UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2000

MSc in Computing Science
BEng Honours Degree in Mathematics and Computer Science Part III
MEng Honours Degree in Mathematics and Computer Science Part III
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 Royal College of Science

PAPER M313

COMPUTER NETWORKS AND DISTRIBUTED SYSTEMS

Friday 5 May 2000, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions

Section **A (Use a separate answer book for this Section)**

1a i) What is the purpose of Medium Access Control in a Local Area Network (LAN)?

ii) IEEE 802.3 uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Describe its operation and explain why it is appropriate for the network.

iii) IEEE 802.11 uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Describe its operation and explain why it is appropriate for the network.

iv) What is the difference between a shared-bandwidth Ethernet LAN and a switched Ethernet LAN? Your answer should include how the network behaves in each case.

b i) Explain the difference between a protocol address and a physical address. Include in your answer why both are needed.

ii) What advantages does BOOTP have over RARP for allowing a diskless client machine to discover its IP address on start up?

c i) List the functionality that TCP adds to the IP service it is layered over.

ii) When might UDP be useful, despite only providing unreliable "best effort" delivery? Include some examples in your answer.

The three parts carry, respectively, 40%, 30%, 30% of the marks.

2a i) Outline the functions of a bridge and a router. Include in your answer at what layer of the OSI reference model each operates.

ii) If virtually all packet-switching networks use some form of adaptive routing strategy, when might a non-adaptive one still be needed?

b i) Explain how Mobile IP provides a Mobile Node with a continuous Internet connection when it is away from its home network.

ii) Mobile IP probably prevents the most efficient routing of IP packets from Correspondent Node to Mobile Node. Discuss what would be required to improve the situation.

c i) Explain why Post Office Protocol (POP) is needed in addition to Simple Mail Transfer Protocol (SMTP) for Internet email.

ii) A commercial Internet Service Provider (ISP) may offer "WebMail", where a user's mail is sent and received via a World Wide Web page. Discuss any advantages and disadvantages of this method compared to an SMTP/POP-based service.

iii) Why does Hypertext Transfer Protocol (HTTP) v1.0 perform badly? Describe how this drawback is addressed by HTTP v1.1.

The three parts carry, respectively, 30%, 30%, 40% of the marks.

Section **B (Use a separate answer book for this Section)**

3a Explain the following call semantics associated with Remote Procedure Call Mechanisms. For each one, outline the implementation issues and give an example of where it would be used.

i) Maybe
ii) At-least-once
iii) At-most-once

b Specify the RPC interface to an Election Service which allows a client to both query the current number of votes for a specified candidate and vote for one of the set of candidates. Each client has a voter number used for identification in requests and candidates are identified by a string name.

c Give a *pseudocode* implementation for the Election Service (server only) which would permit the interface to be invoked using an RPC mechanism which supports *at-least-once* calling semantics. Explain why your implementation deals with this calling semantics.

The three parts carry, respectively, 45%, 10%, 45% of the marks.

4a Explain what a public-key (*asymmetric*) cryptographic system is and how it can be used to both authenticate the originator of a message and provide secrecy for the data in transit. Briefly describe the advantages and disadvantages of using public-key cryptography.

b An electronic cash system allows Alice to withdraw an electronic cash token for a requested amount (e.g. £50) from her account at BA Bank to her electronic wallet. She can then use this token to pay Bob for a £50 item. Assume the token cannot be split into smaller value tokens and that Alice and Bob have the same Bank. Bob sends the token to the bank to be credited to his account, and delivers the item once he receives positive confirmation that his account has been credited.

i) Draw a diagram of the various interactions between Alice, Bob and the BA Bank, indicting the order in which they occur.

ii) Assuming a *public-key* cryptographic system, describe and explain the message contents in the interactions between Alice, Bob and the BA Bank, assuming secrecy and authentication is required. Your solution must indicate how to prevent a token being used more than once. Use the following notation:

K_{sX} {M} denotes a message encrypted with the secret key of X
K_{pX} {M} denotes a message encrypted with the public key of X

The two parts carry, respectively, 30% and 70% of the marks.