Introduction to the Wireshark Protocol Analyzer

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 twelve Wireshark labs prepared by J.F. Kurose and K.W. Ross, authors of the book "Computer Networking."

If you prepare by reading the lab descriptions before coming to the lab you should be able to complete the two labs during your lab session.

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

Pre-Lab

The Wireshark labs are available from:
`http://www-net.cs.umass.edu/wireshark-labs`

The two labs to be done are:

- Getting Started, and
- IP

For the IP lab you may want to have access to the lecture notes and perhaps RFC 791 - IP and RFC 792 - ICMP protocol specifications.

Submit a short report to the dropbox on the course web site with the usual identification information and answers to the following questions (the answers can be found in the "Getting Started" lab):

- 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 Procedure

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

Note: When asked to print your results, first expand the sections you want to print as explained in the instructions, then use the Wireshark print menu to print in "Plain text" format to a file with the "as displayed" option. You can then open this file and copy/paste the text into your report. You may want to reduce the font size to minimize line breaks.

Note: Skip the Fragmentation section of the second (IP) lab (the questions starting at 10) since fragmentation is almost never required by modern networking equipment.

Note: You are not doing the fragmentation portion of the IP lab so *do not use Pingplotter*. Instead, follow the instructions for Linux/Unix/MacOS but use the standard Windows `tracert` program in a command prompt window. Simply use the command `tracert` instead of `traceroute` and omit the second (numeric) argument (56, 2000 or 3500). In other words, use only one `tracert` command and omit the length argument.

Note: Shut down your browser before starting the wireshark capture for the second (IP) lab to minimize the number of unrelated packets captured.

Note: When answering questions 5 and 6 of the IP lab don't simply compare the packets to see which header fields have changed. Consider the purpose of each header field (see lecture notes) and decide whether that field *should* be changing from packet to packet or not. Then examine the captured packets to verify your answer. This is a good way to check your understanding of the IP header fields.

Note: The ICMP echo response (the response to a 'ping') and the ICMP TTL exceeded response frames contain a copy of the IP frame that triggered this response, including the header. Don't confuse the response packet's header with the embedded header.

Warning

Your instructor is a fairly patient fellow but he will get annoyed if you ask a question that is already answered above.

Report

Submit a report in PDF format containing:

- The usual identification information.
- The answers to questions 1 through 4 in the Wireshark Introduction lab. For question 4, follow the instructions above rather than printing the packet.
- The answers to questions 1 through 9 (only) in Section 2 of the IP lab. You do *not* need to do the section on Fragmentation which includes questions 10 through 15.