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

BITCNE: Computer Networks

Final Examination, Semester 1, 1999

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 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*** such as SMTP (for email delivery) and HTTP (the protocol of the WWW) share some common characteristics. Give ***two*** such common characteristics.

(b) Give the general format of an RFC822 ***electronic mail message***, and explain *very briefly* how this format is modified to handle ***MIME*** (Multipart Internet Mail Extensions) attachments, or enclosures. Detailed description of all aspects of the MIME specification is not required here, just an outline of the basic ideas.

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

```
% telnet www.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.

(iii) One interesting aspect of the HTTP/1.0 protocol is that, after the second line given above was entered at the command line, you have to hit the *ENTER* (or *RETURN*) key twice before anything happens. Why?

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

(4 + 4 + (3 + 3 + 3 +3) = 20 Marks)

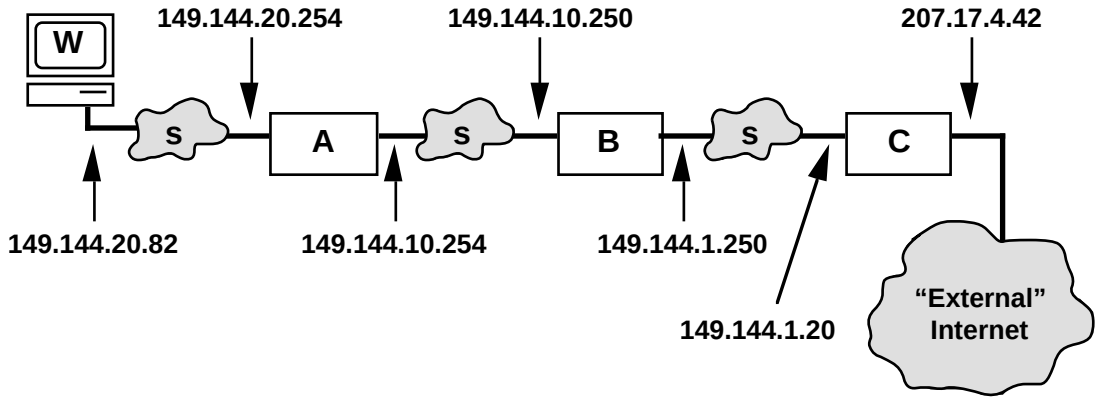
[1] Note that the first line is shown as if it were typed at a Unix shell—the "**%**" character is a common Unix shell prompt. However, there is nothing in this question which is specific to Unix; it would be much the same in any other command-line version of **telnet**.

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? Give the name of the standard Internet protocol which is used to provide ***reliable interprocess communications*** over the IP-based Internet, and briefly describe some of its characteristics.

(c) Here is a diagram of a (hypothetical) small region of the Internet, showing various important components. Each network interface is labelled with its IP address.



(i) What is the generic name for the network components labelled "**A**", "**B**" and "**C**" in this diagram?

(ii) What do the items labelled "**S**" represent?

(iii) A user seated at workstation **W** executes the `traceroute` command, with a destination address located somewhere in the "external" Internet. Give the list of IP addresses which will be revealed by execution of `traceroute`.

(iv) If we desired to refer to these network components using ***names***, instead of IP addresses, what network service would need to be available?

(3 + 4 + (3 + 3 + 3 + 3) = 20 Marks)

Question 3 – Network Technologies

(a) The interface between a computer and a modem usually employs ***asynchronous*** signalling. What does the word "asynchronous" mean in this context? Explain in detail.

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

(c) The ***ISDN*** system is entirely digital, so analogue-to-digital conversions (as in modems) are not necessary. However, if you wish to use an ISDN service to transfer data from one computer to another you normally must buy an extra piece of hardware. What is this extra component?

(d) Explain how a ***frame relay*** service operating at a port speed of 64 kbps differs from an ISDN semi permanent link at the same speed. In particular, why would you expect the frame relay service to be cheaper?

(e) In the early days of the Internet, the major telecommunications providers (such as Telstra and C&W Optus in Australia) sold basic, leased-line point-to-point datalink services. Nowadays, these companies prefer to offer Internet service directly—that is, to operate as an Internet Service Provider (ISP). What distinguishes this from the older service types?

(4 + 4 + 2 + 4 + 6) = 20 Marks)

Question 4 – Network Management

(a) The simplest (and arguably one of the most useful) network management software tool is the ***ping*** command.

(i) What does **`ping`** actually do? In other words, explain very briefly how **`ping`** works.

(ii) What information can the network manager obtain from the **`ping`** command? Give two 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)

(i) What is the general format of an ASN.1 data structure which has been encoded for transmission using the BER?

(ii) Give an example showing a small integer value encoded using BER. NB: the UNIVERSAL tag value for an integer is 02.

(c) Explain the difference between the ***SNMP*** (Simple Network Management Protocol) request types ***`get`*** and ***`get-next`***, and (using a suitable command syntax which includes the *community name* for the data) show how each of them could be used to fetch the actual value of the MIB–2 variable:

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

(d) Much of the management information in the ***SNMP MIB*** is tabular in nature—that is, it is conveniently represented using tables. Explain briefly how the tree-structure of the MIB is used to represent this tabular information. Use as an example (if you wish) the MIB variable giving the speed in bps of the first hardware interface: **`interfaces.ifTable.ifEntry.ifSpeed.1`**

((3 + 3) + (3 + 3) + 4 + 4) = 20 Marks)

Question 5 – Security

(a) A certain company intends to connect its "internal" LAN (or network) 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 Networking 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) Explain very briefly the difference between the Electronic Code Book mode and the Chain Block Cypher mode of the ***Data Encryption Standard*** (DES), and explain why CBC mode is normally used in practice.

(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.

(d) Explain briefly how a public key cryptosystem such as RSA can be used to implement ***digital signatures***, and give at least one reason why digital signatures are used.

((2 + 6) + 4 + 4 + 4) = 20 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 following URL is typical of those observed when performing queries to the *AltaVista* search engine:

http://altavista.digital.com/cgi-bin/query?q=%22phil+scott%22+bendigo&search=Search

(i) Does this URL suggest that the FORM METHOD used to generate it was specified as GET or POST? Give the reason for your answer.
(ii) What is the name of the CGI program which is executed by the Web server?
(iii) How does the CGI program access the data which is submitted when this URL is accessed?

(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) Your lecturer has been known, on a few occasions, to purchase books from an online (Web) bookstore. Now whenever he returns to the particular bookstore's homepage, he notices a little customised welcome message, saying something like "**Welcome back, Philip Scott**", on the page. How is this implemented?

(e) What is a ***site certificate***, and why is it considered a desirable (if not essential) tool for conducting Electronic Commerce on the Web?

(2 + (2 + 2 + 2) + 4 + 4 + 4) = 20 Marks)