

# 计算机网络实验二：网络层数据分组的捕获和解析 实验报告

毛子恒

2019211397

北京邮电大学 计算机学院

日期：2021 年 6 月 5 日

## 1 实验内容和实验环境描述

### 1.1 实验内容

本次实验内容：

1. 捕获在连接 Internet 过程中产生的网络层分组：DHCP 分组，ARP 分组，IP 数据分组，ICMP 分组。
2. 分析各种分组的格式，说明各种分组在建立网络连接过程中的作用。
3. 分析 IP 数据分组分片的结构。

通过本次实验了解计算机上网的工作过程，学习各种网络层分组的格式及其作用，理解长度大于 1500 字节 IP 数据组分片传输的结构。

### 1.2 实验环境

- Windows 10 version 1909
- Wireshark Version 3.4.4
- Visual Studio Code 1.56.2

## 2 实验步骤和网络层分组结构分析

### 2.1 准备工作

启动计算机，连接网络确保能够上网。断开连接，禁用网卡。

### 2.2 捕获和分析 DHCP 和 ARP 分组

#### 2.2.1 捕获 DHCP 分组

开启监控，连接网络。在 Wireshark 过滤器中输入 `dhcp`，过滤出四个 DHCP 分组如图 1。四个 DHCP 分组的内容如图 2。

2	0.011739	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover	- Transaction ID 0xe87552dd
34	1.018784	10.122.192.1	10.122.193.19	DHCP	342	DHCP Offer	- Transaction ID 0xe87552dd
35	1.019228	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request	- Transaction ID 0xe87552dd
37	1.047541	10.122.192.1	10.122.193.19	DHCP	342	DHCP ACK	- Transaction ID 0xe87552dd

```

Ethernet II, Src: IntelCon_71:25:14 (58:a0:23:71:25:14), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
  User Datagram Protocol, Src Port: 68, Dst Port: 67
  Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe87552dd
    Seconds elapsed: 0
    Bootp Flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCon_71:25:14 (58:a0:23:71:25:14)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
    Option: (61) Client Identifier
    Option: (12) Host Name
    Option: (60) Vendor class identifier
    Option: (55) Parameter Request List
    Option: (255) End
    Padding: 00000000

0000  ff ff ff ff ff ff 58 a0 23 71 25 14 00 00 45 00 .....X..qgk...E
0010  01 45 b4 27 00 00 00 00 00 00 00 00 00 00 ff ff ..H.....
0020  ff ff 00 44 00 43 01 34 01 f5 01 81 06 00 e8 75 .....D..C..4.....u
0030  52 dd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....R.....
0040  00 00 00 00 00 58 a0 23 71 25 14 00 00 00 00 00 .....X..qgk...
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 .....
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0100  00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 .....c.....
0110  00 00 00 00 00 00 63 82 53 43 53 40 51 3d 07 01 .....c..ScS....
0120  58 a0 23 71 25 14 0c 0f 44 65 53 4b 54 4f 50 2d X..qgk...DESKTOP-
0130  47 4b 42 46 52 35 3c 08 21 2b 2c 54 56 20 35 f9 GKRKRN<..MSFT 5-
0140  30 37 0e 01 03 06 0f 1f 01 2b 2c 2e 2f 77 79 2e ..e.../.../.../...
0150  fc ff ff 00 00 00 00

```

```

> Ethernet II, Src: RuijieLan_7d:fa:db (00:74:9c:7d:fa:db), Dst: IntelCor_71:25:14 (58:a0:23:71:25:14)
> Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.193.19
> User Datagram Protocol, Src Port: 67, Dst Port: 68
  Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0xe67552ad
    Seconds elapsed: 0
    > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.122.193.19
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.122.192.1
    Client MAC address: IntelCor_71:25:14 (58:a0:23:71:25:14)
    Client hardware address padding: 000000000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    > Option: (53) DHCP Message Type (Offer)
    > Option: (54) DHCP Server Identifier (10.3.9.2)
    > Option: (51) IP Address Lease Time
    > Option: (1) Subnet Mask (255.255.192.0)
    > Option: (3) Router
    > Option: (6) Domain Name Server
    > Option: (255) End

```

---

```

0000  58 a0 23 71 25 14 04 00 9c 7d fa db 08 00 45 00  X-#%-t-)-...E-
0010  01 48 37 41 00 00 40 11 ac 5b 0a 7a c0 01 0a 7a  -H-A-@-[...-z
0020  c1 13 03 04 00 44 01 34 e4 38 02 01 06 01 e8 75  C-D-4-8-...u
0030  52 d4 00 00 00 00 00 00 00 00 0a 7a c1 13 00 00  R-...-...-...
0040  00 0a 7a c0 01 58 ab 23 71 25 14 00 00 00 00 00  -Z-X-#%-...-
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  .....
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0110  00 00 00 00 00 63 82 53 63 35 01 02 36 04 0a 0a  ...C-5-6-...
0120  03 09 02 33 04 00 1c 20 01 04 ff ff c0 00 03  ....-3-...-...
0130  04 0a 7a c0 01 06 08 0a 03 09 2d 0a 03 09 2c ff  -Z-...-...-...
0140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

```

Frame 35: 370 bytes wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device
Ethernet II, Src: IntelCor_71:25:14 (58:a0:23:71:25:14), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xe87552dd
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: IntelCor_71:25:14 (58:a0:23:71:25:14)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Client file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Request)
  Option: (61) Client identifier
  Option: (50) Requested IP Address (10.122.193.19)
  Option: (54) DHCP Server Identifier (10.3.9.2)
  Option: (12) Host Name
  Option: (81) Client Fully Qualified Domain Name
  Option: (60) Vendor class identifier
  Option: (55) Parameter Request List
  Option: (255) End
0000  ff ff ff ff ff ff ff ff 58 a0 23 71 25 14 08 00 00 45 00 .....X-#q%-E-
0010  01 64 b4 28 00 00 80 11 00 00 00 00 00 00 ff ff .....d-(
0020  ff ff ff 00 44 00 43 01 50 59 de 01 01 06 00 e8 75 .....D-C-P-Y-u
0030  52 dd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....R-
0040  00 00 00 00 00 00 58 a0 23 71 25 14 00 00 00 00 .....X-#q%-
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 .....
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0110  00 00 00 00 00 00 63 82 53 63 35 01 03 3d 07 01 .....c-Sc5=-
0120  58 a0 23 71 25 14 52 34 0a 7a c1 13 36 0a 0a 03 X-#q%-2-z-6-
0130  09 02 0c 0f 44 45 43 46 54 4f 50 2d 47 4b 42 4b .....DESK TOP-GKBK
0140  52 4e 45 35 12 00 00 00 44 45 53 46 54 2f 50 2d RN5Q- DESKTOP-
0150  47 4b 32 4b 52 4e 35 3c 08 4d 53 46 54 2f 50 2e GKBKRN5C-MSFT 5.
0160  30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 07-...+.,/w/y-
0170  fc ff

```

```
> Frame 37: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on Interface {Device/NPF-C}
> Ethernet II, Src: Wi-Fi_Rule_7a:c:d0 (00:71:9c:7d:fa:d0), Dst: IntelCor_71:25:14 (58:a0:23:71:25:14)
> Internet Protocol Version 4, Src: 10.122.192.1, Dst: 10.122.193.19
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0xe87552dd
    Seconds elapsed: 0
    > Bootp flags: 0x0000 (Unicast)
        Client IP address: 0.0.0.0
        Your (client) IP address: 10.122.193.19
        Next server IP address: 0.0.0.0
        Relay agent IP address: 10.122.192.1
        Client MAC address: IntelCor_71:25:14 (58:a0:23:71:25:14)
        Client hardware address padding: 00000000000000000000000000000000
        Server host name not given
        Boot file name not given
        Magic cookie: DHCP
    > Option: (53) DHCP Message Type (ACK)
    > Option: (54) DHCP Server Identifier (10.3.9.2)
    > Option: (51) IP Address Lease Time
    > Option: (1) Subnet Mask (255.255.192.0)
    > Option: (3) Router
    > Option: (6) Domain Name Server
    > Option: (255) End
    Padding: 0000000000000000000000000000000000000000000000000000000000000000
```

```
0000  58 a0 23 71 25 14 00 74   9c 7d fa db 08 00 45 00   X %q%t }...E-
0010  01 48 37 4b 0b 40 4d 11   ac 51 0a 7a c0 01 0a 7a   .H7K @ .Q z-z
0020  c1 13 00 43 00 44 01 34   e1 38 02 01 06 01 e8 75   ...C-D-4 -z...u
0030  52 dd 00 00 00 00 00 00   00 00 0a 7a c1 13 00 00   R.....8.....
0040  00 00 0a 7a c0 01 58 a0   23 71 25 14 00 00 00 00   ..z-X %q%....
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   .....
0090  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   .....
00a0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   .....
00b0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   .....
00c0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   .....
00d0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   .....
00e0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   .....
00f0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   .....
0100  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   .....
0110  03 00 00 00 00 00 63 82   53 63 35 01 05 36 04 0a   ....c Sc$-6-
0120  03 0a 02 c3 34 04 01 0c   20 01 02 ff ff c0 00 03   ...3...
0130  04 0a 7a c0 01 06 08 0a   03 09 2d 0a 83 09 2c ff   ....,
0140  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   .....
0150  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   .....
```

图 2: 四个 DHCP 分组的内容

## 2.2.2 分析 DHCP 分组

序号为 2 的 DHCP 分组内容的分析如表 1。

表 1: DHCP Discover 分组内容分析

字段 (字节数)	内容 (16 进制)	解释
OP (1)	01	消息类型: 引导请求
HTYPE (1)	01	硬件地址类型: 以太网
HLEN (1)	06	硬件地址长度: 6
HOPS (1)	00	经过的 DHCP 中继的数目: 0
XID (4)	e8 75 52 dd	处理 ID, 标记一次 IP 地址请求过程: 0xe87552dd
SECS (2)	00 00	从获取到 IP 地址或者续约过程开始到现在所消耗的时间: 0 秒
FLAGS (2)	00 00	标记: 第一位为 0, 表示单播
CIADDR (4)	00 00 00 00	客户端 IP 地址: 0.0.0.0 还未分配 IP 地址
YIADDR (4)	00 00 00 00	你的 (客户端) IP 地址 (服务器分配的地址): 0.0.0.0 仅在 Offer 和 ACK 分组中有效
SIADDR (4)	00 00 00 00	在 bootstrap 过程中下一台服务器的地址: 0.0.0.0 DHCP 服务器未知
GIADDR (4)	00 00 00 00	客户端发出请求分组后经过的第一个中继的地址: 0.0.0.0 没有经过中继
CHADDR (16)	58 a0 23 71 25 14	客户端的 MAC 地址: 58:a0:23:71:25:14 后接 10 个字节的填充
SNAME (64)	全部为 00	为客户端分配 IP 地址的服务器域名: 未给出
FILE (128)	全部为 00	为启动客户端指定的配置文件路径: 未给出
magic cookie(4)	63 82 53 63	可选字段的格式: DHCP
OPTION (3)	35 01 01	DHCP 消息类型: Discover
OPTION (9)	3d 07 01 58 a0 23 71 25 14	客户端标识符: 以太网, MAC 地址 58:a0:23:71:25:14
OPTION (17)	0c 0f 后略	主机名, 长度为 15
OPTION (8)	3c 08 后略	供应商标识符, 长度为 8
OPTION (16)	37 0e 后略	参数需求列表, 长度为 14
OPTION (1)	ff	选项字段结束

序号为 34、35、37 的 DHCP 分组内容的分析如表 2、表 3 和表 4, 表中仅展示与第一个分组不同的部分。

## 2.2.3 分析 DHCP 的工作流程

DHCP 协议用于对连接到网络的设备自动分配 IP 地址和其他通信变量。

1. 客户端连入局域网后, 向局域网内发送广播, 发送一个 DHCP Discover 分组, 分组内容中有本机的 MAC 地址, 并在 OPTION 字段中附带一个请求参数的列表。

表 2: DHCP Offer 分组内容分析

字段 (字节数)	内容 (16 进制)	解释
OP (1)	02	消息类型: 引导回复
HOPS (1)	01	经过的 DHCP 中继的数目: 1
YIADDR (4)	0a 7a c1 13	你的 (客户端) IP 地址 (服务器分配的地址): 10.122.193.19
GIADDR (4)	0a 7a c0 01	客户端发出请求分组后经过的第一个中继的地址: 10.122.192.1
OPTION (3)	35 01 02	DHCP 消息类型: Offer
OPTION (6)	36 04 0a 03 09 02	DHCP 服务器标识符: 10.3.9.2
OPTION (6)	33 04 00 00 1c 20	IP 地址释放时间: 7200 秒
OPTION (6)	01 04 ff ff c0 00	子网掩码: 255.255.192.0
OPTION (6)	03 04 0a 7a c0 01	路由器: 10.122.192.1
OPTION (10)	06 08 0a 03 09 2d 0a 03 09 2c	域名服务器: 10.3.9.45、10.3.9.44
OPTION (1)	ff	选项字段结束

表 3: DHCP Request 分组内容分析

字段 (字节数)	内容 (16 进制)	解释
OPTION (3)	35 01 03	DHCP 消息类型: Request
OPTION (9)	3d 07 01 58 a0 23 71 25 14	客户端标识符: 以太网, MAC 地址 58:a0:23:71:25:14
OPTION (6)	32 04 0a 7a c1 13	请求的 IP 地址: 10.122.193.19
OPTION (6)	36 04 0a 03 09 02	DHCP 服务器标识符: 10.3.9.2
省略一部分选项字段		
OPTION (1)	ff	选项字段结束

表 4: DHCP ACK 分组内容分析

字段 (字节数)	内容 (16 进制)	解释
OP (1)	02	消息类型: 引导回复
HOPS (1)	00	经过的 DHCP 中继的数目: 1
YIADDR (4)	0a 7a c1 13	你的 (客户端) IP 地址 (服务器分配的地址): 10.122.193.19
GIADDR (4)	0a 7a c0 01	客户端发出请求分组后经过的第一个中继的地址: 10.122.192.1
OPTION (3)	35 01 05	DHCP 消息类型: ACK
省略一部分选项字段		
OPTION (1)	ff	选项字段结束

2. 服务器为客户端分配 IP，并向之前的 MAC 地址发送 DHCP Offer 分组，分组内容中有分配的 IP 地址，分组的 OPTION 字段中附带服务器标识符、IP 租期、子网掩码等信息。
3. 客户端再次发送广播，发送一个 DHCP Request 分组，在 OPTIONS 字段中指明请求的 IP 地址和服务器标识符。
4. 服务器向客户端发送 DHCP ACK 分组确认。

## 2.2.4 捕获 ARP 分组

在 Wireshark 过滤器中输入 arp，过滤出数个 ARP 分组。分组的内容如图 3。

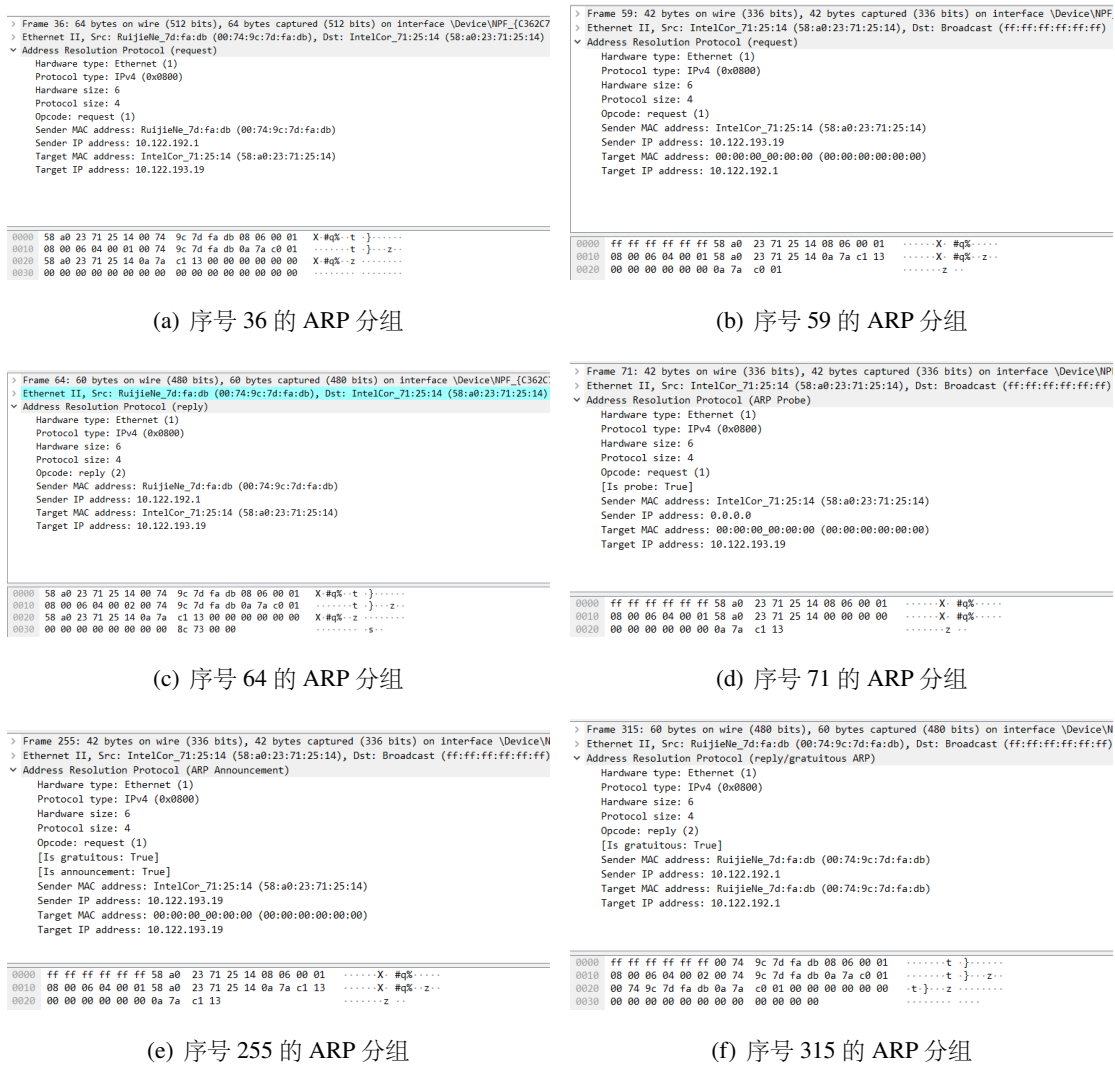


图 3: ARP 分组的内容

## 2.2.5 分析 ARP 分组

序号为 36 的 ARP 分组内容的分析如表 5。

表 5: 序号为 36 的 ARP 分组内容分析

字段 (字节数)	内容 (16 进制)	解释
HTYPE (2)	00 01	硬件类型: 以太网
PTYPE (2)	08 00	协议类型: IPv4
HLEN (1)	06	硬件地址长度: 6
PLEN (1)	04	协议地址长度: 4
OPER (2)	00 01	ARP 消息类型: request
SHA (6)	00 74 9c 7d fa db	发送方 MAC 地址: 00:74:9c:7d:fa:db
SPA (4)	0a 7a c0 01	发送方 IP 地址: 10.122.192.1
THA (6)	58 a0 23 71 25 14	接收方 MAC 地址: 58:a0:23:71:25:14
TPA (6)	0a 7a c1 13	接收方 IP 地址: 10.122.193.19

## 2.2.6 分析 ARP 的工作流程

ARP 协议用于将网络层地址 (比如 IPv4), 映射到链路层地址 (比如 MAC)。

1. 序号为 36 的 ARP 分组发送在 DHCP Request 和 DHCP ACK 之间, 此时路由器请求 10.122.193.19 的 MAC 地址, 但是此时 IP 地址还没有分配, 所以本机没有回复。
2. 序号为 59 的 ARP 分组发送在 IP 地址分配完成之后, 本机向局域网发送广播, 请求 10.122.192.1, 即路由器的 MAC 地址。
3. 序号为 64 的 ARP 分组是对第二个 ARP 的回复, 其中 OPER 字段设为 2, 表示一个回复分组, 分组内容中发送方的部分为路由器的 IP 和 MAC 地址。
4. 序号为 71 的 ARP 分组是一个 ARP 探针 (ARP Probe) 分组, 意图是探测 IP 地址在局域网中是否已经被使用, 其发送方 MAC 地址被设为本机, 发送方 IP 地址和接收方 MAC 地址被设为空, 接收方 IP 地址设为想要探测的 IP 地址, 即本机的 IP 地址。
5. 序号为 255 的 ARP 分组是一个 ARP 声明 (ARP Announcement) 分组, 意图是在局域网中“声明”这个 IP 地址, 除了发送方 IP 地址被设为本机 IP 之外, 其他内容和 ARP Probe 分组相同, 其他主机可以用发送方 IP 和 MAC 地址在 ARP 缓存中建立映射。
6. 序号为 315 的 ARP 分组是一个免费 ARP (Gratuitous ARP) 分组, 分组中 OPER 字段设为 2 (但是并不意味着对某个请求的回复), 发送方 MAC 与接收方 MAC 相同、发送方 IP 与接收方 IP 相同。路由器向局域网广播这个分组, 用于让主机更新 ARP 缓存中的映射。

## 2.3 捕获和分析 IP 分组

### 2.3.1 捕获 IP 分组

任意捕获一个 IP 分组, 如图 4。

### 2.3.2 分析 IP 分组

IP 分组的分析如表 6。

数据部分是 UDP 分组和 DNS 查询分组, 略。

```

> Frame 29: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{C362C
> Ethernet II, Src: IntelCor_71:25:14 (58:a0:23:71:25:14), Dst: RuijieNe_7d:fa:db (00:74:9c:7d:fa:db)
> Internet Protocol Version 4, Src: 10.122.193.19, Dst: 10.3.9.44
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 61
    Identification: 0x67f2 (26610)
    > Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.122.193.19
    Destination Address: 10.3.9.44
> User Datagram Protocol, Src Port: 50532, Dst Port: 53
> Domain Name System (query)
0000 00 74 9c 7d fa db 58 a0 23 71 25 14 08 00 45 00 .t.}.X. #q%...E.
0010 00 3d 67 f2 00 00 00 11 00 00 0a 7a c1 13 0a 03 .=g.....Z....
0020 09 2c c5 64 00 35 00 29 de f6 2d 9a 01 00 00 01 .,d-5.) .....
0030 00 00 00 00 00 00 04 61 70 69 31 06 6f 72 69 67 .....a pil orig
0040 69 6e 03 63 6f 6d 00 00 01 00 01 in.com...

```

图 4: 序号为 29 的 IP 分组

表 6: 序号为 29 的 IP 分组头分析

字段 (位数)	内容 (默认 16 进制)	解释
Version (4)	0100B	版本: 4
IHL (4)	0101B	头部长度的: 20 字节
DSCP (6)	000000B	区分服务信息: 默认
ECN (2)	00B	显式拥塞通知: 否
Total Length (16)	00 3d	分组总长度: 61 字节
Identification (16)	67 f2	分组标识: 0x67f2
Flags (3)	000B	Don't Fragment (不要分段) 标志位: 0 More Fragments (更多的段) 标志位: 0
Fragment Offset (13)	00000000000000B	分段偏移量: 0
TTL (8)	80	生存期: 128 跳
Protocol (8)	11	协议: UDP
Header CheckSum (32)	00 00 00 00	头校验和: 不验证
Source IP Address (32)	0a 7a c1 13	源地址: 10.122.193.19
Destimation IP Address (32)	0a 03 09 2c	目标地址: 10.3.9.44



### 2.3.3 捕获长 IP 分组

获取连接到 BUPT-mobile 的手机的 IP 地址为 10.21.245.157。

在 cmd 中输入指令 `ping 10.21.245.157 -n 1 -l 8000`，向手机发送一个长度为 8000 的 IP 数据包。

运行结果如图 5。

```
C:\WINDOWS\system32>ping 10.21.245.157 -n 1 -l 8000

正在 Ping 10.21.245.157 具有 8000 字节的数据:
来自 10.21.245.157 的回复: 字节=8000 时间=75ms TTL=63

10.21.245.157 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 75ms, 最长 = 75ms, 平均 = 75ms
```

图 5: ping指令运行结果

在 Wireshark 过滤器中输入 `ip.src eq 10.122.193.19 or ip.dst eq 10.122.193.19`，过滤出 12 个分组如图 6。

14	1.896422	10.122.193.19	10.21.245.157	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5b83) [Reassembled in #19]
15	1.896422	10.122.193.19	10.21.245.157	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=5b83) [Reassembled in #19]
16	1.896422	10.122.193.19	10.21.245.157	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=5b83) [Reassembled in #19]
17	1.896422	10.122.193.19	10.21.245.157	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=5b83) [Reassembled in #19]
18	1.896422	10.122.193.19	10.21.245.157	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=5b83) [Reassembled in #19]
19	1.896422	10.122.193.19	10.21.245.157	ICMP	642	Echo (ping) request id=0x0001, seq=144/36864, ttl=128 (reply in 27)
22	1.970962	10.21.245.157	10.122.193.19	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=1fbc) [Reassembled in #27]
23	1.971941	10.21.245.157	10.122.193.19	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=1fbc) [Reassembled in #27]
24	1.971941	10.21.245.157	10.122.193.19	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=1fbc) [Reassembled in #27]
25	1.971941	10.21.245.157	10.122.193.19	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=1fbc) [Reassembled in #27]
26	1.971941	10.21.245.157	10.122.193.19	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=1fbc) [Reassembled in #27]
27	1.971941	10.21.245.157	10.122.193.19	ICMP	642	Echo (ping) reply id=0x0001, seq=144/36864, ttl=63 (request in 19)

图 6: 捕获到的 12 个 IP 分组

限于篇幅原因，仅展示序号为 14 的 IP 分组的内容，如图 7。

```
> Frame 14: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF{...}
> Ethernet II, Src: IntelCor_71:25:14 (58:a0:23:71:25:14), Dst: RuijieNe_7d:fa:db (00:74:9c:7d:fa:db)
v Internet Protocol Version 4, Src: 10.122.193.19, Dst: 10.21.245.157
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x5b83 (23427)
  > Flags: 0x20, More fragments
    Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.122.193.19
    Destination Address: 10.21.245.157
    [Reassembled IPv4 in frame: 19]
v Data (1480 bytes)
  Data: 0800eb64000100906162636465666768696a6b6c6d6e6f70717273747576776162636465...
  [Length: 1480]

0000  00 74 9c 7d fa db 58 a0 23 71 25 14 08 00 45 00  .t.}.X. #q%.E.
0010  05 dc 5b 83 20 00 80 01 00 00 0a 7a c1 13 0a 15  ..[. ....z...
0020  f5 9d 08 00 eb 64 00 01 00 90 61 62 63 64 65 66  ....d...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  pqrstuvwxyz abcdefgh
0060  69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61  ijklmnop qrstuvw
0070  62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71  bcdefghi jklmnopq
0080  72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a  rstuvwab cdefghij
0090  6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63  klmnopqr stuvwabc
00a0  64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73  defghijk lmnopqrs
00b0  74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c  tuvabcd efghijkl
00c0  6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65  mnopqrst uvwabcde
00d0  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  fghijklm nopqrstu
00e0  76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e  vwabcdef ghijklmn
```

图 7: 序号为 14 的 IP 分组的内容



### 2.3.4 分析长 IP 分组

序号为 14 的 IP 分组的分组头部分的分析如表 7。

表 7: 序号为 14 的 IP 分组头分析

字段 (位数)	内容 (默认 16 进制)	解释
Version (4)	0100B	版本: 4
IHL (4)	0101B	头部长度的 20 字节
DSCP (6)	000000B	区分服务信息: 默认
ECN (2)	00B	显式拥塞通知: 否
Total Length (16)	05 dc	分组总长度: 1500 字节
Identification (16)	5b 83	分组标识: 0x5b83
Flags (3)	001B	Don't Fragment (不要分段) 标志位: 0 More Fragments (更多的段) 标志位: 1
Fragment Offset (13)	0000000000000B	分段偏移量: 0
TTL (8)	80	生存期: 128 跳
Protocol (8)	01	协议: ICMP
Header CheckSum (32)	00 00 00 00	头校验和: 不验证
Source IP Address (32)	0a 7a c1 13	源地址: 10.122.193.19
Destination IP Address (32)	0a 15 f5 9d	目标地址: 10.21.245.157

前六个分组的分组头的大部分内容都一致, 它们的 MF 标志位以及分段偏移量的对比如表 8。

表 8: IP 分组头对比

分组序号	MF 标志位	分段偏移量
14	1	0
15	1	$185 \times 8 = 1480$
16	1	$370 \times 8 = 2960$
17	1	$555 \times 8 = 4440$
18	1	$740 \times 8 = 5920$
19	0	$925 \times 8 = 7400$

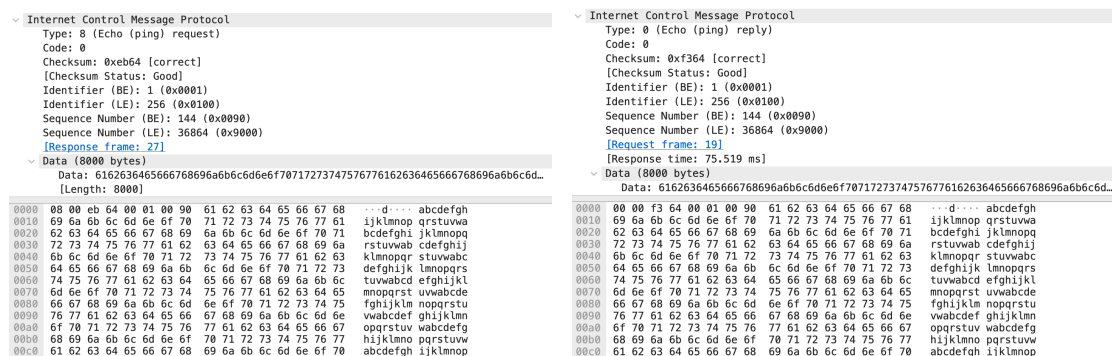
由于以太网数据链路层的 MTU 为 1500 字节, 除去头之后剩余 1480 字节, 正好是 8 的倍数, 因此长度为 8000 字节的数据被拆分成 6 个分段, 前五个的长度为 1480 字节, 最后一个的长度为 600 字节, 分段偏移量表示该分段在原数据段中的位置, 通过 MF 标志位为 0 确定数据的结束。

## 2.4 捕获和分析 ICMP 分组

### 2.4.1 分析 ping 命令产生的 ICMP 分组

ping 命令产生的 ICMP 分组的内容如图 8。

序号为 19 的 ICMP 分组头的分析如表 9。



(a) 序号为 19 的 ICMP 分组

(b) 序号为 27 的 ICMP 分组

图 8: ping命令产生的 ICMP 分组的内容

表 9: 序号为 19 的 ICMP 分组头分析

字段 (字节数)	内容 (16 进制)	解释
Type (1)	08	类型
Code (1)	00	与 Type 字段共同构成 Control Message: Echo Request
Checksum (2)	eb 64	校验和: 0xeb64
Identifier (2)	00 01	标识符, 用于区分不同进程 ping 消息
Sequence Number (2)	00 90	ping 请求序号

序号为 27 的 ICMP 分组是对上一个分组的回复, 其分组头除了 Type 字段改为 0, 表示 Echo Reply, 以及校验和发生变化之外, 其他和第一个 ICMP 分组头没有区别。

## 2.4.2 捕获 tracert 命令产生的 ICMP 分组

在 cmd 中输入指令 `tracert -d 10.21.245.157`, 追踪从本机到手机的路由。运行结果如图 9。

```
C:\WINDOWS\system32>tracert -d 10.21.245.157
通过最多 30 个跃点跟踪到 10.21.245.157 的路由

  1    1 ms    1 ms    1 ms    10.122.192.1
  2   57 ms    5 ms    8 ms    10.21.245.157

跟踪完成。
```

图 9: tracert指令运行结果

在 Wireshark 过滤器中输入 `icmp`, 过滤出 12 个分组如图 10。其中有三对 TTL 为 1 的 ping 请求和回复, 还有三对 TTL 为 2 的请求和回复。

其中序号为 166、167、10、182 的 ICMP 分组的内容如图 11。

序号为 166 的分组的 IP 部分的 TTL 为 1, ICMP 分组头的分析如表 10。

这个分组经过一跳之后, TTL 变为 0, 路由器返回超时信息, 即序号为 167 的分组, 其数据部分附带原来分组的 IP 头部和 8 个字节的 ICMP 头部, 其 ICMP 分组分析如表 11。

166	15.741802	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request	id=0x0001, seq=155/39680, ttl=1 (no response found!)
167	15.743199	10.122.192.1	10.122.193.19	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)	
168	15.743540	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request	id=0x0001, seq=156/39936, ttl=1 (no response found!)
169	15.744672	10.122.192.1	10.122.193.19	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)	
170	15.745004	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request	id=0x0001, seq=157/40192, ttl=1 (no response found!)
171	15.746924	10.122.192.1	10.122.193.19	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)	
180	16.760817	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request	id=0x0001, seq=158/40448, ttl=2 (reply in 182)
182	16.817800	10.21.245.157	10.122.193.19	ICMP	106 Echo (ping) reply	id=0x0001, seq=158/40448, ttl=63 (request in 180)
184	16.819359	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request	id=0x0001, seq=159/40704, ttl=2 (reply in 185)
185	16.825162	10.21.245.157	10.122.193.19	ICMP	106 Echo (ping) reply	id=0x0001, seq=159/40704, ttl=63 (request in 184)
186	16.826240	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request	id=0x0001, seq=160/40960, ttl=2 (reply in 187)
187	16.834917	10.21.245.157	10.122.193.19	ICMP	106 Echo (ping) reply	id=0x0001, seq=160/40960, ttl=63 (request in 186)

[illegible]

(b) 序号为 167 的 ICMP 分组

(d) 序号为 182 的 ICMP 分组

表 10: 序号为 166 的 ICMP 分组头分析

字段 (字节数)	内容 (16 进制)	解释
Type (1)	08	类型
Code (1)	00	与 Type 字段共同构成 Control Message: Echo Request
Checksum (2)	f7 63	校验和: 0xf763
Identifier (2)	00 01	标识符, 用于区分不同进程 ping 消息
Sequence Number (2)	00 9b	ping 请求序号

表 11: 序号为 167 的 ICMP 分组分析

字段 (字节数)	内容 (16 进制)	解释
Type (1)	11	类型
Code (1)	00	与 Type 字段共同构成 Control Message: TTL expired in transit
Checksum (2)	f4 ff	校验和: 0xf4ff
- (4)	00 00 00 00	未使用
IPv4 报文头 (20)	略	序号为 166 的分组的 IP 头
ICMP (8)	略	序号为 166 的分组的 ICMP 头

本机经过两跳之后就能到达手机, 于是 TTL 为 2 时可以收到回复。序号为 180、182 的分组的 ICMP 头分析如表 12、表 13。

表 12: 序号为 180 的 ICMP 分组头分析

字段 (字节数)	内容 (16 进制)	解释
Type (1)	08	类型
Code (1)	00	与 Type 字段共同构成 Control Message: Echo Request
Checksum (2)	f7 60	校验和: 0xf760
Identifier (2)	00 01	标识符, 用于区分不同进程 ping 消息
Sequence Number (2)	00 9e	ping 请求序号

表 13: 序号为 182 的 ICMP 分组头分析

字段 (字节数)	内容 (16 进制)	解释
Type (1)	00	类型
Code (1)	00	与 Type 字段共同构成 Control Message: Echo Reply
Checksum (2)	ff 60	校验和: 0xff60
Identifier (2)	00 01	标识符, 用于区分不同进程 ping 消息
Sequence Number (2)	00 9e	ping 请求序号

### 3 实验总结和心得体会

完成本实验大约耗费我 4 个小时的时间, 其中主要的时间花费在查阅英文文档上, 这使我查找和阅读英文文档的能力有所增强。

调试时，我学习并且灵活运用了 Wireshark 的筛选功能，从诸多报文中筛选需要的一部分，节省了许多时间。

在本次实验过程中，我主要查阅相关 RFC 文档、wiki 和 Wireshark 的帮助文档，通过与课本上理论知识联系，对 IP、DHCP、ARP、ICMP 协议报文的内容和部分功能有了初步的认识，对其作用原理有更深刻的理解。