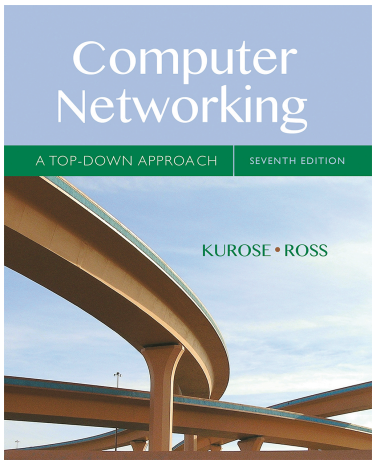
Wireshark Lab: UDP v7.0

Supplement to *Computer Networking: A Top-Down Approach, 7th ed.,* J.F. Kurose and K.W. Ross



"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

---

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. 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.[2]

---

[1] References to figures and sections are for the 7th edition of our text, *Computer Networks, A Top-down Approach, 7th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.*

[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

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[3] 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.

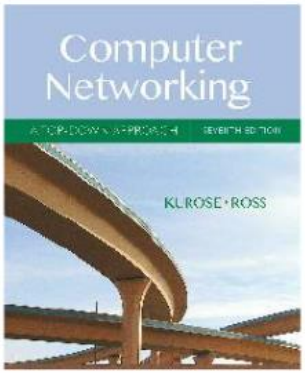
1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.
2. By consulting the displayed information in Wireshark's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

---

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.

[3] 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.

Wireshark Lab: UDP
SOLUTION



Supplement to *Computer Networking: A Top-Down Approach, 7th ed.*, J.F. Kurose and K.W. Ross

---

The answers below are based on the trace file http-ethereal-trace-5, in

http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

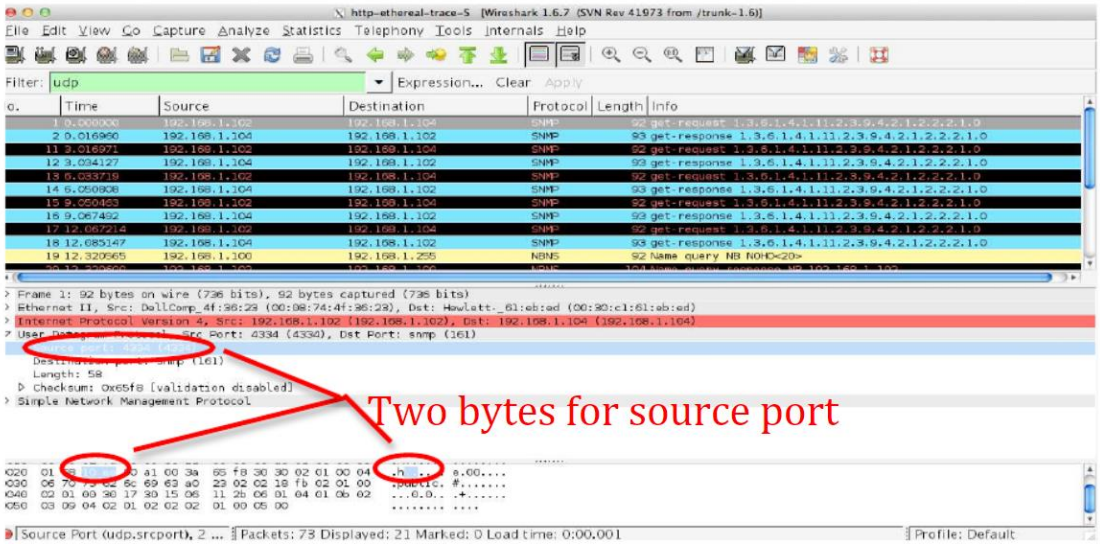
Here is what is printed out for packet 1 in this trace:

```
No.     Time        Source                Destination
Protocol Length Info
      1 0.000000    192.168.1.102         192.168.1.104         SNMP
92     get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst:
Hewlett-_61:eb:ed (00:30:c1:61:eb:ed)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102),
Dst: 192.168.1.104 (192.168.1.104)
User Datagram Protocol, Src Port: 4334 (4334), Dst Port: snmp (161)
    Source port: 4334 (4334)
    Destination port: snmp (161)
    Length: 58
    Checksum: 0x65f8 [validation disabled]
Simple Network Management Protocol
```

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. *Answer: There are four fields in the header: 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. *Answer: by clicking on the source port field (top red circle in the figure below), we see the value corresponding to that port number value in the packet content window at the bottom of the Wireshark display. The port number is shown as a hexadecimal number (small lower left red circle) and in ASCII format (small lower right red circle), and is two 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. *Answer: The UDP length field is the length of the header and data fields of the UDP segment, measured in bytes)." The displayed packet has a length field of 58 bytes. We know there are 8 byres of header. If we look at the packet content field, we also find 50 bytes of hexadecimal or ASCII-encoded data which corresponds to the payload of this UDP segment.*
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). *Answer: Since there are only 16 bits, the maximum length of a UDP segment (including header) is 2**16 -1 or 65535 bytes.*
5. What is the largest possible source port number? (Hint: see the hint in 4.) *Answer: Since there are only 16 bits, the maximum source port number is 2**16 -1 or 65535 bytes.*
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). *Answer: UDP has a protocol number of 17 (this number is displayed in Wireshark as the value of the "protocol:" field in the IPV4 datagram.*
7. 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. *Answer: Let's look at packets 1 and 2 in the trace. These packets carry SNMP application-level messages encapsulated inside of UDP. (Got that? If not, re-read section 1.5 and Figure 1.24 in the text, in particular) The IP address of the sender of packet 1 is the IP address of the destination of packet 2, and the IP address of the destination of packet 1 is the IP*

address of the sender of packet 2, The names in the Info field of get-request and get-response suggest that the second packet (a response) is sent in reply to the first packet (a request). Indeed this is the case. The value of the source port in packet 1 is the value of the destination port of packet 2; the value of the destination port of packet 1 is the value of the source port of packet 2,