Computer Networks CSE 5344

Project 3

User Datagram Protocol Analysis using Wireshark

Instructor: **Fred Kashefi**

GTA: Marnim Galib

Spring 2018

Objectives

In this lab, we'll take a quick look at the UDP transport protocol. As we saw in Chapter 3 of the text[1], UDP is a streamlined, no-frills protocol. You may want to re-read section 3.3 in the text before doing this lab.

Due Date

April 25, 2018 (Wednesday) 11:59 PM[2]

Submission Guidelines

- Submit a single zipped file with the naming convention,

  `< your_UTA_id >_< your_name >.zip`

- Your submission should have the following items to be considered for evaluation,
  (a) The PDF document, that is the answer to the questions in the assignment[3]
  (b) The name of the solution document should be *your_name_ID_No.pdf*.
  (c) The document should have your name in the header or footer in every page along with page numbers.
  (d) Include a screenshot of the packet(s) within the trace that you used to answer a question whenever possible. Highlight the relevant item(s) in the screenshot to explain your answer.
  (e) Your own captured trace file wherever it is necessary.

---

[1] References to figures and sections are for the 6th edition of our text, *Computer Networks, A Top-down Approach, 6th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2012.*

[2] All Submissions should be completed through BlackBoard

[3] Strictly this should be *.pdf* file as this enables us to read the answer in a way you want us to read it

- Make sure you write your **name** and your UTA ID in the final document that you are submitting.
- Make sure that submission of the zipped file is through *UTA BlackBoard* [4].

The Assignment:

Start capturing packets in Wireshark and then do something that will cause your host to send and receive several UDP packets. It's also likely that just by doing nothing (except capturing packets via Wireshark) that some UDP packets sent by others will appear in your trace. In particular, the Simple Network Management Protocol (SNMP -chapter 9 in the text) sends SNMP messages inside of UDP, so it'll find some SNMP messages (and therefore UDP packets) in your trace.

After stopping packet capture, set your packet filter so that Wireshark only displays the UDP packets sent and received at your host. Pick one of these UDP packets and expand the UDP fields in the details window. If you are unable to find UDP packets or are unable to run Wireshark on a live network connection, you can download a packet trace containing some UDP packets.[5]

Whenever possible, when answering a question below, you should hand in a printout (pdf) of the packet(s) within the trace that you used to answer the question asked. Annotate the printout[6] to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose Packet summary *line*, and select the minimum amount of packet detail that you need to answer the question.

[4] Please strictly follow the naming convention of the zipped file.

[5] [2]Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file http-ethereal-trace-5, which contains some UDP packets carrying SNMP messages. The traces in this zip file were collected by Wireshark running on one of the author's computers. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the http-ethereal-trace-5 trace file.

[6] What do we mean by "annotate"? If you hand in a paper copy, please highlight where in the printout you've found the answer and add some text (preferably with a colored pen) noting what you found in what you have highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate.

Questions:

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

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.

3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

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 (see Figure 4.13 in the text, and the discussion of IP header fields).

7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.