

华东师范大学软件工程学院实验报告

实验课程:	计算机网络	年 级:	2022 级
实验编号:	Lab 05	实验名称:	UDP
姓 名:	李鹏达	学 号:	10225101460

1 实验目的

- 1) 学会通过 Wireshark 获取 UDP 消息
- 2) 掌握 UDP 数据包结构
- 3) 掌握 UDP 数据包各字段的含义
- 4) 了解 UDP 协议适用领域

2 实验内容与实验步骤

2.1 实验内容

2.1.1 获取 UDP 消息

启动 Wireshark，在菜单栏的捕获 → 选项中进行设置，选择已连接的以太网，设置捕获过滤器为 `udp`，将混杂模式设为关闭。

点击开始，打开浏览器，在地址栏中输入网址浏览，例如 `www.baidu.com` 或者在命令行中输入 `nslookup www.baidu.com` 查询 DNS 服务器如果没有 DNS 解析，在命令行中输入 `ipconfig /flushdns` 清空 DNS 缓存（`ipconfig /displaydns` 在 windows 下可以使用来获取当前的 DNS 缓存）

然后停止捕获。

2.1.2 分析 UDP 包

选择一个数据帧，分析其 UDP 包头字段。

问题：

- 1) UDP 数据报头中的 `Length` 字段指的是 UDP 有效载荷？还是 UDP 有效载荷加上 UDP 头的总长度？还是 UDP 有效载荷和 UDP 头以及低层协议的头部三者总长度？
- 2) UDP 头中的校验和的长度是多少位？
- 3) 整个 UDP 头的长度是多少字节？

启动命令行，输入 `ipconfig` 获得计算机的 IP 地址，与数据包中的 Source Port 比较。

问题：

- 1) 在 IP 协议中哪个字段指明交给上一层的 UDP 传输进程？该字段值是多少？
- 2) 有的数据包的 source 和 destination IP 地址都不是你计算机的 IP 地址，给出该数据包的 destination IP 地址。
- 3) 一般 UDP 消息的长度是多少？

2.1.3 问题讨论

1. You might examine the traffic of UDP-based applications to look at packet sizes and loss rates. Voice-over-IP and its companion protocols like RTP (Real-Time Protocol) are good candidates.
2. Similarly, you might explore streaming and real-time applications to see which use UDP and which use TCP as a transport.
3. 在计算校验和时，为什么要加上 ipv4 伪头部，伪头部和 UDP 首部中都有 UDP length 字段，该字段出现两次是无意义的重复吗？还是有什么意义？
4. 计算校验和时，为补足偶数字节在 UDP 载荷数据末尾加上的 0，是否在 UDP 长度字段中体现？

2.2 实验步骤

- 1) 启动 Wireshark，在菜单栏的捕获 → 选项中进行设置，选择已连接的以太网，设置捕获过滤器为 `udp`，将混杂模式设为关闭，然后开始捕获。
- 2) 在命令行中输入 `nslookup www.baidu.com` 查询 DNS 服务器

```
1 PS> nslookup www.baidu.com
```

- 3) 打开 Wireshark，停止捕获。
- 4) 分析捕获到的 UDP 数据包，并回答相关问题。
- 5) 问题讨论

3 实验环境

- 操作系统: Windows 11 家庭中文版 23H2 22631.2715
- 网络适配器: Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter(201NGW)
- Wireshark: Version 4.2.0 (v4.2.0-0-g54eedfc63953)
- wget: GNU Wget 1.21.4 built on mingw32

4 实验结果与分析

4.1 获取 UDP 消息

打开 Wireshark, 在菜单栏的捕获 → 选项中进行设置, 选择已连接的以太网, 设置捕获过滤器为 `udp`, 将混杂模式设为关闭。

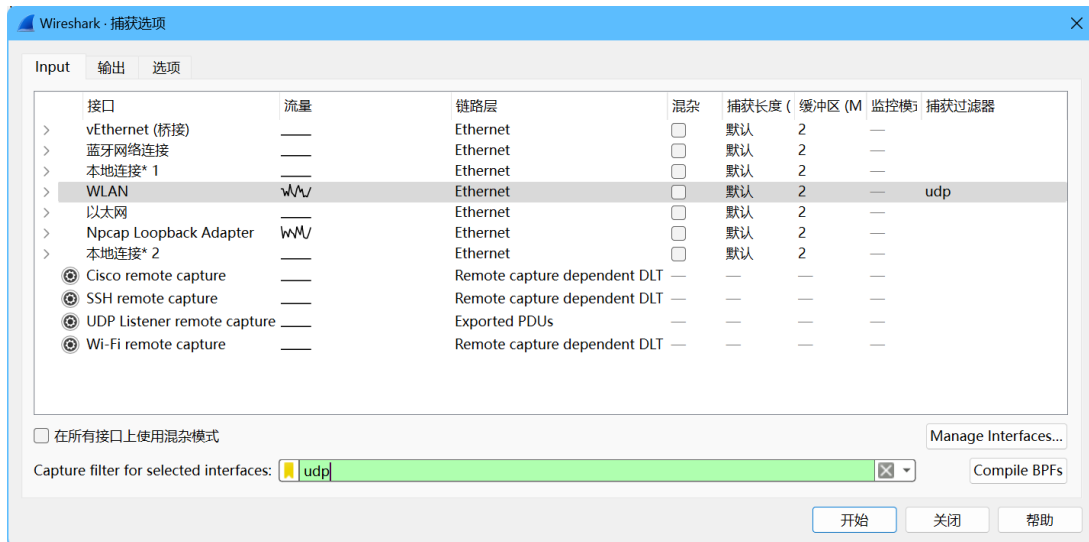


图 1: 设置捕获过滤器

点击开始, 在命令行中输入 `nslookup www.baidu.com` 查询 DNS 服务器。



图 2: 查询 DNS 服务器

捕获结果如下:

357 117.196986	192.168.1.1	239.255.255.250	SSDP	388 NOTIFY * HTTP/1.1
358 128.161131	PC.local	ns-nh2.online.sh.cn	DNS	98 Standard query 0xc6fd A v18.events.data.microsoft.com
359 128.145067	ns-nh2.online.sh.cn	PC.local	DNS	226 Standard query response 0xc6fd A v18.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net
360 121.826386	PC.local	ns-nh2.online.sh.cn	DNS	98 Standard query 0xb551 A v20.events.data.microsoft.com
361 121.828992	ns-nh2.online.sh.cn	PC.local	DNS	226 Standard query response 0xb551 A v20.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net
362 121.879842	PC.local	mdns.mcast.net	MDNS	458 Standard query response 0x0000 TXT, cache flush PTR _nvstream_ohd_tcp.local PTR 3.27.0.120-PC.f9a7f166-63e5-44ce-af5c-c97b
363 126.889822	PC.local	ns-nh2.online.sh.cn	DNS	88 Standard query 0x0001 PTR 118.255.168.180.in-addr.arpa
364 126.893434	ns-nh2.online.sh.cn	PC.local	DNS	121 Standard query response 0x0001 PTR 118.255.168.180.in-addr.arpa PTR ns-nh2.online.sh.cn
365 126.896752	PC.local	ns-nh2.online.sh.cn	DNS	73 Standard query 0x0002 A www.baidu.com
366 126.100847	ns-nh2.online.sh.cn	PC.local	DNS	132 Standard query response 0x0002 A www.baidu.com CNAME www.a.shifen.com A 180.181.58.242 A 180.181.58.188
367 126.107476	PC.local	ns-nh2.online.sh.cn	DNS	73 Standard query 0x0003 AAAA www.baidu.com
368 126.110842	ns-nh2.online.sh.cn	PC.local	DNS	156 Standard query response 0x0003 AAAA www.baidu.com CNAME www.a.shifen.com AAAA 240e:e9:6802:15c:0:ff:b015:146f AAAA 240e:e9:
369 126.738956	PC.local	ns-nh2.online.sh.cn	DNS	98 Standard query 0xb3b6 A www.msftconnecttest.com
370 126.742350	ns-nh2.online.sh.cn	PC.local	DNS	227 Standard query response 0xb3b6 A www.msftconnecttest.com CNAME ncsl-geo.trafficmanager.net CNAME www.msftncsl.com.edgesuite
371 126.765722	PC.local	ns-nh2.online.sh.cn	DNS	98 Standard query 0xb750 A ipv6.msftconnecttest.com
372 126.768438	ns-nh2.online.sh.cn	PC.local	DNS	269 Standard query response 0xb750 A ipv6.msftconnecttest.com CNAME ncslv6-geo.trafficmanager.net CNAME ipv6.msftconnecttest.c
373 136.717939	192.168.1.109	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
374 137.250005	192.168.1.1	255.255.255.255	UDP	173 1024 * complex-link(5001) Len=131

图 3: 捕获结果

4.2 分析 UDP 包

选择一个数据帧，分析其 UDP 包头字段。

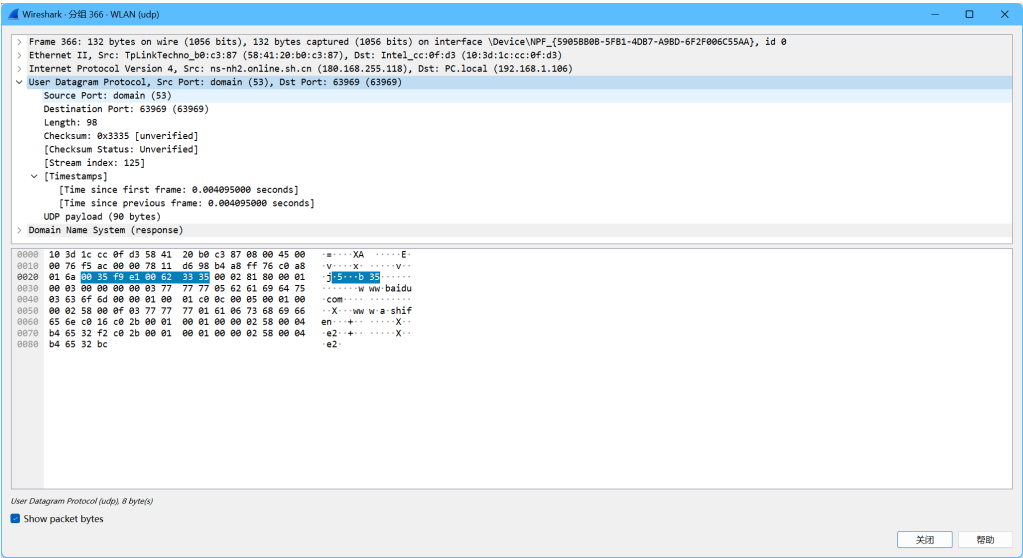


图 4: UDP 包

可以画出 UDP 包的结构如下：

源端口	目的端口	长度	校验和
Source Port	Destination Port	Length	Checksum
2 bytes	2 bytes	2 bytes	2 bytes
载荷			
Payload			
n bytes			

表 1: UDP 包结构

- 1) UDP 数据报头中的 Length 字段指的是 UDP 有效载荷? 还是 UDP 有效载荷加上 UDP 头的总长度? 还是 UDP 有效载荷和 UDP 头以及低层协议的头部三者总长度?

在上面的 UDP 包中, Payload 长度为 90 字节, UDP 头长度为 8 字节, 而 Length 字段的值为 98。

因此可以得出 UDP 数据报头中的 Length 字段指的是 UDP 有效载荷加上 UDP 头的总长度。

- 2) UDP 头中的校验和的长度是多少位?

UDP 头中的校验和的长度是 16 位。

- 3) 整个 UDP 头的长度是多少字节?

整个 UDP 头的长度是 8 字节。

启动命令行, 输入 ipconfig 获得计算机的 IP 地址, 与数据包中的 Source Port 比较。

```
无线网络适配器 WLAN:

连接特定的 DNS 后缀 . . . . . :
本地连接 IPv6 地址 . . . . . : fe80::d281:e59b:e8b4:5fe4%10
IPv4 地址 . . . . . : 192.168.1.106
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 192.168.1.1
```

图 5: IP 地址

可以看到, IP 地址为 192.168.1.106, 而数据包中的 Source Port 为 63969, 两者不同。

```
√ User Datagram Protocol, Src Port: domain (53), Dst Port: 63969 (63969)
  Source Port: domain (53)
  Destination Port: 63969 (63969)
  Length: 98
  Checksum: 0x3335 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 125]
  > [Timestamps]
    UDP payload (90 bytes)
  > Domain Name System (response)
```

图 6: Source Port

- 1) 在 IP 协议中哪个字段指明交给上一层的 UDP 传输进程? 该字段值是多少?

在 IP 协议中, Protocol 字段指明交给上一层的 UDP 传输进程, 该字段值为 17。

```
> Frame 366: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface \Device\NPF_{5905B80B-5FB1-4DB7-A9BD-6F2F006C55AA}, id 0
> Ethernet II, Src: TpLinkTechno_b0:c3:87 (58:41:20:b0:c3:87), Dst: Intel_cc:0f:d3 (10:3d:1c:cc:0f:d3)
> Internet Protocol Version 4, Src: ns-nh2.online.sh.cn (180.168.255.118), Dst: PC.local (192.168.1.106)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 118
  Identification: 0xf5ac (62892)
> 0000 .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header Checksum: 0xd698 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: ns-nh2.online.sh.cn (180.168.255.118)
  Destination Address: PC.local (192.168.1.106)
0000 10 3d 1c cc 0f d3 58 41 20 b0 c3 87 08 00 45 00  ..X.....E
0010 00 76 f5 ac 00 00 78 11 d6 98 b4 a8 ff 76 c0 a8  ..v....x....V..
0020 01 6a 00 35 f9 e1 00 62 33 35 00 02 81 80 00 01  ..j.5...b 35....
0030 00 03 00 00 00 00 03 77 77 77 05 62 61 69 64 75  ....w ww.baidu
0040 03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 00 01 00  ..com.....
0050 00 02 58 00 0f 03 77 77 77 01 61 06 73 68 69 66  ..X...ww w-a-shif
0060 65 6e c0 16 c0 2b 00 01 00 01 00 00 02 58 00 04  en.....X..
0070 b4 65 32 f2 c0 2b 00 01 00 01 00 00 02 58 00 04  ..e2+...X..
0080 b4 65 32 bc                                     ..e2..
```

图 7: Protocol 字段

2) 有的数据包的 source 和 destination IP 地址都不是你计算机的 IP 地址，给出该数据包的 destination IP 地址。

378	147.182946	192.168.1.1	239.255.255.250	SSDP	318	NOTIFY * HTTP/1.1
379	147.188515	192.168.1.1	239.255.255.250	SSDP	327	NOTIFY * HTTP/1.1
380	147.188516	192.168.1.1	239.255.255.250	SSDP	390	NOTIFY * HTTP/1.1
381	147.188516	192.168.1.1	239.255.255.250	SSDP	327	NOTIFY * HTTP/1.1
382	147.188522	192.168.1.1	239.255.255.250	SSDP	366	NOTIFY * HTTP/1.1
383	147.188522	192.168.1.1	239.255.255.250	SSDP	327	NOTIFY * HTTP/1.1
384	147.188522	192.168.1.1	239.255.255.250	SSDP	386	NOTIFY * HTTP/1.1
385	147.188523	192.168.1.1	239.255.255.250	SSDP	382	NOTIFY * HTTP/1.1
386	147.188523	192.168.1.1	239.255.255.250	SSDP	398	NOTIFY * HTTP/1.1
387	147.285737	192.168.1.1	239.255.255.250	SSDP	380	NOTIFY * HTTP/1.1
388	157.217587	192.168.1.1	255.255.255.255	UDP	173	1024 → complex-link(5001) Len=131

图 8: 数据包

可以看到，这些数据包的 destination IP 地址为 239.255.255.250

3) 一般 UDP 消息的长度是多少？

由于 UDP 报头中 Length 长度为 2 Bytes，即最大长度可以达到 $2^{16} - 1$ 即 65535 字节。但由于以太网一帧的最大载荷为 1500 字节，IP 报头为 20 字节，也就是说 UDP 消息总长度不能超过 1480 字节。

4.3 问题讨论

1. You might examine the traffic of UDP-based applications to look at packet sizes and loss rates. Voice-over-IP and its companion protocols like RTP (Real-Time Protocol) are good candidates.
QQ 采用的 OICQ 协议是基于 UDP 的，因此可以捕获 QQ 的数据包来分析。

22275	5168.938211	sz5.tencent.com	PC-2.local	OICQ	193 OICQ Protocol
22276	5168.940333	PC-2.local	sz5.tencent.com	OICQ	97 OICQ Protocol
22277	5168.950288	sz5.tencent.com	PC-2.local	OICQ	193 OICQ Protocol
22278	5168.951921	PC-2.local	sz5.tencent.com	OICQ	97 OICQ Protocol
22279	5168.985058	sz5.tencent.com	PC-2.local	OICQ	169 OICQ Protocol
22280	5168.986634	PC-2.local	sz5.tencent.com	OICQ	97 OICQ Protocol

图 9: 捕获到的 OICQ 数据包

选择一个 OICQ 数据包。

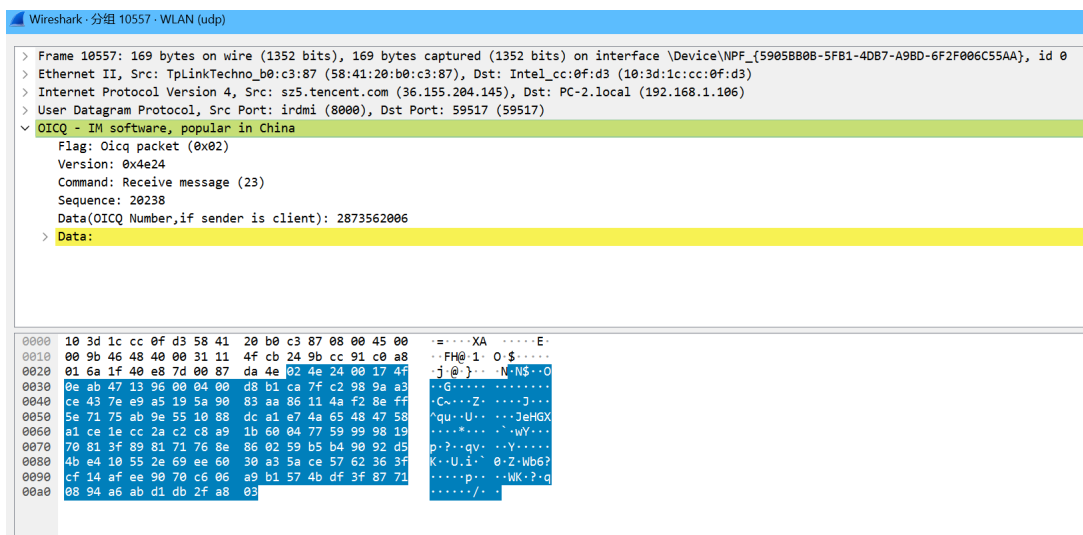


图 10: OICQ 数据包

可以看到，OICQ 数据包的长度为 647 字节。

2. Similarly, you might explore streaming and real-time applications to see which use UDP and which use TCP as a transport.

由于文件传输需要保证数据的完整性，因此文件传输一般使用 TCP 协议，而流媒体传输、实时通讯则可以使用 UDP 协议，因为即使丢包也不会产生太大影响，时效性更重要。

3. 在计算校验和时，为什么要加上 ipv4 伪头部，伪头部和 UDP 首部中都有 UDP length 字段，该字段出现两次是无意义的重复吗？还是有什么意义？

保证数据传输的完整性和准确性，同时增加了数据的安全性。通过包含源 IP 地址、目的 IP 地址等信息，提高了校验和的准确性和可靠性。

4. 计算校验和时，为补足偶数字节在 UDP 载荷数据末尾加上的 0，是否在 UDP 长度字段中体现？

不会体现。因为 UDP 长度字段只是指明 UDP 数据报的长度，而不是指明 UDP 数据报的长度加上补足偶数字节的 0 的长度。

5 实验结果总结

通过本次实验，我学会了通过 Wireshark 获取 UDP 消息，掌握了 UDP 数据包结构，掌握了 UDP 数据包各字段的含义，了解了 UDP 协议适用领域。

6 附录

无