For the purpose of this homework, people who have taken TLEN 5330 Data Comm I, are considered “advanced networkers”.

1. You will need a windows-based machine to do this lab. Download the software IOServer from www.ioserver.com. IOServer is an industrial software for setting up masters and slaves on personal computers. Install it according to the IOServer instructions which are on the class homework page. Set it up as a master according to the instructions. This master, if set up correctly, will query a slave located in the ITP lab using TCP/IP over the Internet.

   (a) Describe the behavior of a typical Master-Slave exchange with a protocol diagram. (Advanced networkers can do an optional second diagram that includes all of the TCP packets that are exchanged).

   (b) How would you change the rate that the master sends requests?

2. Now download the Wireshark software from www.wireshark.org. Use the latest “stable” release. Wireshark is a generic network protocol analysis tool for TCP/IP and other protocols. It can analyze DNP3.0. Install Wireshark according to the Wireshark instructions which are on the class homework page. Install it on the same machine that has the IOServer.

   Find a DNP request packet in the upper window of Wireshark and highlight the packet. In the middle window, highlight the line that says “Distributed Network Protocol 3.0”. The lower window will highlight in blue the bytes (written as two hexadecimal digits) of the DNP packet.

   (a) How many bytes are in the DNP packet.

   (b) Write out the bytes in the DNP packet and identify the purpose of each byte (no need to go to the bit level).

   (c) Describe the control bits for the Application, Transport, and Link layer.

   (d) Look now at the TCP/IP header, what is the source address, source port, destination address, and destination port. (Advanced networkers: how does Wireshark know that this is a DNP packet?)

   (e) Look at the next request packet. What differences if any exist between this and the previous request.
3. In IOServer, right click the port in the left window (labeled with the IP address), and select Stop Port. Start a wireshark capture and observe the packets (you need to Stop Port and then Start Wireshark in less than 10 seconds to see what goes on). Draw a protocol diagram of the sequence of packets and approximate timing (to the nearest second) until the normal 5 second M-S exchange is started. (Advanced networkers: does the IOServer start one TCP session per M-S exchange or does it keep the session across multiple M-S exchanges? Does it end its sessions politely with a TCP-FIN?)

4. Observe your request-response pairs with IOServer. Note the typical response time. From my home I observe that it is about 40ms with occasional outlier values greater than 50ms (about one in 4 packets).

   (a) Describe how you are accessing the network (e.g. “From campus wireless.” or “Over a satellite link from my cabin in Durango.”) and the time of day. What are your typical response times and outlier values?

   (b) Click on the “DNP Channel” tab of the IOServer port window on the right. Set the TimeOut value to your typical response time (Can you see why this would be a bad idea in a production system?). Describe the behavior of the DNP protocol. Turn Confirm Mode to “Always”. Does this improve the behavior?

   (c) Try increasing the “Retries” from 1 to 5. Capture a longer exchange (more than 5 Tx/Rx packets) with Wireshark and carefully reconstruct the exchange in a protocol diagram. You may need to look at sequence numbers and other clues to connect elements of the exchange.