Department of Computer Science and Engineering

COSC 4213: Computer Networks II (Fall 2005)

Instructor: N. Vlajic

Final Examination

December 13, 2005

Instructions:

- Examination time: 180 min.
- Print your name and CS student number in the space provided below.
- This examination is closed book and closed notes. Use of calculators is allowed.
- There are 8 questions. The points for each question are given in square brackets, next to the question title. The overall maximum score is 100.
- Answer each question in the space provided. If you need to continue an answer onto the back of a page, clearly indicate that and label the continuation with the question number.

FIRST NAME: _____

LAST NAME: _____

STUDENT #: _____

Question	Points
1	/ 10
2	/ 10
3	/ 10
4	/ 20
5	/ 15
6	/ 15
7	/ 8
8	/ 12
Total	/ 100

1. Multiple Choice, True/False [10 points]

1.1) Multiple choice questions – each question is worth [1 point].

(a) The loopback IP address is used to send a packet from _____ to _____ .

(a) host; all other hosts in the LAN
(b) router; all other routers in the LAN
(c) host; a specific host
(d) host; itself

(b) Which IP option is used if exactly four specific routers are to handle an IP datagram?

(a) record route
(b) strict source route
(c) loose source route
(d) timestamp

(c) A system uses group-shared trees for multicasting. If there are 100 sources and 5 groups, there is a maximum of _____ different trees.

(a) 5
(b) 20
(c) 100
(d) 500

(d) The symptom of the TCP Silly Window Syndrome is:

(a) TCP segments receive multiple acknowledgments.
(b) TCP segments carry only a small amount of data.
(c) TCP segments are never acknowledged.
(d) Every TCP segment is resent exactly once.

(e) Which of the following is true for Random Early Detection (RED) algorithm?

(a) RED is tolerant of bursts because it never drops consecutive packets from the same flow.

(b) RED always drops packets, with probability 1, when the router's queue length is greater than the minimum threshold value.

(c) RED attempts to 'desynchronize' competing TCP sources by causing them to lose packets at different times.

(d) If two flows, one TCP and one UDP, share a RED router, the RED algorithm will ensure that both flows receive an identical share of the outgoing links.

1.2) True/false questions – each question is worth [1 point].

(a) Consider a router with 3 interfaces. Suppose all three interfaces use class C addresses. The IP addresses of the three interfaces have the same first 24 bits.

TRUE

FALSE

(b) Suppose host A sends host B a TCP segment encapsulated in an IP datagram. When the network layer in host B receives the datagram and checks its header, it knows that the content of the datagram should be passed to the TCP layer (i.e. TCP module).

TRUE

FALSE

(c) An ICMP Echo Request and Reply can be used to determine if we have connectivity between a client and a server at the Application Layer level?

TRUE

FALSE

(d) An application implemented on top of UDP may provide reliable communication.

TRUE

FALSE

(e) Two distinct web pages from the same server can be sent over the same persistent HTTP connection.

TRUE

FALSE

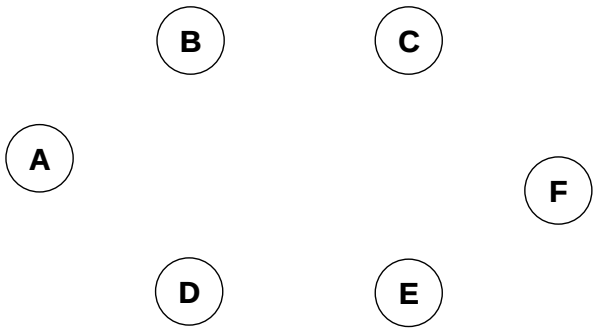
2. Routing [10 points]

You are observing Link State Packets (LSPs) entering a router.

Link State Packets:

	Router A		Router B		Router C		Router D		Router E		Router F	
Links	C	1	A	2	A	1	B	5	A	3	C	8
Links	B	2	D	5	F	8	E	3	F	1	E	1
Links	E	3	-	-	-	-	F	1	D	3	D	1

2.1) [3 points] Based on the above LSPs, construct the topology of the network in question.



2.2) [7 points] Use the Dijkstra's shortest path algorithm to determine the shortest path from A to D. In your answer, clearly specify the shortest path between A and D and its respective cost!

3. IP Addressing and Subnetting [10 points]

3.1) [4 points] Assume classful IP addressing.

A router receives a packet with *destination host address* of 190.240.7.91. Show how the router finds the address of the corresponding destination network to route the given packet. Explain your work!

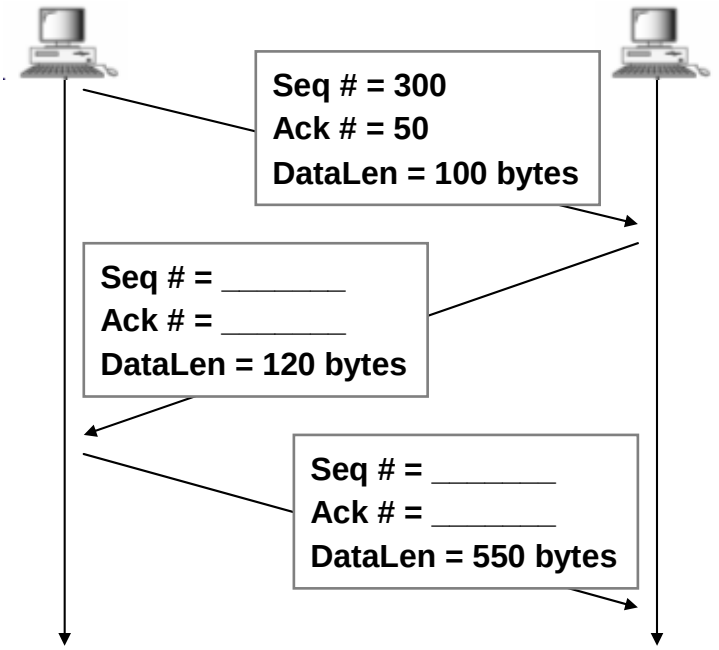
3.2) [6 points] Assume classless IP addressing.

In a network which has been allocated the address of 165.65.y.z and a subnet mask of 255.255.240.0, the use of subnet/host IDs with all 1's and all 0's is NOT permitted.

What will be the first and last assignable addresses on the 3rd useable subnet of such a network? Explain your work!

4. TCP Potpourri [20 points]

4.1) [4 points] For the TCP segments indicated below, specify the omitted values. Assume the packets are transmitted over a reliable link with no packet loss or corruption.

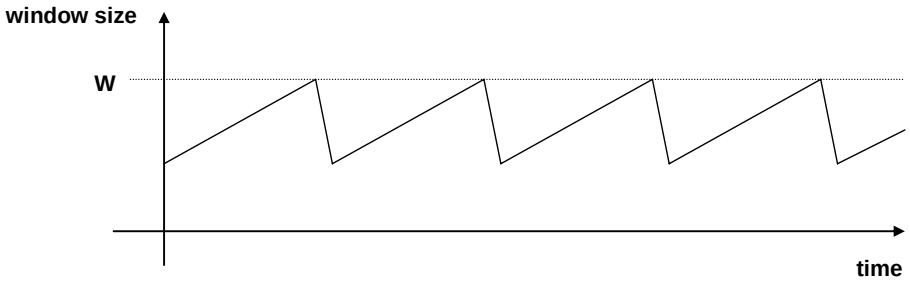


4.2) [4 points] A TCP connection has just been established between two computers (A and B). Assume:

- round trip time (RTT) = 100 [ms],
- congestion window threshold = 4 [segments],
- receiver's advertised window = 12 [segments].

What is the largest window size that the sender is allowed to have? What is the least amount of time before the sender reaches this window size?

4.3) [5 points] The graph below shows the 'sawtooth' evolution of a TCP sender's window size as a function of time. W is the maximum window size (measured in packets). Assume that all packets are P bits long, and that exactly one packet is dropped every time the window size reaches W.



If we ignore the "slow-start" phase at the beginning of the flow, find the average rate at which the transmitter sends packets. Explain your work!

4.4) [7 points] For the TCP connection from 4.3), what is the (average) fraction of dropped packets? Explain your work!

5. NAT and P2P [15 points]

The figure below shows a set-up with a private IP network and its respective NAT firewall. The NAT firewall has a public address of **128.6.13.3** and a private IP address of **192.168.1.1**. The two hosts attached to the same (private) network as the NAT firewall have the IP addresses as shown.

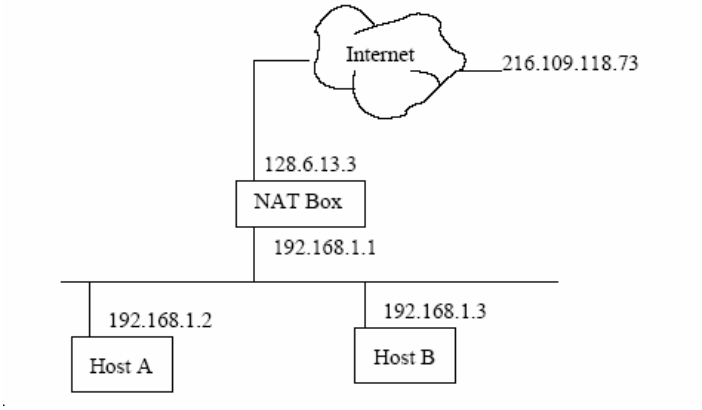


Figure 5

5.1) [3 points] Host A in Figure 5 sends a TCP-SYN request to IP address 216.109.118.73, port 80, with its local port set to 6789. Show the main fields of the corresponding (resulting) entry in the NAT firewall. (You may have to improvise some of the fields.)

5.2) [2 points] Once the TCP-SYN request from 5.1) reaches the host at 216.109.118.73, what will be found in the following four of its fields: destination address, destination port, source address, and source port?

5.3) [3 points] Describe how the ACK for SYN sent in 5.1) will reach host A.

(In the remainder of this question, we study the impact of Network Address Translation (NAT) on peer-to-peer applications.)

Suppose a peer with user name Alice discovers through a Centralized Directory Server (CDS) that a peer with user name Bob has a file she wants to download. Also, suppose Bob is behind a NAT firewall, whereas Alice is not. Bob's NAT firewall is not specifically configured for this P2P application. Let **128.6.13.3** be the WAN-side address of Bob's NAT firewall, and let **10.0.0.4** be the internal IP address for BOB.

NOTE: The given P2P application uses port number **p**. P2P peers are capable of forwarding TCP-and P2P application- related requests on behalf of other peers. However, P2P peers refuse to upload (i.e. transfer) files on behalf of other peers.

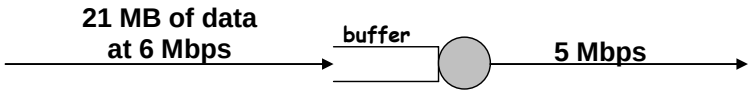
5.4) [4 points] Can Alice obtain the file she wants from Bob, assuming she knows the WAN-side address of Bob's NAT firewall as well as Bob's internal IP address? If so, how? If not, why not?

5.5) [3 points] Now suppose that Alice does not know Bob's internal IP address. However, both Bob and Alice have an ongoing TCP connection with another peer, Cindy, who is not behind a NAT. Can, in this case, Alice obtain the file she wants from Bob? If so, how? If not, why not?

6. Leaky Bucket / Token Bucket [15 points]

6.1) [8 points] Computer A has to 'inject' 21 MB of data into the network. The data is generated and transmitted in bursts of 6 Mbps. The minimum sustainable transmission rate across routers in the network is 5 Mbps.

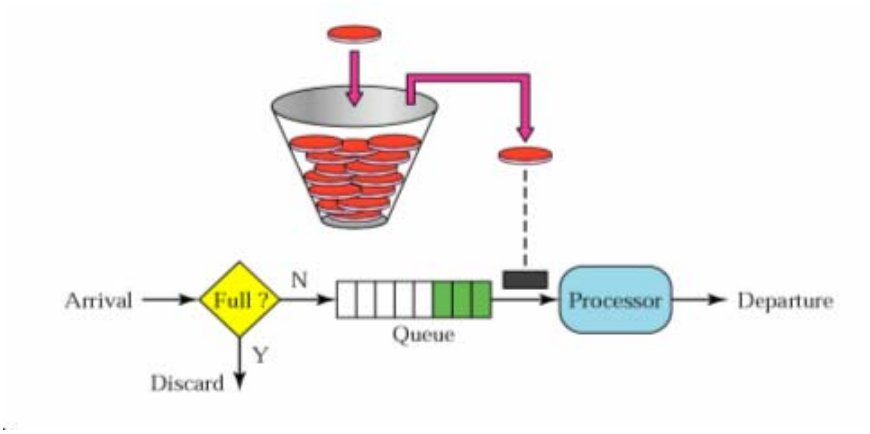
If computer A's transmission is shaped using a leaky bucket (see figure below), what is the minimum size of the buffer to prevent any data loss? (Show your work!)



Leaky Bucket Regulator

6.2) [7 points] Host A has to 'inject' 30 Mbits of data into a network via a token bucket regulator. The token bucket has a capacity of 15 Mbits and is filled with tokens at the rate of 5 Mbps. Data is buffered if it arrives at the regulator when there are no tokens in the bucket.

How long does it take, <u>in total</u>, for the 30 Mbits of data to enter the network, assuming that the host sends at a peak rate of 20 Mbps and the token bucket is initially full?



7. Multimedia [8 points]

Recall there are two types of Forward Error Correction (FEC) that help recover packet losses in multimedia traffic: (1) ***redundancy encoding***: a redundant encoded packet is sent after every n packets by XOR-ing the n original packets; (2) ***low-bit redundant encoding***: a lower-resolution stream is sent.

Suppose the first scheme generates a redundant packet for every 4 original packets. Suppose the second scheme uses a low-bit rate encoding whose transmission rate is 25 percent of the transmission rate of the nominal stream.

7.1) [2 points] How much additional bandwidth does each scheme require?

7.2) [2 points] How much playback delay (in terms of number of packets) does each scheme add?

7.3) [2 points] Assume in every group of five packets the first packet gets lost. Which scheme will provide better quality of the received multimedia stream?

7.4) [2 points] Now assume that every second packet gets lost. Which scheme will provide better quality of the received multimedia stream in this case?

8. Security [12 points]

In network communications, there are several desirable security properties.

For example, ***confidentiality*** is the property that the original plain-text message cannot be determined by an attacker who intercepts the ciphertext-encryption of the original plaintext message.

Another important property is ***message integrity***. This means that the receiver can detect whether the message sent (regardless if it was encrypted) was altered in transit.

Digital signatures is an electronic signature used to authenticate the identity of the sender of a message.

8.1) [3 points] For the two properties of *confidentiality* and *message integrity*, can you have one without the other? Justify your answer. (If your answer is yes, show an example of where one can exist without the other. If your answer is no, explain why one would imply the other.)

8.2) [3 points] Assume that you want to send a non-confidential message M to your lawyer, while giving him/her the assurance that:

1) the message was unchanged from what you sent (message integrity);
2) the message is really from you (message authenticity).

Describe how you can achieve this using public key encryption. Both you and your lawyer own a pair of keys: ($K_{you\text{-}public}$, $K_{you\text{-}private}$), ($K_{lawyer\text{-}public}$, $K_{lawyer\text{-}private}$).
(Note: The message itself must remain <u>non-confidential</u> at all times!)

8.3) [3 points] You have achieved message integrity and authenticity in 8.2). Describe how you can add message confidentiality to 8.2), by (slightly) modifying your solution.

8.4) [3 points] To prevent reply attacks (you do not want an attacker to be able to resend the same message to your lawyer, and yet remain undetected), describe a simple modification to your solution from 8.3).