PRINCE OF SONGKLA UNIVERSITY

FACULTY OF ENGINEERING

Final Examination: Semester 2	**Academic Year:** 2005-2006
Date: March 5, 2006	**Time:** 09:00 – 12:00
Subject Number: 240-362	**Room:** Robot Head
Subject Title: Internet Engineering	

Exam Duration: 3 hours

This paper has 7 pages (including this page).

- Write answers in the answer book provided.
- There are 180 marks total for this exam.
  This will contribute 30% of the course total.

Authorised Materials:

- Anything the student can carry (except mobile/cell phones.)

Instructions to Students:

- Attempt all 12 questions.
- **Clearly Number** the answers. It is **not** required that questions be answered in order.
- Anything illegible is incorrect.
- Show all calculations, not just the final result.
- Answer briefly where possible, essays are **not** required.
- The marks allocated for each question are shown next to that question. There are 180 marks total for this examination.
- *Answer questions in English.* Good English is **not** required.

Question 1. *(5 marks)*

Which of the following are information that we can ask from the DNS, and which are not?

A) IP addresses of fivedots.coe.psu.ac.th

B) Host name of the machine that has IP address 172.30.130.164.

C) What is the mail exchange for coe.psu.ac.th.

D) List of host names of machines that have IP addresses starting with 172.30

E) List of the IP addresses of the machines that have host names starting with "coelab".

Question 2. *(15 marks)*

There are 4 sections of resource record (RR) in each DNS message. They are the question, answer, authority and additional sections. When a resolver would like to send a DNS query message to a DNS server, it can add only one RR in the question section. This is one of DNS limitations.

Explain why the resolver cannot put more than one RR in the question section of a DNS query message.

Question 3. *(20 marks)*

One of the limitations of the DNS is that the size of a DNS message transmitted in a UDP packet should not be bigger than 512 bytes. This is not a problem for DNS query message because it has not much information (only one RR per query message). But it is possible for a DNS reply message to be bigger than 512 bytes.

When a DNS client receives a DNS reply message sent from a DNS server, explain how does it know that the reply message does not contain the complete answer? Also: What is the DNS client will do next in order to get the complete data of that DNS reply message?

Question 4. *(20 marks)*

There is a web page, named gallery.html, located in a web server. This page contains 10 JPEG images and the HTML tag of this page, which is as follows:

```
<html>
<head>
<title>Picture Gallery<title>
</head>

<body>
<h1>This is my gallery</h1>
<img src = "p1.jpg"> <img src = "p2.jpg">  <br>
<img src = "p3.jpg"> <img src = "p4.jpg">  <br>
<img src = "p5.jpg"> <img src = "p6.jpg">  <br>
<img src = "p7.jpg"> <img src = "p8.jpg">  <br>
<img src = "p9.jpg"> <img src = "p10.jpg"> <br>
</body>
</html>
```

Given that you would like to browse this web page and the round trip time between your machine and the web server is 40 milliseconds. Assume that each HTTP object is small and the transfer time of each object is very short (can be discarded).

Calculate the latency (time you have to wait) from submitting the web page request until you receive the complete page in the case of your web browser uses the following methods:

A) Persistent Connection

B) Pipeline

You must show how you calculated each answer.

Question 5. *(20 marks)*

There are 2 classes of encryption, symmetric key encryption and public key encryption. The second, public key encryption can be more versatile but takes more time for encryption. So it is appropriate for small amounts of data and sometimes needs to be used in combination with symmetric key encryption such as the case of a secure web page.

Describe the security steps that a web browser (client) uses to communicate with a web server in order to provide secure transmission of data from the web browser. For each step you must explain what data is sent, who sends it, how it is encrypted or decrypted (which key is used, for example) and how that data can be checked to determine that it is correct and secure.

Question 6. *(15 marks)*

Imagine an E-Mail client Mail Transfer Agent (MTA) attempting to transfer a message to a server MTA. The client connects to the server, and begins the SMTP *(Simple Mail Transfer Protocol)* transaction. During the protocol exchange, the server replies with a **4nn** (temporary error) code to one of the recipient addresses.

A) Give some example reasons why the server MTA might reply with a temporary error code when asked to deliver a message to a particular recipient.

[5 marks]

B) Explain the actions of the client MTA when it receives this error response, both upon the remainder of the current SMTP connection, and as to how it deals with the message in the future.

[10 marks]

Question 7. *(15 marks)*

Explain, using time-line diagrams, exactly when responsibility for a e-mail message passes from one MTA to another (when the client releases its responsibility, and when the server becomes responsible) relating this to the sequence of steps (commands) used during the SMTP transaction.

Show what happens if the TCP connection should be broken (for any reason) at various times during the SMTP message transaction.

Explain why the concept of ownership of responsibility for the message is important, and what might occur if this concept did not exist.

Question 8. *(5 marks)*

Which of the following cannot be provided using Quality of Service (QoS) mechanisms?

(Note: There might be any number of answers from – 0 to 5)

A) Lower packet delay.

B) Ordered packet delivery.

C) Less variation in the intervals between packet arrival times (that is, less jitter).

D) Higher probability of packet loss.

E) Reliable data transfer.

Question 9. *(20 marks)*

Multicast packet delivery, like unicast packet delivery, relies upon routing protocols to determine the path through the network from the sender to the recipient(s).

Explain the requirements of multicast routing protocols, and contrast those with the requirements of unicast routing protocols.

In your answer, indicate what the differences are between unicast and multicast traffic (packets) that influence the requirements placed upon the routing protocols.

Question 9

Question 10. *(20 marks)*

Using an example, explain how the SNMP (Simple Network Management Protocol) **GetNext** operator operates on the MIB (Management Information Base) of an SNMP agent.

Your answer should show a sample MIB (you can invent this MIB, and the OIDs (Object Identifers) used for it —there is no need to use any of the many standard MIBs that exist).

You should show what queries the SNMP manager (client) might make of the agent (server) and explain why those queries are useful. You may assume for this purpose that the data in the MIB that you have chosen or invented is useful, and that the SNMP manager desires to obtain that data. There is no need to explain why the data is useful, nor what use the manager will make of it.

You should also show what replies the manager will send the client.

You do not need to show SNMP packet formats, all that is required is the OIDs (and/or names) of the variables contained in each SNMP request (and the type of that request) and response.

Question 11. *(10 marks)*

Explain how a playout buffer can help reduce the effects of jitter upon a real time application.

Indicate what is the cost (in terms of application or network performance, or apparent performance) of using a playout buffer.

Is a playout buffer ever useful for applications using TCP? Why, or why not?

Question 12. *(15 marks)*

Which of the following statements do you agree with, and which do you disagree with? In each case, indicate whether you agree or disagree, and give reasons for your decision.

You may expand upon the statements below (add more detail) if that will help your answer.

A) With e-mail, the most important security issue is to make sure that the e-mail is not lost, or stolen.

B) Use of any kind of certificate based authentication is not practical for e-mail security purposes, as e-mail users are not prepared to spend the money (or time) required to have a certificate signed by a certificate authority.

C) IPsec (network level security) and SSL (secure sockets layer) (or TLS, Transport Layer Security) are not very useful for e-mail, because they protect the message only between one MTA (Message Transfer Agent) and the next.