CHAPTER 5

5. Application Layer

Objectives

- Understanding Traditional Applications.
- Illustrating the basics of e-mail, POP3, SMTP, MIME, IMAP.
- Illustrating HTTP design and online documents.
- Explaining FTP.
- Learning the fundamentals of web services.
- To understand the DNS and how it is distributed.
- Learning about the SNMP.

5.1. Traditional Applications

Among the common global technologies, the World Wide Web (WWW) and E-mail, facilitates the model of request / reply methodology. The request is submitted to server and the response is received accordingly. Such applications come under the category of "traditional" applications, as they describe the kind of applications which have been in existence from the very start of the computer age. (Web plays an advanced role than simple text application, yet the file transfers that predated it have their roots). On the other hand, the group of applications which are popular in the current era ranges as applications based on streaming and imaging.

Generally, an important point has to be taken a close look with priority before exploring the details of these applications. It is the discrepancy of application programs with that of application protocols which has to be understood. The Hyper Text Transport Protocol (HTTP), for instance, is an application protocol used to obtain Web pages from remote servers. Other application programs like web clients - Internet Explorer, Chrome, Firefox, and Safari deliver an appealing window environment to users, even though they use the HTTP protocol in common, to connect over the Internet with web servers. It is a known truth that the protocol is published and standardized which allows interoperation of application programs created by various companies and individuals. That's how many browsers can communicate with all of the web servers.

5.2. Email

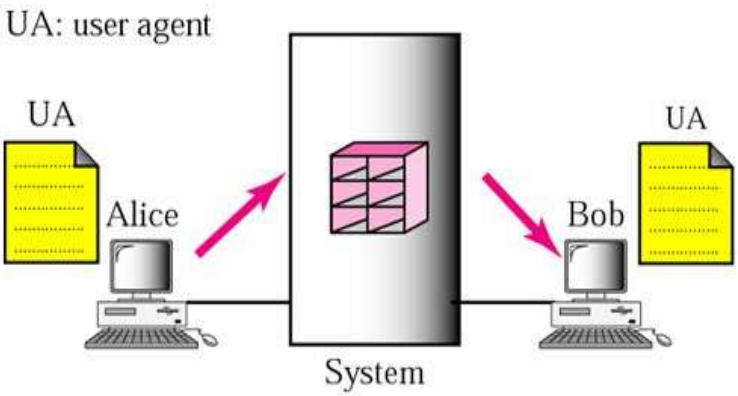
Electronic mail (Email) is among the most popular internet services. The message sent via electronic mail was brief and contains only text. It allows text, audio and video to be included into a post. This enables one message to be sent to one additional recipient.

5.2.1. Architecture

The email architecture is explained in 4 scenarios.

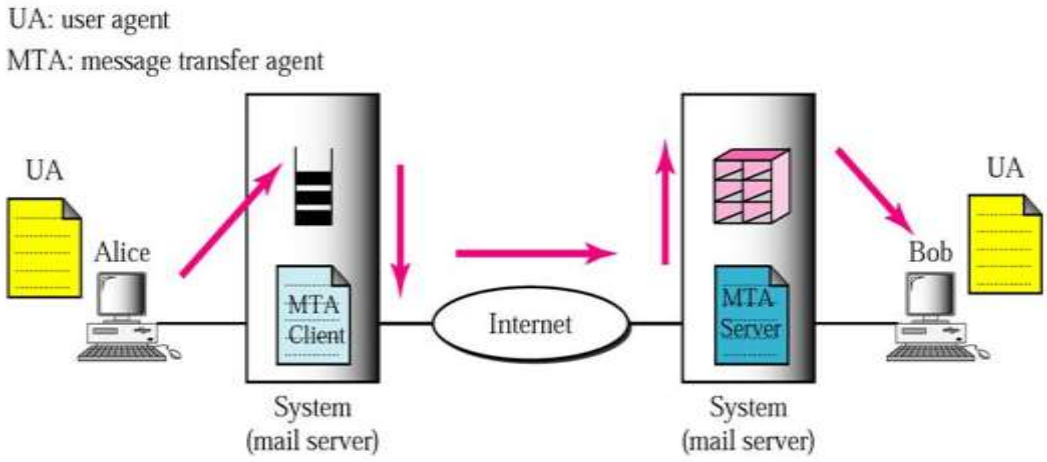
1. First Scenario

The Email's sender and receiver are uses on the same device that a common device directly links. A mailbox is a particular file with permission restrictions that is part of a local storage device. It is used to receive and store messages.



A user wants to send a message to Bob, while Alice is operating. Alice runs a User Agent (UA) program to prepare and store the message in Bob's mailbox. The message contains addresses of mailbox of sender and receiver. Using a user agent the contents of his mailbox will be capable of being retrieved and read at their convenience. If the sender and the email recipient dwell on the same platform, we just require user agents.

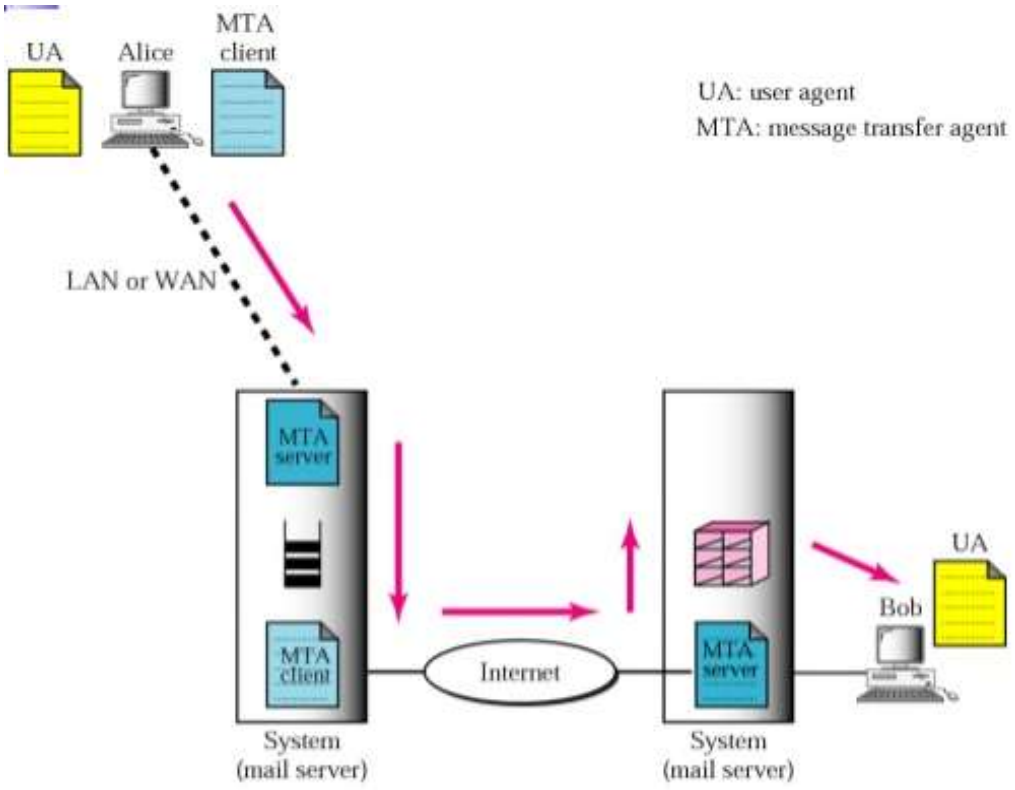
2. Second Scenario



To deliver her message to the device at her own place, an agent programme is necessitated for Alice. The mail server uses a queue to store message which is waiting for its turn for transmission. In order to retrieve messages saved in the system's mailbox at his location, Bob also requires a user agent application. The receiving message has two client and server message transfer agents. It obviously requires 2 UA and 2 MTA (client and server) where the sender and the recipient of an email exist in separate systems.

3. Third Scenario

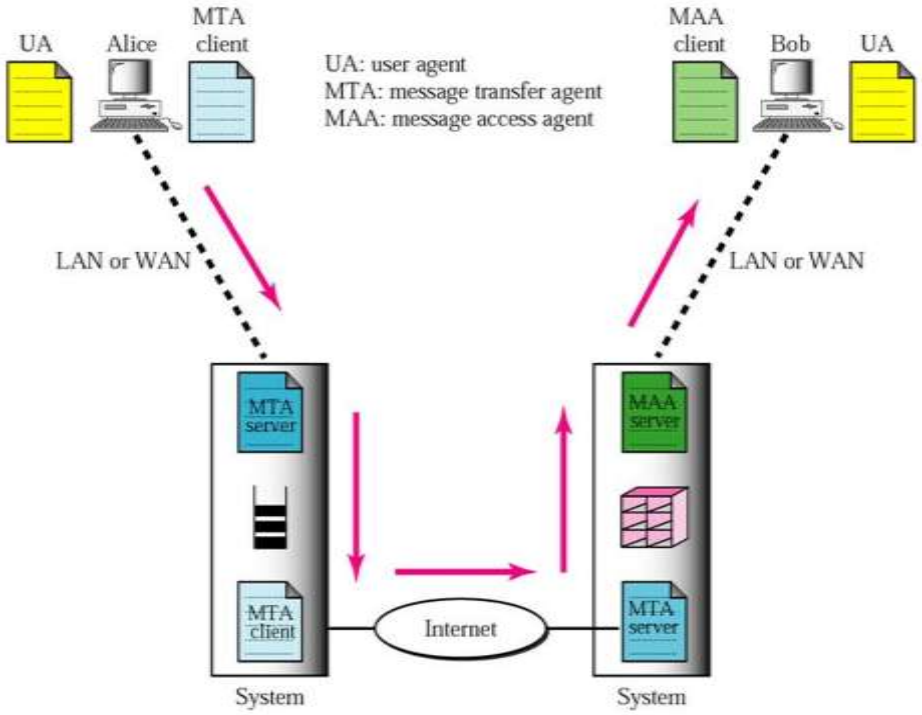
Bob is specifically related to a system of lies. Alice is connected using a dial-up modem, DSL or cable modem though WAN, to the system.



Alice requires a UA to prepare its message and send the same via the LAN / WAN. The UA is called, which further proceeds to call MTA client, when Alice has to send a request. The MTA client creates a link that is running all the time with the MTA server on the device. The machine at the Alice site queues all received messages and the MTA client sends the messages to the Bob site. It requires 2 UA and 2 MTA pairs when the sender is attached via LAN / WAN to the mail server.

4. Fourth Scenario

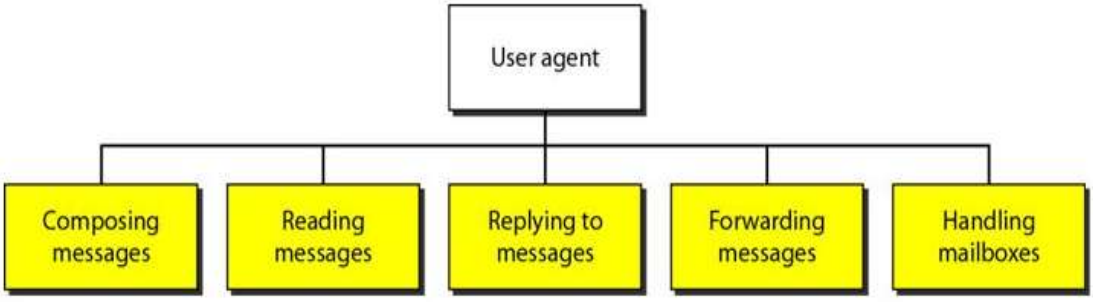
Here also a WAN / LAN links Bob to his mail server. The mail's reception at Bob's mail server makes Bob to retrieve it. The Message Access Agent (MAA) retrieves Bob's messages to the client. Then a request is initiates by the client to MAA server which is active always to facilitate message transfer.



When both sender and receiver are linked via a LAN / WAN to the mail server, 2 UA, 2 MTA pairs and 2 MAA are required and this turns to be the general issue.

5.2.2. User Agent

UA provides different uses with service to promote the sending and receiving of messages. The services provided by a UA were,



1. Composing Messages

The email address that has to be sent will be composed by the user and assisted by agent.

2. Reading Messages

A user agent processing the incoming messages.

3. Replying to Messages

A user will then use UA to respond to a message after reading the message. Typically, a UA agent helps in enabling the user in responding the actual sender in addressing all message recipients.

4. Forwarding Messages

Forwarding is described as the sending to a third party of an email.

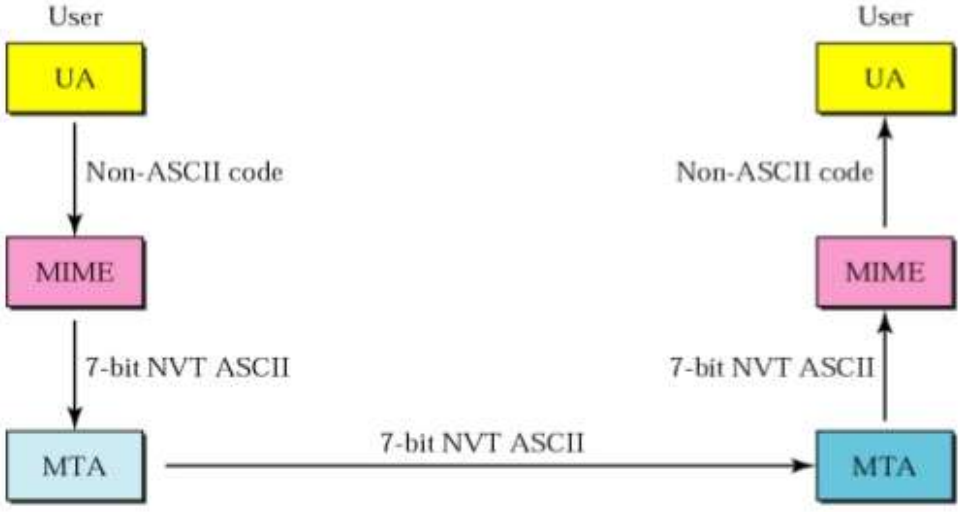
5. Handling Messages (Inbox & Outbox)

The agent utilizes a special format for managing a file that is a box.

5.2.3. Message Transfer Agent

A) MIME-Multipurpose Internet Mail Extensions (MIME)

MIME is a supplementary protocol that allows e-mail sending of non-ASCII data. It converts non-ASCII data to NVT ASCII data at the sending zone and delivers at MTA client that is to be sent over the internet. Further, the message is converted back to the original data at the receiving side.



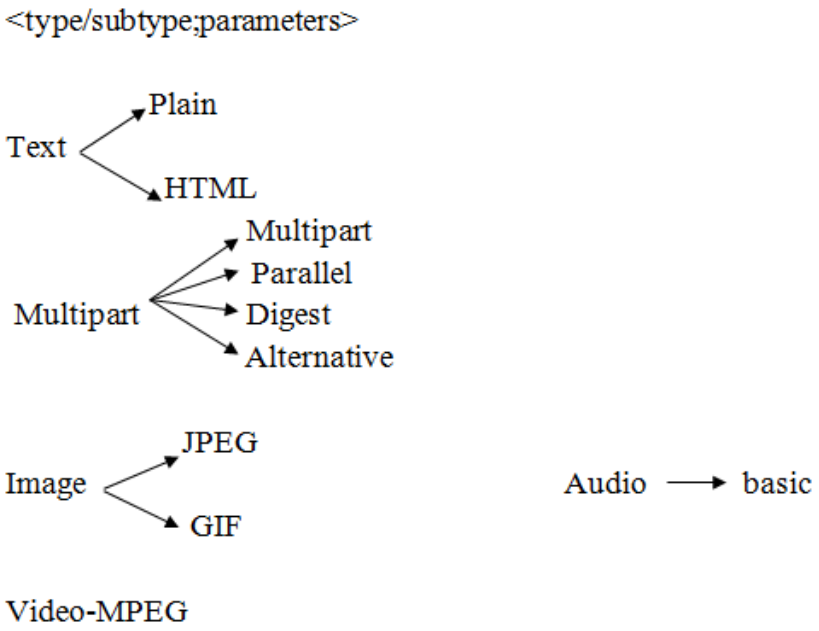
MIME defines 5 headers to describe the parameters that were applied to the original email header portion. They were MIME version, Content version, Content transfer encoding, Content ID, Content description.

MIME Version

The header specifies the version used in MIME. The new update is version 1.1.

Content Type

Header specifies the data's type which is in the message's body. The subtype of content and material is divided by a slash.



Content Transfer Encoding

This header defines the entire message uniquely within a multiple message setting.

ID=<content-id>

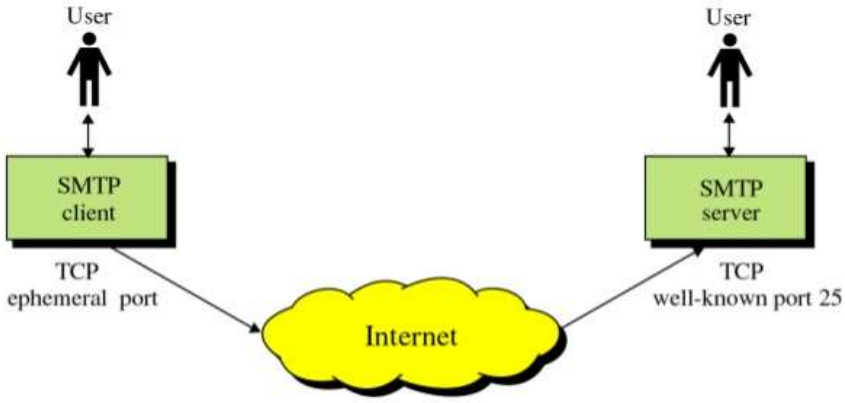
Content Description

The nature of the message be it an imagery or audio wave or visual, this header defines it.

<description>

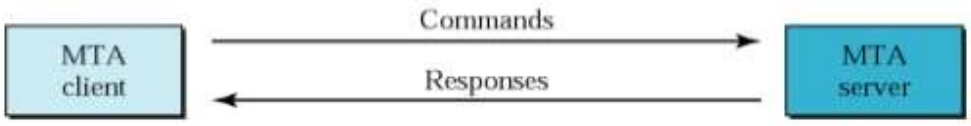
B) Simple Mail Transfer Protocol (SMTP)

The mail is transferred and gets completed through message transfer agents. If a mail has to be sent the system requires an MTA client, and MTA server is required for receiving a mail. The simple mail transfer protocol (SMTP) is considered the formal protocol that describes the MTA client and server on the internet. Between the sender and the sender's mail server and between two mail servers, SMTP is used twice. Simply it describes how to give back and forth requests and responses. At the time of execution, each and every network has the freedom to choose a software.



Commands / Responses

All commands or responses are concluded with delimiter token of two-character end of line (carriage return and line feed). Commands and responses are used by SMTP to transmit messages from MTA client to MTA server.



Commands

Commands are sent to the server from the client. The format and commands contain a keyword which is followed by a zero argument or more. It brings out fourteen instructions. The first 5 are necessary that implication of these five commands must help. Sometimes the following 3 are used and highly recommended. Rarely are the last six included.

Keyword: argument(S)		
HELLO	**NOOP**	**211-reply**
MAIL FROM	**TURN**	**214-help**
RCPT TO	**EXPN**	**220-service ready**
DATA	**HELP**	**221-service closing**
QUIT	**SEND FROM**	**250-request**
RSET	**SMOL FROM**	**251-forwarded**
VRFY	**SMAL FROM**	**354-start i/p**
		421-service unavailable
		450-mailbox unavailable
		451-local error

Responses

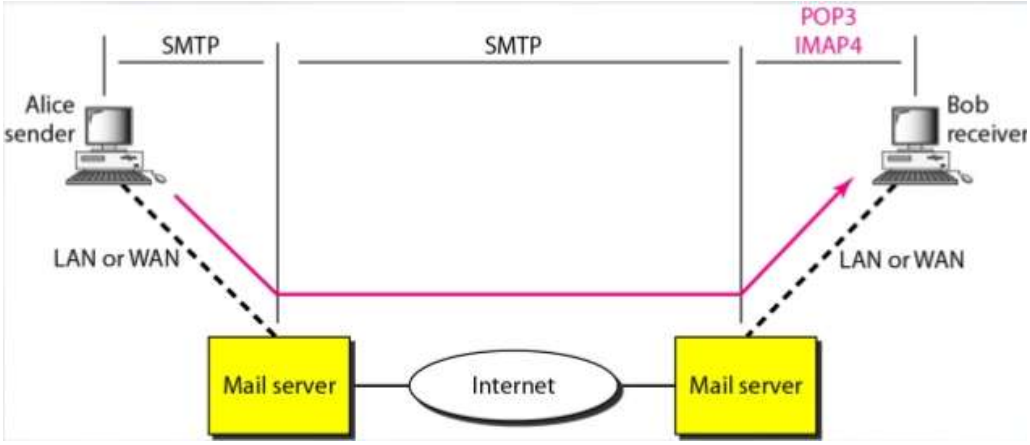
Responses are transmitted to client from server. It is a code of about 3-digit length which can append with additional text.

Mail Transfer Phases

The method of e-mail transmission takes place in 3 phases. They start with connection establishment followed by a mail transfer and ends with connection termination.

C) POP & IMAP: (MAA)

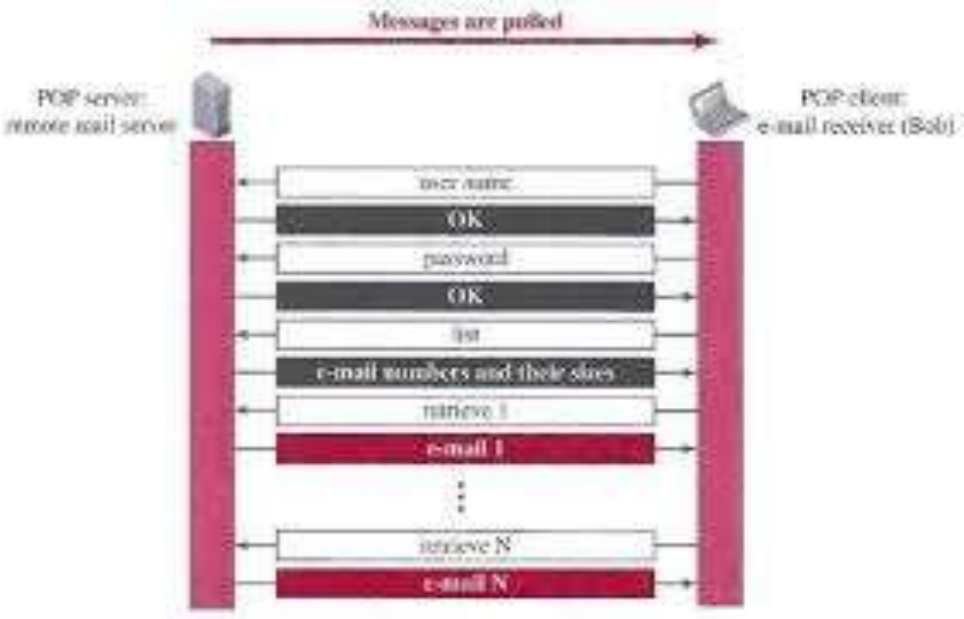
There are 2 messages access protocol. They were Post Office Protocol version: 3 (POP 3) & Internet, Mail Access Protocol version: 4 (IMAP4).



Pop 3

In accessibility, POP 3 is easy & restricted. The POP 3 client software is installed on the receiving machine and the POP3 application software is installed on the mail server. When the user has to retrieve email from the mailbox on the mail server, mail access begins with the client. On TCP port 110 the client opens a connection to the server. If the username and password are then sent to enter the mailbox. The user will then list the mail messages one by one and retrieve them.

There are 2 modes: one mode is delete and the other is keep. After each retrieval, the mailbox's mail will be removed when the mode delete is in progress and widely used while a permanent machine is used by the user. The mail of the mail box stays after retrieval is invoked in keep mode and is preferred while the user is away to access in order to access their initial device. Although the mail gets read, it stays in the organising and retrieval store for future use.



IMAP4

IMAP4 is more active and complex. Prior to uploading, a user should review the email header. Scanning of contents of the email is permissible until it is downloaded by the user. In part, downloading an email by user is possible. If bandwidth stands small and the mail includes multimedia content which demand high bandwidth as its requirements, this is generally advantageous. A user can build mailboxes, remove or rename them. Mailboxes may be created, removed or renamed by a user. In an email storage folder, the mailboxes' hierarchy can be constructed by the user.

5.3. Hypertext Transfer Protocol (HTTP)

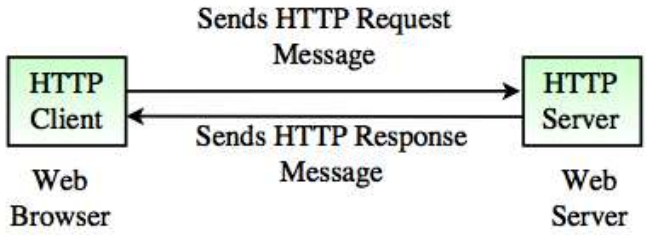
The HTTP is employed mostly for data access on the www. As a mix of FTP and SMTP, HTTP works. This technology reflects the core of FTP, since it shares files along with the utilization of TCP services. HTTP is twinned with SMTP, where the content delivery from client to server is done. The message format is regulated by the MIME-like headers. HTTP utilizes TCP services in a well-known port namely, port 80.

HTTP Transaction

- HTTP transfers between server and client
- HTTP utilizes TCP services; HTTP is considered as a stateless protocol itself.
- The transaction is initialized by the client by transmitting a request message.
- The server responds with a reply message.

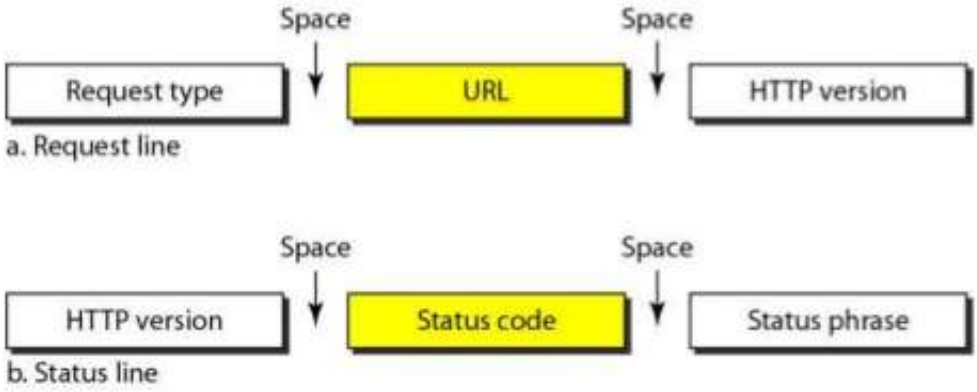
Messages

The request message is a request line, a header with a body whereas a response message is a status line, a header which seems to be a body.



Request and Status Line

A request line is considered the first line of request message. The request line is termed as a status line of response message.



Request Type

The request type is categorized into methods and this field is useful for request message.

GET	requests a document from source
HEAD	requests info about document
POST	sends some information
PUT	sends a document
TRACE	echoes the incoming request
CONNECT	reserved
OPTION	inquiries about available options

Version

The version 1.1 is observed to be the recent one of HTTP.

Status Code

It is a part of the message sequence which is identical to the one in FTP as well as SMTP protocols. It contains a 3-digit code of range. They are,

100 ranges - informational
200 ranges - successful request
300 ranges - connects to another URL
400 ranges - error at client site
500 ranges - error at server site

Status Phrases

Response message utilizes by the field and status code is described in the text format.

Header

The client and server get some additional information that will be shared by header. One or extra lines of header is found at the header. Each header line has a name for the header, a column, and a space and a value for the header. The header line may go in with any of the mentioned 4 groups under General or Response or Request or Entity.

A request header consists of general request and an entity header. A response header consists of general, response and an entity header.

Header Name: Header Value

General Header

General information is available for the message and can be found in requests and response, is provided in the general header.

Connection	- Shows if the connection is to be terminated or not
Date	- Displays the current date
MIME-version	- Shows MIME version
Upgrade	- Notifies which communication protocol is preferred

Request Header

The request header is blocked only when a request message is invoked and clients' configuration and the format of the document is specified.

Accept	Shows the client accepts.
Authorization	Shows permission held by the client
From	Shows email address
Host	Shows host and port number
User-agent	Identifies the client program.

Response Header

The response header can only be blocked by a reply message and also specifies the configuration of the server and the basic details on the request.

Age	Shows age of the document
Server	Shows the server name & version
Public	Shows the supported list

Entity Header

The information regarding the body of text is held in this header, which is represented in the methods of response messages or request messages, namely POST or PUT along with a body.

Body

The body might be found in the request or reply message. It demands a request to either transmit or retrieve.

Proxy Server

HTTP is supported by proxy servers which is a machine holding the response copy that is a recent one. Proxy server will receive a request from the HTTP client and its cache will be reviewed. When the cache contains the response, the response would be sent by the proxy server to the corresponding server. It receives the incoming response and process to align with the future requests of other clients.

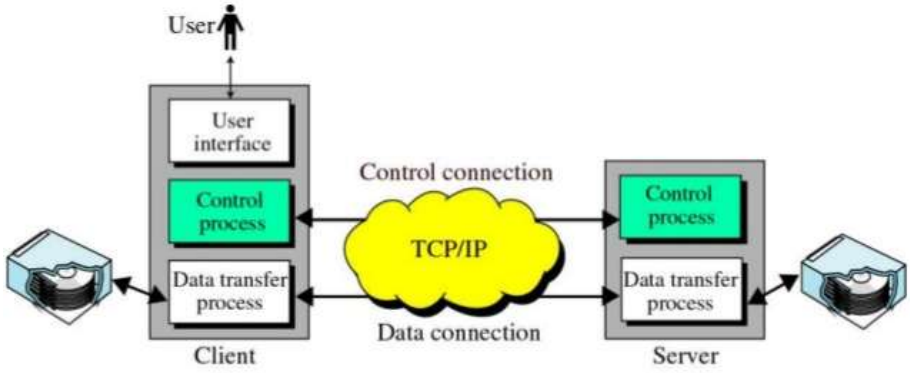
File Transfer

File transfer is an essential and a very important task required during the transfer of files from a device to another, be it in intranet or internet.

5.4. File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is used to copy a file from one host to another host. It is a standard mechanism which is provided by TCP/IP. It separates commands and transferring

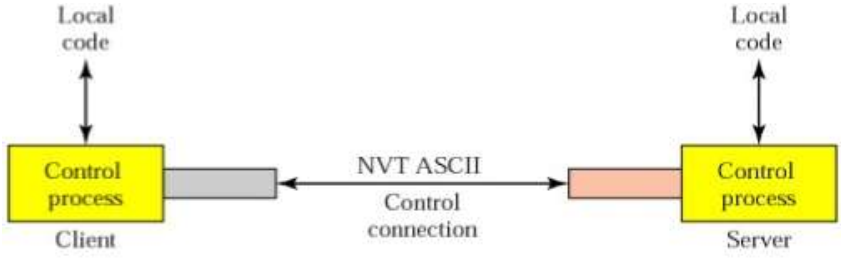
data makes FTP more effective. FTP uses the TCP operation. It require two connectivity to the TCP. The well-known port 21 is used for control connection and the well-known section 20 for network connectivity. There are three components in the client: the user interface, the device control and the data transfer. There are two components in the server: the server control process and the server transfer process. The control is done by the control communication and the data transfer is done by data link.



The connection control is connected throughout the FTP session. For each file transfer the data connection is opened and closed. It opens when the commands that require moving files are to be used and when the file is moved, it will be closed.

Communication Over Control Connection

FTP uses the same technique as SMTP to communicate over a control link. It uses a set of 7 bit ASCII characters. Communication is carried out by each command or response is a short line. The termination for each line is done by two characters that are line feed and carriage return at the end-of-line token.

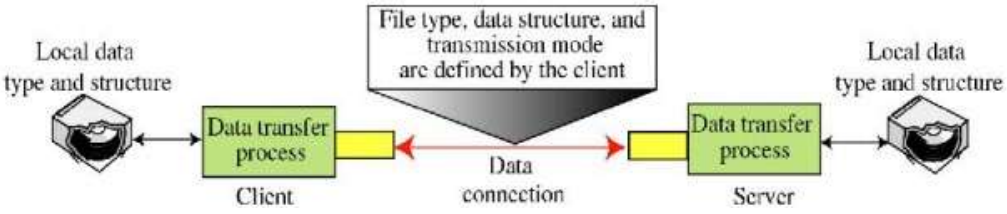


Communication Over Data Communication

It is different from the purpose of the control connection. The transfer of file takes place over the data connection link under the supervision of the commands sent over the control connection.

There are 3 things to transfer in FTP:

1. The file which is copied from the server to the client is said as retrieving a file and it is performed by the command RETR.
2. The file which is copied from the client to the server is said as storage of a file and it is performed by the command STOR.
3. A list file names or directory must be sent from the server to the client by the command LIST.



The client must specify the type of file to be transmitted, the configuration of the files and the mode of transmission. Before sending a file through a data connection, forward it through a control connection. The heterogeneity problem is overcome by specifying three contact attributes:

- File type
- Data structure
- Transmission mode

1. File Type

File type is used to transfer any one of the following over a connection of data; an ASCII file, an EBCDIC file or an image file. The ASCII file is used to transfer text files; it is said as the default format. The EBCDIC file format is used to transfer EBCDIC encoding and it is used by IBM. The image file is used to transfer binary data it is said as the default format.

2. Data Structures

A file which is transferred as data link through one of the structure of data interruptions:

- File structure
- Record structure
- Page structure

A continuous stream of bytes was used in this file structure format. It is divided into records (file: text) in the record structure. In the page structure, the files are divided into pages with a page number and a page header for each page.

3. Transmission Mode

A file which is transferred as data link through FTP by anyone of the 3 following modes of transmission:

- Stream mode
- Block mode
- Compressed mode

The default mode of data is provided from File Transfer Protocol to Transmission Control Protocol as a continuous stream of bytes in stream mode. Data can be delivered from FTP to TCP in block mode. In compressed mode, if the file is large, the data can be compressed.

Anonymous FTP

A user should have an account that is user name and password on a remote server to use FTP. Some pages will provide a collection of information that may be available for public access so it is said to be as anonymous FTP access. You don't need an account or password to access these files. An anonymous user can be used as a username and a guest as a password.

5.5. World Wide Web (WWW)

The World Wide Web (WWW) is a repository of knowledge linked from all over the world. The WWW has a special combination of versatility, portability and user-friendly features that differentiate it from other internet services. The www project was initiated by CERN.

5.5.1. Architecture

World Wide Web is a browser based client which can access through a server so it is said to be a distributed client/server. The server supports through a variety of locations called sites.

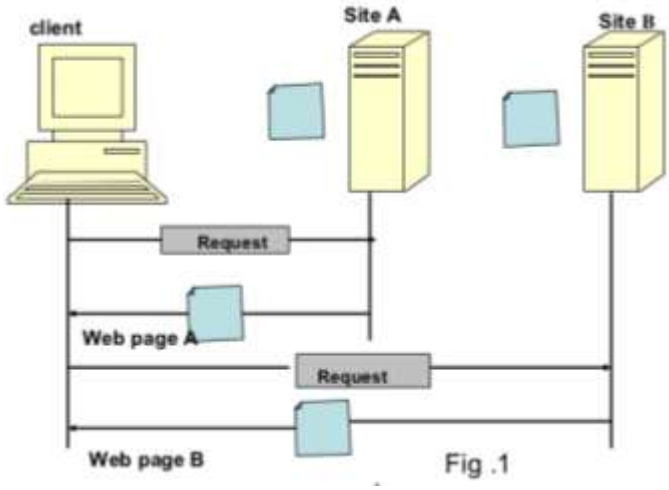


Fig .1

One or more documents in each site is said to be as web pages. Each page links with another page on the same or on other pages. Each site contains one or more documents referred to as web pages. Each page can contain a link to another page on the same site or on other pages. Pages can be retrieved and accessed using a browser.

5.5.2. Client (Browser)

A number of vendors provide commercial browsers that interpret and display a web document and all use almost the same architecture. Each browser is normally made up of three sections.

- Controller
- Client protocol
- Interpreters

The controller will receive input from the keyboard or mouse and will use the client programmes to access the text. The controller will use one of the interpreters to view the text on the screen. The client protocol can be one of the mentioned protocols (FTP / HTTP). The interpreter can be an HTML, Java or Java script, depending on the type of document.

5.5.3. Server

The website is stored in the server. Every time a client request arrives, the corresponding document is forwarded to the client. To improve efficiency, servers usually store the requested files in the memory cache; the memory is faster to access than the disk. The server can also be made more effective by multi-threading or multi-processing. The server can respond to more than one request at a time.

5.5.4. Uniform Resource Locator (URL)

A client who wants to access a website requires an address. HTTP uses locators to allow access to documents scattered around the world. The URL is a standard for specifying any type of information on the Internet. The URL describes four things:-

- Protocol
- Host computer
- Port
- Path

Protocol:// host : port / path

The protocol is a client / server program that is used to retrieve a document. A document can be obtained by several different protocols, including HTTP/FTP. The information is stored

on the host; the name of the machine can differ. The web pages are mainly stored in the computers and the alias names were given to computers that usually start with "www" characters. The URL has the port number of the server. When it is in usage it can be inserted between the path and host. A colon is used to separate from the host. The path name of the file is used to store the information.

Cookies

The www was actually designed to be a stateless body. The client is sending a request; the server is responding. It retrieves the accessible documents publically which suits this function.

1. The registered clients will have access for particular websites.
2. Websites can also use as electronic shop.
3. It allow users to search and select the content what they want, add them in cart and pay at the end.
4. Users can choose the website as portals when they want to visit the website.
5. Some of the blogs are all ads.

Creation and Storage of Cookies

The production and storage of cookies depends on the implementation, but the concept is the same.

1. When a server receives a request from a client, it stores the client information in a file or in a strong file. The details may include the client's domain name, cookie content, time stamp and on the development.
2. Client response side also has a cookie which is sent by the server.
3. The browser stores cookies in the cookie directory once client receives a response and that is aligned in the DNS.

How to Use Cookies

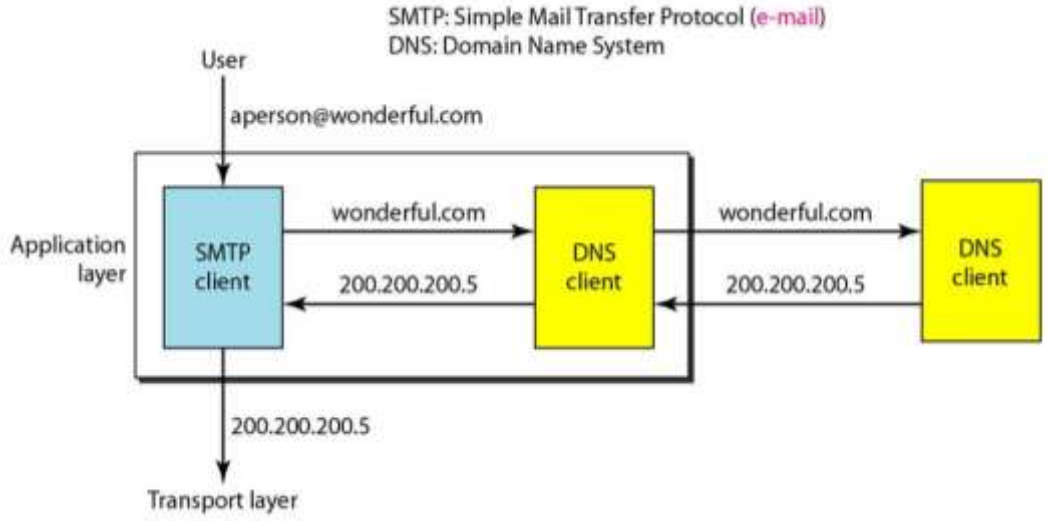
When a server receives a request from the client, the web page will search the directory of cookies to check whether server received cookies. It includes the request when the cookie is found. The server should understand whether it is an old client or new client when it receives a request. It's a cookie made by the server and eaten by the server.

1. The registered clients have a limits access to send a cookie to the client when it is registered first.
2. Client shoppers use an electronic store to use a cookie.

3. The web portal uses cookies to submit the server to reveal what the client is searching for.
4. Advertising companies often use a cookie.

5.6. Domain Name Systems (DNS)

Domain Name Systems (DNS) is support software used for other applications such as e-mail. The recipient's email address may be known to the user of the email program. The IP address was required in the IP protocol. The DNS server receives the request to the DNS client which helps to map the e-mail address with its corresponding IP address.



To define an entity TCP / IP protocol, use an IP address that uniquely identifies the connection of a host to the Internet. The host that needs mapping can contact the lost computer holding the information needed for this method to be used by the DNS.

Namespace

A unique name maps the each address in namespace and it can be arranged in two ways they are,

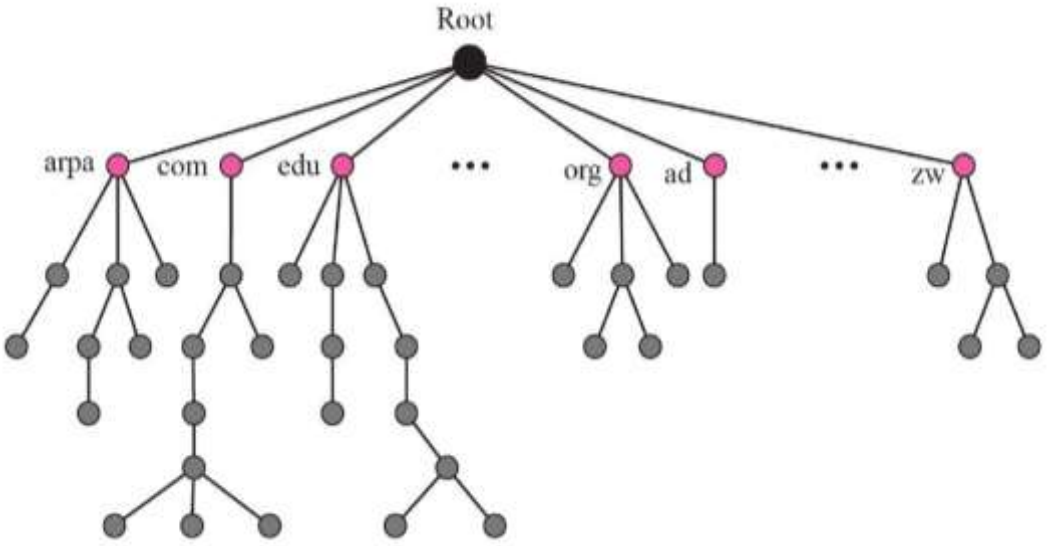
- Flat namespace
- Hierarchical namespace

5.6.1. Flat Name Space

In name space, the name is allocated to an address. Sequence of characters without any structure is said to be a name. they does not have any meaning to have a common section.

5.6.2. Hierarchical Name Space

Each name is made up of many parts in the hierarchical name space. The first part can define the meaning of the organization, the second part can define the name of the organization, and the third part can define the sections of the organization and so on. A central authority may assign a part of the name that defines the goal of the system and the organization name.



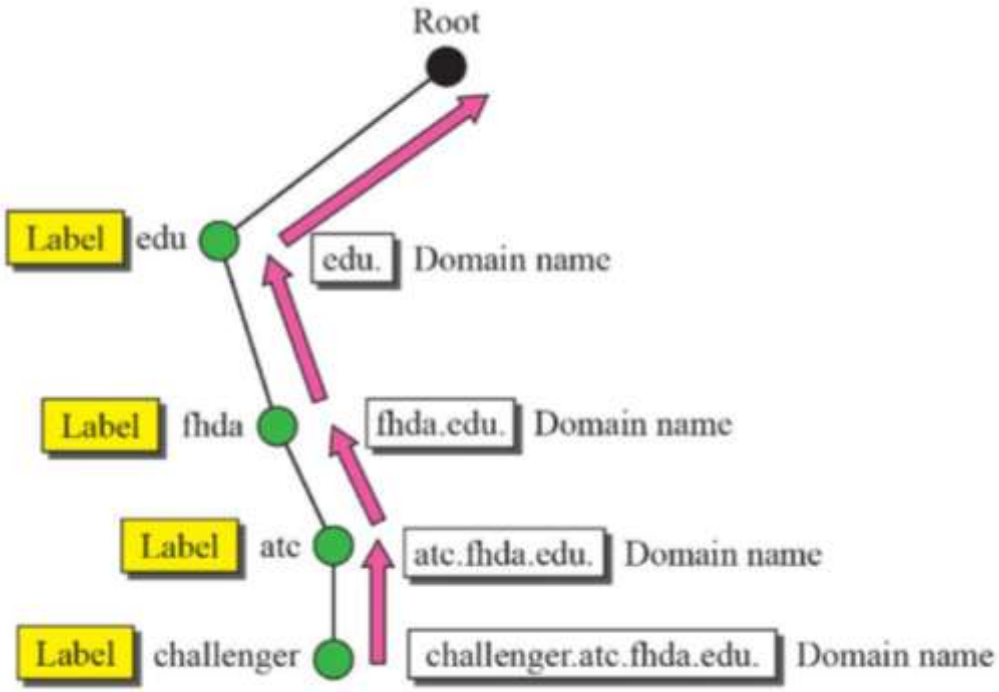
A domain name space has been designed to have a hierarchical name space. From the top level of the inverted tree it is said to be as names. The tree can only have 128 levels and it starts from level 0 (root) to level 127 (nodes).

Label

A node in the tree has a name, a string with a maximum of 63 characters. The root label is a null string or an empty string. DNS requires that node children (nodes that branch from the same node) have separate labels that ensure the uniqueness of domain names.

Domain Name

Each node in the tree has a domain name. The full domain name is separated by dot (.) for list of labels. Domain names are read from the node to the root. The last label is the root mark said to be as null, which means that the full domain name always ends in the null mark. The last character is a dot which means the null string is nothing.



Fully Qualified Domain Name (FQDN)

If a label is terminated by a null string, it will be considered a fully qualified domain name.

Eg:- challenger.atc.fhda.edu

It includes the entire host name which contains all the labels. It specifies the most general and uniquely defines the host name. Only a FQDN can match a DNS server to an address. The name must end with a null mark and since null means nothing the label will end with a dot (.)

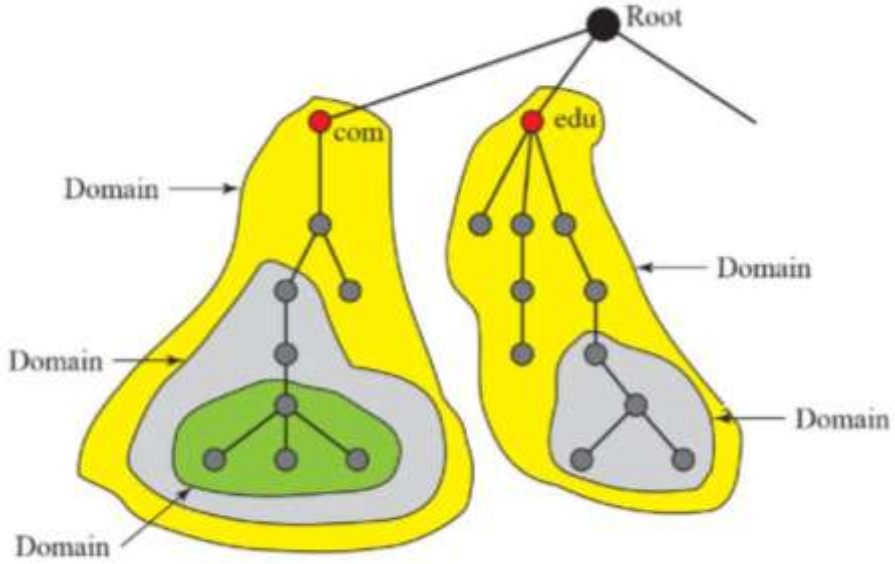
Partially Qualified Domain Name (PQDN)

Partially Qualified Domain Name (PQDN) is said when a label does not transmit a null string. It starts from the node, and doesn't reach the root. When the name is fixed on same site as client PQDN is used. The missing element is said to be as suffix to generate FQDN.

Eg:-challenger User->fhda.edu

Domain

In DNS, the domain is a sub-tree. The domain name is the name given for the node at the top level. It divides domain into subdomain by itself.

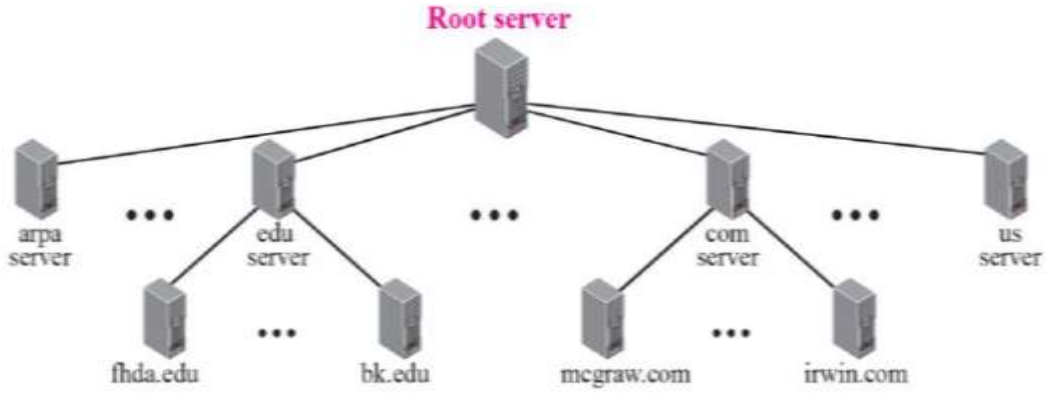


5.6.3. Namespace Distribution

The solution to these problems is to transmit information to a number of computers called the DNS service. It divides the entire space into a number of domains centered on the first level.

Name Server Hierarchy

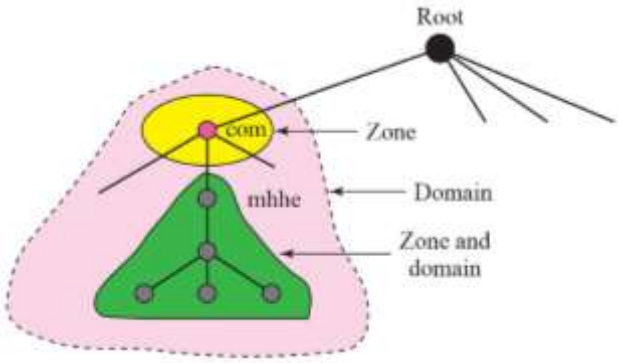
The information which found must be processed in the DNS. This is not accurate and quite expensive to store such a large amount of knowledge in one computer.



In DNS, domains are divided into subdomains. Each server is responsible for each domain either it is large or small.

Zone

The entire hierarchy cannot able be store on a single server, so it has been splited between multiple servers. What a server is responsible for or has authority over is referred to as a zone. If the server takes responsibility for the domain and does not break the domain into smaller domains, the domain and the zone will refer to the same thing.



Root Server

The root server is holds the entire tree. It does not store any information from domain, but it assigns permission to another server by referring other servers. The root servers cover the entire domain name space. The server is spread all over the world.

Primary and Secondary Server

DNS server was divided in to 2 types: one is primary and another is secondary.

A server stores a file for authority is said to be as the primary server. It is mainly used for developing and managing the zone. It is saved in the local drive.

A server which is used to transfers the complete information about the zone to another server which can either be a primary or secondary and it stores the data on the local drive. This type of server does not build or change zone files. The primary server loads all information from the secondary server disk file and loads all information from the primary server. When secondary information is downloaded from the original, it is called zone transfer.

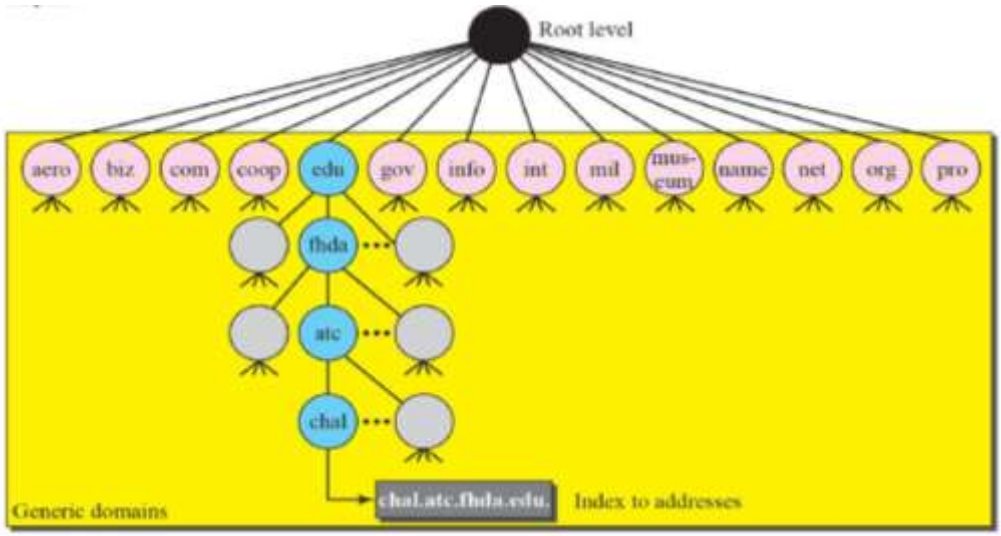
5.6.4. DNS in the Internet

DNS protocol is used in various platforms. It is divided as 3 sections in the internet:

- Generic domain
- Country domain
- Inverse domain

1. Generic Domains

Generic domains identify registered hosts by their generic behavior. Each node in the tree defines a domain that is an index to the domain name space database.



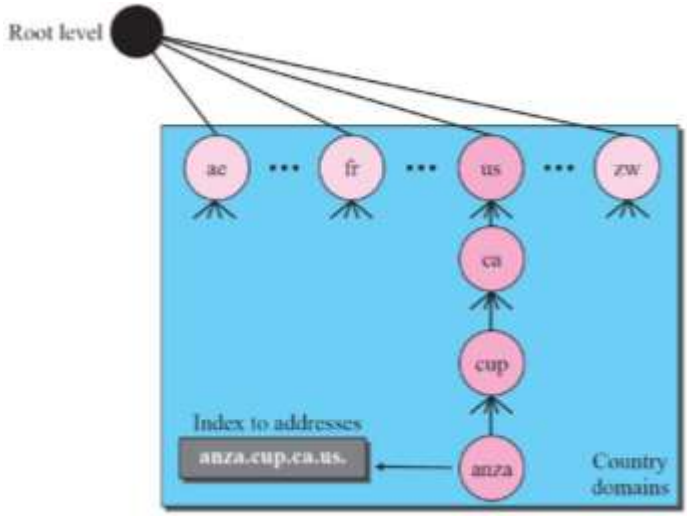
Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other non-profit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

2. Country Domains

In this section, two characters were used as abbreviation to display a country.

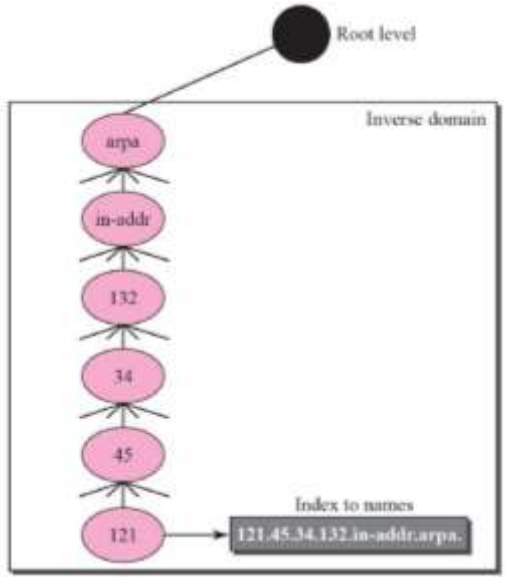
Eg:- US for United States

For organization or national destination, second labels were used.



3. Inverse Domains

Inverse domain is used to map a name address. (e.g) when the server has received a request from the client to perform an operation. The server has a file containing a list of authorised clients with only the IP address of the client. The server asks to send a request to the DNS server to map the address to the name to decide whether the client is on the authorised list. This type of query is called the inverse or pointer (PTR) query. To manage a pointer query, the inverse domain is applied to the domain namespace with the first level node called arpa and the second level is just a single node named in-addr. The rest of the domain will determine the IP address.



Mapping

Name address resolution is mapping a name to an address or a name address.

Resolver

A client/server program is designed by DNS. A host which maps an address to a name or a name for an address can call a DNS client called a resolver.

Mapping Name to Addresses

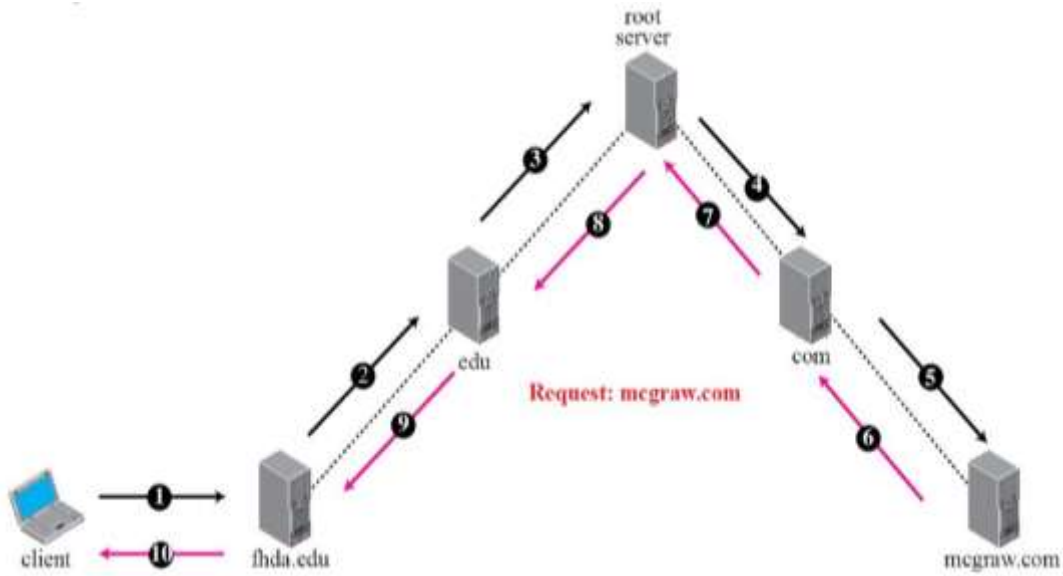
Resolve gives the server a domain name and asks for the corresponding address. For mapping, the server checks the generic domain or the country domain.

Mapping Addresses to Names

An IP address is sent by the client which is mapped to domain name to the server.

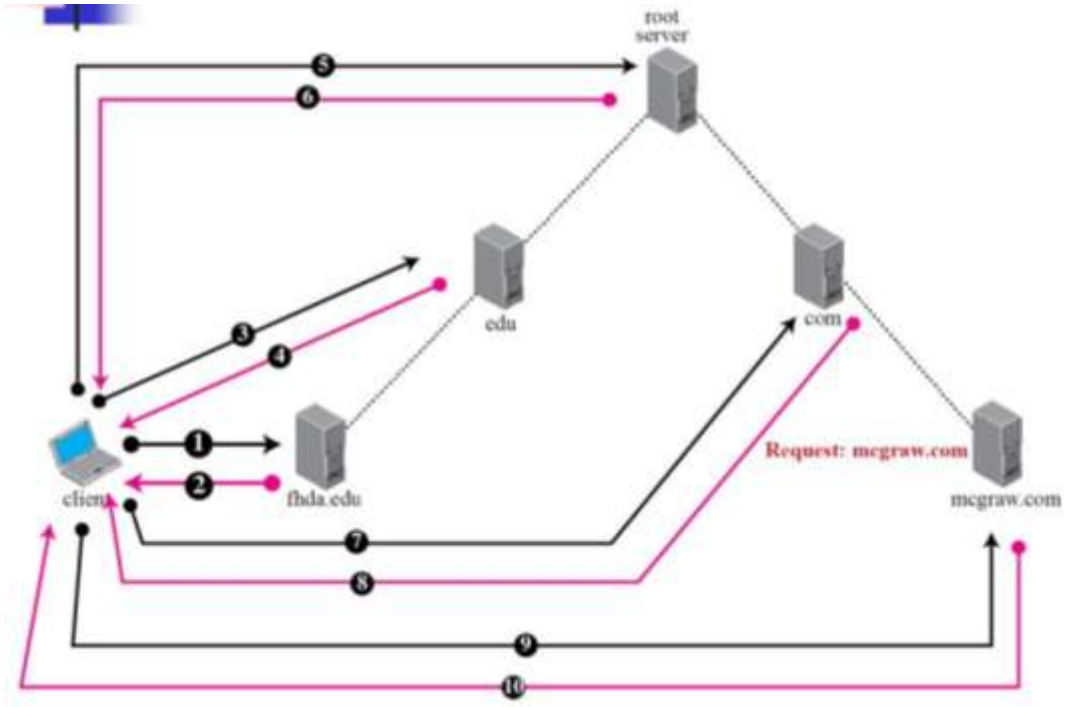
Recursive Resolution

A recursive response will be requested by the client from the name server. Server waits for the final response to be applied. If the server is the domain name authority, it checks the database and responds. If the server is not an authority, it sends the request to another server (usually the parent) and waits for the response If the parent is the authority that responds otherwise, the request would be sent to another server. When the request is eventually resolved, the answer will move back before it finally reaches the requesting client. This is called a recursive resolution.



Iterative Recursive

If the client does not ask for a recursive answer, mapping can be done iteratively. If the server is the name authority, it sends the response or returns the IP addresses of the server that it thinks can resolve the query. It is the duty of the client to repeat the query to this second server. If the newly addressed server is able to resolve the query, it will answer the query with the IP address to return the new server's IP address to the client. The client must now repeat the query to the third server. This method is called a recursive iterative.



Caching

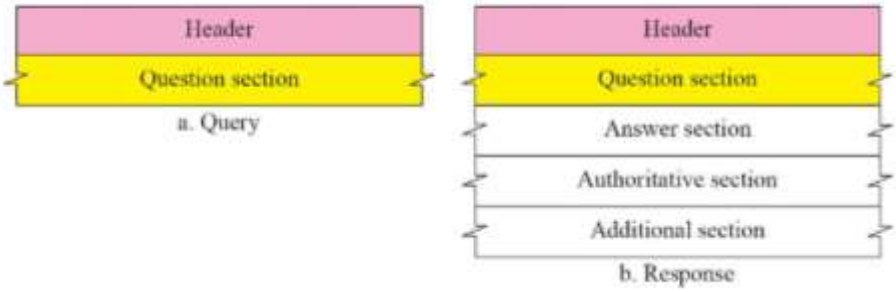
When a query is received at server side which is not in domain, a server IP address needs to be searched for in its database. Reducing this search time will improve productivity. This process is called caching.

5.6.5. Messages in DNS

There are two types of DNS message: request and response. In request message, the header and query records are placed and in response message, the header, query records, reply records, authoritative records and additional records are found.

Header

In same header, both response and request messages filled as zero for query message in certain fields.



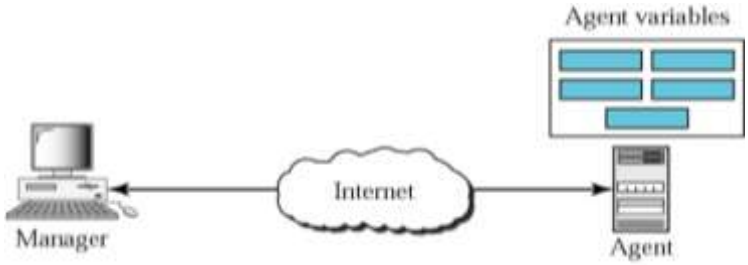
The client uses identification to fit the response to the query. Every time question is sent, the client uses a different identification number. The flags determine the form of the message the form of desired resolution. In sub field, the count of request records includes the count of response records of the message. The count of response records in the sub-field includes the count of response records in the reply portion of the reply letter. The count of authoritative parts includes the count of authoritative records in the authority's part of the responses. The count of additional ones in this includes the count of additional records in the additional portion of the responses.

5.7. Simple Network Management Protocol (SNMP)

A mechanism which is used for controlling devices using Transmission Control Protocol/Internet Protocol on the Internet is said to be as Simple Network Management Protocol (SNMP). Mainly collection of basic operations are monitored and maintained in the Internet.

5.7.1. Concept

The concept of manager and agent is used by SNMP. The host manager normally manages and tracks a group of agents, normally the header.



An application level protocol which has a few management stations to manage the number of users/agents. It is structured at the stage of the application; it can control the system which is created by various mechanisms. It is mounted on different physical networks. It releases control functions from both the physical features of managed devices and the underlying networking technologies. Heterogeneous connection is done at different LANs and WANs network which connected by routers in SNMP.

Managers and Agents

The manager acts as a host who running the SNMP client program. An agent called management station where a router running the SNMP server program. Management is accomplished by clear contact between the agent and manager. The output details are stored in the database by the agent. The value in the database and router navigation is done by manager. Agents can also contribute to management process.

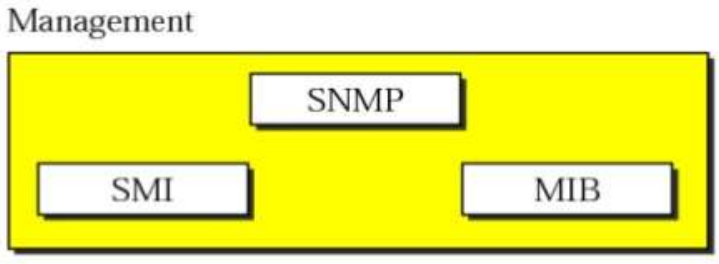
The process status will be checked by agent who running the server program and, if anything went wrong, an alert message will be send called a trap to the manager. SNMP is based on three simple concepts.

1. The manager checks the agent by requesting information that reflects the behavior of the agent.
2. The manager requires the agent to perform the assignment by resetting the value in the agent database.
3. The agent contributes directly to the management process by warning the manager of an unusual situation.

5.7.2. Management Components

SNMP uses 2 protocols to perform management tasks. They are,

- MIB - Management Information Base
- SMI - Structure of Management Information



Role of SNMP

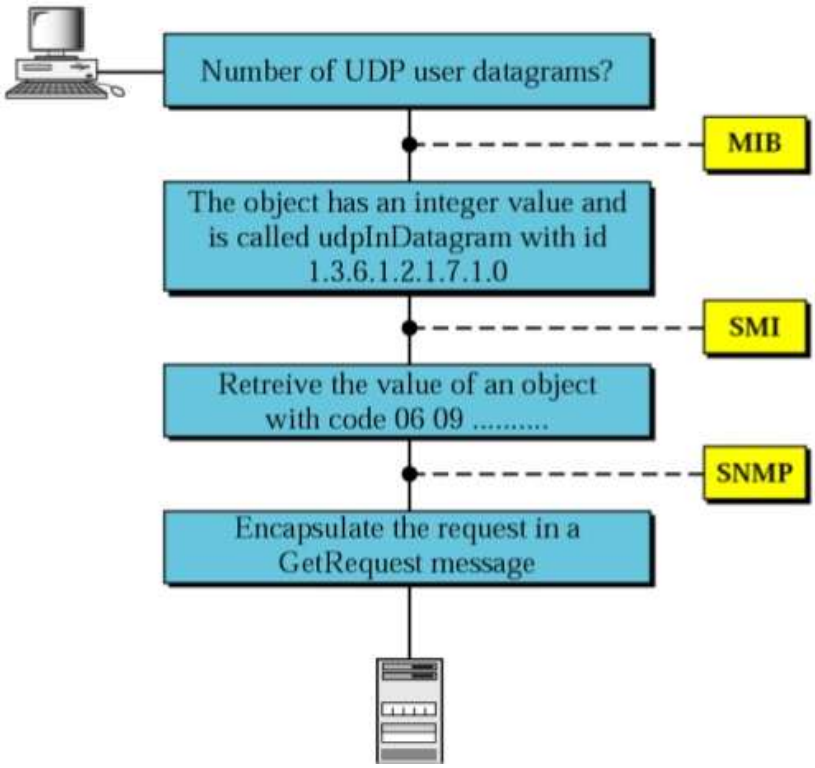
- Reading and altering is carried out by SNMP.
- Exchanged packets have object name and its status. It interprets the statistics which produced and outcomes.
- It has many important functions in the network management.
- The packet format which sent from the manager to the agent is determined, and also vice versa.

Role of SMI

- SMI specifies the common rules to name types of entity range and its length and demonstrates the values and objects production.
- It does not specify objects count where the entity can control or managed by the objects name and establishes the relation between values and object.

Role of MIB

- A list of named objects, forms and its relationship between the entity are generated and controlled by MIB.



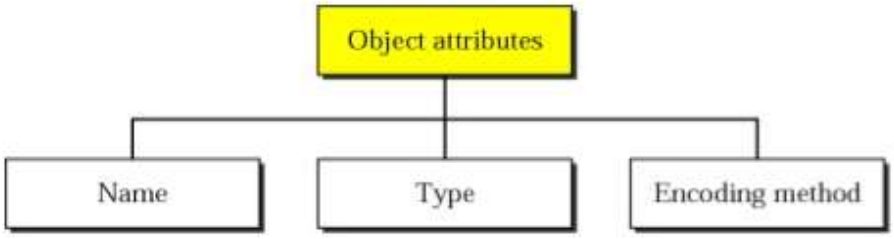
5.7.3. Structure of Management Information (SMI)

The structure of management information version 2 (SMIV2) is a network management. The properties include:

1. Object name.
2. Data type should be defined to store in the object.
3. Data transmission over the network.

SNMP guides the structure of management information and it has 3 attributes to treat it as an object,

- Object name
- Data type
- encoding method



Name

A hierarchical identifier is used to identify the objects in SMI like a tree structure to label objects globally. It always starts with 1.3.6.1.2.1.

Type

Abstract Syntax Notation 1 (ASN.1) is used to define the data type in SMI. It acts as a subset and also a superset, and two large categories of data types were used.

- Simple
- Structured.

Simple

Efficient data types all types of atomic data. The remaining types are taken directly from ASN.1 and added by SMI.

5: ASN.1 & 7: SMI

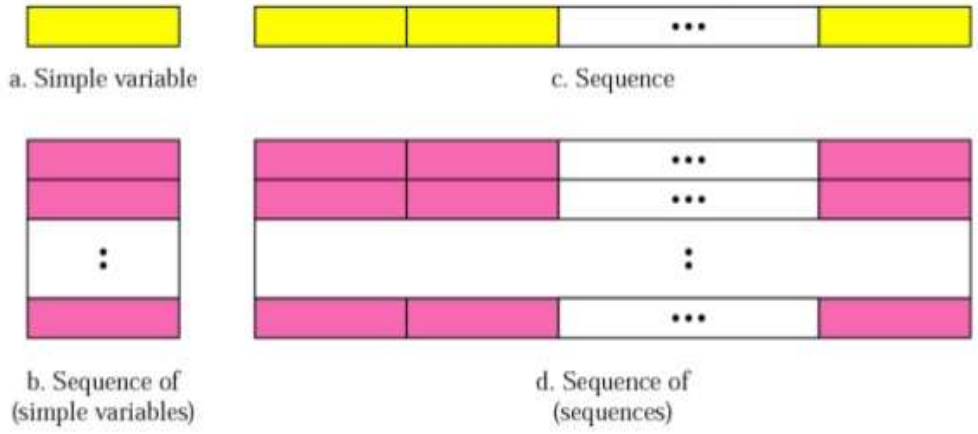
Integer	4 bytes
Integer 32	4 bytes

Unsigned 32	4 bytes
Octet string	variable
Object identifier	variable
IP address	4 bytes
Counter 32	4 bytes
Counter 64	8 bytes
Gauge32	4 bytes
Time ticks	4 bytes
BITS	bits
Opaque	variable

Structured Type

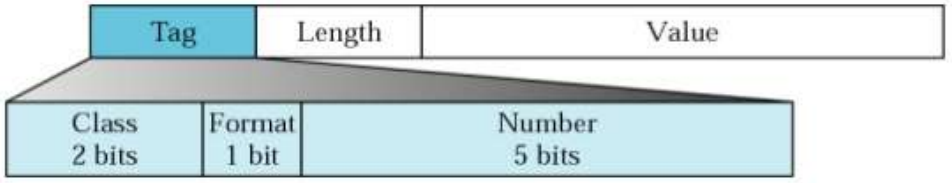
There are two types in SMI structured data. They are:

1. **Sequence:** It is a collection of basic data forms.
2. **Sequence of**: It is a combination of a single/sequence data type of the same type.



Encoding Format

Basic Encoding Rules (BER) is used to encode data which is going to be transmitted over the network. It indicates all the data to be encoded in a triplet format as follows:



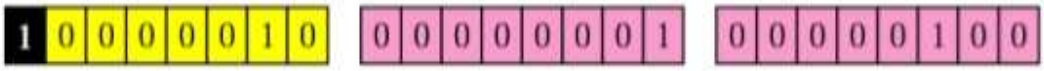
Tag

This field is used to specify the data type. Its field is 1 byte and consists of three sub-fields. They are 2 bits for Class, 1 bit for format and 5 bits for number. These subfield are used to indicate whether the data is simple (n) or structured (i).

Length

In this field, the length may be 1 or more bytes. The MSB will be 0 when it is 1 byte and the data length is defined by other remaining 7 bits.

a. The colored part defines the length (2)



b. The yellow part defines the length of the length (2 bytes); the pink bytes define the length (260 bytes)

Value

In this field, the data values are coded by BER rules.

5.7.4. Management Information Base (MIB)

In network management MIB 2 that is Version 2 of the Management Information Base is the second aspect. The manager is able to handle each agent with its own MIB objects. These objects are classified by 10 groups. They were interface, ip, udp, system, tcp, address translation, icmp, egp, snmp tables, variables and transmission are specified in each category.

sys	system
if	interface
at	address translation
ip	IP address
icmp	ICMP
tcp	TCP
udp	UDP
snmp	SNMP

MIB Variable Access

Simple Variables

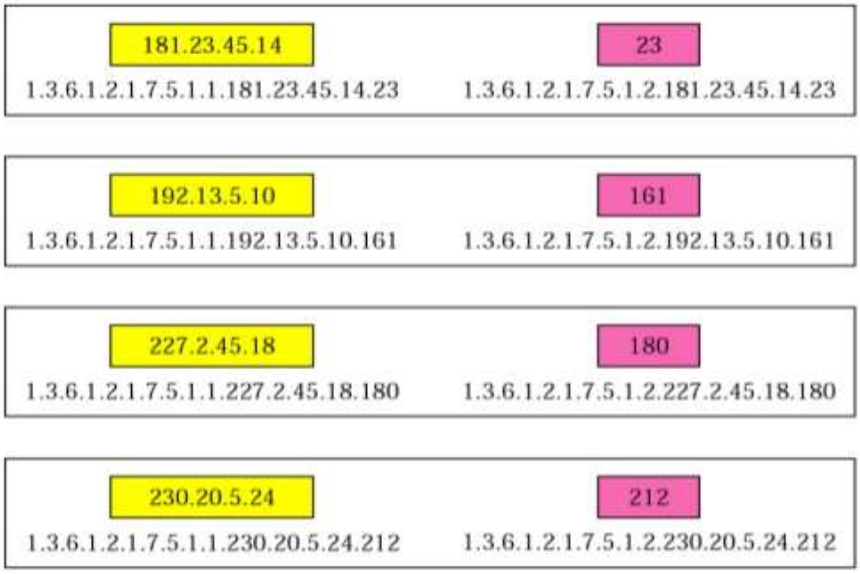
Simple variables are accessed by using the group ID (1.3.6.1.2.1.7) followed by the variable ID.

- Udp in datagrams ->1.3.6.1.2.1.7.1
- Udp no ports->1.3.6.1.2.1.7.2
- Udp in errors->1.3.6.1.2.1.7.3
- Udp out datagrams->1.3.6.1.2.1.7.4

Tables

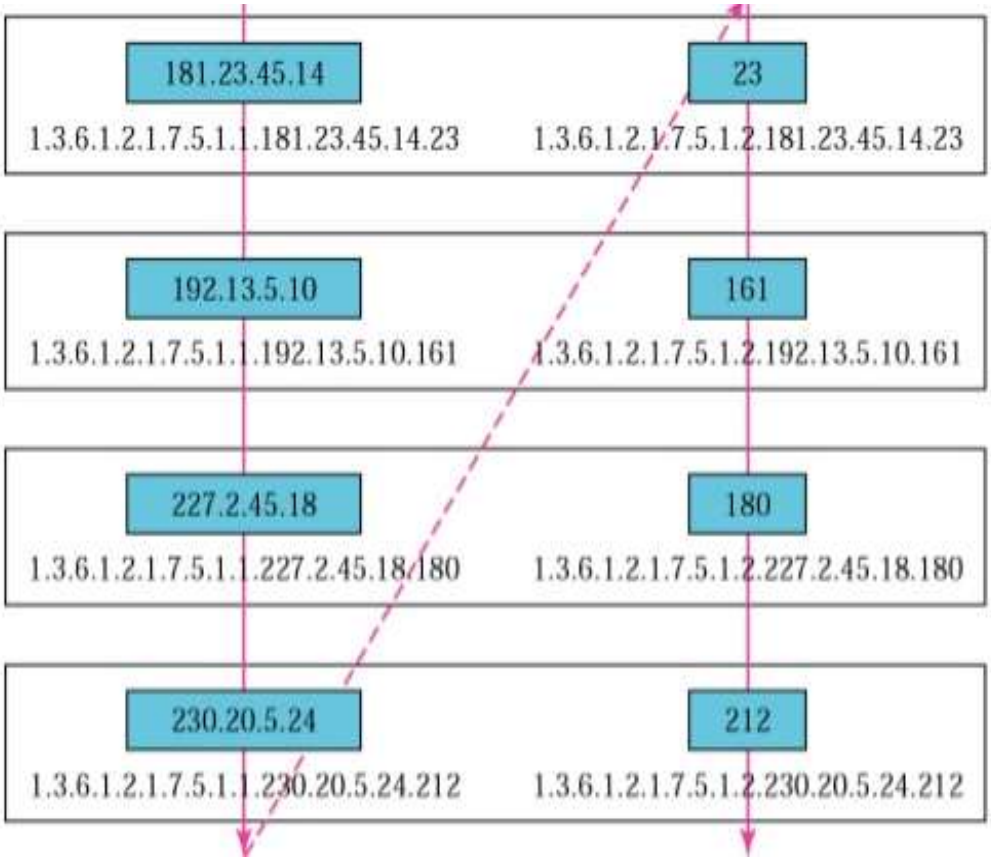
The udp creates tables with table id.

- Udp table->1.3.6.1.2.1.7.2
- Udp entry->1.3.6.1.2.1.7.5.1
- Udp local address->1.3.6.1.2.1.7.5.1.7.
- Udp local port->1.3.6.1.2.1.7.5.1.2



Lexicographic Ordering

An object identifier over the variables of the MIB is ordered by lexicography. It will be sorted by column row table manner, which means top to bottom of the column. One should go from top to bottom in each column. The manager should have access to set a variable after the first variable over the next by lexicographic ordering.



SNMP

For Internet network control in SNMP, it uses both MBI and SMI. SNMP is application software where,

1. An object is identified by the agent to manager to retrieve the value.
2. A value is stored in agent specified object by manager.
3. A warning on irregular process is given by agent to the manager.

PDUs

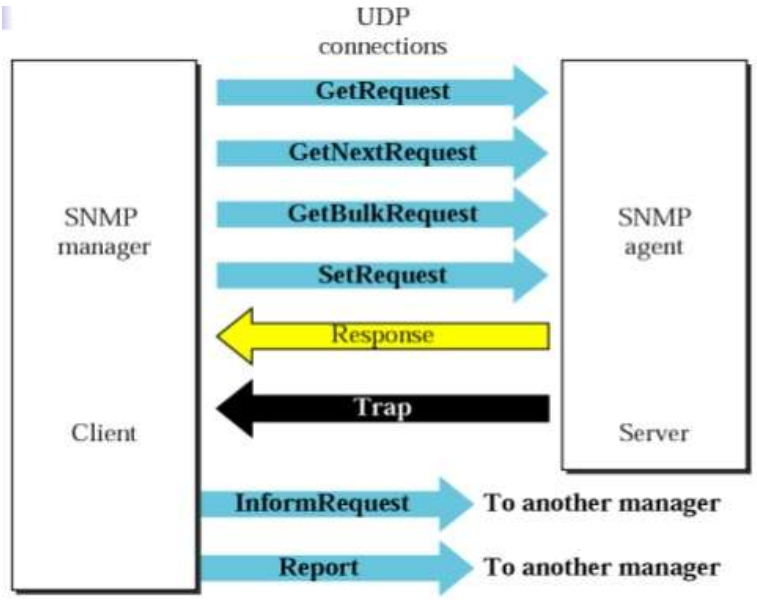
There are 8 packet types in SNMP Version 3. They are,

-> get request -> response

-> get bulk request -> trap

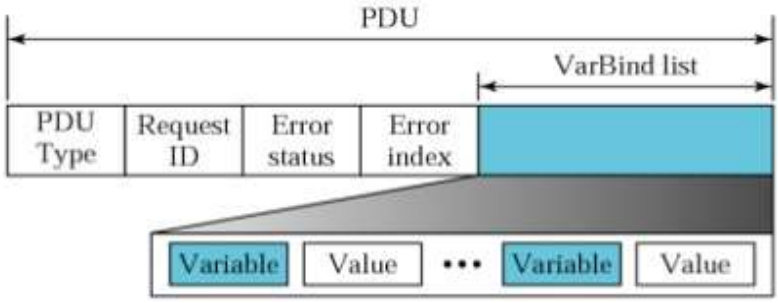
-> get next request -> information request

-> set request -> report



Format

This format is for the 8 SNMP PDU**.** The get bulk request PDU differs from the others in 2 areas.

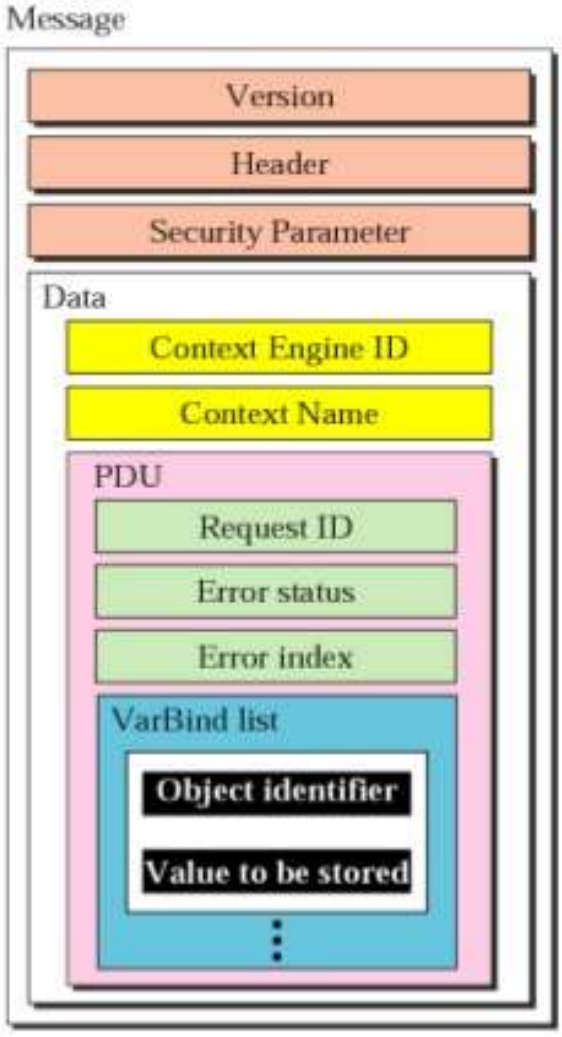


The status and error index values are zero for all request messages except to get a bulk response. Error status field is replaced by a non-repeater field and the error index field is replaced by a max-repeater field in get bulk request. The fields are listed.

- **PDU type -** Says the type of PDU.
- **Request ID -** Denotes sequence number and agent response over the PDU request.
- **Error status** - Reports the error type by the agent.
- **Non repeaters -** Replaces the error by using GetBulkRequest.
- **Error index -** Indicates the index of the error to the manager.
- **Max-repetition -** Replaces the error which is empty by using GetBulkRequest.
- **Var bind list -** Variables with values can be set or retrieved when manager wants.

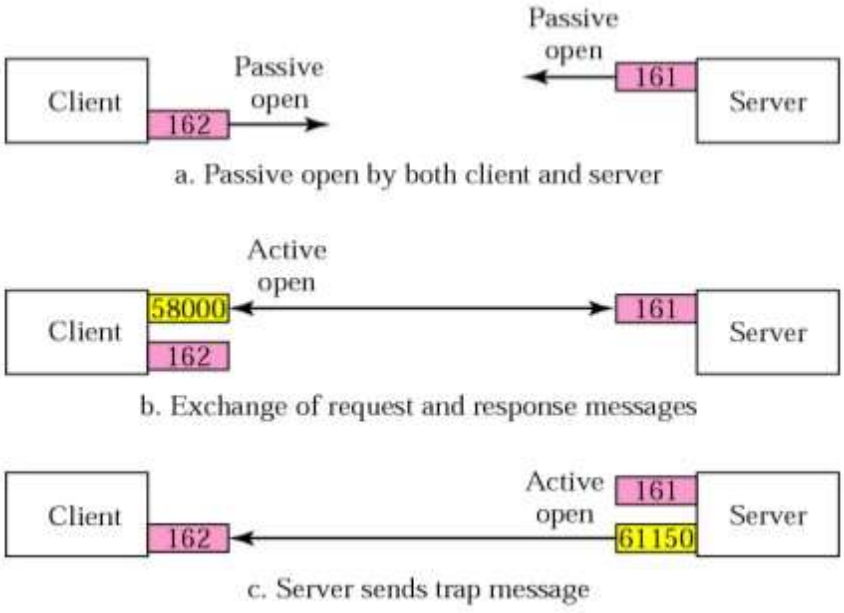
Messages

The SNMP encloses the PDU in a message. The SNMP Version 3 message consists of version which describes the new version as 3, the header includes the message identification values of the message size and how message protects, and the security message parameter is used to build a message digest. The data contains the PDU. SNMP uses a tag to describe the form of PDU. The class is sensitive to context (10).



UDP Ports

161 - Server (as agent) and 162 - Client (as manager) are the two ports used by SNMP. The port 761 is a server's passive open and port 162 is a client's active open.



5.7.5. SNMP Securities

The two securities are given by SNMP version 3. They are specific and general. SNMP Version 3 offers authentication of messages, anonymity and management authorization. It allows the manager to change the security configuration remotely. It also ensures that the manager does not have to be physically present at the manager station.