TRINITY COLLEGE DUBLIN

THE UNIVERSITY OF DUBLIN

Faculty of Engineering, Mathematics & Science
School of Computer Science & Statistics

Integrated Computer Science Programme **Trinity Term 2015**
Year 3 Annual Examinations

Advanced Telecommunications (CS3031)

Tuesday 5th May, 2015 **Luce Lower** **09:30 – 11:30**

Dr. Hitesh Tewari

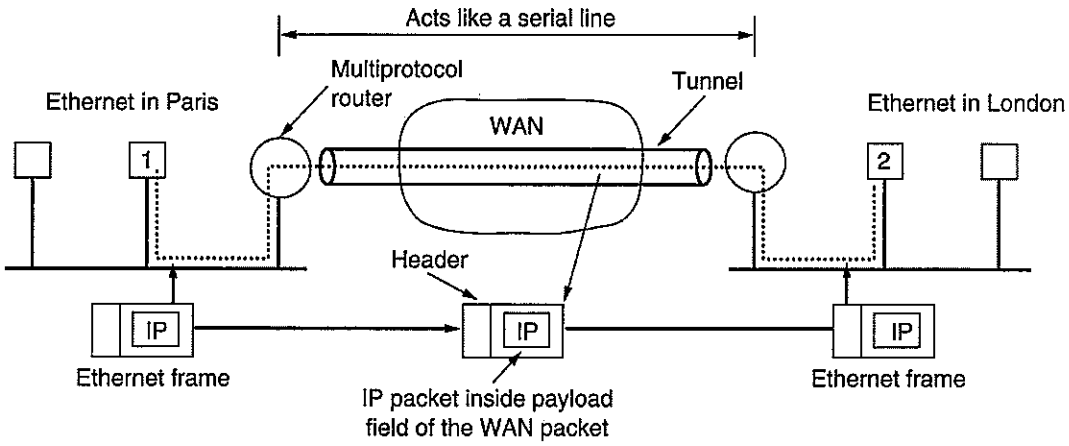
Instructions to Candidates:

- Answer TWO questions
- All questions carry equal marks
- Use diagrams where appropriate

Materials permitted for this examination:

- Non-programmable calculators are permitted for this examination

Q1a) Briefly describe the various datalink and network layer protocols used in transporting IP datagrams from the source to destination machines in the figure below.



(12 marks)

b) Distinguish between Classful and Classless addressing in IP networks highlighting the advantages and disadvantages of each approach.

(8 marks)

c) An organization is granted the block 130.56.0.0/16. The administrator wants to create 1024 subnets. Find:

i. The number of addresses in each subnet.

ii. The subnet prefix.

iii. The first and last address of the first subnet.

iv. The first and last address of the last subnet.

(12 marks)

d) In order for a host to be able to send an HTTP request message to a Web server (www.somesite.com), the user's host must first obtain the IP address of the server. Explain the steps through which the client obtains the IP address for such a hostname.

(10 marks)

e) Is it possible for an organization's Web server and mail server to have exactly the same alias for a hostname (e.g. foo.com)? What would be the type of RR that contains the hostname for the mail server?

(8 marks)

[50 marks]

Q2 a) Distinguish between the terms 'Confidentiality', 'Authentication' and 'Message Integrity' with regards to network security protocols.

(6 marks)

b) Consider RSA with $p = 7$ and $q = 13$.

i. What are n and $\Phi(n)$?

ii. Let e be 5. Why is this an acceptable choice for e?

iii. Find d such that $e * d \equiv 1 \pmod{\Phi(n)}$.

iv. Encrypt the message $m = 9$ using the key (e, n).

(12 marks)

c) In what way does a hash provide a better message integrity check than a checksum (e.g. a CRC)? Can you "decrypt" a hash of a message to get the original message? Explain your answer.

(8 marks)

Question 2 continues on next page...

...Question 2 continued from previous page

d) Show with the aid of an example how Alice and Bob can exchange a "Signed and Enveloped Message" using digital signatures.

(12 marks)

e) Compare and contrast Macropayment and Micropayment systems giving examples of each. (6 marks)

f) Explain what you understand by the phrase "Proof-of-Work" in the context of the Bitcoin electronic cash scheme.

(6 marks)

[50 marks]

Q3 a) Describe the various Medium Access Control (MAC) schemes employed in cellular networks, highlighting their advantages and disadvantages.

(12 marks)

b)In a typical mobile phone system with hexagonal cells, it is forbidden to reuse a frequency band in an adjacent cell. If 840 frequencies are available, how many can be used in a given cell?

(4 marks)

c) Describe in detail the steps involved during a GSM "Mobile Terminated Call", e.g. when a node in the PSTN makes a call to roaming mobile node.

(12 marks)

Question 3 continues on next page...

...Question 3 continued from previous page

d) Explain why is there a need for "handover" to take place in mobile networks. What are the various types of handover that can occur in GSM networks? Identify the network entities involved in each case.

(10 marks)

e) With the aid of an example outline the inefficiencies of Mobile IP regarding data forwarding from a correspondent node to a mobile node. What are the optimizations and what additional problems do they cause?

(12 marks)

[50 marks]