Xi'an Jiaotong-Liverpool University

西交利物浦大学

Paper CODE	EXAMINER	DEPARTMENT	TEL
CAN201	Fei Cheng	CAN	9089

1st SEMESTER 2021/22 FINAL EXAMINATION

Undergraduate – Year 3

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. **There are 5 questions. Answer all questions.**
4. **Answer should be written in the answer booklet(s) provided.**
5. **Only English solutions are accepted.**
6. **All materials must be returned to the exam supervisor upon completion of the exam. Failure to do so will be deemed academic misconduct and will be dealt with accordingly**.

Question 1 (20 points)

Accessing web pages through a browser is one of the most commonly used network operations.

1. Suppose the IP address for the associated URL is not cached in your local host and n 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 through a router, and you enter https://www.xjtlu.edu.cn/ in the address bar of your browser and open the homepage of the university, which contains texts and images. 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. Please list error detection methods for all IP stack five layers. If no error detection method is used for some layers, please indicate them. (5 points)
2. Suppose you have the following three 16-bit bytes: `0101001101010011`, `1011010011001100`, `1001010000001100.` What is the 1s complement of the sum of these 16-bit bytes? (10 points)

3. Cyclic redundancy check (CRC) is also widely used in network communication. Please briefly introduce features of CRC. (5 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.

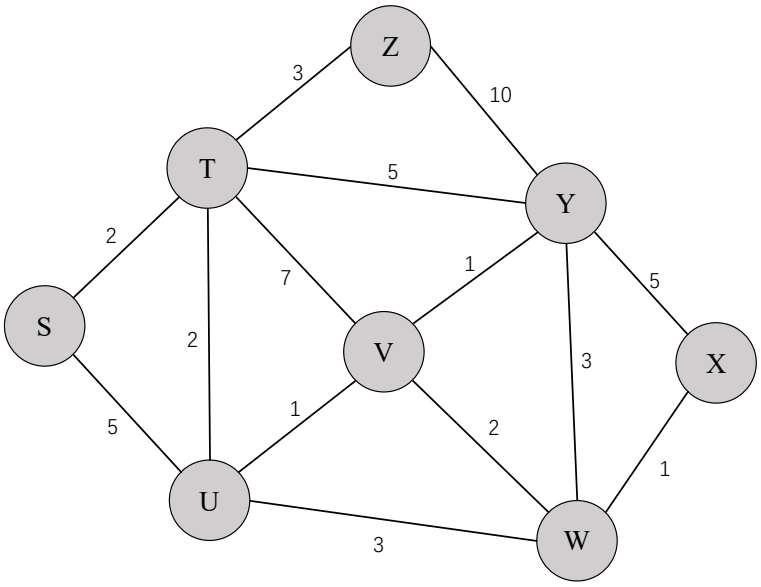

Fig. 3

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

Question 4 (20 points)

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

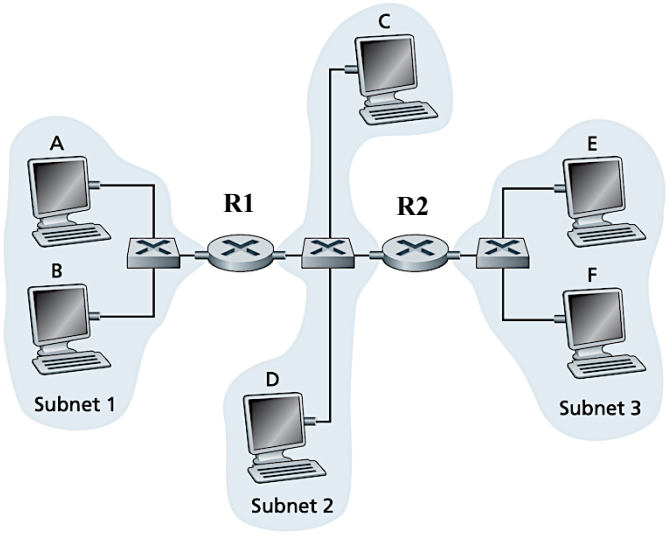

Fig. 4

1. If the interface of R1 in subnet 2 has an IP address 192.168.2.1, 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)
2. 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 E. Suppose A has an empty ARP table, while R1 and R2 both have up-to-date ARP tables and routing tables respectively. Enumerate all the steps for sending the IP datagram. (8 points)
3. If we replace the center switch (the device between R1 and R2) with a router R3, then how many subnets are in this figure? List them. (6 points)

Question 5 (20 points)

Alice wants to communicate with Bob using symmetric-key cryptography (e.g. DES) with a session-key K_S. In the lectures we learned how public-key cryptography (e.g. RSA) can be used to distribute a session key K_S from Alice to 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 trusty method.

1. What is the main advantage of first distributing a session key and then using symmetric-key cryptography rather than using public-key cryptography techniques for the whole communication? (5 points)
2. Draw a diagram that shows the message exchange between Alice and Bob which achieves this, i.e., using the public-key cryptography to distribute a symmetric session-key. (7 points)
3. Describe the difference between confidentiality and integrity (using digital signature) using public-key cryptography. (8 points)

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