TAIBAH UNIVERSITY

College of Computer Science and Engineering

Computer Engineering Department

COE332
Computer Networks
Student's Lab Manual
V7

Prepared by:
Dr. Mohamed ZAYED Dr. Ahmed ABDELMONEM
Dr. Abdullah AL BINALI

Lab 05

Student Name: Norah Fahad Aloufi

Student ID: 4050772

Section: C8C **Group:**

Session (Fall / Spring / Summer): 21/03/2022

Lab-5: UPD Protocol

In this lab, we'll take a quick look at the UDP transport protocol. As we saw in Chapter 3 of the text[10], 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.

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 – see section 5.7 in the text) 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 download a packet trace containing some UDP packets.[11]

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[12] 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. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

Last Page

[10] References to figures and sections are for the 8th edition of our text, *Computer Networks, A Top-down Approach, 8th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.*

[11] 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.

[12] 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 've highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate.

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.

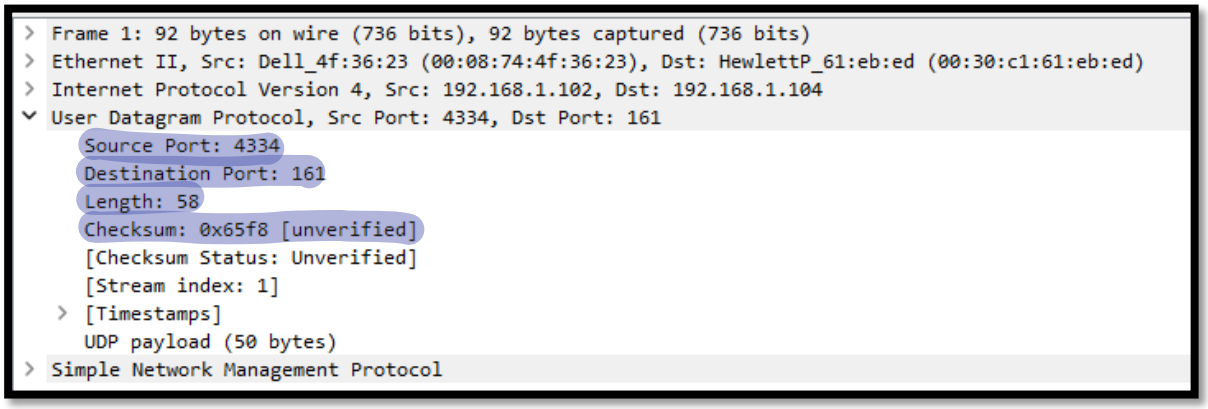
4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

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

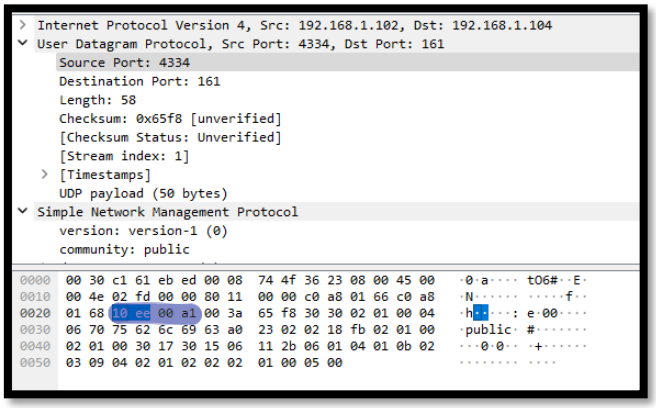
6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

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.

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields. **source port, destination port, length, and checksum.**



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. **8 bytes Each header fields are 2 bytes long**

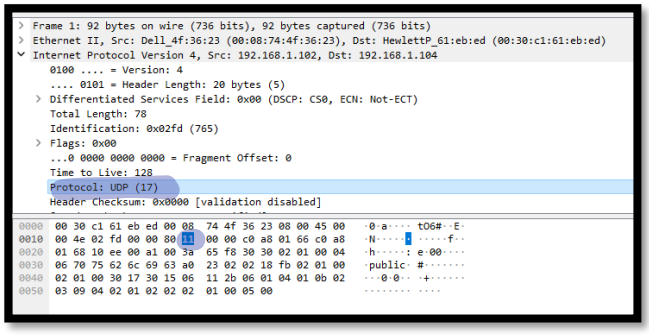


3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet. **The value in the length field is 58 it is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet.**

4. What is the maximum number of bytes that can be included in a UDP payload? **The maximum number of bytes that can be in the payload is 2^16- the bytes already being used by the header field (8). Therefore, the maximum payload is 65535-8= 65527 bytes.**

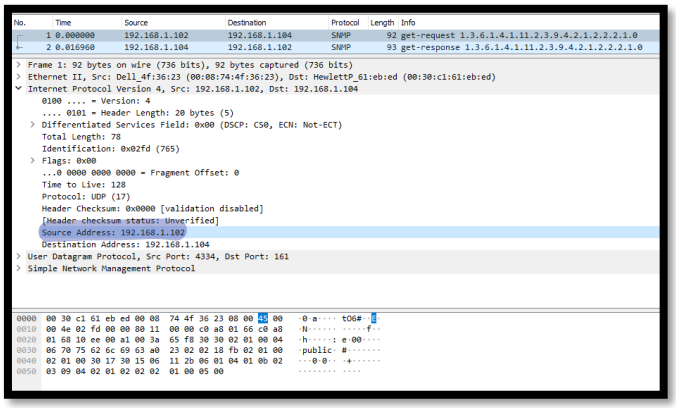
5. What is the largest possible source port number? **The largest possible source port number is 2^16 or 65535.**

6. What is the protocol number for UDP? **The protocol number for UDP is 17 in decimal notation which in hexadecimal notation is 0x11.**

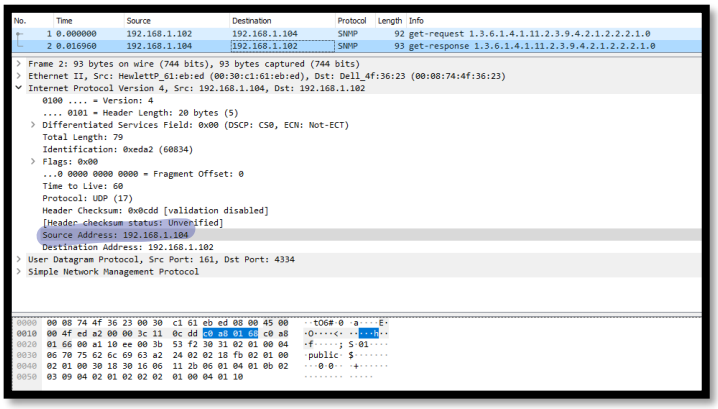


7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet.

UDP Sent by my host



UDP Reply to Host



the relationship between port numbers is that the source port on the send message is the destination port of the receive message. The destination port for the send message is also the source port for the receive message.