山东建筑大学　　计算机学院
班级：软件 161　　姓名：黄良运　　学号：201611104033　　课程：

# 实验五　IPv4 协议分析

## 一、 实验目的及任务

1、熟悉 IP 协议的基本原理
2、利用 Wireshark 对 IP 进行协议分析

## 二、 实验环境

与 Internet 连接的计算机网络系统；操作系统为 windows；Wireshark、IE 等软件。

## 三、 实验报告内容

**在实验的基础上，回答以下问题：**

1． 源节点的 IP 地址是什么？

答：10.216.37.93

2． 检查 IP 数据报头部。高层协议(protocol) 字段的值是多少？

答：Protocol：ICMP（0x01）

3．IP 数据报的头部长度是多少字节？数据报中携带的有效载荷(payload)是多少字节？解释如何获得有效载荷长度。

答：20 bytes ; 36 bytes ; 总长度减去 IP 首部长度。

4．该数据包是否被分片？解释你是如何确定该数据报是否被分片的。

答：没有，Flags 中，More fragment 为 0 说明后面没有片段。

5．按循序选择源节点发送的 ICMP Echo Request 消息过程中，两个相邻的 IP 数据报头部哪些字段的值总是变化？

答：Identification (标识)，Header checksum (头部校验和)

6．接上题。IP 数据报中哪些字段的值总是保持不变？哪些字段的值必须保持不变？哪些字段的值必须变化？

答：

必须改变：Identification (标识)，Header checksum (头部校验和)

必须保持不变：Version (版本) ，Header length (头部长度) ，Differentiated Services Field (区分服务) , Flag (标记) , Fragment offset (片偏移) , Protocol (协议)

7．接上题。描述一下 IP 数据报中的 Identification 字段值变化的模式(规律)。

答：11650

8．找到第一跳路由器向源节点发送的第一个 ICMP TTL-Exceeded 消息。IP 数据报头部的 Identification 字段和 TTL 字段的值各是多少？

答：Identification: 0xe94d (59725) , TTL:255

9．在第一跳路由器向源节点发送的一系列 ICMP TTL-Exceeded 消息中，IP 数据报头部的 Identification 字段的值是否不同？为什么？

答：是。

10．找到在 pingplotter 中将 Packet Size 改为 2000 字节后源节点发送的第一个 ICMP Echo Request 消息。这个消息是否已经被分成了多个片？分成了几片？[注意：如果计算机中安装的是 Ethernet 网卡，长度为 2000 字节的数据报应该导致被分片[1]，应为 Ethernet 链路的 MTU 为 1500 字节]

答：是.

11．将数据报的第一片打印输出。IP 数据报头部的什么字段指示该数据报已经被分片？数据报头部的什么字段指示该片是第一片，或是最后一片？分片前数据报的长度是多少字节？

答：没有。

【1】.从 http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip 下载的跟踪数据[ip-ethereal-trace-1]中，所有数据报的长度均小于等于 1500 字节。这是因为收集跟踪数据的计算机中安装的是 Ethernet 网卡，它限制了数据报的最大长度为 1500 字节，包括 40 字节的 TCP/IP 头部以及 1460 字节的应用层消息。因为 Ethernet 链路的 MTU 为 1500 字节，故 Ethernet 网络中 IP 数据报的最大长度为 1500 字节。如果使用 Ethernet 网卡捕获分组，且分组的长度大于 1500 字节，Wireshark 将报告 IP 数据报长度错误。但是，Wireshark 可能只显示一个大的 IP 数据报，而不是多个较小的数据报。导致这种不一致现象的原因是 Ethernet 网卡和 Wireshark 的交互。因此，建议本实验使用从上述地址下载的跟踪数据 ip-ethereal-trace-1。

12. 将第二片数据报打印输出。IP 数据报头部的什么字段指示该片不是第一片？还有其他片吗？请解释。

答：Fragment offset：1480 ，说明不是第一片；More fragment 为 0，说明没有更多片段。

13. 第一片和第二篇数据报头部的什么字段值发生了变化？

答：Total length ，Flags 中的 More fragment，Fragment offset，Header checksum 改变了，Identification 没改变。

14。原始数据报被分成了几片？

答：3 片，0,1480,2960。

15. 在原始数据报分成的多个片中，数据报(分片后)头部的哪些字段值发生了变化？

答：片偏移，总长度，标志，首部校验和。