

北京邮电大学《计算机网络》课程实验报告

[illegible]

注：评语要体现每个学生的工作情况，可以加页。

北京邮电大学

计算机网络实验报告



题目： 网络层数据分组的捕获和解析

班 级： 2018211318 班

学 号： 2018210074

姓 名： 熊宇

学 院： 计算机学院

2020 年 6 月 5 日

实验报告

一 实验内容和实验目的

(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。

二 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。

三 实验步骤

(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) 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。

(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。

(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。

(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。

四 实验内容

(1) 分析网络层分组结构

A、捕获 DHCP 分组

1、DHCP 简介

DHCP，动态主机配置协议，前身是 BOOTP 协议，是一个局域网的网络协议，使用 UDP 协议工作，常用的 2 个端口：67(DHCP server),68(DHCP client)。DHCP 通常被用于局域网环境，主要作用是集中的管理、分配 IP 地址，使 client 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。简单来说，DHCP 就是一个不需要账号密码登录的、自动给内网机器分配 IP 地址等信息的协议。

2、DHCP 协议中的报文

DHCP DISCOVER：客户端开始 DHCP 过程发送的包，是 DHCP 协议的开始

DHCP OFFER：服务器接收到 DHCP DISCOVER 之后做出的响应，它包括了给予客户端的 IP (yiaddr)、客户端的 MAC 地址、租约过期时间、服务器的识别符以及其他信息

DHCP REQUEST：客户端对于服务器发出的 DHCP OFFER 所做出的响应。在续约租期的时候同样会使用。

DHCP ACK：服务器在接收到客户端发来的 DHCP REQUEST 之后发出的成功确认的报文。在建立连接的时候，客户端在接收到这个报文之后才会确认分配给它的 IP 和其他信息可以被允许使用。

DHCP NAK：DHCP ACK 的相反的报文，表示服务器拒绝了客户端的请求。

DHCP RELEASE：一般出现在客户端关机、下线等状况。这个报文将会使 DHCP 服务器释放出此报文的客户端的 IP 地址

DHCP INFORM：客户端发出的向服务器请求一些信息的报文

DHCP DECLINE：当客户端发现服务器分配的 IP 地址无法使用（如 IP 地址冲突时），将发出此报文，通知服务器禁止使用该 IP 地址。

3、DHCP 的工作过程

Client 端在局域网内发起一个 DHCP Discover 包，目的是想发现能够给它提供 IP 的 DHCP Server。

可用的 DHCP Server 接收到 Discover 包之后，通过发送 DHCP Offer 包给予 Client 端应答，意在告诉 Client 端它可以提供 IP 地址。

Client 端接收到 Offer 包之后，发送 DHCP Request 包请求分配 IP。

DHCP Server 发送 ACK 数据包，确认信息。

4、实验步骤

打开 Wireshark 软件，在首页选择当前电脑所使用的接口（如 WLAN），双击当前接口，弹出的页面中已经在不断的显示抓包的信息。在上方显示输入过滤器的条形窗口内输入 bootp，使其只显示 DHCP 数据包。

打开命令提示符窗口，输入 ipconfig /release 断开网络连接；此时计算机中所有网卡都已断开，Wireshark 中显示截获到一个 DHCP Release 数据包。

0000	50 3a a0 bc d1 06 b0 fc 36 58 57 01 08 00 45 00	P:..... 6XW...E.
0010	01 48 f5 ab 00 00 80 11 c2 41 c0 a8 00 66 c0 a8	.H..... .A...f..
0020	00 01 00 44 00 43 01 34 03 d6 01 01 06 00 b6 27	...D.C.4
0030	d5 70 00 00 00 00 00 c0 a8 00 66 00 00 00 00 00	.p..... .f.....
0040	00 00 00 00 00 00 00 b0 fc 36 58 57 01 00 00 00 6XW.....
0050	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
0070	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
0090	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
00b0	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
00d0	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
00f0	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
0110	00 00 00 00 00 00 63 82 53 63 35 01 07 36 04 c0c. Sc5..6..
0120	a8 00 01 3d 07 01 b0 fc 36 58 57 01 ff 00 00 00	...=.... 6XW.....
0130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0140	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0150	00 00 00 00 00 00

```

Frame 106: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
on interface \Device\NPF_{A1C9129E-1345-4E45-8F51-87974B691679}, id 0
Ethernet II, Src: CyberTAN_58:57:01 (b0:fc:36:58:57:01), Dst:
Shenzhen_bc:d1:06 (50:3a:a0:bc:d1:06)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Release)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xb627d570
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 192.168.0.102
  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: CyberTAN_58:57:01 (b0:fc:36:58:57:01)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Release)
  Option: (54) DHCP Server Identifier (192.168.0.1)
  Option: (61) Client identifier
  Option: (255) End

```

0000	50 3a a0 bc d1 06 b0 fc 36 58 57 01 08 00 45 00	P:..... 6XW...E.
0010	01 58 0c f5 00 00 80 11 aa e8 c0 a8 00 66 c0 a8	·X..... ····f.
0020	00 01 00 44 00 43 01 44 49 71 01 01 06 00 3b cd	···D·C·D Iq····;
0030	77 28 00 00 00 00 c0 a8 00 66 00 00 00 00 00 00	w(····· ·f·····
0040	00 00 00 00 00 00 b0 fc 36 58 57 01 00 00 00 00	····· 6XW····
0050	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	····· ·····
0070	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	····· ·····
0090	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	····· ·····
00b0	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	····· ·····
00d0	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	····· ·····
00f0	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	····· ·····
0110	00 00 00 00 00 00 00 63 82 53 63 35 01 03 3d 07 01	·····c· Sc5··=·
0120	b0 fc 36 58 57 01 0c 0f 4c 41 50 54 4f 50 2d 52	··6XW·· LAPTOP-R
0130	33 49 39 45 34 56 44 51 12 00 00 00 4c 41 50 54	BI9E4VDQ ····LAPT
0140	4f 50 2d 52 33 49 39 45 34 56 44 3c 08 4d 53 46	OP-R3I9E 4VD<·MSF
0150	54 20 35 2e 30 37 0e 01 03 06 0f 1f 21 2b 2c 2e	T 5.07·· ····!+,.
0160	2f 77 79 f9 fc ff	/wy···

```

Frame 40: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on
interface \Device\NPF_{A1C9129E-1345-4E45-8F51-87974B691679}, id 0
Ethernet II, Src: CyberTAN_58:57:01 (b0:fc:36:58:57:01), Dst:
Shenzhen_bc:d1:06 (50:3a:a0:bc:d1:06)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
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: 0x3bcd7728
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.0.102
    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: CyberTAN_58:57:01 (b0:fc:36:58:57:01)
    Client hardware address padding: 00000000000000000000

```

```

Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Request)
Option: (61) Client identifier
Option: (12) Host Name
Option: (81) Client Fully Qualified Domain Name
Option: (60) Vendor class identifier
Option: (55) Parameter Request List
Option: (255) End

```

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 192.168.0.102。

B、捕获 IP 数据分组

1、IP 数据报报文格式

2、实验步骤

打开 Wireshark，开启抓包，在过滤器一栏输入 ip.src eq 你要 Ping 的目标 IP 地址 or ip.dst eq 你要 Ping 的目标 IP 地址（如 www.baidu.com,则输入 ip.src eq 61.135.169.121 or ip.dst eq 61.135.169.121），用来过滤 IP。

命令提示符窗口输入 ping www.baidu.com,观察 Wireshark 中出现的新数据包,并分析数据包。

0000	50 3a a0 bc d1 06 b0 fc 36 58 57 01 08 00 45 00	P:.....6XW...E.
0010	00 28 f2 73 40 00 80 06 9f 56 c0 a8 00 66 df cb	.(.s@... .V...f..
0020	c8 2b 19 ff 01 bb 74 51 7f 26 bb 18 f6 16 50 14	+.tQ .&....P.
0030	00 00 86 69 00 00	...i..

Encode 分析如下:

```

Frame 3350: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on
interface \Device\NPF_{A1C9129E-1345-4E45-8F51-87974B691679}, id 0
Ethernet II, Src: CyberTAN_58:57:01 (b0:fc:36:58:57:01), Dst:
Shenzhen_bc:d1:06 (50:3a:a0:bc:d1:06)
    Destination: Shenzhen_bc:d1:06 (50:3a:a0:bc:d1:06)
    Address: Shenzhen_bc:d1:06 (50:3a:a0:bc:d1:06)
    .... ..0. .... = LG bit: Globally unique address
(factory default)
    .... ...0 .... = IG bit: Individual address
(unicast)
    Source: CyberTAN_58:57:01 (b0:fc:36:58:57:01)
    Address: CyberTAN_58:57:01 (b0:fc:36:58:57:01)
    .... ..0. .... = LG bit: Globally unique address
(factory default)
    .... ...0 .... = IG bit: Individual address
(unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 223.203.200.43

```

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xf273 (62067)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x9f56 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.0.102
Destination: 223.203.200.43
Transmission Control Protocol, Src Port: 6655, Dst Port: 443, Seq: 989,
Ack: 3736, Len: 0
Source Port: 6655
Destination Port: 443
[Stream index: 131]
[TCP Segment Len: 0]
Sequence number: 989 (relative sequence number)
Sequence number (raw): 1951498022
[Next sequence number: 989 (relative sequence number)]
Acknowledgment number: 3736 (relative ack number)
Acknowledgment number (raw): 3138975254
0101 .... = Header Length: 20 bytes (5)
Flags: 0x014 (RST, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .1.. = Reset: Set
.... .... ..0. = Syn: Not set
.... .... ...0 = Fin: Not set
[TCP Flags: .....A.R..]
Window size value: 0
[Calculated window size: 0]
[Window size scaling factor: 256]
Checksum: 0x8669 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 4.677887000 seconds]
[Time since previous frame in this TCP stream: 4.475056000 seconds]
```

IP 分组格式为:



分析 IP 数据分组：

字段	报文	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	0028	40
标识	f273	标识为 62607
标志	40	DF=1 MF=0 不允许分片
片偏移	00	偏移量为 0
生存周期	80	每跳生存周期为 128 秒
协议	06	携带数据来自 TCP 协议
头部校验和	9f56	头部校验和为 0x9f56
源地址	c0a8 0066	源地址为 192.168.0.102
目的地址	dfcb c82b	目的地址为 223.203.200.43

C、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？

向默认网关发送一个 DHCP REQUEST 报文以申请获得 IP 地址。

网关收到报文后回送一个 DHCP ACK

利用 ARP 数据报本机广播自己的地址映射关系，使其他主机知道当前主机的地址。

D、捕获 ICMP 分组

1、ICMP 简介

ICMP 是“Internet Control Message Protocol”（Internet 控制消息协议）的缩写，它是 TCP/IP 协议族的一个子协议。用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息尽管并不传输用户数据。可是对于用户数据的传递起着关键的数据。ICMP 报文作为 IP 层数据报的数据，加上数据报的首部，组成数据报发送出去。ICMP 报文的种类有两种，即 ICMP 差错报告报文和 ICMP 询问报文。

2、ICMP 分组格式

3、实验步骤

打开 Wireshark，开启抓包，在过滤器一栏输入 icmp，使其只显示 ICMP 协议。

命令提示符窗口输入 ping www.baidu.com,观察 Wireshark 中出现的新数据包,并分析数据包。

0000	b0 fc 36 58 57 01 50 3a a0 bc d1 06 08 00 45 00	..6XW·P:E·
0010	00 3c bf ed 00 00 33 01 1f c1 3d 87 a9 7d c0 a8	·<....3· ..=..}..
0020	00 66 00 00 50 ea 00 01 04 71 61 62 63 64 65 66	·f··P··· ·qabcdef
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

Encode 分析如下:

```

Frame 32390: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
interface \Device\NPF_{A1C9129E-1345-4E45-8F51-87974B691679}, id 0
Ethernet II, Src: Shenzhen_bc:d1:06 (50:3a:a0:bc:d1:06), Dst:
CyberTAN_58:57:01 (b0:fc:36:58:57:01)
  Destination: CyberTAN_58:57:01 (b0:fc:36:58:57:01)
    Address: CyberTAN_58:57:01 (b0:fc:36:58:57:01)
      .... ..0. .... = LG bit: Globally unique address
(factory default)
      .... ...0 .... = IG bit: Individual address
(unicast)
    Source: Shenzhen_bc:d1:06 (50:3a:a0:bc:d1:06)
      Address: Shenzhen_bc:d1:06 (50:3a:a0:bc:d1:06)
        .... ..0. .... = LG bit: Globally unique address
(factory default)
        .... ...0 .... = IG bit: Individual address
(unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 61.135.169.125, Dst: 192.168.0.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0xbfed (49133)
  Flags: 0x0000

```

```
Fragment offset: 0
Time to live: 51
Protocol: ICMP (1)
Header checksum: 0x1fc1 [validation disabled]
[Header checksum status: Unverified]
Source: 61.135.169.125
Destination: 192.168.0.102
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x50ea [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 1137 (0x0471)
Sequence number (LE): 28932 (0x7104)
[Request frame: 32389]
[Response time: 38.531 ms]
Data (32 bytes)
  Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
  [Length: 32]
```

ICMP 分组格式:



分析 ICMP 分组:

字段	报文 (16 进制)	内容
类型	00	Echo(ping) reply
代码	00	
校验和	5aea	校验和为 0x5aea

E、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。

1、实验步骤

打开 Wireshark，开启抓包，在过滤器一栏输入 ip.src eq 你要 Ping 的目标 IP 地址 or ip.dst eq 你要 Ping 的目标 IP 地址（如 www.baidu.com,则输入 ip.src eq 61.135.169.121 or ip.dst eq 61.135.169.121），用来过滤 IP。

命令提示符窗口输入 ping -l 8000 www.baidu.com（ping -l size ip 用来指定发送数据包的大小），观察 Wireshark 中出现的新数据包，查看每个数据包的 Fragment offset，分析所有分片的结构。

2.分片分析

第一个分片

0000	50 3a a0 bc d1 06 b0 fc 36 58 57 01 08 00 45 00	P:..... 6XW...E.
0010	05 dc e3 c1 20 00 80 01 89 50 c0 a8 00 66 3d 87P...f=.
0020	a9 79 08 00 e7 7f 00 01 04 75 61 62 63 64 65 66	.y..... ·uabcdef
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	wabcdefgh hijklmno
0050	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	pqrstuvw 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	tuvwabcd 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
00f0	6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67	opqrstuv wabcdefgh
0100	68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77	hijklmno pqrstuvw

字段	报文	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	05dc	1500
标识	e3c1	标识为 58305
标志	20	DF=0 MF=1 允许分片且不是最后一片
片偏移	00	偏移量为 0
生存周期	80	每跳生存周期为 128 秒
协议	01	携带数据来自 ICMP(1)协议
头部校验和	8950	头部校验和为 0x8950
源地址	c0a8 0066	源地址为 192.168.0.102
目的地址	3d87 a979	目的地址为 61.135.169.121

第二个分片

0000	50 3a a0 bc d1 06 b0 fc 36 58 57 01 08 00 45 00	P:..... 6XW...E.
0010	05 dc e3 c1 20 b9 80 01 88 97 c0 a8 00 66 3d 87f=.
0020	a9 79 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e	·yabcdef ghijklmn
0030	6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67	opqrstuv wabcdefg
0040	68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77	hijklmno pqrstuvw
0050	61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70	abcdefgh ijklmnop
0060	71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69	qrstuvw bcdefghi
0070	6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62	jklmnopq rstuvwab
0080	63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72	cdefghij klmnopqr
0090	73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b	stuvwabc defghijk
00a0	6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64	lmnopqrs tuvabcd
00b0	65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74	efghijkl mnopqrst
00c0	75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d	vwabcde fghijklm
00d0	6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66	nopqrstu vwabcdef
00e0	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
00f0	77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	wabcdefg hijklmno
0100	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	pqrstuvw abcdefgh

字段	报文	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	05dc	1500
标识	e3c1	标识为 58305
标志	20	DF=0 MF=1 允许分片且不是最后一片
片偏移	b9	偏移量为 1480
生存周期	80	每跳生存周期为 128 秒
协议	01	携带数据来自 ICMP(1)协议
头部校验和	8897	头部校验和为 0x8897
源地址	c0a8 0066	源地址为 192.168.0.102
目的地址	3d87 a979	目的地址为 61.135.169.121

第三个分片

0000	50 3a a0 bc d1 06 b0 fc 36 58 57 01 08 00 45 00	P:..... 6XW...E.
0010	05 dc e3 c1 21 72 80 01 87 de c0 a8 00 66 3d 87!r... ..f=.
0020	a9 79 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	·yijklmn opqrstuv
0030	77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	wabcdefg hijklmno
0040	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	pqrstuvw abcdefgh
0050	69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61	ijklmnop qrstuvw
0060	62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71	bcdefghi jklmnopq
0070	72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a	rstuvwab cdefghij
0080	6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63	klmnopqr stuvwabc
0090	64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73	defghijk lmnopqrs
00a0	74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c	tuvwabcd efghijkl
00b0	6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65	mnopqrst uvwabcde
00c0	66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75	fghijklm nopqrstu
00d0	76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e	vwabcdef ghijklmn
00e0	6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67	opqrstuv wabcdefg
00f0	68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77	hijklmno pqrstuvw
0100	61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70	abcdefgh ijklmnop

字段	报文	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	05dc	1500
标识	e3c1	标识为 58305
标志	21	DF=0 MF=1 允许分片且不是最后一片
片偏移	72	偏移量为 2960
生存周期	80	每跳生存周期为 128 秒
协议	01	携带数据来自 ICMP(1)协议
头部校验和	87de	头部校验和为 0x87de
源地址	c0a8 0066	源地址为 192.168.0.102
目的地址	3d87 a979	目的地址为 61.135.169.121

第四个分片

0000	50 3a a0 bc d1 06 b0 fc 36 58 57 01 08 00 45 00	P:..... 6XW...E.
0010	05 dc e3 c1 22 2b 80 01 87 25 c0 a8 00 66 3d 87"+... .%...f=.
0020	a9 79 71 72 73 74 75 76 77 61 62 63 64 65 66 67	·yqrstuv wabcdefg
0030	68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77	hijklmno pqrstuvw
0040	61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70	abcdefgh ijklmnop
0050	71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69	qrstuvw bcdefghi
0060	6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62	ijklmnopq rstuvwab
0070	63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72	cdefghij klmnopqr
0080	73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b	stuvwabc defghijk
0090	6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64	lmnopqrs tuvwabcd
00a0	65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74	efghijkl mnopqrst
00b0	75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d	uvwabcde fghijklm
00c0	6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66	nopqrstu vwabcdef
00d0	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
00e0	77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	wabcdefg hijklmno
00f0	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	pqrstuvw abcdefgh
0100	69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61	ijklmnop qrstuvwa

字段	报文	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	05dc	1500
标识	e3c1	标识为 58305
标志	22	DF=0 MF=1 允许分片且不是最后一块
片偏移	2b	偏移量为 4440
生存周期	80	每跳生存周期为 128 秒
协议	01	携带数据来自 ICMP(1)协议
头部校验和	8725	头部校验和为 0x8725
源地址	c0a8 0066	源地址为 192.168.0.102
目的地址	3d87 a979	目的地址为 61.135.169.121

第五个分片

0000	50 3a a0 bc d1 06 b0 fc 36 58 57 01 08 00 45 00	P:..... 6XW...E.
0010	05 dc e3 c1 22 e4 80 01 86 6c c0 a8 00 66 3d 87".... .l...f=.
0020	a9 79 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	.ybcdefg hijklmno
0030	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	pqrstuvw abcdefgh
0040	69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61	ijklmnop qrstuvw
0050	62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71	bcdefghi jklmnopq
0060	72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a	rstuvwab cdefghij
0070	6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63	klmnopqr stuvwabc
0080	64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73	defghijk lmnopqrs
0090	74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c	tuvwabcd efghijkl
00a0	6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65	mnopqrst uvwabcde
00b0	66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75	fghijklm nopqrstu
00c0	76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e	vwabcdef ghijklmn
00d0	6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67	opqrstuv wabcdefg
00e0	68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77	hijklmno pqrstuvw
00f0	61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70	abcdefgh ijklmnop
0100	71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69	qrstuvw bcdefghi

字段	报文	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	05dc	1500
标识	e3c1	标识为 58305
标志	22	DF=0 MF=1 允许分片且不是最后一块
片偏移	e4	偏移量为 5920
生存周期	80	每跳生存周期为 128 秒
协议	01	携带数据来自 ICMP(1)协议
头部校验和	866c	头部校验和为 0x866c
源地址	c0a8 0066	源地址为 192.168.0.102
目的地址	3d87 a979	目的地址为 61.135.169.121

第六片分片

0000	50 3a a0 bc d1 06 b0 fc 36 58 57 01 08 00 45 00	P:..... 6XW...E.
0010	02 74 e3 c1 03 9d 80 01 a9 1b c0 a8 00 66 3d 87	.t.....f=.
0020	a9 79 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77	.yjklmno pqrstuvwxyz
0030	61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70	abcdefghijklm nopqrstuvw
0040	71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69	qrstuvwxyz abcdefghi
0050	6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62	abcdefghijklm nopqrstuvw
0060	63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72	qrstuvwxyz abcdefghi
0070	73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b	abcdefghijklm nopqrstuvw
0080	6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64	qrstuvwxyz abcdefghi
0090	65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74	abcdefghijklm nopqrstuvw
00a0	75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d	qrstuvwxyz abcdefghi
00b0	6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66	abcdefghijklm nopqrstuvw
00c0	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	qrstuvwxyz abcdefghi
00d0	77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	abcdefghijklm nopqrstuvw
00e0	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	qrstuvwxyz abcdefghi
00f0	69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61	abcdefghijklm nopqrstuvw

字段	报文	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	0274	628
标识	e3c1	标识为 58305
标志	03	DF=0 MF=0 允许分片且是最后一片
片偏移	9d	偏移量为 7400
生存周期	80	每跳生存周期为 128 秒
协议	01	携带数据来自 ICMP(1)协议
头部校验和	a91b	头部校验和为 0xa91b
源地址	c0a8 0066	源地址为 192.168.0.102
目的地址	3d87 a979	目的地址为 61.135.169.121

上述前五个分组1500字节，净荷部分长度为 $1500 - 20 = 1480$ ，五个共 $1480 * 5 = 7400$ ；最后一个分组628字节，除了减去头部20字节以外，还要减去ICMP的8字节，净荷部分为 $628 - 20 - 8 = 600$ ， $7400 + 600 = 8000$ ，总长度吻合，分片正确。

六 实验总结

(1) 问题解决

完成本次实验花了大约2个小时左右，选择的时间是在周五晚上。

(2) 心得体会

通过这次实验，我对课堂上介绍的各种分组的结构有了更加实际的认识，也理解得更加深刻。此外，在 wireshark 的智能性辅助下分析分组结构，让我感受到了 wireshark 的强大，却也增强了我今后独立分析分组结构的信心和决心。