**1. How does HTTPS work behind the scene?**

Https is a secure version of Http which is the primary protocol used to send data between web browsers and a website.Https is encrypted in order to increase the security of data transfer.

Https uses an encryption protocol to encrypt communication. Protocol is called TLS(Transport layer security),and secures the communication by using an asymmetric public key infrastructure.

There is two key Public and the private key:-

Private key: Lives on a web browser and decrypts the information encrypted by the public key.

Public Key: It is public to anyone who wants to interact with the server and encrypt the information and convert it into the cipher text with the help of a session layer and transferred over the browser.

When we use the same key for transmission on both ends it’s called symmetric encryption.

But it becomes more complicated to website on the public internet because we don't control the other end's connection.

And in asymmetric connection you used different keys.

Steps:

1) our browser reaches out to the website server and requests a connection.

2) The server sends the public key and keeps it a private key secret.

3) The browser generates a third key called session key.

4) The session key is encrypted by our computer using the public key we got from the server.

5) Encrypted session key then shared with the server .

6) Server decrypts the session key using its private key.

7) The public key encryption is terminated and replaced with symmetric encryption. And now we are in the session with the server and that's how it remains until we leave the website.

**2. What are the different https methods available and what are they exactly?**

HTTP is designed to enable communications between clients and servers.HTTP works as a request-response protocol between a client and server.

There are several of different methods:

1) **GET Method:** Get is one of the most common methods of http and used to request the data from the specified source.also the get command can be cached and the get method has length restrictions.

A GET request retrieves data from a web server by specifying parameters in the URL portion of the request.This is the main method used for document retrieval.

2) **Post Method:** Post is one of the most common methods of http and used to send data to a server to create a resource. Post method is used when you want to send some data to the server. Post requests are never cached and have no restrictions on data limit.

3) **Put Method:** Put is used to send data to a server to create a resource.The PUT method is used to request the server to store the included entity-body at a location specified by the given URL.

The difference between put and post method is that put method is idempotent.if we call the same put request again and again its gonna give the same result at every time while in post request repeatedly have side effects of creating the same resource multiple times.

4) **Head Method:** The HEAD method is functionally similar to GET, except that the server replies with a response line and headers, but no entity-body.

In other words, if GET /users returns a list of users, then HEAD /users will make the same request but will not return the list of users.

5) **Delete Method:** The DELETE method is used to request the server to delete a file at a location specified by the given URL.

6) **Option Method:** The option method is used by the client to find out the http methods and other options supported by a web server. The client can specify a url for the options method, or an asterisk (\*) to refer to the entire server.The option method describes the communication options for the target resource.

**3. Understand and explain the use of various http response codes?**

HTTP response status codes indicate whether a specific Http request has been successfully completed.The Status-Code element in a server response, is a 3-digit integer where the first digit of the Status-Code defines the class of response and the last two digits do not have any categorization role.

1) **Information Response:** It means the request has been received and the process is continuing.

**100 continue:** This interim response indicates that everything so far is OK and that the client should continue the request, or ignore the response if the request is already finished.

**101 Switching:** This code is sent in response to an upgrade request header from the client, and indicates the protocol the server is switching to.

**102 processing:** This code indicates that the server has received and is processing the request, but no response is available yet.

2) **Successful Response:** It means the action was successfully received, understood, and accepted.

**200 ok:** The request has succeeded. The meaning of the success depends on the HTTP method which we are using i.e Get,Head,Put,Post.

**201 created:** The request has succeeded and a new resource has been created as a result. This is typically the response sent after post requests, or some put requests.

**202 Accepted:** The request has been received but not yet acted upon. It is noncommittal, since there is no way in HTTP to later send an asynchronous response indicating the outcome of the request.

**203 Non-authoritative Information:** The information in the entity header is from a local or third-party copy, not from the original server.

**204 No Content:** A status code and a header are given in the response, but there is no entity-body in the reply.

3) **Redirect Response:** It means further action must be taken in order to complete the request.

**300 Multiple Choices:** The request has more than one possible response. The user-agent or user should choose one of them.

**301 Moved Permanently:** The URL of the requested resource has been changed permanently. The new URL is given in the response.

**302 Found:** This response code means that the URI of requested resource has been changed temporarily. Further changes in the URI might be made in the future. Therefore, this same URI should be used by the client in future requests.

**303 See Other:** The server sent this response to direct the client to get the requested resource at another URI with a GET request.

**304 Not Modified:** This is used for caching purposes. It tells the client that the response has not been modified, so the client can continue to use the same cached version of the response.

4) **Client Error:** It means the request contains incorrect syntax or cannot be processed.

**400 Bad Request:** The server could not understand the request due to invalid syntax.

**401 Unauthorized:** Although the HTTP standard specifies "unauthorized", semantically this response means "unauthenticated". That is, the requested page needs a username and a password.

**402 Payment Required:** This response code is reserved for future use. The initial aim for creating this code was using it for digital payment systems, however this status code is used very rarely and no standard convention exists.

**403 Forbidden:** The client does not have access rights to the content; that is, it is unauthorized, so the server is refusing to give the requested resource. Unlike 401, the client's identity is known to the server.

**404 Not Found:** The server can not find the requested resource. In the browser, this means the URL is not recognized.

**405 Method Not Allowed:** The method specified in the request is not allowed.

**406 Not Acceptable:** The server can only generate a response that is not accepted by the client.

**407 Proxy Authentication Required:** This is similar to 401 but authentication is needed to be done by a proxy.

**408 Request Timeout:**The request took longer than the server was prepared to wait.

**409 Conflict:** This response is sent when a request conflicts with the current state of the server.

**5) Server Error:** It means the server failed to fulfill an apparently valid request.

**500 Internal Server Error:** The request was not completed. The server met an unexpected condition.

**501 Not Implemented:** The request was not completed. The server did not support the functionality required. The only method servers are required to support are GET and HEAD.

**502 Bad Gateway:** This error response means that the server, while working as a gateway to get a response needed to handle the request, got an invalid response.

**503 Service Unavailable:** The server is not ready to handle the request. Common causes are a server that is down for maintenance or that is overloaded.

**504 Gateway Timeout:** This error response is given when the server is acting as a gateway and cannot get a response in time.

**505 HTTP Version Not Supported:** The HTTP version used in the request is not supported by the server.

**4. What are the different web communications protocols and their use cases?**

**1) Transmission control protocol:** TCP is a communication protocol which is used for communicating over the internet.TCP establishes a connection between a source and its destination, which it ensures remains live until communication begins and then it divides any message into a series of packages and sent from one source to the designation.

**2) User Datagram protocol:** UDP is a suitable communication protocol to the transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.

**3) Post office protocol(POP)**: It is designed to receive the mails.it is a message access agent protocol work for SMTP. When the message is sent, then SMTP is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent.

**4) Simple mail transfer protocol(SMTP):** It is also a communication protocol for web browsers.it is a protocol used to send the mail over the internet.

**5) File transfer protocol(FTP):** FTP is the file transmission protocol over a network that uses TCP. FTP allows our data to be transferred between two computers.TCP, or Transmission Control Protocol, is what makes FTP reliable; checking and ensuring that your data actually arrives at its destination.

**6) Hyper text transfer protocol(HTTP):** The Hypertext Transfer Protocol is [an application protocol](https://tools.ietf.org/html/rfc2616) for distributed, collaborative, hypermedia information systems that allows users to communicate data on the World Wide Web.

**7) Hyper Text Transfer Protocol Secure (HTTPS):** Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from a web server. HTTPS is used for transferring data between the client browser and the web server in the hypertext format.it uses the encryption method with the help of public and private keys.

**5. Pros and cons of single page and multipage application**:

**Multi Page application**: Multi-page applications are the traditional web applications that reload the entire page and display the new one when a user interacts with the web app and try to exchange data each time a new page is created.

**Pros of MPA**:

Multi-page applications are more SEO-friendly in comparison with single-page solutions. Their content is being constantly updated.

There are almost no restrictions on the number of pages to add to the existing application. Single-page applications don’t have such privileges as they are limited to the amount of content.

There are almost no restrictions on the number of pages to add to the existing application. Single-page applications don’t have such privileges as they are limited to the amount of content.

**Cons of MPA**:

Since multi-page applications have a higher number of features compared to single-page solutions, their creation requires more effort and resources.

The development time increases in proportion to the number of pages to be built and the functionality to be implemented.

The content in multi-page applications is constantly reloaded which increases the load on your servers. This can affect web page speed and overall system performance in a negative way.

Maintaining security may be problematic because developers need to secure each separate page. Single-page apps allow developers to just secure data endpoints.

**Single Page applications:**

A single-page application works in the browser and requires no page reloads and no extra time for waiting. The page doesn’t need to be updated since content is downloaded automatically.

**Pros of SPA:**

Since single-page applications don’t update the entire page but only require content, they significantly improve a website’s speed.

A single-page can cache any local data effectively. An SPA sends only one request to a server and then stores all the data it receives.

SPAs provide users with a simple linear experience.

The development is simplified and streamlined. There is no need to write code to render pages on the server.

**Cons of SPA:**

It is very tricky and not an easy task to make SEO optimization of a Single-Page Application.

An SPA doesn’t save visitors from jumping between states. This means that when users click the back button, they won’t go back. A browser only takes users to the previous page.

Automated security scans can have difficulty discovering links when your entire page is built dynamically by a SPA framework.

SPAs require a lot of resources from the browser since the browser is doing most of the tasks for the SPAs.

**6. What is TCP ,Why do we use TCP, How does it work?**

**TCP(Transmission control protocol):**

TCP is a communications standard protocol 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.

TCP organizes data so that it can be transmitted between a server and a client. It guarantees the integrity of the data being communicated over a network. Before it transmits data, TCP establishes a connection between a source and its destination, which it ensures remains alive until communication begins.

**WHY:**

TCP helps you to determine how a specific computer should be connected to the internet and how data should be transmitted between them. It helps you to create a virtual network when multiple computer networks are connected together**.**

**How does it work:**

TCP provides communication between an application program and the Internet Protocol.TCP allows for transmission of information in both directions. This means that computer systems that communicate over TCP can send and receive data at the same time.

The TCP protocol uses segments (packets) as the basic units of data transmission.It divides the whole message into the segment and sends over the internet to the receiving end.

TCP divides a stream of data into chunks, and then adds a TCP header to each chunk to create a TCP segment. A TCP segment consists of a header and a data section. The TCP header contains 10 mandatory fields, and an optional extension field. The payload data follows the header and contains the data for the application.and send these chunks over the internet after the connection being made between the two ends.