UNIT V

APPLICATION LAYER

WWW and HTTP – FTP – Email –Telnet –SSH – DNS – SNMP.

5.1 WWW

The World Wide Web (WWW) is a repository of information linked together from points all over the world. The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet

Architecture

The WWW today is a distributed client/server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called sites.

Each site holds one or more documents, referred to as Web pages. Each Web page can contain a link to other pages in the same site or at other sites. The request, among other information, includes the address of the site and the Web page, called the URL.

The server at site A finds the document and sends it to the client. When the user views the document, she finds some references to other documents, including a Web page at site B. The reference has the URL for the new site. The user is also interested in seeing this document. The client sends another request to the new site, and the new page is retrieved.

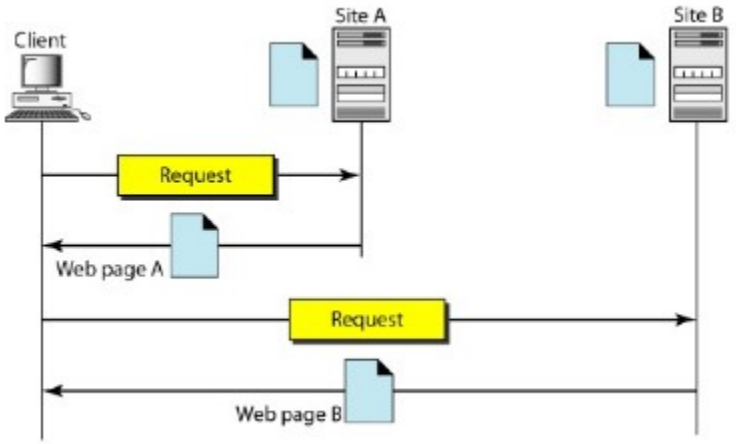


Figure 5.1 Architecture of WWW

Client (Browser)

A variety of vendors offer commercial browsers that interpret and display a Web document, and all use nearly the same architecture. Each browser usually consists of three parts: **a controller, client protocol, and interpreters.**

Server

The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client.

Uniform Resource Locator

A client that wants to access a Web page needs the address. To facilitate the access of documents distributed throughout the world, HTTP uses locators. The uniform resource locator (URL) is a standard for specifying any kind of information on the Internet. The URL defines four things: **protocol, host computer, port, and path.**

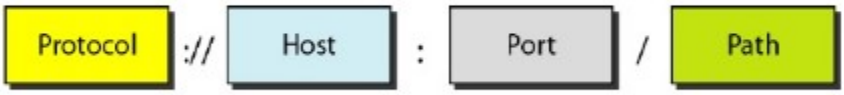


Figure 5.3 URL

The protocol is the client/server program used to retrieve the document. The most commonly used Protocol today is HTTP.

The host is the computer on which the information is located.

The URL can optionally contain the port number of the server.

Path is the pathname of the file where the information is located.

Cookies

- A cookies is small file. Frequently access browsers information are stored in a cookies directory.
- A cookie may contain upto five fields.

a) Domain b) Path c) Content

d) Expires e) Secure

a)Domain : It tells where the cookies came from.

b) Path : The path is a path in the server's directory structure that identifies which parts of the server's file tree may use the cookie.

c) Content : It takes the form name value.

d) Expires : The expires field specifies when the cookies expires.

e) Secure : This field can be set to indicate that the browser may only return the cookie to secure server.

Examples of cookies

Domin	Path	Content	Expires	Secure
toms-casino.com	/	customer ID=497793521	15-10-02, 17:00	Yes
joes-store.com	/	cart=1-00501;1-07031;2-13721	11-10-02,15:20	No
Sneaky.com	/	User ID=3456789	30-12-06, 11:00	Yes

5.1.1 WEB DOCUMENTS

The documents in the WWW can be grouped into three broad categories: static, dynamic, and active.

1. Static Documents

Static documents are fixed-content documents that are created and stored in a server. The client can get only a copy of the document. In other words, the contents of the file are determined when the file is created, not when it is used.

HTML

Hypertext Markup Language (HTML) is a language for creating Web pages.

- HTML documents are in plain text format that contain embedded HTML tags. Documents can be created in any text editor. There are also many other tools, including editors, designed specifically to assist in creating HTML documents. To HTML document, the user needs a browser.
- A document will be ready by both graphical and character based web browser. The three basic tagging pairs used to create the highest level of structure in an HTML documents are as follows :

  <HTML> HTML documents </HTML>

  <HEAD> Header information of documents </HEAD>

  <BODY> Body of the HTML document </BODY>

  The general structure of the HTML is

  <HTML>

  <HEAD>

  <TITLE>

  Title here

  </TITLE>

  </HEAD>

  <BODY>

  Body element and content

  </BODY>

  </HTML>

  A simple HTML document is given below.

  <HTML>

  <HEAD>

  <TITLE> Communication Networks </TITLE>

  </HEAD>

<BODY>
<H/> Information about the communication networks </H/>
<P> Information about the communication networks is available
<A HREF :http://www.technicalpublicationspune.com></A></P>
</BODY>
</HTML>

- Structural elements in the document are identified by Start andEnd tags. For example the <TITLE> and </TITLE> tags are used to specify the title of the document.
- The <H/> and </H/> tags' are used to define the first level heading. Headings are generated by an <Hn> tags, where n is a digit in the range 1 to 6. <H/> is the most important heading and <H6> is the less important. Typically the lower numbered heading will be displayed in a larger and heavier font.
- The browser may also choose to use different colors for each level of heading. Typically <H1> headings are large and bold face with at least one blank line above and below.
- In contrast <H2> headings are in a smaller font, and with less space above and below. The
, <P> and <HR> tags all indicate a boundary between sections of text.
- The precise format can be determined by the style sheet associated with the page. The
 tag just forces a line break. <P> starts a paragraph, which might for example, insert a blank line and possibly some indentation. <HR> (horizontal-rule) tag forces the browser to generate a horizontal rule or line, across the display. It breaks pages into logical sections and is useful when creating forms. There is no equivalent vertical rule.

Advantages and Disadvantages of HTML

A) Advantages of HTML

1. Applications are quickly developed
2. Web applications are easy to maintain and update.

B) Disadvantages

1. **Locking**: HTML is not a compiled data format. .
2. **Security :** Information is easily accessible and travels unimpeded between hosts and desktops.

5.1.2 Dynamic Web Documents

Server Side dynamic web page generation using the various scripting languages

Scripting Technologies for Dynamic Documents

A few technologies have been involved in creating dynamic documents using scripts. Among the most common are Hypertext Preprocessor (pHP), which uses the Perl language; Java Server Pages (JSP), which uses the Java language for scripting; Active Server Pages (ASP), a Microsoft

product which uses Visual Basic language for scripting; and ColdFusion, which embeds SQL database queries in the HTML document.

Active Documents

For many applications, we need a program or a script to be run at the client site. These are called active documents. For example, suppose we want to run a program that creates animated graphics on the screen or a program that interacts with the user.

Java Applets

One way to create an active document is to use Java applets.

JavaScript

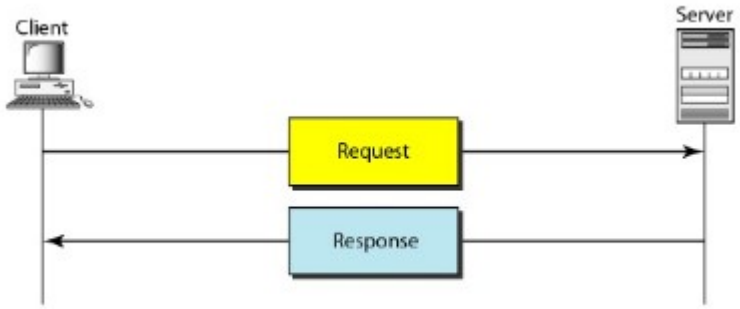
The idea of scripts in dynamic documents can also be used for active documents. If the active part of the document is small, it can be written in a scripting language; then it can be interpreted and run by the client at the same time.

5.2 HTTP

The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World.

HTTP Transaction

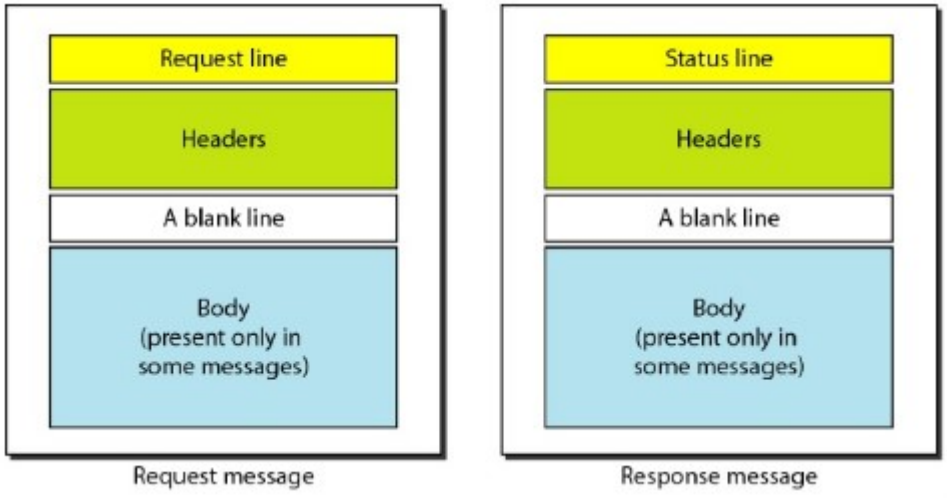
Although HTTP uses the services of TCP, HTTP itself is a stateless protocol. The client initializes the transaction by sending a request message. The server replies by sending a response.



HTTP transaction

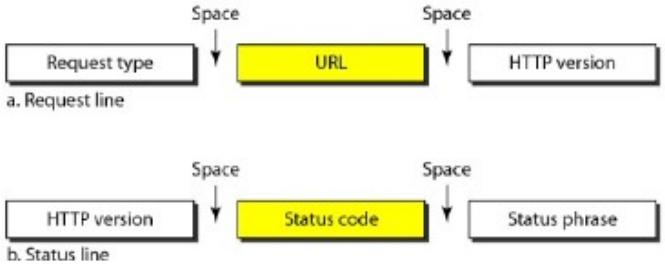
Messages

The formats of the request and response messages are similar. A request message consists of a request line, a header, and sometimes a body. A response message consists of a status line, a header, and sometimes a body.



Request and response message

Request and Status Lines The first line in a request message is called a request line; the first line in the response message is called the status line.



Request and status lines

Request type: This field is used in the request message. In version1.1of HTTP, several request types are defined. The request types is categorized into methods as follow

Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Reserved
OPTION	Inquires about available options

Version: The most current version of HTTP is 1.1.

Status code: This field is used in the response message. It consists of three digits.

Status phrase: This field is used in the response message. It explains the status code in text form.

Header: The header exchanges additional information between the client and the server.

Difference between Persistent and Non-persistent

Sr. No.	Persistent HTTP	Non-persistent HTTP
1.	Persistent version is 1.1	Non-persistent HTTP version is 1.0
2.	It uses one RTT.	It uses two RTT.
3.	TCP connection is not closed.	TCP connection is closed after every request response
4.	Client make multiple request over the same TCP connection.	Client make multiple request over the multiple TCP connection.
5.	It is default mode.	It is not default mode.
6.	Request methods are GET, HEAD, POST, PUT, DELETE, TRACE and OPTIONS.	Request methods used are GET, POST and HEAD.

5.3 ELECTRONIC MAIL

One of the most popular Internet services is electronic mail (e-mail).

Architecture

To explain the architecture of e-mail, we give four scenarios. We begin with the simplest situation and add complexity as we proceed. The fourth scenario is the most common in the exchange of email.

First Scenario

In the first scenario, the sender and the receiver of the e-mail are users (or application programs) on the same system; they are directly connected to a shared system. When Alice, a user, needs to send a message to Bob, another user, Alice runs a user agent (VA) program to prepare the message and store it in Bob's mailbox. The message has the sender and recipient mailbox addresses (names of files). Bob can retrieve and read the contents of his mailbox at his convenience, using a user agent.

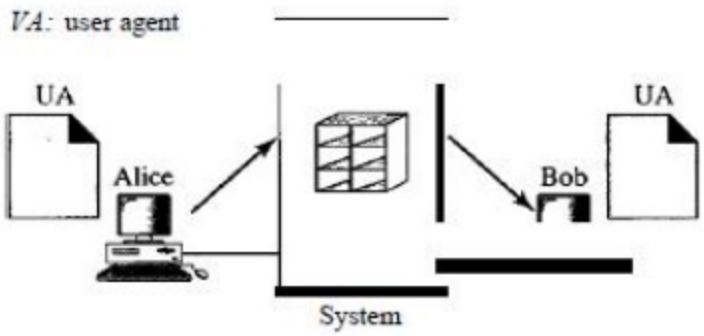


Figure 5.7 First Scenario in e-mail

Second Scenario

In the second scenario, the sender and the receiver of the e-mail are users (or application programs) on two different systems. The message needs to be sent over the Internet. Here we need user agents (VAs) and message transfer agents (MTAs).

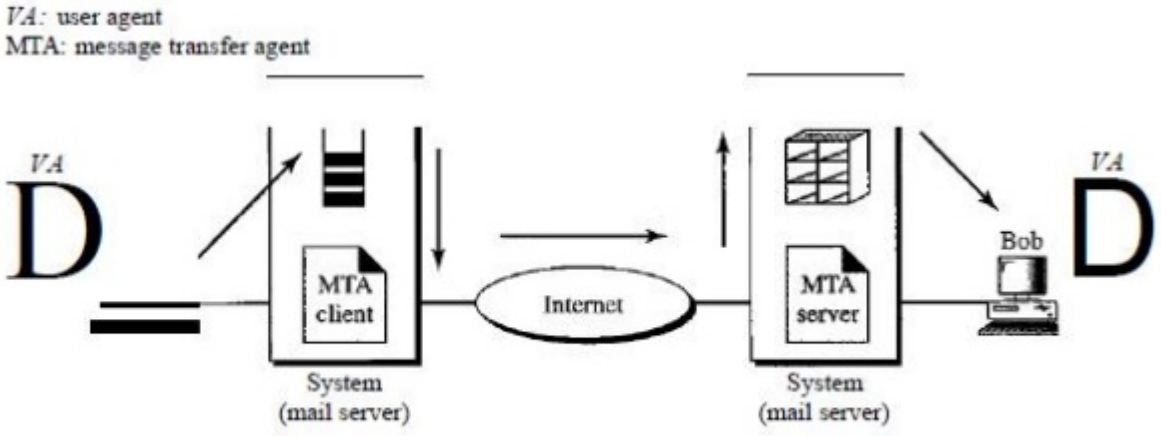


Figure 5.8 Second Scenario in e-mail.

Third Scenario

In the third scenario, Bob, as in the second scenario, is directly connected to his system. Alice, however, is separated from her system. Either Alice is connected to the system via a point-to-point WAN, such as a dial-up modem, a DSL, or a cable modem; or she is connected to a LAN in an organization that uses one mail server for handling e-mails-all users need to send their messages to this mail server.

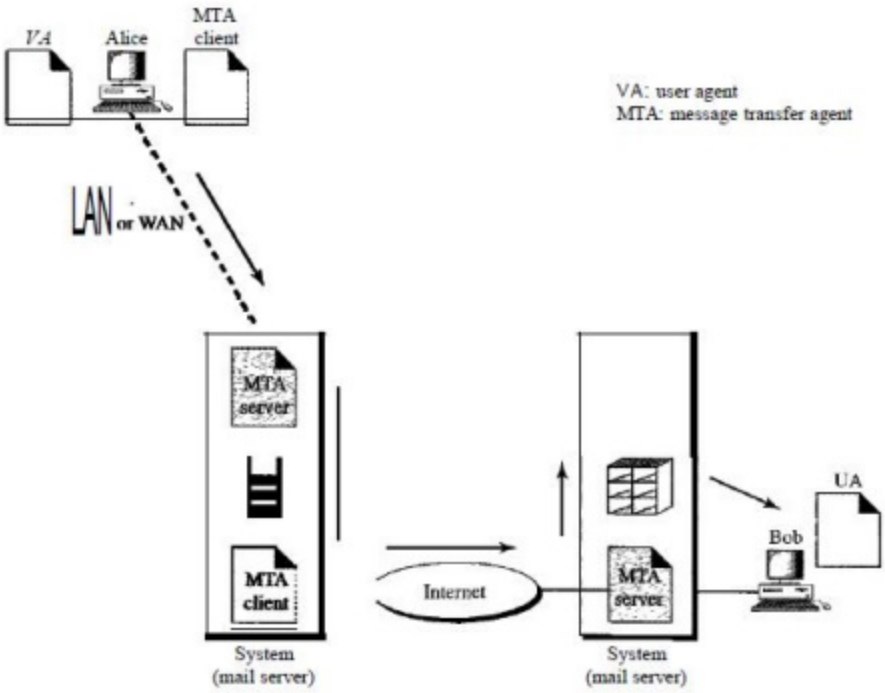


Figure 5.9 Third Scenario in e-mail

Fourth Scenario

In the fourth and most common scenario, Bob is also connected to his mail server by a WAN or a LAN. After the message has arrived at Bob's mail server, Bob needs to retrieve it. Here, we need another set of client/server agents, which we call message access agents (MAAs). Bob uses an MAA client to retrieve his messages. The client sends a request to the MAA server, which is running all the time, and requests the transfer of the messages.

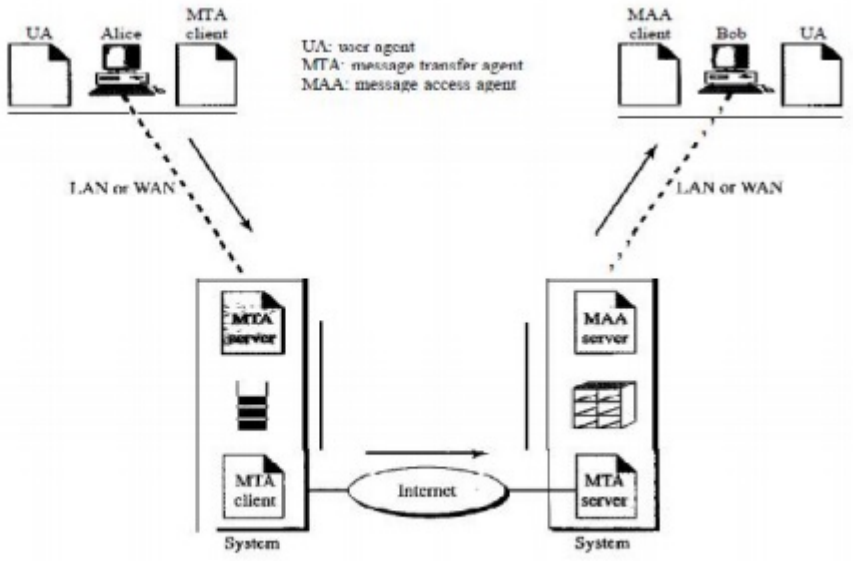


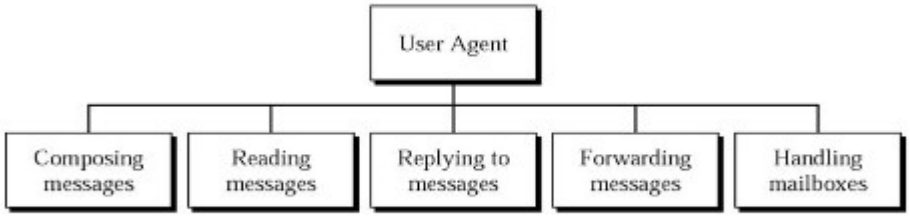
Figure 5.10 Fourth Scenario in e-mail

User Agent

The first component of an electronic mail system is the user agent (UA). It provides service to the user to make the process of sending and receiving a message easier.

Services Provided by a User Agent

A user agent is a software package (program) that composes reads, replies to, and forwards messages. It also handles mailboxes.



Service of user agent

Composing Messages A user agent helps the user compose the e-mail message to be sent out. Most user agents provide a template on the screen to be filled in by the user. Some even have a built-in editor that can do spell checking, grammar checking, and other tasks expected from a sophisticated word processor.

Reading Messages The second duty of the user agent is to read the incoming messages. When a user invokes a user agent, it first checks the mail in the incoming mailbox. Most user agents show a one-line summary of each received mail. Each e-mail contains the following fields.

1. A number field.
2. A flag field that shows the status of the mail such as new, already read but not replied to, or read and replied to.
3. The size of the message.
4. The sender.
5. The optional subject field.

Replying to Messages After reading a message, a user can use the user agent to reply to a message.

Forwarding Messages Replying is defined as sending a message to the sender a message to the sender or recipients of the copy. Forwarding is defined as sending the message to a third party.

3. User Agent Types

There are two types of user agents: command-driven and GUI-based.

Command-Driven

Command-driven user agents belong to the early days of electronic mail. They are still present as the underlying user agents in servers. A command-driven user agent normally accepts a one-character command from the keyboard to perform its task.

GUI-Based Modem user agents are GUI-based. They contain graphical-user interface (GUI)components that allow the user to interact with the software by using both the keyboard and the mouse.

Sending Mail

To send mail, the user, through the UA, creates mail that looks very similar to postal mail. The message contains the header and the body. The header of the message defines the sender, the receiver, the subject of the message, and some other information (such as encoding type, as we see shortly)..

Receiving Mail

The user agent is triggered by the user (or a timer). If a user has mail, the VA informs the user with a notice. If the user is ready to read the mail..

4. Message Transfer Agent: SMTP

The actual mail transfer is done through message transfer agents.

To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.

The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol (SMTP).

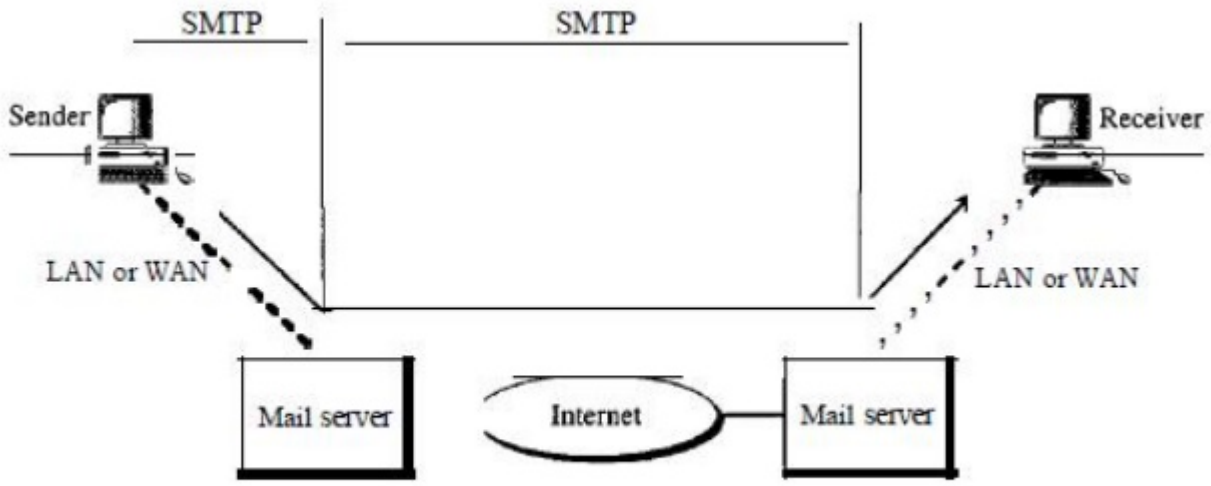


Figure 5.11 SMTP Range

SMTP is used two times, between the sender and the sender's mail server and between the two mail servers.

SMTP simply defines how commands and responses must be sent back and forth.

Commands and Responses

SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.

Commands: Commands are sent from the client to the server. It consists of a keyword followed by zero or more arguments.

Responses: Responses are sent from the server to the client. A response is a three digit code that may be followed by additional textual information.

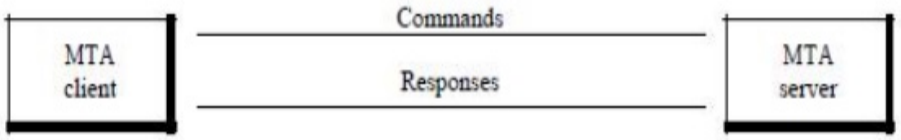


Figure 5.12 Commands and responses

5. Mail Transfer Phases

The process of transferring a mail message occurs in three phases: connection establishment, mail transfer, and connection termination.

Currently two message access protocols are available: Post Office Protocol, version 3 (POP3) and Internet Mail Access Protocol, version 4 (IMAP4).

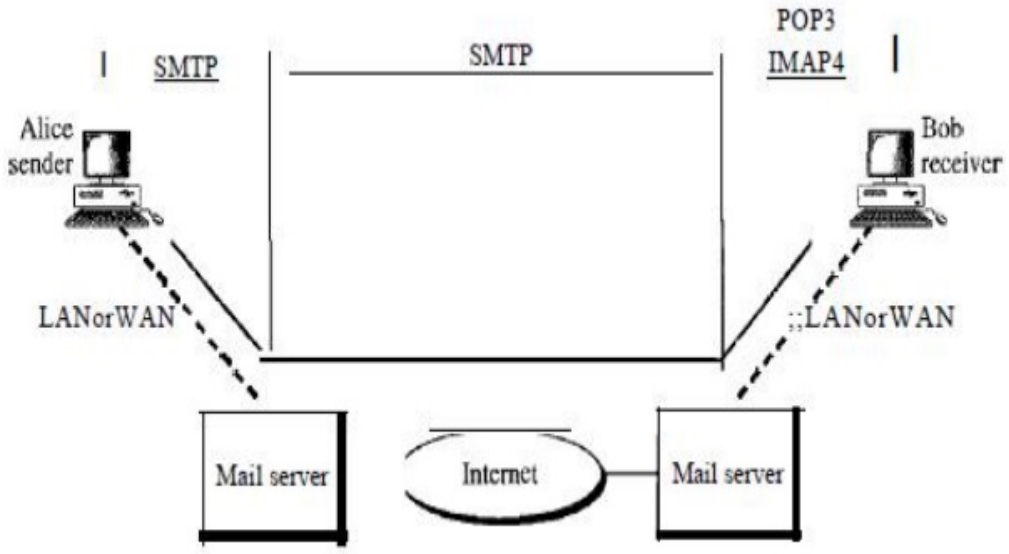


Figure 5.13 POP3 and IMAP4

Post Office Protocol (POP)

- Post Office Protocol 3 (POP3) is used to transfer e-mail messages from a mail server to mail client software.
- POP3 begins when the user agent opens a TCP connection to the mail server on port 110.
- After TCP connection established, POP3 progresses three phases :

i) Authorization ii) Transaction iii) Update

- In **authorization phase**, user agent sends a user name and a password to authenticate the user downloading the mail.
- In **transaction phase**, the user agent retrieves messages. In this phase, user agent can also mark messages for deletion, remove deletion marks.
- **In update phase**, it occurs after the client has issued the quit command, ending the POP3 session.
- POP3 has two modes : **Delete mode and the keep mode.**
- In the delete mode, mail is deleted from the mailbox after each retrieval.
- In the keep mode, the mail remains in the mailbox after retrieval.
- Fig. 5.4.7 shows downloading using POP3.

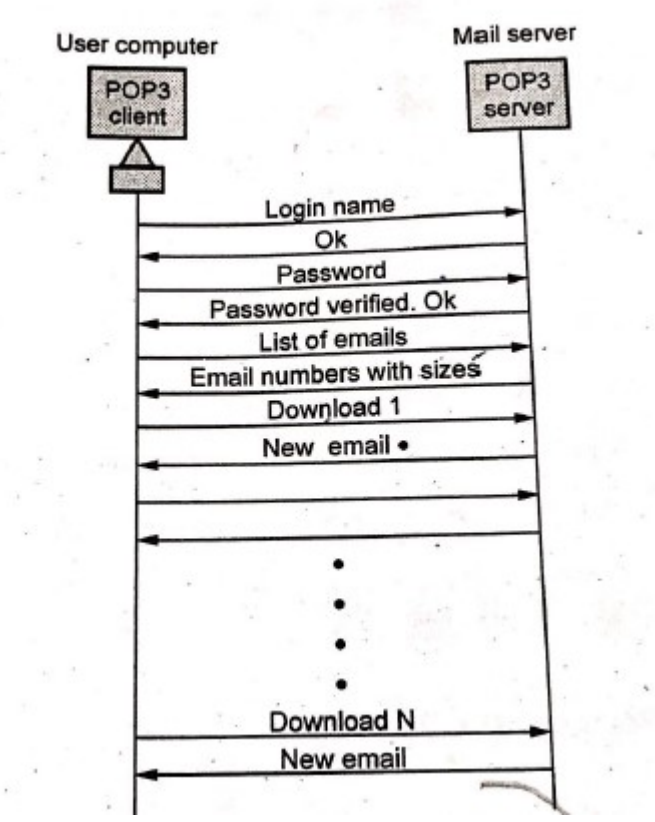


Fig. 5.4.7 *POP3*

IMAP

- IMAP is the Internet Mail Access Protocol. IMAP4 is more power and more complex. IMAP is similar to SMTP.
- It was designed to help the user who uses multiple computers.
- An IMAP client connects to a server by using TCP.
- IMAP supports the following modes for accessing e-ma me

i) Offline mode ii) Online mode iii) Disconnected mode

Offline mode: A client periodically connects to the server to download e-mail messages. After downloading, messages are deleted from the server.

Online mode : Client process e-mail messages on the server. The e-mail messages are stored on the server itself but are processed by an application on the client's end.

Disconnected mode : In this mode, both offline and online modes are supported.

IMAP4 provides the following extra functions.

1. User can check the e-mail header prior to downloading.
2. User can partially download e-mail.
3. A user can create, delete or rename mailboxes on the mail server.
4. A user can create a hierarchy of mailboxes in a folder for e-mail storage.
5. User can search the contents of the e-mail for a specific string of characters.

- Fig. 5.4.8 shows IMAP state transition diagram.

1. **Not authenticated:** Client provides authentication information to the server.
2. **Authenticated:** Server verify the information and client is now allowed to perform operations on a mailbox.
3. **Selected:** Client is allowed to access of manipulate individual messages within the mailbox.
4. **Logout:** Client send logout command for closing IMAP session.

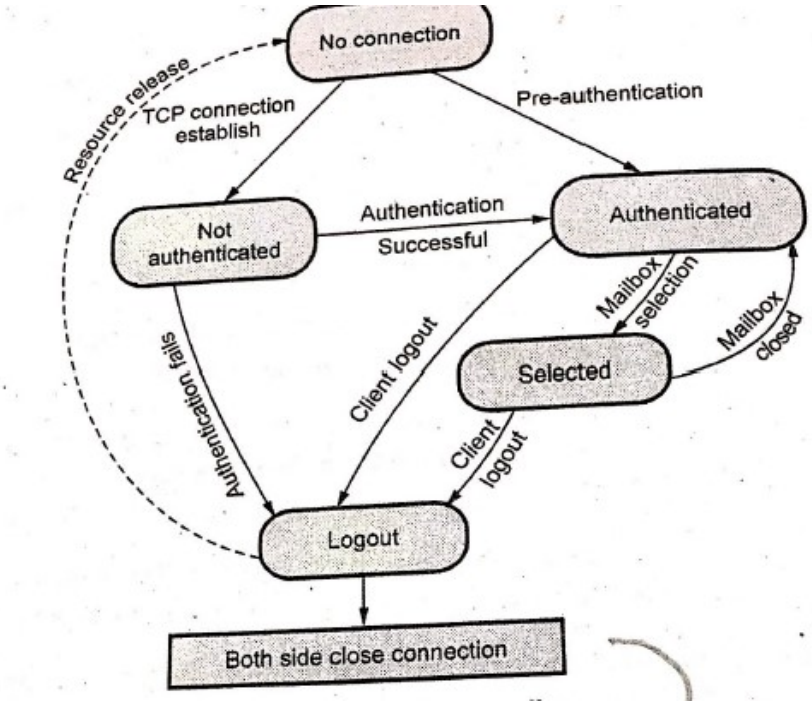


Fig.5.4.8 IMAP *state diagram*

5.4 TELNET

- TELNET means a TErminaLNETwork which is TCP/IP standard.
- TELNET is a network protocol used in LAN connections. The bi-directional, eight-bit byte oriented communications facility. TELNET is a client-server protocol, based on TCP and clients generally connect to port 23 on the host providing the service.
- Fig. 5.5.1 shows the local log-in and remote log-in. When user wants to access an application program located on a remote machine, he/she perform remote log-in

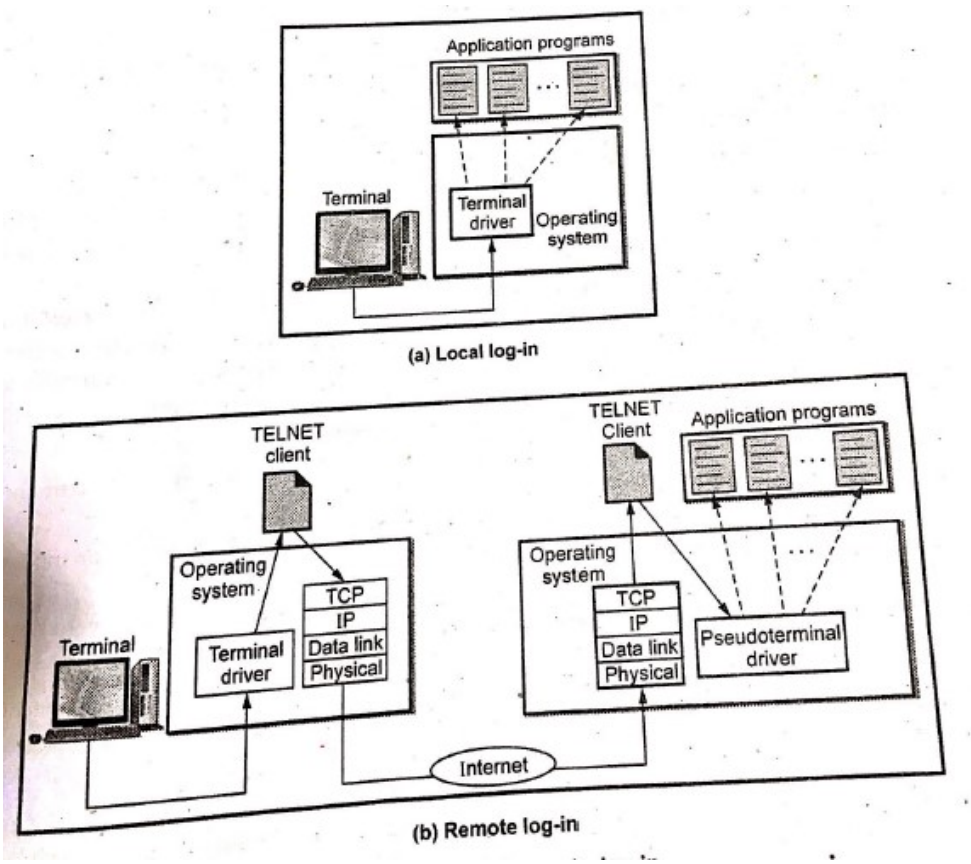


Fig. 5.5.1 *Local and remote log-in*

Modes of TELNET

- TELNET operates in three modes : **default mode, character mode and line mode**
  1. **Default mode :** The echoing is done by the client. The user types a character and the client echoes the character on the screen but does not send it until whole line is completed.
  2. **Character mode :** Each character typed is sent by the client to the server:
  3. **Line mode :** In this mode, line editing is done by the client. The client then sends the whole line to the server.
- There are three main problems with TELNET,
  1. Not Secure.
  2. It does not encrypt any data sent over the connection.
  3. Lacks of an authentication scheme.

5.5 FILE TRANSFER PROTOCOL (FTP):

File Transfer

Transferring files from one computer to another is one of the most common tasks expected from a networking or internetworking environment

File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first.

FTP differs from other client/server applications in that it establishes two connections between the hosts. One connection is used for **data transfer**, the other for **control information** (commands and responses). Separation of commands and data transfer makes FTP more efficient. The control connection uses very simple rules of communication. The data connection, on the other hand, needs more complex rules due to the variety of data types transferred.

The client has three components: user interface, client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.

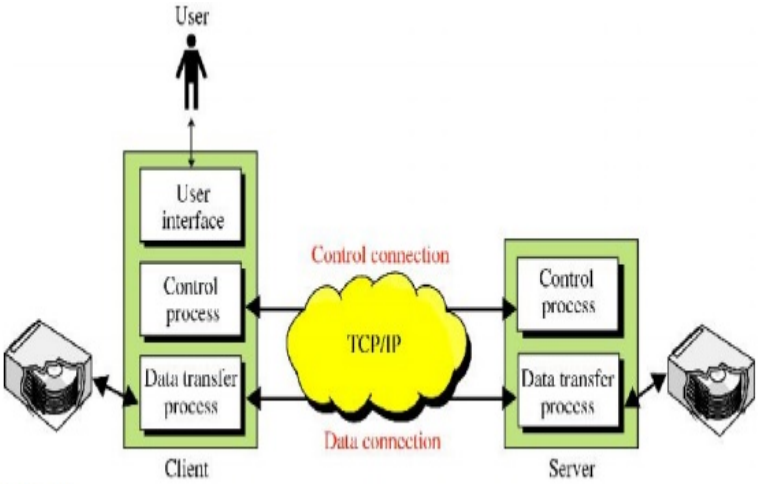


Figure 5.14 FTP

The control connection remains connected during the entire interactive FTP session. The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when the file is transferred. In other words, when a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.

1. Communication over Control Connection

Communication is achieved through commands and responses. This simple method is adequate for the control connection because we send one command (or response) at a time.

2. Communication over Data Connection (Trivial File Transfer Protocol(TFTP))

We want to transfer files through the data connection. File transfer occurs over the data connection under the control of the commands sent over the control connection. However, we should remember that file transfer in FTP means one of three things:

- A file is to be copied from the server to the client. It is done under the supervision of the RETR command.
- A file is to be copied from the client to the server. It is done under the supervision of the STOR command.
- A list of directory or file names is to be sent from the server to the client. This is done under the supervision of the LIST command.

The client must define the type of file to be transferred, the structure of the data, and the transmission mode. The heterogeneity problem is resolved by defining three attributes of communication: file type, data structure, and transmission mode

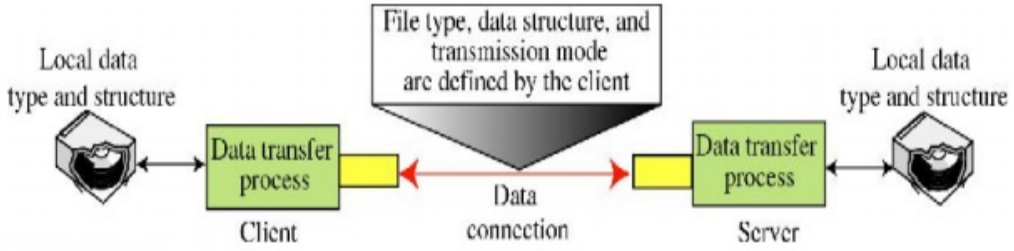


Figure 5.16 Data Connection

File Type:

FTP can transfer one of the following file types across the data connection: an ASCII file, EBCDIC file, or image file.

Data Structure

File structure, record structure, and page structure. In the file structure format, the file is a continuous stream of bytes. In the record structure, the file is divided into records.

Transmission Mode

The following three transmission modes: stream mode, block mode, and compressed mode. The stream mode is the default mode.

Difference between FTP and TFTP

Sr. No.	FTP	TETP
1.	FTP uses two connections	TETP uses one connection
2.	Provides many commands	Provides only five commands
3.	Uses TCP	Uses UDP
4.	Client must login to server	No long procedure
5.	Allow for user authentication	TETP does not allow for user authentication
6.	FTP provides a reliable service	TETP must handle its own

		retransmissions

5.6 Domain Name System (DNS)

The client/server programs can be divided into two categories: those that can be directly used by the user, such as e-mail, and those that support other application programs. The Domain Name System (DNS) is a supporting program that is used by other programs such as e-mail.

Components of DNS

- DNS includes following components

1. Domain 2. Domain name 3. Name server
4. Name resolver 5. Name cache 6. Zone

1) For example, google.com. Here com is the domain.
2) google.com could be domain name.
3) In name server, software (program) that maps names to addresses.
4) Name resolver is a software that functions as a client interacting with a name server.
5) Name cache is the storage used by the name resolver to store reformation frequently used.
6) Zone is a contiguous part of a domain.

2. DNS in the Internet:

DNS is a protocol that can be used in different platforms. In the Internet, the domain name space is divided into three sections are

1. Generic domains
2. Country domains and
3. Inverse domain

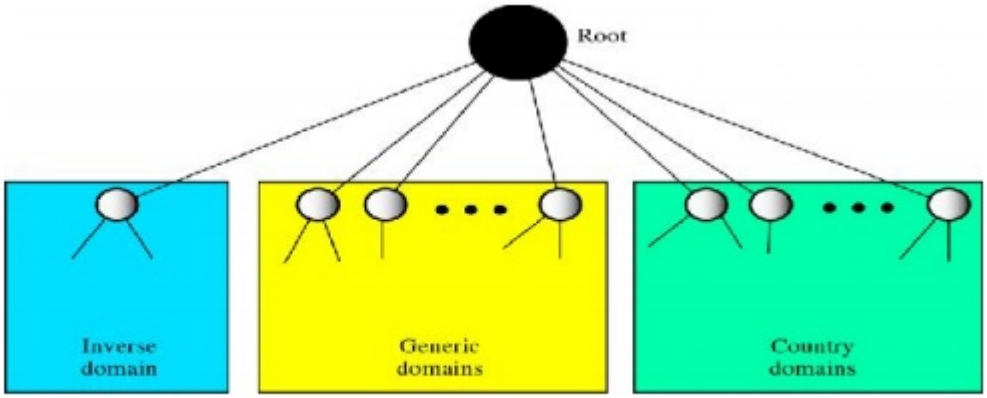


Figure 5.1 DNS in the Internet

1. Generic domain:

There are 14 generic domains, each specifying an organization type. The generic domain defines registered hosts according to their generic behaviour.

These labels describe the organization types as shown below

Label	Description
Com	Commercial organizations
Edu	Educational Institutions
Gov	Government Institutions
Int	International organizations
Mil	Military groups
Net	Network support centers
Org	Non profit organizations

Recently a few more first level labels are proposed as,

Label	Description
Arts	Cultural Organizations
Firm	Business or firms
Info	Information service providers

Nom	Personal Nomenclatures
Rec	Recreation/Entertainment Organization
Store	Business offering goods to purchase
web	Web related organizations

2. Country domains:

Each country domain specifies a country. Such as in for india, jp for japan , uk for United kingdom and us for United State , etc

3. Inverse domain:

The inverse domain finds a domain name for a given IP address. This is called address-to-name resolution. It is used to map an address to a name.

3. Types of Records:

There are two types of DNS records:

1. Question records
2. Resource records

Question Records:

The question records are used in the question section of the query and response messages. It is used by the client to get information from a server.

Resource Records:

Every domain whether it is a single host or a top level domain, can have a set of resource records associated with it. For a single host, the most common resource record is just its IP address, but many other kinds also exist. When a resolver gives a domain name to DNS, what it gets back are the resource records associated with that name. Thus, the primary function of DNS is to map domain names onto resource records. The server database consists of resource records. This record is used in the answer, authoritative and additional information sections of the response message.

Name Spaces

- Name spaces are of two types: Flat name spaces and Hierarchical names.

i) Flat name spaces

- A name is assigned to an address.

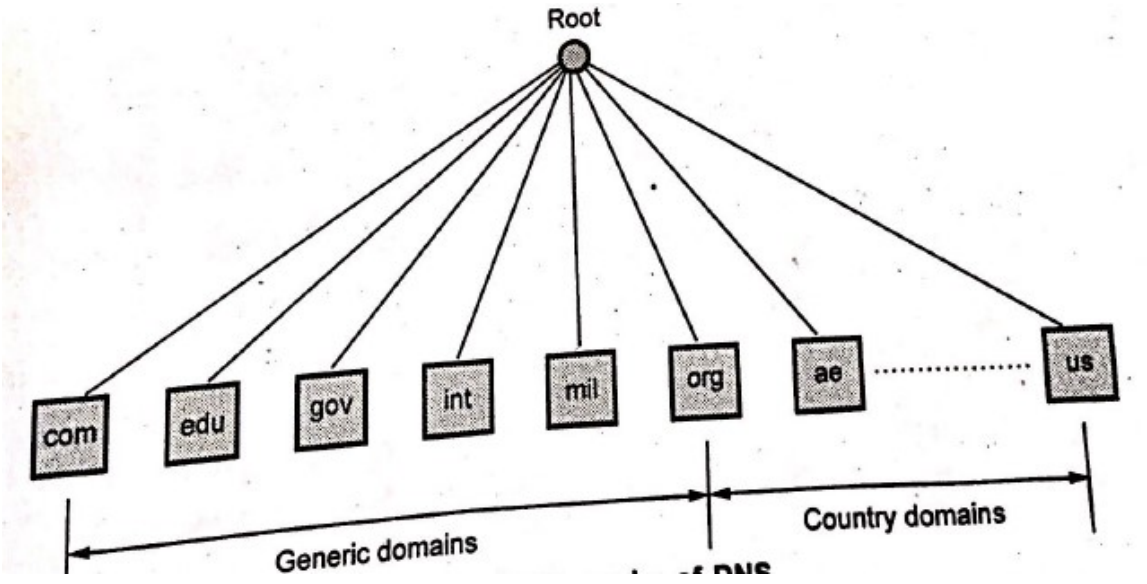
ii) Hierarchical names

- Hierarchical namespaces provides a simple yet flexible naming structure.
- The namespace is partitioned at the top level.

The top level domains are divided into three areas :

1. Arpa is a special domain used for the address-to-name mappings.
2. The 3 character domains are called the generic domains.
3. The 2 character domains are based on the counter codes found in ISO 3166. These are called the country domains.

- Fig. 5.7.5shows the hierarchy of DNS.



- **Hierarchy of Name Servers**

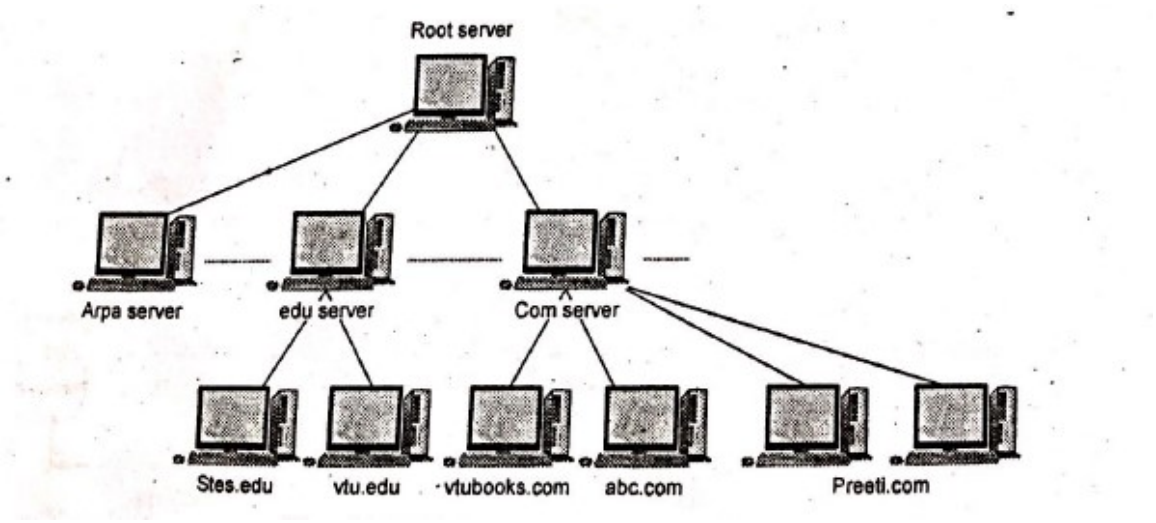


Fig.5.7.7 *Hierarchy of name server*

- To distribute the information among many computers, DNS servers are used.Creates many domains as there are first level nodes. Fig. 5.7.7 shows hierarchy of name servers.
- **Root server**: If zone consists of the full tree then that zone server is called root server. Root server do not maintain any information about domains.

  DNS uses two types of servers:

1. Primary server 2. Secondary server

- **Primary server**: This server keeps a file about the zone for which it is responsible and have authority. It performs operation on zone file like create, update and maintaining.
- **Secondary server**: It loads all information from the primary server. Secondary server cannot perform any operation on zone file.

Message Format

- Messages are sent between domain clients and domain servers with a specific format.
- DNS has two types of messages: Query and Response. Both types have the same format.
- The query message consists of the header and the question records, the response message consists of a header, question record, answer record, authoritative record and additional records.
- Fig. 5.7.11 shows the query and response messages.

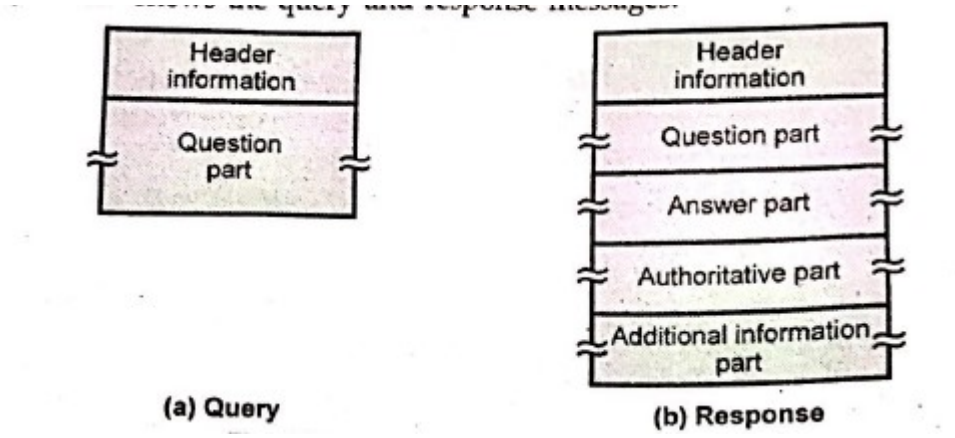


Fig. 5.7.11 *Query and response message*

- Fig. 5.7.12 shows the header format of the DNS.

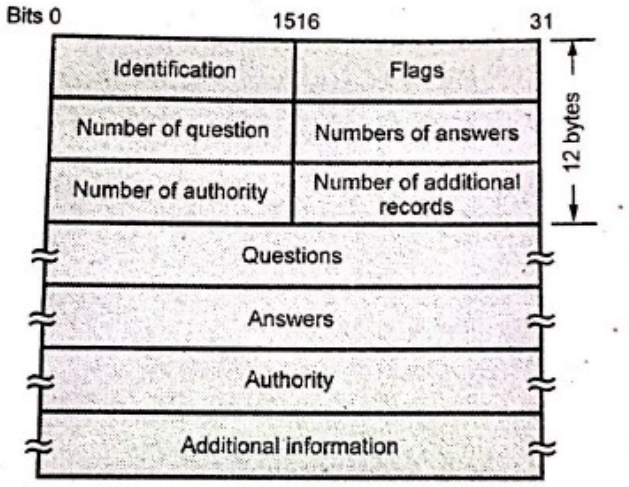
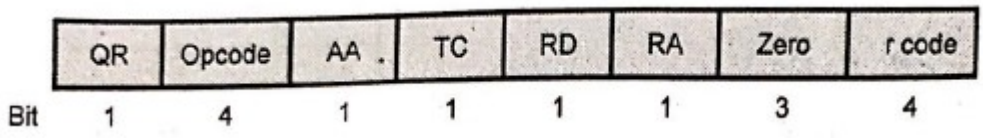


Fig. 5.7.12 *General format of DNS*

- **Identification:** It is 16 bits fields and unique value used by the client to match responses to queries.
- **Flags:** It is the collection of subfields that define the type of messages and type of the answers requested and so on.
- Number of question record contains the number of queries in the question section of the message.
- Number of answer record contains the number of answer records in the answer section of the response message.
- Number of authority record contains the number of authority records in the authoritative section of the response message.
- Number of additional records contains the number of additional records in the additional section of the response message. The message has a fixed 12-byte header followed by 4

variable length fields. The identification field is set by client and returned by the server. It lets the client, match responses to requests.

- Fig. 5.7.13 flag fields in DNS header.



- The flags field is divided into 8 parts.

QR = 0 For message is a query
= 1 It is response
Opcode = 0 Standard query
= 1 Inverse query
= 2 Server status request
AA = Authoritative answer
TC = Truncated
RD = Recursive query
RA = Recursion available
r code = Return code

Advantages of DNS

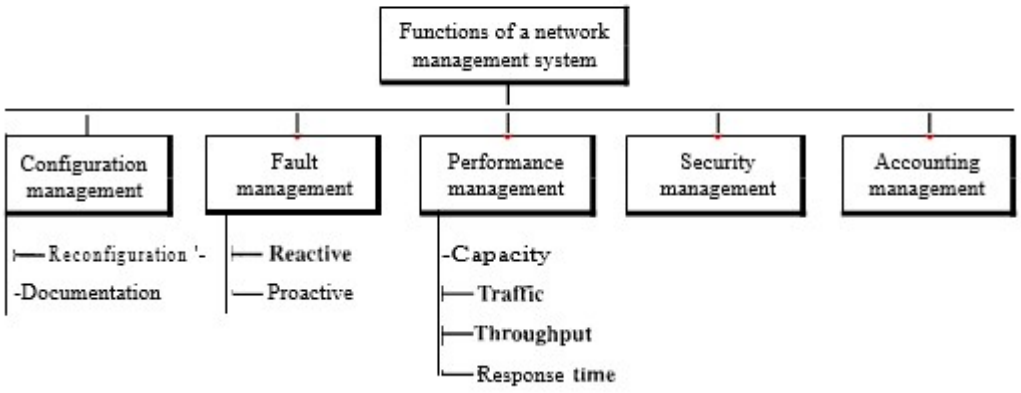
1. DNS has hierarchical structure and database.
2. DNS has small and manageable zones.
3. It is scalable.
4. DNS helps in eliminating host tables.
5. It is consistent on all hosts.
6. The Internet couldn't exist without it.
7. Easy to implement with minimal configuration changes in DNS server.

5.7 NETWORK MANAGEMENTSYSTEM

Network Management System is a collection of tools for network monitoring and control. A network management system consists of hardware and software addition implemented among existing components.

A network management system can be divided into five broad categories: configuration management, fault management, performance management, security management, and accounting management, as shown in Figure 28.1.

Figure 28.1 *Functions of a network management system*



Simple Network Management Protocol(SNMP)

SNMP uses the concept of manager and agent. That is, a manager, usually a host, controls and monitors a set of agents, usually routers

Managers and Agents

A management station, called a manager, is a host that runs the SNMP client program. A managed station, called an agent, is a router (or a host) that runs the SNMP server program. Management is achieved through simple interaction between a manager and an agent.

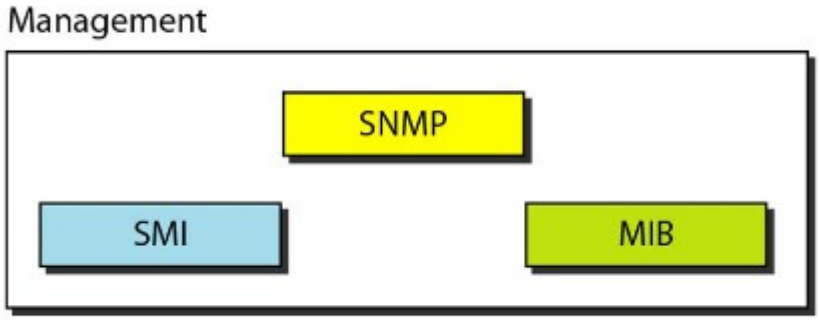
The agent keeps performance information in a database. The manager has access to the values in the database. For example, a router can store in appropriate variables the number of packets received and forwarded. The manager can fetch and compare the values of these two variables to see if the router is congested or not.

In other words, management with SNMP is based on three basic ideas:

1. A manager checks an agent by requesting information that reflects the behaviour of the agent.
2. A manager forces an agent to perform a task by resetting values in the agent database.
3. An agent contributes to the management process by warning the manager of an un usualsituation.

Management Components

To do management tasks, SNMP uses two other protocols: Structure of Management Information (SMI) and Management Information Base (MIB). In other words, management on the Internet is done through the cooperation of the three protocols SNMP, SMI, and MIB, as shown in Figure 28.3.



Role of SNMP

SNMP defines the format of packets exchanged between a manager and an agent. It reads and changes the status (values) of objects (variables) in SNMP packets.

Role of SMI

SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values.

Role of MIB

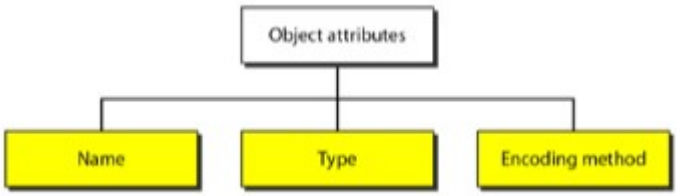
MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.

Structure of Management Information(SMI)

Its functions are

1. To name objects
2. To define the type of data that can be stored in an object
3. To show how to encode data for transmission over the network

SMI is a guideline for SNMP. It emphasizes three attributes to handle an object: name, data type, and encoding method (see Figure 28.5).

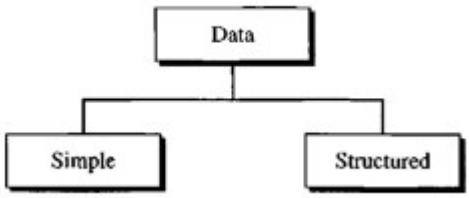


Name

SMI requires that each managed object (such as a router, a variable in a router, a value) have a unique name. To name objects globally, SMI uses an object identifier, which is a hierarchical identifier based on a tree structure (see Figure28.6).

Type

The second attribute of an object is the type of data stored in it. To define the data type, SMI uses fundamental Abstract Syntax Notation 1 (ASN.l) definitions and adds some new definitions. .
SMI has two broad categories of data type: *simple* and *structured.*



Simple Type The simple data types are atomic data types.
Table28.1*Datatypes*

Type	*Size*	*Description*
INTEGER	4 bytes	An integer with a value between _2^{31} and 2^{31} - 1
Integer32	4 bytes	Same as INTEGER
Unsigned32	4 bytes	Unsigned with a value between 0 and 2^{32} - 1
OCTET STRING	Variable	Byte string up to 65,535 bytes long
OBJECT IDENTIFIER	Variable	An object identifier
IPAddress	4 bytes	An IP address made of four integers
Counter32	4 bytes	An integer whose value can be incremented from 0 to 2^{32}; when it reaches its maximum

		value, it wraps back to O.
Counter64	8 bytes	64-bit counter
Gauge32	4 bytes	Same as Counter32, but when it reaches its maximum value, it does not wrap; it remains there until it is reset
TimeTicks	4 bytes	A counting value that records time in s $\frac{1}{100}$
BITS		A string of bits
Opaque	Variable	Uninterpreted string

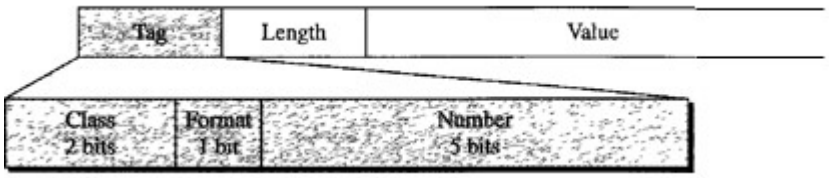
Structured Type: By combining simple and structured data types. SMI defines two structured data types: *sequence* and *sequence of.*

Sequence. A *sequence* data type is a combination of simple data types, not necessarily of the same type.

Sequence of. A *sequence of* data type is a combination of simple data types all of the same type.

Encoding Method

SMI uses another standard, Basic Encoding Rules (BER), to encode data to be trans mitted over the network.



Tag. The tag is a 1 -byte field that defines the type of data. It is composed of three subfields:*class*(2*bits),format*(1bit),and*number*(5bits).Theclasssubfielddefines the scope of the data..

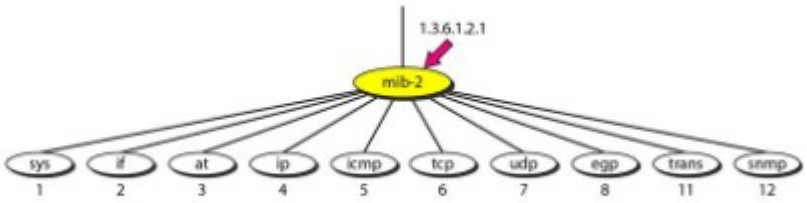
Length. The length field is 1 or more bytes. If it is 1 byte, the most significant bit must be O. The other 7 bits define the length of the data. If it is more than 1 byte, the most significant bit of the first byte must be 1.

Value. The value field codes the value of the data according to the rules defined in BER.

Management Information Base (MIB)

The Management Information Base, version 2 (MIB2) is the second component used in network management. Each agent has its own MIB2, which is a collection of all the objects that the

manager can manage. The objects in MIB2 are categorized under 10different groups: system, interface, address translation, ip, icmp, tcp, udp, egp, trans• mission, and snmp. These groups are under the mib-2 object in the object identifier tree (see Figure 28.15). Each group has defined variables and/or tables.



The following is a brief description of some of the objects:

Sys: Thisobject *(system)* defines general information about the node (system), such as the name, location, and lifetime.

if :This object *(interface)* defines information about all the interfaces of the node including interface number, physical address, and IPaddress.

at : Thisobject*(addresstranslation)*definestheinformationabouttheARPtable.

ip: Thisobject defines information related to IP, such as the routing table and the IPaddress.

icmp :This object defines information related to ICMP, such as the number of packets sent and received and total errors created.

tcp: This object defines general information related to TCP, such as the connection table, time-out value, number of ports, and number of packets sent and received.

Udp : This object defines general information related to UDP, such as the number of ports and number of packets sent and received.

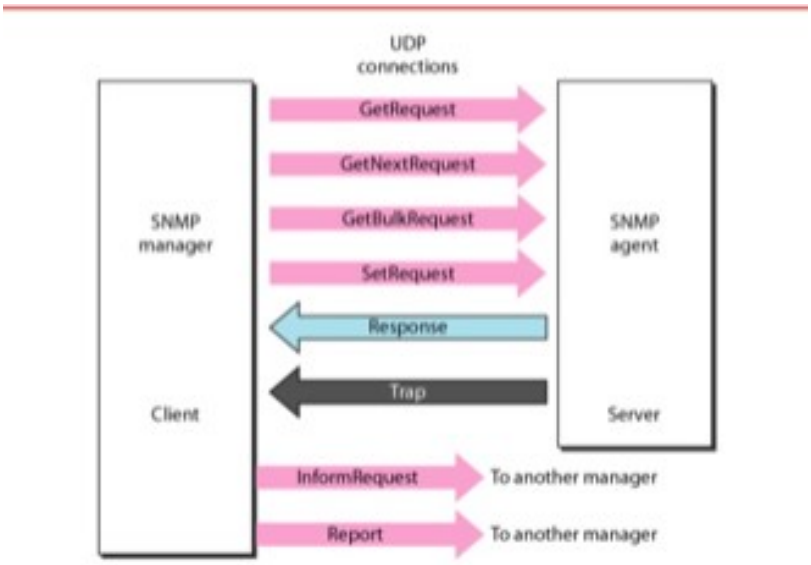
Snmp :This object defines general information related to SNMP itself.

SNMP

1. A manager to retrieve the value of an object defined in an agent
2. A manager to store a value in an object defined in an agent
3. An agent to send an alarm message about an abnormal situation to the manager

PDUs

SNMPv3 defines eight types of packets (or PDUs): GetRequest, GetNextRequest, GetBulkRequest,SetRequest,Response,Trap,InformRequest,andReport(seeFigure28.20).



GetRequestTheGetRequest PDU is sent from the manager (client) to the agent (server) to retrieve the value of a variable or a set of variables.

GetNextRequestTheGetNextRequestPDU is sent from the manager to the agent to retrievethevalueofavariable.

GetBulkRequestThe GetBulkRequest POD is sent from the manager to the agent to retrieve a large amount of data. It can be used instead of multiple GetRequest and GetNextRequestPODs.

SetRequestThe SetRequest PDD is sent from the manager to the agent to set (store) a value in a variable.

Response The Response PDD is sent from an agent to a manager in response to GetRequest or GetNextRequest. It contains the value(s) of the variable(s) requested by the manager.

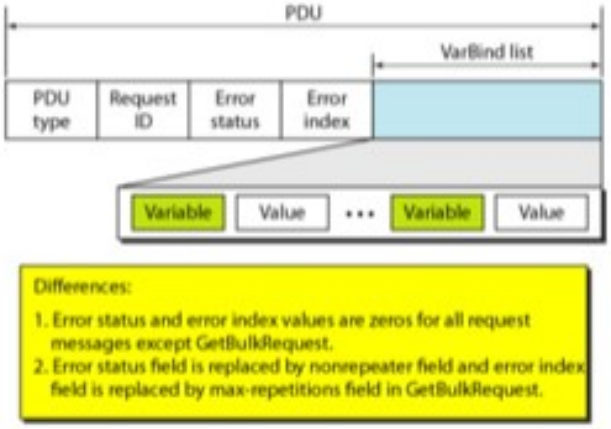
TrapThe Trap (also called SNMPv2 Trap to distinguish it from SNMPv1 Trap) POD is sent from the agent to the manager to report an event. For example, if the agent is rebooted, it informs themanager and reports the time of rebooting.

InformRequest The Inform Request POD is sent from one manager to another remote manager to get the value of some variables from agents under the control of the remote manager. The remote manager responds with a Response POD.

Report The Report POD is designed to report some types of errors between managers.
It is not yet in use.

Format

The format for the eight SNMP PODs is shown in Figure 28.21. The GetBulkRequest POD differs from the others in two areas, as shown in the figure.



The fields are listed below:

PDU type. This field defines the type of the POD

Request ID.This field is a sequence number used by the manager in a Request POD and repeated by the agent in a response. It is used to match a request to a response.

Error status. This is an integer that is used only in Response PDUs to show the types of errors reported by the agent. Its value is 0 in Request PDUs.

Nonrepeaters. Thisfieldused only in GetBulkRequestand replaces the error status field, which is empty in RequestPDUs.

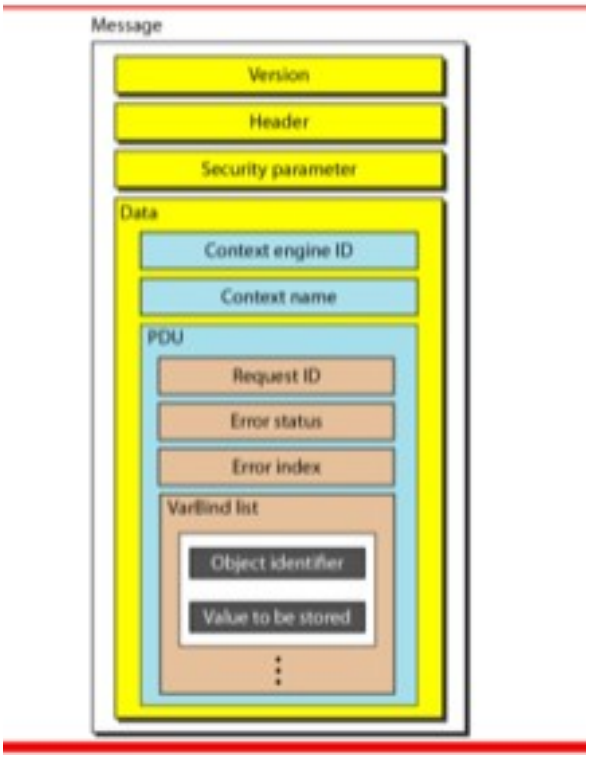
Error index. The error index is an offset that tells the manager which variable Caused the error.

Max repetition : This field is also used only in GetBulkRequest and replaces the error index field, which is empty in Request PDUs.

VarBindlist. This is a set of variables with the corresponding values the manager wants to retrieve or set.

Messages

SNMP does not send only a PDU, it embeds the PDU in a message. A message in SNMPv3 is made of four elements: version, header, security parameters, and data (which include the encoded PDU), as shown in Figure 28.22.



Strength of SNMP

1. It is simple to implement.
2. Agents are widely implemented.
3. Agent level overhead isminimal.
4. It is robust and extensible.
5. Polling approach is good for LAN based managed object.
6. It offers the best direct manager agent interface.
7. SNMP meet a critical need.

Weakness of SNMP

1. It is too simple and does not scale well.
2. There is no object oriented data view.
3. It has no standard control definition.
4. It has many implementation specific (private MIB) extensions.
5. It has high communication overhead due to polling.

5.8 SSH

- SSH is a protocol for secure remote login and other secure network services over an insecure network.
- Secure Shell (SSH) is a protocol for secure network communications designed to be relatively simple and inexpensive to implement.

- Secure shell provides strong authentication and encrypted data communications between two computers connecting over an open network such as the internet.
- SSH uses the client-server model, connecting a secure shell client application, the end at which the session is displayed, with an SSH server, the end at which the session runs.
- Fig. 5.9.1 shows SSH protocol stack.

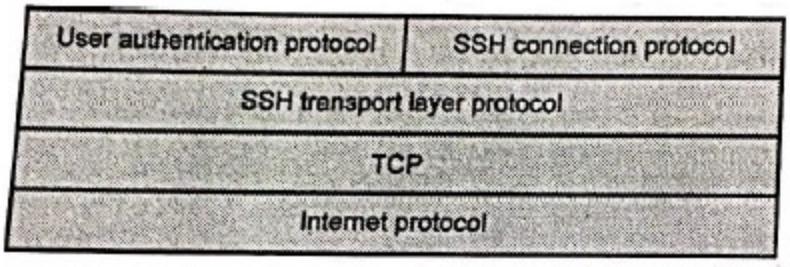


Fig. 5.9.1 *SSH protocol stack*

- The SSH protocol consists of three major components :

1. **SSH transport layer protocol :** Provides server authentication, confidentiality and integrity with perfect forward secrecy.
2. **SSH user authentication protocol :** Authenticates the client to the server. It runs over the transport layer protocol.
3. **SSH connection protocol :**Multiplexes the encrypted tunnel into several logical channels.

SSH port forwarding

- Port-Forwarding is also called tunnelling.
- The main benefit of port forwarding is that the tunnelled traffic between the user's computer and the remote server is encrypted through the SSH protocol.
- The SSH protocol V2 offers three types of port forwarding :
    1. **Local-to-remote forwarding:** Local (user side) port is created and all traffic is forwarded to a predefined destination server and port.
    2. **Remote-to-local forwarding:** A remote (server side) port is created and traffic from connections to that port are routed to the local (user) computer and is forwarded to a destination and port from there.
    3. **Dynamic port forwarding:** A local (user side) port is created and all traffic is forwarded to a destination server and port. The server and port can be chosen at connection time.
- Fig. 5.9.2 shows setup flow of a secure shell connection.

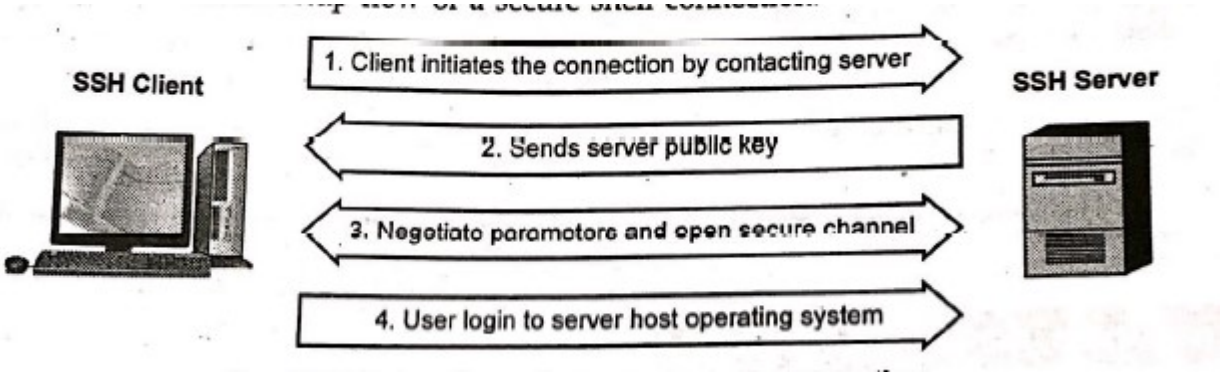


Fig. 5.9.2 *Setup flow of a secure shell connection*

- The protocol works in the client-server model, which means that the connection is established by the SSH client connecting to the SSH server.
- The SSH client drives the connection setup process and uses public key cryptography to verify the identity of the SSH server.
- After the setup phase the SSH protocol uses strong symmetric encryption and hashing algorithms to ensure the privacy and integrity of the data that is exchanged between the client and server.
- Once a connection has been established between the SSH client and server, the data that is transmitted is encrypted according to the parameters negotiated in the setup.
- During the negotiation the client and server agree on the symmetric encryption algorithm to be used and generate the encryption key that will be used.
- The keys used for authentication are called SSH keys.
- The protocol is used in networks for :
    1. Providing secure access for users and automated processes.
    2. Interactive and automated file transfers.
    3. Issuing remote commands.
    4. Managing network infrastructure and other mission-critical system components.

Difference between SSH Version 1 and SSH Version 2

It uses one monolithic protocol	It uses separate transport, authentication and connection protocols.
Weak CRC-32 integrity check.	Strong cryptographic integrity check.
Exactly one session channel per connection.	Any number of session channels per connection.
Negotiates only the bulk cipher; all others are fixed.	Full negotiation of modular cryptographic and compression algorithms, including bulk encryption, MAC and public-key.

The same algorithms and keys are used in both directions	Encryption, MAC and compression are negotiated separately for each direction, with independent keys.
Server key used for forward secrecy on the session key.	Use of Diffie-Hellman key agreement removes the need for a server key.

Questions and Answers :

1 What is DNS ? (May 18)

Ans: DNS is a client/server application that identifies each host on the Internet with a unique user friendly name.

2 What is the purpose of inverse domain ?

Ans: The inverse domain is used to map an address to a name.

3 What is SMTP ?(May,Dec 15)

Ans: Simple Mail Transfer Protocol is a standard and reliable host to host mail transport protocol that operates over the TCP port 25.

4 What is Telnet ?(Dec 11)

Ans: TELNET is a client/server application that allows a user to log on to a remote machine giving the user access to the remote system.

5 State the purpose of SNMP. (Dec 11)

Ans: The primary purpose of SNMP is to allow the network administrator to monitor and configure devices on the network, remotely via the network. These configuration and monitoring capabilities are collectively referred to as management.

6 When web pages are sent out, they are prefixed by MIME headers. Why ? (May 11)

Ans: The MIME headers tell the browser what type of file is contained on the Web page and also what type of helper application or plug-in needs to be used to display the content.

7 Why email security Is necessary ? (Dec 11)

Ans: Email security is the process of using email encryption to send messages that can only be opened by the intended recipient. Sending a message without secure email encryption is similar to dropping a post card in the mail - it can be read by almost any one handling the postcard during its journey from sender to receiver. Secure email encryption protects both your online data and customers' sensitive information.

8 Define SNMP (May 12)

Ans: Simple network management protocol; a standard for gathering statistical data about network traffic and the behavior of network components; SNMP uses management information bases (MTBs), which define what information is available from any manageable network device.

9 What are the four groups of HTTP Headers ? (May 15)

Ans: The four groups of HTTP headers are : General Headers, Entity Headers, Request Headers, and Response Headers.

10 Define URL ? (May 16)

Ans: Uniform Resource Locator (URL) is a string identifier that identifies a page onthe World Wide Web.

11 Compare the HTTP and FTP?

Ans: Comparison between HTTP and FTP:

Sr. No.	FTP	HTTP
1.	FTP transfers the file from client to server and server to client.	HTTP transfer the file from server to client (i.e. web pages)
2.	It uses two different port connection (i.e. port 20 and port 21)	HTTP use only one port connection (i.e. Port 80)
3.	Uses TCP protocol.	It also the TCP protocol.

12 What is meant by PORT or MAILBOX related with UDP ? (Dec 12)

Ans: The UDP port is a 16-bit address that exists only for the purpose of passing certain types of datagram information to the correct location above the transport layer of the protocol stack. The UDP ports can receive more than one message at a time, and they are identified by "well known" port numbers.

13 What are the advantages of allowing persistent TCP connections in HTTP? (May 13)

Ans:

a. HTTP requests and responses can be pipelined on a connection.

b. Network congestion is reduced by reducing the number of packets caused by TCP opens, and by allowing TCP sufficient time to determine the congestion state of the network.

c. Latency on subsequent requests is reduced since there is no time spent in TCP's connection opening handshake.

14 What DNS cache issues are involved in changing the IP address of a web server host name ? (Dec 13)

Ans: This is an example where using an obsolete entry can be a serious problem, since you might get served the wrong page if you contact the "old" owner of a given me. This problem might be minimized by providing a mechanism for sending "DNS update" messages to inform hosts that their entries have gone bad.

15 Differentiate application programs and application protocols.(Dec 13)

Ans: An application program is any program designed to perform a specific function directly for the user or, in some cases, for another application program. Examples of application programs include word processors; database programs; web browsers; development tools;

drawing, paint and image editing programs; and communication programs. HTTP is application protocols. Users invoke applications which "speak" using application protocol. Applications interact with a transport protocol to send or receive data.

16 What do you mean by TELNET ? (May 14)

Ans: TELNET is used to connect remote computers and issue commands on those computers.

17 State the difference between SMTP and MIME. (Dec 14)

Ans:

Sr. No.	SMTP	MIME
1.	SMTP is protocol used to exchange messages between mail servers.	MIME expands the messaging abilities of SMTP and supports all formats.
2.	SMTP is the most widely used Internet application.	MIME allows multimedia and other non-textual formats to be handled reliably throughout the message transport process.

18 List down the key lengths supported by PGP. (Dec 14)

Ans: Key length supported by PGP:

1. 385 bits 2. 512 bits 3. 1024 bits

19 Mention the types of HTTP messages. (Dec 15)

Ans: Types of HTTP messages : Request and Response

20 Mention the different labels in domain name space. (May 16)

Ans:

Sr. No.	Label	Description
1.	com	Commercial organization
2.	edu	Educational organization
3.	gov	Government organization
4.	int	International organization
5.	mil	Military group
6.	net	Network support centers
7.	org	Nonprofit organization

21 Expand POP3 and IMAP4 (Dec 16)

Ans: POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail.

IMAP (Internet Message Access Protocol) is an internet standard protocol used bye-mail clients to receive e- mail messages from a mail server over a TCP/IFconnection.

22 What is persistent HTTP ? (Dec 16)

Ans: A single TCP connection to send and receive multiple HTTP requests/responsesis termed as persistent HTTP connection.

23 State the usage of conditional get in HTTP. (May 17)

Ans. : A conditional GET is an HTTP GET request that may return an HTTP 304response. An HTTP 304 response indicates that the resource has not been modified since the previous GET, and so the resource is not returned to the client in such aresponse.

The use of conditional GET has significant benefits, on both the client and the server. On the InCommonmetadata server, roughly 3/4 of all metadata requests result in HTTP 304. That translates into many thousands of metadata requests per day that conveniently avoid the unnecessary overhead of metadata refresh. For a file whose size is large and growing, that represents a significant cost savings.

Conditional has security benefits as well. Since requests that result in HTTP 304 are issued virtually without penalty, a client can request metadata more frequently than absolutely necessary.

24 Present the Information contained in a DNS resource record. (May 17)

Ans: DNS records type, meaning and value are as under.

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterrupted ASCII text.

25 Write the use of Hyper Text Transfer Protocol (HTTP). (Dec 17, May 18)

Ans: HTTP is the protocol used to transfer data over the web. It is part of the Internet protocol suite and defines commands and services used for transmitting webpage data. HTTP uses a server-client model.

26 What do you mean by Web Services Description Language (WSDL) ? (Dec 17)

Ans: The web services description language (WSDL) is the XML-based service representation language used to describe the details of the complete interfaces exposed by Web services and thus is the means to accessing a Web service.

27 Consider an HTTP client that wants to retrieve a web document at a given URL. The IP address of the HTTP server is initially unknown. The web document at the URL has one embedded GIF image that resides at the same server as the original document. What transport and application layer protocols besides HTTP are needed in this scenario ? (Dec 18)

Ans: Before the HTTP GET request can be sent for the web document, the HTTP client needs to obtain the IP address of the HTTP server hosting the document. So a DNS request is sent out to obtain the hostname to IP address mapping.

Application layer protocols : DNS and HTTP.

Transport layer protocols : UDP for DNS; TCP for HTTP.

28 What is the use of SNMP protocol in a network ? (Dec 18)

Ans: SNMP is provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language that is used for monitoring and managing devices in a network.

Prepared by **Verified by** **Approved by**