|  |  |
| --- | --- |
| 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  © 2005-2016, J.F Kurose and K.W. Ross, All Rights Reserved |  |

In this lab, we’ll take a quick look at the UDP transport 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 (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.[[1]](#footnote-2)

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.

Four: Source port, destination port, length, and checksum.

1. 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.

2 bytes each.

1. 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 length field is the total UDP packet length in bytes, including its headers and payload.

The UDP portion of the captured packet is the hex dump below:

0020 .. .. a2 59 00 35 00 3c 21 80 77 be 01 00 00 01

0030 00 00 00 00 00 00 12 66 6c 6f 72 69 64 61 70 6f

0040 6c 79 74 65 63 68 6e 69 63 0b 69 6e 73 74 72 75

0050 63 74 75 72 65 03 63 6f 6d 00 00 01 00 01

1. 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)

2 bytes size: 216 – 4 bytes

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

65535

1. 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).

17 == 0x11

1. Download the zip file [http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip](http://gaia.cs.umass.edu/ethereal-labs/ethereal-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. [↑](#footnote-ref-2)