La Trobe University, Bendigo
School of Management, Technology and Environment

BITCNE: Computer Networks

Final Examination, Semester 1, 2000

Reading Time: . . . 15 mins
Writing Time: . . . . 3 hours

Number of Pages: . . 7 (including this page)
Number of Questions: 6

Instructions to Candidates:

- All questions should be attempted.
- All questions ***do not have*** equal marks. Please note this important change from previous examinations in this subject.
- Marks for this paper total 120.
- Sixty percent (60%) of the final assessment for this subject will be based on this examination paper.
- No reference material may be used.
- Non–programmable calculators may be used.
- Any assumptions made in answering questions should be stated.

Examiner: Philip Scott, Ext 7277

Question 1 – Application Protocols

(a) Many Internet application protocols are based on the exchange of "lines of text" complying with the ***Telnet NVT*** specification. What characteristics do these "lines of text" have?

(b) Internet application protocols commonly use a 3-digit numeric code in responses sent from the server process to the client. What, in general terms, would you expect a "200-series" code (ie, one whose first digit is "2") to indicate?

(c) Give the general format of an ***RFC822 electronic mail message***.

(d) The Internet ***MIME*** (Multipart Internet Mail Extensions) standard for email attachments uses (among others) the "**`Content-Type:`** " email header. Give two values (or "MIME types") which are valid for this header.

(e) What is the ***Post Office Protocol*** (POP) used for?

(f) In order to enhance your understanding of the ***HTTP/1.0*** protocol, you decide to use a command-line version of the **telnet** program to fetch a HTML (or "Web") page from the La Trobe University, Bendigo main Web server. In order to do this, you type the following commands[1]:

```
% telnet www.bendigo.latrobe.edu.au 80
GET /index.html HTTP/1.0
```

(i) What is the purpose of the "**`80`**" on the command line, and what would happen if it wasn't there?

(ii) What would you normally expect to see on your screen after you entered the commands given above? Explain in some detail. Be sure to distinguish between protocol information and application data.

[1] Note that the first line is shown as if it were typed at a Unix shell—the "**`%`**" character is a common Unix shell prompt. However, there is nothing in this question which is specific to Unix; it would be much the same in any other command-line version of **`telnet`**. Also, http://www.bendigo.latrobe.edu.au/index.html is, in fact, a valid URL.

(iii) Suppose the word "GET" was replaced with the word "HEAD" in the commands given above. What difference would you expect to observe in the information you receive back from the server?

(iv) Suppose you now want to modify the above GET request given above to return the page only if it has been modified since a specified date. How is this done?

(v) Describe at least one aspect of the ***HTTP/1.1*** protocol which is clearly superior to the older HTTP/1.0 specification.

(3 + 3 + 3 + 2 + 3 + (2 + 4 + 3 + 4 + 3) = 30 Marks)

Question 2 – Network and Transport Protocols

(a) Datagram (IP packet) delivery in the Internet is ***unreliable***. What are the three things that can happen to datagrams during their travel across the Internet which are characteristic of this unreliability?

(b) Given that datagram delivery in the Internet is unreliable, how can application software processes communicate in a reliable way using the Internet? Describe briefly some of the characteristics of the standard Internet protocol which is used to provide ***reliable interprocess communications*** over the IP-based Internet.

(c) The **`traceroute`** command is very useful for revealing the structure of the Internet in a region. The following is the (slightly edited to suit the question) output of an execution of **`traceroute`** on the *ironbark* Unix system at Bendigo:

```
ironbark> traceroute www.latrobe.edu.au
traceroute to www.latrobe.edu.au (131.172.4.23), 30 hops max, 40 byte
packets
 1  149.144.21.252 (149.144.21.252)  1 ms
 2  149.144.8.253 (149.144.8.253)  2 ms
 3  r-bgoatm72-fe.bendigo.latrobe.edu.au (149.144.2.250)  1 ms
 4 .r-rsm-pw.latrobe.edu.au (131.172.239.12)  3 ms
 5  www.latrobe.edu.au (131.172.4.23)  3 ms
```

(i) Use this information to draw a clearly-labelled diagram of the various network components which connect *ironbark* to the La Trobe Web server, *www.latrobe.edu.au*. Use only the information contained here—you are not expected to know any more about how the La Trobe University network is structured than is revealed by this run of **`traceroute`**.

(ii) The **`traceroute`** software obviously uses both ***domain names*** and ***IP addresses*** to refer to network components. How is a domain name such as *www.latrobe.edu.au* converted to an IP address in the Internet?

(5 + 5 + (5 + 3) = 18 Marks)

Question 3 – Network Technologies

(a) Domestic Internet users normally connect to an ***Internet Service Provider*** (ISP) using a ***modem***, giving a point-to-point data link.

(i) Why is a modem usually needed for domestic Internet access?

(ii) Long distance router-to-router interconnections in the Internet are usually carried on point-to-point data links and can even involve the use of modems, just as in a domestic dial-in situation. What is the fundamental difference in the way ***IP addresses*** are usually allocated in this kind of point-to-point link, compared to a domestic dial-in?

(b) ***Ethernet/802.3*** is the most common multi-access network (or LAN) technology in current use.

(i) Briefly describe the operation of the ***CSMA/CD*** MAC sublayer protocol which is used in Ethernet/802.3 LANs.

(ii) What is an Ethernet/802.3 ***hub***? It may be useful to illustrate your answer with a simple sketch/diagram.

(iii) An Ethernet/802.3 ***switching hub*** is considerably more expensive than an "ordinary" (ie, non-switching) hub. What extra performance features does the switching hub have?

(c) In the early days of the Internet in Australia, long distance router-to-router links between the universities and various other Internet-connected organisations operated over leased-line point-to-point datalink services. Nowadays these links are, in the main, carried by "backbone" ISPs such as C&W Optus. Technically speaking, what distinguishes the current arrangements from those originally used?

((3 + 3) + (3 + 3 + 3) + 3 = 18 Marks)

Question 4 – Network Management

(a) The Internet Protocol IP has a built-in network management facility based on the transfer of ICMP ECHO_REQUEST and ECHO_RESPONSE messages, or packets.

.

(i) What is usual name for the command-line software utility which provides user-level access to this network management functionality?

(ii) What information can the network manager obtain using these ICMP message types? Give three examples.

(b) The ***ASN.1*** specification language is an integral part of the OSI Reference Model upper layer architecture, and is used in some protocols in the Internet. ASN.1 data objects are (normally) encoded for transmission using the ***Basic Encoding Rules*** (BER). What is the general format of an ASN.1 data structure which has been encoded for transmission using the BER?

(c) This section refers to the ***Simple Network Management Protocol*** (SNMP)

(i) The Structure of Managed Information in SNMP is defined in the (so-called) ***Management Information Base***, or MIB, the most common version of which is called MIB-2. An example of a MIB-2 variable is:

```
sys.sysDescr ::= {1 3 6 1 2 1 1 1}
```

What "real world" quantity does this particular data item represent?

(ii) The SNMP ***get-request*** takes as its argument one or more SNMP "instance values". What is the difference between a MIB variable, such as the one given in part (i), and an "instance value"?

(iii) What would be returned in response to an SNMP ***get-next-request*** for the instance value mentioned in part (ii)?

((3 + 3) + 3 + (3 + 3 + 3) = 18 Marks)

Question 5 – Security

(a) A certain company intends to connect its "internal" LAN (or Intranet) to the Internet. They intend running a Web server, as well as email and maybe some other network services. They have asked you, as a Computer Security Consultant, for information on various security issues in relation to this.

(i) There are a variety of ***security attacks*** which could potentially be directed at the company's Internet-connected hosts. Describe two typical attacks which they might expect to encounter.

(ii) Many companies implement one or more ***firewalls*** between their "internal" network (ie, their Intranet), and the external Internet. Describe, using a diagram, a typical firewall-based Internet interface, and describe briefly the purpose and likely configuration of each of the components.

(b) Briefly outline the advantages and disadvantges of ***single-key cryptosystems*** (such as DES, IDEA, etc) compared to a ***public-key cryptosystem*** such as RSA. Give at least one advantage and one disadvantage of each.

(c) In a public key cryptosystem based on RSA technology, explain briefly what aspect of the system makes it difficult to discover someone else's private key K_S even though you know their public key K_P.

((4 + 6) + 4 + 4) = 18 Marks)

Question 6 – Electronic Commerce

(a) In the lectures for this subject we looked at electronic commerce from two perspectives: the pre-Internet era, and the Internet era. What are the key technologies for each of these periods?

(b) The ***FORM*** markup in HTML is the basic enabling technology for Electronic Commerce on the World Wide Web. The following HTML markup is an example of typical usage of a FORM in a Web page:

```
<FORM
ACTION="http://ironbark.bendigo.latrobe.edu.au/htbin/myprog.cgi
        METHOD="GET">
<INPUT TYPE="TEXT" NAME="Name" MAXLENGTH="64" SIZE="20">
<INPUT TYPE="SUBMIT" VALUE="Submit">
</FORM>
```

(i) Draw a diagram illustrating how this HTML markup would normally be displayed on a typical Web browser such as Netscape or Internet Explorer.

(ii) Note that this FORM specifies the ***GET*** method. Describe briefly how the data in the FORM is submitted to a Web server.

(c) A particular "Web store" sells goods using a typical ***shopping cart*** application. During the "shopping" phase the list of items currently in the customer's "cart" is stored in a ***hidden field***. What is a hidden field, and how does it store the information?

(d) A ***site certificate*** is considered a desirable (if not essential) tool for conducting Electronic Commerce on the Web.

(i) What is the basic purpose of a site certificate?

(ii) What are the two vital pieces of information which are contained (along with lots of other stuff) in a site certificate, and how is the site certificate encoded to ensure that its contents are trusted by the user's Web browser?

(2 + (2 + 3) + 4 + 2 + 5) = 18 Marks)