1. Explain briefly what happens when you hit a URL? Explain DNS lookup.

Ans. The browser initiates a TCP connection with the server. The browser sends the HTTP request to the server. Server processes request and sends back a response. The browser renders the content.

A DNS lookup, in 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” . Interconnected computers, servers and smart phones need to know how to translate the email addresses and the domain name people use into meaningful numerical addresses. A DNS lookup performs this function.

2. What is URL full form?

Ans. URL stands for Uniform Resource Locator. It is used to locate a resource on the Internet. It is also referred to as a web address. URLs consist of multiple parts – including a protocol and domain name – that tell a web browser how and where to retrieve a resource.

a: The scheme – The scheme identifies the protocol to be used on the internet . It can be HTTP(without SSL) or HTTPS (with SSL).

b: A host- The host name identifies the host that holds the resource. For example – [www.example.com](http://www.example.com) . A server provides services in the name of the host. But hosts and servers do not have a one-to-one mapping. Host names can also be followed by a Port number.

c: The path- The path identifies the specific resource in the host that the web client wants to access. For example /software/htp/cics/index.html.

d: A query String: If a query string is used , it follows the path component and provides a string of information that the resource can use for search or as data to be processed. The query string is usually a string of name and value pairs. For example: term=bluebird. Name and value pairs are separated by each other by an ampersand(&) for example: term=bluebird&search=browser-search.

3. What is HTTP protocol?

Ans. HTTP protocol stands for Hyper Text Transfer Protocol. It is foundation of world wide web, and is used to load web page using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message.

4. What is TCP protocol?

Ans. TCP(Transmission Control Protocol) is a communication standard which enables the application program and computing devices to send packets across the internet and make sure that the message or data is successfully delivered.

5.Explain all the different HTTP methods?

Ans. 1.GET – The GET method requests a representation of the specified resource . Request using GET only retrieve data.

2. HEAD – The HEAD method asks for a response identical to a GET request , but without the response body.

3.POST – The POST method submit an entity to the specified resource , often causing a change in state or side effects on the server.

4. PUT – The PUT request replaces all the current representations of the target resource with the request payload.

5. DELETE- The DELETE method deletes the specified resource.

6. CONNECT- The CONNECT method established a tunnel to the server identified by the target resource.

7. OPTIONS- The OPTION method describes the communication options for the target resource.

8. TRACE- The TRACE method performs a message loop-back test along the path to the target.

PATCH- The PATCH method applies partial modifications to a resource .

6.What are HTTP headers?

Ans. HTTP headers let pthe client and the server pass additional information with an HTTP request or response . An HTTP header consist of its case-insensitive name followed by a colon(:) then by its value. Whitespace before the values is ignored.

7.What are some HTTP response code? What does it mean? 2xx,3xx,4xx,5xx?

Ans. Some response codes are:

1. Informational response (100-199)
2. Successful response(200-299)
3. Redirection messages(300-399)
4. Client error responses(400-499)
5. Server error responses(500-599)

2xx mean successful, 3xx means redirection,4xx mean client error response

8.What does cache control on HTTP response mean?

Ans. Cache-control is HTTP header used to specify browser caching poilicies for both client requests and server responses. Policies include how a resource is cached, where a resource is cached and its maximum age before expiring.

9.What is polling?

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

10. What is long polling?

Ans. Long polling allows some king of event driven notifying, so the server is able to actively send data to the client.

11. What are web sockets?

Ans. Web sockets is bidirectional , full duplex protocol that is used in the scenario of client server communication.

12. How is web socket different from HTTP?

Ans. Unlike HTTP is starts with ws:// or wss://. HTTP is a stateless protocol where after sending the response the connection gets closed whereas in web socket the connection between client and server will keep alive until it gets terminated by either of the parties.

13. What is HTTPS?

Ans. HTTPS is Hypertext Transfer Protocol Secure which is secure version of HTTP which is a primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when used transmits sensitive data, such as bank account details, email service or health insurance provider.

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

Ans. Cross Origin resource sharing is a mechanism which allows JavaScript web page to make AJAX request to different domain, different from the domain where it is originated. By default such web requests are forbidden in browsers and show the result as same origin security policy error.

The cors origin mechanism support secure cross-origin requests and data transfer between browsers and servers.

15.What does access-control-allow-origin header do?

Ans. Acess-control-allow-origin includes the response from one website to the request originating from the other website and identifies the permitted origin of the resource.

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

Ans. Clickjacking is caused due to allowing permission to any third party website to embed vulnerable site using iframe.

We can use X-FRAME options to fix it. The X-FRAME options in HTTP response header can be used to indicate whether or not browser should be allowed to open a page in frame or iframe.

17. What are some performance metrics for your website?

Ans. Some of the performance metrices of the website are:

1. Page speed: It is most important and have far greater impact then one can even realise
2. Time to Title
3. Time to start render
4. Time to interact
5. DNS lookup speed
6. Bounce rate
7. Requests per second
8. Error rate

18. What does the following term mean?

Ans. a. Time to First byte: It is a metric for determining the responsiveness of a web server. It measures the time between creating a connection to the server and downloading the contents of a web page.

b. Page load: In the simplest terms it is the average amount of time it takes for a page to show up on the screen.

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

Ans. CDN(Content Delivery Network) refers to geographically distributed group of servers which work together to provide fast internet content. A CDN allows for the quick transfer of assets needed for loading internet content including HTML pages, javascirpt files, stylesheets , images and videos.

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

Ans. Client side rendering manages the routing dynamically without refreshing the page every time a user requests a different route. Whereas the web side rendering is able to display a fully populated page on the first load of any route of the website whereas client side display a blank page first.

21.What is progressive rendering?

Ans. It is the sequential rendering of portions web page on the server side and sending them to the client piece by piece, without waiting for the entire page to render.

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

Ans. Preloading is an early fetch instruction to the browser to request a resource needed for a page(key scripts, hero images, web fonts) .

Prefetch serves a slightly different usecase- a future navigation by the user(ex. Between views and pages) where fetched resources and requests need to persist across navigation.

23. What are service workers?

Ans. A service worker is a web worker. It is essentially a javascript file that runs separately from the main browser thread, intercepting network requests, catching or retrieving resources from the cache, and delivering push messages.