华东师范大学数据科学与工程学院实验报告

课程名称：计算机网络与编程	**年级：**2021 级	**上机实践成绩：**
指导教师：张召	**姓名：**彭一珅	**学号：**10215501412
上机实践名称：IP 协议分析		**上机实践日期：**2023.6.9
上机实践编号：14	**组号：**	**上机实践时间：**9:50

一、 实验目的

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、 实验任务

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。

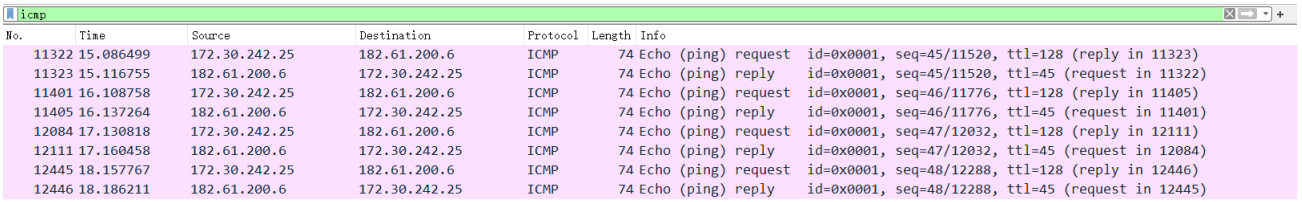
使用 ping 指令向百度服务器交换数据包：

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

正在 Ping www.a.shifen.com [182.61.200.6] 具有 32 字节的数据:
来自 182.61.200.6 的回复: 字节=32 时间=30ms TTL=45
来自 182.61.200.6 的回复: 字节=32 时间=28ms TTL=45
来自 182.61.200.6 的回复: 字节=32 时间=29ms TTL=45
来自 182.61.200.6 的回复: 字节=32 时间=28ms TTL=45

182.61.200.6 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 = 28ms, 最长 = 30ms, 平均 = 28ms
```

捕获如图这些数据报



icmp

No.	Time	Source	Destination	Protocol	Length	Info
11322	15.086499	172.30.242.25	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 11323)
11323	15.116755	182.61.200.6	172.30.242.25	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=45 (request in 11322)
11401	16.108758	172.30.242.25	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 11405)
11405	16.137264	182.61.200.6	172.30.242.25	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=45 (request in 11401)
12084	17.130818	172.30.242.25	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (reply in 12111)
12111	17.160458	182.61.200.6	172.30.242.25	ICMP	74	Echo (ping) reply id=0x0001, seq=47/12032, ttl=45 (request in 12084)
12445	18.157767	172.30.242.25	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (reply in 12446)
12446	18.186211	182.61.200.6	172.30.242.25	ICMP	74	Echo (ping) reply id=0x0001, seq=48/12288, ttl=45 (request in 12445)

以下是一个从我的主机发送给百度服务器的数据包：

```
Internet Protocol Version 4, Src: 172.30.242.25, Dst: 182.61.200.6
  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: 60
  Identification: 0xe68c (59020)
  000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.30.242.25
  Destination Address: 182.61.200.6
```

根据捕获的 ICMP 数据报，IP 协议的报文格式如下：

版本号：4

首部长度：20 字节

服务类型：0x00

总长度：60 字节

标识号(唯一的标识主机发送的报文。如果 IP 协议报文被分包(分片)了，那么每一个包(片)里面的这个 id 都是相同的。)：0xe68c

标志位：0x0

片偏移：0

生存时间：128

协议：ICMP (0x01)

校验和：0x0000

源地址：172.30.242.25

目的地址：182.61.200.6

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。

尝试 ping 更长的数据包，如 3005 字节：

```
C:\Users\tuzi>ping -n 6 -l 3005 www.ecnu.edu.cn

正在 Ping www.ecnu.edu.cn [202.120.92.60] 具有 3005 字节的数据:
来自 202.120.92.60 的回复: 字节=3005 时间=3ms TTL=123
来自 202.120.92.60 的回复: 字节=3005 时间=4ms TTL=123
来自 202.120.92.60 的回复: 字节=3005 时间=6ms TTL=123
来自 202.120.92.60 的回复: 字节=3005 时间=6ms TTL=123
来自 202.120.92.60 的回复: 字节=3005 时间=6ms TTL=123
来自 202.120.92.60 的回复: 字节=3005 时间=5ms TTL=123

202.120.92.60 的 Ping 统计信息:
    数据包: 已发送 = 6, 已接收 = 6, 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 = 6ms, 平均 = 5ms
```

```
[3 IPv4 Fragments (3013 bytes): #667(1480), #668(1480), #669(53)]
    [Frame: 667, payload: 0-1479 (1480 bytes)]
    [Frame: 668, payload: 1480-2959 (1480 bytes)]
    [Frame: 669, payload: 2960-3012 (53 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 3013]
    [Reassembled IPv4 data: 0800879f000100576162636465666768696a6b6c6d6e6f707172737475767761626364 65…]
```

根据上述内容，可以看出捕获的数据包被分成了 3 个分片，分别是#670、#672 和#671。这个 IP 数据报的原始大小为 3013 字节，因此需要进行分片传输。第一个分片#670 的 payload 是 0-1479（1480 字节），第二个分片#672 的 payload 是 1480-2959（1480 字节），第三个分片#671 的 payload 是 2960-3012（53 字节）。分片数量为 3，经过重组后的 IPv4 数据报长度为 3013 字节，重组后的 IPv4 数据为很长的一串 16 进制字符，表示数据报的具体内容。

五、总结

本次实验通过使用 Wireshark 软件，实践了课程中学到的 IP 协议，并研究了 IP 数据报的分片方法。我了解到，当一个 IP 数据包超过物理网络的最大传输单元（MTU）时，就需要将该包进行分片发送。每个分片都有一个 IP 报文头，除分片偏移、MF 标志位和校验字段不同外，其他都一样。为了测试分片功能，我使用 ICMP 包进行测试，并捕获了属于同一个 ICMP 请求报文的两个分片，它们的片偏移都是 0，大小都是 1480 字节。实验中还学习了如何使用 ping 命令来指定发送包的大小和次数，以及如何捕获 IP 数据报。通过本次实验，我更深入地了解了 IP 协议的工作原理。