Web server runs an application program or a script that creates the dynamic document. The server returns the output of the program or script as a response to the browser that requested the document. Because a fresh document is created for each request, the contents of a dynamic document may vary from one request to another.

Example : retrieval of the time and date from a server. (every time the server process has to execute to send response)

dynamic documents are prepared using **CGI**

Scripting Technologies for Dynamic Documents

The problem with CGI technology is the inefficiency that results if part of the dynamic document that is to be created is fixed and not changing from request to request

Eg : in a web apge which is displaying cost & quantity of various items. Here items name can remain fixed. Only stock & cost can change

items name	Stock	Cost per unit

If we use CGI, the program must create an entire document each time a request is made.
The solution is to create a file containing the fixed part of the document using HTML and embed a script, a source code, that can be run by the server to provide the stock & cost.
most common scripting languages are:

- **Hypertext Preprocessor (PHP),** which uses the Perl language;

- **Java Server Pages (JSP),** which uses the Java language for scripting;
- **Active Server Pages (ASP),** a Microsoft product, which uses Visual Basic language for scripting;
- **ColdFusion,** which embeds SQL database queries in the HTML document.

3. Active Documents
For some applications, we need a program or a script to be run at the client site. These are called active documents.

For example, suppose we want to run a program that creates animated graphics on the screen or a program that interacts with the user.

The program definitely needs to be run at the client site where the animation or interaction takes place. When a browser requests an active document, the server sends a copy of the document or a script. The document is then run at the client (browser) site.

Java Applets

One way to create an active document is to use **Java applets. Java** is a combination of a high-level programming language, a run-time environment, and a class library that allows a programmer to write an active document (an applet) and a browser to run it. It can also be a stand-alone program that doesn't use a browser

An **applet** is a program written in Java on the server. It is compiled and ready to be run. The document is in bytecode (binary) format. The client process (browser) creates an instance of this applet and runs it. A Java applet can be run by the browser in two ways. In the first method, the browser can directly request the Java applet program in the URL and receive the applet in binary form. In the second method, the browser can retrieve and run an HTML file that has embedded the address of the applet as a tag.
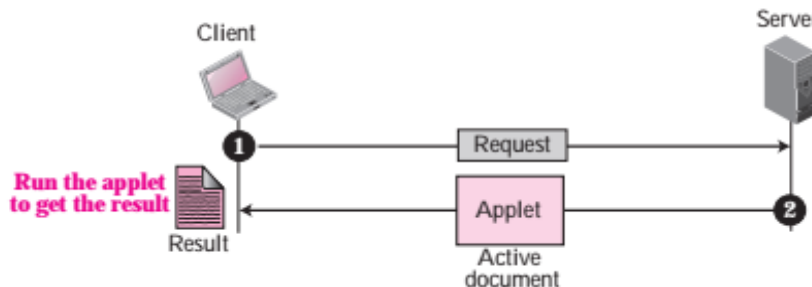
JavaScript

The idea of scripts in dynamic documents can also be used for active documents. If the active part of the document is small, it can be written in a scripting language; then it can be interpreted and run by the client at the same time. The script is in source code (text) and not in binary form. The scripting technology used in this case is usually JavaScript.

JavaScript, which bears a small resemblance to Java, is a very high level scripting language developed for this purpose.
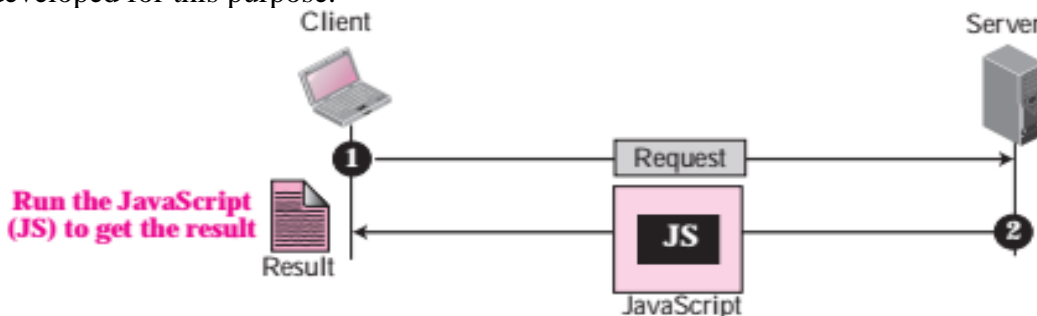
Common Gateway Interface (CGI)

is a technology that creates and handles dynamic documents. CGI is a set of standards that defines how a dynamic document is written, how data are input to the program, and how the output result is used.

CGI is not an another language , it allows programmers to use any of several languages such as C, C++, Bourne Shell, Korn Shell, C Shell, Tcl, or Perl.

The only thing that CGI defines is a set of rules and terms that the programmer must follow. The term **common** indicates that the standard defines a set of rules that is common to any language or platform. The term **gateway** means that a CGI program can be used to access other resources such as databases, graphic packages, and so on. The term **interface** means that there is a set of predefined terms, variables, calls, and so on that can be used in any CGI program
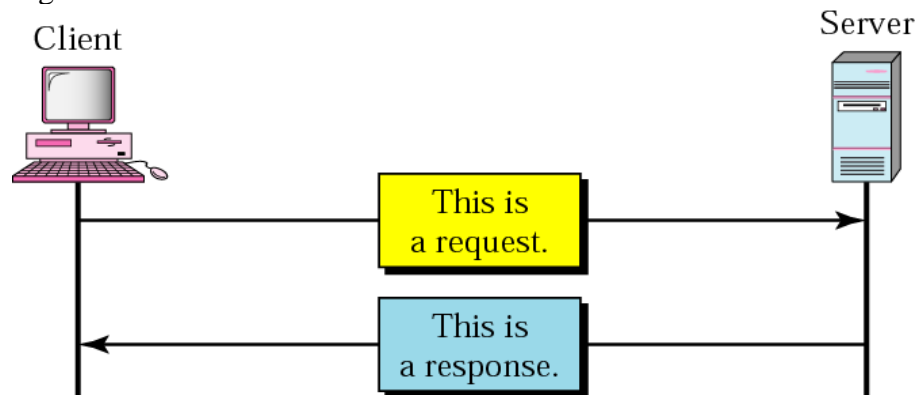
Hypertext Transfer Protocol (HTTP)

This protocol is used mainly to access data (i.e. web pages) on the World Wide Web.

HTTP functions like a combination of FTP and SMTP

HTTP uses the services of TCP on well-known port 80.

HTTP Transaction

Figure the HTTP transaction between the client and server.


Although HTTP uses the services of TCP, HTTP itself is a stateless protocol, which means that the server does not keep information about the client. The client initializes the transaction by sending a request. The server replies by sending a response.

A request message (sent by clent) : consists of a request line, a header, and sometimes a body.

Request message
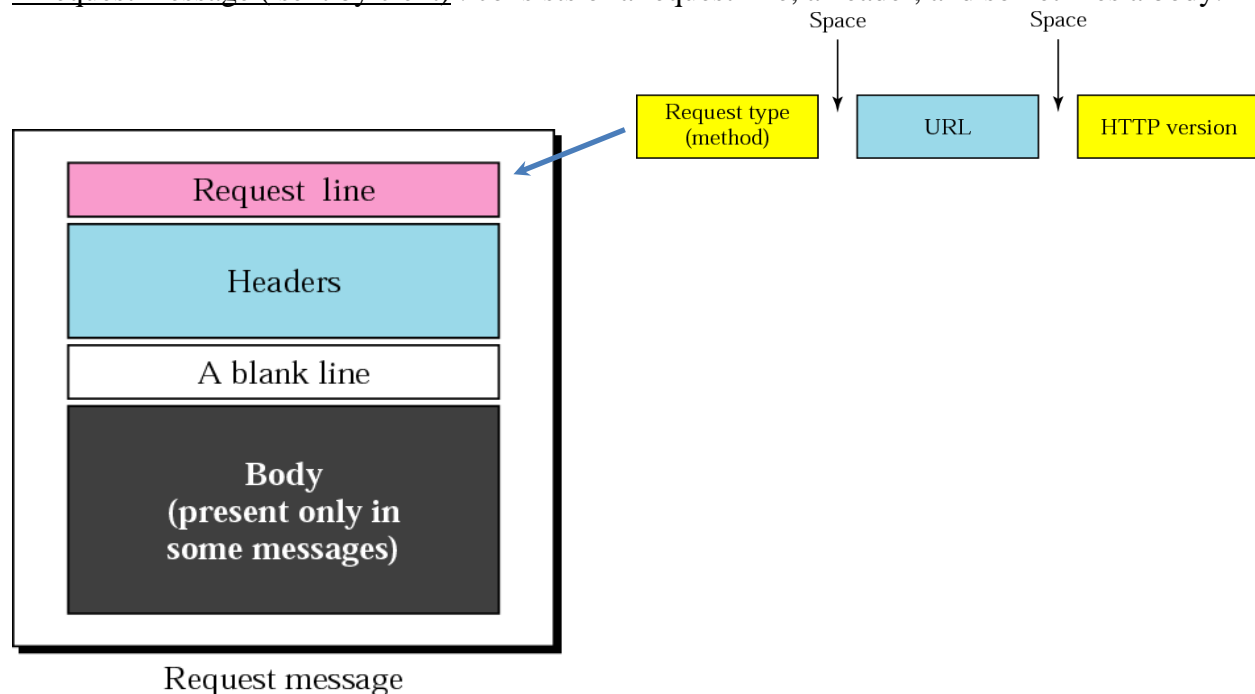
Request line consists of

Space   Space

Request type (method)	URL	HTTP version
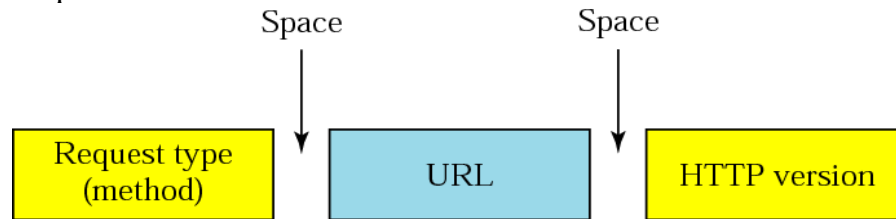
Request type (Methods)

Method	Action
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Reserved
DELETE	Remove the Web page
OPTIONs	Enquires about available options

URL, as discussed earlier is the address and name of corresponding Web page.
The third field, version, gives the version of the protocol; the most current version of HTTP is 3.0

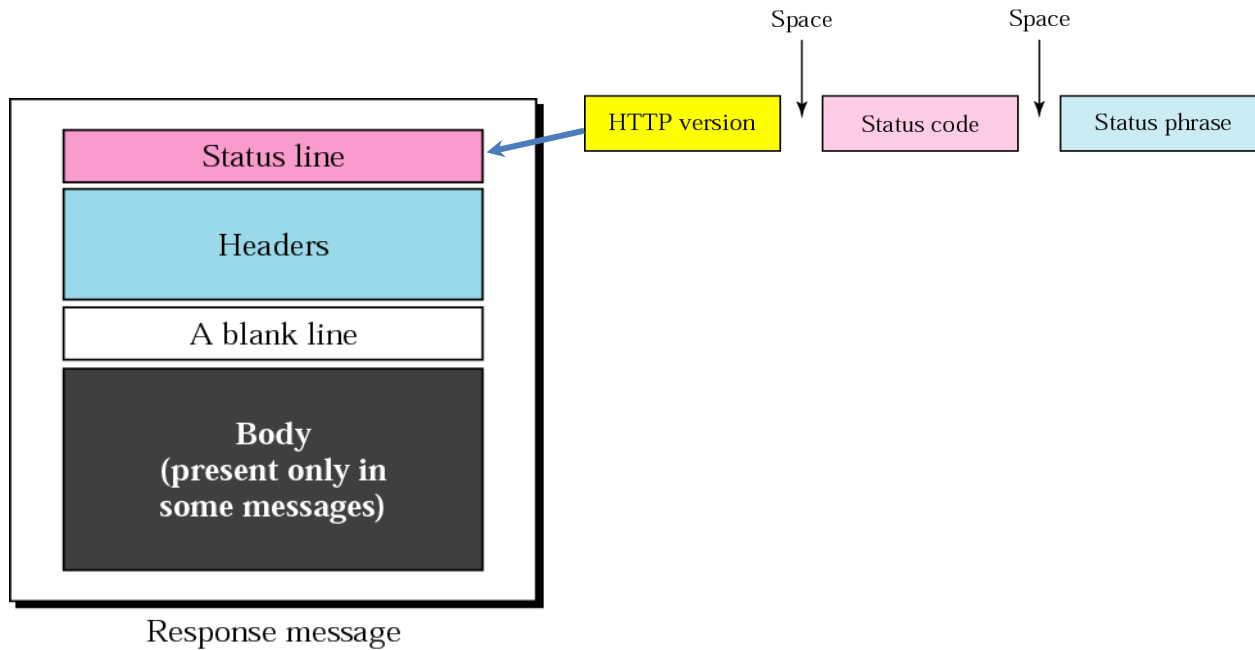Header Lines In Request Message
 After the request line, we can have zero or more **request header** lines.

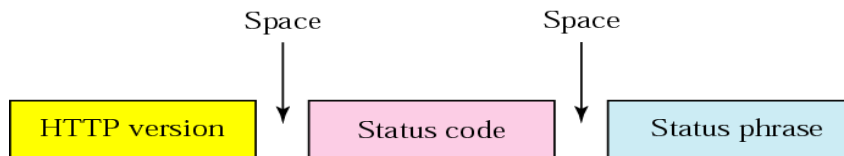| Header	Description
User-agent	Identifies the client program
Accept	Shows the media format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-encoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorization	Shows what permissions the client has
Host	Shows the host and port number of the client
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Cookie	Returns the cookie to the server
If-Modified-Since	Returns the cookie to the server

Each header line sends additional information from the client to
the server. For example, the client can request that the document be sent in a special format.
A response message (sent by server)
consists of a status line, header lines, a blank line and sometimes a body.

Space   Space

| HTTP version | | Status code | | Status phrase |

Status line

Headers

A blank line

**Body
(present only in
some messages)**

Response message

Status line

Space   Space

| HTTP version | | Status code | | Status phrase |

    The first field defines the version of HTTP protocol

    The status code field defines the status of the request. It consists of three digits.

    100 range are only informational,

    200 range indicate a successful request.

    300 range redirect the client to another URL,

    400 range indicate an error at the client site.

    500 range indicate an error at the server site

The third field status phrase indicates the short description of status

Some examples of status codes

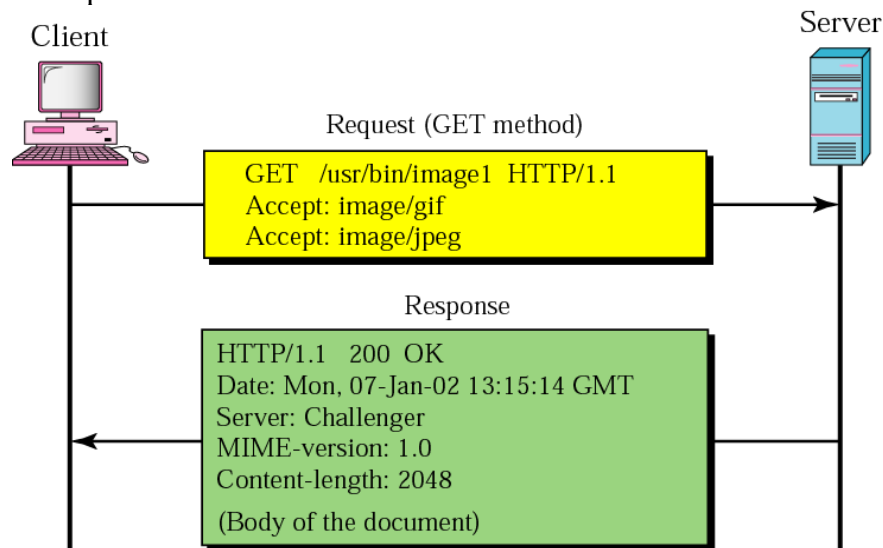| Client Error		
400	Bad request	There is a syntax error in the request.
401	Unauthorized	The request lacks proper authorization.
403	Forbidden	Service is denied.
404	Not found	The document is not found.
405	Method not allowed	The method is not supported in this URL.
406	Not acceptable	The format requested is not acceptable.
Server Error		
500	Internal server error	There is an error, such as a crash, at the server site.

Header Lines In Response Message

After the status line, we can have zero or more response header lines. Each header line sends additional information from the server to the client.

Some response headers

Header	Description
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Server	Gives information about the server
Set-Cookie	The server asks the client to save a cookie
Content-Encoding	Specifies the encoding scheme
Content-Language	Specifies the language
Content-Length	Shows the length of the document
Content-Type	Specifies the media type
Location	To ask the client to send the request to another site
Accept-Ranges	The server will accept the requested byte-ranges
Last-modified	Gives the date and time of the last change

Example

Client   Server

Request (GET method)

```
GET   /usr/bin/image1  HTTP/1.1
Accept: image/gif
Accept: image/jpeg
```

Response

```
HTTP/1.1   200  OK
Date: Mon, 07-Jan-02 13:15:14 GMT
Server: Challenger
MIME-version: 1.0
Content-length: 2048

(Body of the document)
```

example retrieves a document. GET method to retrieve an image with the path /usr/bin/image1. HTTP version (1.1). client can accept images in GIF and JPEG format. The request does not have a body.
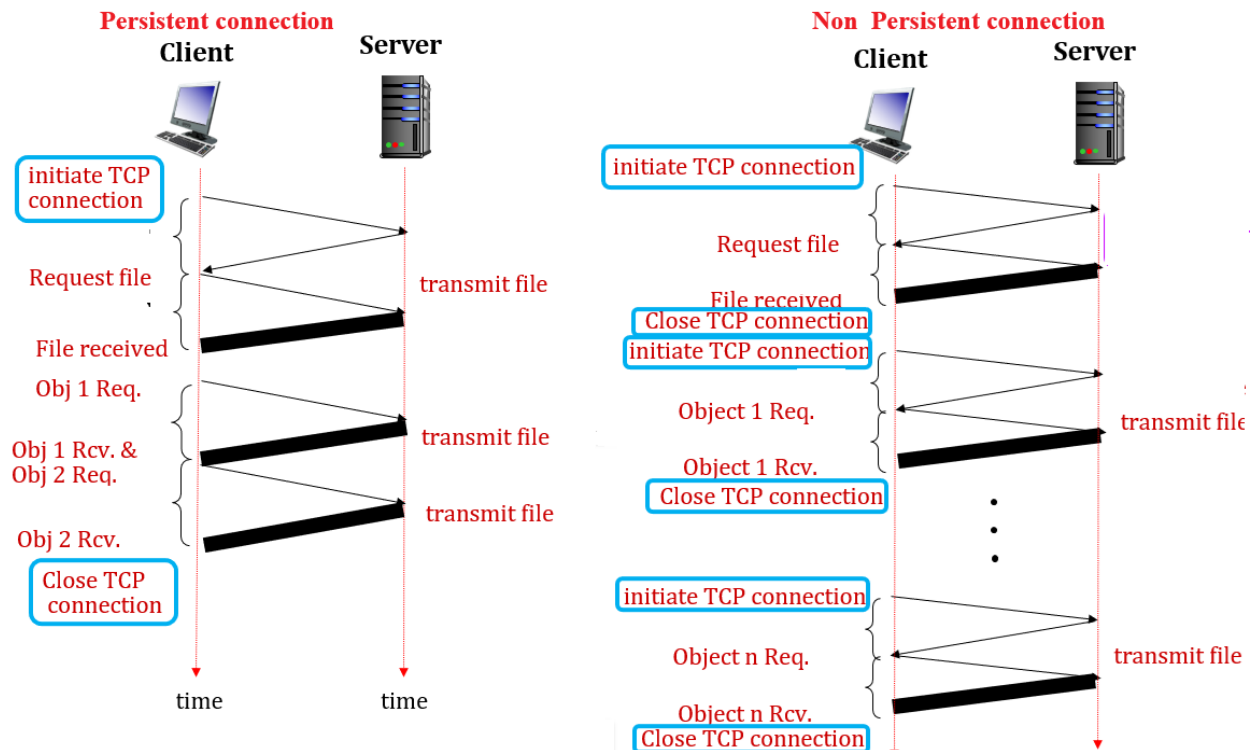
The response message contains the status line and 4 lines of header. The header lines define the date, server, MIME version, and length of the document. The body of the document follows the header

What is the difference between persistent & non persistent HTTP?

A non-persistent connection is closed by the server after the server sends the requested object to the client. The connection is used exactly for one request and one response. So For downloading multiple objects, it requires multiple TCP connections. This was in HTTP version 1.0

In a persistent connection, The server now keeps the TCP connection open for a certain period of time after sending a response. The connection can be used many requests. So For downloading multiple objects, it requires only one connection .There are two types of Persistent HTTP Connection: Persistent HTTP without pipelining and Persistent HTTP with pipelining.

This was in HTTP version 1.1 onwards

Persistent connection

Client   Server

- initiate TCP connection
- Request file   transmit file
- File received
- Obj 1 Req.
- Obj 1 Rcv. & Obj 2 Req.   transmit file
- Obj 2 Rcv.   transmit file
- Close TCP connection

time   time

Non Persistent connection

Client   Server

- initiate TCP connection
- Request file
- File received
- Close TCP connection
- initiate TCP connection
- Object 1 Req.   transmit file
- Object 1 Rcv.
- Close TCP connection
- initiate TCP connection
- Object n Req.   transmit file
- Object n Rcv.
- Close TCP connection

Cookies

A **cookie** is **information saved by your web browser**. When you visit a website, the site may place a cookie on your web browser so it can recognize your device in the future. If you return to that site later on, it can read that cookie to remember you from your last visit and keep track of you over time.

Since the data in cookies doesn't change, **cookies themselves aren't harmful**. They can't infect computers with viruses or other malware. However, some cyber attacks can hijack cookies and enable access to your browsing sessions. The danger lies in their ability to track individuals' browsing histories.

Accepting cookies will give you the best user experience on the website, while declining cookies could potentially interfere with your use of the site. For example, online shopping. Cookies enable the site to keep track of all of the items that you've placed in your cart while you continue to browse.

Cookies are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience.

Data stored in a cookie is created by the server upon your connection. This data is labeled with an ID unique to you and your computer.

When the cookie is exchanged between your computer and the network server, the server reads the ID and knows what information to specifically serve to you.

It can be useful in following
❑ Websites are being used as *electronic stores* that allow users to browse through the store, select wanted items, put them in an electronic cart, and pay at the end with a credit card.
❑ Some websites need to allow access to *registered clients* only.
❑ Some websites are used as *portals:* The user selects the Web pages he wants to see.
❑ Some websites are just *advertising*

Web Caching: Proxy Server

A proxy server is a computer that keeps copies of responses to recent requests.
The HTTP client sends a request to the proxy server. The proxy server checks its cache.
If the response is already stored in the cache (previous response) , the proxy server sends the copy from its cache.
If the response is not found in the cache, the proxy server sends the request to the corresponding server. Incoming responses are sent to the proxy server and stored for future requests from other clients.
The proxy server reduces the load on the original server, decreases traffic, and improves speed.
The proxy servers are normally located at the client site

4 types of web cache
1. Site cache
- A site cache or page cache stores website data the first time a webpage is loaded. Each time a user returns to your website, saved elements are quickly accessed and displayed to visitors.
- This is a type of client-side caching, which means that all the stored elements are controlled by the end-user. As a website owner, the only say you have is how long content remains in the cache.
site caching is ideal for websites with a lot of static content. Since your site rarely changes, users will be able to continue loading your pages quickly while still seeing the latest version of your site.
2 Browser cache
- Browser caching is a type of site caching built into the end-user's web browser. Website elements are stored by the browser on your visitor's computer and grouped with other files associated with your content. A browser cache can contain HTML pages, CSS stylesheets, images, and other multimedia content.
- Browser caching overlaps with site caching because they are both client-side systems. The primary difference is that the browser, rather than the end-user, controls the cache. All browsers have a cache that flushes out old files without any need for user intervention.
3. Server cache
- Server cache is an umbrella term covering a number of different types of caching. This includes Content Delivery Network (CDN) caching, object caching, and opcode caching. Each stores different content on your website's server. This type of caching is administered by website owners without any input from end-users.

- Server caching is one of the best methods for reducing server loads. When a request is made, the server checks its temporary storage for the necessary content before processing it the request in full.
- If the requested content is available in the server cache, it will be returned to the browser right away. This enables your server to handle more traffic and return your webpages faster.

4. Micro cache
- Another type of caching that many website owners might not be aware of is micro caching. This method stores content for very short periods of time. It generally saves static versions of dynamic elements for up to 10 seconds. As this is a type of site cache, it's controlled by end-users with limited input from website owners.
- Micro caching is not a common type of cache because of the short storage time. The sites that benefit from this form of caching also fit into a small profile. They're typically high traffic and feature rapidly changing content, such as the constantly updating graphs on currency exchange and stock websites.

Advantages Web caching:
- Faster delivery of Web objects to the end user.
- Reduces bandwidth needs and cost. It benefits the user, the service provider and the website owner.
- Reduces load on the website servers.

Domain Name System (DNS)

The Domain Name System (DNS) is the phonebook of the Internet.
DNS, or the Domain Name System, translates human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example, 192.0.2.44).
Why is it required ?
TCP/IP protocols use the IP address for each host, which uniquely identifies the a host in the Internet.
However, people prefer to use names instead of numeric addresses. Therefore, we need a system that can map a name to an IP address or an IP address to a name
In this method, the host that needs mapping can contact the closest computer holding the needed information. This method is used by the **Domain Name System (DNS).**

DNS steps:
Steps
1. The user passes the host name eg google.com to the file transfer client.
2. The file transfer client passes the host name to the DNS client.
3. each computer, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query
4. The DNS server responds with the IP address of the desired file transfer server.
5. The DNS client passes the IP address to the file transfer client.
6. The file transfer client now uses the received IP address to access the file transfer server.
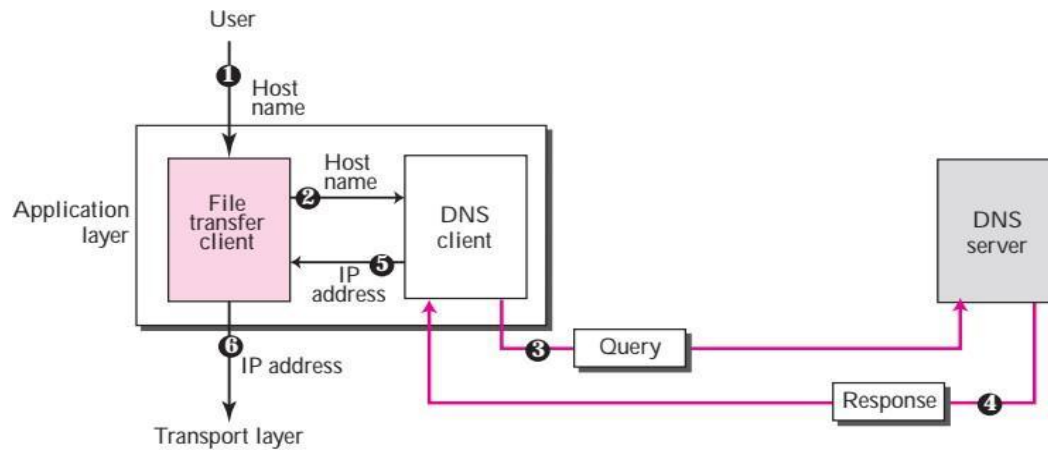
Domain Name Space

In this the domain names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127
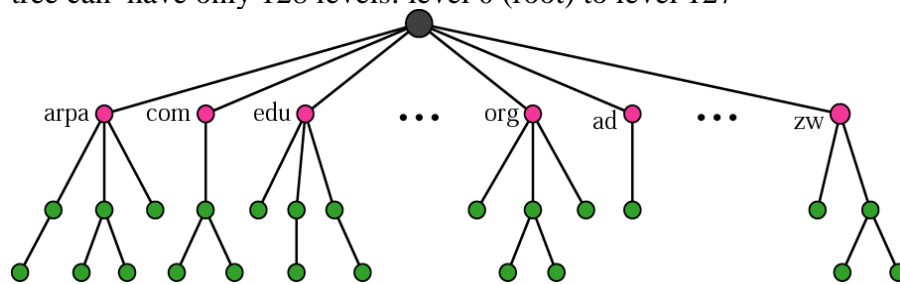

Label

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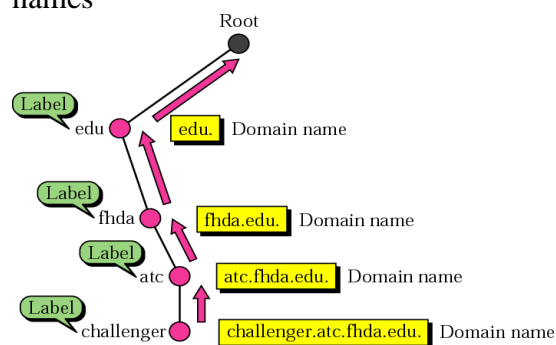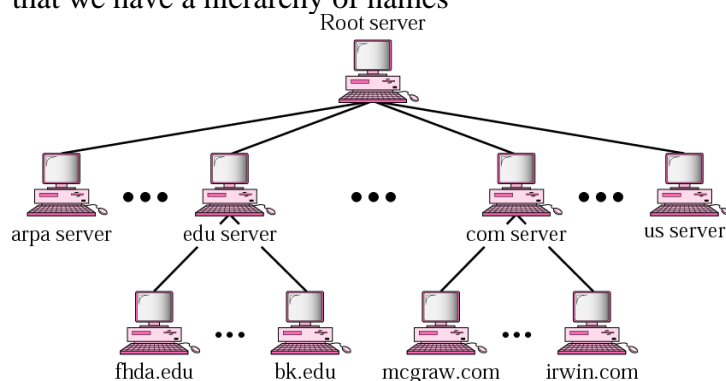

Domain

A **domain** is a subtree of the domain name space. The name of the domain is the name of the node at the top of the subtree. Figure shows some domains. Note that a domain may itself be divided into domains (or **subdomains**)
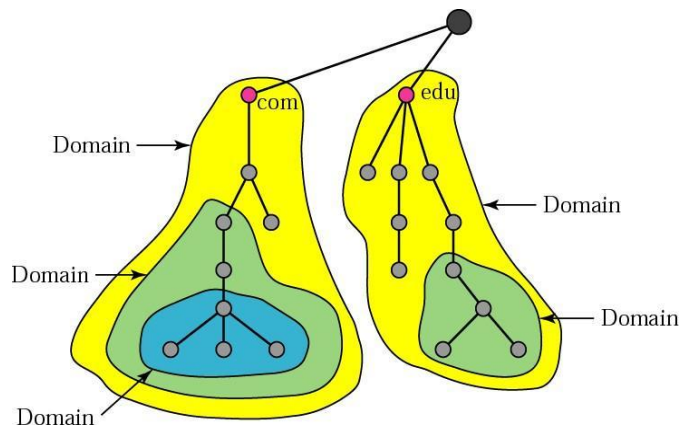
The information contained in the domain name space must be stored. the information is stored among many computers called **DNS servers.** we have a hierarchy of servers in the same way that we have a hierarchy of names


A **root server** is a server whose zone consists of the whole tree.
   • A root server usually does not store any information about domains but delegates its authority to other servers, keeping references to those servers.
   • There are several root servers, each covering the whole domain name space.
   • The root servers are distributed all around the world
   • DNS defines two types of servers: **primary** and **secondary**.

## DNS IN THE INTERNET

DNS is a protocol that can be used in different platforms.
In the Internet, the domain name space (tree) is divided into three different sections: generic domains, country domains, and the inverse domain
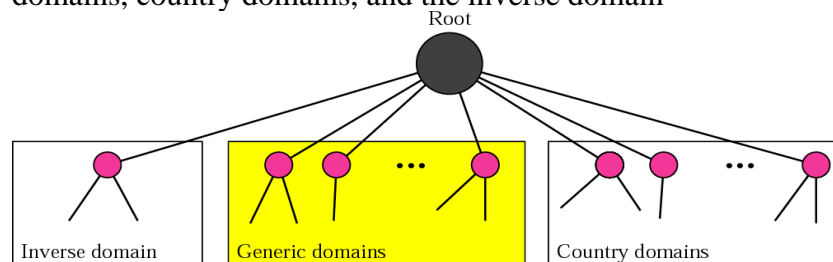
1. Generic domains
   • the first level in the generic domains section allows 14 possible labels.
   • These labels describe the organization types as listed in next slide
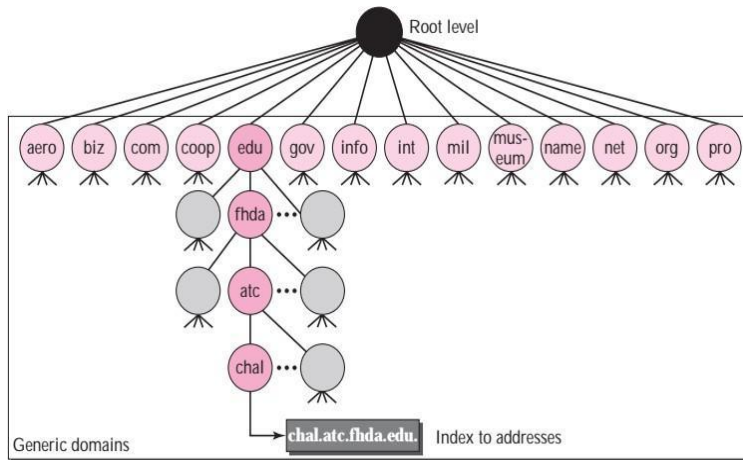
Label	Description
com	Commercial organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations

2. Country domains
 Name of the country abbreviated in two-character
Eg : .in .us . fr .nz etc
3. Inverse Domain
The inverse domain is used to map an address to a name.
Domain name registration
new domains added to DNS ,through a **registrar,** which is a commercial entity by ICANN. A registrar first verifies that the requested domain name is unique and then enters it into the DNS database. For assigning domain name, a fee is charged.

DNS RESOLUTION (DNS Lookup)

Mapping a name to an IP address is called *DNS resolution.*
there are Domain Name Servers built across world that takes your DNS look-up request and resolve it. There are 5 types of Name Servers –
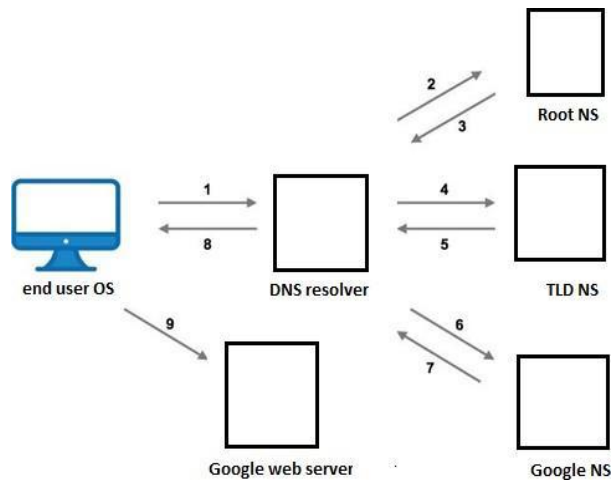1. Caching Name Servers.
2. Recursive Name Servers.
3. Root Name Servers.
4. Top Level Domain (TLD) Name Servers.
5. Authoritative Name Servers.

The DNS Resolution process
It starts when the user types a URL address (eg google.com) on the browser and hits Enter.
Then browser asks the operating system about its IP address

Step 1: OS Query to DNS Resolver
Since the operating system doesn't know where "www.google.com" is, it queries a DNS resolver, which is managed by the user's Internet service provider (ISP)

Step 2: DNS Resolver Query to the Root Server
The DNS resolver forwards the request for getting IP address of www.example.com to a DNS root name server

Step 3: Root Server Response
These root servers hold the locations of all of the Top Level Domains (TLDs) such as .com, .edu .org etc.
so it returns the location of the .com servers. The root responds with a list of the 13 locations of the .com TLD servers, listed as NS or "name server" records.

Step 4: DNS Resolver Query to the TLD Server
Then the resolver queries one of the .com name servers for the location of google.com..

Step 5: TLD Server Response
The .com TLD server does not have the IP addresses for google.com, but it knows the location of google.com's name servers. The .com TLD server responds with a list of all of google.com's NS records. In this case Google has four name servers, "ns1.google.com" to "ns4.google.com."

Step 6: DNS Resolver Query to the Google.com NS (name servers)
Finally, the DNS resolver queries one of Google's name server for the IP of www.google.com."

Step 7: Google.com NS Response
This time the queried Name Server responds with IPv4 and IPv6 address record of requested page www.google.com.

Step 8: DNS Resolver Response to OS
the resolver has finished the process and sends IP address to operating system of requesting client.

Step 9: Browser Starts TCP Handshake
The operating system, sends the IP address to the Application (i.e. browser), which initiates the TCP connection with server having that IP address, to request the web page.

Explain the email architecture / process
Email app has following architecture
User agent ,Message transfer agent (Mail server) , Message access agents (MAAs).
User agent program : which does following

Message transfer agent (MTA) (Mail server)
 The actual mail transmission is done through MTAs.
It has two parts :
 MTA client : to send message
MTA server : to receive message
Message access agents (MAAs).
User agent program uses MAA to collect messages from MTA server
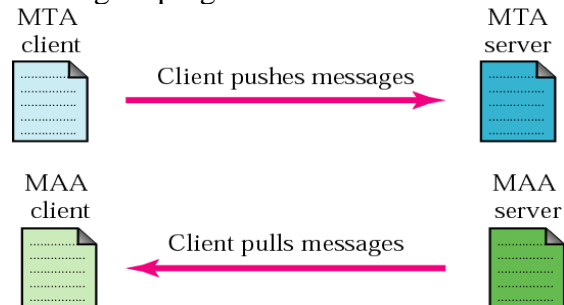
When both sender and receiver are connected to the two different mail servers via a LAN or a
WAN, we need two User agents UAs, two pairs of MTAs (client and server), and a pair of
MAAs (client and server). This is the most common situation today

- *Format of an e-mail*

Format of an e-mail

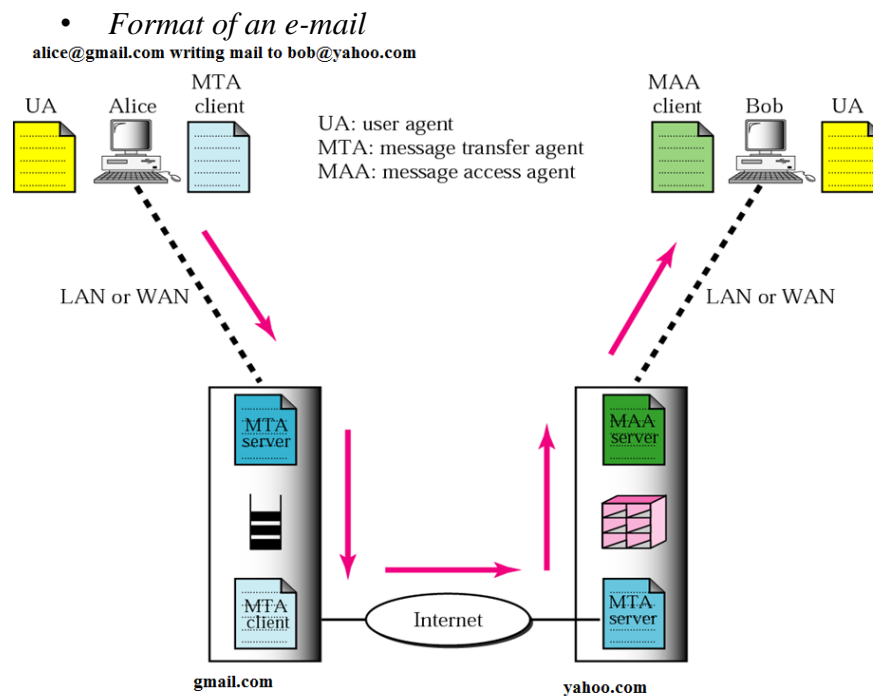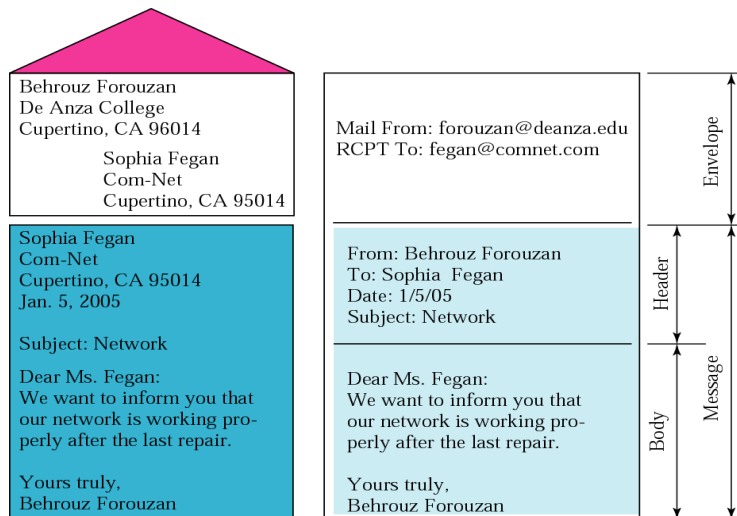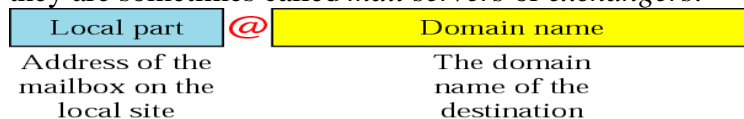Behrouz Forouzan
De Anza College
Cupertino, CA 96014

Sophia Fegan
Com-Net
Cupertino, CA 95014

Sophia Fegan
Com-Net
Cupertino, CA 95014
Jan. 5, 2005

Subject: Network

Dear Ms. Fegan:
We want to inform you that
our network is working pro-
perly after the last repair.

Yours truly,
Behrouz Forouzan

Mail From: forouzan@deanza.edu
RCPT To: fegan@comnet.com

From: Behrouz Forouzan
To: Sophia Fegan
Date: 1/5/05
Subject: Network

Dear Ms. Fegan:
We want to inform you that
our network is working pro-
perly after the last repair.

Yours truly,
Behrouz Forouzan

Envelope

Header

Body

Message

Email address format

The local part for a particular user it is the name of a special file, i.e. the user mailbox

domain name : An organization usually selects one or more hosts to receive and send e-mail; they are sometimes called *mail servers* or *exchangers*.

| Local part | @ | Domain name |

Address of the
mailbox on the
local site

The domain
name of the
destination

Limitation of email

Electronic mail has a simple structure. Its simplicity, however It can send messages only in NVT 7-bit ASCII format.
 For example, it cannot be used for languages that are not supported by 7-bit ASCII characters (such as,, Hebrew, Russian, Chinese, and Japanese , marathi).
Also, it cannot be used to send binary files or video or audio data.
Solution:
Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail.

Multipurpose Internet Mail Extensions (MIME)

is a supplementary protocol that allows non-ASCII data to be sent through e-mail. Because Electronic mail can send messages only in NVT 7-bit ASCII format.
 For example, it cannot be used for languages that are not supported by 7-bit ASCII characters (such as,, Hebrew, Russian, Chinese, and Japanese , marathi).
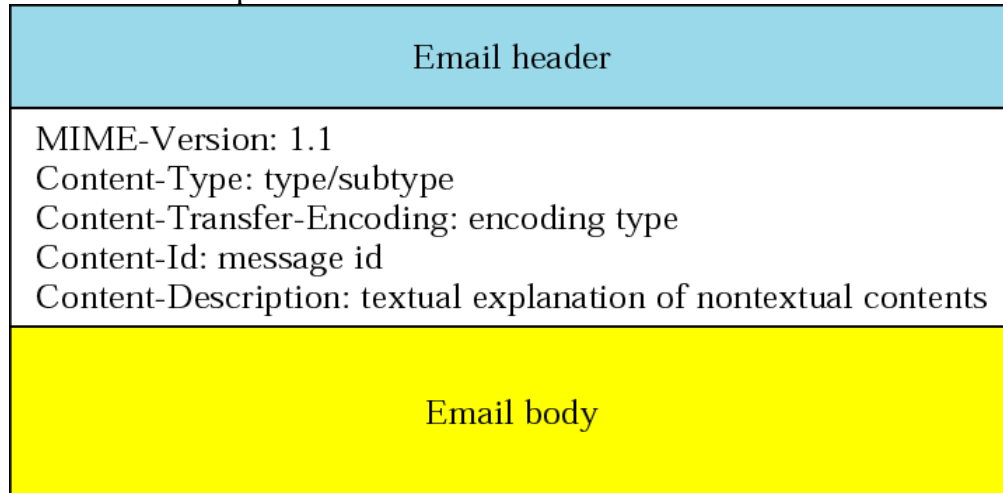Also, it cannot be used to send binary files or video or audio data.
MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers them to the client MTA to be sent through the Internet. The message at the receiving side is transformed back to the original data.

User

User

Non-ASCII code

Non-ASCII code

MIME

MIME

7-bit ASCII

7-bit ASCII

SMTP

7-bit ASCII

SMTP
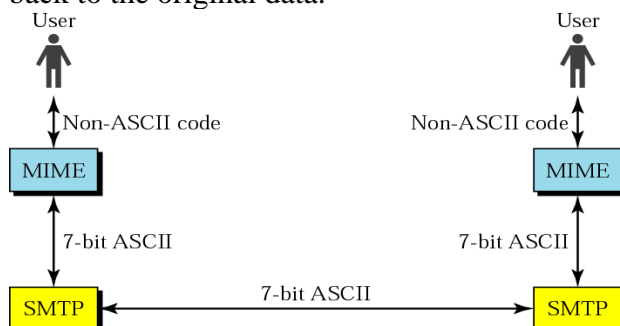
MIME defines five headers that can be added to the original e-mail header section to define the transformation parameters:
1. MIME-Version
2. Content-Type
3. Content-Transfer-Encoding
4. Content-Id
5. Content-Description

| Email header	
MIME-Version: 1.1 Content-Type: type/subtype Content-Transfer-Encoding: encoding type Content-Id: message id Content-Description: textual explanation of nontextual contents	**MIME header**
Email body	

Simple Mail Transfer Protocol (SMTP)

The actual mail transfer is done through message transfer agents. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.
The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol (SMTP)
SMTP is used two times, between the sender and the sender's mail server and between the two mail servers.

| | First Stage (SMTP) | Second Stage (SMTP) | Third Stage (Mail Access Protocol) |
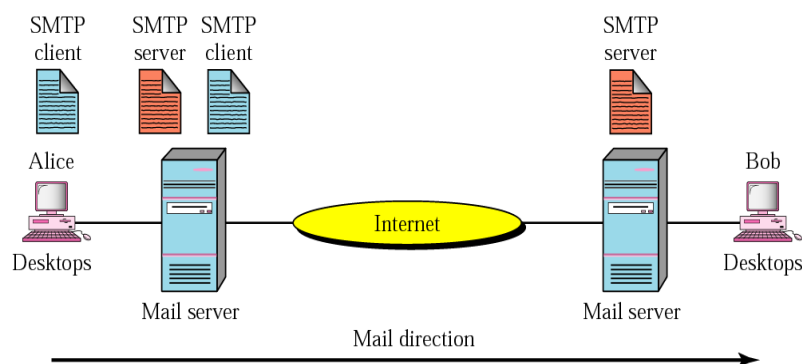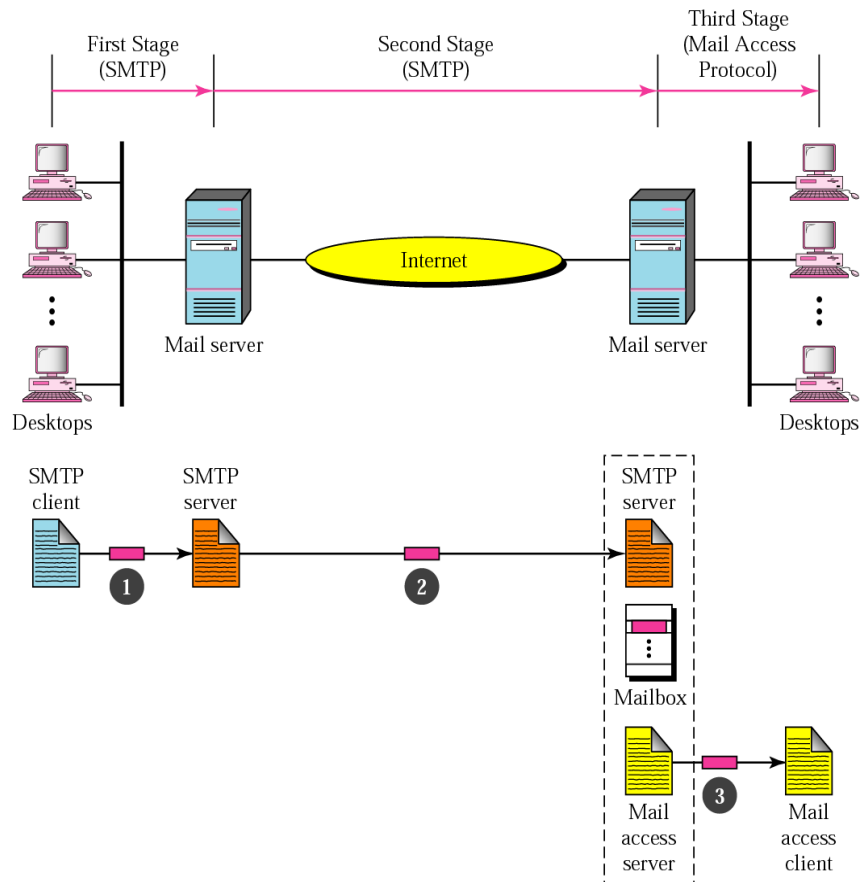
- SMTP simply defines how commands and responses must be sent back and forth.
- Commands are sent by client
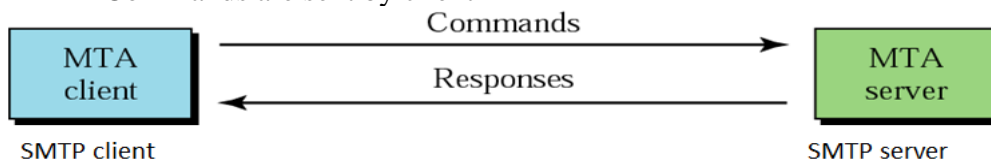
List of commands sent by client

Keyword	Argument(s)
HELO	Sender's host name
MAIL FROM	Sender of the message
RCPT TO	Intended recipient of the message
DATA	Body of the mail
QUIT	

Sample List of responses by server

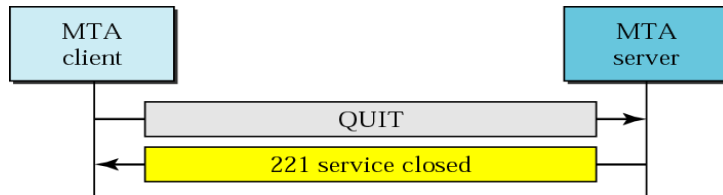| Service ready |
|---|
| Request command completed |
| Start mail input |
| Service not available |
| Mailbox not available |
| Syntax error; unrecognized command |
| Syntax error in parameters or arguments |

Connection establishment

```
        MTA                              MTA
        client                           server

         ◄──────── 220 service ready ──────────
         ───────── HELO: deanza.edu ──────────►
         ◄──────── 250 OK ─────────────────────
```

Message transfer

```
        MTA                              MTA
        client                           server

         ──── MAIL FROM: forouzan@deanza.edu ───►
         ◄─── 250 OK ────────────────────────────   Envelope
         ──── RCPT TO: sophie@net.edu ──────────►
         ◄─── 250 OK ────────────────────────────

         ──── DATA ─────────────────────────────►
         ◄─── 354 start mail input ──────────────
         ──── From: Behrouz Forouzan ──────────►
         ──── To: Sophia Fegan ────────────────►   Header
         ──── Date: 1/6/05 ────────────────────►
         ──── Subject: Network ────────────────►

         ──── ──────────────────────────────────►   Blank line

         ──── Dear Ms. Fegan ──────────────────►
         ──── We want to inform you that ──────►
                            ⋮
         ──── Yours truly ─────────────────────►   Body
         ──── Behrouz Forouzan ────────────────►
         ──── • ───────────────────────────────►
         ◄─── 250 OK ────────────────────────────
```
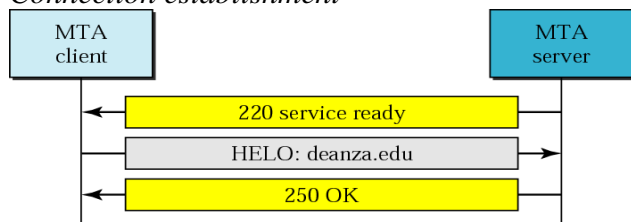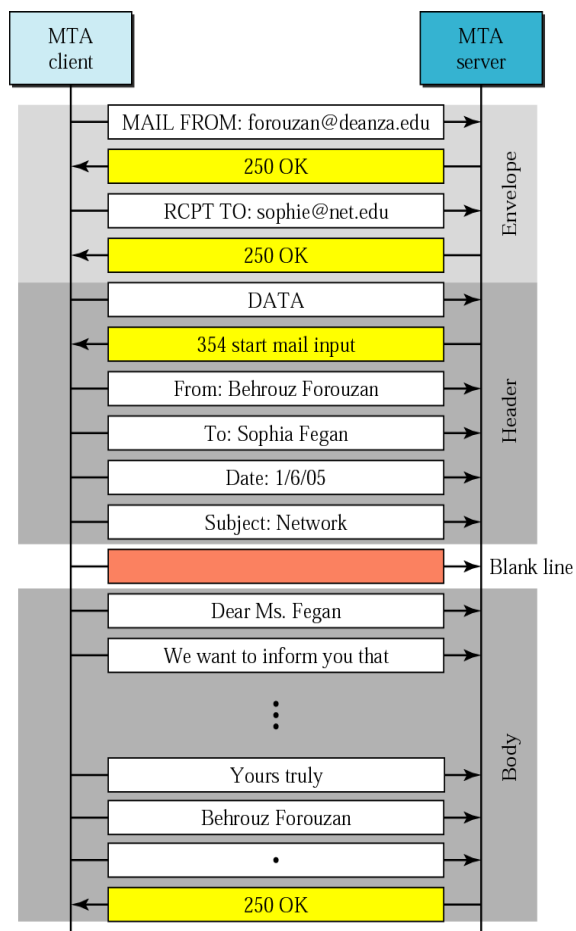
• *Connection termination*
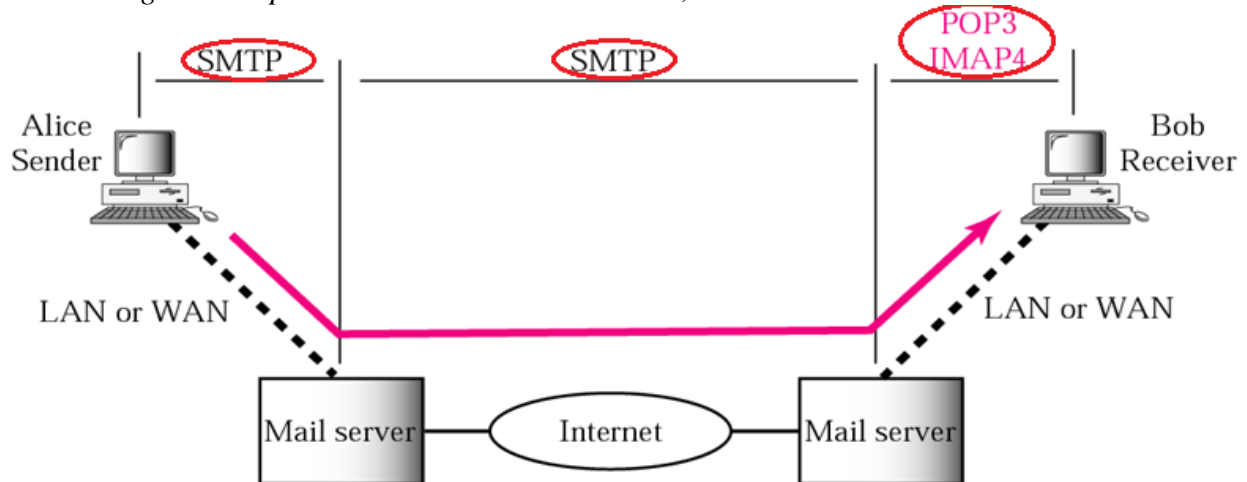
The first and the second stages of mail delivery use SMTP. However, SMTP is not involved in the third stage because SMTP is a *push* protocol.
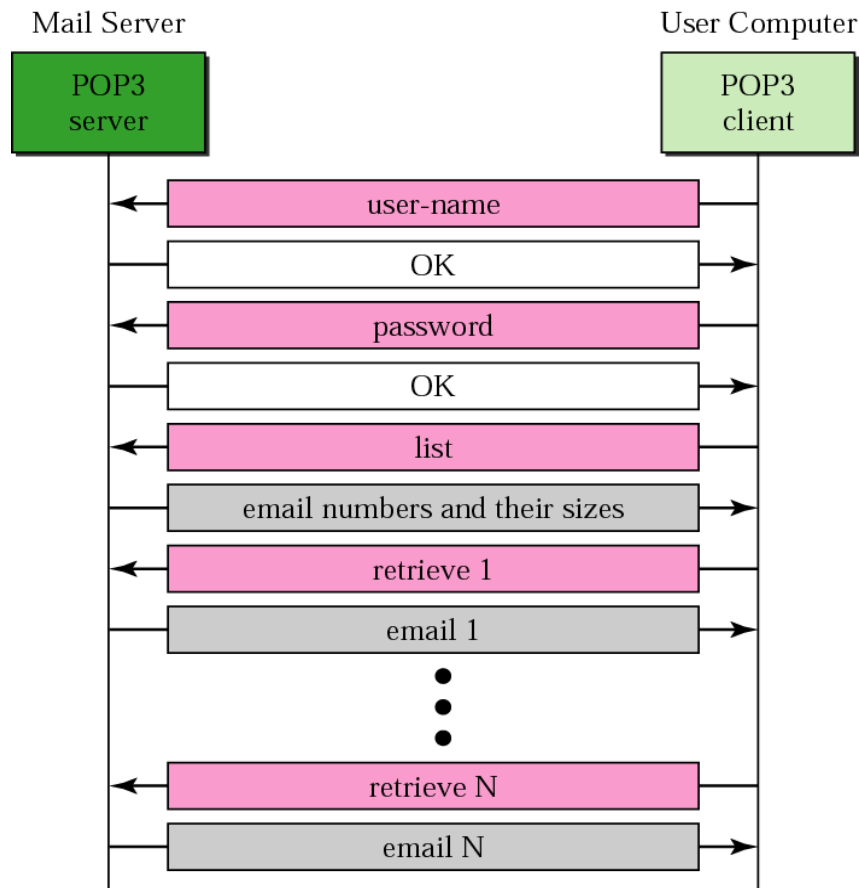
the third stage needs a *pull* protocol; the client must pull messages from the server. The third stage uses a **message access agent.**

two message access protocols are available: POP3 , IMAP4

Post Office Protocol, version 3 (POP3)

- The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server.

  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.

Mail Server

POP3 server		POP3 client
	← user-name	
	OK →	
	← password	
	OK →	
	← list	
	email numbers and their sizes →	
	← retrieve 1	
	email 1 →	
	⋮	
	← retrieve N	
	email N →	

User Computer

POP3 has two modes:
1. the delete mode and the keep mode.
2. In the delete mode, the mail is deleted from the mailbox after each retrieval.

In the keep mode, the mail remains in the mailbox after retrieval.

IMAP4 (Internet Mail Access Protocol, version 4)

is similar to POP3, but it has more features; IMAP4 is more powerful and more complex.
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

Compare POP3 with IMAP4

POP3	IMAP4
Mail access Agent	Mail access Agent
simple and limited in functionality	more complex & More functionality

|	
It does not allow the user to organize her mail on the server; the user cannot have different folders on the server	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.
A user can not partially download e-mail.	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.
does not allow the user to partially check the contents of the mail before downloading	does not allow the user to partially check the contents of the mail before downloading
A user can check the e-mail header before downloading. A user can not search the contents of the e-mail for a specific string of characters before downloading	A user can check the e-mail header before downloading. A user can search the contents of the e-mail for a specific string of characters before downloading

Some websites provide email service to anyone who accesses their site.
Three common sites are Hotmail, Yahoo, and Google.

Case I
the sender, uses a traditional mail server;, the receiver, has an account on a Web-based server.
- Mail transfer from Alice's browser to her mail server is done through SMTP. The transfer of the message from the sending mail server to the receiving mail server is still through SMTP.
- However, the message from the receiving server (the web server) to receiver browser is done through HTTP, instead of using POP3 or IMAP4. When receiver needs to retrieve his e-mails, he sends a request HTTP message to the website (Hotmail, for example). The website sends a form to be filled in by receiver, which includes the log-in name and the password. If the log-in name and password match, the list of e-mails is transferred from the Web server to receiver browser in HTML format. Now receiver can browse through his received e-mails and then, using more HTTP transactions, can get his e-mails one by one
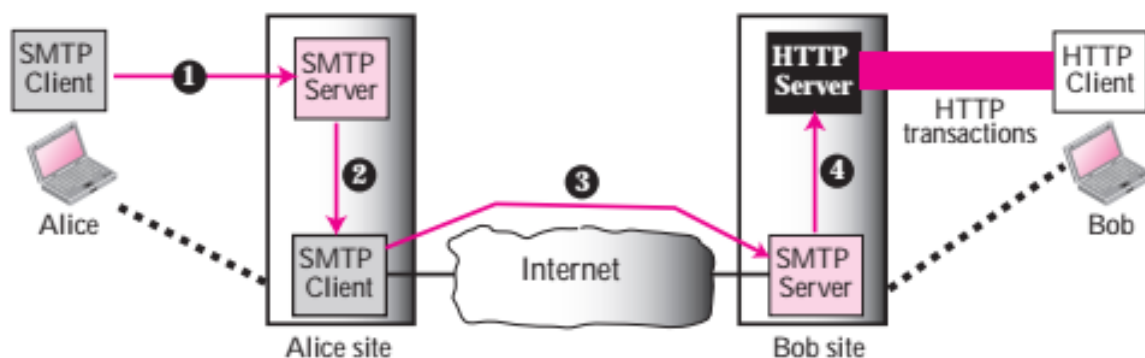

Case II
both sender and receiver use Web servers, but not necessarily the same server. (eg sender using gmail.com receiver using yahoo.com)

- Sender sends an HTTP request message to her Web server using the name and address of receiver's mailbox as the URL. The server at the sender site passes the message to the SMTP client and sends it to the server at the receiver site using SMTP protocol.

- receiver retrieves the message using HTTP transactions. However, the message from the server at the sender site to the server at the receiver site still takes place using SMTP protocol.
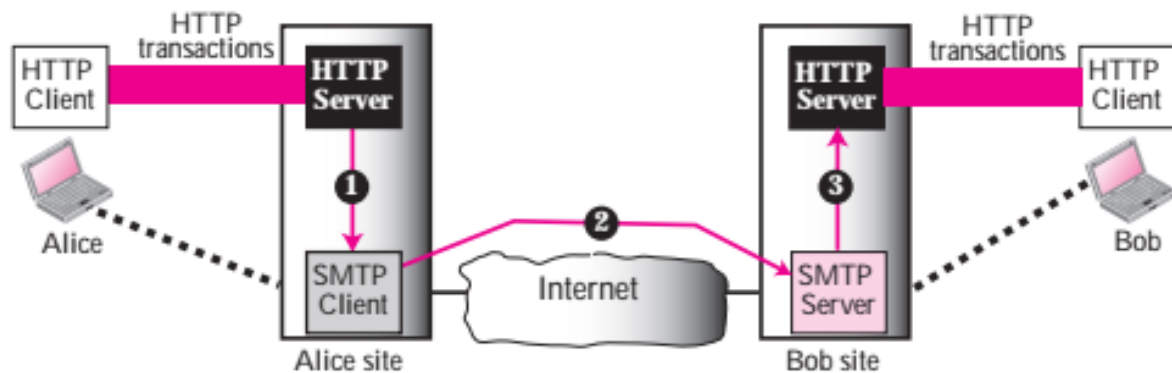
What is Dynamic Host Control Protocol (DHCP)? Why is it required?

It is a protocol for automatically assigning IP addresses and other communication parameters(such as subnet mask, default gateway and DNS server information) to nodes.

Why is it required:

Every node connected to a network , must have an IP address . It can be assigned either manually or automatically . Manual assigning of IP to every node is tedious . So it is automated by using pop.

What are the allocation methods of DHCP ?

1. Dynamic allocation

A network administrator sets a range of IP addresses in DHCP server, . The IP addresses are given on lease for a time period. Devices release their IP addresses when their DHCP leases expire and then request a renewal from the DHCP server if they are staying online. The DHCP server may assign a new address rather than renewing an old one.

2. Automatic allocation

The DHCP server permanently assigns an IP address to a requesting client from a range defined by an administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.

3. static allocation

This method is also called static DHCP allocation/ fixed address allocation/reservation, and MAC/IP address binding. Devices such as web servers and switches are assigned permanent IP addresses.

4. Manual

In this mapping the IP addresses to physical addresses needs to be manually configured. This means that every time there is a change in a physical or IP address, the administrator needs to manually enter the changes.

Thus DHCP provides static and dynamic address allocation that can be manual or automatic.

DHCP allocation process

In DHCP, the client is one which requests for IP address and the DHCP server assigns IP address. To get IP address from DHCP server, the client uses UDP protocol.
 DHCP port number for DHCP server is 67 and for the DHCP client is 68.
Client & server exchange mainly 4 DHCP messages in order to make a connection, also called **DORA** process, but there are total 8 DHCP messages in the process.
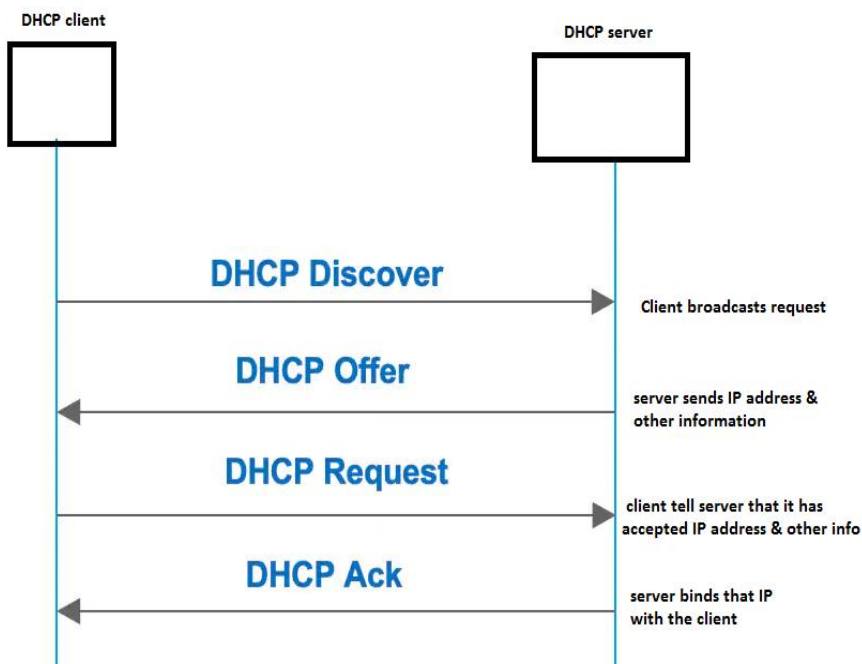
DHCP discover message –
This message is sent by Client host to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server.
DHCP offer message –
The server(s) send response, specifying the IP address and other information. This message is

broadcasted by server(s). If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives

DHCP request message –

Then client responds by broadcasting a DHCP request message. It is broadcasted in the network showing the acceptance of IP address.

DHCP acknowledgement message –

In response to the request message received, the server will make an entry to lock the IP address with specified client for a specified lease time. The client can now start using the IP for itself..

Other messages

> **DHCP negative acknowledgement message –**
>
> Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it send DHCP Nak message to client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.
>
> **DHCP decline –**
>
> If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server .When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.
>
> **DHCP release –**
>
> A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.
>
> **DHCP inform –**
>
> If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the dhcp inform message, DHCP server generates DHCP ack message with local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

To get IP address from DHCP server, the client uses UDP protocol

 DHCP port number for DHCP server is 67 and for the DHCP client is 68.
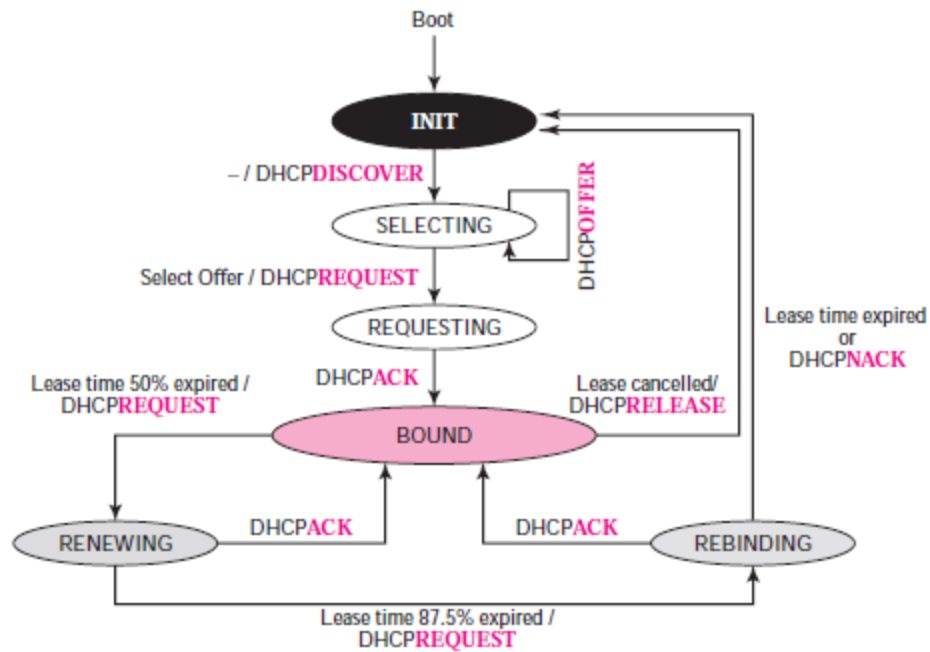
FTP

It is File Transfer Protocol which works at application layer.

It used to transfer files between client & server. But it is different than client -server architecture. In client -server architecture, there in only one TCP connection made. But in FTP there are two TCP connections. One connection is used for data transfer, the other for control information (commands and responses). Separation of commands and data transfer makes FTP more efficient.

It needs two TCP connections.
> The well-known port 21 is used for the control connection, and
> the well-known port 20 is used for the data connection
- when a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.
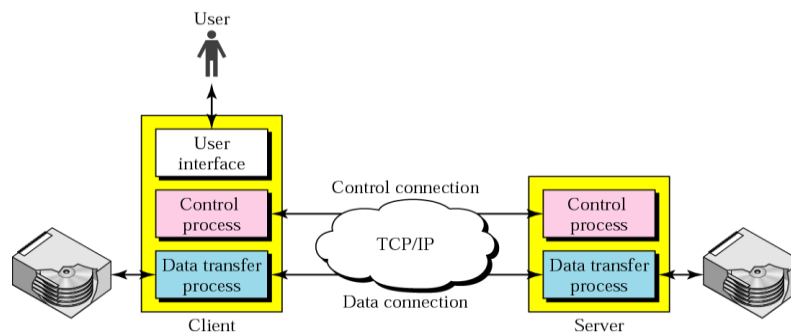
- FTP can transfer one of the following file types across the data connection: an ASCII file, EBCDIC file, or image file.

- Data Structure in file can be file structure, record structure, and page structure.

- FTP can transfer a file across the data connection by using one of the following three transmission modes: stream mode, block mode, and compressed mode.
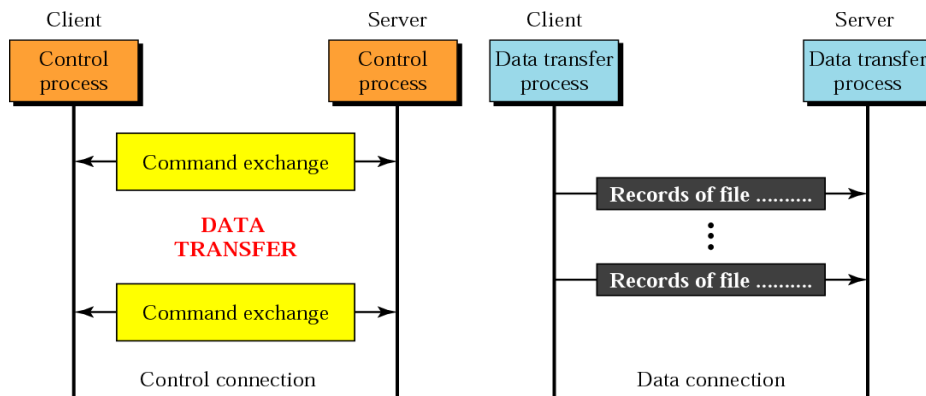
Subtypes of FTP :

  TFTP (trivial FTP i.e. simple FTP)

  Anonymous FTP (i.e. FTP which doesn't require password to access)

Few examples of FTP commands

  FTP url   ; to make FTP connection

  Ls   ; to see list of files in the server

  Get filename ; to download a file from the server

  Put filename ; to upload a file to the server
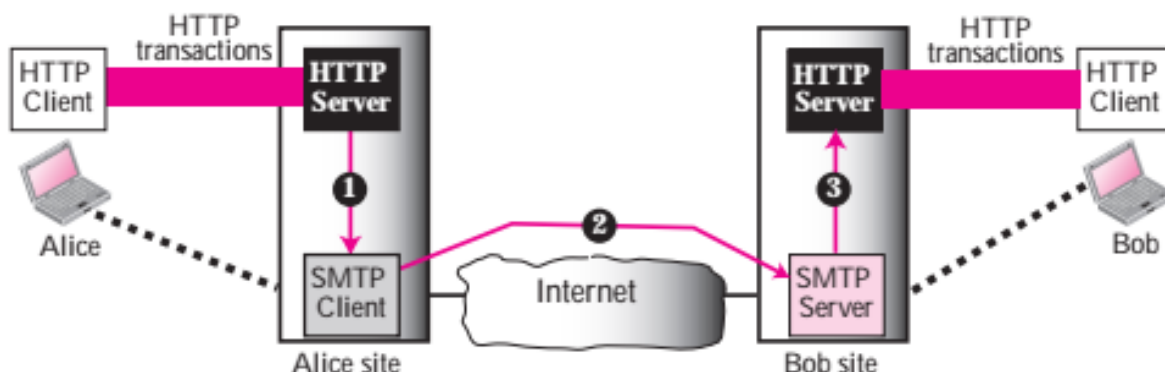
  Close ; colse the session

Web mail

Also called as Web based mail

Some websites provide email service to anyone who accesses their site.
Examples of sites providing web mail are

  AOL Mail, Proton Mail, Gmail, GMX Mail, Mailfence, Outlook.com/Hotmail.com, and
  Yahoo! Mail.

The clients use HTTP for sending & receiving mails through SMTP

Advantages of Webmail

Convenience

when you travel frequently and work from remote locations. With the help of using an internet connection, you can access and use it through any computer. Public access terminals like libraries and hotels are included in it..

Cost

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

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.

Large Storage

the storage in gigabytes or unlimited storage is offered by big webmail providers that allows you to save a large number of messages as well as large attachments.

Disadvantages of Webmail

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. Whenever you try to create an address on webmail with your own name, it may be this name has taken by another one..

Ads

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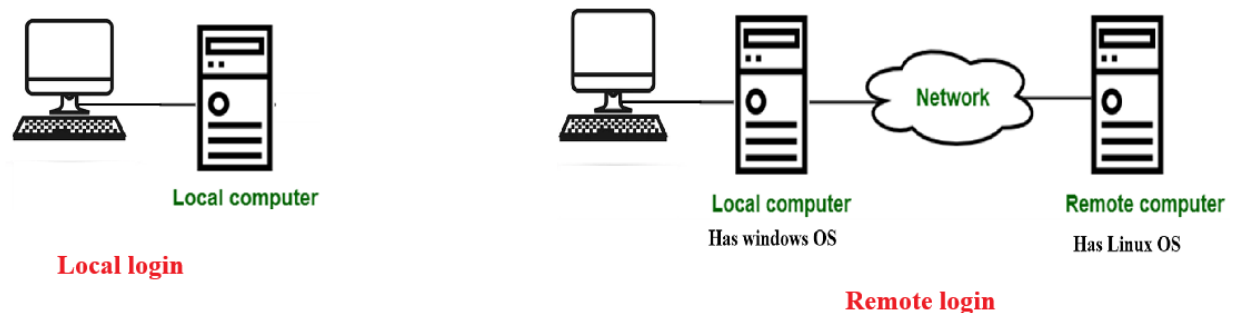
More Spam

Because of spammers' large customer base, they target webmail services more as compared to traditional providers. Therefore, the spammer can find your address and bombard you even if you are cautious not to sign up for commercial services.

Telnet

TELNET (*TErminaL NETwork)*
- Telnet is remote login program
- It is at application layer
- TELNET enables a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.

Local computer

Local login

Local computer
Has windows OS

Remote computer
Has Linux OS

Remote login

- it is impossible to write a specific client-server program for each requirement of client
- The better solution is a general-purpose client-server program that lets a user access any application program on a remote computer;

- in other words, allow the user to log on to a remote computer. After logging on, a user can use the services available on the remote computer and transfer the results back to the local computer.
- two such application programs are
  TELNET (for both windows & linux) and SSH (only for linux).
  puTTY is a popular application which can provide ssh & telnet service

When a user wants to access an application program or utility located on a remote machine, he performs remote log-in using TELNET client program in local machine.
The user type characters in to the terminal driver, the local **OS** accepts the characters but **does not interpret** them. The characters are sent to the TELNET client program in the local machine, which converts characters to **NVT** form (***Network Virtual Terminal***) and then sends it to the local *TCP/IP* protocol stack, For sending it to remote machine

Some examples of the telnet commands are :

Command	Meaning
open	Connect to a remote computer
close	Close the connection
display	Show the operating parameters
mode	Change to line mode or character mode
set	Set the operating parameters
status	Display the status information
send	Send special characters
quit	Exit TELNET

TELNET has security problems.
Telnet is an insecure system that transmits everything in plain text. Anyone who can intercept the network traffic can find passwords, read, modify, or redirect your commands/ files.