La Trobe University, Bendigo
School of Business and Technology

INT21/31CN: Computer Networks

Final Examination, Semester 1, 2002

Reading Time:	**15 mins**
Writing Time:	**3 hours**
Number of Pages:	**8 (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 are based on the exchange of "lines of text" complying with the ***Telnet NVT*** specification. What are the distinguishing characteristics of these "lines of text"?

(b) What does the following line of ***Java source code*** achieve when compiled and executed? Explain briefly.

```
Socket myclientsocket = new Socket("ironbark", 79);
```

(c) In recent years, the original ***RFC822*** electronic mail message format has been extended by the ***MIME*** (Multipart Internet Mail Extensions) standard. The following is a minimal MIME message, edited for space reasons—some non-essential lines have been removed, and the message is truncated.

```
Date: Mon, 3 Jun 2002 22:52:43 +1000
From: Phil Scott <P.Scott@latrobe.edu.au>
Subject: This is a test
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="sdtB3X0nJg68CQEu"

--sdtB3X0nJg68CQEu
Content-Type: text/plain; charset=us-ascii

Test message

--sdtB3X0nJg68CQEu
Content-Type: image/gif
Content-Transfer-Encoding: base64

R0lGODdhgAEgAcYAAAAADNmAAAzZjOZZmYzmZmZmQBmzDPMzGZm/5nM/zMAADMzZmaZZsyZ
mTNmzGbMzMzM/wAzMzOZM2YzZpmZZgBmmWZmzJnMzP/M/zMzM8yZZgAAmTNmmWbMmZlmzMzM
zDOZ/2b.....
          [etc]
```

Comment briefly on the general format of this message, and explain the purpose of each of the three "**`Content-Type:`**" headers, and the "**`Content-Transfer-Encoding:`**" header.

Question 1 continues on the next page

(d) The ***Domain Name System (DNS)*** is a crucial component of all Internet applications.

(i) An enquiry to a ***DNS nameserver*** commonly returns a ***Type A Resource Record*** (informally: an "A-Record"). What important information does this contain?

(ii) What is the essential difference between a ***recursive*** and an ***iterative*** nameserver query?

(4 + 4 + 8 + (2 + 2) = 20 Marks)

Question 2 – HTTP

(a) A ***Web browser*** (eg Netscape or Internet Explorer) sends the following request to a Web server:

```
GET  /index.html  HTTP/1.0<newline><newline>
```

(i) Assuming the file "**`/index.html`**" exists (and is readable) on the server, describe what is returned to the browser as a result of this request. Be sure to distinguish between protocol information and application data.

(ii) Suppose that at some later time, the Web browser needs to once again display the same document (**`/index.html`**) from the same server. The browser has cached the document, but doesn't know if the cached copy is up-to-date. It's possible for the browser to structure a new "**`GET`**" request in such a way that the server will not return the contents of the file if the cached copy is unchanged from the copy on the server. How is the "**`GET`**" request restructured to achieve this?

(iii) Suppose that the reponse to the original "**`GET`**" request contained the following headers:

```
HTTP/1.1  401  Authorization  Required
Date:  Mon,  03  May  2002  01:17:56  GMT
WWW-Authenticate:  Basic  realm="ByPassword"
```

How would the Web browser proceed to fetch the page? Description of the general technique is needed here, not full technical detail.

(b) What is a ***cookie*** in the context of HTTP and what is it used for?

(c) A Web browser can collect data from the end user (ie, a human) using an ***HTML FORM***. If the FORM ***submission method*** is specified as "GET", how (in the context of HTTP) does the browser submit the FORM data to the server?

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

Question 3 – Network and Transport Protocols

(a) The ***IP (Internet Protocol) Address*** of machine *redgum* (the Department of IT's student server at Bendigo) is, using the modern notation, **`149.144.21.3/24`**. What are the ***network***, ***subnet*** and ***host*** parts of *redgum*'s IP address?

(b) Datagram (IP packet) delivery in the Internet is characteristed 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 4> traceroute www.latrobe.edu.au
traceroute to www.latrobe.edu.au (131.172.4.24)
 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  pw-121-r6509.latrobe.edu.au (131.172.239.2)  3 ms
 4  www.latrobe.edu.au (131.172.4.24)  2 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`**. Be sure to indicate *what* the various components are, and how they're connected.

(4 + 5 + 5 + 6 = 20 Marks)

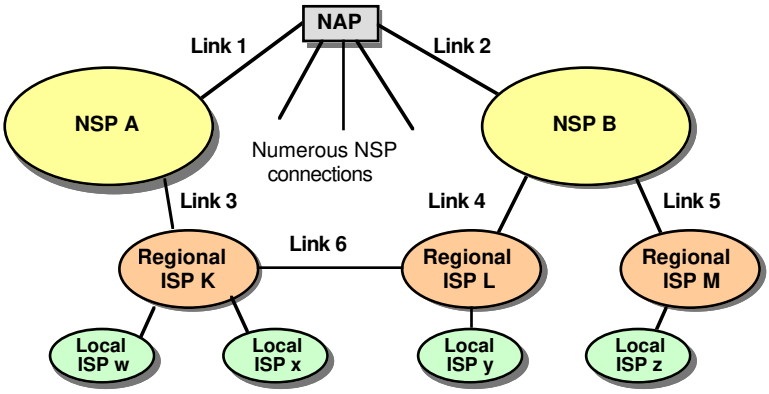
Question 4 – Network Technologies

(a) ***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) 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?

(b) Consider the following diagram. The entities shown have their normal meaning.



(i) What, in general terms, distinguishes a ***peering relationship*** from a ***client-provider relationship*** in this structure? Describe briefly.

(ii) Which of the numbered links in this diagram is a peering relationship, and which are client-provider relationships?

(iii) Give, as a list of numbered links from the diagram, a route which you would ***not*** normally expect packets to flow over.

((4 + 4) + (4 + 4 + 4) = 20 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) 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) 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.

(6 + 5 + 3 + 6 = 20 Marks)

Question 6 – 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. Describe briefly ***three*** useful network management functions which could be implemented using **`ping`**.

(b) 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? That is, if you requested the value of this variable from a router, what would you know about its operation?

(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"? Give the instance value corresponding to this variable.

(iii) The MIB-2 variable "**`ip.ipForwDatagrams`**" is of SNMP-type **`Counter`**, for which the TAG is 41_{hex}. How is this variable encoded for transmission in the SNMP protocol? Illustrate your answer with an example—invent a suitable value for the variable.

(iv) Assume you are designing a network management system. You want your system to plot a graph of the value of "**`ip.ipForwDatagrams`**" against time. How is this achieved?

(6 + 4 + 3 + 4 + 3 = 20 Marks)