UNIT 4 APPLICATION LAYER PROTCOLS

Structure **Page Nos.**

4.0 INTRODUCTION

The application layer provides means for the user to access information on the network through an application. This layer is the main interface/environment for the user to interact with the application and therefore with the network. The application layer can be assumed to be the level of TCP/IP protocol hierarchy where the user-accessed network processes reside. The applications running at the application layer are some network processes that occur above the transport layer. This includes all the processes that the users can interact with. Thus, application layer provides the services user applications communicate through the network for e.g., SMTP, FTP, Telnet and Rlogin. In this unit, we shall discuss the various standard services such as DNS, FTP, Telnet and SMTP being offered by the application layer.

4.1 OBJECTIVES

Our objective is to introduce you to the basic concept of the application layer and its prolocols. On successful completion of this unit, you should be able to:

- have a reasonable understanding of the application layer;
- describe the operation of application layer protocols;
- understand the role and meaning of Domain Name System (DNS), and
- describe and understand the working of Simple Mail Transfer Protocol (SMTP), Telnet and File Transfer Protocol (FTP).

4.2 DOMAIN NAME SYSTEM (DNS)

As we already know, each host machine on the Internet is assigned an IP address. The 32-bit IP address is represented in the numerical form, e.g., 202.12.32.22. However, it is vny difficult for a user to remember the address of a machine in terms of an IP address. Therefore, the IP addresses have been denoted as a set of characters in

English e.g., for the other name, of IP address 68.142.226.32 is yahoo.com. This human readable name in place of an IP address is known as domain name, e.g., google.com. The domain names are registered by an organization called ICANN. The domain names are not case sensitive and can contain alphabetic or numeric letters or the hyphen. Whenever a user accesses the Internet, he or she types the domain name instead of an IP address. Therefore, there is a need for a system that can convert the domain names of hosts into IP addresses and vice-versa. Such conversions are carried out by a system known as Domain Name System. The main function of Domain Name System (DNS) is to map the IP addresses into domain names (human readable names).

4.2.1 Hierarchical Name Space

The DNS is a large database that resides on various computers and it contains the IP addresses of various hosts on the Internet and various domains. The Domain Name System (DNS) is basically a distributed Internet directory service. In this system, the host needs to map the closest DNS computer machine which has the required information.

In order to assign the names to various machines, some kind of naming system was required. Thus, a hierarchical name space was designed such that each domain name was divided into several parts of the tree, e.g., the domain name 'yahoo.com' consists of two parts. First the domain name is read from right to left, i.e., com signifies a commercial website (upper level of hierarchical system) and yahoo denotes the name of the website (lower level of hierarchical system) see Figure 1.

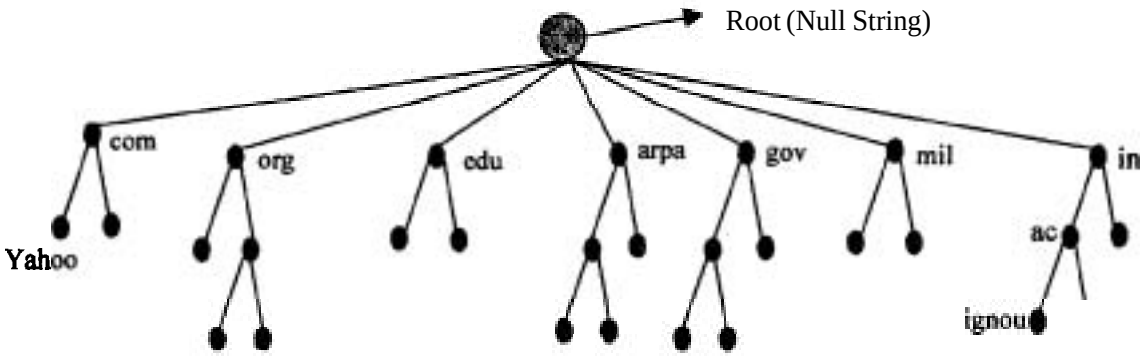

Figure 1: Hierarchical Name Space for DNS

In DNS, a tree structure has been designed such that root of the tree binds the complete tree. The maximum levels of the tree are 128 and each label of the tree can have a string of 63 characters. The root of the DNS hierarchy (tree) is designated with a period '.'. Thereafter the tree contains a group of top-level domains including familiar names like *com,* org, edu, various country-level domains like in (India) etc. However, the domain names at this level cannot be assigned to an individual machine. The next levels of the DNS tree are the second-level registered domains such as hotmail.com. Below the second level, local domains names can be specified. Remember, the domain names are always read from the current node up to the root of the tree as shown in Figure 2.

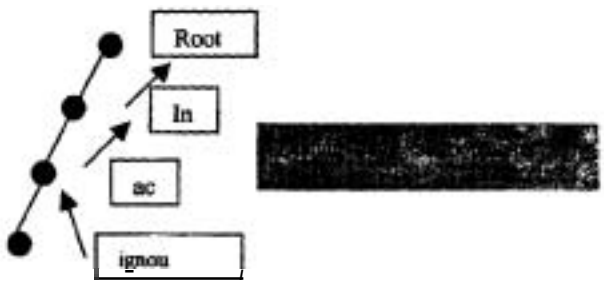

Figure 2: Labeling for domain names

The above mentioned tree structure has to be stored into the computer machine. However, storage of such a huge amount of information on a single computer system is prone to inefficient computing due to the following reasons:

1. Availability of the system.
2. Reliability.
3. Computing capacity of the system.
4. Network load on that particular transmission link.

4.2.2 Domain Servers

Due to these reasons, domain name information has been distributed among various servers known as Domain Servers. The server is responsible or has an authority over a specific region called a zone **i.e.,** the DNS database is divided into zones. The servers in their respective zones are responsible for answering queries for their zones and are called name servers.

A name server is a server program that holds a master or a copy of a name-to-address mapping database, or otherwise points to a server that does and that answers requests from the client software, called a name resolver. Conceptually, all Internet domain servers are arranged in a tree structure that corresponds to the naming hierarchy.

A zone is simply a sub-tree of DNS and is administered separately. There are multiple name servers for a zone. There is usually one primary name server and one or more secondary name servers. A name server may be authoritative for more than one zone.

The root server is the server whose zone consists of the complete tree. Basically a root server does not keep information about domain names but actually delegates its own authority to other servers. At present, there are around 13 root servers distributed all over the world which are able to cover the entire set of domain names.

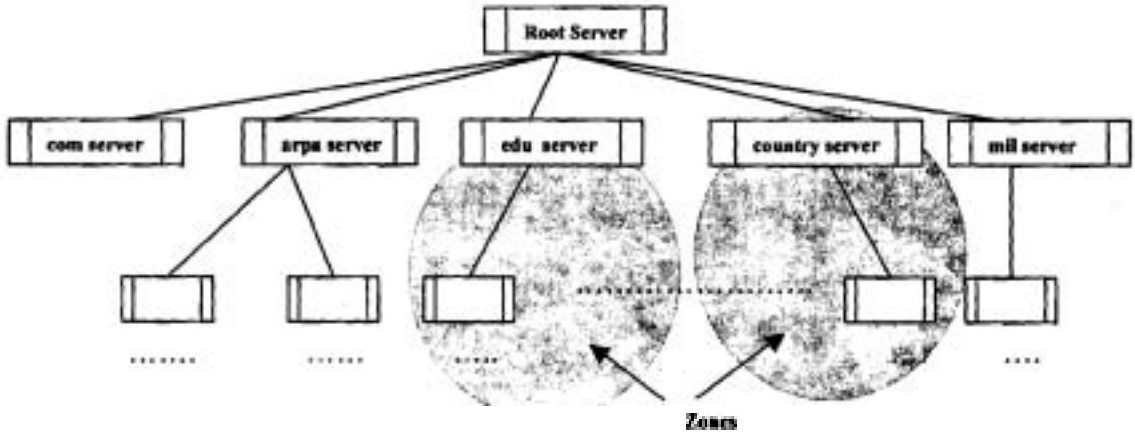

Figure 3: Name Servers

Thus we have discussed in general the working of Domain Name Systems.

4.2.3 How does DNS Work in Internet?

The ***hierarchical*** system of domain names in Internet has been broadly classified into three categories:

1. Generic domain names
2. Country based domain names
3. Inverse domains

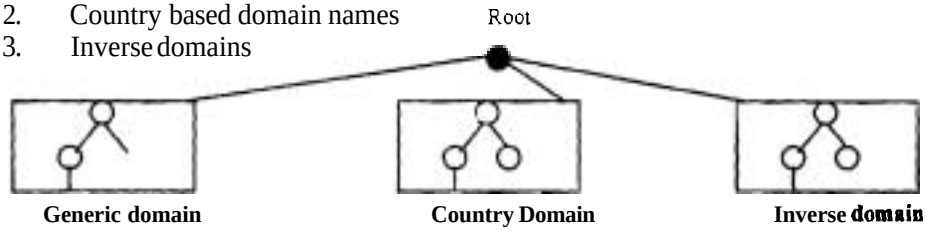

Figure 4: Hierarchy of Domains in Internet

The three-character top-level names are called the generic domains or the organisational domains. The generic domain defines registered hosts in accordance with their behaviour for example, yahoo.com uses 'com' as top level name as it signifies that yahoo is a commercial organisation. *Table 1* shows some of the top-level domains of today's Internet domain hierarchy.

Table 1: Generic Domain Names

Domain Name	Meaning
Com	Commercial organisations
Gov	Government institutions
Org	Non-profit organisations
Mil	Military groups
Edu	Educational institutions
Net	Major network support centers
Int	International organisations

There are also top-level domains named for each of the ISO 3166 international 2-character country codes (e.g., zw for Zimbabwe). These are called the country domains. Many countries have their own second-level domains underneath, which parallel the generic top-level domains.

As it is a simple matter in principle to search the database for an IP address with its symbolic name (because of the hierarchical structure), the reverse process cannot follow the hierarchy. Therefore, there is another namespace for the reverse mapping called Inverse domain. The information about the inverse domain is always stored in the domain "in-addr.arpa". Here, the IP addresses are stored in a hierarchical form such that each level of the tree depicts 8 bits of information of IP address. However, since domain names have the least significant parts of the name first, but dotted decimal format has the most significant bytes first, the dotted decimal address is shown in reverse order. For example, the domain in the domain name system corresponding to the IP address 171.10.1.2 is 2.1.10.171.in-addr.arpa. The above mapping is carried out by using a special kind of query called inverse pointer query.

4.2.4 Domain Name Resolution

The concept of mapping a domain name to an IP address and *vice-versa* is known *as* resolution process. The resolution process is basically a client server platform. Whenever a user needs to map an address to a domain or *vice-versa,* the DNS calls a client program called resolver. The resolver subsequently contacts the nearest DNS server (name server) with a request. In case the server has the desired information, it replies back with the results. Otherwise it suggests the resolver to other domain servers or asks other servers to provide the desired information. The resolver, after receiving the results asserts the information and thereafter delivers the desired information to the specific host process. The steps followed in the resolution are below:

1) The user program issues a request such as the gethostbyname( ) system call. ***(This particular call is used to ask for the IP address of a host bypassing the host name as a parameter).***

2) The resolver formulates a query to the name server.

3) The name server checks to see if the answer is in its local authoritative database or cache, and if so, returns it to the client. Otherwise, it will query other available name server(s), starting down from the root of the DNS tree or as high up the tree as possible.

4) The user program will finally be given a corresponding IP address (or host name, depending on the query) or an error if the query could not be answered.

As the resolution process is carried out with the help of queries, these domain name request queries can be one of two types: ***recursive*** or ***iterative.*** A flag bit in the domain name query specifies whether the client desires a recursive query, and a flag bit in the response specifies whether the server supports recursive queries. A recursive query requests that the server should itself issue a query to determine the requested information and return the complete answer to the client. However, an iterative query means that the name server should return what information it has available and also a list of additional servers for the client to contact to complete the query.

The concept of caching is also utilised in DNS. Whenever a name-server receives a request from a client, the name server subsequently sends the query to other servers. Later on, when it receives the response, it first stores this information in its own cache memory before sending the desired information to the client. Now onwards, if any client desires the same information, first the name-server can simply check its cache memory and resolve the query. However, such a response is designated as **non-**authoritative. The domain name responses from the name server can be one of two types: authoritative and non-authoritative.

4.2.5 Messages used in DNS

As DNS follows the client server paradigm, it has two types of messages: Query and Response. The messages in the DNS use a single format **i.e.,** similar format. The general format of a query message and that of a response message are shown in ***Figures5*** and 6.

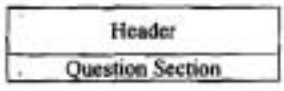

Figure 5: Query Message

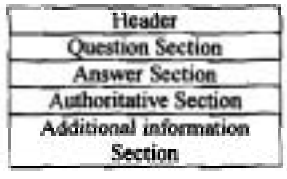

Figure 6: Response Message

The format of the header of the message is shown in ***Figure*** 7. The header section is always present and has a fixed length of 12 bytes.

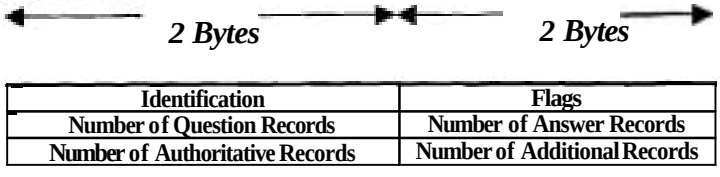

Figure 7: Header format for Query/Response

- **Identification** used by the source of the message in order to match the response of the query.
- **Flags** contains various fields that define the kind of message **i.e.,** recursive, iterative, authoritative, non-authoritative etc.
- **Number of Question Records** contains the total number of queries asked by the resolver in the Question Section.
- **Number of Answer Records** contains the total number of answers specified in the Answer Section.
- **Number of Authoritative Records** contains the total number of Authoritative records in the Authoritative Section.
- **Number of Additional Records** contains the total number of Additional records in the Additional Section.

It may be noted that the Number of Answer Records, Number of Authoritative Records, Number of Additional Records sections will have ZERO value in the query message.

Example

Now let us take up an example and illustrate the complete procedure of mapping a domain name to an IP address.

1) Let us say a user opens a web browser and tries to connect to a website, say www.ignou.ac.in.
2) The operating system not knowing the IP Address for www.ignou.ac.in, asks the (Internet Service Provider) ISP's DNS Server for this information.
3) The ISP's DNS Server does not know this information, so it connects to a Root Server to find out what name server, running somewhere in the world, knows the information about ignou.ac.in.
4) The Root Server tells the ISP's DNS Server to contact a particular name server that knows the information about ignou.ac.in.
5) Thereafter, the ISP's DNS Server connects to IGNOU's DNS server and asks for the IP Address for www.ignou.ac.in.
6) IGNOU's DNS Server responds to the ISP's DNS server with the appropriate IP Address.
7) The ISP's DNS Server tells the User's operating system the IP Address for ignou.ac.in.
8) The operating system tells the Web Browser the IP Address for www.ignou.ac.in.
9) The web browser connects and starts communication with www.ignou.ac.in.

4.2.6 Dynamic DNS (DDNS)

The Dynamic Domain Name System (DDNS) is a protocol that defines extensions to the DNS in order to enable the DNS servers to accept the requests to add, update and delete entries in the DNS database dynamically. Because DDNS offers a functional superset to existing DNS servers, a DDNS server can serve both static and dynamic domains at the same time. Rather than allowing any host to update its DNS records, the secure version of DDNS uses public key security and digital signatures to authenticate update requests from DDNS hosts.

Three common utilities for querying name servers are provided with many DNS implementations:

1) Host obtains an IP address associated with a host name or a host name associated with an IP address.
2) Nslookup allows you to locate information about network nodes, examine the contents of a name server database and establish the accessibility of name servers.
3) Hig allows you to exercise name servers, gather large volumes of domain name infomation, and execute simple domain name queries. DIG stands for Domain Internet Groper.

The following RFCs define the Domain Name System standard and the infomation kept in the system:

1) RFC 1032 – Domain Administrator's Guide
2) RFC 1033 – Domain Administrator Operations Guide
3) RFC 1034 – Domain Names – Concepts and Facilities
4) RFC 1035 – Domain Names – Implementation and Specification
5) RFC 1101 – DNS Encoding of Networks Names and Other Types.

Check Your Progress 1

1) In the following domain names, identify the name using a country based domain name

a) www.yahoo.com
b) www.ignou.ac.in
c) www.hotmail.com
d) www.aol.com

.....

.....

2) The domain name resolution can be carried out through which of these methods?

a) Iterative
b) Recursive
c) Caching
d) All of the above

.....

.....

.....

3) If the IP address of the machine is known and we want to enquire about its domain name, which one of the following is used?

a) Generic domains
b) Country domains
c) Inverse domain
d) None of the above

.....

.....

.....

4.3 ELECTRONIC MAIL

Electronic mail (e-mail) is probably the most popular service of TCPAP. For most people, it has become an integral part of everyday life. Electronic mail provides a platform for exchanging information between two end users. It is basically used for sending and receiving mails/messages, e.g., textual, voice, graphical and video messages between end users. This section provides an overview of the TCPAP application protocol dealing with electronic mail.

4.3.1 Simple Mail Transfer Protocol (SMTP)

The standard mechanism for electronic mail in the Internet is Simple Mail Transfer Protocol (SMTP). It provides mail and message exchange between TCPAP hosts. SMTP is based on end-to-end delivery i.e., an SMTP client contacts the destination host's SMTP server directly for delivering the mail. The destination host's SMTP server keeps the mail until the mail has been successfully copied into the recipient's SMTP. The SMTP is a connection service based on client-server environment and runs on port number 25 at the server side as shown in the following Figure 8. The various components of SMTP are:

1) Mail Transfer Agent (MTA)

2) User Agent (UA)

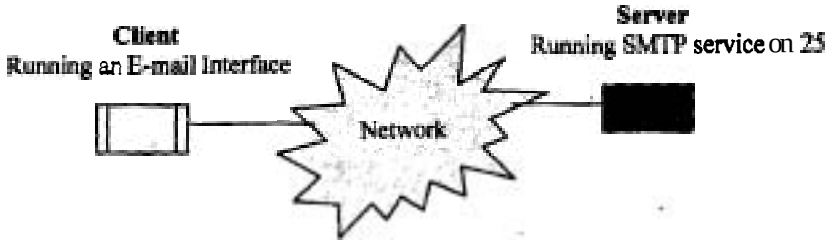

Figure 8: SMTP Service

4.3.2 Message Transfer Agent

The transfer of messages i.e., mails is delivered through an agent known as Message Transfer Agent (MTA). MTAs assist a user in sending as well as receiving the messages. The MTA consists of two shades i.e., MTA client for sending the mail while MTA server for listening/receiving the mails as shown in *Figure10*. The MTA is generic and deʌnes how the commands and responses should be sent back and forth. A popular example of MTA in UNIX is known as sendmail.

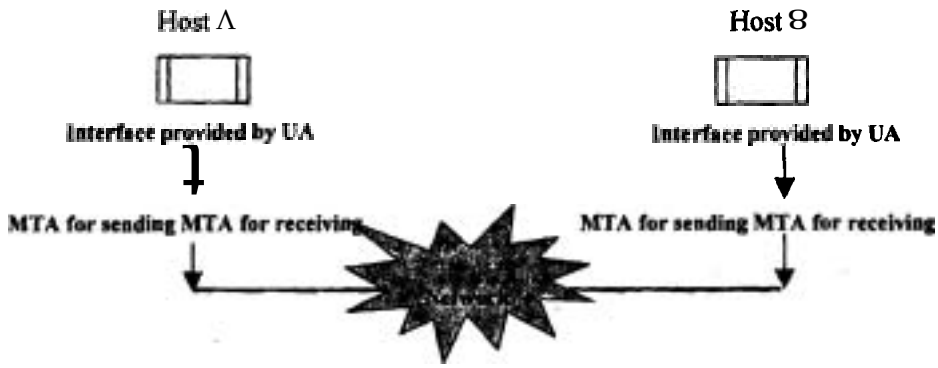

Figure 9: SMTP

4.3.3 User Agent

The usei agent mainly deals with the composition of messages. The usei agent provides an interface in the form as shown in *Figure 10* wherein s/he can write the message, specify the destination address (that is create an envelope). Therefore, UA puts the message into the envelope. The various services offered by the user agent are as under:

1) Reading the received messages
2) Replying to the read messages
3) Composing the messages
4) Forwarding the messages
5) Handling the various mailbox settings

Figure 10: Interface provided by UA for composing a message

The address of a usei (E-mail address) consists of two parts: the usei name and the domain name. For example, amitgoel@yahoo.com is an e-mail address, wherein "amitgoel" depicts the usei name, yahoo.com represents the domain name and these

two parts are separated by an @ sign. Therefore, the mechanism of representing an e-mail address used by SMTP includes user name, @ and domain name. Remember that UA does not provide the facility for sending and receiving messages. The address of the destination host contains the domain name for identifying a particular network and thereafter a specific user on its network.

The interface presented by the user agents can be two types: command based or graphical interface based. The various examples of user agents with respect to command based interface are pine, mail etc. and with respect to GUI, some examples are: Netscape, outlook express etc.

4.3.4 Post Office Protocol (POP)

As SMTP is based on TCP/IP protocol, a TCP connection is required to be established between both ends. However, user machines cannot be expected to be online 24 x 7, especially a desktop machine owned by a home user. Therefore, there was a need for developing a system by which a user could receive his/her e-mails even though the machine was powered off. Therefore, most of the organisations install a SMTP server which is always online and receives e-mails on the behalf of each and every user of the organisation on its network. Basically the SMTP server acts as a "post office".

In order to retrieve the e-mails stored in the SMTP server on the behalf of the users, a protocol called ***Post Office Protocol (POP)*** has been devised. It assists in downloading the e-mails from the SMTP server as shown in ***Figure 11***.

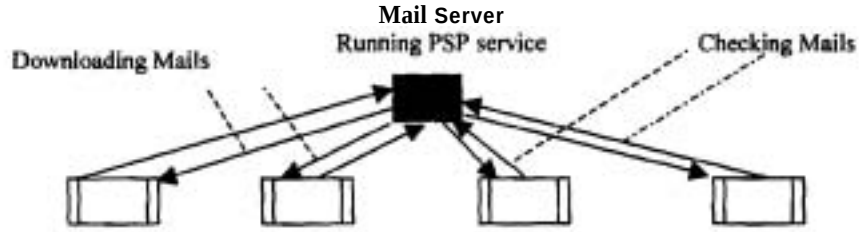

Figure 11: POP

4.3.5 Internet Mail Access Protocol (IMAP)

In POP, whenever a user accesses the mails from the mail server, i.e., downloads the mails, instantantly those accessed mails are deleted from the mail server. Thus, POP is not suitable for people accessing their mails from various locations, i.e., cyber cafe, home, hotel etc. POP does not provide the facility for creating folders, organising the mails on the mail server etc.

In order to avoid the deletion of the mails from the mail server, another protocol called Internet Mail Access Protocol (IMAP) has been devised. In addition to services offered by POP, IMAP provides the following services:

1) The user can create, rename or delete the mailbox on the mail server.

2) The user can check the header part of the mail before downloading the message

4.3.6 Multipurpose Internet Mail Extension (MIME)

The SMTP protocol sends the mails i.e., the messages only in a Network Virtual Terminal seven-bit ASCII format. That is, it will support only those languages that can be represented by a seven-bit ASCII format. Therefore, messages written in languages such as German, Russian and French cannot be sent through SMTP. Moreover, SMTP does not support the transfer of video files, audio files and binary files. Thus, there was a need for developing a mechanism for allowing the transfer of incompliant formats.

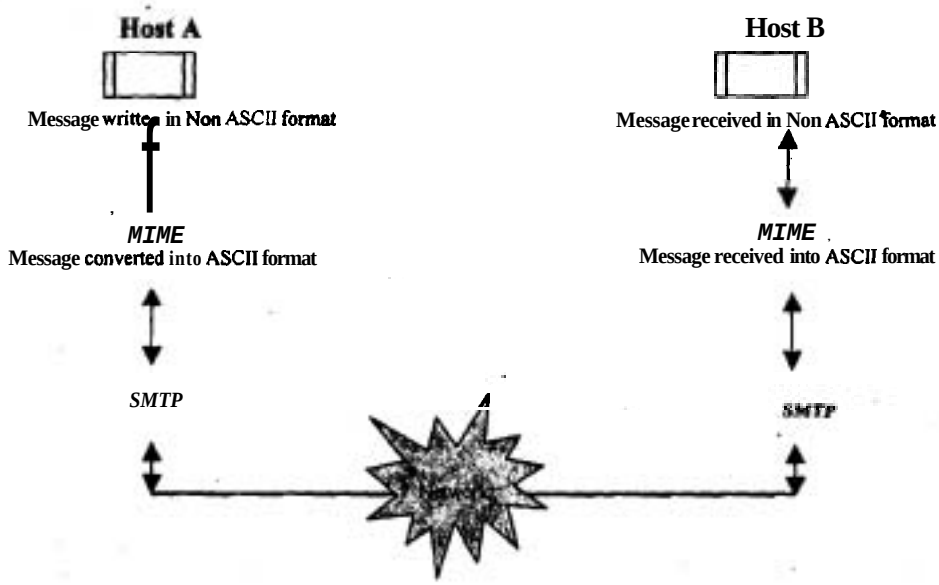

Figure 12: MIME

A protocol called Multipurpose Internet Mail Extension (MIME) supports transfer of Non-ASCII formats through SMTP. Primarily, MIME converts the non-ASCII formats into ASCII format and passes the data to SMTP. Consequently, the SMTP sends the ASCII form of data to the destination machine. The SMTP service at the destination machine passes the ASCII form of data to MIME which in turn converts the data into non-ASCII format as shown in Figure 12. Remember that MIME is simply an extension of SMTP and is not a mail protocol.

MIME defines five headers which can be supplemented with the original SMTP header in order to define the following parameters:

- **MIME Version:** It defines the version of MIME being used. The current version of MIME is 1.1
- **Content**-Type: It defines the type of data used in the body of the message, e.g., text, image, video, audio, postscript etc.
- **Content-Transfer-Encoding:** It defines the method to encode the mail message into 0's and 1's. The various kinds of encoding techniques are as follows: ASCII-7 bit, Non-ASCII-8 bit, Non-ASCII-Binary, Non-ASCII-Base64 and Non-ASCII-Quoted-printable.
- **Content-id:** It identifies the complete message in a multiple-message scenario.
- **Content-Description:** It describes whether the body of the message is text, image, video audio etc.

Check Your Progress 2

1) What is the purpose of Message Transfer Agents?

a) Creation of envelopes

b) Transfer of messages

c) Writing the messages

d) None of the Above

.....

.....

2) Which field of MIME header describes the method to encode the message?

a) Content-type
b) Content-id
c) Content-transfer-encoding
d) Content-description

.....

.....

3) How is the Non-ASCII formats converted into ASCII format?

a) MIME
b) POP
c) IMAP
d) SMTP

.....

.....

4) Give a difference between POP and IMAP.

.....

.....

4.4 TELNET

The most fundamental method of data communication employed on a network is the ability to perform remote execution i.e. calling an application on a remote terminal. TELNET is a widely known application protocol that provides remote execution capability.

TELNET is ə popular client server application program. TELNET is an abbreviation for ***TErminal NETwork***. TELNET is a standard application protocol that provides an interface, through which ɐ program on a host i.e., *TELNET client* can access the resources of another host i.e., *TELNET server*. TELNET provides an environment such that the client acts as a local terminal connected to the server as shown in *Figure 13*. Basically, TELNET is ɐ utility whereby ə user first logs into ɐ remote machine and thereafter the user can access the files / programs located remotely.

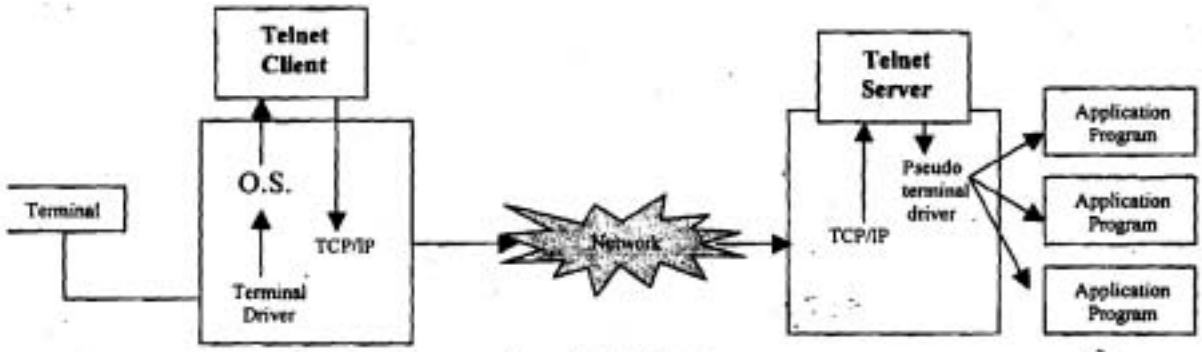

Figure 13: TELNET

The working of TELNET is as follows: The user types on the host machine /terminal that runs ɐ driver known as terminal driver (ɐ module of the operating system). It basically receives the keystrokes typed by the user on the terminal and pəsses the corresponding characters to the operating system. The operating system in turn sends these characters to the TELNET client. As discussed in SMTP, the language/format acceptable to the terminal might be different from the format allowed by TELNET. Therefore, the characters received by the TELNET client from the terminal driver ɯe

converted into a generic character set known as Network Virtual Terminal (NVT) characters. The transformed form of characters is sent to the TCP/IP protocol stack of the local machine.

The characters travel through the network using TCP/IP and finally reach the destination's operating system. The operating system passes the NVT characters to the TELNET server. The TELNET server in turn transforms the characters into characters understandable by the destination machine. The set of characters is sent to the operating system through a special kind of driver called pseudoterminal driver. As the TELNET server cannot directly interact with the operating system, the pseudoterminal driver helps the TELNET server in simulating a terminal. Thus, these characters from the operating system are delivered to the appropriate application program of the remote machine.

4.5 FILE TRANSFER PROTOCOL (FTP)

The transfer of files between two machines is one of the most common operations in a network. The standard mechanism for copying files from one machine to another is known as File Transfer Protocol (FTP).

Although it might seem quite simple to transfer data between two hosts, there are many issues which are to be resolved in such a transfer. For instance, two systems may use different file name conventions, different representation of data, different directory structures etc. These issues have been resolved with the help of FTP. FTP employs a client server environment. In order to access remote files in FTP, the user must firstly authenticate to the server before it allows the file transfer. Remember, FTP uses a connection-oriented service i.e., it is necessary to have both hosts up and running TCP/IP to establish a file transfer. After the establishment of connection, the data transfer between client and server takes place.

FTP uses TCP as a transport protocol to provide reliable end-to-end connection. The FTP server listens to connections on well-known port number 20 for transfer of data (data connection) and 21 for establishment/termination of connection (control connection). The control connection performs the task of authentication with the help of login and thereafter follows the TELNET protocol. As it is necessary to log into the remote host, the user must have a user name and a password to access files and directories.

The FTP application is built with a user interface at the top of the protocol, a Data Transfer Process (DTP) and protocol interpreter (PI) as shown in *Figure* 14. On the client side, the user interface communicates with the protocol interpreter which is in charge of the control connection. This protocol interpreter (PI) has to communicate any necessary control commands to the remote system. On the Server side, the protocol interpreter, besides its function of responding to the TELNET protocol, has to initiate the data connection. During the file transfer, the data management is performed by DTPs. After a user's request is completed, the server's PI has to close the data connection.

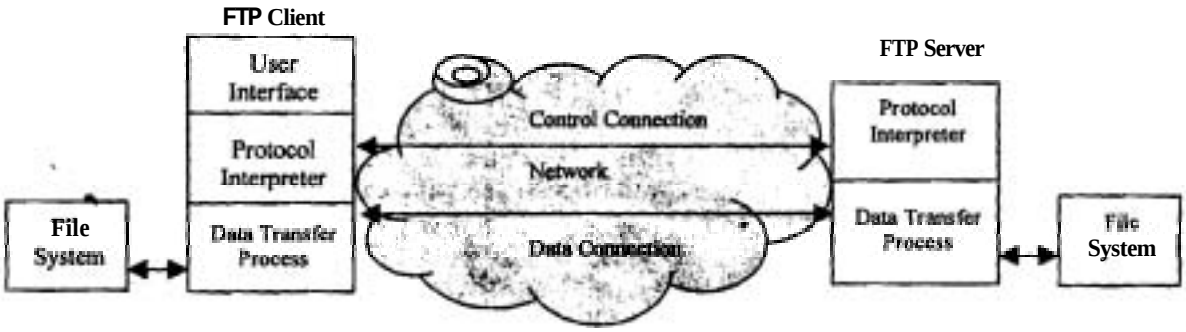

Figure 14: File Transfer Protocol (FTP)

The basic steps performed by a client during an FTP session are as given below:

1) **Connect the user to a remote host**

First the user has to authenticate the server machine about the user's authenticity with the help of a valid user name and password. The various commands that are required for connection establishment are:

- On the command prompt type "ftp".
- Then write a command "open" along with the IP address of the server machine, e.g., open 202.12.14 1.8 1. The open command imitates a login session on the remote machine.
- After connecting to the remote host, the remote machine enquires about the user name and its corresponding password.

  ftp> login
  ftp> password

- The other commands are user and pass. The purpose of user command is to identify a remote user id. The purpose of pass command is to authenticate the remote user id.

2) **Select a directory**

After connection is established, the client searches for the appropriate directory using "cd" (change directory) command. The user can select a local directory with the lcd (local change directory) command.

3) **List files available for transfer**

Commands like dir or ls are used for listing the various files in a particular folder depending upon the operating system.

4) Define the transfer mode

As the data transfer can take place between dissimilar systems, transformations of the data into an understandable form is required. The user has to mainly decide on two aspects of the data handling: first, the method through which the bits will be moved from one place to another and secondly, the different representations of data. In order to deal with the above issues, the following commands are used:

- **Mode:** It specifies whether the file is to be assumed as record structure in a byte stream format.
- **Type:** It specifies the character set being used for representation of data, i.e., ASCII, Image etc.

5) **Copy files to or from the remote host**

The following commands can be used to copy files between FTP clients and servers:

- **Get command:** It copies a file from the remote host to the local host.
- **Mget command:** It copies multiple files from the remote to the local host.
- **Put command:** It copies a file from the local host to the remote host.
- **Mput command:** It copies multiple files from the local host to the remote host.

6) **Disconnect from the remote host**

In order to disconnect a connection, the following commands can be used:

- **Close:** It disconnects from the remote host but leaves the FTP client running.
- **Quit / bye:** It disconnects from the remote host and terminates FTP.

FTP Illustration

Example 1

C:\] ftp www.ymcaie.ernet.in
Connected to ymcaie.ernet.in 220

```
ymcaie FTP server (Version 4.1) ready.
Name: Amit
Password required for Amit.
Password: ******
User Amit logged in.
ftp> put file.txt filel .txt
200 PORT command successful.
150 Opening data connection for file.txt (3453 bytes).
226 Transfer complete.
Local: file.txt remote: filel .txt 3453 bytes received in 0.082 seconds
ftp> close
221 Goodbye.
ftp> quit
```

Example 2

```
C:\] ftp www.ymcaie.ernet.in
Connected to ymcaie.ernet.in 220
ymcaie FTP server (Version 4.1) ready.
Name: Amit
Password required for Amit.
Password: ******
User h i t logged in.
ftp> Is /usr/amit
200 PORT command successful.
150 Opening ASCII mode.
226 Transfer complete.
ftp> close
221 Goodbye.
ftp> quit
```

Anonymous FTP

The first step required for establishing a connection with a remote host is a valid id and password. However, there are few FTP servers that are available for general public access. Thus, in order to provide access to those public remote servers,,a user need not have valid user id. ***The user name for such servers is anonymous and password is guest.*** **Remember,** the user access is limited in such cases.

Example 3

```
C:\] ftp www.ymcaie.ernet.in
Connected to ymcaie.ernet.in 220
ymcaie FTP server (Version 4.1) ready.
Name: anonymous
331 guest login OK, send "guest" as password
Password: guest .
ftp> get file.txt filel.txt
200 PORT command successful.
150 Opening data connection for file.txt (3453 bytes).
226 Transfer complete.
Remote: file.txt Local: filel.txt 3453 bytes received in 0.072 seconds
150 Opening ASCII mode.
226 Transfer complete.
ftp> close
221 Goodbye.
ftp> quit
```

Check Your Progress 3

1) Which command is used in ftp for connection establishment?

a) open
b) get
c) put
d) quit

.....

2). Which command is used in ftp for transfer of data from local machine to remote machine?

a) open
b) get
c) put
d) quit

.....

3). How many times is the control connection required in an FTP session?

a) Once
b) Twice
c) Many times
d) None of the above.

.....

4) How many times is the data connection required in an FTP session?

a) Once
b) Twice
c) As many times as required
d) None of the above.

.....

.....

.....

4.6 SUMMARY

This unit provides a complete overview of application layer of TCP/IP. Till now we have studied that there are various kinds of application layer related protocols. Some of them have been discussed in this unit, e.g., DNS, SMTP, TELNET and FTP. The domain name system is a client server based application that maps the domain names in the form of IP addresses. DNS maintains a hierarchical structure in order to store the information about a huge set of domain names. The name space is distributed among DNS servers. Every server is assigned a responsibility for a particular zone. There are 13 root servers located in different geographical regions. Each zone has its own primary server known as zone server. Whenever a user requests for an IP address, the name resolution, through a function called resolver, maps the domain name to the IP address and *vice-versa*.

The SMTP protocol provides a mechanism for providing a user interface and transfers the messages on the network. It has the following components: UA and MTA. The UA provides the interface for composing, reading, replying and forwarding the mail messages. The MTA performs the actual transfer of messages, on the network. MIME is a supplement to SMTP for allowing Non-ASCII format messages like video, audio etc. to be transferred through SMTP. POP and IMAP are extensions of SMTP that allow the messages to be stored into the mail server, so that later on, a user can access the mail server and read his/her mails.

TELNET protocol is a client server based application that provides remote login. FTP is a TCP/IP based application protocol employed for transferring files from one host to another. The basic commands required for connection establishment are: *open,* site etc. The commands used for data transfer are: ***get, mget, put and mput.*** The commands *used* for terminating a connection are: quit and close. The next block of this course covers the concepts of network programming.

4.7 SOLUTIONS/ANSWERS

Check Your Progress 1

1) B
2) D
3) C

Check Your Progress 2

1) B
2) C
3) A
4) POP downloads the mail messages on its client end and those mails are deleted automatically at the mail server end. However, IMAP avoids such deletions.

Check Your Progress 3

1) A
2) C
3) A
4) C

4.8 FURTHER READINGS

1) Andrew S. Tanenbaum, *Computer Networks,* Third edition.
2) Behrouz A. Forouzan, *Data Communications and Networking,* Third edition.
3) Douglas E. Comer, ***Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture (4th*** Edition).
4) James F. Kurose, *Computer Networking: A* Top-Down Approach Featuring the Internet (3rd Edition).
5) Larry L. Peterson, *Computer Networks:* A Systems Approach, 3rd Edition (The Morgan Kaufmann Series in Networking).
6) W. Richard Stevens, ***The Protocols (TCP/IP Illustrated, Volume 1)***.
7) William Stallings, *Data* and *Computer Communications,* Seventh Edition.