PROTOCOL ANALYSIS INSTITUTE

Quick Reference Step-by-Step Lab 3 Instructions: Hello! Hello! Goodbye! Goodbye!

Step-by-Step Instructions:	**uglytrace.pdf**
Trace File:	**uglytrace.dmp**
“Watch the Lab” File:	***uglytrace.avi*** **(XviD codec) or uglytrace.wmv**

Step 1: **Create an *Ethereal Labs* directory** on your hard drive and **copy the trace files** from the LLK6 over to that directory.

Step 2: **Launch Ethereal**.

Step 3: Select **File > Open** on the Ethereal menu bar. Select **your local drive** off the drive list and double-click on the **Ethereal Labs directory** you created in Step 1. Double-click on the ***uglytrace.dmp*** trace file.

Step 4: Scroll through the trace – you’ll see that it is filled with duplicate packets throughout.

Step 5: Check out **packets 5 and 6** in the trace. Why does 12.234.13.89 send two SYNs? Looking at the Info column, these packets appear to be handshake packets with the same source and destination ports.

Step 6: We need to look inside the packets to figure out what is going on here – are these really duplicates? **Click on packets 5 and 6** in the middle window (detail decode window). You may need to right mouse click in this window and select **Expand All**.

Step 7: We see that the addressing, port numbers and sequence numbers are the same. The Time to Live (TTL) value is not the same, however. We now know that these two packets are NOT the same. It appears that the client is not sending out two copies of the same packet—the client wouldn’t increment the TTL value in subsequent packets. We also know that the switch is not guilty of sending duplicate packets down to the analyzer port—the switch wouldn’t change the TTL value either. So what has happened?

Step 8: Fill out the following chart for **packets 5 and 6**.

Field Name	Packet 5	Packet 6
Source MAC Address		
Destination MAC Address		

Does this answer the puzzle? Yes… we see the packet has been routed – the MAC address shows the router’s MAC address in the center of the communication. The TTL has been decremented by 1.

This is called local routing. A packet is sent from one local machine to a router that sends it back to the same network. If we are sniffing on only one network, we shouldn’t see packets more than once.

If you’d like to be walked through this process, check out the *BYOL* section of LLKv6.
See the ***Laura Chappell Master Library (LCML)*** at www.packet-level.com for additional self-paced labs.