江苏大学

JIANGSU UNIVERSITY

计算机网络实验报告

实验名称：抓包与分析

学院名称：计算机科学与通信工程学院

专业班级：物联网工程 2303

学生姓名：邱佳亮

学生学号：3230611072

教师姓名：李峰

报告日期：2024/10/22

目录

1 作业目的

（1）了解网络通信的分层实现过程，了解不同层次 PDU 的逐层封装与解封过程；

（2）了解数据通信的过程，进一步认知协议的构成与通信过程，进而对 TCP/IP 分层体系结构有更深刻的了解。

2 作业内容

1. 在局域网范围内从协议层面分析 ping 命令的执行过程，包括所使用协议，以及不同层级的数据包封装与解封的过程。

2. 访问 www.ujs.edu.cn 网站，分析其中所使用的协议，以及数据包的逐层封装与解封过程。

3. 思考在数据链路层的数据包与网络层数据包的异同，包括包长度和数据构成等，并进一步思考为何会存在这些区别？

3 作业要求

（1）能够正确捕捉 ping 命令执行过程中所产生的数据包，并逐层分析其构成，进而了解数据包的封装与解封过程；

（2）能够正确捕捉访问 www.ujs.edu.cn 网站过程所产生的相关数据包，分析出其所使用的协议，以及各协议的访问流程；

（3）能够正确分析数据链路层的数据包与网络层数据包的异同。

（4）了解并熟悉常见的抓包工具，例如 Wireshark、Sniffer 等，熟悉以太网数据帧和 IP 数据包的结构

（5）以 PDF 文档提交本次作业报告。

4 实现过程

4.1 利用 Wireshark 捕获数据包

在 windows 命令行输入 *ipconfig/all* 获取本机的网络信息：

图 1　网络配置信息

看到本机的 IP 地址为：*192.168.41.22*

本机的默认网关为：*192.168.41.114*

DNS 服务器为：*192.168.41.114*

本机的 MAC 地址为：*74-97-79-E2-DF-D1*

在命令行输入 *ping 192.168.1.1* 测试连通，同时使 Wireshark 开始捕获 WLAN 上的数据包：

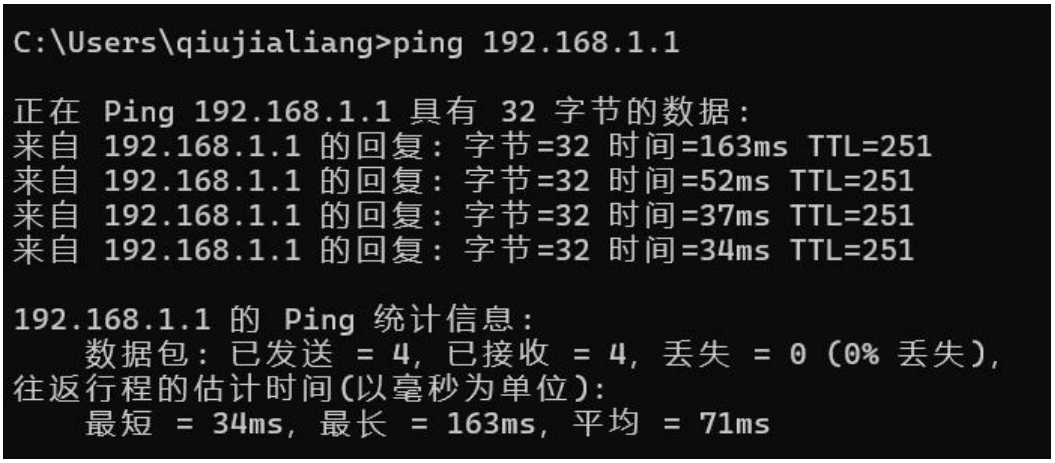
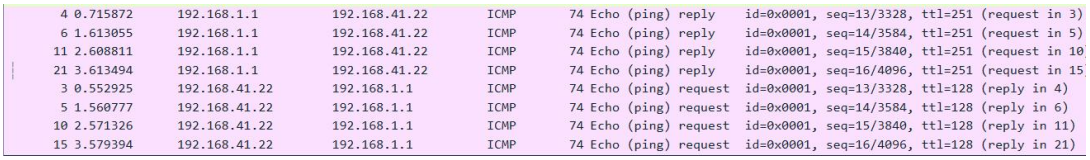


图 2　使用 Ping 命令

Ping 连通后，停止捕获并发现 Wireshark 成功捕获了 Ping 命令产生的 8 个数据包：



4	0.715872	192.168.1.1	192.168.41.22	ICMP	74 Echo (ping) reply id=0x0001, seq=13/3328, ttl=251 (request in 3)
6	1.613055	192.168.1.1	192.168.41.22	ICMP	74 Echo (ping) reply id=0x0001, seq=14/3584, ttl=251 (request in 5)
11	2.608811	192.168.1.1	192.168.41.22	ICMP	74 Echo (ping) reply id=0x0001, seq=15/3840, ttl=251 (request in 10
21	3.613494	192.168.1.1	192.168.41.22	ICMP	74 Echo (ping) reply id=0x0001, seq=16/4096, ttl=251 (request in 15
3	0.552925	192.168.41.22	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 4)
5	1.560777	192.168.41.22	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 6)
10	2.571326	192.168.41.22	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 11)
15	3.579394	192.168.41.22	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 21)

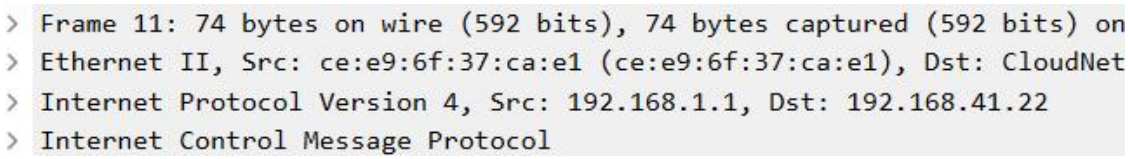
图 3　捕获的数据包

从左至右分别是 No，表示数据包编号；Time，表示捕获所用的时间；Source，表示来源 IP 地址，下方 4 个数据包的 Source 即为本机 IP 地址；Destination：表示目的 IP 地址，下方 4 个数据包的 Destination 为 Ping 的目标，即为 192.168.1.1；Protocol，表示协议，所示的协议是 ICMP，这是 TCP/IP 协议簇中重要的子协议，属于网络层协议，主要用于在 IP 主机和路由器之间传递消息；Length，表示数据包长度，这 8 个数据包的长度均为 74；Info 显示了数据包的信息，分别是 request 和 reply。

4.2 分层分析数据包

4.2.1 数据包的层次

选择一个数据包，发现其具有 4 层结构：



```
> Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
> Ethernet II, Src: ce:e9:6f:37:ca:e1 (ce:e9:6f:37:ca:e1), Dst: CloudNet
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.41.22
> Internet Control Message Protocol
```

图 4　数据包的层次

分别为 Frame，表示物理层数据帧；Etherent II，表示数据链路层的帧信息；Internet Protocol Version 4，表示网络层的 IP 信息；Internet Control Message Protocol，表示协议总述。

由此可见网络是分层的，由低到高为物理层、数据链路层、网络层、传输层和应用层，即为 TCP/IP 五层模型。

4.2.2 数据包的封装

数据封装分为五层，第一层是应用层数据，第二层是 TCP/UDP 封装，第三层为 IP 封装，第四层为以太网封装，最后转换为二进制的物理报文。

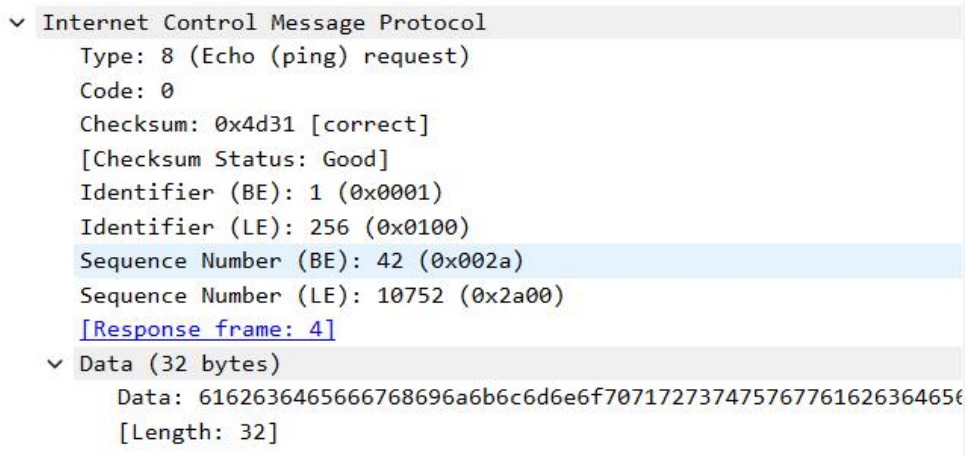


图 5　Internet Control Message Protocol

Internet Control Message Protocol 中包含了 Type（类型），Code（代码），Checksum（校验和）、Sequence Number（序列号）和 Data（数据）。

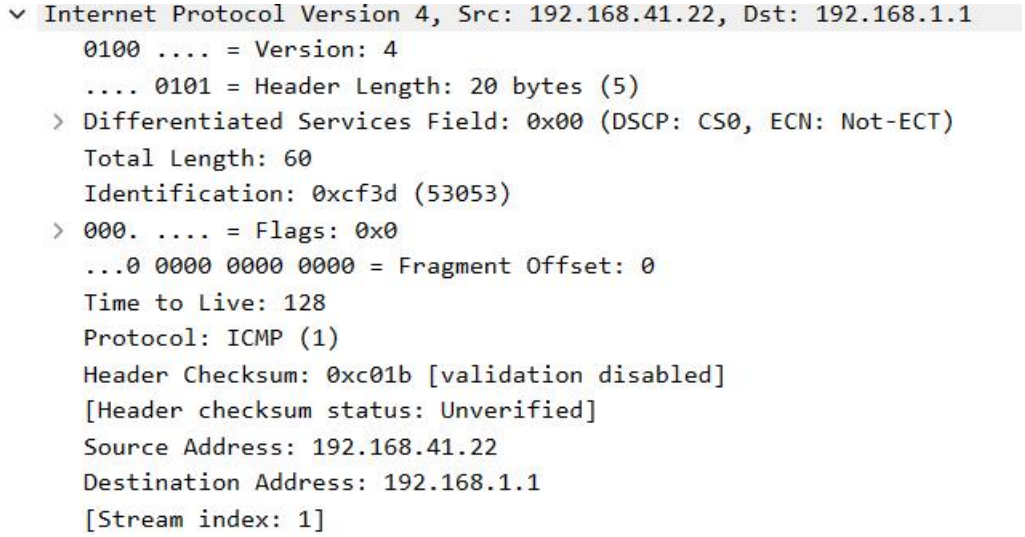


图 6　Internet Protocol Version 4

Internet Protocol Version 4 中，二进制 0100 表示协议为 IPV4；....0101 表示长度为 20 个字节，字段最小值为 5；Total Length 表示包总长度为 60；Identification 为 16 位标识字段，发现一次请求和回应的表示字段相同；Fragment Offset 表示偏移量；Time to Live 表示生存时间；Protocol 表示包的协议为 TCMP；Source Address 和 Destination Address 分别表示起始和目的 IP 地址。

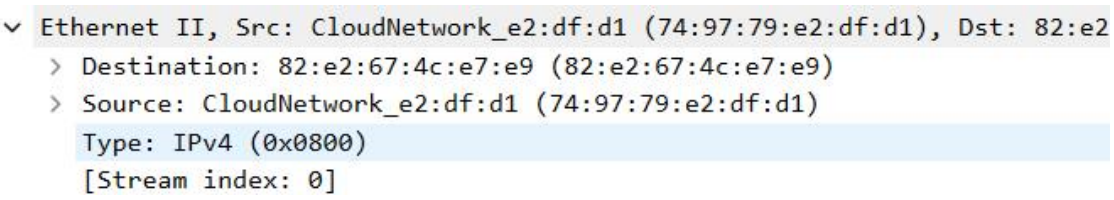


图 7　Etherent II

Etherent II 中，Destination 表示目标的 MAC 地址，Source 表示源 MAC 地址，这里就是本机的 MAC 地址；Type 表示协议为 IPv4。

可以看出，该数据帧在传输层被封装为 ICMP 数据包，在网络层被封装为 IP 数据包，在数据链路层使用 Ethernet II 协议封装，最终在物理层转化为二进制信号发送。

4.3 Ping www.ujs.edu.cn

打开命令行，使用 *ping www.ujs.edu.cn*：

```
C:\Users\qiujialiang>ping www.ujs.edu.cn

正在 Ping www.ujs.edu.cn [172.20.1.185] 具有 32 字节的数据:
来自 172.20.1.185 的回复: 字节=32 时间=21ms TTL=61
来自 172.20.1.185 的回复: 字节=32 时间=18ms TTL=61
来自 172.20.1.185 的回复: 字节=32 时间=14ms TTL=61
来自 172.20.1.185 的回复: 字节=32 时间=16ms TTL=61

172.20.1.185 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 14ms, 最长 = 21ms, 平均 = 17ms
```

图 8　Ping 命令

在 Wireshark 中进行捕获，在过滤器中输入 ip.addr==172.20.1.185，发现过滤出 8 个数据包：

62	1.117883	10.16.137.206	172.20.1.185	ICMP	74	Echo (ping) request id=0x0001, seq=166/42496, ttl=128 (reply in 63)
63	1.121220	172.20.1.185	10.16.137.206	ICMP	74	Echo (ping) reply id=0x0001, seq=166/42496, ttl=62 (request in 6…
79	2.135280	10.16.137.206	172.20.1.185	ICMP	74	Echo (ping) request id=0x0001, seq=167/42752, ttl=128 (reply in 80)
80	2.139681	172.20.1.185	10.16.137.206	ICMP	74	Echo (ping) reply id=0x0001, seq=167/42752, ttl=62 (request in 7…
85	3.142611	10.16.137.206	172.20.1.185	ICMP	74	Echo (ping) request id=0x0001, seq=168/43008, ttl=128 (reply in 86)
86	3.146504	172.20.1.185	10.16.137.206	ICMP	74	Echo (ping) reply id=0x0001, seq=168/43008, ttl=62 (request in 8…
95	4.156881	10.16.137.206	172.20.1.185	ICMP	74	Echo (ping) request id=0x0001, seq=169/43264, ttl=128 (reply in 96)
96	4.161260	172.20.1.185	10.16.137.206	ICMP	74	Echo (ping) reply id=0x0001, seq=169/43264, ttl=62 (request in 9…

图 9　数据包

这 8 个数据协议均为 ICMP，与先前结构类似，为四层结构：

```
> Frame 62: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
> Ethernet II, Src: CloudNetwork_e2:df:d1 (74:97:79:e2:df:d1), Dst: Huawe
> Internet Protocol Version 4, Src: 10.16.137.206, Dst: 172.20.1.185
> Internet Control Message Protocol
```

图 10　数据包结构

因此，该数据帧在传输层被封装为 ICMP 数据包，在网络层被封装为 IP 数据包，在数据链路层使用 Ethernet II 协议封装，最终在物理层转化为二进制信号

发送，其中没有应用层协议。

4.4 访问 www.ujs.edu.cn

在浏览器中访问 www.ujs.edu.cn 网址，并使用 Wireshark 抓包。在过滤器中输入 dns，发现本机向 DNS 服务器发送了域名请求，DNS 服务器进行了回复：

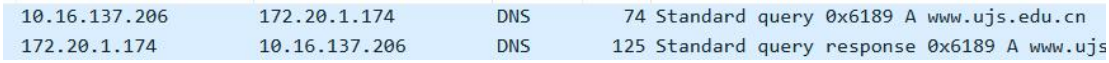


图 11 DNS 数据

该数据包协议为 DNS，分为 5 层结构：

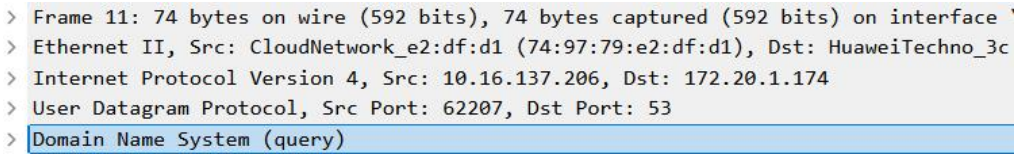


图 12 数据包结构

其中，请求和应答的数据包内容略有不同：

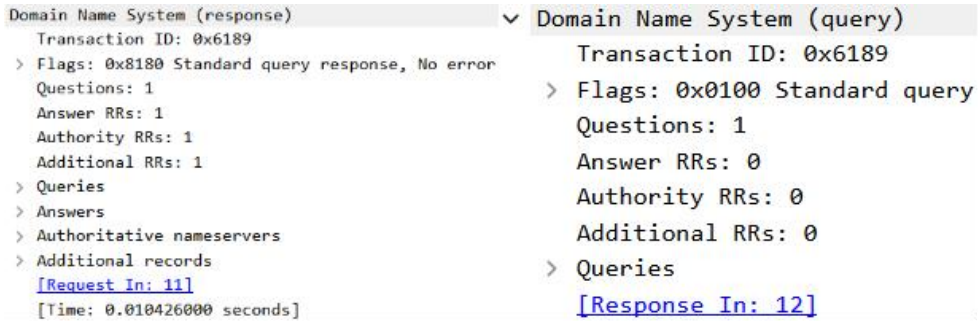


图 13 Domain Name System

Domain Name System 中，Transaction ID 为 DNS 的 ID 号；Questions 为问题计数，Answer RRs 为回答计数，Authority RRs 为域名服务器计数；Queries 包含了请求的域名，Answers 包含了返回的 IP 地址。

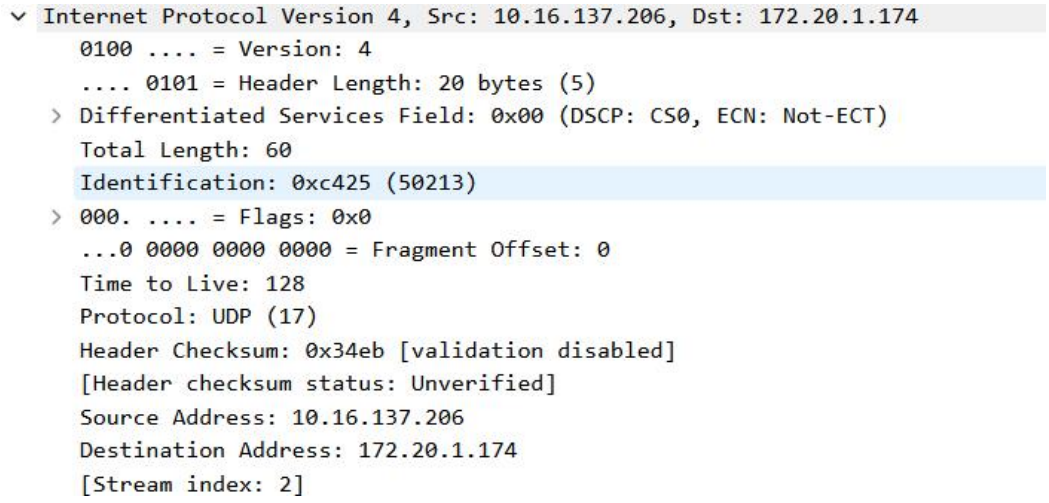


图 14　Internet Protocol

此外，这些数据包传输层均使用了 UDP 协议，与先前不同。

可以看出，这些数据帧在应用层被封装为 DNS 数据包，在传输层被封装为 UDP 数据包，在网络层被封装为 IP 数据包，数据链路层用 Ethernet II 协议封装，在物理层转化为二进制信号。

综上所述，执行访问网址时，首先终端会访问 DNS 服务器询问域名的 IP 地址，DNS 服务器收到询问请求后发送包含域名 IP 信息的 DNS 数据包，此过程中应用层协议为 DNS，传输层协议为 UDP，网络层协议为 IP。终端获得 www.ujs.edu.cn 的 IP 地址后，再向其寻求访问，www.ujs.edu.cn 收到访问请求后发送回复，此过程中传输层/网络层协议为 ICMP，在网络层封装为 IP 数据包。

4.5 数据链路层的数据包和网络层数据包的异同

数据链路层在物理层提供的服务的基础上向网络层提供服务，网络层在数据链路层提供的两个相邻端点之间的数据帧的传送功能上，进一步管理网络中的数据通信，将数据设法从源端经过若干个中间节点传送到目的端，从而向运输层提供最基本的端到端的数据传送服务。

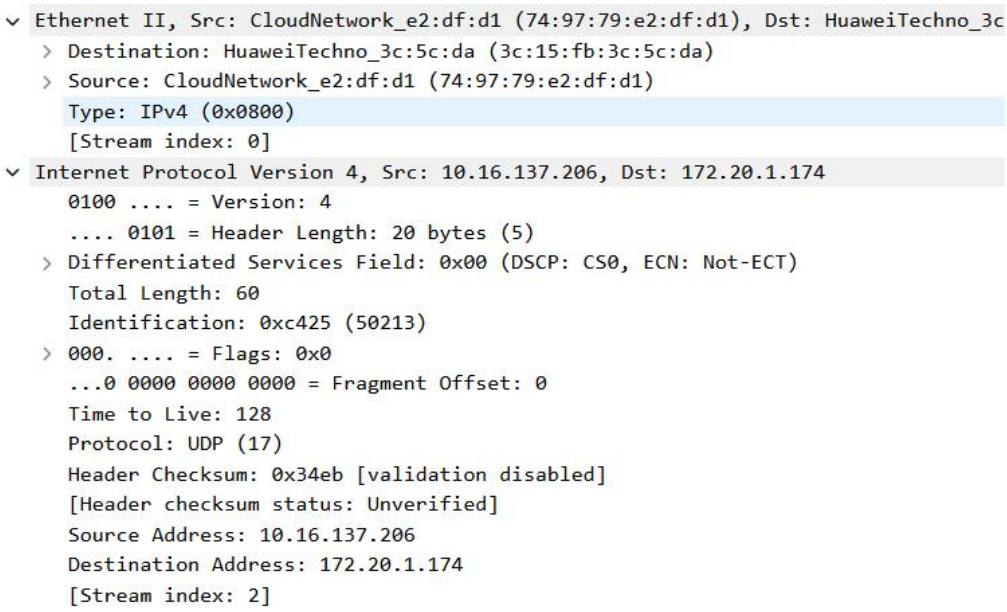


图 15　数据链路层和网络层

数据链路层的报头包括了原地址和目的地址的 MAC 地址，网络层的报头包括原地址和目的地址的 IP 地址。从内容看，数据链路层包括了 MAC 地址和协议类型，网络层包括了协议类型、首部长度、偏移量、生存时间、校验码、IP 地址等内容。可以看出，数据链路层数据包报头和网络层数据包报头有很大不同，这些区别取决于网络层与数据链路层面临问题不同和功能不同。