

实验四 UDP

张舒恒 PB19030888

实验目的

- 1.快速简单了解 UDP 协议
- 2.了解 UDP 的标头数据, 报文段数据结构

实验环境

pc一台, win10操作系统, wireshark工具, 浏览器

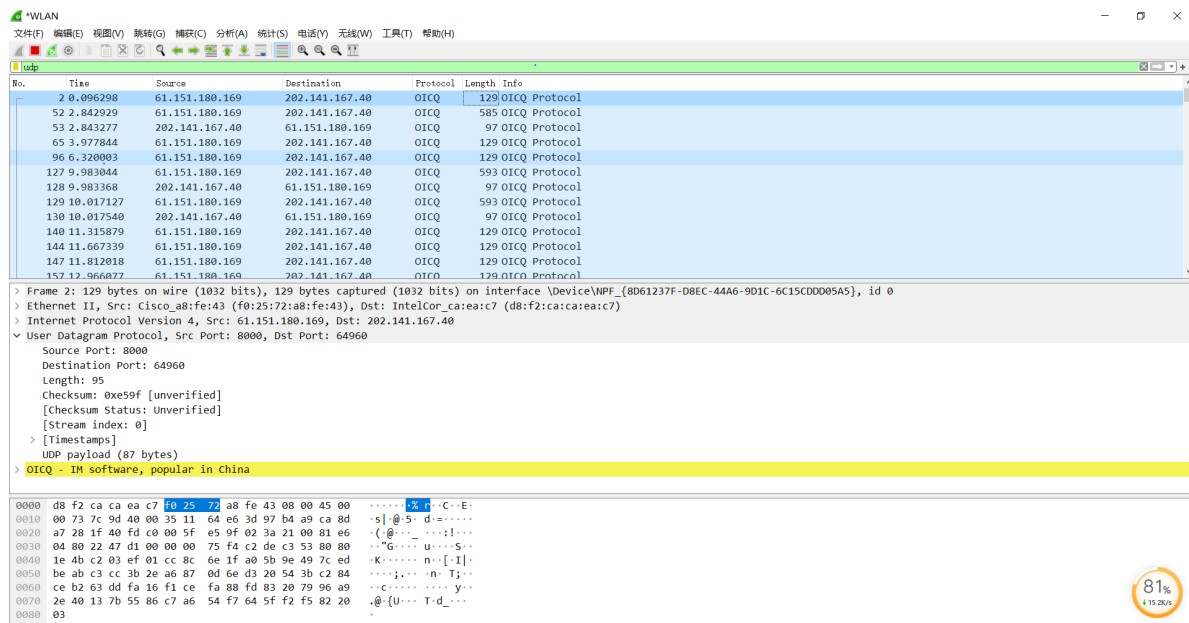
实验步骤

- 1.启动wireshark, 选择wlan开始捕获。
- 2.启动浏览器
- 3.关闭捕获
- 4.使用过滤器过滤UDP协议
- 5.截图, 打印并分析报文

问题回答

1.从跟踪中选择一个 UDP 数据包。从此数据包中, 确定 UDP 标头中有多少字段。(建议不要查看课本, 直接根据您的数据包跟踪结果回答), 并为这些字段命名。

UDP 头包括4个部分, 每个部分2Byte。分别是Source Port源端口号, Destination Port目标端口号, Length报文长度(包括 UDP 头+数据长度), Checksum校验和(可选, 用来数据校验)。



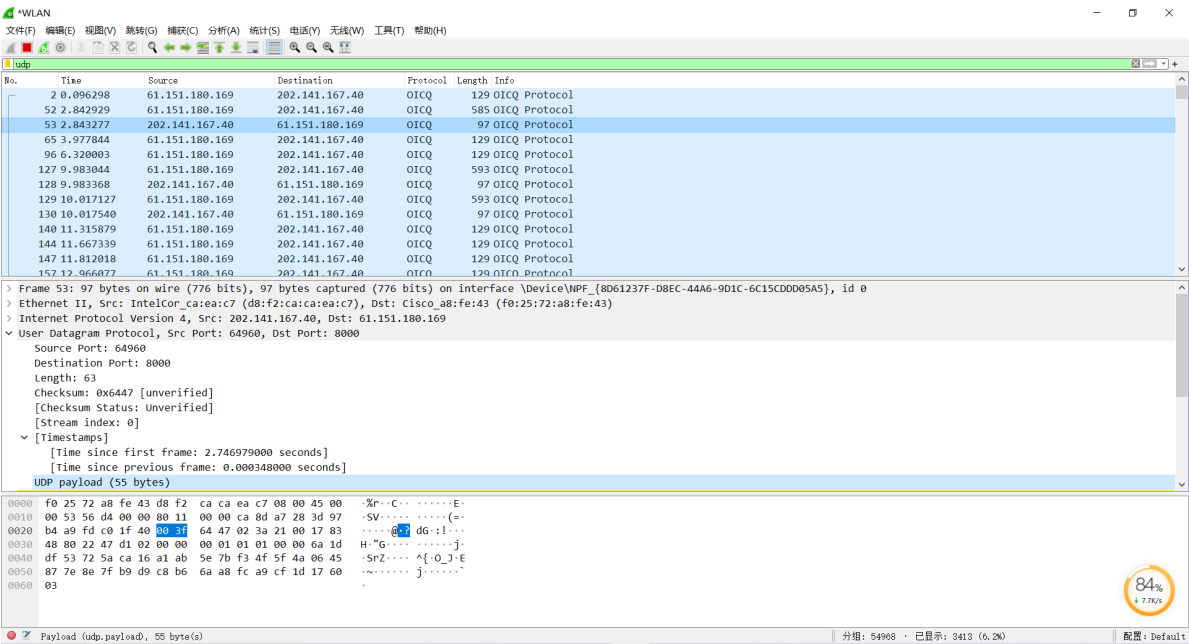
Wireshark packet capture analysis of a UDP packet. The packet list shows a UDP packet at time 2.0096298. The packet details pane shows the UDP header fields: Source Port: 8000, Destination Port: 64960, Length: 95, Checksum: 0xe59f. The packet bytes pane shows the raw data in hexadecimal and ASCII.

2.通过查询 Wireshark 的数据包内容字段中显示的信息, 确定每个 UDP 报头字段的长度 (以字节为单位)

每个字段两个字节。

3.长度字段中的值是指的是什么？（此问题您可以参考课本）。使用捕获的 UDP 数据包验证您的声明。

长度是UDP 头+数据长度，UDP 头8Byte，这里数据长度55Byte，所以Length=63Byte



4.UDP 有效负载中可包含的最大字节数是多少？（提示：这个问题的答案可以通过你对上述 2 的回答来确定）

在一个UDP负载中最多可以包含的字节数为 $2^{16} - 1 = 65535$ ，除去首部8字节，则最多65527个字节。

5.最大可能的源端口号是多少？（提示：见 4 中的提示）

最大可能的源端口号是65535。

6.UDP 的协议号是什么？以十六进制和十进制表示法给出答案。要回答这个问题，您需要查看包含此 UDP 段的 IP 数据报的 Protocol 字段（参见书中的图 4.13 和 IP 头字段的讨论）。

十六进制：0x11，十进制：17

```
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 83
  Identification: 0x56d4 (22228)
> Flags: 0x00
  Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 202.141.167.40
  Destination Address: 61.151.180.169
v User Datagram Protocol, Src Port: 64960, Dst Port: 8000
```

7.观察发送 UDP 数据包后接收响应的 UDP 数据包，这是对发送的 UDP 数据包的回复，请描述两个数据包中端口号之间的关系。（提示：对于响应 UDP 目的地应该为发送UDP 包的地址）

发送者发送端口号在接收返回（响应）UDP 时候会变成接收端口号，接收者发送返回（响应）UDP 时候接受端口号会变成发送端口号。

WLAN

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

l uap

No.	Time	Source	Destination	Protocol	Length	Info
2	0.096298	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol
52	2.842929	61.151.180.169	202.141.167.40	OICQ	585	OICQ Protocol
53	2.843277	202.141.167.40	61.151.180.169	OICQ	97	OICQ Protocol
65	3.977844	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol
96	6.320003	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol
127	9.983044	61.151.180.169	202.141.167.40	OICQ	593	OICQ Protocol
128	9.983368	202.141.167.40	61.151.180.169	OICQ	97	OICQ Protocol
129	10.017127	61.151.180.169	202.141.167.40	OICQ	593	OICQ Protocol
130	10.017540	202.141.167.40	61.151.180.169	OICQ	97	OICQ Protocol
140	11.315879	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol
144	11.667339	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol
147	11.812018	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol

> Frame 53: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface \Device\NPF_{8061237F-D8EC-44A6-901C-6C15CDD005A5}, id 0
> Ethernet II, Src: IntelCor_ca:ea:c7 (d8:f2:ca:ca:ea:c7), Dst: Cisco_a8:fe:43 (f0:25:72:a8:fe:43)
> Internet Protocol Version 4, Src: 202.141.167.40, Dst: 61.151.180.169
> User Datagram Protocol, Src Port: 64960, Dst Port: 8000
> OICQ - IM software, popular in China

0000 f0 25 72 a8 fe 43 d8 f2 ca ca ea c7 08 00 45 00 %r--C-E-
0010 00 53 56 d4 00 00 80 00 00 ca 8d a7 28 3d 97 :SV+.... (=-
0020 b4 a9 f0 c0 1f 40 00 3f 64 47 02 3a 21 00 17 83 :...@-? dG:|...
0030 48 80 22 47 d1 02 00 00 00 01 01 00 00 6a 1d H"G.....j:
0040 df 53 72 5a ca 16 a1 ab 5e 7b f3 4f 5f 4a 06 45 :SrZ.... ^[-0_}E
0050 87 7e 8e 7f b9 d9 c8 b6 6a a8 fc a9 cf 1d 17 60 :~..... j.....
0060 03

Protocol (ip.proto), 1 byte(s) 分组: 96075 · 已显示: 5748 (6.0%) · 已丢弃: 0 (0.0%) 配置: Default

WLAN

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

l uap

No.	Time	Source	Destination	Protocol	Length	Info
2	0.096298	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol
52	2.842929	61.151.180.169	202.141.167.40	OICQ	585	OICQ Protocol
53	2.843277	202.141.167.40	61.151.180.169	OICQ	97	OICQ Protocol
65	3.977844	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol
96	6.320003	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol
127	9.983044	61.151.180.169	202.141.167.40	OICQ	593	OICQ Protocol
128	9.983368	202.141.167.40	61.151.180.169	OICQ	97	OICQ Protocol
129	10.017127	61.151.180.169	202.141.167.40	OICQ	593	OICQ Protocol
130	10.017540	202.141.167.40	61.151.180.169	OICQ	97	OICQ Protocol
140	11.315879	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol
144	11.667339	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol
147	11.812018	61.151.180.169	202.141.167.40	OICQ	129	OICQ Protocol

> Frame 65: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface \Device\NPF_{8061237F-D8EC-44A6-901C-6C15CDD005A5}, id 0
> Ethernet II, Src: Cisco_a8:fe:43 (f0:25:72:a8:fe:43), Dst: IntelCor_ca:ea:c7 (d8:f2:ca:ca:ea:c7)
> Internet Protocol Version 4, Src: 61.151.180.169, Dst: 202.141.167.40
> User Datagram Protocol, Src Port: 8000, Dst Port: 64960
> OICQ - IM software, popular in China

0000 d8 f2 ca ca ea c7 f0 25 72 a8 fe 43 08 00 45 00% r--C-..E-
0010 00 73 7e 5c 40 00 35 11 63 27 3d 97 b4 a9 ca 8d :s~\@-5- c'a.....
0020 a7 28 1f 40 fd c0 00 5f 7b a1 02 3a 21 00 81 19 :(.@... (:::|...
0030 90 80 22 47 d1 30 00 00 87 d0 39 8d 75 d6 6b 8f :~"G.... +9-u-k:
0040 0a d2 ca 78 37 09 eb 08 3d 01 26 79 ba 69 ad 01 :...x71.. +8y.i...
0050 9b bf e2 75 c7 27 90 a7 db ef a3 f3 71 f9 fd 55 :...0... ..q-q-d
0060 a9 27 c6 7c 2a e2 d2 a6 00 91 ce f6 ce b8 c7 75 :..|*... ..d
0070 c3 d9 ee d3 0a 19 dc 8e 6a 30 02 dc 8e e0 2b ef :..... j0+...+
0080 03

82% 8°C