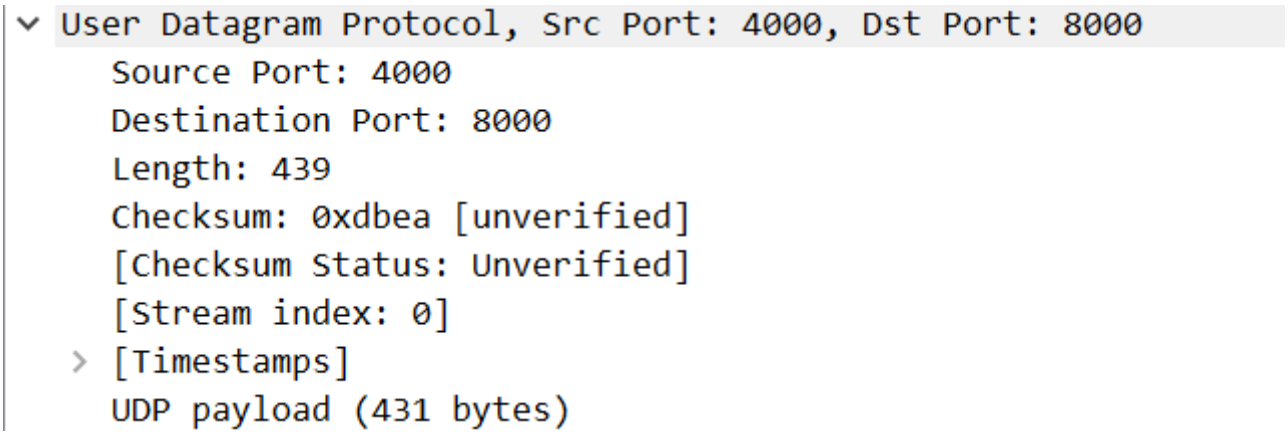
Computer Network Study Lab 4

- Author:PB19000362 钟书锐
- Time:2021.10.15

Q1. 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.



- How many fields in the UDP header： UDP 头部一共有四个字段：分别是 Source Port，Destination Port，Length，Checksum
- eg:抓的包为例
  - User Datagram Protocol, Src Port: 4000, Dst Port: 8000
  - Source Port: 4000
  - Destination Port: 8000
  - Length: 439
  - Checksum: 0xdbea [unverified]

Q2. 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.

```
User Datagram Protocol, Src Port: 4000, Dst Port: 8000
    Source Port: 4000
    Destination Port: 8000
    Length: 439
    Checksum: 0xdbea [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (431 bytes)
Data (431 bytes)
    Data: 023a2103fb7cbe4ffb39ba0400000001010100006a1d0000000000000000c7bf7ce26786…
```

```
0020  b4 a9 0f a0 1f 40 01 b7  db ea 02 3a 21 03 fb 7c   ·····@·· ···:!··|
0030  be 4f fb 39 ba 04 00 00  00 01 01 01 00 00 6a 1d   ·O·9···· ······j·
0040  00 00 00 00 00 00 00 00  c7 bf 7c e2 67 86 1c f9   ········ ··|·g···
0050  e8 3c 7d 17 d3 e5 a8 46  18 1d 7f cc de a5 8e 0b   ·<}····F ········
0060  f6 f9 c6 4f ba 92 49 37  1c f4 dc 66 02 81 b1 de   ···O··I7 ···f····
0070  23 d5 f7 d9 43 c8 74 62  91 92 6d 23 28 19 5e 8a   #···C·tb ··m#(·^·
0080  04 05 66 bc 30 3d 01 f3  78 88 24 30 77 1b 74 07   ··f·0=·· x·$0w·t·
0090  5b 40 b0 6b e7 c2 25 e6  bf 9a 8a 59 3b 43 aa ce   [@·k··%· ···Y;C··
```

- UDP 头部的大小: 439 bytes - 431 bytes = 8bytes
- 比如截图中
  1. 0f a0 2 个字节代表 Source Port: 4000
  2. 1f 40 2 个字节代表 Destination Port: 8000
  3. 01 b7 2 个字节代表 Length: 439
  4. db ea 2 个字节代表 Checksum: 0xdbe
- 所以 UDP 头部的每个字段的大小 : 2 bytes

Q3. 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.

```
User Datagram Protocol, Src Port: 4000, Dst Port: 8000
    Source Port: 4000
    Destination Port: 8000
    Length: 439
    Checksum: 0xdbea [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (431 bytes)
Data (431 bytes)
    Data: 023a2103fb7cbe4ffb39ba0400000001010100006a1d0000000000000000c7bf7ce26786…
    [Length: 431]
```

- Length 表示整个 UDP 报文段的字节数（首部加数据）
- length = 8（UDP 头部的大小） + lenth of the data
- eg:抓的包为例
  1. lenth = 439 bytes
  2. lenth of the data:431 bytes

Q4. 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)

- length 为 2 字节(16 位),
- 所以 lenth 最大值为 max_lenth=2^16-1=65535 代表 65535 bytes
- payload 有效负载只包含 data 段，减去 UDP 头部大小
- max_lenth -8 = 65527 bytes
- 所以 UDP 最大有效负载 65527 bytes

Q5. What is the largest possible source port number? (Hint: see the hint in 4.)

- source port number 也是 2 字节(16 位)
- 最大值为 max_port number=2^16-1=65535
- source port number 的范围 0-65535
- 最大源端口号是 65535

Q6. 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).

```
Internet Protocol Version 4, Src: 192.168.39.57, Dst: 61.151.180.169
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 459
    Identification: 0x9d56 (40278)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.39.57
    Destination Address: 61.151.180.169
```

- Protocol: UDP (17)
- The UDP protocol number in decimal is: 17
- The UDP protocol number in hexadecimal is: 0x11

Q7. 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.

No.	Time	Source	Destination	Protocol	Length	Info
24	0.860203	192.168.39.198	192.168.39.57	DNS	366	Standard query response 0x644e A fp-vs.azureedge.net CNAME fp-
44	2.074135	61.151.180.169	192.168.39.57	OICQ	377	OICQ Protocol
45	2.074345	192.168.39.57	61.151.180.169	OICQ	97	OICQ Protocol
56	2.294661	61.151.180.169	192.168.39.57	OICQ	129	OICQ Protocol
75	2.884780	61.151.180.169	192.168.39.57	OICQ	129	OICQ Protocol
78	3.484638	61.151.180.169	192.168.39.57	OICQ	129	OICQ Protocol
79	3.627576	61.151.180.169	192.168.39.57	OICQ	609	OICQ Protocol
80	3.627817	192.168.39.57	61.151.180.169	OICQ	97	OICQ Protocol
85	4.593687	61.151.180.169	192.168.39.57	OICQ	337	OICQ Protocol
86	4.593862	192.168.39.57	61.151.180.169	OICQ	97	OICQ Protocol
87	4.714763	192.168.39.57	61.151.180.169	UDP	473	4000 → 8000 Len=431
88	4.716617	192.168.39.57	61.151.180.169	UDP	745	4000 → 8000 Len=703
89	4.752673	61.151.180.169	192.168.39.57	OICQ	129	OICQ Protocol
90	4.782069	61.151.180.169	192.168.39.57	UDP	113	8000 → 4000 Len=71

```
> Frame 87: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, i
> Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
> Internet Protocol Version 4, Src: 192.168.39.57, Dst: 61.151.180.169
v User Datagram Protocol, Src Port: 4000, Dst Port: 8000
    Source Port: 4000
    Destination Port: 8000
    Length: 439
    Checksum: 0xdbea [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (431 bytes)
> Data (431 bytes)
```

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

udp

No.	Time	Source	Destination	Protocol	Length	Info
79	3.627576	61.151.180.169	192.168.39.57	OICQ	609	OICQ Protocol
80	3.627817	192.168.39.57	61.151.180.169	OICQ	97	OICQ Protocol
85	4.593687	61.151.180.169	192.168.39.57	OICQ	337	OICQ Protocol
86	4.593862	192.168.39.57	61.151.180.169	OICQ	97	OICQ Protocol
87	4.714763	192.168.39.57	61.151.180.169	UDP	473	4000 → 8000 Len=431
88	4.716617	192.168.39.57	61.151.180.169	UDP	745	4000 → 8000 Len=703
89	4.752673	61.151.180.169	192.168.39.57	OICQ	129	OICQ Protocol
90	4.782069	61.151.180.169	192.168.39.57	UDP	113	8000 → 4000 Len=71
91	4.782069	61.151.180.169	192.168.39.57	UDP	113	8000 → 4000 Len=71
94	5.719138	61.151.180.169	192.168.39.57	OICQ	129	OICQ Protocol
95	6.090714	61.151.180.169	192.168.39.57	OICQ	393	OICQ Protocol
96	6.091366	192.168.39.57	61.151.180.169	OICQ	97	OICQ Protocol
97	6.358659	61.151.180.169	192.168.39.57	OICQ	385	OICQ Protocol
98	6.358848	192.168.39.57	61.151.180.169	OICQ	97	OICQ Protocol

```
> Frame 90: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0), Dst: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c)
> Internet Protocol Version 4, Src: 61.151.180.169, Dst: 192.168.39.57
v User Datagram Protocol, Src Port: 8000, Dst Port: 4000
    Source Port: 8000
    Destination Port: 4000
    Length: 79
    Checksum: 0x8d92 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (71 bytes)
v Data (71 bytes)
```

- 第一个 packet 的源端口号是第二个 packet 的目标端口号
- 第二个 packet 的源端口号是第一个 packet 的目标端口号
- 例如
  - 第一个包源端口号是 4000 目标端口号是 8000
  - 第二个包源端口号是 8000 目标端口号是 4000

```
No.     Time           Source                Destination           Protocol Length Info
     87 4.714763       192.168.39.57         61.151.180.169        UDP      473    4000 → 8000 Len=431
Frame 87: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-
BB3C-4A3C9BE2354E}, id 0
Ethernet II, Src: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c), Dst: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0)
Internet Protocol Version 4, Src: 192.168.39.57, Dst: 61.151.180.169
User Datagram Protocol, Src Port: 4000, Dst Port: 8000
    Source Port: 4000
    Destination Port: 8000
    Length: 439
    Checksum: 0xdbea [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
    UDP payload (431 bytes)
Data (431 bytes)
0000  02 3a 21 03 fb 7c be 4f fb 39 ba 04 00 00 00 01   .:!..|.O.9......
0010  01 01 00 00 6a 1d 00 00 00 00 00 00 00 c7 bf   ....j...........
0020  7c e2 67 86 1c f9 e8 3c 7d 17 d3 e5 a8 46 18 1d   |.g....<}....F..
0030  7f cc de a5 8e 0b f6 f9 c6 4f ba 92 49 37 1c f4   .........O..I7..
0040  dc 66 02 81 b1 de 23 d5 f7 d9 43 c8 74 62 91 92   .f....#...C.tb..
0050  6d 23 28 19 5e 8a 04 05 66 bc 30 3d 01 f3 78 88   m#(.^...f.0=..x.
0060  24 30 77 1b 74 07 5b 40 b0 6b e7 c2 25 e6 bf 9a   $0w.t.[@.k..%...
0070  8a 59 3b 43 aa ce 8c 19 aa 5c aa ed 19 e3 5f df   .Y;C.....\....._.
0080  a1 63 4f cb fc 78 e3 f7 55 fe 08 81 58 f6 4e 0d   .cO..x..U...X.N.
0090  f5 26 4c 1d 79 39 ec 3c bf d2 d7 58 7d a6 58 8a   .&L.y9.<...X}.X.
00a0  5e ab eb 3e 46 44 c2 90 6e 49 7a 96 10 07 fd d3   ^..>FD..nIz.....
00b0  7e 66 a0 bd 25 11 dd bf 88 31 cf f1 61 1f 99 af   ~f..%....1..a...
00c0  53 c1 99 1d 41 21 bf f3 bd cf a1 2f de b1 70 b6   S...A!...../..p.
00d0  e5 eb 35 51 6d b1 ee 50 ae 20 a3 f9 af 86 8a fc   ..5Qm..P. ......
00e0  45 b4 56 ea 52 59 97 c6 49 68 5a 45 39 7b b0 0b   E.V.RY..IhZE9{..
00f0  70 ca 04 ff 4c 59 f8 b7 e8 9f 0f 80 c6 02 b6 e0   p...LY..........
0100  c6 23 96 0b f1 54 bd 0a 66 5e 0e 9e 6d db ab d5   .#...T..f^..m...
0110  97 25 e1 b0 d3 a3 b1 67 26 2a a0 72 22 1c 04 62   .%.....g&*.r"..b
0120  4b ff 96 0e 32 51 4e dd 16 a0 75 90 0a 73 2a 06   K...2QN...u..s*.
0130  45 a1 2b 59 d6 47 69 9d c2 d4 bb 81 cf a0 c6 85   E.+Y.Gi.........
0140  e4 bf b7 e6 f0 ce 2a 04 12 40 eb 1c bb f8 c9 39   ......*..@.....9
0150  fe be 7c bf 1f ca d4 63 6d 65 a3 30 24 a7 5b c7   ..|....cme.0$.[.
0160  aa 8d 74 c0 9c 30 eb 94 c2 cd 36 19 4d 66 b2 9d   ..t..0....6.Mf..
0170  02 07 cd 7c 3a 8f 3f 14 fa 7c 9a 86 16 ed 3e 9d   ...|:.?..|....>.
0180  2c 30 9c 2a eb ba a5 d4 33 a7 42 bd 1f b4 f8 bd   ,0.*....3.B.....
0190  46 00 ce db e1 6a ae fd cb 31 dd d0 f9 eb e6 81   F....j...1......
01a0  71 c9 fe 6d 63 9a db a1 1e fe 17 4e ca 2b 03      q..mc......N.+.
    Data: 023a2103fb7cbe4ffb39ba040000000101010000 6a1d0000000000000000c7bf7ce26786…
    [Length: 431]
No.     Time           Source                Destination           Protocol Length Info
     90 4.782069       61.151.180.169        192.168.39.57         UDP      113    8000 → 4000 Len=71
Frame 90: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-
BB3C-4A3C9BE2354E}, id 0
Ethernet II, Src: 92:a7:22:ec:13:b0 (92:a7:22:ec:13:b0), Dst: IntelCor_b5:68:3c (c8:58:c0:b5:68:3c)
Internet Protocol Version 4, Src: 61.151.180.169, Dst: 192.168.39.57
User Datagram Protocol, Src Port: 8000, Dst Port: 4000
    Source Port: 8000
    Destination Port: 4000
    Length: 79
    Checksum: 0x8d92 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
    UDP payload (71 bytes)
Data (71 bytes)
0000  02 3a 21 03 fb 7c be 4f fb 39 ba 00 04 00 7f 67   .:!..|.O.9.....g
0010  97 75 44 a7 6f df c0 7f dd fa 85 af d5 d3 28 ec   .uD.o.........(.
0020  03 bb d2 0e 61 01 53 e6 1c 9b 50 6a 82 8d 6d 25   ....a.S...Pj..m%
0030  60 c8 0a 2c 40 c3 7c df df b9 14 b5 86 90 8e f0   `..,@.|.........
0040  d9 66 e5 bf 08 11 03                              .f.....
    Data: 023a2103fb7cbe4ffb39ba0004007f67977544a76fdfc07fddfa85afd5d328ec03bbd20e…
    [Length: 71]
```