Coláiste na Tríonóide, Baile Átha Cliath
Trinity College Dublin
Ollscoil Átha Cliath | The University of Dublin

Faculty of Engineering, Mathematics and Science

School of Computer Science & Statistics

Integrated Computer Science Programme **Trinity Term 2016**
Year 3 Annual Examinations

Advanced Telecoms

20 May 2016 **Regent House** **09:30 – 11:30**

Dr Hitesh Tewari

Instructions to Candidates:

Attempt **two** questions. All questions carry equal marks. Each question is scored out of a total of 50 marks.

You may not start this examination until you are instructed to do so by the invigilator.

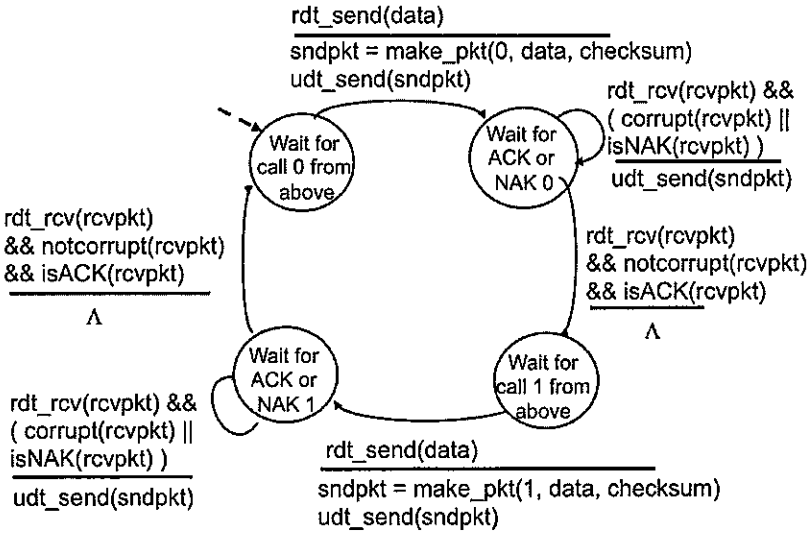
Materials Permitted for this Examination:

Non-programmable calculators are permitted for this examination — please indicate the make and model of your calculator on each answer book used.

1. (a) Distinguish between the user datagram protocol (UDP) and the transport control protocol (TCP) in terms of reliable data transfer, header size and connection overheads. For IP Telephony and IP Videoconferencing, which one of TCP and UDP would be preferable. Justify your answer. [10 marks]

   (b) Suppose a Web server runs in Host C on port 80. Suppose this Web server uses persistent connections, and is currently receiving requests from two different Hosts, A and B. Are all the requests being sent through the same socket in Host C? If they are being passed through different sockets, do both the sockets have port 80? Discuss and explain. [6 marks]

   (c) The diagram below shows the finite state machine (FSM) for a reliable sender that can handle garbled ACKs and NAKs. Draw the FSM for the corresponding receiver.



[12 marks]

   (d) Suppose Host A sends two segments back to back to Host B over a TCP connection. The first segment has sequence number 65; the second has sequence number 92.

   - How much data is in the first segment?
   - Suppose the first segment is lost but the second segment arrives at B. In the acknowledgement that Host B sends to Host A, what will be the acknowledgement number?

[6 marks]

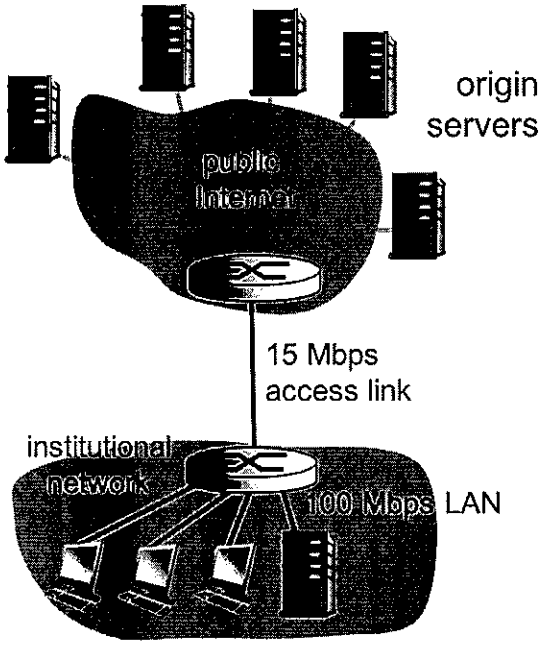
(e) With the aid of an example describe the TCP "Fast Retransmit" algorithm and its advantages. [8 marks]

(f) Why is TCP congestion control referred to as an additive-increase, multiplicative decrease (AIMD) form of congestion control? [8 marks]

2. (a) Briefly explain the role of hypertext transfer protocol (HTTP) in web communications. Why is HTTP 1.0 called a stateless protocol? [10 marks]

   (b) Consider an e-commerce site that wants to keep a purchase record of each of its customers. Describe how this can be done with cookies. [10 marks]

   (c) Consider the institutional network below which is connected to the Internet via a 15 Mbps access link. Suppose that the average object size is 960,000 bits and that the average request rate from the institution's browsers to the origin servers is 15 requests per second. Also suppose that the amount of time it takes from when the router on the Internet side of the access link forwards an HTTP request until it receives the response is 2 seconds on average. Model the total average response time as the sum of the average access delay (that is, the delay from the Internet router to the institution router) and the average Internet delay. For the average access delay, use $\triangle(1 - \triangle\beta)$, where $\triangle$ is the average time required to send an object over the access link and β is the arrival rate of objects to the access link.



   - Find the average response time
   - Now suppose a cache is installed in the institutional LAN. Suppose the miss rate is 0.4. Find the total response time.

   [12 marks]

   (d) Consider what happens when a browser (i.e. a HTTP client), running in

some user's host, requests the URL somesite.com/index.html. In order for the user's host to be able to send a HTTP request message to the Web server www.somesite.com, the user's host must first obtain the IP address of www.somesite.com. Explain the steps through which the IP address for such a hostname is obtained by the client. [12 marks]

(e) In BitTorrent, suppose Alice provides chunks to Bob throughout a 30-second interval. Will Bob necessarily return the favor and provide chunks to Alice in the same interval? Also consider a new peer Trudy that joins the BitTorrent without possessing any chunks. Without any chunks, she cannot become a top-four uploader for any other peers, since she has nothing to upload. How will then Trudy get her first chunk? [6 marks]

3. (a) Describe some of the components that comprise modern day block ciphers? In particular describe with the aid of an example the Vigenère Cipher. [8 marks]

   (b) With the aid of an example show why the electronic code book (ECB) mode is susceptible to substitution attacks. Describe the cipher block chaining (CBC) mode and how it can provide probabilistic encryption which overcomes the deterministic features of ECB mode. [10 marks]

   (c) Define a cyclic group G. What is the primitive element or generator of the group G? Check if $a = 2$ is a primitive element of $\mathbb{Z}_{11}^*$. Is the group $\mathbb{Z}_{11}^*$ a cyclic group? [8 marks]

   (d) Compute the two public keys and the common key for the Diffie-Hellman key exchange (DHKE) scheme with the parameters $p = 467$, $\alpha = 2$, and $a = 228$, $b = 57$. Show with the aid of an example how the DHKE scheme is vulnerable to the man-in-the-middle (MITM) attack. [12 marks]

   (e) Describe in detail the Handshake in the secure sockets layer (SSL) protocol. When we talk about authentication in SSL, do we mean *message authentication* or *entity authentication* - explain? What is the purpose of the random nonces in the SSL handshake? [12 marks]