Xi'an Jiaotong-Liverpool University

西交利物浦大學

Paper CODE	EXAMINER	DEPARTMENT	TEL
CAN201		CAN	

1st SEMESTER 2023/24 RESIT 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)

Fig. 1

Assume that we know the bottleneck link along the path from the server to the client is the first link with rate R_s bits/sec. Suppose we send a pair of packets back-to-back from the server to the client, and there is no other traffic on this path. Assume each packet of size L bits, and both links have the same propagation delay d_{prop}.

1. What is the packet inter-arrival time at the destination? That is, how much time elapses from when the last bit of the first packet arrives until the last bit of the second packet arrives? (5 points) $\frac{L}{R_s}$

$\frac{2L}{R_s} + d_{prop} < \frac{L}{R_s} + d_{prop} + \frac{L}{R_c}$

2. Now suppose that the second link is the bottleneck link (i.e., $R_c < R_s$). Is it possible that the second packet queues at the input queue of the second link? Explain. (7 points) Yes.
3. Now suppose that the server sends the second packet T seconds after sending the first packet ($R_c < R_s$). How large must T be to ensure no queuing before the second link? Explain. (8 points)

$\frac{2L}{R_s} + d_{prop} + T = \frac{L}{R_s} + d_{prop} + \frac{L}{R_c} \Rightarrow T = \frac{L}{R_c} - \frac{L}{R_s}$

Question 2 (20 points)

The Hyper-Text Transfer Protocol (HTTP), one of the mostly used application-layer protocol, is at the heart of the Web.

1. Decide whether the following statements related to HTTP are correct (True / False):

True a) The server side normally doesn't maintain the state data. (2 points)

False b) The client side should have Permanent IP address. (2 points)

True c) Two distinct Web pages (for example, https://sat.xjtlu.edu.cn/research.html and https://sat.xjtlu.edu.cn/staff.html) can be sent over the same persistent connection. (2 points)

False d) HTTP 1.1 has "MODIFY" mothed. (2 points)

False e) The port number used by HTTP can only be 80. (2 points)

2. Consider the following string of ASCII characters that were captured by Wireshark when the browser sent an HTTP GET message (i.e., this is the actual content of an HTTP GET message). The characters <cr><lf> are carriage return and line-feed characters. Answer the following questions, indicating where in the HTTP GET message below you find the answer.

```
GET /sat/index.html HTTP/1.1<cr><lf>Host:
sat.xjtlu.edu.cn<cr><lf>User-Agent: Mozilla/5.0 (Windows;U; Windows NT
7.1; en-US; rv:1.7.2) Gecko/20040804 Netscape/7.2 (ax) <cr><lf>Accept:
text/xml, application/xml, application/xhtml+xml, text /html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5 <cr><lf>Accept-Language: en-
us,en;q=0.5<cr><lf>Accept- Encoding: zip,deflate<cr><lf>Accept-
Charset: ISO -8859-1,utf-8;q=0.7,*;q=0.7<cr><lf>Keep-Alive:
300<cr><lf>Connection:keep-alive<cr><lf><cr><lf>
```

a) What is the URL of the document requested by the browser? (3 points) ~~/sat/index.html~~

b) What version of HTTP is the browser running? (3 points) HTTP 1.1

c) How does the browser get IP address? (4 points) DNS

Question 3 (20 points)

Complete the following table using Dijkstra's algorithm. Compute the shortest path from node A to all network nodes shown in Fig. 2. Note: Possible ties are broken in favor of the leftmost column.

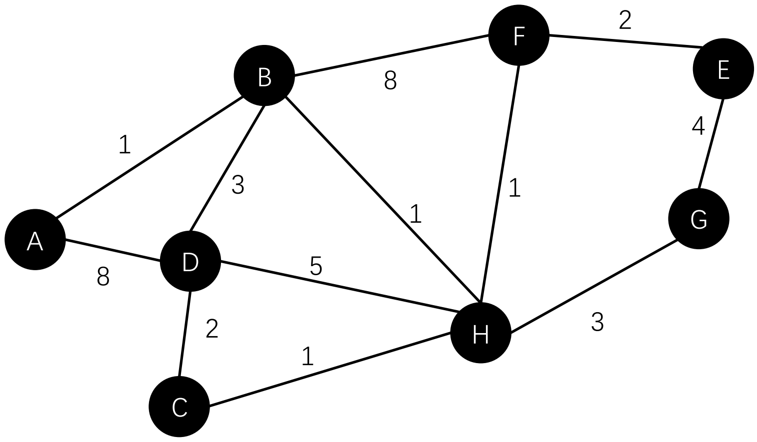

Fig. 2

Step	*N'*	*D(B), p(B)*	*D(C), p(C)*	*D(D), p(D)*	*D(E), p(E)*	*D(F), p(F)*	*D(G), p(G)*	*D(H), p(H)*
0	A	1, A	∞	8, A	∞	∞	∞	∞
1	AB	Done	∞	4, B	∞	9, B	∞	2, B
2	ABH		3, H	4, B	∞	~~3, B~~ 3, H	5, H	Done
3	ABCH		Done	4, B	∞	3, H	5, H	
4	ABCHF			4, B	5, F	Done	5, H	
5	ABCHFD			Done	5, F		5, H	
6	ABCDEFH				Done		5, H	
7	ABCDEFGH						Done	

Question 4 (20 points)

Consider the following Fig.3, where several subnets are interconnected.

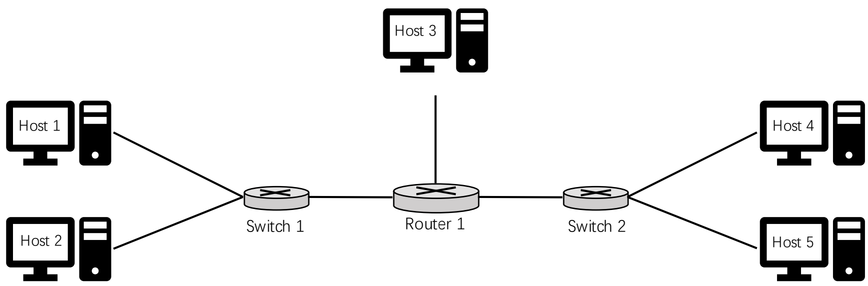

Fig. 3.

1. How many subnets in this network? List them in terms of network interfaces. (8 points)
2. If the interface of Router 1 linked with Host 3 has an IP address 10.0.2.1/25, which would be the largest IP address that can be assigned to the interface of Host 3 and the corresponding network mask? (4 points)
3. Assuming the interface of Host 1 has an IP address 10.0.1.2, and the adapter for that interface has a MAC address aa-aa-aa-aa-aa-aa; the interface of Router 1 lined with Switch 1 has an IP address 10.0.1.1, and the adapter for that interface has a MAC address 11-11-11-11-11-11. Now, consider sending an IP datagram from Host 1 to Host 5. Suppose Host 1 has an empty ARP table, while Router 1 has the up-to-date ARP table and routing table respectively. Describe all the steps to succeed in sending the IP datagram. (8 points)

1. 3.
Host1 and Host 2
Host 3
Host 4 and Host 5.

2. ~~10.0.2.127~~ 10.0.2.126
255.255.255.128

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)

一般用k_A^-加密用于数字签名.

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

3. Alice Bob.

$k_s \xrightarrow{k_A^-} k_A^-(k_s) \xrightarrow{k_B^+} k_B^+(k_A^-(k_s)) \xrightarrow{k_B^-} k_A^-(k_s) \xrightarrow{k_A^+} k_s$

Alice Bob

$k_s \xrightarrow{k_B^+} k_B^+(k_s) \longrightarrow k_B^+(k_s) \xrightarrow{k_B^-} k_s$

1. key distribution. How to share the key securely before communication begins.

2. Computational efficiency. The cryptography algorithm will cost too much time, power and computational resources.

4. There will be Man-in-the-Middle Attack. Bob and Alice don't know whether the public key is belong to others or not.