IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2011

BEng Honours Degree in Information Systems Engineering Part III
MEng Honours Degree in Information Systems Engineering Part III
BSc Honours Degree in Mathematics and Computer Science Part III
MSci Honours Degree in Mathematics and Computer Science Part III
MSc in Computing Science
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the Associateship of the City and Guilds of London Institute
This paper is also taken for the relevant examinations for the Associateship of the Royal College of Science

PAPER C527

COMPUTER NETWORKS AND DISTRIBUTED SYSTEMS

Thursday 12 May 2011, 14:30
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators required

Section A (Use a separate answer book for this section.)

1 a Briefly explain each of the following terms and relate it to a layer in the OSI model:

i) Broadband network

ii) Token frame

iii) Backwards learning algorithm

iv) Address Resolution Protocol (ARP)

v) Top Level Domain (TLD)

b Four hosts A, B, C and D are connected to the same Ethernet segment. Host D is currently transmitting a frame. Suppose that hosts A, B and C all want to transmit a frame at some future point in time.

i) Describe the operation of Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

ii) Draw a timeline with time slots that shows one possible sequence of events on the Ethernet segment that includes *frame transmission attempts*, *frame collisions*, *exponential backoff* and *successful frame transmissions*.

Your timeline should meet the following criteria:

a. initial frame transmission attempts should be in the order host A, B and C;
b. successful frame transmissions should be in the order host A, B and C;
c. there should be at least **three** frame collisions.

iii) Explain how you would improve Ethernet's backoff strategy if no more than four hosts were ever connected to the same Ethernet segment.

The two parts carry, respectively, 35% and 65% of the marks.

2a A company is allocated a block of IP addresses starting with 194.128.224.1 and having 255.255.224.0 as the netmask.

i) Briefly explain Classless Internet-Domain Routing (CIDR) and why it was introduced.

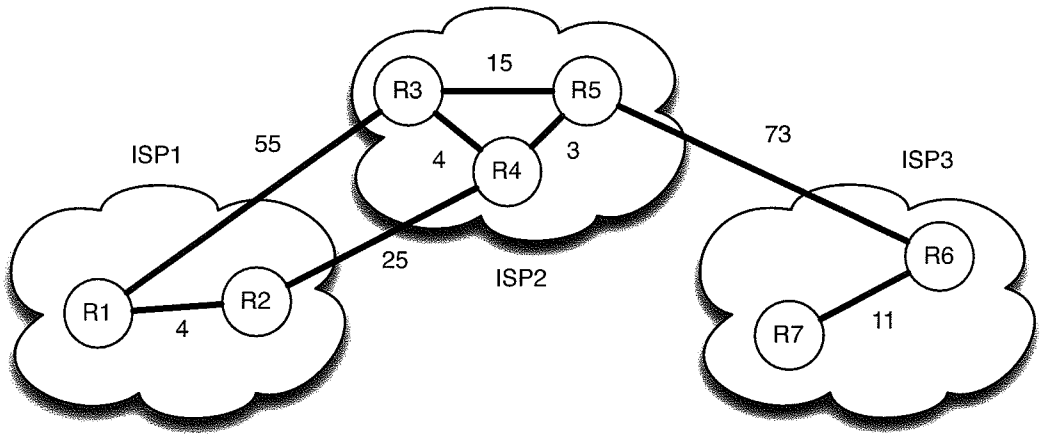
ii) What IP class do the allocated IP addresses belong to?

iii) What is the total number of hosts that the company can connect to their network?

iv) What is the subnet mask to create exactly **four** subnets from the allocated IP block?

v) What is the number of hosts on each subnet?

b An internetwork with three Internet Service Providers (ISPs) has the topology shown below. It consists of seven routers with the stated link costs in terms of packet communication latencies in milliseconds. The routers use the *distance-vector* routing algorithm.



i) Write down the routing tables for **each** router

(1) when routers only know the costs to their immediate neighbours;

(2) after **one** additional round of information exchange;

(3) after **two** additional rounds of information exchange.

ii) Assume that there is packet congestion on the network link between routers R2 and R4. Explain what happens and why the routing set-up is not ideal in this case.

The two parts carry, respectively, 45% and 55% of the marks.

Section B (Use a separate answer book for this section.)

3a The following message passing primitives are supported by a set of library calls:

send (dest, msg) – an *asynchronous* send message primitive, where dest is the name of the process to which the message msg is to be sent.

receive (source, msg) – this causes the receiving process to block waiting for a message from the process with name source. msg is a buffer into which the incoming message is copied.

receiveany (source, msg) – the process is blocked waiting for a message from any source. The name of the sender is received in source and the incoming message is received in msg.

i) Explain what is meant by an *asynchronous* send message primitive and why it may lead to buffer exhaustion at the receiver.
ii) Present a plausible scenario to justify why both the above receive and receiveany primitives are needed.

b A car park has spaces for 100 cars and has a single entry and exit, each controlled by a gate. When a car arrives at the gate, the driver presses a button. The exit gate always opens but the entry gate only opens if there is a space available in the car park. Assume drivers know if there are spaces available and can decide to wait for a space at the entrygate. Using the above message primitives, design a car park system with entrygate and exitgate controllers and a coordinator which decides when the entrygate can be opened. In addition to the above message primitives, the gate controllers have access to the following calls:

button () – returns when the button is pressed by the driver.
detector () – returns when a car has passed through.
open () – opens the gate.
close () – closes the gate.

Provide pseudocode for:

i) Only the entrygate controller (exit and entry controllers have the same code).
ii) The coordinator that communicates with the controllers by message passing.

Assume reliable communication so acknowledgments and retransmissions should not be included.

c A double-linked list (forward & backward pointers) is used to maintain a workschedule ordered on length of job. Explain why simply 'flattening' this data structure for transfer to another computer will not work. Explain how this data structure can be serialised.

The three parts carry, respectively, 25%, 50%, 25% of the marks.

4a Define each of the following terms and give examples of how they can be achieved:

- Authentication
- Confidentiality
- Integrity
- Non-repudiation

b Compare asymmetric encryption systems (i.e. public key) with symmetric key encryption systems (i.e. shared key). Outline how asymmetric encryption techniques can be used to authenticate users.

c You are in charge of designing an Internet music service called Streamy. The system will consist of two parts: a Streamy Server; and a Streamy Client to be run on customer computers. The Streamy Client needs a token to play music downloaded from the Streamy Server. This token is provided by Streamy to paying customers. A token is tied to a particular Streamy Client and is only valid for a set time (e.g., 1 month). The token can be revoked by the Streamy Server.

You are to assume that each of the Streamy Clients has a unique public/private key pair, as does the Streamy Server.

i) Describe the fields in the token, providing a justification for each.
ii) Digital signatures can be used to provide message integrity for tokens. Outline the steps that must be taken by the Streamy Server to digitally sign tokens and by the Streamy Client to verify a token. Use the notation below when describing the steps.

SS – Streamy Server

SC – Streamy Client

Kss - Streamy Server secret key

Ksp - Streamy Server public key

Kcp - Streamy Client public key

Kcs - Streamy Client secret key

H(t) – is the hash of token t

The three parts carry, respectively, 20%, 35% and 45% of the marks.