VICTORIA UNIVERSITY OF WELLINGTON

Te Whare Wananga o te Upoko o te Ika a Maui

EXAMINATIONS — 2003

END OF YEAR

COMP 306

DATA COMMUNICATIONS

Time Allowed: 3 Hours

Instructions: There are five questions.
Answer all questions.
Each question is worth 20 marks.
Paper foreign to English language dictionaries are allowed.
Electronic dictionaries and programmable calculators are not allowed.

Question 1. Warmup [20 marks]

(a) [2 marks] Draw the TCP/IP protocol stack.

(b) [2 marks] What is the role of the socket API?

(c) [2 marks] Give one reason why the FTP protocol uses separate control and data connections.

(d) [2 marks] Give two reasons why an application might use UDP rather than TCP.

(e) [2 marks] Why should an institutional proxy cache be better at reducing bandwidth demands than a browser cache?

(f) [2 marks] In the context of IP, what is an autonomous system?

(g) [2 marks] What is the main difference between the OSPF protocol and the RIP protocol?

(h) [2 marks] What are the two things that are known before the execution of a link state algorithm?

(i) [2 marks] What is the main idea behind a carrier sense protocol?

(j) [2 marks] Explain how a host can have multiple IP addresses.

Question 2. DNS and Naming [20 marks]

(a) [2 marks] What is the primary role of the DNS?

(b) [2 marks] Explain how recursive DNS queries differ from iterative DNS queries.

(c) [2 marks] In what situation is an iterative DNS query preferable to a recursive DNS query? Why?

(d) [2 marks] In what situation is a recursive DNS query preferable to an iterative DNS query? Why?

(e) [4 marks] Within the context of naming, define:

i. Binding.

ii. Aliasing.

(f) [2 marks] Outline the problem that URNs are designed to overcome.

(g) [6 marks] Outline:

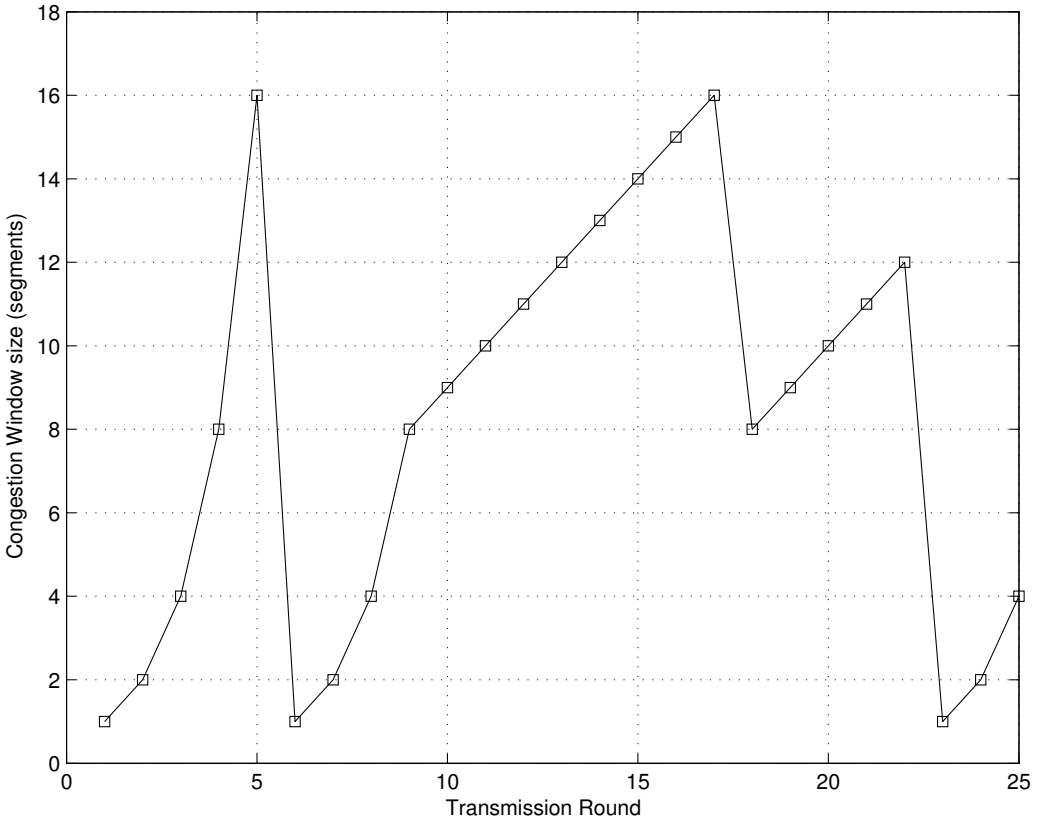
i. What changes would be needed to the web before URNs could be adopted.

ii. Any advantages, and

iii. any disadvantages.

Question 3. Transport Protocols [20 marks]

(a) [7 marks] The TCP Reno congestion control algorithm has a faster recovery mechanism than the Tahoe algorithm it replaces. Consider the following plot of TCP window size as a function of transmission round for TCP Reno.



Answer all of the following questions. In all cases you should provide a brief explanation to justify your answer.

i. Identify the intervals of time when TCP slow start is operating.

ii. Identify the intervals of time when TCP congestion avoidance is operating.

iii. After the 5th transmission round, is segment loss detected by a triple duplicate ACK, or by timeout?

iv. After the 17th transmission round, is segment loss detected by a triple duplicate ACK, or by timeout?

v. What is the value of Threshold at the 1st transmission round?

vi. What is the value of Threshold at the 7th transmission round?

vii. Assuming a packet loss is detected after the 25th round by the receipt of a triple duplicate ACK, what will be the values of the congestion window and the threshold.

(b) [8 marks] Imagine a variation on the *GoBackN* protocol that uses only negative acknowledgements. Explain:

i. How this protocol will work.

ii. How this protocol affects the sender's window.

iii. How the protocol performs with packet loss for both high and low arrival rates.

(c) [5 marks] Consider the situation where we have an indirect connection between hosts A and B, with the packets between A and B passing through a variety of links and routers. Applications running on hosts A and B communicate via a protocol stack with a stop and wait transport protocol that uses alternating 0's and 1's as sequence numbers.

The stop and wait protocol will not work properly in this situation.

i. Draw a diagram to clearly illustrate the problem.

ii. How will the errors appear to applications running on hosts A and B?

iii. Outline a strategy to solve this problem.

Question 4. Random Access Protocols and Ethernet [20 marks]

(a) [6 marks] Consider the ALOHA protocols.

i. What is the major difference between the slotted ALOHA and pure ALOHA protocols?

ii. Explain the main advantage that the pure ALOHA protocol has over the slotted ALOHA protocol.

iii. Explain the main advantage that the slotted ALOHA protocol has over the pure ALOHA protocol.

(b) [6 marks] Discuss why the Ethernet protocol uses an exponential backoff period rather than fixed backoff period.

(c) [8 marks] Suppose nodes A and B are on the same 10Mbps Ethernet segment, and the propagation delay between the two nodes is 290 bit times. Suppose node A begins transmitting a frame, and before it finishes, node B begins transmitting a frame (remember that A must transmit 512 + 64 bits). Show that A will transmit the entire frame before it detects a collision and discuss the consequences. Show all your workings when answering this question.

Question 5. Cryptography and Authentication [20 marks]

In the following questions we have three parties: Alice, Bob and Slippery Sam. Alice and Bob are friends, while Slippery Sam is an active intruder.

(a) [10 marks] Alice wants to authenticate Bob using a challenge-response protocol.

i. Briefly describe the key difference between authentication and authorisation.

ii. Describe how Alice would use the challenge-response protocol to authenticate Bob.

iii. Explain how Slippery Sam could pretend that he is Bob.

iv. Consider whether Slippery Sam could still break the protocol if the responses were encrypted.

v. Briefly describe how could Alice and Bob make the authentication process more secure without using encryption.

(b) [10 marks] Alice sends Bob a secret message encrypted using an symmetric encryption algorithm and a key she only shares with Bob. Slippery Sam is acting as an active intruder. Justify your answers to the following.

i. Could Slippery Sam read the contents of the secret message?

ii. Could Slippery Sam substitute his own message for Alice's message without Bob detecting the change?

iii. Slippery Sam knows that Alice always starts her messages with "Dear Bob". What type of cryptanalysis attack could Slippery Sam use to discover the encryption key?

iv. Alice decides to switch to asymmetric encryption. She publishes her public key using a trusted certification authority and sends Bob messages encrypted with her private key. Would this stop Slippery Sam reading her messages?

v. Alice and Bob decide to go back to using symmetric encryption. They need to establish a new symmetric key. Bob sends Alice a message that contains a new symmetric key encrypted using her public key. Should Alice use this key for future communication – why or why not?

****