

A Previous Final Examination

May 5, 2005

Print Your Name:

Read the following now.

- Write your name on *all* pages.
- You have 120 minutes to earn up to 180 points.
- For problems involving calculation, show intermediate steps to ensure partial credit (that is, in case your answers are incorrect).
- Brief and concise answers will be favored in grading.
- Write down your answers clearly. I reserve the right to take off points due to poor writing or English structures.
- One blank page is provided at the end for your convenience.

STOP! Do not turn to the next page until instructed to do so.

1. (35pt in total) Physical and Data Link Layers

(a) (7pt) Give the delay modulation encoding of the bit stream 0, 1, 0, 1, 0, 0, 0, 1. The signal starts with a low value.

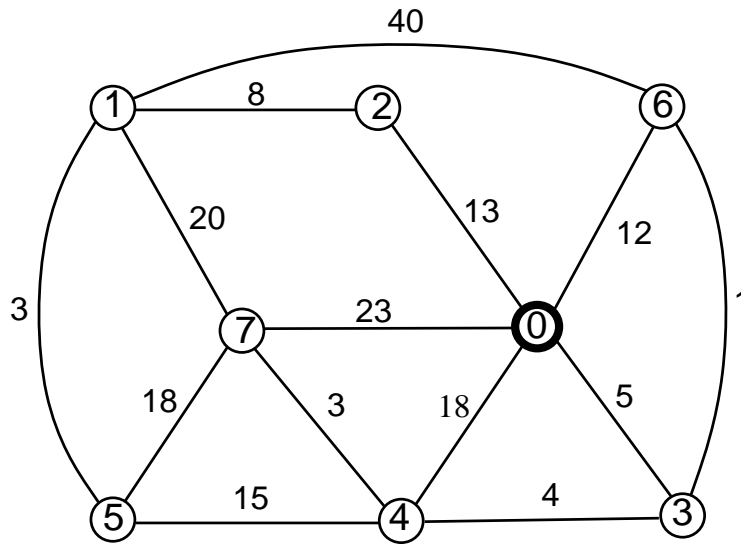
(b) (8pt) Describe the purpose of medium access control in two sentences.

- (c) Consider a communication link with bandwidth $H=5,000$ Hz and $S/N=30$ dB.
- i. (10pt) Calculate its maximum data rate according Shannon's theorem.

- ii. (10pt) Calculate its maximum data rate according to Nyquist's theorem with a QAM encoding that uses 4 phase shifts and 4 amplitudes.

2. (40pt total) Routing

- (a) (20pt) Perform Dijkstra's algorithm on the network below, using node 0 as the starting point. Give the contents of the `dist` and `nhop` arrays after the completion of 4 iterations.



(b) (16pt) The distance vector of a router G is given below:

$$(A, 1, 1), (B, 0, 1), (C, 0, 4), (E, 2, 1), (F, 0, 6), (G, -1, 0), (H, 0, 7), (I, 1, 3))$$

where an entry (Y, p, c) indicates X reaches Y through port p in c hops. X receives via port **1** a vector

$$((A, -1, 0), (B, 0, 2), (C, 0, 1), (D, 3, 1), (E, 2, 1), (F, 3, 3), (G, 1, 1), (H, 4, 1), (I, 4, 6))$$

Answer the following questions.

- i. Give the vector of X after processing the incoming vector. Please show entries in the alphabetic order of routers.

ii. (4pt) Circle the neighboring routers of G .

A B C D E F G H I

(c) (40pt in total) Internet Architecture

(a) (8pt) Describe the purpose of the ARP protocol and how it works.

(b) (8pt) Give 4 items in the bootstrap configurations of an Internet host.

(c) (8pt) Explain the purpose of the DHCP protocol and how it works.

(d) (6pt) A TCP segment is *entering* a private network that uses a gateway PC to perform IP masquerading. Circle the field(s) in TCP/IP headers of the packet that has/have to be updated by the gateway PC.

- source IP address
- source port number
- destination IP address
- destination port number
- window size advertisement
- IP header checksum

- (e) (5pt) Circle correct statement(s) about Internet data delivery.
- Datagrams may be lost in transit.
 - Datagrams may be fragmented in transit.
 - Datagrams suffering transmission errors must be discarded by routers.
 - Segments of a TCP connection always arrive at the destination in the right order.
 - Segments of a TCP connection always use the same path to reach destination.
- (f) (5pt) Circle the functions that are performed by the network layer in the Internet model.
- DNS
 - fragmentation
 - flow control
 - congestion control
 - routing
 - data encryption

(d) (35pt total) Transmission Control Protocol

(a) In this question, you use the RTT estimation that accounts for sample variations, to process three RTT samples: 150, 200 and 210 in that order. Initial $RTT=200$ and initial $DEV=50$. Answer the following questions.

i. (3pt) Show the initial Timeout (that is, the value before processing the three samples.)

ii. (12pt) Give the RTT and Timeout after processing the three samples.

(b) (15pt) Show the acknowledgments in response to the following segments, arriving in that order:

- Seg(2500,500,with SYN=1)
- Seg(4000,200)
- Seg(4200,300)
- Seg(3000,1000)
- Seg(4500,100, with FIN=1)

where Seg(X, Y) denotes a segment with sequence number X and Y bytes of data.

(c) (5pt) Circle correct statement(s) of TCP connections.

- initial sequence number is 0
- initial window size is 1 (segment)
- segments of a connection follows the same path
- segments of a connection arrive at the destination “machine” in the right order
- segments of a connection arrive at the destination “application” in the right order

(e) (30pt) Security

Consider the following remote login procedure:

Step 1. the client asks the user to enter username and password.

Step 2. the client asks the server to provide an IDEA key.

Step 3. the server chooses a random IDEA key k and computes $k' = \text{RSA_encrypt}(k, \text{private_key}(\text{server}))$.

Step 4. the server sends k' to the client.

Step 5. the client computes the digest of the password: $D = \text{MD5}(\text{password})$

Step 6. the client computes $M' = \text{IDEA_encrypt}(M, k)$, where $M = \text{username} \parallel D$.

Step 7. the client computes $k'' = \text{RSA_encrypt}(k, \text{private_key}(\text{client}))$.

Step 8. the client sends (M', k'') to the server.

Answer the following questions.

(a) (8pt) Give the computation/equation the server uses to recover the plaintext request M .

(b) (8pt) Give the computation/equation the server uses to authenticate the message, that is, to ensure it comes from the client machine.

- (c) (8pt) Give the computation/equation the server uses to check the correctness of the password. We assume that the server maintains a file of usernames and passwords. Use the notation $\text{Passwd}(x)$ to refer to the password of user x stored in that file.

- (d) (6pt) Suppose a third part intercepts the message (M', k'') . Argue that a replay of the message will not allow the third party to login successfully.

Name:

13

This page is intentionally left blank.