

# 华东师范大学数据科学与工程学院上机实践报告

|               |                |               |
|---------------|----------------|---------------|
| 课程名称：计算机网络与编程 | 年级：22级         | 上机实践成绩：       |
| 指导教师：张召       | 姓名：朱天祥         |               |
| 上机实践名称：IP协议分析 | 学号：10225501461 | 上机实践日期：23/6/9 |
| 上机实践编号：No.14  | 组号：            |               |

## 一、目的

快速简单了解IP协议，特别是IP数据报

了解IP数据报各字段的含义

研究IP数据的分片方法

## 二、实验内容

使用Wireshark快速了解IP协议

## 三、使用环境

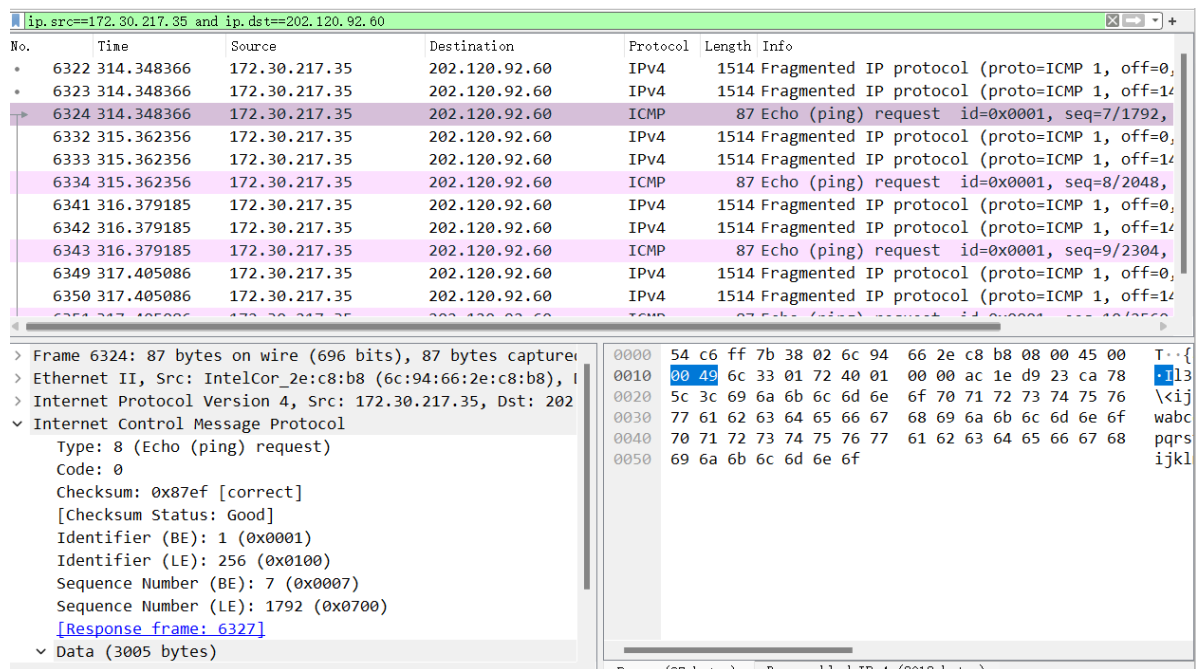
IntelliJ IDEA

JDK 版本: Java 19

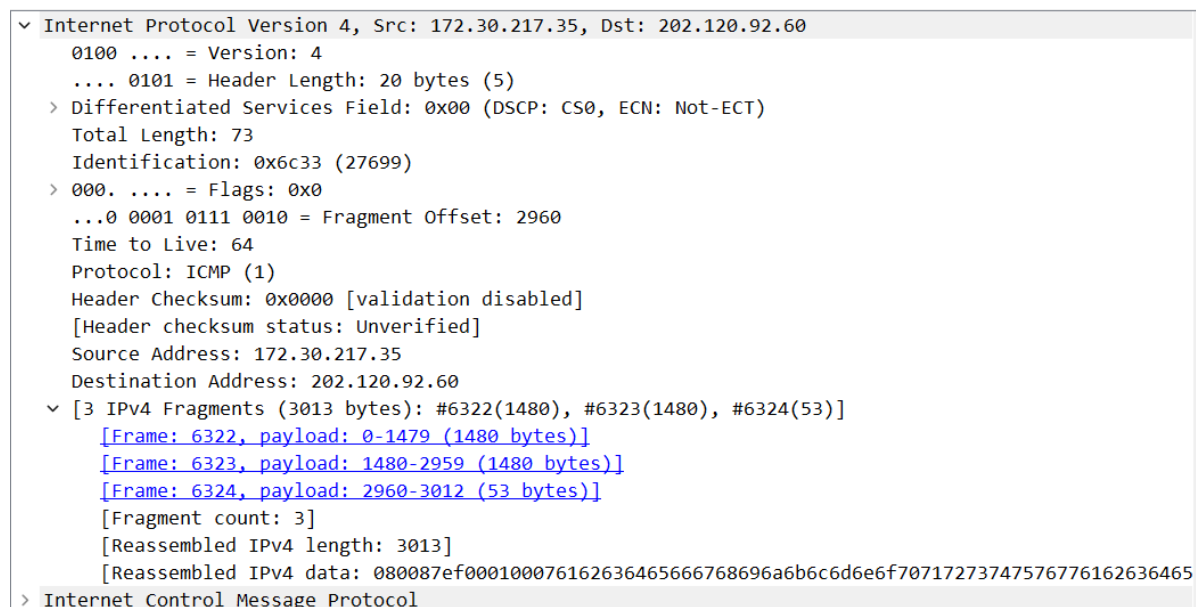
## 四、实验过程

**task1: 任取一个有IP协议的ICMP数据报并根据该报文分析IP协议的报文格式（正确标注每一个部分），请将实验结果附在实验报告中。**

在命令行执行如下命令后利用wireshark后得到如下数据报



我们看到有IPv4协议报文，也有ICMP协议报文，取第三条ICMP报文进行报文结构分析。以下是该ICMP报文的IP首部



1. Version: 4表示ip报文的版本号为4，即IPv4报文。

2. Header Length: 20 bytes表示ip首部的长度为20字节

3. Differentiated Services Field: 0x00为区分服务字段，展开后如下图所示

- 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)

4. Total Length为总长度，上图中总长度为73

5. Identification为标识字段，在该ICMP报文中标识字段值为0x6c33

6. Flags为标志，该报文的flags字段值为0

7. Fragment Offset为片偏移量，值为2960

8. Time to Live为生存时间，值为64

9. Protocol为协议，即ICMP

10. Header Checksum为头部校验和，值为0

11. 接下来是Source Address, 即源ip地址, 为172.30.217.35

12. Destination Address, 即目的ip地址, 为202.120.92.60

**task2: 对截获的报文进行分析, 将属于同一个ICMP请求报文的分片找出来, 并分析其字节长度特点 (如, 每个分片的大小, 片偏移等), 请将实验结果附在实验报告中。**

下图显示task1的第一张图片的完整数据报

| No.  | Time       | Source        | Destination   | Protocol | Length | Info   |
|------|------------|---------------|---------------|----------|--------|--|
| 6322 | 314.348366 | 172.30.217.35 | 202.120.92.60 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=0, I |
| 6323 | 314.348366 | 172.30.217.35 | 202.120.92.60 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=1480 |
| 6324 | 314.348366 | 172.30.217.35 | 202.120.92.60 | ICMP     | 87     | Echo (ping) request id=0x0001, seq=7/1792, tt  |
| 6332 | 315.362356 | 172.30.217.35 | 202.120.92.60 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=0, I |
| 6333 | 315.362356 | 172.30.217.35 | 202.120.92.60 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=1480 |
| 6334 | 315.362356 | 172.30.217.35 | 202.120.92.60 | ICMP     | 87     | Echo (ping) request id=0x0001, seq=8/2048, tt  |
| 6341 | 316.379185 | 172.30.217.35 | 202.120.92.60 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=0, I |
| 6342 | 316.379185 | 172.30.217.35 | 202.120.92.60 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=1480 |
| 6343 | 316.379185 | 172.30.217.35 | 202.120.92.60 | ICMP     | 87     | Echo (ping) request id=0x0001, seq=9/2304, tt  |
| 6349 | 317.405086 | 172.30.217.35 | 202.120.92.60 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=0, I |
| 6350 | 317.405086 | 172.30.217.35 | 202.120.92.60 | IPv4     | 1514   | Fragmented IP protocol (proto=ICMP 1, off=1480 |
| 6351 | 317.405086 | 172.30.217.35 | 202.120.92.60 | ICMP     | 87     | Echo (ping) request id=0x0001, seq=10/2560, t  |

我们发现这12个报文可以分成四组, 即连续的IPv4, IPv4, ICMP可以分为一组, 每一组就对应了之前执行的ping -l 3005 [www.ecnu.edu.cn](http://www.ecnu.edu.cn)发送的一组数据, 前两个IPv4的有效负载为1480字节, 如下图所示

```
▼ Data (1480 bytes)
  Data: 080087ef000100076162636465666768696a6b6c6d6e
  [Length: 1480]
```

因此即使我们不看每一组最后的ICMP报文的数据长度也能计算出来它的有效负载应该为 $3005 - 2 * 1480 = 45$ , 事实也是如此

```
▼ [3 IPv4 Fragments (3013 bytes): #6322(1480), #6323(1480), #6324(53)]
  [Frame: 6322, payload: 0-1479 (1480 bytes)]
  [Frame: 6323, payload: 1480-2959 (1480 bytes)]
  [Frame: 6324, payload: 2960-3012 (53 bytes)]
  [Fragment count: 3]
  [Reassembled IPv4 length: 3013]
  [Reassembled IPv4 data: 080087ef000100076162636465666768696a6b6c6d6e6f6g6h6i6j6k6l6m6n6o6p6q6r6s6t6u6v6w6x6y6z6aa6ab6ac6ad6ae6af6ag6ah6ai6aj6ak6al6am6an6ao6ap6aq6ar6as6at6au6av6aw6ax6ay6az6ba6bb6bc6bd6be6bf6bg6bh6bi6bj6bk6bl6bm6bn6bo6bp6bq6br6bs6bt6bu6bv6bw6bx6by6bz6ca6cb6cc6cd6ce6cf6cg6ch6ci6cj6ck6cl6cm6cn6co6cp6cq6cr6cs6ct6cu6cv6cw6cx6cy6cz6da6db6dc6dd6de6df6dg6dh6di6dj6dk6dl6dm6dn6do6dp6dq6dr6ds6dt6du6dv6dw6dx6dy6dz6ea6eb6ec6ed6ee6ef6eg6eh6ei6ej6ek6el6em6en6eo6ep6eq6er6es6et6eu6ev6ew6ex6ey6ez6fa6fb6fc6fd6fe6ff6fg6fh6fi6fj6fk6fl6fm6fn6fo6fp6fq6fr6fs6ft6fu6fv6fw6fx6fy6fz6ga6gb6gc6gd6ge6gf6gg6gh6gi6gj6gk6gl6gm6gn6go6gp6gq6gr6gs6gt6gu6gv6gw6gx6gy6gz6ha6hb6hc6hd6he6hf6hg6hh6hi6hj6hk6hl6hm6hn6ho6hp6hq6hr6hs6ht6hu6hv6hw6hx6hy6hz6ia6ib6ic6id6ie6if6ig6ih6ii6ij6ik6il6im6in6io6ip6iq6ir6is6it6iu6iv6iw6ix6iy6iz6ja6jb6jc6jd6je6jf6jg6jh6ji6jj6jk6jl6jm6jn6jo6jp6jq6jr6js6jt6ju6jv6jw6jx6jy6jz6ka6kb6kc6kd6ke6kf6kg6kh6ki6kj6kk6kl6km6kn6ko6kp6kq6kr6ks6kt6ku6kv6kw6kx6ky6kz6la6lb6lc6ld6le6lf6lg6lh6li6lj6lk6ll6lm6ln6lo6lp6lq6lr6ls6lt6lu6lv6lw6lx6ly6lz6ma6mb6mc6md6me6mf6mg6mh6mi6mj6mk6ml6mm6mn6mo6mp6mq6mr6ms6mt6mu6mv6mw6mx6my6mz6na6nb6nc6nd6ne6nf6ng6nh6ni6nj6nk6nl6nm6nn6no6np6nq6nr6ns6nt6nu6nv6nw6nx6ny6nz6oa6ob6oc6od6oe6of6og6oh6oi6oj6ok6ol6om6on6oo6op6oq6or6os6ot6ou6ov6ow6ox6oy6oz6pa6pb6pc6pd6pe6pf6pg6ph6pi6pj6pk6pl6pm6pn6po6pp6pq6pr6ps6pt6pu6pv6pw6px6py6pz6qa6qb6qc6qd6qe6qf6qg6qh6qi6qj6qk6ql6qm6qn6qo6qp6qq6qr6qs6qt6qu6qv6qw6qx6qy6qz6ra6rb6rc6rd6re6rf6rg6rh6ri6rj6rk6rl6rm6rn6ro6rp6rq6rr6rs6rt6ru6rv6rw6rx6ry6rz6sa6sb6sc6sd6se6sf6sg6sh6si6sj6sk6sl6sm6sn6so6sp6sq6sr6ss6st6su6sv6sw6sx6sy6sz6ta6tb6tc6td6te6tf6tg6th6ti6tj6tk6tl6tm6tn6to6tp6tq6tr6ts6tt6tu6tv6tw6tx6ty6tz6ua6ub6uc6ud6ue6uf6ug6uh6ui6uj6uk6ul6um6un6uo6up6uq6ur6us6ut6uu6uv6uw6ux6uy6uz6va6vb6vc6vd6ve6vf6vg6vh6vi6vj6vk6vl6vm6vn6vo6vp6vq6vr6vs6vt6vu6vv6vw6vx6vy6vz6wa6wb6wc6wd6we6wf6wg6wh6wi6wj6wk6wl6wm6wn6wo6wp6wq6wr6ws6wt6wu6wv6ww6wx6wy6wz6xa6xb6xc6xd6xe6xf6xg6xh6xi6xj6xk6xl6xm6xn6xo6xp6xq6xr6xs6xt6xu6xv6xw6xx6xy6xz6ya6yb6yc6yd6ye6yf6yg6yh6yi6yj6yk6yl6ym6yn6yo6yp6yq6yr6ys6yt6yu6yv6yw6yx6yy6yz6za6zb6zc6zd6ze6zf6zg6zh6zi6zj6zk6zl6zm6zn6zo6zp6zq6zr6zs6zt6zu6zv6zw6zx6zy6zz]
```

我们看到第三个片段的payload是53, 好像比45还多了8个字节, 这8个字节应该是ICMP首部。

那么自然的就可以推测出每组的第一个IPv4报文偏移量应该是0, 第二个IPv4报文偏移量应该是1480, 第三个ICMP报文偏移量应该是 $2 * 1480 = 2960$ , 我们看到每组中的这些报文的偏移量信息确实是如此

```
...0 0000 0000 0000 = Fragment Offset: 0
...0 0000 1011 1001 = Fragment Offset: 1480
Time to live: 64
...0 0001 0111 0010 = Fragment Offset: 2960
```

ping发送的每一组3005字节的数据为了遵循以太网1500字节这一最大ip报文长度, 将3005字节的数据需要拆成好几份 $1500 - 20(\text{ip首部长}) = 1480$ 字节的数据, 设总共需要拆成n份数据报, 那么前n-1份加上20字节ip首部后成为1500字节的ip报文, 最后一份除了需要加20字节的ip首部, 还要加8字节的ICMP首部, 最后3005字节数据被拆成三份进行传输。

## 五、实验总结

### IP协议结构如下：

版本号 (Version)：占4位，表示该报文的版本，IPv4为4，IPv6为6。

首部长度 (Header Length)：占4位，表示该报文首部的长度，最小值为20字节。

区分服务 (Differentiated Services)：占8位，用于标识该数据包的服务类型。

总长度 (Total Length)：占16位，表示该报文的总长度，包括首部和数据。

标识 (Identification)：占16位，用于标识数据包的唯一性。

标志 (Flags)：占3位，其中一位为0，另外两位用于数据报分片（不分片、后续分片、首个分片）。

分片偏移量 (Fragment Offset)：占13位，表示数据报分片的位置。

生存时间 (Time to Live)：占8位，表示数据报在网络中传输的最大跳数。

协议 (Protocol)：占8位，表示该报文数据部分使用的协议类型，如TCP、UDP或ICMP等。

首部校验和 (Header Checksum)：占16位，用于确保IP首部是否在传输过程中被修改。

源地址 (Source Address)：占32位，表示数据包发送方的IP地址。

目标地址 (Destination Address)：占32位，表示数据包接收方的IP地址。

选项 (Options)：占可变长度，包括记录路由、时间戳等信息。

**当一个数据包超过MTU后，需要将其分片成多个IP数据报进行传输，每个IP数据报都包含其原始数据的一部分。**

每个分片除了最后一个分片外，都需要设置MF (More Fragments) 标志为1，表示该分片不是最后一个分片。

每个分片除了最后一个分片外，需要设置分片偏移量字段表示该分片的位置，每个分片偏移量必须是8字节的倍数。

最后一个分片的MF标志必须设置为0，表示这是最后一个分片。

每个分片必须保留原始IP数据报的一定头部，例如，源地址、目标地址、协议类型和标识等，以便接收方重组分片。

分片后，每个IP分片除了IP首部信息外，还包含一个分片首部，包括偏移量、MF标志和分片长度等信息。最后，接收方会将分片进行重组，以恢复原始的数据包。