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

Homework 4 Solutions

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?

At 760 bit-times.

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.)

At 544 bit-times.

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

At 744 bit-times.

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

Yes, because the line is busy from A's retransmission. B will wait until the line is idle, plus an additional 96 bit-tiems, before trying to retransmit again.

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

No, since the first bit of A's retransmission arrives at B before B starts its retransmission, B will observe the line is busy and delay its retransmission, so the two retransmissions will not collide again.

A table of the entire process is shown below:

Node A		Node B	
Time	Event	Time	Event
0	Transmission starts; frame length is at least 512 bit times	0	Transmission starts; frame length is at least 512 bit times
200	First bit from B arrives; collision detected and jam signal transmission starts	200	First bit from A arrives; collision detected and jam signal transmission starts
248	Last bit of jam signal sent; A can retry right away but has to wait until line goes idle	248	Last bit of jam signal sent; B schedules retry at 248 + 512 bit times
200-400	Bits from B continue to arrive	200-400	Bits from A continue to arrive
400-448	Jam signal from B arriving	400-448	Jam signal from A arriving
448	Line goes idle; A has to wait 96 bit times before transmitting		
448-544	Inter-frame gap (A waits the 96 bit times)		
544	A starts retransmission		
		744	First bit from A arrives
		760	Retransmission scheduled, but the line is busy, so B has to wait until the line is idle (+ 96 bit-times) before transmitting

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?

Answer

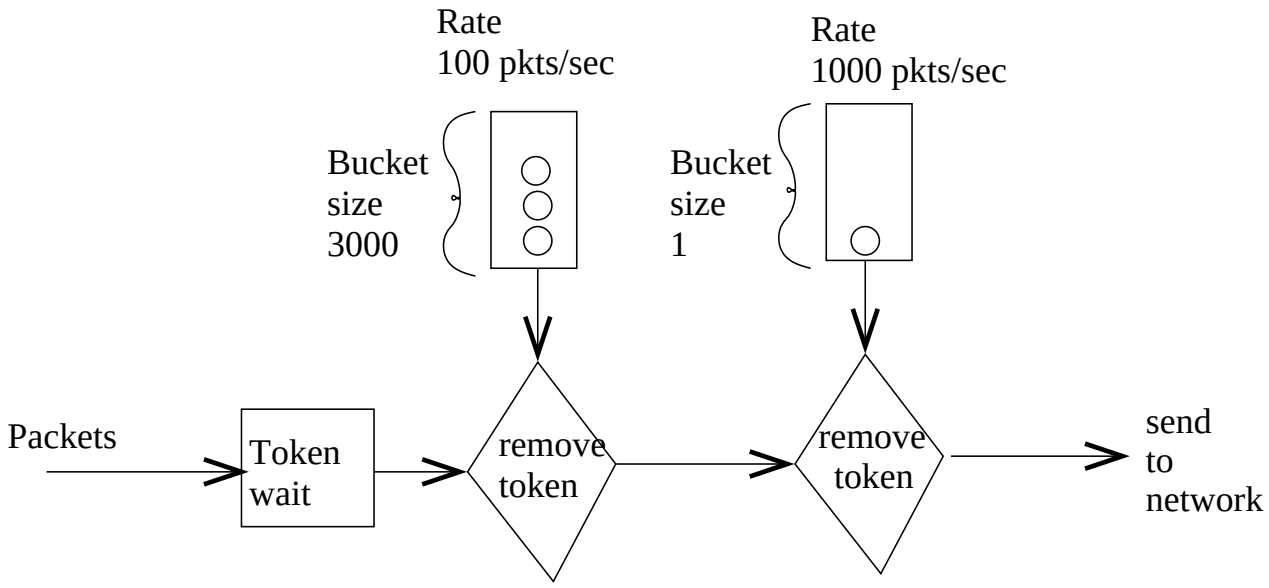
A B A [A B] A

where [A B] means that A and B both finish packets at the same time. Accepted answers were A B A A B A and A B A B A A.

- A sends first packet — B is 2/3 done.
- B completes last 1/3 of packet during the time when A gets 1/2 of one of its packets done, so B sends next packet.
- A completes half a packet and sends 2nd packet, during the time when B gets another 1/3 done.
- A completes another packet, while B does 2/3 packet, so they both are done at exact same time. Thus the 4th and 5th packets sent are A and B in any order.
- A now does packet 6.

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.

Answer

Graph 1 is incorrect because the peak rate of 1000 packets per second is only allowed to continue for 3 seconds, not 4 seconds.

Graph 2 is correct.

Graph 3 is incorrect because there is a peak rate of 1000 packets per second, so it is impossible to send 3000 packets in a single second.

Graph 4 is correct.

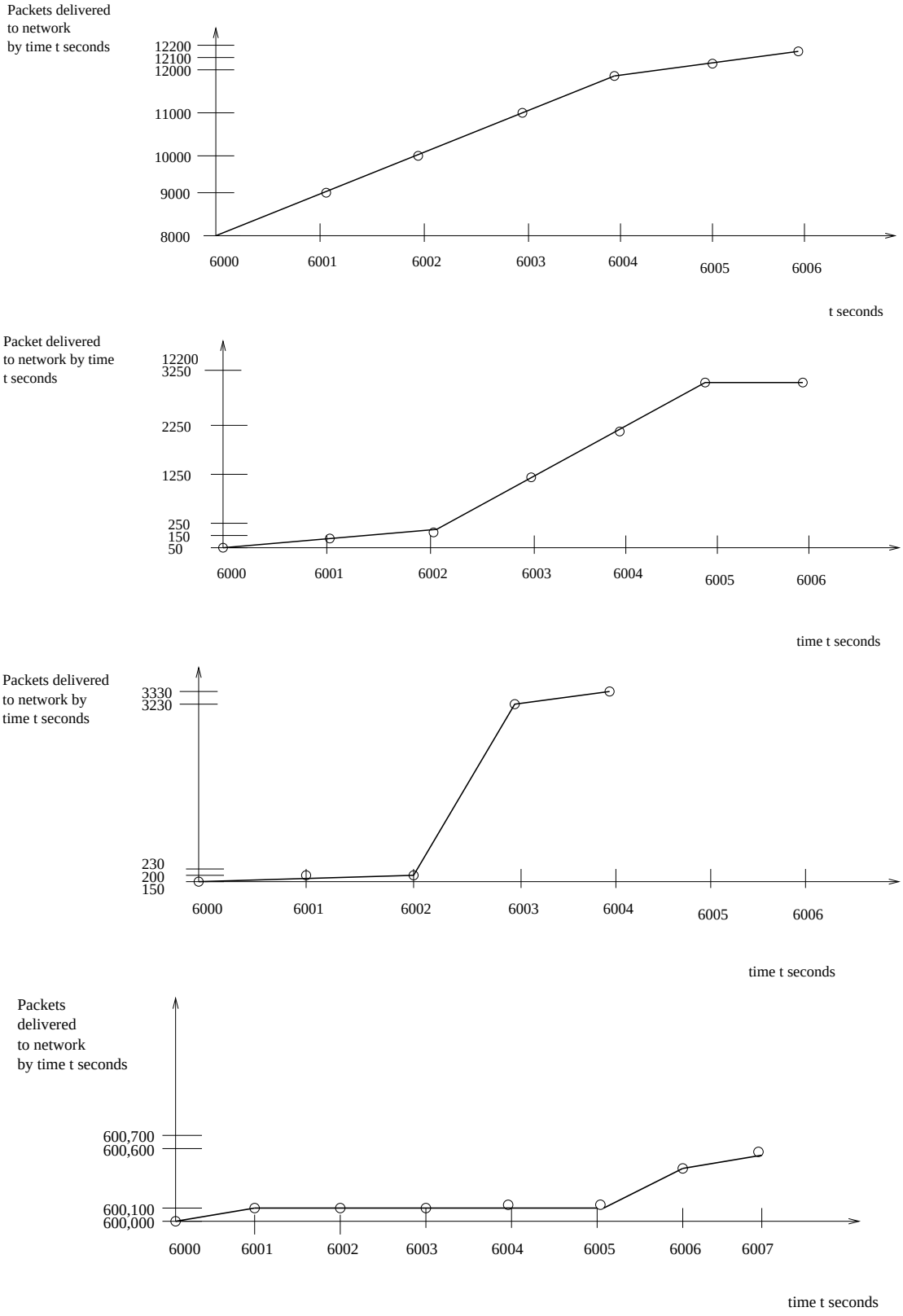


Figure 1: Figure for Problem 3

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: 00110001

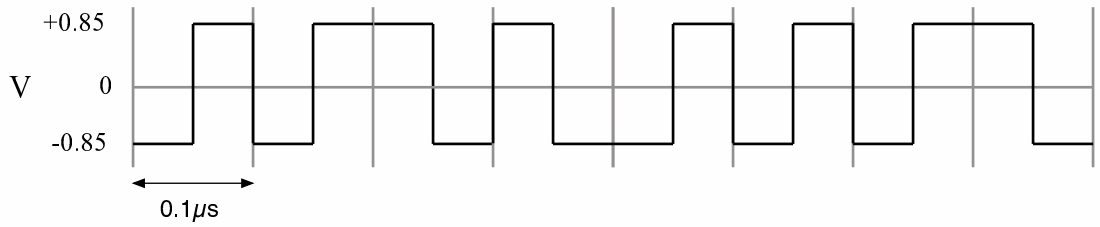


Figure 2: Figure for Problem 4

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

1	0	1	1	0	1
1	1	0	0	1	1
0	0	1	1	1	1
0	1	0	0	0	0

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
	1	0	1	1	(1)	0	1
	1	1	0	0	1	1	1
	0	0	1	1	1	1	1
B	0	1	0	0	1	0	X
A	0	1	0	0	0	X	0

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

Bob's parity bits do not match Alice's. Bob's parity for row 1 is 0, whereas Alice's is 1, and Bob's parity for column 5 is 1 whereas Alice's is 0. These mis-matchings give the row and column of the bit which is out of place, so it is easy to fix.

Note however that this technique may not work if there are 2 bits which are out of place. To convince yourself of this, try "100010" and "101110", using 2 rows of 3 bits. Two row and column checks will fail, and it is not obvious which bits were really the ones which got flipped. This is why stronger integrity checks, such as CRC, are used.

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

Add an extra 0 after every block of 5 consecutive 1's:

01011111010001011010111110111000011011111001110

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.

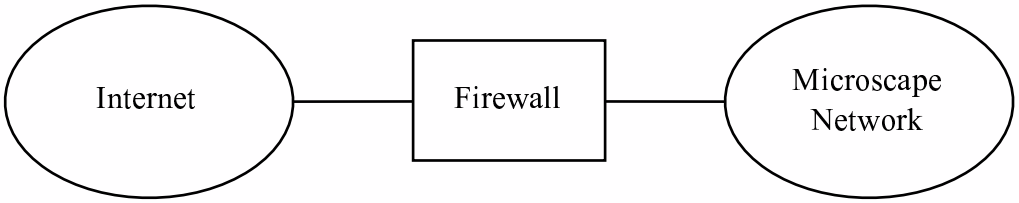


Figure 3: Figure for Problem 5

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
*	10.1/16	HTTP (80)	*	TCP	allow
10.1/16	*	*	HTTP (80)	TCP	allow

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?

Yes, an attacker could still interfere. The attacker could send a flood of packets on port 80 (HTTP) to either A or B. These do not have to be part of an active connection. This is the weakness of simple packet filtering firewalls.

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)?

Replace all 10.1/16's with the proxy's IP address

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?

No. The proxy only forwards data to A or B (or into the Microscape network in general) if it is part of an active Web request. Therefore, outsiders can send arbitrary amounts of traffice into the proxy but it will not affect the rest of the Microscape network.