

# 实验一 常用网络命令及 WireShark 使用

## 1、实验目的

- 掌握常用网络命令的使用方法
- 熟悉和掌握网络管理、网络维护的基本内容和方法
- 了解 WireShark 的使用方法和基本特点，掌握使用 WireShark 分析协议的方法

## 2、实验前的准备

- 熟悉各种网络命令
- 了解 WireShark 的功能和工作原理

## 3、实验内容

- 运行网络的基本命令，体会学习使用方法和相应的参数
- 使用 WireShark 抓取数据包：
  - 使用 ping 命令，抓取 ping www.baidu.com 后的数据包进行分析。写出源 ip 地址、目的 ip 地址、IP 标识、总长度、TTL 值这几项
  - 通过筛选得到 arp 数据包，分析某个 arp 数据包的硬件类型、协议类型、发送源 ip 地址、发送源 MAC 地址、目的主机 ip 地址、目的 MAC 地址
  - tracert 跟踪百度，捕捉 tracert 使用的 icmp 报文，显示该数据包的 TTL 域
  - 对 TCP 三次握手、四次挥手过程进行抓包分析，并通过抓取的包进行握手与挥手过程，通过截图体现传输内容。写出某 TCP 数据包的源 ip 地址、目的 ip 地址、源端口、目的端口、窗口大小，以及三次握手和四次挥手中 SYN、ACK、seq 和 ack 等值

## 4、实验查验

- 参考 ppt 中内容进行实验，在实验课上简单阐述实验原理
- 完成电子版实验报告【命名格式：学号-姓名-AdvancedNetLab1】，并上传提交
- 报告提交截止时间为：10 月 31 日 0 点
- 严禁相互抄袭，如发现雷同，实验成绩计 0 分