**Xi’an Jiaotong-Liverpool University**



|  |  |  |  |
| --- | --- | --- | --- |
| **Paper CODE** | **EXAMINER** | **DEPARTMENT** | **TEL** |
| **CAN201** |  | **CAN** |  |

**1st SEMESTER 2023/24 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**.

**CAN201 (1st SEMESTER 2023/24 FINAL EXAMINATION) Page 1 of 5**

**Xi’an Jiaotong-Liverpool University**

**Question 1 (20 points)**



|  |
| --- |
|  |

Fig 1. Locations of two hosts.

Suppose two hosts, located in Kunming and Shanghai, are separated by 2,000 kilometers, and are connected by a direct link of *R* = 2 Mbps. Suppose the propagation speed over the link is 2.5 . 108 meters/sec. (In this question, 1Mb=1,000Kb=1,000,000b)

1. Calculate the bandwidth-delay product: *R. dprop*. (5 points)

The bandwidth-delay product can be calculated by multiplying the bandwidth (R = 2 Mbps = 2,000,000 bits/sec) by the propagation delay (dprop = distance/speed = 2,000,000 meters / (2.5 × 10⁸ meters/sec) = 0.008 sec). Therefore, R · dprop = 2,000,000 × 0.008 = 16,000 bits.

1. Consider sending a file of 100,000 bits from the host in Kunming to the host in Shanghai. Suppose the file is sent continuously as one large image. What is the maximum number of bits that will be in the link at any given time? (5 points)

The maximum number of bits in the link at any given time is equal to the bandwidth-delay product, which we calculated as 16,000 bits. This represents the maximum number of bits that can be "in flight" on the link at any moment.

1. Provide a definition of the “*bandwidth-delay product*”. (5 points)

The bandwidth-delay product is a measure that represents the maximum amount of data that can be in transit through a network path at any given time. It is calculated by multiplying the link's bandwidth by its propagation delay, indicating the network's data capacity in transit.

1. What is the width (in meters) of a bit in the link? (2 points)

The width of a bit can be calculated by dividing the total distance by the number of bits in the link: 2,000,000 meters / 16,000 bits = 125 meters per bit.

1. Derive a general expression for the width of a bit in terms of the propagation speed *s*, the transmission rate *R*, and the length of the link *m*. (3 points)

The width of a bit can be expressed as: bit width = m/(R·dprop) = m/(R·(m/s)) = s/R, where m is the link length, s is the propagation speed, and R is the transmission rate.

**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):

a) A user requests a Web page that consists of some text and 4 images. For this page, the client will send one request message and receive 5 response messages. (2 points)

True. When a user requests a webpage containing text and 4 images, the browser will indeed send one initial HTTP request for the HTML page and then receive 5 separate responses (one for the HTML page and one for each of the four images). This is because each image is a separate resource that requires its own HTTP response.

b) Two distinct Web pages (for example, <https://www.suda.edu.cn/research.html> and

<https://sat.xjtlu.edu.cn/staff.html>) can be sent over the same persistent connection. (2 points)

True. Different web pages can indeed be sent over the same persistent HTTP connection. This is one of the key features of HTTP/1.1 and later versions, where multiple requests and responses can be handled over a single TCP connection, improving efficiency.

c) With non-persistent connections between browser and origin server, it is possible for a single TCP segment to carry two distinct HTTP request messages. (2 points)

False. With non-persistent connections, each TCP connection is used for exactly one request-response pair and then closed. It's not possible for a single TCP segment to carry multiple HTTP requests in non-persistent connections.

d) HTTP response messages never have an empty message body. (2 points)

False. HTTP response messages can have empty message bodies. This is common in responses to HEAD requests, some responses to DELETE requests, and certain status codes like 204 (No Content).

e) The HTTP protocol can only be used for webpages. (2 points)

False. HTTP protocol is not limited to webpages. It can be used for various types of data transfer including APIs, file downloads, streaming media, and other types of data transfer. It's a general-purpose application layer protocol.

**CAN201 (1st SEMESTER 2023/24 FINAL EXAMINATION) Page 2 of 5**

**Xi’an Jiaotong-Liverpool University**

2. The text below shows the reply sent from the server in response to an HTTP GET message. Answer the following questions, indicating where in the message below you find the answer.

|  |
| --- |
| HTTP/1.1 200 OK<cr><lf>Date: Tue, 07 Mar 2023  12:39:45GMT+8<cr><lf>Server: Apache/4.0.52<cr><lf>Last-Modified: Sat,  10 Dec 2022 18:27:46 GMT+8<cr><lf>Accept-Ranges: bytes<cr><lf>Content-  Length: 3874<cr><lf>Keep-Alive: timeout=max=100<cr><lf>Connection:  Keep-Alive<cr><lf>Content-Type: text/html; charset=utf-  8<cr><lf><cr><lf><!doctype html public ”-//w3c//dtd html 4.0  transitional//en”><lf><html><lf><head><lf> <meta http-equiv=”Content-  Type”content=”text/html; charset=utf-8”><lf> <meta name=”GENERATOR”  content=”Mozilla/4.79 [en] (Windows NT 5.0; U) Netscape]”><lf>  <title>Unleash Yourselves and Dare to be Rationally  Unconventional</title><lf></head><lf><body><H1>Unleash Yourselves and  Dare to be Rationally Unconventional</H1><p>Last Modify Date: 1 Dec  2022</p> ...<much more document text following here (not shown)> |

1. Was the server able to successfully find the document or not? What time was the document reply provided? (2 points)

The server successfully found the document (indicated by "200 OK" status code) and the reply was provided at 12:39:45 GMT+8 on Tuesday, March 7, 2023.

1. When was the document last modified? (2 points)

The document was last modified on Saturday, December 10, 2022, at 18:27:46 GMT+8, as shown in the "Last-Modified" header.

1. How many bytes are there in the document being returned? (2 points)

The document being returned is 3874 bytes, as indicated by the "Content-Length" header.

1. What are the first 9 bytes of the document being returned? (2 points)

The first 9 bytes of the document are "<!doctype", which begins the HTML document type declaration.

1. Did the server agree to a persistent connection? (2 points)

Yes, the server did agree to a persistent connection, as indicated by the "Connection: Keep-Alive" header and the presence of a "Keep-Alive" timeout parameter.

**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.

1

B

8

A

D

3

1

2

F

1

C

2

H

E

4

2

G

3



Fig. 2

**CAN201 (1st SEMESTER 2023/24 FINAL EXAMINATION) Page 3 of 5**



**Xi’an Jiaotong-Liverpool University**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***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 | 8, A | ∞ | 3, A | ∞ | ∞ | ∞ | ∞ |
| 1 | AD | 8, A | 4, D | Done | ∞ | ∞ | ∞ | 5, D |
| 2 | ADC | 8, A | Done |  | ∞ | ∞ | ∞ | 5, D |
| 3 | ADCH | 8,A |  |  | ∞ | 6,h | 8,h | done |
| 4 | ADCHF | 7,A |  |  | 8,F | done | 8,h |  |
| 5 | ADCHFB | done |  |  | 8,F |  | 8,h |  |
| 6 | ADCHFBE |  |  |  | done |  | 8,h |  |
| 7 | ADCHFBEH |  |  |  |  |  |  | done |

**Question 4 (20 points)**

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

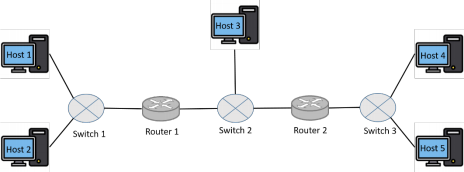


Fig. 3

1. Please list all the subnets in this network? Hint: list them in terms of network interfaces. (9 points)

In this interconnected network topology, we can identify five distinct subnets based on the network interfaces. The first subnet encompasses Host 1, Host 2, and Switch 1, forming a local network segment. The second subnet exists between Switch 1 and Router 1, creating a point-to-point connection. Moving further, the third subnet connects Router 1 to Switch 2, while the fourth subnet links Switch 2 to Router 2. Finally, the fifth subnet includes Switch 3 along with Host 4 and Host 5, completing the network topology. Each subnet represents a separate broadcast domain, effectively segmenting the network traffic.

1. If Router 1 is removed, and Switch 1 and Switch 2 are linked directly, then there are how many subnets left? Explain what they are. (5 points)

The first subnet would include Host 1, Host 2, Host 3, Switch 1, and Switch 2, all becoming part of the same broadcast domain.

The second subnet would include Switch 3, Host 4, and Host 5, separated by Router 2.

1. 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 3. 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. (6 points)

The process of sending an IP datagram from Host 1 to Host 3 involves several key steps. Initially, Host 1 (IP: 10.0.1.2) determines that Host 3 is on a different subnet and identifies Router 1 (IP: 10.0.1.1) as its default gateway. Since Host 1's ARP table is empty, it broadcasts an ARP request to obtain Router 1's MAC address. Router 1 responds with its MAC address (11-11-11-11-11-11), allowing Host 1 to encapsulate the IP datagram with the correct MAC addressing information. The datagram is then sent to Router 1, which forwards it through the appropriate interface toward Host 3.

**CAN201 (1st SEMESTER 2023/24 FINAL EXAMINATION) Page 4 of 5**



**Xi’an Jiaotong-Liverpool University**

**Question 5 (20 points)**

Alice wants to communicate with Bob. Assuming they are using public-key cryptography (e.g., RSA) directly, and so Alice has her public key KA+ and private key kA- while Bob has his public key KB+ and private key kB- . Also, we assume that Alice and Bob have got each other’s public key through a

certificate authority (CA). With the above, Alice now would like to send a message M to Bob.

1. If Alice would like to ensure the confidentiality of this message transmission. That means only Bob can decrypt the cipher-text of M. Please draw a diagram to show how Alice would encrypt the message M. (6 points)

To ensure message confidentiality when Alice sends a message M to Bob, she needs to use Bob's public key (KB+) to encrypt the message. The process works as follows: Alice first obtains Bob's public key KB+ through the Certificate Authority (CA), which ensures the authenticity of the key. She then uses this public key to encrypt her message M, creating the cipher-text C = E(KB+, M). When Bob receives the encrypted message, only he can decrypt it using his private key KB-, as the encryption is asymmetric. This ensures that even if an attacker intercepts the message, they cannot read its contents without Bob's private key.

1. If Alice would like to ensure the integrity of this message transmission. That means Bob can verify that M was sent by Alice and M was not altered during transmission. Please draw a diagram to show how Alice would transmit the message M. (Hint: you can use H(x) to express the hash function). (6 points)

To ensure message integrity, Alice needs to create a digital signature of the message. The process involves the following steps: First, Alice generates a hash of the message M using a hash function, represented as H(M). She then encrypts this hash value using her private key KA-, creating a digital signature S = E(KA-, H(M)). The complete transmission includes both the original message M and the signature S. When Bob receives these, he can verify the integrity by decrypting the signature using Alice's public key KA+ and comparing the resulting hash with his own calculation of H(M). If they match, it confirms both the message's integrity and Alice's authorship.

1. Now if Alice and Bob want to share a secret key KS and will use the secret key for encrypting the message. Please use a diagram to show how Alice would use the public-key cryptography to transmit KS to Bob whereby both confidentiality and integrity should be guaranteed. (8 points)

To securely transmit a secret key KS while ensuring both confidentiality and integrity, Alice needs to combine both encryption and digital signature techniques. The process works as follows: First, Alice encrypts the secret key KS using Bob's public key KB+ to ensure confidentiality: C = E(KB+, KS). Then, she creates a digital signature of the encrypted key using her private key KA-: S = E(KA-, H(C)). Alice sends both C and S to Bob. Upon receipt, Bob first verifies the signature using Alice's public key KA+ to ensure integrity and authenticity. If verified, he then uses his private key KB- to decrypt C and obtain KS. This process ensures that only Bob can access the secret key while also verifying it came from Alice.

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

**CAN201 (1st SEMESTER 2023/24 FINAL EXAMINATION) Page 5 of 5**