1. **Define WWW.**

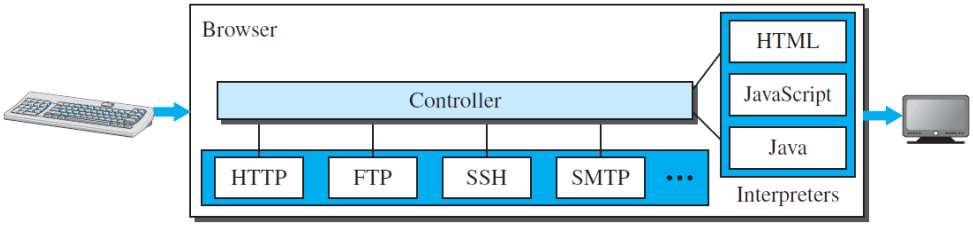
- The WWW(World Wide Web) is defined as a repository of information in which the documents, called web pages, are distributed all over the world and related documents are linked together.

2. **Explain the architecture of WWW.**

- The architecture of the World Wide Web (WWW) is composed of several fundamental components as follows.
    - Web browsers
    - Web servers
    - URLs
    - Web documents.
- The World Wide Web (WWW) today is a distributed client-server model, where a client using a web browser can access a service hosted on a particular server by using its URL.

Web Browsers

- A web browser is software which allows the user to access the website.



- Each browser usually consists of three parts: a controller, client protocols, 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, such as HTTP or FTP.
- The interpreter can be HTML, Java, or JavaScript, depending on the type of document.
- Example of web browsers are Edge, Google Chrome, and Firefox.

Web Servers

- Web servers are like the computers that store and send web pages to user who request them.
- When someone asks for a web page, the web server finds the right page and sends it back to that person.
- Web servers are very powerful computers that can handle many requests at once.
- Example of web servers are Apache, XAMPP, WAMP, and IIS.

URLs

- URL stands for Unique Resource Locator.
- It is a unique identifier to distinguish a web page from other web pages.
- There are four components of URL: Protocol, Host, Port and Path.
- Example http://www.google.com:80/myfile/image. In this http is the protocol, www.google.com is the host, 80 is the port number, and /myfile/image is the path.

Web Documents

- There are three categories of web documents.

  - Static Document
  - Dynamic Document
  - Active Document
- Static Document
  - Static documents are pre-created files stored on a server that users can view but not modify.
  - They are created using languages like HTML, XML, XSL, or XHTML.
- Dynamic Document
  - A dynamic document is created by a web server whenever a browser requests the document.
  - When a request arrives, the web server runs an application program or a script that creates the dynamic document.
- Active Document
  - A document which is created using a script on the client side, called as active documents.
  - Example: Java Applets, A document created using JavaScript.

3. Explain the components of URL.

- URL stands for Uniform Resource Locator; it is a unique identifier which is used to distinguish a web page from another web page.
- There are four components of URL: Protocol, Host, Port and Path, which are described below.
- Protocol
  - Protocol defines the type of client-server application that user wants to access.
  - Example: HTTP is used to access web page from the web server, FTP is used to access file from the file server.
- Host
  - It can be the IP address of the server, or the unique name given to the server.
  - Example: google.com is the host name to access the google server's webpage.
- Port
  - The port, a 16-bit integer, is normally predefined for the client-server application.
  - Example: if the HTTP protocol is used for accessing the web page, the well-known port number is 80.
- Path
  - The path identifies the location and the name of the file in the underlying operating system. The format of this identifier normally depends on the operating system.
  - Example: www.google.com/image/myfile.jpg
    - In the above example /image/myfile.jpg is the path of the file myfile.jpg in the google server.

4. Describe three different types of web documents.

- A web document is an electronic resource that can be accessed through the World Wide Web (WWW).
- It is typically written in HTML, which defines the structure and content of the document.
- Web documents can also include other types of data, such as images, videos, and scripts.
- The documents in the WWW can be grouped into three broad categories:
  - Static Document,
  - Dynamic Document
  - Active Document

Static Document

- Static documents are fixed-content documents that are created and stored in a server.
- When a client accesses the document, a copy of the document is sent.
- The content of the document is same for each request.
- Static documents are prepared using one of several languages: HTML, XML, XSL, and XHTML.

Dynamic Document

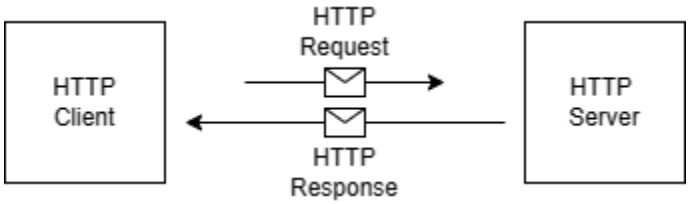
- A dynamic document is created by a web server whenever a browser requests the document.
- When a request arrives, the web server runs an application program or a script that creates the dynamic document. The server returns the result of the program or script as a response to the browser that requested the document.
- Because a fresh document is created for each request, the contents of a dynamic document may vary from one request to another.
- A very simple example of a dynamic document is the retrieval of the time and date from a server.
- Dynamic document can be created by embedding the SQL code in the HTML page.

Active Document

- A document which is created using a script on the client side, called as active documents.
- 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.
- For example, suppose we want to run a program that creates animated graphics on the screen or a program that interacts with the user.
- Active document can also be created using JavaScript.

5. Explain HTTP.

- HTTP stands for HyperText Transfer Protocol.
- It is a client-server protocol which used to retrieve web pages from the Web.
- An HTTP client sends a request; an HTTP server returns a response.



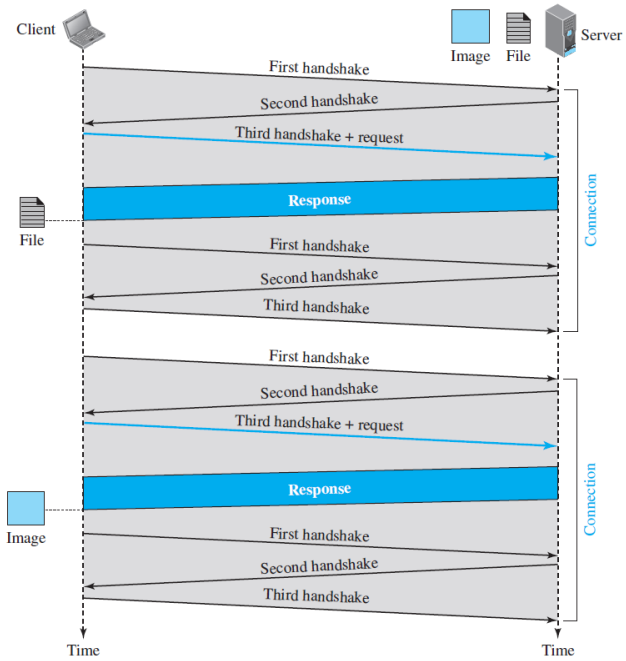
- The server uses the port number 80; the client uses a temporary port number.
- HTTP uses the services of TCP on the transport layer protocol.
- There are two types of connections associated with HTTP protocol: persistent connection and non-persistent connection.
    - HTTP versions prior to 1.1 supports only non-persistent connections.
    - HTTP versions 1.1 supports both persistent and non-persistent connections.
- HTTP protocol can use eight different types of methods in request message.
    - GET
    - HEAD
    - PUT
    - POST
    - TRACE

- DELETE
- CONNECT
- OPTIONS

- A client can add a condition in its request. In this case, the server will send the requested web page if the condition is met.
- HTTP supports proxy servers.
- HTTP per se does not provide security. However, HTTP can be run over the secure socket layer. In this case HTTP is referred to as HTTPS.

6. Explain non-persistent connection of HTTP with diagram.

- In non-persistent connections, each time a client makes a request, it needs to establish a new TCP connection with the server before data can be transferred. This means that for each object that the client wants to fetch, there will be two round-trip times (RTTs) of overhead.
- The following lists the steps in this strategy:
  1. The client opens a TCP connection and sends a request.
  2. The server sends the response and closes the connection.
  3. The client reads the data until it encounters an end-of-file marker; it then closes the connection.
- In this strategy, if a file contains links to N different pictures in different files (all located on the same server), the connection must be opened and closed N + 1 times.
- The nonpersistent strategy imposes high overhead on the server because the server needs N + 1 different buffers each time a connection is opened.
- Consider the following diagram to understand the non-persistent strategy.

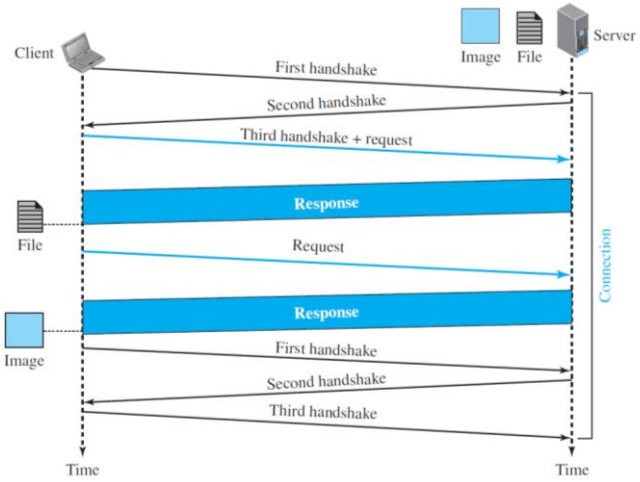


- As shown in the above figure, The client needs to access a file that contains one link to an image. The text file and image are located on the same server. Here we need two connections.
- For each connection, TCP requires at least three handshake messages to establish the connection, but the request can be sent with the third one. After the connection is established, the object can be transferred. After receiving an object, another three handshake messages are needed to terminate the connection.

- The client and server are involved in two connection establishments and two connection terminations.
- If the transaction involves retrieving 10 or 20 objects, the round-trip times spent for these handshakes add up to a big overhead.

7. Explain persistent connection of HTTP with diagram.

- HTTP version 1.1 specifies a persistent connection by default.
- In a persistent connection, the server leaves the connection open for more requests after sending a response. The server can close the connection at the request of a client or if a time-out has been reached.
- Time and resources are saved using persistent connections. Only one set of buffers and variables needs to be set for the connection at each site. The round trip time for connection establishment and connection termination is saved.
- Consider the following diagram to understand the persistent strategy.



- As shown in the above figure, The client needs to access a file that contains one link to an image. The text file and image are located on the same server. Here we need only one connection in this persistent strategy.
- The client first establishes the TCP connection. Then it requests for the file transfer, then it requests for the image. Once the image is transferred, connection will be terminated. Thus, this strategy helps to reduce the overhead, which was there in the non-persistent strategy.

8. Describe different HTTP methods.

- HTTP protocol can use eight different types of methods in request message.
- GET
  - It is used to retrieve data from a specified resource.
  - It is Used to fetch data from a server, such as a webpage or API response.
- HEAD
  - It Retrieves only the header information of a resource, not the content.
  - It is Used to check the metadata of a resource without downloading the entire file.
- PUT
  - It Updates an existing resource with new data.
  - It is used to replace existing data on a server with new information.
- POST
  - It Submits data to be processed to a specified resource.
  - It is Used to send data to a server, such as submitting a form or creating a new resource.

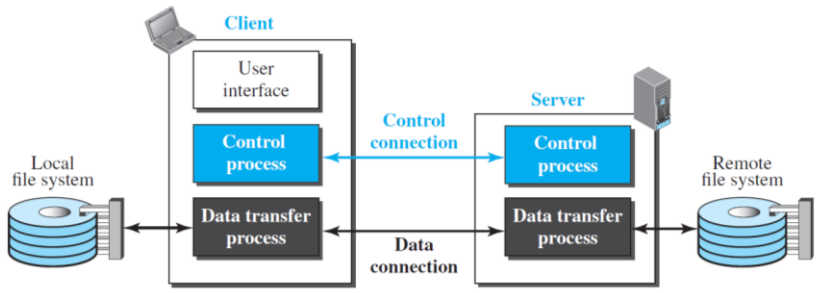
- TRACE
    - It traces the path of a request through a network of servers.
    - It is used for debugging and troubleshooting network issues.
- DELETE
    - It removes a specified resource from the server.
    - It used to delete data from a server, such as removing a file or cancelling a subscription.
- CONNECT
    - It Establishes a tunnel through an HTTP proxy server to another server.
    - It Enables secure communication over an HTTP proxy, bypassing firewalls, and censorship.
- OPTIONS
    - It Describes the HTTP methods supported by a server for a specific resource.
    - It used to determine which HTTP methods are allowed for a particular resource.

9. Describe HTTP cookies.

- An HTTP cookie (web cookie, browser cookie) is a small piece of data that a website stores on a user's computer or mobile device.
- Cookies are used to remember information about a user's visit to a website, such as their login credentials, preferences, and shopping cart items. This information can be used to improve the user's experience on the website by making it easier for them to log in, access their preferences, and complete purchases.
- Cookies are sent back to the website by the user's browser when they revisit the site. This allows the website to remember the user's information and provide them with a personalized experience.
- There are two main types of cookies:
    - Session cookies are temporary cookies that are stored in the user's browser memory and are deleted when they close their browser. Session cookies are typically used to store information about a user's current visit to a website, such as their login credentials and shopping cart items.
    - Persistent cookies are permanent cookies that are stored on the user's computer or mobile device until they expire or are manually deleted. Persistent cookies are typically used to store information about a user's preferences, such as their language preference or theme settings.
- Benefits cookies:
    - Improved user experience
    - Targeted advertising
    - Website analytics
- Drawbacks of using cookies:
    - Privacy concerns: Cookies can be used to track a user's browsing activity across multiple websites, which can be a privacy concern.
    - Security risks: Cookies can be used to store sensitive information, such as login credentials. If cookies are compromised, this information could be stolen.
    - Third-party tracking: Third-party cookies can be used to track a user's browsing activity across multiple websites, which can be a privacy concern.

10. Explain FTP.

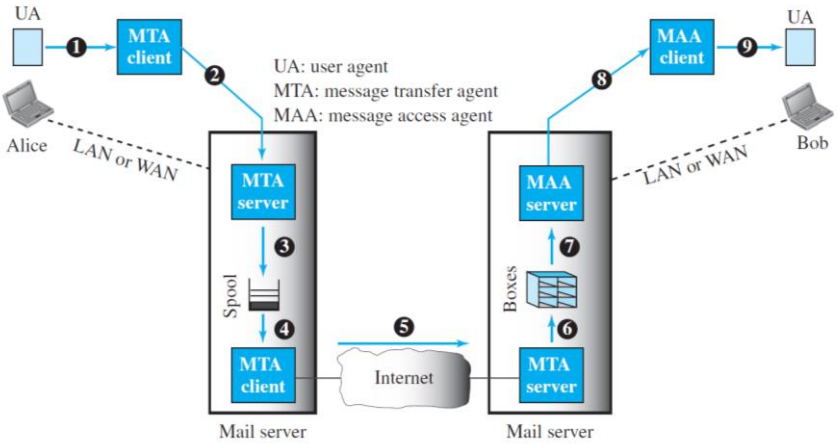
- File Transfer Protocol (FTP) is the standard protocol that is used for copying a file from one host to another.
- It is better choice to transfer large files or to transfer files using different formats.
- The following figure shows the basic model of FTP.



- The client has three components: the user interface, the client control process, and the client data transfer process.
- The server has two components: the server control process and the server data transfer process.
- FTP uses two different connections.
    - Control Connection
    - Data Connection
- Control Connection
    - The control Connection is made between the control processes.
    - The control connection remains connected during the entire interactive FTP session.
    - FTP uses port number 21 for the control connection.
    - FTP uses different commands for different task in control connection such as USER for user id, PASS for the password, QUIT for the logout.
- Data Connection
    - The data connection is made between the data transfer processes.
    - It opens each time commands that involve transferring files are used, and it closes when the file is transferred.
    - The data connection needs more complex rules due to the variety of data types transferred.
    - FTP uses port number 20 for the data connection.
- Separation of commands and data transfer makes FTP more efficient.
- By adding an SSL layer between FTP and TCP can make the FTP connection more secure

11. Explain the architecture of E-mail.

- E-mail stands for Electronic Mail, it is one type of messaging system just like postal system.
- Consider the following diagram to understand the architecture of the E-mail.

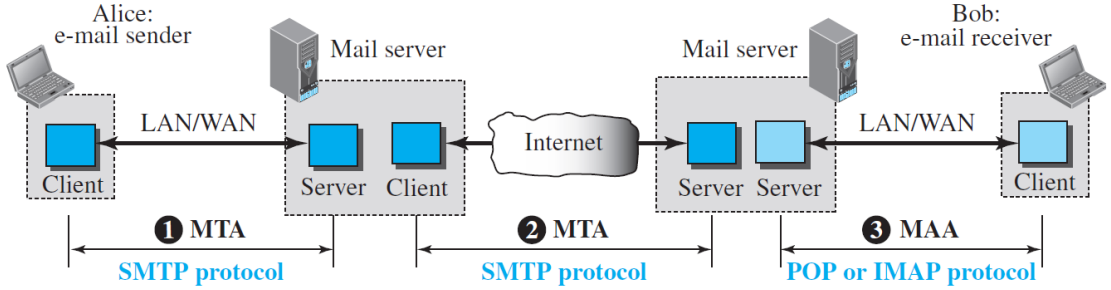


- As shown in the above figure, the sender and the receiver of the e-mail, Alice and Bob respectively, are connected via a LAN or a WAN to two mail servers.

- The administrator has created one mailbox for each user where the received messages are stored. A mailbox is part of a server hard drive, a special file with permission restrictions. Only the owner of the mailbox has access to it.
- The administrator has also created a queue (spool) to store messages waiting to be sent.
- A simple e-mail from Alice to Bob takes nine different steps, as shown in the figure.
- Alice and Bob use three different agents:
    - A user agent (UA)
        - The first component of an electronic mail system is the user agent (UA).
        - It provides service to the user to make the process of sending and receiving a message easier.
        - A user agent is a software package (program) that composes, reads, replies to, and forwards messages. It also handles local mailboxes on the user computers.
        - There are two types of user agents: command-driven and GUI-based.
    - A message transfer agent (MTA)
        - It is a push protocol.
        - It is a client server protocol such as SMTP, which transfers mail from MTA client to MTA server.
    - A message access agent (MAA).
        - It is a pull protocol.
        - It is client server protocol such as POP, IMAP, which fetches messages from the MAA server to MAA client.
- When Alice needs to send a message to Bob, she runs a UA program to prepare the message and send it to her mail server. (MTA Client to MTA Server).
- The mail server at her site uses a queue (spool) to store messages waiting to be sent. (MTA Server to Queue)
- The message, however, needs to be sent through the Internet from Alice's site to Bob's site using an MTA. Here two message transfer agents are needed: one client and one server. Like most client-server programs on the Internet, the server needs to run all the time because it does not know when a client will ask for a connection. The client, on the other hand, can be triggered by the system when there is a message in the queue to be sent.
- The user agent at the Bob site allows Bob to read the received message.
- Bob later uses an MAA client to retrieve the message from an MAA server running on the second server. (MAA Server to MAA Client).

12. Explain SMTP.

- SMTP stands for Simple Mail Transfer Protocol.
- It uses TCP as the transport layer protocol and its default port number is 25.
- As shown in the figure below, SMTP is used two times, between the sender and the sender's mail server and between the two mail servers.



- SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.
- Command
    - The command is from an MTA client to an MTA server.
    - The format of a command is: Keyword: argument(s).
    - SMTP defines different 14 commands. Example MAIL FROM which identifies the sender of the mail.
- Response
    - The response is from an MTA server to the MTA client.
    - It is a three-digit code that may be followed by additional textual information. Example 220 means service is ready.
- Each command or reply is terminated by a two-character (carriage return and line feed) end-of-line token.
- SMTP done process of mail transferring in three different phases.
    - Connection Establishment.
    - Mail Transfer.
    - Connection termination.
- SMTP Applications
    - Email Clients
    - Webmail Services
    - Email Relay Servers
    - Mailing List Servers

13. Explain mail transfer phases of SMTP.

- The process of transferring a mail message occurs in three phases:
    - connection establishment,
    - mail transfer,
    - connection termination

Connection Establishment

- After a client has made a TCP connection to the well-known port 25, the SMTP server starts the connection phase. This phase involves the following three steps:
    1. The server sends code 220 (service ready) to tell the client that it is ready to receive mail. If the server is not ready, it sends code 421 (service not available).
    2. The client sends the HELO message to identify itself, using its domain name address. This step is necessary to inform the server of the domain name of the client.
    3. The server responds with code 250 (request command completed) or some other
    4. code depending on the situation.

Mail Transfer

- After connection has been established between the SMTP client and server, a single message between a sender and one or more recipients can be exchanged. This phase involves eight steps. Steps 3 and 4 are repeated if there is more than one recipient.
    1. The client sends the MAIL FROM message to introduce the sender of the message. It includes the mail address of the sender (mailbox and the domain name). This step is needed to give the server the return mail address for returning errors and reporting messages.
    2. The server responds with code 250 or some other appropriate code.

3. The client sends the RCPT TO (recipient) message, which includes the mail address of the recipient.
4. The server responds with code 250 or some other appropriate code.
5. The client sends the DATA message to initialize the message transfer.
6. The server responds with code 354 (start mail input) or some other appropriate message.
7. The client sends the contents of the message in consecutive lines. Each line is terminated by a two-character end-of-line token (carriage return and line feed). The message is terminated by a line containing just one period.
8. The server responds with code 250 (OK) or some other appropriate code. Connection Termination

Connection Termination

- After the message is transferred successfully, the client terminates the connection. This phase involves two steps.
    1. The client sends the QUIT command.
    2. The server responds with code 221 or some other appropriate code.

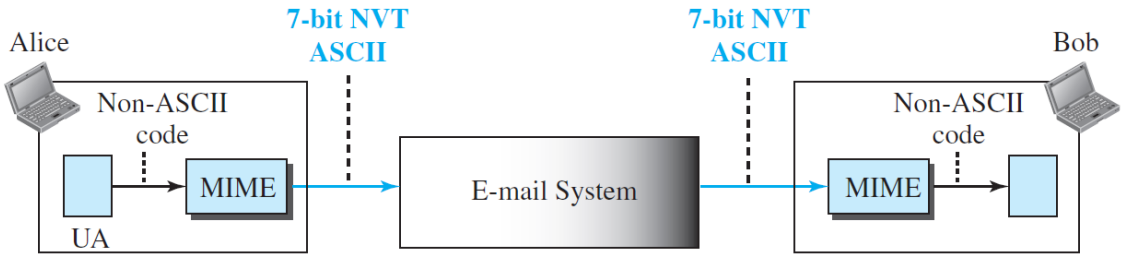
14. Differentiate POP and IMAP.

Post Office Protocol (POP3)	Internet Message Access Protocol (IMAP)
It is a simple protocol that only allows downloading messages from your Inbox to your local computer.	It is much more advanced and allows the user to see all the folders on the mail server.
The POP server listens on port 110, and the POP with SSL secure(POP3DS) server listens on port 995	The IMAP server listens on port 143, and the IMAP with SSL secure(IMAPDS) server listens on port 993.
In POP3 the mail can only be accessed from a single device at a time.	Messages can be accessed across multiple devices
To read the mail it has to be downloaded on the local system.	The mail content can be read partially before downloading.
The user can not organize mails in the mailbox of the mail server.	The user can organize the emails directly on the mail server.
The user can not create, delete or rename email on the mail server.	The user can create, delete or rename an email on the mail server.
It is unidirectional i.e. all the changes made on a device do not affect the content present on the server.	It is Bi-directional i.e. all the changes made on the server or device are made on the other side too.
It does not allow a user to sync emails.	It allows a user to sync their emails.
It is fast.	It is slower as compared to POP3.
A user can not search the content of mail before downloading it to the local system.	A user can search the content of mail for a specific string before downloading.
It has two modes: delete mode and keep mode. In delete mode, the mail is deleted from the mailbox after retrieval. In keep mode, the mail remains in the mailbox after retrieval.	Multiple redundant copies of the message are kept at the mail server, in case of loss of message of a local server, the mail can still be retrieved
Changes in the mail can be done using local email software.	Changes made to the web interface or email software stay in sync with the server.

All the messages are downloaded at once.	The Message header can be viewed prior to downloading.

15. Describe 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 it to the client MTA to be sent through the Internet.
- The message at the receiving site is transformed back to the original data.
- We can think of MIME as a set of software functions that transforms non-ASCII data to ASCII data and vice versa, as shown in Figure below.

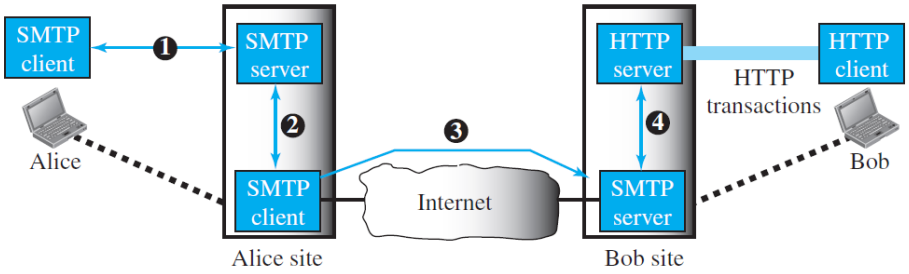


- Key Features of MIME:
  - **Content Representation**: MIME defines different methods for representing different types of data, ensuring that the content is preserved during transmission.
  - **Content Type Identification**: MIME utilizes content types to identify the specific format of the data, allowing email clients to handle the content appropriately.
  - **Content Transfer Encoding**: MIME employs content transfer encodings to ensure that the data is not corrupted during transmission and can be correctly decoded by the recipient.
- Application of MIME
  - **Email Attachments:** MIME is widely used for attaching files to email messages, enabling users to share documents, images, audio, video, and other types of data.
  - **Web Content:** MIME is also used in web content to specify the format of data embedded in HTML pages, such as images, scripts, and style sheets.
  - **Multimedia Messaging:** MIME plays a crucial role in multimedia messaging protocols, such as MMS (Multimedia Messaging Service), enabling the transmission of rich media content through mobile devices.

16. Explain Web based Mail.

- E-mail is such a common application that some websites today provide this service to anyone who accesses the site.
- The common examples of web mail are Gmail, Yahoo Mail, Hotmail.
- Here, the web mails are explained using two different cases.

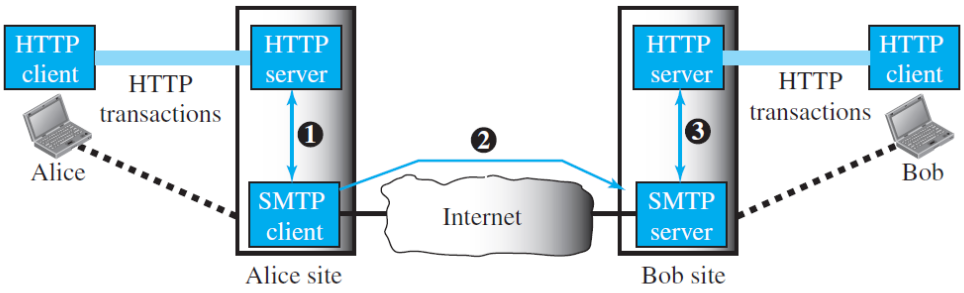
Case -I



Case 1: Only receiver uses HTTP

- In the first case, Alice, the sender, uses a traditional mail server; Bob, 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 Bob's browser is done through HTTP. In other words, instead of using POP3 or IMAP4, HTTP is normally used.
- When Bob 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 Bob, 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 Bob's browser in HTML format.
- Now Bob can browse through his received e-mails and then, using more HTTP transactions, can get his e-mails one by one.

Case-II



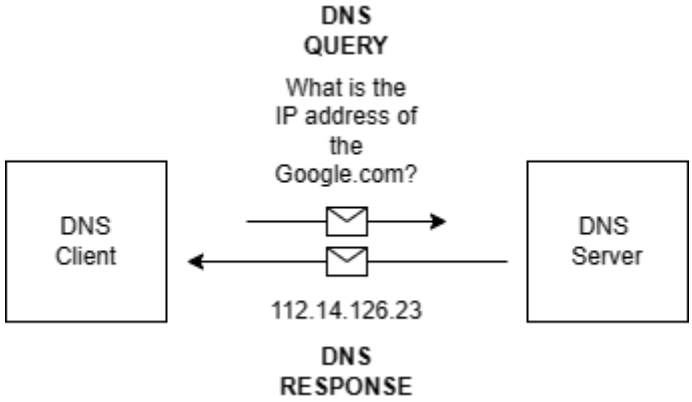
Case 2: Both sender and receiver use HTTP

- In the second case, both Alice and Bob use web servers, but not necessarily the same server.
- Alice sends the message to the web server using HTTP transactions.
- Alice sends an HTTP request message to her web server using the name and address of Bob's mailbox as the URL.
- The server at the Alice site passes the message to the SMTP client and sends it to the server at the Bob site using SMTP protocol.
- Bob receives the message using HTTP transactions.
- However, the message from the server at the Alice site to the server at the Bob site still takes place using SMTP protocol.

17. Explain DNS

- It is an application layer protocol in the TCP/IP protocol stack. It uses mostly UDP as the transport layer protocol. If the size of the DNS query is more than 512 Bytes, then it uses TCP as the transport layer protocol.

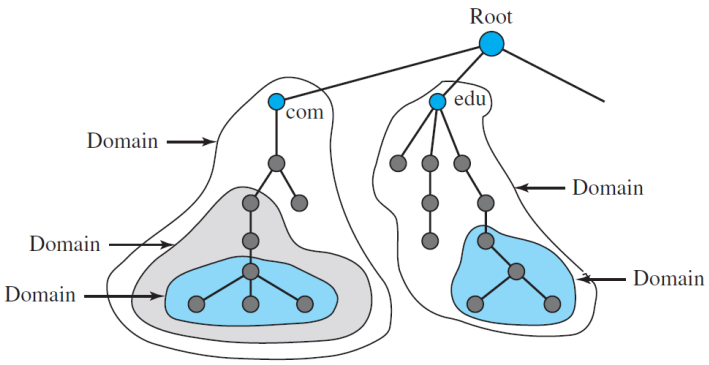
- The default port number of DNS is 53.
- The Domain Name System (DNS) is the phonebook of the Internet. It translates domain names into IP addresses. It can be used for mail aliasing.
- When you type a domain name into your web browser, your computer (DNS client) sends a query to a DNS server. The DNS server then looks up the IP address for the domain name and sends it back to your computer. Your computer can then use the IP address to connect to the website.



- The DNS system is hierarchical and distributed.
- There are many different DNS servers, each of which is responsible for a different part of the DNS hierarchy. The root servers are at the top of the hierarchy, and they are responsible for pointing to the top-level domain (TLD) servers. The TLD servers are responsible for pointing to the domain servers, which are responsible for pointing to the host servers.
- The DNS system is an essential part of the Internet. Without DNS, we would have to memorize IP addresses for every website we want to visit. This would be impractical, and it would make the Internet much less user-friendly.
- Benefits of DNS
    - Makes the Internet easier to use: DNS makes it easy to access websites by translating domain names into IP addresses.
    - Improves performance: DNS caching can improve the performance of websites by caching the IP addresses of frequently visited websites.

18. Define Domain

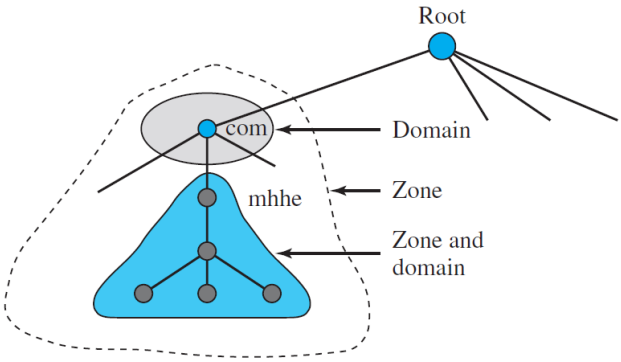
- A domain is a subtree of the domain name space.
- The name of the domain is the name of the node at the top of the subtree.
- Figure-1 shows some domains.



- Note that a domain may itself be divided into domains.

19. Describe Zone

- A DNS zone, also known as a domain zone, is a portion of the Domain Name System (DNS) namespace that is delegated to a specific organization or administrator.
- A DNS zone can also be defined as a contiguous part of the entire tree. If a server accepts responsibility for a domain and does not divide the domain into smaller domains, the "domain" and the "zone" refer to the same thing. The server makes a database called a zone file and keeps all the information for every node under that domain.
- However, if a server divides its domain into subdomains and delegates part of its authority to other servers, "domain" and "zone" refer to different things.
- It is a hierarchical tree-like structure, with the root domain at the top and subdomains further down the tree.
- Each zone contains resource records (RRs) that map domain names to IP addresses or other resources. These RRs are used by DNS servers to resolve domain names to IP addresses, which allows users to access websites and other internet resources.



20. Explain Servers of DNS.

- Generally, there are three types of server used in DNS which are as follows
    - Root Server
    - Top level domain server
    - Authoritative server

Root Server

- A root server is a type of DNS (Domain Name System) server that is responsible for answering queries for the root zone of the DNS hierarchy.
- The root zone is the highest level of the DNS hierarchy, and it contains information about the top-level domains (TLDs) such as .com, .org, .net, and country code TLDs like .us, .uk, .ca, etc.
- There are 13 sets of root servers located around the world, with each set containing multiple servers.
- These servers are operated by various organizations, including universities, government agencies, and private companies.
- The root servers work together to ensure that the DNS system is distributed and highly available, even in the event of failures or attacks.

Top level domain server (TLDs)

- A top-level domain (TLD) server is a type of DNS (Domain Name System) server that is responsible for managing the domain names associated with a specific top-level domain.
- Top-level domains are the highest level of the DNS hierarchy and include generic TLDs like .com, .org, and .net, as well as country code TLDs like .us, .uk, and .ca.

- Each TLD has its own set of authoritative name servers, which are responsible for maintaining information about the domain names registered within that TLD.
- For example, the .com TLD has a set of authoritative name servers that are responsible for managing all of the domain names that end with .com.

Authoritative server

- An authoritative name server is a DNS (Domain Name System) server that has the original and definitive information about a particular domain.
- When a DNS resolver needs to look up information for a specific domain, it sends a query to the authoritative name server for that domain.
- The authoritative name server responds with the requested information, such as the IP address of the domain's web server or the mail server responsible for handling email for the domain.
- In other words, the authoritative name server is responsible for providing the correct and up-to-date information about a specific domain, such as the IP addresses of the domain's servers or the domain's DNS records.
- It is the final authority for a particular domain, meaning that its responses are considered the most accurate and reliable.

21. List out generic domain names and country level domain names.

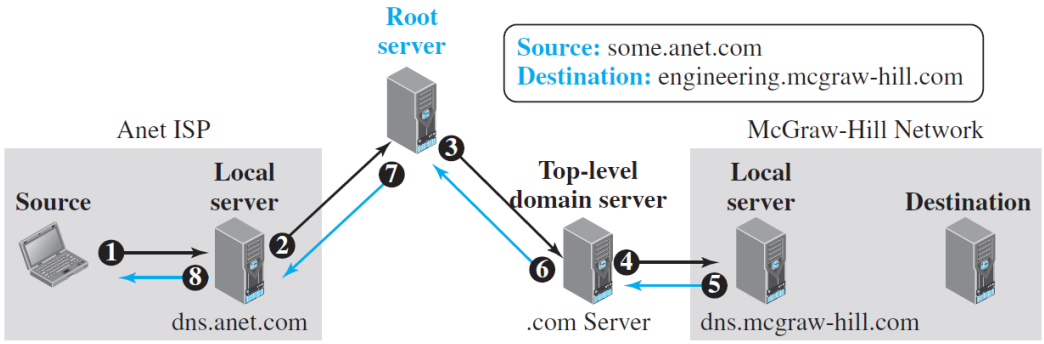
- Generic domain names
    - .com (commercial)
    - .org (organization)
    - .net (network)
    - .int (international)
    - .edu (education)
    - .gov (government)
    - .mil (military)
- Country level domains
    - .in (India)
    - .us (United States)
    - .uk (United Kingdom)
    - .ca (Canada)
    - .au (Australia)
    - .de (Germany)
    - .fr (France)
    - .jp (Japan)

22. What is name resolution? Explain different techniques of name resolution.

- The process of finding IP address of the particular domain is known as name resolution.
- There two ways of name resolution.
    - Recursive Name Resolution. (Recursive Query)
    - Iterative Name Resolution. (Iterative Query)

Recursive Name Resolution

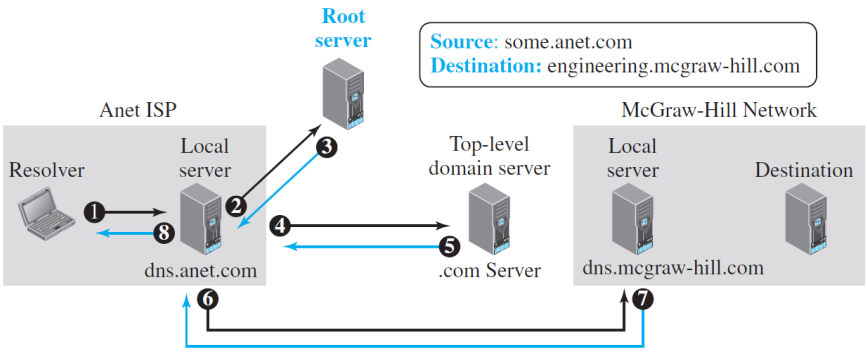
- Figure-1 shows a simple example of a recursive resolution.
- An application program running on a host named some.anet.com needs to find the IP address of another host named engineering.mcgraw-hill.com to send a message to.
- The source host is connected to the Anet ISP; the destination host is connected to the McGraw-Hill network.



Recursive Domain Name Resolution

- The application program on the source host calls the DNS resolver (client) to find the IP address of the destination host.
- The resolver, which does not know this address, sends the query to the local DNS server (for example, dns.anet.com) running at the Anet ISP site (event 1). This local DNS server does not know the IP address of the destination host either.
- It sends the query to a root DNS server, Root DNS servers do not normally keep the mapping between names and IP addresses, but a root server knows about one server at each top-level domain. The query is sent to this top-level-domain server (event 3).
- The top-level domain server does not know the name-address mapping of this specific destination, but it knows the IP address of the local DNS server in the McGraw-Hill company (for example, dns.mcgraw-hill.com). The query is sent to this server (event 4), which knows the IP address of the destination host.
- The local dns server of the McGraw-Hill company sent IP address of the specific domain back to the top-level DNS server (event 5).
- Then Top-level domain server sent IP address back to the root server (event 6).
- Then Root server sent IP address back to the ISP DNS server, which may cache it for the future queries (event 7),
- Finally, local DNS server sent the IP address back to the source host (event 8).

Iterative Name Resolution



Iterative Domain Name Resolution

- The application program on the source host calls the DNS resolver (client) to find the IP address of the destination host.

- The resolver, which does not know this address, sends the query to the local DNS server (for example, dns.anet.com) running at the Anet ISP site (event 1). This local DNS server does not know the IP address of the destination host either.
- It sends the query to a root DNS server, Root DNS servers do not normally keep the mapping between names and IP addresses, but a root server knows about one server at each top-level domain. Then Root DNS server gives the IP address of the Top-level domain server to Local DNS server(dns.anet.com). (event 3).
- Local DNS server sends the same query to top-level domain server.(.com server) (event 4).
- Top-level domain server does not know the name-address mapping of this specific domain, but it knows the IP address of the local DNS server in the McGraw-Hill company (for example, dns.mcgraw-hill.com). Then Top-level DNS server gives the IP address of the local DNS server in the McGraw-Hill company to the Local DNS server of Anet ISP. (event 5).
- The local dns of Anet ISP sends the same query to the local dns server of the McGraw-Hill company (event 6).
- The local dns server of the McGraw-Hill company sent IP address of the requested domain back to the local DNS server of Anet ISP , which may cache it for the future queries (event 7),
- Finally, local DNS server sent the IP address back to the source host (event 8).

23. Describe DNS Resource records.

- Resource Records are the records which contain information about host and sub domain of DNS.
- Resource records have in two representations.
  - Textual Format
  - Binary Format
- The generic format of the Resource Record in the Textual form is as follow.

OWNER NAME	TTL	CLASS	TYPE	TYPE SPECIFIC DATA

- OWNER NAME:-
  - The owner-name of the node in the zone file to which this record belongs.
- TTL:-
  - It is a 32 bit value which represents the time to live in seconds.
  - It indicates how long the RR may be cached. The value zero indicates the records should not be cached.
- CLASS: -
  - A 16 bit value which defines the protocol family or an instance of the protocol.
  - The normal value is IN=internet Protocol
- TYPE: -
  - The resource record type which determines the value(s) of the type-specific-data field.
- TYPE SPECIFIC DATA: -
  - Data content of each record is defined by the type and class values.
- Example:
  - Example.net 172800 IN NS a.iana-servers.net
    - In this example.net is the owner's name, 172800 is TTL in seconds, IN is internet class, NS is type i.e. Name Server and a.iana-servers.net is type specific data.
  - a.iana-servers.net 172800 IN A 199.43.132.53
    - In this a.iana-servers.net is the owner's name, 172800 is TTL in seconds, IN is internet class, A is for IPV4 address and 199.43.132.53 is the IP address.

- Some of the most used classes are as follows.
  - SOA- start of authority.
  - A – IPV4 address
  - AAAA- IPv6 Address
  - CNAME- canonical name. To create alias for the website.
  - MX- mail exchange
  - NS- name server
- The generic format of the Resource Record in the Binary form is as follow.

NAME	TTL	CLASS	TYPE	RDLEN RDATA

24. Explain DNS Registration Process?

- The diagram of the domain name registration process is shown below.
- The components of the domain name registration process are as follows
  - Registrant
  - Resellers
  - Registrars
  - Registry Operators
  - ICANN

- Registrant:
  - The registrant is end-user who want to purchase domain name.
- Resellers
  - It is web hosting company. For example BigRock, GoDaddy.
- Registrars
  - It is ICANN accredited organizations who do process of domain name registration.
- Registry Operators
  - It an authoritative master database of all domain names registered for each top-level domain name.
- ICANN
  - It is non-profit corporation for domain name system management.
  - It manages root server and name management system.
- Whenever any user wants to register domain names or purchase domain name. A user has to apply online through resellers that is web hosting company and has to pay subscription fees for that

domain. The Web hosting company will contact to registrar to register the particular domain name and information regarding it in its registry database.

25. Describe DDNS.

- In DNS, when there is a change, such as adding a new host, removing a host, or changing an IP address, the change must be made to the DNS master file. These types of changes involve a lot of manual updating. The size of today's Internet does not allow for this kind of manual operation.
- The DNS master file must be updated dynamically. The Dynamic Domain Name System (DDNS) therefore was designed to respond to this need.
- In DDNS, when a change in the binding between a name and an address is determined, the information is sent, usually by DHCP to a primary DNS server.
- The primary server updates the zone. The secondary servers are notified either actively or passively.
- In active notification, the primary server sends a message to the secondary servers about the change in the zone, whereas in passive notification, the secondary servers periodically check for any changes. In either case, after being notified about the change, the secondary server requests information about the entire zone (called the zone transfer).
- To provide security and prevent unauthorized changes in the DNS records, DDNS can use an authentication mechanism.
- For example,
    - if a web administrator is operating a small website with a domain name of www.example.com and an IP address of 192.0.2.0, anytime another user enters www.example.com into their browser, the DNS will direct them to the server at 192.0.2.0. If the admin's ISP dynamically changes the IP to 192.0.2.1, a dynamic DNS service can automatically update the admin's DNS records so that other users trying to visit www.example.com will now go to the correct IP address.

26. Describe Security of DNS.

- DNS is one of the most important systems in the Internet infrastructure; it provides crucial services to Internet users. Applications such as Web access or e-mail are heavily dependent on the proper operation of DNS. D
- NS can be attacked in several ways including:
    - The attacker may read the response of a DNS server to find the nature or names of sites the user mostly accesses. This type of information can be used to find the user's profile. To prevent this attack, DNS messages need to be confidential.
    - The attacker may intercept the response of a DNS server and change it or create a totally new bogus response to direct the user to the site or domain the attacker wishes the user to access. This type of attack can be prevented using message origin authentication and message integrity.
    - The attacker may flood the DNS server to overwhelm it or eventually crash it. This type of attack can be prevented using the provision against denial-of-service attack.
- To protect DNS, IETF has devised a technology named DNS Security (DNSSEC) that provides message origin authentication and message integrity using a security service called digital signature.
- DNSSEC, however, does not provide confidentiality for the DNS messages. There is no specific protection against the denial-of service attack in the specification of DNSSEC.

27. Differentiate HTTP and FTP

HTTP	FTP
It is used to transfer hypertext data between client and server.	It is used to transfer files between two devices on the network.
It is stateful protocol.	It is stateless protocol.
Default port number is 80.	It required two port number 20 and 21. 20 for data connection, 21 for control connection.
It is less secure than FTP.	It is more secure than HTTP.

28. Differentiate HTTP and SMTP

HTTP	SMTP
It is used to transfer hypertext data between client and server.	It is used to transfer email messages between client and server.
Default port number is 80	Default port number is 25
It can use both persistent and non-persistent connection type.	It supports only persistent type of connection.
It does supports both session management and cookies.	It does not support session management and cookies.
It does not require authentication for browsing a web page.	It requires authentication for sending emails.

29. Differentiate HTTP and DNS

HTTP	DNS
It is used to transfer hypertext data between client and server.	It is used to map URL to IP address.
Default port number is 80	Default port number is 53.
It uses TCP as the transport layer protocol.	It mostly uses UDP as the transport layer protocol.
It does supports both session management and cookies.	It does not support session management and cookies.
Data format is HTML	Data format is Resource Records