La Trobe University, Bendigo
School of Business and Technology

INT21/31CN: Computer Networks

Final Examination, Semester 1, 2003

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) This part concerns the general design principles which characterise typical Internet ***application protocols*** such as HTTP, SMTP, FTP, POP and various others.

(i) Describe, in general terms, the format of ***protocol messages*** (requests and responses) in Internet application protocols such as those mentioned. You do not have to give examples here—simply state how, in general terms, protocol messages are structured.

(ii) What is the particular advantage of the approach described in part (i) in relation to ***testing*** and ***debugging*** these protocols.

(b) Describe, using an example, the structure of an email message of MIME type `multipart/mixed` which contains two parts: a plain text part and an image part. Full and exact detail is not required, however you should ensure that you mention *where* the various "`Content-Type:`" headers, the "`Content-Transfer-Encoding:`" header(s) and any other important headers will be found in the message. Give typical values for the headers where appropriate.

(c) The Domain Name System (DNS) is a crucial part of all Internet applications.

(i) The most common enquiry, or query, to a ***DNS nameserver*** 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*** sends the following minimal 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) A "Real World" HTTP request (such as would be generated by IE or Netscape) usually contains lots of information about the browser, such as its name, version and the range of data types which it can accept. How is the "**`GET`**" request given above modified to send this information to the server? Give examples.

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

```
HTTP/1.1  401  Authorization  Required
Date:  Fri,  16  May  2003  02:54:05  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? Give an example, showing how a basic cookie (ie, one with no added attributes) is sent from an HTTP client to a server, or vice-versa.

(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 "***POST***", how (in the context of HTTP) does the browser submit the FORM data to the server? It may be convenient to use an example to illustrate your answer.

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

Question 3 – Network and Transport Protocols

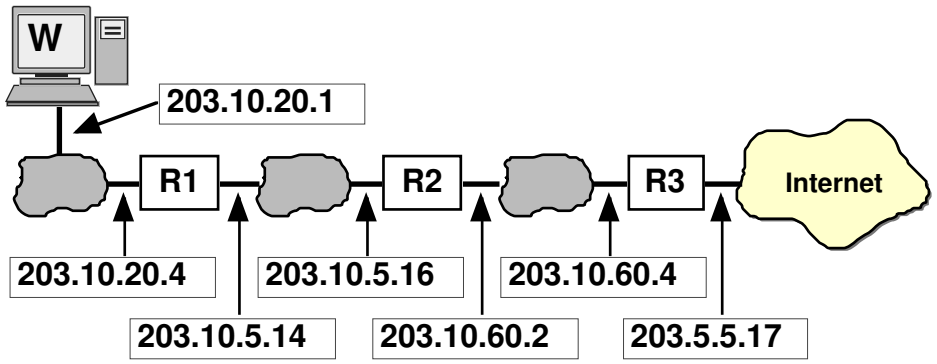
(a) Two computers have, respectively, the following ***IP (Internet Protocol) Addresses*****:** `149.144.21.3/24` and `149.144.21.60/24`[1]. One of these computers wishes to send an IP packet to the other. How many routers would you expect the packet to cross, and why?

(b) Datagram (IP packet) delivery in the Internet is ***unreliable***. What are the basic characterstics of this unreliability?

(c) The ***TCP*** protocol is, in general, only implemented in ***edge systems***. What is meant by the term "edge system" in the Internet?

(d) Explain briefly how TCP transforms the unreliable delivery service provided by IP into a reliable communications service. Full and exact detail is not required here, just the general principles.

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



A user seated at the computer labelled **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`.

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

[1] These addresses are expressed in the modern CIDR-like notation. Alternatively we could say that their IP addresses are respectively `149.144.21.3` and `149.144.21.60`, both with netmask `255.255.255.0`.

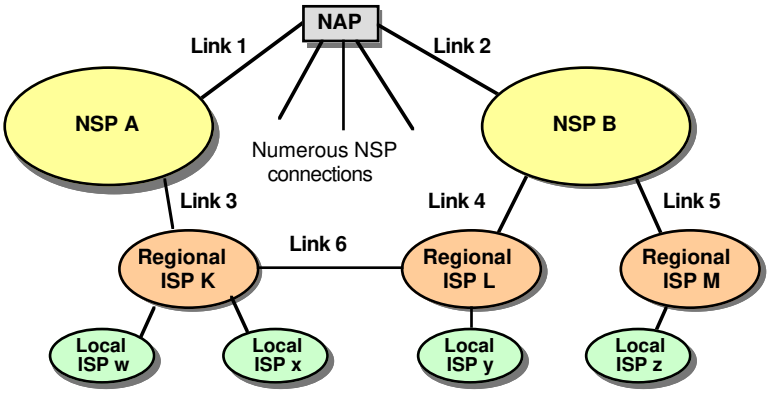
Question 4 – Network Technologies

(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? Give an answer for each of the 5 labelled links in the diagram.

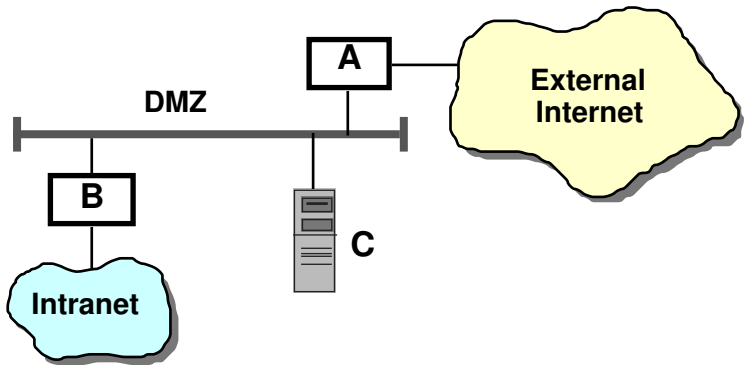
(iii) Give, as a list of numbered links from the diagram, a route which you ***would*** expect IP packets to flow in the normal course of events. Then give a route over which, in consequence of commercial arrangements between the owners of the various networks depicted, you would ***not*** expect packets to flow .

((4 + 3) + (4 + 5 + 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. The following diagram indicates a typical structure



Describe briefly the purpose and likely configuration of the components labelled **A**, **B** and **C** in this diagram.

(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.

(3 + 6 + 5 + 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, which is specified using ***ASN.1***. An example of a (very useful) MIB-2 variable is, in ASN.1 syntax:

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

A network manager requests, using SNMP, the value of this variable from a router. What important information does he/she now have 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"?

(iii) The MIB-2 variable "**`ip.ipForwDatagrams`**" is of SNMP-type **`Counter`**, for which the ASN.1 TAG is 41_{hex}. How is this variable encoded for transmission in the SNMP protocol? Illustrate your answer with an example.

(iv) It isn't very useful to request the value of "**`ip.ipForwDatagrams`**" once only. How would you expect the network manager would make use of this variable in the "Real World"?

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