Question 1 (20 points)

In packet-switched networks, the source host segments long application-layer messages (e.g., an image or a music file) into smaller packets and sends the packets into the network. The receiver then reassembles the packets back into the original message. We refer to this process as message segmentation. Fig. 1 illustrates the end-to-end transport of a message with and without message segmentation respectively. Consider a message that is 12 $\times 10^6$ bits long is to be sent from the source to the destination in Fig 1. Suppose each link in the figure is 2 Mbps. Ignore propagation, queuing, and processing delays.

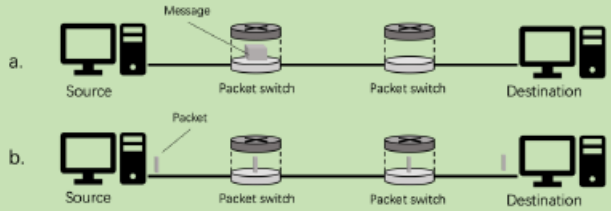

Figure 1. End-to-end message transport: (a) without message segmentation; (b) with message segmentation.

1. Consider sending the message from the source to the destination without message segmentation. How long does it take to move the message from the source to the destination? Keeping in mind that each switch uses store-and-forward packet switching. (3 points)
2. Now suppose that the message is segmented into 1,200 packets, with each packet being 10,000 bits long. How long does it take to move the first packet from the source to the first (left-most) switch? When the first packet is being sent from the first (left-most) switch to the second switch, the second packet is being sent from the source to the first switch. So, assuming the timestamps start from the source sends out the first packet, at what time will the second packet be fully received by the first switch? (4 points)

Q1 Answer:

(1)

Time to send message from source host to first packet switch = 12 X 10^6/2Mbps = 6sec

With store-and-forward switching, the total time to move message from source host to destination host = 6sec X 3 hop=18sec

(2)

Time to send 1st packet from source host to first packet switch = (1*10^4) / (2*10^6) sec=5m sec=5*10 ^ (-3) sec

Time at which 2nd packet is received at the first switch = time at which 1st packet is received at the second switch = 2*5msec=10 msec=10 ^ (-2) sec

3. How long does it take to move the file from the source to the destination when message segmentation is used? (3 points)
4. In addition to reducing delay, what are the reasons for using message segmentation? (5 points)
5. Discuss the drawbacks of message segmentation. (5 points)

(3)
Time at which 1st packet is received at the destination host = 5 msec*3 hops=15 m sec.
After this, every 5msec one packet will be received; thus, time at which last (1,200th) packet is received = 15 msec+(1200-1) * 5msec=6010msec=6.01sec.
(4)
1. Easy to detect errors and retransmit
2.Unsegmented packets tend to make the router cache inadequate and lead to packet loss
(5)
1. Packets have to be put in sequence at the destination.
2. Header size is usually the same for all packets regardless of their size.

Question 2 (20 points)

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 /can201/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>*

1. What is the URL of the document requested by the browser? (3 points)
2. Which version of HTTP is the browser running? (2 points)
3. Does the browser request a non-persistent or a persistent connection? (3 points)
4. What is the IP address of the client host where the browser is running? How does the browser get the web server's IP address? (7 points)
5. What type of browser initiates this message? Why is the browser type needed in an HTTP request message? (5 points)

Q2 Answer:

(1) URL: http://sat.xjtlu.edu.cn/can201/index.html
(2) The browser is running HTTP version 1.1
(3) The browser is requesting a persistent connection, as indicated by the Connection: 'keep-alive'.
(4) This information is not contained in an HTTP message anywhere. You need information from the IP datagrams (that carried the TCP segment that carried the HTTP GET request) to answer this question.
(5) Mozilla/5.0. The browser type information is needed by the server to send different versions of the same object to different types of browsers.

Note: The Host: field indicates the server's name and /can201/index.html indicates the file name.

Question 3 (20 points)

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

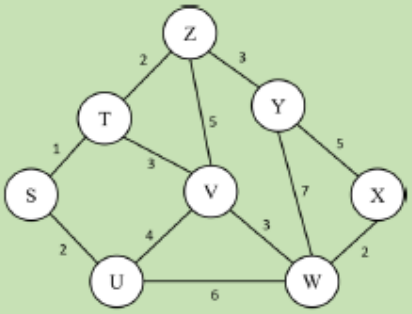

Figure 3. A network topology for performing Dijkstra's algorithm.

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

Q3 Answer:

Step	*N'*	*D(T), p(T)*	*D(U), p(U)*	*D(Z), p(Z)*	*D(V), p(V)*	*D(Y), p(Y)*	*D(W), p(W)*	*D(X), p(X)*
0	S	1, S	2, S	∞	∞	∞	∞	∞
1	ST	Done	2, S	3, T	4, T	∞	∞	∞
2	STU		Done	3, T	4, T	∞	8, U	∞
3	STUZ			Done	4.T	6.Z	8.U	∞
4	STUZV				Done	6.Z	7.V	∞
5	STUZVY					Done	7.V	11.Y
6	STUZVYW						Done	9.W
7	STUZVYWX							Done

Question 4 (20 points)

Consider the following Fig.4, where several subnets are interconnected.

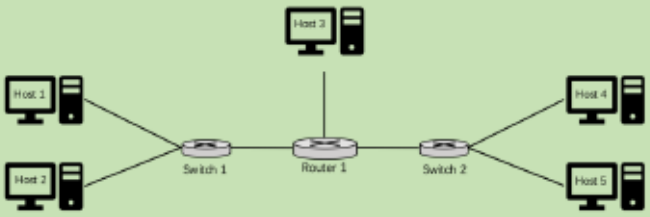

Figure 4. One computer network example consists of router, switches and hosts.

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)

Q4 Answer:

(1)

There are three subnets in this network.

Network interface Switch 1 corresponds to Host 1 and Host 2;

Network interface Router 1 corresponds to Host 3;

Network interface Switch 2 corresponds to Host 4 and Host 5.

(2)

The IP address in hexadecimal is 10.0.2.1/25, which is converted to 0000 1010. 0000 0000. 0000 0010. 0000 0001/25. [0000 1010. 0000 0000. 0000 0010. 0] is the network number, and [000 0001] is the host number. So the maximum IP address that can be assigned in hexadecimal form is 10.0.2.126. The corresponding netmask binary form is 1111 1111. 1111 1111. 1111 1111. 1100 0000. The corresponding netmask hexadecimal form is 255 255. 255. 192.

(3)

Step 1: ARP table is empty; it sends an ARP request message to the broadcast address of subnet 1.

Step 2. R1 receives the ARP request message and checks its ARP table to see if it has an entry for the IP address of Host 1. Since it does not have an entry, it sends an ARP reply message to Host 1, providing its MAC address (11-11-11-11-11-11).

Step 3. Host 1 receives the ARP reply message and updates its ARP table with the MAC

address of R1 in subnet 1 (11-11-11-11-11-11).
Step 4. Host 1 constructs an IP datagram with the destination IP address of Host 5 and the MAC address of R1 in subnet 1 (11-11-11-11-11-11) as the destination MAC address.
Host 1 sends the IP datagram to R1 in subnet 1.
Step 5. R1 receives the IP datagram and checks its routing table to see if it has an entry for the destination IP address of Host 5. Since it does, it sends the IP datagram to R2 using its MAC address.
Step 6. R2 receives the IP datagram and checks its routing table to see if it has an entry for the destination IP address of Host 5.
Step 7. R2 sends the IP datagram to Host 5 using its MAC address.
Step 8. Host 5 receives the IP datagram and processes it.

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)

Q5 Answer:

(1)
The main problem with symmetric key encryption is that it can be attacked by the middleman because the middleman is constantly playing another peer and knows all the information, so all public and private keys can be obtained.
(2)
i. The speed of encryption and decryption of public key cryptography is much slower than that of symmetric cryptography. Then the calculation cost is very obvious: the public key can be used for any system it exposes (the public key system on the Internet, such as exposing the public key to the entire Internet). In order to compensate, the public key and private key must be very large to ensure a stronger encryption level
ii. Compared with designing symmetric cryptographic algorithms, designing public key cryptographic algorithms has greater restrictions and lower freedom, because public key can provide more information to attack algorithms.
(3) Alice -> Bob: Send public key KA+ Bob -> Alice: Send public key KB+
Alice -> Bob: Encrypt KS using KB+ and send Bob -> Alice: Decrypt KS using kB-
(4) If there is no authentication center, there may be man-in-the-middle attacks. (AB 之间的信息无限被中间人 C 获取，A 给 C key, C 给 B 假 key, C 用 key 解密信息后把假信息给 B)