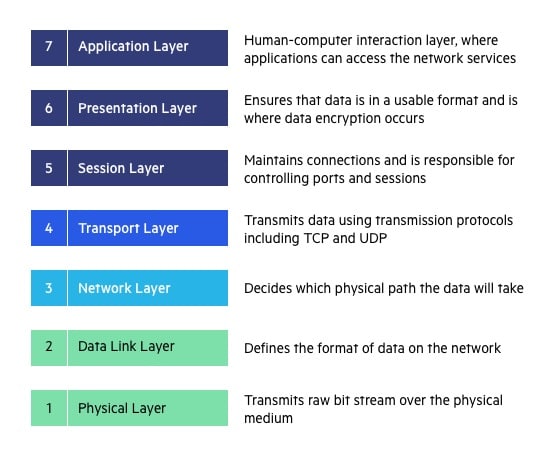
Computer networks

Data communication

data communication refers to the exchange of data between two or more networked or connected devices. These devices must be capable of sending and receiving data over a communication medium.

The OSI Model

* The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.
* It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s
* The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.



**Application Layer**

* The application layer is used by end-user software such as web browsers and email clients.
* It provides protocols that allow software to send and receive information and present meaningful data to users.
* A few examples of application layer protocols are the [Hypertext Transfer Protocol](https://www.imperva.com/learn/performance/http2/) (HTTP), File Transfer Protocol (FTP),Simple Mail Transfer Protocol (SMTP)

**Presentation Layer**

* The presentation layer prepares data for the application layer.
* It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end.
* The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

**Session Layer**

* The session layer creates communication channels, called sessions, between devices.
* It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends.
* The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

**Transport Layer**

* The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end.
* It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer.
* The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

**Network Layer**

* The network layer has two main functions.
* One is breaking up segments into network packets, and reassembling the packets on the receiving end.
* The other is routing packets by discovering the best path across a physical network.
* The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

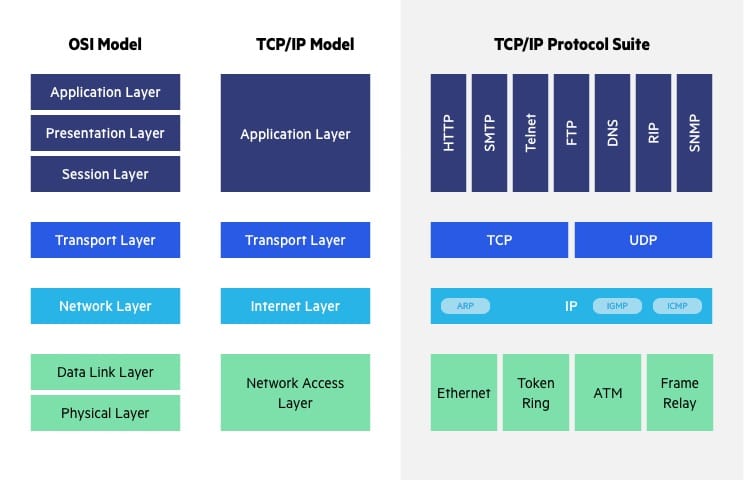
**Data Link Layer**

* The data link layer establishes and terminates a connection between two physically-connected nodes on a network.
* It breaks up packets into frames and sends them from source to destination.
* This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

**Physical Layer**

* The physical layer is responsible for the physical cable or wireless connection between network nodes.
* It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

OSI vs TCP/IP Model



The [Transfer Control Protocol/Internet Protocol](https://www.imperva.com/learn/application-security/tcp-transmission-control-protocol/) (TCP/IP) is older than the OSI model and was created by the US Department of Defense (DoD). A key difference between the models is that TCP/IP is simpler, collapsing several OSI layers into one:

* OSI layers 5, 6, 7 are combined into one Application Layer in TCP/IP
* OSI layers 1, 2 are combined into one Network Access Layer in TCP/IP – however TCP/IP does not take responsibility for sequencing and acknowledgement functions, leaving these to the underlying transport layer.

Other important differences:

* TCP/IP is a functional model designed to solve specific communication problems, and which is based on specific, standard protocols. OSI is a generic, protocol-independent model intended to describe all forms of network communication.
* In TCP/IP, most applications use all the layers, while in OSI simple applications do not use all seven layers. Only layers 1, 2 and 3 are mandatory to enable any data communication.

Transmission media types

Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

* High Speed
* Secure
* Used for comparatively shorter distances

Unguided Media:   
It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Features:

* The signal is broadcasted through air
* Less Secure
* Used for larger distances

Network devices

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another.

Network devices play two roles.

* The first is establishing a network connection, as a router or a modem does.
* The second one is maintaining, protecting and enhancing that connection, as with a hub, repeater, switch or gateway.

## Types of network devices

 Repeater –

* A repeater operates at the physical layer.
* Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network.
* An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it.
* When the signal becomes weak, they copy it bit by bit
* It is a 2-port device.

Hub –

* A hub is a basically multi-port repeater.
* A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
* Hubs cannot filter data, so data packets are sent to all connected devices.
* Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Bridge

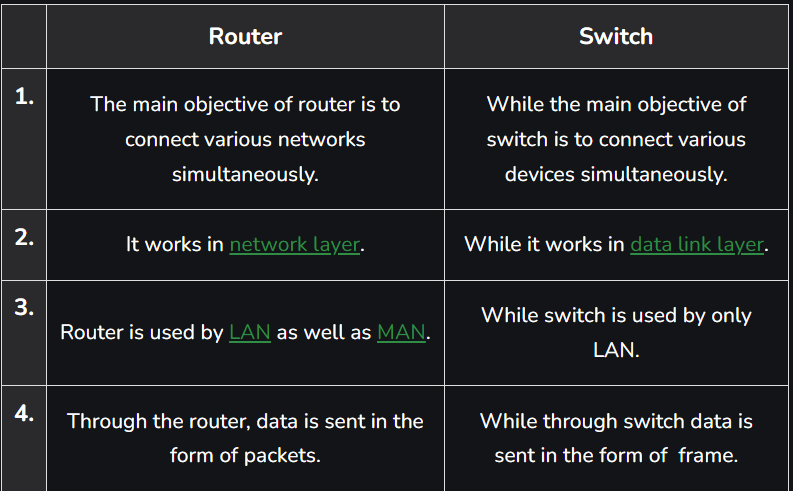
* A bridge operates at the data link layer.
* A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination.
* It is also used for interconnecting two LANs working on the same protocol.
* It has a single input and single output port, thus making it a 2 port device.

Switch –

* A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance.
* A switch is a data link layer device.
* The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.

Routers –

* A router is a device like a switch that routes data packets based on their IP addresses.
* The router is mainly a Network Layer device.
* Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets



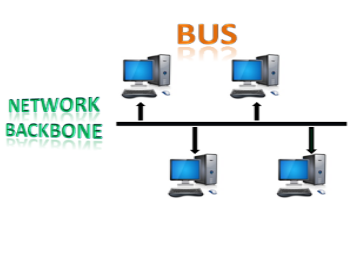
Gateway –

* A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models.
* They work as messenger agents that take data from one system, interpret it, and transfer it to another system.
* Gateways are also called protocol converters and can operate at any network layer.
* Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

# **Network Topology**

Topology defines the structure of the network of how all the components are interconnected to each other.

## Bus Topology



* The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
* The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

**CSMA:** It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

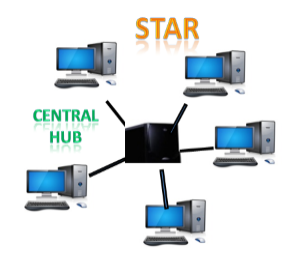
* **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
* **CSMA CA:** **CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

## Ring Topology



* Ring topology is like a bus topology, but with connected ends.
* The node that receives the message from the previous computer will retransmit to the next node.
* The data flows in one direction, i.e., it is unidirectional.
* The data flows in a single loop continuously known as an endless loop.
* It has no terminated ends, i.e., each node is connected to other node and having no termination point.
* The data in a ring topology flow in a clockwise direction

## Star Topology



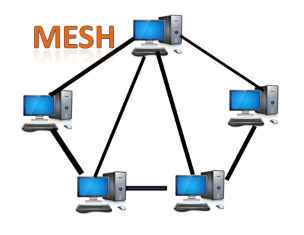
* Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
* The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.

## Tree topology

## Computer Network Topologies

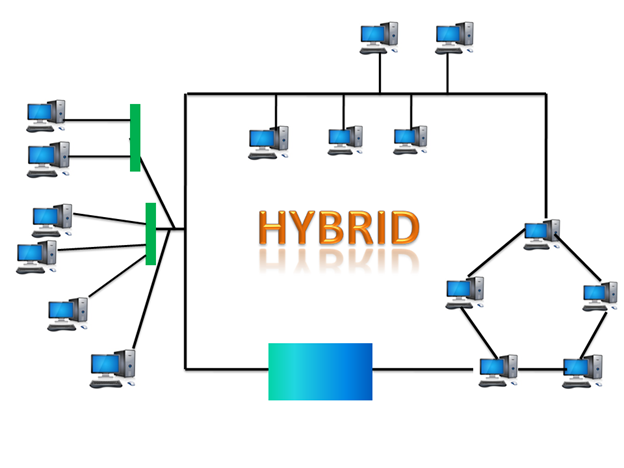
* Tree topology combines the characteristics of bus topology and star topology.
* A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
* The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
* There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

## Mesh topology



* Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
* There are multiple paths from one computer to another computer.

Hybrid Topology



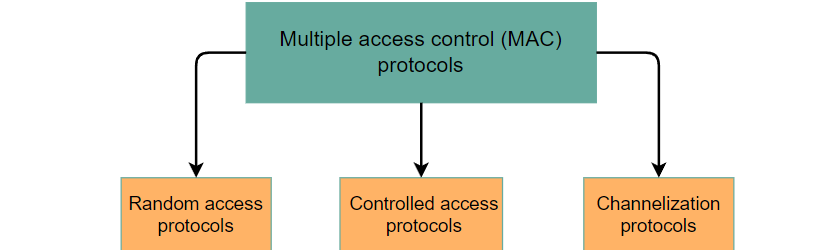
* The combination of various different topologies is known as **Hybrid topology**.

DATA LINK LAYER

MAC protocol

MAC protocol stands for Medium Access Control protocol. It is a set of rules that govern how devices on a shared network communicate with each other. The MAC protocol is responsible for preventing collisions when two or more devices try to transmit data at the same time.

MAC protocol classification



In **random access protocol**, no station has a higher priority than another station. Instead, all are equal. There is no predetermined time for sending data; it depends on the channel's status. The order of the stations transmitting data is not predefined.

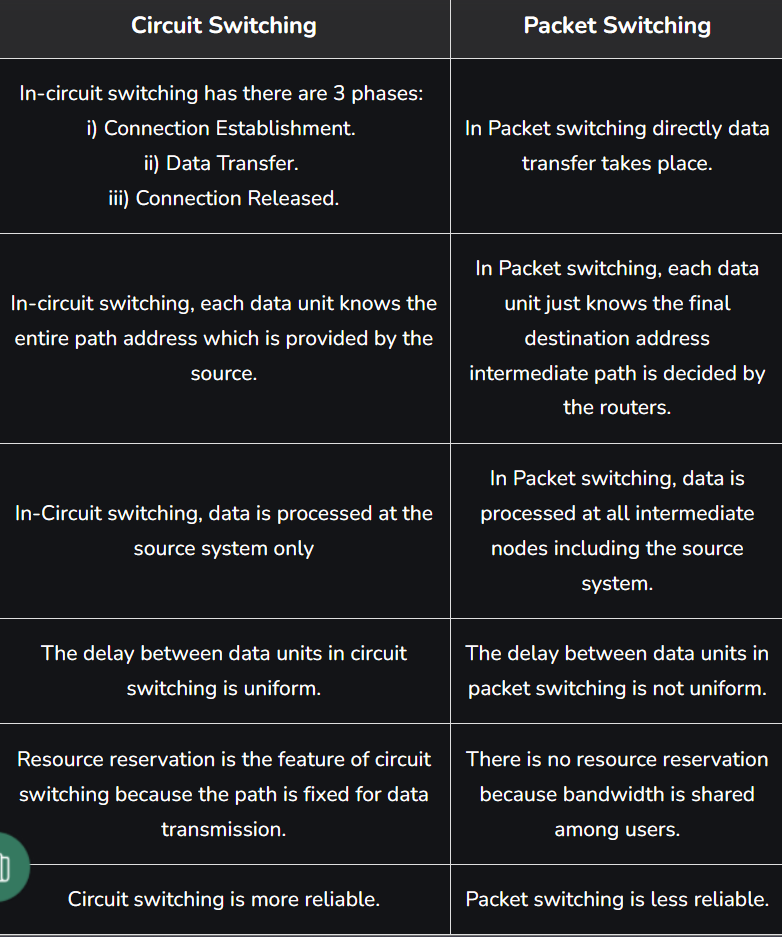
In the **controlled access** approach, all the stations communicate with each other to determine which station has the authority to send data in order to avoid collision.

Channelization protocols are a type of MAC protocol that divide the available bandwidth of a shared medium into smaller channels. This allows multiple devices to transmit data simultaneously without interfering with each other.

Network layer

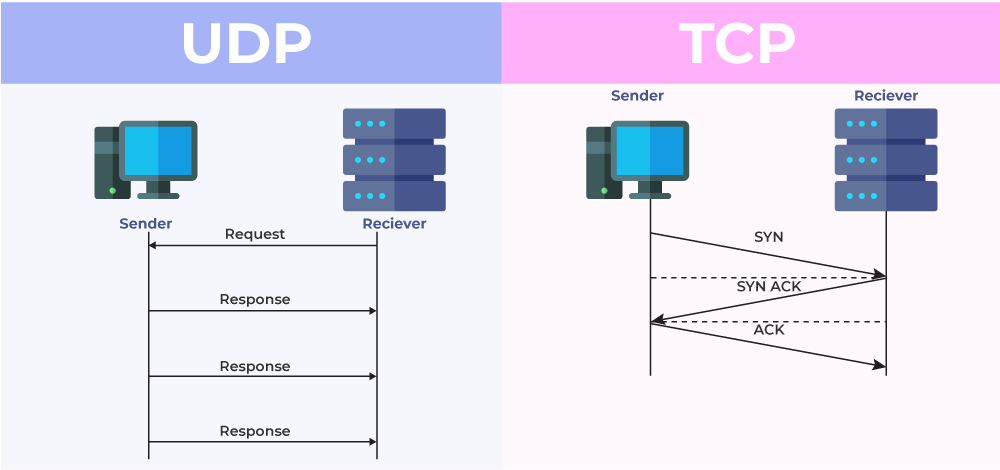
Switching

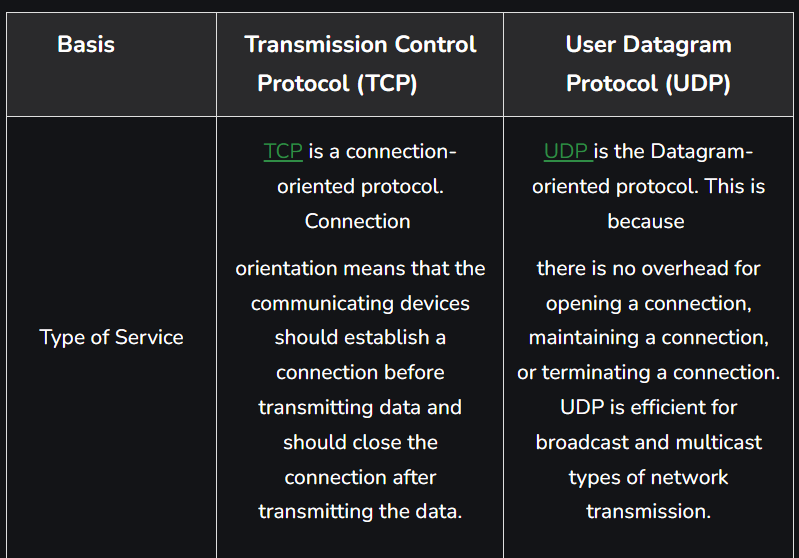
Switching in computer networks is the process of transferring data packets from one device to another in a network, or from one network to another, using specific devices called switches.



TRANSPORT LAYER

Udp vs tcp





A black and white grid with white text

Description automatically generated

A black and white text

Description automatically generated

Congestion control and resource allocation

* Congestion control and resource allocation involve both hosts and network elements such as routers. In network elements, various queuing disciplines can be used to control the order in which packets get transmitted and which packets get dropped.
* The queuing discipline can also segregate traffic to keep one user’s packets from unduly affecting another user’s packets.
* At the end hosts, the congestion-control mechanism paces how fast sources are allowed to send packets.
* This is done in an effort to keep congestion from occurring in the first place and, should it occur, to help eliminate the congestion.

application layer

DNS

* DNS stands for Domain Name System.
* DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
* DNS is required for the functioning of the internet.
* Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
* DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
* For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

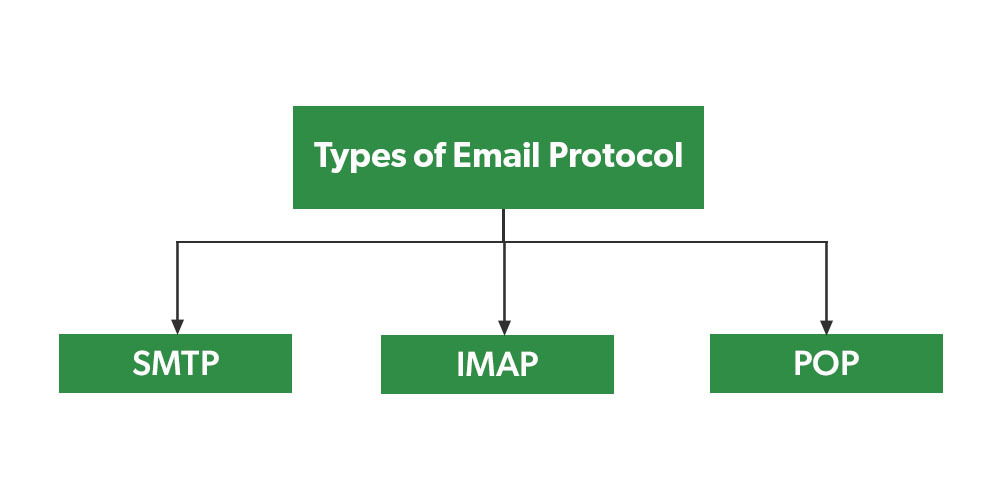
Electronic mails

Electronic mail, commonly known as email, is a method of exchanging messages over the internet. Here are the basics of email:

An email address: This is a unique identifier for each user, typically in the format of name@domain.com.

An email client: This is a software program used to send, receive and manage emails, such as Gmail, Outlook, or Apple Mail.

An email server: This is a computer system responsible for storing and forwarding emails to their intended recipients.



## What is POP3?

* POP3, short for post office protocol, version 3, is an inbound email protocol.
* An inbound protocol allows a device to retrieve email messages from a server.
* For example, if your computer supports POP3, you can download email messages to your local machine from a server.
* This protocol stores the emails within your inbox folder on your device.
* By default, POP3 deletes the messages from the server once the download is complete.
* This protocol lacks synchronization between devices.
* The absence of synchronization means that if you have two computers set up to the same email account, the emails you access with one computer are unavailable on the other device.

## What is IMAP?

* Internet Message Access Protocol (IMAP) is an inbound email protocol.
* IMAP keeps your emails on the server by default and stores only small reference copies of them on your devices.
* This feature synchronizes your emails within every folder across all the computers associated with the account, allowing you to access your messages via multiple devices

## What is SMTP?

* Simple Mail Transfer Protocol (SMTP) is an outbound email protocol.
* [Outbound email](https://www.indeed.com/career-advice/career-development/what-is-email-outbound) protocols manage the sending of email messages from a server to a client.
* Servers can use these protocols to control how they route email messages, ensure that messages arrive on time and track any errors during delivery.
* When you click "send" on an email, the message travels from your device to an SMTP server.
* An SMTP protocol on the server finds a correct route.
* The server sends the email to the recipient using the route it selects. The message uses SMTP to travel to the recipient's email server, where it stays until the recipient retrieves the email.
* SMTP is the primary outbound email protocol.

http

* HTTP represents "Hypertext Transfer Protocol." HTTP is the protocol that can transfer information over the network. It is the Internet protocol suite method and defines commands and functions used for sharing web page data.
* HTTP uses a server-client model. A client, for example, maybe a laptop or telephone device. The HTTP server is frequently a web host running web server software, such as Apache or IIS.
* HTTP also represents commands such as GET and POST, which are used to handle submissions on websites. The CONNECT command can act as a fast connection that is encrypted using a secure socket layer (SSL).
* HTTP is equivalent to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in how the messages are sent from the client to the server and from the server to the client. SMTP messages are saved and advanced, while HTTP messages are delivered directly.

ftp

* File transfer protocol (FTP) is a way to download, upload, and transfer files from one location to another on the Internet and between computer systems.
* FTP enables the transfer of files back and forth between computers or through the cloud.
* Users require an Internet connection in order to execute FTP transfers.
* FTP is an essential tool for those who build and maintain websites.
* File transfer protocol allows individuals and businesses to share electronic files with others without having to be in the same space. This can be done using an FTP client
* File transfer protocol allows individuals and businesses to share electronic files with others without having to be in the same space. This can be done using an FTP client