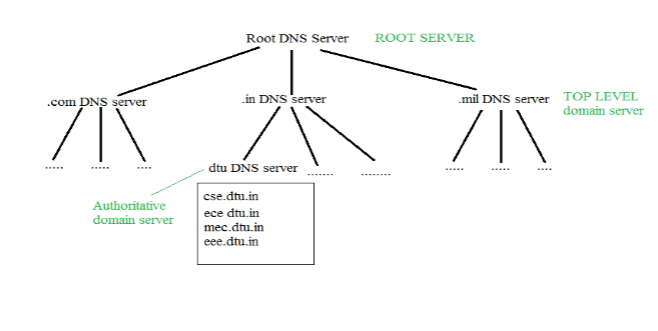
6. Application Layer

**Domain Name System (DNS) in Application Layer**

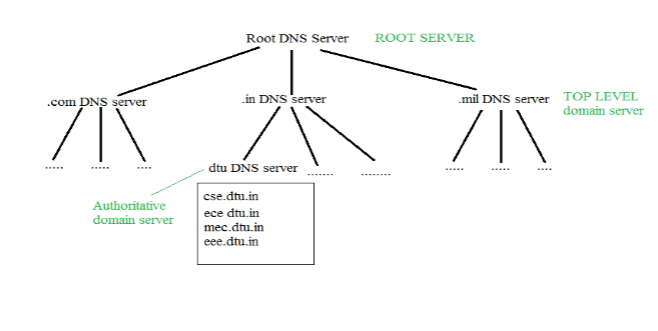
DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

**Requirement**

Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

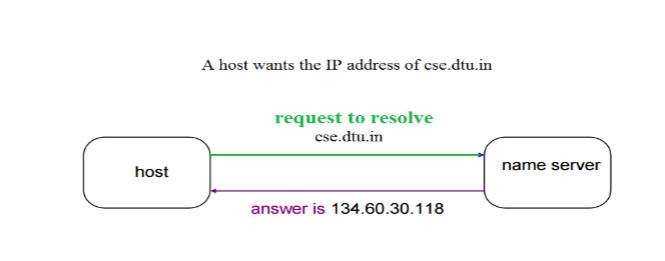
**Domain:**   
There are various kinds of DOMAIN :

1. Generic domain : .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.
2. Country domain .in (india) .us .uk
3. Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup [www.geeksforgeeks.org](http://www.geeksforgeeks.org).

Organization of Domain  


It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately,  
there should not be a lot of delay for that to happen organization of database is very important.

**Namespace** – Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –



Domain name servers are a fundamental part of the Domain Name System. Nameserver is a server on the Internet specialized in handling queries regarding the location of the domain name’s various services. In easy words, name servers define your domain’s current DNS provider.

**There are three types of queries in the DNS system:**

### Recursive Query

In a recursive query, a DNS client provides a hostname, and the DNS Resolver “must” provide an answer—it responds with either a relevant resource record, or an error message if it can't be found. The resolver starts a recursive query process, starting from the DNS Root Server, until it finds the Authoritative Name Server (for more on Authoritative Name Servers see DNS Server Types below) that holds the IP address and other information for the requested hostname.

### Iterative Query

In an iterative query, a DNS client provides a hostname, and the DNS Resolver returns the best answer it can. If the DNS resolver has the relevant DNS records in its cache, it returns them. If not, it refers the DNS client to the Root Server, or another Authoritative Name Server which is nearest to the required DNS zone. The DNS client must then repeat the query directly against the DNS server it was referred to.

### Non-Recursive Query

A non-recursive query is a query in which the DNS Resolver already knows the answer. It either immediately returns a DNS record because it already stores it in local cache, or queries a DNS Name Server which is authoritative for the record, meaning it definitely holds the correct IP for that hostname. In both cases, there is no need for additional rounds of queries (like in recursive or iterative queries). Rather, a response is immediately returned to the client.

## DNS Types: 4 Types of DNS Servers

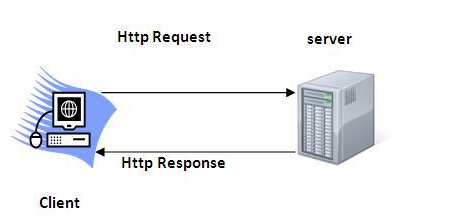
The following are the most common DNS server types that are used to resolve hostnames into IP addresses.

* **DNS recursive resolver** - The recursive can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursive is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursive is then responsible for making additional requests in order to satisfy the client’s DNS query.
* **Root name server** - The [root server](https://www.cloudflare.com/learning/dns/glossary/dns-root-server/) is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.
* [**TLD nameserver**](https://www.cloudflare.com/learning/dns/dns-server-types#tld-nameserver) - The top level domain server (TLD) can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is “com”).
* [**Authoritative nameserve**r](https://www.cloudflare.com/learning/dns/dns-server-types#authoritative-nameserver) - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.

# HTTP (Hyper Text Transfer Protocol)

The Hypertext Transfer Protocol (HTTP) is application-level protocol for collaborative, distributed, hypermedia information systems. It is the data communication protocol used to establish communication between client and server.

HTTP is TCP/IP based communication protocol, which is used to deliver the data like image files, query results, HTML files etc on the World Wide Web (WWW) with the default port is TCP 80. It provides the standardized way for computers to communicate with each other.



**The Basic Characteristics of HTTP (Hyper Text Transfer Protocol):**

* It is the protocol that allows web servers and browsers to exchange data over the web.
* It is a request response protocol.
* It uses the reliable TCP connections by default on TCP port 80.
* It is stateless means each request is considered as the new request. In other words, server doesn't recognize the user by default.

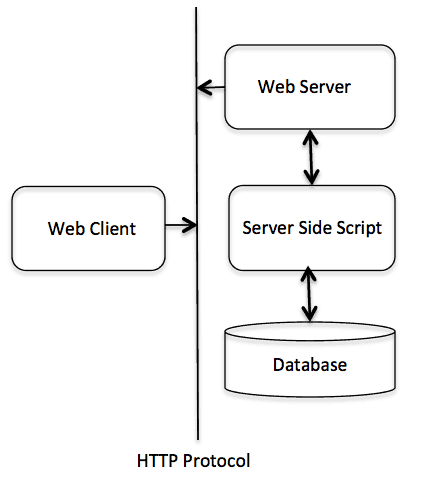
**The Basic Features of HTTP (Hyper Text Transfer Protocol):**

There are three fundamental features that make the HTTP a simple and powerful protocol used for communication:

* **HTTP is media independent:** It specifies that any type of media content can be sent by HTTP as long as both the server and the client can handle the data content.
* **HTTP is connectionless:** It is a connectionless approach in which HTTP client i.e., a browser initiates the HTTP request and after the request is sent the client disconnects from server and waits for the response.
* **HTTP is stateless:** The client and server are aware of each other during a current request only. Afterwards, both of them forget each other. Due to the stateless nature of protocol, neither the client nor the server can retain the information about different request across the web pages.

**The Basic Architecture of HTTP (Hyper Text Transfer Protocol):**

The below diagram represents the basic architecture of web application and depicts where HTTP stands:



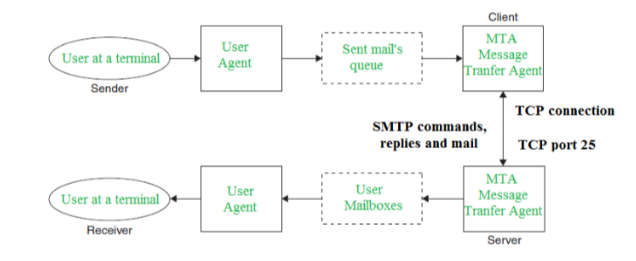
HTTP is request/response protocol which is based on client/server based architecture. In this protocol, web browser, search engines, etc. behave as HTTP clients and the Web server like Servlet behaves as a server

**SMTP**

* SMTP stands for Simple Mail Transfer Protocol.
* SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
* It is a program used for sending messages to other computer users based on e-mail addresses.
* It provides a mail exchange between users on the same or different computers, and it also supports:
  + It can send a single message to one or more recipients.
  + Sending message can include text, voice, video or graphics.
  + It can also send the messages on networks outside the internet.
* The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

**Model of SMTP system**

In the SMTP model user deals with the user agent (UA) for example Microsoft Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the MTA it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.



**Communication between sender and the receiver:**   
The senders, user agent prepare the message and send it to the MTA. The MTA functioning is to transfer the mail across the network to the receivers MTA. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.

**SENDING EMAIL:**   
Mail is sent by a series of request and response messages between the client and a server. The message which is sent across consists of a header and the body. A null line is used to terminate the mail header. Everything which is after the null line is considered as the body of the message which is a sequence of ASCII characters. The message body contains the actual information read by the receipt.

**RECEIVING EMAIL:**   
The user agent at the server-side checks the mailboxes at a particular time of intervals. If any information is received it informs the user about the mail. When the user tries to read the mail it displays a list of mails with a short description of each mail in the mailbox. By selecting any of the mail user can view its contents on the terminal.

**Some SMTP Commands:**

* HELO – Identifies the client to the server, fully qualified domain name, only sent once per session
* MAIL – Initiate a message transfer, fully qualified domain of originator
* RCPT – Follows MAIL, identifies an addressee, typically the fully qualified name of the addressee and for multiple addressees use one RCPT for each addressee
* DATA – send data line by line

# FTP

* FTP stands for File transfer protocol.
* FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
* It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
* It is also used for downloading the files to computer from other servers.

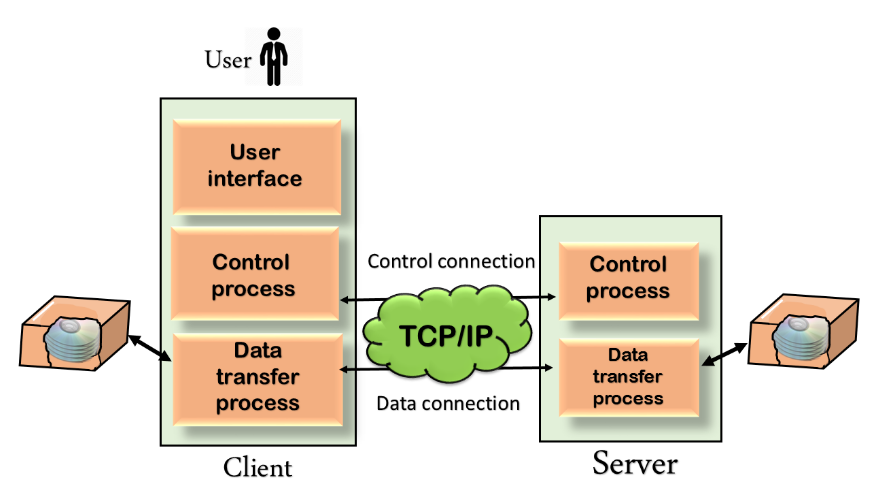
## Objectives of FTP

* It provides the sharing of files.
* It is used to encourage the use of remote computers.
* It transfers the data more reliably and efficiently.

## Why FTP?

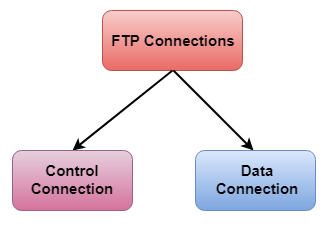
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

## Mechanism of FTP



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

**There are two types of connections in FTP:**



* **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
* **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

## FTP Clients

* FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
* It allows a user to connect to a remote host and upload or download the files.
* It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
* The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

### Advantages of FTP:

* **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
* **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
* **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
* **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

### Disadvantages of FTP:

* The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provide encryption.
* FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
* Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
* It is not compatible with every system.

## Telnet

Telnet is a simple, text-based network protocol that is used for accessing remote computers over TCP/IP networks like the Internet. Telnet was created and launched in 1969 and, historically speaking, you can say that it was the first Internet.

In the old days, you had to physically walk to a server in order to access its data. This meant, among other things, that you had to spend some time arriving at the server's location and then you had to wait for your turn to work with the server. Even if the server had the hardware power to do multiple things at the same time, you were blocked from using it at its full and you had to wait for others to finish their work first. In many circumstances you couldn't even touch the actual server. You had to hand your card stack to an attendant and come back later for your printout.

Telnet brought extraordinary change. Using it meant you could simultaneously connect multiple users to a single server. In order to connect to the server, people only needed access to a terminal, which could be the simplest and cheapest computer available. This computer didn't need to have powerful hardware, it only needed a network connection and a text based interface. Basically, their Telnet Client was like a Command Prompt that people could use in order to work with their servers. This brought a huge boost in productivity.

## What are the Telnet Client & the Telnet Server from Windows?

In Windows, you can add two Telnet related features:

* **Telnet Server** - if you install this feature, you will be able to configure your Windows computer to run as a Telnet server. This means that your computer will listen for incoming connections and allow others to use it. If you're not beneath a firewall and you have a public IP address, anyone in the world will be able to remote control your computer using a Telnet Client.
* **Telnet Client** - this will enable you to connect through Telnet to any server of this type, using just a Command Prompt window.

## How Does Telnet Work?

Telnet originally was used on terminals. These computers require only a keyboard because everything on the screen displays as text. The terminal provides a way to remotely log on to another device, just as if you were sitting in front of it and using it like any other computer.

Nowadays, Telnet can be used from a virtual terminal, or a terminal emulator, which is essentially a modern computer that communicates with the same Telnet protocol. One example of this is the telnet command, available from the Command Prompt in Windows. The telnet command uses the Telnet protocol to communicate with a remote device or system.

Telnet commands can also be executed on other operating systems such as Linux and macOS, in the same way that telnet commands are executed in Windows.

Telnet isn't the same as other TCP/IP protocols such as HTTP, which transfers files to and from a server. Instead, the Telnet protocol has you log on to a server as if you were an actual user, then grants you direct control and all the same rights to files and applications as the user that you're logged in as.

**TELNET** stands for**Tel**etype **Net**work. It is a type of protocol that enables one computer to connect to the local computer. It is used as a standard [**TCP/IP protocol**](https://www.geeksforgeeks.org/tcp-ip-in-computer-networking/) for virtual terminal service which is provided by [**ISO**](https://www.geeksforgeeks.org/iso-full-form/). The computer which starts the connection is known as the**local computer**.

The computer which is being connected to i.e. which accepts the connection known as the **remote computer**.

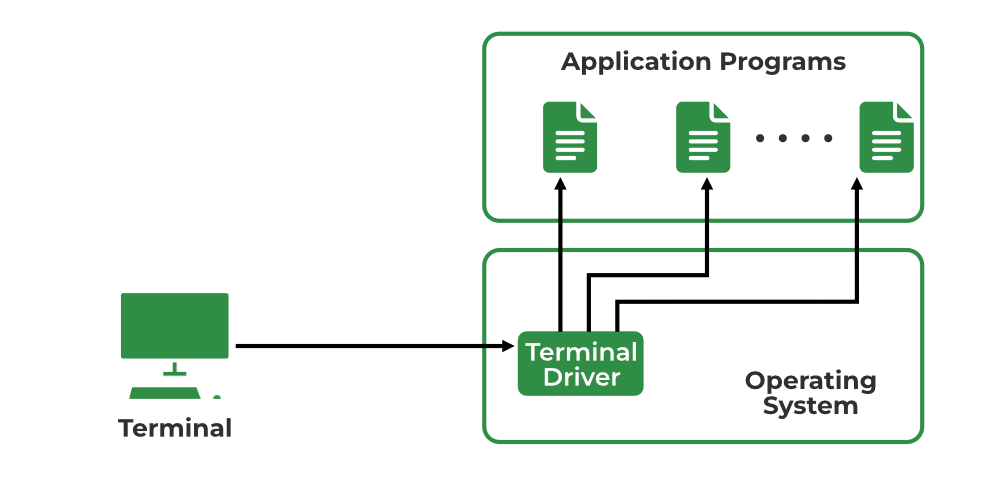
During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/server principle. The local computer uses a telnet client program and the remote computers use a telnet server program.

## Logging

The logging process can be further categorized into two parts:

1. Local Login
2. Remote Login

**1. Local Login:**Whenever a user logs into its local system, it is known as local login.



*Local Login*

**The Procedure of Local Login**

* Keystrokes are accepted by the terminal driver when the user types at the terminal.
* Terminal Driver passes these characters to OS.
* Now, OS validates the combination of characters and opens the required application.

1. **Remote Login:** [Remote Login](https://www.geeksforgeeks.org/introduction-to-remote-login/) is a process in which users can log in to a remote site i.e. computer and use services that are available on the remote computer. With the help of remote login, a user is able to understand the result of transferring the result of processing from the remote computer to the local computer.

### What is HTTPS?

HTTPS stands for **HyperText Transfer Protocol Secure**. It is the most common protocol for sending data between a web browser and a website. It is the secure variant of HTTP used for communication between the browser and the webserver.  In order to make the data transfer more secure, it is encrypted. Encryption is required to ensure security while transmitting sensitive information like passwords, contact information, etc.

### How does HTTPS work?

HTTPS establishes the communication between the browser and the webserver. It uses the **Secure Socket Layer**(SSL) and **Transport Layer Security** (TLS) protocol for establishing communication. The new version of SSL is TSL.

HTTPS uses the conventional HTTP protocol and adds a layer of SSL/TSL over it. The [workflow of HTTP](https://www.geeksforgeeks.org/understanding-http-using-browsers/) and HTTPS remains the same, the browsers and servers still communicate with each other using the HTTP protocol. However, this is done over a secure SSL connection. The SSL connection is responsible for the encryption and decryption of the data that is being exchanged in order to ensure data safety.

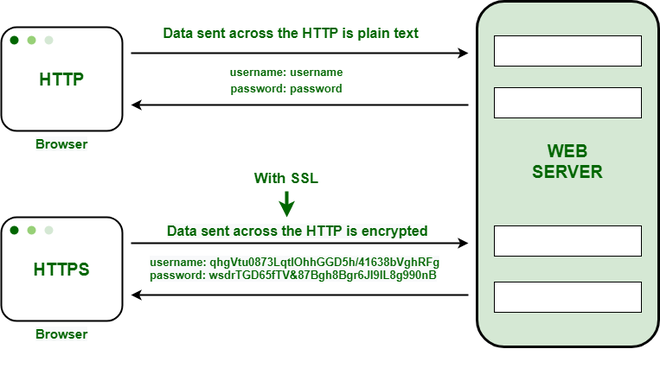
#### Secure Socket Layer (SSL)

The main responsibility of SSL is to ensure that the data transfer between the communicating systems is **secure and reliable**. It is the standard security technology that is used for encryption and decryption of data during the transmission of requests.

As discussed earlier, HTTPS is basically the same old HTTP but with SSL. For establishing a secure communication link between the communicating devices, SSL uses a digital certificate called **SSL certificate**.

There are two major roles of the SSL layer –

* Ensuring that the browser communicates with the required server directly.
* Ensuring that only the communicating systems have access to the messages they exchange.



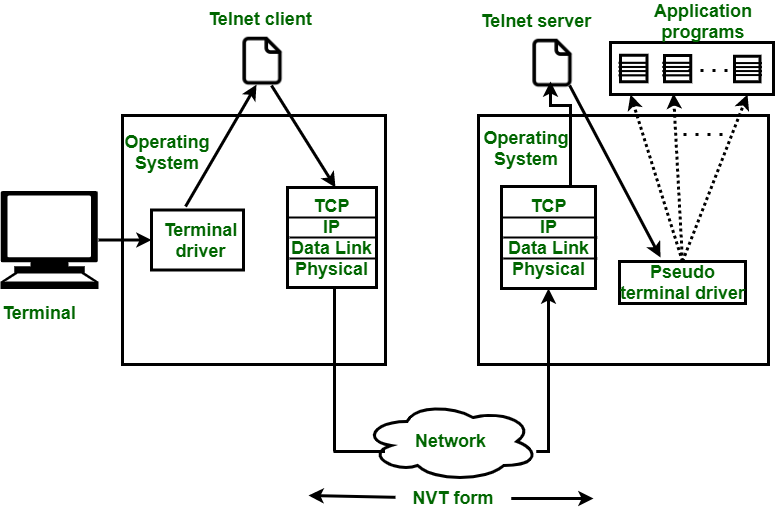
HTTP transfers data in a hypertext format between the browser and the web server, whereas HTTPS transfers data in an encrypted format. As a result, HTTPS protects websites from having their information broadcast in a way that anyone eavesdropping on the network can easily see. During the transit between the browser and the web server, HTTPS protects the data from being accessed and altered by hackers. Even if the transmission is intercepted, hackers will be unable to use it because the message is encrypted.

It uses an asymmetric public key infrastructure for securing a communication link. There are two different kinds of keys used for encryption –

1. **Private Key**: It is used for the decryption of the data that has been encrypted by the public key. It resides on the server-side and is controlled by the owner of the website. It is private in nature.
2. **Public Key**:  It is public in nature and is accessible to all the users who communicate with the server. The private key is used for the decryption of the data that has been encrypted by the public key.

### Advantage of HTTPS

1. **Secure Communication:** HTTPS establishes a secure communication link between the communicating system by providing encryption during transmission.
2. **Data Integrity:** By encrypting the data, HTTPS ensures data integrity. This implies that even if the data is compromised at any point, the hackers won’t be able to read or modify the data being exchanged.
3. **Privacy and Security:** HTTPS prevents attackers from accessing the data being exchanged passively, thereby protecting the privacy and security of the users.
4. **Faster Performance:**TTPS encrypts the data and reduces its size. Smaller size accounts for faster data transmission in the case of HTTPS.



*Remote Login in Logging*

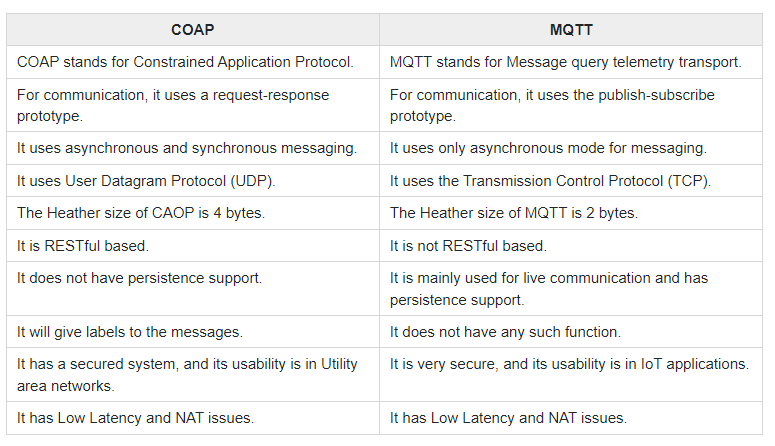
**The Procedure of Remote Login**

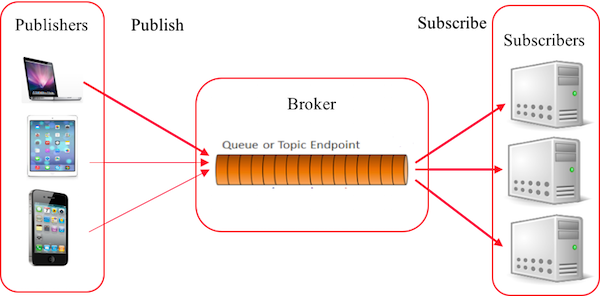
* When the user types something on the local computer, the local operating system accepts the character.
* The local computer does not interpret the characters, it will send them to the TELNET client.
* TELNET client transforms these characters to a universal character set called [Network Virtual Terminal (NVT)](https://www.geeksforgeeks.org/what-is-network-virtual-terminal-in-telnet/) characters and it will pass them to the local TCP/IP protocol Stack.
* Commands or text which are in the form of NVT, travel through the Internet and it will arrive at the [TCP/IP](https://www.geeksforgeeks.org/tcp-ip-model/) stack at the remote computer.
* Characters are then delivered to the operating system and later on passed to the TELNET server.
* Then TELNET server changes those characters to characters that can be understandable by a remote computer.
* The remote operating system receives characters from a pseudo-terminal driver, which is a piece of software that pretends that characters are coming from a terminal.
* The operating system then passes the character to the appropriate application program.

## MQTT (Message Queue Telemetry Transport)

**MQTT (Message Queue Telemetry Transport)** is a messaging protocol which was introduced by IBM in 1999. It was initially built for monitoring sensor node and faraway tracking in IoT. Its suits are small, cheap, low-memory and low-power devices. MQTT provides embedded connectivity between applications and middleware in one side and another side it connects networks and communicators.

MQTT protocol is based on publish/subscribe architecture. The publish/subscribe architecture consists of three major components: publishers, subscribers, and a broker. According to IoT point of view, publishers are lightweight sensor devices that send their data to connected broker and goes back to sleep whenever possible. Subscribers are applications, which are interested in a certain topic or sensory data, so they are connected to brokers to be informed whenever new data are received. The broker receives the sensory data and filters them in different topics and sends them to subscribers according to interest in the topics.

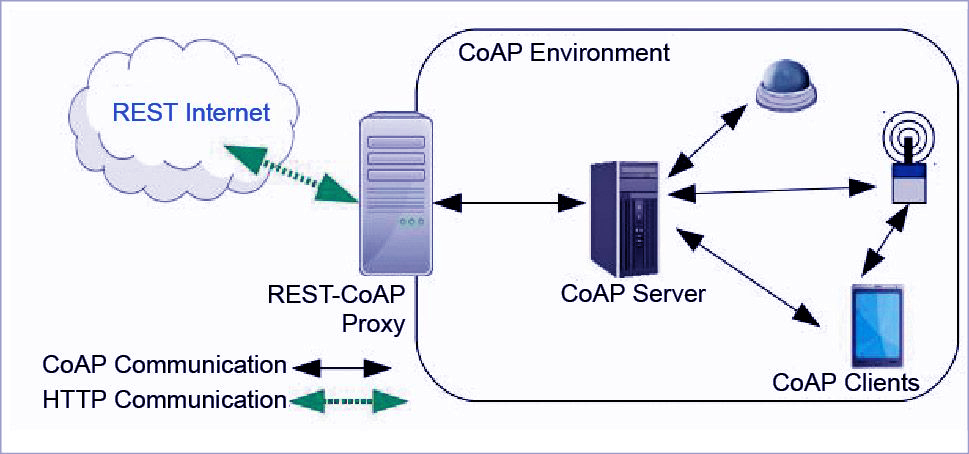




## CoAP

**CoAP (Constrained Application Protocol)** is a session layer protocol that provides the RESTful (HTTP) interface between HTTP client and server. It is designed by IETF Constrained RESTful Environment (CoRE) working group. It is designed to use devices on the same constrained network between devices and general nodes on the Internet. CoAP enables low-power sensors to use RESTful services while meeting their low power constraints. This protocol is specially built for IoT systems primarily based on HTTP protocols.

This network is used within the limited network or in a constrained environment. The whole architecture of CoAP consists of CoAP client, CoAP server, REST CoAP proxy, and REST internet.



The data is sent from CoAP clients (such as smartphones, RFID sensors, etc.) to the CoAP server and the same message is routed to REST CoAP proxy. The REST CoAP proxy interacts outside the CoAP environment and uploads the data over REST internet.