15-441 Computer Networks **Homework 4**
Assigned: Nov. 18, 2002 **Due: Nov. 25, 2002, in class**

Homework 4

1 Ethernet Protocol

Suppose nodes A and B are on the same 10 Mbps Ethernet segment and the propagation delay between the two nodes is 200 bit times. Suppose A and B send frames at the same time, the frames collide, and then A and B choose different values of K in the CSMA/CD algorithm. Assuming no other nodes are active, can the retransmissions from A and B collide? For our purposes, it suffices to work out the following example. Suppose A and B begin transmission at $t = 0$ bit times. They both detect collisions at $t = 200$ bit times. They finish transmitting a jam signal at $t = 200 + 48 = 248$ bit times. Suppose $K_A = 0$ and $K_B = 1$.

Part a. At what time does B schedule its retransmission?

Part b. At what time does A begin retransmission? (Note: The nodes must wait for an idle channel after returning to Step 2–see p.461 of your book.)

Part c. At what time does A's retransmitted signal reach B?

Part d. Does B refrain from transmitting at its scheduled retransmission time? Why or why not?

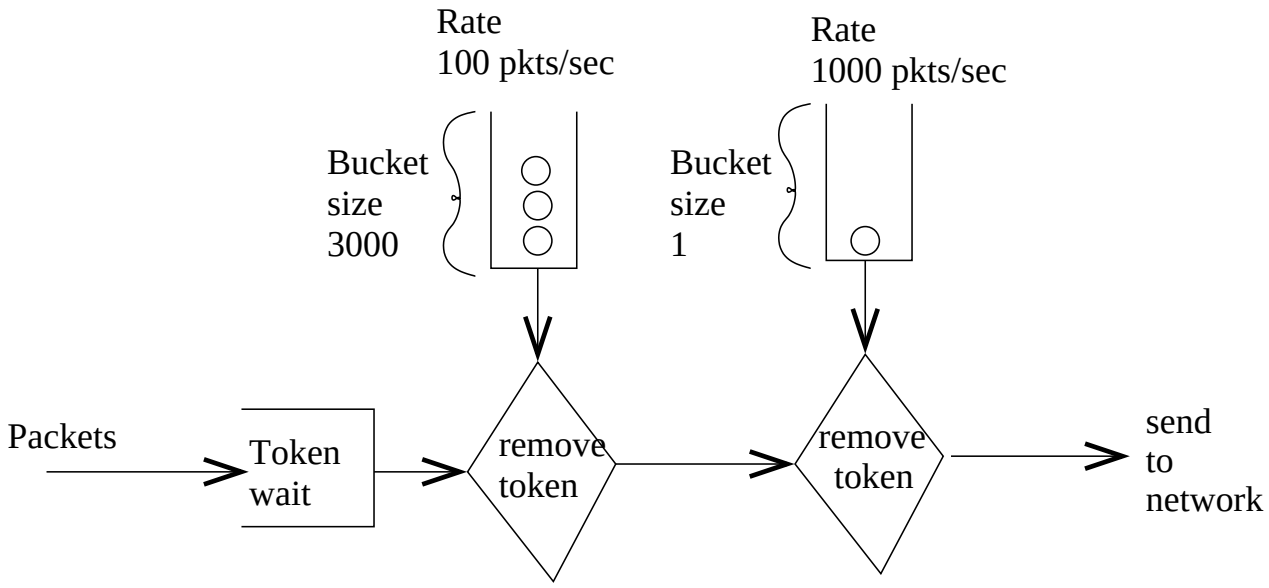
Part e. Can the retransmissions from A and B collide? Why or why not?

2 Weighted-Fair-Queueuing

Two flows A and B arrive at a router with a WFQ scheduling policy. The WFQ scheduling is modeled after GPS. Flow A has reserved 1/3 of the bandwidth on the outgoing link. Flow B has reserved 2/3 of the bandwidth on the outgoing link. Flow A's packets are one third the size of flow B's packets. What are the first 6 packets to leave the link?

3 Leaky Buckets

Consider the figure below showing a flow passing through 2 leaky buckets before it enters the network.



On the next page, you are shown 4 flow behaviors. Circle those that could have been generated by the tandem leaky bucket policer and briefly explain your answer (why or why not) for each case.

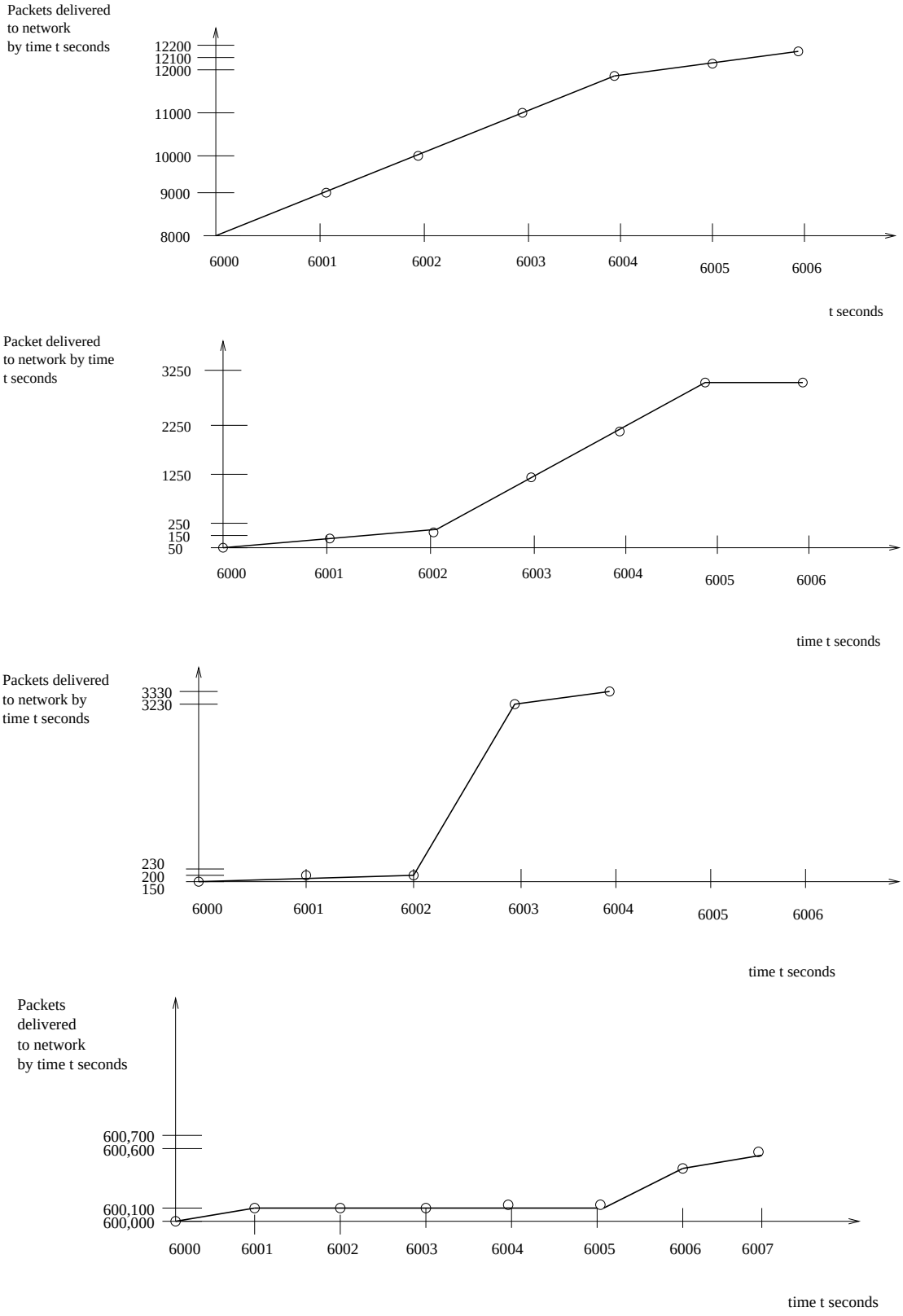


Figure 1: Figure for Problem 3

4 Wire and Datalink Layers

Part a. Give the sequence of bits for the voltages shown in Figure 2. Assume that Manchester encoding is being used.

Bit sequence: _____

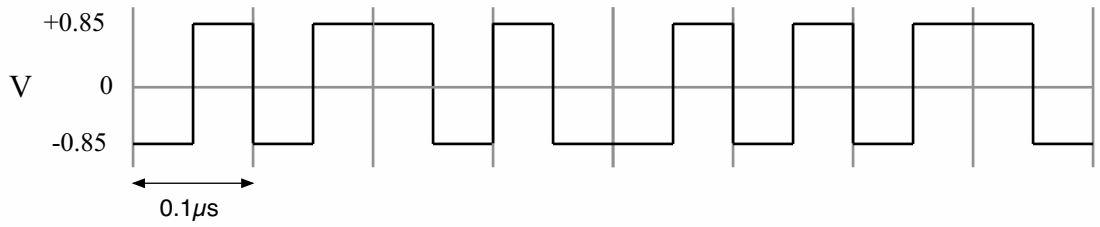


Figure 2: Figure for Problem 4

Part b. What is the parity of this bit sequence (even or odd)? _____

Part c. In this problem you will show that two-dimensional parity checks can detect and correct a single bit error. First, Alice sends the bit string "101101100100111" to Bob.

In the table below, show the two dimensional parity check for Alice's bit string. Use 1 for an odd parity and 0 for an even parity. (Hint: see page 428 in your book)

Now, Bob receives the bit string "101111100100111" from Alice. In the next table, show the two dimensional parity check that Bob performs on Alice's bit string, and fill in the "outer" parity row and column with Alice's parity results.

						B	A
B							X
A						X	

Circle the incorrect bit and explain below how Bob will detect it using Alice's parity information.

_____

_____

_____

Part d. What are the resulting bits after framing the following bit string using bit stuffing? (Hint: ignore Ethernet-specific framing guidelines, just perform bit stuffing on the bit string)

01011111100010110101111111100001101111101110

_____

5 Firewalls

Harry Bovik is given a job as a network administrator for Microscape. His first assignment is to setup a firewall for the company. He decides to use a simple packet filtering firewall. Unfortunately, Harry is not too familiar with firewalls and needs some help setting up his system. The topology of his network is shown below. The Microscape network uses 10.1/16 addresses.

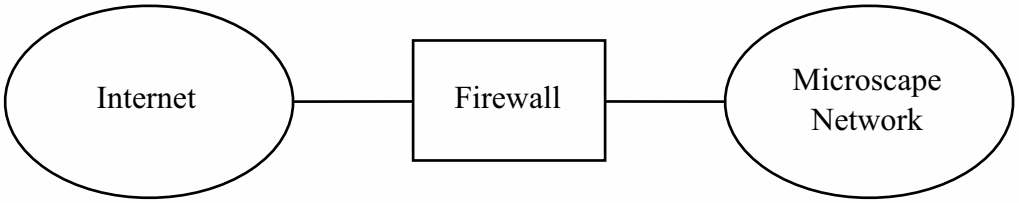


Figure 3: Figure for Problem 5

Rules for this firewall are described using simple rules as shown in the table below. Both simple prefix matching (e.g. 128.32/16) and wildcards (*) are allowed. Packets that do not match any rule are discarded by default.

Src Addr	**Dst Addr**	**Src Port**	**Dst Port**	**Protocol**	**Action**
128.32/16	*	*	telnet	TCP	discard
10.1/16	*	*	sendmail	TCP	allow

The first rule prevents hosts in the 128.32/16 network from telnetting into the Microscape network, and the second rule allows hosts in the Microscape network to send mail to hosts in the Internet. These rules may effectively allow or disallow other traffic as well.

Part a. Write a simple rule(s) that allows Microscape employees to browse the Web. Make this rule(s) as restrictive as possible (i.e. it should not let other traffic into/out of Microscape if possible)

Src Addr	Dst Addr	Src Port	Dst Port	Protocol	Action

Part b. Suppose there are two hosts (A and B) inside the Microscape network. Assume that the firewall has only the rules you added in part a. Could an attacker in the Internet perform a bandwidth denial of service attack that interferes with traffic between host A and B? Why or why not?

Part c. Harry installs an HTTP caching proxy in the Microscape network. He wants to ensure that all clients in Microscape use this proxy to browse the Web. The address of the proxy is 10.1.2.3. How should he modify his rules from part a in order to accomplish this goal (write out the new rule(s) or explain the changes)?

Part d. Assuming the resulting setup from part c and that the Web proxy is not on one of the links between host A and host B, can transfers between A and B be affected by a denial of service attack coming from an attacker in the Internet?