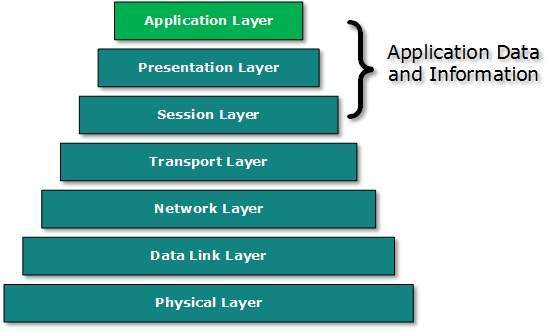
**Unit-V - Application Layer**

Introduction

Application layer is the top most layer in OSI and TCP/IP layered model. This layer exists in both layered Models because of its significance, of interacting with user and user applications. This layer is for applications which are involved in communication system.

A user may or may not directly interacts with the applications. Application layer is where the actual communication is initiated and reflects. Because this layer is on the top of the layer stack, it does not serve any other layers. Application layer takes the help of Transport and all layers below it to communicate or transfer its data to the remote host.

When an application layer protocol wants to communicate with its peer application layer protocol on remote host, it hands over the data or information to the Transport layer. The transport layer does the rest with the help of all the layers below it.



There’is an ambiguity in understanding Application Layer and its protocol. Not every user application can be put into Application Layer. except those applications which interact with the communication system. For example, designing software or text-editor cannot be considered as application layer programs.

On the other hand, when we use a Web Browser, which is actually using Hyper Text Transfer Protocol (HTTP) to interact with the network. HTTP is Application Layer protocol.

Another example is File Transfer Protocol, which helps a user to transfer text based or binary files across the network. A user can use this protocol in either GUI based software like FileZilla or CuteFTP and the same user can use FTP in Command Line mode.

Hence, irrespective of which software you use, it is the protocol which is considered at Application Layer used by that software. DNS is a protocol which helps user application protocols such as HTTP to accomplish its work.

Domain Name System (DNS)

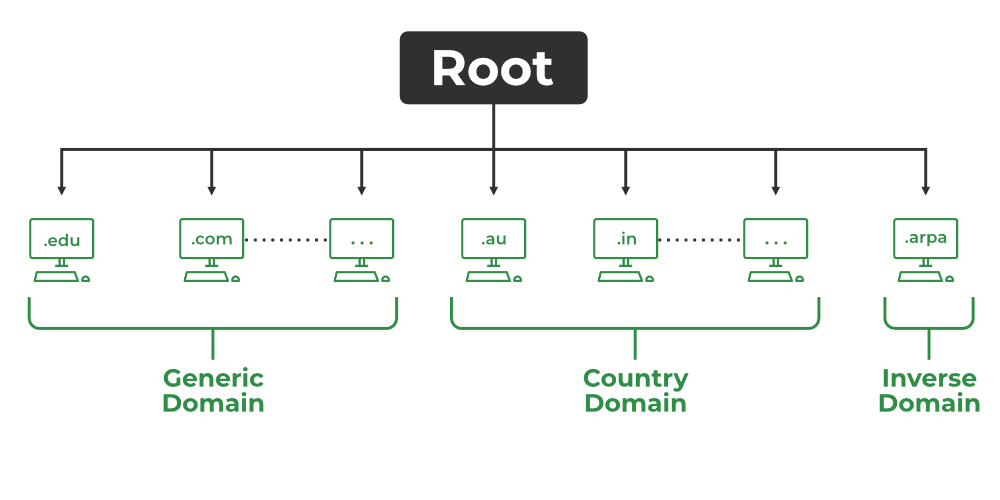
Domain Name System (DNS) is a hostname for **IP address**translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers. It is required for the functioning of the Internet.

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

**Types of Domain**

There are various kinds of domain:

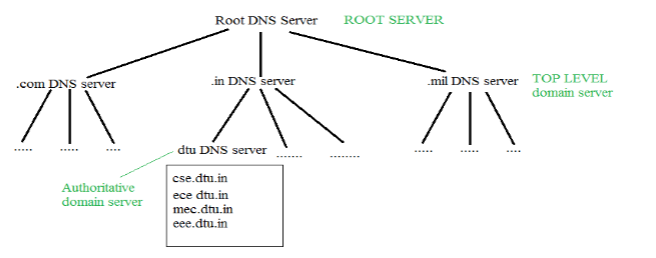
1. **Generic domains:** .com(commercial), .edu(educational), .mil(military), .org(nonprofit organization), .net(similar to commercial) all these are generic domains.
2. **Country domain:** .in (India) .us .uk
3. **Inverse domain:** if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the IP addresses of geeksforgeeks.org then we have to type



**Types of DNS**

**Organization of Domain**

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



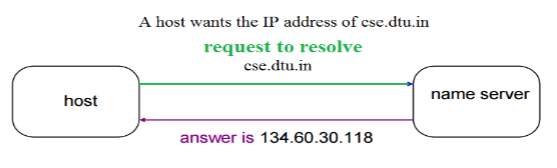
*Root DNS Server*

* **DNS record:** Domain name, IP address what is the validity? what is the time to live? and all the information related to that domain name. These records are stored in a tree-like structure.
* **Namespace:** Set of possible names, flat or hierarchical. The naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value.
* **Name server:** It is an implementation of the resolution mechanism.

DNS = Name service in Internet – A zone is an administrative unit, and a domain is a subtree.

**Name-to-Address Resolution**

The host requests the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

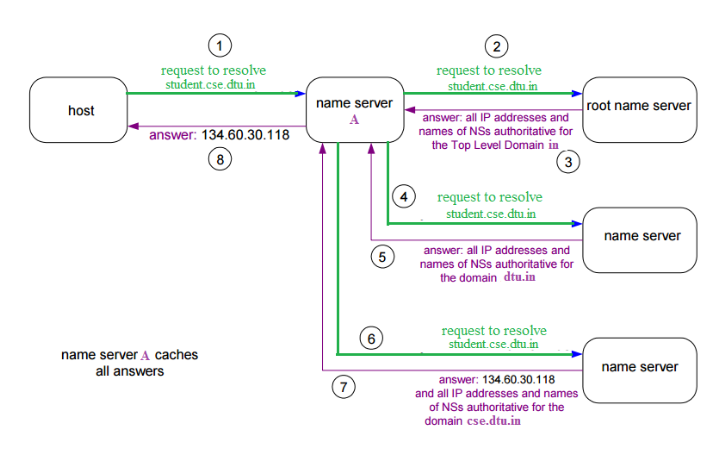


*Name-to-Address Resolution*

1. **Hierarchy of Name Servers** **Root name servers:** It is contacted by name servers that cannot resolve the name. It contacts the authoritative name server if name mapping is not known. It then gets the mapping and returns the IP address to the host.
2. **Top-level domain (TLD) server:** It is responsible for com, org, edu, etc, and all top-level country domains like uk, fr, ca, in, etc. They have info about authoritative domain servers and know the names and IP addresses of each authoritative name server for the second-level domains.
3. **Authoritative name servers**are the organization’s DNS servers, providing authoritative hostnames to IP mapping for organization servers. It can be maintained by an organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top-level domain server and then to the authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative IP address.

**Domain Name Server**

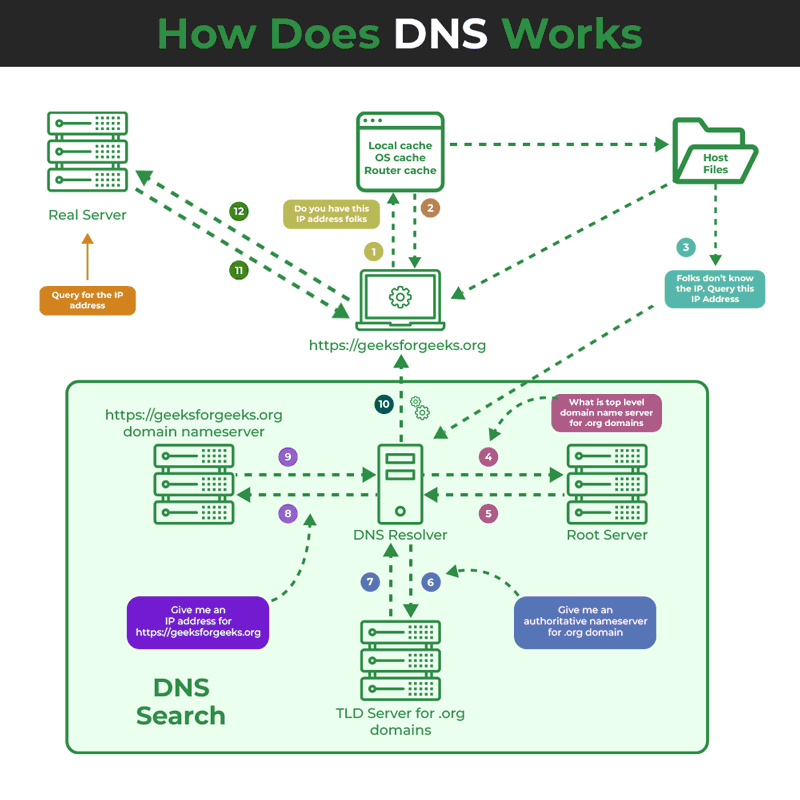
The client machine sends a request to the local name server, which, if the root does not find the address in its database, sends a request to the root name server, which in turn, will route the query to a top-level domain (TLD) or authoritative name server. The root name server can also contain some hostName to IP address mappings. The Top-level domain (TLD) server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.



*Domain Name Server*

**How Does DNS Work?**

The working of DNS starts with converting a hostname into an IP Address. A domain name serves as a distinctive identification for a website. It is used in place of an IP address to make it simpler for consumers to visit websites. Domain Name System works by executing the database whose work is to store the name of hosts which are available on the Internet. The top-level domain server stores address information for top-level domains such as .com and .net, .org, and so on. If the Client sends the request, then the DNS resolver sends a request to DNS Server to fetch the IP Address. In case, when it does not contain that particular IP Address with a hostname, it forwards the request to another DNS Server. When IP Address has arrived at the resolver, it completes the request over Internet Protocol.



Authoritative DNS Server Vs Recursive DNS Resolver

| **Parameters** | **Authoritative DNS Server** | **Recursive DNS Resolver** |
| --- | --- | --- |
| **Function** | Holds the official DNS records for a domain | Resolves DNS queries on behalf of clients |
| **Role** | Provides answers to specific DNS queries | Actively looks up information for clients |
| **Query Handling** | Responds with authoritative DNS data | Queries other DNS servers for DNS data |
| **Client Interaction** | Doesn’t directly interact with end-users | Serves end-users or client applications |
| **Data Source** | Stores the DNS records for specific domains | Looks up data from other DNS servers |
| **Caching** | Generally, doesn’t perform caching | Caches DNS responses for faster lookups |
| **Hierarchical Resolution** | Does not participate in the recursive resolution | Actively performs recursive name resolution |
| **IP Address** | Has a fixed, known IP address | IP address may vary depending on ISP |
| **Zone Authority** | Manages a specific DNS zone (domain) | Does not manage any specific DNS zone |

**DNS Lookup**

DNS Lookup or DNS Resolution can be simply termed as the process that helps in allowing devices and applications that translate readable domain names to the corresponding IP Addresses used by the computers for communicating over the web.

**DNS Servers Involved in Loading a Webpage**

Upon loading the webpage, several DNS Servers are responsible for translating the domain name into the corresponding IP Address of the web server hosting the website. Here is the list of main DNS servers involved in loading a Webpage.

* Local DNS Resolver
* Root DNS Servers
* Top-Level Domain (TLD) DNS Servers
* Authoritative DNS Servers
* Web Server

This hierarchical system of DNS servers ensures that when you type a domain name into your web browser, it can be translated into the correct IP address, allowing you to access the desired webpage on the internet.

**DNS Resolver**

DNS Resolver is simply called a DNS Client and has the functionality for initiating the process of DNS Lookup which is also called DNS Resolution. By using the DNS Resolver, applications can easily access different websites and services present on the Internet by using domain names that are very much friendly to the user and that also resolves the problem of remembering IP Address.

**Types of DNS Queries**

There are basically three types of DNS Queries that occur in DNS Lookup. These are stated below.

1. **Recursive Query:**In this query, if the resolver is unable to find the record, in that case, DNS client wants the DNS Server will respond to the client in any way like with the requested source record or an error message.
2. **Iterative Query:**Iterative Query is the query in which DNS Client wants the best answer possible from the DNS Server.
3. **Non-Recursive Query:** Non-Recursive Query is the query that occurs when a DNS Resolver queries a DNS Server for some record that has access to it because of the record that exists in its cache.

**DNS Caching**

DNS Caching can be simply termed as the process used by DNS Resolvers for storing the previously resolved information of DNS that contains domain names, and IP Addresses for some time. The main principle of DNS Caching is to speed up the process of future DNS lookup and also help in reducing the overall time of DNS Resolution.

Simple Network Management Protocol (SNMP)

If an organization has 1000 devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

**Simple Network Management Protocol (SNMP) –**

SNMP is an application layer protocol that uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.

**SNMP components –**

There are 3 components of SNMP:

1. **SNMP Manager –** It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)
2. **SNMP agent –** It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.
3. **Management Information Base –** MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

**SNMP messages –**

Different variables are:

1. **GetRequest –**  - SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.
2. **GetNextRequest -** This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.
3. **GetBulkRequest –**This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.
4. **SetRequest –** It is used by the SNMP manager to set the value of an object instance on the SNMP agent.
5. **Response –** It is a message sent from the agent upon a request from the manager. When sent in response to get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.
6. **Trap –** These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.
7. **InformRequest –** It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn’t provide.
8. **SNMP security levels –** It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are **3 security levels** namely:

* **noAuthNoPriv –** This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.
* **authNopriv –** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
* **authPriv –** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses the DES-56 algorithm.

**SNMP versions –**

There are 3 versions of SNMP:

1. **SNMPv1 –**  It uses community strings for authentication and uses UDP only.
2. **SNMPv2c –** It uses community strings for authentication. It uses UDP but can be configured to use TCP.
3. **SNMPv3 –** It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, the conclusion is the higher the version of SNMP, the more secure it will be.

**Strength of SNMP:**

1. It is simple to implement.
2. Agents are widely implemented.
3. Agent level overhead is minimal.
4. It is robust and extensible.
5. Polling approach is good for LAN based managed object.
6. It offers the best direct manager agent interface.
7. SNMP meet a critical need.

**Limitation of SNMP:**

1. It is too simple and does not scale well.
2. There is no object oriented data view.
3. It has no standard control definition.
4. It has many implementation specific (private MIB) extensions.
5. It has high communication overhead due to polling

Electronic Mail

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

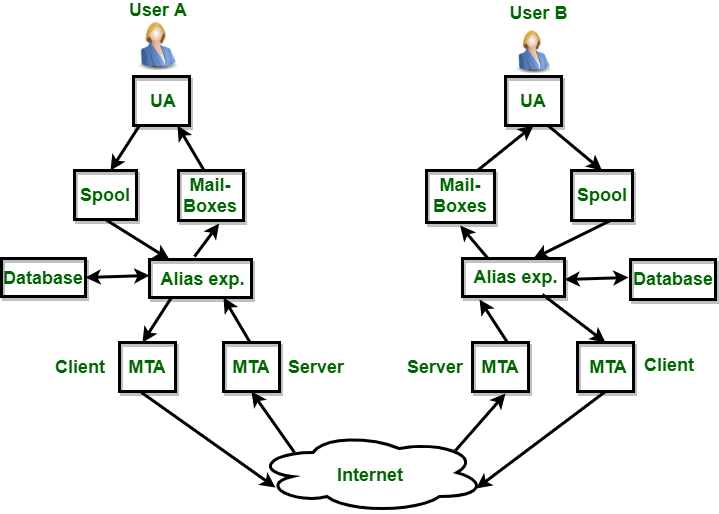
1. **An email address:** This is a unique identifier for each user, typically in the format of name@domain.com.
2. **An email client:** This is a software program used to send, receive and manage emails, such as Gmail, Outlook, or Apple Mail.
3. **An email server:** This is a computer system responsible for storing and forwarding emails to their intended recipients.

**To send an email:**

1. Compose a new message in your email client.
2. Enter the recipient’s email address in the “To” field.
3. Add a subject line to summarize the content of the message.
4. Write the body of the message.
5. Attach any relevant files if needed.
6. Click “Send” to deliver the message to the recipient’s email server.
7. Emails can also include features such as cc (carbon copy) and bcc (blind carbon copy) to send copies of the message to multiple recipients, and reply, reply all, and forward options to manage the conversation.

**Electronic Mail** (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a **message in formatted manner (mail)** to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called **sender** and person who receives mail is called**recipient**. It is just like postal mail service. **Components of E-Mail System:** The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. **User Agent (UA):** The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.
2. **Message Transfer Agent (MTA):** MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.



1. **Mailbox:** It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox. Access to mailbox is only to owner of mailbox.
2. **Spool file:** This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an **alias**, to represent several different e-mail addresses. It is known as **mailing list**, Whenever user have to send a message, system checks recipient’s name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

**Services provided by E-mail system:**

1. **Composition –** The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
2. **Transfer –** Transfer means sending procedure of mail i.e. from the sender to recipient.
3. **Reporting –** Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
4. **Displaying –** It refers to present mail in form that is understand by the user.
5. **Disposition –** This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

**Advantages of email:**

* Convenient and fast communication with individuals or groups globally.
* Easy to store and search for past messages.
* Ability to send and receive attachments such as documents, images, and videos.
* Cost-effective compared to traditional mail and fax.
* Available 24/7.

**Disadvantages of email:**

* Risk of spam and phishing attacks.
* Overwhelming amount of emails can lead to information overload.
* Can lead to decreased face-to-face communication and loss of personal touch.
* Potential for miscommunication due to lack of tone and body language in written messages.
* Technical issues, such as server outages, can disrupt email service.
* It is important to use email responsibly and effectively, for example, by keeping the subject line clear and concise, using proper etiquette, and protecting against security threats.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is an application layer protocol that moves files between local and remote file systems. It runs on top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection.

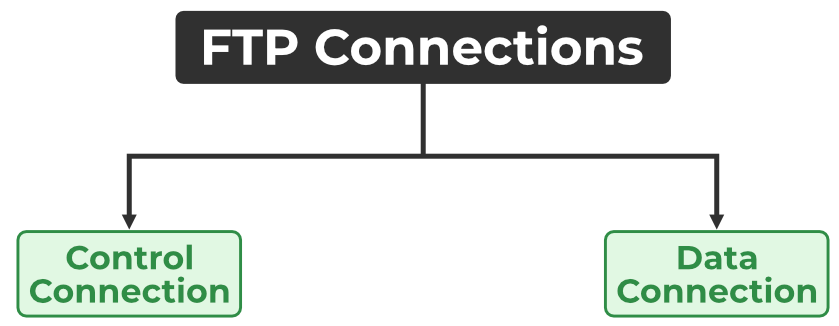
FTP is a standard communication protocol. There are various other protocols like HTTP which are used to transfer files between computers, but they lack clarity and focus as compared to FTP. Moreover, the systems involved in connection are heterogeneous systems, i.e. they differ in operating systems, directories, structures, character sets, etc the FTP shields the user from these differences and transfers data efficiently and reliably. FTP can transfer ASCII, EBCDIC, or image files. The ASCII is the default file share format, in this, each character is encoded by NVT ASCII. In ASCII or EBCDIC the destination must be ready to accept files in this mode. The image file format is the default format for transforming binary files.

**Mechanism of File Transfer Protocol**



Types of Connection in FTP

1. Control Connection
2. Data Connection



*Types of Connection in FTP*

1. **Control Connection:** For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of a control connection. The control connection is initiated on port number 21.
2. **Data connection:**For sending the actual file, FTP makes use of a data connection. A data connection is initiated on port number 20.

FTP sends the control information out-of-band as it uses a separate control connection. Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples.

**FTP Session**

When an FTP session is started between a client and a server, the client initiates a control TCP connection with the server side. The client sends control information over this. When the server receives this, it initiates a data connection to the client side. Only one file can be sent over one data connection. But the control connection remains active throughout the user session. As we know HTTP is stateless i.e. it does not have to keep track of any user state. But FTP needs to maintain a state about its user throughout the session.

**FTP Clients**

FTP works on a client-server model. The FTP client is a program that runs on the user’s computer to enable the user to talk to and get files from remote computers. It is a set of commands that establishes the connection between two hosts, helps to transfer the files, and then closes the connection.

Some of the commands are:

* *get the filename(retrieve the file from the server)*
* *get the filename(retrieve multiple files from the server )*
* *ls(list files available in the current directory of the server)*

There are also built-in FTP programs, which makes it easier to transfer files and it does not require remembering the commands.

**FTP Data Structures**

FTP allows three types of data structures:

1. **File Structure:**In file structure, there is no internal structure and the file is considered to be a continuous sequence of data bytes.
2. **Record Structure:**In record structure, the file is made up of sequential records.
3. **Page Structure:**In page structure, the file is made up of independent indexed pages.

**FTP Commands**

Some of the FTP commands are:

* USER – This command sends the user identification to the server.
* PASS – This command sends the user password to the server.
* CWD – This command allows the user to work with a different directory or dataset for file storage or retrieval without altering his login or accounting information.
* RMD – This command causes the directory specified in the path name to be removed as a directory.
* MKD – This command causes the directory specified in the pathname to be created as a directory.
* PWD – This command causes the name of the current working directory to be returned in the reply.
* RETR – This command causes the remote host to initiate a data connection and send the requested file over the data connection.
* STOR – This command causes the storage of a file in the current directory of the remote host.
* LIST – Sends a request to display the list of all the files present in the directory.
* ABOR – This command tells the server to abort the previous FTP service command and any associated transfer of data.
* QUIT – This command terminates a USER and if file transfer is not in progress, the server closes the control connection.

**FTP Replies**

Some of the FTP replies are:

* 200 – Command okay.
* 530 – Not logged in.
* 331 – User name okay, need a password.
* 225 – Data connection open; no transfer in progress.
* 221 – Service closing control connection.
* 551 – Requested action aborted: page type unknown.
* 502 – Command not implemented.
* 503 – Bad sequence of commands.
* 504 – Command not implemented for that parameter.

**Characteristics of FTP**

* FTP uses TCP as a transport layer protocol.
* It is good for simple file transfers, such as during boot time.
* Errors in the transmission (lost packets, checksum errors) must be handled by the TFTP server.
* It uses only one connection through well-known port 69.
* TFTP uses a simple lock-step protocol (each data packet needs to be acknowledged). Thus the throughput is limited.

**Advantages of FTP**

* Speed is one of the advantages of FTP (File Transfer Protocol).
* File sharing also comes in the category of advantages of FTP in this between two machines files can be shared on the network.
* Efficiency is more in FTP.

**Disadvantages of FTP**

* File size limit is the drawback of FTP only 2 GB size files can be transferred.
* Multiple receivers are not supported by the FTP.
* FTP does not encrypt the data this is one of the biggest drawbacks of FTP.
* FTP is unsecured we use login IDs and passwords making it secure but they can be attacked by hackers.

**Anonymous FTP**

Anonymous FTP is enabled on some sites whose files are available for public access. A user can access these files without having any username or password. Instead, the username is set to anonymous, and the password is to the guest by default. Here, user access is very limited. For example, the user can be allowed to copy the files but not to navigate through directories.

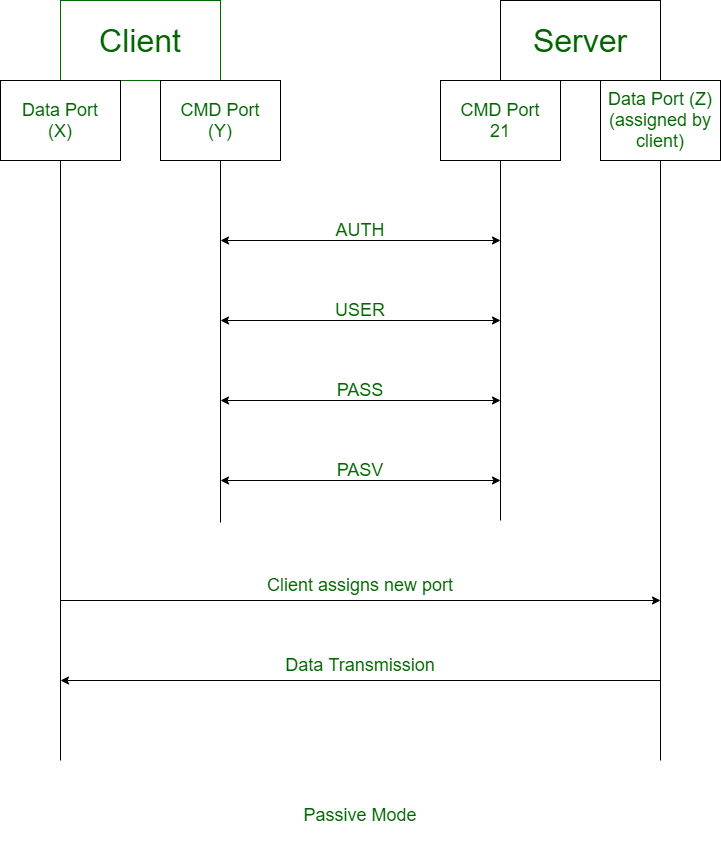
**Difference between Active and Passive FTP**

FTP stands for File Transfer Protocol. It is an application layer protocol which transfers files over a network. It uses TCP based service. FTP works in two different modes:

**1. Active FTP:**  In the active mode, the client connects on a random port for incoming data connections from the server. Client again sends next port to FTP server which is acknowledged on command channel.



**2. Passive FTP:** In the passive mode, the client uses the control connection to send a *PASV* signal to the server. FTP server sends back IP address and server port number.



Differences between Active and Passive FTP:

| **Active FTP** | **Passive FTP** |
| --- | --- |
| In active FTP, client establishes the command channel and the server establishes the data channel. | In passive FTP, both the command channel and the data channel are established by the client. |
| Active FTP provides security to the FTP server. | Passive FTP does not provide security to the FTP server. |
| Active FTP may cause problems because of firewalls. | Passive FTP does not have connection issues from firewalls. |
| Active mode is not used as a default mode of a browser. | Passive mode is used as a default mode of a browser. |
| FTP client acknowledges on data channel. | FTP server acknowledges on data channel. |
| Client sends random port number to the server. | Client sends PASV command to the server. |
| In Active FTP, the data connection is made and the file transfers are then done through  client and server ports. | In passive FTP, the client still have to initiates the command channel (control connection) to the server. |

TELNET

**TELNET** stands for**Tel**etype **Net**work. It is a type of protocol that enables one computer to connect to the local computer. It is used as a standard **TCP/IP protocol** for virtual terminal service which is provided by **ISO**. The computer which starts the connection is known as the**local computer**.

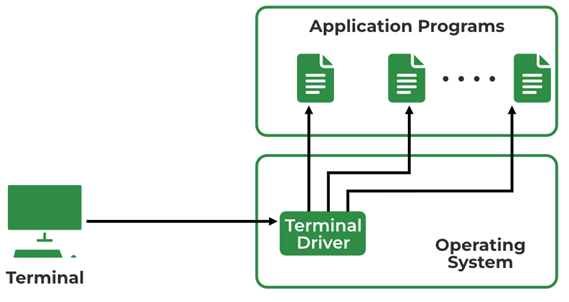
The computer which is being connected to i.e. which accepts the connection known as the **remote computer**.

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

**Logging**

The logging process can be further categorized into two parts:

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

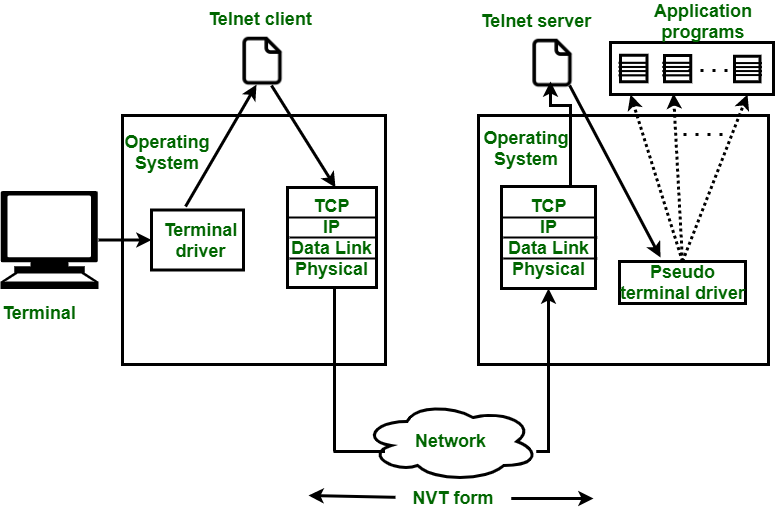


*Local Login*

**The Procedure of Local Login**

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

1. **Remote Login:** Remote Login is a process in which users can log in to a remote site i.e. computer and use services that are available on the remote computer. With the help of remote login, a user is able to understand the result of transferring the result of processing from the remote computer to the local computer.



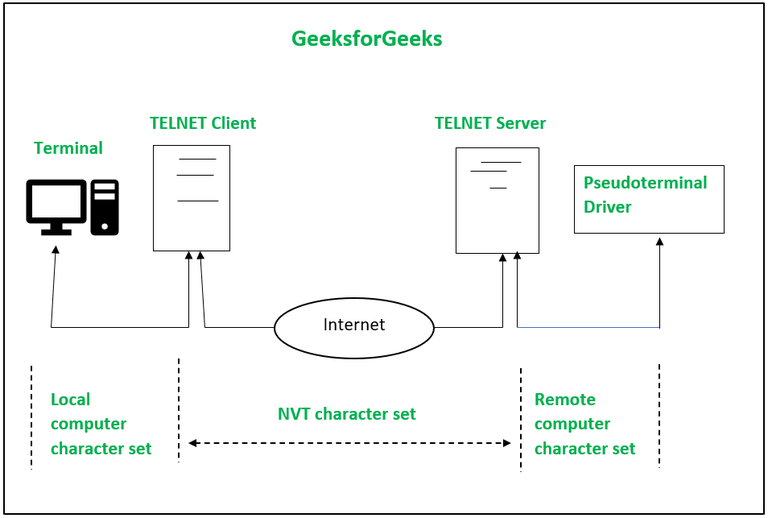
*Remote Login in Logging*

**The Procedure of Remote Login**

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

**Network Virtual Terminal (NVT)**

NVT (Network Virtual Terminal) is a virtual terminal in TELNET that has a fundamental structure that is shared by many different types of real terminals. NVT (Network Virtual Terminal) was created to make communication viable between different types of terminals with different operating systems.



*Network Virtual Terminal (NVT) in Telnet*

**TELNET Commands**

Commands of Telnet are identified by a prefix character, Interpret As Command (IAC) with code 255. IAC is followed by command and option codes.

The basic format of the command is as shown in the following figure :



**TELNET commands:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Character** | **Decimal** | **Binary** | **Meaning** |
| WILL | 251 | 11111011 | 1. Offering to enable.  2. Accepting a request to enable. |
| WON’T | 252 | 11111100 | 1. Rejecting a request to enable.  2. Offering to disable.  3. Accepting a request to disable. |
| DO | 253 | 11111101` | 1. Approving a request to enable.  2. Requesting to enable. |
| DON’T | 254 | 11111110 | 1. Disapproving a request to enable.  2. Approving an offer to disable.  3. Requesting to disable. |

**Common options used with the telnet:**

| **Code** | **Option** | **Meaning** |
| --- | --- | --- |
| 0 | Binary | It interprets as 8-bit binary transmission. |
| 1 | Echo | It will echo the data that is received on one side to the other side. |
| 3 | Suppress go ahead | It will suppress go ahead signal after data. |
| 5 | Status | It will request the status of TELNET. |
| 6 | Timing mark | It defines the timing marks. |
| 8 | Line width | It specifies the line width. |
| 9 | Page size | It specifies the number of lines on a page. |
| 24 | Terminal type | It set the terminal type. |
| 32 | Terminal speed | It set the terminal speed. |
| 34 | Line mode | It will change to the line mode. |

**Advantages of Telnet**

* It provides remote access to someone’s computer system.
* Telnet allows the user for more access with fewer problems in data transmission.
* Telnet saves a lot of time.
* The oldest system can be connected to a newer system with telnet having different operating systems.

**Disadvantages of Telnet**

* As it is somehow complex, it becomes difficult to beginners in understanding.
* Data is sent here in form of plain text, that’s why it is not so secured.
* Some capabilities are disabled because of not proper interlinking of the remote and local devices.

**Modes of Operation**

Most telnet implementations operate in one of the following three modes:

1. **Default Mode:**If no other modes are invoked then this mode is used. Echoing is performed in this mode by the client. In this mode, the user types a character and the client echoes the character on the screen but it does not send it until the whole line is completed.
2. **Character Mode:** Each character typed in this mode is sent by the client to the server. A server in this type of mode normally echoes characters back to be displayed on the client’s screen.
3. **Line Mode:**  Line editing like echoing, character erasing, etc. is done from the client side. The client will send the whole line to the server.

Hyper Text Transfer Protocol (HTTP)

**HTTP** stands for HyperText Transfer Protocol. Tim Berner invents it. HyperText is the type of text which is specially coded with the help of some standard coding language called HyperText Markup Language (HTML). **HTTP/2** is the successor version of HTTP, which was published on May 2015. HTTP/3 is the latest version of HTTP, which is published in 2022.

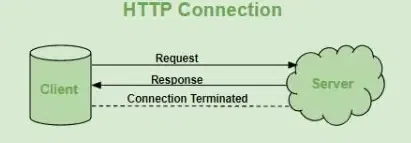
The protocol used to transfer hypertext between two computers is known as HyperText Transfer Protocol.

HTTP provides a standard between a web browser and a web server to establish communication. It is a set of rules for transferring data from one computer to another. Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, the user indirectly uses HTTP. It is an application protocol that is used for distributed, collaborative, hypermedia information systems.

**Working of HTTP**

First of all, whenever we want to open any website then first open a web browser after that we will type the URL of that website (e.g., www.facebook.com). This URL is now sent to Domain Name Server (DNS). Then DNS first check records for this URL in their database, and then DNS will return the IP address to the web browser corresponding to this URL. Now the browser is able to send requests to the actual server.

After the server sends data to the client, the connection will be closed. If we want something else from the server we should have to re-establish the connection between the client and the server.



*HTTP Connection*

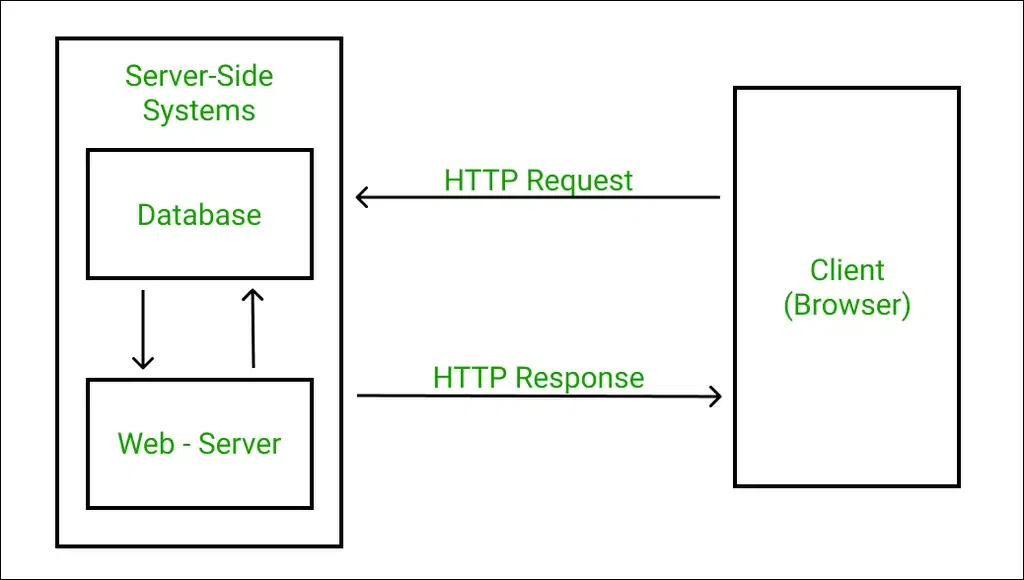
**HTTP Request**

HTTP request is simply termed as the information or data that is needed by Internet browsers for loading a website. This is simply known as HTTP Request.

There is some common information that is generally present in all HTTP requests. These are mentioned below.

1. HTTP Version
2. URL
3. HTTP Method
4. HTTP Request Headers
5. HTTP Body

* **HTTP Request Headers -** HTTP Request Headers generally store information in the form of key-value and must be present in each HTTP Request. The use of this Request Header is to provide core information about the client’s information, etc.
* **HTTP Request Body -** HTTP Request Body simply contains the information that has to be transferred. HTTP Request has the information or data to be sent to these browsers.
* **HTTP Method -** HTTP Methods are simply HTTP Verb. In spite of being present so many HTTP Methods, the most common HTTP Methods are HTTP GET and HTTP POST. These two are generally used in HTTP cases. In HTTP GET, the information is received in the form of a website.
* **HTTP Response -** HTTP Response is simply the answer to what a Server gets when the request is raised. There are various things contained in HTTP Response, some of them are listed below.
* HTTP Status Code
* HTTP Headers
* HTTP Body



*HTTP Response*

**HTTP Response Headers -** HTTP Response headers are simply like an HTTP Request where it has that work to send some important files and data to the HTTP Response Body.

**HTTP Response Body -** HTTP Responses are the responses that are received successfully upon the request. Generally, it comes under the requests generated by the web. In most cases, the request is of transferring the HTML data into a webpage.

**HTTP Status Code**

HTTP Status Codes are the 3-Digit codes that tell the message or simply tell us about the HTTP Request whether it has been completed or not. There are simply 5 types of status codes.

1. Informational
2. Successful
3. Re-directional
4. Client-Error
5. Server-Error

**History of HTTP**

Tim Berners Lee and his team at CERN get credit for inventing original HTTP and associated technologies.

* **HTTP version 0.9:**This was the first version of HTTP which was introduced in 1991.
* **HTTP version 1.0:**In 1996, RFC 1945 (Request For Comments) was introduced in HTTP version 1.0.
* **HTTP version 1.1:**In January 1997, RFC 2068 was introduced in HTTP version 1.1. Improvements and updates to the HTTP version 1.1 standard were released under RFC 2616 in June 1999.
* **HTTP version 2.0:**The HTTP version 2.0 specification was published as RFC 7540 on May 14, 2015.
* **HTTP version 3.0:**HTTP version 3.0 is based on the previous RFC draft. It is renamed as Hyper-Text Transfer Protocol QUIC which is a transport layer network protocol developed by Google.

**Characteristics of HTTP**

HTTP is IP based communication protocol that is used to deliver data from server to client or vice-versa.

* The server processes a request, which is raised by the client, and also server and client know each other only during the current bid and response period.
* Any type of content can be exchanged as long as the server and client are compatible with it.
* Once data is exchanged, servers and clients are no longer connected.
* It is a request and response protocol based on client and server requirements.
* It is a connection-less protocol because after the connection is closed, the server does not remember anything about the client and the client does not remember anything about the server.
* It is a stateless protocol because both client and server do not expect anything from each other but they are still able to communicate.

**Advantages of HTTP**

* Memory usage and CPU usage are low because of fewer simultaneous connections.
* Since there are few TCP connections hence network congestion is less.
* Since handshaking is done at the initial connection stage, then latency is reduced because there is no further need for handshaking for subsequent requests.
* The error can be reported without closing the connection.
* HTTP allows HTTP pipe-lining of requests or responses.

**Disadvantages of HTTP**

* HTTP requires high power to establish communication and transfer data.
* HTTP is less secure because it does not use any encryption method like HTTPS and use TLS to encrypt regular HTTP requests and response.
* HTTP is not optimized for cellular phones and it is too gabby.
* HTTP does not offer a genuine exchange of data because it is less secure.
* The client does not close the connection until it receives complete data from the server; hence, the server needs to wait for data completion and cannot be available for other clients during this time.

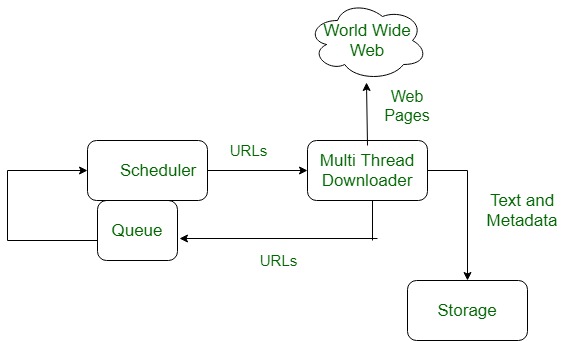
World Wide Web (WWW)

The **World Wide Web** is abbreviated as WWW and is commonly known as the web. The WWW was initiated by CERN (European library for Nuclear Research) in 1989.

WWW can be defined as the collection of different websites around the world, containing different information shared via local servers (or computers).

**History:** It is a project created, by Timothy Berner Lee in 1989, for researchers to work together effectively at CERN. is an organization, named the World Wide Web Consortium (W3C), which was developed for further development of the web. This organization is directed by Tim Berner’s Lee, aka the father of the web.

**System Architecture:** From the user’s point of view, the web consists of a vast, worldwide connection of documents or web pages. Each page may contain links to other pages anywhere in the world. The pages can be retrieved and viewed by using browsers of which internet explorer, Netscape Navigator, Google Chrome, etc are the popular ones. The browser fetches the page requested interprets the text and formatting commands on it, and displays the page, properly formatted, on the screen.



The basic model of how the web works are shown in the figure below. Here the browser is displaying a web page on the client machine. When the user clicks on a line of text that is linked to a page on the abd.com server, the browser follows the hyperlink by sending a message to the abd.com server asking it for the page.

Here the browser displays a web page on the client machine when the user clicks on a line of text that is linked to a page on abd.com, the browser follows the hyperlink by sending a message to the abd.com server asking for the page.

**Working of WWW**

The World Wide Web is based on several different technologies: Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).

A Web browser is used to access web pages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interfaces provided by Web browsers. Initially, Web browsers were used only for surfing the Web but now they have become more universal. Web browsers can be used for several tasks including conducting searches, mailing, transferring files, and much more. Some of the commonly used browsers are Internet Explorer, Opera Mini, and Google Chrome.

**Features of WWW:**

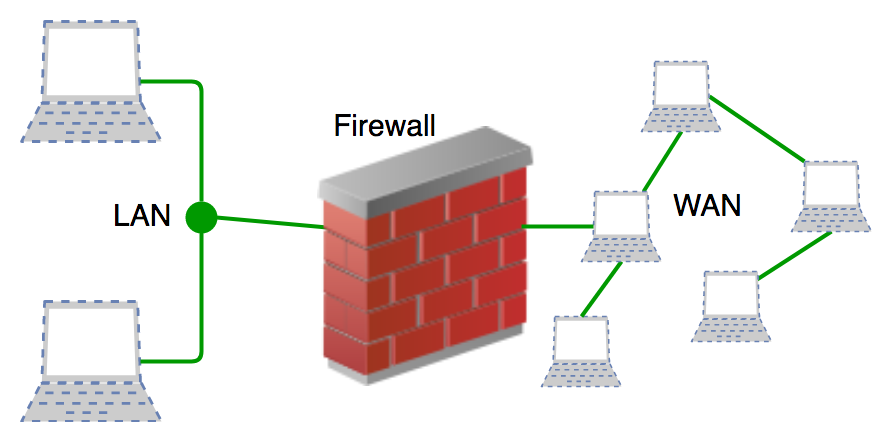
* HyperText Information System
* Cross-Platform
* Distributed
* Open Standards and Open Source
* Uses Web Browsers to provide a single interface for many services
* Dynamic, Interactive and Evolving.
* “Web 2.0”

**Components of the Web:**There are 3 components of the web:

1. **Uniform Resource Locator (URL):** serves as a system for resources on the web.
2. **HyperText Transfer Protocol (HTTP):** specifies communication of browser and server.
3. **Hyper Text Markup Language (HTML):** defines the structure, organisation and content of a webpage.

Firewall

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic. **Accept :** allow the traffic **Reject :** block the traffic but reply with an “unreachable error” **Drop :**block the traffic with no reply A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



**History and Need for Firewall**

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address. But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced. Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

**Work of Firewall**

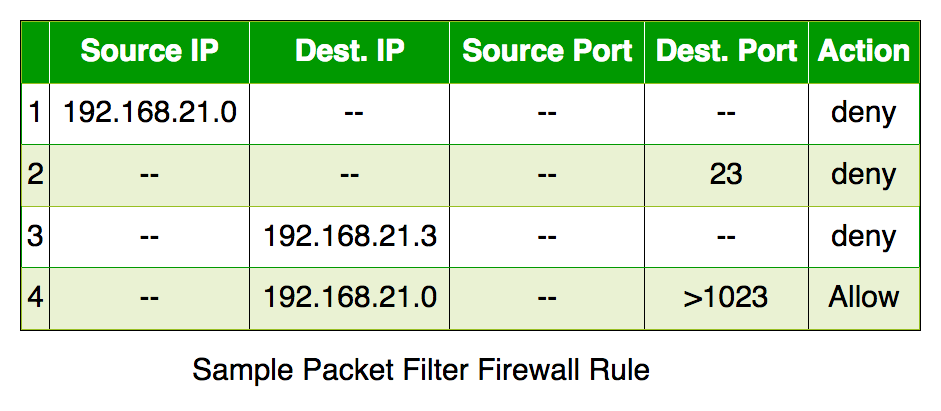
Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

**Default policy:** It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop). Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop*(or reject) is always a good practice.

**Generation of Firewall**

Firewalls can be categorized based on their generation.

1. **First Generation- Packet Filtering Firewall:**Packet filtering firewall is used to control network access by monitoring outgoing and incoming packets and allowing them to pass or stop based on source and destination IP address, protocols, and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers). Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers. Packet filtering firewall maintains a filtering table that decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be filtered according to the following rules:



* Incoming packets from network 192.168.21.0 are blocked.
* Incoming packets destined for the internal TELNET server (port 23) are blocked.
* Incoming packets destined for host 192.168.21.3 are blocked.
* All well-known services to the network 192.168.21.0 are allowed.

1. **Second Generation- Stateful Inspection Firewall:**Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet’s history in the state table.
2. **Third Generation- Application Layer Firewall:**Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused. In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules. *Note: Application layer firewalls can also be used as Network Address Translator(NAT).*
3. **Next Generation Firewalls (NGFW):**Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

**Magic Firewall**

“Magic Firewall” is a term used to describe a security feature provided by the web hosting and security company Cloudflare. It is a cloud-based firewall that provides protection against a wide range of security threats, including DDoS attacks, SQL injections, cross-site scripting (XSS), and other types of attacks that target web applications.

The Magic Firewall works by analyzing traffic to a website and using a set of predefined rules to identify and block malicious traffic. The rules are based on threat intelligence from a variety of sources, including the company’s own threat intelligence network, and can be customized by website owners to meet their specific security needs.

The Magic Firewall is considered “magic” because it is designed to work seamlessly and invisibly to website visitors, without any noticeable impact on website performance. It is also easy to set up and manage, and can be accessed through Cloudflare’s web-based control panel.

Overall, the Magic Firewall is a powerful security tool that provides website owners with an additional layer of protection against a variety of security threats.

**Types of Firewall**

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls:**Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls:**Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

**Advantages of using Firewall**

* **Protection from unauthorized access:** Firewalls can be set up to restrict incoming traffic from particular IP addresses or networks, preventing hackers or other malicious actors from easily accessing a network or system. Protection from unwanted access.
* **Prevention of malware and other threats:**Malware and other threat prevention: Firewalls can be set up to block traffic linked to known malware or other security concerns, assisting in the defense against these kinds of attacks.
* **Control of network access:**By limiting access to specified individuals or groups for particular servers or applications, firewalls can be used to restrict access to particular network resources or services.
* **Monitoring of network activity:** Firewalls can be set up to record and keep track of all network activity. This information is essential for identifying and looking into security problems and other kinds of shady behavior.
* **Regulation compliance:**Many industries are bound by rules that demand the usage of firewalls or other security measures. Organizations can comply with these rules and prevent any fines or penalties by using a firewall.
* **Network segmentation:** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

**Disadvantages of using Firewall**

* **Complexity:**Setting up and keeping up a firewall can be time-consuming and difficult, especially for bigger networks or companies with a wide variety of users and devices.
* **Limited Visibility:**Firewalls may not be able to identify or stop security risks that operate at other levels, such as the application or endpoint level, because they can only observe and manage traffic at the network level.
* **False sense of security:** Some businesses may place an excessive amount of reliance on their firewall and disregard other crucial security measures like endpoint security or intrusion detection systems.
* **Limited adaptability:** Because firewalls are frequently rule-based, they might not be able to respond to fresh security threats.
* **Performance impact:** Network performance can be significantly impacted by firewalls, particularly if they are set up to analyze or manage a lot of traffic.
* **Limited scalability:** Because firewalls are only able to secure one network, businesses that have several networks must deploy many firewalls, which can be expensive.
* **Limited VPN support:**Some firewalls might not allow complex VPN features like split tunneling, which could restrict the experience of a remote worker.
* **Cost:**Purchasing many devices or add-on features for a firewall system can be expensive, especially for businesses.

**Real-Time Applications of Firewall**

1. **Corporate networks:** Many businesses employ firewalls to guard against unwanted access and other security risks on their corporate networks. These firewalls can be set up to only permit authorized users to access particular resources or services and to prevent traffic from particular IP addresses or networks.
2. **Government organizations:**Government organizations frequently employ firewalls to safeguard sensitive data and to adhere to rules like HIPAA or PCI-DSS. They might make use of cutting-edge firewalls like Next-generation firewalls (NGFW), which can detect and stop intrusions as well as manage access to particular data and apps.
3. **Service providers:**Firewalls are used by service providers to safeguard their networks and the data of their clients, including ISPs, cloud service providers, and hosting firms. They might make use of firewalls that accommodate enormous volumes of traffic and support advanced features such as VPN and load balancing.
4. **Small enterprises:** Small firms may use firewalls to separate their internal networks, restrict access to specific resources or applications, and defend their networks from external threats.
5. **Networks at home:**To guard against unwanted access and other security risks, many home users employ firewalls. A firewall that many routers have built in can be set up to block incoming traffic and restrict access to the network.
6. **Industrial Control Systems (ICS):**Firewalls are used to safeguard industrial control systems against illegal access and cyber-attacks in many vital infrastructures, including power plants, water treatment facilities, and transportation systems.