

# 计算机网络实验指导书

北京邮电大学计算机学院

# 目 录

目 录 .....	2
实验二：网络层数据分组的捕获和解析.....	3
1. 实验类别 .....	3
2. 实验内容和实验目的 .....	3
3. 实验学时 .....	3
4. 实验组人数 .....	3
5. 实验设备环境 .....	3
6. 教学要点与学习难点 .....	3
7. 实验步骤 .....	3
7.1 准备工作 .....	3
7.2 捕获和分析网络层分组 .....	3
7.3 发送 ICMP 分组，捕获并分析格式.....	3
7.4 分析数据分组的分片传输过程.....	4
7.5 撰写实验报告 .....	4
8. Wireshark 软件 .....	4
9. 实验内容 .....	4
9.1 实验内容和实验环境描述.....	4
9.2 分析网络层分组结构 .....	4
9.3 实验结论和实验心得 .....	7

## 实验二：网络层数据分组的捕获和解析

### 1. 实验类别

协议分析

### 2. 实验内容和实验目的

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 数据组分的结构。

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 数据组分的结构。

### 3. 实验学时

4 学时。

### 4. 实验组人数

每组 1 人，进行数据捕获并分析，撰写实验报告。

### 5. 实验设备环境

1 台装有 Windows 操作系统的 pc 机，要求能够连接到 Internet，并安装 Wireshark 等软件。

### 6. 教学要点与学习难点

重点分析网络层分组的格式，掌握各种分组在网络通信中的应用，了解整个上网的工作过程。发送 ICMP 分组，并分析其结构和功能。制作长度大于 1500 字节的 IP 数据分组，发送并分析其分片传输的过程。

### 7. 实验步骤

#### 7.1 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。

#### 7.2 捕获和分析网络层分组

开启监控，连接网络。一段时间后查看捕获的分组。分析各种分组的格式以及在上网过程中所起的作用。

#### 7.3 发送 ICMP 分组，捕获并分析格式

开启监控，使用 ping 命令，tracert 命令，捕获 ICMP 分组格式。

#### 7.4 分析数据分组的分片传输过程

制作 8000 字节的 IP 数据分组并发送，捕获后分析其分片传输的分组结构。

#### 7.5 撰写实验报告

按要求撰写实验报告，并接受实验指导教师面对面现场提问。

### 8. Wireshark 软件

Official website

■ <http://www.wireshark.org/>

Download page

■ <http://www.wireshark.org/download.html>

### 9. 实验内容

#### 9.1 实验内容和实验环境描述

描述本次实验的任务、内容和实验环境。

#### 9.2 分析网络层分组结构

##### 1) 捕获 DHCP 分组

```
00000000: 00 e0 fc 86 27 db 00 16 36 70 1e 94 88 64 11 00
00000010: 07 8f 01 4a 00 21 45 00 01 48 61 67 00 00 40 11
00000020: 18 ea de 83 20 d1 ff ff ff ff 00 44 00 43 01 34
00000030: f3 3c 01 08 06 00 18 e3 bf d4 06 00 00 00 de 83
00000040: 20 d1 00 00 00 00 00 00 00 00 00 00 00 00 53
00000050: 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 63 82
00000120: 53 63 35 01 08 3d 07 08 00 53 45 00 00 00 0c 0f
00000130: 35 32 35 31 61 61 66 36 65 36 36 62 34 65 38 3c
00000140: 08 4d 53 46 54 20 35 2e 30 37 06 06 2c 01 f9
00000150: 0f ff 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Encode 分析如下：

```

DHCP:
DHCP: Boot record type      = 1 (Request)
DHCP: Hardware address type = 8 (HyperChannel)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops                  = 0
DHCP: Transaction id       = 18E3BFD4
DHCP: Elapsed boot time    = 1536 seconds
DHCP: Flags                 = 0000
DHCP: 0... = No broadcast
DHCP: Client self-assigned IP address = [222.131.32.209]
DHCP: Client IP address    = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent          = [0.0.0.0]
DHCP: Client hardware address = 005345000000
DHCP:
DHCP: Host name            = ""
DHCP: Boot file name      = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type         = 8 (DHCP Inform)
DHCP: Client Identifier    = 08005345000000
DHCP: HostName             = "5251aaf6e66b4e8"
DHCP: Class identifier     = 4D53465420352E30
DHCP: Parameter Request List: 6 entries
DHCP: Option Type         = 6 (Domain name server)
DHCP: Option Type         = 44 (NetBIOS over TCP/IP name server)
DHCP: Option Type         = 43 (Vendor specific information)
DHCP: Option Type         = 1 (Client's subnet mask)
DHCP: Option Type         = 249 (Reserved tag)
DHCP: Option Type         = 15 (Domain name)
DHCP: End of Options      = 255
DHCP: 12 byte(s) of header padding
DHCP:

```

计算机以广播方式发送一个 DHCP request 请求信息，该信息中包含向它所选定的 DHCP 服务器请求 IP 地址 222.131.32.209。

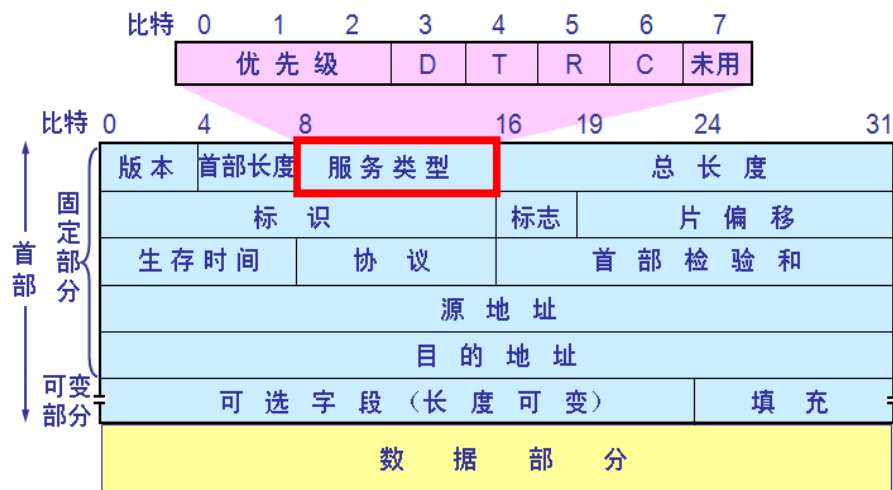
## 2) 捕获 IP 数据分组:

```

ff ff ff ff ff ff 00 16 36 70 1e 94 08 00 45 00
00 4e b4 6c 00 00 40 11 b7 bc a9 fe ba 79 a9 fe
ff ff 00 89 00 89 00 3a ec 49 83 2b 01 10 00 01
00 00 00 00 00 00 20 46 48 45 50 46 43 45 4c 45
48 46 43 45 50 46 46 46 41 43 41 43 41 43 41 43
41 43 41 43 41 42 4c 00 00 20 00 01

```

IP 分组格式为:



分析 IP 数据分组:

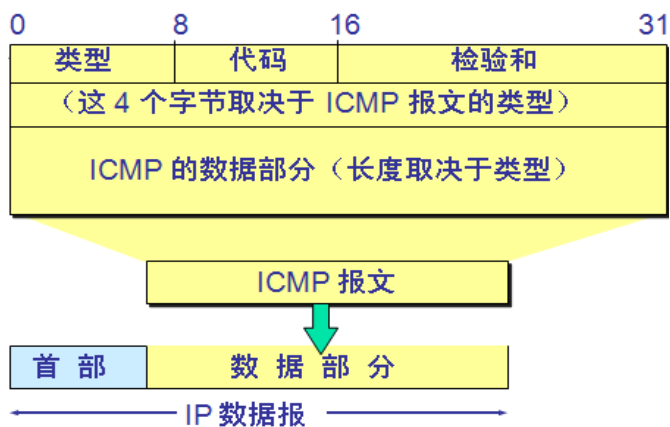
字 段	报 文 (16 进制)	内 容
包头长度	45	包头长 20 字节
服务类型	00	正常时延, 正常吞吐量, 正常可靠性
总长度	004e	数据分组长 78 字节
标识	b46c	标识为 46188
标志	00	MF=0,DF=0 允许分片, 此片为最后一片
片偏移	00	偏移量为 0
生存周期	40	每跳生存时间为 64 秒
协议	11	携带的数据来自 UDP 协议
头部校验和	b7bc	IP 头部校验和为 b7bc
源地址	a9feba79	源地址为 169.254.186.121
目的地址	a9feffff	目的地址 169.254.255.255

3) 分析整个上网的工作过程, 需要收发什么分组? 每个分组的内容是什么?

4) 捕获 ICMP 分组:

```
00 16 36 70 1e 94 00 e0 fc 86 27 db 88 64 11 00
0d 22 00 3a 00 21 45 00 00 38 b5 e4 00 00 72 01
d4 a5 3d 0e 82 4a de 83 20 5f 03 03 a3 1a 00 00
00 00 45 00 00 5c 49 b5 00 00 37 11 7b a1 de 83
20 5f 3d 0e 82 4a 1f 40 1f 40 00 48 1b 1a
```

ICMP 分组格式:



分析 ICMP 分组:

字 段	报文 (16 进制)	内 容
类型	03	终点不可达
代码	03	端口不可达
校验和	a31a	头部校验和为 a31a

此 ICMP 报文是差错报文, 报告差错为终点不可达中的端口不可达。

5) 制作一个 8000 字节的 IP 数据分组, 发送后捕获分析。由于分组长度大于 1500 字节, 因此需要分片传输。按照 2) 中的方法分析所有分片的结构。

### 9.3 实验结论和实验心得

如果一切顺利，那么完成本次实验的工作大约需要 2~3 个小时。你用的时间超过了这个预测吗？描述在调试过程中都遇到了哪些问题和解决的过程。总结本次实验，你有哪些收获？