La Trobe University, Bendigo
School of Business and Technology

INT21/31[B]CN: Computer Networks

Final Examination, Semester 1, 2004

Reading Time: 15 mins
Writing Time: 2.5 hours

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

Instructions to Candidates:

- This paper contains six (6) questions. Students should attempt **any five 5 questions.**
- All questions **have equal marks**
- Marks for this paper total 100.
- 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) This concerns the structure of Internet email messages.

(i) Describe the general structure of an ***RFC822*** email message. Full and exact detail is not required here, and it may be easiest to use an example.

(ii) The ***MIME*** standards extend the RFC822 format to permit email attachments. Describe briefly the mechanism used to distinguish the various parts of a ***`multipart/mixed`*** MIME message from one another—in other words, how are the parts separated from one another in the message?

(iii) Give the ***MIME-type*** specifiers for a message part containing ordinary ASCII text, and for a message part containing a JPEG image file.

(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) When an Internet-connected computer is manually configured, the nameserver to be used is always identified by its IP address, not its name. Why?

((4 + 3) + (3 + 3 + 2) + (3 + 2) = 20 Marks)

Question 2 – HTTP

(a) A ***Web browser*** (eg IE, Netscape) sends the following request to a Web server:

```
GET http://www.asdf.com/home.cgi?name=phil HTTP/1.0<newline><newline>
```

(i) In the URL of this request, what are the values of each of the ***domain name***, the ***filepath*** and the ***query string***?

(ii) Assume that this request returns an HTML document to the browser. What other information accompanies the document that is sent, and how is it structured? Full detail is not required here, just the general format with some examples.

(iii) As mentioned in part (i), the URL in this "**GET**" request contains a query string. We assume the request occurred as a result of submission on an HTML FORM—that is, a user clicked a "submit" button on a Web page. Give HTML code for a FORM which could have produced this request. Syntactically perfect HTML is not required here, so long as the basic ideas are apparent.

(iv) The "**GET**" request given above is terminated with ***two*** newlines. Why are two required? Explain briefly.

(v) Suppose that the response to the original "**GET**" request included the following headers:

```
HTTP/1.1 401 Authorization Required
Date: Sun, 16 May 2004 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) Why is Web ***caching*** particularly effective for Web page images? Explain briefly.

((3 + 3 + 3 + 3 + 3) + 3 + 2 = 20 Marks)

Question 3 – Network and Transport Protocols

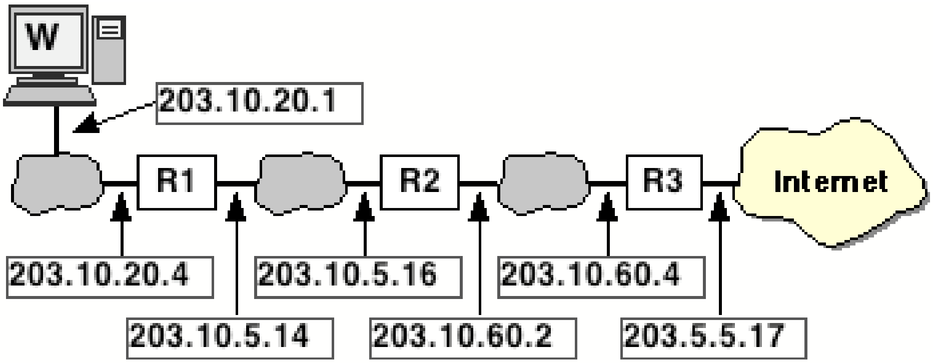
(a) Two computers have, respectively, the following ***IP (Internet Protocol) Addresses*:** `203.10.56.7/24` and `203.10.56.220/24`[1]. One of these computers wishes to send an IP packet to the other. How many routers would you expect the packet to cross, and why?

(b) What is a ***routing table*** and how is it used in Internet datagram delivery? Explain briefly.

(c) Datagram (IP packet) delivery in the Internet is ***unreliable***. What are the three essential characteristics of this unreliability??

(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 located in the Internet executes the command "`traceroute 203.10.20.1`". Give the list of the last few IP addresses which will be revealed by this 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 **203.10.56.7** and **203.10.56.220**, each with netmask **255.255.255.0**.

Question 4 – Network Technologies

(a) Modems are sometimes said to "convert digital data into analog form". This is highly simplistic. Give a somewhat better description of the basic function performed by modern modems.

(b) What is the purpose of the PPP protocol in a data link? Explain briefly.

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

(i) "Traditional[2]" Ethernet/802.3 is a ***shared medium, multi-access*** network technology. What do each of these two terms mean?

(ii) An Ethernet/802.3 ***Switching Hub*** (or switch) uses a table which maps destination MAC addresses to physical interface port numbers. How do they build this table, and how do they make use of it in transferring frames?

(iii) An IP packet is "encapsulated" into an Ethernet frame for delivery within the network. How will this encapsulation differ in the case where the packet is sent to a router for "Internet Delivery", compared to IP "local delivery"?

(d) What, in general terms, distinguishes a ***peering relationship*** from a ***client-provider relationship*** between two or more Internet Service Providers (ISPs) and/or Network Service Providers (NSPs)? Describe briefly.

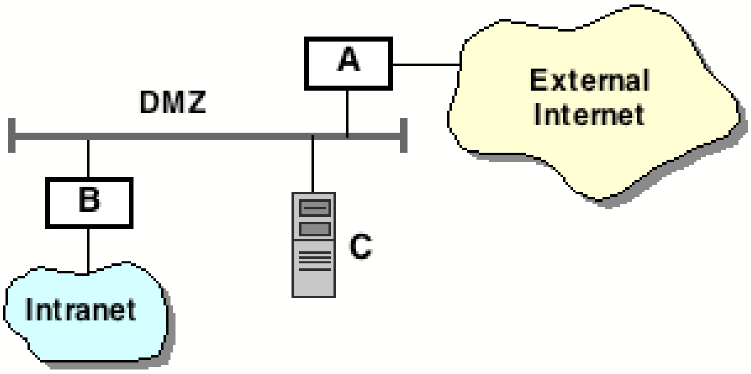
(3 + 3 + (4 + 3 + 4) + 3 = 20 Marks)

[2] In other words, non-switched Ethernet/802.3—until recently the most common technology.

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) The following diagram indicates a typical ***firewall*** structure between a company's "internal" network (commonly termed their ***Intranet***), and the external Internet.



How would you expect the two components labelled **A** and **B** in this diagram to be configured? In other words, what is their purpose?

(c) The following string is ***ciphertext***, encrypted using a very ancient method: **FKQBOKBQ**. Crack the code and give the plaintext message.

(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 $\mathbf{K_S}$ even though you know their public key $\mathbf{K_P}$.

(e) A ***Site Certificate*** is a necessary component in the ***Secure Sockets Layer (SSL)*** technology used to facilitate encrypted communications in the World Wide Web.

(i) How does a Web browser establish that a site certificate is trusted. Explain briefly.

(ii) How does a Web browser use the information contained in the certificate to set up a secure (encrypted) communications channel to the server Again, only a brief (overview) explanation is required.

(3 + 4 +1 + 4 + (4 + 4) = 20 Marks)

Question 6 – Network Management

(a) It is possible to perform many network management (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) The Structure of Managed Information in the ***Simple Network Management Protocol*** (SNMP) is defined in the (so-called) ***Management Information Base-2***, or MIB-2, which is specified using ***ASN.1***.

(i) Some examples of useful MIB-2 variables are, in (simplified) ASN.1 syntax:

```
ip.ipInReceives    ::= { 1 3 6 1 2 1 4 3}
ip.ipForwDatagrams ::= { 1 3 6 1 2 1 4 6}
ip.ipInDiscards    ::= { 1 3 6 1 2 1 4 8}
```

Draw a diagram of the MIB "tree" showing the region where these variables are located.

(ii) The SNMP ***`get-request`*** takes as its argument one or more SNMP "instance values". What is the difference between the name of a MIB-2 variable, such as those given in part (i), and an "instance value"?

(iii) Looking at its name only, what information would you guess that the MIB-2 variable `ip.ipInDiscards` contains?

(iv) 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 a low-valued example.

(v) How, in a practical sense, would you expect network management software packages to make use of the information in these variables in the "Real World"?

(6 + (3 + 3 + 1 + 4 + 3) = 20 Marks)