CS 145 Lab Exercise 6
Wireshark Lab: UDP
A.Y. 2016-2017, 2nd Semester

1 Introduction

In this laboratory exercise you are going to explore the structure of a UDP segment, as well UDP's protocol number (as recognized by the Internet Protocol). As such, it would be helpful for you to review Lecture 9 (as well as Laboratory Exercises 1 and 3) before doing the laboratory exercise.

2 Restrictions

For this laboratory exercise the following restrictions apply:

- The trace for Laboratory Exercise 3 **must** have been generated in a Teaching Laboratory machine.
- Trace analysis may be done in any machine with the Wireshark software installed.

3 Instructions: Trace Generation

1. Start up the Wireshark software.
2. Open the trace file from Laboratory Exercise 3. If you followed the instructions in Laboratory Exercise 3, the file should be named `labexercise3.pcapng`. If you were not able to do Laboratory Exercise 3, you can copy a classmate's tracefile; if you do this however, kindly state so in the Laboratory report.
3. At this stage, you are now ready to work on the laboratory report.

---

4 What to hand in

Answer the following questions in the laboratory report, based on your Wireshark experimentation:

1. Select the first UDP packet generated by `traceroute`. From this packet, determine how many fields there are in the UDP header. (Do not look in the textbook or slides. Answer these questions directly from what you observe in the packet trace.) Name these fields. Include an annotated screenshot supporting your answer.

2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields. Include an annotated screenshot supporting your answers.

3. The value in the Length field is the length of what? (You can consult the textbook or the slides for this answer). Verify your claim with your captured UDP packet. Include an annotated screenshot supporting your answer.

4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: The answer to this question can be determined by your answer to (2) above.)

5. What is the largest possible *source port* number? (Hint: See the hint in (4).)

6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment. Include an annotated screenshot supporting your answer.

Note: Do not forget to close down or terminate the Wireshark software.

5 Submission

The laboratory report is due on Sunday, March 12, 2017, 2359 hours. You can submit the laboratory report via UVLE.