**实验7 ICMP协议分组结构**

**实验目的：**

掌握网络层ICMP协议。

**实验内容：**

1. 在命令提示符中，利用ipconfig /all查看自己主机的ip及MAC地址，查看自己的网关ip地址并记录，方法同实验1。
2. 运行wireshark抓包分析工具，在命令提示符输入”ping 网关地址”， 然后输入“ping 125.88.254.3 -i 4”过一段时间后停止捕获，观察捕获到的数据包。
3. 在过滤栏中，设置过滤条件过滤本机ip地址发出和接受的ICMP数据包，找到ICMP echo request与reply及TTL过期的数据包，查看捕获数据包的ICMP协议分组结构，并记录下表，其中报头内后四个字节的内容请根据实际捕获数据包填写（注意LE：little-endian与BE：big-endian大小端的数据存储模式）。

ICMP echo request:

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 校验和 | |
|  |  |  | |
|  |  |  |  |
|  |  |  |  |

ICMP echo reply:

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 校验和 | |
|  |  |  | |
|  |  |  |  |
|  |  |  |  |

TTL exceeded:

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 校验和 | |
|  |  |  | |
|  |  |  |  |
|  |  |  |  |

根据捕获的数据包信息思考并回答以下问题：

1. ICMP echo request与reply以及TTL exceeded三个报文的类型与代码字段分别是多少？请查阅相关资料了解这两个字段可能的取值与含义。
2. 在这三个报文中，报头的后四个字节分别是什么内容？表示什么含义？
3. 对比ICMP echo request与reply报文的数据部分，请问是否一样？说明echo请求时发送方与接受方的操作。
4. 仔细观察TTL exceeded报文的ICMP数据部分，请问该数据部分包括了哪些部分？为什么这样？
5. 思考：请根据今天实验的所有实验结果
6. 说明ICMP的触发机制是什么？
7. 尝试捕获其他类型的ICMP报文。
8. 当IP数据包传输出错时ICMP协议如何封装差错报文？