Notes on Application Layer

Application Layer:

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers.

The Application layer includes the following functions:

- **Identifying communication partners:** The application layer identifies the availability of communication partners for an application with data to transmit.
- **Determining resource availability:** The application layer determines whether sufficient network resources are available for the requested communication.
- **Synchronizing communication:** All the communications occur between the applications requires cooperation which is managed by an application layer.

Services of Application Layers

- **Network Virtual terminal:** An application layer allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which in turn, talks to the host. The remote host thinks that it is communicating with one of its own terminals, so it allows the user to log on.
- **File Transfer, Access, and Management (FTAM):** An application allows a user to access files in a remote computer, to retrieve files from a computer and to manage files in a remote computer. FTAM defines a hierarchical virtual file in terms of file structure, file attributes and the kind of operations performed on the files and their attributes.
- **Addressing:** To obtain communication between client and server, there is a need for addressing. When a client made a request to the server, the request contains the server address and its own address. The server response to the client request, the request contains the destination address, i.e., client address. To achieve this kind of addressing, DNS is used.
- **Mail Services:** An application layer provides Email forwarding and storage.
- **Directory Services:** An application contains a distributed database that provides access for global information about various objects and services.
    - Authentication: It authenticates the sender or receiver's message or both.

Network Application Architecture

Application architecture is different from the network architecture. The network architecture is fixed and provides a set of services to applications. The application architecture, on the

other hand, is designed by the application developer and defines how the application should be structured over the various end systems.

Application architecture is of two types:

- **Client-server architecture:** An application program running on the local machine sends a request to another application program is known as a client, and a program that serves a request is known as a server. For example, when a web server receives a request from the client host, it responds to the request to the client host.

Characteristics of Client-server architecture:

- In Client-server architecture, clients do not directly communicate with each other. For example, in a web application, two browsers do not directly communicate with each other.
- A server is fixed, well-known address known as IP address because the server is always on while the client can always contact the server by sending a packet to the sender's IP address.

Disadvantage of Client-server architecture:

It is a single server based architecture which is incapable of holding all the requests from the clients. For example, a social networking site can become overwhelmed when there is only one server exists.

- **P2P (peer-to-peer) architecture:** It has no dedicated server in a data center. The peers are the computers which are not owned by the service provider. Most of the peers reside in the homes, offices, schools, and universities. The peers communicate with each other without passing the information through a dedicated server, this architecture is known as peer-to-peer architecture. The applications based on P2P architecture includes file sharing and internet telephony.

Features of P2P architecture

- **Self scalability:** In a file sharing system, although each peer generates a workload by requesting the files, each peer also adds a service capacity by distributing the files to the peer.
- **Cost-effective:** It is cost-effective as it does not require significant server infrastructure and server bandwidth.

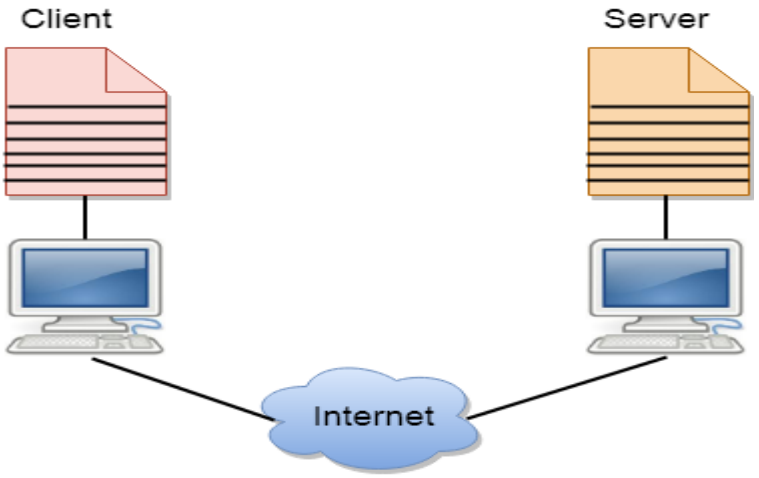
Client and Server processes

- A network application consists of a pair of processes that send the messages to each other over a network.

- In P2P file-sharing system, a file is transferred from a process in one peer to a process in another peer. We label one of the two processes as the client and another process as the server.
- With P2P file sharing, the peer which is downloading the file is known as a client, and the peer which is uploading the file is known as a server. However, we have observed in some applications such as P2P file sharing; a process can be both as a client and server. Therefore, we can say that a process can both download and upload the files.

Client and Server model

- A client and server networking model is a model in which computers such as servers provide the network services to the other computers such as clients to perform a user based tasks. This model is known as client-server networking model.
- The application programs using the client-server model should follow the given below strategies:



- An application program is known as a client program, running on the local machine that requests for a service from an application program known as a server program, running on the remote machine.
- A client program runs only when it requests for a service from the server while the server program runs all time as it does not know when its service is required.
- A server provides a service for many clients not just for a single client. Therefore, we can say that client-server follows the many-to-one relationship. Many clients can use the service of one server.
- Services are required frequently, and many users have a specific client-server application program. For example, the client-server application program allows the user to access the files, send e-mail, and so on. If the services are more customized, then we should have one generic application program that allows the user to access the services available on the remote computer.

Client

A client is a program that runs on the local machine requesting service from the server. A client program is a finite program means that the service started by the user and terminates when the service is completed.

Server

A server is a program that runs on the remote machine providing services to the clients. When the client requests for a service, then the server opens the door for the incoming requests, but it never initiates the service.

A server program is an infinite program means that when it starts, it runs infinitely unless the problem arises. The server waits for the incoming requests from the clients. When the request arrives at the server, then it responds to the request.

Advantages of Client-server networks:

- **Centralized:** Centralized back-up is possible in client-server networks, i.e., all the data is stored in a server.
- **Security:** These networks are more secure as all the shared resources are centrally administered.
- **Performance:** The use of the dedicated server increases the speed of sharing resources. This increases the performance of the overall system.
- **Scalability:** We can increase the number of clients and servers separately, i.e., the new element can be added, or we can add a new node in a network at any time.

Disadvantages of Client-Server network:

- **Traffic Congestion** is a big problem in Client/Server networks. When a large number of clients send requests to the same server may cause the problem of Traffic congestion.
- It does not have a robustness of a network, i.e., when the server is down, then the client requests cannot be met.
- A client/server network is very decisive. Sometimes, regular computer hardware does not serve a certain number of clients. In such situations, specific hardware is required at the server side to complete the work.
- Sometimes the resources exist in the server but may not exist in the client. For example, If the application is web, then we cannot take the print out directly on printers without taking out the print view window on the web.

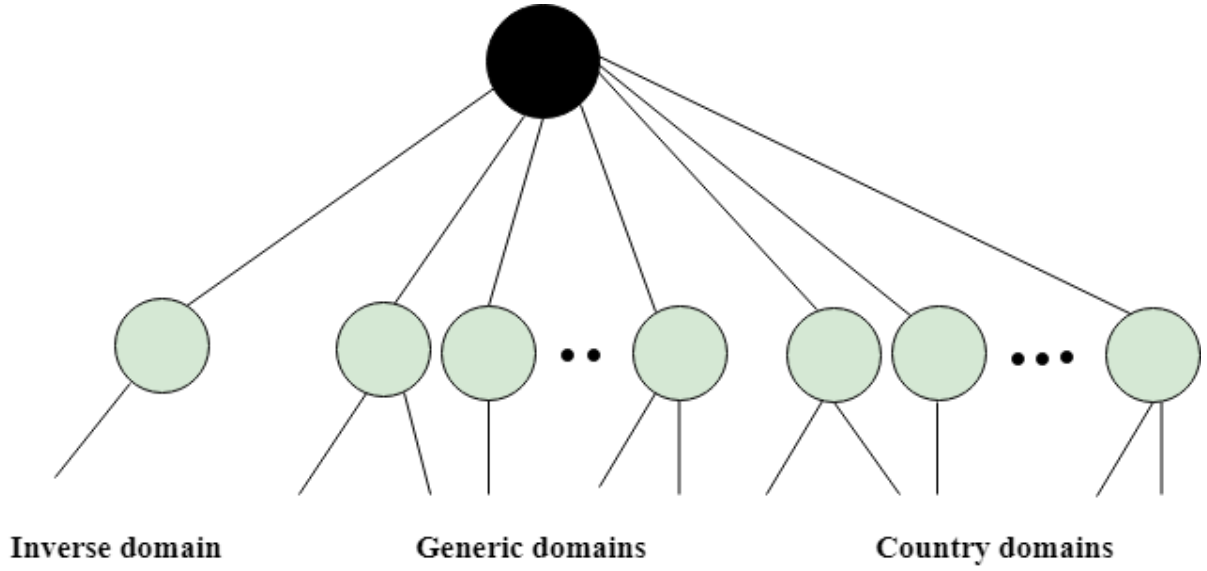
DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- 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.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

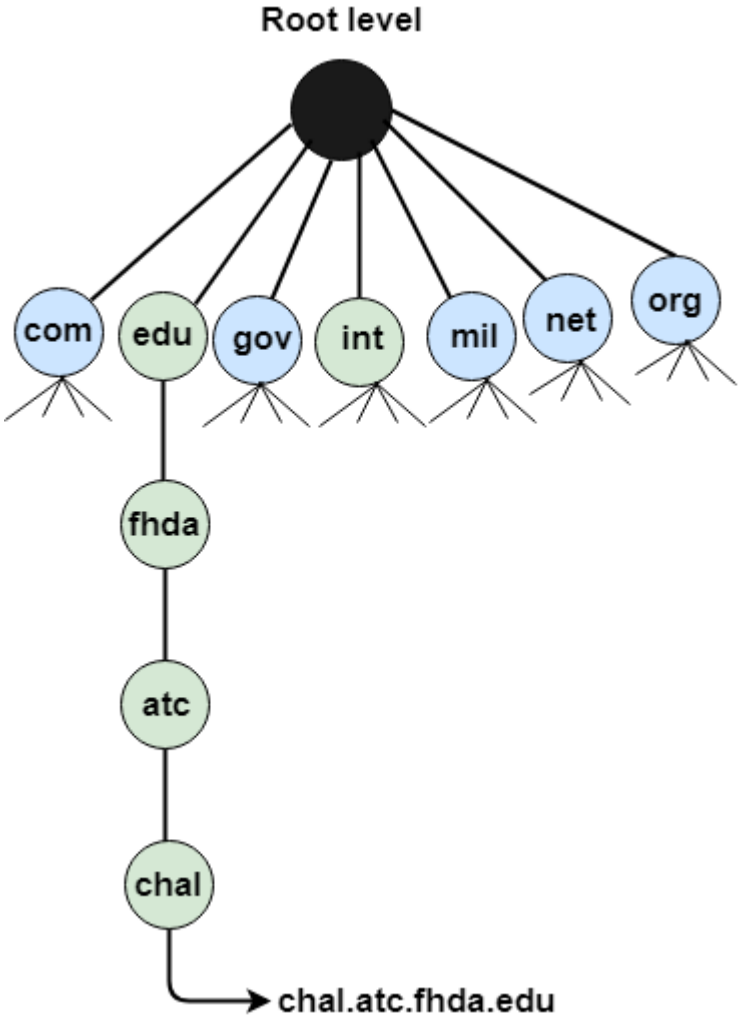


Generic Domains

- It defines the registered hosts according to their generic behaviour.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations

coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations



Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three-character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookup while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

Differentiate between FQDN and PQDN

The difference between FQDN and PQDN

FQDN

A fully qualified domain name (FQDN) is the complete domain name for a specific computer, or host, on the Internet. The FQDN consists of two parts: the hostname and the domain name. For example, an FQDN for a hypothetical mail server might bemymail.somecollege.edu. The hostname is my mail, and the host is located within the domainsomecollege.edu.

PQDN

If a label is not terminated by a null string, it is called a partially qualified domain name (PQDN). A PQDN starts from a node, but it does not reach the root. It is used when the name to be resolved belongs to the same site as the client. Here the resolver can supply the missing part, called suffix, to create an FQDN.

Dynamic Domain Name System (DDNS) in Application Layer:

When DNS (Domain Name System) was designed, nobody expected that there would be so many address changes such as adding a new host, removing a host, or changing an IP

address. When there is a change, the change must be made to the DNS master file which needs a lot of manual updating and it must be updated dynamically.

Dynamic Domain Name System (DDNS) :

It is a method of automatically updating a name server in the Domain Name Server (DNS), often in real-time, with the active DDNS configuration of its configured hostnames, addresses, or other information. In DDNS, when a binding between a name and an address is determined, the information is sent, usually by DHCP (Dynamic Host Configuration Protocol) to a primary DNS server.
The primary server updates the zone. The secondary servers are notified either actively or passively. Inactive notification, the primary server sends a message to secondary servers, whereas, in the passive notification, the secondary servers periodically check for any changes. In either case, after being notified about the change, the secondary requests information about the entire zone (zone transfer).

DDNS can use an authentication mechanism to provide security and prevent unauthorized changes in DNS records.

Advantages :

1. It saves time required by static addresses updates manually when network configuration changes.
2. It saves space as the number of addresses are used as required at one time rather than using one for all the possible users of the IP address.
3. It is very comfortable for users point of view as any IP address changes will not affect any of their activities.
4. It does not affect accessibility as changed IP addresses are configured automatically against URL's.

Disadvantages :

1. It is less reliable due to lack of static IP addresses and domain name mappings.
2. Dynamic DNS services alone can not make any guarantee about the device you are attempting to connect is actually your own.

Uses :

1. It is used for Internet access devices such as routers.
2. It is used for for security appliance manufacturers and even required for IP-based security appliances like DVRs.

- **The main difference between DNS and DDNS**
  - DNS is used with static IP address
  - Dynamic DNS is used with dynamic IP addresses. In this IP address gets an IP from DHCP server therefore the IP address changes periodically.
  - DDNS allows you to access devices in your home such as computer, router or CC camera.You can access them from anywhere in the world even if your IP address changes.
  - DDNS is mostly used in Homes because internet service that are used in home are mostly given dynamic IP but not a static IP.
  - DDNS allows you to access your computer even if your IP address changes.

What is FTP?

What is FTP? One of the most popular uses of the Internet is to download files – that is, transfer files from a computer on the Internet to your computer. Many thousands of files are downloaded every day from the Internet. Most of these files are downloaded using the Internet's File Transfer Protocol, commonly referred to as FTP. This protocol can also be used to upload files from your computer to another computer on the Internet.

FTP (File Transfer Protocol)

File Transfer Protocol is a standard network protocol used to exchange and manipulate files over a TCP/IP-based network, such as the Internet. FTP is built on client-server architecture and utilizes separate control and data connections between the client and server applications. FTP is used with user-based password authentication or with anonymous user access. Applications were originally interactive command-line tools with standardized command syntax, but graphical user interfaces have been developed for all desktop operating systems in use today. The Trivial File Transfer Protocol (TFTP) is a similar, but simplified, not interoperable, and unauthenticated version of FTP.

Numerous FTP servers all over the world allow users anywhere on the Internet to log in and down-load files placed on them. The main competitor for FTP is HTTP (Hyper Text Transfer Protocol) and the day is not very far when sites would run HTTP servers instead of the FTP servers. It is so because HTTP servers can do whatever FTP server can do and do it more efficiently.

As the Web gains popularity, downloading software is becoming even easier. You can use your Web browser and click on links to files; behind the scenes, FTP is often still downloading the files.

One problem with downloading files over the Internet is that some files are so large that it can take a tremendous amount of time to download them. As a way to speed up file transfers and save space on the FTP server, files are commonly *compressed.* Many different methods are used to compress files. After the files have been downloaded, you will need to run the decompression software such as PK UNZIP to decompress the files to use them.

Once you have the compressed file such as data. zip, you will need to unzip or decompress it to get to the setup file and install the program.

Features of FTP

The basic features of FTP are:

1. Data representation

• FTP handles three types of data representations-ASCII (7 bit), EBCDIC (8-bit) and 8-binary data.

• The **ASCII file** is the default format for transferring text files

• Each character is encoded using 7-bit ASCII. The sender transforms the file from its own representation into ASCII characters and the receiver transforms the ASCII character to its own representation.

• The **image file** is the default format for transferring binary files. The file is sent as continuous streams of bits without any interpretation or encoding.

2. File organization and Data structures

• FTP supports both unstructured and structured file.

• An unstructured file contains string of bytes and is enl-marked by EOF (End of file). The data structure that corresponds to such a file is called **file structure.**

• A structured file contains a list of records and each record is delimited by EDR (End of Record). The data structure of such file is called **record structure** *i.e.* file is divided into records.

• Another structured file contains pages, with each page having a page number and a page header. The pages can be stored and accessed randomly or sequentially. The corresponding data structure is called **page structure** *i.e.* file is divided into pages.

3. Transmission modes

• FTP can transfer a file by using one of the following three modes:

Stream mode

• It is the default mode.

• File is transmitted as continuous stream of bytes to TCP.

• TCP is responsible for chopping data into segments of appropriate size.

• If data is simply a stream of bytes (file structure), no end-of-file is needed. EOF in this case is the closing of the data connection by the sender.

• If data is divided into records (record structure), each record has a I-byte EOR (End-of-Record) character and the end of the file has a I-byte EOF (End-of-file) character.

Block mode

• Data is delivered from FTP to TCP in blocks.

• Each block is preceded by 3 bytes header.

• The first byte is called the block descriptor.

• The second and third byte defines the size of the block in bytes.

Compressed mode

• Data is usually compressed if the file to be transmitted is very big.

• The compression method normally used in Run-length encoding.

• In a text file, usually spaces (blanks) are removed.

• In a binary file, null characters are compressed.

4. Error control

• Since TCP is used for data transfer no additional error recovery mechanism is required.

5. Access control

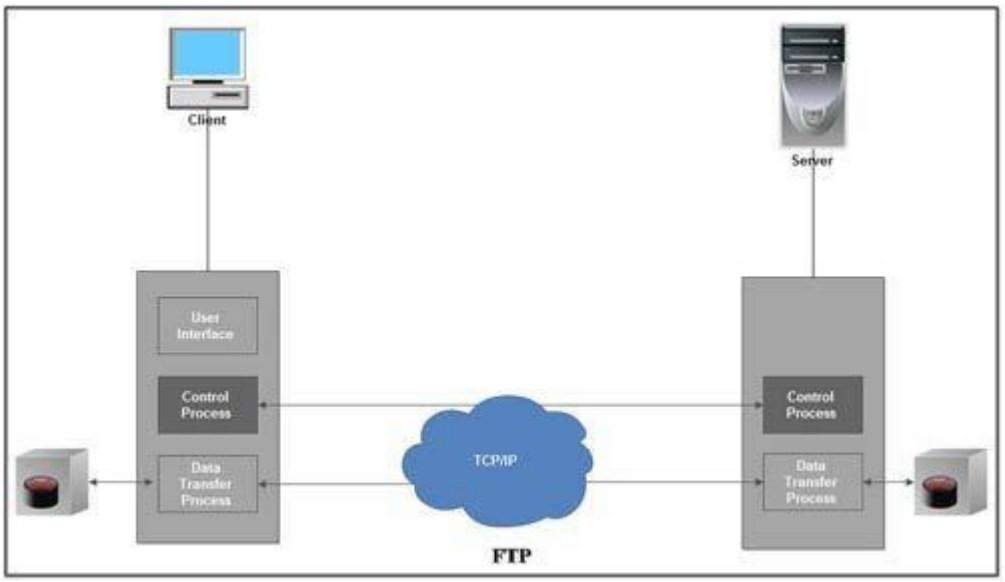
• File access protection is done using login procedure with login name and password.

FTP operation

• FTP uses client/server model for communication.

• Two TCP connections are used for file transfer.

• On one connection control signals (commands and responses) are exchanged and the other connection is used for actual data transfer. These two connections are called control connection and data connection respectively.



Control Connection

The Control connection has following features:

1. It is used to transfer control signals (commands and responses) between the client and server.

2. This connection is used by the control process of client and server. The control process is called Protocol Interpreter (PI).

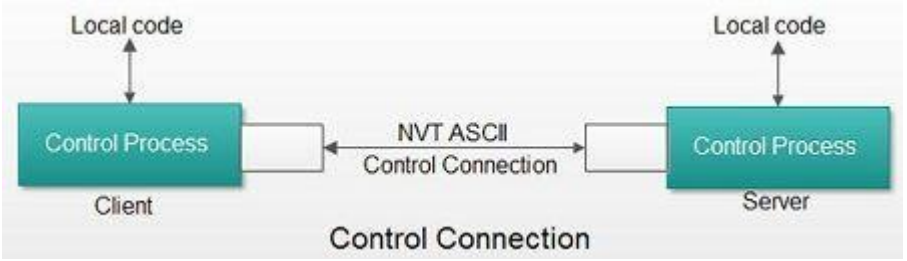
3. The TCP connection for control signal uses well-known FTP server port 21.

4. This control connection remains connected during the entire interactive FTP session.

5. The control connection uses very simple rules of communication. We need to transfer only a line of command or a line of response at a time.

6. The two control processes (client & server) or PI communicates using NVT syntax.

7. The PIs are responsible for translating the local code or syntax. (e.g. DOS or UNIX) into NVT syntax and vice-vers



Data Connection

The Data connection has following features:

1. Data connection is used for actual data transfer.

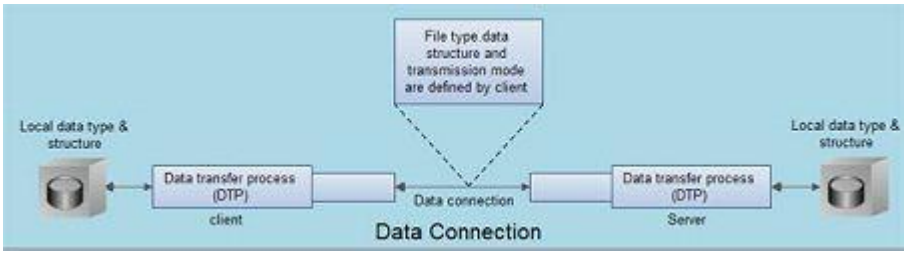
2. This connection is established between the Data Transfer Process (DTP) of client and server

3. The server port used for data connection is Port 20.

4. The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when the file is transferred.

5. File transfer occurs over the data connection under the control of the commands sent over the control connection.

6. During the file transfer, the client must define the type of file to be transferred, the structure of data and the transmission mode.



Thus, file transfer in FTP means one of three things:

1. A file is to be copied from the server to the client. This is called *retrieving a file.* It is done with help of *RETR command.*

2. A file is to be copied from the client to the server. This is called *storing a file.* It is done with *STOR command.*

3. A list of directory or file names is to be sent from the server to the client. This is done with *LLST command.*

Anonymous FTP

• To Use FTP, a user needs an account (user name) and a password on the Remote server.

• Some sites have a set of files available for public access; to enable *anonymous FTP.*

• To access these files, a user does not need to have an account or password. Instead, the user can use *Anonymous* as the user name and *guest* as the password.

FTP Servers

Similar to the Web servers, the Internet also has the installations of FTP servers. Many organizations use FTP servers to handle the distribution of files. When a user links to download something, the link actually redirects to FTP, instead of HTTP. Some files in the FTP servers may be accessible to the general public, while others are accessible only by the user. To separate the general public from the more private users, FTP servers are divided into two parts:

Anonymous server

Non-anonymous server

1. Anonymous Server: Anonymous server is the most common use of FTP, the Internet file transfer protocol. FTP sites that allow anonymous FTP do not require a password for access. You only have to log in as anonymous and enter your e-mail address as password (for their records).

2. Non-anonymous Server: If you use a non-anonymous server, then you will log in as yourself and give your password.

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.

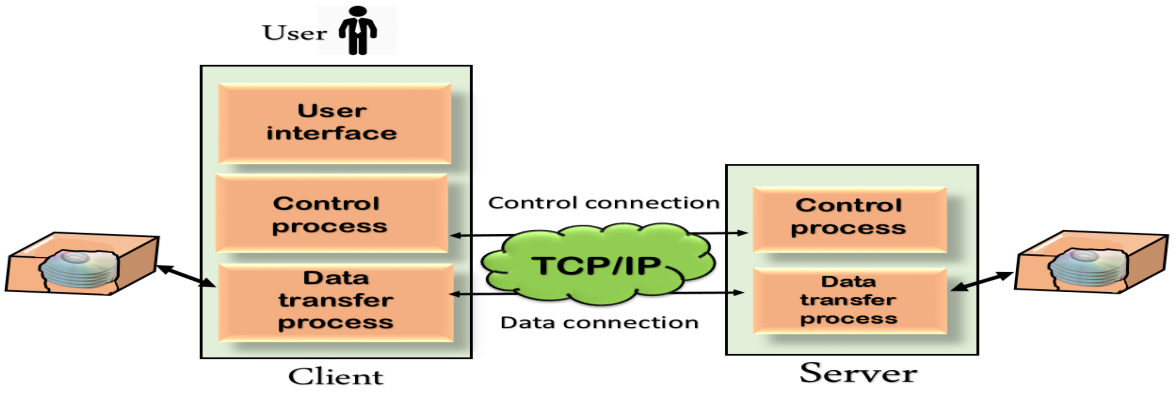
Objectives of FTP

- 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?

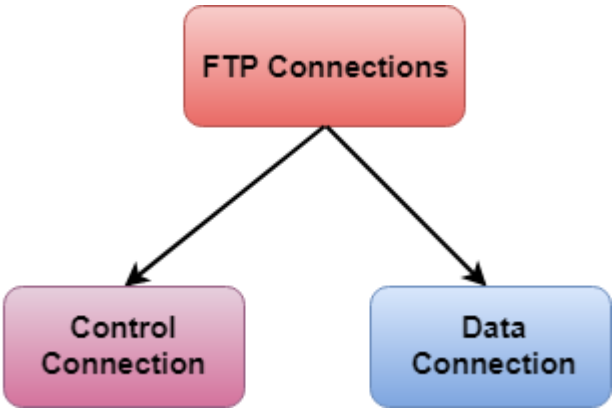
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. 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:

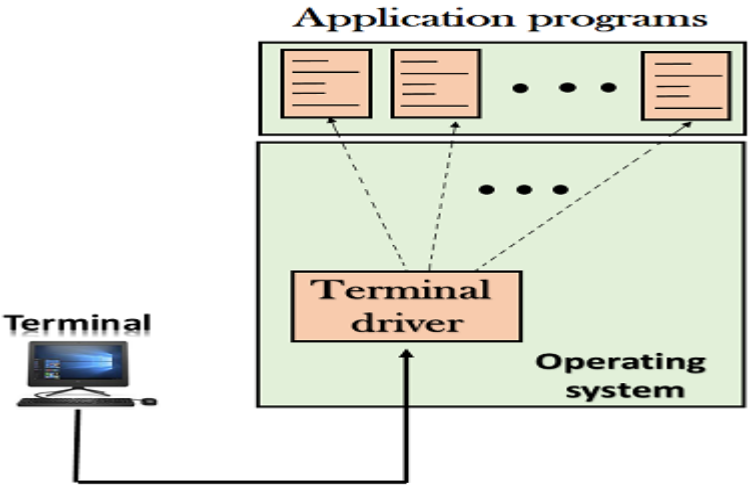
- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to 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:

- The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.
- The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer. A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for **Terminal Network**.
- Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

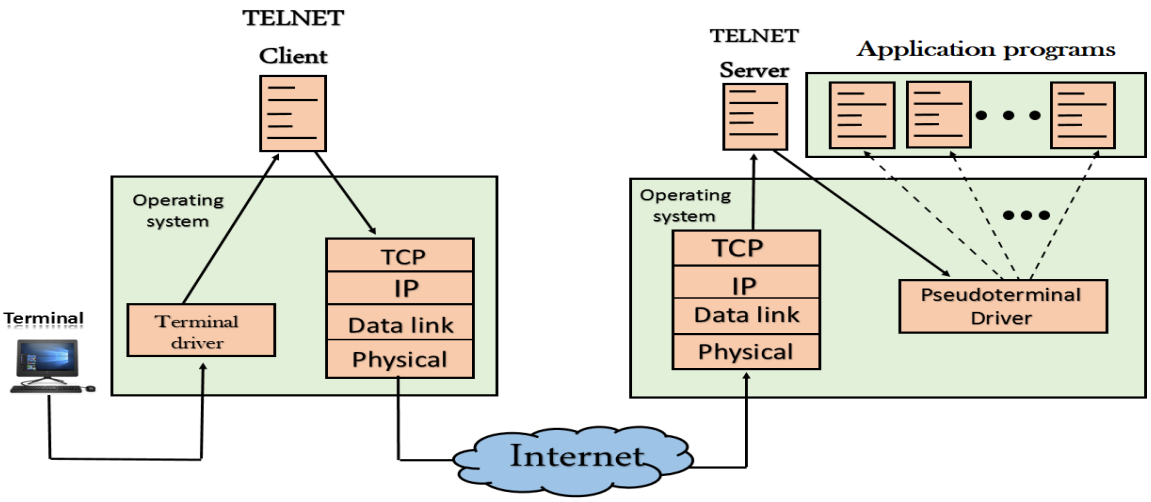
There are two types of login:

Local Login



- **When a user logs into a local computer, then it is known as local login.**
- **When the workstation running terminal emulator, the keystrokes entered by the user are accepted by the terminal driver. The terminal driver then passes these characters to the operating system which in turn, invokes the desired application program.**
- **However, the operating system has special meaning to special characters. For example, in UNIX some combination of characters have special meanings such as control character with "z" means suspend. Such situations do not create any problem as the terminal driver knows the meaning of such characters. But, it can cause the problems in remote login.**

Remote login



- When the user wants to access an application program on a remote computer, then the user must perform remote login.

How remote login occurs

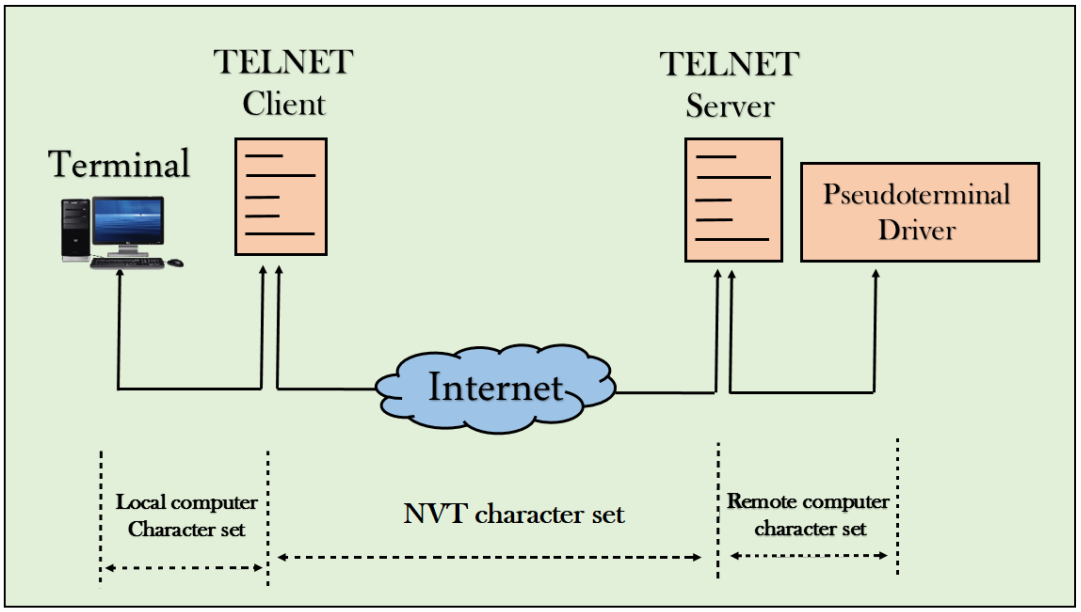
At the local site

The user sends the keystrokes to the terminal driver, the characters are then sent to the TELNET client. The TELNET client which in turn, transforms the characters to a universal character set known as network virtual terminal characters and delivers them to the local TCP/IP stack

At the remote site

The commands in NVT forms are transmitted to the TCP/IP at the remote machine. Here, the characters are delivered to the operating system and then pass to the TELNET server. The TELNET server transforms the characters which can be understandable by a remote computer. However, the characters cannot be directly passed to the operating system as a remote operating system does not receive the characters from the TELNET server. Therefore it requires some piece of software that can accept the characters from the TELNET server. The operating system then passes these characters to the appropriate application program.

Network Virtual Terminal (NVT)



- The network virtual terminal is an interface that defines how data and commands are sent across the network.
- In today's world, systems are heterogeneous. For example, the operating system accepts a special combination of characters such as end-of-file token running a DOS operating system *ctrl+z* while the token running a UNIX operating system is *ctrl+d*.
- TELNET solves this issue by defining a universal interface known as network virtual interface.

- The TELNET client translates the characters that come from the local terminal into NVT form and then delivers them to the network. The Telnet server then translates the data from NVT form into a form which can be understandable by a remote computer.

What is email?

E-mail is short for electronic mail, mail you can send or receive directly on your computer. Yes, with e-mail people can actually write you letters and send them to your computer, and you can turn on your computer and go pick up your mail whenever it's convenient. Many a love affair has begun through e-mail. I know. It's really fun, too. And useful, of course. E-mail can be a verb too, as in "I e-mailed my lover a letter from Lhasa."

Although basically a method of passing messages from one computer to another email is becoming increasingly popular, in part because those computers sending messages to each other could be in adjacent offices or on opposite sides of the world. In fact the ability to send a letter or memo halfway across the world at the speed of electricity instead of the more traditional postal services is one of the strengths of the Internet. Because of email even the remotest office can maintain practically instant communication with headquarters, or even another remote office.

E-mail may not be as personal as a handwritten note, but it's the quickest and most convenient way yet to communicate written information. If something absolutely positively has to be there in ten minutes, e-mail can get it there on time. I write for magazines and corporations all over the country, but I never leave my room. If an article has to be in by Friday at noon, I can finish it Friday at 11:45 and e-mail the computer file to New York before the deadline.

E-mail is also great for taking care of business without having to go through all the social pleasantries we endure in phone conversations you can get straight to the point without having to ask how the kids are doing. "Attached is the file on the DeVere controversy. Tell me what you think." Contrast e-mail with *snailmail.*

To send or receive e-mail, you must have a *modem* or your computer has to be on a *network* (connected to other computers). Your company or organization may have its own e-mail system with its own software-in which case you'll run a version of that software on your machine. Lotus' CC:Mail is probably still the most popular e-mail software around for PCs. Alternatively, e-mail services are available on many *bulletin boards* and *online services)* and there are specialized services such as MCI Mail whose primary mission is to distribute e-mail.

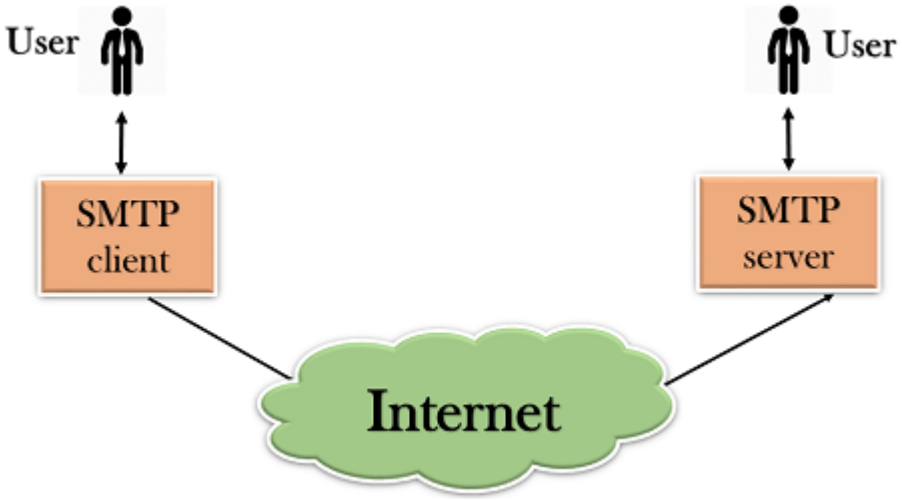
You can also send and receive files by direct *telecommunications)* where your modem calls the other party's modem. But that entails the other person having to wait for your call and hanging around until they receive the entire file. They might not be able to use their computer for anything else in the meantime. With e-mail, you can send the mail anytime you want and they can pick it up anytime they want.

SMTP

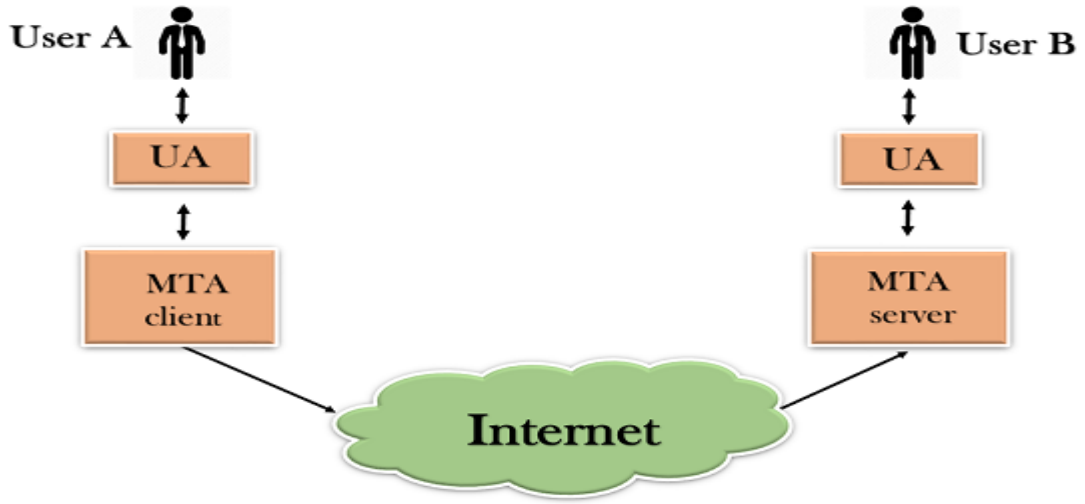
- SMTP stands for Simple Mail Transfer Protocol.

- 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.

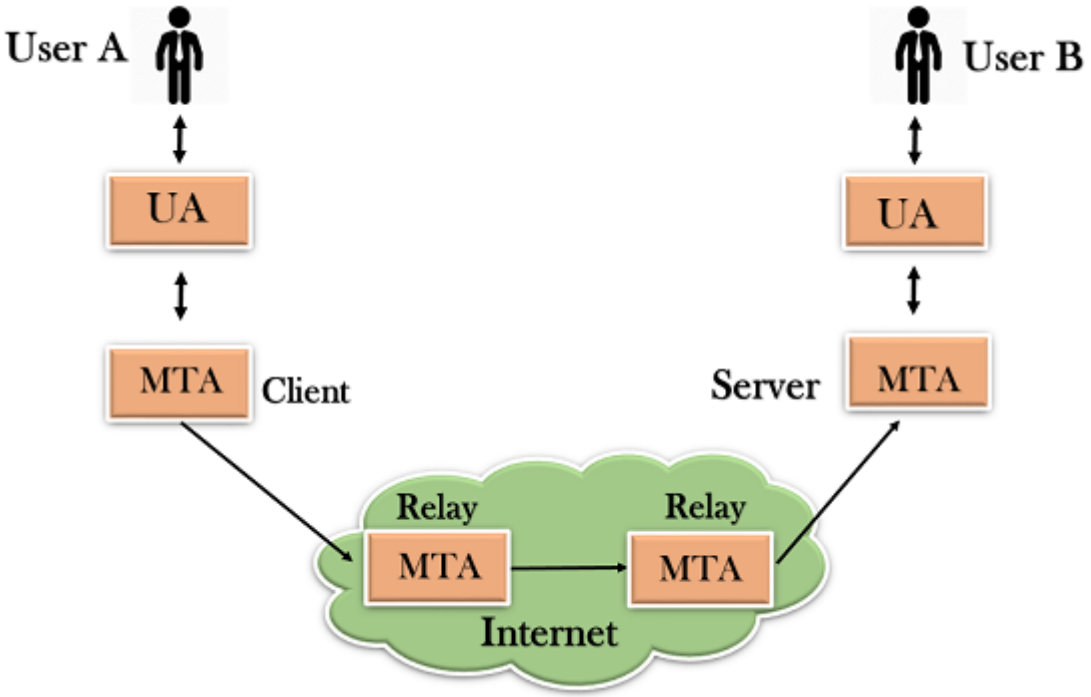
Components of SMTP



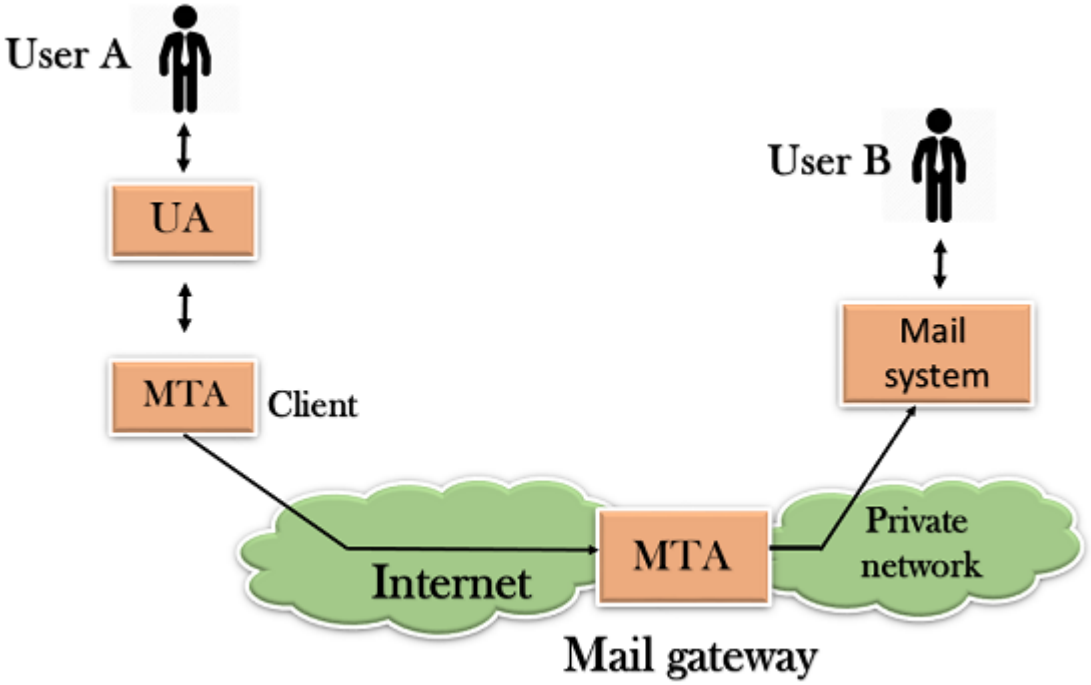
- First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.



- SMTP allows a more complex system by adding a relaying system. Instead of just having one MTA at sending side and one at receiving side, more MTAs can be added, acting either as a client or server to relay the email.



- The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway. The mail gateway is a relay MTA that can be used to receive an email.



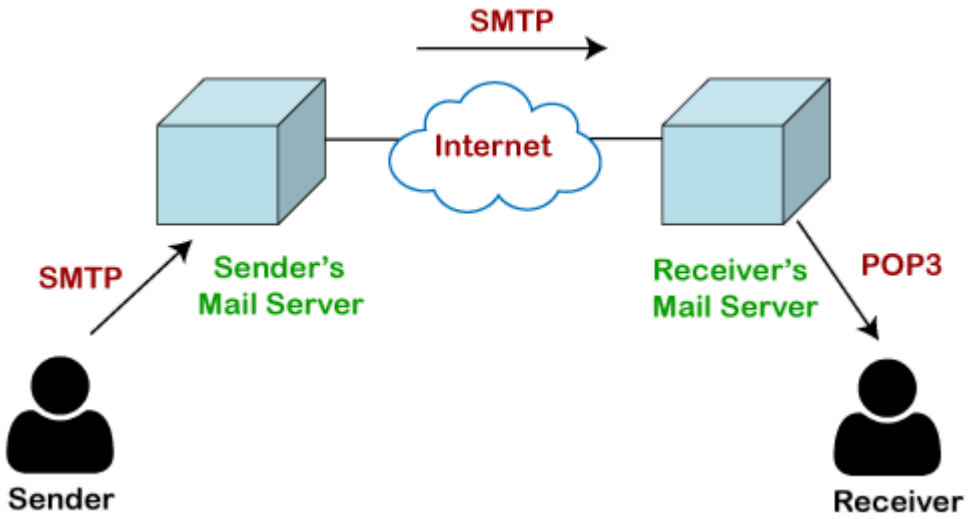
Working of SMTP

1. **Composition of Mail:** A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.
2. **Submission of Mail:** After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.
3. **Delivery of Mail:** E-mail addresses contain two parts: username of the recipient and domain name. For example, vivek@gmail.com, where "vivek" is the username of the recipient and "gmail.com" is the domain name.
   If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain. The MX record contains the domain name and IP address of the recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message.
4. **Receipt and Processing of Mail:** Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.
5. **Access and Retrieval of Mail:** The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

POP Protocol

The POP protocol stands for Post Office Protocol. As we know that SMTP is used as a message transfer agent. 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. The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.

How is mail transmitted?



Suppose sender wants to send the mail to receiver. First mail is transmitted to the sender's mail server. Then, the mail is transmitted from the sender's mail server to the receiver's mail server over the internet. On receiving the mail at the receiver's mail server, the mail is then sent to the user. The whole process is done with the help of Email protocols. The transmission of mail from the sender to the sender's mail server and then to the receiver's mail server is done with the help of the SMTP protocol. At the receiver's mail server, the POP or IMAP protocol takes the data and transmits to the actual user.

Since SMTP is a push protocol so it pushes the message from the client to the server. As we can observe in the above figure that SMTP pushes the message from the client to the recipient's mail server. The third stage of email communication requires a pull protocol, and POP is a pull protocol. When the mail is transmitted from the recipient mail server to the client which means that the client is pulling the mail from the server.

What is POP3?

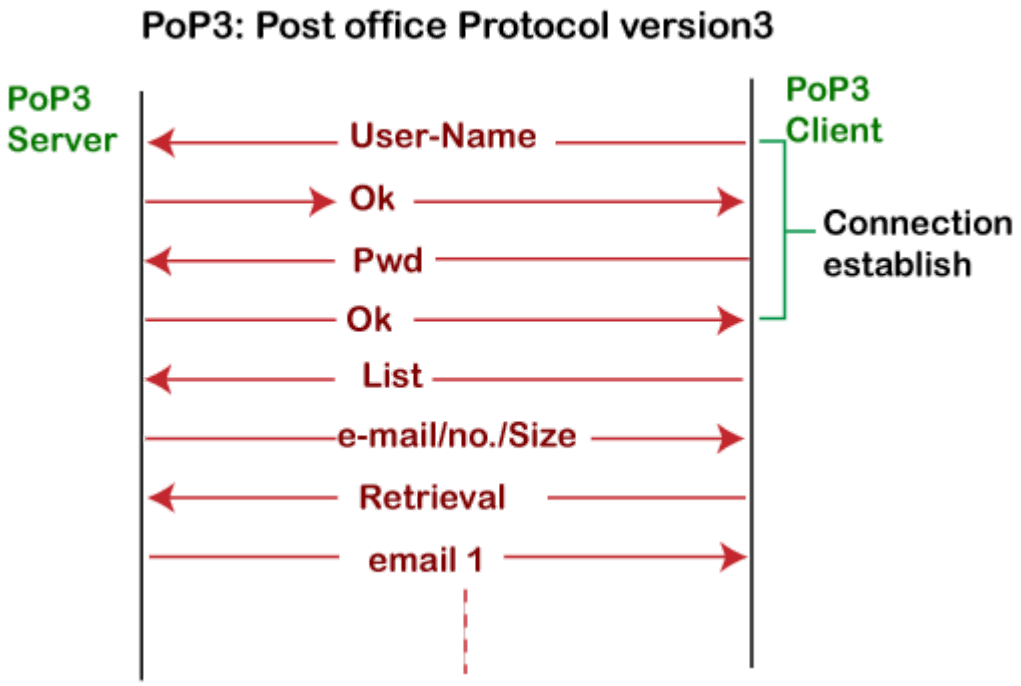
The POP3 is a simple protocol and having very limited functionalities. In the case of the POP3 protocol, the POP3 client is installed on the recipient system while the POP3 server is installed on the recipient's mail server.

History of POP3 protocol

Although the POP3 protocol has undergone various enhancements, the developers maintained a basic principle that it follows a three-stage process at the time of mail retrieval between the

client and the server. They tried to make this protocol very simple, and this simplicity makes this protocol very popular today.

Let's understand the working of the POP3 protocol.



To establish the connection between the POP3 server and the POP3 client, the POP3 server asks for the user name to the POP3 client. If the username is found in the POP3 server, then it sends the ok message. It then asks for the password from the POP3 client; then the POP3 client sends the password to the POP3 server. If the password is matched, then the POP3 server sends the OK message, and the connection gets established. After the establishment of a connection, the client can see the list of mails on the POP3 mail server. In the list of mails, the user will get the email numbers and sizes from the server. Out of this list, the user can start the retrieval of mail.

Once the client retrieves all the emails from the server, all the emails from the server are deleted. Therefore, we can say that the emails are restricted to a particular machine, so it would not be possible to access the same mails on another machine. This situation can be overcome by configuring the email settings to leave a copy of mail on the mail server.

Advantages of POP3 protocol

The following are the advantages of a POP3 protocol:

- It allows the users to read the email offline. It requires an internet connection only at the time of downloading emails from the server. Once the mails are downloaded from the server, then all the downloaded mails reside on our PC or hard disk of our computer, which can be accessed without the internet. Therefore, we can say that the POP3 protocol does not require permanent internet connectivity.
- It provides easy and fast access to the emails as they are already stored on our PC.

- There is no limit on the size of the email which we receive or send.
- It requires less server storage space as all the mails are stored on the local machine.
- There is maximum size on the mailbox, but it is limited by the size of the hard disk.
- It is a simple protocol so it is one of the most popular protocols used today.
- It is easy to configure and use.

Disadvantages of POP3 protocol

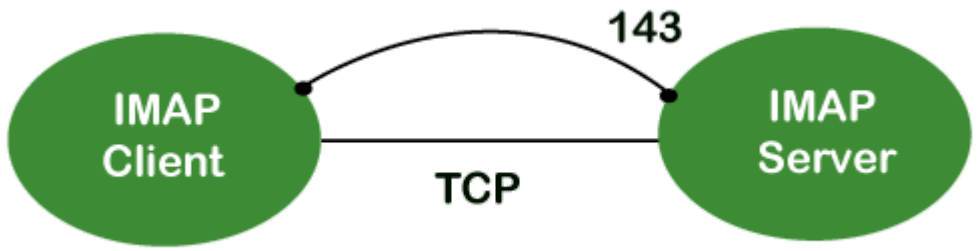
The following are the advantages of a POP3 protocol:

- If the emails are downloaded from the server, then all the mails are deleted from the server by default. So, mails cannot be accessed from other machines unless they are configured to leave a copy of the mail on the server.
- Transferring the mail folder from the local machine to another machine can be difficult.
- Since all the attachments are stored on your local machine, there is a high risk of a virus attack if the virus scanner does not scan them. The virus attack can harm the computer.
- The email folder which is downloaded from the mail server can also become corrupted.
- The mails are stored on the local machine, so anyone who sits on your machine can access the email folder.

IMAP Protocol

IMAP stands for **Internet Message Access Protocol**. It is an application layer protocol which is used to receive the emails from the mail server. It is the most commonly used protocols like POP3 for retrieving the emails.

It also follows the client/server model. On one side, we have an IMAP client, which is a process running on a computer. On the other side, we have an IMAP server, which is also a process running on another computer. Both computers are connected through a network.



The IMAP protocol resides on the TCP/IP transport layer which means that it implicitly uses the reliability of the protocol. Once the TCP connection is established between the IMAP client and IMAP server, the IMAP server listens to the port 143 by default, but this port number can also be changed.

By default, there are two ports used by IMAP:

- Port 143: It is a non-encrypted IMAP port.
- Port 993: This port is used when IMAP client wants to connect through IMAP securely.

Why should we use IMAP instead of POP3 protocol?

POP3 is becoming the most popular protocol for accessing the TCP/IP mailboxes. It implements the offline mail access model, which means that the mails are retrieved from the mail server on the local machine, and then deleted from the mail server. Nowadays, millions of users use the POP3 protocol to access the incoming mails. Due to the offline mail access model, it cannot be used as much. The online model we would prefer in the ideal world. In the online model, we need to be connected to the internet always. The biggest problem with the offline access using POP3 is that the mails are permanently removed from the server, so multiple computers cannot access the mails. The solution to this problem is to store the mails at the remote server rather than on the local server. The POP3 also faces another issue, i.e., data security and safety. The solution to this problem is to use the disconnected access model, which provides the benefits of both online and offline access. In the disconnected access model, the user can retrieve the mail for local use as in the POP3 protocol, and the user does not need to be connected to the internet continuously. However, the changes made to the mailboxes are synchronized between the client and the server. The mail remains on the server so different applications in the future can access it. When developers recognized these benefits, they made some attempts to implement the disconnected access model. This is implemented by using the POP3 commands that provide the option to leave the mails on the server. This works, but only to a limited extent, for example, keeping track of which messages are new or old become an issue when both are retrieved and left on the server. So, the POP3 lacks some features which are required for the proper disconnected access model.

IMAP Features

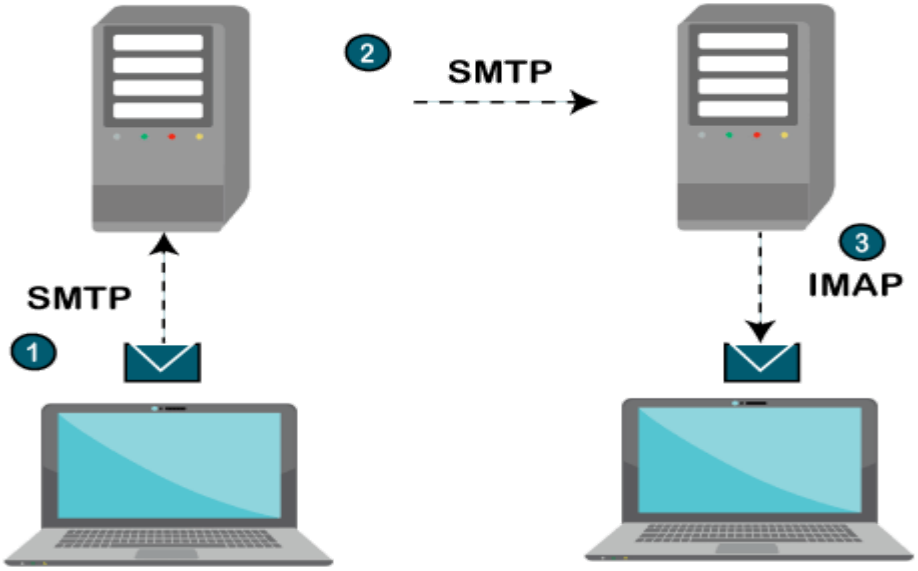
IMAP was designed for a specific purpose that provides a more flexible way of how the user accesses the mailbox. It can operate in any of the three modes, i.e., online, offline, and disconnected mode. Out of these, offline and disconnected modes are of interest to most users of the protocol.

The following are the features of an IMAP protocol:

- Access and retrieve mail from remote server: The user can access the mail from the remote server while retaining the mails in the remote server.
- Set message flags: The message flag is set so that the user can keep track of which message he has already seen.
- Manage multiple mailboxes: The user can manage multiple mailboxes and transfer messages from one mailbox to another. The user can organize them into various categories for those who are working on various projects.
- Determine information prior to downloading: It decides whether to retrieve or not before downloading the mail from the mail server.

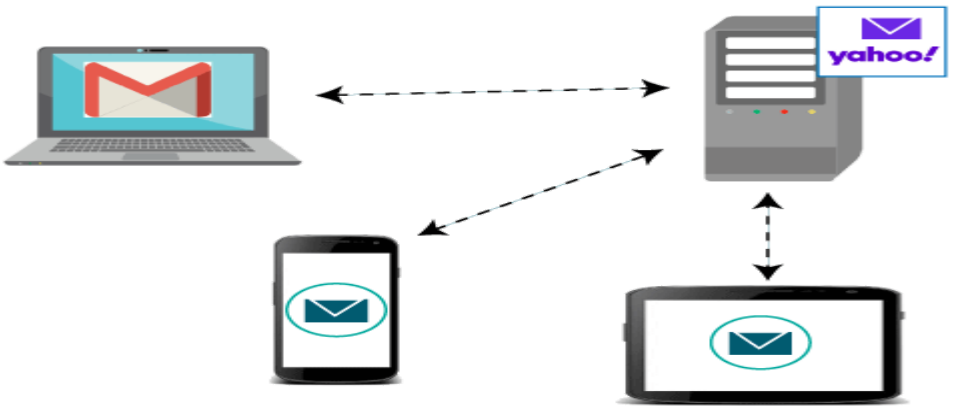
- Downloads a portion of a message: It allows you to download the portion of a message, such as one body part from the mime-multi part. This can be useful when there are large multimedia files in a short-text element of a message.
- Organize mails on the server: In case of POP3, the user is not allowed to manage the mails on the server. On the other hand, the users can organize the mails on the server according to their requirements like they can create, delete or rename the mailbox on the server.
- Search: Users can search for the contents of the emails.
- Check email-header: Users can also check the email-header prior to downloading.
- Create hierarchy: Users can also create the folders to organize the mails in a hierarchy.

IMAP General Operation



1. The IMAP is a client-server protocol like POP3 and most other TCP/IP application protocols. The IMAP4 protocol functions only when the IMAP4 must reside on the server where the user mailboxes are located. In c the POP3 does not necessarily require the same physical server that provides the SMTP services. Therefore, in the case of the IMAP protocol, the mailbox must be accessible to both SMTP for incoming mails and IMAP for retrieval and modifications.
2. The IMAP uses the Transmission Control Protocol (TCP) for communication to ensure the delivery of data and also received in the order.
3. The IMAP4 listens on a well-known port, i.e., port number 143, for an incoming connection request from the IMAP4 client.

Let's understand the IMAP protocol through a simple example.



The IMAP protocol synchronizes all the devices with the main server. Let's suppose we have three devices desktop, mobile, and laptop as shown in the above figure. If all these devices are accessing the same mailbox, then it will be synchronized with all the devices. Here, synchronization means that when mail is opened by one device, then it will be marked as opened in all the other devices, if we delete the mail, then the mail will also be deleted from all the other devices. So, we have synchronization between all the devices. In IMAP, we can see all the folders like spam, inbox, sent, etc. We can also create our own folder known as a custom folder that will be visible in all the other devices.

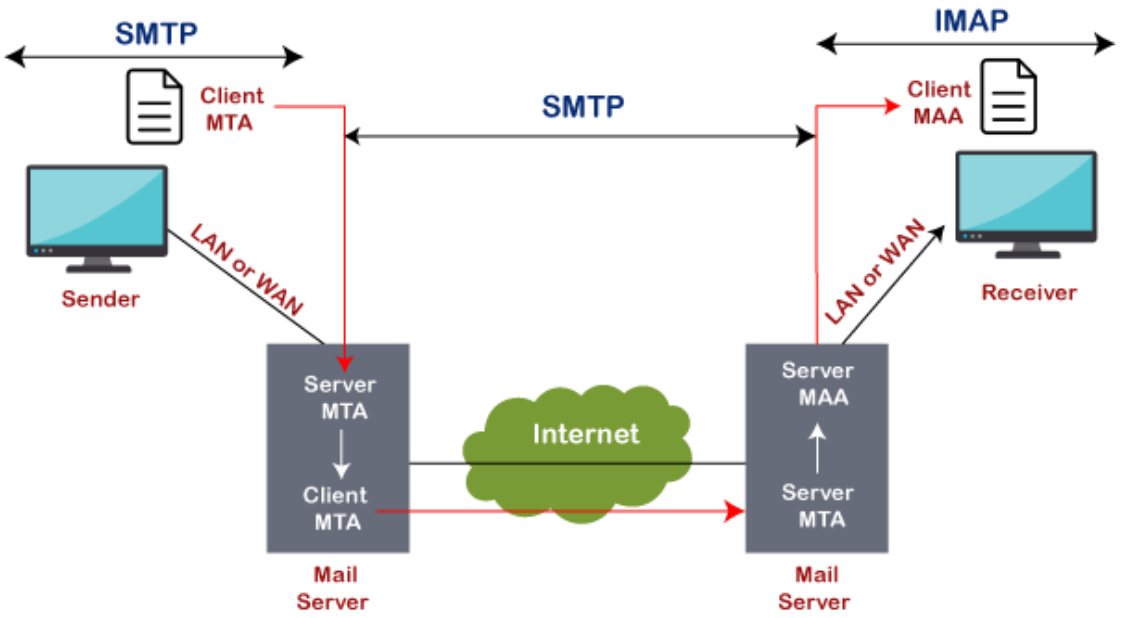
IMAP vs. POP3 | Difference between IMAP and POP3:

POP3 and IMAP are the popular email protocols that are used to access emails from a third-party email client or software. These two are the commonly used Email Protocols on the internet. Both these protocols help to connect to the mail server with the email client through which you have set up your email address. We can select any one of them to set up our email address. Similar to Simple Mail Transfer Protocol (SMTP), POP3 and IMAP also have specific functions and working principles. Let's discuss the POP3 and IMAP in detail, along with their differences.

What is IMAP?

IMAP is abbreviated as **Internet Message Access Protocol**. *IMAP is an internet protocol that works on managing and retrieving emails on the remote server from a local client. It* also works as MAA **or Message Accessing Agent**. Since IMAP deals with the retrieval of messages so we can't send emails using IMAP protocol on the internet. The IMAP protocol is supported by all email clients and web servers.

The working of IMAP is shown in below image:



When to use IMAP?

If you are accessing your email from different devices like mobile, laptop and workstation desktop, etc., then it always better to use the IMAP protocol.

Features of IMAP

There are some features of IMAP, which are as follows:

- Emails are stored on the server instead of an email client.
- Sent messages are also stored on the server-side in the sent folder, which allows us to check the sent email from anywhere.
- You can synchronize the messages and access youremail from multiple devices.
- It is more complex and flexible.
- It helps to download email data from AOL to your device or software.
- We will not lose our emails even if our device is destroyed or stolen.
- The server also saves the status of the emails, such as read, unread, or replied. It helps to check the status of an email from any computer or device.
- When we start downloading emails using IMAP, it firstly shows the header (Sender, date, email subject); at that instant, we can decide whether to download the email or not.

What is POP3?

POP3 is abbreviated as **Post Office Protocol**, and the number three stands for "version 3," which is the latest version and the most widely used email protocol on the internet. Similar to IMAP protocol, it is another protocol for receiving emails from remote servers. It also acts as a message accessing agent to retrieve the message from the mail server to the receiver's system. It helps to protect emails from spam and viruses on the internet.

POP3 works on two modes: **Delete mode** and **Keep mode.**

It works on **Delete mode** when a user is accessing an email service from a permanent device. In this, once the mails are downloaded or retrieved from the mailbox, mails are deleted from the mailbox permanently.

It operates on **Keep mode** when the user is not accessing mails from the primary device. In this, it keeps the mails after retrieval also for later retrieval.

When to Use POP3?

Use POP3 for the following cases:

- We should use POP3 if we want to access mails using a single device
- If the number of emails is high.
- If we want to access the mails offline.

Features of POP3

- In POP3, all the emails are downloaded to the local computer, and once all the emails are downloaded, they are deleted from the server.
- Downloaded emails can be accessed offline also.
- Emails are not synchronized between different devices, which means if we set up our email using our mobile phone with POP3, those emails will be downloaded completely on your mobile phone, and cant be accessed from other devices.

Difference table between IMAP and POP3

Feature	IMAP	POP3
Stands for	IMAP stands for Internet Message Access Protocol.	It stands for Post Office Protocol3.
Used for	IMAP is an advanced protocol that allows a user to check all the folders on the mail server and is used to retrieve the mails.	POP is a simple protocol compared to IMAP and used only for downloading the messages from our inbox to the local computer.
Port number	It listens on port number 143, and IMAPDS(IMAP with SSL) Listens on port 993.	It listens on port number 110, and POP3DS(POP3 with SSL) listens on port 995.
Accessibility	Using IMAP, the messages can be accessed using different devices.	Using POP3, mail can only be accessed using a single device at a time.

Readability	We can partially read the message before finishing the download.	We can only read the message once it is downloaded.
Change	In IMAP, a mail can be updated using email software or a web interface.	In POP3, mail can be updated using the local email software.
Update	IMAP allows the user to create, delete, or update the mailboxes on the mail server and also allows to create a hierarchy of mailboxes in the folder.	POP3 does not allow the user to create, delete, or update the mailboxes on the mail server.
Mail organization	It allows the user to organize the mails on the server.	It does not allow to organize the mails on the server.
Download	In IMAP, the message header is previewed before downloading a message.	Using POP3, all the messages can be downloaded at once.
Email storage	Emails are stored on a single device once they are downloaded and removed from the server.	Emails are stored on the server and synced & can be accessed using multiple devices.

Conclusion

As per the above discussion, we can conclude that IMAP is more powerful, and it is best to use it if we want to access our emails using multiple devices, for example, using smartphones and computers. On the other hand, POP3 is suitable if we access mails using one device only, with a large number of emails, and want to access those emails offline.

Multipurpose Internet Mail Extension (MIME) Protocol:

Multipurpose Internet Mail Extension (MIME) is a standard which was proposed by Bell Communications in 1991 in order to expand limited capabilities of email.
MIME is a kind of *add on or a supplementary protocol* which allows non-ASCII data to be sent through SMTP. It allows the users to exchange different kinds of data files on the Internet: audio, video, images, application programs as well.

Why do we need MIME?

Limitations of Simple Mail Transfer Protocol (SMTP):

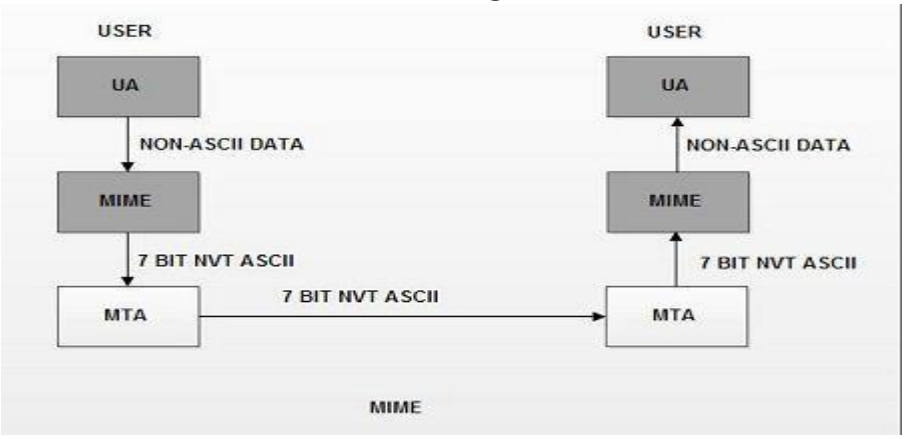
1. SMTP has a very simple structure
2. It's simplicity however comes with a price as it only send messages in NVT 7-bit ASCII format.
3. It cannot be used for languages that do not support 7-bit ASCII format such as- French, German, Russian, Chinese and Japanese, etc. so it cannot be transmitted using SMTP. So, in order *to make SMTP more broad we use MIME*.

4. It cannot be used to send binary files or video or audio data.

Purpose and Functionality of MIME –

Growing demand for Email Message as people also want to express in terms of Multimedia. So, MIME another email application is introduced as it is not restricted to textual data.

MIME *transforms non-ASCII data* at sender side to NVT 7-bit data and delivers it to the client SMTP. The message at receiver side is transferred back to the original data. As well as we can send video and audio data using MIME as it transfers them also in 7-bit ASCII data.



Features of MIME –

1. It is able to send multiple attachments with a single message.
2. Unlimited message length.
3. Binary attachments (executables, images, audio, or video files) which may be divided if needed.
4. MIME provided support for varying content types and multi-part messages.

Working of MIME –

Suppose a user wants to send an email through user agent and it is in a non-ASCII format so there is a MIME protocol which converts it into 7-bit NVT ASCII format. Message is transferred through e-mail system to the other side in 7-bit format now MIME protocol again converts it back into non-ASCII code and now the user agent of receiver side reads it and then information is finally read by the receiver. MIME header is basically inserted at the beginning of any e-mail transfer.

MIME with SMTP and POP –

SMTP transfers the mail being a message transfer agent from senders side to the mailbox of receiver side and stores it and MIME header is added to the original header and provides additional information. while POP being the message access agent organizes the mails from the mail server to the receivers computer. POP allows user agent to connect with the message transfer agent.

MIME Header:

It is added to the original e-mail header section to define transformation. There are *five headers* which we add to the original header:

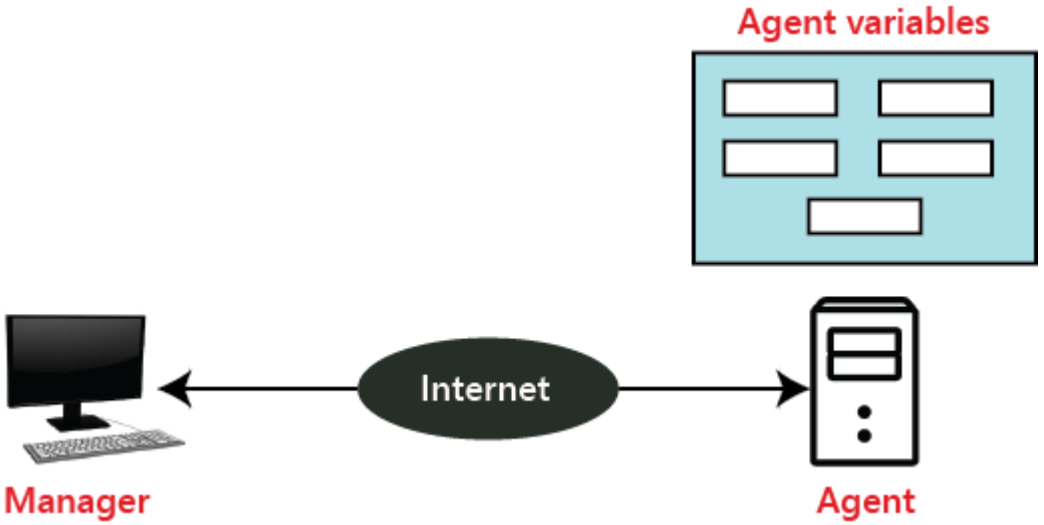
1. **MIME Version** – Defines version of MIME protocol. It must have the parameter *Value 1.0*, which indicates that message is formatted using MIME.

2. **Content Type –** Type of data used in the body of message. They are of different types like text data (plain, HTML), audio content or video content.
3. **Content Type Encoding –** It defines the method used for encoding the message. Like 7-bit encoding, 8-bit encoding, etc.
4. **Content Id –** It is used for uniquely identifying the message.
5. **Content description –** It defines whether the body is actually image, video or audio.

SNMP (Simple Network Management Protocol)

SNMP was defined by **IETF (Internet Engineering Task Force)**. It is used to manage the network. It is an internet standard protocol that monitors devices in IP networks and collects and organizes the information (data) of these devices. SNMP is supported by most network devices such as the hub, switch, router, bridge, server, modem, and printer, etc.

The concept of SNMP is based on the manager and agent. A manager is like a host that controls a group of agents, such as routers.



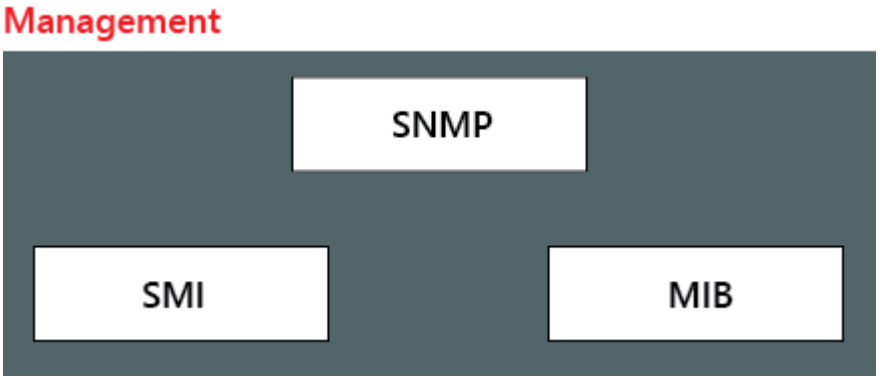
SNMP Manager: It is a computer system that monitors network traffic by the SNMP agent, and it queries these agents, takes answers, and controls them.

SNMP Agent: It is a software program that is located in a network element. It collects real-time information from the device and passes this information to the SNMP manager.

Management components

It has two components.

1. SMI
2. MIB



SNMP: It defines the structure of packets that is shared between a manager and an agent.

SMI (Structure of Management Information): SMI is a network management component that defines the standard rules for the naming object and object type (including range and length) and also shows how to encode objects and values.

MIB (Management Information Base): MIB is the second component of the network management. It is virtual information storage where management information is stored.

SNMP basic operation

- **GetRequest:** The GetRequest operation is used by the SNMP manager to derive one or more values from the SNMP agent.
- **GetNextRequest:** The GetNextRequest is similar to the GetRequest operation, but it is used to get the next value from the SNMP agent.
- **SetRequest:** It is used by the manager to set the value of the agent device.
- **Trap:** This command is used by the SNMP agent to send acknowledgment messages to the SNMP manager.
- **GetBulkRequest:** It is used by the SNMP manager to retrieve the large data from the SNMP agent.

Difference between all versions of the SNMP?

Feature	SNMP Version 1	SNMP Version 2	SNMP Version 3
Developed Year	1988	1993	2002
Access Control	It is based on the SNMP community and MIB view.	It is based on the SNMP community and MIB view.	It is based on the SNMP user, group, and MIB view.
Authentication and privacy	SNMP v1 is not secure because anyone can access the network.	SNMPv2 failed to improve on security.	Its primary feature is enhanced security.

Standards	RFC-1155.1157.1212	RFC-1441,1452 RFC-1909.1910 RFC- 1901 to 1908	RFC-1902 to 1908,2271 to 2275
Message Format	There are five messages format in the SNMP version 1 (GetRequest, GetNextRequest, SetRequest, Trap, Response).	Seven messages instead of five (inform-request, get-bulk-request)	Implements SNMP v1 and v2 specifications along with proposed new features
Default/known passwords	Yes	Yes	No
Susceptible to replay attacks	Yes	No	No
Susceptible to injection attacks	Yes	No	No
Susceptible to brute- force attacks	Yes	Yes	No
Susceptible to buffer-overflow attacks	Yes	Yes	No
Susceptible to sniffing of session keys	Yes	No	No

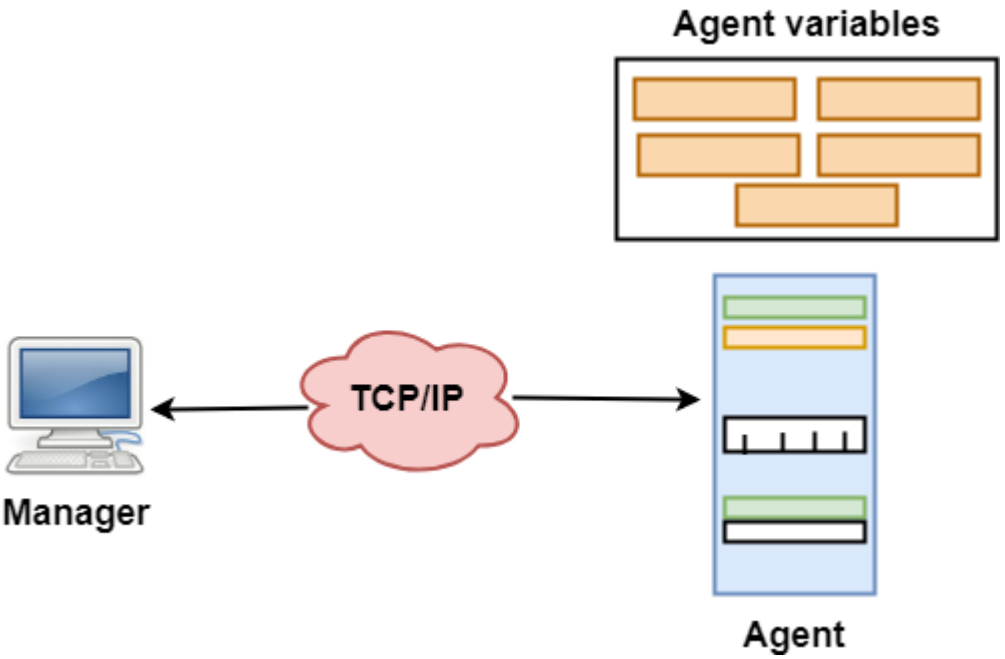
SNMP Port

The SNMP sends instructions and messages using both port 161 and port 162. The SNMP agent uses the port 161, and the SNMP manager uses the port 162.

SNMP

- SNMP stands for **Simple Network Management Protocol**.
- SNMP is a framework used for managing devices on the internet.
- It provides a set of operations for monitoring and managing the internet.

SNMP Concept



- SNMP has two components Manager and agent.
- The manager is a host that controls and monitors a set of agents such as routers.
- It is an application layer protocol in which a few manager stations can handle a set of agents.
- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.
- It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.

Managers & Agents

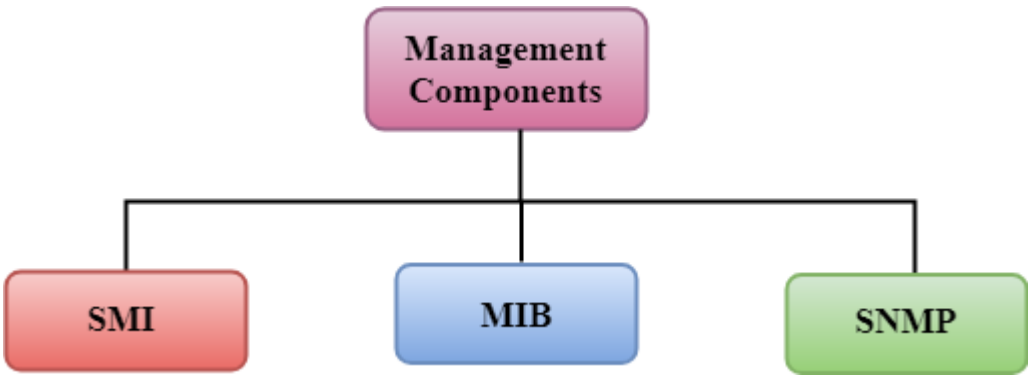
- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

Management with SNMP has three basic ideas:

- A manager checks the agent by requesting the information that reflects the behavior of the agent.
- A manager also forces the agent to perform a certain function by resetting values in the agent database.
- An agent also contributes to the management process by warning the manager regarding an unusual condition.

Management Components

- Management is not achieved only through the SNMP protocol but also the use of other protocols that can cooperate with the SNMP protocol. Management is achieved through the use of the other two protocols: SMI (Structure of management information) and MIB(management information base).
- Management is a combination of SMI, MIB, and SNMP. All these three protocols such as abstract syntax notation 1 (ASN.1) and basic encoding rules (BER).

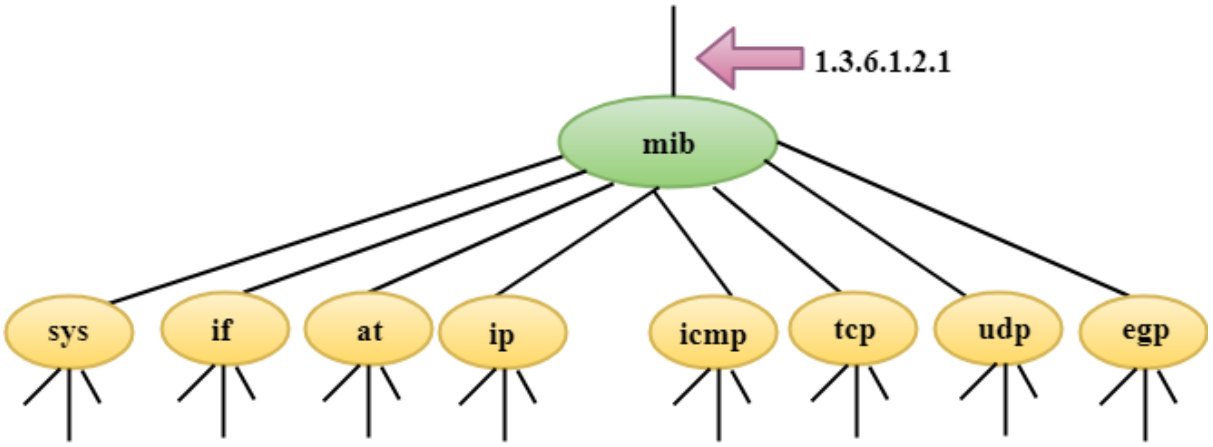


SMI

The SMI (Structure of management information) is a component used in network management. Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.

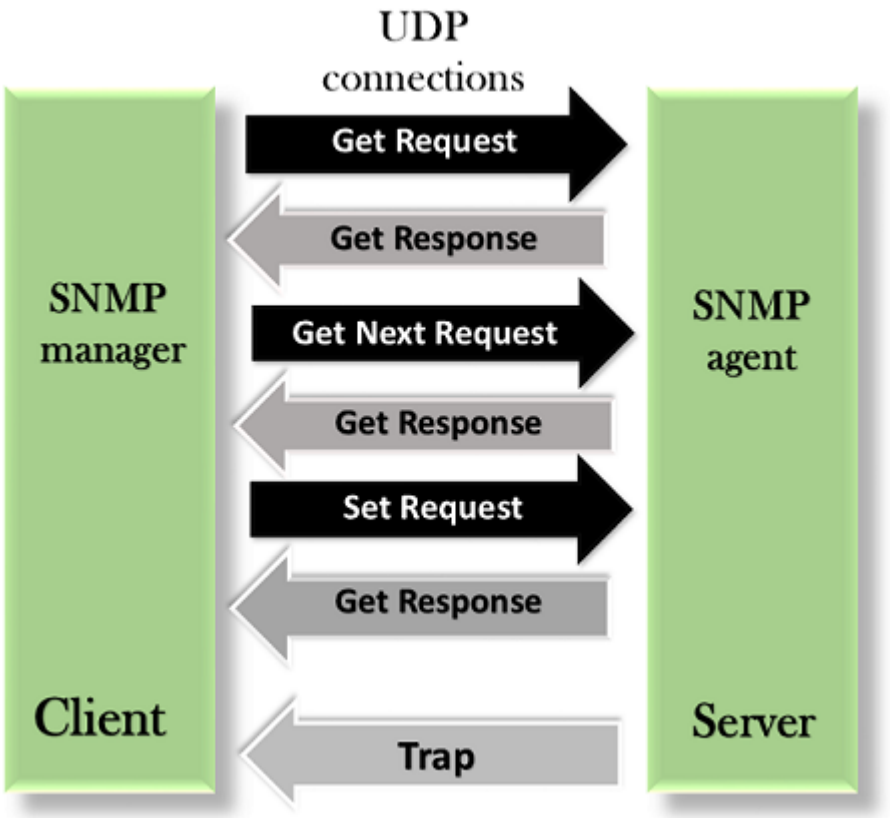
MIB

- The MIB (Management information base) is a second component for the network management.
- Each agent has its own MIB, which is a collection of all the objects that the manager can manage. MIB is categorized into eight groups: system, interface, address translation, ip, icmp, tcp, udp, and egp. These groups are under the mib object.



SNMP

SNMP defines five types of messages: GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap.



GetRequest: The GetRequest message is sent from a manager (client) to the agent (server) to retrieve the value of a variable.

GetNextRequest: The GetNextRequest message is sent from the manager to agent to retrieve the value of a variable. This type of message is used to retrieve the values of the entries in a table. If the manager does not know the indexes of the entries, then it will not be able to retrieve the values. In such situations, GetNextRequest message is used to define an object.

GetResponse: The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message. This message contains the value of a variable requested by the manager.

SetRequest: The SetRequest message is sent from a manager to the agent to set a value in a variable.

Trap: The Trap message is sent from an agent to the manager to report an event. For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting.

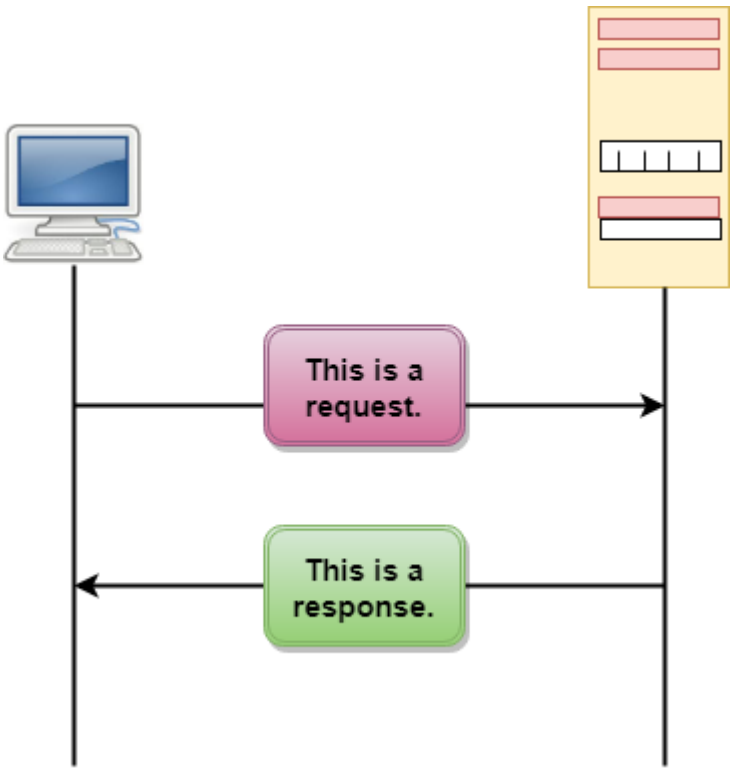
HTTP

- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

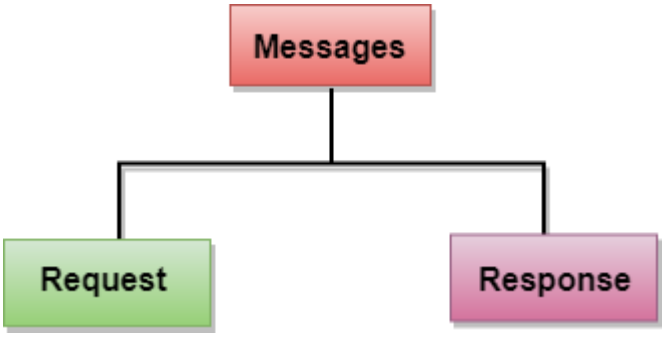
HTTP Transactions



The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

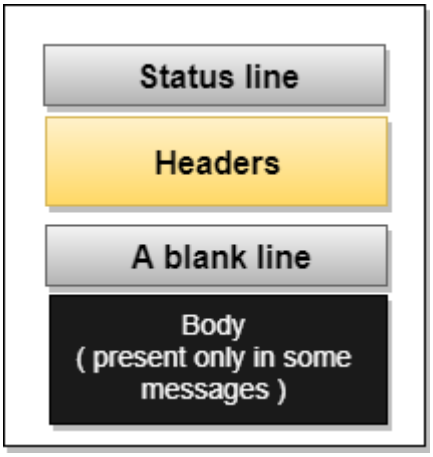
Messages

HTTP messages are of two types: request and response. Both the message types follow the same message format.



Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.

Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



Uniform Resource Locator (URL)

- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
- The URL defines four parts: method, host computer, port, and path.

- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.

- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
- **Path:** Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

HTTP vs HTTPS

What is HTTP?

An HTTP stands for Hypertext Transfer Protocol. The HTTP protocol provides communication between different communication systems. When the user makes an HTTP request on the browser, then the webserver sends the requested data to the user in the form of web pages. In short, we can say that the HTTP protocol allows us to transfer the data from the server to the client.

An HTTP is an application layer protocol that comes above the TCP layer. It has provided some standard rules to the web browsers and servers, which they can use to communicate with each other.

An HTTP is a stateless protocol as each transaction is executed separately without having any knowledge of the previous transactions, which means that once the transaction is completed between the web browser and the server, the connection gets lost.

What is HTTPS?

The full form of HTTPS is Hypertext Transfer Protocol Secure. The HTTP protocol does not provide the security of the data, while HTTP ensures the security of the data. Therefore, we can say that HTTPS is a secure version of the HTTP protocol. This protocol allows transferring the data in an encrypted form. The use of HTTPS protocol is mainly required where we need to enter the bank account details. The HTTPS protocol is mainly used where we require to enter the login credentials. In modern browsers such as chrome, both the protocols, i.e., HTTP and HTTPS, are marked differently. To provide encryption, HTTPS uses an encryption protocol known as Transport Layer Security, and officially, it is referred to as a Secure Sockets Layer (SSL). This protocol uses a mechanism known as asymmetric public key infrastructure, and it uses two different keys which are given below:

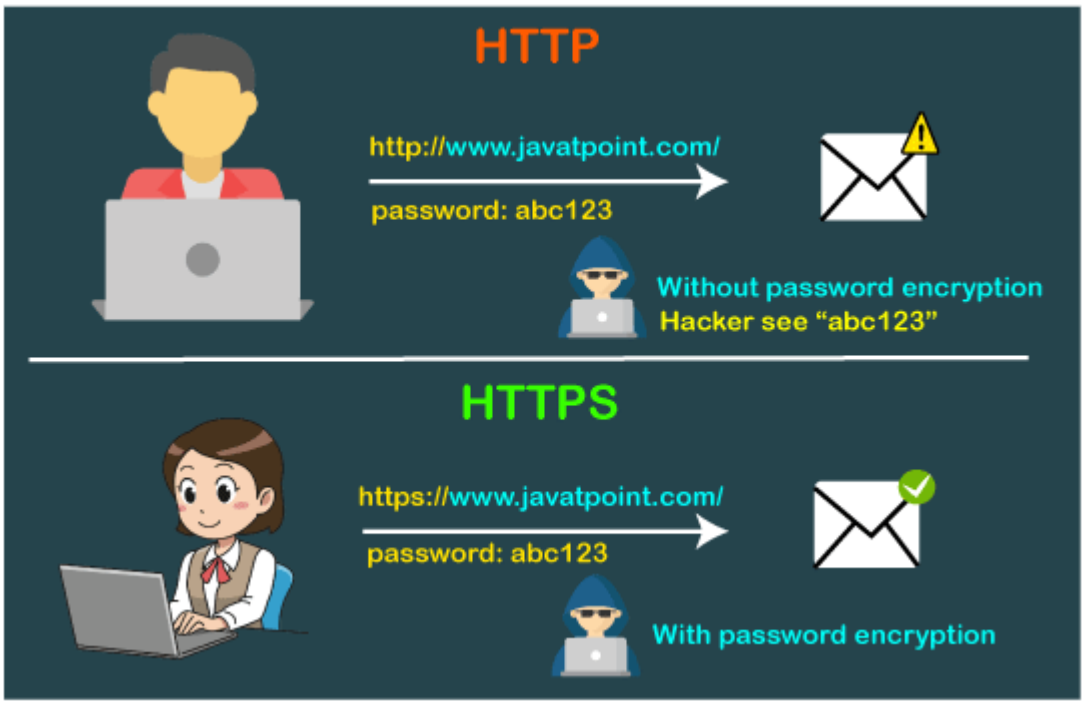
- Private key: This key is available on the web server, which is managed by the owner of a website.

  It decrypts the information which is encrypted by the public key.
- Public key: This key is available to everyone. It converts the data into an encrypted form.

Main difference between the HTTP and HTTPS

The major difference between the HTTP and HTTPS is the SSL certificate. The HTTPS protocol is an extended version of the HTTP protocol with an additional feature of security.

This additional feature of security is very important for those websites which transmit sensitive data such as credit card information.



The HTTPS protocol is secured due to the SSL protocol. The SSL protocol encrypts the data which the client transmits to the server. If someone tries to steal the information which is being communicated between the client and the server, then he/she would not be able to understand due to the encryption. This is the main difference between the HTTP and HTTPS that the HTTP does not contain SSL, whereas the HTTPS contains SSL that provides secure communication between the client and the server.

Which is better, HTTP or HTTPS?

Till now, we read that the HTTPS is better than HTTP because it provides security. Sometimes our website does not contain an e-commerce page that requires sensitive data; in that case, we can switch to the HTTP protocol. Despite the security, HTTPS also provides SEO. So, we do need to put more effort into boosting our SEO.

HTTP vs HTTPS performance

The speed of HTTP is faster than the HTTPS as the HTTPS contains SSL protocol, while HTTPS does not contain an SSL protocol. This additional feature of SSL in HTTPS makes the page loading slower.

Differences between HTTP and HTTPS

The following are the differences between the HTTP and HTTPS:

- **Protocol**

The HTTP protocol stands for Hypertext Transfer Protocol, whereas the HTTPS stands for Hypertext Transfer Protocol Secure.

- **Security**

The HTTP protocol is not secure protocol as it does not contain SSL (Secure Sockets Layer), which means that the data can be stolen when the data is transmitted from the client to the server. Whereas, the HTTPS protocol contains the SSL certificate that converts the data into an encrypted form, so no data can be stolen in this case as outsiders do not understand the encrypted text.

- **Port numbers**

The HTTP transmits the data over port number 80, whereas the HTTPS transmits the data over 443 port number. Under the documentation issued by Tim Berners-Lee, he stated that "if the port number is not specified, then it will be considered as HTTP".

- **Layers**

The HTTP protocol works on the application layer while the HTTPS protocol works on the transport layer. As we know that the responsibility of the transport layer is to move the data from the client to the server, and data security is a major concern. HTTPS operates in the transport layer, so it is wrapped with a security layer.

- **SSL Certificates**

When we want our websites to have an HTTPS protocol, then we need to install the signed SSL certificate. The SSL certificates can be available for both free and paid service. The service can be chosen based on business needs.

The HTTP does not contain any SSL certificates, so it does not decrypt the data, and the data is sent in the form of plain text.

- **SEO Advantages**

The SEO advantages are provided to those websites that use HTTPS as GOOGLE gives the preferences to those websites that use HTTPS rather than the websites that use HTTP.

- **Online Transactions**

If we are running an online business, then it becomes necessary to have HTTPS. If we do not use the HTTPS in an online business, then the customers would not purchase as they are scared that their data can be stolen by the outsiders.

Let's understand the differences in a tabular form.

HTTP	HTTPS
The full form of HTTP is the Hypertext Transfer Protocol.	The full form of HTTPS is Hypertext Transfer Protocol Secure.
It is written in the address bar as http://.	It is written in the address bar as https://.
The HTTP transmits the data over port number 80.	The HTTPS transmits the data over port number 443.
It is unsecured as the plain text is sent, which can be accessible by the hackers.	It is secure as it sends the encrypted data which hackers cannot understand.
It is mainly used for those websites that provide information like blog writing.	It is a secure protocol, so it is used for those websites that require to transmit the bank account details or credit card numbers.
It is an application layer protocol.	It is a transport layer protocol.
It does not use SSL.	It uses SSL that provides the encryption of the data.
Google does not give the preference to the HTTP websites.	Google gives preferences to the HTTPS as HTTPS websites are secure websites.
The page loading speed is fast.	The page loading speed is slow as compared to HTTP because of the additional feature that it supports, i.e., security.

What is HTTP (Hypertext Transfer Protocol)?

What is http: HTTP full form *HyperText Transfer Protocol* used mainly to access data on the World Wide Web. HTTP is a Server and Client communication Protocol, which is primarily set of rules for formatting and transferring webpage data (text, images, video and Multimedia files) over the world wide web. It is the Protocol used to create communication between Web Servers and Web Users. HTTP is an application layer Protocol that works on the top of the TCP/IP suite of Protocols.

HTTP protocol uses server and client model. It acts as a request-response protocol. For Example, A client who uses a web browser and a server is a Web host that hosts the website. Whenever a client transmits a request to the Website server, HTTP protocol proceeds that request and creates a connection between client and server through TCP. After that, HTTP sends a request to the server, which picks up the requested data, and HTTP sends the response back to the client. Let's look into the depth of how these requests work.

HTTP protocol functions as a combination of FTP and SMTP. It is similar to FTP because it transfers files and uses the services of TCP. However, it is much simpler than FTP because it

uses only one TCP connection. There is no separate control connection, only data transferred between the client and the server.

The HTTP protocol is like SMTP protocol because the data transferred between the client and the server look like SMTP messages. Besides, MIME-like headers control the format of the messages. However, HTTP differs from SMTP in how the client's messages sent to the server and from the server to the client. Unlike SMTP, the HTTP messages not destined to be read by humans; they are read and interpreted by the HTTP server and HTTP client (browser). SMTP messages are stored and forwarded, but HTTP messages are delivered immediately.

The idea of the HTTP protocol is very simple. A client sends a request, which looks like mail, to the server. The server sends the response, which looks like a mail reply, to the client. The request and response messages carry data in the form of a letter with a MIME-like format.

The commands from the client to the server embedded in a letter-like request message. The contents of the requested file or other information embedded in a letter-like response message.

Features of HTTP Protocol

The features of the http protocol are as follows:

- **Http is Connectionless**: The http client, i.e., the web browser, makes an http request and waits for the server to respond. Now, it is the task of the server to process the request made by the client. So after processing, the server gives the response to the client. After receiving the response, the client disconnects the connection.
- **Http is media independent**: Here, media-independent means that any data can send. Also, we have to mention the content type as per the client's requirement and the server.
- **Http is stateless**: http is a stateless protocol. Only during the current request, the client and the server know about each other and when the connection disconnects, both client and the server forgets about each other. Due to this nature, both the client and the server do not retain the information between the different requests processed.

Basic Architecture Client/Server

As we know, it is a client/server-based architecture. So, it makes use of a request/response protocol. In this, web browsers, search engines act as the client of the system and the web server acts as the server of the system.

Http Client: The http client requests in the form of a request method. Which is followed by the message body over a TCP/IP connection.

Http Server: The client's request is responded to by the server in the form of a status line followed by the other necessary information with the message body.

HTTP Request Methods

Http Protocol can use two case sensitive request-response Methods between client/server such as GET and POST used to handle form submissions.

GET Method

A GET Requests data from a specified resource using a given URI to retrieve data.

POST Method

A POST request Submits data to process to a specified resource to the server.

Note: URLs that start with "http://" are use port 80 by default, and URL with "https://" is secure connection use port 443.

Differences between "GET" and "POST" Methods

"**GET**" appends a limited amount of variable and their values to the URL string because data sent in the header. It is a non-secure connection because variable and their values exposed in the URL.

"**POST**" appends a large amount of data because data sent in the message body. It is a secure connection because variable and their values not exposed in the URL.

What is an HTTP request?

An Http request message consists of a request line, headers and sometimes a body.

An HTTP request is ways that web browsers ask for information to load website pages. HTTP request contains HTTP version type, a URL, HTTP request headers and HTTP body.

HTTP request headers: HTTP request headers include text information saved in key-value pairs, and these contained in every HTTP request.

URL: A client that wants to access a document needs an address. To facilitate the access of documents distributed throughout the world, HTTP protocol uses the concept of locations. The World Wide Web uses a locator called a URL to identify and intertribal data.

URL called as (**Uniform Resource Locator**). A URL is an internet address of any website in common format https://ecomputernotes.com. A URL has three parts: Method: //Host/Path, which used for accessing any file, document or website.

What is an HTTP response?

An HTTP response means when the web client gets the answer back from the webserver. It contains the information that asked for in the HTTP request. The HTTP response includes an HTTP status code, HTTP response headers, and an HTTP body.

What is HTTPS?

HTTPS is a Hypertext Transfer Protocol Secure. It is the secure version of HTTP Protocol. HTTPS means a secure layer between client and server. HTTPS encrypted our data by Transport Security Layer (TLS). HTTPS is a sign of security. Most of the websites secured with HTTPS.

WWW Defined – What is the World Wide Web (WWW)?

The WWW is the brainchild of Tim Berners Lee a CERN who had the idea of creating an electronic web of research information. The web is currently the fastest growing Internet information system, with new resources being added regularly. The web relies on a set of protocols, conventions and software to operate. The web is a distributed system of delivering linked documents over the Internet.

It is called a distributed system because information can reside on different computers around the world. Yet be easily linked together using hypertext. The web uses hypertext to create links from together using hypertext. The web uses hyperte3xt to create links from one resource to another. A hypertext link is usually displayed by highlighted and underlined text on the page. A hypertext link or hyperlink can also be graphic that acts as a button linking to another resource.

• World Wide Web IS an architectural framework for accessing linked documents called web pages that are spread over thousand of computers all over the world.

• WWW is a set of programs, standards and protocols that allow the text, images, animations, sounds and videos to be stored, accessed and linked together in form of web sites.

• The WWW project was developed at CERN, the European Center for Nuclear Research in 1989.

• It has a unique combination of flexibility, portability, and user-friendly features that distinguishes it from the other services provided by the Internet.

Architecture of WWW

• WWW is basically a distributed client-server service. It this, a client can access the services from a server using a browser.

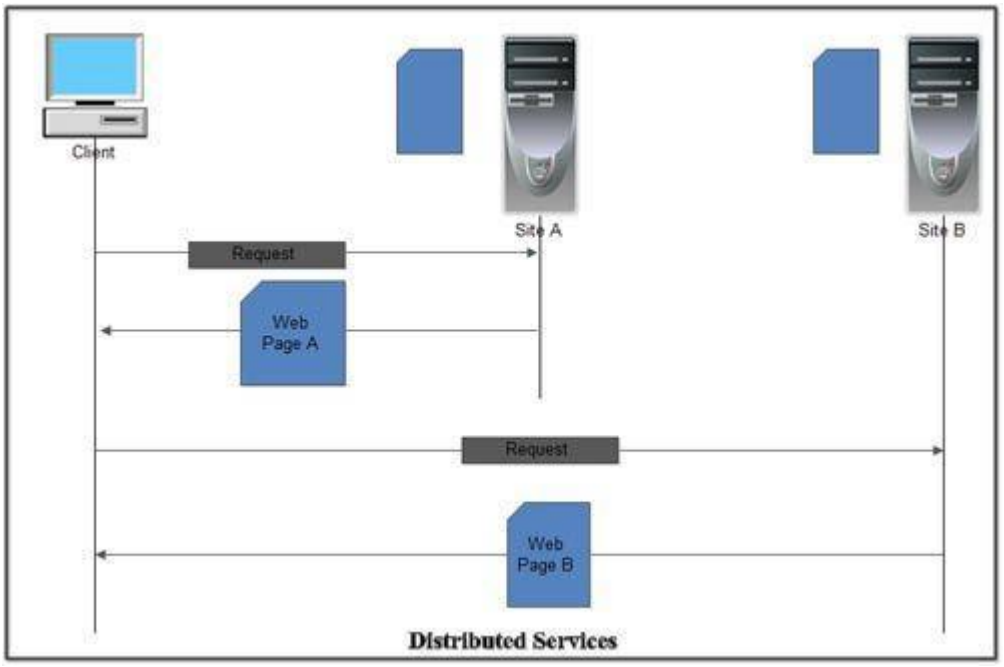
• These services are usually distributed over many locations called sites or websites.

• From the user's point of view web consists of a vast worldwide collection of documents called web pages. These web pages reside on different sites or machines all over the world.

• Each web page can contain link to other pages any where in the world. By clicking on such link user can access another web page.

• This kind of link can be in form of string of text or picture, sound, movie clip etc.

• Such a text or image that enables the user to link to another web page is called hyperlink.



• The string of text that points to another web page is called hypertext. The difference between the normal text and hypertext is that, when you take the mouse pointer over it, it changes into a hand shaped cursor. Such a text is sometime, underlined and blue is colour.

• Hypermedia is enhanced form of a hyperlink which not only links to the other pages or other sections within the same page but can also link with various medium like sound, animation, movie clip etc, Hypermedia is grouping of different media like sound, graphics, animations and text in a single file.

• These hyperlinks are created with the help of specialized language called Hypertext Mark up Language (HTML).

• In order to access these web pages on different sites, each of these pages has a specific address called Uniform Resource Locator (URL).

• Web pages are viewed with a program called a browser.

Three Basic Types of Web Documents

- Static:
  - A static document resides in a file on a web server.
  - The server transfers the same file in response to every client request for the URL of the document.

- Dynamic:
  - Using a program, the server creates a new version of the document in response to each client request for the document's URL.
  - The document can be different for each client request.

- Active:
    - In response to the request from the client the server sends a program to the client.
    - The client runs the program to display and interact with the document.
    - The program can continuously update the display.

Advantages and Disadvantages of Each Document Type

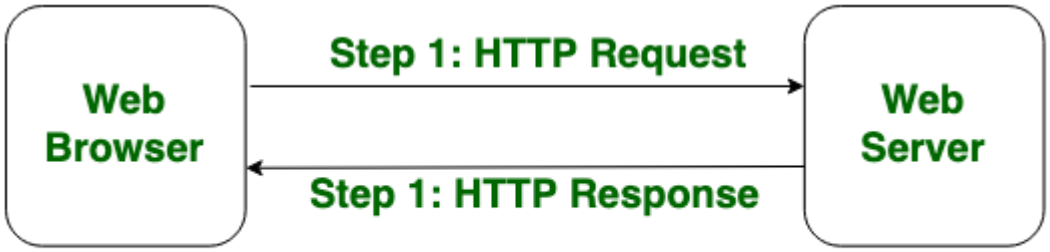
- Static:
    - advantages: simple, reliable, efficient
    - disadvantages: inflexible - it can be inconvenient and costly to change static documents.
- Dynamic:
    - advantages: provides current information
    - disadvantages:
        - document cannot change after reaching the client;
        - creators must have knowledge of programming;
        - greater demand is placed on servers;
        - it tends to take longer for the server to execute the program and transmit the document to the client;
- Active:
    - advantages: can update the browser user's screen continuously
    - disadvantages:
        - cost of creating, testing, and running;
        - security: documents and export information;
        - requires more sophisticated browser and more powerful computer;
        - care must be taken that the programs are portable.

Difference between Static and Dynamic Web Pages

In context of internet surfing there is two party communication i.e between web browser (client) and the web server (server).Now to regulate this communication there are some protocols among which most common is HTTP protocol which allows such communication in which the browser sends an HTTP request to the server, and then the server sends an HTTP response to the browser.

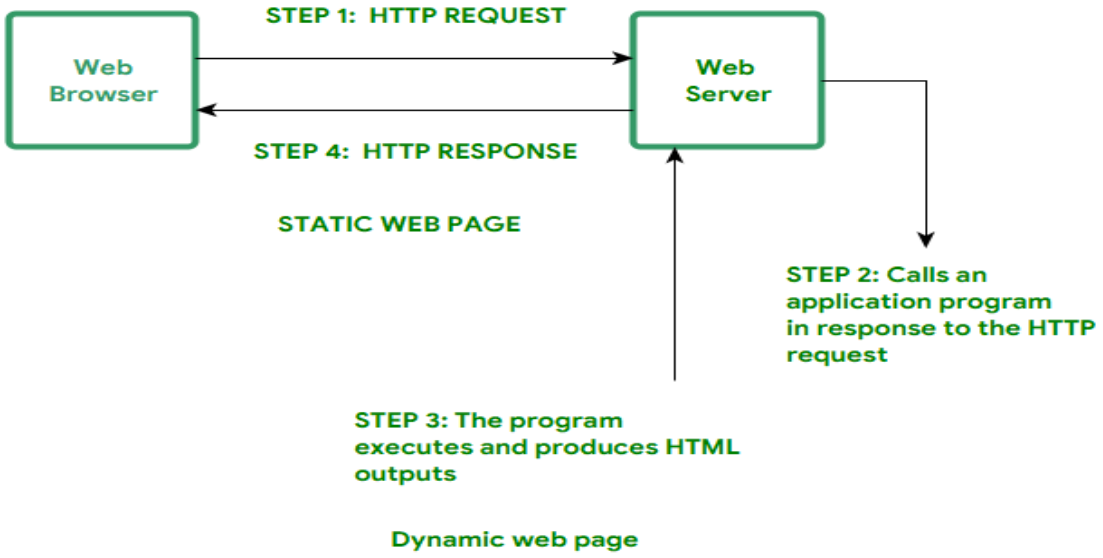
Now on the basis of type of response sent to the browser we can classify this response in two categories one is Static web page and other is Dynamic web page.

Static Web pages:
Static Web pages are very simple. It is written in languages such as HTML, JavaScript, CSS, etc. For static web pages when a server receives a request for a web page, then the server sends the response to the client without doing any additional process. And these web pages are seen through a web browser. In static web pages, Pages will remain the same until someone changes it manually.



Static Web Page

Dynamic Web Pages:
Dynamic Web Pages are written in languages such as CGI, AJAX, ASP, ASP.NET, etc. In dynamic web pages, the Content of pages is different for different visitors. It takes more time to load than the static web page. Dynamic web pages are used where the information is changed frequently, for example, stock prices, weather information, etc.



Difference between Static and Dynamic Web Pages:

SL.NO	Static Web Page	Dynamic Web Page
1.	In static web pages, Pages will remain same until someone changes it manually.	In dynamic web pages, Content of pages are different for different visitors.
2.	Static Web Pages are simple in terms of complexity.	Dynamic web pages are complicated.

3.	In static web pages, Information are change rarely.	In dynamic web page, Information are change frequently.
4.	Static Web Page takes less time for loading than dynamic web page.	Dynamic web page takes more time for loading.
5.	In Static Web Pages, database is not used.	In dynamic web pages, database is used.
6.	Static web pages are written in languages such as: HTML, JavaScript, CSS, etc.	Dynamic web pages are written in languages such as: CGI, AJAX, ASP, ASP.NET, etc.
7.	Static web pages does not contain any application program .	Dynamic web pages contains application program for different services.
8.	Static web pages require less work and cost in designing them.	Dynamic web pages require comparatively more work and cost in designing them.

Following are the important differences between Static Web Page and Dynamic Web Page.

Sr. No.	Key	Static Web Page	Dynamic Web Page
1	Definition	Static web pages are generally simple HTML written pages which serve as response from browser to server in which all the information and data is static in nature and it does not get changed until someone changed it manually.	On other hand Dynamic webpages are the pages written in some more complex language such as ASP.NET in which data is rendered after some interpretation and capacity to produce distinctive content for different calls.
2	Complexity	As mentioned in above point as data in static web pages is static and do not require any interpretation before rendering so static web pages are simple in complexity.	Dynamic web pages on other hand does the interpretation process which make data dynamic in nature and due to which dynamic web pages become complex in complexity as compare to static web pages.

3	Language used	Static web pages are generally written in simpler languages such as HTML, JavaScript, CSS, etc.	On other Dynamic web pages are written in more complex languages such as CGI, AJAX, ASP, ASP.NET, etc.
4	Rendered Data	For static web pages data do not changes until someone changes it manually and hence data is static in nature.	On other hand for Dynamic web page data is first interoperate at server side and due to which it does not remain same on every call and this makes data dynamic in nature..
5	Time	Static web pages due to static data take less time to get load.	While Dynamic web pages due to dynamic data take comparatively more time as compare to static web pages.
6	Database	In Static web pages generally no involvement of database for data redecoration.	On other hand in case of Dynamic web page database is used for data redecoration.

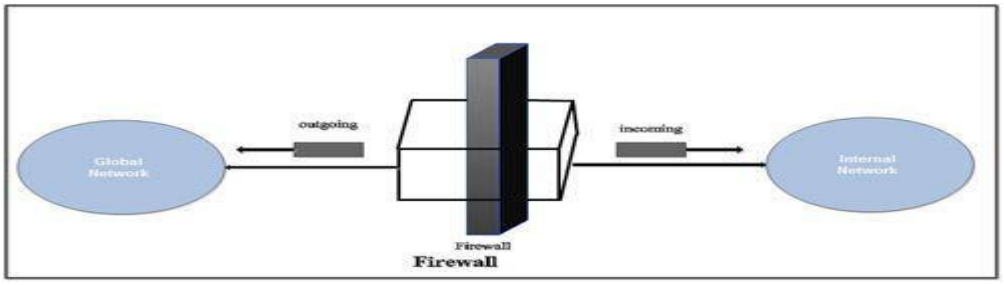
What is Firewall?

A firewall is a device installed between the internet network of an organization and the rest of Internet. When a computer is connected to Internet, it can create many problems for corporate companies. Most companies put a large amount of confidential information online. Such an information should not be disclosed to the unauthorized persons. Second problem is that the virus, worms and other digital pests can breach the security and can destroy the valuable data.

The main purpose of a firewall is to separate a secure area from a less secure area and to control communications between the two. Firewall also controlling inbound and outbound communications on anything from a single machine to an entire network.

On the Other Hand Software firewalls, also sometimes called personal firewalls, are designed to run on a single computer. These are most commonly used on home or small office computers that have broadband access, which tend to be left on all the time.

A software firewall prevents unwanted access to the computer over a network connection by identifying and preventing communication over risky ports. Computers communicate over many different recognized ports, and the firewall will tend to permit these without prompting or alerting the user.



A firewall can serve the following functions:

1- Limit Internet access to e-mail only, so that no other types of information can pass between the intranet and the Internet

2- Control who can *telnet* into your intranet (a method of logging in remotely

3- Limit what other kinds of traffic can pass between your intranet and the Internet .

A firewall can be simple or complex, depending on how specifically you want to control your Internet traffic. A simple firewall might require only that you configure the software in the router that connects your intranet to your ISP. A more complex firewall might be a computer running UNIX and specialized software.

Firewall systems fall into two categories.

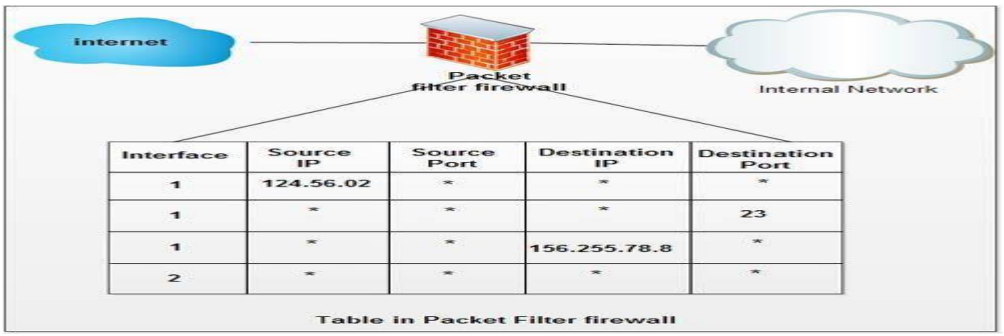
• network-level

• application-level.

Network-Level Firewalls

It can be used as packet filter. These firewalls examine only the headers of each packet of information passing to or from the Internet. The firewall accepts or rejects packets based on the packet's sender, receiver, and port. For example, the firewall might allow e-mail and Web packets to and from any computer on the intranet but allow telnet (remote login) packets to and from only selected computers.

Packet filter firewall maintains a filtering table that decides which packets are to be forwarded or discarded. A packet filter firewall filters at the network or transport layer.



As shown in fig. the packets are filtered according to following specifications :1. Incoming packets from network 124.56.0.2 are block (* means any).
2. Incoming packets destined for any internal TELNET server (port 23) are blocked.

3. Incoming packets for internal host 156.255.7.8.8 are blocked.
4. Outgoing packets destined for an HTTP server (port 80) are blocked i.e. employees of organization are not allowed to browse the internet and cannot send any HTTP request.

Application-Level Firewalls

These firewalls handle packets for each Internet service separately, usually by running a program called a *proxy server,* which accepts e-mail, Web, chat, newsgroup, and other packets from computers on the intranet, strips off the information that identifies the source of the packet, and passes it along to the Internet.

When the replies return, the proxy server passes the replies back to the computer that sent the original message. A proxy server can also log all the packets that pass by, so that you have a record of who has access to your intranet from the Internet, and vice versa.

Types of Firewall Architectures

Conceptually, there are three types of firewalls:

- Packet filter
- Circuit filter
- Application-level filter

The level of protection that any firewall is able to provide in securing a private network when connected to the public Internet is directly related to the architecture(s) of the firewall. The generally available firewalls utilize following technologies for firewall architectures:

- Static packet filter
- Dynamic (state aware) packet filter
- Circuit level gateway
- Application-level gateway (proxy)
- Stateful inspection
- Cut-off proxy
- Air gap.

1. Static Packet Filter

All internet traffic travels in the form of packets. A packet is a quantity of data of limited size. When larger amount of continuous data is sent, it is broken up into numbered packets at the senders end for transmission and reassembled at the receiving end. The entire ·file downloads, Web page retrievals, emails – all these internet communications always occur in **TCP /IP** packets.

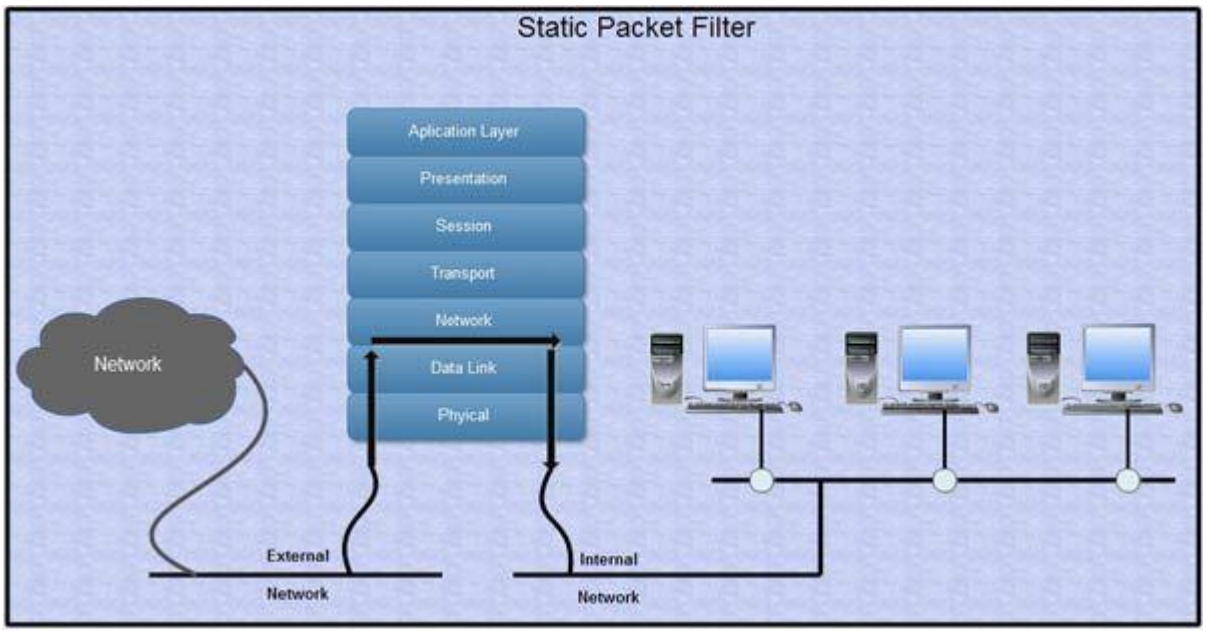
In packet filtering, only the protocol and the address information of each **TCP/*IP*** packet is examined. Its data contents and context (relation to other packets and to the intended application) are ignored. The firewall pays no attention to applications on the host or local network and "knows" nothing about the sources of incoming data.

Filtering consists of examining incoming or outgoing packets and allowing or disallowing their transmission or acceptance on the basis of a set of configurable rules, called policies.

Packet filtering policies may be based upon any of the following:

- Allowing or disallowing packets on the basis of the source IP address (sender)
- Allowing or disallowing packets on the basis of their destination port (service port)
- Allowing or disallowing packets according to protocol.

The packet filtering is usually made up of a series of checks based on the source and destination IP address and ports. A static packet filter operates at the network layer or OSI layer 3.



The decision to accept or deny a packet is based upon an examination of specific fields within the packet's TCP/*IP* headers.

Before forwarding a packet, the firewall compares the IP header and TCP header against a user-defined table – rule base – which contains the rules that dictate whether the firewall should deny or permit packets to pass. The rules are scanned in sequential order until the packet filter finds a specific rule that matches the criteria specified in the packet-filtering rule. If the packet filter does not find a rule that matches the packet, then it imposes a default rule. The default rule explicitly defined in the firewall's table "typically" instructs the firewall to drop a packet that meets none of the other rules.

There are two approaches on the default rule used with the packet filter:

(a) **Ease of use:** Permits all traffic unless it is explicitly denied by prior rule. By default, it is 'allow all' rule.

(b) **Security first:** Deny all traffic unless explicitly allowed by prior rule. By default, it is 'deny all' rule.

Within the static packet filter rules database, the administrator can define rules that determine which packets are accepted and which packets are denied. The IP header information allows the administrator to write rules that can deny or permit packets to and from a specific IP address or range of IP addresses. The TCP header information allows the

administrator to write service specific rules, i.e. allow or deny packets to or from ports related to specific services.

The administrator can write rules that allow certain services such as HTTP from any IP address to view the Web pages on the Web server. The administrator can also write rules that block certain IP address or entire ranges of addresses from using the HTTP service and viewing the web pages on the protected server. In the same respect, the administrator can write rules that allow certain services such as SMTP from a trusted IP address or range of IP addresses to access files on the protected mail server. The administrator could also write rules that block access for certain IP addresses or entire ranges of addresses to access the FTP server.

Problem with Static firewall

A packet filter only examines the information present in the IP header and TCP header; it does not know the difference between real and forged information. If an address is present and meets the packet filter rules along with the other rule criteria, the packet will be allowed to pass.

(i) IP Spoofing: Suppose, the administrator took the precaution to create a rule that instructed the packet filter to drop any incoming packets with unknown source addresses. This packet-filtering rule would make it difficult, but not impossible for a hacker to access at least some trusted servers with IP addresses. The hacker could simply substitute the actual source address on a malicious packet with the source address of a known trusted client. This common form of attack is called *IP address spoofing*. This form of attack is very effective against a packet filter.

(ii) Unaware of Packet Payload: The static packet filter does not examine packet payload, hence a hacker can hide malicious commands or data in unexamined headers. Further, since the static packet filter does not inspect the packet payload, the hacker has the opportunity to hide malicious commands or data within the packet's payload. This attack methodology is often referred to as a covert channel attack and is becoming more popular.

(iii) State unawareness: The static packet filter is not connection-state aware. Simply put, the administrator must configure rules for both sides of the ~conversation to a protected server. To allow access to a protected Web server the administrations create a rule, which allows both the inbound request from the remote client as well as the outbound response from the protected Web server. Of further consideration is that many services such as ITP and e-mail servers in operation today require the use of dynamically allocated ports for responses, so an administrator of a static packet filtering-based firewall has little choice but to open up an entire range of ports with static packet filtering rules.

Advantages

- Low impact on network performance
- Low cost

Disadvantages

- Operates only at network layer therefore it only examines IP and TCP headers
- Unaware of packet payload-offers low level of security.

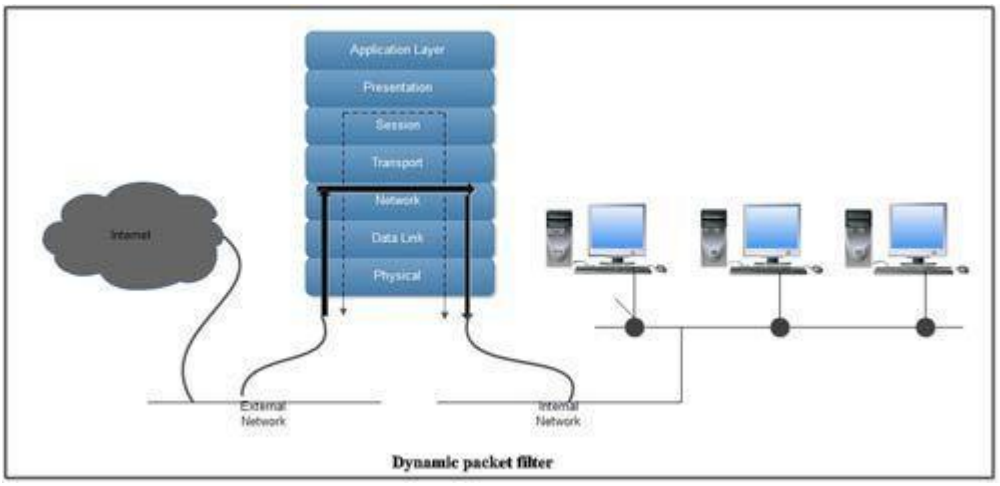
- Lacks state awareness-may require numerous ports be left open to facilitate services that use dynamically allocated ports.
- Susceptible to IP spoofing
- Difficult to create rules (order of precedence).

2. Dynamic (State Aware) Packet filter

A dynamic packet filter firewall is a fourth-generation firewall technology. A dynamic packet filter can monitor the state of active connections and use the information obtained to determine which network packets to allow through the firewall. By recording session information such as IP address and port numbers, a dynamic packet filter combines the best of application level gateways with simple packet filters to make it secure and fast.

It shares many of the inherent limitations of the static packet filter with one important difference: state awareness. This is particularly relevant to UDP packets.

The typical dynamic packet filter, like the static packet filter, operates at the network layer or OSI layer 3. An advanced dynamic packet filter may operate up into the transport layer-OSI layer 4 to collect additional state information.



Dynamic packet filter

Most often, the decision to accept or reject a packet is based upon examination of the packet's IP and protocol headers.

In simplest terms, the typical dynamic packet filter is "aware" of the difference between a new and an established connection. Once a connection is established, it is entered into a table that typically resides in RAM. Subsequent packets are compared to this table in RAM, most often, by software running at the operating system (OS) kernel level. When the packet is found to be an existing connection, it is allowed to pass without any further inspection. By avoiding having to parse the packet filter rule base for each and every packet that enters the firewall and by performing this already established connection table test at the kernel level in RAM, the dynamic packet filter enables a measurable performance increase over a static packet filter.

Advantages

- Low cost

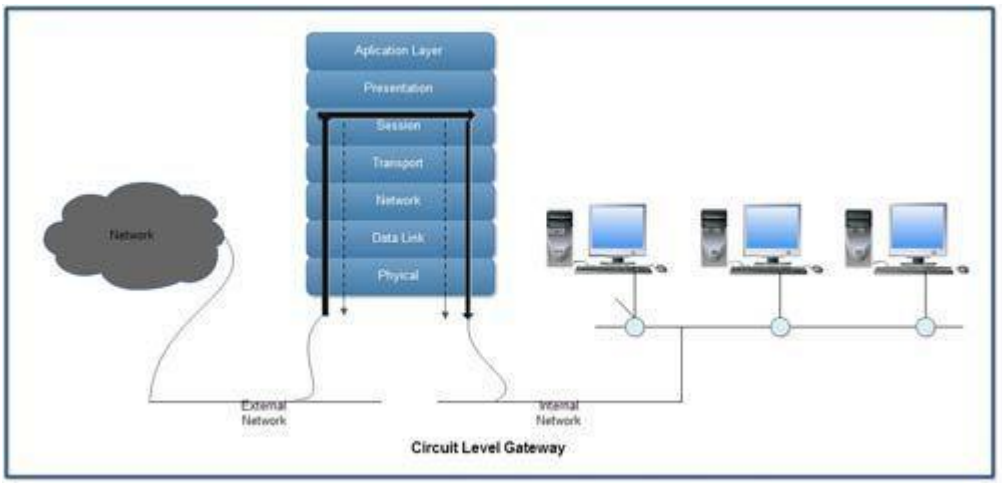
- State awareness provides measurable. performance benefit, scalability and extensibility

Disadvantages

- Operates only at network layer therefore, it only examines IP and TCP headers.
- Unaware of packet payload-offers low level of security
- Susceptible to IP spoofing
- Difficult to create rules (order of precedence)
- Can introduce additional risk if connections
- Can be established without following the RFC-recommended 3 way-handshake.

3. Circuit level Gateway

The circuit level gateway operates at the session layer-OSI layer 5. In many respects, a circuit level gateway is simply an extension of a packet filter in that it typically performs basic packet filter operations and then adds verification of proper handshaking of TCP and the legitimacy of the session information used in establishing the connection. Hence, the circuit level gateway has more data to act upon than a standard static or dynamic packet filter.



Before allowing data to be exchange, the firewall first validates connection. Whether a connection is valid may be based upon:

- Source IP address and/or port
- Destination IP address and/or port
- Application or protocol
- User and password
- Handshaking and sequence numbers.

Most often, the decision to accept or reject a packet is based upon examining the packet's IP header and TCP header.

Similar to a packet filter, before forwarding the packet, a circuit level gateway compares the IP header and TCP header against a user-defined table containing the rules that dictate whether the firewall should deny or permit packets to pass. The circuit level gateway then determines that a requested session is legitimate only if the SYN flags, ACK flags and sequence numbers involved in the TCP handshaking. between the trusted client and the untrusted host are logical.

If the session is valid, the packet filter rules are scanned until it finds one that agrees with the information in a packet's full association. If the packet filter does not find a rule that applies to the packet, then it imposes a default rule. The default rule explicitly defined in the firewall's table "typically" instructs the firewall to drop a packet that meets none of the other rules.

The circuit level gateway is literally a step up from a packet filter in the level of security it provides. Further, like a packet filter operating at a low level in the OSI model; it has little impact on network performance. However, once a circuit level gateway establishes a connection, any application can run across that connection because 'l. circuit level gateway filters packets only at the session and network layers of the OSI model. In other words, a circuit level gateway cannot examine the data content of the packets it relays between a trusted network and an untrusted network. The potential exists to slip harmful packets through a circuit level gateway to a server behind the firewall.

Benefits

- Low to moderate impact on network performance
- Breaks direct connection to server behind firewall
- Higher level of security than a static or dynamic (state aware) packet filter
- Provides services for a wide range of protocols.

Drawbacks

- Shares many of the same negative issues associated with packet filters
- Allows any data to simply pass through the connection
- Only provides for a low to moderate level of security.

4. Application level Gateway

A firewall that filters information at the application level blocks all IP traffic between the private network and the Internet. No IP packets from the clients or servers of the private network are allowed to enter or leave the Internet.

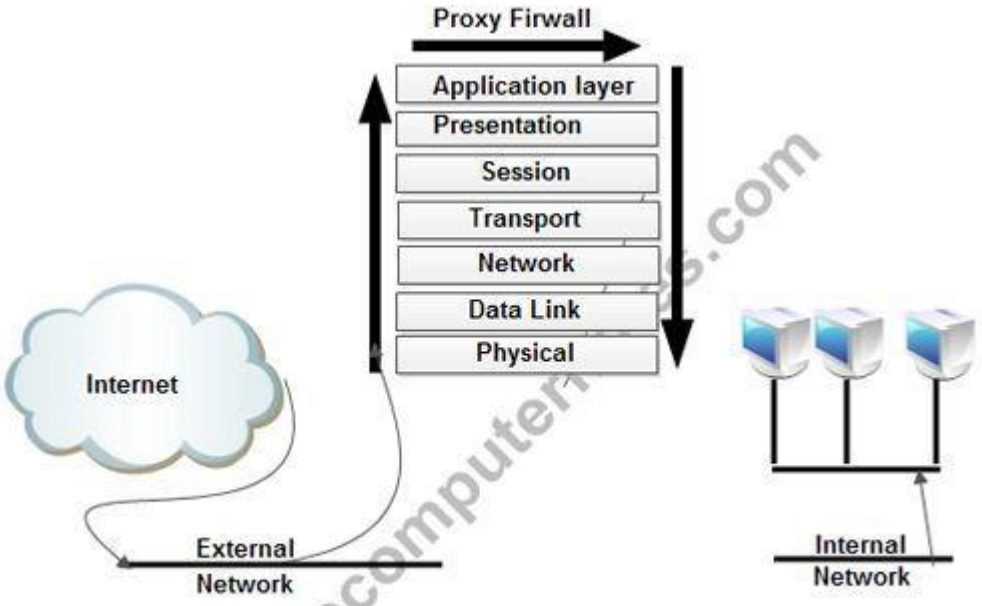
Instead, this type of firewall operates according to what is referred to as the proxy principle. This means that internal clients set up connections to the firewall and communicate with a proxy server. If the firewall decides that the internal client should be allowed to communicate, it sets up a connection with the external server and performs the operation on behalf of the client. This method solves many of the security problems associated with IP.

Each proxy server uses a particular application protocol, such as http-proxy or ftp-proxy. The proxy firewall uses a combination of different proxy servers which allows many different applications to be handled.

In addition to providing the best security, the proxy firewall can be used to fetch and store information from the Internet in a cache memory. The proxy firewall can achieve short response and download times because it "understands" the application programs and can see which URLs are most in demand.

Like a circuit level gateway, an application level gateway intercepts incoming and outgoing packets, acts as a proxy for applications, providing information exchange across the gateway. It also functions as a proxy server, preventing any direct connection between a trusted server or client and an untrusted host. The proxies that an application level gateway runs often differ in two important ways from the circuit level gateway:

- The proxies are application specific
- The proxies examine the entire packet and can filter packets at the application layer of the OSI model.



Application Level Gateway Firewall

Unlike the circuit gateway, the application-level gateway accepts only packets generated by services. They are designed to copy, forward and filter. For example, only an HTTP proxy can copy, forward and filter HTTP traffic. If a network relies only on an application-level gateway, incoming and outgoing packets cannot access services for which there is no proxy. For example, if an application-level gateway ran ITP and HTTP proxies, only packets generated by these services could pass through the firewall. All other services would be blocked.

The application-level gateway runs proxies that examine and filter individual packets, rather than simply copying them and recklessly forwarding them across the gateway. Application specific proxies check each packet that passes through the gateway, verifying the contents of the packet up through the application layer (layer 7) of the OSI model. These proxies can filter on particular information or specific individual commands in the application protocols the proxies are designed to copy, forward and

As an example, an application-level proxy is able to block FTP put commands while permitting FTP get commands.

Current technology application-level gateways are often referred to as strong application proxies. A strong application proxy extends the level of security afforded by the application-level gateway. Instead of copying the entire datagram on behalf of the user, a strong application proxy actually creates a brand */I* new empty datagram inside the firewall. Only those commands and data found acceptable to the strong application proxy are copied from the original datagram outside the firewall to the new datagram inside the firewall. Then, and only then, is this new datagram forwarded to the protected server behind the firewall. By employing this methodology, the strong application proxy can mitigate the risk of an entire class of covert channel attacks.

An application-level gateway fitters information at a higher OSI layer than the common static or dynamic packet filter, and most automatically create any necessary packet filtering rules, usually making them easier to configure then traditional packet filters.

Benefits

- Better logging handling of traffic (because all data between the client and the server is routed through the application proxy it is able to both control the session and provide detailed logging; This ability to log and control all incoming and outgoing traffic is one of the main advantages of application level gateway
- State aware of services (FTP, XII, etc.)
- Packet air gap like architecture, i.e. breaks direct connection to server behind firewall eliminating
- the risk of an entire class of covert channel attacks
- Strong application proxy that inspects protocol header lengths can eliminate an entire class of
- buffer overrun attacks
- Highest level of security.

Weaknesses

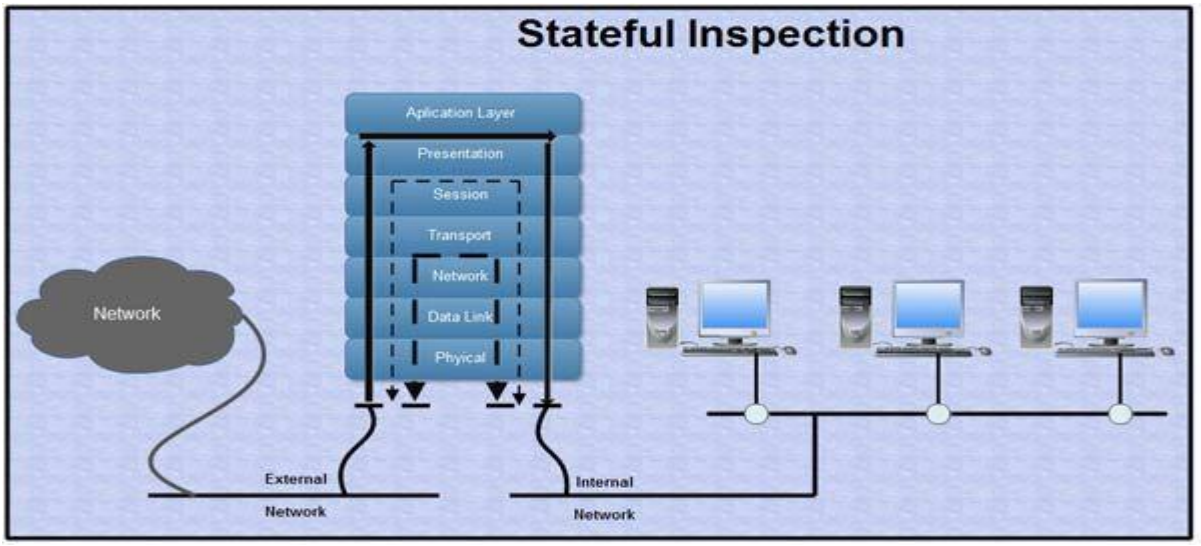
- A poor implementation that relies on the underlying as Inetd daemon will suffer from a severe limitation to the number of allowed connections in today's demanding high simultaneous session environment.
- Complex setup of application firewall needs more and detailed attentions to the applications that use the gateway.

5. Stateful Inspection

Stateful inspection combines the many aspects of dynamic packet filtering, circuit *level* and application-level gateways.

As indicated, stateful inspection can also function as a circuit level gateway, determining whether the packets in a session are appropriate. For example, stateful inspection can verify that inbound SYN and ACK flags and sequence numbers are logical: However, in most

implementations the stateful inspection-based firewall operates *only* as a dynamic packet filter and, dangerously, allows new connections to be established with a single SYN packet.



A unique limitation of one popular stateful inspection implementation is that it does not provide the ability to inspect sequence numbers on outbound packets from users behind the firewall. This leads to a flaw whereby internal users can easily spoof IP address of other internal users to open holes through the associated firewall for inbound connections.

Finally, stateful inspection can mimic an application-level gateway. Stateful inspection can evaluate the contents of each packet up through the application layer and ensure that these contents match the rules in the administrator's network security policy.

Benefits

- Offers the ability to inspect all seven layers of the OSI model and is user configurable to customize specific filter constructs
- Does not break the client server model
- Provides an integral dynamic (stateful) packet filter
- Fast when operated as dynamic packet filter, however many SMP-compliant dynamic packet filters are actually faster.

Weaknesses

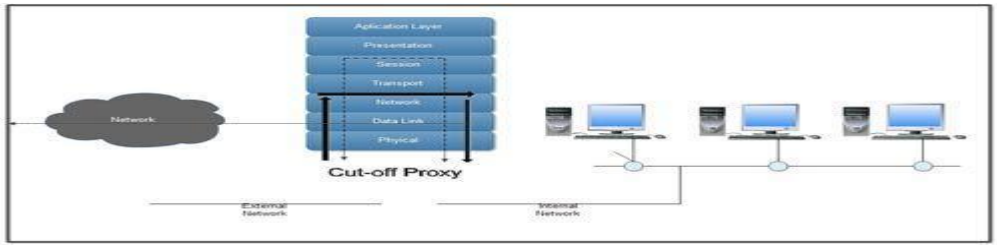
- The single-threaded process of the stateful inspection engine has a dramatic impact on performance, so many users operate the stateful inspection based firewall as nothing more than a dynamic packet filter
- Many believe the failure to break the client server model creates an unacceptable security risk as the hacker has a direct connection to the protected server
- A poor implementation that relies on the underlying OS Inetd demon will suffer from a severe limitation to the number of allowed connections in today's demanding high simultaneous session environment

Low level of security. No stateful inspection-based firewall has achieved higher than a Common Criteria EAL 2. Per the Common Criteria EAL 2 certification documents, EAL 2 products are not intended for use in protecting private networks when connecting to the public Internet.

6. Cutoff Proxy

The cutoff proxy is a hybrid combination of a dynamic (stateful) packet filter and a circuit level proxy. In simplest terms, the cutoff proxy first acts as a circuit level proxy in verifying the RFC-recommended three-way handshake and any required authenticating actions, then switches over to a dynamic packet filtering mode of operation. Hence, it initially works at the session layer-OSI layer 5; then switches to a dynamic packet filter working at the network layer OSI Layer 3. After the connection, authentication process is completed.

The cutoff proxy verifies the RFC-recommended three-way handshake" provides for limited application-based authentication and then switches to a dynamic packet filter mode of operation.



The cutoff proxy is not a traditional circuit level proxy that breaks the client/server model for the duration of the connection. There is a direct connection established between the remote client and the protected server behind the firewall. This is not to say that a cutoff proxy does not provide a useful balance between security and performance. The cutoff proxy offers a level of security equivalent to a traditional circuit level gateway with the added benefit of the performance of a dynamic packet filter.

If the security policy requires authentication of basic services, examination of the three-way handshake and does not require breaking of the client/server model, the cutoff proxy is a good fit. However, administrators must be fully aware and understand that a cutoff proxy clearly is not equivalent to a circuit level proxy as the client/server model is not broken for the duration of the connection.

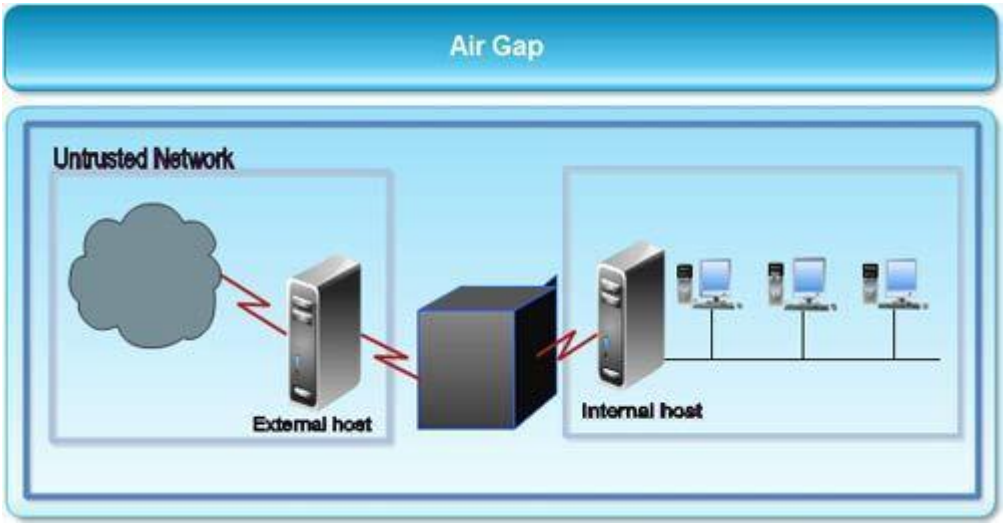
7. Air Gap

The latest entry into the array of available firewall architectures is the air gap. This is an extreme kind of firewall where there is no direct or automated connection between two devices.

Air gap technology provides a physical gap between trusted and untrusted networks, creating an isolated path for moving files between an external server and a company's internal network and systems.

In air gap technology, the external client connection "causes the connection data to be written to an SCSI e-Disk. The internal connection then reads this data from the SCSI e-Disk. By breaking the direct connection between the client to the server and independently writing to and reading from the SCSI e-Disk, a higher level of security is provided and a resultant "air gap."

The basic operation of air gap technology closely resembles that of the application level gateway.



Advantage of Air-gap

- Inside is insulated from outside
- Packets are not "automatically" passed through
- Only explicitly launched services work
- No unexpected traffic via other sockets.

Difference between Packet Filters, Circuit-Level Gateway and Application-Level Gateway

Packet filters	Circut-Level Gateway	Application-Level Gateway
• Simple and least secure firewall mechanism • Many routers provide this function • Passes or rejects packet based on rules • Hard to manage • Easy to make mistake	• More secure than packet filter,but not as secure as application level • Relay TCP connection • Permission granted by port address • No application level checking • Can understand what is in packet	• Most secure approach • Unique program for each application • Good for authentication logging • Not always transparent to users • Used for email,FTP,TELNET,WWW

Bluetooth:

It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon the version. The spreading technique which it uses is FHSS (Frequency hopping spread spectrum).

Bluetooth specification details the entire protocol stack. Bluetooth employs Radio Frequency (RF) for communication. It makes use of **frequency modulation** to generate radio waves in the **ISM** band.

Symbol of Bluetooth

An example of a Bluetooth device

The usage of Bluetooth has widely increased for its special features.

- Bluetooth offers a uniform structure for a wide range of devices to connect and communicate with each other.
- Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can be connected with Bluetooth enabled devices.
- Low power consumption of Bluetooth technology and an offered range of up to ten meters has paved the way for several usage models.
- Bluetooth offers interactive conference by establishing an adhoc network of laptops.
- Bluetooth usage model includes cordless computer, intercom, cordless phone and mobile phones.

Bluetooth is, with the infrared, one of the major wireless technologies developed to achieve WPAN. Bluetooth is a wireless LAN technology used to connect devices of different functions such as telephones, computers (laptop or desktop), notebooks, cameras, printers and so on. Bluetooth is an example of personal area network.
• Bluetooth project was started by SIG (Special Interest Group) formed by four companies IBM, Intel, Nokia and Toshiba for interconnecting computing and communicating devices using short-range, lower-power, inexpensive wireless radios.
• The project was named Bluetooth after the name of Viking king – Harald Blaat and who unified Denmark and Norway in 10th century.

• Nowadays, Bluetooth technology is used for several computer and non computer application:

1. It is used for providing communication between peripheral devices like wireless mouse or keyboard with the computer.
2. It is used by modern healthcare devices to send signals to monitors.
3. It is used by modern communicating devices like mobile phone, PDAs, palmtops etc to transfer data rapidly.
4. It is used for dial up networking. Thus allowing a notebook computer to call via a mobile phone.
5. It is used for cordless telephoning to connect a handset and its local base station.
6. It also allows hands-free voice comml1nication with headset.

7. It also enables a mobile computer to connect to a fixed LAN.
8. It can also be used for file transfer operations from one mobile phone to another.
9. Bluetooth uses omni directional radio waves that can through walls or other non-metal barriers.

Bluetooth devices have a built-in short range radio transmitter. The rate provided is 1Mbps and uses 2.4 GHz bandwidth.

Bluetooth is that when the device is within the scope of a other devices automatically start the transfer information without the user noticing. a small network between the devices is created and the user can accessed as if there were cables.

Bluetooth Architecture

Bluetooth architecture defines two types of networks:

1. Piconet

2. Scattemet

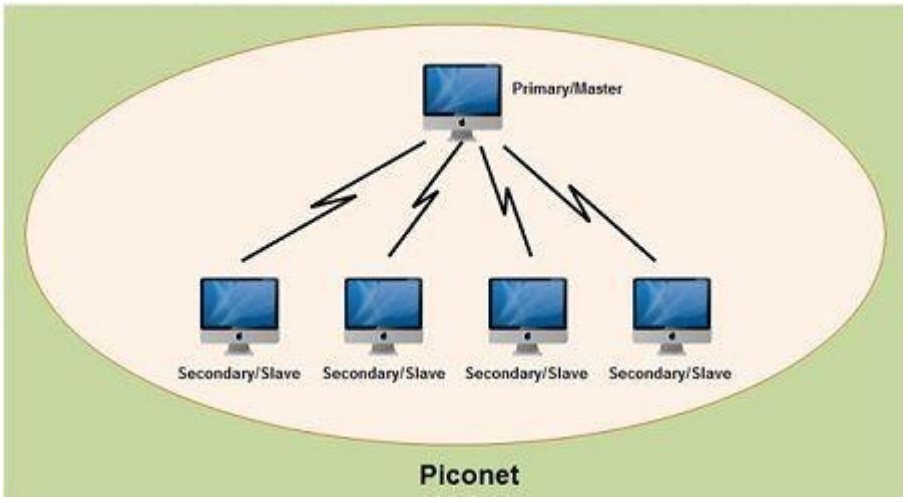
1. Piconet

• Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.

• Thus, piconet can have up to eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.

• There can be only one primary or master station in each piconet.

• The communication between the primary and the secondary can be one-to-one or one-to-many.



• All communication is between master and a slave. Salve-slave communication is not possible.

• In addition to seven active slave station, a piconet can have up to 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.

3. Scatternet

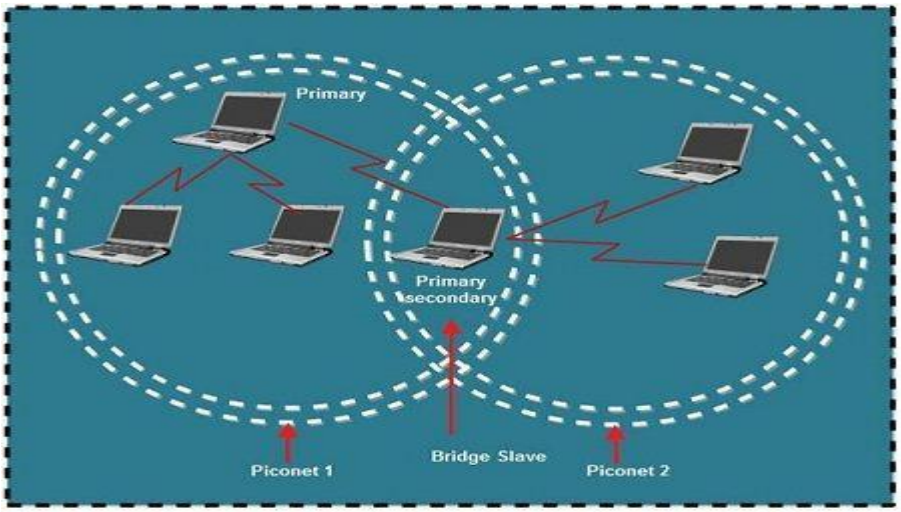
• Scattenet is formed by combining various piconets.

• A slave in one piconet can act as a master or primary in other piconet.

• Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.

• Thus a station can be a member of two piconets.

• A station cannot be a master in two piconets.

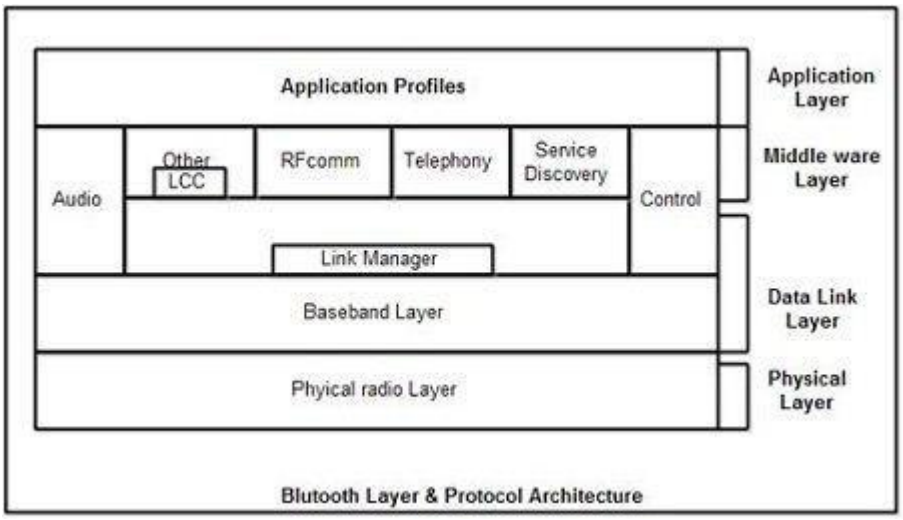


Bluetooth layers and Protocol Stack

• Bluetooth standard has many protocols that are organized into different layers.

• The layer structure of Bluetooth does not follow OS1 model, TCP/IP model or any other known model.

• The different layers and Bluetooth protocol architecture.

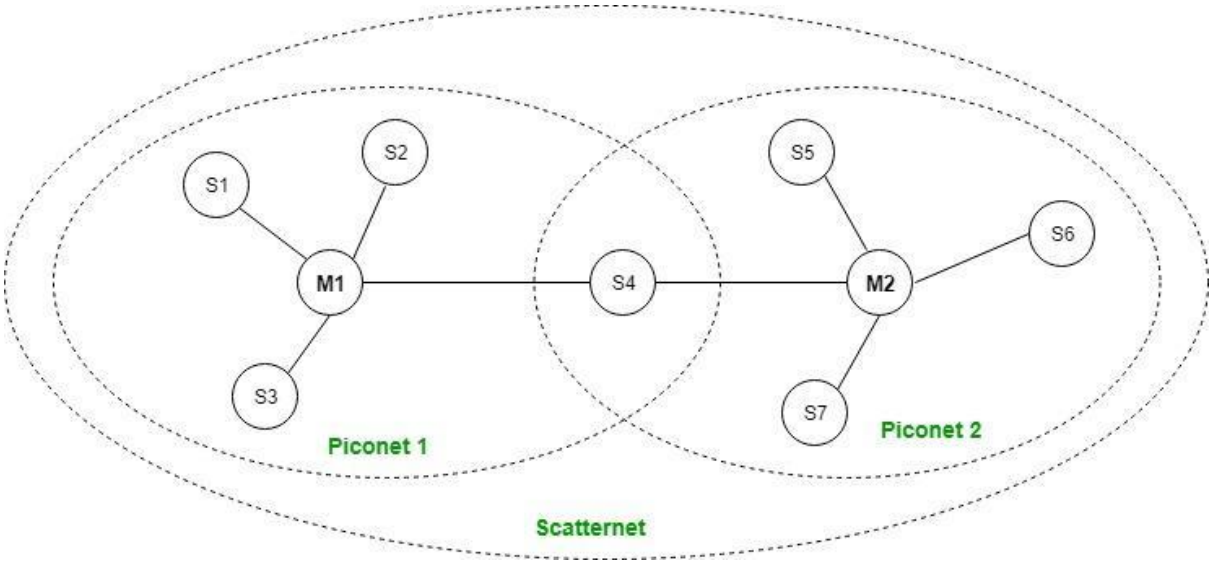


A bluetooth network is called **piconet** and a collection of interconnected piconets is called **scatternet**.

Bluetooth Architecture:
The architecture of bluetooth defines two types of networks:

1. Piconet

2. Scatternet



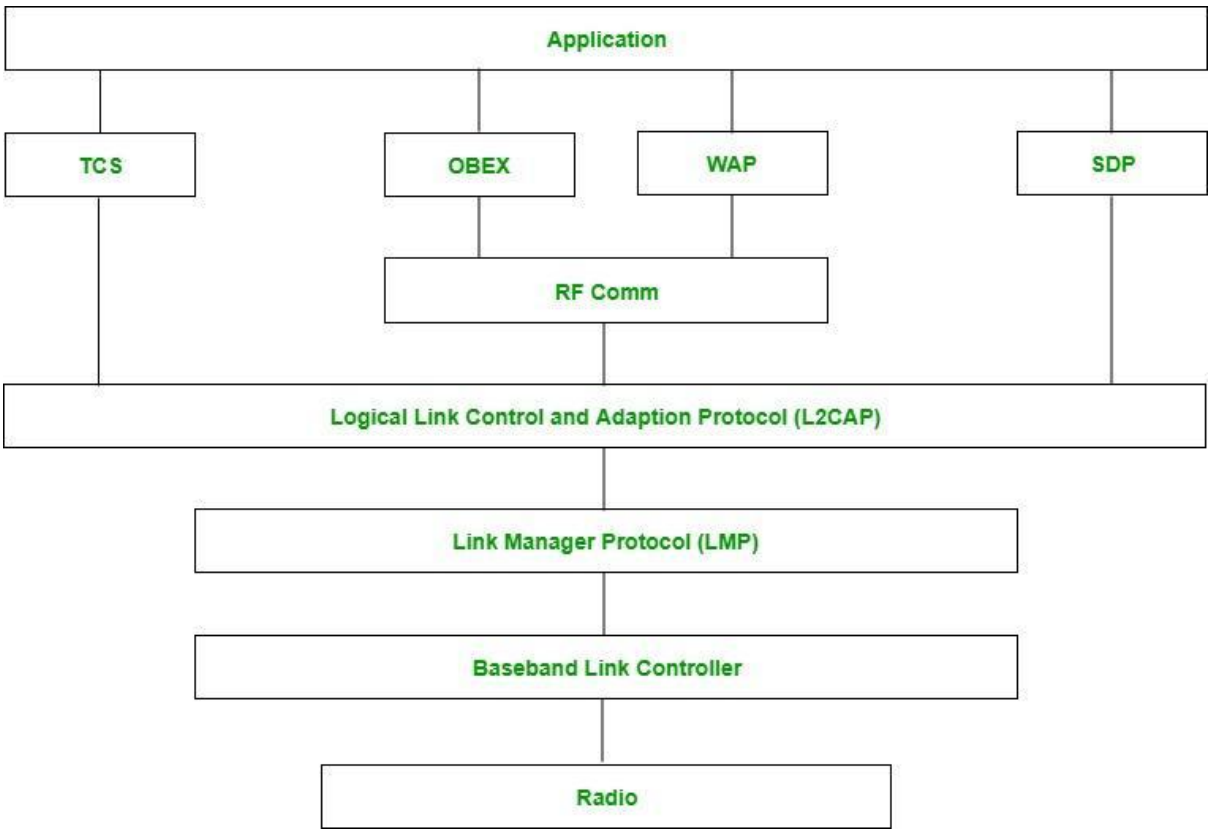
Piconet:

Piconet is a type of bluetooth network that contains **one primary node** called master node and **seven active secondary nodes** called slave nodes. Thus, we can say that there are total of 8 active nodes which are present at a distance of 10 metres. The communication between the primary and secondary node can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also have **255 parked nodes**, these are secondary nodes and cannot take participation in communication unless it get converted to the active state.

Scatternet:

It is formed by using **various piconets**. A slave that is present in one piconet can be act as master or we can say primary in other piconet. This kind of node can receive message from master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave. This type of node is refer as bridge node. A station cannot be master in two piconets.

Bluetooth protocol stack:



1. **Radio (RF) layer:**
   It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of bluetooth transceiver. It defines two types of physical link: connection-less and connection-oriented.

2. **Baseband Link layer:**
   It performs the connection establishment within a piconet.

3. **Link Manager protocol layer:**
   It performs the management of the already established links. It also includes authentication and encryption processes.

4. **Logical Link Control and Adaption protocol layer:**
   It is also known as the heart of the bluetooth protocol stack. It allows the communication between upper and lower layers of the bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs the segmentation and multiplexing.

5. **SDP layer:**
   It is short for Service Discovery Protocol. It allows to discover the services available on another bluetooth enabled device.

6. **RF comm layer:**
   It is short for Radio Frontend Component. It provides serial interface with WAP and OBEX.

7. **OBEX:**
   It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.

8. **WAP:**
   It is short for Wireless Access Protocol. It is used for internet access.

9. **TCS:**
   It is short for Telephony Control Protocol. It provides telephony service.

10. **Application layer:**
    It enables the user to interact with the application.

Spectrum

Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ, using a spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec. the 2.4 GHZ ISM band is available and unlicensed in most countries.

Range

Bluetooth operating range depends on the device Class 3 radios have a range of up to 1 meter or 3 feet Class 2 radios are most commonly found in mobile devices have a range of 10 meters or 30 feet Class 1 radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.

Data rate

Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.

Advantages:

- Low cost.
- Easy to use.
- It can also penetrate through walls.
- It creates an adhoc connection immediately without any wires.
- It is used for voice and data transfer.

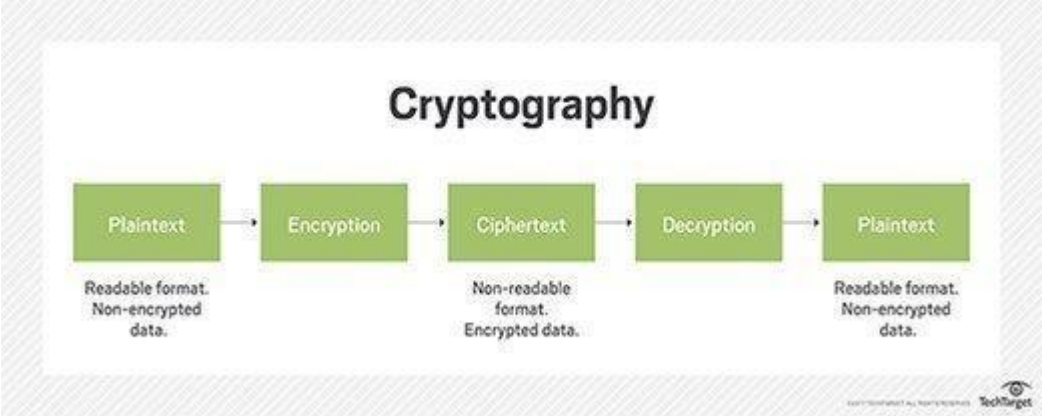
Disadvantages:

- It can be hacked and hence, less secure.
- It has slow data transfer rate: 3 Mbps.
- It has small range: 10 meters.

Cryptography and its Types:

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process

it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.
In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.



Techniques used For Cryptography:

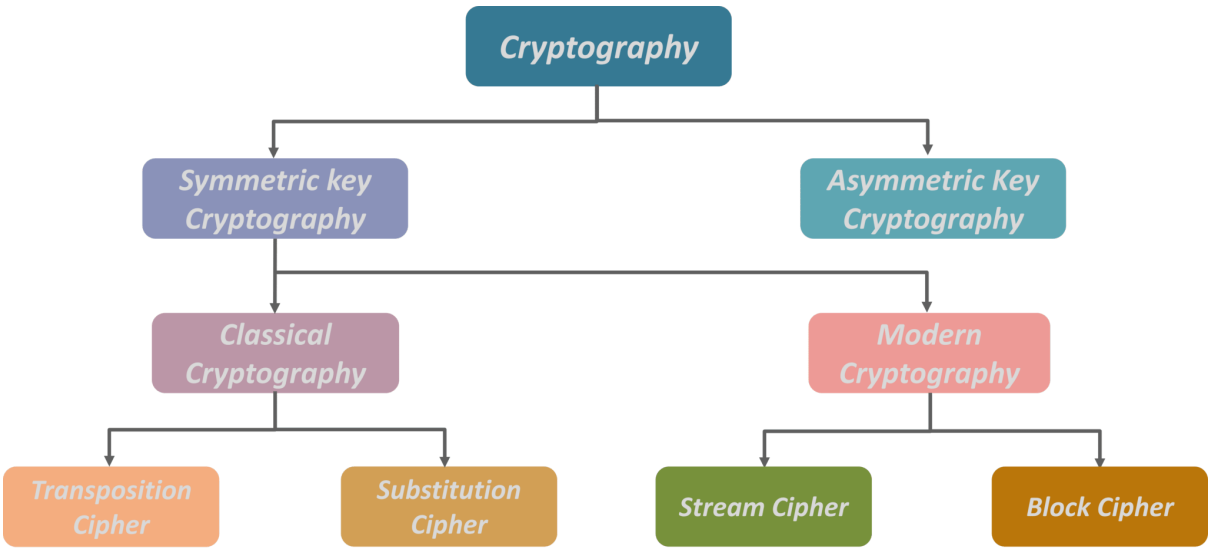
In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

1. **Confidentiality:**
   Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:**
   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:**
   The creator/sender of information cannot deny his or her intention to send information at later stage.
4. **Authentication:**
   The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

In general there are three types Of cryptography:

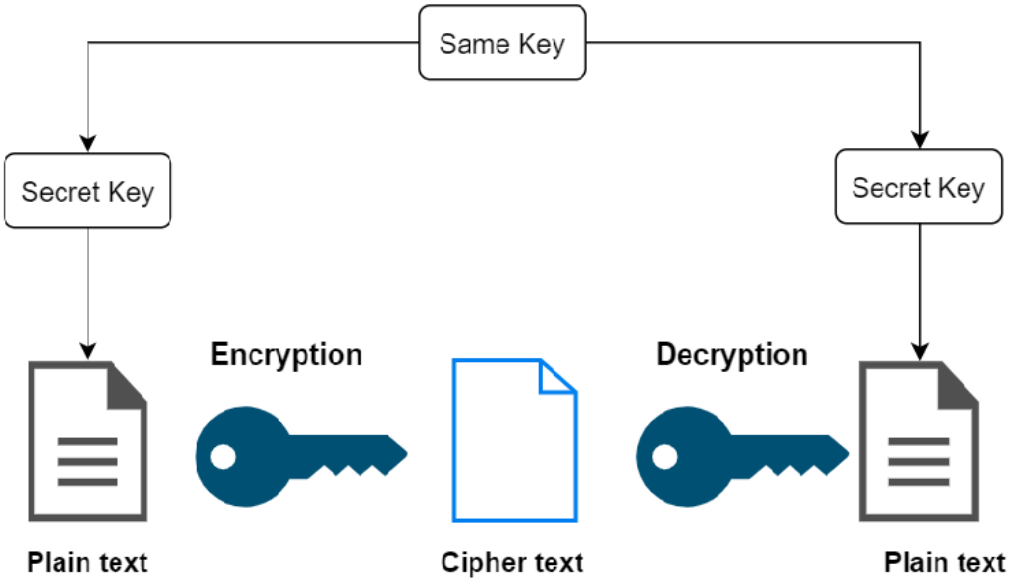


Cryptography Types

In **cryptography**, encryption of the information is classified as three types where those are discussed below:

Symmetric Key Cryptography – This is also termed as Private or Secret key cryptography. Here, both the information receiver and the sender make use of a single key to encrypt and decrypt the message. The frequent kind of cryptography used in this method is AES (Advanced Encryption System). The approaches implemented through this type are completely streamlined and quicker too. Few types of Symmetric key cryptography are

- Block
- Block cipher
- DES (Data Encryption System)
- RC2
- IDEA
- Blowfish
- Stream cipher

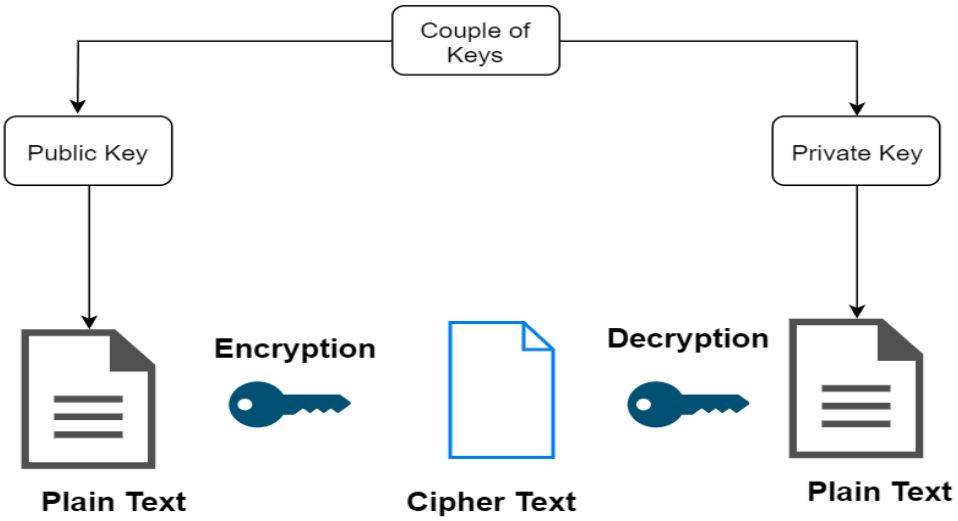


symmetric encryption

Asymmetric Key Cryptography

This is also termed as Public-key cryptography. It follows a varied and protected method in the transmission of information. Using a couple of keys, both the sender and receiver go with encryption and decryption processes. A private key is stored with each person and the public key is shared across the network so that a message can be transmitted through public keys. The frequent kind of cryptography used in this method is RSA. The public key method is more secure than that of a private key. Few of the kinds of Asymmetric key cryptography are:

- RSA
- DSA
- PKCs
- Elliptic curve techniques

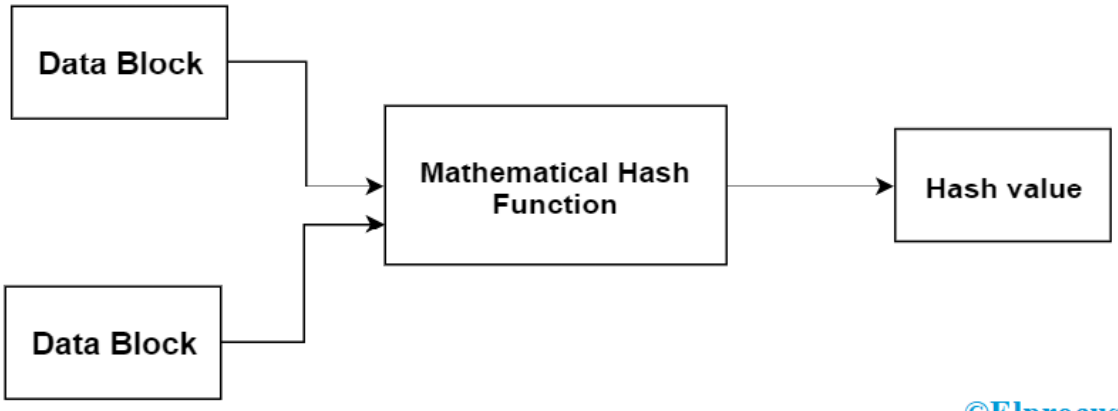


- asymmetric encryption

Hash Function

Taking the arbitrary length of the message as input and delivering a fixed length of the output is the algorithm followed by a hash function. It is also termed as a mathematical equation by taking numerical values as input and produce the hash message. This method will not need any kind of key as it functions in a one-way scenario. There are various rounds of hashing operations and every round considers input as an array of the recent block and generates last round activity as output. Few of the functionalities of the hash are:

- Message Digest 5 (MD5)
- RIPEMD
- Whirlpool
- SHA (Secure hash Algorithm)



1. hash function

Applications of Cryptography

Applications for **cryptography** as below.

Conventionally, cryptography was in implementation only for securing purposes. Wax seals, hand signatures and few other kinds of security methods were generally utilized to make sure of reliability and accuracy of the transmitter. And with the arrival of digital transmissions, security becomes more essential and then cryptography mechanisms began to outstrip its utilization for maintaining utmost secrecy. A few of the applications of cryptography are discussed below.

To Maintain Secrecy in Storage

Cryptography allows storing the encrypted data permitting users to stay back from the major hole of circumvention by hackers.

Reliability in Transmission

A conventional approach that allows reliability is to carry out a checksum of the communicated information and then communicate the corresponding checksum in an encrypted format. When both the checksum and encrypted data is received, the data is again checksummed and compared to the communicated checksum after the process of decryption. Thus, effective cryptographic mechanisms are more crucial to assure reliability in message transmission.

Authentication of Identity

Cryptography is strongly linked to the approach of using passwords, and innovative systems probably make use of strong cryptographic methods together with the physical methods of individuals and collective secrets offering highly reliable verification of identity.

Types of Cryptography

"Cryptography is the standard of encrypting all the data and information by converting Plain text into cipher text for secure communication."

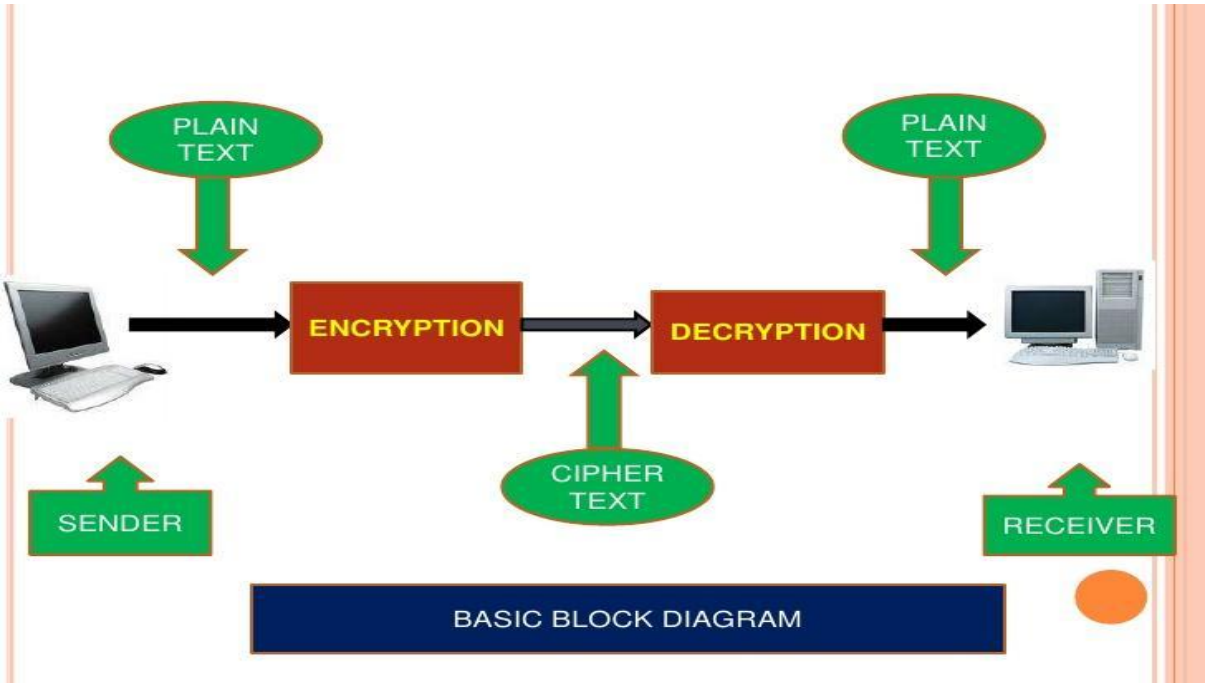
Encryption is the key to secure all our data and information while we communicate with others over any transmission channel. Now, you might be thinking why this encryption matters a lot?

Data is something that is important in each field. It may include your personal identity, your financial stats, your bank account details, or anything else. No one wants that their data should be accessed by any unauthorized user. But unfortunately, there are adversaries present in the market to snatch that information in a very smart way.

There are a lot of hackers and unauthorized users who want access to public data, so they can mislead that information for their benefits. For this purpose, Cryptography standards were introduced to protect our data from such threats.

- **Plain Text:** The message which we send to the receiver. For e.g.- "Hello"
- **Cipher Text:** Conversion of that plain text into a non-readable format. For e.g.- "H@#$5"

Now let's start with the basics.



Now, suppose there is one sender A who wants to send a message to receiver B who is in the other part of the world. The sender obviously wants this message to be private and no one should access it except the receiver. Here, the only motive is to secure the communication.

The sender A will first convert its plain text message into cipher text (unreadable format) using a key. The message is then encrypted and now A sends this message to receiver B over any transmission media.

B now receives the message and will require a decryption key to decode the message into a readable format. He then uses the key and decrypts the message to find the original plain text.

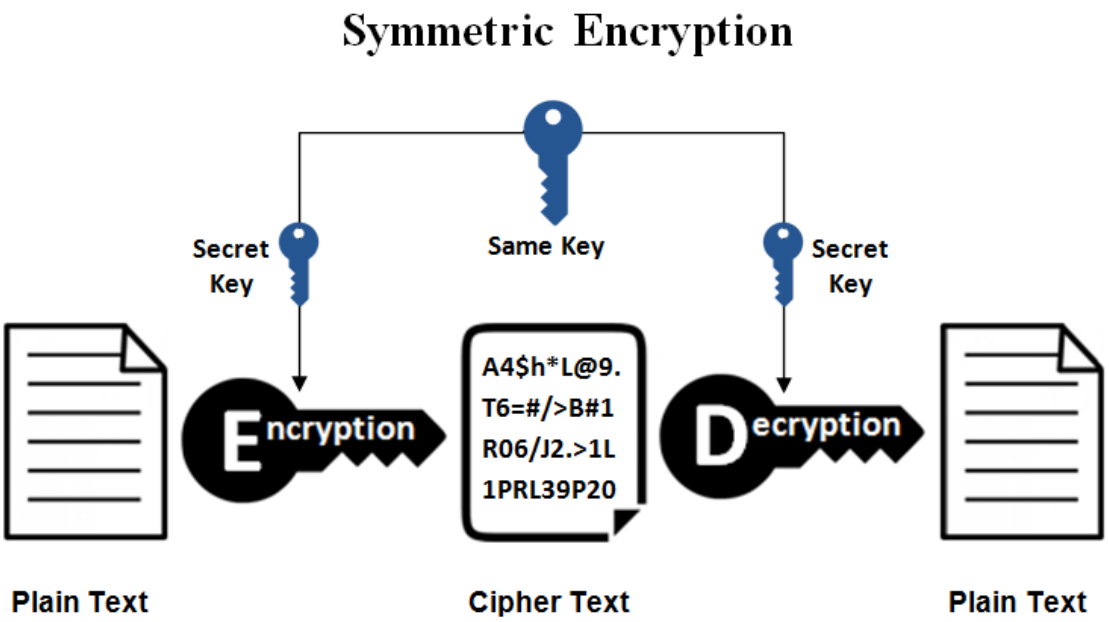
This is how cryptography works and data is encrypted to secure them from external threats and attacks. There are several different types of cryptography algorithms with each different working methodologies to encrypt the data in the best possible way.

Types of Cryptography

Cryptography is further classified into three different categories:

- **Symmetric Key Cryptography** (Private/Secret Key Cryptography)
- **Asymmetric Key Cryptography** (Public Key Cryptography)
- **Hash Function**

Symmetric Key Cryptography

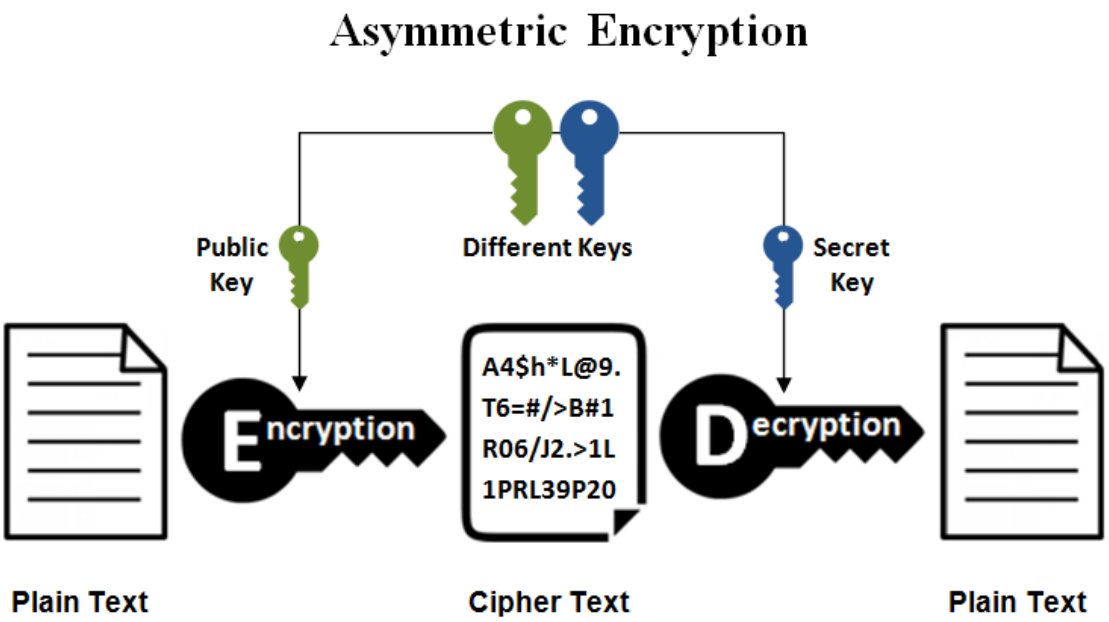


Symmetric key cryptography is a type of cryptography in which the single common key is used by both sender and receiver for the purpose of encryption and decryption of a message. This system is also called private or secret key cryptography and AES (Advanced Encryption System) is the most widely uses symmetric key cryptography.

The symmetric key system has one major drawback that the two parties must somehow exchange the key in a secure way as there is only one single key for encryption as well as decryption process.

Types: AES (Advanced Encryption Standard), DES, Triple DES, RC2, RC4, RC5, IDEA, Blowfish, Stream cipher, Block cipher, etc. are the types of symmetric key cryptography.

Asymmetric Key Cryptography

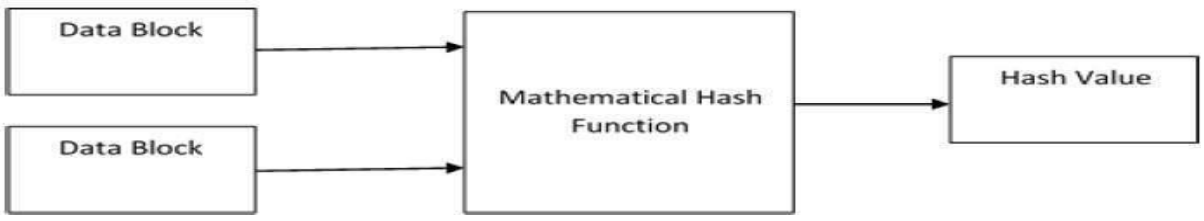


Asymmetric Key Cryptography is completely different and a more secure approach than symmetric key cryptography. In this system, every user uses two keys or a pair of keys (private key and public key) for encryption and decryption process. Private key is kept as a secret with every user and public key is distributed over the network so if anyone wants to send message to any user can use those public keys.

Either of the key can be used to encrypt the message and the one left is used for decryption purpose. Asymmetric key cryptography is also known as public key cryptography and is more secure than symmetric key. RSA is the most popular and widely used asymmetric algorithm.

Types: RSA, DSA, PKCs, Elliptic Curve techniques, etc. are the common types of asymmetric key cryptography.

Hash Function



A Hash function is a cryptography algorithm that takes input of arbitrary length and gives the output in fixed length. The hash function is also considered as a mathematical equation that takes seed (numeric input) and produce the output that is called hash or message digest. This system operates in one-way manner and does not require any key. Also, it is considered as the building blocks of modern cryptography.

The hash function works in a way that it operates on two blocks of fixed length binary data and then generate a hash code. There are different rounds of hashing functions and each round takes an input of combination of most recent block and the output of the last round.

Types: Some popular hash functions are Message Digest 5 (MD5), SHA (Secure Hash Algorithm), RIPEMD, and Whirlpool. MD5 is the most commonly used hash function to encrypt and protect your passwords and private data.

Difference between Symmetric, Asymmetric and Hash Function Cryptography

- Symmetric Key uses single key to encrypt and decrypt the message while asymmetric key uses a pair of keys in which one key is used for encryption and other for decryption whereas hash function does not require any key for encryption as well as decryption.
- Symmetric key is relatively faster than asymmetric and hash function but less reliable in terms of security.
- Asymmetric key was introduced to overcome the problem of key exchange in symmetric key and hash functions were introduced to provide more security than ever.
- If the key is compromised over the network then there will loss of both sender and receiver in symmetric key, only loss of key owner in asymmetric key, and in hash function, there is no key to compromise.
- Asymmetric key has higher complexity than hash function and symmetric key has very less complexity.

Conclusion

Encryption of data is much needed in our modern time and the latest schemes may necessarily be the best fit. There are the latest algorithms and techniques being developed as hackers and eavesdroppers have made it tough to secure data to the best possible way. Cryptography is going to enhance more methods in the coming years to make personal data more secure and it’s standards more reliable.