

## Module 5

### Application Layer:

Introduction to Application Layer and its services. **Applications layer paradigms-** Client-Server Model, HTTP, E-mail, WWW, TELNET, DNS, and RSA algorithm.

The Application Layer is the topmost layer in the OSI (Open Systems Interconnection) model and the TCP/IP protocol suite. It serves as the interface between the application software running on a device and the underlying network services provided by lower layers of the OSI model. The Application Layer is responsible for providing a wide range of network services and protocols to support various applications and user interactions. Here is a detailed note on the Application Layer, including some of the key protocols and services it provides:

### Role of the Application Layer:

1. **User Interface:** The Application Layer provides the user interface for interacting with networked services and applications. It is where end-user applications, such as web browsers, email clients, and file transfer programs, reside.
2. **Data Presentation:** It is responsible for data formatting, encryption, and compression to ensure that data sent and received by applications is in a suitable format for processing.
3. **Application Services:** The Application Layer offers a wide range of services to support various applications, including data exchange, messaging, remote access, and more.

Protocols and Services Provided by the Application Layer:

#### 1. HTTP (Hypertext Transfer Protocol):

- **Service:** HTTP is used for web browsing and allows clients (browsers) to request and retrieve web pages from web servers.

- **Usage:** It is the foundation of the World Wide Web and is responsible for fetching web content.

#### 2. SMTP (Simple Mail Transfer Protocol):

- **Service:** SMTP is used for sending and routing email messages between email clients and servers.

- **Usage:** It handles the transmission of emails across the Internet and within email networks.

#### 3. POP3 (Post Office Protocol version 3) and IMAP (Internet Message Access Protocol):

- **Service:** POP3 and IMAP are email retrieval protocols used by email clients to fetch messages from email servers.

- **Usage:** They enable users to access and manage their email messages from different devices.

4. FTP (File Transfer Protocol):

- Service: FTP is used for transferring files between a client and a server.
- Usage: It is commonly used for uploading and downloading files to and from web servers.

5. DNS (Domain Name System):

- Service: DNS is responsible for resolving human-readable domain names (e.g., www.example.com) into IP addresses.
- Usage: It is essential for web browsing, email, and many other network services.

6. SNMP (Simple Network Management Protocol):

- Service: SNMP is used for monitoring and managing network devices, such as routers, switches, and servers.
- Usage: It facilitates network management tasks, including device configuration and performance monitoring.

7. Telnet and SSH (Secure Shell):

- Service: Telnet and SSH are used for remote access to networked devices and servers.
- Usage: Administrators can use these protocols to manage and configure remote devices securely.

8. HTTPS (Hypertext Transfer Protocol Secure):

- Service: HTTPS is a secure version of HTTP that encrypts data transmitted between web clients and servers.
- Usage: It ensures the confidentiality and integrity of sensitive web transactions, such as online banking and e-commerce.

9. DNSSEC (Domain Name System Security Extensions):

- Service: DNSSEC adds a layer of security to the DNS to prevent DNS spoofing and cache poisoning attacks.
- Usage: It enhances the trustworthiness of DNS data and helps ensure the authenticity of domain name resolutions.

10. NTP (Network Time Protocol):

- Service: NTP is used to synchronize the time on networked devices with a highly accurate time source.
- Usage: It ensures that all devices in a network are synchronized and have accurate time information.

11. SMTPS and IMAPS:

- Service: SMTPS and IMAPS are secure versions of SMTP and IMAP that use encryption for secure email communication.
- Usage: They provide secure email transmission and retrieval.

#### 12. VoIP Protocols (e.g., SIP, RTP):

- Service: VoIP (Voice over Internet Protocol) protocols enable voice and multimedia communication over IP networks.

- Usage: VoIP services like Skype and Zoom use these protocols for voice and video calls.

#### 13. Web Services Protocols (e.g., SOAP, REST, JSON-RPC):

- Service: Web services protocols enable communication and data exchange between distributed applications over the web.

- Usage: They are the foundation of modern web APIs and services used for various purposes, including data sharing and integration.

The Application Layer provides a wide range of protocols and services that facilitate communication and interaction between end-user applications and the underlying network infrastructure. These protocols support various applications, such as web browsing, email, file transfer, remote access, network management, and more, making the Application Layer a crucial component of modern networking and communication systems.

### **Difference Between SMTP, IMAP, And POP3 (+ Comparisons)**

You must have heard about SMTP, POP3, and IMAP quite often. They are TCP/IP protocols that have been in use for email delivery since 1981. Popular Services like Gmail, Outlook, and Yahoo use this underlying technology to transact over 300 Billion emails every day.

Since you are reading this online, chances are you've already used these three one way or another. Now before we set out to learn what SMTP, IMAP, and POP3 are, let's start with some basics

### **What Is A Protocol?**

A protocol is a set of standard rules that let electronic devices communicate with each other. Two devices supporting the same protocol can communicate effectively, no matter who their manufacturer is and also what type of devices they are.

TCP/IP stands for "Transmission Control Protocol/Internet Protocol". TCP/IP protocols aim to allow computers to communicate with each other over long-distance networks.

#### **How Are Emails Transferred?**

The following three parties are involved in transferring an email:

1. The sender
2. The recipient

### 3. A mail server

The email goes to the mail server from the sender, which allows the recipient to receive the email.

Now, to make a connection between the three parties, you need email protocols. SMTP, IMAP, and POP3 are precisely that. They are also the most commonly used TCP/IP protocols.

#### Journey Of An Email From A Sender To A Recipient

If the sender is jeff@amazon.com and the recipient is elon@spacex.com, following is how an email from the sender reaches the recipient,

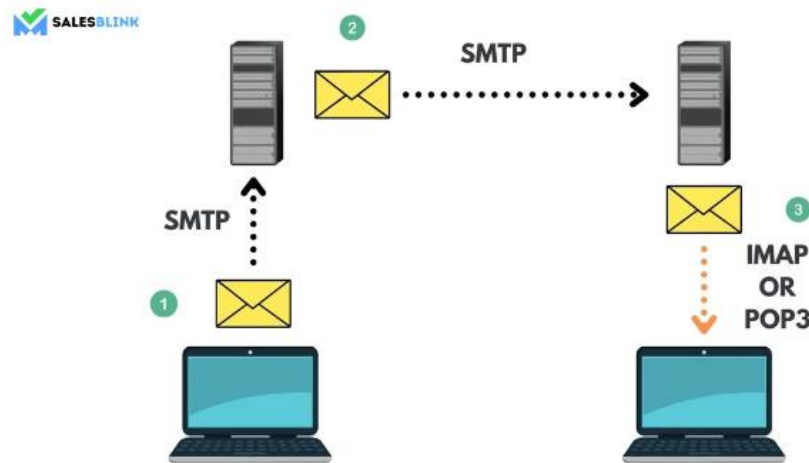


Fig 5.1 Email Process

1. The email client of the sender connects to that of the SMTP server (for example, smtp.gmail.com)
2. The SMTP server authenticates the email address of the recipient.
3. After the authorization of the recipient, the Gmail SMTP server sends the email to spacex.com's SMTP server.
4. The SMTP server of spacex.com checks whether elon@spacex.com is valid or not.
5. After that, the SMTP server sends the email to the IMAP/POP3 server.

What Are SMTP, IMAP, And POP3?

What Is SMTP?

SMTP stands for Simple Mail Transfer Protocol. It is the standard protocol for sending email messages using SMTP.

Your email client and internet servers use SMTP after you finish typing your email, upon hitting send. It moves your message over the internet and also makes it land into the recipient's mailbox.

SMTP servers are of two types: Relays and Receivers.

Relays accept the user's emails and route them to the recipient, while receivers deliver them to the mailbox after accepting the email from the relay servers.

## **Working of SMTP**

It involves the SMTP client sending commands and the SMTP server replying to them. The conversation has the following three stages –

1. SMTP handshake – Here, the SMTP client connects to the SMTP server
2. Email transfer – Launches the email transfer
3. Termination – The client and server bid goodbye to each other.

## **Advantages of SMTP**

Here are some of the advantages of SMTP:

**Reliable message delivery:** SMTP ensures that email messages are delivered reliably to the intended recipient. It employs error-checking mechanisms to verify that messages are delivered without any corruption or loss.

**Wide support:** SMTP is supported by virtually all email servers and clients, making it a universal standard for email communication.

**Simple and easy to use:** SMTP is a simple protocol that is easy to understand and use. It has a clear and straightforward message format that allows users to send and receive email messages quickly and easily.

**Scalable:** SMTP is a highly scalable protocol that simultaneously handles several email messages. This makes it ideal for use in large organizations where email communication is essential.

**Security features:** SMTP includes security features such as authentication and encryption to ensure email messages are transmitted securely over the Internet.

## **What Is IMAP?**

IMAP is an abbreviation for Internet Message Access Protocol. It is a popular protocol for receiving email messages. The most significant advantage of the IMAP protocol is that it lets you receive email on more than one computer (or device). That is because after getting delivered, the email stays on the mail server. In short, you can read your email on your office computer, the desktop at home, your tablet and your smartphone.

Also, it doesn't download the entire message until you open it. That helps in a faster initial connection and startup.

However, it won't perform well when you have a slow internet connection. And you won't be able to read your emails.

## Working of IMAP

The basic IMAP client and server interaction is as mentioned below,

1. The email client of the recipient connects with the server where the message is stored.
2. The recipient can view the message headers on the server.
3. If the recipient selects a message to read it, IMAP downloads that one for the recipient.

## Advantages of IMAP

Here are some of the advantages of IMAP:

**Access to emails from multiple devices:** As you just read above, IMAP allows users to access their email messages from multiple devices. The email messages are stored on a server, not on the user's device.

**Synchronization:** IMAP synchronizes the user's email messages across all devices. This means that any changes made to an email message on one device automatically reflect on all other devices.

**Offline access:** IMAP allows users to access their email messages even when they are offline. This is because a copy of the email messages is stored on the user's device, and changes are synchronized with the server when the user goes online.

**Efficient use of storage space:** IMAP allows users to manage their email messages more efficiently. This is because only the header of an email message is downloaded to the user's device, and the full message gets downloaded when the user opens it.

## What Is POP3?

Like IMAP, POP3 is another protocol for receiving emails. POP3 is an abbreviation for Post Office Protocol, whereas '3' refers to the version. Version 3 is the latest and most widely used one.

It is a simple protocol not having much to offer apart from the download.

POP3 downloads an email from the server to one computer (or device) and ends up removing it from the server once it gets downloaded on your computer. That means it won't be possible to read your email messages from multiple locations, which is not ideal.

The best part of this protocol are that you can read your emails when you are offline. And the use of the email server's storage is less.

However, as it works with one device and doesn't store the messages on the server, there is a need to backup your computer. Failing to do so will result in you losing all your emails when your computer dies.

## Working of POP3

There are four stages in a POP3 connection,

1. Authorization stage – The client connects with the server.
2. Transaction stage – The client retrieves the email
3. Update Stage – The server deletes the message stored
4. The client and server disconnect from each other.

## Advantages of POP3

Here are some of the advantages of POP3:

**Offline access:** As you just read, POP3 allows users to access their email messages even when they are offline. This is because the email messages are downloaded to the user's device and can be read and replied to at any time.

**Simple to set up:** POP3 is easy to set up and use, making it a popular choice for many email users. It only requires a few settings, such as the user's email address and password, to be entered into the email client.

**Efficient use of bandwidth:** POP3 is a bandwidth-friendly protocol, as it only downloads email messages when the user requests them. This means that it does not use unnecessary bandwidth, which is particularly useful for users with limited internet connectivity.

**Lower resource requirements:** POP3 has lower resource requirements than other email protocols, such as IMAP. This means that it works on less powerful hardware or in environments where resources are limited.

### 1. What is SMTP?

SMTP stands for Simple Mail Transfer Protocol. It is the standard protocol for sending email messages. Your email client and internet servers use SMTP after you finish typing your email, upon hitting send.

### 2. What Is IMAP?

IMAP is an abbreviation for Internet Message Access Protocol. It is a popular protocol for receiving email messages. The biggest advantage of the IMAP protocol is that it lets you receive email on more than one computer.

### 3. What Is POP3?

POP3 is an abbreviation for Post Office Protocol, whereas '3' refers to the version. Version 3 is the latest and most widely used one. It is a simple protocol not having much to offer apart from the download.

| IMAP vs SMTP   | POP3 vs SMTP  | IMAP vs POP3   |
|--|---|--|
| <p><b>IMAP VS SMTP</b></p> <p>IMAP IS USED TO RETRIEVE MESSAGES</p> <p>SMTP IS FOR SENDING DATA</p> <p>IMAP WORKS BETWEEN THE SERVER AND CLIENT FOR COMMUNICATION</p> <p>SMTP WORKS BETWEEN SERVERS TO TRANSFER INFORMATION</p> <p>IMAP IS A MESSAGE TRANSFER AGENT BETWEEN USER AND SERVER</p> <p>SMTP IS A MESSAGE TRANSFER AGENT BETWEEN SERVERS</p> <p>IMAP, USERS CAN ALSO ORGANISE EMAILS ONTO THE SERVER</p> <p>SMTP, YOU CAN ORGANISE EMAILS ON CLIENT STORAGE</p> | <p><b>SMTP VS POP3</b></p> <p>SMTP IS AN MTA OR MESSAGE TRANSFER AGENT FOR SENDING THE MESSAGE TO THE RECIPIENT</p> <p>POP3 IS AN MUA OR MESSAGE ACCESS AGENT TO ACCESS MESSAGES FROM THE MAILBOX</p> <p>SMTP IS REFERRED TO AS PUSH PROTOCOL</p> <p>POP3 IS REFERRED TO AS POP PROTOCOL</p> <p>SMTP SENDS THE EMAIL FROM SENDER'S DEVICE TO THE MAILBOX FROM RECEIVER'S MAILBOX</p> <p>POP3 RETRIEVES AND ORGANISE EMAILS FROM THE RECEIVER'S MAIL SERVER TO THE COMPUTER OF THE RECEIVER</p> <p>SMTP FUNCTIONS BETWEEN THE MAIL SERVERS OF THE SENDER AND RECEIVER</p> <p>POP3 FUNCTIONS BETWEEN THE RECEIVER AND THE MAIL SERVER OF THE RECEIVER</p> | <p><b>POP3 VS IMAP</b></p> <p>POP3 DOWNLOADS AN EMAIL FROM THE SERVER TO ONE COMPUTER AND THEN DELETES IT FROM THE SERVER</p> <p>IMAP STORES THE EMAIL ON THE SERVER AND SYNCs IT ACROSS SEVERAL DEVICES TO ACCESS OVER MULTIPLE CHANNELS</p> <p>POP3, YOU CAN'T ORGANISE EMAILS IN THE MAILBOX OF THE MAIL SERVER</p> <p>IMAP, YOU CAN ORGANISE EMAILS IN THE MAILBOX OF THE MAIL SERVER</p> <p>YOU CAN DOWNLOAD ALL THE EMAILS AT ONCE WITH POP3</p> <p>WHILE WITH IMAP, YOU SEE THE MESSAGE HEADER BEFORE YOU DOWNLOAD THE EMAIL</p> <p>THERE ARE TWO MODES OF POP3 - DELETE MODE AND KEEP MODE IN THE DELETE MODE</p> <p>WITH IMAP, THERE ARE SEVERAL COPIES OF THE EMAIL ON THE MAIL SERVER TO RETRIEVE IT EASILY</p> |

Table 5.0 Compare between IMAP SMTP POP3

Ports associated with the protocols

Here are the port numbers commonly associated with various network services:

| Port Number | Protocol description   |
|-------------|--|
| 20, 21      | port number 20 is used for FTP data while port number 21 is used for FTP Control |
| 23          | Used for TELNET  |
| 80, 8080    | HTTP   |
| 443         | HTTPS  |
| 161         | SMTP (Simple Mail Transfer Protocol)   |



|               |  |
|---------------|--|
| 110           | POP3   |
| 143           | IMAP i.e. Interim Mail Access Protocol   |
| 137, 138, 139 | port number 137 is used for BIOS Name service, 138 for NetBIOS-dgm, 139 for NetBIOS Datagram service |
| 22            | Used for SSH remote login protocol, SSH is short form of Secure Shell                                |
| 67, 68        | The port number 68 is used for DHCP client and 67 is used for DHCP server                            |
| 53            | DNS (Domain Name System)   |
| 69            | TFTP (Trivial File Transfer Protocol)  |
| 70            | Gopher services  |
| 79            | Finger   |
| 161           | SNMP   |
| 179           | BGP (Border Gateway Protocol)  |
| 389           | LDAP (Lightweight Directory Access Protocol)   |
| 5800, 5900    | VNC  |

## Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.

### DHCP does the following:

1. DHCP manages the provision of all the nodes or devices added or dropped from the network.
2. DHCP maintains the unique IP address of the host using a DHCP server.
3. It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

4. DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

There are many versions of DHCP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

## How DHCP works

DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

## The DHCP lease process works as follows:

1. First of all, a client (network device) must be connected to the internet.
2. DHCP clients request an IP address. Typically, client broadcasts a query for this information.
3. DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.
4. When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

## Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components:

1. **DHCP Server:** DHCP server is a networked device running the DHCP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
2. **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
3. **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
4. **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
5. **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.

6. **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

## Benefits of DHCP

There are following benefits of DHCP:

1. **Centralized administration of IP configuration:** DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.
2. **Dynamic host configuration:** DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.
3. **Seamless IP host configuration:** The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.
4. **Flexibility and scalability:** Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

## DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

1. DNS stands for Domain Name System.
2. DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
3. DNS is required for the functioning of the internet.
4. Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
5. DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
6. For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.
7. DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

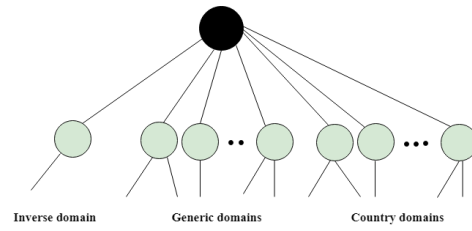


Fig 5.2 DNS Domain Distribution

| Label  | Description                            |
|--------|--|
| aero   | Airlines and aerospace companies       |
| biz    | Businesses or firms                    |
| com    | Commercial Organizations               |
| coop   | Cooperative business Organizations     |
| edu    | Educational institutions               |
| gov    | Government institutions                |
| info   | Information service providers          |
| int    | International Organizations            |
| mil    | Military groups                        |
| museum | Museum & other nonprofit organizations |
| name   | Personal names                         |
| net    | Network Support centers                |
| org    | Nonprofit Organizations                |
| pro    | Professional individual Organizations  |

Table 5.1 Different Domains and details

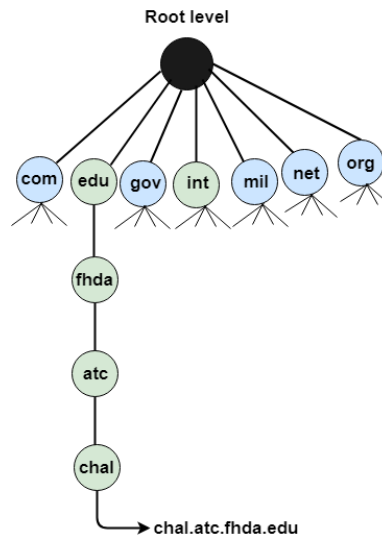


Fig 5.3 Domain Details and Distribution

## Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

## Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and asks for mapping an address to the name.

## Working of DNS

1. DNS is a client/server network communication protocol. DNS clients send requests to the server while DNS servers send responses to the client.
2. Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
3. DNS implements a distributed database to store the name of all the hosts available on the internet.
4. If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

## World Wide Web

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.



Fig 5.4 world wide web

the building blocks of the Web are web pages which are formatted in HTML and connected by links called "hypertext" or hyperlinks and accessed by HTTP. These links are electronic connections that link related pieces of information so that users can access the desired information quickly. Hypertext offers the advantage to select a word or phrase from text and thus to access other pages that provide additional information related to that word or phrase.

A web page is given an online address called a Uniform Resource Locator (URL). A particular collection of web pages that belong to a specific URL is called a website, e.g., [www.facebook.com](http://www.facebook.com), [www.google.com](http://www.google.com), etc. So, the World Wide Web is like a huge electronic book whose pages are stored on multiple servers across the world.

Small websites store all of their web pages on a single server, but big websites or organizations place their WebPages on different servers in different countries so that when users of a country search their site they could get the information quickly from the nearest server.

So, the web provides a communication platform for users to retrieve and exchange information over the internet. Unlike a book, where we move from one page to another in a sequence, on World Wide Web we follow a web of hypertext links to visit a web page and from that web page to move to other web pages. You need a browser, which is installed on your computer, to access the Web.

### Difference between World Wide Web and Internet:

Some people use the terms 'internet' and 'World Wide Web' interchangeably. They think they are the same thing, but it is not so. Internet is entirely different from WWW. It is a worldwide network of devices like computers, laptops, tablets, etc. It enables users to send emails to other users and chat with them online. For example, when you send an email or chatting with someone online, you are using the internet.

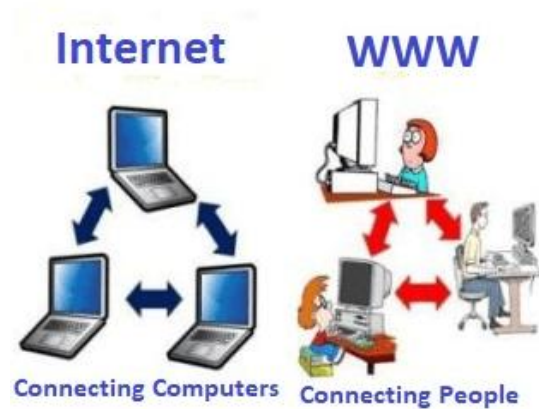


Fig 5.6 WWW vs Internet

But, when you have opened a website like [google.com](http://google.com) for information, you are using the World Wide Web; a network of servers over the internet. You request a webpage from your computer using a browser, and the server renders that page to your browser. Your computer is called a client who runs a program (web browser), and asks the other computer (server) for the information it needs.

### Comparison Table

| Parameters of Comparison | Internet   | World Wide Web  |
|--------------------------|--|---|
| Founded                  | It was established in the later 1960s.   | It was established in 1989.   |
| Meaning                  | It is a massive global network made up of millions of small subnetworks.                                       | It is a system of information where data is kept for public access. |
| Nature                   | There is a whole infrastructure there.   | It is a specific service contained within an infrastructure.        |
| Type                     | It emphasizes hardware.  | The emphasis is on software.  |
| Dependency               | It is independent of the world wide web.   | Here, the internet is a need.                                       |
| Use                      | It may be used for a variety of things, including banking, entertainment, research, education, and navigation. | It is employed to gain access to resources all across the world.    |

## How the World Wide Web Works?

Now, we have understood that WWW is a collection of websites connected to the internet so that people can search and share information. Now, let us understand how it works!

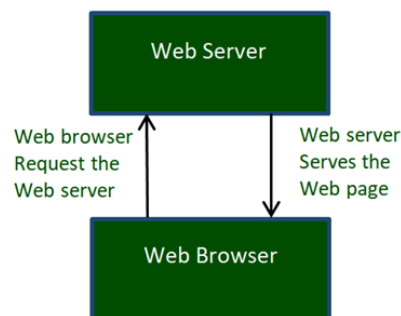


Fig 5.7 web server & web browser

The Web works as per the internet's basic client-server format as shown in the following image. The servers store and transfer web pages or information to user's computers on the network when requested by the users. A web server is a software program which serves the web pages requested by web users using a browser. The computer of a user who requests documents from a server is known as a client. Browser, which is installed on the user's computer, allows users to view the retrieved documents.

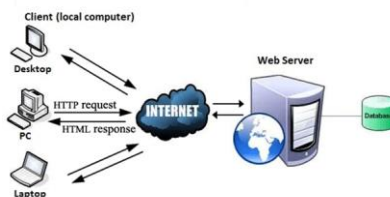


Fig 5.8 Internet



All the websites are stored in web servers. Just as someone lives on rent in a house, a website occupies a space in a server and remains stored in it. The server hosts the website whenever a user requests its WebPages, and the website owner has to pay the hosting price for the same.

The moment you open the browser and type a URL in the address bar or search something on Google, the WWW starts working. There are three main technologies involved in transferring information (web pages) from servers to clients (computers of users). These technologies include Hypertext Markup Language (HTML), Hypertext Transfer Protocol (HTTP) and Web browsers.

### Hypertext Markup Language (HTML):



HTML is a standard markup language which is used for creating web pages. It describes the structure of web pages through HTML elements or tags. These tags are used to organize the pieces of content such as 'heading,' 'paragraph,' 'table,' 'Image,' and more. You don't see HTML tags when you open a webpage as browsers don't display the tags and use them only to render the content of a web page. In simple words, HTML is used to display text, images, and other resources through a Web browser.

### Web Browser:

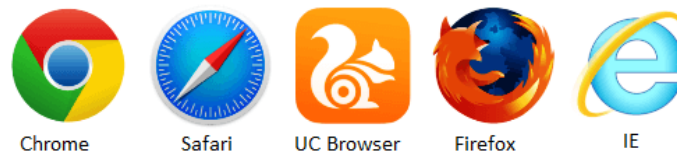


Fig 5.9 Browser

A web browser, which is commonly known as a browser, is a program that displays text, data, pictures, videos, animation, and more. It provides a software interface that allows you to click hyperlinked resources on the World Wide Web. When you double click the Browser icon installed on your computer to launch it, you get connected to the World Wide Web and can search Google or type a URL into the address bar.

In the beginning, browsers were used only for browsing due to their limited potential. Today, they are more advanced; along with browsing you can use them for e-mailing, transferring multimedia files, using social media sites, and participating in online discussion groups and more. Some of the commonly used browsers include Google Chrome, Mozilla Firefox, Internet Explorer, Safari, and more.

### Is It Possible to Use the Web Without Internet?

The opposite isn't true; it's actually impossible to access the internet without one. You must connect to a web resource (such as a website) on another server through the internet in order to access it. Otherwise, there is no connection between your device and the other device's network.

However, you may still access web resources on your local network by using a web browser. Your business, for instance, may have a network-required internal website that must be linked to in order to view (called the "intranet").

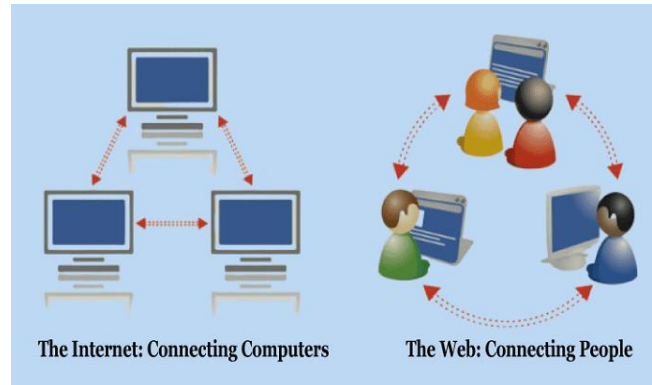


Fig 5.10 example

Although you may access and read this information using your web browser, you aren't technically connected to the internet because the server is part of your local network. It wouldn't function if you tried to view those pages from another city. As a result, even if you are accessing local resources off the internet, you are still able to take advantage of the World Wide Web's well-known organizational structure.

## Conclusion

Since the term World Wide Web (WWW) and the Internet are used synonymously, it is simple to overlook their key distinctions. Simply described, the World Wide Web (WWW) is essentially a central hub for connecting computers throughout the world to share information. On the contrary hand, the internet connects computers with innumerable other devices to create a vast network of interconnected systems.

There is a clear distinction between the Internet and the World Wide Web, despite the fact that many people mistake them for being the same thing. World Wide Web is software, whereas Internet is hardware.

In a nutshell, the World Wide Web is an internet-based program. As a result of this debate, it is clear the web is accessible over the internet and pages are displayed on the device's screen within a zone of global coverage. Therefore, we might conclude that whereas the web links individuals, the internet connects gadgets.