PRIFYSGOL CYMRU; UNIVERSITY OF WALES

DEGREE EXAMINATIONS MAY/JUNE 2002

SWANSEA

Computer Science

CS 238 Data Communications and Computer Networks

Attempt 2 questions out of 3

Time allowed: 2 hours

Students are permitted to use the dictionaries provided by the University

Students are permitted to use the calculators provided by the University

CS_238 (June 2002)
DATA COMMUNICATIONS AND COMPUTER NETWORKS
*(Attempt **2** questions out of 3)*

Question 1.

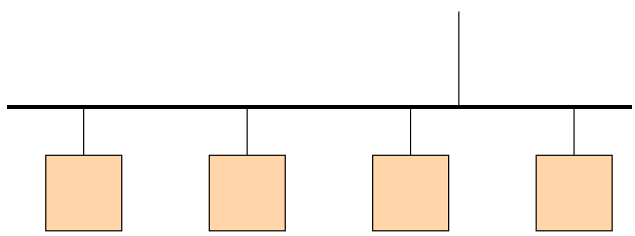
(a) In the context of the ISO 7-layer model (the reference model for OSI), name each layer in the correct order, and state in which layer(s) the following functions are featured.

(i)	congestion control,	(ii)	file transfer protocol (FTP),
(iii)	data compression,	(iv)	data encryption,
(v)	flow control.		

Medium Access Control (MAC) was not featured in the original 7-layer model, but later introduced into the model as a sub-layer. What is the main function of the MAC sub-layer, and where does it locate in the 7-layer hierarchy?

[7 marks]

(b) A trainee network operator was given a task to set up a local area network with subnet number 137.44.34.192. He connected four hosts to the subnet, and assigned an IP address for each of the hosts (as shown on the right). During the process, the trainee made some mistakes. Identify all mistakes.



Assign an appropriate subnet mask for this subnet, and give both decimal and binary representations of the subnet mask. With your subnet mask, what is the maximum number of hosts this subnet can accommodate?

[5 marks]

(c) Three codes, each with only four valid codewords, are given below. For each code, state the Hamming distance of the code. How many bit errors could it detect, and how many could it correct?

(i) **001**, **010**, **100**, **110**;
(ii) **00000000000000**, **00000001111111**, **11111110000000**, **11111111111111**;
(iii) **000100**, **101001**, **110010**, **011111**.

[6 marks]

(d) A station needs to transmit a binary string **011111111 ($b_1b_2...b_9$)**. The data string is:

(i) first extended to include, after b_9, a 5-bit frame check sequence, **11011**, which is calculated using the Cyclic Redundancy Check (CRC) scheme with a divisor pattern **110101;**
(ii) then bit stuffed based on the ISO HDLC standard delimiter pattern **01111110**;
(iii) and finally framed with the ISO HDLC standard delimiter **01111110** at both ends.

Verify that the frame check sequence, **11011**, is calculated correctly. (You must show all steps of the modulo-2 operation concerned.) Work out the final frame to be transmitted in the form of a binary string.

[7 marks]

Question 2.

(a) With the aid of one or more diagrams, describe the use of hubs, bridges, routers and gateways, and the differences between them.

[8 marks]

(b) With the aid of an example, describe the need for *packet filtering* performed by an intelligent bridge.

[4 marks]

(c) In the context of CSMA/CD (IEEE 802.3), answer the following questions:

- What is a "jam sequence" and what is it used for?
- Why does a station wait for a *random* amount of time after a collision, and how is the waiting time calculated?
- The protocol also imposes the minimum packet size of 64 bytes. Suggest a reason for this restriction. (Hint: collision detection.)

[7 marks]

(d) The *distributed routing algorithm* is used for packet routing in a subnet as shown below. Consider the current routing table of IMP G (Table 1), and the time delay vectors received by G from its neighbours (Table 2). The most recent delays measured by G are 12 for GB, 4 for GF, and 7 for GH (i.e. there is a long delay along the connection between G and B). Update the route table for IMP G based on the new information. All delays are measured in seconds.

Briefly discuss the advantages of this algorithm in comparison with centralised and isolated routing algorithms.

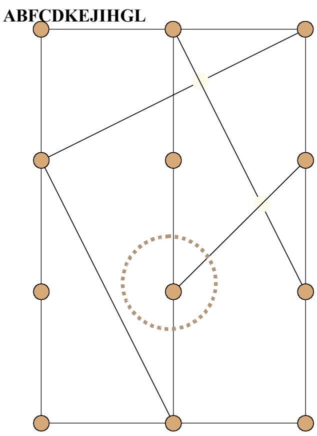


Table 1

from G to	delay	via
A	9	B
B	5	B
C	10	B
D	13	H
E	8	F
F	4	F
G	0	-
H	6	H
I	12	F
J	12	H
K	14	H
L	11	H

Table 2

to	B	F	H
A	3	9	16
B	0	12	11
C	4	8	15
D	11	15	7
E	9	4	14
F	11	0	10
G	8	5	7
H	12	10	0
I	13	8	10
J	11	12	3
K	15	17	8
L	15	16	5

[6 marks]

Question 3.

(a) For each of the following pairs of techniques, state their main use. With the aid of diagrams in some cases if necessary, contrast the two techniques in each pair.

(i) “go back n” and “selective repeat” methods used for a noisy channel;
(ii) token ring (IEEE 802.5) and token bus (IEEE 802.4);
(iii) frame relay and cell relay;
(iv) time-division multiplexing and frequency-division multiplexing.

[10 marks]

(b) Consider a code consisting of six symbols A-F, and the following character string:

E E E A A A A A B B F C C A D D E E E E

Derive a Huffman code specifically for the transmission of this string. You must show a Huffman tree and the corresponding set of binary codewords. If the original set was represented by a fixed-length binary code, what compression ratio would you have achieved in this transmission?

Describe another compression method that would be suitable for this case. Using this method, what compression ratio would you have achieved in this transmission?

[8 marks]

(c) Merkle’s Puzzles consist of 20,000 cryptograms. The plaintext of each puzzle starts out with 128 zero bits, followed by a 16-bit puzzle number and then a 56-bit key. Each of the 200-bit cryptograms is encrypted using the Data Encryption Standard (DES) with a key whose final 22 bits are zeros. (We assume that one encryption operation takes 1 μsec, and 2^{33} encryption operations take about 3 hours on average).

In the context of DES, what are Merkle’s Puzzles used for?

After receiving the Puzzles, what should the designated receiver do in order to establish a secured communication line with the sender?

Why does the sender use keys with 22 zero bits to encrypt the cryptograms?

If the speed of computers increases and encryption operations take much less time, what would you do to make the Puzzles more secure?

[7 marks]