

实验报告：UDP 实验五

课程名称：计算机网络 年级：大二

上机实践成绩：

实践

指导教师：章玥

姓名：邱吉尔

学号：10235101533

上机实践日期：

2024/12/16

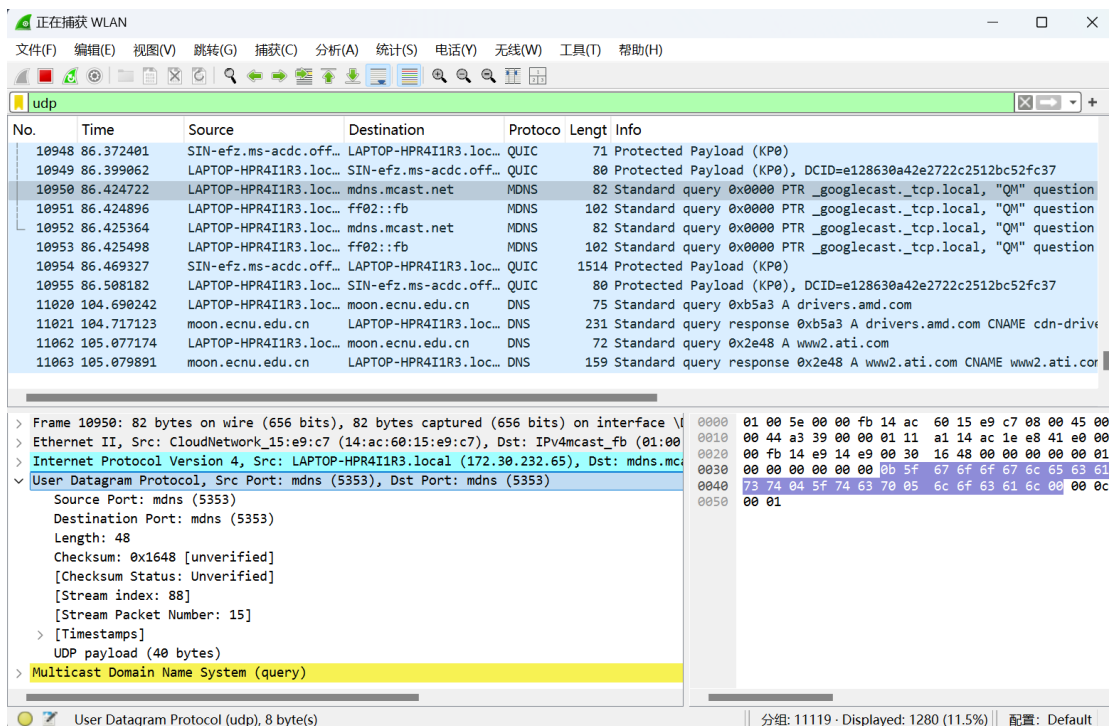
一、 目的

1. 熟悉使用 wireshark 软件进行抓取 UDP 数据包 ；
2. 分析抓取到的 UDP 数据包，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 协议使用领域；

二、 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”，关闭混杂模式；
2. 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；
3. 打开 Wireshark， 停止捕获；
4. 查看 Wireshark 界面中抓取的 UDP 数据包。

实验抓包截图：



三、通过查看 UDP 消息的详细信息，回答以下问题：

1、UDP 数据包头中的 Length 字段包括哪些部分？UDP 有效载荷，还是 UDP 有效载荷加上 UDP 头部的总长度，还是 UDP 有效载荷和 UDP 头部以及低层协议的头部三者总长度？

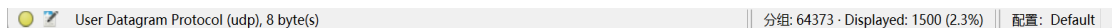
Length 字段中的值是 48

Length 字段表示 UDP 有效载荷和 UDP 头部的字节长度之和

2、UDP 校验和为多少位？

校验和为 0x1648,为 16 位二进制

3、整个 UDP 头部的长度为多少字节？



整个 UDP 头部长度为 8 字节

四、 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？

```
> Frame 10950: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface
> Ethernet II, Src: CloudNetwork_15:e9:c7 (14:ac:60:15:e9:c7), Dst: IPv4mcast_fb (01:
✓ Internet Protocol Version 4, Src: LAPTOP-HPR4I1R3.local (172.30.232.65), Dst: mdns.
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 68
    Identification: 0xa339 (41785)
> 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xa114 [correct]
    [Header checksum status: Good]
```

字段值为 17

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。

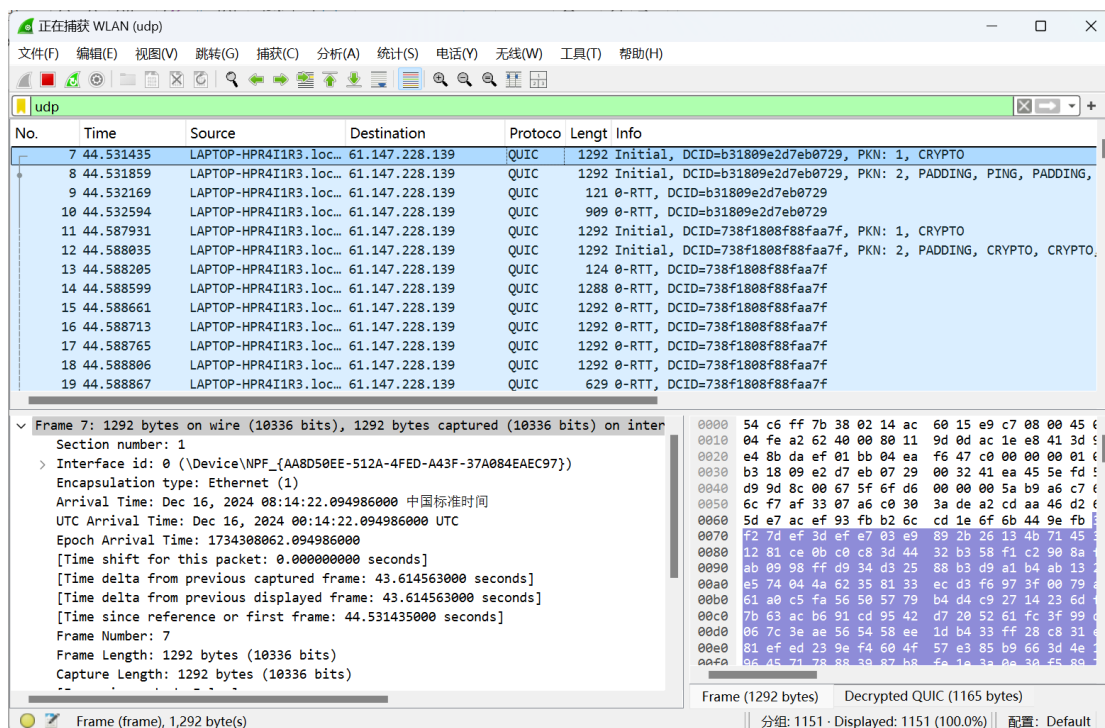
The image shows a Wireshark packet capture window titled "正在捕获 WLAN (udp)". The packet list on the left shows several packets, with packet 298 selected. The packet details pane on the right shows the structure of the selected packet, which is an Internet Protocol Version 6 (IPv6) packet. The packet is an ICMPv6 Echo Request (ping) from source address fe80::1e9e:b03c:a1e4:d480 to destination address ff02::fb. The packet length is 105 bytes. The packet is captured on interface CloudNetwork_15:e9:c7 (14:ac:60:15:e9:c7). The packet is an IPv6 multicast packet (IPv6mcast_fb (33:33)). The packet is an Internet Protocol Version 6 (IPv6) packet. The packet is an ICMPv6 Echo Request (ping) from source address fe80::1e9e:b03c:a1e4:d480 to destination address ff02::fb. The packet length is 105 bytes. The packet is captured on interface CloudNetwork_15:e9:c7 (14:ac:60:15:e9:c7). The packet is an IPv6 multicast packet (IPv6mcast_fb (33:33)).

No.	Time	Source	Destination	Protocol	Length	Info
292	57.319986	172.30.232.65	61.147.228.139	QUIC	76	Protected Payload (KPo), DCID=0e887d47f6c02c2a
293	57.349404	61.147.228.139	172.30.232.65	QUIC	70	Protected Payload (KPo)
294	57.350944	61.147.228.139	172.30.232.65	QUIC	70	Protected Payload (KPo)
295	57.350944	61.147.228.139	172.30.232.65	QUIC	70	Protected Payload (KPo)
296	57.352086	61.147.228.139	172.30.232.65	QUIC	70	Protected Payload (KPo)
297	82.014218	172.30.232.65	mdns.mcast.net	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" quest:
298	82.014953	fe80::1e9e:b03c:a1e4:d480	ff02::fb	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" quest:
299	82.537235	172.30.232.65	moon.ecnu.edu.cn	DNS	83	Standard query 0xa9df A b.c2r.ts.cdn.office.net
300	82.540261	moon.ecnu.edu.cn	172.30.232.65	DNS	334	Standard query response 0xa9df A b.c2r.ts.cdn.office.net CNAME r
301	82.952168	172.30.232.65	moon.ecnu.edu.cn	DNS	143	Standard query 0x5e12 PTR 0.8.4.d.a.e.1.a.c.3.0.b.e.9.e.1.0.0.0
302	82.952500	172.30.232.65	moon.ecnu.edu.cn	DNS	143	Standard query 0x90d3 PTR b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
303	83.024003	172.30.232.65	mdns.mcast.net	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" quest:
304	83.024737	fe80::1e9e:b03c:a1e4:d480	ff02::fb	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" quest:

Frame 298: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \\\n> Ethernet II, Src: CloudNetwork_15:e9:c7 (14:ac:60:15:e9:c7), Dst: IPv6mcast_fb (33:33:33:33:33:33)\n> Internet Protocol Version 6, Src: fe80::1e9e:b03c:a1e4:d480 (fe80::1e9e:b03c:a1e4:d480), Dst: ff02::fb (ff02::fb)\n 0110 = Version: 6\n 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)\n 0011 0101 1011 1010 1001 = Flow Label: 0x35ba9\n Payload Length: 51\n Next Header: UDP (17)\n Hop Limit: 1\n Source Address: fe80::1e9e:b03c:a1e4:d480 (fe80::1e9e:b03c:a1e4:d480)\n Destination Address: ff02::fb (ff02::fb)\n [Stream index: 0]\n> User Datagram Protocol, Src Port: mdns (5353), Dst Port: mdns (5353)\n Multicast Domain Name System (query)

目的 ip 地址为 ff02::fb

3、一般 UDP 消息的长度为多少？



一般为 1292 字节

五、在完成本实验后继续探索 UDP 协议：

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。

严重性	消息	协议	消息	丢失率
Warning	DNS response missing	Protocol	LLMHR	4
Warning	DNS query retransmission	Protocol	mDNS	16
Warning	DNS response missing	Protocol	mDNS	0
Warning	Failed to decrypt handshake	Decryption	QUIC	68
Note	Time to Live	Sequence	IPv4	10
Note	This QUIC frame has a reused stream offset (retransmission?)	Sequence	QUIC	3
Chat	This legacy_version field MUST be ignored. The supported ver...	Deprecated	TLS	10

共丢失了 12 个包，丢包率约为 1.8%

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。

使用 UDP：

1. 视频会议
2. 实时在线游戏
3. DNS 查询
4. 视频流服务

使用 TCP：

1. HTTP/HTTPS
2. 文件传输
3. MySQL 数据库连接