[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. 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。

2. 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
```

3. 实验步骤

i. 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。

ii. 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。

iii. 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。

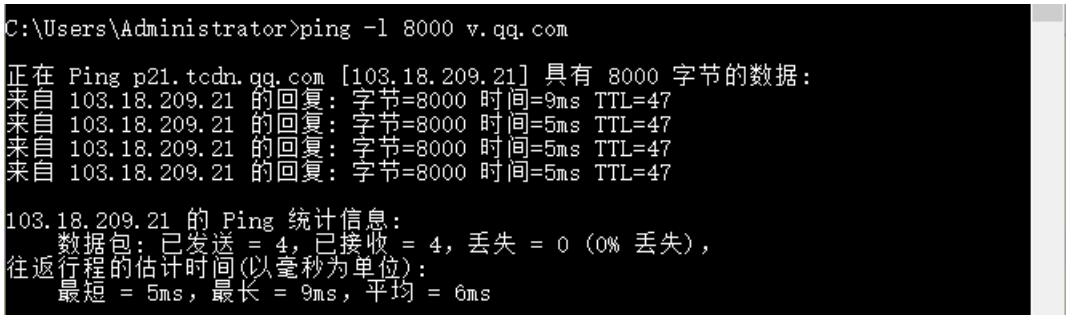
iv. 撰写实验报告

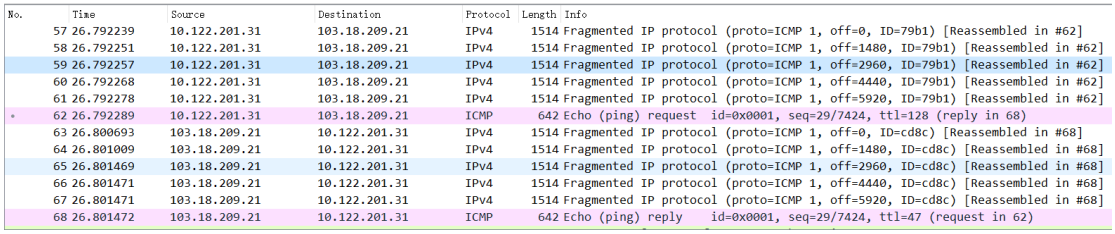
按要求撰写实验报告,对于捕获到的数据进行认真分析,归纳各协议的工作原理和实现要点。

二、 若干协议分析

1. IP 协议分析

使用 ping -l 8000 v.qq.com 命令捕获 IP 包消息



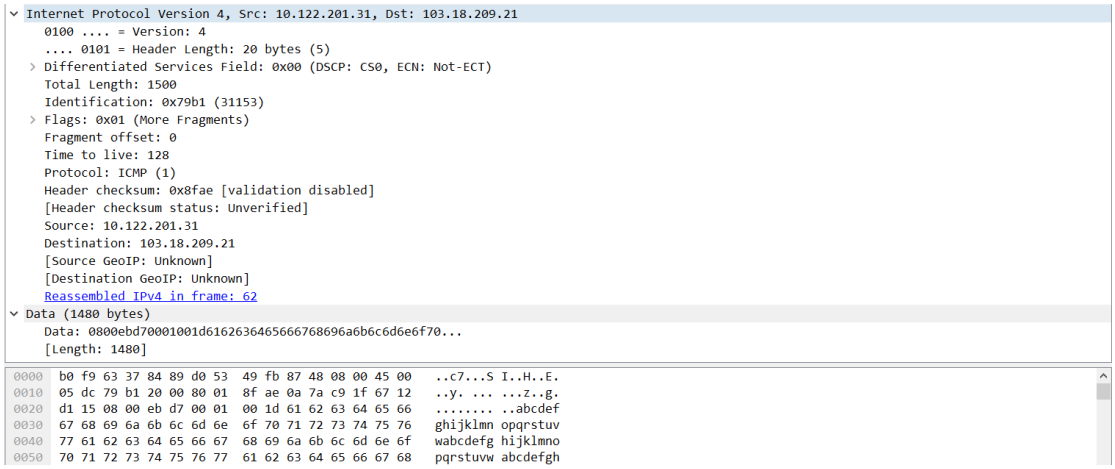


No.	Time	Source	Destination	Protocol	Length	Info
57	26.792239	10.122.201.31	103.18.209.21	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=79b1) [Reassembled in #62]
58	26.792251	10.122.201.31	103.18.209.21	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=79b1) [Reassembled in #62]
59	26.792257	10.122.201.31	103.18.209.21	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=79b1) [Reassembled in #62]
60	26.792268	10.122.201.31	103.18.209.21	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=79b1) [Reassembled in #62]
61	26.792278	10.122.201.31	103.18.209.21	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=79b1) [Reassembled in #62]
62	26.792289	10.122.201.31	103.18.209.21	ICMP	642	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (reply in 68)
63	26.800693	103.18.209.21	10.122.201.31	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cd8c) [Reassembled in #68]
64	26.801009	103.18.209.21	10.122.201.31	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=cd8c) [Reassembled in #68]
65	26.801469	103.18.209.21	10.122.201.31	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=cd8c) [Reassembled in #68]
66	26.801471	103.18.209.21	10.122.201.31	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=cd8c) [Reassembled in #68]
67	26.801471	103.18.209.21	10.122.201.31	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=cd8c) [Reassembled in #68]
68	26.801472	103.18.209.21	10.122.201.31	ICMP	642	Echo (ping) reply id=0x0001, seq=29/7424, ttl=47 (request in 62)

对序号 seq 为 57~61 号的 IPv4,及 62 号 ICMP 进行分析

i. 实验中 IP 包头各字段

分组 57 号信息截图如下



```
Internet Protocol Version 4, Src: 10.122.201.31, Dst: 103.18.209.21
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x79b1 (31153)
  > Flags: 0x01 (More Fragments)
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x8fae [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.122.201.31
    Destination: 103.18.209.21
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 62
Data (1480 bytes)
    Data: 0800ebd70001001d6162636465666768696a6b6c6d6e6f70...
    [Length: 1480]
```

```
0000  b0 f9 63 37 84 89 d0 53  49 fb 87 48 08 00 45 00   ..c7...S I..H..E.
0010  05 dc 79 b1 20 00 80 01  8f ae 0a 7a c9 1f 67 12   ..y. ... ...z..g.
0020  d1 15 08 00 eb d7 00 01  00 1d 61 62 63 64 65 66   ........ ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69 6a 6b 6c 6d 6e 6f   wabcdefg hijklmno
0050  70 71 72 73 74 75 76 77  61 62 63 64 65 66 67 68   pqrstuvw abcdefgh
```

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

ii. IP 包头校验和的校验原理，校验和实验验证

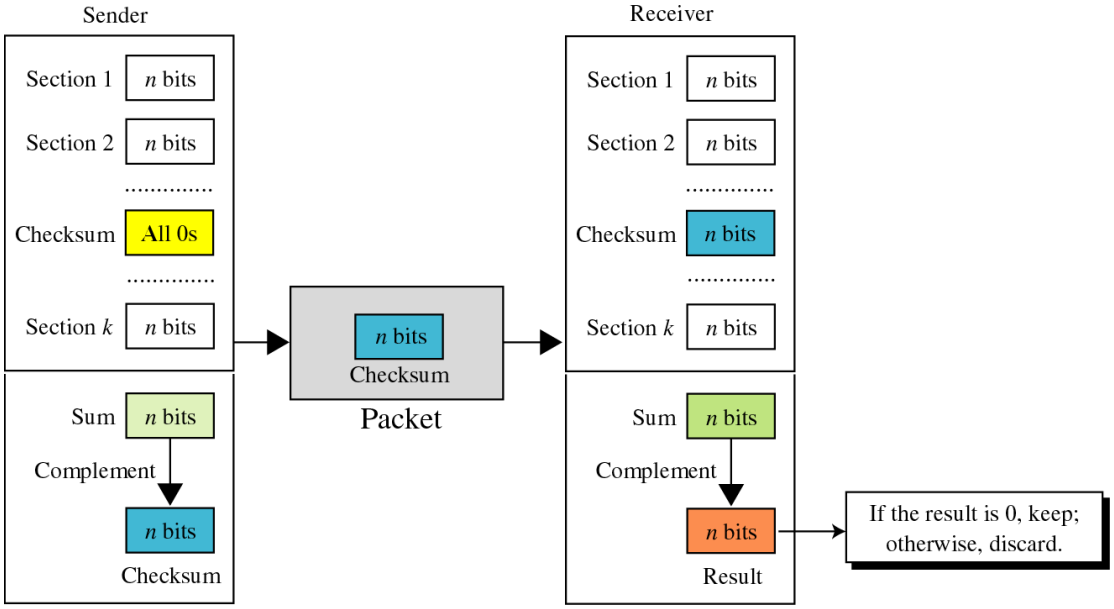
Checksum(校验和/检验和) Concept(RFC 1071)，原理：

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。

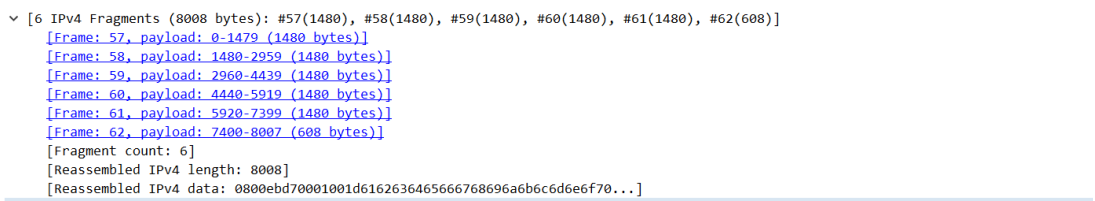
iii. IP 包分段原理，实验验证。

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

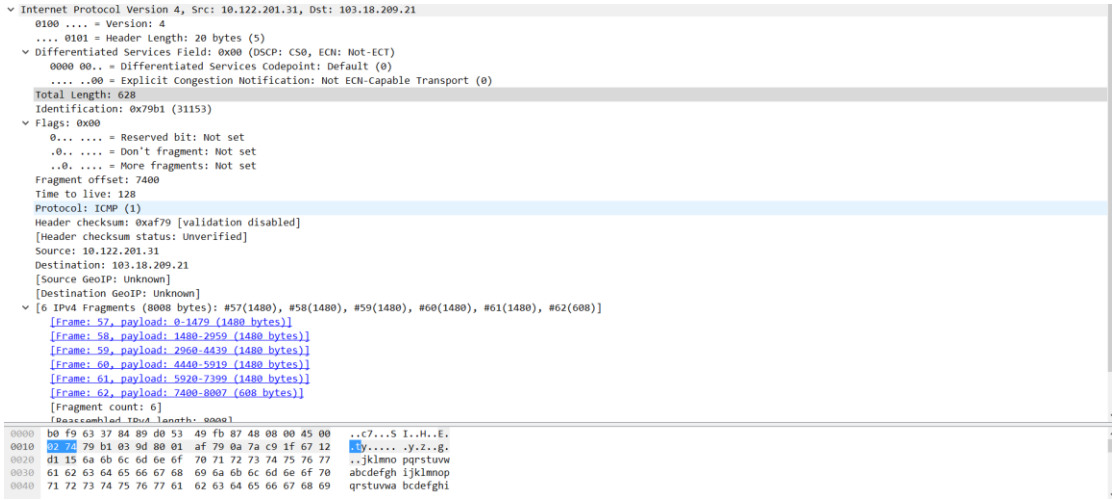
分组 60 号信息如下:

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:

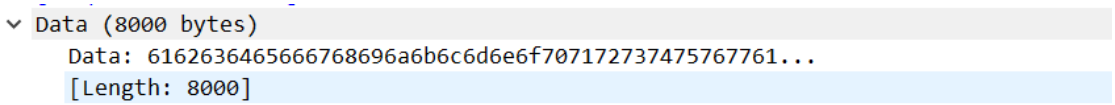
字 段	报 文(16进制)	内 容
包头长度	45	IPV4,包头长20字节,(20=5*4)
服务类型	00	正常时延，正常吞吐量，正常可靠性
总长度	05dc	数组分组长1500字节（首部加数据）
标识	79b1	标识为31153
标志	001(二进制)	DF=0，MF=1允许分片，后面还有分片
片偏移	02 e4	偏移量为740,即740*8=5920字节
生存周期	80	TTL=128,生存时间128跳
协议	01	携带数据来自ICMP协议
头部校验和	8cca	IP头部校验和为8cca
源地址	0a 7a c9 1f	源地址为10.122.201.31
目的地址	67 12 d1 15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



2. ICMP 协议分析

i. 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）

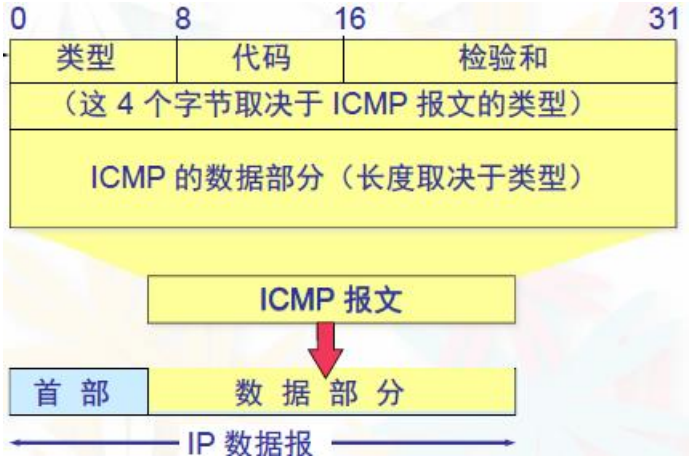
ICMP 询问报文有四种：

- 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。

ii. 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。

类型	代码	描述
8	0	回显请求
10	0	路由器请求
13	0	时间戳请求
15	0	信息请求（废弃不用）
17	0	地址掩码请求

ICMP 的回答报文有以下 5 种：

类型	代码	描述
0	0	回显回答
9	0	路由器回答
14	0	时间戳回答
16	0	信息回答（废弃不用）
18	0	地址掩码回答

实验内容，ping www.baidu.com 分析：

```
C:\Users\Administrator>ping www.baidu.com

正在 Ping www.a.shifen.com [220.181.111.188] 具有 32 字节的数据:
来自 220.181.111.188 的回复: 字节=32 时间=3ms TTL=49
来自 220.181.111.188 的回复: 字节=32 时间=3ms TTL=49
来自 220.181.111.188 的回复: 字节=32 时间=3ms TTL=49
来自 220.181.111.188 的回复: 字节=32 时间=3ms TTL=49

220.181.111.188 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 = 3ms, 最长 = 3ms, 平均 = 3ms
```

icmp 表达式…

No.	Time	Source	Destination	Protocol	Length	Info
596	24.286302	10.122.201.31	220.181.111.188	ICMP	74	Echo (ping) request id=0x0001, seq=37/9472, ttl…
597	24.289254	220.181.111.188	10.122.201.31	ICMP	74	Echo (ping) reply id=0x0001, seq=37/9472, ttl…
601	25.288906	10.122.201.31	220.181.111.188	ICMP	74	Echo (ping) request id=0x0001, seq=38/9728, ttl…
602	25.291809	220.181.111.188	10.122.201.31	ICMP	74	Echo (ping) reply id=0x0001, seq=38/9728, ttl…
607	26.294302	10.122.201.31	220.181.111.188	ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl…
608	26.297142	220.181.111.188	10.122.201.31	ICMP	74	Echo (ping) reply id=0x0001, seq=39/9984, ttl…
619	27.300411	10.122.201.31	220.181.111.188	ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, tt…
620	27.303357	220.181.111.188	10.122.201.31	ICMP	74	Echo (ping) reply id=0x0001, seq=40/10240, tt…

选取第一个序号为 596 的 ICMP 包分析：

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d36 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 37 (0x0025)
    Sequence number (LE): 9472 (0x2500)
    [Response frame: 597]
  Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
      [Length: 32]
```

```
0000  b0 f9 63 37 84 89 d0 53  49 fb 87 48 08 00 45 00   ..c7...S I..H..E.
0010  00 3c 5a 59 00 00 80 01  c0 5c 0a 7a c9 1f dc b5   .<ZY.... .\.z....
0020  6f bc 08 00 4d 36 00 01  00 25 61 62 63 64 65 66   o...M6.. .%abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

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

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5536 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 37 (0x0025)
    Sequence number (LE): 9472 (0x2500)
    [Request frame: 596]
    [Response time: 2.952 ms]
  Data (32 bytes)
      Data: 61626364656667686 96a6b6c6d6e6f707172737475767761...
      [Length: 32]
```

```
0000  d0 53 49 fb 87 48 b0 f9  63 37 84 89 08 00 45 00   .SI..H.. c7....E.
0010  00 3c 5a 59 00 00 31 01  0f 5d dc b5 6f bc 0a 7a   .<ZY..1. .]..o..z
0020  c9 1f 00 00 55 36 00 01  00 25 61 62 63 64 65 66   ....U6.. .%abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

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。

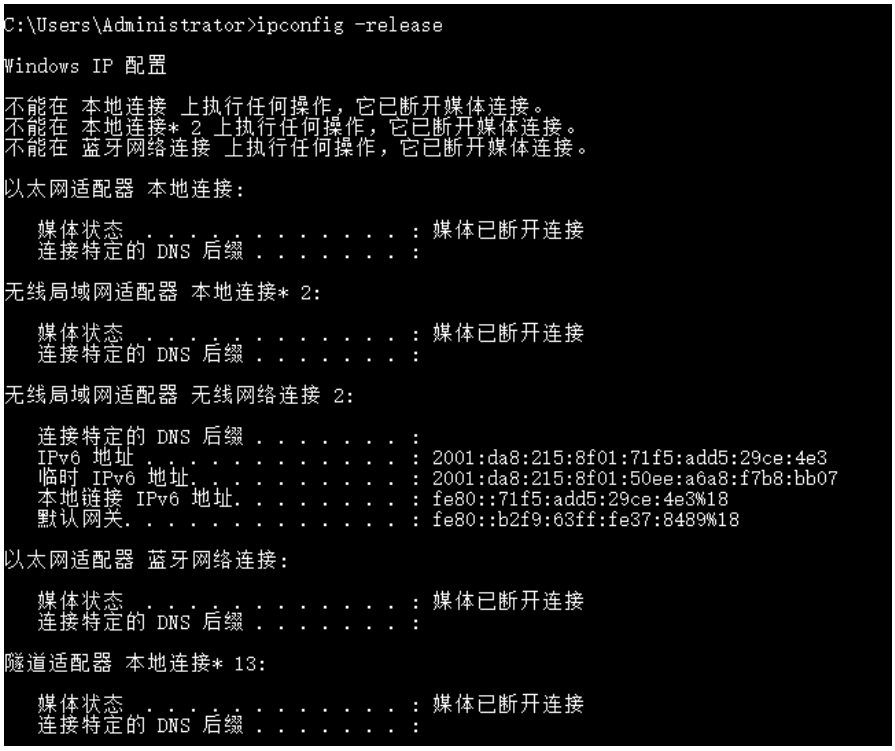
```
Info
Echo (ping) request  id=0x0001, seq=37/9472, ttl=128 (reply in 597)
Echo (ping) reply    id=0x0001, seq=37/9472, ttl=49 (request in 596)
Echo (ping) request  id=0x0001, seq=38/9728, ttl=128 (reply in 602)
Echo (ping) reply    id=0x0001, seq=38/9728, ttl=49 (request in 601)
Echo (ping) request  id=0x0001, seq=39/9984, ttl=128 (reply in 608)
Echo (ping) reply    id=0x0001, seq=39/9984, ttl=49 (request in 607)
Echo (ping) request  id=0x0001, seq=40/10240, ttl=128 (reply in 620)
Echo (ping) reply    id=0x0001, seq=40/10240, ttl=49 (request in 619)
```

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。

3. DHCP 协议分析

准备阶段：

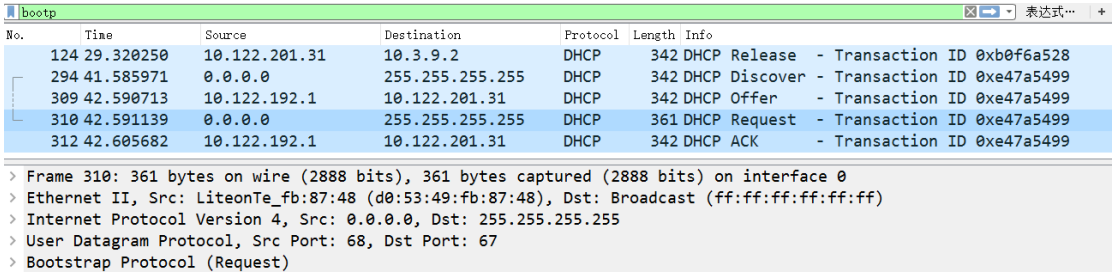
使用 ipconfig 命令释放计算机的 IP 地址（c>ipconfig -release）



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

```
C:\Users\Administrator>ipconfig -renew

Windows IP 配置

不能在 本地连接 上执行任何操作，它已断开媒体连接。
不能在 本地连接* 2 上执行任何操作，它已断开媒体连接。
不能在 蓝牙网络连接 上执行任何操作，它已断开媒体连接。

以太网适配器 本地连接:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 本地连接* 2:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

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
   IPv6 地址 . . . . . . . . . . . . : 2001:da8:215:8f01:71f5:add5:29ce:4e3
   临时 IPv6 地址. . . . . . . . . . : 2001:da8:215:8f01:50ee:a6a8:f7b8:bb07
   本地链接 IPv6 地址. . . . . . . . : fe80::71f5:add5:29ce:4e3%18
   IPv4 地址 . . . . . . . . . . . . : 10.122.201.31
   子网掩码  . . . . . . . . . . . . : 255.255.192.0
   默认网关. . . . . . . . . . . . . : fe80::b2f9:63ff:fe37:8489%18
                                       10.122.192.1

以太网适配器 蓝牙网络连接:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

隧道适配器 isatap.bupt.edu.cn:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . : bupt.edu.cn

隧道适配器 本地连接* 13:

   连接特定的 DNS 后缀 . . . . . . . :
   IPv6 地址 . . . . . . . . . . . . : 2001:0:9d38:6ab8:2879:5994:8d00:d7df
   本地链接 IPv6 地址. . . . . . . . : fe80::2879:5994:8d00:d7df%6
   默认网关. . . . . . . . . . . . . :
```

在 wireshark 中捕获 DHCP 包



i. 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：

```
> Frame 312: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: LiteonTe_fb:87:48 (d0:53:49:fb:87:48)
> Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.201.31
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Bootstrap Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe47a5499
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.122.201.31
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.122.192.1
    Client MAC address: LiteonTe_fb:87:48 (d0:53:49:fb:87:48)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (54) DHCP Server Identifier
  > Option: (51) IP Address Lease Time
  > Option: (1) Subnet Mask
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (255) End
```

```
0020  c9 1f 00 43 00 44 01 34  f4 d6 02 01 06 00 e4 7a   ...C.D.4 .......z
0030  54 99 00 00 00 00 00 00  00 00 0a 7a c9 1f 00 00   T....... ...z....
0040  00 00 0a 7a c0 01 d0 53  49 fb 87 48 00 00 00 00   ...z...S I..H....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

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	060c0a0309040a03090 50a030906	长度：12 10.3.9.4/10.3.9.5/10.3.9.6
Domain Name	0f0b627570742e65647 52e636e	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：

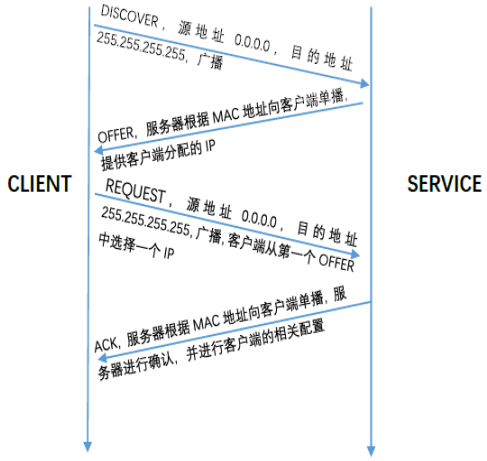
```
Option: (55) Parameter Request List
    Length: 13
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (31) Perform Router Discover
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (43) Vendor-Specific Information
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (252) Private/Proxy autodiscovery
```

在 DHCP ACK 中，服务器回应客户端以提供的字段：

```
Option: (53) DHCP Message Type (ACK)
Option: (54) DHCP Server Identifier
Option: (51) IP Address Lease Time
Option: (1) Subnet Mask
Option: (3) Router
Option: (6) Domain Name Server
Option: (15) Domain Name
Option: (255) End
Padding: 0000000000
```

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。

ii. 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。

2） 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)

3） 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。

```
Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: LiteonTe_fb:87:48 (d0:53:49:fb:87:48)
Option: (50) Requested IP Address
    Length: 4
    Requested IP Address: 10.122.201.31
Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 10.3.9.2
```

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。

```
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:da8:215:8f01:50ee:a6a8:f7b8:bb07(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17日 21:44:28
   租约过期的时间  . . . . . . . . . : 2017年6月18日 0:14:26
   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
```

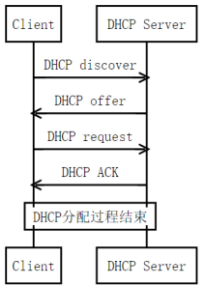
4） DHCP ACK

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。

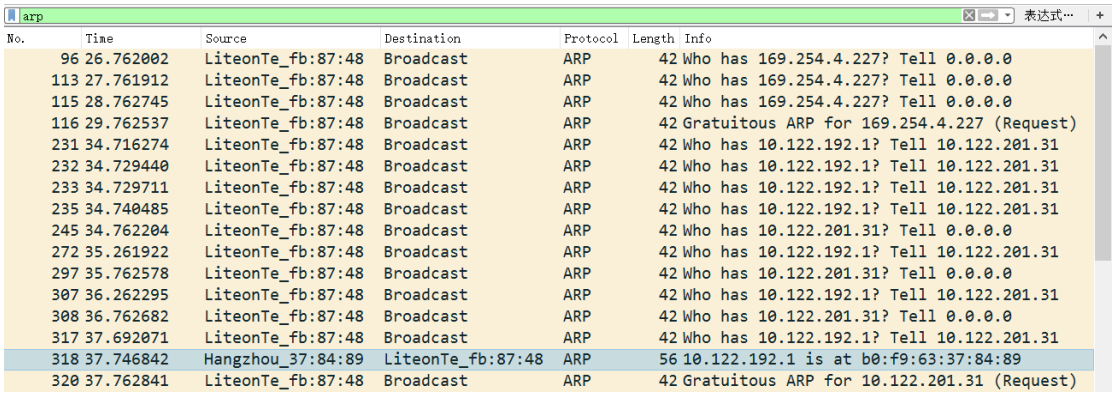
4.本地主机收到 DHCP offer 报文后，向 DHCP 服务器发送 DHCP request 报文。

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。

4. ARP 协议分析

i. ARP 功能与操作原理

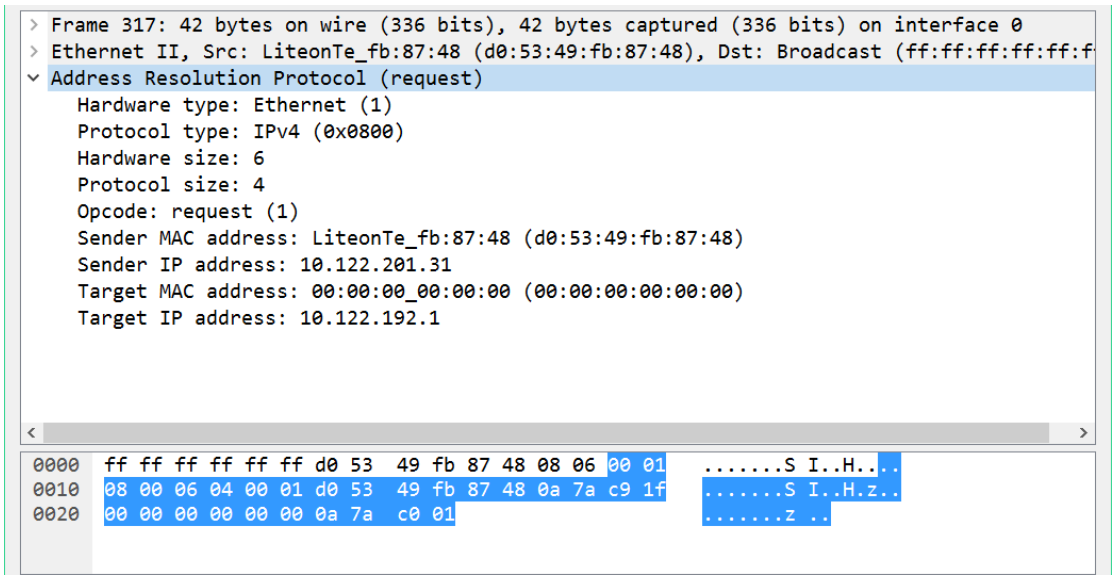
使用 ipconfig 命令释放计算机的 IP 地址（c>ipconfig -release）
使用 ipconfig 命令重新申请 IP 地址（c>ipconfig -renew）
设置过滤器 ARP,wireshark 中显现：



arp 表达式…

No.	Time	Source	Destination	Protocol	Length	Info
96	26.762002	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 169.254.4.227? Tell 0.0.0.0
113	27.761912	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 169.254.4.227? Tell 0.0.0.0
115	28.762745	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 169.254.4.227? Tell 0.0.0.0
116	29.762537	LiteonTe_fb:87:48	Broadcast	ARP	42	Gratuitous ARP for 169.254.4.227 (Request)
231	34.716274	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 10.122.192.1? Tell 10.122.201.31
232	34.729440	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 10.122.192.1? Tell 10.122.201.31
233	34.729711	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 10.122.192.1? Tell 10.122.201.31
235	34.740485	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 10.122.192.1? Tell 10.122.201.31
245	34.762204	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 10.122.201.31? Tell 0.0.0.0
272	35.261922	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 10.122.192.1? Tell 10.122.201.31
297	35.762578	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 10.122.201.31? Tell 0.0.0.0
307	36.262295	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 10.122.192.1? Tell 10.122.201.31
308	36.762682	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 10.122.201.31? Tell 0.0.0.0
317	37.692071	LiteonTe_fb:87:48	Broadcast	ARP	42	Who has 10.122.192.1? Tell 10.122.201.31
318	37.746842	Hangzhou_37:84:89	LiteonTe_fb:87:48	ARP	56	10.122.192.1 is at b0:f9:63:37:84:89
320	37.762841	LiteonTe_fb:87:48	Broadcast	ARP	42	Gratuitous ARP for 10.122.201.31 (Request)

request 包：



```
> Frame 317: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: LiteonTe_fb:87:48 (d0:53:49:fb:87:48), Dst: Broadcast (ff:ff:ff:ff:ff:f
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: LiteonTe_fb:87:48 (d0:53:49:fb:87:48)
    Sender IP address: 10.122.201.31
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.122.192.1
```

```
0000  ff ff ff ff ff ff d0 53  49 fb 87 48 08 06 00 01   .......S I..H....
0010  08 00 06 04 00 01 d0 53  49 fb 87 48 0a 7a c9 1f   .......S I..H.z..
0020  00 00 00 00 00 00 0a 7a  c0 01                     .......z ..
```

Reply 包：

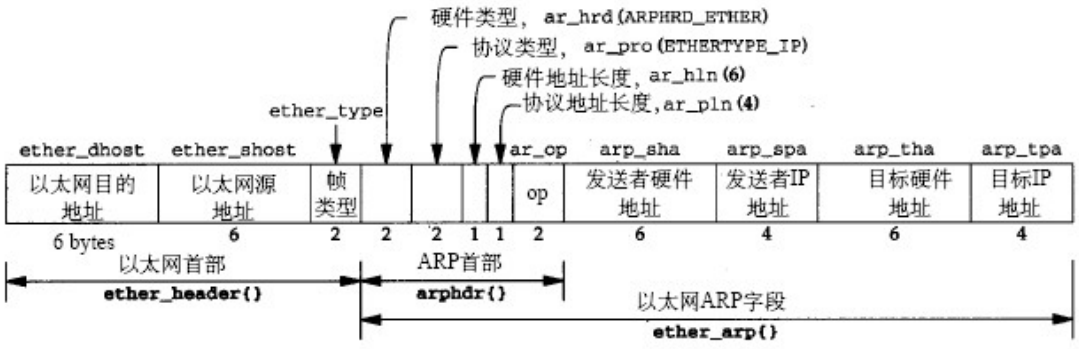
```
> Frame 318: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
> Ethernet II, Src: Hangzhou_37:84:89 (b0:f9:63:37:84:89), Dst: LiteonTe_fb:87:48 (d0:53:49
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Hangzhou_37:84:89 (b0:f9:63:37:84:89)
    Sender IP address: 10.122.192.1
    Target MAC address: LiteonTe_fb:87:48 (d0:53:49:fb:87:48)
    Target IP address: 10.122.201.31

0000  d0 53 49 fb 87 48 b0 f9  63 37 84 89 08 06 00 01   .SI..H.. c7......
0010  08 00 06 04 00 02 b0 f9  63 37 84 89 0a 7a c0 01   ........ c7...z..
0020  d0 53 49 fb 87 48 0a 7a  c9 1f 00 00 00 00 00 00   .SI..H.z ........
0030  00 00 00 00 00 00 00 00                           ........
```

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。

ii. 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

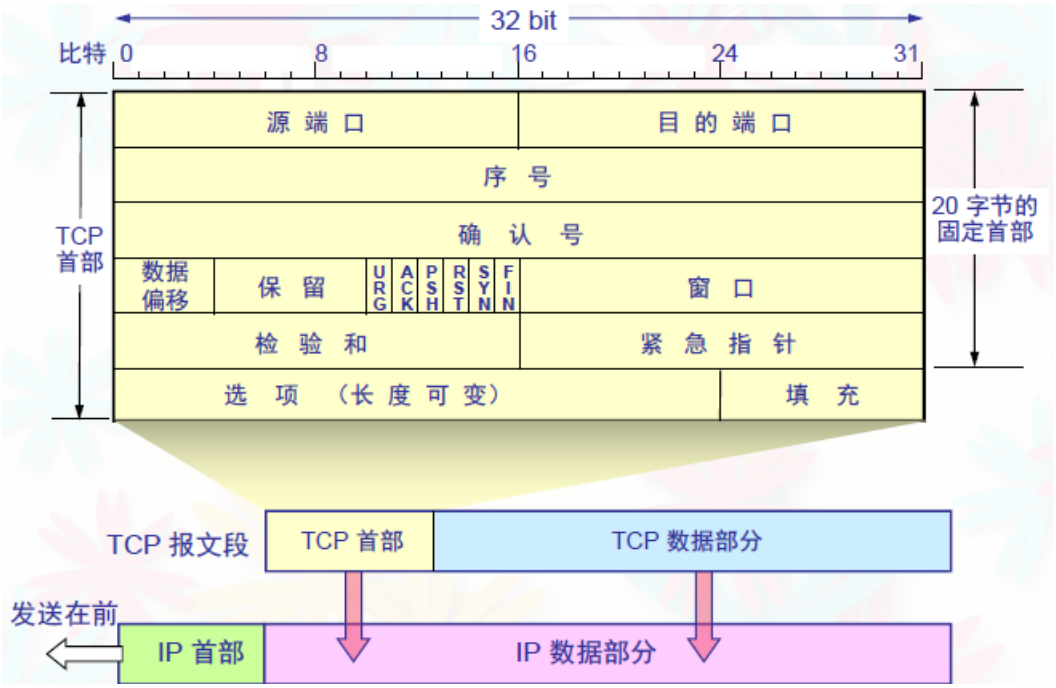
Opcode	0001(ARP请求) 0002(ARP响应) 0003(RARP请求) 0004(RARP响应)	操作码指明操作类型
Sender MAC address	D05349fb8748	发送方mac地址
Sender IP address	0a7ac91f	发送方IP 10.122.201.31
Target MAC address	000000000000	目标mac地址
Target IP address	0a7ac001	目标IP 10.122.192.1

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

5. TCP 协议分析

i. TCP 报文字段功能

TCP 报文格式：



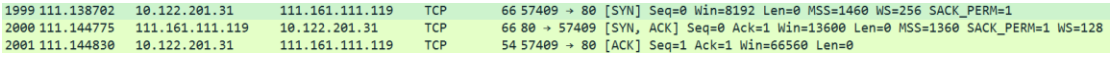
各字段功能：

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

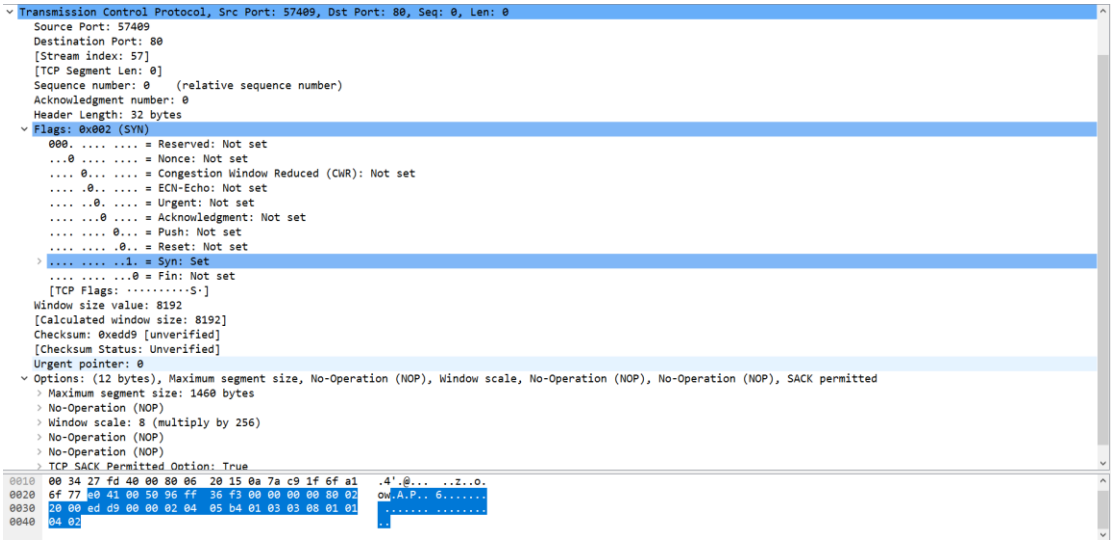
ii. 建立和连接释放过程的消息序列图

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：

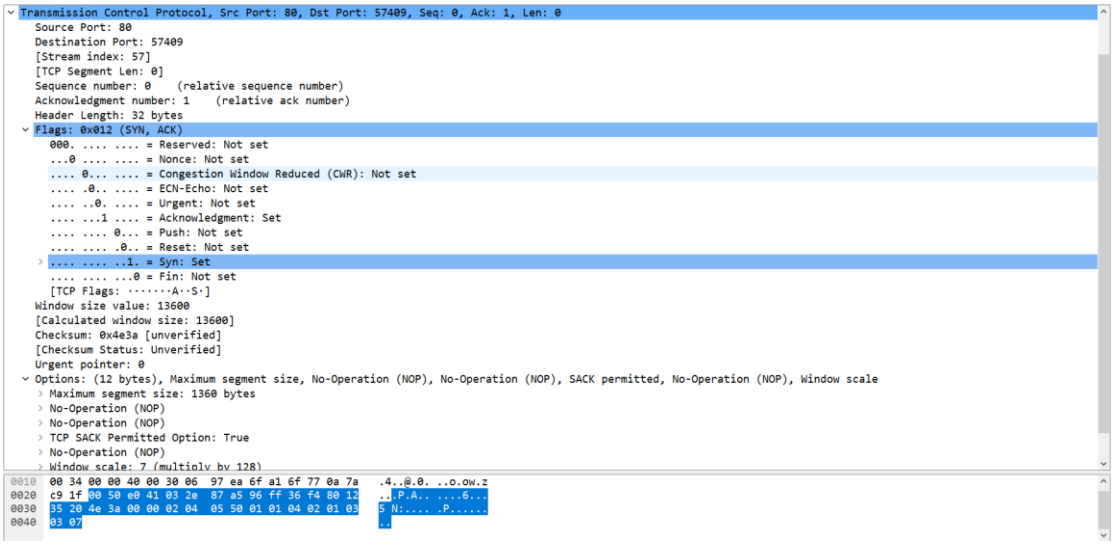
1） 第一次握手：



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

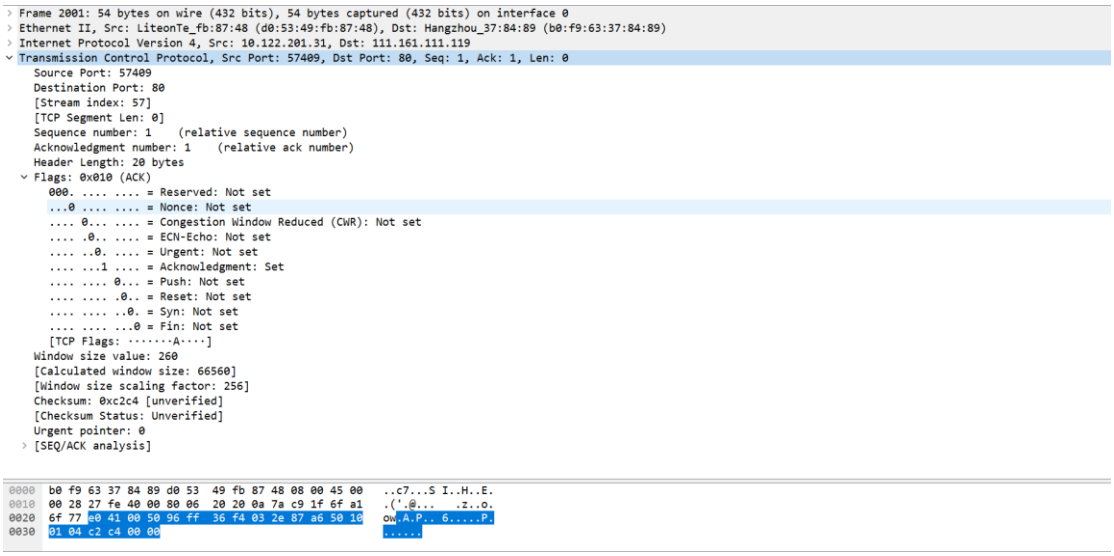
size 8192，校验和 0xedd9，状态表明还未经证实。

2） 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。

3） 第三次握手：

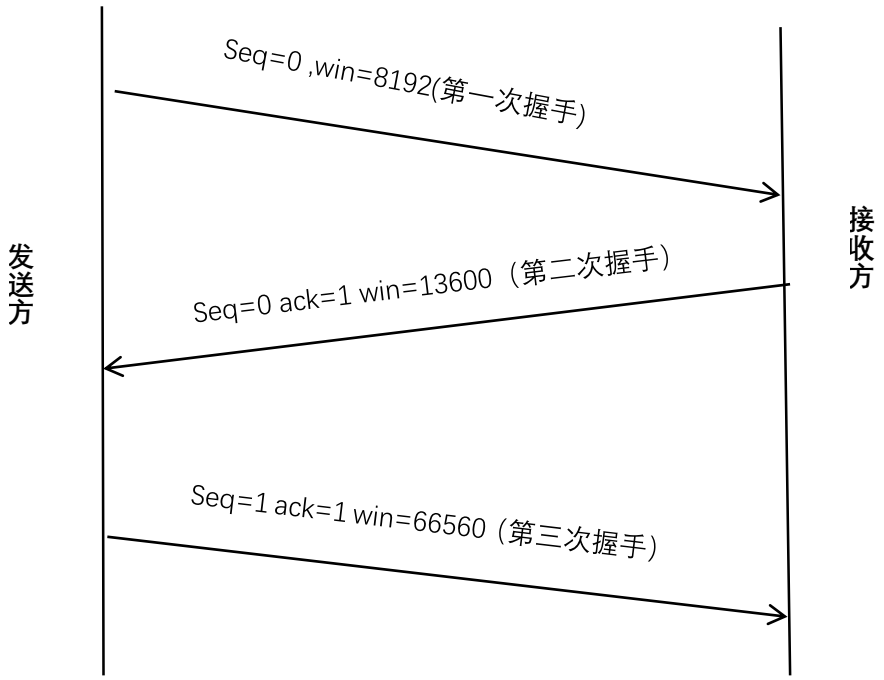


客户端发给服务器，序号 seq 增长为 1（96ff36f4=上一个包的 ACK 字段），确认了服务器发来的 0 号包，标识字段 ACK 为 1，第三次握手表明连接的确立。

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：



TCP 释放连接的 4 次挥手和定时器：

2198	131.233987	111.161.111.119	10.122.201.31	TCP	60 80 → 57409 [FIN, ACK] Seq=1240 Ack=303 Win=14720 Len=0
2199	131.234085	10.122.201.31	111.161.111.119	TCP	54 57409 → 80 [ACK] Seq=303 Ack=1241 Win=65280 Len=0
2200	131.234159	10.122.201.31	111.161.111.119	TCP	54 57409 → 80 [FIN, ACK] Seq=303 Ack=1241 Win=65280 Len=0
2201	131.240508	111.161.111.119	10.122.201.31	TCP	60 80 → 57409 [ACK] Seq=1241 Ack=304 Win=14720 Len=0

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。

2） 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。

3） 第三次挥手

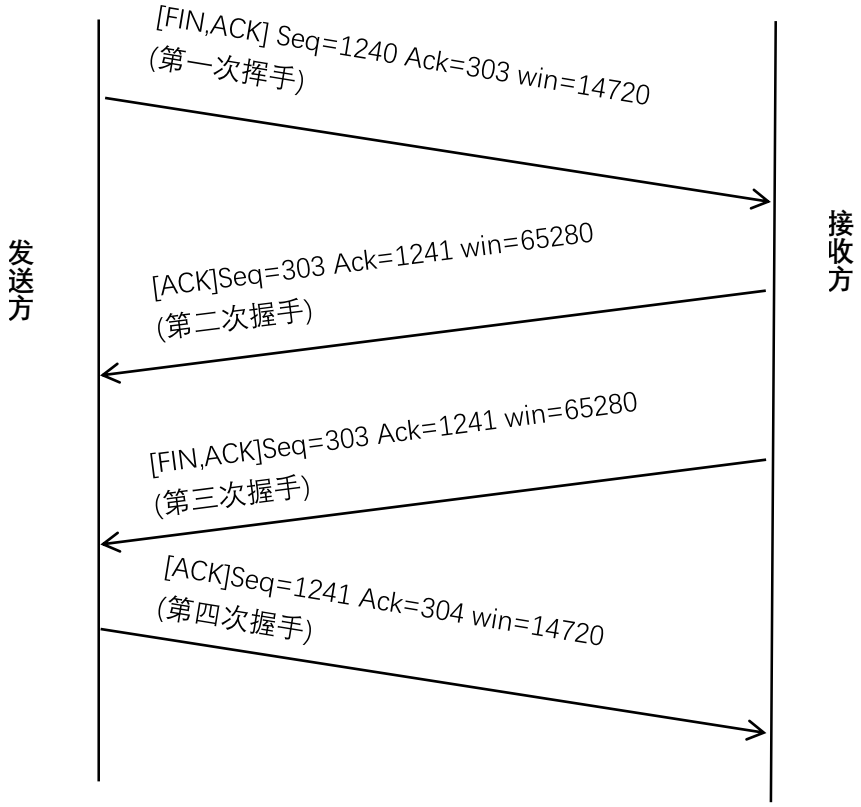
客户端发给服务器，相对序号 seq=303，与上次一样，因为服务器不可能主动给客户端发送消息了。ACK 位置 1，相对 ACK 序号位=1241。FIN 位为 1，表示客户端请求释放连接。Win=65280。客户端第三次挥手完毕后等待服务器的确认。

4） 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。

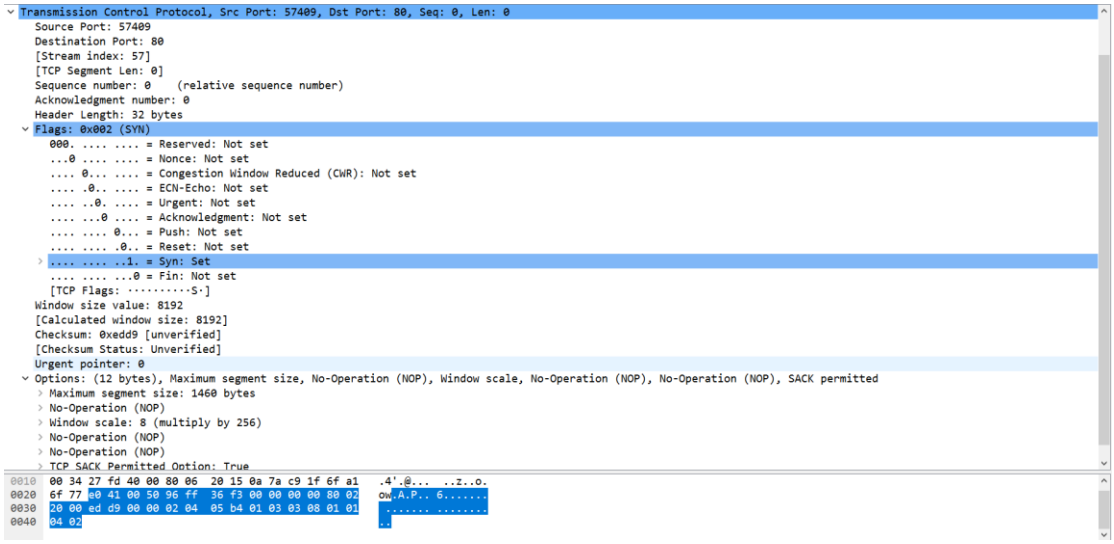
若一开始是客户端主动释放的连接，最后第四次握手是客户端发送给服务器的确认消息，那么此时服务器立即释放连接，客户端等待两倍数据包最长生存周期，再释放连接。

释放连接序列图为：



iii. 数据传输过程的消息序列图

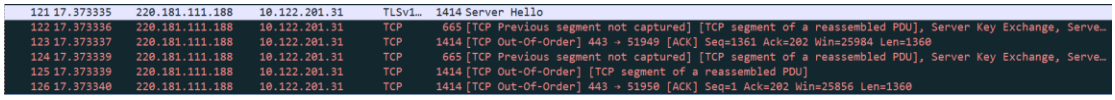
TCP 的传输策略：
基于确认和可变窗口大小；
窗口大小为 0 时，正常情况下，发送方不能再发送 TCP 段。



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。

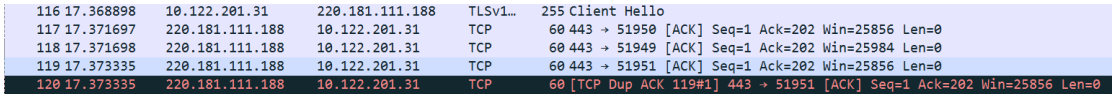
数据长度与 MSS：
用于标识该报文段中的数据长度。MSS 指明本端所能够接收的最大长度的报文段。当一个 TCP 连接建立时，连接的双方都要通告各自的 MSS 协商可以传输的最大报文长度。我们常见的 MSS 如以太网可达 1460 字节。
本次实验，MSS 为 1460 字节。

乱序到达情况：



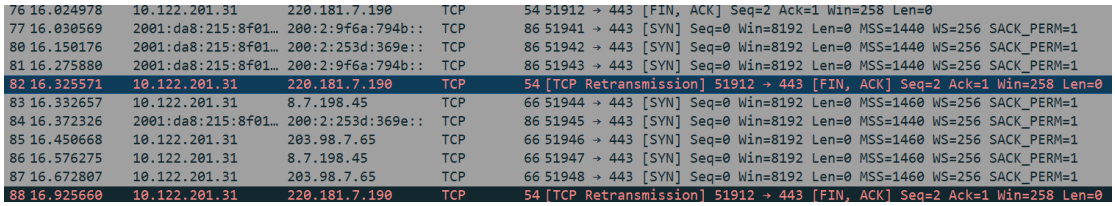
带有[out-of-order]标签的都是此前未按序到达的包。

ACK 重传：



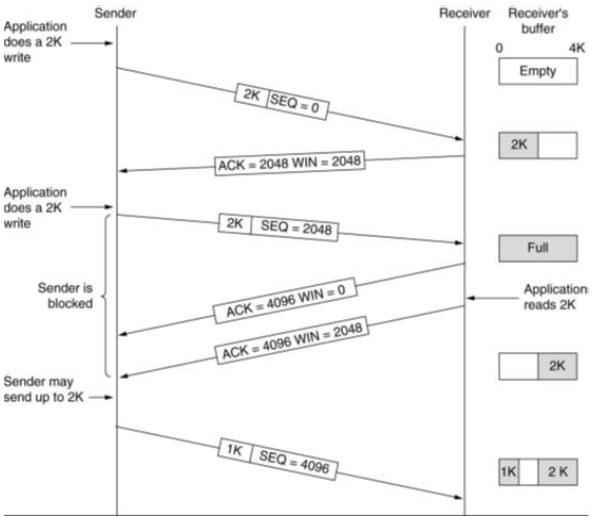
TCP 规定，连续收到三次个重复的 ACK 重传包就要立刻重传，所以服务器在收到 117，118，119 三个重复的 ACK 后，快重传了 120 号包（带有[Dup ACK]）。

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：



三、 实验总结和实验心得

1. 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。

2. 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。