TRINITY COLLEGE DUBLIN

THE UNIVERSITY OF DUBLIN

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

Integrated Engineering **Trinity Term 2015**
Junior Sophister Annual Examination

Computer Networks (CS3D3)

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

Dr. Hitesh Tewari

Instructions to Candidates:

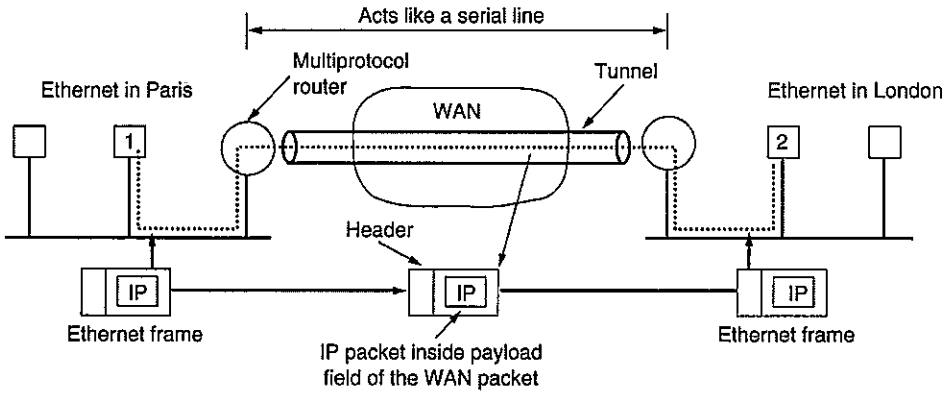
- Answer TWO questions
- All questions carry equal marks
- Use diagrams where appropriate

Materials permitted for this examination:

- Non-programmable calculators are permitted for this examination

1.

a) 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) 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)

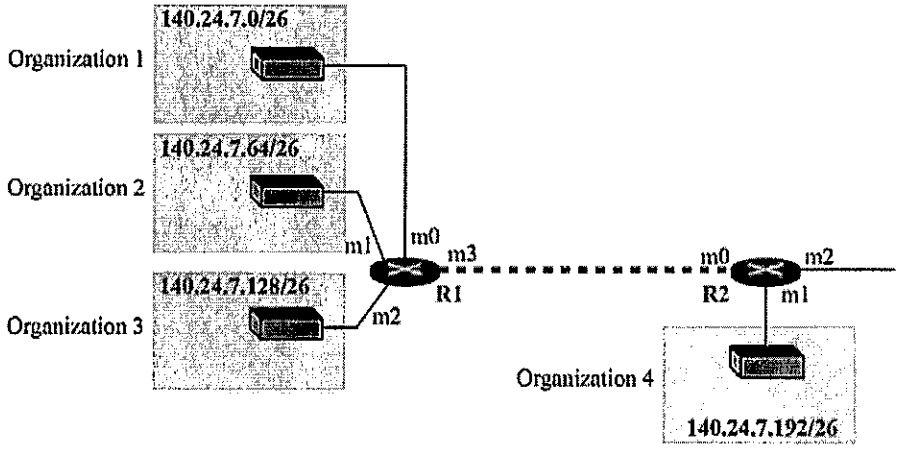
(Question 1 continues on next page)...

... (Question 1 continued from previous page)

c) Use an example network to distinguish between "Direct Delivery" and "Indirect Delivery" of datagrams on the Internet.

(8 marks)

d) Assume router R2 in the figure below receives a packet with destination address 140.24.7.42.



How is the packet routed to its final destination? Illustrate your answer by constructing the routing tables for both R1 and R2.

(10 marks)

e) What are the main distinguishing features of the IPv6 protocol? What are the advantages of keeping the IPv6 base header to be of a fixed length? (8 marks)

[50 marks]

2.

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

(6 marks)

b) Distinguish between a substitution cipher and a transposition cipher giving an example of each.

(6 marks)

c) Suppose N people want to communicate with $N - 1$ other people using symmetric key encryption. All communication between any two people, i and j is visible to all other people on this group N, and no other person in this group should be able to decode their communication. How many keys are required in the system as a whole? Now suppose public key encryption is used. How many keys are required in this case?

(6 marks)

d) 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)

(Question 2 continues on next page)...

...(Question 2 continued from previous page)

e) 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)

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

(12 marks)

[50 marks]

3.

a) Using examples distinguish between Circuit and Packet switching techniques highlighting the advantages and disadvantages of each approach. Explain how the Virtual Circuit approach provides the user with the best of both worlds.

(12 marks)

b) Calculate the baud rate for the given bit rate and type of modulation:

i. 3000bps, FSK

ii. 4000bps, QAM

iii. 36,000bps, 64-QAM

(9 marks)

c) Draw and graph the NRZ-I and Differential Manchester encoding schemes for the following data stream – 00110011. Explain why is it acceptable to use the Differential Manchester scheme for encoding bits over a LAN but not a WAN?

(9 marks)

d) Explain in detail how the Parity and Cyclic Redundancy Check (CRC) techniques can detect errors giving examples of each?

(10 marks)

e) With the aid of an example show how the "Credit Based" Sliding Window scheme employed in TCP networks can be used to de-couple flow control from the acknowledgement process.

(10 marks)

[50 marks]