6. Application Layer

A) Application Layer and its Function

It is the top most layer of OSI Model. Manipulation of data(information) in various ways is done in this layer which enables user or software to get access to the network. Some services provided by this layer includes: E-Mail, transferring files, distributing the results to user, directory services, network resources, etc.
The Application Layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is **HTTP (Hyper Text Transfer Protocol)**, which is the basis for the World Wide Web.

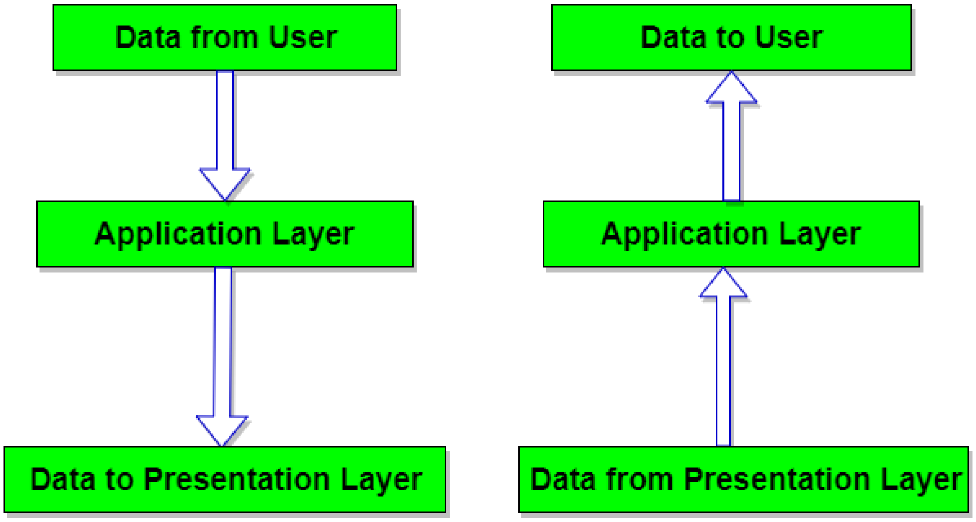
Functions of Application Layer

i. **Mail Services:** This layer provides the basis for E-mail forwarding and storage.

ii. **Network Virtual Terminal:** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.

iii. **Directory Services:** This layer provides access for global information about various services.

iv. **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.



Design Issues with Application Layer

There are commonly reoccurring problems that occur in the design and implementation of Application Layer protocols and can be addressed by patterns from several different pattern languages:

- Pattern Language for Application-level Communication Protocols
- Service Design Patterns
- Patterns of Enterprise Application Architecture
- Pattern-Oriented Software Architecture

B) Electronic Mail: SMTP (Simple Mail Transfer Protocol : SMTP)

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side.

SMTP Protocol

The SMTP model is of two type :

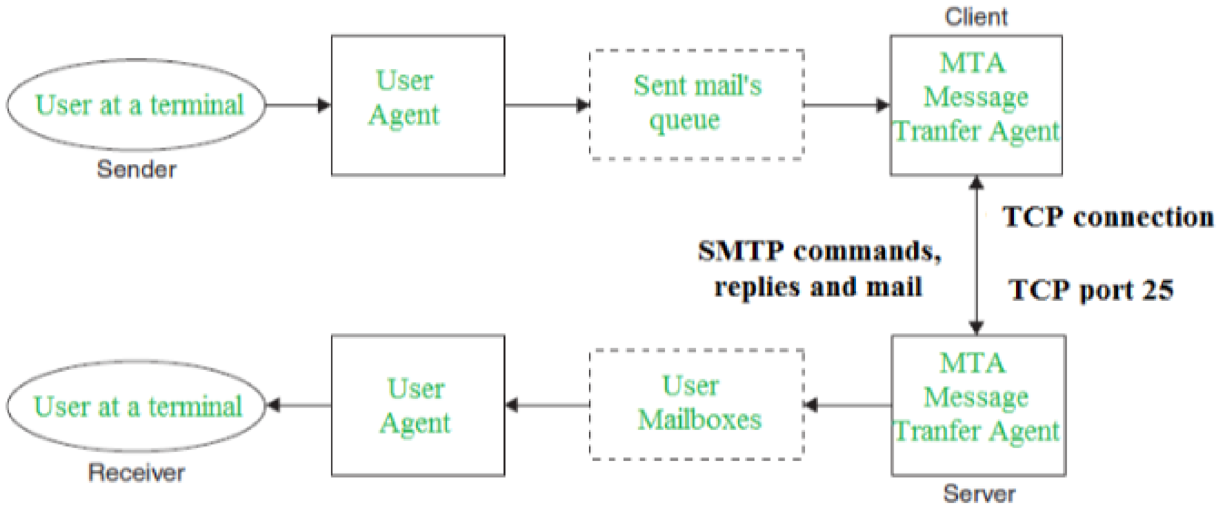
1. End-to- end method
2. Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method is used within an organization. A SMTP client who wants to send the mail will contact the destination's host SMTP directly in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP.

The client SMTP is the one which initiates the session let us call it as client- SMTP and the server SMTP is the one which responds to the session request and let us call it as receiver-SMTP. The client- SMTP will start the session and the receiver-SMTP will respond to the request.

Model of SMTP system

In the SMTP model user deals with the user agent (UA) for example Microsoft outlook, netscape, Mozilla etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the MTA it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.



Both the SMTP-client and MSTP-server should have 2 components:

1. User agent (UA)
2. Local MTA

Communication between sender and the receiver :

The senders, user agent prepare the message and send it to the MTA . The MTA functioning is to transfer the mail across the network to the receivers MTA.

SENDING EMAIL:

Mail is send by a series of request and response messages between the client and a server. The message which is send across consists of a header and the body. A null line is used to terminate the mail header. Everything which is after the null line is considered as body of the message which is a sequence of ASCII characters. The message body contains the actual information read by the receipt.

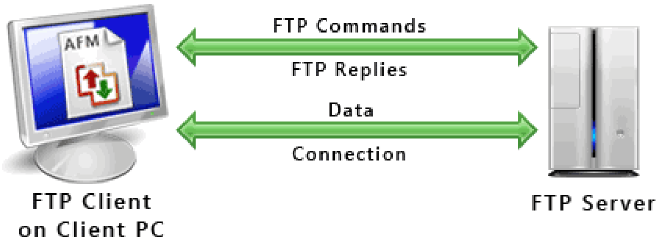
RECEIVING EMAIL:

The user agent at the server side checks the mailboxes at a particular time of intervals. If any information is received it informs the user about the mail. When user tries to read the mail it displays a list of mails with a short description of each mail in the mailbox. By selecting any of the mail user can view its contents on the terminal.

C) File Transfer: FTP, Telnet

1. File Transfer Protocol (FTP) [TCP Port 20,11]

FTP refers to a network protocol responsible for transferring files from one computer to another over a TCP computer network or the Internet. Transferring files from a client computer to a server computer is called "uploading" and transferring from a server to a client is "downloading".



FTP uses one connection for commands and the other for sending and receiving data. FTP has a standard port number on which the FTP server "listens" for connections. The standard port number used by FTP servers is 21 and is used only for sending **commands**. Since port 21 is used exclusively for sending commands, this port is referred to as a **command port**. For example, to get a list of folders and files present on the FTP server, the FTP Client issues a "LIST" command. The FTP server then sends a list of all folders and files back to the FTP Client.

Some common ftp commands are:

Cd: Change the directory on the remote computer.

Close: Close the connection to the remote computer.

Del: Delete files from the remote computer.

Rmdir: Remove a directory on the remote host

Bye (or quit): Close the connection to the remote computer and exit FTP.

So what about the internet connection used to send and receive data? The port that is used for transferring data is referred to as a data port. The port used for sending data is port 20.

2. Terminal Network (TELNET):

- It is a client/ server application program. TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.
- In TELNET a user can run different application programs at a remote site and create results that can be transferred to his local computer. After logging on, a user can use the services available on the remote computer and transfer the results back to the local computer. When a user wants to access an application program utility located on a remote machine he performs remote login operation.
- As a user types at a terminal or a workstation running a terminal emulator, the keystrokes are accepted by the terminal driver.

- The terminal passes the characters to the operating system. The local operating system accepts the characters but does not interpret them.
- The characters are sent to the TELNET client, which transforms the characters to a universal set called Network Virtual Terminal (NVT) characters and delivers them to the TCP/ IP stack as shown in the below figure:

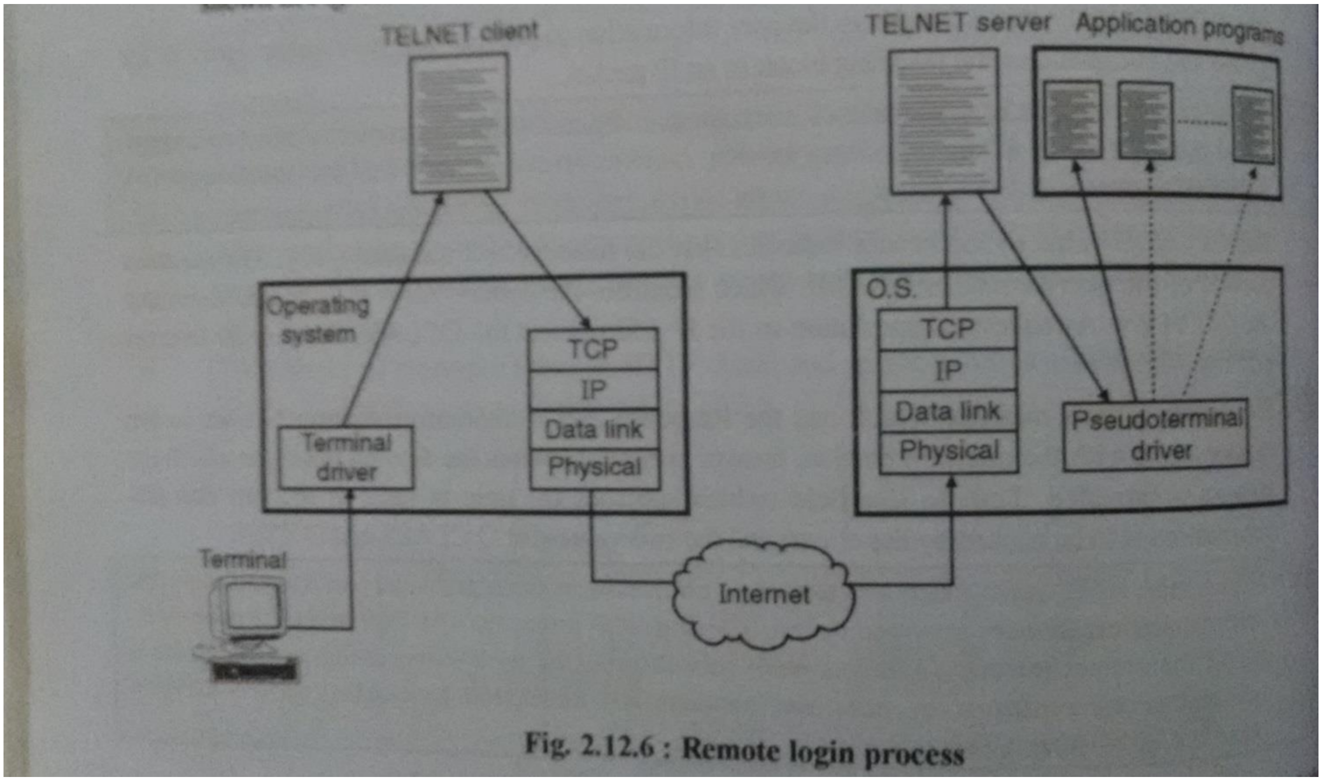


Fig. 2.12.6 : Remote login process

- As shown in the figure the text messages or commands in the NVT form travel through the internet and arrive at the TCP/ IP stack at the remote machine.
- From the TCP/ IP stack the characters are delivered to the operating system and passed to the TELNET server.
- The characters cannot be passed directly to the operating system because the remote operating system is not designed to receive characters from a TELNET server, but it is designed to receive characters from a terminal driver.
- To overcome this problem, software called pseudo-terminal driver is used, which pretends that the characters are coming from a terminal.
- The operating system then passes the characters to the appropriate applications program.

D) DHCP (Dynamic Host Configuration Protocol)

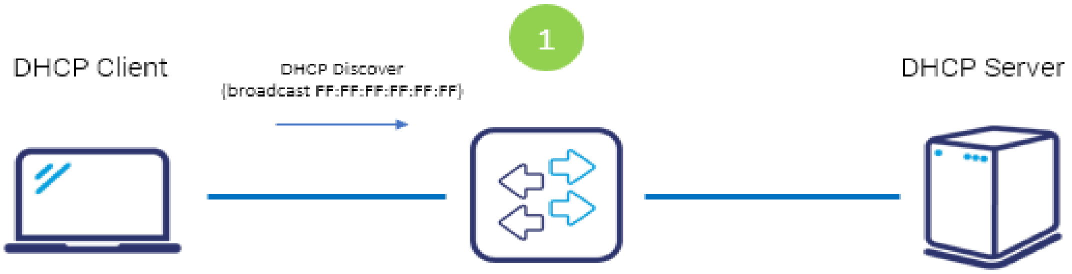
DHCP (Dynamic Host Configuration Protocol) is a protocol that is commonly used in networks for dynamic IP addressing configuration. Every user’s device needs at least IP address to join the network and connect to services. When computer first connects to local network with cable or WiFi SSID, first thing is to look for IP address, netmask, default gateway and DNS servers.

DHCP Provides:

- IP Address (leases IP for fixed amount of time after which it has to be renewed)
- Subnet Mask
- Gateway Address
- DNS Server etc.

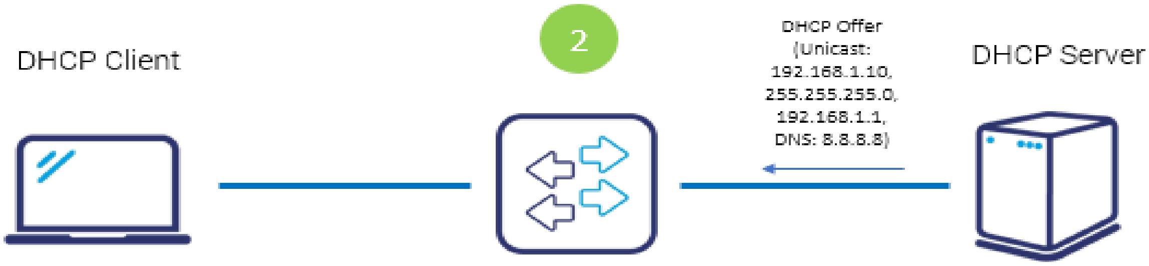
How does DHCP work?

a) Host connecting to network (cable or wireless) sends DHCP discover message to all hosts in Layer 2 segment (destination address is FF:FF:FF:FF:FF:FF). Frame with this **DISCOVER** message hits the DHCP Server.

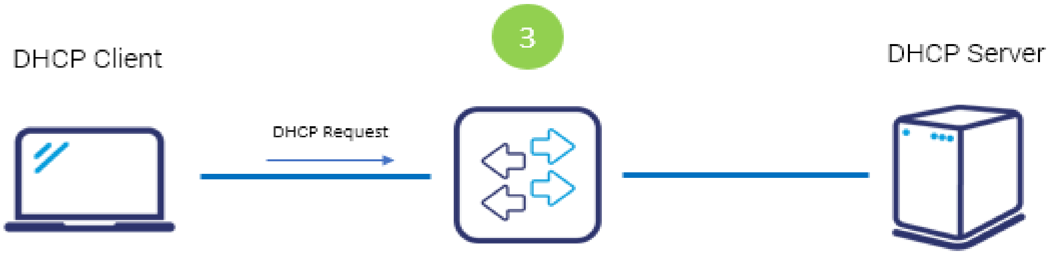


b) After the DHCP Server receives discover message it suggests the IP addressing offering to the client host by unicast. This **OFFER** message contains:

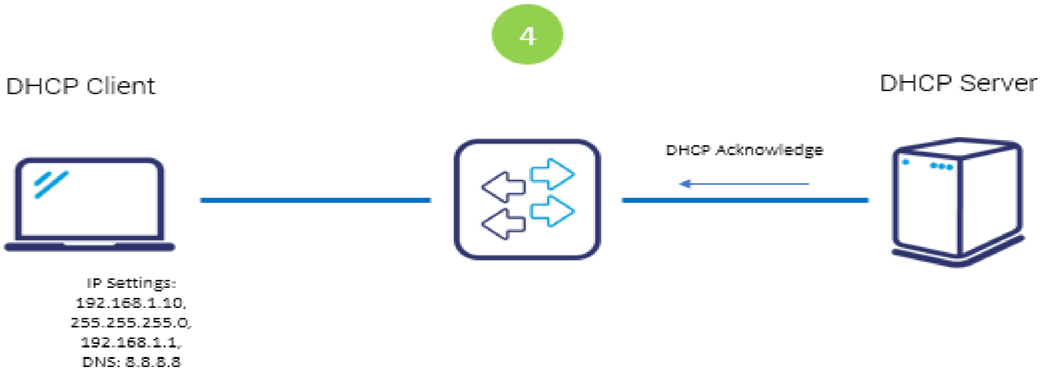
- proposed IP address for client (here 192.168.1.10)
- subnet mask to identify the subnet space (here 255.255.255.0)
- IP of default gateway for subnet (here 192.168.1.1)
- IP of DNS server for name translations (here 8.8.8.8)



c) Now after the client receives the offer it requests the information officially sending REQUEST message to server this time by unicast.



d) Server sends **ACKNOWLEDGE** message confirming the DHCP lease to client. Now client is allowed to use new IP settings.



E) DNS, HTTP, WWW, SNMP

1. Domain Name System (DNS) [TCP/UDP Port 53]

DNS or Domain Name System is an application that allows us to find the ip address of a domain name.Let us say that we want to access www.abc.com from our browser then, the chain of events to get the IP address for www.abc.com are

First your computer queries the name server (DNS server) it is set up to use. This is the recursive name server shown above.

The name server doesn’t know the IP address for www.abc.com, so it will start the following chain of queries before it can report back the IP address to your computer (the numbers below correspond to the numbers in the image).

i. Query the Internet root servers to get the name servers for the .com TLD.
ii. Query the .com TLD name servers to get the authoritative name servers for abc.com.
iii. Query the authoritative name servers for abc.com to finally get the IP address for the host www.abc.com, then return that IP address to your computer.
iv. Done! Now that your computer has the IP address for www.abc.com, it can access that host.

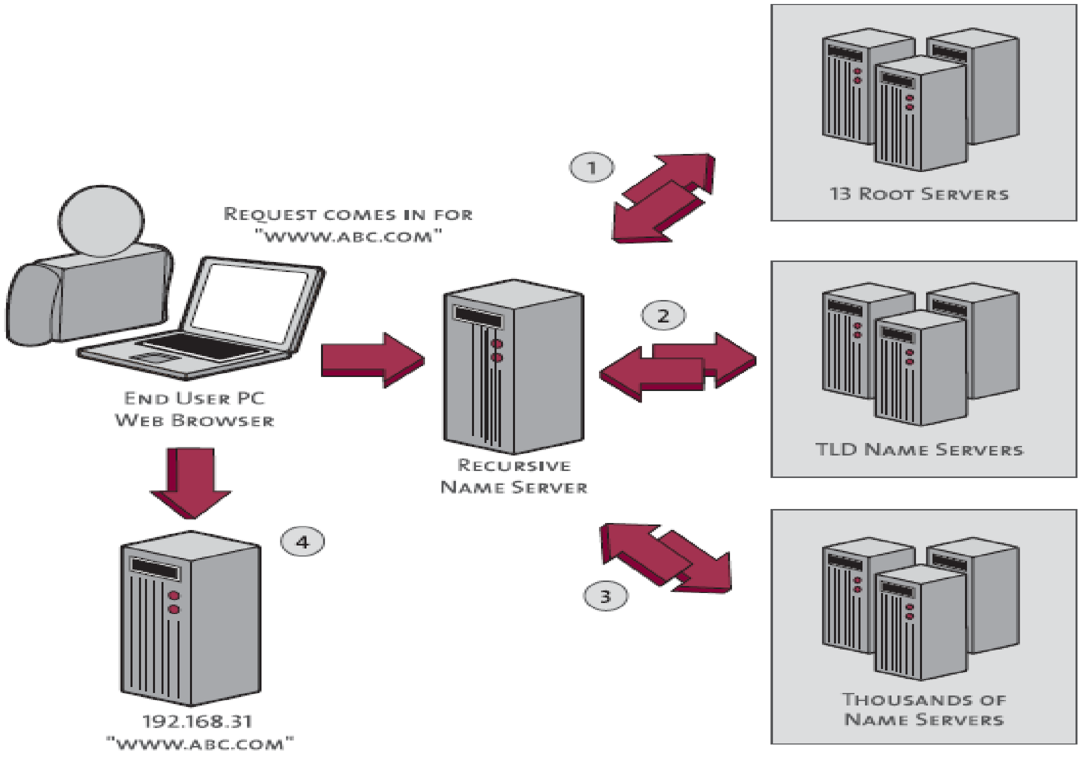
The basic records provided by DNS are:

A (Address) Host IP addresses.

CNAME (Canonical Name) Defines a host alias.

MX (Mail Exchange) Identifies where to send mail for a given domain name.

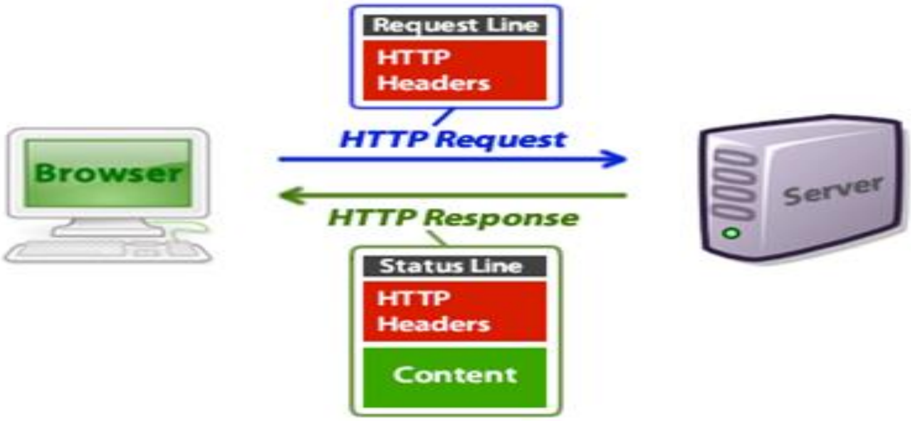
NS (Name Server) Identifies a domain's name servers



2. HypetText Transfer Protocol (HTTP):

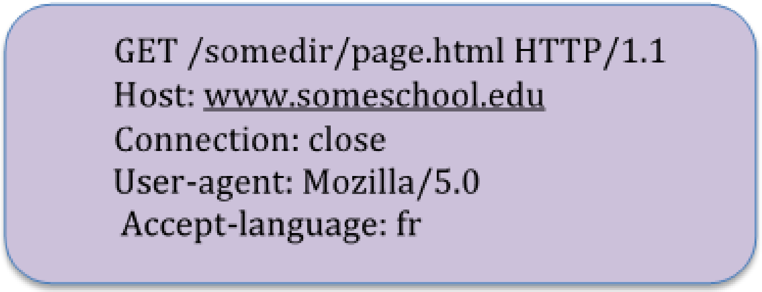
It's a protocol by which hypertext (that is, the content of a web page) is transferred between a web server and your machine.

Whenever a web client (web browser) needs to get web object from a web server, it needs to send a GET request for that object. The GET request is included in the HTTP header. After receving the request the server sends the HTTP response message requested object if available.

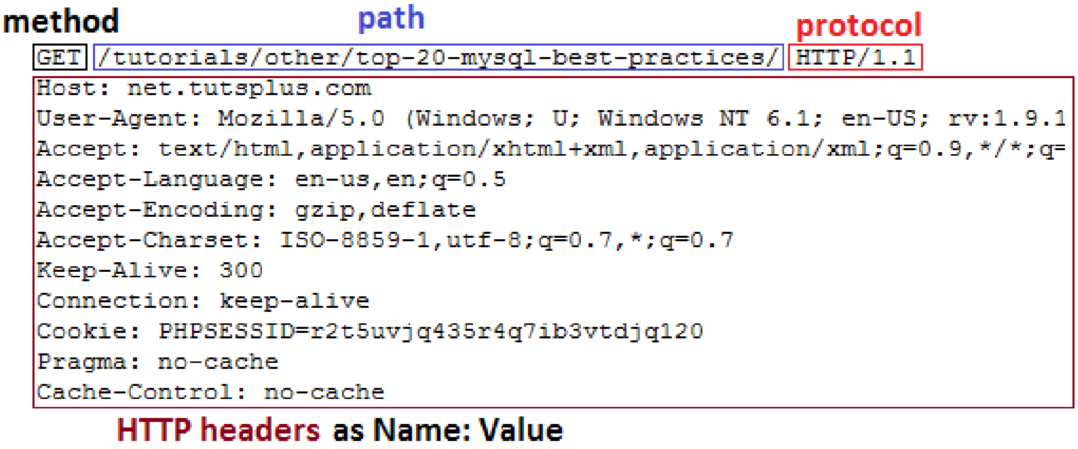


HTTP Message Format

1. The web client makes a request for a object with at GET Request in the HTTP header. The basic structure of HTTP GET is as follow;



```
GET /somedir/page.html HTTP/1.1
Host: www.someschool.edu
Connection: close
User-agent: Mozilla/5.0
 Accept-language: fr
```


method
path
protocol
HTTP headers as Name: Value

```
GET /tutorials/other/top-20-mysql-best-practices/ HTTP/1.1
Host: net.tutsplus.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120
Pragma: no-cache
Cache-Control: no-cache
```

The first line of an HTTP request message is called the request line; the subsequent lines are called the header lines. The request line has three fields: the method field, the URL field, and the HTTP version field. The method field can take on several different values, including GET, POST, HEAD, PUT, and DELETE. The broser is requesting the object /somedir/page.html. And the browser is requesting using HTTP version 1.1.

The header line Host: www.someschool.edu specifies the host on which the object resides. The Connection:close header line tells the browser no to implement persistant connection. The User-agent Mozilla/5.0 tells that the request is made using Mozilla browser version 5.0. The last line tells the preferred language

Http Cookies

A cookie is a small file that is stored on a user pc by the web server. The HTTP cookie is there to remember helpful information on that page or website. If you put items into your shopping cart on Amazon you are adding information of those items to a cookie that is stored so if you leave and come back you still have those stored in your shopping cart page. They are also common for letting each page know if the user is logged in, and to which account they are logged in with.

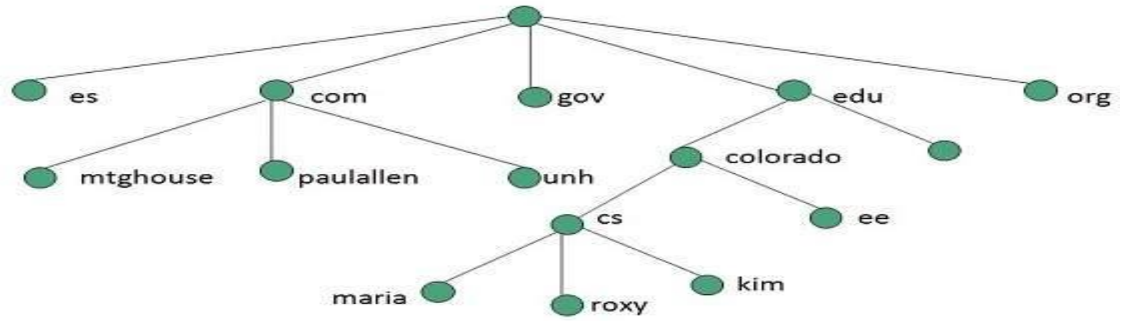
3. WWW (World Wide Web)

WWW stands for **World Wide Web.** A technical definition of the World Wide Web is : all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

A broader definition comes from the organization that Web inventor **Tim Berners-Lee** helped found, the **World Wide Web Consortium (W3C).**

The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge. In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet, tying them together into a vast collection of interactive multimedia resources.

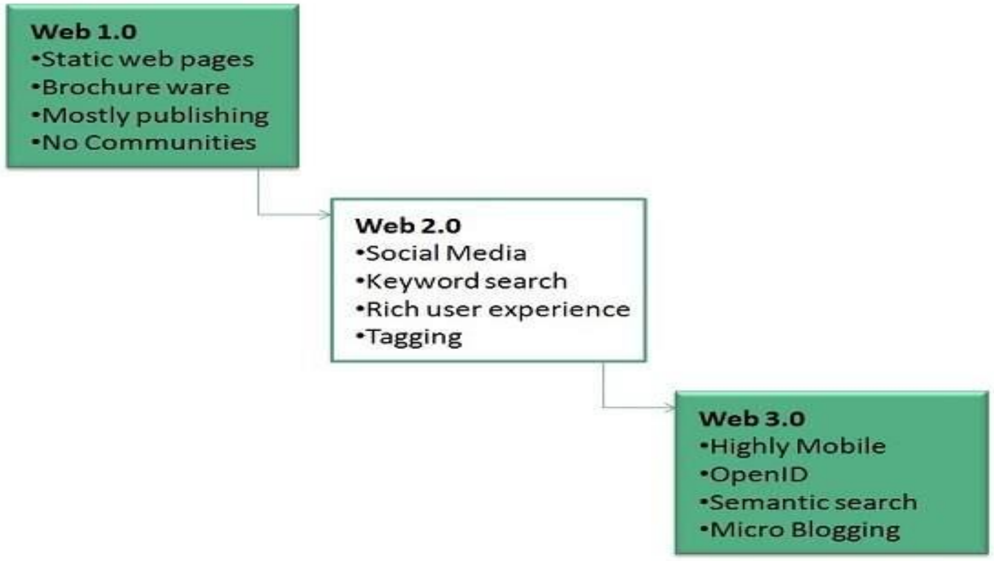
Internet and **Web** is not the same thing: Web uses internet to pass over the information.



Evolution

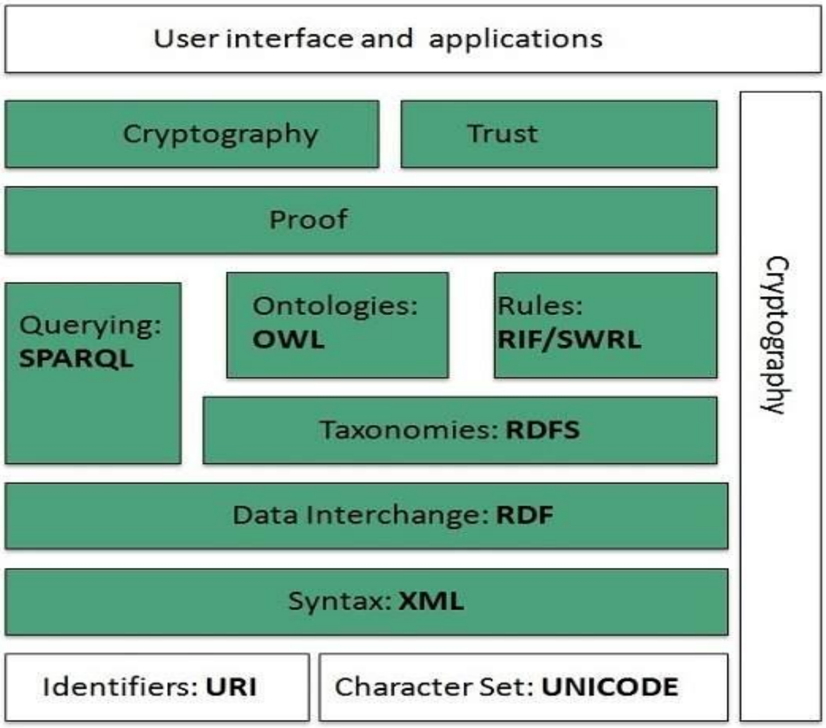
World Wide Web was created by **Timothy Berners Lee** in 1989 at **CERN** in **Geneva.** World Wide Web came into existence as a proposal by him, to allow researchers to work together effectively and efficiently at **CERN.** Eventually it became **World Wide Web.**

The following diagram briefly defines evolution of World Wide Web:



WWW Architecture

WWW architecture is divided into several layers as shown in the following diagram:



i. Identifiers **and Character Set: Uniform Resource Identifier (URI)** is used to uniquely identify resources on the web and **UNICODE** makes it possible to built web pages that can be read and write in human languages.

ii. Syntax: **XML (Extensible Markup Language)** helps to define common syntax in semantic web.

iii. Data Interchange: **Resource Description Framework (RDF)** framework helps in defining core representation of data for web. RDF represents data about resource in graph form.

iv. Taxonomies: **RDF Schema (RDFS)** allows more standardized description of **taxonomies** and other **ontological** constructs.

v. Ontologies: **Web Ontology Language (OWL)** offers more constructs over RDFS.

vi. Rules: **RIF** and **SWRL** offers rules beyond the constructs that are available from **RDFs** and **OWL.** Simple Protocol and **RDF Query Language (SPARQL)** is SQL like language used for querying RDF data and OWL Ontologies.

vii. Proof: All semantic and rules that are executed at layers below Proof and their result will be used to prove deductions.

viii. Cryptography: **Cryptography** means such as digital signature for verification of the origin of sources is used.

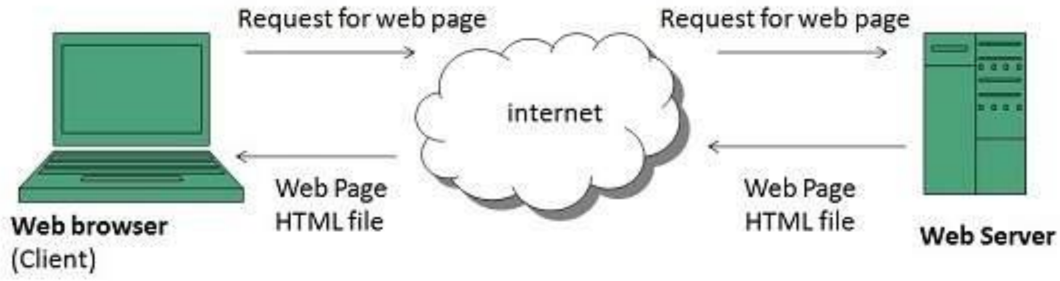
ix. User Interface and Applications: On the top of layer **User interface and Applications** layer is built for user interaction.

WWW Operation

WWW works on client- server approach. Following steps explains how the web works:

1. User enters the URL (say, **http://www.tutorialspoint.com**) of the web page in the address bar of web browser.
2. Then browser requests the Domain Name Server for the IP address corresponding to www.tutorialspoint.com.

3. After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.
4. Then web server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.
5. Now the web browser receives the web page, It interprets it and display the contents of web page in web browser's window.



4. **Simple Network Management Protocol (SNMP)**

If an organization has 1000 of devices then to check all devices, one by one everyday, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.
SNMP is an application layer protocol which uses UDP port number 161/162. SNMP is used to monitor network, detect network faults and sometimes even used to configure remote devices.

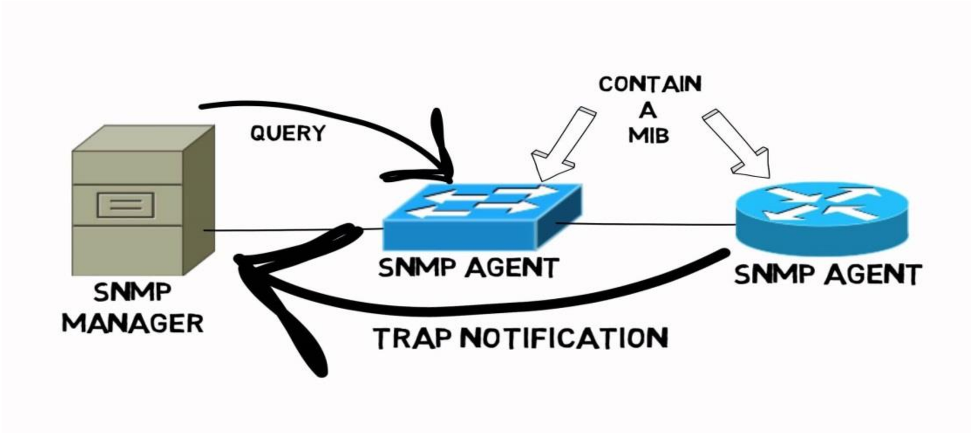
SNMP components –

There are 3 components of SNMP:

a) **SNMP Manager –**
It is a centralised system used to monitor network.It is also known as Network Management Station (NMS)

b) **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. There can be large number of SNMP Agents.

c) **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:

a) **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.

b) **GetNextRequest –**
This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.

c) **GetBulkRequest –**
This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.

d) **SetRequest –**
It is used by SNMP manager to set the value of an object instance on the SNMP agent.

e) **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.

f) **Trap –**
These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.

g) **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:

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

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

c) **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:

a) **SNMPv1 –**
It uses community strings for authentication and use UDP only.

b) **SNMPv2c –**
It uses community strings for authentication. It uses UDP but can be configured to use TCP.

c) **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.