Lab 0 - Wireshark Protocol Analyzer

This lab is for students who did not take 3525 last term.

Introduction

In this lab you will use the Wireshark Protocol Analyzer to capture, filter and examine IP frames.

You will follow the procedure described in two of the Wireshark labs prepared by J.F. Kurose and K.W. Ross, authors of the book "Computer Networking." The lab descriptions are available online.

If you read the lab descriptions before coming to the lab you should be able to complete the Introductory and IP Protocol labs during your lab session.

Although we will not have time to study all of the IP protocols mentioned in the labs in detail, the lab should help you become familiar with this useful tool.

Pre-Lab

Download and read the following labs (available from http://www-net.cs.umass.edu/wireshark-labs/):

- Getting Started
- IP

For the second lab you may want to have access to RFC 791 and RFC 792.

Submit a short report to the dropbox on the course web site with your name, ID, lab number and answers to the following questions:

- what protocol layer is shown in the 'Protocol' column in the top window?
- what is the purpose of the filter?
- how do you get Wireshark show you more or less detail about a particular protocol layer?
- which window shows the contents of the frame in hex format?

Lab

Wireshark has been installed on the lab computers. Go through the instructions in the two lab writeups to practice using Wireshark.

Answer questions 1 to 9 in Section 2. Skip the Fragmentation section (questions 10 and 11) since modern networks almost never fragment packets.

Run the Windows `tracert` program in a command window and follow the Unix/Mac instructions instead of using pingplotter for the IP lab[1]

For questions 5 and 6, limit yourself to the IP protocol fields that were described in the IP lecture. Use your understanding of the IP protocol rather than blindly comparing the contents of the packets.

Shut down the browser when doing the IP lab to minimize the number of unrelated packets captured.

Note that the ICMP echo response (response to a 'ping') and TTL exceeded response frames contain copies of the transmitted IP frame (or header). Don't confuse the two IP headers.

Report

Submit a report in PDF format containing:

- The lab number, your name, BCIT ID and date.
- The answers to questions 1 through 4 in the "What to Hand In" section of the "Getting Started" lab. For question 4, print the packets to a text file and copy the text into your report.
- The answers to questions 1 through 9 in Section 2 of the IP lab.

[1] Since we are not looking at fragmentation you will not need the pingplotter feature that lets you set the packet length.