

Computer Networks

Unit V Application Layer

Domain Name Space or Domain Name System in Application Layer

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

Requirement

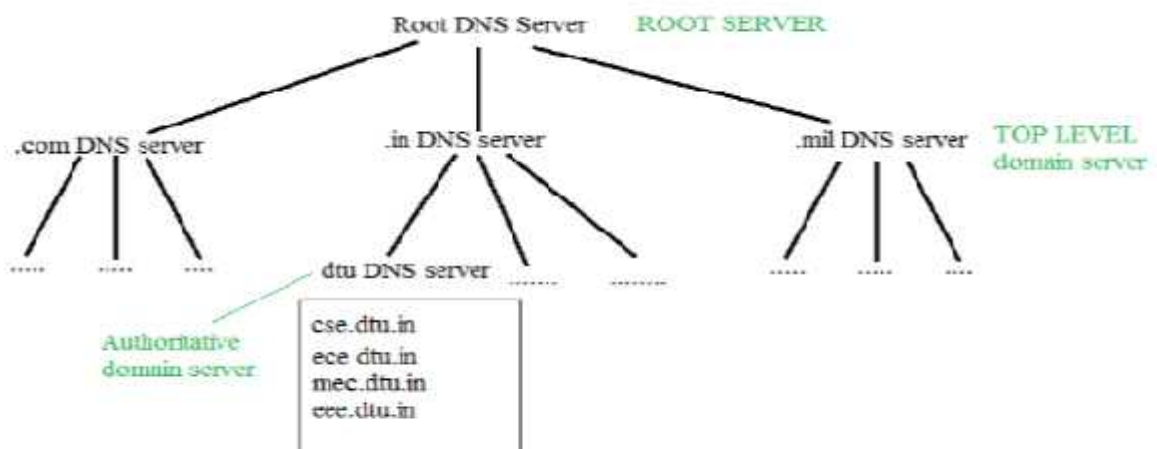
Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Domain :

There are various kinds of DOMAIN :

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

Organization of Domain



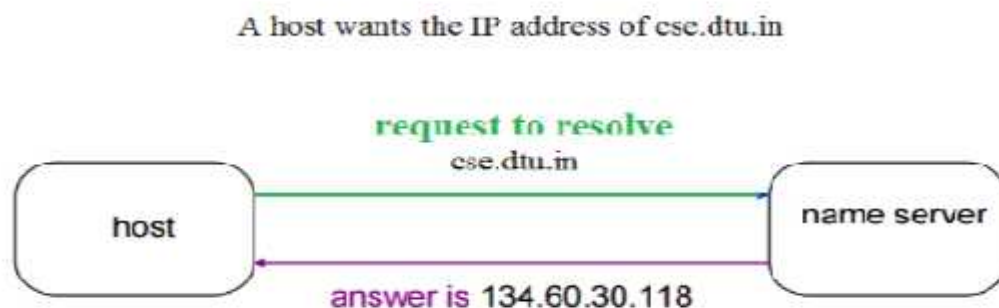
It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately, there should not be a lot of delay for that to happen organization of database is very important.

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 tree like structure.

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

Name server – It is an implementation of the resolution mechanism.. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.

Name to Address Resolution



The host request 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.

Hierarchy of Name Servers

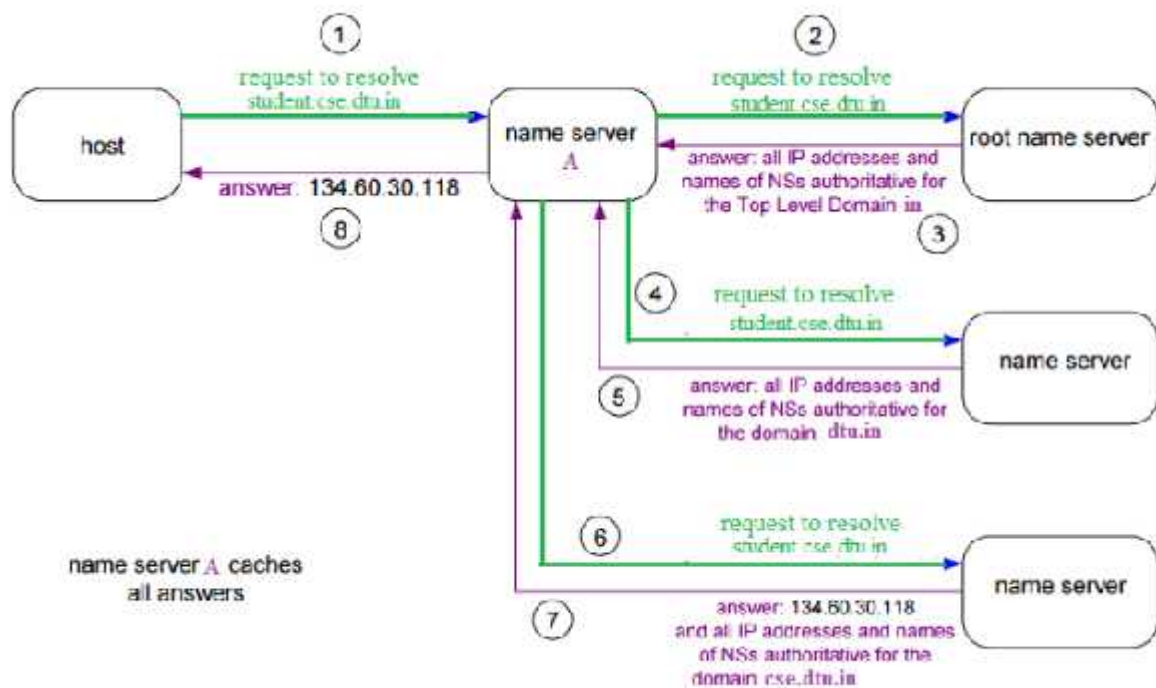
Root name servers – It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.

Top level 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 names and IP addresses of each authoritative name server for the second level domains.

Authoritative name servers This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by 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 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 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 an intermediate or authoritative name server. The root name server can also contain some hostName to IP address mappings. The intermediate name 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.

Dynamic Domain Name Space or System (DDNS)

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. In active 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 :

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 security appliance manufacturers and even required for IP-based security appliances like DVRs.

TELNET:

TELNET stands for **TErminaL NETwork**. It is a type of protocol that enables one computer to connect to local computer. It is used as a standard TCP/IP protocol for virtual terminal service which is given by ISO. Computer which starts connection known as the **local computer**. Computer which is being connected to i.e. which accepts the connection known as **remote computer**. When the connection is established between local and remote computer. During telnet operation whatever that is performing on the remote computer will be displayed by local computer. Telnet operates on client/server principle. Local computer uses telnet client program and the remote computers uses telnet server program.

TELNET Commands :

Commands of the telnet are identified by a prefix character, Interpret As Command (IAC) which is having code 255. IAC is followed by command and option codes. Basic format of the command is as shown in the following figure :



Following are some of the important **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.

Modes of Operation

Most telnet implementation operates in one of the following **three modes** :

Default Mode :

- If there is no other modes are invoked then this mode is used.
- Echoing is performed in this mode by client.
- In this mode, user types a character and client echoes the character on the screen but it does not send it until whole line is completed.

Character Mode :

- Each character typed in this mode is sent by client to server.
- Server in this type of mode is normally echoes character back to be displayed on the client's screen.

Line Mode :

- Line editing like echoing, character erasing etc is done from the client side.
- Client will send the whole line to the server.

Electronic Mail (Email)

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.

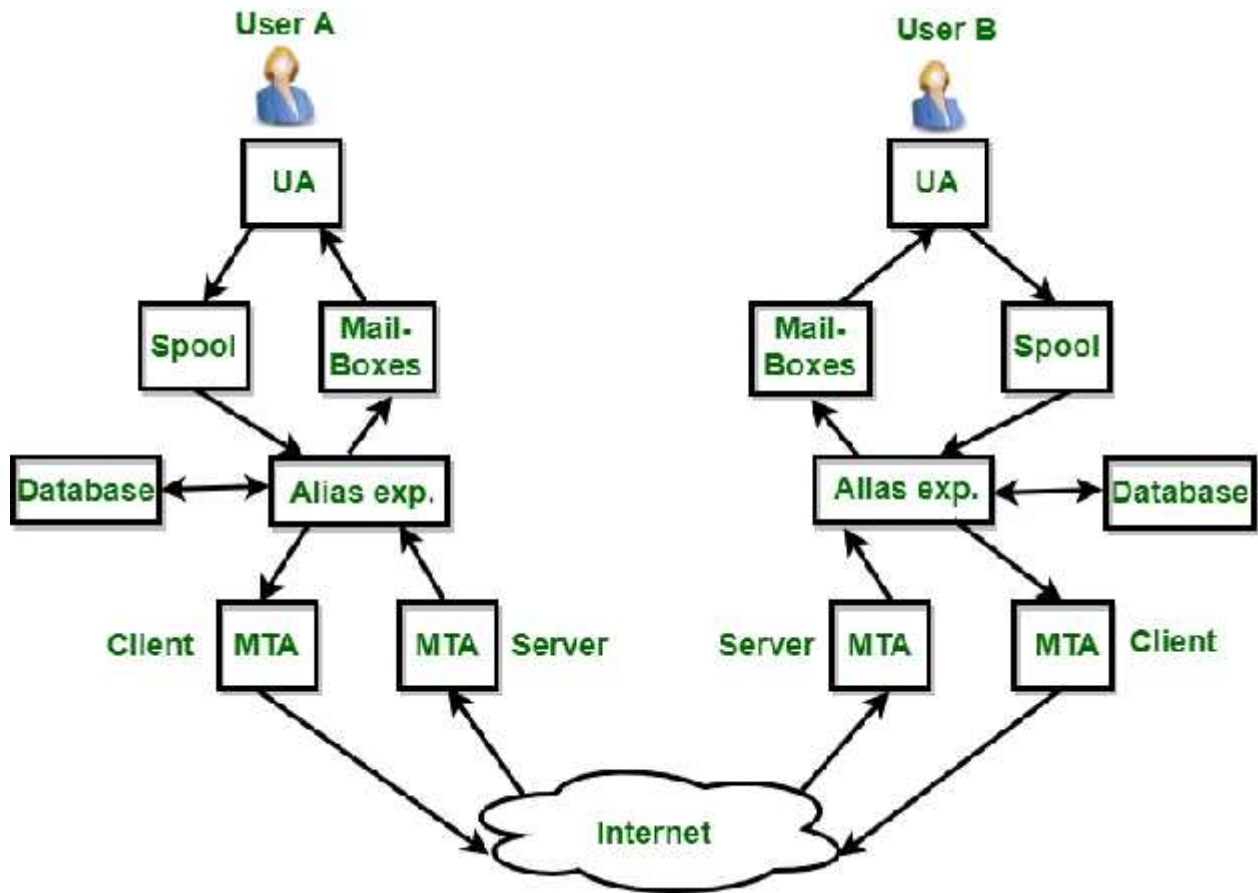
1. User Agent (UA) :

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.



3. 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.

4. 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 sent a message, system checks recipients'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 :

- **Composition –**
A user agent helps the user compose the e-mail message to be sent out. Most user agents provide a template on the screen to be filled in by the user. Some even have a built-in editor that can do spell checking, grammar checking and other tasks expected from a sophisticated word processor. A user could alternatively use his or her favourite text editor or word processor to create the message and import it or cut and paste it, into to the user.
- **Reading Messages –**
The second duty of the user agent is to read the incoming messages. When a user invokes a user agent, it first checks the mail in the incoming mailbox. Most user agents show a one-line summary of each received mail. Each e-mail contains the following fields.
 - 1) A number field
 - 2) A flag field that shows the status of the mail such as new, already read but not replied to or read and replied to.
 - 3) The size of the message.
 - 4) The sender.
 - 5) The optional subject field.
- **Replying to Messages –**
After reading a message, a user can use the user agent to reply to a message. A user agent usually allows the user to reply to the original sender or to reply to all recipients of the message. The reply message may contain the original message (for quick reference) and the new message.
- **Forwarding Messages –**
Replying is defined as sending a message to the sender or recipients of the copy. Forwarding is defined as sending the message to a third party. A user agent allows the receiver to forward the message, with or without extra comments, to a third party.
- **Handling Mailboxes –**
A user agent normally creates two mailboxes: an inbox and an outbox. Each box is a file with a special format that can be handled by the user agent. The inbox keeps all the the received e-mails until they are deleted by the user. The outbox keeps all the sent e-mails until the user deletes them. Most user agents today are capable of creating customized mailboxes.
- **Transfer –**
Transfer means sending procedure of mail i.e. from the sender to recipient.
- **Reporting –**
Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
- **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

There are many advantages of email, which are as follows:

- **Cost-effective:** Email is a very cost-effective service to communicate with others as there are several email services available to individuals and organizations for free of cost. Once a user is online, it does not include any additional charge for the services.
- Email offers users the benefit of accessing email from anywhere at any time if they have an Internet connection.
- Email offers you an incurable communication process, which enables you to send a response at a convenient time. Also, it offers users a better option to communicate easily regardless of different schedules users.
- **Speed and simplicity:** Email can be composed very easily with the correct information and contacts. Also, minimum lag time, it can be exchanged quickly.
- **Mass sending:** You can send a message easily to large numbers of people through email.
- Email exchanges can be saved for future retrieval, which allows users to keep important conversations or confirmations in their records and can be searched and retrieved when they needed quickly.
- Email provides a simple user interface and enables users to categorize and filter their messages. This can help you recognize unwanted emails like junk and spam mail. Also, users can find specific messages easily when they are needed.
- As compared to traditional posts, emails are delivered extremely fast.
- Email is beneficial for the planet, as it is paperless. It reduces the cost of paper and helps to save the environment by reducing paper usage.
- It also offers a benefit to attaching the original message at the time you reply to an email. This is beneficial when you get hundreds of emails a day, and the recipient knows what you are talking about.
- Furthermore, emails are beneficial for advertising products. As email is a form of communication, organizations or companies can interact with a lot of people and inform them in a short time.

Disadvantages of Email

- **Impersonal:** As compared to other forms of communication, emails are less personal. For example, when you talk to anyone over the phone or meeting face to face is more appropriate for communicating than email.
- **Misunderstandings:** As email includes only text, and there is no tone of voice or body language to provide context. Therefore, misunderstandings can occur easily with email. If someone sends a joke on email, it can be taken seriously. Also, well-meaning information can be quickly typed as rude or aggressive that can impact wrong. Additionally, if someone types with short abbreviations and descriptions to send content on the email, it can easily be misinterpreted.
- **Malicious Use:** As email can be sent by anyone if they have an only email address. Sometimes, an unauthorized person can send you mail, which can be harmful in terms of stealing your personal information. Thus, they can also use email to spread gossip or false information.
- **Accidents Will Happen:** With email, you can make fatal mistakes by clicking the wrong button in a hurry. For instance, instead of sending it to a single person, you can accidentally send sensitive information to a large group of people. Thus, the information can be disclosed, when you have clicked the wrong name in an address list. Therefore, it can be harmful and generate big trouble in the workplace.
- **Spam:** Although in recent days, the features of email have been improved, there are still big issues with unsolicited advertising arriving and spam through email. It can easily become overwhelming and takes time and energy to control.
- **Information Overload:** As it is very easy to send email to many people at a time, which can create information overload. In many modern workplaces, it is a major problem where it is required to move a lot of information and impossible to tell if an email is important. And, email needs organization and upkeep. The bad feeling is one of the other problems with email when you returned from vacation and found hundreds of unopened emails in your inbox.
- **Viruses:** Although there are many ways to travel viruses in the devices, email is one of the common ways to enter viruses and infect devices. Sometimes when you get a mail, it might be the virus come with an attached document. And, the virus can infect the system when you click on the email and open the attached link. Furthermore, an anonymous person or a trusted friend or contact can send infected emails.

- **Pressure to Respond:** If you get emails and you do not answer them, the sender can get annoyed and think you are ignoring them. Thus, this can be a reason to make pressure on your part to keep opening emails and then respond in some way.
- **Time Consuming:** When you get an email and read, write, and respond to emails that can take up vast amounts of time and energy. Many modern workers spend their most time with emails, which may be caused to take more time to complete work.
- **Overlong Messages:** Generally, email is a source of communication with the intention of brief messages. There are some people who write overlong messages that can take much time than required.
- **Insecure:** There are many hackers available that want to gain your important information, so email is a common source to seek sensitive data, such as political, financial, documents, or personal messages. In recent times, there have been various high-profile cases occurred that shown how email is insecure about information theft.

Different types of Email

There are many types of email; such are as follows:

Newsletters: It is studied by Clutch, the newsletter is the most common type of email that are routinely sent to all mailing list subscribers, either daily, weekly, or monthly. These emails often contain from the blog or website, links curated from other sources, and selected content that the company has recently published. Typically, Newsletter emails are sent on a consistent schedule, and they offer businesses the option to convey important information to their client through a single source. Newsletters might also incorporate upcoming events or new, webinars from the company, or other updates.

Lead Nurturing: Lead-nurturing emails are a series of related emails that marketers use to take users on a journey that may impact their buying behavior. These emails are typically sent over a period of several days or weeks. Lead-nurturing emails are also known as trigger campaigns, which are used for solutions in an attempt to move any prospective sale into a completed purchase and educate potential buyers on the services. These emails are not only helpful for converting emails but also drive engagement. Furthermore, lead-nurturing emails are initiated by a potential buyer taking initial action, such as clicking links on a promotional email or downloading a free sample.

Promotional emails: It is the most common type of B2B (Business to Business) email, which is used to inform the email list of your new or existing products or services. These types of emails contain creating new or repeat customers, speeding up the buying process, or encouraging contacts to take some type of action. It provides some critical benefits to buyers, such as a free month of service, reduced or omitted fees for managed services, or percentage off the purchase price.

Standalone Emails: These emails are popular like newsletters emails, but they contain a limitation. If you want to send an email with multiple links or blurbs, your main call-to-action can weaken. Your subscriber may skip your email and move on, as they may click on the first link or two in your email but may not come back to the others.

Onboarding emails: An onboarding email is a message that is used to strengthen customer loyalty, also known as post-sale emails. These emails receive users right after subscription. The onboarding emails are sent to buyers to familiarize and educate them about how to use a product effectively. Additionally, when clients faced with large-scale service deployments, these emails help them facilitate user adoption.

Transactional: These emails are related to account activity or a commercial transaction and sent from one sender to one recipient. Some examples of transactional email are purchase confirmations, password reminder emails, and personalized product notifications. These emails are used when you have any kind of e-commerce component to your business. As compared to any other type of email, the transactional email messages have 8x the opens and clicks.

Plain-Text Emails: It is a simple email that does not include images or graphics and no formatting; it only contains the text. These types of emails may worth it if you try to only ever send fancy formatted emails, text-only messages. According to HubSpot, although people prefer fully designed emails with various images, plain text emails with less HTML won out in every A/B test. In fact, HTML emails contain lower open and click-through rates, and plain text emails can be great for blog content, event invitations, and survey or feedback requests. Even if you do not send plainer emails, but you can boost your open and click through rates by simplifying your emails and including fewer images.

Welcome emails: It is a type of B2B email and common parts of onboarding emails that help users get acquainted with the brand. These emails can improve subscriber constancy as they include additional information, which helps to the new subscriber in terms of a business objective. Generally, welcome emails are sent buyers who got a subscription to a business's opt-in activities, such as a blog, mailing list, or webinar. Also, these emails can help businesses to build a better relationship between customers.

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.

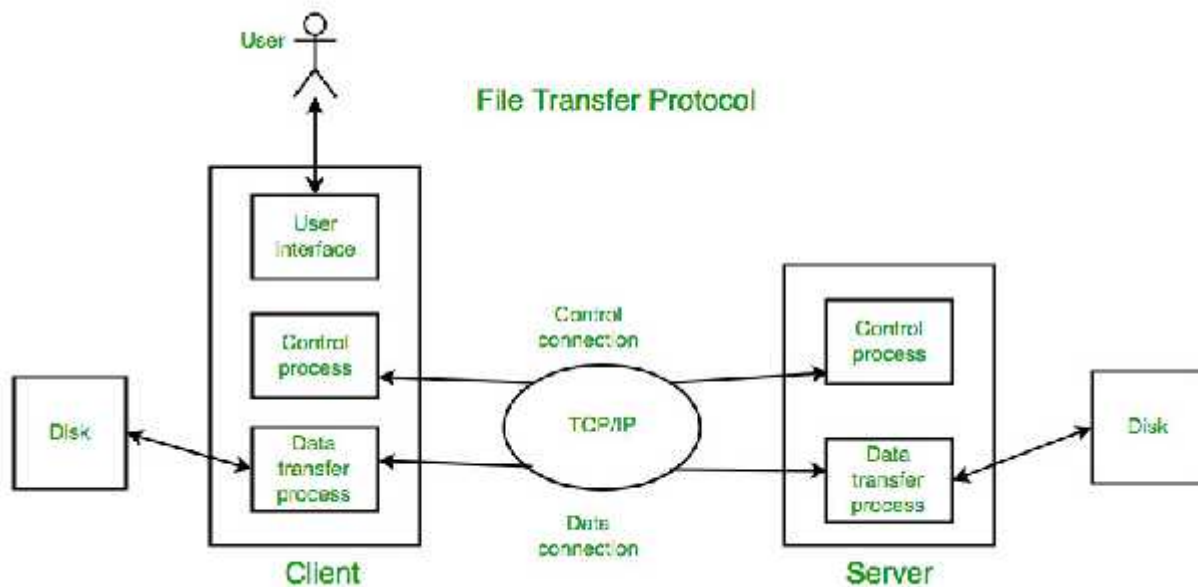
MIME Header:

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.

File Transfer Protocol (FTP)

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



What is 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 control connection. The control connection is initiated on port number 21.

What is data connection?

For sending the actual file, FTP makes use of 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 a 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.

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 to send the requested file over the data connection.

STOR – This command causes to store a file into 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.

Trivial File Transfer Protocol (TFTP): It is also file transfer protocol without sophisticated features of FTP.

- It is good for simple file transfers, such as during boot time.
- It uses UDP as transport layer protocols. 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

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 password 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.

World Wide Web (WWW)

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

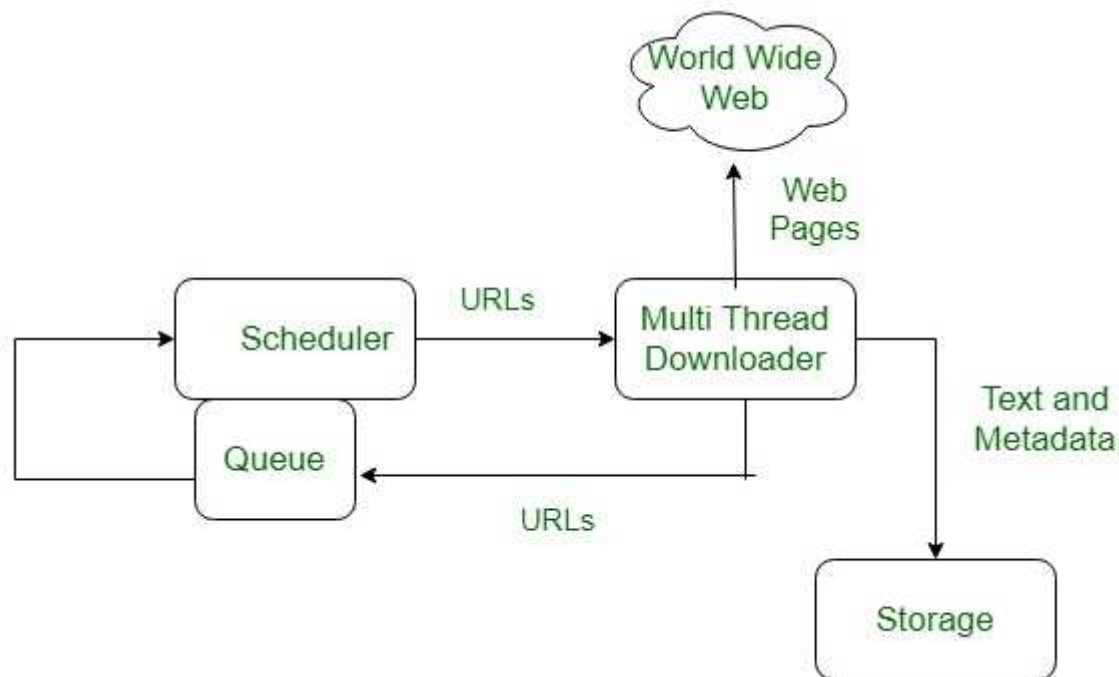
History:

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

System Architecture:

From 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 is shown in 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 displaying 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 vbrowser follows the hyperlink by sending a message to abd.com server asking it 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).

An Web browser is used to access webpages. 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 interface 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, 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 Web

There are 3 components of web:

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

Hyper Text Transfer Protocol (HTTP)

HTTP stands for HyperText Transfer Protocol. It is invented by **Tim Berner**. HyperText is the type of text which is specially coded with the help of some standard coding language called as HyperText Markup Language (HTML).

The protocols that are used to transfer hypertext between two computers is known as HyperText Transfer Protocol.

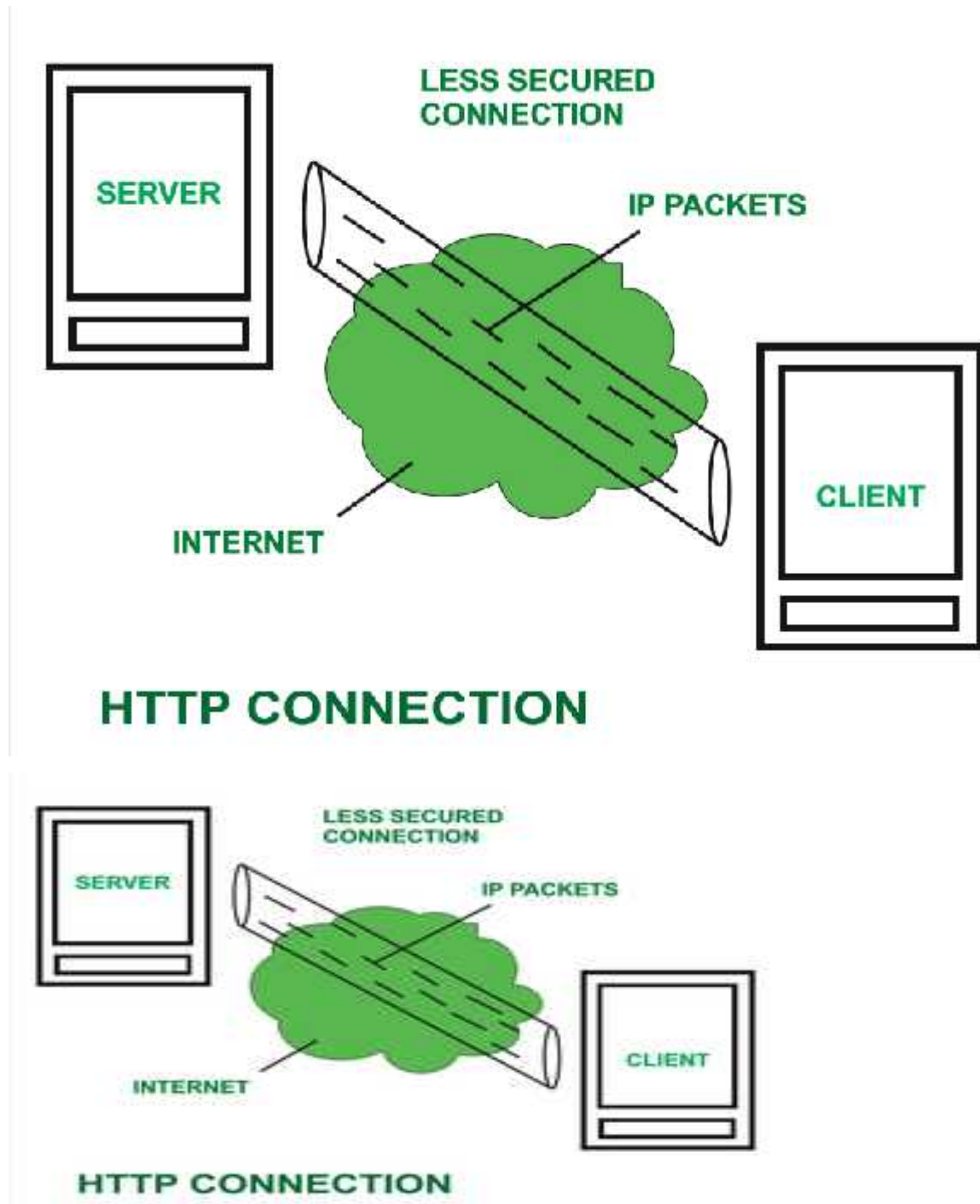
HTTP provides standard between a web browser and web server to establish communication. It is set of rules for transferring data from one computer to another. Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, user will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

How it works ?

First of all, whenever we want to open any website then first we open web browser after that we will type 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,

then DNS will return IP address to web browser corresponding to this URL. Now browser is able to send request to actual server.

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



History ::

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

1. **HTTP version 0.9 –**

This was first version of HTTP which was introduced in 1991.

2. **HTTP version 1.0 –**

In 1996, RFC 1945 (Request For Comments) was introduced in HTTP version 1.0.

3. **HTTP version 1.1 –**

In January 1997, RFC 2068 was introduced in HTTP version 1.1. Improvements and updates to HTTP version 1.1 standard were released under RFC 2616 in June 1999.

4. **HTTP version 2.0 –**

The HTTP version 2.0 specification was published as RFC 7540 on May 14, 2015.

5. **HTTP version 3.0 –**

HTTP version 3.0 is based on previous RFC draft. It is renamed as HyperText Transfer Protocol QUIC which is a transport layer network protocol developed by Google.

Characteristics of HTTP :

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

1. Server processes a request, which is raised by client and also server and client knows each other only during current request and response period.
2. Any type of content can be exchanged as long as server and client are compatible with it.
3. Once data is exchanged then servers and client are no more connected with each other.
4. It is a request and response protocol based on client and server requirements.
5. It is connection less protocol because after connection is closed, server does not remember anything about client and client does not remember anything about server.
6. It is stateless protocol because both client and server does not expecting anything from each other but they are still able to communicate.

Advantages :

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

Disadvantages :

- HTTP requires high power to establish communication and transfer data.
- HTTP is less secure, because it does not uses any encryption method like https use TLS to encrypt normal http requests and response.
- HTTP is not optimized for cellular phone and it is too gabby.
- HTTP does not offer genuine exchange of data because it is less secure.

- Client does not close connection until it receives complete data from server and hence server needs to wait for data completion and cannot be available for other clients during this time.

Simple Network Management Protocol (SNMP)

If an organization has 1000 of 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 which 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 centralised 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, router, switches, servers etc.
3. **Management Information Base –**
MIB consists of information of resources that are to be managed. These information is organised 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 SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.
2. **GetNextRequest –**
This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continuously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.
3. **GetBulkRequest –**
This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.
4. **SetRequest –**
It is used by SNMP manager to set the value of an object instance on the SNMP agent.

5. **Response** –

It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.

6. **Trap** –

These are the message send 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 set trap continuously until it receives an Inform message. It is same as trap but adds an acknowledgement that trap doesn't provide.

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:

1. **noAuthNoPriv** –

This (no authentication, no privacy) security level uses community string for authentication and no encryption for privacy.

2. **authNopriv** – This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.

3. **authPriv** – This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses DES-56 algorithm.

SNMP versions –

There are 3 versions of SNMP:

1. **SNMPv1** –

It uses community strings for authentication and use 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, conclusion is the higher the version of SNMP, more secure it will be.

Bluetooth

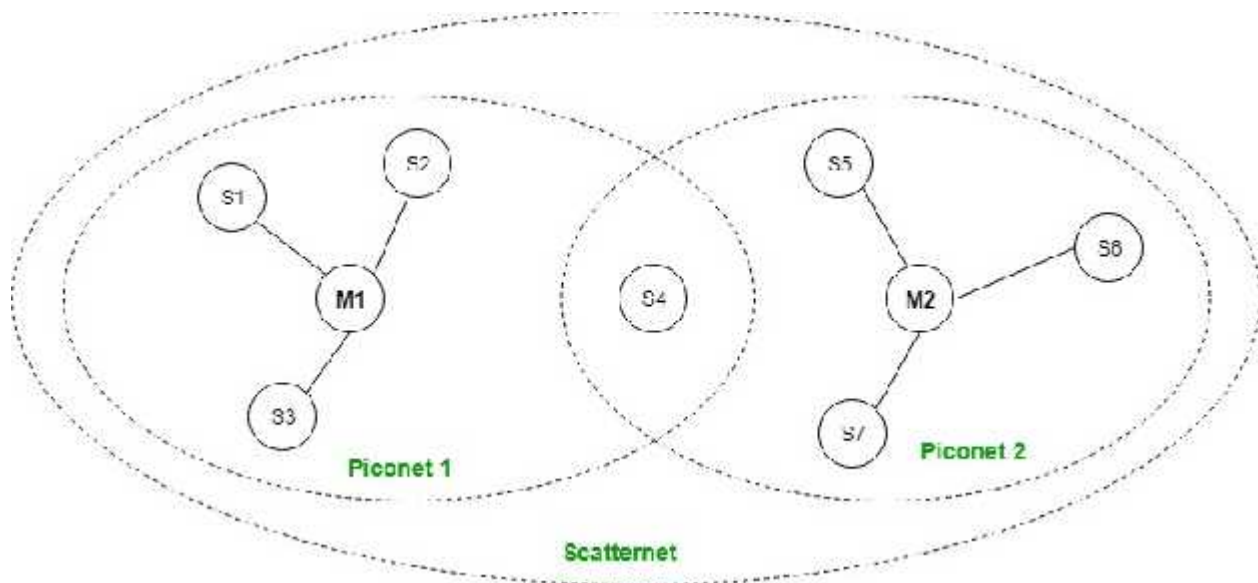
It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected 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). 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:

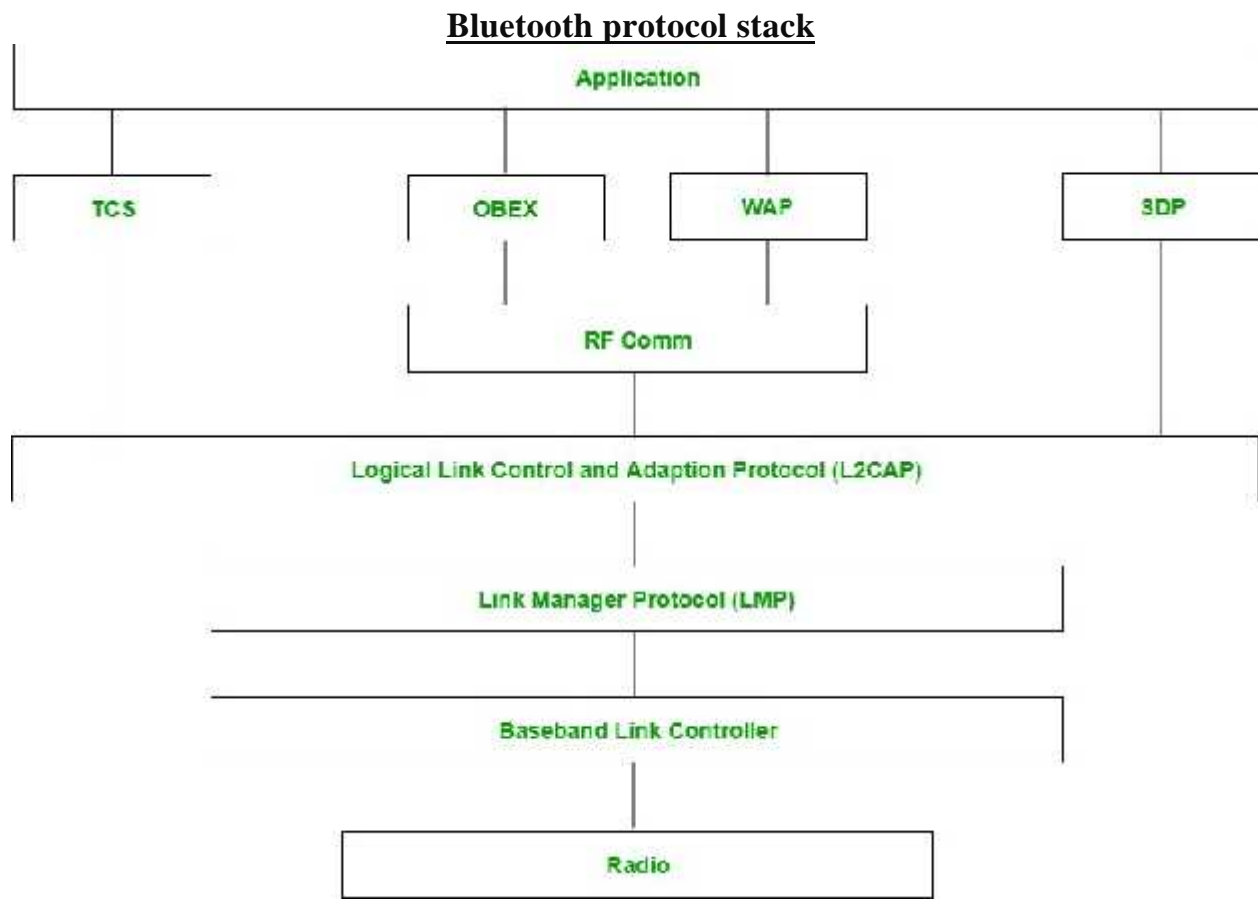
- 1) **Piconet**
- 2) **Scatternet**



Piconet 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.



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.

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.

Firewalls

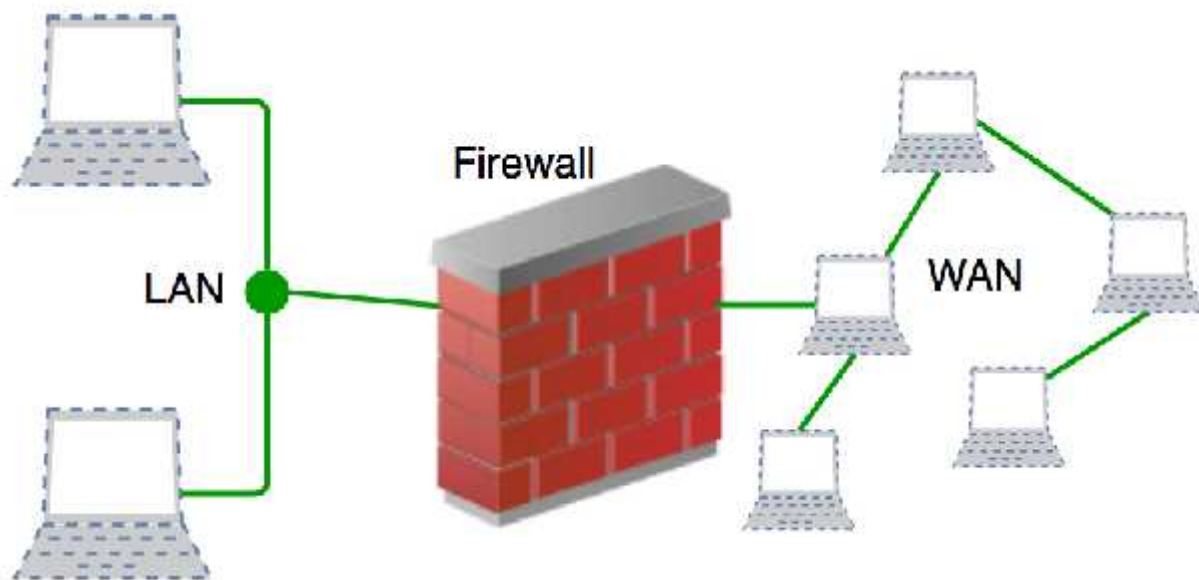
A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

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.

How Firewall Works

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.

Generations of Firewall

Firewalls can be categorized based on its generation.

1. **First Generation- Packet Filtering Firewall :** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet 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 which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to following rules:

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.

2. Incoming packets destined for internal TELNET server (port 23) are blocked.
 3. Incoming packets destined for host 192.168.21.3 are blocked.
 4. All well-known services to the network 192.168.21.0 are allowed.
2. **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.
3. **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).
4. **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.

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.

Basic concepts of Cryptography

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:

1. Symmetric Key Cryptography:

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

2. Hash Functions:

There is no usage of any key in this algorithm. A hash value with fixed length is

calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3. **Asymmetric Key Cryptography:**

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.