EE3A2: Unassessed Laboratory Exercises

Aims and objectives

To provide us an opportunity to use and explore command line IP utilities and the Wireshark protocol analyzer.

Introduction

This is a very short and informal laboratory activity to provide a little time to explore the recommended software. There are no deliverables and there is no assessment.

My hesitation in preparing this activity was that our laboratory computers are connected to an unusually busy, complex, managed network. There are many protocols in use. You should expect to see a great deal of traffic and you are not expected to know most of the protocols. However, you may like to check Wikipedia for a simple definition of one or two of the protocol names you see.

Exercise 1: Open a command window by typing `command` in the "Search programs and files" box of the Start menu and selecting "command prompt". Here we can run IP utilities: ipconfig, netstat, ping and tracert.

ipconfig can tell us our IP address. Type `ipconfig`. Next type `ipconfig /all`
netstat tells us about our active communications. Type `netstat` at the prompt.
ping, if it were not blocked, would tell us if hosts are reachable. We cannot ping across campus or beyond. To ping our departmental web server type `ping www.eee.bham.ac.uk`
tracert (trace route) is also blocked but type `tracert www.eee.bham.ac.uk`

Exercise 2: In this exercise we will use the protocol analyzer, Wireshark, to capture network traffic including a web page download from our browser.

Open Wireshark from "All Programs". Select Capture then Options.
Note. Selecting Start immediately appears not to work because Wireshark wants an interface to be selected, even if there is only one interface to select. On your next capture you can just select Start from the Capture menu.
Have a look at the default settings, then before selecting Start, open a browser and type in a url, but don't press Enter.

Now go back to Options and select Start, and then download the web page and after it loads, stop the capture. You should have captured your own packets and also everyone else's. (Later try another capture but unselect "Promiscuous mode" in Options so that we see only your own packets.)

Have a look at the results and see if you can find some of your own TCP datagrams. (You will know your IP address from ipconfig.) You can sort the results or search to find your IP address or the web page url. Ctrl F will open a Find window and you can select "string" for your search. Briefly explore inside your encapsulated packets. You should see Ethernet frames (with MAC addresses in the header) encapsulating IP packets (with IP source and destination addresses in the header) encapsulating TCP datagrams (with source and destination port numbers in the header).

Exercise 3: Explore VisualWare free on-line services MCS MySpeed and MCS MyRoute at **http://www.mycooltools.com**
(Note. MyRoute is a traceroute service but clicking on it currently runs MySpeed. You can access MyRoute by selecting "Route" as a test type option on the right of the page.)