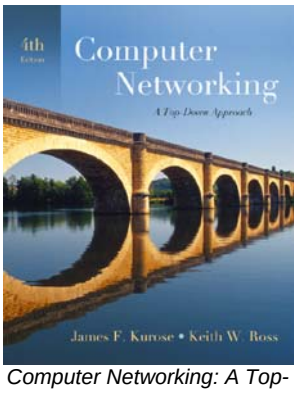
Wireshark Lab: UDP



Computer Networking: A Top-down Approach, 4th edition.

Version: 2.0

In this lab, we'll take a quick look at the UDP transport protocol. As we saw in Chapter 3, UDP is a streamlined, non-thrills protocol. 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 an 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.

The Assignment

Start capturing packets in Wireshark and then do something that will cause your host to send and receive several UDP packets. (One way to do this would be to use the nslookup command, as we saw in the DNS Wireshark lab. If you are unable to run Wireshark on a live network connection, you can download a packet trace file that was captured while following the first two steps of the nslookup section of the Wireshark DNS lab on one of the author's computers[1].) 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.

Whenever possible, when answering a question you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use *File->Print*, choose *Selected*

[1] Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file tcp-ethereal-trace-1. The traces in this zip file were collected by Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark lab. 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 udp-wireshark-trace trace file.

packet only, choose *Packet summary line*, and select the minimum amount of packet detail that you need to answer the question.

1. Select one packet. From this packet, determine how many fields there are in the UDP header. (Do not look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.
2. From the packet content field, determine the length (in bytes) of each of the UDP header fields.
3. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.
4. What is the maximum number of bytes that can be included in a UDP payload?
5. What is the largest possible source port number?
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 IP header.)
7. Search "UDP" in Google and determine the fields over which the UDP checksum is calculated.
8. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.

Extra Credit

1. Capture a small UDP packet. Manually verify the checksum in this packet. Show all work and explain all steps.