实验3：ICMP协议分析
2学时 | 验证性

- **实验目的**
  - 了解ICMP报文结构和类型
  - 熟悉ICMP协议的作用
  - 掌握PING和TRACERTOUTE的工作原理
- **实验任务**
  - 完成ICMP报文结构的分析
  - 完成ICMP报文类型的分析
  - 完成PING通信分析
  - 完成TRACEROUTE通信分析
- **实验概览**
  - ICMP协议分析
    - ICMP报文结构
      - 首部
        - 类型
        - 代码
        - 校验和
        - 标识符
        - 序列号
      - 数据段
    - ICMP报文类型
      - 差错报告报文
        - 终点不可达
        - 源点抑制
        - 时间超过
        - 参数问题
        - 改变路由
      - 询问报文
        - 回送请求和回答
        - 时间戳请求和回答
  - PING通信分析
    - PING通信过程
      - PING使用的是ICMP
      - PING通信时的报文结构
      - PING域名地址时的通信过程
    - PING应用
  - TRACEROUTE通信分析
    - Traceroute原理
      - 利用ICMP差错报告报文中的时间超时
    - Tracetoute应用
      - 侦测主机到目的主机之间所经路由情况
- **实验步骤**
  - 任务01：分析ICMP报文结构
    - 步骤01：获取ICMP报文
    - 步骤02：查看ICMP报文结构
    - 步骤03：分析ICMP报文结构
  - 任务02：基于PING分析ICMP响应结果
    - 步骤01：使用主机Host-8对NET-A网络进行通信测试
    - 步骤02：在主机Host-1运行正常的情况下，使用主机Host-8 Ping 主机Host-1
    - 步骤03：在主机Host-2关机的情况下，使用主机Host-8 Ping 主机Host-2
    - 步骤04：在主机Host-3网关配置错误的情况下，使用主机Host-8 Ping 主机Host-3
    - 步骤05：使用主机Host-8 Ping Net-A部分中可配置未使用的任一IP地址
    - 步骤06：使用主机Host-8 Ping 不属于Net-A或Net-B的任一IP地址
  - 任务03：基于TRACEROUTE分析ICMP通信过程
    - 步骤01：设置抓包点，启动Wireshark进行抓包
    - 步骤02：使用Host-8对主机Host-1进行Traceroute路由测试
    - 步骤03：对抓包点1的ICMP报文进行分析
    - 步骤04：对抓包点2的ICMP报文进行分析
    - 步骤05：对抓包点3的ICMP报文进行分析
    - 步骤06：对抓包点4的ICMP报文进行分析
    - 步骤07：对抓包点5的ICMP报文进行分析
    - 步骤08：分析相邻抓包点间的报文异同，并分析Traceroute工作原理
- **实验考核**
  - 实验随堂查
    - 考核点1：完成ICMP报文结构的分析
    - 考核点2：完成ICMP报文类型的分析
    - 考核点3：完成PING通信分析
    - 考核点4：完成TRACEROUTE通信分析
  - 实验线上考
    - 本实验线上考共10题，其中单选3题、多选2题、判断3题、填空2题

Presented with xmind