PRINCE OF SONGKLA UNIVERSITY

FACULTY OF ENGINEERING

Final Examination: Semester 1	**Academic Year:** 2007-2008
Date: October 5, 2007	**Time:** 09:00 – 12:00
Subject Number: 240-643	**Room:** A400
Subject Title: The Internet and its Protocols	

Exam Duration: 3 hours

This paper has 3 pages (including this page).

Authorised Materials:

- Anything the student can carry, except for mobile phones.

Instructions to Students:

- *Answer questions in English.* Good English is **not** required.
- Write answers in an answer book.
- Start the answer to each question on a new page.
- **Clearly Number** the answers. It is **not** required that questions be answered in order.
- The marks allocated for each question are shown next to that question. There are 100 marks total for this examination. This will contribute 50% of the course total. Questions assigned higher numbers of marks expect a more detailed and thorough answer than questions allocated less marks.
- Attempt all 5 questions.
- Anything illegible is incorrect.
- Answer briefly where possible, essays are **not** required.

Question 1. *(20 marks)*

Some protocols use a binary packet format with fixed fields, others protocols use a binary packet format with an encoded representation of what the various data represents, and yet other protocols use a text based packet format, with words (or strings that approximate words) as the field identification.

Given an example of a protocol of each type.

Explain in what circumstances each might be a suitable technique to use when a new protocol is to be defined.

Question 2. *(20 marks)*

Explain the tradeoffs and design decisions that led to the IP fragmentation requirement, for both IPv4 and IPv6, that the size of all fragments except the last fragment of a packet must be a multiple of 8 octets.

Why was 8 (eight) chosen?

What other values might have been reasonable, and what would the advantages and disadvantages of those values have been?

Would there have been any reason to consider changing this requirement when IPv6 fragmentation was being designed? If so, what reason? If not, why not?

Was retaining fragmentation in IPv6 necessary? If so, why? If not, why do you believe fragmentation still exists in IPv6?

Question 3. *(15 marks)*

Which do you believe is more important when designing a protocol, efficiency, or extensibility?

Why?

Give reasons for your opinion, including examples from protocols that support your argument (which can be cases where a positive result was achieved from following the advice you would give, or cases where a poor result was achieved after adopting the other approach).

Question 4. *(20 marks)*

A new protocol is to be designed, containing some number of options, and allowing for new options to be created in the future.

The designers of the protocol propose to use a single octet (byte) to number the options (far less than 100 are assumed to ever need to be defined).

They also propose to allocate numbers from 1 to 127 for "standard" options, and from 128 to 254 for user or vendor created (private) options. (Option 0 is reserved, and 255 retained to provide a method of extending the option number space if that is ever required.)

Give the reasons you would use to support, or to oppose, this proposed design.

You should ignore all issues other than the question of option numbers – that is, assume that the rest of the protocol design is perfect...

Question 5. *(25 marks)*

Explain the security issues with the Neighbor Discovery (ND) protocol for IPv6 as it was originally designed. (That is, Neighbor Solicitations and Advertisments, and Router Solicitations and Advertisments – you can ignore the other ND packets for the purposes of this question.)

Contrast this with the Address Resolution Protocol (ARP) for IPv4. (That is, explain whether there are any new problems, any solved problems, related to security with ND, as compared with ARP.)

Explain how the use of Cryptographically Generated Addresses (CGA) can benefit ND.

Include in your answer an explanation of what can be deduced from correct use of a CGA in an ND packet, and what cannot.

What else, apart from using CGAs, is necessary to secure the ND protocol? What does this extra mechanism accomplish?