DNS Protocol

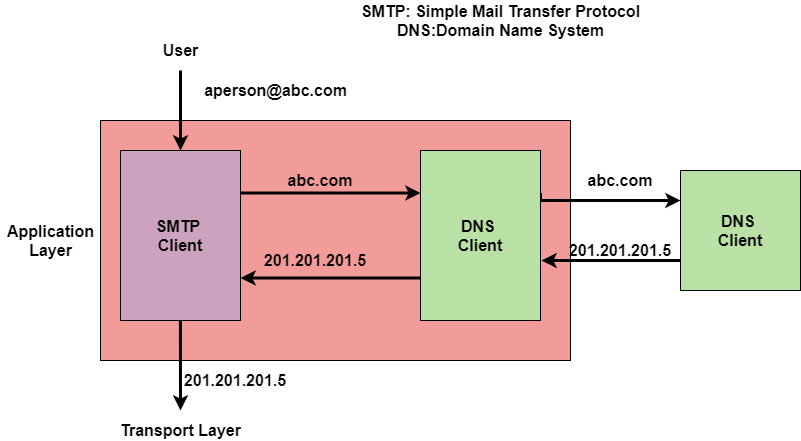
DNS is an abbreviation of Domain Name System or Domain Name Service. It is an application layer protocol.

* Basically, a Domain name system is a supporting program that is used by other programs such as an E-mail.
* The user of the email program knows the email address of the recipient; the Internet protocol needs the IP address.
* Mainly the DNS client program sends a request to the DNS server in order to map the e-mail address to the corresponding IP address.
* In order to identify an entity, the TCP/IP protocols also make use of an IP address that uniquely identifies the connection of the host to the internet. But people usually prefer to use names instead of numeric addresses. Thus, there is a need for the system that can map a name to an address or an address to a name.

Domain Name System is a system that can map a name to an address or an address to a name.

Example

Given below is an example of using the Domain name system:





Name Space

NameSpace basically maps each address to a unique name. The names assigned to the machines must be unique because addresses are unique.

It is further categorized into two:

* Flat Name Space
* Hierarchical Name Space

**Flat Name Space**

In the Flat Name Space basically, a name is assigned to an address.

* A name in this space is basically a sequence of characters without any structure.
* Also, the names may or may not have a common section. In case if they have a common section then it has no meaning.
* One of the main disadvantages of this system is that it cannot be used in the case of large systems; because there is no central control and it will lead to ambiguity and duplication.

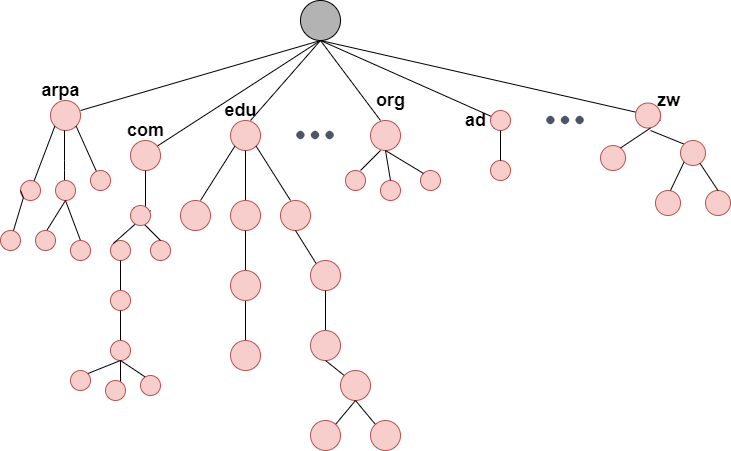
**Hierarchical Name Space**

In Hierarchical Name Space each name consists of several parts.

* The first part mainly indicates the nature of the organization.
* The second part mainly indicates the name of the organization.
* The third part mainly defines the departments in the organization and so on.
* The central authority can assign the part of the name that indicates the name and nature of the organization and the responsibility of the rest of the name is given to the organization itself.
* An organization can also add suffixes(or prefixes) to the name in order to define the host or resources.

Domain Name Space

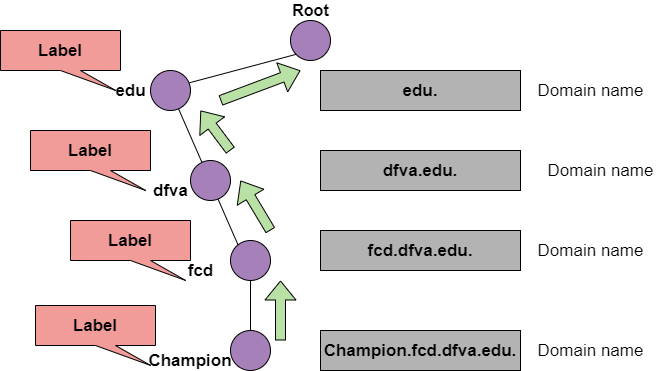
When we use the hierarchical Name Space in that case, we need to design the **Domain Name Space**.In this Design, the names are defined in the inverted-tree structure where the root lies at the top.



Domain Name

Each node of the tree has a domain name.

* A Full domain name is basically a sequence of labels that are usually separated by dots(.).
* The domain name is always read from the node up to the root.
* The last label is the label of the root that is always null.
* All this means that the full domain name always ends in the null label, which means that the last character is always a dot because the null string is nothing.



The figure shows the domain names and labels

Domain Names are further categorized into two:

**1. Fully Qualified Domain Name**

* If the label is terminated by the null string then it is known as a fully qualified domain name. This domain name contains the full name of the host.
* FQDN mainly consists of two parts: **hostname** and **domain name**.
* The FQDN mainly contains all the labels from the most specific one to the most general one that helps to uniquely define the name of the host.
* Example:Champion.fcd.dfva.edu. in this the hostname is Champion.

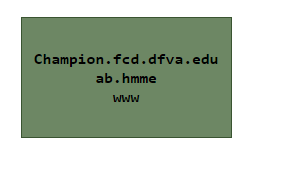
Given below are some Fully Qualified Domain names;



2.Partially Qualified Domain Name

If the label is not terminated by the null string, then it is known as Partially Qualified Domain Name.

* This name starts from the node but does not reach the root.
* It is mainly used when the name to be resolved belongs to the same site as the client and in this case, the resolver can supply the missing part that is known as a **suffix** in order to create an FQDN.



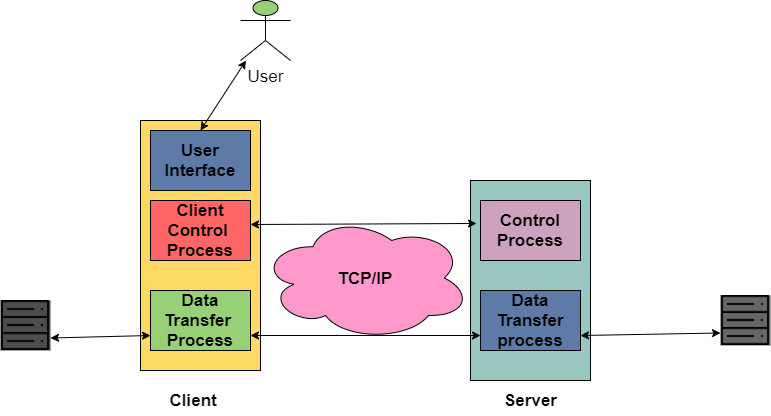
# FTP Protocol

FTP means File Transfer Protocol and it is the standard mechanism provided by the TCP/IP in order to copy a file from one host to another.

* File Transfer Protocol is a protocol present at the Application layer of the OSI Model.
* FTP is one of the easier, simpler, and secure ways to exchange files over the Internet.
* FTP is different from the other client/server applications as this protocol establishes two connections between the hosts.
  + where one connection is used for the data transfer and is known as a **data connection.**
  + while the other connection is used to control information like commands and responses and this connection is termed as **control connection.**
* FTP is more efficient as there is the separation of commands.
* The File Transfer Protocol makes the use of two protocols; **Port 21** for the **Control connection**and **Port 20** is used for **Data connection.**
* The transferring of files from the client computer to the server is termed as "uploading", while the transferring of data from the server to the client computer is termed as "downloading".

## Working of FTP

Given below figure shows the basic model of file Transfer Protocol, where the client comprises of three components: User Interface, Client control process, and client data transfer process. On the other hand, the server comprises of two components mainly the server control process and the server data transfer process.



1. Also, the control connection is made between the control processes while the data connection is made between the data transfer processes.
2. The control Connection remains connected during the entire interactive session of FTP while the data connection is opened and then closed for each file transferred.
3. In simple terms when a user starts the FTP connection then the control connection opens, while it is open the data connection can be opened and closed multiple times if several files need to be transferred.

## Advantages of FTP

Following are some of the benefits of using File Transfer protocol:

* Implementation of FTP is simple.
* FTP provides one of the fastest ways to transfer files from one computer to another.
* FTP is a standardized protocol and is widely used.
* File Transfer protocol is more efficient as there is no need to complete all the operations in order to get the entire file,

## Disadvantages of FTP

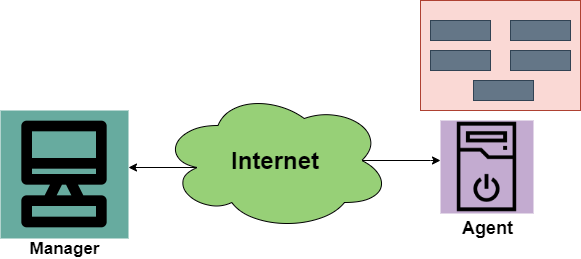
Let us take a look at the drawbacks of FTP:

* File Transfer Protocol is not a secure way to transfer the data.
* FTP does not allow the copy from server to server and also not allows removal operations for the recursive directory.
* The spoofing of the server can be done in order to send data to a random unknown port on any unauthorized computer.

**SNMP Protocol-**

* SNMP mainly stands for Simple Network Management protocol.
* It is basically a framework that is used for managing the devices on the internet by using the TCP/IP protocol suite.
* Basically, SNMP provides a set of fundamental operations in order to monitor and maintain the Internet.
* It is an application layer protocol that was defined by the Internet engineering task force.
* This protocol is mainly used to monitor the network, detect the faults in the Network, and sometimes it is also used to configure the remote devices.

Concept of SNMP



The SNMP protocol makes the use of Manager and Agent; where the manager is usually a host that controls and monitors the set of agents.

* The SNMP is an application-level protocol and it consists of a few manager stations that mainly controls a set of agents. This protocol is mainly designed at the application level so that it can monitor the devices that are mainly made by different manufacturers and that are installed on different physical networks.

Thus, there are three components in the architecture of the SNMP:

* SNMP Manager
* SNMP Agent
* Management Information Base

**SNMP Manager**

It is basically a centralized system and it is mainly used to monitor and manage devices that are connected with the network. SNMP manager is typically a computer and it is used to run one or more network management systems.

Given below are the main functions of SNMP Manager:

1. Collects response from the agents.
2. To acknowledge asynchronous events from the agents.
3. To set variables in the agent.
4. Queries the Agent

**SNMP Agent**

SNMP Agent is basically a software program that is packaged within the network element. It is mainly installed on a managed device where managed devices can be switches, servers, routers, PC, etc.

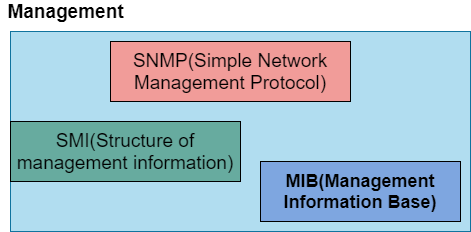
Mainly the agents keep the information in the database also the manager has the access to the values present in the database.

Given below are the main responsibilities of the SNMP Agent:

* SNMP agents mainly collect the management information about its local environment
* The SNMP agent mainly signals an event to the manager.
* The SNMP agents also act as a proxy for some non–SNMP manageable network nodes.

Management Components

In order to perform the Management tasks, the SNMP protocol makes the use of two other protocols and are SMI and MIB. We can also say that the Management on the Internet is done by the cooperation of three protocols and these are SNMP, MIB, SMI.



**Role of SNMP**

The SNMP protocol performs some specific roles in Network Management;

* It mainly defines the format of the packet that needs to be sent from the manager to the agent or vice-versa.
* SNMP is also used to interpret the result and create the statistics.
* The packets that are exchanged between the manager and agent contains the name of the object(variable) and their status(values).
* The SNMP is also responsible for reading and changing these values.

**Role of SMI**

In order to use the SNMP, there is a need for some rules and these rules are for naming the objects. Now its time to take a look at the roles of SMI:

* SMI(Structure of Management Information) is mainly used to define the general rules for naming the objects.
* It is also used to define the type of objects that includes (range and length).
* This is also used to show how to encode the objects and values.
* The SMI does not define the number of objects that should be managed by an entity.

**Role of MIB**

In order to manage each entity, this protocol is mainly used to define the number of objects and then to name them according to the rules defined by the SMI and after that associate a type to each named object.

* MIB (Management Information Base) is mainly used to create a set of objects that are defined for each entity that is similar to the database.
* Thus, MIB mainly creates a collection of named objects, their types.

**Advantages of SNMP Protocol**

Given below are some of the benefits of using SNMP :

1. It is the standard network management protocol.
2. This protocol is independent of the operating system and programming language.
3. The functional design of this protocol is Portable.
4. The SNMP is basically a core set of operations and it remains the same on all managed devices. Thus, SNMP supports extendibility.
5. SNMP is a universally accepted protocol.
6. It is a lightweight protocol.
7. This protocol allows distributed management access.

**Disadvantages**

Some of the drawbacks of SNMP are as follows:

* This protocol leads to the reduction of the bandwidth of the network.
* Access control, authentication, and privacy of data are some largest security issues using this.

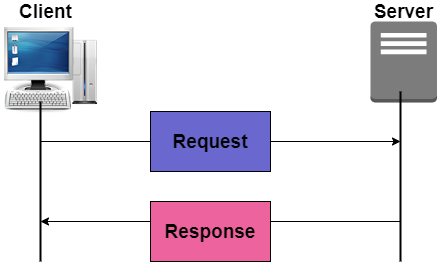
**HTTP Protocol**

**HTTP** stands for Hypertext Transfer Protocol and is mainly used to access the data on the world wide web i.e. **(WWW)**. The **HTTP** mainly functions as the combination of **FTP** (File Transfer Protocol) and **SMTP** (Simple Mail Transfer Protocol).

* **HTTP** is one of the protocols used at the **Application Layer**.
* The **HTTP** is similar to **FTP** because **HTTP** is used to transfer the files and it mainly uses the services of **TCP.**
* Also, **HTTP** is much simpler than**FTP** because there is only **one TCP connection**.
* In **HTTP,** there is no separate control connection, as only data is transferred between the client and the server.
* The **HTTP** mainly uses the services of the**TCP**on the well-known port that is**port 80.**
* **HTTP** is a **stateless protocol.**
* In**HTTP, the**client initializes the transaction by sending a request message, and the server replies by sending a response.
* This protocol is used to transfer the data in the form of plain text, hypertext, audio as well as video, and so on.

**Working of HTTP**

The HTTP makes use of Client-server architecture. As we have already told you that the browser acts as the HTTP client and this client mainly communicates with the webserver that is hosting the website.



The figure shows the HTTP transaction

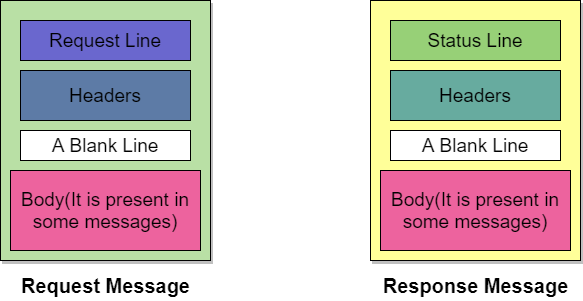
The format of the request and the response message is similar. The Request Message mainly consists of a request line, a header, and a body sometimes. A Response message consists of the status line, a header, and sometimes a body.

At the time when a client makes a request for some information (say client clicks on the hyperlink) to the webserver. The browser then sends a request message to the HTTP server for the requested objects.

After that the following things happen:

* There is a connection that becomes open between the client and the webserver through the TCP.
* After that, the HTTP sends a request to the server that mainly collects the requested data.
* The response with the objects is sent back to the client by HTTP
* At last, HTTP closes the connection.

Let us take a look at the format of the request message and response message:



**Request Line and Status line**

The first line in the Request message is known as the request line, while the first line in the Response message is known as the Status line.

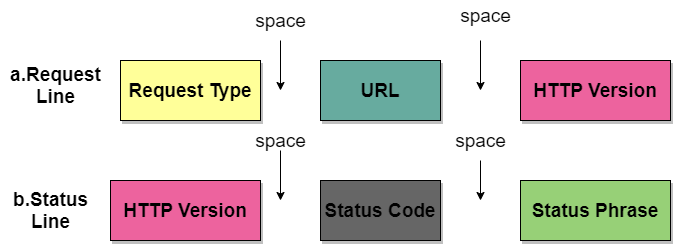


Figure: Request Line and Status Line

Advantages of HTTP

Given below are the benefits of using HTTP:

1. There is no runtime support required to run properly.
2. As it is connectionless so there is no overhead in order to create and maintain the state and information of the session.
3. HTTP is usable over the firewalls and global application is possible.
4. HTTP is platform-independent.
5. HTTP reports the errors without closing the TCP connection.

Disadvantages of HTTP

There are some drawbacks of using the HTTP protocol:

* HTTP is not optimized for mobile.
* It can be only used for point-to-point connections.
* This protocol does not offer reliable exchange.

enlightened