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:	2023 级
实验编号:	Lab 05	实验名称:	UDP
姓　　名:	王海生	学　　号:	10235101559

目录

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。

通过查看 UDP 消息的详细信息，回答以下问题:

1) UDP 数据报头中的 Length 字段包括哪些部分？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 校验和为多少位？
3) 整个 UDP 头部的长度是多少字节？

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。

为了了解 UDP 在实践中是如何进行传输的，观察数据包的 IP 头部并思考以下问题：

1) 将上层协议标识为 UDP 的 IP 头部的协议字段值为多少？
2) 查看源 IP 地址与目的 IP 地址都不是你的计算机的 IP 地址的数据包，并给出这些数据包的目的 IP 地址。
3) 一般 UDP 消息的长度是多少？

2.1.3 问题讨论

1. 了解基于 UDP 的应用程序的流量，查看数据包大小和丢失率。
2. 探索流和实时应用程序，查看哪些使用 UDP 以及哪些使用 TCP 进行传输。

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

```
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。

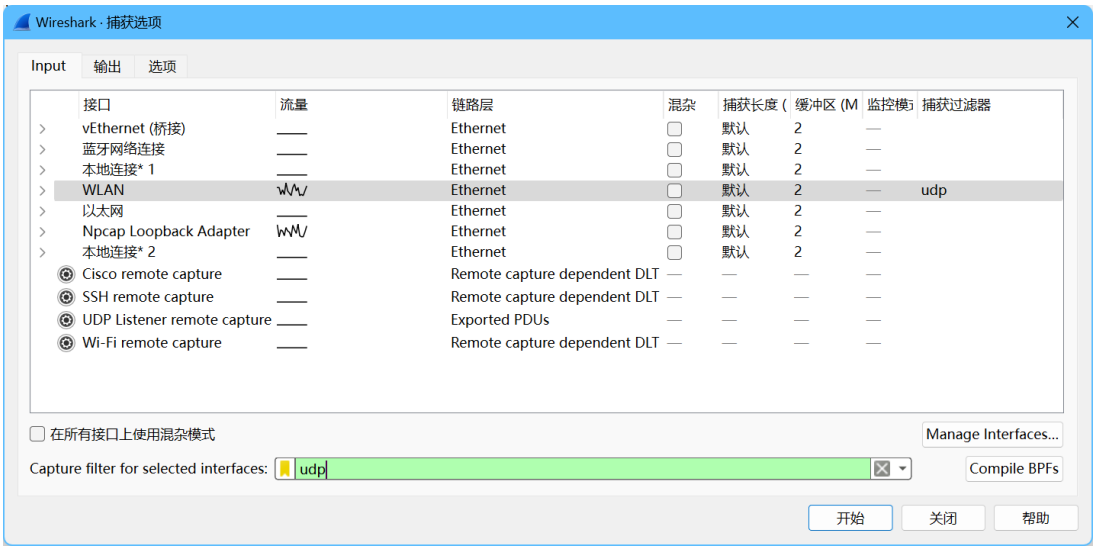

图 1: 设置捕获过滤器

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

```
pwsh ~
❯ nslookup www.baidu.com
服务器:  ns-nh2.online.sh.cn
Address:  180.168.255.118

非权威应答:
名称:    www.a.shifen.com
Addresses:  240e:e9:6002:15c:0:ff:b015:146f
          240e:e9:6002:15a:0:ff:b05c:1278
          180.101.50.242
          180.101.50.188
Aliases:  www.baidu.com
```

图 2: 查询 DNS 服务器

捕获结果如下：

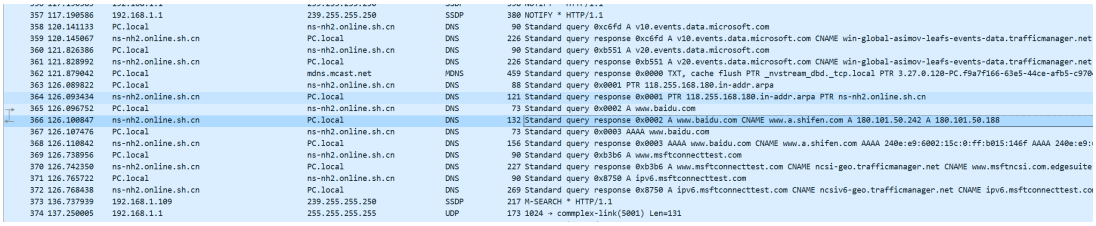

图 3: 捕获结果

4.2 分析 UDP 包

选择一个数据帧，分析其 UDP 包头字段。

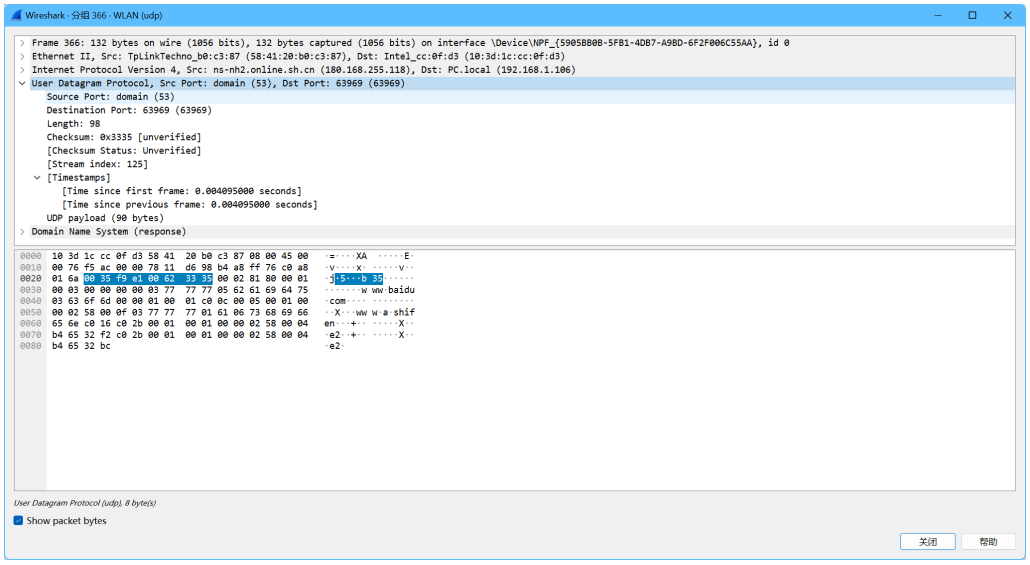

图 4: UDP 包

可以画出 UDP 包的结构如下：

源端口 Source Port 2 bytes	目的端口 Destination Port 2 bytes	长度 Length 2 bytes	校验和 Checksum 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。

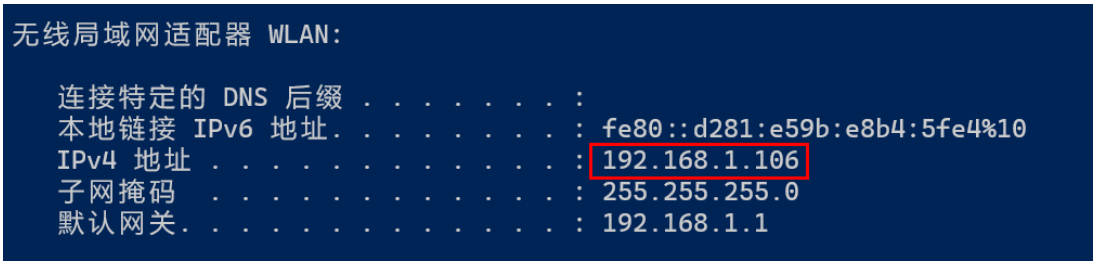

图 5: IP 地址

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。

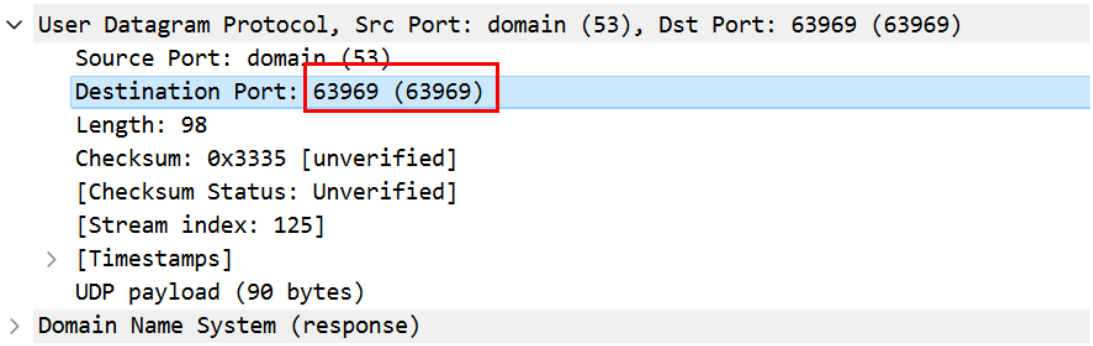

图 6: Source Port

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。

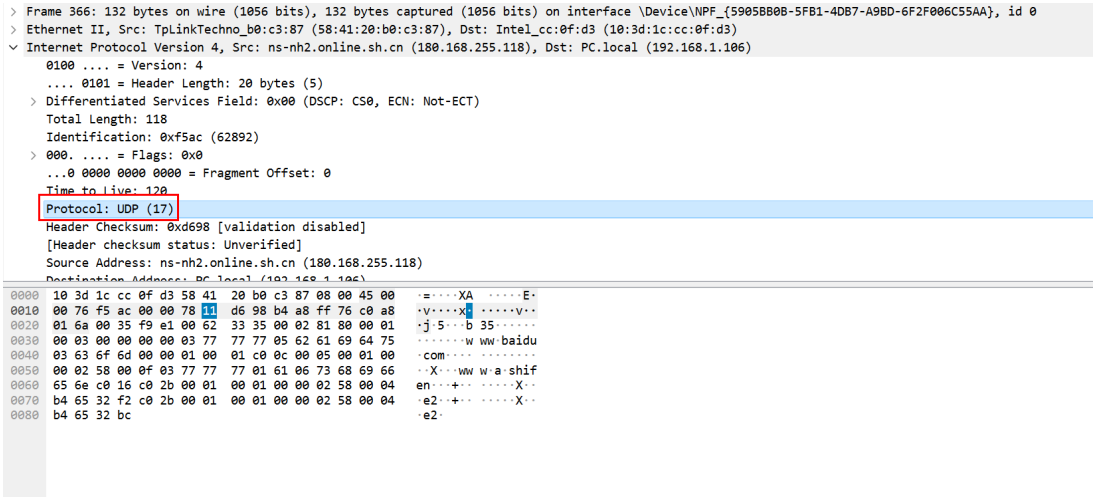

图 7: Protocol 字段

2) 查看源 IP 地址与目的 IP 地址都不是你的计算机的 IP 地址的数据包，并给出这些数据包的目的 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 → commplex-link(5001) Len=131

图 8: 数据包

可以看到，这些数据包的目的 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. 了解基于 UDP 的应用程序的流量，查看数据包大小和丢失率。
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。

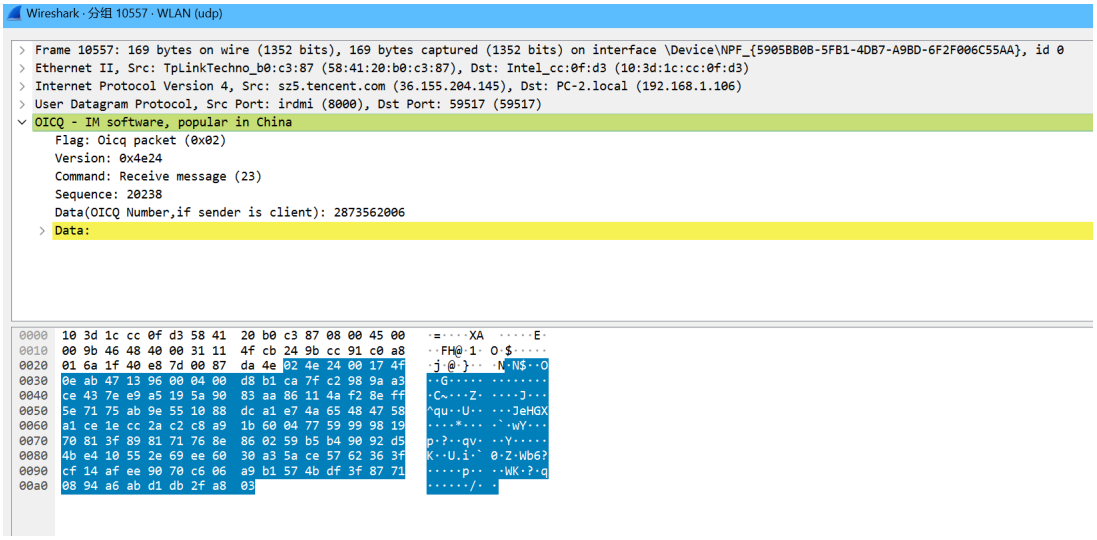

图 10: OICQ 数据包

可以看到，OICQ 数据包的长度为 647 字节。

2. 探索流和实时应用程序，查看哪些使用 UDP 以及哪些使用 TCP 进行传输。
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。

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