

[计算机网络 实验报告]

[实验二：协议数据的捕获和解析]



* IP、ICMP、DHCP、ARP、TCP协议数据的捕获和解析

姓名：裴子祥

学号：2015211921

班级：2015211307

学院：计算机学院

2017-6-16

[北京邮电大学]

Ctrl+单击访问链接

**目录**

[一、 实验内容与实验步骤描述 1](#_Toc485551524)

[1. 实验任务与内容 1](#_Toc485551525)

[2. 实验环境 2](#_Toc485551526)

[3. 实验步骤 3](#_Toc485551527)

[i. 准备工作 3](#_Toc485551528)

[ii. 数据捕获 3](#_Toc485551529)

[iii. 协议分析 4](#_Toc485551530)

[iv. 撰写实验报告 4](#_Toc485551531)

[二、 若干协议分析 4](#_Toc485551532)

[1. IP协议分析 4](#_Toc485551533)

[i. 实验中IP包头各字段 5](#_Toc485551534)

[ii. IP 包头校验和的校验原理，校验和实验验证 5](#_Toc485551535)

[iii. IP包分段原理，实验验证。 7](#_Toc485551536)

[2. ICMP协议分析 10](#_Toc485551537)

[i. 理解 ICMP 的功能 10](#_Toc485551538)

[ii. ICMP 的包格式，各字段的功能。 11](#_Toc485551539)

[3. DHCP协议分析 14](#_Toc485551540)

[i. DHCP 的功能、配置参数 15](#_Toc485551541)

[ii. DHCP地址分配过程消息序列图 19](#_Toc485551542)

[4. ARP协议分析 21](#_Toc485551543)

[i. ARP功能与操作原理 21](#_Toc485551544)

[ii. ARP包格式，各字段功能 22](#_Toc485551545)

[5. TCP协议分析 23](#_Toc485551546)

[i. TCP报文字段功能 23](#_Toc485551547)

[ii. 建立和连接释放过程的消息序列图 24](#_Toc485551548)

[iii. 数据传输过程的消息序列图 27](#_Toc485551549)

[三、 实验总结和实验心得 29](#_Toc485551550)

[1. 实验总结 29](#_Toc485551551)

[2. 实验心得 29](#_Toc485551552)

# 实验内容与实验步骤描述

## 实验任务与内容

本次实验主要包含下列内容：

1）使用Wireshark 软件捕获在使用ping 命令时产生的ICMP 消息；

2）分析网络层IP 包头格式，理解各字段的作用，对于分段和校验和进行验证；

3）使用Wireshark 软件捕获在使用ARP 消息，分析其消息格式，理解其工作原理；

4）使用Wireshark 捕获DHCP 消息，分析其消息序列，理解DHCP 的功能和操作原理；

5）使用Wireshark 捕获TCP 消息，分析TCP 报文段头格式，理解连接建立和释放的原理，差错控制原理、序号和窗口管理的原理。

通过本实验学生可以深入理解分层体系结构，理解和掌握TCP/IP 协议栈的代表协议——IP、TCP、UDP、ICMP、ARP 和DHCP 协议的要点。

通过使用Wireshark 软件来捕获网络上实际传输的数据，可以加深对于上述协议的要点的理解，可以通过分析数据格式和协议流程进行自学和了解例如IP 包头校验和的计算、TCP 的MSS 概念、ICMP 的消息格式、ARP 的消息格式、DHCP 的消息格式及操作过程等。

## 实验环境

MS Windows 10操作系统的计算机，能连接到Internet，使用Wireshark-win64-2.2.7（v2.2.7-0-g1861a96）进行协议的捕获与分析。

在cmd窗口中输入ipconfig /all,获取本机ip与mac地址，本机初始状态如下：

Windows IP 配置

主机名 . . . . . . . . . . . . . : Peipeilvhxy

主 DNS 后缀 . . . . . . . . . . . :

节点类型 . . . . . . . . . . . . : 混合

IP 路由已启用 . . . . . . . . . . : 否

WINS 代理已启用 . . . . . . . . . : 否

DNS 后缀搜索列表 . . . . . . . . : bupt.edu.cn

无线局域网适配器 无线网络连接 2:

连接特定的 DNS 后缀 . . . . . . . : bupt.edu.cn

描述. . . . . . . . . . . . . . . : Qualcomm Atheros AR5BWB222 Wireless Network Adapter #2

物理地址. . . . . . . . . . . . . : D0-53-49-FB-87-48

DHCP 已启用 . . . . . . . . . . . : 是

自动配置已启用. . . . . . . . . . : 是

IPv6 地址 . . . . . . . . . . . . : 2001:da8:215:8f01:71f5:add5:29ce:4e3(首选)

临时 IPv6 地址. . . . . . . . . . : 2001:da8:215:8f01:29a0:973d:16b8:18c1(首 选)

本地链接 IPv6 地址. . . . . . . . : fe80::71f5:add5:29ce:4e3%18(首选)

IPv4 地址 . . . . . . . . . . . . : 10.122.201.31(首选)

子网掩码 . . . . . . . . . . . . : 255.255.192.0

获得租约的时间 . . . . . . . . . : 2017年6月16日 19:39:29

租约过期的时间 . . . . . . . . . : 2017年6月16日 23:22:54

默认网关. . . . . . . . . . . . . : fe80::b2f9:63ff:fe37:8489%18

10.122.192.1

DHCP 服务器 . . . . . . . . . . . : 10.3.9.2

DHCPv6 IAID . . . . . . . . . . . : 349197129

DHCPv6 客户端 DUID . . . . . . . : 00-01-00-01-1D-1D-42-A7-30-65-EC-71-61-96

DNS 服务器 . . . . . . . . . . . : 101.226.4.6

114.114.114.114

TCPIP 上的 NetBIOS . . . . . . . : 已启用

## 实验步骤

### 准备工作

1)下载 Wireshark 软件并了解其功能和使用方法。

2)确保计算机已经连接到网络。

3)启动 Wireshark，设置捕获接口（Interface）为本机网卡，选中混杂模式（promiscuous mode）

捕获选项，设置合适的捕获过滤器（Capture Filter）：

 ● 对于 ping 命令，设置过滤器为icmp

 ● 对于 DHCP 消息，设置过滤器为udp port 67

 ● 对于 ARP 消息，设置过滤器为arp

 ● 对于通过网页浏览应用来捕获 TCP 消息，设置过滤器为 tcp port 80

4)开始捕获。

### 数据捕获

**捕获ICMP 协议数据:**

1) 运行 ping 命令（例如：c> ping 192.168.0.1），远程主机地址可以是本机地址、网关路由器地址，也可以是域名（如www.bupt.edu.cn）。将捕获到的数据保存为文件。

2) 使用 Windows 中ping 命令的-l 选项（例如：c>ping -l 8000 192.168.0.1），制作大于8000 字节的IP 包并发送，捕获后分析其分段传输的包结构。

**捕获 DHCP 协议数据:**

1) 使用 ipconfig 命令释放计算机的IP 地址（c>ipconfig -release）；

2) 使用 ipconfig 命令重新申请IP 地址（c>ipconfig -renew）。

此时 wireshark 窗口中可以捕获到完整的DHCP 地址分配的流程，将捕获到的数据保存为文件。

**捕获 ARP 协议数据:**

采用与捕获 DHCP 协议数据相同的方法释放IP 地址并重新申请，在wireshark 窗口中可以捕获到ARP 请求和响应消息，保存为文件。

**捕获 TCP 协议数据:**

打开浏览器，输入一个页面内容较简单网页URL，如www.baidu.com；网页全部显示后关

闭浏览器。

### 协议分析

运行Wireshark 软件，打开所捕获的数据文件，完成下列分析工作：

1) IP 包头分析：对于采用ping 命令-l 选项捕获的ICMP 消息，对承载ICMP 消息的IP 包进行分析，记录包头各字段的值，对照讲义和教材分析各字段的功能，并对于校验和和分段进行验证；

2) ICMP 消息分析：记录并分析ICMP 消息中分析各字段的功能；

3) DHCP 消息分析：针对一次地址分配过程（Transaction ID 相同的4 个消息），分析其通信过程，画出地址分配的消息序列图，并记录采用DHCP 协议配置的各个参数。

4) ARP 消息分析：对照讲义理解ARP 的操作过程，记录并分析消息中各字段的功能。

5) TCP 报头及消息分析：针对TCP 连接建立、连接释放、数据和应答报文段，对照讲义和教材分析各字段的功能；针对一次完整的TCP 通信过程，画出消息序列图，应包含连接建立、数据传送和连接释放阶段。

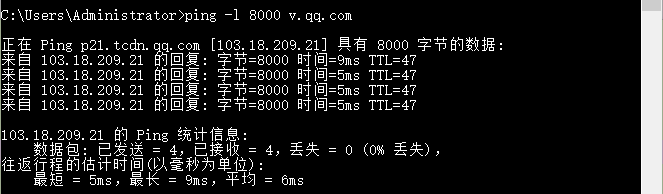
### 撰写实验报告

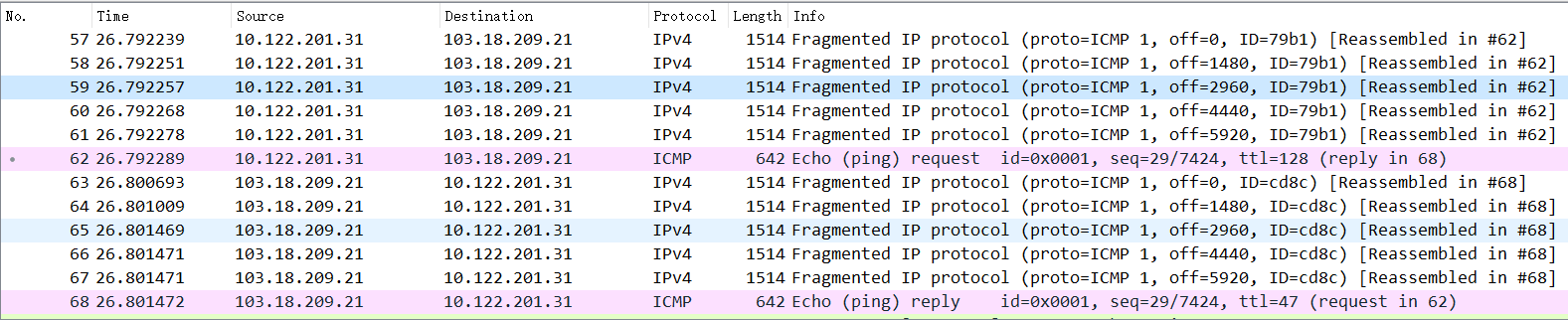
按要求撰写实验报告，对于捕获到的数据进行认真分析，归纳各协议的工作原理和实现要点。

# 若干协议分析

## IP协议分析

使用ping –l 8000 v.qq.com命令捕获IP包消息

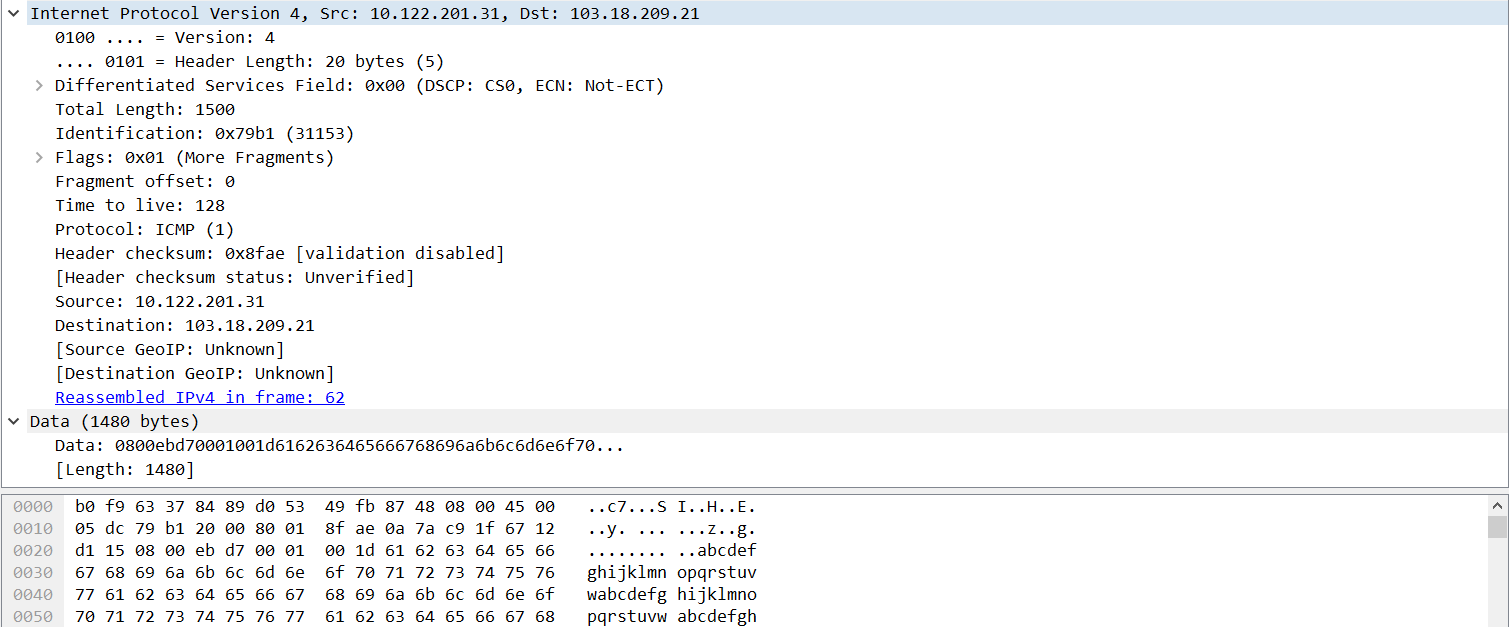




对序号seq为57~61号的IPv4,及62号ICMP进行分析

### 实验中IP包头各字段

分组57号信息截图如下



|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| 包头长度 | 45 | IPV4,包头长20字节,(20=5\*4) |
| 服务类型 | 00 | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc | 数组分组长1500字节（首部加数据） |
| 标识 | 79b1 | 标识为31153 |
| 标志 | 001(二进制) | DF=0，MF=1允许分片，后面还有分片 |
| 片偏移 | 00 00 | 偏移量为0 |
| 生存周期 | 80 | TTL=128,生存时间128跳 |
| 协议 | 01 | 携带数据来自ICMP协议 |
| 头部校验和 | 8fae | IP头部校验和为8fae |
| 源地址 | 0a 7a c9 1f | 源地址为10.122.201.31 |
| 目的地址 | 67 12 d1 15 | 目的地址为103.18.209.21 |

### IP 包头校验和的校验原理，校验和实验验证

Checksum(校验和/检验和) Concept(RFC 1071)，原理：

IP包头的校验和字段是对IP首部进行校验计算得到的校验码，不对数据进行校验。

发送方先将效验字段(16位)置0，然后将所有的16位（半字）累加起来，再取结果的反码，获得16位校验和放入IP该字段中。接收方则依次将所有的16位（半字）累加，求和结果再取补，若结果为0，保留；否则，丢弃。该算法的目的是到达数据包的头校验和计算结果应该为0。这样的校验和对于检测数据包穿过网络时是否发生错误非常有用。

反码求和：将待运算数作为16bit二进制数，然后做带进位加法，将进位作为一个16bit二进制数，加在结果的低位上，重复运算直到没有进位，最后将结果取反。

为了计算一份数据报的IP校验和，先把校验和字段置为0。然后，发送方对首部中每一个16位数据进行二进制反码求和，得到的结果保存在校验和字段中。当接收方收到一份IP数据报之后，对首部中每个16位数据进行二进制反码求和。由于接收方在计算过程中包含了发送方存在首部中的校验和，所以，如果首部在传输过程中没有任何差错，那么接收方计算的结果应该为全1，否则就丢弃收到的数据报。不生成差错报文，由上层发现丢失的数据报并请求进行重传。



以第57号IP包为例

|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| 包头长度 | 45 | IPV4,包头长20字节,(20=5\*4) |
| 服务类型 | 00 | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc | 数组分组长1500字节（首部加数据） |
| 标识 | 79b1 | 标识为31153 |
| 标志 | 001(二进制) | DF=0，MF=1允许分片，后面还有分片 |
| 片偏移 | 00 00 | 偏移量为0 |
| 生存周期 | 80 | TTL=128,生存时间128跳 |
| 协议 | 01 | 携带数据来自ICMP协议 |
| 头部校验和 | 8fae | IP头部校验和为8fae |
| 源地址 | 0a 7a c9 1f | 源地址为10.122.201.31 |
| 目的地址 | 67 12 d1 15 | 目的地址为103.18.209.21 |

包头为(16进制)，20字节：4500 05dc 79b1 2000 8001 8fae 0a7a c91f 6712 d115

4500 🡪🡪🡪🡪 0100 0101 0000 0000

05DC 🡪🡪🡪🡪 0000 0101 1101 1100

79B1 🡪🡪🡪🡪 0111 1001 1011 0001

2000 🡪🡪🡪🡪 0010 0000 0000 0000

8001 🡪🡪🡪🡪 1000 0000 0000 0001

8FAE 🡪🡪🡪🡪 1000 1111 1010 1110

0A7A 🡪🡪🡪🡪 0000 1010 0111 1010

C91F 🡪🡪🡪🡪 1100 1001 0001 1111

6712 🡪🡪🡪🡪 0110 0111 0001 0010

D115 🡪🡪🡪🡪 1100 0001 0001 0101

**+**

**(11) 1111 1111 1111 1100**

**+ 11**

**1111 1111 1111 1111**

**最终所得结果全为1，故IP包中的效验和8fae是正确的。**

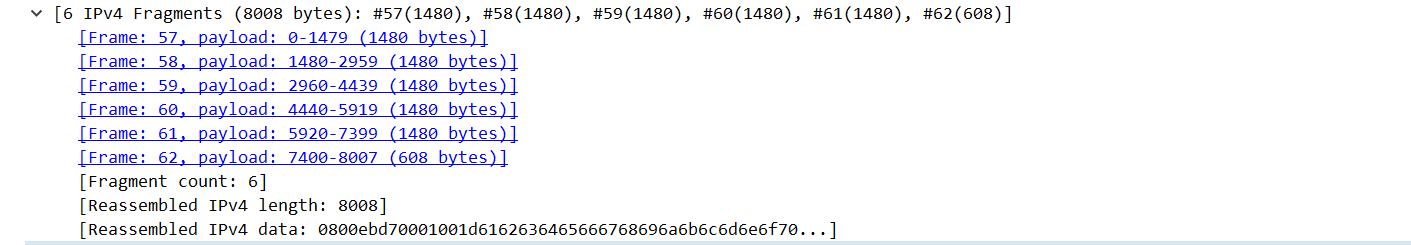
### IP包分段原理，实验验证。

IP包分段原理

●数据链路层具有最大传输单元MTU，限制了数据帧的最大长度，不同的网络类型都有一个上限值。如果IP层进行传输，且IP数据报大小超过MTU，则要进行分段处理，使得每一段的片段长度应该是不超过MTU的最大长度（包括包头），除最后一个片段外，其他片段内长度应该是8的整数倍。

●分段中的每一段都具有相同的标识（Identification）值，使用MF与DF以及偏移Fragment offset来确定该包的相对位置。MF=1表明后续还有分段，MF=0表明该分段是该IP数据报的最后一个分段。DF=0时，表明该数据报允许分段，DF=1表明该数据报不允许分段。

●Fragment offset分段偏移字段指明了该分段在当前数据报中的什么位置上。除了一个数据包的最后一个分段以外，其他所有的分段必须是8字节的倍数，8字节是片偏移基本分段单位。



在此次实验中，ping包长度8000字节，在传输过程中进行了分段处理，一共分为6段，序号57~62，第一段offset=0，第二段offset=1480，第三段offset=2960，第四段offset=4440，第五段offset=5920，第六段offset=7400，都指明了各段在数据报中的位置，并且都是1480的倍数，当然也是8的倍数，同时第6段中MF=0，表明后续不再有分段。

一个数据链路层的帧长为1514字节，除去数据链路层的源地址、目的地址各占6字节，还有类型2字节。剩余1500字节为IP数据报的最大长度，除去IP包首部的20字节，每个IP包实际最大数据长度为1480字节，刚好是每个分段偏移量公差。最后一个包将剩余不足1480字节的数据全部发出去。

数据链路层使用以太网V2 MAC帧 。

以下是序号57~62号包的全部信息，符合IP数据报的分段原理。

分组57号信息如下:

|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| 包头长度 | 45 | IPV4,包头长20字节,(20=5\*4) |
| 服务类型 | 00 | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc | 数组分组长1500字节（首部加数据） |
| 标识 | 79b1 | 标识为31153 |
| 标志 | 001(二进制) | DF=0，MF=1允许分片，后面还有分片 |
| 片偏移 | 00 00 | 偏移量为0 |
| 生存周期 | 80 | TTL=128,生存时间128跳 |
| 协议 | 01 | 携带数据来自ICMP协议 |
| 头部校验和 | 8fae | IP头部校验和为8fae |
| 源地址 | 0a 7a c9 1f | 源地址为10.122.201.31 |
| 目的地址 | 67 12 d1 15 | 目的地址为103.18.209.21 |

分组58号信息如下:

|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| 包头长度 | 45 | IPV4,包头长20字节,(20=5\*4) |
| 服务类型 | 00 | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc | 数组分组长1500字节（首部加数据） |
| 标识 | 79b1 | 标识为31153 |
| 标志 | 001(二进制) | DF=0，MF=1允许分片，后面还有分片 |
| 片偏移 | 00 b9 | 偏移量为185,即185\*8=1480字节 |
| 生存周期 | 80 | TTL=128,生存时间128跳 |
| 协议 | 01 | 携带数据来自ICMP协议 |
| 头部校验和 | 8ef5 | IP头部校验和为8ef5 |
| 源地址 | 0a 7a c9 1f | 源地址为10.122.201.31 |
| 目的地址 | 67 12 d1 15 | 目的地址为103.18.209.21 |

分组59号信息如下:

|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| 包头长度 | 45 | IPV4,包头长20字节,(20=5\*4) |
| 服务类型 | 00 | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc | 数组分组长1500字节（首部加数据） |
| 标识 | 79b1 | 标识为31153 |
| 标志 | 001(二进制) | DF=0，MF=1允许分片，后面还有分片 |
| 片偏移 | 01 72 | 偏移量为370,即370\*8=2960字节 |
| 生存周期 | 80 | TTL=128,生存时间128跳 |
| 协议 | 01 | 携带数据来自ICMP协议 |
| 头部校验和 | 8e3c | IP头部校验和为8e3c |
| 源地址 | 0a 7a c9 1f | 源地址为10.122.201.31 |
| 目的地址 | 67 12 d1 15 | 目的地址为103.18.209.21 |

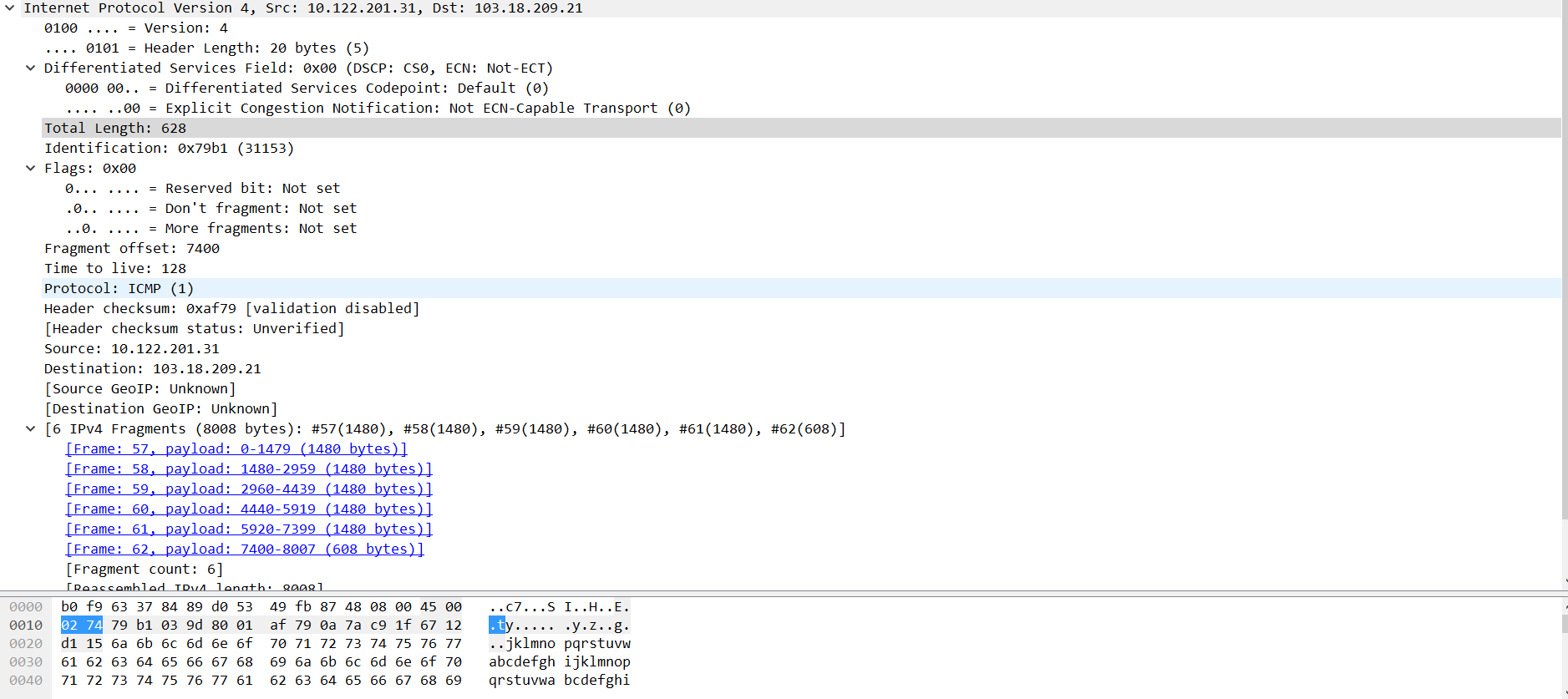
分组60号信息如下:

|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| 包头长度 | 45 | IPV4,包头长20字节,(20=5\*4) |
| 服务类型 | 00 | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc | 数组分组长1500字节（首部加数据） |
| 标识 | 79b1 | 标识为31153 |
| 标志 | 001(二进制) | DF=0，MF=1允许分片，后面还有分片 |
| 片偏移 | 02 2b | 偏移量为555,即555\*8=4440字节 |
| 生存周期 | 80 | TTL=128,生存时间128跳 |
| 协议 | 01 | 携带数据来自ICMP协议 |
| 头部校验和 | 8d83 | IP头部校验和为8d83 |
| 源地址 | 0a 7a c9 1f | 源地址为10.122.201.31 |
| 目的地址 | 67 12 d1 15 | 目的地址为103.18.209.21 |

分组61号信息如下:

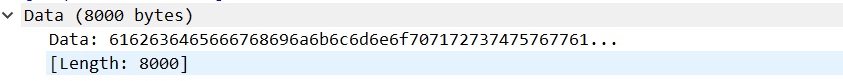
|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| 包头长度 | 45 | IPV4,包头长20字节,(20=5\*4) |
| 服务类型 | 00 | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 05dc | 数组分组长1500字节（首部加数据） |
| 标识 | 79b1 | 标识为31153 |
| 标志 | 001(二进制) | DF=0，MF=1允许分片，后面还有分片 |
| 片偏移 | 02 e4 | 偏移量为740,即740\*8=5920字节 |
| 生存周期 | 80 | TTL=128,生存时间128跳 |
| 协议 | 01 | 携带数据来自ICMP协议 |
| 头部校验和 | 8cca | IP头部校验和为8cca |
| 源地址 | 0a 7a c9 1f | 源地址为10.122.201.31 |
| 目的地址 | 67 12 d1 15 | 目的地址为103.18.209.21 |

分组62号信息如下:



|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| 包头长度 | 45 | IPV4,包头长20字节,(20=5\*4) |
| 服务类型 | 00 | 正常时延，正常吞吐量，正常可靠性 |
| 总长度 | 0274 | 数组分组长628字节（首部加数据） |
| 标识 | 79b1 | 标识为31153 |
| 标志 | 000(二进制) | DF=0，MF=0允许分片，最后一个分片 |
| 片偏移 | 03 9d | 偏移量为925,即95\*8=7400字节 |
| 生存周期 | 80 | TTL=128,生存时间128跳 |
| 协议 | 01 | 携带数据来自ICMP协议 |
| 头部校验和 | af79 | IP头部校验和为af79 |
| 源地址 | 0a 7a c9 1f | 源地址为10.122.201.31 |
| 目的地址 | 67 12 d1 15 | 目的地址为103.18.209.21 |

该包是第六段，即最后一段，长度为628字节，除去IP包头20字节，除去该ICMP包的8字节，剩余600字节数据，再加上前5个分段的数据，600+5\*1480=8000字节。表明ping –l 8000 v.qq.com命令，可知IP数据报完整达到。



## ICMP协议分析

### 理解 ICMP 的功能

为了提高 IP 数据报交付成功的机会，在网际层使用了因特网控制报文协议 ICMP (Internet Control Message Protocol)。ICMP 允许主机或路由器报告差错情况和提供有关异常情况的报告。

ICMP 报文作为 IP 层数据报的数据，加上数据报的首部，组成IP 数据报发送出去，并且ICMP协议数据包对IP分组在传送时出现的异常情况进行报告，对IP报文传输时出现的差错、拥塞、路由改变、以及路由器或主机信息的获取等情况，向源端主机提交报告，由源主机采取相应措施，改进传输质量。

ICMP 报文的种类有两种，即 ICMP 差错报告报文和 ICMP 询问报文。

ICMP 差错报告报文共有 5 种：

• 终点不可达

• 源站抑制

• 时间超过

• 参数问题

• 改变路由（重定向）

ICMP 询问报文有四种：

• 回送请求和回答报文

• 时间戳请求和回答报文

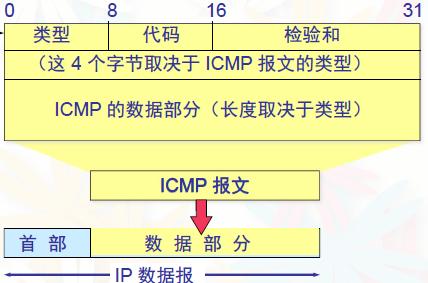
• 掩码地址请求和回答报文

• 路由器询问和通告报文

PING 使用了 ICMP 回送请求与回送回答报文，用来测试两个主机之间的连通性和到达目的主机的路径和跳数等。

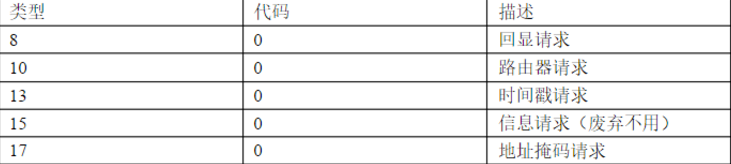
### ICMP 的包格式，各字段的功能。

ICMP 报文的前 4 个字节是统一的格式，共有三个字段：即类型、代码和检验和。后 4 个字节的内容与 ICMP 的类型有关。格式如下：

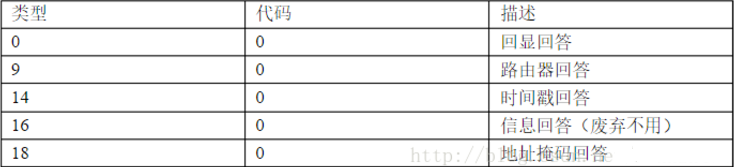


ICMP不同报文类型，其Type值不同，通过查阅资料得：

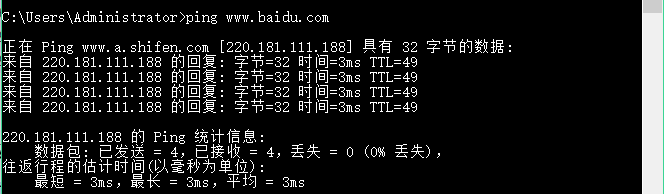
ICMP不同的报文类型号不同，比如08代表回显请求，00代表回显应答等。

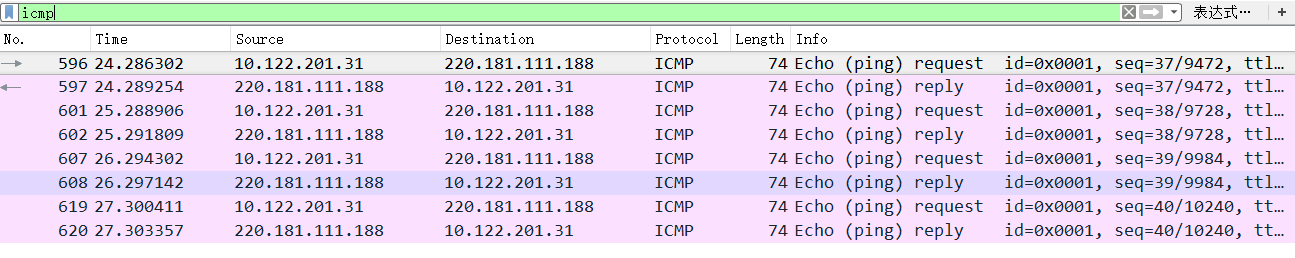


ICMP的回答报文有以下5种：

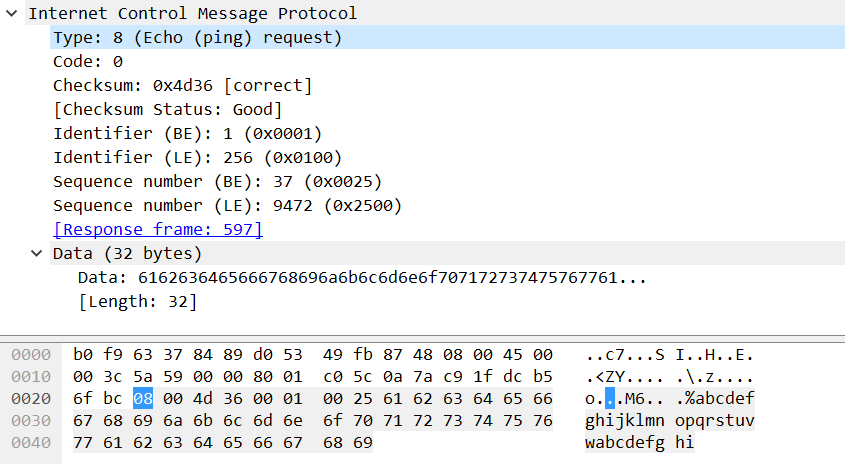


实验内容，ping www.baidu.com分析：





选取第一个序号为596的ICMP包分析：



该包是ICMP请求包（16进制）：08 00 4d 36 00 01 00 25，含义如下

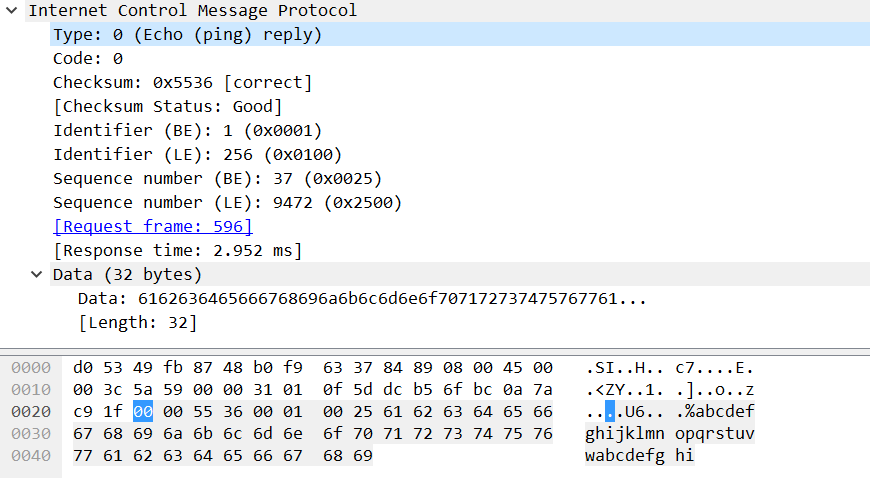
|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| 类型 | 08 | 回显请求报文 |
| 代码 | 00 | 表明是一个回显请求报文 |
| 校验和 | 4d36 | 整个ICMP部分的校验和 |
| 标识符 | 大端表示0001  小端表示0100 | 标明上层进程ID |
| 序列号 | 大端表示0025  小端表示2500 | 包的序列号，37号 |

效验和分析，采用与IP数据报一样的反码求和运算：

0800+4d36+0001+0025+6162+6364+6566+6768+696a+6b6c+6d6e+6f70+7172+7374+7576+7761+6263+6465+6667+6869=ffff

能够获得与IP效验类似的效验效果，但对象是对整个ICMP部分效验。

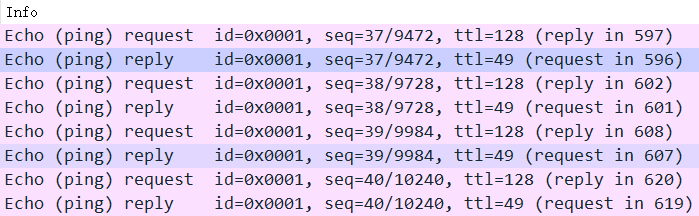
选取序号597的ICMP包进行分析



该包是ICMP应答包（16进制）：00 00 55 36 00 01 00 25，含义如下

|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| 类型 | 00 | 回显应答报文 |
| 代码 | 00 | 表明是一个回显应答报文 |
| 校验和 | 5536 | 整个ICMP部分的校验和 |
| 标识符 | 大端表示0001  小端表示0100 | 标明上层进程ID |
| 序列号 | 大端表示0025  小端表示2500 | 包的序列号，37号 |

Type:08为回显请求；Type:00为回显应答。

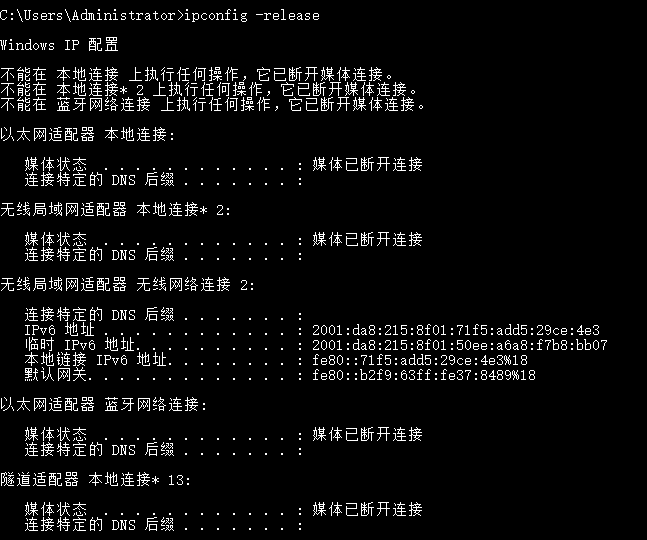


ID与序列号部分，一次PING命令会发送4个包，它们的ID是相同的，序号递增。

## DHCP协议分析

**准备阶段：**

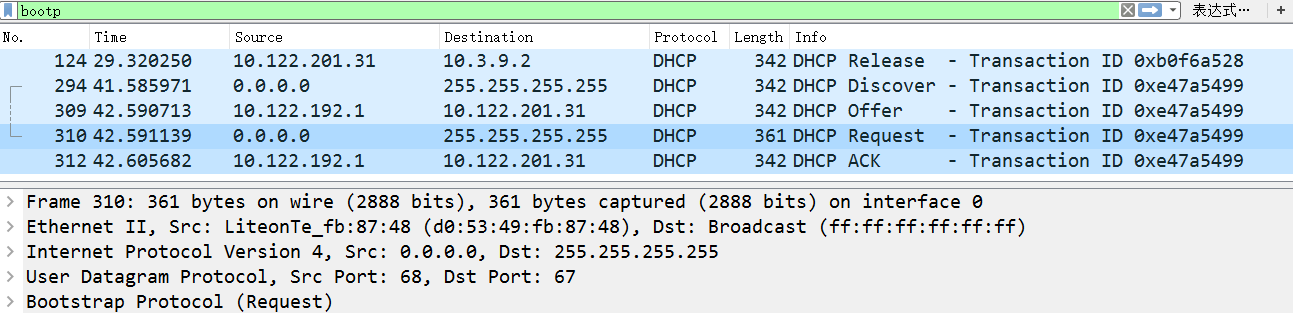
使用 ipconfig 命令释放计算机的IP 地址（c>ipconfig -release）



使用 ipconfig 命令重新申请IP 地址（c>ipconfig -renew）



在wireshark中捕获DHCP包



### DHCP 的功能、配置参数

DHCP是动态主机配置协议（Dynamic host configuration protocol）的简称，它提供对于远程主机的自动配置，包括IP地址、路由地址、子网掩码、DNS服务器地址，是一个应用层上的协议，使网络环境中的主机动态的获得IP地址、Gateway地址、DNS服务器地址等信息，并能够提升地址的使用率。

●DHCP有三种机制分配IP地址：

1) 自动分配方式（Automatic Allocation），DHCP服务器为主机指定一个永久性的IP地址，一旦DHCP客户端第一次成功从DHCP服务器端租用到IP地址后，就可以永久性的使用该地址。

2) 动态分配方式（Dynamic Allocation），DHCP服务器给主机指定一个具有时间限制的IP地址，时间到期或主机明确表示放弃该地址时，该地址可以被其他主机使用。

3) 手工分配方式（Manual Allocation），客户端的IP地址是由网络管理员指定的，DHCP服务器只是将指定的IP地址告诉客户端主机。

三种地址分配方式中，只有动态分配可以重复使用客户端不再需要的地址。

●DHCP的报文格式

|  |  |  |  |
| --- | --- | --- | --- |
| OP(1) | Htype(1) | Hlen(1) | Hops(1) |
| Transaction ID(4) | | | |
| Seconds(2) | | Flags(2) | |
| Ciaddr(4) | | | |
| Yiaddr(4) | | | |
| Siaddr(4) | | | |
| Giaddr(4) | | | |
| Chaddr(16) | | | |
| Sname(64) | | | |
| File(128) | | | |
| Options | | | |

OP：若是client送给server的封包，设为1，反向为2；

Htype：硬件类别，ethernet为1； Hlen：硬件长度，ethernet为6；

Hops：若数据包需经过router传送，每站加1，若在同一网内，为0；

Transaction ID：事务ID，是个随机数，用于客户和服务器之间匹配请求和相应消息；

Seconds：由用户指定的时间，指开始地址获取和更新进行后的时间；

Flags：从0-15bits，最左一bit为1时表示server将以广播方式传送封包给 client，其余尚未使用；

Ciaddr：用户IP地址； Yiaddr：服务器分配给客户的IP地址；

Yiaddr：服务器分配给客户的IP地址；

Siaddr：用于bootstrap过程种的IP地址；（服务器的IP地址）

Giaddr：转发代理（网关）IP地址；

Chaddr：Client的硬件地址；

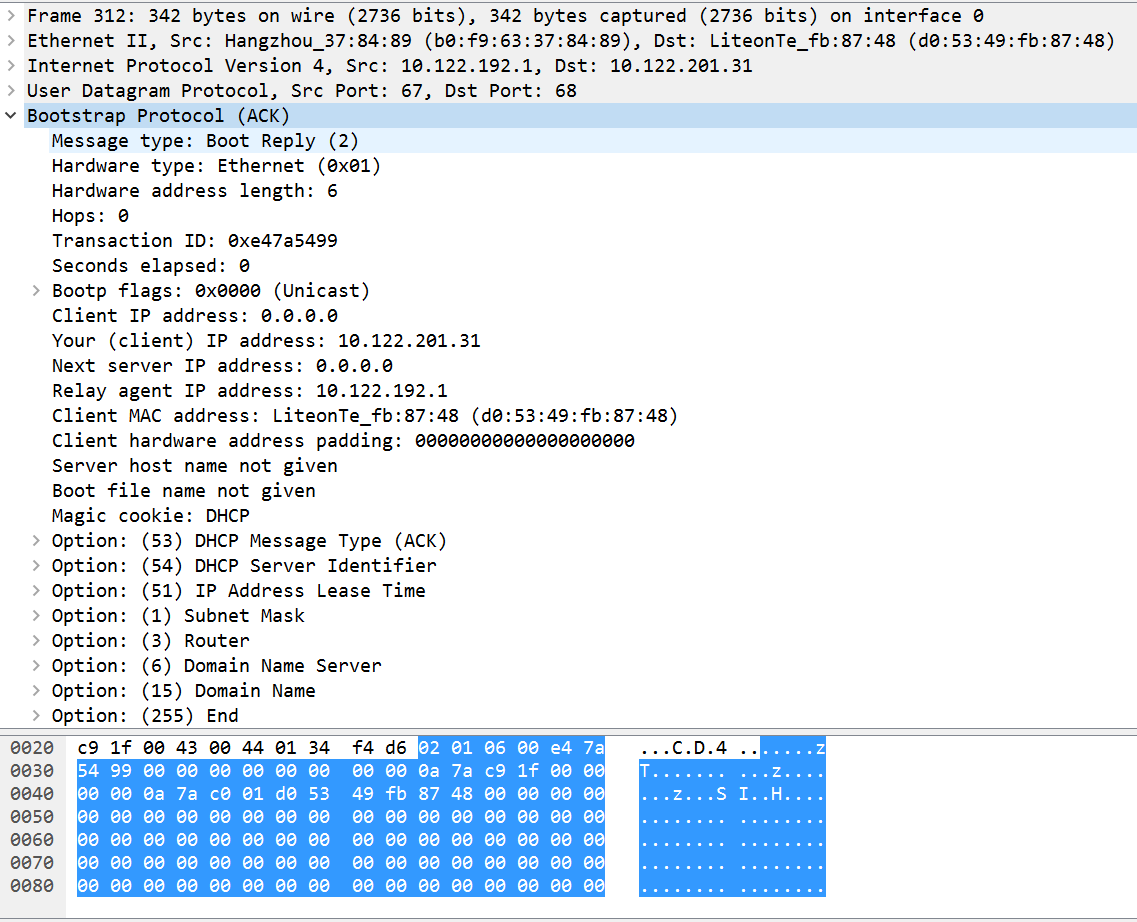
Sname：可选server的名称，以0x00结尾；

File：启动文件名；

Options：厂商标识，可选的参数字段。

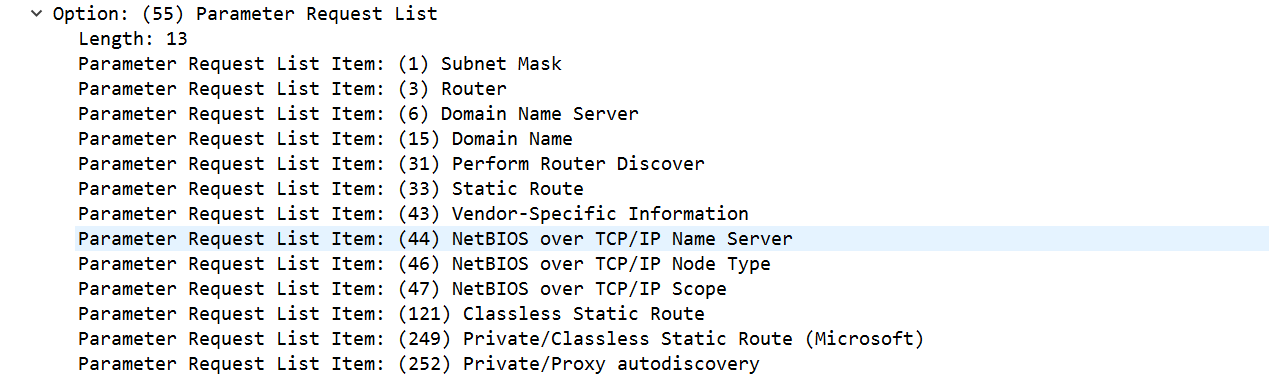
●DHCP ACK信息

对已经捕获的DCHP ACK 进行分析：

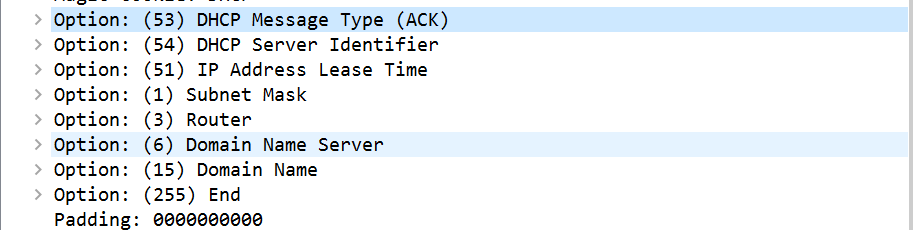


|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| Message type | 02 | boot reply，操作码 |
| Hardware type | 01 | Ethernet，硬件类型 |
| Hardware address length | 06 | 硬件地址长度 |
| Hop | 00 | 跳数，默认0 |
| Transaction ID | 0xe47a5499 | 事务标识，本次通信客户端选择的随机数 |
| Seconds elapsed | 00 | 过去的秒数 |
| Bootp flags | 0000 | 标志字段，0表示单播 |
| Client IP address | 00000000 | 客户IP 0.0.0.0 |
| Your IP address | 0a7ac91f | 填写分配给client(自己)的ip地址10.122.201.31 |
| Next server IP address | 00000000 | 若 client 需要透过网络开机，此栏填写开机程序代码所在 server 之地址 |
| Relay agent IP address | 0a7ac001 | 若需跨网域进行 DHCP 发放，此栏为 relay agent 的地址，否则为0 |
| Client MAC address | d05349fb8748 | 客户端MAC地址 |
| Client hardware address padding | 00000000000000000000 | 客户端MAC地址填充字段 |
| DHCP message type | 350105 | 长度：1 ACK：5 |
| Server identifier | 36040a030902 | 长度：4 服务商标识符 10.3.9.2 |
| IP Address Lease Time | 330400000e10 | 长度：4 IP地址释放时间1小时后 |
| Subnet mask | 0104ffffc000 | 长度：4  255.255.192.0 |
| Router | 03040a7ac001 | 长度：4 路由器地址10.122.192.1 |
| Domain Name server | 060c0a0309040a0309050a030906 | 长度：12  10.3.9.4/10.3.9.5/10.3.9.6 |
| Domain Name | 0f0b627570742e6564752e636e | 长度：11  域名：bupt.edu.cn |
| End | Ff | 结束标志 |

对于可选字段，是客户端与主机协商使用的字段，在DHCP Request中，客户端发送一个需求列表，表明想要获得的字段：

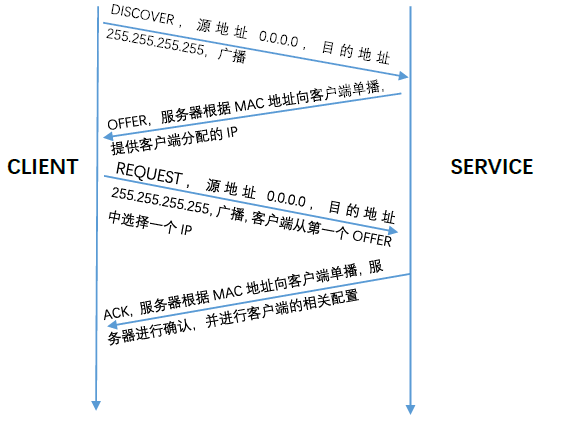


在DHCP ACK中，服务器回应客户端以提供的字段：



DHCP向网络主机提供配置参数，它由两个基本部分组成：一部分是向网络主机传送专用的配置信息，另一部分是给主机分配网络地址。DHCP是用于向客户传送配置信息的，客户从DHCP服务器那里获得配置信息后应该可以和Internet上任何一台主机通信。在初始化一台主机时并不需要配置所有这些参数，客户和服务器可以通过一种商讨机制决定传送哪些参数。DHCP允许（不要求）客户参数配置不直接与IP协议相关，而且它也不将最加入的主机加入域名系统（DNS）中。

### DHCP地址分配过程消息序列图



发生“四次握手”

1. DHCP DISCOVER

用户申请IP地址发送DHCP discover, discover包是客户端发送的广播包，数据链路层的mac地址也是广播地址，UDP数据包报中的src port 68，dst port 67。客户端简要汇报自己的网络信息，并在可选字段中附加DHCP type为discover，表示申请一个IP地址。

1. DHCP OFFER

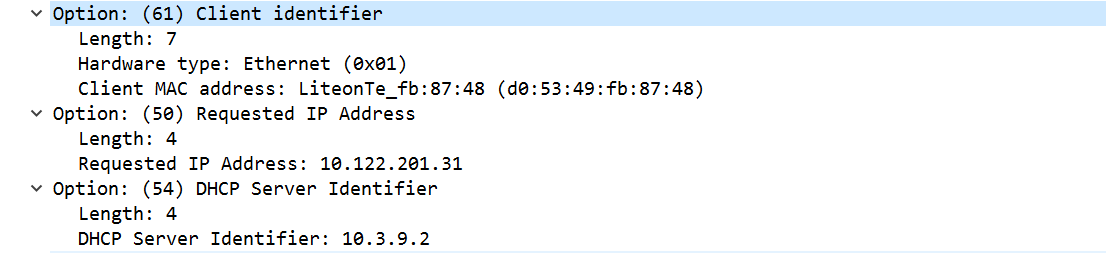
DHCP服务器会保存一定时间的IP与MAC绑定的信息，所以申请ip时在第二阶段DHCP服务器就分配了该客户端上次的IP地址，并填入目的地址处发回。DHCP服务器广播一个DHCP offer。在DHCP offer 包中有：

Your (client) IP address: 10.122.201.31

Client MAC address: LiteonTe\_fb:87:48 (d0:53:49:fb:87:48)

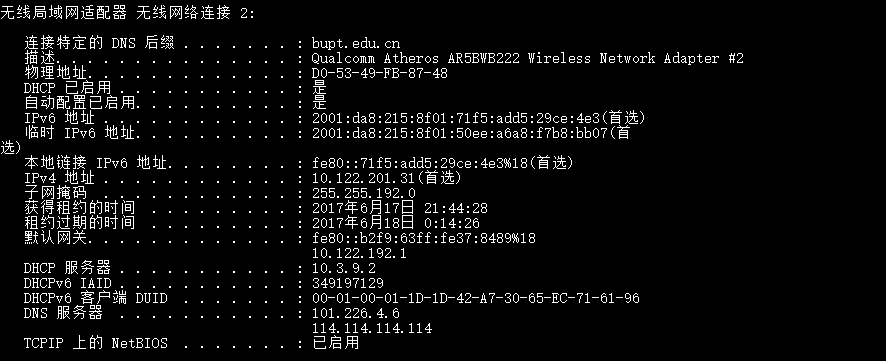
1. DHCP REQUEST

第三次，客户端发给服务器的包也是广播包，因为可能有多个DHCP服务器都给客户端发送了可用IP地址，而客户端需要让所有的DHCP服务器知道它接受哪个DHCP服务器提供的IP地址。



可选字段可以看出，客户端确认了mac地址(61),接受IP地址(50),接受DHCP服务器(54), 以便DHCP服务器在IP与mac表中记录。

总结：客户端mac d0-53-49-fb-87-48 接受了DHCP服务器10.3.9.2 所提供的IP地址 10.122.201.31。通过ipconfig /all命令，可查看：与包中记录匹配。



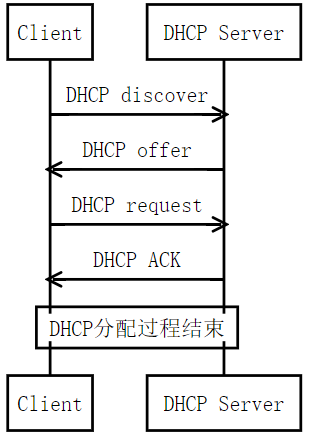
1. DHCP ACK

最后一次确认，DHCP服务器回复上一次request中客户端要求的额外信息。此时，租用时间开始生效。

在实际使用中，当DHCP客户端启动或IP地址租约期限达到一半时，client会自动向DHCP Server发送DHCP request报文，以完成IP租约的更新。如果此IP地址有效，则DHCP Server回一个DHCP ACK，通知client已获得新的ip租约。

●当前网络环境下，路由器与DHCP服务器并非同一个设备，因为路由器IP与DHCP服务器IP并不一致。更多的，本次抓包实验并未发生DHCP relay。

消息序列图：



总体流程：

1.执行ipconfig /release 释放本机ip地址。

2.执行ipconfig /renew更新所有适配器，由于本地主机没有ip地址，也不知道DHCP服务器的地址，所以发送DHCP discover报文时，源地址为0.0.0.0，目的地址为255.255.255.255，本地网络上所有的主机都能收到该报文。

3.DHCP收到DHCP discover报文后，向网络广播DHCP offer报文。

4.本地主机收到DHCP offer报文后，向DHCP服务器发送DHCP request报文。

5.DHCP服务器收到DHCP request报文后，回复DHCP ack报文，给本地主机分配一个IP地址。本地主机就得到一个临时ip地址。至此四次握手完成。

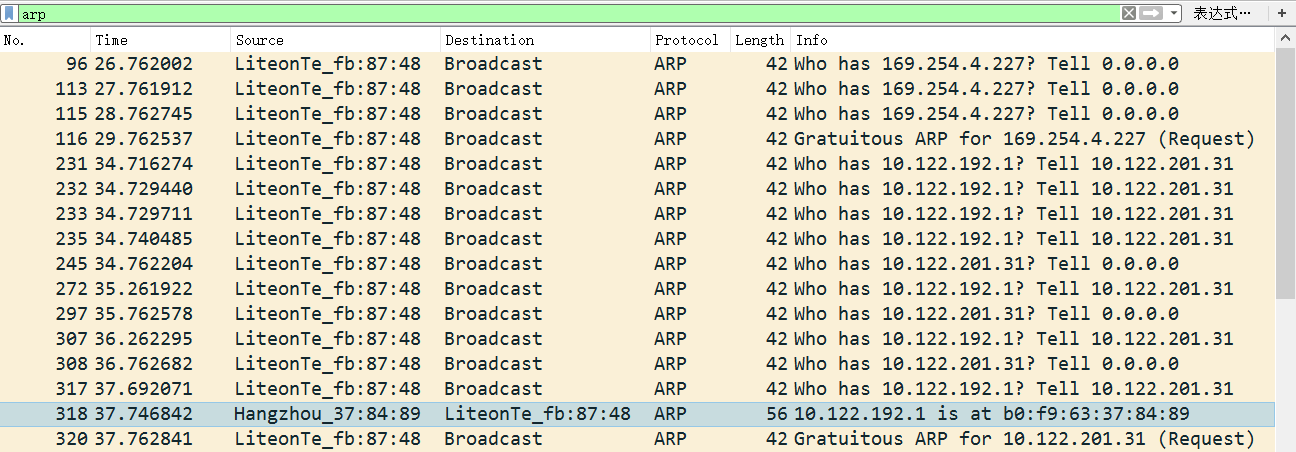
## ARP协议分析

### ARP功能与操作原理

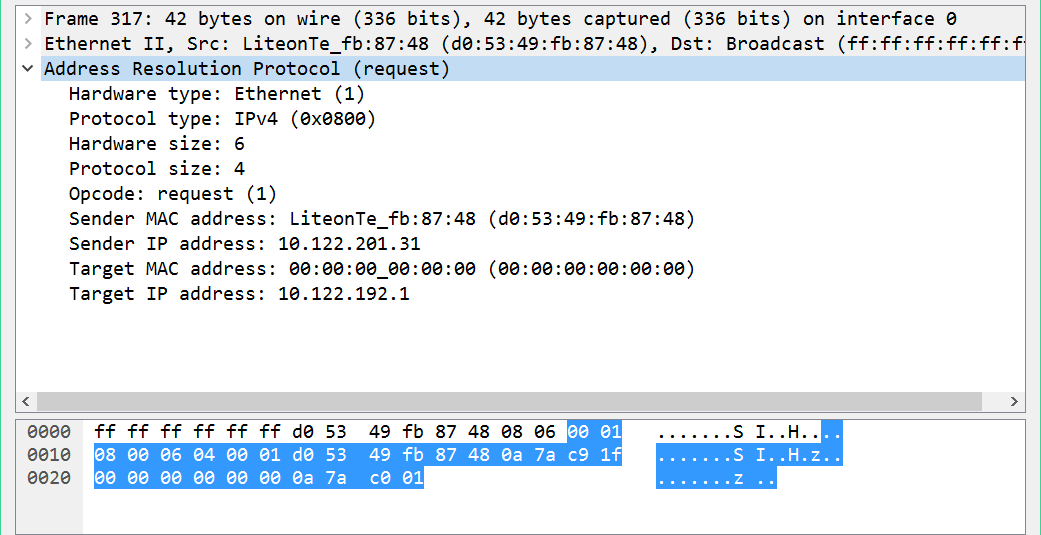
使用 ipconfig 命令释放计算机的IP 地址（c>ipconfig -release）

使用 ipconfig 命令重新申请IP 地址（c>ipconfig -renew）

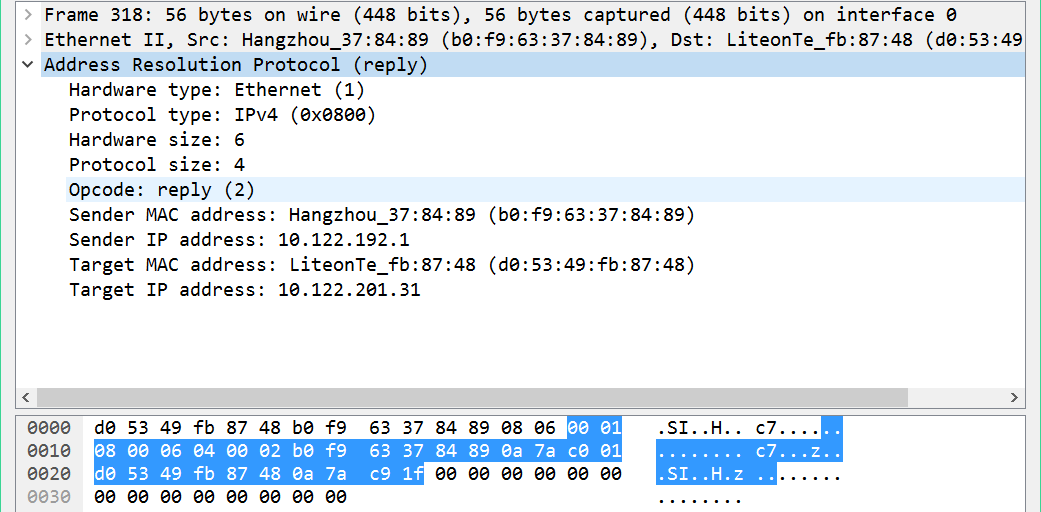
设置过滤器ARP,wireshark中显现：



request包：



Reply 包：

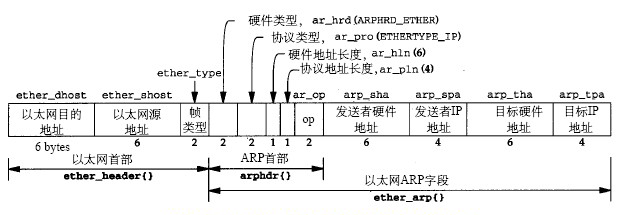


本地局域网内的主机用广播的方式发送ARP报文，来获取彼此的硬件地址。

ARP基本功能：在以太网协议中规定，同一局域网中的一台主机要和另一台主机进行直接通信，必须要知道目标主机的MAC地址。而在TCP/IP协议栈中，网络层和传输层只关心目标主机的IP地址。这就导致在以太网中使用IP协议时，数据链路层的以太网协议接到上层IP协议提供的数据中，只包含目的主机的IP地址。于是需要一种方法，根据目的主机的IP地址，获得其MAC地址。这就是ARP协议要做的事情。所谓地址解析（address resolution）就是主机在发送帧前将目标IP地址转换成目标MAC地址的过程。

### ARP包格式，各字段功能

ARP包格式：



request包数据链路层帧头部分源地址是本机mac，目的地址是广播地址全f，表格列出了ARP协议的数据内容。

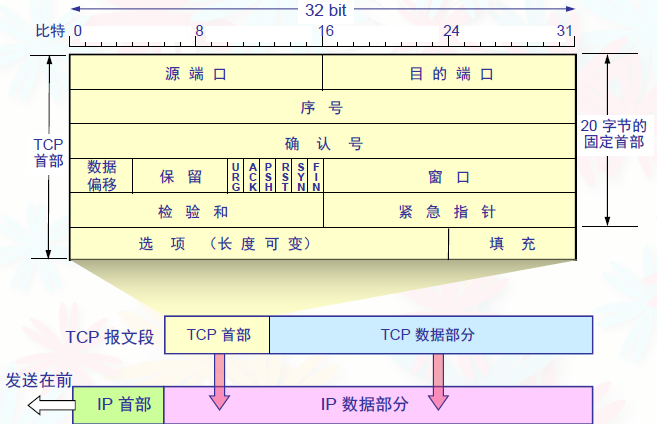
|  |  |  |
| --- | --- | --- |
| 字 段 | 报 文(16进制) | 内 容 |
| Hardware type | 0001 | Ethernet，硬件类型 |
| Protocol type | 0800 | IPv4 |
| Hardware size | 06 | 硬件地址长度6字节 |
| Protocol size | 04 | 协议长度 |
| Opcode | 0001(ARP请求)  0002(ARP响应)  0003(RARP请求)  0004(RARP响应) | 操作码指明操作类型 |
| Sender MAC address | D05349fb8748 | 发送方mac地址 |
| Sender IP address | 0a7ac91f | 发送方IP 10.122.201.31 |
| Target MAC address | 000000000000 | 目标mac地址 |
| Target IP address | 0a7ac001 | 目标IP 10.122.192.1 |

同样可知，reply包中，IP地址为10.122.192.1的mac地址为b0f963378489。

## TCP协议分析

### TCP报文字段功能

TCP报文格式：

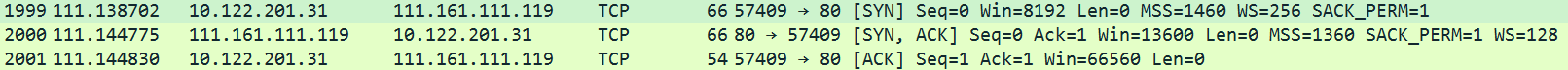


各字段功能：

|  |  |  |
| --- | --- | --- |
| 字 段 | 长 度 | 功 能 |
| 源端口 | 2字节 | 发送方端口 |
| 目的端口 | 2字节 | 接收方端口 |
| 序号 | 4字节 | 本报文段所发送的数据的第一个字节的序号 |
| 确认号 | 4字节 | 期望收到对方的下一个报文段的数据的第一个字节的序号 |
| 数据偏移 | 4bits | TCP 报文段的数据起始处距离,TCP 报文段的起始处有多远, “数据偏移”的单位是4字节。 |
| 保留字段 | 6bits | 保留为今后使用，但目前应置为0 |
| URG紧急比特 | 1bit | 表明紧急指针字段有效 |
| ACK确认比特 | 1bit | 当 ACK=1 时确认号字段才有效 |
| PSH推送比特 | 1bit | 置1，则尽快交付 |
| RST复位比特 | 1bit | 置1，出现严重差错，释放连接，重新接力运输连接 |
| SYN同步比特 | 1bit | 置1，表明一个连接请求或连接接受报文 |
| FIN终止比特 | 1bit | 置1，用来释放一个连接 |
| 窗口 | 2字节 | 控制对方发送的数据量. |
| 校验和 | 2字节 | 检验和字段检验的范围包括（包括伪首部）首部和数据这两部分 |
| 紧急指针 | 2字节 | 指出在本报文段中的紧急数据的最后一个字节的序号 |
| 选项 | 长度可变 | 告知最大报文段长度 MSS |
| 填充 | 不定 | 使整个首部长度是 4 字节的整数倍 |

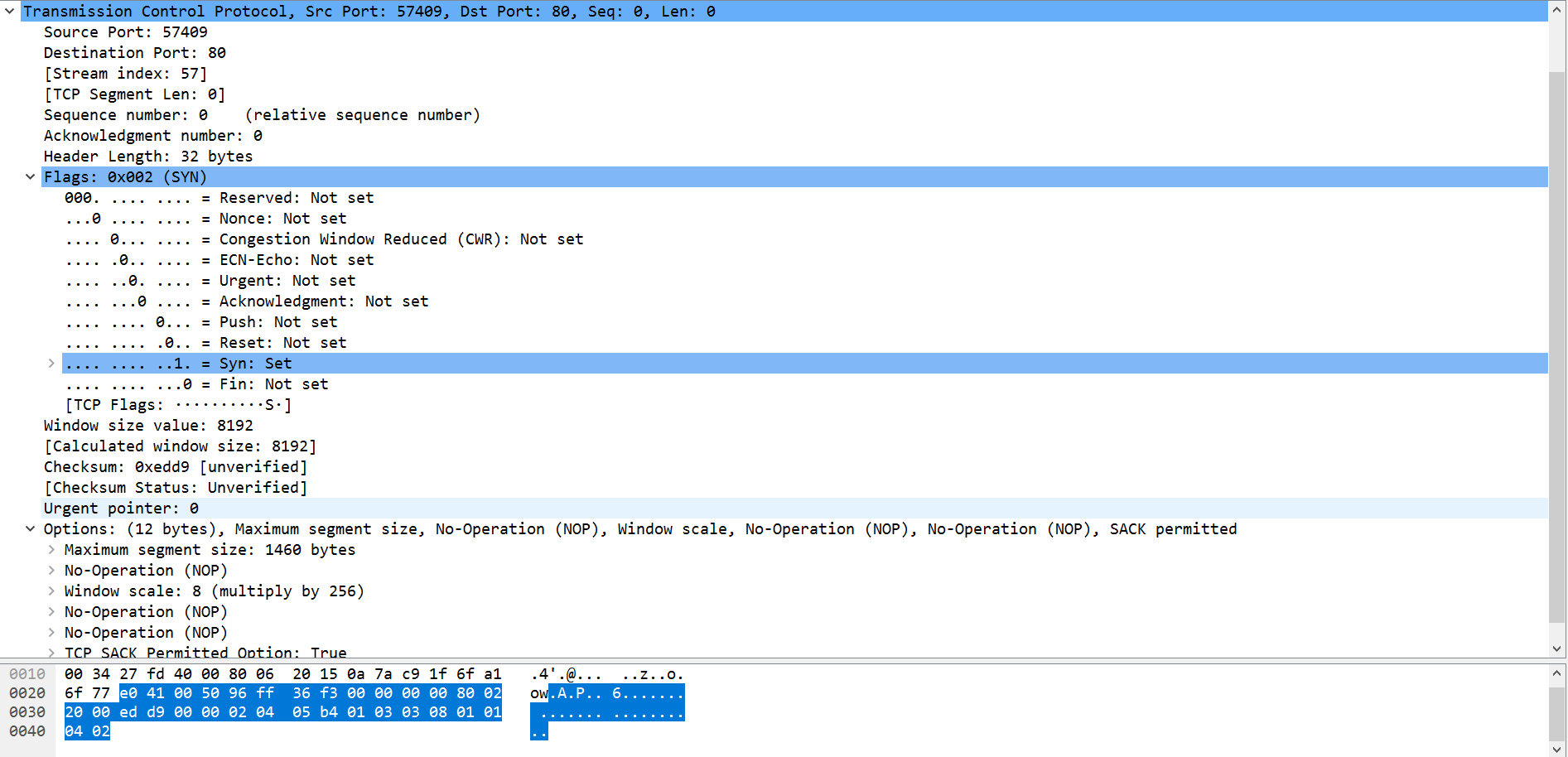
### 建立和连接释放过程的消息序列图

TCP建立连接的三次握手：



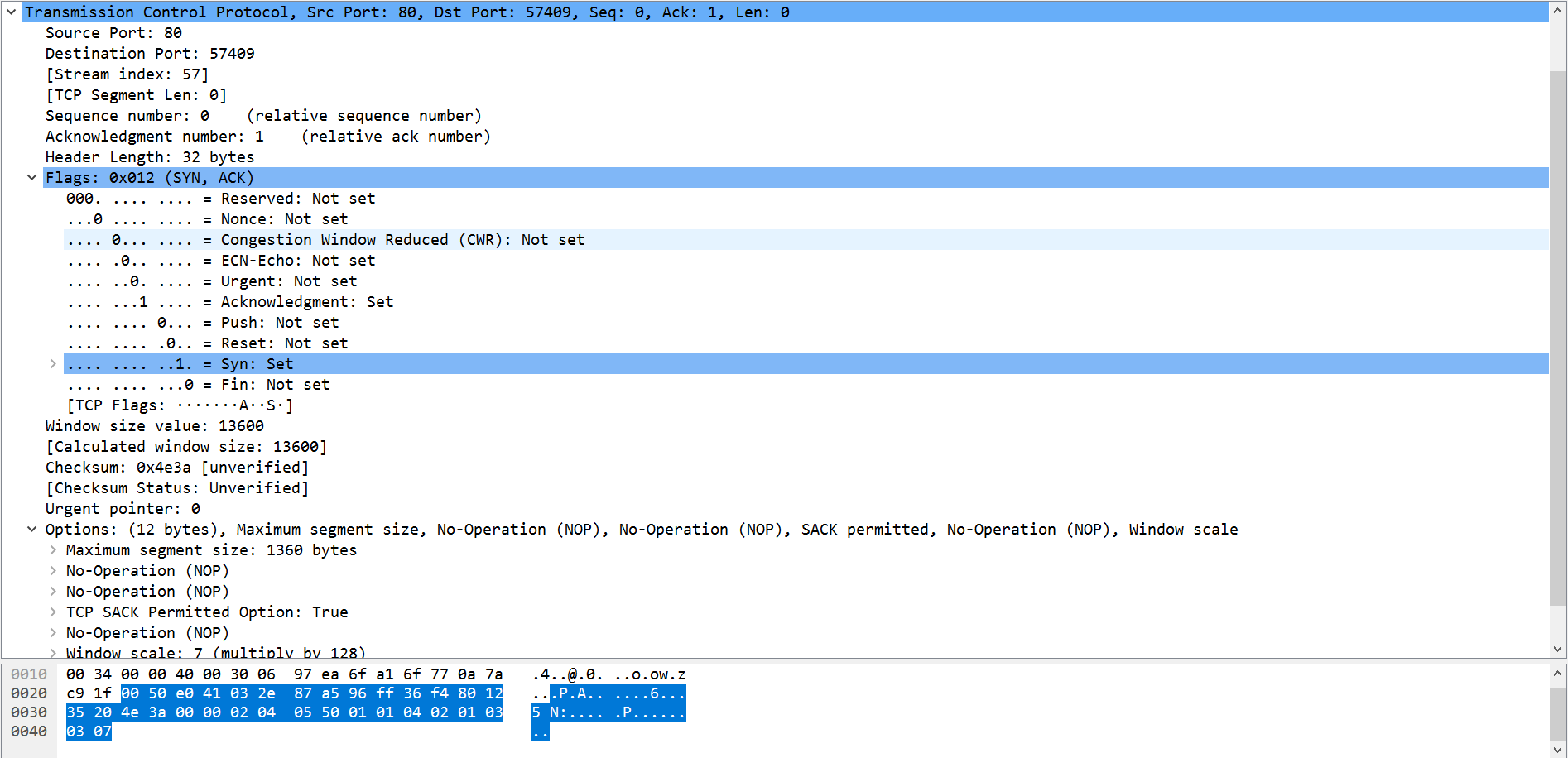
上图三个包对应一次三次握手建立连接：

1. 第一次握手：



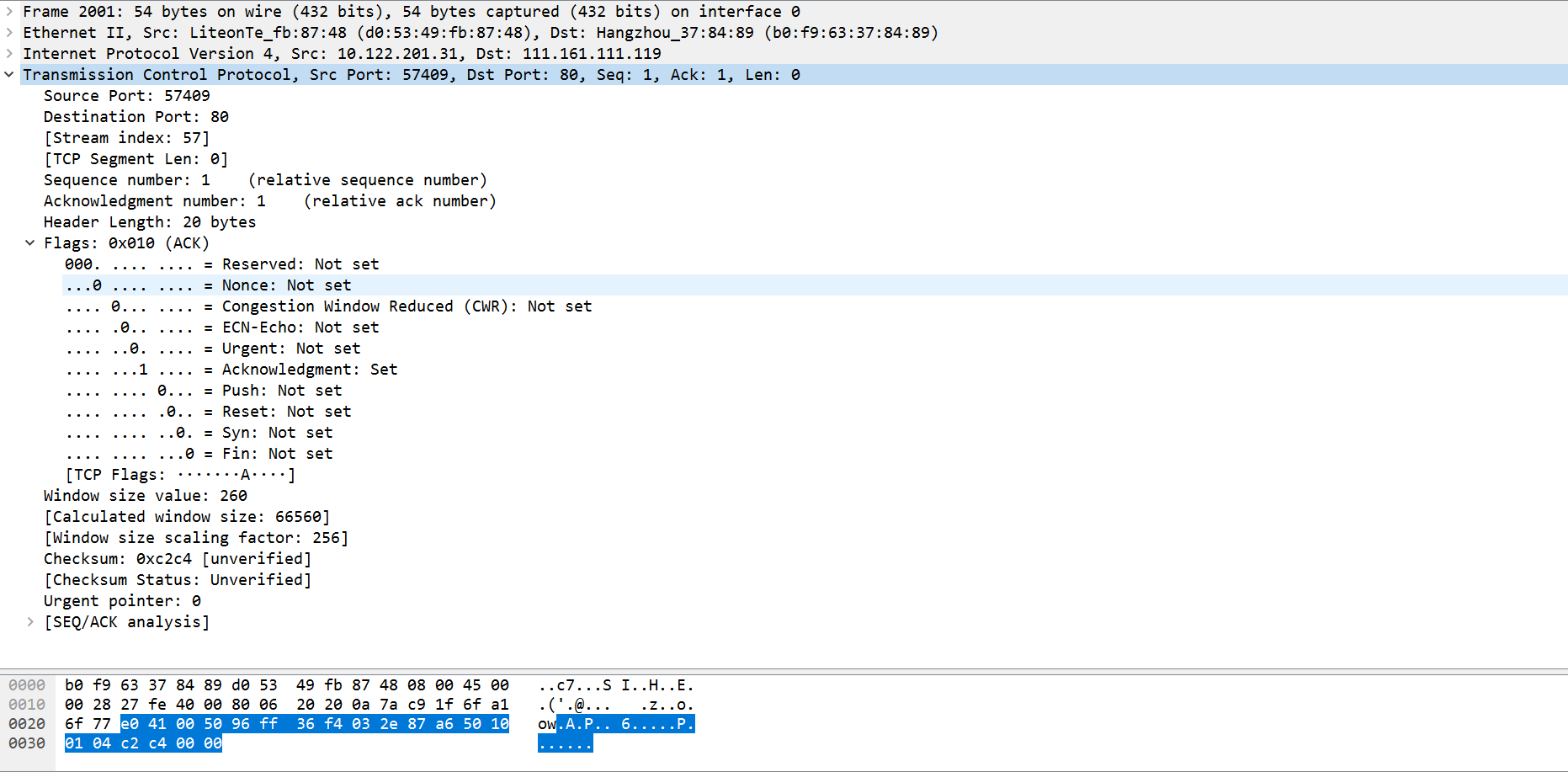
客户端发送请求给服务器，源端口57409，目的端口80，相对序号seq=0（实际96ff36f3）ACK序号00000000，首部长32字节，同步比特SYN为1，表明是一个连接请求的报文。Window size 8192，校验和0xedd9，状态表明还未经证实。

1. 第二次握手：



服务器回应客户端，源端口号80，目的端口号57409，相对序号seq=0，ACK序号1（96ff36f4=等于上一个包实际seq+1）。Win=13600。标志字段SYN与ACK为1，表示确认了客户端发过来的0号包，回复了一个同意申请建立连接的包。

1. 第三次握手：



客户端发给服务器，序号seq增长为1（96ff36f4=上一个包的ACK字段），确认了服务器发来的0号包，标识字段ACK为1，第三次握手表明连接的确立。

流程文字描述：

在 TCP/IP 协议中，TCP 协议提供可靠的连接服务，采用三次握手建立一个连接。 第一次握手： 建立连接时， 客户端发送 syn 包(syn=j)到服务器， 并进入 SYN\_SEND 状态，等待服务器确认； 第二次握手：服务器收到 syn 包，必须确认客户的 SYN（ack=j+1），同时自己 也发送一个 SYN 包（syn=k），即 SYN+ACK 包，此时服务器进入 SYN\_RECV 状态； 第三次握手：客户端收到服务器的 SYN＋ACK 包，向服务器发送确认包 ACK(ack=k+1)，此包发送完毕，客户端和服务器进入 ESTABLISHED 状态，完成三 次握手。 完成三次握手，客户端与服务器开始传送数据。

建立连接序列图为：

Seq=0 ,win=8192(第一次握手)

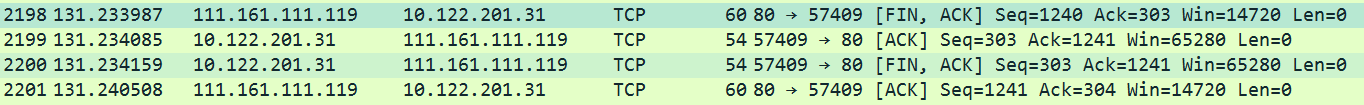
**接收方**

Seq=0 ack=1 win=13600（第二次握手）

**发送方**

Seq=1 ack=1 win=66560（第三次握手）

TCP释放连接的4次挥手和定时器：



1. 第一次挥手

服务器发向客户端，相对序号为seq=1240，相对ACK序号303，FIN置1，表明请求释放连接，WIN=14720。

1. 第二次挥手

相对序号seq=303，ACK为1241（1240+1），标志位ACK=1，同意释放连接，Win=65280。此时TCP协议在单方向（服务器至客户端）的连接已经关闭，即服务器不给客户端发消息，但可以接受客户端的消息。

1. 第三次挥手

客户端发给服务器，相对序号seq=303，与上次一样，因为服务器不可能主动给客户端发送消息了。ACK位置1，相对ACK序号位=1241。FIN位为1，表示客户端请求释放连接。Win=65280。客户端第三次挥手完毕后等待服务器的确认。

1. 第四次挥手

服务器发送给客户端的确认消息。双方释放连接，seq=1241，ack=304。Win=14720。

若一开始是客户端主动释放的连接，最后第四次握手是客户端发送给服务器的确认消息，那么此时服务器立即释放连接，客户端等待两倍数据包最长生存周期，再释放连接。

释放连接序列图为：

[FIN,ACK] Seq=1240 Ack=303 win=14720

(第一次挥手)

**接收方**

[ACK]Seq=303 Ack=1241 win=65280

(第二次握手)

**发送方**

[FIN,ACK]Seq=303 Ack=1241 win=65280

(第三次握手)

[ACK]Seq=1241 Ack=304 win=14720

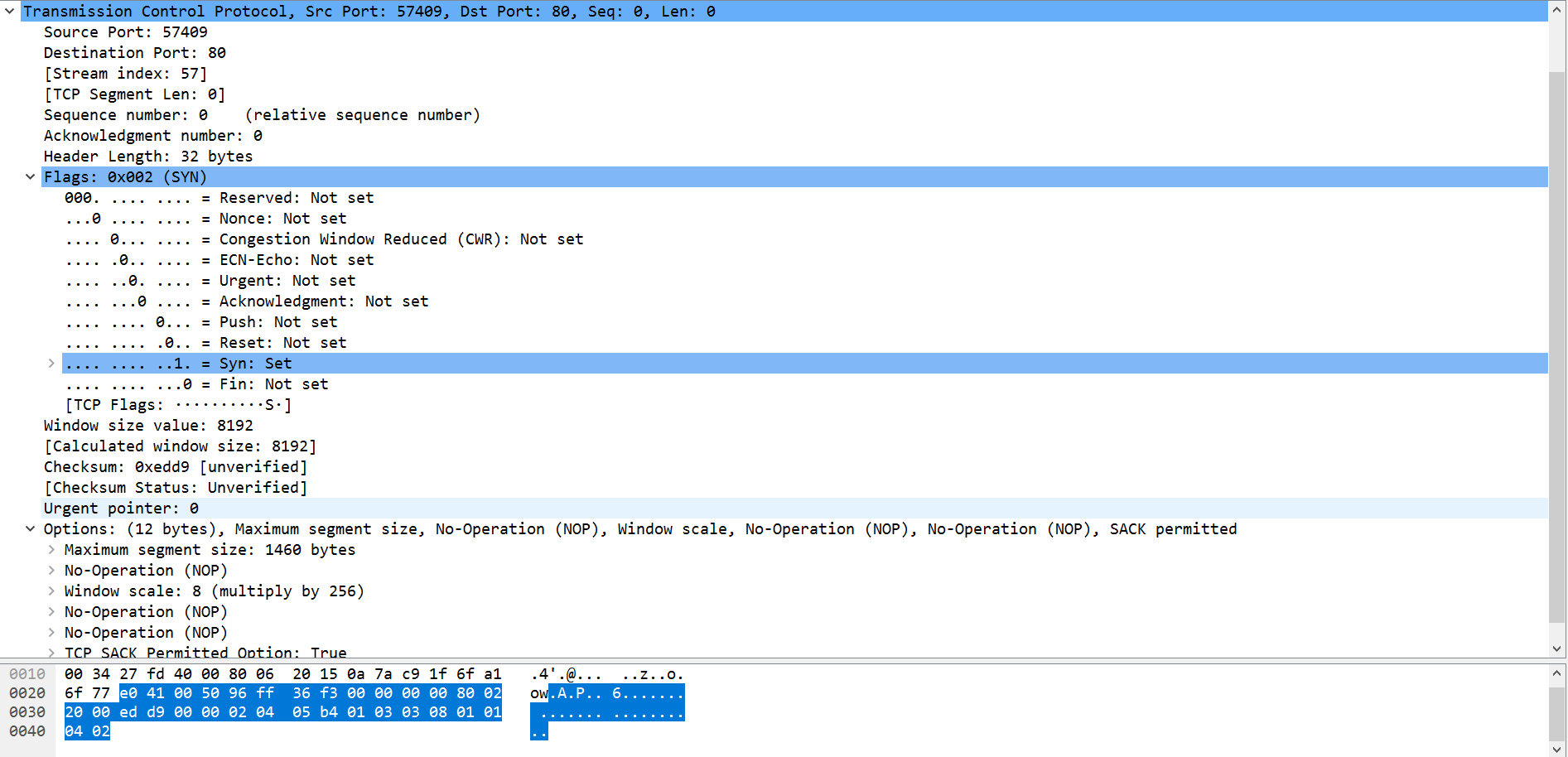
(第四次握手)

### 数据传输过程的消息序列图

TCP的传输策略：

基于确认和可变窗口大小；

窗口大小为0时，正常情况下，发送方不能再发送TCP段。



窗口大小：

TCP的流量控制由连接的每一端通过声明窗口的大小来提供。窗口大小字段用来控制对方发送的数据量，单位为字节。窗口大小用数据包来表示，Windows size=8, 表示一次可以发送八个数据包。窗口大小起始于确认字段指明的值，是一个16bits字段。窗口大小可以调节。窗口大小有一个调节因子，一般在建立连接的时候协商确定。

客户端窗口Window Scale = 8,乘积因子256

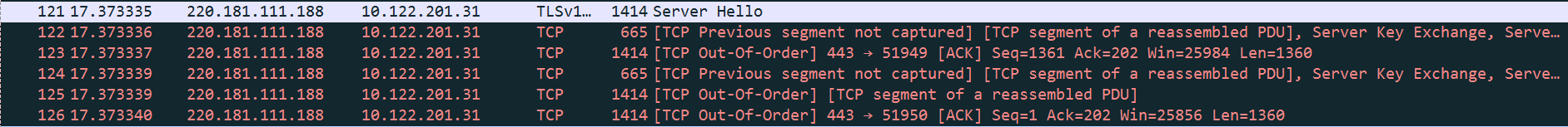
服务器窗口Window Scale = 7，乘积因子128。

数据长度与MSS：

用于标识该报文段中的数据长度。MSS指明本端所能够接收的最大长度的报文段。当一个TCP连接建立时，连接的双方都要通告各自的MSS协商可以传输的最大报文长度。我们常见的MSS如以太网可达1460字节。

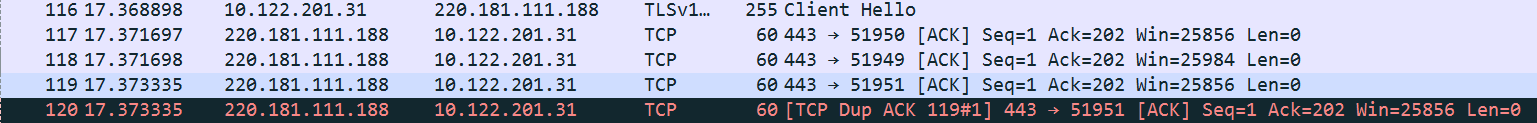
本次实验，MSS为1460字节。

乱序到达情况：



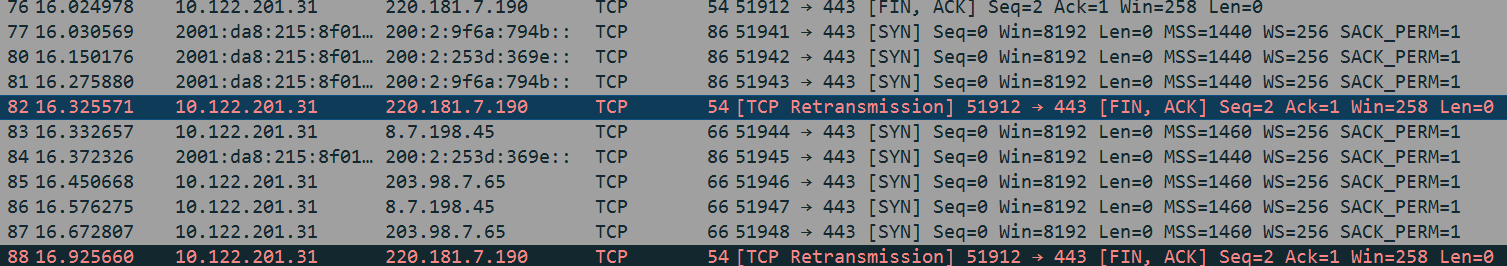
带有[out-of-order]标签的都是此前未按序到达的包。

ACK重传：



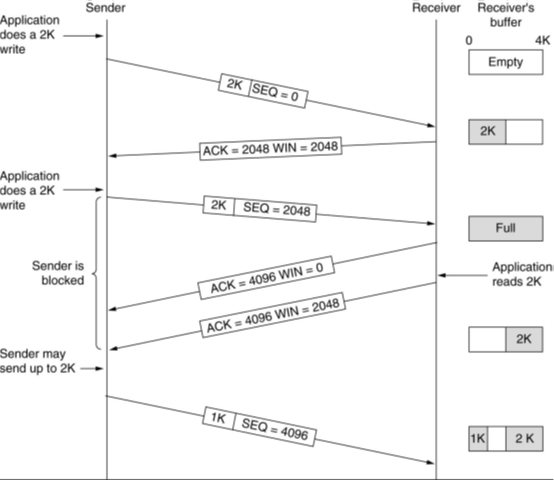
TCP规定，连续收到三次个重复的ACK重传包就要立刻重传，所以服务器在收到117，118，119三个重复的ACK后，快重传了120号包（带有[Dup ACK]）。

重传：



[Retransmission]网络较好情况下，重传多由于不正常释放连接导致，比如客户端强行关闭了程序，导致服务器没有收到ACK而不断超时重传.

数据传输策略时序图：



# 实验总结和实验心得

## 实验总结

本次协议数据的捕获和解析实验二共计花费大约16小时时间，主要在实验期间对网际层各个协议数据包的字段分析，深入理解其中含义。虽然课堂上已经对这些协议已经有了初步了解，但对IP 包头校验和的计算、TCP 的MSS 概念、ICMP 的消息格式、ARP 的消息格式、DHCP 的消息格式及操作过程这一系列的知识还是太不熟悉。此次实验的困难在于一边查询有关资料获得相关参考一边对使用wireshark软件所获得的包进行对应与分析，结合讲义与计算机网络教材。刚开始时还是略显生疏，但在慢慢了解记忆中，已经能够理清思路。并对所学协议内容进行概括总结，还有一些细节问题，如IP的效验、ICMP的效验、TCP的效验的差别，校验和的反码加法算法等，还有各个字段所使用的单位，IP包首部长度以字节为单位，IP分段偏移量以8字节为单位，TCP偏移量以4字节为单位。

实验过程中，对wireshark的上手也是个小考验，但是这并不需要很久，了解窗口输出的信息代表什么，再了解输入过滤器部件，就能对此有较好的掌握，wireshark也算是一个易用高效的软件呢。

## 实验心得

实验过后，最大的收获就是知识的扩充，对IP协议、ICMP、ARP、DHCP、TCP协议都有更为直观的理解，在抓包的乐趣中获得知识，何乐不为。学习到计算机之间，的通信过程，对三次握手，TCP的建立与释放过程的思想也有一些新的体会，很好的完成了实验预期的目的。当然还值得一说的是，耐心，不要因为大量的英文或者长篇大论而气馁，自有柳暗花明之处。