Electronics Engineering

Advanced Communication

Comprehensive Theory

with Solved Examples and Practice Questions

MADE EASY Publications

MADE EASY Publications

Corporate Office: 44-A/4, Kalu Sarai (Near Hauz Khas Metro Station), New Delhi-110016
E-mail: infomep@madeeasy.in
Contact: 011-45124660, 8860378007

Visit us at: www.madeeasypublications.org

Advanced Communication

First Edition: 2017
Second Edition: 2018
Third Edition: 2019
Fourth Edition: 2020

Contents

Advanced Communication

Advance Communication-I

Advance Communication-II

■■■

Prelude to Advanced Communication-I

Every user in telecommunication is interested in higher and higher data rates and need for the high data rates is never ending. For higher data rates, we are going at higher and higher frequencies. The figure shown below shows the electromagnetic spectrum for the telecommunication.

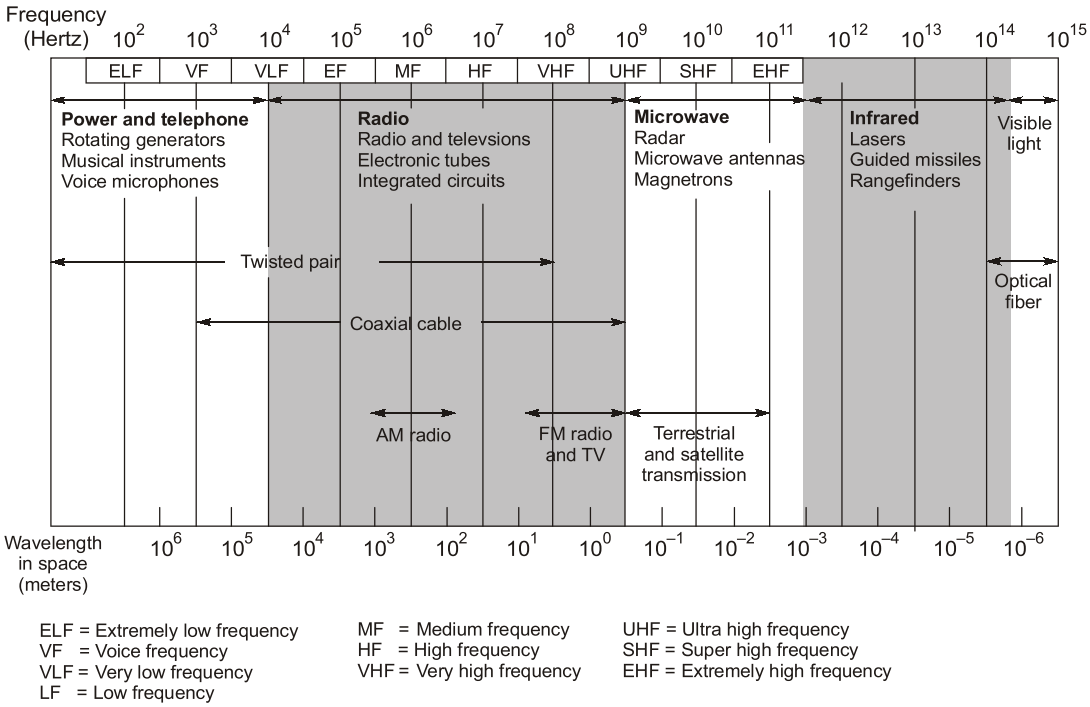


Figure : *Electromagnetic spectrum for telecommunication*

Microwave Line of Sight (LOS) includes both terrestrial and satellite communication. The communication media between the two users depends on the surrounding environment conditions. In the hilly areas, where the optical fibre cable is very difficult to lay down, the satellite communication is preferred over optical fibre.

While, the areas where optical fibre cable is easy to lay down, we prefer optical fibre to microwave LOS system. Also, from the above figure as we see the carrier frequencies of optical fibre is more as compared to that of terrestrial and satellite transmission system, so higher data rates are achievable with the help of optical fibre system.

We have divided this part of book into three parts. Chapter 1 deals with the microwave communication in which we study various types of communication mechanism at different frequencies we have also discussed various types of microwave communication systems.

In chapter 2, we are dealing with orbits of satellite and calculated various losses in satellite communication system alongwith link margin of satellite communication system.

In chapter 3, we have studied the transmission characteristics of optical fibre, different types of optical fibre, sources and detectors in optical fibre system and link margin of the system.

CHAPTER 6

Application Layer

6.1 Introduction

Application layer protocols specifies the format and control information necessary for many of the common Internet communication functions. Among these TCP/IP protocols are:

- Domain Name Service Protocol (DNS): It is used to **resolve Internet names to IP addresses**.
- Hypertext Transfer Protocol (HTTP): It is used to **transfer files that make up the Web pages** of the World Wide Web.
- Simple Mail Transfer Protocol (SMTP): It is used for the **transfer of mail messages and attachments**.
- File Transfer Protocol (FTP): It is used for interactive **file transfer between systems**.

6.2 Application Layer Protocols

Application layer **uses protocols that are implemented within applications and services.**

While applications provide people with a way to create messages and application layer services establish an interface to the network, protocols provide the rules and formats that govern how data is treated.

The Application layer, protocols specify what messages are exchanged between the source and destination hosts, the syntax of the control commands, the type and format of the data being transmitted, and the appropriate methods for error notification and recovery.

6.2.1 Application Layer Protocol Functions

Application layer protocols are used by both the source and destination devices during a communication session.

Protocols specify how **data inside the messages is structured** and the types of messages that are sent between source and destination. Protocols establish consistent rules for exchanging data between applications and services loaded on the participating devices.

The messages exchanged can be requested for services, acknowledgments, data messages, status messages, or error messages. Protocols also define message dialogues, ensuring that a message being sent is met by the expected response and the correct services are invoked when data transfer occurs.

Applications and services may also use multiple protocols in the course of a single conversation. One protocol may specify how to establish the network connection and another describe the process for the data transfer when the message is passed to the next lower layer. Application layer protocols define:

1. Types of messages
2. Syntax of messages
3. Meaning of any informational fields
4. How messages are sent and the expected response
5. Interaction with next lower layer

6.2.2 Port Numbers

Transport layer uses an addressing scheme called a port number. Port numbers identify applications and Application layer services that are the source and destination of data.

For TCP/IP Application layer protocols and services, we will be referring to the TCP and UDP port numbers normally associated with these services. Some of these services are:

- Domain Name System (DNS): TCP/UDP Port 53
- Hypertext Transfer Protocol (HTTP): TCP Port 80
- Simple Mail Transfer Protocol (SMTP): TCP Port 25
- Post Office Protocol (POP): UDP Port 110
- Telnet: TCP Port 23
- Dynamic Host Configuration Protocol: UDP Port 67
- File Transfer Protocol (FTP): TCP Ports 20 and 21

6.3 Application Layer Protocols and Services Examples

DNS (Domain Name Service)

- In data networks, devices are labelled with numeric IP addresses, so that they can participate in sending and receiving messages over the network. However, most people have a hard time remembering this numeric address. Hence, domain names were created to convert the numeric IP address into a simple, recognizable name.
- On the Internet these domain names, such as www.cisco.com, are much easier for people to remember than 198.133.219.25, which is the actual numeric address for this server. Also, if Cisco decides to change the numeric address, it is transparent to the user, since the domain name will remain www.cisco.com. The new address will simply be linked to the existing domain name and connectivity is maintained.
- When networks were small, it was a simple task to maintain the mapping between domain names and the addresses they represented. However, as networks began to grow and the number of devices increased, this manual system became unworkable. The Domain Name System (DNS) was created for domain name to address resolution for these networks. DNS uses a distributed set of servers to resolve the names associated with these numbered addresses.
- **The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data formats. DNS protocol communications use a single format called a message.**

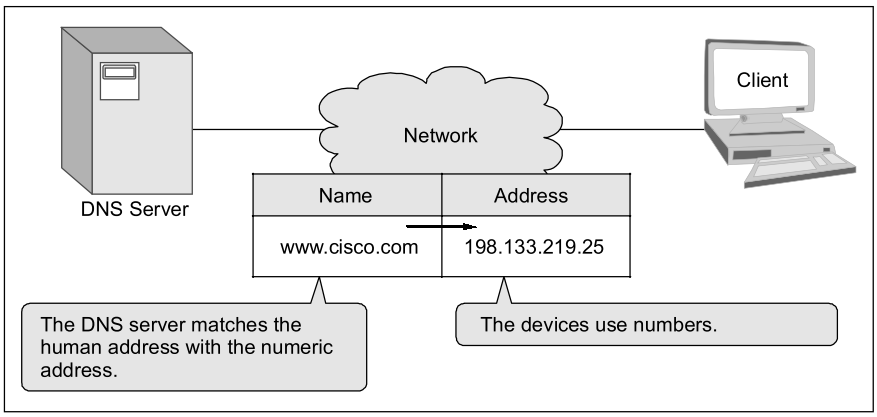


Figure-6.1

- This message format is used for all types of client queries and server responses, error messages, and the transfer of resource record information between servers.
- **DNS is a client/server** service; however, it differs from the other client/server services. While other services use a client that is an application (such as web browser, e-mail client), the **DNS client runs as a service itself**. The DNS client, sometimes called the DNS resolver, supports name resolution for our other network applications and other services that need it. When configuring a network device, we generally provide one or more DNS Server addresses that the DNS client can use for name resolution.
- Usually the Internet service provider provides the addresses to use for the DNS servers. When a user's application requests to connect to a remote device by name, the requesting DNS client queries one of these name servers to resolve the name to a numeric address. A DNS server provides the name resolution using the name domain, which is often called named, (pronounced name-dee). The DNS server stores different types of resource records used to resolve names.

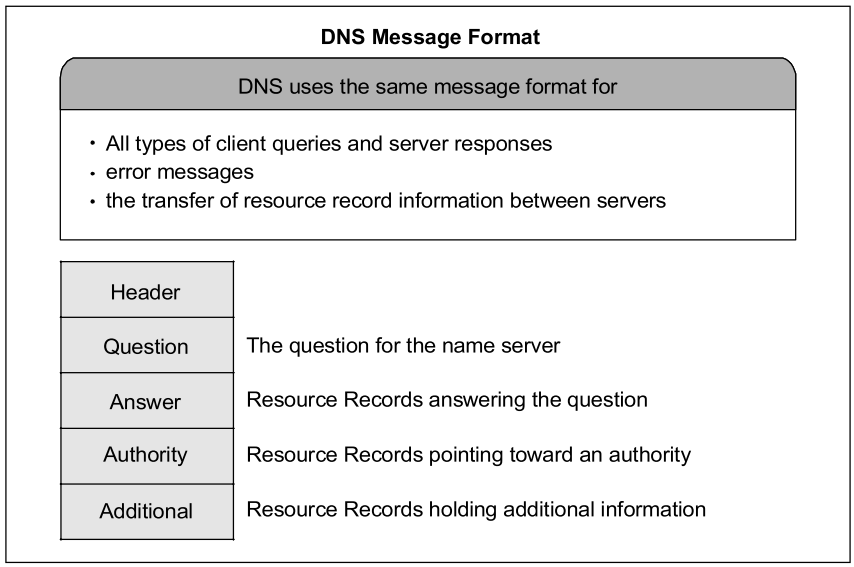


Figure-6.2

- **The Domain Name System uses a hierarchical system to create a name database to provide name resolution.**
- The hierarchy looks like an **inverted tree with the root at the top and branches below**. At the top of the hierarchy, the root servers maintain records about how to reach the top-level domain servers, which in turn have records that point to the secondary level domain servers and so on. The different top-level domains represent either the type of organization or the country of origin.
- Examples of top-level domains are:
  (i) .au - Australia
  (ii) .co - Colombia
  (iii) .com - a business or industry
  (iv) .jp - Japan
  (v) .org - a non-profit organization

- After top-level domains are second-level domain names, and below them are other lower level domains. Each domain name is a path down this inverted tree starting from the root. For example, as shown in the figure, the root DNS server may not know exactly where the e-mail server mail.cisco.com is located, but it maintains a record for the "com" domain within the top-level domain.
- Likewise, the servers within the "com" domain may not have a record for mail.cisco.com, but they do have a record for the "cisco.com" domain.
- The servers within the cisco.com domain have a record (a MX record to be precise) for mail.cisco.com. The Domain Name System relies on this hierarchy of decentralized servers to store and maintain these resource records. The resource records list domain names that the server can resolve and alternative servers that can also process requests. If a given server has resource records that correspond to its level in the domain hierarchy, it is said to be authoritative for those records.
- For example, a name server in the cisco.netacad.net domain would not be authoritative for the mail.cisco.com record because that record is held at a higher domain level server, specifically the name server in the cisco.com domain.

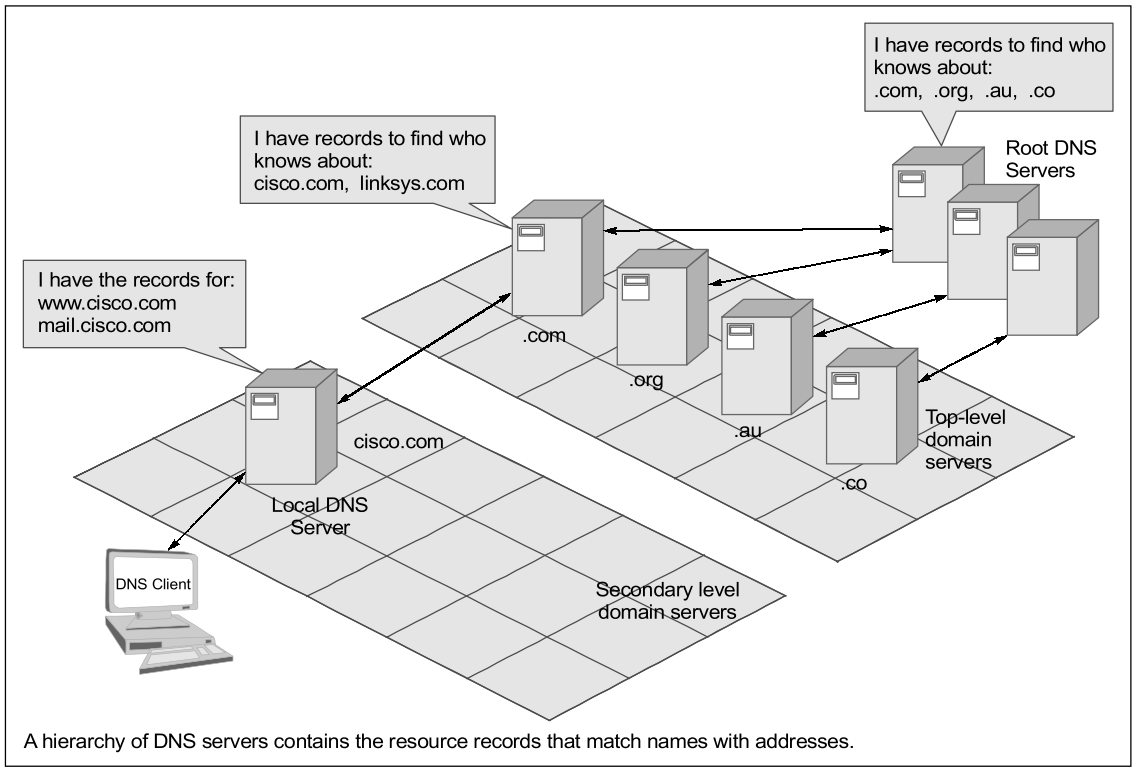


Figure-6.3

6.4 WWW Service and HTTP

- When a web address (or URL) is typed into a web browser, the web browser establishes a connection to the web service which are running on the **server using the HTTP protocol. URLs (or Uniform Resource Locator) and URIs (Uniform Resource Identifier)** are the names most people associate with web addresses. The URL http://www.mysite.com/index.html is an example of a URL that refers to a specific resource - a web page namedindex.html on a server identified as mysite.com. Web browsers are the client applications. Our computers use to connect to the World Wide Web and access resources stored on a web server.

- As with most server processes, the web server runs as a background service and makes different types of files available. In order to access the content, web clients make connections to the server and request the desired resources. The server replies with the resources and, upon receipt, the browser interprets the data and presents it to the user.
- Browsers can interpret and present many data types, such as plain text or Hypertext Markup Language (HTML, the language in which web pages are constructed). The Hypertext Transfer Protocol (HTTP), one of the protocols in the TCP/IP suite, was originally developed to publish and retrieve HTML pages and is now used for distributed, collaborative information systems. Other types of data, however, may require another service or program, typically referred to as plug-ins or add-ons. To help the browser determine what type of file it is receiving, the server specifies what kind of data the file contains. Let us consider a example of URL: http://www.mysite.com/web-server.html opened in a browser.
- First, the browser interprets the three parts of the URL:
  1. http (the protocol or scheme)
  2. www.mysite.com (the server name)
  3. web-server.html (the specific file name requested).
- Using the HTTP protocol requirements, the browser sends a GET request to the server and asks for the file web-server.htm. The server in turn sends the HTML code for this web page to the browser. Finally, the browser deciphers the HTML code and formats the page for the browser window.

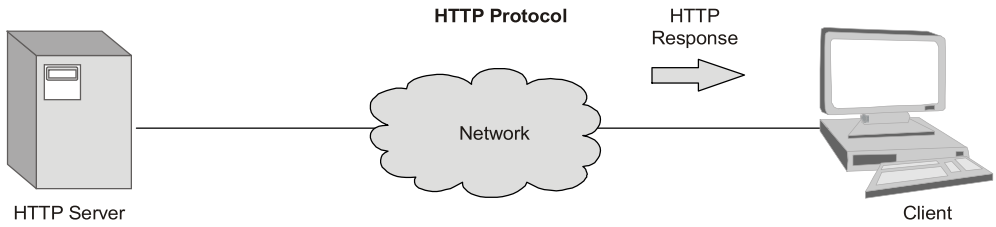


Figure-6.4: *In response to the request, the HTTP server returns code for a web page.*

- HTTP is used across the World Wide Web for data transfer and is one of the most used application protocols. HTTP specifies a request/response protocol. When a client, typically a web browser, sends a request message to a server, the HTTP protocol defines the message types the client uses to request the web page and also the message types the server uses to respond.
- The three common message types are GET, POST, and PUT. GET is a client request for data. A web browser sends the GET message to request pages from a web server. POST and PUT are used to send messages that upload data to the web server. For example, when the user enters data into a form embedded in a web page, POST includes the data in the message sent to the server. PUT uploads resources or content to the web server.
- Although it is remarkably flexible, **HTTP is not a secure protocol**. The POST messages upload information to the server in plain text that can be intercepted and read.
- Similarly, the server responses, typically HTML pages, are also unencrypted. For secure communication across the Internet, the **HTTP Secure (HTTPS) protocol is used for accessing or posting web server information**. HTTPS can use authentication and encryption to secure data as it travels between the client and server. HTTPS specifies additional rules for passing data between the Application layer and the Transport Layer.

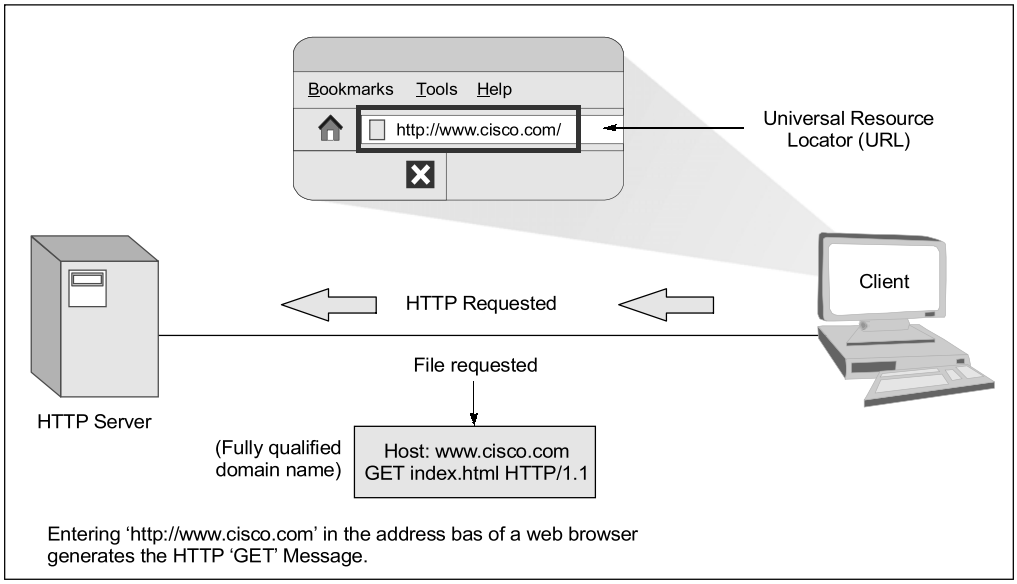


Figure-6.5

6.5 File Transfer Protocol (FTP)

The File Transfer Protocol (FTP) is another commonly used Application layer protocol. FTP was developed to allow for file transfers between a client and a server. An FTP client is an application that runs on a computer that is used to push and pull files from a server running the FTP daemon (FTPd). To successfully transfer files, FTP requires two connections between the client and the server: **one for commands and replies, the other for the actual file transfer**. The client establishes the first connection to the server on TCP port 21. This connection is used for control traffic, consisting of client commands and server replies. The client establishes the second connection to the server over TCP port 20. This connection is for the actual file transfer and is created every time there is a file transferred. The file transfer can happen in either direction. The client can download (pull) a file from the server or, the client can upload (push) a file to the server.

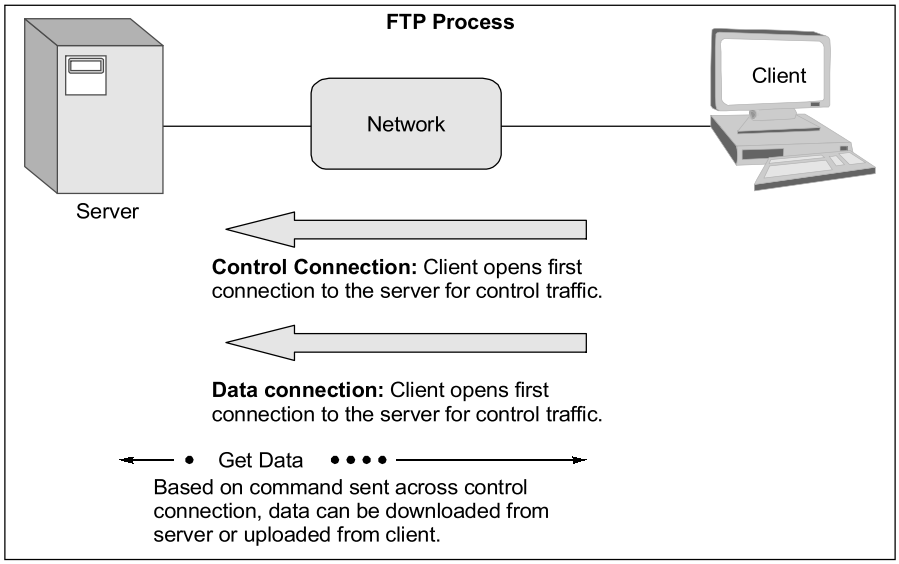


Figure-6.6

6.6 Simple Mail Transfer Protocol (SMTP)

The SMTP is TCP/IP protocol that supports electronic mail (e-mail) on the internet. IT is the system for sending messages to other computer users based on email address.

e-mail address contains two parts (i) Local part, (ii) domain part

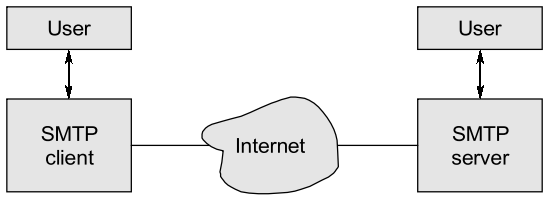
localpart@domainpart

madeeasy@yahoo.com

There are two types of agents : (i) UA (user agent), (ii) MTA (mail transfer agent)

- **User Agent (UA) :** Converts and prepares the message, creates the envelope and put the message in the envelope. The user agent is a program normally used to send and receive mail.
- **Mail Transfer Agent (MTA):** The actual mail transfer is done through MTA. To send a mail system must have client MTA and to receive mail system must have server MTA.

  The mail gateway is a relay MTA that can receive mail prepared by protocol other than SMTP and transform it to SMTP format before sending it and vice-versa.



User Agent

Figure-6.7

6.6.1 Multi-purpose Internet Mail Extension (MIME)

- MIME is a supplementary protocol that allows non-ASCII data to be send through SMTP.
- MIME transforms non-ASCII data at sender side to ASCII data and delivers it to the SMTP.

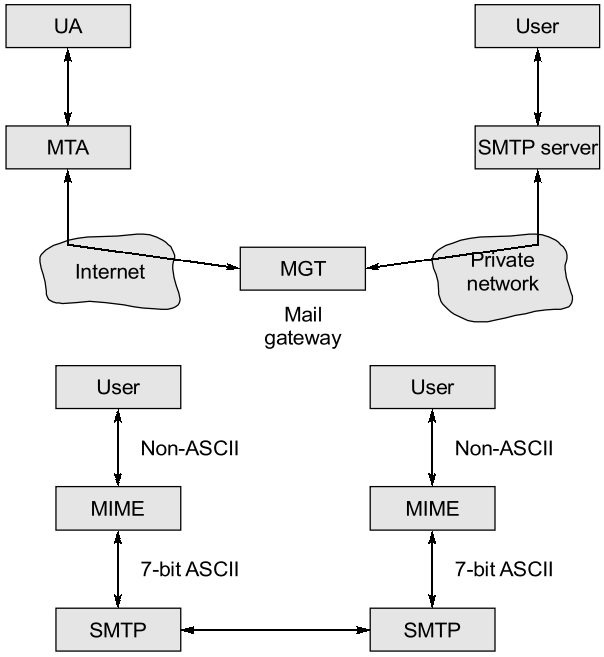


Figure-6.8

Student's Assignment

Q.1 Which of the following statements are true?

S_1 : UDP of transport layer protocol uses FTP

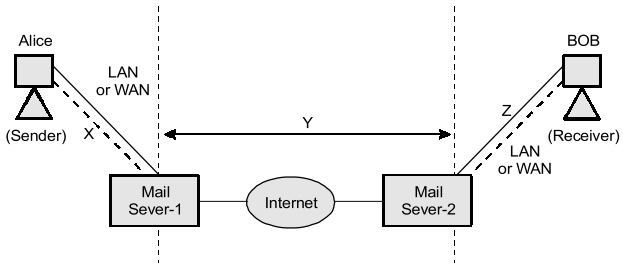
S_2 : TCP of transport layer protocol uses TFTP

S_3 : TCP uses both FTP and TFTP.

(a) Only S_1 (b) Only S_3

(c) Only S_1 and S_2 (d) None of these

Q.2 Identify the protocols X, Y and Z respectively used for mail transfer (Assume mail sent by Alice is received by Bob).



(a) POP_3, SMTP, $IMAP_4$

(b) $IMAP_4$, SMTP, SMTP

(c) SMTP, POP_3, SMTP

(d) SMTP, SMTP, $IMAP_4$

Q.3 Which of the following statement is incorrect?

(a) A reliable data transfer protocol may send multiple packets without waiting for acknowledgments, rather than operating in a stop and wait manner. This technique is called "Pipelining'.

(b) A process sends/receives messages to/ from the network through a software interface called a "Socket".

(c) Because an HTTP server maintains no information about the clients, an HTTP server said to be "Statefull".

(d) The "Traceroute" can be used to determine the number of hops to a destination and the round trip time for each hop.

Q.4 The post office protocol is an _____ protocol with both client (sender/receiver) and _____ functions

(a) Electronic mail, server (storage)

(b) Three layer, server

(c) UDP, transfer

(d) TCP, server

Q.5 PGP is one of the protocol used to provide security at the _____ it is designed to create authenticated and confidential _____.

(a) application layer, e-mail

(b) network layer, packets

(c) application layer, packets

(d) network layer, e-mail

ANSWERS

1. (d) 2. (d) 3. (c) 4. (a) 5. (a)

■■■■