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

1. You type a URL in your browser and press Enter. Browser looks up IP address for the domain. Browser initiates TCP connection with the server. Browser sends the HTTP request to the server.
2. A DNS lookup, in a general sense, is the process by which a DNS record is returned from a DNS server. This is like looking up a phone number in a phone book - that is why it is referred to as a "lookup"

Q. **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**

1. URL- Uniform Resource Locator.
2. A URL is nothing more than the address of a given unique resource on the Web. In theory, each valid URL points to a unique resource. Such resources can be an HTML page, a CSS document, an image, etc.
   1. **The Protocol:** Used to access a resource on the internet. Protocols include http, https, ftps, mailto and file. The resource is reached through the domain name system
   2. **The Hostname:** The unique reference represents a webpage.
   3. **The Location:** It refers to the location on the web server.
   4. **The Arguments:** Pieces of information in a query string of a URL. Multiple arguments can be separated by ampersands.

Q. **What is HTTP protocol?**

1. The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web, and is used to load web pages using hypertext links. HTTP is an [application layer](https://www.cloudflare.com/learning/ddos/application-layer-ddos-attack/) protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack.

Q. **What is TCP Protocol?**

1. TCP stands for Transmission Control Protocol a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.

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

1. The DELETE method deletes the specified resource.
2. The CONNECT method establishes a tunnel to the server identified by the target resource.
3. The OPTIONS method describes the communication options for the target resource.
4. The TRACE method performs a message loop-back test along the path to the target resource.

Q. **What are HTTP headers?**

1. HTTP headers let the client and the server pass additional information with an HTTP request or response. An HTTP header consists of its case-insensitive name followed by a colon ( : ), then by its value.

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

1. An HTTP status code is a server response to a browser's request. When you visit a website, your browser sends a request to the site's server, and the server then responds to the browser's request with a three-digit code: the HTTP status code.
2. **2xx**: This class of status codes indicates the action requested by the client was received, understood, and accepted.
3. **3xx**: This class of status code indicates the client must take additional action to complete the request. Many of these status codes are used in [URL redirection](https://en.wikipedia.org/wiki/URL_redirection).
4. **4xx**: This class of status code is intended for situations in which the error seems to have been caused by the client. Except when responding to a HEAD request, the server *should* include an entity containing an explanation of the error situation, and whether it is a temporary or permanent condition.

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

1. Cache-control is an HTTP header used to specify browser caching policies in both client requests and server responses. Policies include how a resource is cached, where it's cached and its maximum age before expiring.

Q. **What is polling?**

1. Polling is a technique by which the client asking the server for new data regularly.

Q. **What is long polling?**

1. Long polling is a mechanism where the server can send data independently or push data to the client without the web client making a request.

Q. **What are web sockets?**

1. 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.

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

1. 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.

Q. **What is HTTPS?**

1. Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol. It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security or, formerly, Secure Sockets Layer.

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

1. Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain.
2. We need CORS because 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.

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

1. The Access-Control-Allow-Origin header is included in the response from one website to a request originating from another website, and identifies the permitted origin of the request.

Q. **What is clickjacking? How do you fix it?**

1. Clickjacking is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages.
2. Clickjacking is caused due to allowing permission to a third party website to embed the vulnerable site using Iframe. Disallowing this can be done by setting HTTP headers that direct browser to not allow the target website to be iframed. This can be done by configuring server on the following two response headers: X-Frame-Options Content-Security-Policy. It can also be done using JavaScript code that kills the iframe.

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

1. a. Page Speed.

b. Time to Title.

c. Time to Start Render.

d. Time to Interact.

e. DNS Lookup Speed.

Q. **What does the term Time to First Byte mean?**

1. 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.

Q. **What does the term Page Load time mean?**

1. 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).

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

1. CDNs cache content like web pages, images, and video in proxy servers near to your physical location. This allows you to do things like watch a movie, download software, check your bank balance, post on social media, or make purchases, without having to wait for content to load.
2. We need CDNs to deliver the content to the client quickly and efficiently even during the high-traffic period.

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

1. 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.

Q. **What is Progressive Renderring?**

1. Progressive Rendering is the key to a faster web page is the technique of sequentially rendering parts of the web page on the server-side and send it to the client in portions without waiting for the entire page to be rendered.

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

1. 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.

Q. **What are service workers?**

1. 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.