



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: UDP Protocol

In this lab, we'll take a quick look at the UDP transport protocol. As we saw in Chapter 3 of the text¹⁰, 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 printout¹² 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.**

```
> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: HewlettP_61:eb:ed (00:30:c1:61:eb:ed)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
▼ User Datagram Protocol, Src Port: 4334, Dst Port: 161
    Source Port: 4334
    Destination Port: 161
    Length: 58
    Checksum: 0x65f8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
> [Timestamps]
    UDP payload (50 bytes)
> Simple Network Management Protocol
```

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

```
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
▼ User Datagram Protocol, Src Port: 4334, Dst Port: 161
    Source Port: 4334
    Destination Port: 161
    Length: 58
    Checksum: 0x65f8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
> [Timestamps]
    UDP payload (50 bytes)
▼ Simple Network Management Protocol
    version: version-1 (0)
    community: public
```

0000	00 30 c1 61 eb ed 00 08	74 4f 36 23 08 00 45 00	0 a t06# . E .
0010	00 4e 02 fd 00 00 00 11	00 00 c0 a8 01 66 c0 a8	N f . .
0020	01 68 10 cc 00 3a 65 f8	30 30 02 01 00 04	h e 00 . .
0030	06 70 75 62 6c 69 63 a0	23 02 02 18 fb 02 01 00	public #
0040	02 01 00 30 17 30 15 06	11 2b 06 01 04 01 0b 02	. . 0 . . +
0050	03 09 04 02 01 02 02 02	01 00 05 00

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.

```
> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: HewlettP_61:eb:ed (00:30:c1:61:eb:ed)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 78
  Identification: 0x02fd (765)
> Flags: 0x00
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]

0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00 0-a-t06#-E-
0010 00 4e 02 fd 00 00 00 11 00 00 c0 a8 01 66 c0 a8 0-.....f-
0020 01 68 10 ee 00 a1 00 3a 65 f8 30 30 02 01 00 04 h-.....e-0-
0030 06 70 75 62 6c 69 63 a0 23 02 02 18 fb 02 01 00 public-#-.....
0040 02 01 00 30 17 30 15 06 11 2b 06 01 04 01 0b 02 --0-0-+.....
0050 03 09 04 02 01 02 02 02 01 00 05 00 .....
```

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

```
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
2 0.016960 192.168.1.104 192.168.1.102 SNMP 93 get-response 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: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: HewlettP_61:eb:ed (00:30:c1:61:eb:ed)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 78
  Identification: 0x02fd (765)
> Flags: 0x00
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 192.168.1.104
> User Datagram Protocol, Src Port: 4334, Dst Port: 161
> Simple Network Management Protocol

0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00 0-a-t06#-
0010 00 4e 02 fd 00 00 00 11 00 00 c0 a8 01 66 c0 a8 0-.....f-
0020 01 68 10 ee 00 a1 00 3a 65 f8 30 30 02 01 00 04 h-.....e-0-
0030 06 70 75 62 6c 69 63 a0 23 02 02 18 fb 02 01 00 public-#-.....
0040 02 01 00 30 17 30 15 06 11 2b 06 01 04 01 0b 02 --0-0-+.....
0050 03 09 04 02 01 02 02 02 01 00 05 00 .....
```

UDP Reply to Host

```
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
2 0.016960 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

> Frame 2: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
> Ethernet II, Src: HewlettP_61:eb:ed (00:30:c1:61:eb:ed), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 79
  Identification: 0xa2da (68034)
> Flags: 0x00
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 60
  Protocol: UDP (17)
  Header Checksum: 0x0cdd [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.104
  Destination Address: 192.168.1.102
> User Datagram Protocol, Src Port: 161, Dst Port: 4334
> Simple Network Management Protocol

0000 00 08 74 4f 36 23 00 30 c1 61 eb ed 00 00 45 00 --t06#0-a-...E-
0010 00 4f ed a2 00 00 3c 11 0c dd 00 01 01 c0 a8 --0-....<-...-
0020 01 68 00 a1 10 ee 00 3b 53 f2 30 11 02 01 00 04 -f-...;5-0-...
0030 06 70 75 62 6c 69 63 a2 24 02 02 18 fb 02 01 00 public-$-.....
0040 02 01 00 30 18 30 16 06 11 2b 06 01 04 01 0b 02 --0-0-+.....
0050 03 09 04 02 01 02 02 02 01 00 04 01 10 .....
```

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.