Wireshark Lab 4a: UDP

In this lab, we'll take a quick look at the UDP transport protocol. UDP is a streamlined, no-frills protocol.

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 sends SNMP messages inside of UDP, so it's likely that you'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 use the UDP file as given in the MyLearning page[1].

Whenever possible, when answering a question below, 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 packet only*, choose *Packet summary line*, and select the minimum amount of packet detail that you need to answer the question.

1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. 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? 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.
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.

---

[1] Use the file udp_sample2. You can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the udp_sample2 trace file.

Extra Task

Capture a small UDP packet (or use the given trace file, udp_sample2, packet no. 162). Manually verify the checksum in this packet. Show all work and explain all steps.

Note: use the following table to calculate the checksum value.

Field	Hex Value
IP header: Source IP address	
IP header: Destination IP address	
IP header: Protocol number(zero padded on left)	
16 bit UDP Length	
UDP header: source port	
UDP header: destination port	
UDP header: length	
UDP Data	
Sum all hex values	
Carry	
Add in the carry	
1s complement = checksum!	

Note: This lab is based on Kurose Book:

James F. Kurose and J. Rose, Computer Networks: A Top-Down Approach Featuring the Internet, 8th Edition (2016), ADDISON WESLEY, ISBN-13: 9780135928523.

[1] Use the file udp_sample2. You can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the udp_sample2 trace file.