Week 14: IP协议分析

一、实验目的

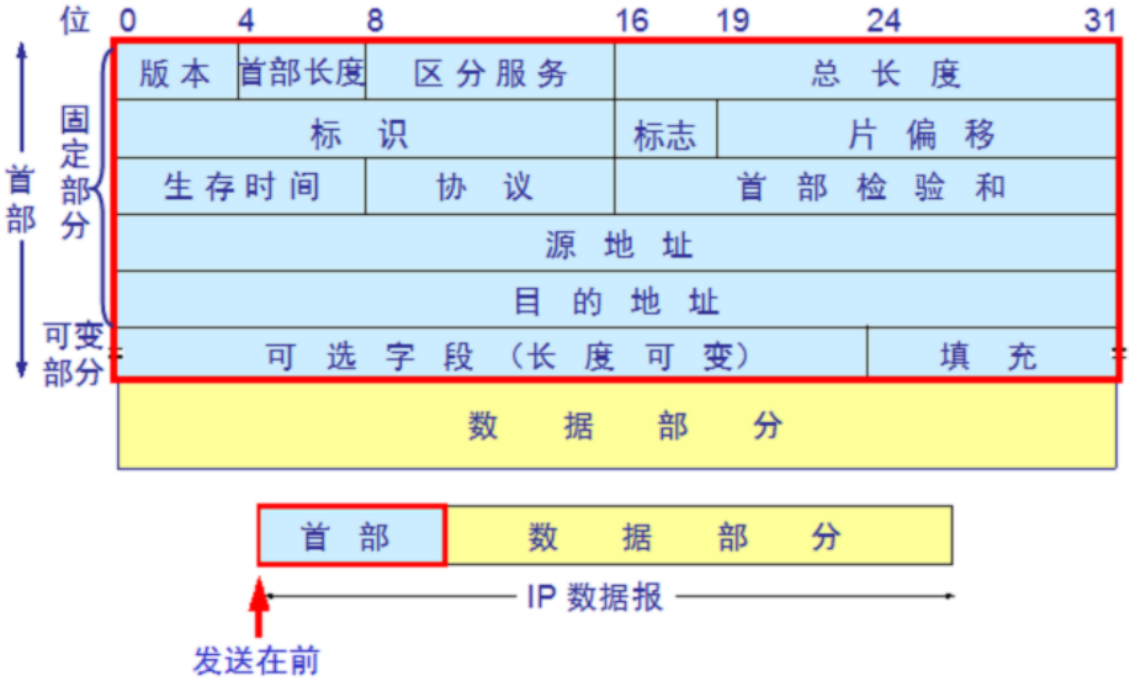
- 快速简单了解IP协议，特别是IP数据报
- 了解IP数据报各字段的含义
- 研究IP数据的分片方法

二、实验任务

- 使用Wireshark快速了解IP协议

三、实验过程

3.1 IP报文格式



- IP报文要交给数据链路层封装后才能发送，理想情况下，每个IP报文正好能放在同一个物理帧中发送。如果一个数据包超过1500字节（以太网的帧中最多可容纳1500字节的数据），就需要将该包进行分片发送，这个上限被称为物理网络的最大传输单元（MTU，Maxium Transfer Unit）。
- TCP/IP协议在发送IP数据报文时，一般选择一个合适的初始长度。当这个报文要从一个MTU大的子网发送一个MTU小的网络时，IP协议就报这个报文的数据部分分割成能被目的子网所容纳的较小数据分片，组成较小的报文发送。每个较小的报文被称为一个分片（fragment）。每个分片都有一个IP报文头，分片后的数据报的IP报头和原始IP报头除分片偏移、MF标志位和校验字段不同外，其他都一样。
- 下面通过使用ICMP包，来产生IP分片数据包。使用ICMP包进行测试时，如果不指定包的大小，可能无法看到分片的数据包。由于IP首部占用20个字节，ICMP首部占8个字节，所以捕获ICMP包大小最大为1472字节。但是一般情况下，ping命令默认的大小都不会超过1472。这样，发送的ICMP包就可以顺利通过，不需要经过分片后再传输。如果想捕获到IP分片的包，需要指定发送的ICMP包

必须大于1472字节。

- 可通过下方命令指定发送包的大小，如：ping -l 3005 www.ecnu.edu.cn

```
C:\Users\13219>ping -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=4ms 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=4ms TTL=123
来自 202.120.92.60 的回复: 字节=3005 时间=18ms TTL=123

202.120.92.60 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 = 4ms, 最长 = 18ms, 平均 = 7ms
```

3.2 抓取IP数据报

启动wireshark，使用ping指令生成IP数据包

Linux下ping包的默认大小为64byte，次数不限。但有时我们需要尝试ping大数据包，来测试网络的状况，这时就要指定ping包的大小了。

- Linux下ping（vxworks基本上和Linux的一样）大数据包的格式；

  语法：ping [-dfnqrRv] [-c<完成次数>] [-i<间隔秒数>] [-I<网络界面>] [-l<前置载入>] [-p<范本样式>] [-s<数据包大小>] [-t<存活数值>] [主机名称或IP地址]

  例如：①指定数据包大小为1500Byte：ping -s 1500 ip; ②指定次数为4次，数据包大小为32767Byte：ping -c 4 -s 32767 ip

- Windows下默认ping包次数为4次，ping包大小为32Byte：

  例如：①指定ping包大小为1500Byte：ping -l 1500 ip; ②指定次数为6次，ping包大小为1500：ping -n 6 -l 1500 ip

```
C:\Users\13219>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=4ms TTL=123
来自 202.120.92.60 的回复: 字节=3005 时间=5ms TTL=123
来自 202.120.92.60 的回复: 字节=3005 时间=5ms 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=4ms TTL=123
来自 202.120.92.60 的回复: 字节=3005 时间=4ms 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 = 4ms, 最长 = 5ms, 平均 = 4ms
```

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。

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。