Homework 1 for CSE/EE 461 (Winter 2004; Davis)

Due: Wednesday, January 28, 2004, at the beginning of class.

1. Framing. Consider the following two byte-stuffing schemes:

PPP, defined officially in RFC1661 and used over most dialup links. Here, the byte 0x7E is added at the sender to mark the end of the previous packet and the beginning of the current one. Within the payload, the sender replaces 0x7E with 0x7D, 0x5E. Occurrences of 0x7D must also be escaped; they are replaced with 0x7D, 0x5D. At the receiver, 0x7D and the following byte are replaced with one byte that is the XOR of the second byte with 0x20. Thus 0x7D, 0x5D is replaced with a single 0x7D and 0x7D, 0x5E with a single 0x7E, reversing the process.

COBS, an alternative for this question. Here, the byte 0x00 (that is, zero) is added at the sender to mark the end of the previous packet and the beginning of the current packet. Zeros must now be removed from the payload. First, a start byte is added to indicate the number of bytes until a zero is encountered. That zero is replaced with the number of bytes until the next zero, and so forth until the end of the packet. To handle the last zero in the packet, we pretend that there is an extra zero just off the end of the real packet. For example, the packet 0x22, 0x00, 0x00, 0x55 becomes 0x00, 0x02, 0x22, 0x01, 0x02, 0x55. We must also handle the situation in which there are no zeros in the payload. To do this we use 0xFF to indicate a run of 254 consecutive non-zero bytes without a following zero. After the 254 bytes there is a count of bytes until a zero or another 0xFF. At the receiver the reverse process is performed.

Now compare PPP and COBS in terms of a) their implementation complexity; b) their average case framing overhead; and c) their worst case framing overhead.

2. Checksums. Consider the 16-bit Internet checksum as given in Peterson 2.4.2. (Also see RFC 1071 for interest.)

Characterize the error detection capabilities of this checksum against both burst and random bit errors. Explain what errors will always detected and why. Explain what errors will sometimes be detected and the probability with which they will be detected and why. Make simplifying assumptions as you need them.

3. CRCs.

a), b) Peterson & Davie 2.18

c) CRCs are typically placed on the wire at the end of the frame (that is, they are the last portion transmitted). Why?

4. Bandwidth and Latency. Explain, by giving a procedure and equations, how a node can use the Fishnet ping protocol to determine the latency and bandwidth of each link along a multi-hop path to the destination. You may assume that the source knows the address of all the intermediate nodes along the path, that routing is symmetric, and that the rate and propagation delay of each link are the same in both directions. (Hint: start with the base case of directly connected end nodes, and recurse.)

5. **Sliding Windows.** Consider a standard sliding window protocol. The size of the sliding window affects the transfer rate that transport protocols such as TCP can achieve.

   a) Give an expression for the throughput as a function of the size of the sliding window. What would this throughput be in practice if stop-and-wait were used on a cross-country connection (100ms round trip time)?

   b) TCP's maximum receive buffer size for flow control is 64K without the use of extensions. (Defaults are typically 16 or 32K too.) At what throughput will flow control become the limiting factor for cross-country connections? What sliding window size would be needed to support a 1Gbps cross-country connection?

—END—