CSC358 Assignment 3 Wireshark

February 14, 2016

1 UDP

In this lab, we'll take a quick look at the UDP transport protocol. As we saw in Chapter 3 of the text1, UDP is a streamlined, no-frills protocol. You may want to re-read section 3,3 in the text before doing this lab. Because UDP is simple and sweet, we'll be able to cover it pretty quickly in this lab. So if you've another appointment to run off to in 30 minutes, no need to worry, as you should be able to finish this lab with ample time to spare.

At this stage, you should be a Wireshark expert. Thus, we are not going to spell out the steps as explicitly as in earlier labs. In particular, we are not going to provide example screenshots for all the steps.

Doing the following to obtain the trace we need:

- Start capturing packet in Wireshark.
- Open a terminal on your PC (cmd for Windows, shell for Linux/Mac), execute this command: "nslookup www.google.com 8.8.8.8".
- Stop capturing packet.

After stop capturing, you can set your filter to "ip.addr == 8.8.8.8" to only display the UDP packets we are going to discuss (it should be just two packets). Then answer the following questions. Whenever possible, when answering a question below, you should hand in a printout or screenshot of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer (you can provide one screenshot and annotate different parts for different 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). What is the length of UDP payload for your selected 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.
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.

2 TCP

Download this packet trace `http://packetlife.net/captures/HTTP.cap` and answer the following questions:

1. What is the IP address of the client (the initiator of this TCP connection), and what is the server's IP address? From which port the client initiates the connection, and what is the port number used for this connection on the server side?

2. Roughly speaking, what is the RTT of this connection? (just need a rough number, answer within ±10ms will be fine). Roughly how many RTT does it take (in total) for this TCP connection to establish, tranfer data and close?

3. During the handshaking of this connection, what is the length of the TCP header? Is this TCP header the basic one? If not, what is the optional field(s) in the TCP header.

4. Answer 3 after the handshaking stage. What is the length of maximum TCP payload of a packet after this tcp connection is established?

5. How many HTTP data the server sends to the client during the 2nd RTT, 3rd RTT and 4th RTT (respectively)?

6. What is the initial buffer size (window size) advertised by the client? Has the buffer size on the client side ever become the bottleneck during the transferring of data? (Be careful when answer this question, show how you get your conclusion).