1. Subject Name: E-Commerce (BBAA405SE2)
2. Semester / Year: Semester IV
3. Name of the Teacher: Pinaki Dey
4. Name of the topic: Technology in E-Commerce (Part III)

IPv5 is an experimental protocol for Unix-based systems and was never released to be used by the general public. All odd-numbered versions are developed for experimental purposes.

Table 6.3 highlights the differences between two versions of the IP.

Table 6.3 Differences between IPv4 and IPv6

IPv4	IPv6
Provides a 32-bit address	Provides a 128-bit address
Expressed in decimal format	Expressed in hexadecimal format
Can support 4.3 billion devices	Can support an infinitely large number of devices
Getting obsolete	Technologically more advanced with new features
Comparatively less compatible	More compatible for mobile networks
Comparatively small-sized data can be sent	Bigger-sized data can be sent
Comparatively less secure	More secure than IPv4

6.7.2 Transmission Control Protocol

Transmission control protocol (TCP) works at the transport layer. It is used in conjunction with the IP protocol which works on the network layer and is responsible for sending data packets between sender and receiver devices. The working of IP can be compared with the postal system which allows users to address a letter and submit it to the postal system that has no direct link between the sender and the receiver. The main responsibility of the TCP is, therefore, to establish a connection between the sender and the receiver so that reliable and error-free data transmission can take place. The connection established by TCP exists until both the devices have finished their data transmission.

Another important responsibility of TCP is segmentation and reassembly as shown in Figure 6.7. At the sender's site, TCP breaks the message into several smaller segments and at the receiver's site, TCP reassembles the fragmented data to form the complete message. Since each data packet of the same message may reach the receiver through different routes, it may happen that packet 3 arrives before packet 1. Therefore, the TCP at the receiver's site rearranges the packet in the correct sequence and then assembles them to form the complete message.

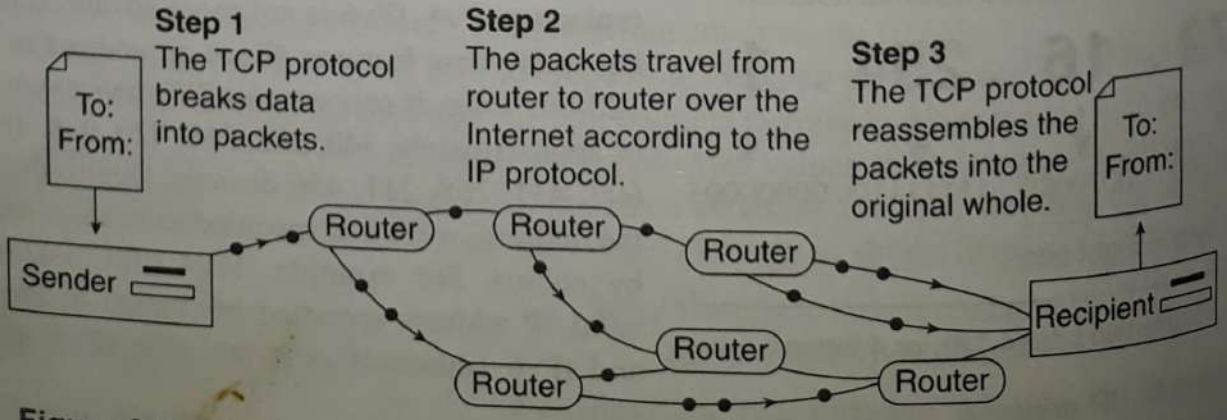


Figure 6.7 How TCP/IP works

6.7.3 User Datagram Protocol

Like TCP, the user datagram protocol (UDP) is a communications protocol that works on the transport layer (layer 4). The combination IP and UDP is known as UDP/IP. UDP is an alternative to TCP. While some applications prefer to use TCP, others make use of UDP. UDP offers limited service as compared to TCP. Unlike TCP, UDP does not break the message into smaller segments; therefore, it need not even reassemble or sequence them. If some erroneous data is received, UDP does nothing to ask the sender to resend it. For these reasons, many network applications such as trivial file transfer protocol (TFTP), videoconferencing, online computer games, watching videos online, and listening to audio online may want to save processing time because for very small data, exchanges prefer to use UDP rather than TCP. Table 6.4 and Figure 6.8 highlight the differences between TCP and UDP.

Table 6.4 Differences between transmission control protocol and user datagram protocol

TCP	UDP
Breaks the message into smaller segments at the sender's end	Does not break the message into smaller segments
Reassembles the segments at the receiver	No need to reassemble since the message was never broken
Preferable when data to be exchanged is large	Preferable for small data exchanges
Slower as compared to UDP	Faster since it provides limited services
Asks sender to resend erroneous data	Does not ask sender to resend erroneous data
Supports error checking and error correction mechanisms and ensures a reliable data transfer	Does nothing to correct errors and supports unreliable data transfer
Is a connection-oriented protocol	Is a connection-less protocol
Before data exchange, handshaking signals exchanged to establish connection	Data exchange is not preceded by any handshaking signals
Sends acknowledgement for data that has been received	No acknowledgments are sent

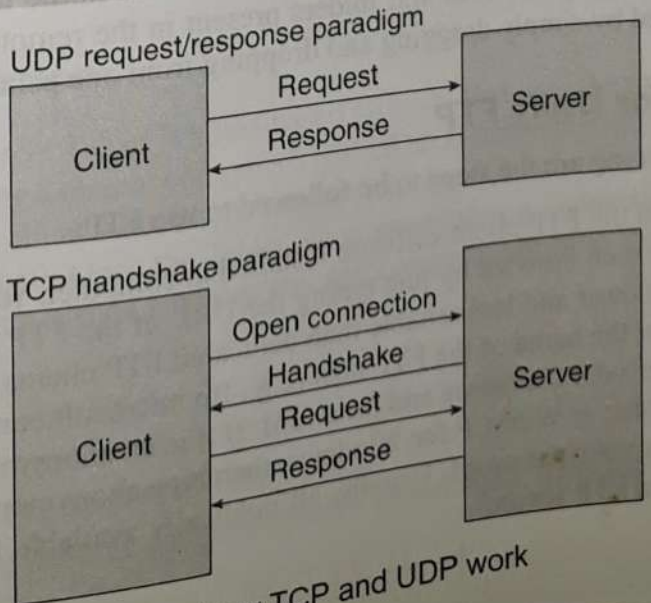


Figure 6.8 How TCP and UDP work

6.7.4 File Transfer Protocol

FTP is the preferred method of exchanging files because it is faster and reliable. It is usually used to perform the following functions:

- Enable users to share files, computer programs, and/or data.
- Enhance the use of remote computers.
- Provide authentication and security to stored files and programs.
- Transfer data reliably and efficiently.

Generally, users use FTP to transfer web page files from their computers to the server so that the pages can be available for everyone on the Internet. Using FTP, users can easily update (delete, rename, move, and copy) files on a server. However, it is also used to download programs and other files to the user's computer from other servers. The FTP program can be invoked either by typing the FTP commands on a simple command line interface (like the MS-DOS Prompt window) or with a commercial program that offers a graphical user interface (GUI). Even the Web browser can make FTP requests to download the selected programs.

In FTP terminology, the following rules are followed:

- The machine on which the file exists is called the server and the machine that requests that file is called the client.
- Copying files from a client to a server is called uploading, whereas transferring files from a server to a client is called downloading.
- The term 'get' refers to receiving files from the server and 'put' refers to sending files (synonymous with download and upload respectively).

How to Use FTP

Nowadays, using the FTP is as simple as using Windows Explorer. FTP is widely being used to upload web pages on the Internet. Users create web page files on their computers and transfer them to the ISP's web server by using FTP.

To enable this, an FTP client software is already installed in the user's computer. This software allows users to log in to a remote computer. The software has two window panes: the one on the left displays all files and directories in the user's computer and the pane on the right displays all files and folders present in the remote computer. Files can be easily transferred by simply dragging and dropping from one pane to another.

Steps for Using FTP

The following are the steps to be followed to use FTP:

- Open the FTP client software installed in computer. You can also use the FTP through your web browser by just typing the URL of the FTP server. However, web browsers are slower and less reliable than dedicated FTP clients.
- Enter the name of the FTP host (e.g., ftp.microsoft.com).
- Enter your username and password. If it is an anonymous FTP server like Cyberduck for Mac or WinSCP for Windows, then type anonymous as username and your email id as your password. Usually, all publically available files are accessed using anonymous FTP server.

Using FTP through Command Line Instructions

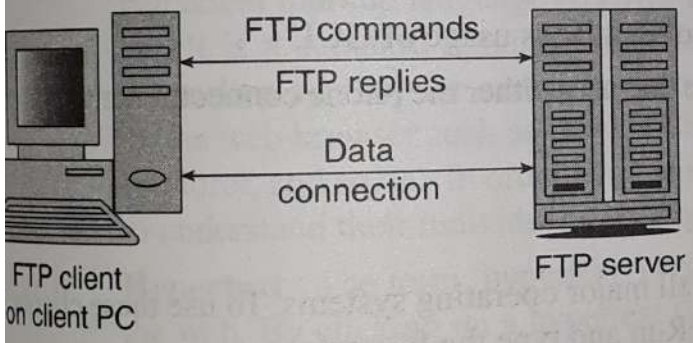
While GUI-enabled FTP clients need to be downloaded from the Internet, users can also use FTP through command line instructions in Windows, Mac OS X, and Linux by typing ftp ftp.microsoft.com. Basic FTP support is provided by all computers.

Provide your username and password. In case of an anonymous FTP site, enter anonymous as username and email address as password.

FTP also allows users to delete, rename, move, and copy files on the server.

Modes of File Transfer

FTP can transfer files in the following three modes.



gure 6.9 Two connections in FTP

Stream mode It is that mode in which it transfers files as a continuous stream with no intervention or processing of information into different formats.

Block mode In this mode, the data to be transferred is divided into blocks.

Compressed mode In this mode, FTP compresses the files by encoding them.

In Figure 6.9, FTP uses two connections for data exchange—one for sending commands and the other for sending or receiving data.

Active and passive connection mode FTP supports two modes of connection—active and passive.

In active mode, the client initiates the connection. Once the server gets connected with the client, the data can be exchanged.

In passive mode, the server is always waiting for any request from the client. Most FTP clients use passive connection mode by default.

6.7.5 Terminal Emulation

Terminal emulation or Telnet is a text-based protocol that uses the underlying TCP/IP technology for accessing a remote computer's (called host) data and application programs. Users can use the Telnet client software to connect with the Telnet server (or the remote host) as shown in Figure 6.10. Once the Telnet client establishes a connection to the remote host, the client becomes a virtual terminal and can communicate with the remote host from his computer.

Features

The following are the features of Telnet.

Bidirectional It is used to send and receive information. This means that data travels in both directions.

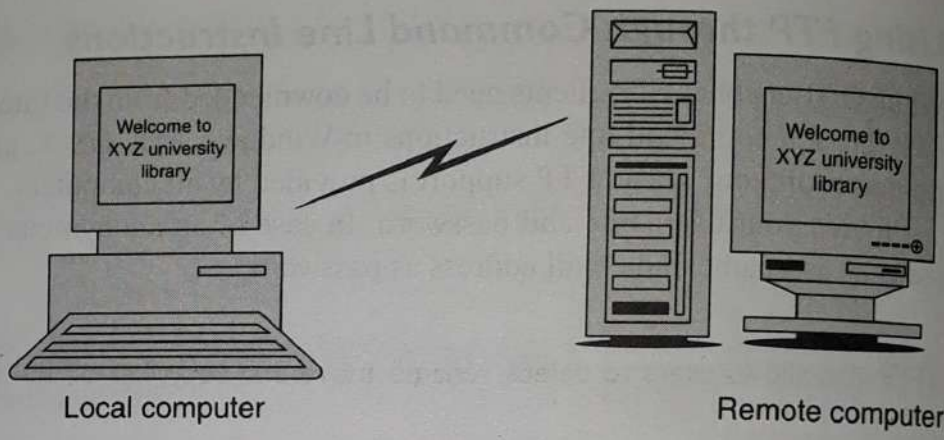


Figure 6.10 Telnet connection

Interactive It accepts a command from the user, executes it on the remote computer, and displays the result on the user's screen.

Text-oriented It is a text-based protocol that lacks usage of GUI.

Versatile It can be used with any device that uses either the phone connection or the Internet connection.

How to Use Telnet

Telnet client programs are available for all major operating systems. To use these clients, go to command prompt by clicking Start->Run and type the following:

```
telnet the.libraryat.whatis.edu
```

where Telnet is the name of the protocol and the.libraryat.whatis.edu is the name of the host. You can also specify the IP address of the host instead of its name. The syntax of using the Telnet command is as follows:

`telnet host port` (where `port` is optional)

Next, enter your username and password to log in to the remote computer.

Once the connection is established, users can enter commands which will be executed by the remote computer.

Uses

Telnet is used in the following areas:

- It is used to access specific applications or data located at a remote computer.
- It allows users to log in as users of the remote host.
- Even a dumb terminal can use the applications hosted on the world's most powerful computer.
- It enables users to control the server and communicate with it over the network.
- It enables research scholars and professors to log in to the university's computer from any terminal.
- It allows users to connect them to databases, library catalogues, and other information resources around the world.

Telnet has now evolved as secure shell (SSH) and is used by network administrators to manage Unix and Linux computers from a remote computer.

Shortcomings

The drawbacks of Telnet are as follows:

- It is a text-based computer protocol and lacks a fancy screen with images, animation, and hyperlinks.
- It is insecure because it transfers all data in clear text.
- Users cannot transfer files using Telnet.