Xi'an Jiaotong-Liverpool University
西交利物浦大学

MODULE CODE	EXAMINER	ACADEMIC UNIT	TEL
CAN201	Wenjun Fan	CAN	9134

1st **SEMESTER** ***2022/23 RESIT*** **EXAMINATION**

INTRODUCTION TO NETWORKING

TIME ALLOWED: ***2 Hours***

INSTRUCTIONS TO CANDIDATES

1. **This is a *closed-book* examination, *which is to be written without books or notes*.**
2. **Total marks available are 100.**
3. **This exam consists of *five* questions.**
4. **Answer all questions. There is NO penalty for providing a wrong answer.**
5. **Only English solutions are accepted. Answer should be written in the answer booklet(s) provided.**
6. **All materials must be returned to the exam invigilator upon completion of the exam. Failure to do so will be deemed academic misconduct and will be dealt with accordingly.**

Question 1 (20 points)

Browsing website through a browser is one of the daily used network operations.

1. Suppose the IP address for the associated URL is not cached in your local host and 2 DNS servers are visited before your host receives the IP address from DNS; the successive visits incur an RTT of RTT1,...,RTTn. Let RTT_0 denote the RTT between the local host and the server containing the object. Assuming zero transmission time of the object. Web page associated with the link contains exactly one object, consisting of a small amount of HTML text. How much time elapses from when the client clicks on the link until the client receives the object? (5 points)

2. Suppose your computer is connected to the Internet directly. You enter http://www.baidu.com/ in the address bar of your browser and open the homepage of the Baidu, which contains texts and images. Your browser completed many processes. Please briefly introduce all the related protocols in different layers of IP stack used in the mentioned webpage visiting. Tips: You should consider the provided network condition and the type of web address. (15 points)

Question 2 (20 points)

Due to the issues such as interferences and device errors, bit errors often occur in networking communication. In order to receive the correct information through the internet, error detection and correction methods are applied in some layers.

1. Suppose you have the following three 8-bit bytes: `01010011`, `11001100`, `00001100`. What is the 1s complement of the sum of these 8-bit bytes? (10 points)
2. With the 1s complement scheme, how does the receiver detect errors? Is it possible that a 1-bit error will go undetected? How about a 2-bit error? (10 points)

Question 3 (20 points)

Complete the following table using Dijkstra's algorithm. Compute the shortest path from node Z to all network nodes shown in Fig. 3. Note: Possible ties are broken in favor of the leftmost column.

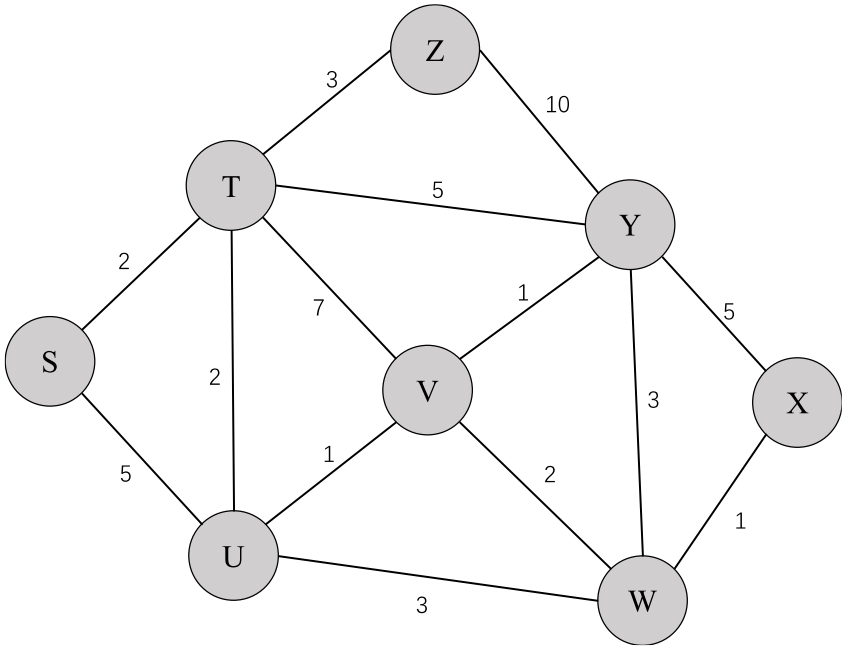

Fig. 3

Step	*N'*	*D(T), p(T)*	*D(Y), p(Y)*	*D(S), p(S)*	*D(V), p(V)*	*D(X), p(X)*	*D(U), p(U)*	*D(W), p(W)*
0	Z	3, Z	10, Z	∞	∞	∞	∞	∞
1	ZT	Done	8, T	5, T	10, T	∞	5, T	∞
2	ZTS		8, T	Done	10, T	∞	5, T	∞
3								
4								
5								
6								
7								

Question 4 (20 points)

Consider the following Figure 4, where several subnets are interconnected by two routers, i.e., R1 and R2.

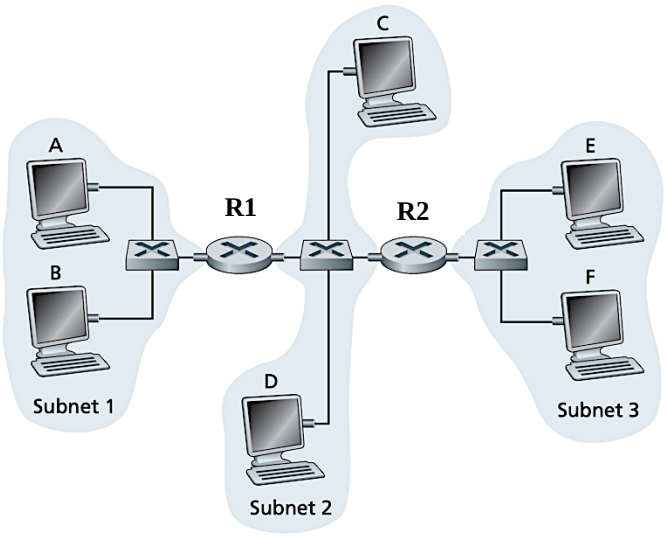

Fig. 4

1. Describe the difference between router and switch? (6 points)
2. If the interface of R2 in subnet 2 has an IP address 192.168.2.2, assign IP addresses to all the other interfaces in subnet 2, and also, show the network mask you used for those IP addresses. (6 points)
3. Assuming the interface of A has IP address 192.168.1.2, and the adapter for that interface has MAC address aa-aa-aa-aa-aa-aa; the interface of R1 in subnet 1 has IP address 192.168.1.1, and the adapter for that interface has MAC address 11-11-11-11-11-11. Now, consider sending an IP datagram from Host A to Host C. Suppose A has an empty ARP table, while R1 has the up-to-date ARP table and routing table respectively. Enumerate all the steps for sending the IP datagram. (8 points)

Question 5 (20 points)

Alice wants to communicate with Bob using symmetric-key cryptography (e.g., DES) with a session-key K_S. We learned how public-key cryptography (e.g., RSA) can be used to distribute a session key K_S between Alice and Bob. Suppose the private keys of Alice and Bob are k_A^- and k_B^-, while the public keys are K_A^+ and K_B^+. Also, we assume that Alice and Bob have got each other's public key through a certificate authority (CA).

1. Describe the main problem for using symmetric-key cryptography. (4 points)
2. Describe the main disadvantage of using public-key cryptography instead of symmetric-key cryptography for the whole communication. (4 points)
3. Draw a diagram to show how Alice would use the public-key cryptography to distribute the symmetric session-key K_S to Bob. (6 points)
4. Describe the problem when there is no CA distributing the public keys. (6 points)

----------END OF EXAM----------