Module4

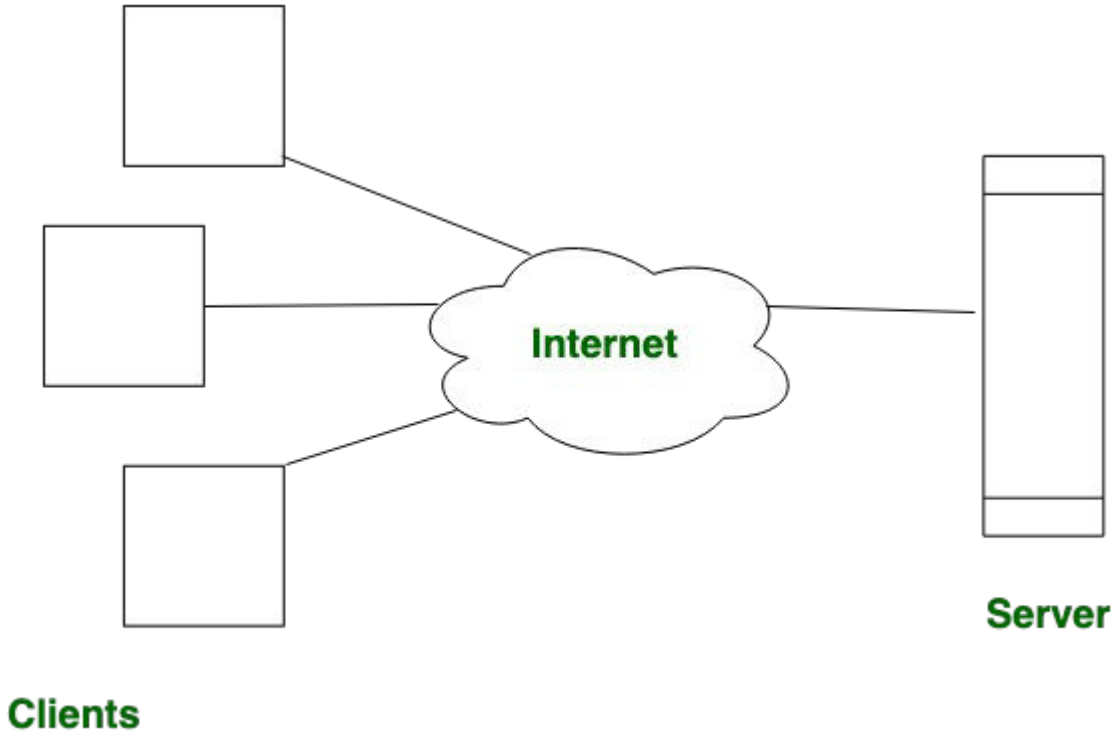
Functions of application layer

The functions of application layer are explained below −

- **User Interface:** It represents the user interface to low-level layers and multiple application processes.
- **Security:** It is responsible for the execution of the security tests at the user entity points.
- **File Transfer:** The application layer supports the file transfer access and management (FTAM). It enables customers to create files in a remote system to retrieve the documents from a remote system and to handle or control the files in a remote system.
- **E-mail:** It supports a basis for email forwarding and string.
- **Database Access:** It supports distributed database sources and global data about several objects and functions.
- **Addressing:** It is used for the connection between user and server. There is a requirement for addressing. When a user requests the server, the request includes the server address and its address. The server responds to the user request and the request consists of the destination address, i.e., client address.
- **Directory Services:** An application includes a distributed database that supports the global data about multiple objects and functions.

Difference between Client-Server and Peer-to-Peer Network

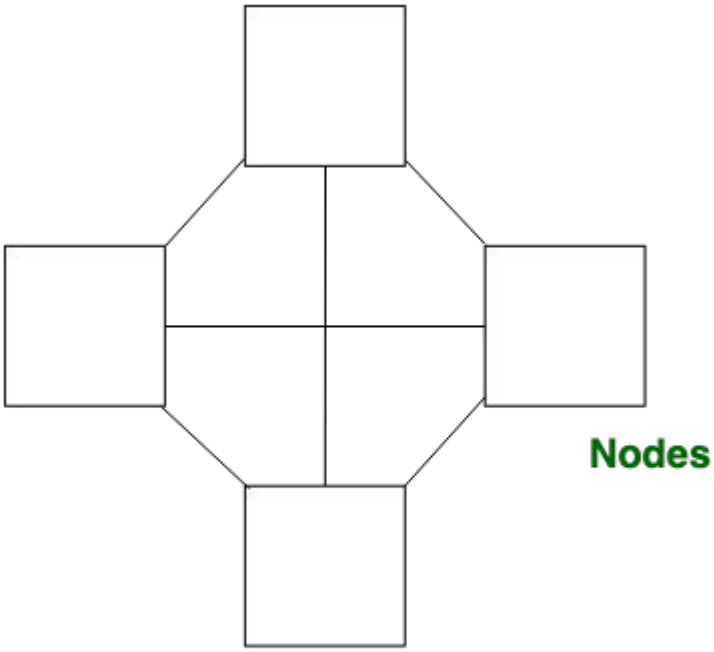
Client-Server Network: This model are broadly used network model. In Client-Server Network, Clients and server are differentiated, Specific server and clients are present. In Client-Server Network, Centralized server is used to store the data because its management is centralized. In Client-Server Network, Server respond the services which is request by Client.



Client-Server Network Model

Peer-to-Peer Network: This model does not differentiate the clients and the servers, In this each and every node is itself client and server. In Peer-to-Peer Network, Each and every node can do both request and respond for the services.

- Peer-to-peer networks are often created by collections of 12 or fewer machines. All of these computers use unique security to keep their data, but they also share data with every other node.
- In peer-to-peer networks, the nodes both consume and produce resources. Therefore, as the number of nodes grows, so does the peer-to-peer network's capability for resource sharing. This is distinct from client-server networks where an increase in nodes causes the server to become overloaded.
- It is challenging to give nodes in peer-to-peer networks proper security because they function as both clients and servers. A denial of service attack may result from this.
- The majority of contemporary operating systems, including Windows and Mac OS, come with software to implement peer



Peer-to-Peer Network Model

Difference between Client-Server and Peer-to-Peer Network:

S.NO	Client-Server Network	Peer-to-Peer Network
1.	In Client-Server Network, Clients and server are differentiated, Specific server and clients are present.	In Peer-to-Peer Network, Clients and server are not differentiated.
2.	Client-Server Network focuses on information sharing.	While Peer-to-Peer Network focuses on connectivity.
3.	In Client-Server Network, Centralized server is used to store the data.	While in Peer-to-Peer Network, Each peer has its own data.
4.	In Client-Server Network, Server respond the services which is request by Client.	While in Peer-to-Peer Network, Each and every node can do both request and respond for the services.
5.	Client-Server Network are costlier than Peer-to-Peer Network.	While Peer-to-Peer Network are less costlier than Client-Server Network.
6.	Client-Server Network are more stable than Peer-to-Peer Network.	While Peer-to-Peer Net
7.	Client-Server Network is used for both small and large networks.	While Peer-to-Peer Network is generally suited for small networks with fewer than 10 computers.

Features of application layer

The following are the features of application layer.

1. Efficient User Interface Design:
Application layer, the top layer of the OSI model serves as the Interface between user and application and also between user and the network. It provides the user, a way of accessing information present on the network through an application. Since the application layer is closest to the end user, both the user and the application layer can interact directly with the application.

2. Identification of Communicating Parties:
Application layer defines the way 'how' an application running on one system communicates with an application on another system. In addition to this, the layer also determines 'who' the communicating partners are and whether they are ready for communication or not (i.e., their identity and availability) whenever there is an application which has data to transmit.

3. Determination of Resource Availability:
For a communication to be successful a variety of resources are required. So, whenever a communication request is made, the application layer verifies whether the existing network resources are sufficient for handling the communication request. Thus, it determines the availability of resources.

4. Synchronization of communication:
The application layer is responsible for verifying either the two communicating parties are synchronized. It does this by ensuring that both the parties employ similar network protocols and that the communication is done in a cooperative manner.

5. Implementation of Protocols:
The application layer implements various protocols like Telnet, HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) etc. Among which the most widely used one is HTTP. This protocol is the basis for the World Wide Web. When the users need to access some web pages of a website, then they specify the name of the page in the URL and send it to the servers using the browser. This request is sent as HTTP request and response is also sent to the user using HTTP protocol.

Then communication protocols of application layer are used by, many applications that are responsible for providing network functionality. The other protocols are used for purposes like file transfer, emails and network news.

Application layer protocol

Hyper Text Transfer (HTTP) Protocol

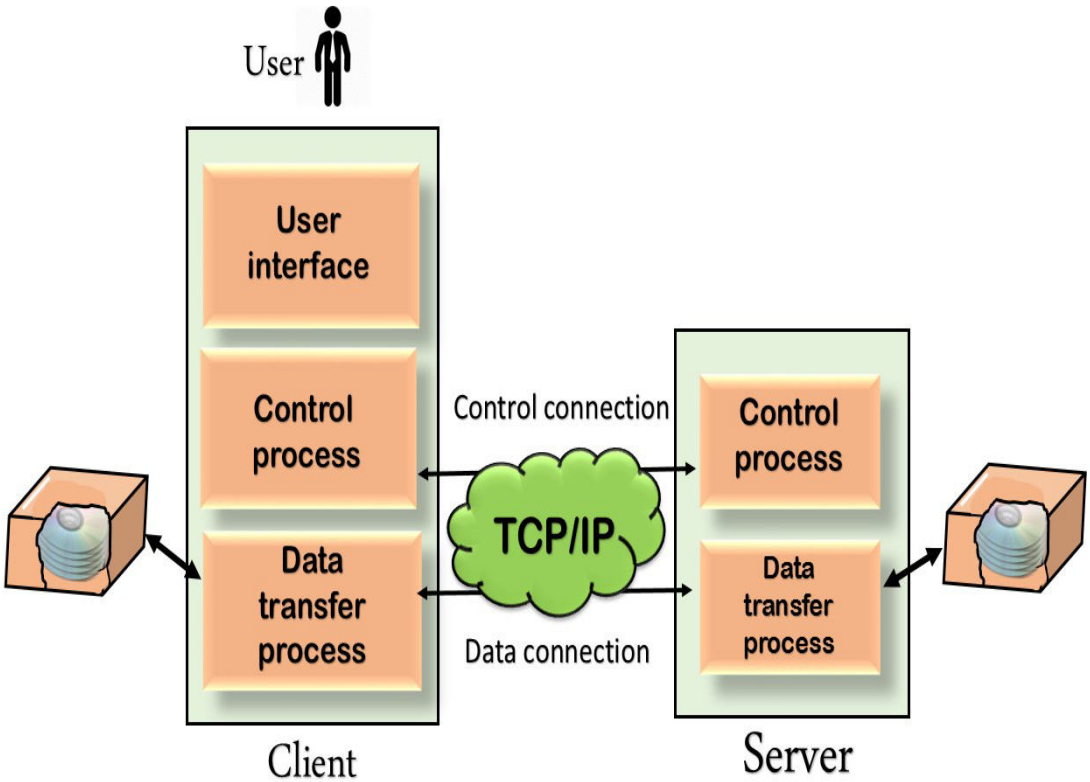
- HTTP is used to access the data on the *World Wide Web (www).*
- It is is an application layer protocol.
- It is connectionless, media-independent, TCP/IP based, and stateless protocol.
- The HTTP protocol uses ***port 80*** by default but it also can use other ports well.
- It transfers the data in the form of plain text, hypertext, audio, video, Html files, query results, etc.
- HTTP is similar to FTP *in terms of transferring* the files from one host to another host.

- But, HTTP is simpler than FTP because HTTP uses only one connection that is a ***data connection,*** in HTTP *there is no control connection* is used to transfer the files.
- HTTP is also similar to SMTP *in terms of data transferred* between the client and server.
- But, HTTP differs from SMTP in the way the messages are sent from the client to the server and from the server to the client.
- In HTTP messages are delivered immediately instead of stored and forward later happened in SMTP.
- It is further categorized as ***HTTP 1.0, HTTP 1.1, HTTP 2.0*** and ***HTTP 3.0.***

Why FTP?

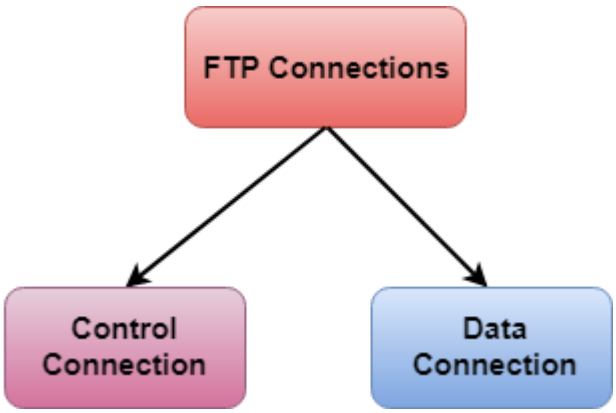
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Mechanism of FTP



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

There are two types of connections in FTP:



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

File Transfer Protocol (FTP)

- FTP is an application layer protocol.
- It is used to exchange files over the internet and enables the users to upload and download the files from the internet.
- It transfers both text and binary files over the Internet. But mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It transfers the data more reliably and efficiently.
- FTP uses TCP at the transport layer.
- FTP is a connection-oriented protocol.
- FTP is an out-of-band protocol as data and control information flow over different connections.
- FTP creates two connections between the computers one connection for the commands and replies called ***control connection*** and a second connection for data transfers called ***data connection.***

- FTP uses **Port number 21** for the ***control connection*** and **Port number 20** for the ***data connection***
- FTP is built on a ***client-server model architecture*** using the control connection and data connection between the client and server.

What is E-mail?

E-mail is defined as the transmission of messages on the Internet. It is one of the most commonly used features over communications networks that may contain text, files, images, or other attachments. Generally, it is information that is stored on a computer sent through a network to a specified individual or group of individuals.

Email messages are conveyed through email servers; it uses multiple protocols within the TCP/IP suite.

Email messages include three components, which are as follows:

1. **Message envelope:** It depicts the email's electronic format.
2. **Message header:** It contains email subject line and sender/recipient information..
3. **Message body:** It comprises images, text, and other file attachments.

The email was developed to support rich text with custom formatting, and the original email standard is only capable of supporting plain text messages. In modern times, email supports HTML (Hypertext markup language), which makes it capable of emails to support the same formatting as websites. The email that supports HTML can contain links, images, CSS layouts, and also can send files or "email attachments" along with messages. Most of the mail servers enable users to send several attachments with each message. The attachments were typically limited to one megabyte in the early days of email. Still, nowadays, many mail servers are able to support email attachments of 20 megabytes or more in size.

Simple Mail Transfer Protocol (SMTP)

- SMTP is mainly used for sending emails efficiently and reliably over the internet.
- SMTP is a push protocol and uses TCP at the transport layer.
- SMTP uses persistent TCP connections, so it can send multiple emails at once.
- SMTP is a connection-oriented, stateless, and in-band protocol.
- SMTP uses ***port number 25.***
- SMTP is a general set of interaction guidelines that allow the software to transmit electronic mail over the internet.
- It set up communication rules between servers and allows the exchange of emails between the users on the same or different computers.
- SMTP is a pure text-based protocol. It can only handle the messages containing 7 bit ASCII text and can not transfer other types of data like images, video, audio, etc.
- SMTP can not transfer executable files and binary objects.
- MIME extends the limited capabilities of email. It enables the users to send and receive graphics, audio files, video files, etc in the message.*MIME was specially designed for SMTP.*
- Sometimes ***SMTP Auth*** stands for SMTP Authentication has been provided for authentication purposes.

TELNET

Telnet is a network protocol used to virtually access a computer and to provide a two-way, collaborative and text-based communication channel between two machines.

It follows a user command Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocol for creating remote sessions. On the web, Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) simply enable users to request specific files from remote computers, while, through Telnet, users can log on as a regular user with the privileges they are granted to the specific applications and data on that computer.

-

World Wide Web

In this tutorial, we will be covering the concept of the World Wide Web in Computer Networks.

The **World Wide Web** or Web is basically a collection of information that is linked together from points all over the world. It is also abbreviated as **WWW.**

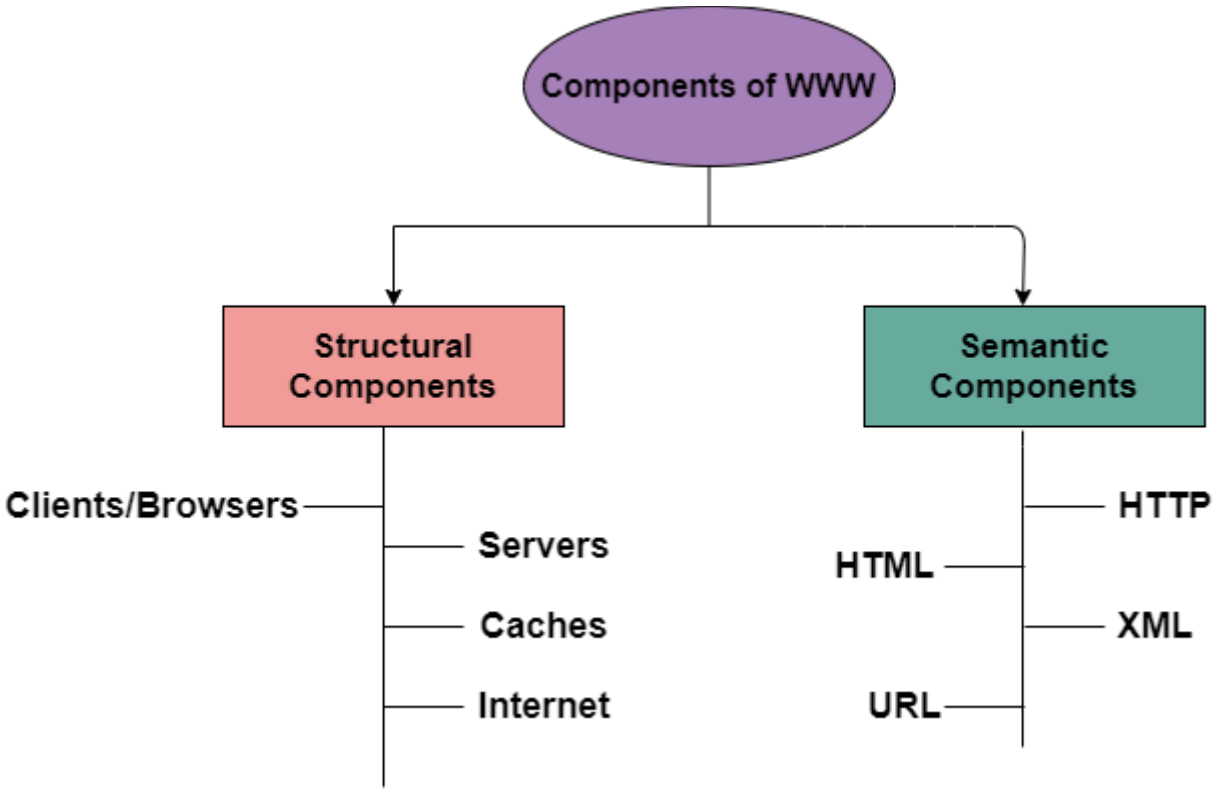
World wide web provides flexibility, portability, and user-friendly features.

- It mainly consists of a worldwide collection of electronic documents (i.e, Web Pages).
- It is basically a way of exchanging information between computers on the Internet.
- The WWW is mainly the network of pages consists of images, text, and sounds on the Internet which can be simply viewed on the browser by using the browser software.
- It was invented by Tim Berners-Lee.

Components of WWW

The Components of WWW mainly falls into two categories:

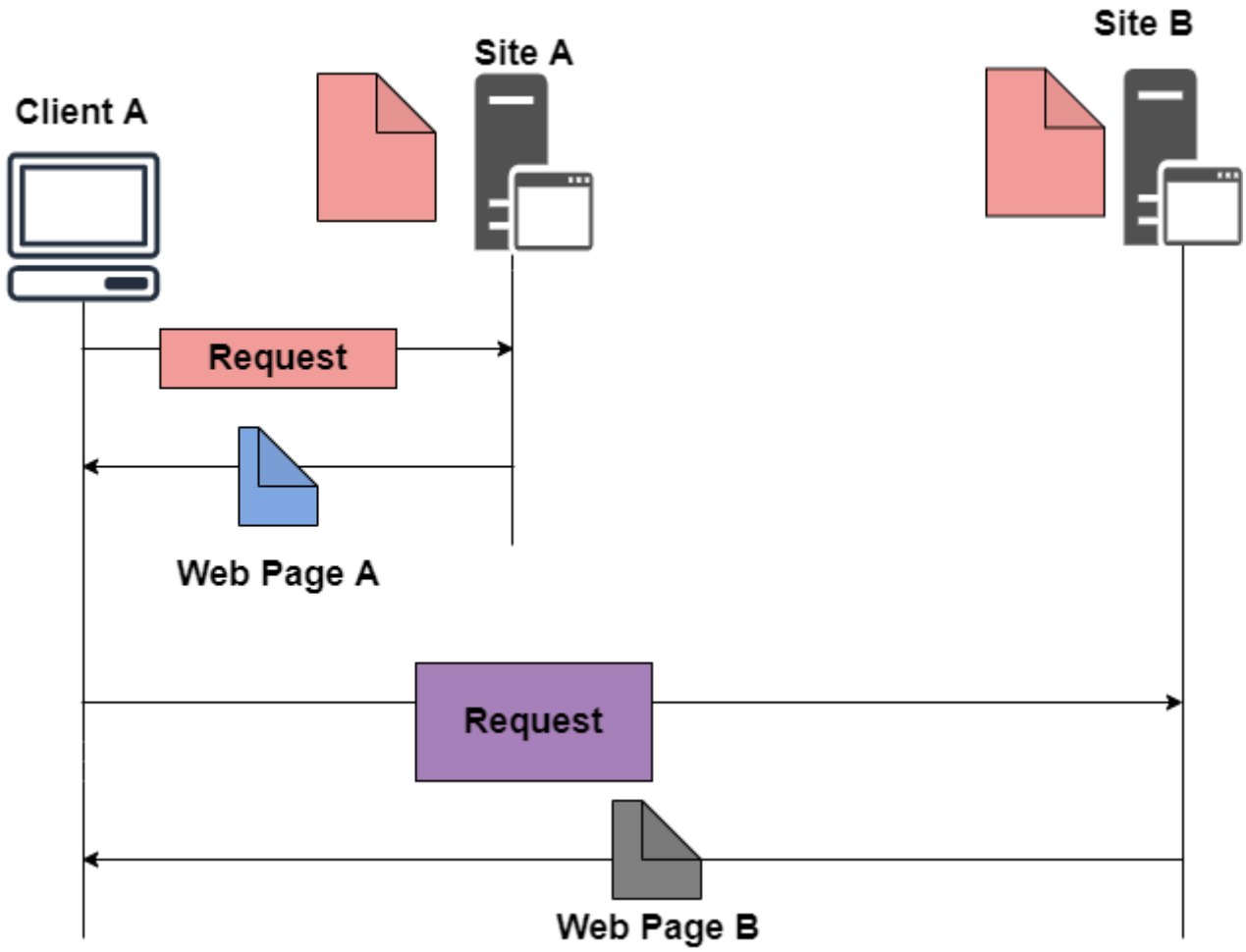
1. Structural Components
2. Semantic Components



Architecture of WWW

The **WWW** is mainly a distributed **client/server** service where a client using the browser can access the service using a server. The Service that is provided is distributed over many different locations commonly known as **sites/websites.**

- Each website holds one or more documents that are generally referred to as **web pages.**
- Where each web page contains a link to other pages on the same site or at other sites.
- These pages can be retrieved and viewed by using browsers.



In the above case, the client sends some information that belongs to **site A**. It generally sends a request through its browser (It is a program that is used to fetch the documents on the web). and also the request generally contains other information like the address of the site, web page(URL).

The server at **site A** finds the document then sends it to the client. after that when the user or say the client finds the reference to another document that includes the web page at **site B**.

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

1.Client/Browser

The Client/Web browser is basically a program that is used to communicate with the webserver on the Internet.

- Each browser mainly comprises of three components and these are:
    - Controller
    - Interpreter
    - Client Protocols
- The Controller mainly receives the input from the input device, after that it uses the client programs in order to access the documents.

- After accessing the document, the controller makes use of an interpreter in order to display the document on the screen.
- An interpreter can be Java, HTML, javascript mainly depending upon the type of the document.
- The Client protocol can be FTP, HTTP, TELNET.

2.Server

The Computer that is mainly available for the network resources and in order to provide services to the other computer upon request is generally known as the **server.**

- The Web pages are mainly stored on the server.
- Whenever the request of the client arrives then the corresponding document is sent to the client.
- The connection between the client and the server is TCP.
- It can become more efficient through multithreading or multiprocessing. Because in this case, the server can answer more than one request at a time.

3.URL

URL is an abbreviation of **the Uniform resource locator.**

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

URL mainly defines the four things:

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

Features of WWW

Given below are some of the features provided by the World Wide Web:

- Provides a system for Hypertext information
- Open standards and Open source
- Distributed.
- Mainly makes the use of Web Browser in order to provide a single interface for many services.
- Dynamic
- Interactive
- Cross-Platform

Advantages of WWW

Given below are the benefits offered by WWW:

- It mainly provides all the information for Free.
- Provides rapid Interactive way of Communication.
- It is accessible from anywhere.
- It has become the Global source of media.
- It mainly facilitates the exchange of a huge volume of data.

Disadvantages of WWW

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

- It is difficult to prioritize and filter some information.
- There is no guarantee of finding what one person is looking for.
- There occurs some danger in case of overload of Information.
- There is no quality control over the available data.
- There is no regulation.

2

Three basic types of web documents

Static.

A static web document resides in a file that it is associated with a web server. The author of a static document determines the contents at the time the document is written. Because the contents do not change, each request for a static document results in exactly the same response.

Dynamic.

A dynamic web document does not exist in a predifined form. When a request arrives the web server runs an application program that creates the document. The server returns the output of the program 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 can vary from one request to another.
Active
An active web document consists of a computer program that the server sends to the browser and that the browser must run locally. When it runs, the active document program can interact with the user and change the display continously.

DNS Namespace

The DNS name space is the set of all domain names that are registered in the DNS. These domain names are organized into a tree-like structure, with the top of the tree being the root domain. Below the root domain, there are a number of top-level domains, such as .com, .net, and .org. Below the top-level domains, there are second-level domains, and so on. Each domain name in the DNS name space corresponds to a set of resource records, which contain information about that domain name, such as its IP address, mail servers, and other information.

The DNS name space is hierarchical, meaning that each domain name can have subdomains beneath it. For example, the domain name "example.com" could have subdomains such as "www.example.com" and "mail.example.com". This allows for a very flexible and scalable naming structure for the Internet.

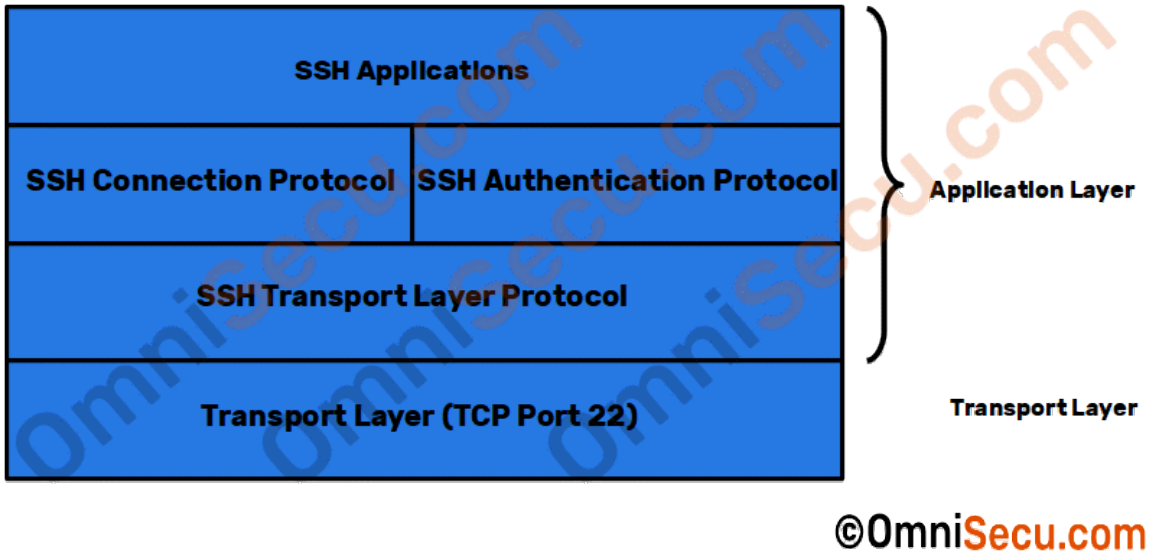
The DNS name space is managed by a number of organizations, including the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for coordinating the allocation of unique domain names and IP addresses.

The basic process of a DNS resolution follows these steps:

1. The user enters a web address or domain name into a browser.
2. The browser sends a message, called a *recursive DNS query*, to the network to find out which IP or network address the domain corresponds to.
3. The query goes to a recursive DNS server, which is also called a *recursive resolver*, and is usually managed by the internet service provider (ISP). If the recursive resolver has the address, it will return the address to the user, and the webpage will load.
4. If the recursive DNS server does not have an answer, it will query a series of other servers in the following order: DNS root name servers, top-level domain (TLD) name servers and authoritative name servers.
5. The three server types work together and continue redirecting until they retrieve a DNS record that contains the queried IP address. It sends this information to the recursive DNS server, and the webpage the user is looking for loads. DNS root name servers and TLD servers primarily redirect queries and rarely provide the resolution themselves.
6. The recursive server stores, or caches, the A record for the domain name, which contains the IP address. The next time it receives a request for that domain name, it can respond directly to the user instead of querying other servers.
7. If the query reaches the authoritative server and it cannot find the information, it returns an error message.

SSH COMPONENTS

SSH has mainly four components, SSH Transport Layer Protocol (SSH-TRANS), SSH Authentication Protocol (SSH-AUTH), SSH Connection Protocol (SSH-CONN) and SSH Applications, as shown in below image. These SSH components are supposed to run at the **Application layer** of **TCP/IP protocol suite**.



SSH Transport Protocol (SSH-TRANS)

SSH Transport Protocol (SSH-TRANS) is the component of SSH which allows to establish a secure connection between SSH client and SSH server over TCP. SSH Transport Protocol (SSH-TRANS) negotiates different security parameters between the client and the server, for example, encryption algorithm, HMAC algorithm etc, to create the secure tunnel between SSH client and SSH server.

SSH Connection Protocol (SSH-CONN)

SSH Connection Protocol (SSH-CONN) is the component of SSH, which allows to run multiple channels over the secure connection established.

SSH Authentication Protocol (SSH-AUTH)

SSH Authentication Protocol (SSH-AUTH) is the component of SSH which allows to authenticate the SSH client for the server.

SSH Applications

Once the secure connection is established between SSH client and SSH Server, SSH allows different application programs to use the established secure connection. Remote console login, SFTP (Secure File Transfer Protocol) etc., are the examples of different applications.

HTTP PERSISTENT V/S NONPERSISTENT

Persistent Connection	Non-Persistent Connection
The Persistent Connection is the second version of the HTTP, and it is also called as HTTP/1.1	The Non-Persistent connection was the first version of HTTP, and it is also called as HTTP/1.0
The Persistent connection will always be in the default mode.	The Non-Persistent connection will always be in the non-default mode.
The Persistent connection uses very less time because all the requests and responses are transferred in a single TCP.	The Non-Persistent connection uses more time when compared to Persistent connection because it uses new TCP for every new request and response.
The Persistent connection requires only one round trip time for all the objects.	The Non-Persistent connection requires two RTT's for every object present in the connection.
The request methods used in the Persistent connection are GET, HEAD, POST, PUT, DELETE, etc.	The request methods used in the non-Persistent connection are HEAD, POST, etc.
For downloading the multiple objects, the Persistent connection only uses a single connection	For downloading the multiple objects, the non-Persistent connection requires multiple connections
The usage of the CPU will be less in the persistent connection because it runs on a single TCP	The usage of the CPU will be more when compared to persistent connection because it runs on the multiple TCP's