

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](#_Toc21479)

[2 作业内容 1](#_Toc27317)

[3 作业要求 2](#_Toc11988)

[4 实现过程 2](#_Toc26190)

[4.1 利用Wireshark捕获数据包 2](#_Toc7182)

[4.2 分层分析数据包 4](#_Toc28470)

[4.2.1 数据包的层次 4](#_Toc15800)

[4.2.2 数据包的封装 4](#_Toc19124)

[4.3 Ping www.ujs.edu.cn 5](#_Toc2276)

[4.4 访问www.ujs.edu.cn 6](#_Toc29400)

[4.5 数据链路层的数据包和网络层数据包的异同 8](#_Toc2979)

## 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。

## 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？

## 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。

## 实现过程

### 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：

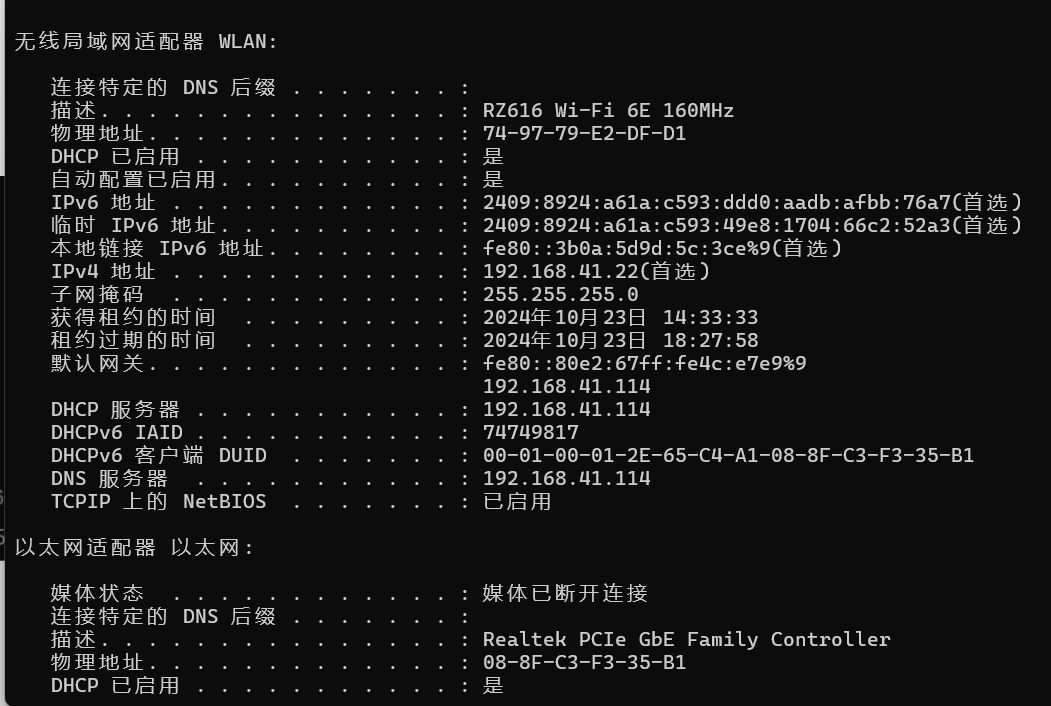


图 1 网络配置信息

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：

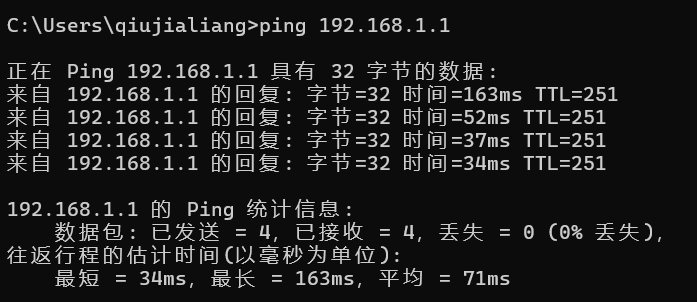


图 2 使用Ping命令

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：

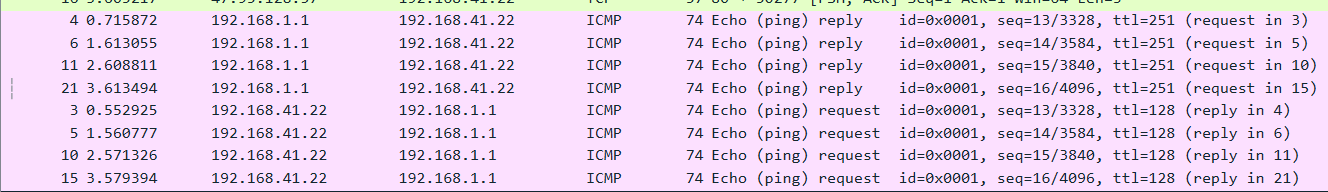


图 3 捕获的数据包

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。

### 分层分析数据包

#### 数据包的层次

选择一个数据包，发现其具有4层结构：

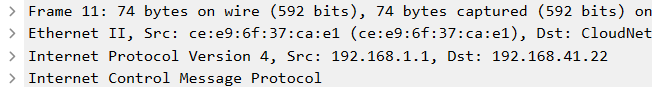


图 4 数据包的层次

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。

#### 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。

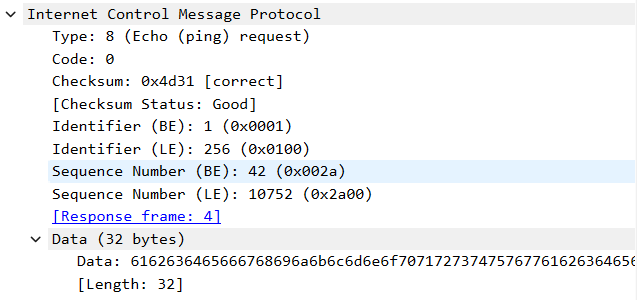


图 5 Internet Control Message Protocol

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）。

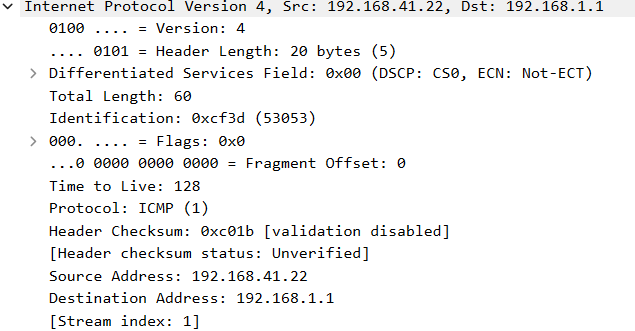


图 6 Internet Protocol Version 4

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。

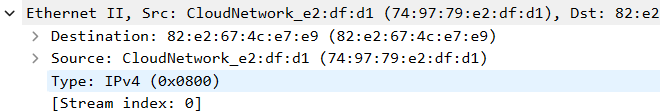


图 7 Etherent II

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。

### Ping [www.ujs.edu.cn](http://www.ujs.edu.cn)

打开命令行，使用*ping www.ujs.edu.cn*：

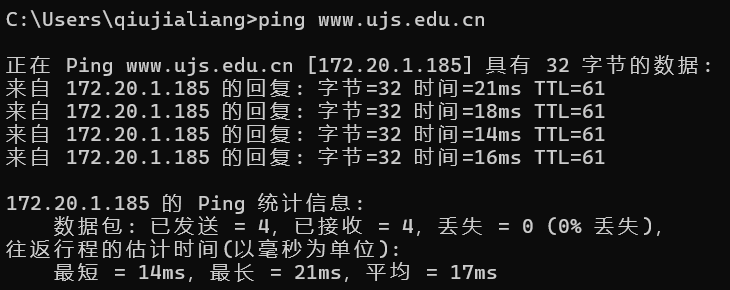


图 8 Ping命令

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：

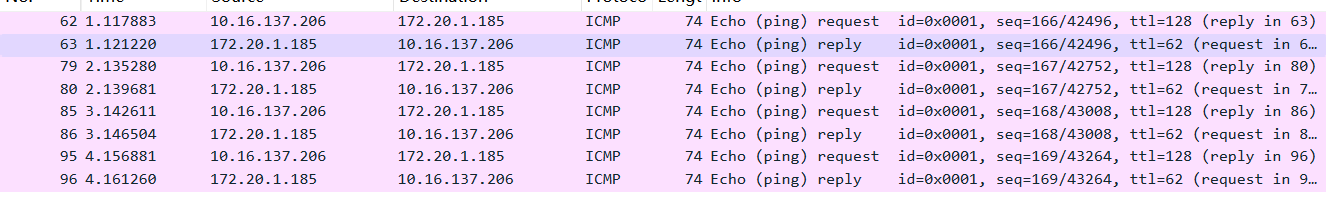


图 9 数据包

这8个数据协议均为ICMP，与先前结构类似，为四层结构：

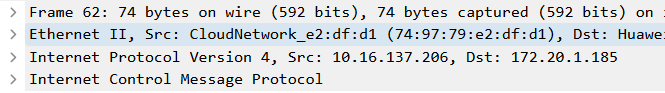


图 10 数据包结构

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。

### 访问[www.ujs.edu.cn](http://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：

屏幕截图 2024-10-24 140454

图 11 DNS数据

该数据包协议为DNS，分为5层结构：

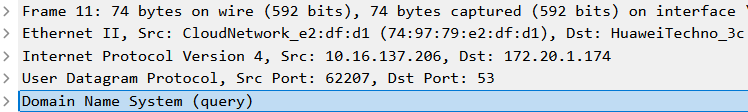


图 12 数据包结构

其中，请求和应答的数据包内容略有不同：

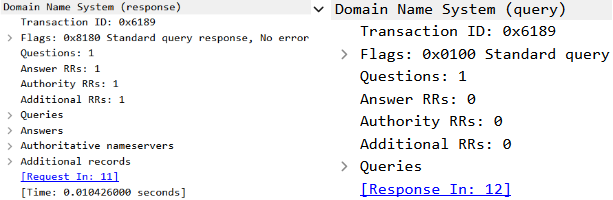


图 13 Domain Name System

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。

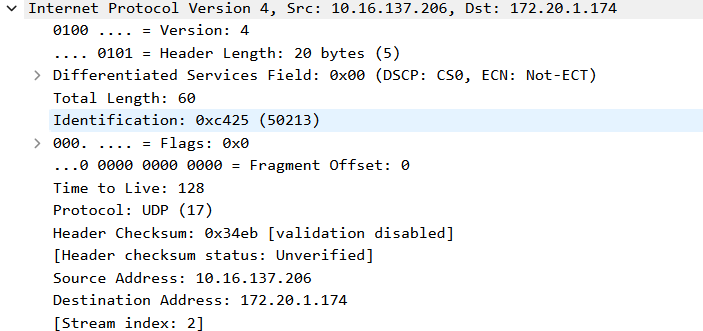


图 14 Internet Protocol

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。

### 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。

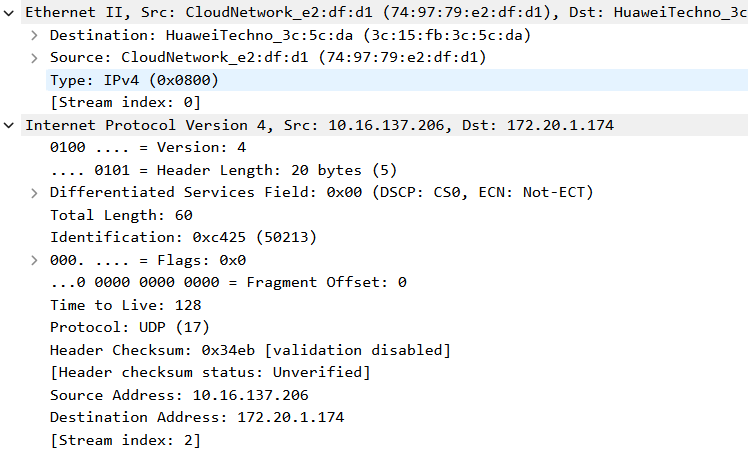


图 15 数据链路层和网络层

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。