A Report on

“APPLICATION LAYER PROTOCOL”

DIPLOMA IN
INFORMATION TECHNOLOGY

SUBMITTED BY

Sr. No.	Enrollment No.	Roll No.	Name of the Student
1	1912260156	2605	BHUMIKA BET
2	1912260178	2627	VAISHNAVI FULPATI
3	1912260179	2628	PRERNA GAIKWAD
4	1912260187	2636	POOJA NAMA
5	1912260200	2650	AKHILA VAGGU

DEPARTMENT OF INFORMATION TECHNOLOGY

SHRI SIDDHESHWAR WOMEN’S

POLYTECHNIC,

SOLAPUR -413 002

Academic Year 2020-2021

Maharashtra State Board of Technical Education,Mumbai

Shri Siddheshwar Women's Polytechnic

Accredited and Reaccredited by NBA, New Delhi
T. P. II, Plot No. 74, Bhawani Peth, Rupa Bhawani Mandir Road, Solapur.

CERTIFICATE

This is to certify that the Micro Project report
on

"APPLICATION LAYER PROTOCOL"

has successfully completed in **COMPUTER NETWORK(CNE)** subject by the Student of fourth semester Diploma in Information Technology for the Academic Year 2020-2021 as prescribed in the "I-Scheme Curriculum" designed by MSBTE, Mumbai.

Submitted By

Sr. No.	Enrollment No.	Roll No.	Name of the Student
1	1912260156	2605	BHUMIKA BET
2	1912260178	2627	VAISHNAVI FULPATI
3	1912260179	2628	PRERNA GAIKWAD
4	1912260187	2636	POOJA NAMA
5	1912260200	2650	AKHILA VAGGU

Under the Guidance of
Ms.Mutha R.D.
(IT Dept)

Ms.Mutha R.D.	**Ms. Alange N.S.**	**Prof. Dharane G.R.**
Guide	**H. O. D.**	**Principal**

❖ Application Layer Protocols

What is application layer?

The Application Layer is the seventh layer of the seven-layer OSI model. Application layer interface directly interacts with the application and provides common web application services. The application layer also makes a request to the presentation layer. Application layer is the highest level of open systems, providing services directly for the application process.

The Application layer includes the following functions:

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

➢ Services of Application Layers

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

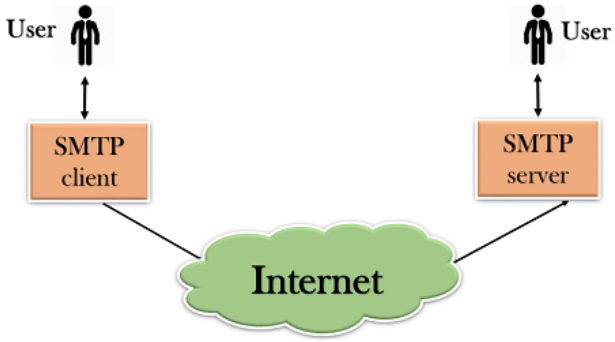
➢ Application layer protocol features:

- Define the process for both parties to the communication.
- Define the message type.
- Define the syntax of the message.
- Definition of the meaning of any informational field.
- Define the way to send the message and the expected response.
- Define interaction with the next level.

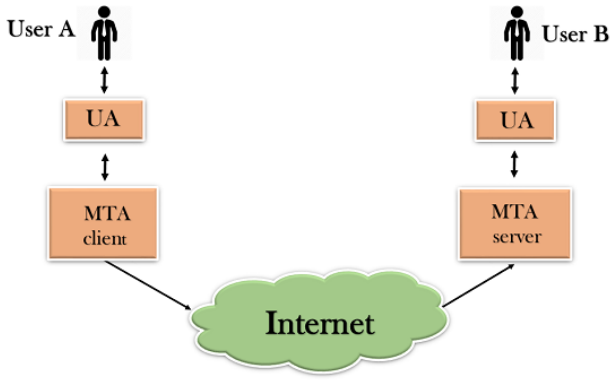
1. SMTP (Simple Mail Transfer Protocol):

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

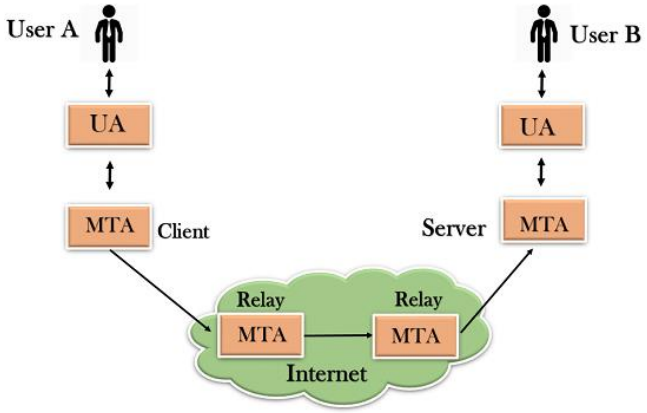
➢ Components of SMTP



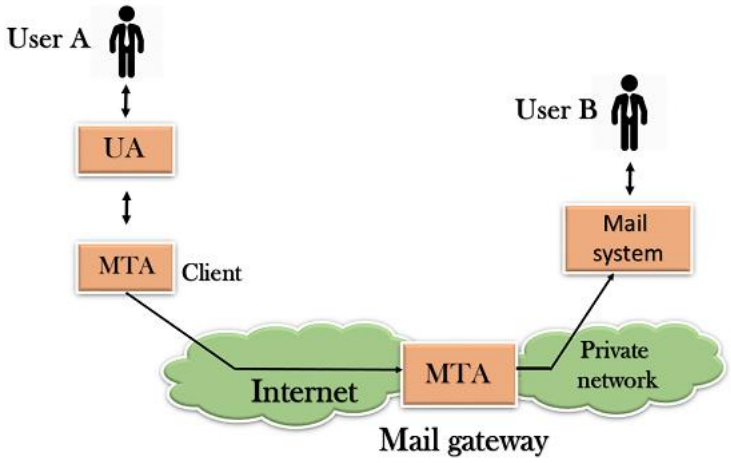
- First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.



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



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



➢ Working of SMTP

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

➢ Advantages of SMTP:

- All you have to do is use your credentials and it will work.
- In case of failure, the message will include an explanation about why email failed to be delivered.
- It is extremely easy to start using mail for your transactional emails. All you have to do is exchange ceremonial and you are set to go. Unlike with API, where coding is required.

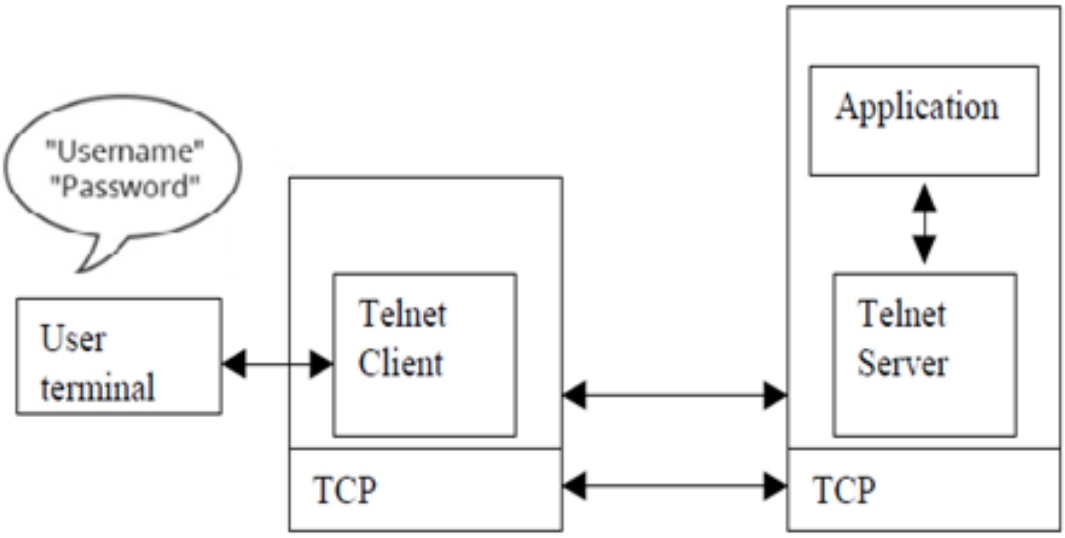
➢ Disadvantages of SMTP:

- Some firewalls can block port commonly used with SMTP.
- Security matter for SMTP is worse.
- Transmission of binary files using SMTP is not possible without converting it into text files. Use MIME to send mail in another format.
- It is usefulness is limited by its simplicity.
- It is limited to only 7 bit ASCII characters.

- SMTP servers may reject all mail messages beyond some specific length.
- Usually require more back and worth conversion between servers in order to deliver your message, Which can delay sending and also increase the chance of the message not being delivered.

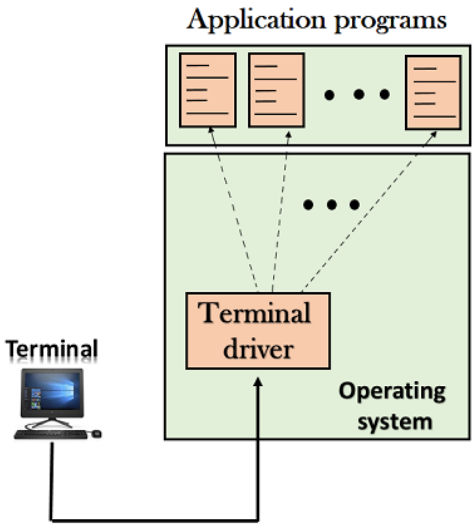
2. TELNET (Terminal Network):

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



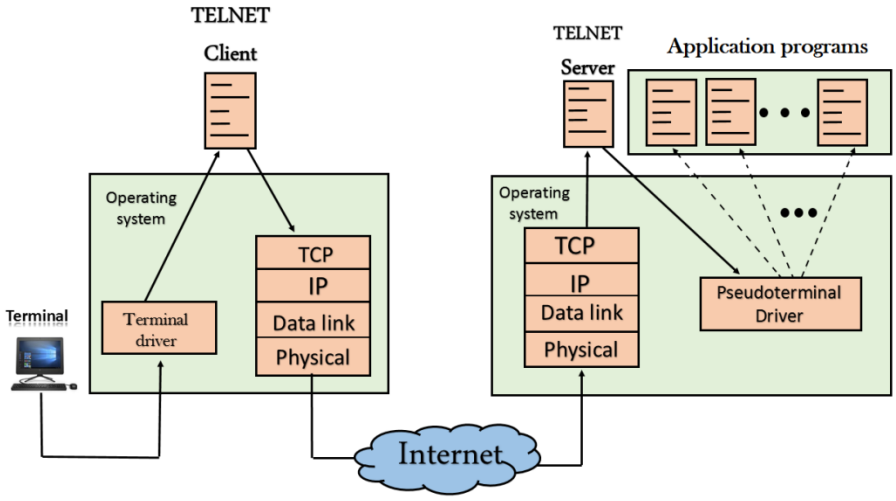
➢ There are two types of login:

I. Local Login



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

II. Remote login



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

- **How remote login occurs**

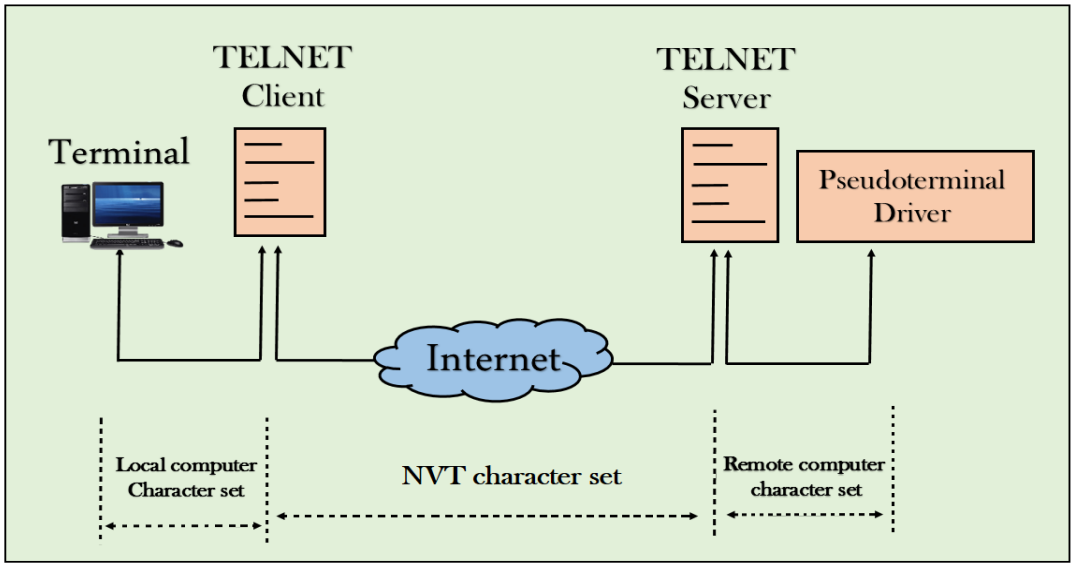
At the local site

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

At the remote site

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

Network Virtual Terminal (NVT)



The network virtual terminal is an interface that defines how data and commands are sent across the network.

- In today's world, systems are heterogeneous. For example, the operating system accepts a special combination of characters such as end-of-file token running a DOS operating system *ctrl+z* while the token running a UNIX operating system is *ctrl+d*.

- TELNET solves this issue by defining a universal interface known as network virtual interface.
- The TELNET client translates the characters that come from the local terminal into NVT form and then delivers them to the network. The Telnet server then translates the data from NVT form into a form which can be understandable by a remote computer.

➢ Advantages of TELNET:

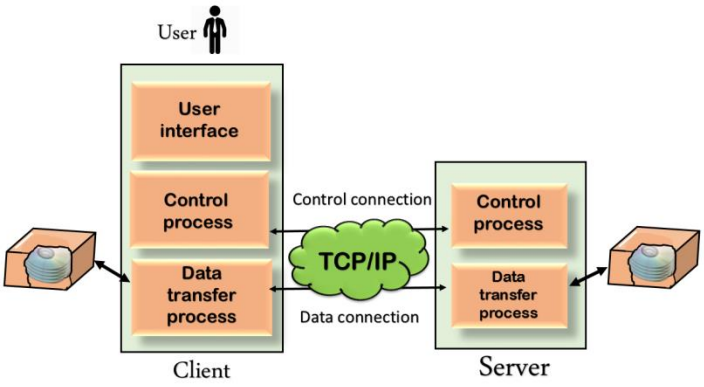
- Telnet protocol can be servers,and clients implement a network virtual terminal(NVT).
- It helps in the administration to work over the net.
- Telnet can be send /receive computer information over the command.
- Telnet can support user confirmation.

➢ Disadvantage of TELNET:

- In the Telnet protocol,User ID and Password can be transmitted encryption command.
- There are chances of risk security in Telnet protocol as snooping eavesdropping are laid-back by hackers or intruders.
- It is very ineffective protocol on the internet.
- It is costly as per slow typing speeds.

3. FTP (File Transfer Protocol):

- FTP is the standard mechanism provided by TCP/IP for copying a file from one host to another.
- FTP differs form other client-server applications because it establishes 2 connections between hosts.
- Two connections are: Data Connection and Control Connection.
- Data Connection uses PORT 20 for the purpose and control connection uses PORT 21 for the purpose.
- FTP is built on a client-server architecture and uses separate control and data connections between the client and the server.
- One connection is used for data transfer, the other for control information (commands and responses).
- It transfer data reliably and efficiently.



➢ Advantages of FTP:

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

➢ Disadvantages of FTP:

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

4. HTTP (Hypertext Transfer Protocol):

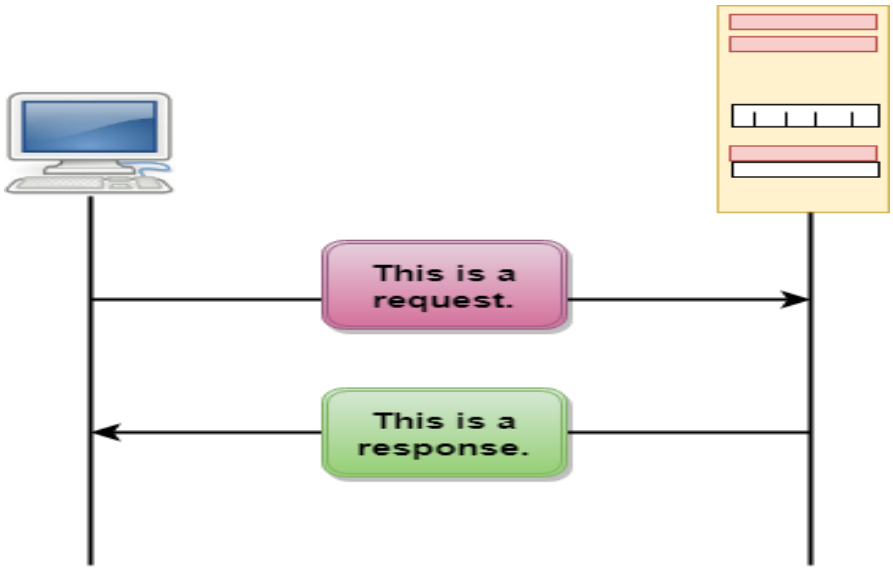
- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.

- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

➢ Features of HTTP:

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

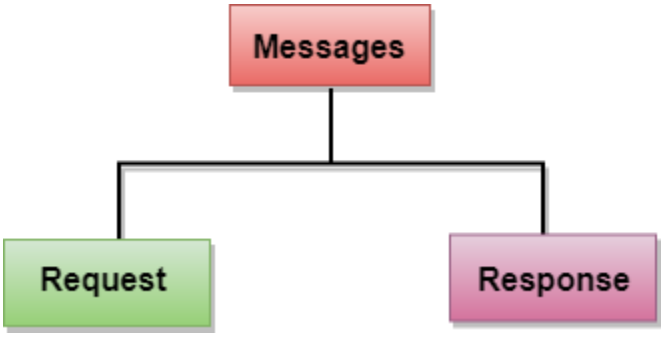
- **HTTP Transactions**



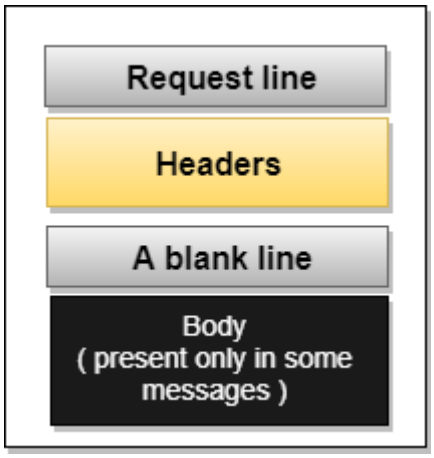
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

- **Messages**

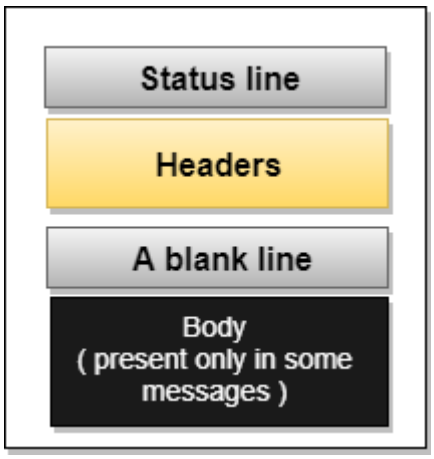
HTTP messages are of two types: request and response. Both the message types follow the same message format.



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



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



- **Uniform Resource Locator (URL)**

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

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

➢ Advantages of HTTP:

1. Addressing
HTTP uses advanced scheme of addressing. It assigns IP address with recognizable names so that it can be identified easily in the World Wide Web. Compared to the standard procedure of IP address with a series of numbers, using this the public can easily engage with the internet.

2. Flexibility
Whenever there are additional capabilities needed by an application, HTTP has the capability to download extensions or plugins and display the relevant data. These can include Flash players and Acrobat reader.

3. Security
In HTTP each files is downloaded from an independent connection and then gets closed. Due to this no more than one single element of a webpage gets transferred. Therefore, the chance of interception during transmission is minimized here.

➢ Disadvantages of HTTP:

1. Data Integrity
Since there are no any encryption methods used in HTTP, there are chances of someone altering the content. That is the reason why HTTP is considered to be an insecure method prone to data integrity.

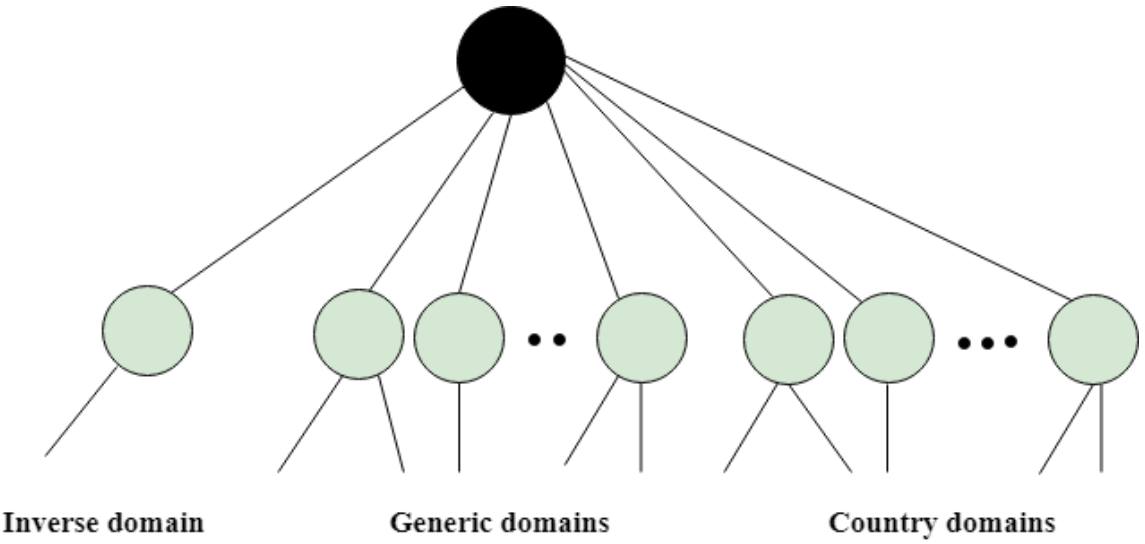
2. Data Privacy
Privacy is another problem faced in a HTTP connection. If any hacker manages to intercept the request they can view all the content present in the web page. Besides that they can also gather confidential informations such as the username and the password.

3. Server Availability
Even if HTTP receives all the data that it needs, clients does not take measures to close the connection. Therefore, during this time period, server will not be present.

5. DNS(Domain Name System):

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

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



- **Generic Domains**

o It defines the registered hosts according to their generic behavior.

o Each node in a tree defines the domain name, which is an index to the DNS database.

o It uses three-character labels, and these labels describe the organization type.

- **Country Domain**

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

- **Inverse Domain**

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

➢ Working of DNS

o DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.

o Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.

o DNS implements a distributed database to store the name of all the hosts available on the internet.

o If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a

hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

➢ Advantages of DNS:

1. Generally DNS is the only system in the entire world that can help you browse the internet. With the internet becoming an integral part of the society, it has increasingly become important that DNS Servers remain maintained. Without them, then the internet would not exist.
2. No need for memorizing IP addresses -DNS servers provide a nifty solution of converting domain or sub domain names to IP addresses. Imagine how it would feel having to memorize the IP addresses of twitter, Facebook, Google or any other site that you normally frequent on a daily basis. It would definitely be horrific. Its system also makes it easy for search engines to be able to categorize and archive information.
3. Security enhancement -DNS servers are an important component for the security of your home or work connections. DNS servers that have been designed for security purposes usually ensure that attempts to hack your server environment are thwarted before entry into your machines. However, it's important to note that the word used is enhanced. This means that you will need other security measures put in place to protect your data, especially if it's a large organization with tons of sensitive data.
4. DNS servers have fast internet connections -People and organizations that use DNS servers can be able to take advantage of high connection speeds that are a key feature in some of these servers.

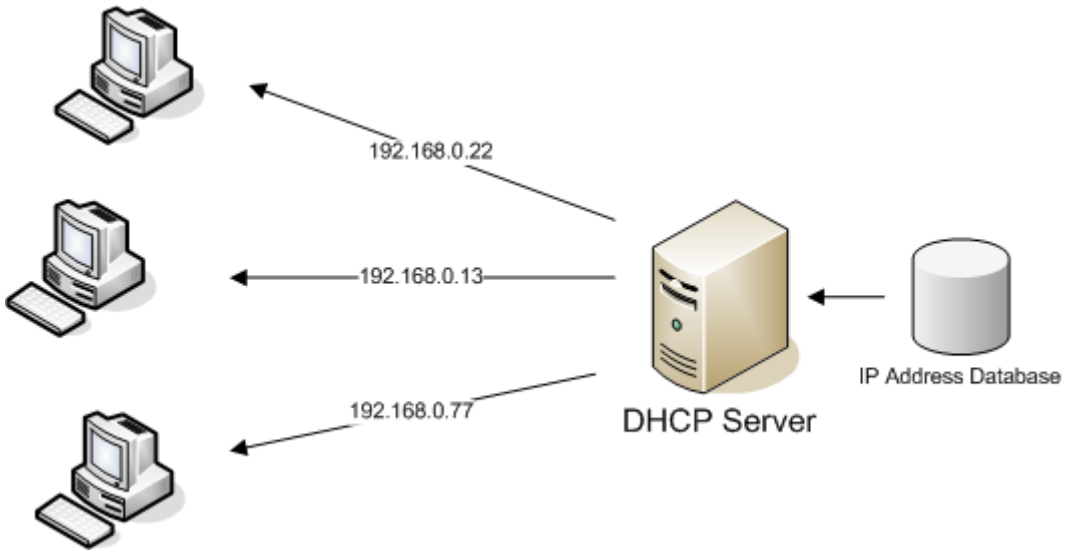
➢ Disadvantages of DNS:

1. One of the main disadvantages of the DNS is the fact that its registry can only be controlled ICANN, a non-profit organisation with roots tied in one country. This challenges the concept of net neutrality and has been a widely propagated argument over the last three decades.
2. DNS queries usually don't carry any information about the clients who initiated it. This is one of the reasons why DNS has been popular among hackers. This is because the server side will only see the IP address from where the query came from and which can at times be manipulated by hackers.
3. DNS servers are based on the principle of a slave-master relationship. This means that if the master server is broken or manipulated in any way, then it will be hard to access the web page or database that was hosted on the server. Hackers have also used this to their advantage. By targeting the server machine and making redirects to other pages, they have been able to find ways of phishing information.

6. DHCP(Dynamic Host Configuration Protocol):

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.



- **DHCP does the following:**

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

➢ How DHCP works

DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

• Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components:

- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

➢ Advantages of DHCP:

- Centralized management of IP address
- Ease adding new clients to the network
- Reuse of IP address
- This implementation does not require any addition black

➢ Disadvantages of DHCP:

- As DHCP server as secure mechanism for authentication of clinet,it can gain unauthorized access to IP addresses.
- The meachine itself does not change the name when IP address is assigned.
- Client is not able to access the network in the absence DHCP server.

7. BOOTP(Bootstrap Protocol):

The Bootstrap Protocol (BOOTP) enables a client workstation to initialize with a minimal IP stack and request its IP address, a gateway address, and the address of a name server from a BOOTP server.

If BOOTP is to be used in your network, the server and client are usually on the same physical LAN segment. BOOTP can only be used across bridged segments when source-routing bridges are being used, or across subnets, if you have a router capable of BOOTP forwarding.

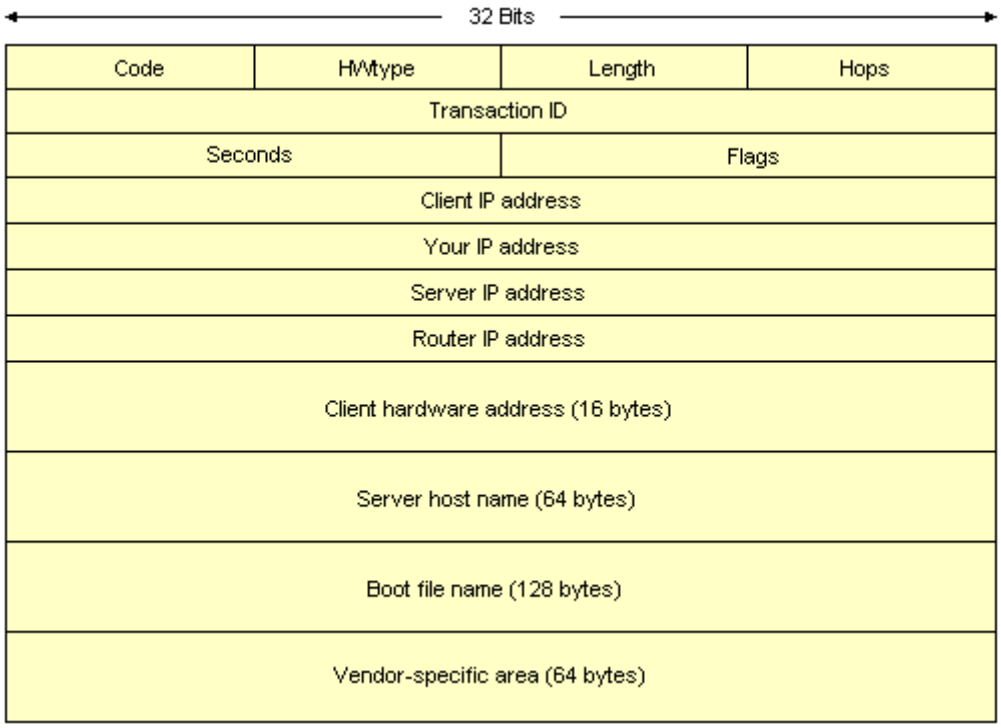
BOOTP is a draft standard protocol. Its status is recommended. There are also updates to BOOTP, some relating to interoperability with DHCP .BOOTP are draft standards with a status of elective and recommended, respectively. The BOOTP protocol was originally developed as a mechanism to enable diskless hosts to be remotely booted over a network as workstations, routers, terminal concentrators, and so on.

It allows a minimum IP protocol stack with no configuration information to obtain enough information to begin the process of downloading the necessary boot code. BOOTP does not define how the downloading is done, but this process typically uses TFTP "Trivial File Transfer Protocol (TFTP)". Although still widely used for this purpose by diskless hosts, BOOTP is also commonly used solely as a mechanism to deliver configuration information to a client that has not been manually configured.

The BOOTP process involves the following steps :

(1) The client determines its own hardware address; this is normally in a ROM on the hardware.

(2) A BOOTP client sends its hardware address in a UDP datagram to the server.



- **Advantages of Bootstrap:**
  - Flexibility
  - Computer decides which item to obtain from local disk and which to obtain over the network.

- **Disadvantages of Bootstrap:**
  - Network traffic and delay.
  - Computer issues request messages to server.Each response returns a small value(IP).Networks enforce min.Packet size, so most of the space in each packet is wasted.