## 1).Whenever you type some URL in a browser’s address bar and hit enter, a lot of activities occur behind the scenes including finding the correct server and obtaining the required documents from it. Now explain all of the behind the scene activities in detail.

## ➤ When you type a URL like "https://www.google.com" into a web browser and hit your enter key, there are a lot of things that go on before you finally get some output on your browser.

## Fortunately, all these things happen in a split second, so you hardly ever stop to think about them. Before I take the individual steps involved and explain them in detail, let me give you a general overview of everything that goes on within those few microseconds.

## Your computer sends a request to the domain name system (DNS) server which serves as an address book for all domain names. This then sends back the exact IP address of the server which https://www.google.com points to.

## Knowing this IP, your computer then establishes a connection with the server through the IP address. The type of this connection is known as Transmission Control Protocol (TCP) and your computer is able to establish this connection through the Internet Protocol (IP). This whole process is known as a "handshake".

## If your computer is behind a firewall, the firewall checks to ensure that the particular request you are making is allowed before permitting it. Also, if the server you are trying to access is also behind a firewall, a similar check will be done before you are finally able to connect to the server.

## After establishing the connection, your browser now sends a request for the webpage using an encryption protocol like Secure Sockets Layer (SSL) or Transport Layer Security (TLS) in order to encrypt the data that will be shared between your computer and the server. This type of encryption is what is responsible for the "s" in "https" which also implies that the connection is secure.

## Companies like Google with high traffic maintain a host of servers and for that matter they have a load balancer that receives most of the requests and sends it to a particular server. The request from your browser will therefore hit the load balancer first which will forward it to a specific server depending on the algorithm used by the load balancer.

## The server that receives the request then sends a response back to the load balancer which also forwards the response back to your browser. This response will mostly include HTML, CSS, and JavaScript files that make up Google's homepage.

## The HTML files returned tells the browser how to render the content of the page. The CSS file tells the browser how to style the content while the JavaScript file adds interactivity to the page.

## If there is a need for some dynamic content such as Google search results, then the web server will make a request to the application server, which in turn may make a request to a database server to get some data and send it back to the web server. The web server will then include these in the response that it sends back to the browser.

## Finally, the browser will render the page and display it to you.

➤For example, if we enter https://pu.edu.np into a browser, then

background activities that happen is explained below:

a) URL Parsing:

The browser parses the URL and breaks down the URL into its

components: the protocol (https), the domain name (pu.edu.np) and

the path to the specific resource on the server.

b) DNS Lookup:

Once the domain name is extracted, the browser performs a DNS

(Domain Name System) Lookup to find the IP address associated

with the domain. DNS is a massive database of millions of registered

domain names, each associated with a particular website#39;s name-

server and IP address. The browser sends a Lookup request (DNS

query) to a DNS server, which responds with the IP address

associated with the domain name.

c) Establishing a TCP Connection:

Knowing this IP, browser then establishes a TCP (Transmission

Control Protocol) connection with the server that host the website

through the IP address. This connection is established through the

Internet Protocol (IP). This whole process is known as &quot;handshake &quot;.

d) Firewall Check:

If your computer is behind a firewall, the firewall checks to ensure

that the particular request we are making is allowed before

permitting it. Also, if the server we are trying to access is also behind

a firewall, a similar check will be done before the connection is

finally made with the server.

e) SSK/ TLS Handshake:

After establishing the connection, if the protocol is &quot;https&quot;, the

browser and the server performs and Secure Sockets Layer (SSL) or

Transport Layer Security (TLS) handshake to establish a secure

connection.

f) Sending an HTTP Request:

Once the secure connection is established, the browser sends an

HTTP (Hypertext Transfer Protocol) Request to the server. The

request includes the HTTP method (e.g. GET, POST), the requested

resource path, headers (such as cookies, etc.) and other relevant

information.

## 2. To make an online presence or just transfer any data there are certain predefined rules to follow. Explain any 5 such commonly used protocols that serve different purposes of their own.

➤Internet Protocol (IP) is a protocol or set of rules for routing and

addressing packets of data so that they can travel across networks

and arrive at they can travel across networks and arrive at the

correct destination.

Any five commonly used protocols are:

a) SNTP (Simple Mail Transfer Protocol): SMTP is a communication

protocol used for delivering email message from the sender#39;s mail

server to a recipient#39;s mail server. The protocol uses the header of

the mail to get the mail id of the receiver and enters the mail into

the queue of outgoing mail. And as soon as it delivers the mail to

the receiving email id, it removes the email from the outgoing list.

b) POP (Post Office Protocol): POP is an internet standard protocol

which works on the application layer of OSI reference model and

is used by the local email software in order to retrieve emails

from the remote email server over the TCP/ IP connection. POP

does not allow any search facility. As this protocol supports offline

access to the message and so less internet usage time is required

by this.

c) IMAP (Internet Message Access Protocol): IMAP is a standard

protocol for accessing and managing email messages on a remote

mail server. It allows you to access your email messages from

multiple devices. You can keep your email messages on the server

and free up space on your local device. It allows you to organise

your email messages into folders on the server.

d) FTP (File Transfer Protocol): FTP is a client server protocol that

relies on two communication channels between client and server

a command channel for controlling the conversation and a data

channel for transmitting the file content. It is a standard internet

protocol provided by TCP/IP used for transmitting the files from

one host to another.

e) HTTP (HyperText Transfer Protocol): HTTP is a protocol used to

access the data on the World Wide Web (WWW). It can be used

to transfer data in the form of plain text, hypertext, audio, video,

and soon. It is similar to FTP as it also transfers files from one host

to another host. But, HTTP is simpler than FTP as HTTP uses only

one connection i.e. no control connection to transfer the files.

## 3).Explain about www and the internet. How is domain name conversion carried out?

➤ **WWW(world wide web)**:An information system on the Internet which allows documents to be connected to other documents by hypertext links, enabling the user to search for information by moving from one document to another.

**Internet**:• A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.

Domain name conversion, also known as Domain Name System (DNS) resolution, is the process of translating a human-readable domain name, such as "www.example.com," into an IP address, which is a unique numerical identifier assigned to each device connected to the Internet. The DNS system performs this conversion to locate the specific server hosting the requested website.

Here's a simplified explanation of how domain name conversion is carried out:

1. User enters a URL: The user enters a domain name (e.g., www.example.com) into the web browser's address bar.

2. Browser contacts DNS resolver: The web browser, by default, contacts a DNS resolver provided by the user's Internet service provider (ISP) or a public DNS resolver like Google DNS or Cloudflare DNS.

3. DNS resolver checks cache: The DNS resolver checks if it has the IP address for the requested domain name in its cache. If the IP address is found and is still valid (not expired), the resolver returns it to the browser. This cache helps speed up the conversion process.

4. Recursive query: If the IP address is not found in the resolver's cache, it initiates a recursive query. The resolver sends a request to the root name server, asking for the IP address of the top-level domain (TLD) server for the requested domain.

5. TLD server lookup: The root name server responds with the IP address of the TLD server responsible for the requested domain's TLD (e.g., ".com").

6. TLD server query: The resolver sends a request to the TLD server, asking for the IP address of the authoritative name server for the requested domain.

7. Authoritative name server lookup: The TLD server responds with the IP address of the authoritative name server responsible for the requested domain.

8. Authoritative name server query: The resolver sends a request to the authoritative name server, asking for the IP address of the specific domain name.

9. IP address retrieval: The authoritative name server responds with the IP address corresponding to the requested domain name.

10. Response to the browser: The DNS resolver relays the IP address back to the web browser.

11. Browser initiates connection: The web browser uses the obtained IP address to establish a connection with the web server hosting the requested website.

12. Web page retrieval: Once the connection is established, the browser requests the specific web page from the web server, and the server responds by sending the web page content back to the browser.

13. Web page rendering: The web browser receives the web page content and renders it, displaying the requested website to the user.

This entire process happens within seconds, allowing users to access websites using human-friendly domain names instead of having to remember and enter IP addresses directly.

## 4). Differentiate between the Web and the Internet.

➤

| WEB | INTERNET |
| --- | --- |
| A system of interconnected hypertext documents and resources accessed through the internet. | A global network of interconnected computers and networks. |
| Facilitates the retrieval and display of information using web browsers. | Enables communication and the exchange of data between devices worldwide. |
| Web pages ,web servers ,web browsers , web clients. | Computers, routers , servers, networking protocols. |
| Relies on protocols like HTTP,HTML,CSS,and JavaScript. | Relies on networking protocols like TCP/IP,DNS and SMTP. |
| Allows browsing websites ,accessing online content ,and interacting with web based applications. | Supports various servers like email,file sharing , messaging and online gaming. |
| Users internet with web content through web browsers and send requests to web servers. | Devices and networks communicate with each other using internet protocols. |
| Website ,web applications ,online servers like search engines and social media platforms. | Online servers ,email clients ,file transfer protocols, onlines gaming platforms. |

## 5).Write short notes on a Fully Qualified domain name with examples.

➤A Fully Qualified Domain Name (FQDN) is a complete domain name that specifies the exact location of a specific resource on the Internet. It consists of two main parts: the hostname and the domain name.

Here are some key points about Fully Qualified Domain Names:

1. Hostname: The hostname is the label that identifies a specific device or service within a domain. It usually represents a specific computer or server. For example, in the FQDN "mail.example.com," the hostname is "mail."

2. Domain Name: The domain name represents the broader grouping or organisation to which the hostname belongs. It consists of multiple labels separated by periods. For example, in the FQDN "mail.example.com," the domain name is "example.com."

3. Top-Level Domain (TLD): The top-level domain is the last part of the domain name and represents the highest level in the domain hierarchy. Common TLDs include ".com," ".org," ".net," and country-specific TLDs like ".us" or ".uk."

4. Fully Qualified Domain Name: A Fully Qualified Domain Name is formed by combining the hostname, domain name, and the top-level domain. It provides a complete and unambiguous address for a specific resource on the Internet. For example, "mail.example.com" is a Fully Qualified Domain Name.

## 6. What is a web browser? Differentiate between FTP and HTTP.

➤• A web browser (commonly referred to as a browser) is a software

application for accessing information on the World Wide Web.

• A software application that allows users to access and view websites

on the World Wide Web. Web browsers interpret HTML, CSS,

JavaScript, and other web technologies to render and display

web pages to users.

| FTP | HTTP |
| --- | --- |
| The term FTP is short form for file transfer protocols. | The term HTTP is short form for hypertext transfer protocols. |
| FTP refers to the set of rules that basically allow the process of uploading and downloading files from a computer to the internet. | HTTP refers to a set of rules that determine the process of transfer of various web pages over various computers present on the internet. |
| It makes use of the TCP . The FTP runs on port 20 and port 21 of TCP. | It also makes use of the TCP. The HTTP runs on port 84 of TCP. |
| It always requires authentication . | The HTTP requires no authentication. |
| It can easily transfer large files with chunks of data . | It is capable of efficiently transferring various small files. |
| We use FTP for downloading as well as uploading files between a server and a client over the internet . | We used HTTP for providing various web pages from the web browser to the web servers |

## 7. Differences between SMTP and POP.

➤

| SMTP | POP |
| --- | --- |
| The term SMTP short form for Simple Mail Transfer Protocols. | The term POP short form for POst Office Protocol. |
| It is used for sending messages. | It is used for accessing messages. |
| The port number of SMTP is 25, 465, and 587 for secured connection (TLS connection). | The port number of POP3 is 110 or port 995 for SSL/TLS connection |
| It is an MTA (Message Transfer Agent) for sending the message to the receiver. | It is an MAA (Message Access Agent) for accessing messages from mailboxes. |
| SMTP is also known as the PUSH protocol. | POP3 is also known as POP protocol. |
| SMTP transfers the mail from sender’s computer to the mailbox present on receiver’s mail serve | POP3 allows you to retrieve and organise mail from the mailbox on the receiver mail server to the receiver's computer. |
| It is implied between sender mail server and receiver mail server. | It is implied between receiver and receiver mail server. |

## 8.Differences between URI and URL.

➤

| URI | URL |
| --- | --- |
| The term URI short form for Uniform Resource Identifier. | The term URL short form for Uniform Resource Locator. |
| URI is the superset of a URN and a URL. | URL is the subset of URI. |
| URI identifies a resource and differentiates it from others by using a name, location, or both. | URL identifies the web address or location of a unique resource. |
| URI contains components like a scheme, authority, path, and query. | URL has similar components to a URI, but its authority consists of a domain name and port. |
| An example of a URI is **ISBN 0-476-35557-4.** | An example of a URL would be **https://hostinger.com.** |
| URI scheme can be a protocol, a specification, or a designation like HTTP, file, or data. | URL scheme is a protocol, such as **HTTP and HTTPS**. |
| URI is usually used in XML, tag library files, and other files, such as JSTL and XSTL. | URL is mainly for searching web pages on the internet. |

## 9. Differences between LAN, MAN, and WAN.

➤

| LAN | MAN | WAN |
| --- | --- | --- |
| LAN stands for Local Area Network. | MAN stands for Metropolitan Area Network. | WAN stands for wide area network. |
| LAN’s ownership is private. | MAN’s ownership can be private or public. | While WAN also might not be owned by one organisation. |
| LAN’s ownership is private. | MAN’s ownership can be private or public. | While WAN also might not be owned by one organisation. |
| Operates in small areas such as the same building or campus. | Operates in large areas such as a city. | Operates in larger areas such as countries or continents. |
| The transmission speed of a LAN is high | While the transmission speed of a MAN is average. | Whereas the transmission speed of a WAN is low. |
| The propagation delay is short in a LAN. | There is a moderate propagation delay in a MAN. | Whereas, there is a long propagation delay in a WAN. |
| LAN’s design and maintenance are easy. | While MAN’s design and maintenance are more difficult than LAN. | Whereas WAN’s design and maintenance are also more difficult than LAN as well as MAN. |

## 10).What is MIME? Explain its headers.

➤ MIME stands for Multipurpose Internet Mail Extensions. MIME

is an email extension protocol which allows both ASCII and non-ASCII

data to be sent via email. IT also lets users exchange audio, video,

images and application programs, over email.

MIME headers are:

a) MIME Version: It defines the version of the MIME protocol. This

header usually has a parameter value 1.0, indicating that the

message is formatted using MIME.

b) Content Type: It describes the type and subtype of information to

be sent in the message. These messages can be of many types

such as text, image, audio, video. They also have many subtypes

such that the subtype of the image can be png or jpeg. Similarly,

The subtype of videos can be webm, mp4, etc.

c) Content Type Encoding: In this field, it is told which method has

been used to convert mail information into ASCII or binary

number, such as 7-bit encoding, 8-bit encoding, etc.

d) Content Id: In this field, a unique &quot;Content Id &quot; number is

appended to all email messages so that they can be uniquely

identified.

e) Content Description: This field contains a brief description of the

content within the email. This means that information about

whatever is being sent in the mail is clearly in the &quot;content

Description &quot;.

f) Content Disposition: This header provides information about how

to present a message or body part. When a body part has an

attached file, this header will include a file name parameter.

11.Explain the evolution of the internet and the web.

Ans: In the 1960's the U.S. Department of Defense (DoD) became interested in developing a new large scale computer network in the 1960s. The purpose of this network were communications, problem sharing, and remote computer access for researchers working on defence related contracts. One fundamental requirement was that the network be sufficiently robust. As it was funded by DoD's Advanced Research Projects Agency (ARPA), the network was called ARPANET. The primary use of ARPAnet was simple text-based communication through email. In 1989, a small group of people led by Tim Berners Lee at CERN (European Council for Nuclear Research) proposed a new protocol for the Internet as well as a system of document access to use it. The intent of this new system, which the group named the World Wide Web, was to allow scientists around the world to use the Internet to exchange documents describing their work. The proposed new system was designed to allow a user anywhere on the Internet to search for and retrieve documents from a database on any number of different document serving computers.

12. Explain CMS (Content Management System).

CMS is a software that helps users create, edit, collaborate, publish and store digital content. CMS are typically used for ECM (Enterprise Content Management) and WCM (Web Content Management). CMS provides a graphical user interface with tools to create, edit and publish web content without the need to write code from scratch CMS has two components. They are: a)CMA (Content Management Application): It enables users to design, create, modify and remove content from a website without developer knowledge. b)CDA (Content Delivery Application): It provides the backend services that support management and delivery of the content once a user creates it in the CMA. Some features of CMS are: Intuitive indexing, search and retrieval: These features index all data for easy access through search functions and enable users to search by attributes such as publication dates, keywords or author. Format management: This helps turn scanned paper documents and legacy electronic documents into html or pdf documents. Revision features: These features enable content to be updated and edited after initial publication. Revision control also tracks any changes individuals make to files. Publishing: This functionality enables individuals to use a template or a set of templates that an organisation approves for content creation and modification.

## 23).How to register a domain name? Differentiate top-level and second-level domains.

➤A domain name is registered by following ways:

1.Find a domain name registrar.

2.Search for your domain name.

3.Finalize your domain name choice.

4.Choose a domain name suffix, such as .com or .net.

5.Purchase the domain name.

6.Add Domain ID protection.

7.Verify ownership

1. Find a domain name registrar: The non-profit Internet Corporation for Assigned Names and Numbers (ICANN) oversees the entire system of domain names, and it allows outside companies, called domain registrars, to sell and manage domain names. You will need to register your domain name through a registrar. Some of the most popular domain registrars include GoDaddy, Bluehost, and Domain.com, although there are many more to choose from. Be sure to carefully consider pricing and policies for each one before choosing your domain registrar, as it will be managing your domain name.

2. Search for your domain name's availability: Once you have found the right domain registrar for you, you'll need to search for your domain name using the registrar's search bar. There are millions of domain names out there, with thousands more added daily. If you have your heart set on a domain name before doing a search, you might be disappointed to find it is already taken. Keep an open mind and incorporate important keywords into your domain when appropriate.

3. Finalise your domain name choice: Once you've brainstormed several domain options, consider which ones are available and choose the one that fits your brand best and will also be easy for users to find. 4. Choose a domain name suffix, such as .com or .net: After settling on the domain name, consider the suffix. The most popular suffix is .com, although .net and .org are also popular. These are considered to be top-level domains, or the highest-level domain suffixes in the domain naming system. There are also other varieties to consider, such as country code top-level domains. These domain names end in a suffix that is particular to a specific country. A website in Germany might end in .de, for example. Finally, there is another class of domain name suffixes called "sponsored, top-level domains," which are sponsored by a specific community related to the domain name. For example, .gov is for the U.S. government and .edu is for education organisations. For most websites, .com is the best suffix for its ease of use, but if you have a specialised website, you might consider a country code or sponsored top-level domain.

5. Purchase the domain name: When you have settled on the domain name and a suffix, you will pay to register the domain name with the domain registrar. This is not a one-time purchase, however. Typically, you will pay to own the domain name for one year, after which you can renew your registration for a fee. You can expect a registration fee of about $10 to $15.

6. Add domain ID protection: When you register a domain name with ICANN, you must provide your contact information including your name, phone number, physical address, and email address. As soon as your domain name is registered, this contact information becomes available to the public — unless you pay for domain privacy through your domain registrar. This domain privacy will shield your information from view, keeping your personal information safe from spammers or worse, identity thieves.

7. Verify ownership: After registering your domain, you'll receive an email confirmation with instructions to verify ownership of the domain.

## 24.Write short notes on

## a. WAP

## b. IMAP

## c. Centralised and distributed system

## d. Domain Name system.

## e. Web hosting

Ans:

**a. WAP:**

➤WAP is the de facto worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants, and other wireless terminals −WAP Forum WAP stands for Wireless Application Protocol. The dictionary definition of these terms are as follows –

•Wireless − Lacking or not requiring a wire or wires pertaining to radio transmission.

•Application − A computer program or piece of computer software that is designed to do a specific task.

•Protocol − A set of technical rules about how information should be transmitted and received using computers.

Working mechanism:

•The user selects an option on their mobile device that has a URL with Wireless Markup language (WML) content assigned to it.

•The phone sends the URL request via the phone network to a WAP gateway using the binary encoded WAP protocol.

•The gateway translates this WAP request into a conventional HTTP request for the specified URL and sends it on to the Internet.

•The appropriate Web server picks up the HTTP request.

Advantages of Wireless Application Protocol (WAP):

Following is a list of some advantages of Wireless Application Protocol or WAP:

•WAP is a very fast-paced technology.

•It is an open-source technology and completely free of cost.

•It can be implemented on multiple platforms.

•It is independent of network standards.

Disadvantages of Wireless Application Protocol (WAP):

Following is a list of some disadvantages of Wireless Application Protocol or WAP:

•The connection speed in WAP is slow, and there is limited availability also.

•In some areas, the ability to connect to the Internet is very sparse, and in some other areas, Internet access is entirely unavailable.

•It is less secure.

•WAP provides a small User interface (UI).

Applications of Wireless Application Protocol (WAP):

The following are some most used applications of Wireless Application Protocol or WAP:

•WAP facilitates you to access the Internet from your mobile devices. •You can play games on mobile devices over wireless devices.

•It facilitates you to access Emails over the mobile Internet.

•Mobile handsets can be used to access timesheets and fill expense claims.

•Online mobile banking is very popular nowadays.

**b. IMAP:**

➤

IMAP stands for Internet Message Access Protocol. It is a standard protocol for accessing and managing email messages on a remote mail server. IMAP is widely used by email clients such as Microsoft Outlook, Apple Mail, and Thunderbird.

How IMAP works:

• IMAP allows you to keep your email messages on the server and synchronises them with your email client.

• When you connect to an email account using IMAP, the email client downloads a copy of the message headers and body from the server.

• You can then read, reply, forward, or delete the messages using your email client.

• Any changes you make to the messages are reflected on the server, so you can access the same messages from multiple devices.

Advantages of using IMAP:

• IMAP allows you to access your email messages from multiple devices.

• You can keep your email messages on the server and free up space on your local device.

• IMAP allows you to organise your email messages into folders on the server, so you can access them from any device.

• IMAP supports advanced features such as server-side searching, message flags, and message threading.

Potential drawbacks of using IMAP:

• IMAP requires a stable internet connection to access your email messages.

• If your email provider has limited storage space on the server, you may need to periodically delete old messages or pay for additional storage.

• Some email clients may not fully support all of the advanced IMAP features.

• IMAP may be slower than POP3 when downloading large attachments or a large number of messages.

**c. Centralised and distributed system:**

**d. Domain Name system:**

➤

The Domain Name System (DNS) can be thought of as the directory of the Internet. We find an online page or website by typing in the URL – like acme.com or some-site.com. Our web browsers, on the other hand, need to translate the URL to Internet Protocol (IP) addresses to find the correct site. It is a DNS that translates domain names to IP addresses so our browsers can resolve, or connect to, requested Internet resources. Every single device on the Internet has a unique IP address by which it can be uniquely identified by the other online devices. A DNS server eliminates the need for us to memorise these IP addresses every time we want to visit a site or connect to a device. It is much easier for us to type in a URL than IPv4 IP addresses (E.g. 192.168.1.1) or, worse, the more complex IPv6 addresses (E.g. 2400:cb00:2048:1::c629:d7a2). The DNS architecture consists of a hierarchical and decentralised name resolution system for computers, services or any other resources connected to the Internet or a private network. It stores the various associated information of the domain names assigned to each of the resources.

**e. Web hosting:**

➤

Web hosting is a process and service through which web application or website files are stored in a Web server to publish to the Internet via the World Wide Web. These files are primarily hosted to be publicly available around the world at any time. A Web server is a high-configuration computer system that stores, processes, and serves website files and other media content (for example, HTML documents, images, CSS stylesheets, and JavaScript files) requested by the client (web browser). Web hosting requires computers that can offer 24x7 uptime and serve multiple client requests simultaneously. Thus, if multiple clients request access to webpage files simultaneously, the server will be able to respond to them without any downtime. It is also possible to set up your PC as a web server and run web applications or websites from it. But since web servers require 100% uptime, you have to keep your PC running at all times, and this is not a practical and cheap way of doing web hosting. On the other hand, hosting companies also provide many additional features with all these services, saving our time and effort.

Different types of Web hosting services are listed below:

free Hosting: This is a free non-paid web hosting service. This type of hosting is available with many prominent sites that offer to host some web pages for no cost, like Hostinger.

Advantages:

• Free of cost

• Use websites to place advertisements. banners and other forms of advertising media

Disadvantages:

• Customer support is missing

• Low bandwidth and lesser data transfer

• No control over your website

Shared/Virtual Hosting: It’s a web hosting service where many websites reside on one web server connected to the internet. This type of hosting is provided under one’s own domain name, www.yourname.com. With a hosting plan with the web hosting company, one can present oneself as a fully independent identity to his/her web audience, like Lindo.

Advantages:

• Easy and affordable

• Secured by hosting provider

• 24/7 Technical support

Disadvantages:

• Shared resources can slow down the whole server

• Less flexible than dedicated hosting

Dedicated Hosting: Hosted on a dedicated server, this type of hosting is best suited for large websites with high traffic. In this, the company wishing to go online rents an entire web server from a hosting company. This is suitable for companies hosting large websites, maintaining others’ sites or managing a big online mall, etc like Google Cloud.

Advantages:

• Ideal for large business

• Strong database support

• Unlimited software support

• Powerful email solutions

• Complete root access to your servers

Disadvantages:

• It's very expensive

• Requires superior skill sets

Co-located Hosting: This hosting lets you place your own web server on the premises of a service provider. It is similar to that of dedicated hosting except for the fact that the server is now provided by the user-company itself and its physical needs are met by the hosting company like AWS.

Advantages:

• Greater Bandwidth High Up-Time

• Unlimited Software Options

• High Security

Disadvantages:

• Difficult to configure and debug

• Its expensive

• Require high skill

## 25. What is a web application? Explain its characteristics, needs, pros and cons.

➤

A web application is a software or program which is accessible using any web browser. Its frontend is usually created using languages like HTML, CSS, JavaScript, which are supported by major browsers. While the backend could use any programming stack like LAMP, MEAN, etc. Unlike mobile apps, there is no specific SDK for developing web applications.

It's characteristics, needs, pros and cons are:

Characteristics:

• Cloud-hosted and highly scalable

• Mostly Cross-platform

• Modular and loosely coupled

• It is easily tested with automated tests.

Needs:

• Compared to desktop applications, web applications are easier to maintain as they use the same code in the entire application. There are no compatibility issues.

• Web applications can be used on any platform: Windows, Linux, Mac… as they all support modern browsers.

• Mobile App store approval not required in web applications.

• Released any time and in any form. No need to remind users to update their applications.

Pros:

• You can access these web applications 24 hours of the day and 365 days a year from any PC.

• You can either make use of the computer or your mobile device to access the required data.

• Web applications are a cost-effective option for any organisation. Seat Licences for Desktop software are expensive where SasS(S/w as a service), are generally, pay as you go.

• Web-Based Apps are Internet-enabled apps that are accessed through the mobile's web browser. Therefore, you don't need to download or install them.

Cons:

• Security is not guaranteed, so it is vulnerable for unauthorised access. • The web app may not support multiple browsers with equal precedence.

• The web application is built explicitly for a certain operating system, so it is difficult to discover from the app store.

• Limited scope to access the device's features.

## 26.Write short notes on architecting web applications.

➤Web application architecture defines the interactions between applications, middleware systems and databases to ensure multiple applications can work together. When a user types in a URL and taps “Go,” the browser will find the Internet-facing computer the website lives on and requests that particular page. The server then responds by sending files over to the browser. After that action, the browser executes those files to show the requested page to the user. Now, the user gets to interact with the website. Of course, all of these actions are executed within a matter of seconds. Otherwise, users wouldn’t bother with websites. What’s important here is the code, which has been parsed by the browser. This very code may or may not have specific instructions telling the browser how to react to a wide swath of inputs. As a result, web application architecture includes all sub-components and external applications interchanges for an entire software application. Of course, it is designed to function efficiently while meeting its specific needs and goals. Web application architecture is critical since the majority of global network traffic, and every single app and device uses web-based communication. It deals with scale, efficiency, robustness, and security.

## 27. What are the Best Practices for Good Web Application Architecture? Explain

➤ The Best Practices for Good Web Application Architecture are as follows:

• You may have a working app, but it also needs to have good web architecture.

• Here are several attributes necessary for good web application architecture: Solves problems consistently and uniformly

• Make it as simple as possible

• Supports the latest standards include Offers fast response times

• Utilises security standards to reduce the chance of malicious penetrations

• Does not crash

• Heals itself

• Does not have a single point of failure

• Scales out easily

• Allows for easy creation of known data

• Errors logged in a user-friendly way

• Automated deployments

## 28.Explain about Architectural issues of web layer.

➤The web layer is also referred to as the UI layer. The web layer is primarily concerned with presenting the user interface and the behaviour of the application (handling user interactions/events).While the web layer can also contain logic, core application logic is usually located in the services layer. The 3 layers within the web layer are:

• HTML: The content layer is where you store all the content that your customers want to read or look at. This includes text and images as well as multimedia. It’s also important to make sure that every aspect of your site is represented in the content layer. That way, your customers who have Java-script turned off or can't view CSS will still have access to the entire site, if not all the functionality.

• CSS: The styles layer : Store all your styles for your web site in an external style sheet. This defines the way the pages should look and you can have separate style sheets for various media types. Store your CSS in an external style sheet so that you can get the benefits of the style layer across the site.