**1. Explain briefly what happens when you hit a url? explain DNS lookup.**

Ans -> When u hit url you will be able to see web page for that url. If web page is not present on our system we need to uniquely identify the system for the url requested. To indetify each system uniquely as per internet standards we need ip address. ip is internet protocol. IP address is unique for networks and internet is network of networks. But we dont type ip addresses while trying to access website.The DNS(Domain Name System) solves our problem it maps our url with ip address and provide ip address for the url requested.

URL -> UNIFORM RESOURCE LOCATOR

HTTP->HYPER TEXT TRANSFER PROTOCOL

URL->protocol+DOMAIN+PORT NUMBER HTTP WORKS ON PORT 80

dns lookup process = client-><-ISP(internet service provider)-> <-DNS SERVER

client(IP address)->ISP ->to url requested.

**2. What is a URLs full form? Explain what a url is and the four parts it consists of The protocol in use The hostname of the server The location of the file The arguments to the file**

Ans->Uniform resource locator. url is a locator for resource on internet. It conists of 4 parts.. 1st is protocol(ex->http,https,ftp,mail), 2nd part is domain name(subDomain(ex->www),.com is top level domain), 3rd part is the filepath, 4th part is parameter or query. and 5th part is anchor to navigate to specific part of web page.

**3. What is HTTP protocol?**

HTTP is hyper text transfer protocol. www is communication between web clients and servers. HTTP is foundation for www to load web pages. The protocol is designed to transfer information between client and server. A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message.

HTTP is stateless protocol that means it breaks connection after it is completed.

**4. What is TCP Protocol?**

TCP is one of protocol of internet protocol. There are four layers application layer which is HTTP protocol then TCP which is Transmission control protocol which divides information in small packets and reassembles on other side. It increases efficiency as opposed to the normal way of sending information in one go. 3rd layer is ip address and 4th is network layer. It is 3 way process create connection -> send data -> close connection

**5. Explain all the different HTTP methods?**

8 type of method:

Most common are first 5 types of methods

DELETE, GET, POST, PUT, PATCH,OPTIONS, HEAD, CONNECT, TRACE

Get-> to get information from server.

Post -> to send data to server.

DELETE-> to delete some information on server side

PUT -> to modify the entire data for target resource

PATCH-> to modify partial data

**6. What are HTTP headers?**

headers are additional information send by server and client. All headers are case insensitive and are in form of object. There are four type of headers.-> General header which is common for both request and response header. -> Request header which has information about the fetched request of client -> Response header which has information about location of response -> Entity header which contains information about the body of the resources.

**7. What are some HTTP response codes? what does it mean? 2xx, 3xx, 4xx, 5x**

1xx: information

2xx: Success

3xx: Redirection

4xx: Client error

5xx Server error

100-> continue

101-> changing protocols

200 -> OK

201 -> Created

202 -> Accepted

301 -> Moved permanently

307 -> Temporary redirect

302-> Found

400-> Bad request

401 -> Unauthorized

402-> Payment required

403->Forbidden

404-> Not found

500-> Internal server error

501->Not implemented

502-> Bad gateway

503->Service unavailable

**8. What does cache control on http response mean?**

A control is HTTP cache header that contains a set of parameters to define browser’s caching policies in the client’s request and server response. When a client makes a request, the browser can keep copies of responses to reduce latency and for faster access. It contains of how it is cached, maximum age before expiring and place where it is cached.

**9. What is polling?**

It is technique for receiving and sending data. In this method the client asks for data from server on regular intervals.

**10. What is long polling?**

In this technique, the client requests for particular data and server responds whenever server event happens with no delay.

**11. What are web sockets?**

WebSocket is bidirectional, a full-duplex protocol that is used in the same scenario of client-server communication, unlike HTTP it starts from ws:// or wss://. It is a stateful protocol, which means the connection between client and server will keep alive until it is terminated by either party (client or server). After closing the connection by either of the client and server, the connection is terminated from both ends**.**

**12. How is web sockets different from HTTP?**

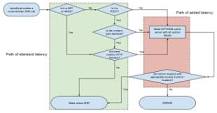
Unlike HTTP, where you have to constantly request updates, with websockets, updates are sent immediately when they are available. WebSockets keeps a single, persistent connection open while eliminating latency problems that arise with HTTP request/response-based methods.

**13. What is HTTPS?**

HTTPS (Hypertext Transfer Protocol Secure) is an internet communication protocol that protects the integrity and confidentiality of data between the user's computer and the site. Users expect a secure and private online experience when using a website.

**14. What is Cross Origin Resource Sharing? ( CORS ) Why do we need it?**

What is CORS cross-origin resource sharing policy?

[[](https://www.google.com/search?sxsrf=APq-WBs7Oe6v4YNE-meCrua65-PRtkbY_Q:1650006561827&q=What+is+CORS+cross-origin+resource+sharing+policy?&tbm=isch&source=iu&ictx=1&vet=1&fir=qFNaoHVe9OByTM%252C6hV3Ds-IiXba5M%252C_&usg=AI4_-kQ2qh0Np6eEYeefPUNX-nm4ftFVJA&sa=X&ved=2ahUKEwjpp_q3wZX3AhVSAd4KHVbCCe8Q9QF6BAgREAE#imgrc=qFNaoHVe9OByTM)](https://www.google.com/search?sxsrf=APq-WBs7Oe6v4YNE-meCrua65-PRtkbY_Q:1650006561827&q=What+is+CORS+cross-origin+resource+sharing+policy?&tbm=isch&source=iu&ictx=1&vet=1&fir=qFNaoHVe9OByTM%252C6hV3Ds-IiXba5M%252C_&usg=AI4_-kQ2qh0Np6eEYeefPUNX-nm4ftFVJA&sa=X&ved=2ahUKEwjpp_q3wZX3AhVSAd4KHVbCCe8Q9QF6BAgREAE" \l "imgrc=qFNaoHVe9OByTM)

Cross-origin resource sharing (CORS) is **a mechanism that allows restricted resources on a web page to be requested from another domain outside the domain from which the first resource was served**. A web page may freely embed cross-origin images, stylesheets, scripts, iframes, and videos.

Cross-origin resource sharing (CORS) is a mechanism that **allows JavaScript on a web page to make AJAX requests to another domain, different from the domain from where it originated**. By default, such web requests are forbidden in browsers, and they will result into same origin security policy errors.

The CORS mechanism **supports secure cross-origin requests and data transfers between browsers and servers**. Modern browsers use CORS in APIs such as XMLHttpRequest or Fetch to mitigate the risks of cross-origin HTTP requests.

**15. What does Access-Control-Allow-Origin header do?**

The **Access-Control-Allow-Origin** response header indicates whether the response can be shared with requesting code from the given origin.

**16 What is clickjacking? How do you fix it?**

Clickjacking is **an attack that fools users into thinking they are clicking on one thing when they are actually clicking on another.**

[**https://auth0.com/blog/preventing-clickjacking-attacks/**](https://auth0.com/blog/preventing-clickjacking-attacks/)

A better approach to prevent clickjacking attacks is to **ask the browser to block any attempt to load your website within an iframe.**

**17. What are some performance metrics for your website?**

### 1. Page Speed

Page speed is one of the most important metrics to be aware of, and it can have a far greater impact than you may even realize.  Simply put: People don’t like waiting around! Keep your page speed as fast as possible to retain as large of an audience as possible.

### 2. Time to Title

Similar to your page speed, the time to title is the amount of time it takes for a website’s title to appear in a browser tab after an individual requests a website. In addition to testing an individual’s patience, the longer it takes for a page’s title to appear makes a website appear less legitimate.

### 3. Time to Start Render

The time it takes from an individual making a request and the amount of time it takes for content to begin loading — even if it does not fully load — is called the time to start render.

### 4. Time to Interact

Another metric that has everything to do with users’ patience is the time to interact. It refers to how much time it takes before individuals can begin to click on links, type in text fields, scroll on a page, and interact in other ways with a website. As you can imagine, this is another important metric because the quicker an individual can begin to interact with a web page, the less likely they are to leave the page, even if the page has not rendered fully.

### 5. DNS Lookup Speed

You’ve likely heard of “DNS lookup speed” or “DNS lookup time,” but you may not fully understand what this metric is. This refers to the amount of time it takes for your Domain Name System (DNS) provider to translate a domain name into an IP address. It’s important to note that there are faster and slower DNS providers out there, and if you’re using a slower provider, it can vastly slow down your DNS lookup speed.

### 6. Bounce Rate

Your bounce rate is pretty much what it sounds like. People are “bouncing” away from your site without thoroughly searching through it, and sometimes without even taking the time for the site to load properly. It can also be defined as a single page visit to your site, with users failing to interact elsewhere.

### 7. Requests Per Second

Also sometimes referred to as “Throughput” or “Average Load,” this metric refers to the number of requests your server receives every second. It is a rather basic metric used to measure the main purpose of your server, and those working on a large scale can reach upwards of 2000 requests per second.

### 8. Error Rate

It is inevitable some errors will occur on your site at any given time. Your error rate measures the number of errors occurring at any given time, keeping track of how many occur within a specific time frame.

### 9. Time to First Byte/Last Byte

We briefly touched on time to first byte as a subset of page speed, but it's an important enough metric to warrant its own breakdown.

### 10. Conversion Rate

### Last but not least, we can’t discuss metrics without talking about conversion rates. This refers to how many unique visitors end up converting into customers. Various factors affect conversion rates, but it is impossible to determine everything that plays a role in what transforms a site visitor into a customer.

### 18. What does the following term mean?

### Time to first byte,- Time to First Byte (TTFB) refers to the time between the browser requesting a page and when it receives the first byte of information from the server.

### Page load time- page load time is the average amount of time it takes for a page to show up on your screen. It's calculated from initiation (when you click on a page link or type in a Web address) to completion (when the page is fully loaded in the browser).

**19. What do CDN or Content Delivery Networks do? When do you need a CDN?**

A content delivery network (CDN) refers to a geographically distributed group of servers which work together to **provide fast delivery of Internet content**. A CDN allows for the quick transfer of assets needed for loading Internet content including HTML pages, javascript files, stylesheets, images, and videos.

CDNs not only **ensure a faster experience to your users, but they also help to prevent site crashes in the event of traffic surges** – CDNs help to distribute bandwidth across multiple servers, instead of allowing one server to handle all traffic.

**20. What is the difference between Client Side Renderring and Server Side Renderring?**

Client-side rendering manages the routing dynamically without refreshing the page every time a user requests a different route. But **server-side rendering is able to display a fully populated page on the first load for any route of the website, whereas client-side rendering displays a blank page first**.

**21. What is Progressive Renderring?**

Progressive Rendering, also known as Progressive Server Side Rendering, is a technique for updating tiny sections of a webpage progressively and streaming it to the client in segments rather than waiting for the full page to be displayed.

**22. What is the difference between Preloading and Prefetching resources?**

**Preload** is an early fetch instruction to the browser to request a resource needed for a page (key scripts, Web Fonts, hero images). **Prefetch** serves a slightly different use case — a future navigation by the user (e.g between views or pages) where fetched resources and requests need to persist across navigations.

**23. What are service workers?**

Service workers are **specialized JavaScript assets that act as proxies between web browsers and web servers**. They aim to improve reliability by providing offline access, as well as boost page performance.

.