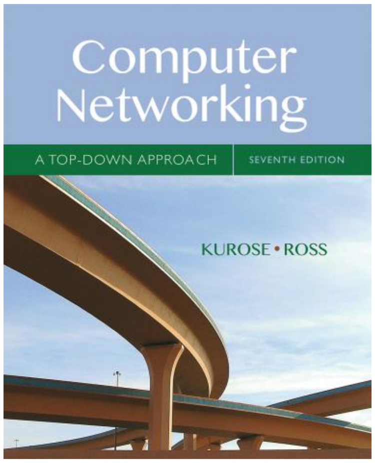
Wireshark Lab: UDP v7.0

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.

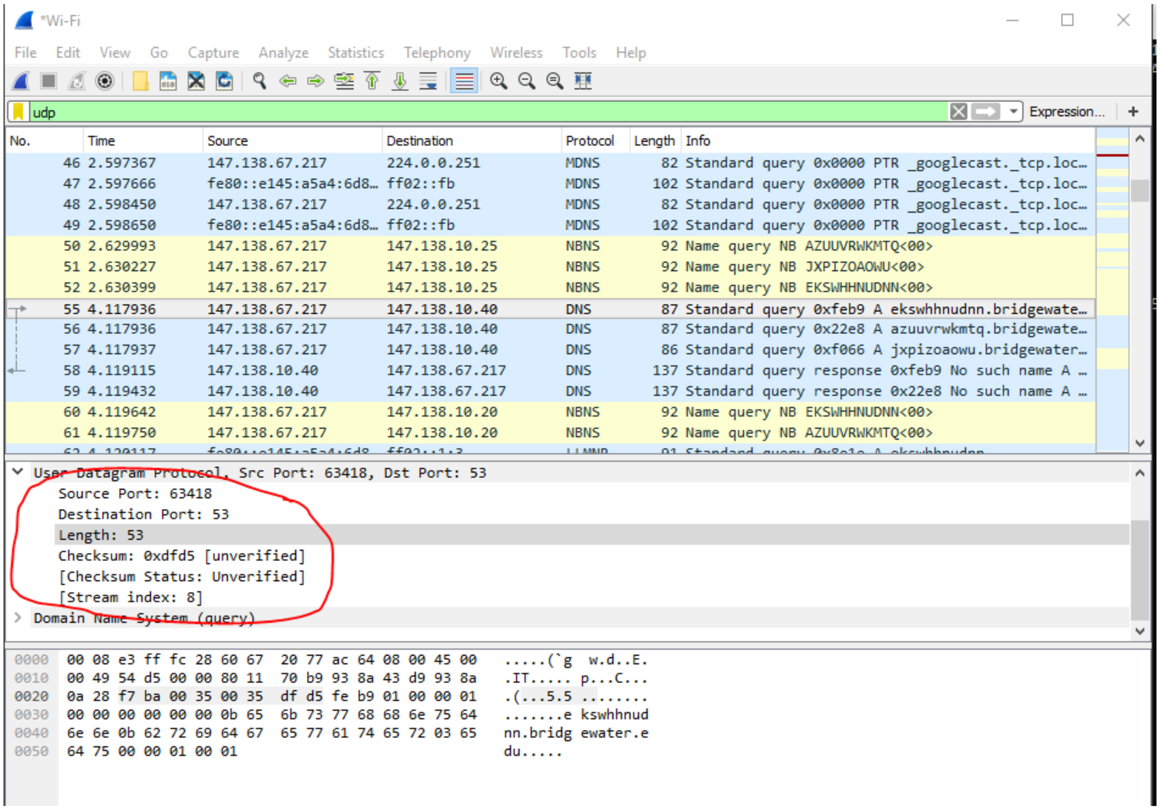
After stopping packet capture, set your packet filter so that Wireshark only displays the UDP packets sent and received at your host. Pick one of these UDP packets and expand the UDP fields in the details window. If you are unable to find UDP packets or are unable to run Wireshark on a live network connection, 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

Include a screen shot with each question were ever possible.

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. (Don't include the fields in brackets)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp

No.	Time	Source	Destination	Protocol	Length	Info
46	2.597367	147.138.67.217	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.loc…
47	2.597666	fe80::e145:a5a4:6d8…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.loc…
48	2.598450	147.138.67.217	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.loc…
49	2.598650	fe80::e145:a5a4:6d8…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.loc…
50	2.629993	147.138.67.217	147.138.10.25	NBNS	92	Name query NB AZUUVRWKMTQ<00>
51	2.630227	147.138.67.217	147.138.10.25	NBNS	92	Name query NB JXPIZOAOWU<00>
52	2.630399	147.138.67.217	147.138.10.25	NBNS	92	Name query NB EKSWHHNUDNN<00>
55	4.117936	147.138.67.217	147.138.10.40	DNS	87	Standard query 0xfeb9 A ekswhhnudnn.bridgewate…
56	4.117936	147.138.67.217	147.138.10.40	DNS	87	Standard query 0x22e8 A azuuvrwkmtq.bridgewate…
57	4.117937	147.138.67.217	147.138.10.40	DNS	86	Standard query 0xf066 A jxpizoaowu.bridgewater…
58	4.119115	147.138.10.40	147.138.67.217	DNS	137	Standard query response 0xfeb9 No such name A …
59	4.119432	147.138.10.40	147.138.67.217	DNS	137	Standard query response 0x22e8 No such name A …
60	4.119642	147.138.67.217	147.138.10.20	NBNS	92	Name query NB EKSWHHNUDNN<00>
61	4.119750	147.138.67.217	147.138.10.20	NBNS	92	Name query NB AZUUVRWKMTQ<00>

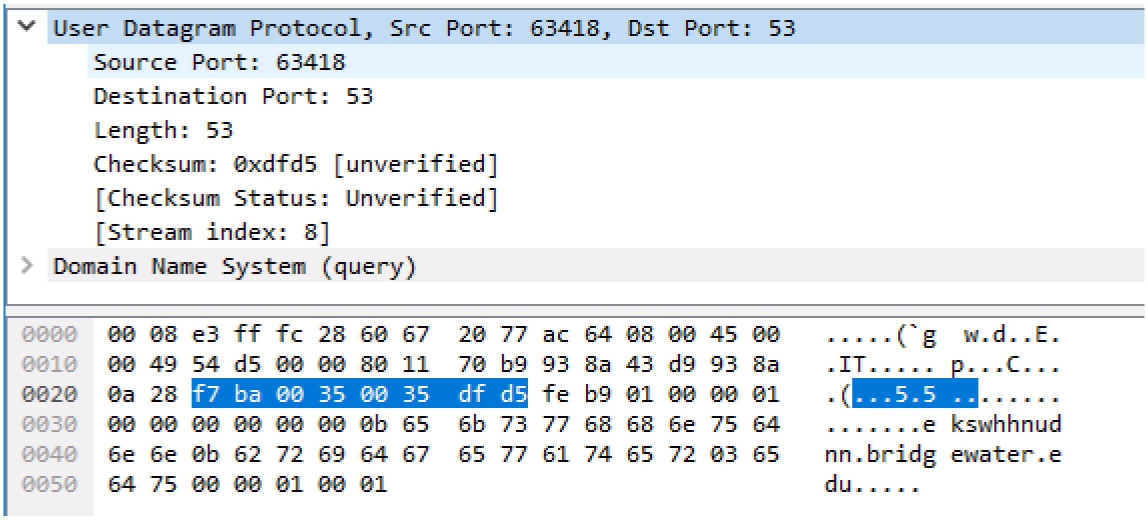
```
User Datagram Protocol, Src Port: 63418, Dst Port: 53
    Source Port: 63418
    Destination Port: 53
    Length: 53
    Checksum: 0xdfd5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 8]
Domain Name System (query)
```

```
0000  00 08 e3 ff fc 28 60 67  20 77 ac 64 08 00 45 00   .....(`g  w.d..E.
0010  00 49 54 d5 00 00 80 11  70 b9 93 8a 43 d9 93 8a   .IT..... p...C...
0020  0a 28 f7 ba 00 35 00 35  df d5 fe b9 01 00 00 01   .(...5.5 ........
0030  00 00 00 00 00 00 0b 65  6b 73 77 68 68 6e 75 64   .......e kswhhnud
0040  6e 6e 0b 62 72 69 64 67  65 77 61 74 65 72 03 65   nn.bridg ewater.e
0050  64 75 00 00 01 00 01                               du.....
```

Source Port, Destination Port, Length, 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.

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.



```
v User Datagram Protocol, Src Port: 63418, Dst Port: 53
     Source Port: 63418
     Destination Port: 53
     Length: 53
     Checksum: 0xdfd5 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 8]
> Domain Name System (query)

0000  00 08 e3 ff fc 28 60 67  20 77 ac 64 08 00 45 00   .....(`g  w.d..E.
0010  00 49 54 d5 00 00 80 11  70 b9 93 8a 43 d9 93 8a   .IT..... p...C...
0020  0a 28 f7 ba 00 35 00 35  df d5 fe b9 01 00 00 01   .(...5.5 ........
0030  00 00 00 00 00 00 0b 65  6b 73 77 68 68 6e 75 64   .......e kswhhnud
0040  6e 6e 0b 62 72 69 64 67  65 77 61 74 65 72 03 65   nn.bridg ewater.e
0050  64 75 00 00 01 00 01                               du.....
```

Highlighting the field will highlight the corresponding hex value. Each hex value corresponds to 1 byte.

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 (The payload does not include the header) ? (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.