
CHAPTER 26

Remote Log-in, Electronic Mail and File Transfer

Solutions to Odd-Numbered Review Questions and Exercises

Review Questions

1. In *local log-in*, the user terminal is directly connected to the target computer; in *remote log-in*, the user computer is connected to the target computer through the Internet.
3. Options in TELNET are negotiated using four control characters **WILL**, **WONT**, **DO**, and **DONT**.
5. A *user agent (UA)* is a software package that composes, reads, replies to, and forwards messages.
7. SMTP is a *push* protocol; it pushes the message from the client to the server. In other words, the direction of the bulk data (messages) is from the client to the server. On the other hand, retrieving messages from mail boxes needs a *pull* protocol; the client must pull messages from the server. The direction of the bulk data is from the server to the client. The third stage uses a message access agent (MAA) such as POP3 or IMAP4.
9. One connection is for *data transfer*, the other connection is for *control information*.
11. The three transmission modes in FTP are *stream*, *block*, and *compressed*.
13. *Anonymous FTP* allows a user to access files without an account or password on a remote server.

Exercises

15. There are **15** characters in the command (including the end of line). Each character is sent separately to the server and each is echoed and acknowledged by the server. Each echo from the server is then acknowledged by the client. A total of **45** packets must be sent.
17. Three transmissions, each with a minimum size of 72 bytes, mean a total of **216 bytes** or **1728 bits**.

19.
 - a. **IAC WILL ECHO**
 - b. **IAC DONT ECHO**
 - c. **IAC IP** (Interrupt Process)
 - d. **IAC GA** (Go Ahead)
21.

MIME-version: 1.1
Content-Type: Image/JPEG; name="something.jpg"
Content-Transfer-Encoding: base64
23. There should be limitations on *anonymous FTP* because it is unwise to grant the public complete access to a system. If the commands that an anonymous user could use were not limited, that user could do great damage to the file system (e.g., erase it completely).