Module 8

The Application Layer

- Domain Name System (DNS)
- Electronic Mail
- The World Wide Web
- Streaming Audio and Video
- Content Delivery

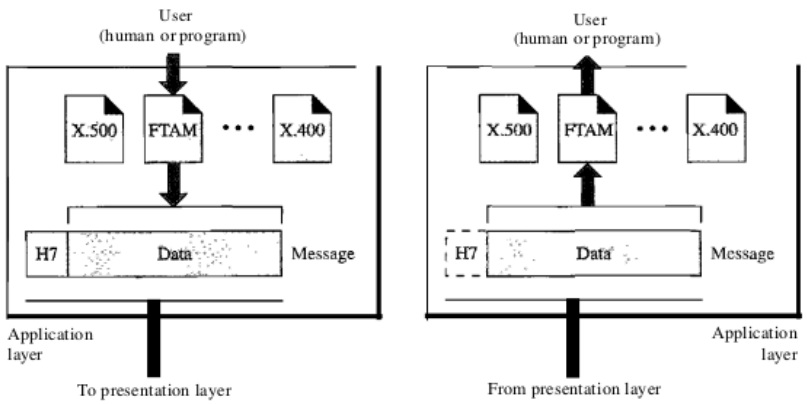
Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Following figure shows the relationship of the application layer to the user and the presentation layer.

Of the many application services available, the figure shows only three:

XAOO (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example employs XAOO to send an e-mail message.



The application layer is responsible for providing services to the user.

services provided by the application layer include the following:

Network virtual terminal. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

File transfer, access, and management. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

Mail services. This application provides the basis for e-mail forwarding and storage.

Directory services. This application provides distributed database sources and access for global information about various objects and services.

Domain Name System (DNS)

- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- 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.
- 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.

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.

Generic Domains

•It defines the registered hosts according to their generic behavior.

•Each node in a tree defines the domain name, which is an index to the DNS database.

•It uses three-character labels, and these labels describe the organization type.

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

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 ask for mapping an address to the name.

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- 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.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- 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.

DNS is a hostname for IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

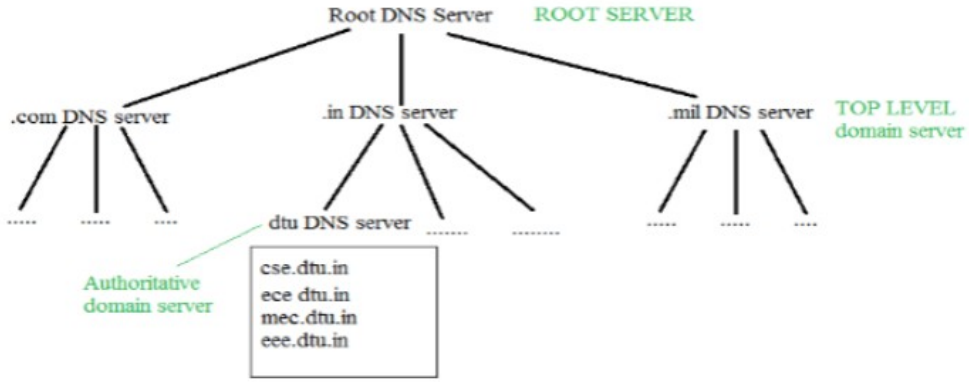
Requirement: Every host is identified by the IP address but remembering numbers is very difficult for the people also the IP addresses are not static therefore a mapping is required to change the domain name to the IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Domain: There are various kinds of DOMAIN:

1.**Generic domain:** .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.
2.**Country domain** .in (india) .us .uk

3.**Inverse domain** if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.

Organization of Domain:



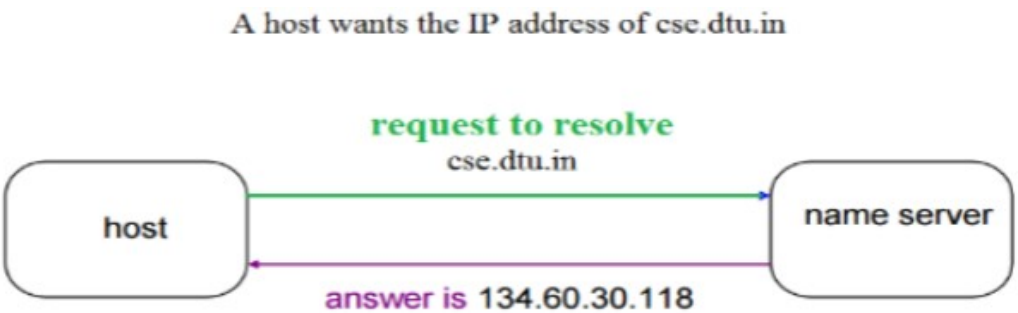
It is very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately, there should not be a lot of delay for that to happen organization of database is very important.

DNS record: Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.

Namespace: Set of possible names, flat or hierarchical. The naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value.

Name server: It is an implementation of the resolution mechanism. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.

Name to Address Resolution:



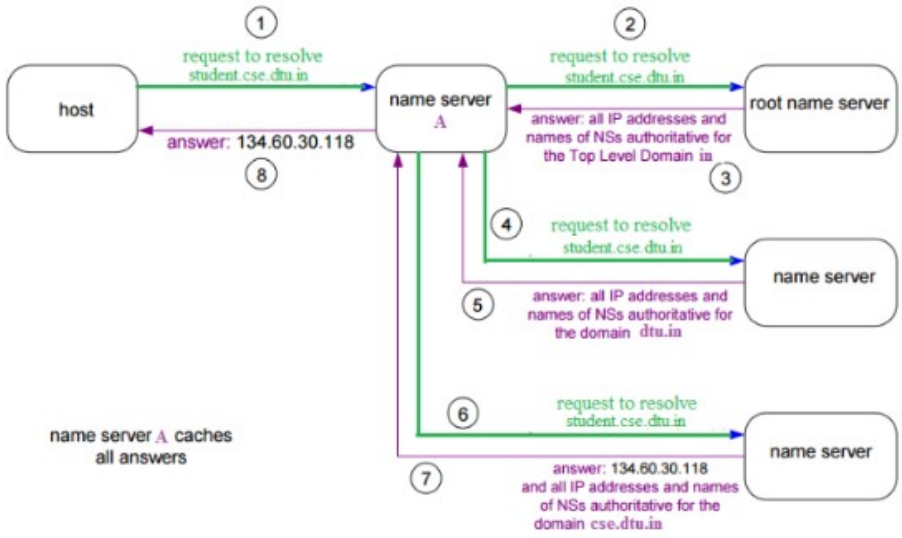
The host requests the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

Hierarchy of Name Servers Root name servers: It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and returns the IP address to the host.

Top level domain (TLD) server: It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know the names and IP addresses of each authoritative name server for the second-level domains.

Authoritative name servers are the organization's DNS server, providing authoritative hostName to **IP mapping for organization servers.** It can be maintained by an organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.

Domain Name Server



The client machine sends a request to the local name server, which , if root does not find the address in its database, sends a request to the root name server , which in turn, will route the query to an top-level domain (TLD) or authoritative name server. The root name server can also contain some hostName to IP address mappings. The Top-level domain (TLD) server always knows who the

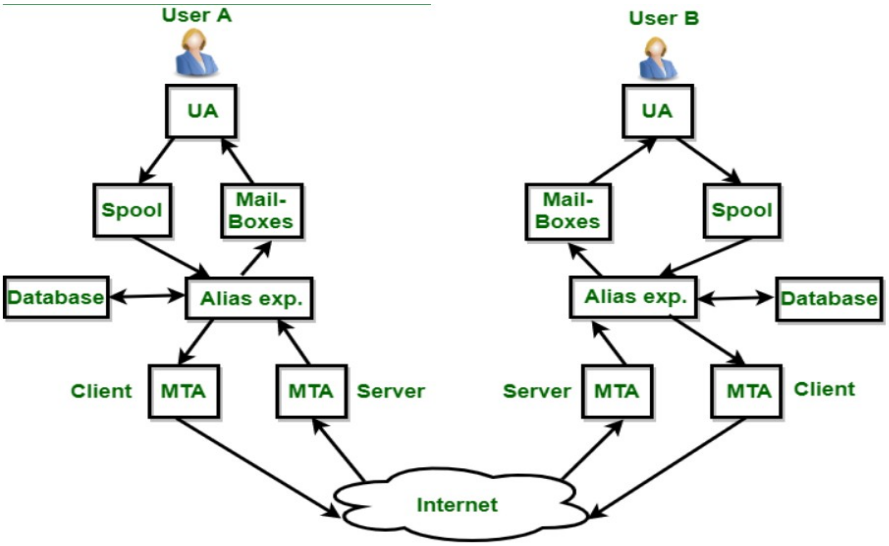
authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.

Electronic Mail

Electronic Mail (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a message in formatted manner (mail) to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called sender and person who receives mail is called recipient. It is just like postal mail service. Components of E-Mail System : The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

User Agent (UA) :The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.

Message Transfer Agent (MTA) : MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by **Simple Mail Transfer Protocol**.



Mailbox : It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.

Spool file : This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an alias, to represent several different e-mail addresses. It is known as mailing list, Whenever user have to sent a message, system checks recipient's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

Services provided by E-mail system :

- Composition – The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
- Transfer – Transfer means sending procedure of mail i.e. from the sender to recipient.
- Reporting – Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
- Displaying – It refers to present mail in form that is understand by the user.
- Disposition – This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

The World Wide Web

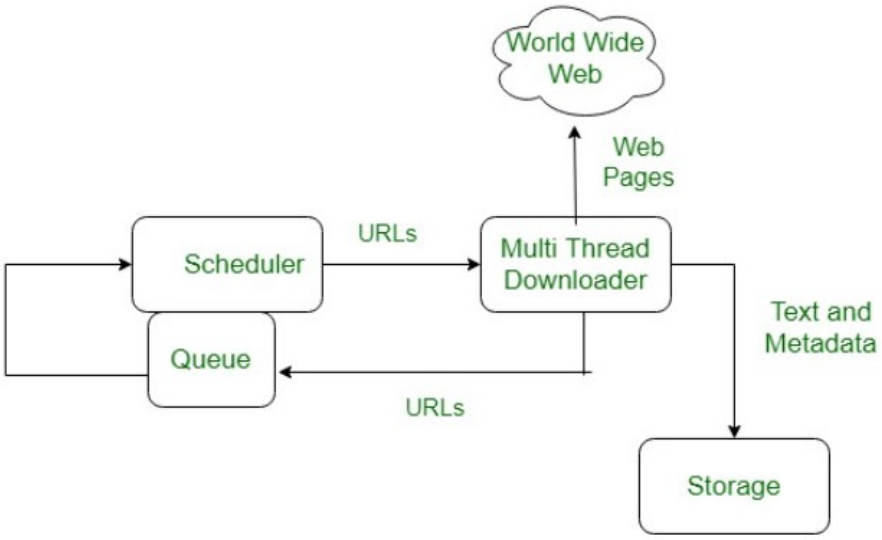
The World Wide Web is abbreviated as WWW and is commonly known as the web. The WWW was initiated by CERN (European library for Nuclear Research) in 1989.

WWW can be defined as the collection of different websites around the world, containing different information shared via local servers(or computers).

System Architecture:

From the user's point of view, the web consists of a vast, worldwide connection of documents or web pages. Each page may contain links to other pages anywhere in the world. The pages can be retrieved and viewed by using browsers of which internet explorer, Netscape Navigator, Google Chrome, etc are the popular ones. The browser fetches the page requested interprets the text and formatting commands on it, and displays the page, properly formatted, on the screen.

The basic model of how the web works are shown in the figure below. Here the browser is displaying a web page on the client machine. When the user clicks on a line of text that is linked to a page on the abd.com server, the browser follows the hyperlink by sending a message to the abd.com server asking it for the page.



Here the browser displays a web page on the client machine when the user clicks on a line of text that is linked to a page on abd.com, the browser follows the hyperlink by sending a message to the abd.com server asking for the page.

Working of WWW:

The World Wide Web is based on several different technologies: Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).

A Web browser is used to access web pages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interfaces provided by Web browsers. Initially, Web browsers were used only for surfing the Web but now they have become more universal. Web browsers can be used for several tasks including conducting searches, mailing, transferring files, and much more. Some of the commonly used browsers are Internet Explorer, Opera Mini, and Google Chrome.

Features of WWW:

- •HyperText Information System
- •Cross-Platform
- •Distributed
- •Open Standards and Open Source
- •Uses Web Browsers to provide a single interface for many services
- •Dynamic, Interactive and Evolving.
- •“Web 2.0”

Components of the Web: There are 3 components of the web:

1. Uniform Resource Locator (URL): serves as a system for resources on the web.
2. HyperText Transfer Protocol (HTTP): specifies communication of browser and server.
3. Hyper Text Markup Language (HTML): defines the structure, organisation and content of a webpage.

Streaming Audio and Video

How streaming works

Streaming files -- audio, video and others -- are stored on a server somewhere on the World Wide Web (WWW). When a user requests the file, it gets transmitted over the web as sequential packets of data that are streamed instantly. Since streaming data is broken down into data packets, its transmission is similar to that of other types of data sent over the internet.

The file is played within a browser on the client's device. An audio or video player hosted by the browser accepts the flow of data packets from the streaming service's remote server and interprets them as video or audio, then plays the media for the user. Unlike traditional media systems where files are downloaded and stored on the device, streaming media files are deleted automatically once the user ends the streaming.

Some streaming services rely on User Datagram Protocol (UDP) to stream their content, while others use Transmission Control Protocol (TCP). Both UDP and TCP are transport protocols used to move data packets across networks. TCP opens a dedicated connection before transmitting data, which makes it a more reliable protocol than UDP. However, TCP also takes longer to transmit data compared to UDP. TCP and UDP are both used with the Internet Protocol (IP).

Most streaming services use content delivery networks (CDNs) to store content in locations that are closer to users. Such proximity reduces streaming latency, speeds up content delivery and reduces buffering.

Streaming requirements

Streaming usually requires a reliable, high-speed internet connection because the media files must be retrieved from a remote location and then delivered to a user's local system with minimal lag or latency (delay). A slow connection decreases the speed at which the content is delivered, affecting the user's streaming experience.

Users must sign up with a streaming service to access and view media files on their local machines. They must also have a compatible display device with a resolution that's high enough to support incoming streaming video and a speaker that can play incoming streaming sound with adequate fidelity and clarity.

The receiving system must also include a media player to play the streaming content. The player can be part of a browser, a plugin, a separate program or a dedicated device.

treaming services and over-the-top platforms

There are many streaming services that offer different kinds of streaming content, such as movies, TV shows, music and podcasts. Some examples of well-known internationally available streaming services include the following:

- Netflix
- Amazon Prime
- Hulu
- Disney+
- ESPN+
- Apple TV+

These service providers are also known as over-the-top (OTT) platforms. OTT simply means TV and film content watched via a streaming service instead of through a cable or satellite television provider. OTT includes services such as Netflix and Hulu, as well as providers that offer live streams with niche content like sports, lifestyle, music or cartoons.

Streaming of videos involve, storing of prerecorded videos on servers.

- Users send request to those servers.
- Users may watch the video from the start till the end, and may pause it anytime, do a forward or reverse skip, or stop the video whenever they want to do so.

There are 3 video streaming categories

1. UDP Streaming
2. HTTP Streaming
3. Adaptive HTTP Streaming

Usually, today's system employs HTTP and Adaptive HTTP Streaming.

Common characteristic of these three streaming technique is that the extensive use of **Client-Side Buffering**.

Advantages of Client Buffering:

1.Client side buffer absorbs variations in server-client delay. Until the delayed packet is received by the client, the received-but not yet-played video will be played.

2.Even if bandwidth drops, user can view the video until the buffer is completely drained.

1. UDP STREAMING: UDP servers send video chunks (Chunk: unit of information that contains either control information or user data) to clients, based on client's consumption rate. It transmits chunks at a rate, that matches client's video consumption rate by clocking out video chunks over UDP over steady state.

Properties:

•UDP does not use congestion-control mechanism. Video chunks are encapsulated before transmission using RTT (Real-Time Transport) Protocol.

•Additional client-server path is maintained to inform the client state to server like pause, resume, skip and so on.

Drawbacks:

•Bandwidth is unpredictable and varying between client and server.

•UDP streaming requires a separate media control server like RTSP server(Real-Time Streaming Protocol) to track client state(pause, resume etc).

•Devices are configured with firewalls to block UDP traffic which prevents the reception of UDP packets to clients.

2. HTTP STREAMING: Video is stored in an HTTP server as a simple ordinary file with a unique URL. Client establishes TCP connection with server and issues a HTTP GET request for that URL. Server sends the video file along with an HTTP RESPONSE. Now the client buffer grabs the video and then displayed on user screen.

Advantages:

•Use of HTTP over TCP allows the video to traverse firewalls and NATs easily.

•Does not need any media control servers like RTSP servers causing reduction in cost of large-scale deployment over internet.

Disadvantages:

- Latency or lag between a video is recorded and played. This can make the viewers more annoyed and irritated. Only a few milliseconds delay is acceptable.
- Early pre-fetching of video, but, what if, the user stops playing the video at a early stage? Wastage of data is not appreciated.
- All clients receive the same encoding of the video, despite the large variations in bandwidth amount available to different clients and also for same client over time.

Uses: Youtube and Netflix uses HTTP streaming mechanism.

3. ADAPTIVE HTTP STREAMING: The major drawbacks of HTTP streaming, lead to development of new type of HTTP based streaming referred to as DASH (Dynamic Adaptive Streaming over HTTP). Videos are encoded into different bit rate versions, having different quality. The host makes a dynamic video request of few seconds in length from different bit versions. When bandwidth is high, high bit rate chunks are received hence high quality similarly, low quality video during low bandwidth.

Advantages:

•DASH uses the user to switch over different qualities of video on screen.

•Client can use HTTP byte-range request to precisely control the amount of pre-fetched video that is locally buffered.

•DASH also stores the audio in different versions with different quality and different bit-rate with unique URL.

Content Delivery

Over the last few years there has been a huge increase in the number of Internet users. YouTube alone has 2 Billion users worldwide, while Netflix has over 160 million users. Streaming content to such a wide demographic of users is no easy task. One can think that a straightforward approach to this can be building a large data center, storing all the content in the servers, and provide it to the users worldwide. But there are issues that arise when this approach is followed-

1.Firstly if the data center is in the USA and the user is in India there will be slower delivery of content.

2.Secondly, a single data center represents a single point of failure.

3.Thirdly, if some content is being accessed frequently from a remote area then it is likely to follow the same links, and this, in turn, results in wastage of bandwidth.

CDN – Content Distribution Network or Content Delivery Network is a solution that provides faster delivery of content to the users distributed worldwide.

What is a CDN?

A CDN is essentially a group of servers that are strategically placed across the globe with the purpose of accelerating the delivery of web content. A CDN-

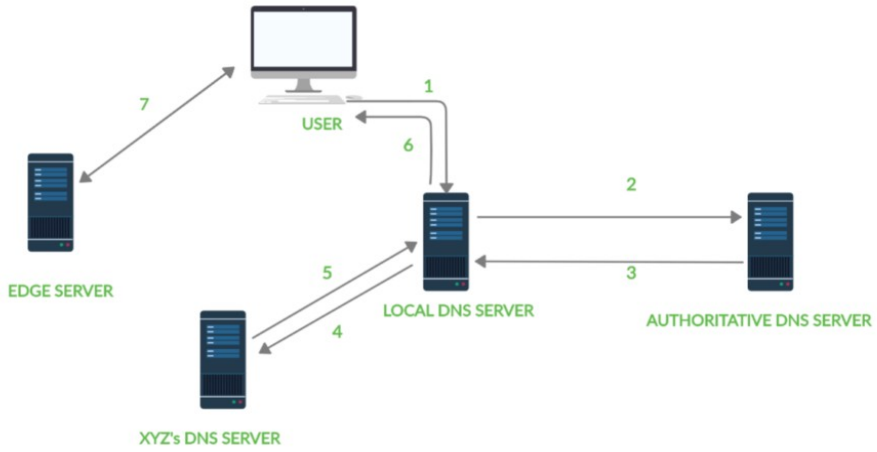
1. Manages servers that are geographically distributed over different locations.
2. Stores the web content in its servers.
3. Attempts to direct each user to a server that is part of the CDN so as to deliver content quickly.

How does CDN work?

- To minimize the distance between the visitors and your website's server, a CDN stores a cached version of original content in multiple geographical locations (a.k.a., points of presence/ PoPs).
- Each PoP contains a number of caching servers known as edge servers that are responsible for content delivery to visitors within its proximity.
- CDN caches content in many places at once, ensuring quick delivery of content.

Let's consider an example: Suppose you are hosting a website, wherein your origin server(server containing the primary source of your website's data, where website files are hosted) is located in Australia and a company XYZ provides you the CDN service. When a user in India clicks on a video on your website, the request goes to the user's local DNS server, which relays the request to the authoritative DNS server of your website. The authoritative DNS server then identifies that the user is situated far away and therefore relays the request to its XYZ's DNS server. Now the DNS query enters XYZ's network which provides the address of the edge server that is closest to the user to the Local DNS server. The video is delivered by this edge server. From this point onwards the local DNS server knows the address of the edge server. So whenever users within its network send a request for content from your website, the local DNS server shall relay the request to the edge server. CDN thus minimizes the number of hops required to deliver the data to a user's browser due to the POPs that are located near the user.

Following image depicts the same:



WITH CDN(2 SECONDS)

WITHOUT CDN(5 SECONDS)

References

https://www.javatpoint.com/e-mail

https://www.javatpoint.com/what-is-world-wide-web

http://www2.ic.uff.br/~michael/kr1999/6-multimedia/6_02-audioVideoOverWeb.html