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

INT20/30CN: Computer Networks

Final Examination, Semester 1, 2001

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
- 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 ASCII text***". What is the particular advantage of this approach to application protocol design?

(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 "400-series" code (ie, one whose first digit is "4") to indicate?

(c) In recent years, the original ***RFC822*** electronic mail message format has been extended by the ***MIME*** (Multipart Internet Mail Extensions) standard for email attachments. Describe briefly how MIME is used to extend the RFC822 format, whilst still maintaining compatability with older RFC822 email software. Use, if you wish, an example such as an image file (eg GIF) sent as a MIME attachment to an email message. Exact detail is not required here, just the general ideas.

(d) 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) Before the **telnet** software mentioned here can establish a connection to `www.bendigo.latrobe.edu.au`, it must first "look up" its network address. Briefly, what does this mean, and what does it entail?

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

(iii) 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

[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.

between protocol information and application data.

(iv) 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?

(v) 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 achieved?

(vi) Suppose the Web site mentioned at the start of this question part was not directly accessible from your location, and had to be accessed using a ***proxy server***. Explain how you might obtain the Web page by telnetting instead to the proxy server. Most importantly, how would the GET request differ in this situation?

(3 + 3 + 6 + (3 + 2 + 4 + 3 + 3 + 3) = 30 Marks)

Question 2 – Network and Transport Protocols

(a) The ***IP (Internet Protocol) Address*** of machine *ironbark* (the Department of IT's main server at Bendigo) is, using the modern notation, **`149.144.21.60/24`**. What are the ***network***, ***subnet*** and ***host*** parts of *ironbark*'s IP address?

(b) Datagram (IP packet) delivery in the Internet is characterised as ***unreliable***, ***connectionless*** and ***best-effort***. Describe very briefly what each of these terms means.

(c) Datagram delivery is unreliable, yet the Internet is commonly used for ***reliable interprocess communications***. How is this reliability achieved? Explain briefly.

(d) The **`traceroute`** software utility is useful for revealing details of the structure of regions of the Internet. The following is the (slightly edited to suit the question) output of an execution of **`traceroute`** on the *ironbark* Unix system at Bendigo:

```
ironbark 33> traceroute www.latrobe.edu.au
traceroute to www.latrobe.edu.au (131.172.4.23)
 1  149.144.21.252 (149.144.21.252)  1 ms
 2  r-bgoatm72-fe.bendigo.latrobe.edu.au (149.144.2.250)  1 ms
 3  r-rsm-pw.latrobe.edu.au (131.172.239.12)  3 ms
 4  www.latrobe.edu.au (131.172.4.23)  3 ms
```

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`**.

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

<u>Question 3 – Network Technologies</u>

(a) Domestic Internet users normally connect to an ***Internet Service Provider*** (ISP) using a ***modem***, giving a point-to-point data link. Why is a modem usually needed for domestic Internet access?

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

(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) What is meant by the term ***peering*** in the context of Internet Network Providers?

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

Question 4 – Network Management

(a) It is possible to perform many network managment (monitoring) functions using only the `ping` command, particularly in a "local" environment where the structure of the network is already well known. How could you use `ping` to achieve the following:

(i) check that specific hosts are "up" and reachable,

(ii) check for congestion (and impending congestion) in specific areas of the network, and

(iii) if the path to a specified host (or section of the network) is "down", discover where the actual fault lies.

(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? Give, as an example, the bytes which would be used for sending a small-valued INTEGER(2).

(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-2***, or MIB-2. An example of a MIB-2 variable is:

```
ip.ipForwDatagrams ::= {1 3 6 1 2 1 4 6}
```

What “real world” quantity does this particular MIB-2 variable 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”?

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

Question 5 – Security

(a) Describe briefly, in general terms, three (3) different ***security attacks*** which may be directed against an Internet-connected computer system.

(b) Many companies implement one or more ***firewalls*** between their "internal" network (commonly termed 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.

(c) 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.

(d) 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 Applications

(a) The ***FORM*** markup in HTML is the basic enabling technology for CGI-based Electronic Commerce on the World Wide Web. A FORM can be specified to send data to the server using either the ***GET*** or ***POST*** submission methods. Explain briefly how the data is sent across the network in each of these.

(b) ***State Maintenance*** (or, to use the currently fashionable terminology, ***Session Management***) in Web-based shopping cart systems was, until recently[2], achieved using either or both of ***hidden fields*** and ***cookies***.

(i) Explain briefly how each of these two technologies is normally used to provide state maintenance (or session management) in the context of a shopping cart system.

(ii) What are the relative advantages and disadvantages of hidden fields and cookies in session management? Give at least one advantage and disadvantage of each.

(c) A ***Site Certificate*** is a necessary component in the ***Secure Sockets Layer (SSL)*** technology used to facilitate encrypted communications in the World Wide Web. Explain briefly how a Web browser firstly establishes that a site certificate is trusted, and secondly how it uses the information contained in the certificate to set up a secure (encrypted) communications channel. Full and exact detail is not required here, just the general principles.

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

[2] For the purposes of this examination. we shall ignore the newer technique of using URL ***Extra Path Information*** to achieve the same purpose.