THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2009
Campus: Tamaki

COMPUTER SCIENCE

Data Communications Fundamentals

(Time allowed: TWO hours)

NOTE:
- Attempt *all* questions. Calculators are NOT permitted.
- This exam has: Section A: MCQ (multiple choice questions) section, and Section B: a short answer section.
- MCQ section: Compare the exam version number on the Teleform sheet supplied with the version number above. If they do not match, ask the exam supervisor for a new sheet.
- MCQ section: Enter your name and student ID on the Teleform sheet. Your name should be entered left aligned. If your name is longer than the number of boxes provided, truncate it.
- MCQ section: Answer all multiple choice questions on the Teleform answer sheet provided.
- MCQ section: Use a dark pencil to mark your answers in the multiple choice answer boxes on the Teleform sheet. Check that the question number on the sheet corresponds to the question number in this question book. If you spoil your sheet, ask the supervisor for a replacement.
- Write *short* answers in the space provided (extra space for answers is available on page 12).
- No marks will be awarded if you merely state a "yes" or "no" answer. To obtain full credit, your script must clearly explain *why* your answer is correct.
- If you require additional information in order to answer a question, you should make a reasonable assumption as required for your answer, and you should explain your assumption on your script.

Surname: . . . . Forenames: . . . .

Student ID: . . . .

Departmental Use Only					
Question	Marks allocated	Marks gained	Question	Marks allocated	Marks gained
Section A: 1	2		Section B: 7	12	
Section A: 2	2		Section B: 8	12	
Section A: 3	2		Section B: 9	14	
Section A: 4	2		Section B: 10	14	
Section A: 5	2		Section B: 11	14	
Section B: 6	12		Section B: 12	12	
Total	22		Total	22+78=100	

Student ID: . . . .

Section A - Multiple Choice Questions
Peer-to-peer

Answer these multiple choice questions on the Teleform answer sheet provided.

1. A Skype network uses the following main entities:
   (a) login server and super nodes.
   (b) super nodes, ordinary nodes and the login server.
   (c) ordinary nodes.
   (d) login server and ordinary nodes.
   (e) super nodes and ordinary nodes.

   [2 marks]

2. Skype operates on
   (a) a traditional server-client model.
   (b) a peer-to-peer model.
   (c) an open source peer-to-peer model.
   (d) a closed-source traditional server-client model.
   (e) an open source traditional server-client model.

   [2 marks]

3. A Super Node may be
   (a) any computer.
   (b) any computer with a public IP and proper hardware configuration.
   (c) any computer behind a fire wall with a public IP.
   (d) any computer with a public IP not running on Linux.
   (e) any computer with a public IP not running on Windows.

   [2 marks]

4. Does Skype operate with a central unit?
   (a) Each Super Node is a central unit in the Skype network.
   (b) The Skype login server is the only central unit in the Skype network.
   (c) There is no central unit in the Skype network.
   (d) Ordinary nodes are central units in the Skype network.
   (e) There are more than one central unit in the Skype network.

   [2 marks]

5. Skype communications
   (a) don't need to be encrypted because they are routed through the public Internet.
   (b) are encrypted only for paid services.
   (c) are encrypted with Advanced Encryption Standard.
   (d) are not encrypted.
   (e) are encrypted only for international communications.

   [2 marks]

Student ID: . . . .

Section B - Short answer questions

6. **Security**   [12 marks]

(a) What is the basic difference between a code such as ASCII and a cryptographic code?
                                                                                                     [2 marks]

(b) In cryptography, what is the difference between symmetric and asymmetric keys? [2 marks]

(c) Consider this statement:
    "Encrypting a message using the sender's private RSA key keeps it private."
    True or false? Explain your answer.   [2 marks]

Student ID: . . . .

(d) Doctor A wants to send a file of secret medical records safely to Doctor B. The method is for
A to encrypt the file and then store it on an Internet server, where B can download it. Both
doctors have private keys and well-known public keys. The server itself has a public key used
as part of a secure login.

Explain the main steps followed by each doctor. Be sure to say which key Doctor A uses
to encrypt the file.   [4 marks]

(e) In the previous case, can a hacker read the medical records? Explain your answer. [2 marks]

Student ID: . . . .

7. **Medium Access Control and Flow Control**   [12 marks]

(a) What is the main difference between *Medium Access Control (MAC)* and *Flow Control*?
[4 marks]

(b) When a program running in a computer connected to Ethernet wants to send data to a program in another computer, does it use MAC or Flow Control first? Explain your answer. [3 marks]

(c) Consider a simple *go-back-N* flow control protocol. What does *N* mean in this case? [3 marks]

(d) If the MAC has to wait when trying to send a frame, will that immediately change the size of the sliding window in the *go-back-N* flow control protocol? Explain your answer. [2 marks]

Student ID: . . . .

8. **Ethernet and 802.11 WiFi**   [12 marks]

(a) Explain in one or two sentences what CSMA means.   [4 marks]

(b) What is a *collision* in the case of Ethernet or 802.11?   [2 marks]

(c) What is the main difference between the way Ethernet and 802.11 deal with collisions?
[4 marks]

(d) If the speed of light is suddenly cut in half, and nothing else changes, how would the length
of the Ethernet collision domain change?   [2 marks]

Student ID: . . . .

9. **Switching and routing** [14 marks]

    (a) Describe three differences between an *Ethernet repeater* and an *Ethernet switch*.   [5 marks]

    (b) Describe three differences between an *Ethernet switch* and an *IP router*.   [5 marks]

Student ID: . . . .

(c) In a routing protocol, what is a *Distance Vector* and what is it used for?   [4 marks]

10. **Booting up of an IP Host**   [14 marks]
When an IP host is booting, it must find out information about itself and the network it is connected
to. It usually does that using the Dynamic Host Configuration Protocol, DHCP, and Address Res-
olution Protocol, ARP.

(a) What four things does a booting IP host need to know?   [3 marks]

(b) Explain briefly how a booting host finds the above information.   [4 marks]

Student ID: . . . .

(c) What's a DHCP relay? Where in an Enterprise network might one be needed?   [2 marks]

(d) How does a host find a hardware address for another host on the same LAN?   [2 marks]

(e) What does it mean if a host gets two different replies to an ARP request? What should a host
do if that happens?   [3 marks]

11. **Transport Control Protocol (TCP)**   [14 marks]
    TCP uses 32-bit unsigned numbers to keep track of the bytes sent and received between the two
    hosts (*initiator* and *listener*) of a TCP connection.

    (a) Explain briefly how the two hosts find out each other's starting sequence numbers. [3 marks]

Student ID: . . . .

(b) How is a TCP host's sequence number updated during the life of a TCP connection? [2 marks]

(c) How does a TCP host know when it may safely remove bytes from its transmit buffer?
[3 marks]

(d) What is the TCP header's checksum field used for? How is that checksum calculated?
[3 marks]

(e) When and how is is the TCP checksum verified? What should a host do if it receives a TCP packet with an incorrect checksum? [3 marks]

Student ID: ....

12. **Network Sockets**   [12 marks]

    (a) What is meant by the terms IP Address, Port, Socket? At which layer (number and name) of the network stack are each of these used?   [6 marks]

    (b) What are the two functions `gethostbyname()` and `getaddrinfo()`? Comment briefly on their similarities and differences.   [4 marks]

    (c) What advantage would an application using `getadrinfo()` have over one that used `gethostbyname()`?   [2 marks]

Student ID: . . . .

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.