CS 528: First Midterm (Fall’03)

Answer all problems. Your answers should be concise – short and to the point, but including the important technical issues. The exam is long, but not difficult – work fast. Clearly state any assumptions. Good luck!

**Problem 1:** (30 points; 20 minutes) Briefly (5 sentences or less) answer any 5 of the following questions:

(a) What factors influence the design of a MAC layer protocol?
(b) What could cause two machines to be assigned the same IP address? the same hardware address? What problems would be observed in each case?
(c) What possible reasons explain wild asymmetry of routes on the Internet? How is that harmful?
(d) What is the primary aim of the Digital fountain paper? Explain why the digital fountain approach is not suitable for unicast traffic, or for real-time multicast traffic.
(e) Consider the following suggestion for the learning bridge algorithm: whenever a destination receives a packet, it sends a dummy ping packet back to the source. How does this help? Can you improve it?
(f) What metrics should be used to evaluate intra-domain routing protocols? Are these metrics really indicative of the observed performance of the network? If they are not suggest some that may be more suitable.

**Problem 2:** (15 points; 10 minutes) Give a short explanation (1–3 sentences) for the following possibly wrong statements:

1. Perfect link layer reliability is not needed; reasonable reliability is sufficient
2. A hacker can use ARP to disrupt communication on a network
3. Perfect error correction is impossible, but perfect error detection is possible.
4. The actual data transmission rate on a physical medium can be computed using Shannon’s Limit.
5. The routing pathologies observed by Paxon are due to the count to infinity problem.

**Problem 3:** (12 points;10 minutes) This problem addresses ARQ.

(a) (6 points) Consider a link of bandwidth 40Kbps and delay 10msec. What frame size would be needed to provide 25% efficiency (i.e., at least 20Kbps send rate). Ignore errors and assume that ACK packets have negligible size.

(b) (6 points) Having a sliding window algorithm allows you to approach 100% efficiency. For the frame size derived in (a) show the important parameters for a sliding window algorithm that allows full utilization of the bandwidth.

**Problem 4:** (27 points; 24 minutes)
After making it big as a networking entrepreneur, you set aside 10 million of your hard earned cash to invest as an “angel” in technically sound ideas that may have commercial upside. You receive the following proposals. First, briefly outline how the proposals would work including any important details, then discuss their merits (Is there a reasons/market for this idea? Is it technically feasible? What are the potential advantages and disadvantages? Any reservations? Suggest any improvements). Pick any 3.

(a) A proposal for using an approach similar to learning bridges with the spanning tree algorithm for small to medium scale IP networks.

(b) A NACK based ARQ mechanism where the receiver sends a NACK when a packet is not received within a timeout value. The sender simply sends packets in order – when it receives a NACK, it initiates retransmission.
(c) A proposal to use OSPF as a replacement to BGP (i.e., as an inter domain routing protocol)?
(d) A proposal for combined encoding and error detection. The general idea is to come up with
a code family with maximum hamming distance between the valid words, but with the code words
chosen to have properties that are desirable from an encoding perspective.

Problem 5: (16 points; 20 minutes)
The following is an excerpt from an article titled “Is the Internet Dying?” by Karl Auerbach
(http://www.circlevid.com/article/215_0_1_0_C/), August, 2003

There are indications that the Internet, at least the Internet as we know it today, is dying.

I am always amazed, and appalled, when I fire up a packet monitor and watch the continuous flow of
useless junk that arrives at my demarcation routers’ interfaces. And I have little reason for optimism that this
increase will cease. Quite the contrary, I find more reason to be pessimistic and believe that this background
noise will become a Niagara-like roar that drowns the usability of the Internet.

Between viruses and spammers and just plain old bad code, the net is now subject to a heavy, and
increasing level of background packet radiation. And the net has very long memory - I still get DNS queries
sent to IP addresses that haven’t hosted a DNS server - or even an active computer - in nearly a decade.
Search engines still come around sniffing for web sites that disappeared (along with the computer that hosted
them, and the IP address on which that computer was found) long ago.

It will not take long before the cumulative weight of this garbage traffic starts to poison the net. Already
it is quite common for individual IP addresses to be contaminated from prior use. I am aware of people
who are continuously bombarded by file access queries because a prior user of that address shared files from
that address. Entire blocks of IP addresses are also contaminated, perhaps permanently, because they once
hosted spammers thus causing those address blocks to be entombed into the memories of an unknown number
of anti-spam filters not merely at the end user level but also deep in the routing infrastructure of the net.
And a denial-of-service virus, once out on the net, can only be quieted, not eliminated; such viruses remain
virulent and ready to spring back to life.

Better security measures, particularly on the sources of traffic, will help, but again, unless something
radical happens, the contamination will merely be slowed, not stopped.

I believe that something radical will happen: We may see the rapid end to the “end-to-end” principle on
the Internet.

We are already observing the balkanization of the net for political and commercial reasons. Self-defense
against the rising tide of the net’s background packet radiation may be another compelling reason (or excuse)
for net communities to isolate themselves and permit traffic to enter (and exit) only through a few well-
protected portals.

This balkanization may be given additional impetus by a desire to escape from the ill effects of poorly
designed regulatory systems.

So, between spam, anti-spam blacklists, rogue packets, never-forgetting search engines, viruses, old ma-
chines, bad regulatory bodies, and bad implementations, I fear that the open Internet is going to die sooner
than I would have expected. In its place I expect to see a more fragmented network - one in which only
"approved" end-to-end communications will be permitted.

The loss of open end-to-end communications will, in itself, be a great loss.

But of even more concern will be the fact that these portals, or gates, will require gatekeepers, which is
merely a polite word for censors. In the present political climate in which government powers are conferred,
without a counterbalancing obligation of accountability, onto private bodies, the loss will be much greater.

(a) What properties of the original design of the Internet make it vulnerable to the problems that are
causing the “background packet radiation”?
(b) How does the segmented (“balkanized”) future of the Internet that the author fears break the end-
to-end principle and the original spirit of the Internet?
(c) Identify some of the tussles that are mentioned by the author.
(d) Discuss the reasoning and conclusions of this piece in light of the tussles paper.