1. Stateless Protocol:
Stateless Protocols are the type of network protocols in which Client send request to the server and server response back according to current state. It does not require the server to retain session information or a status about each communicating partner for multiple request.

HTTP (Hypertext Transfer Protocol), UDP (User Datagram Protocol), DNS (Domain Name System) are the example of **Stateless Protocol**.

Salient features of Stateless Protocols:

- Stateless Protocol simplify the design of Server.
- The stateless protocol requires less resources because system do not need to keep track of the multiple link communications and the session details.
- In Stateless Protocol each information packet travel on it's own without reference to any other packet.
- Each communication in Stateless Protocol is discrete and unrelated to those that precedes or follow.

2. Stateful Protocol:
In Stateful Protocol If client send a request to the server then it expects some kind of response, if it does not get any response then it resend the request. FTP (File Transfer Protocol), TCP, and Telnet are the example of **Stateful Protocol**.
Salient features of Stateful Protocol:

- Stateful Protocols provide better performance to the client by keeping track of the connection information.
- Stateful Application require Backing storage.
- Stateful request are always dependent on the server-side state.
- TCP session follow stateful protocol because both systems maintain information about the session itself during its life.

Stateless Protocol	Stateful Protocol
Stateless Protocol does not require the server to retain the server information or session details.	Stateful Protocol require server to save the status and session information.
In Stateless Protocol, there is no tight dependency between server and client.	In Stateful protocol, there is tight dependency between server and client
The Stateless protocol design simplify the server design.	The Stateful protocol design makes the design of server very complex and heavy.
Stateless Protocols works better at the time of crash because there is no state that must be restored, a failed server can simply restart after a crash.	Stateful Protocol does not work better at the time of crash because stateful server have to keep the information of the status and session details of the internal states.
Stateless Protocols handle the transaction very fastly.	Stateful Protocols handle the transaction very slowly.
Stateless Protocols are easy to implement in Internet.	Stateful protocols are logically heavy to implement in Internet.
Scaling architecture is relatively easier.	It is difficult and complex to scale architecture.
The requests are not dependent on the server side and are self contained.	The requests are always dependent on the server side.
To process different information at a time , different servers can be used.	To process every request , the same server must be utilized.
Example of Stateless are UDP , DNS , HTTP , etc.	Example of Stateful are FTP , Telnet , etc.

Application Layer Protocol in Computer Network

1. TELNET

Telnet stands for the **TEL**etype **NET**work. It helps in terminal emulation. It allows Telnet clients to access the resources of the Telnet server. It is used for managing files on the Internet. It is used for the initial setup of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. The port number of the telnet is 23.

Command

```
telnet [\\RemoteServer]
\\RemoteServer
: Specifies the name of the server
to which you want to connect
```

2. FTP

FTP stands for File Transfer Protocol. It is the protocol that actually lets us transfer files. It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program.FTP promotes sharing of files via remote computers with reliable and efficient data transfer. The Port number for FTP is 20 for data and 21 for control.

Command

```
ftp machinename
```

3. TFTP

The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it. It's a technology for transferring files between network devices and is a simplified version of FTP. The Port number for TFTP is 69.

Command

```
tftp [ options... ] [host [port]] [-c command]
```

4. NFS

It stands for a Network File System. It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the network. The Port number for NFS is 2049.

Command

```
service nfs start
```

5. SMTP

It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called "store and forward," SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. The Port number for SMTP is 25.

Command

```
MAIL FROM:<mail@abc.com?
```

8. SNMP

It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defined values. The Port number of SNMP is 161(TCP) and 162(UDP).

Command

```
snmpget -mALL -v1 -cpublic snmp_agent_Ip_address sysName.0
```

9. DNS

It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.abc.com might translate to 198.105.232.4.
The Port number for DNS is 53.

Command

```
ipconfig /flushdns
```

10. DHCP

It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts. There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68.

Command

```
clear ip dhcp binding {address | * }
```

11. HTTP/HTTPS

HTTP stands for Hypertext Transfer Protocol and HTTPS is the more secured version of HTTP, that's why HTTPS stands for Hypertext Transfer Protocol Secure. This protocol is used to access data from the World Wide Web. The Hypertext is the well-organized documentation system that is used to link pages in the text document.

- HTTP is based on the client-server model.
- It uses TCP for establishing connections.
- HTTP is a stateless protocol, which means the server doesn't maintain any information about the previous request from the client.
- HTTP uses port number 80 for establishing the connection.

12. POP

POP stands for Post Office Protocol and the latest version is known as POP3 (Post Office Protocol version 3). This is a simple protocol used by User agents for message retrieval from mail servers.

- POP protocol work with Port number 110.
- It uses TCP for establishing connections.

POP works in dual mode- *Delete mode, Keep Mode.*

In Delete mode, it deletes the message from the mail server once they are downloaded to the local system.

In Keep mode, it doesn't delete the message from the mail server and also facilitates the users to access the mails later from the mail server.

Difference between POP3 and IMAP

Post Office Protocol (POP3)	Internet Message Access Protocol (IMAP)
POP is a simple protocol that only allows downloading messages from your Inbox to your local computer.	IMAP (Internet Message Access Protocol) is much more advanced and allows the user to see all the folders on the mail server.
The POP server listens on port 110, and the POP with SSL secure(POP3DS) server listens on port 995	The IMAP server listens on port 143, and the IMAP with SSL secure(IMAPDS) server listens on port 993.
In POP3 the mail can only be accessed from a single device at a time.	Messages can be accessed across multiple devices
To read the mail it has to be downloaded on the local system.	The mail content can be read partially before downloading.
The user can not organize mail in the mailbox of the mail server.	On the mail server, the user can directly arrange the email.
The user can not create, delete,e or rename email on the mail server.	The user can create, delete,e or rename an email on the mail server.
It is unidirectional i.e. all the changes made on a device do not affect the content present on the server.	It is Bi-directional i.e. all the changes made on the server or device are made on the other side too.

The user can not create, delete,e or rename email on the mail server.	The user can create, delete,e or rename an email on the mail server.
It is unidirectional i.e. all the changes made on a device do not affect the content present on the server.	It is Bi-directional i.e. all the changes made on the server or device are made on the other side too.
It does not allow a user to sync emails.	It allows a user to sync their emails.
It is fast.	It is slower as compared to POP3.
A user can not search the content of mail before downloading it to the local system.	A user can search the content of mail for a specific string before downloading.
It has two modes: delete mode and keep mode. • In delete mode, the mail is deleted from the mailbox after retrieval. • In keep mode, the mail remains in the mailbox after retrieval.	Multiple redundant copies of the message are kept at the mail server, in case of loss of message on a local server, the mail can still be retrieved
Changes in the mail can be done using local email software.	Changes made to the web interface or email software stay in sync with the server.
All the messages are downloaded at once.	The Message header can be viewed before downloading.

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack. In this article, we are going to discuss SSL in detail, its protocols, the silent features of SSL, and the version of SSL.

What is a Secure Socket Layer?

SSL, or Secure Sockets Layer, is an Internet security protocol that encrypts data to keep it safe. It was created by Netscape in 1995 to ensure privacy, authentication, and data integrity in online communications. SSL is the older version of what we now call TLS (Transport Layer Security).

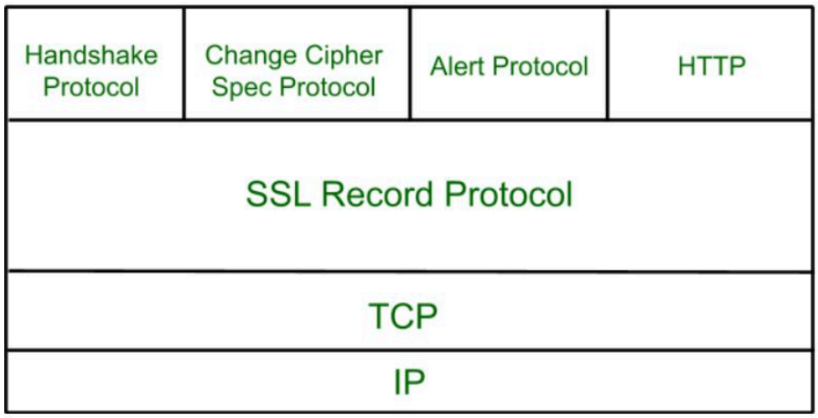
Websites using SSL/TLS have "HTTPS" in their URL instead of "HTTP."

How does SSL work?

- **Encryption**: SSL encrypts data transmitted over the web, ensuring privacy. If someone intercepts the data, they will see only a jumble of characters that is nearly impossible to decode.
- **Authentication**: SSL starts an authentication process called a handshake between two devices to confirm their identities, making sure both parties are who they claim to be.
- **Data Integrity**: SSL digitally signs data to ensure it hasn't been tampered with, verifying that the data received is exactly what was sent by the sender.

Secure Socket Layer Protocols

- SSL Record Protocol
- Handshake Protocol
- Change-Cipher Spec Protocol
- Alert Protocol



SSL Record Protocol

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.