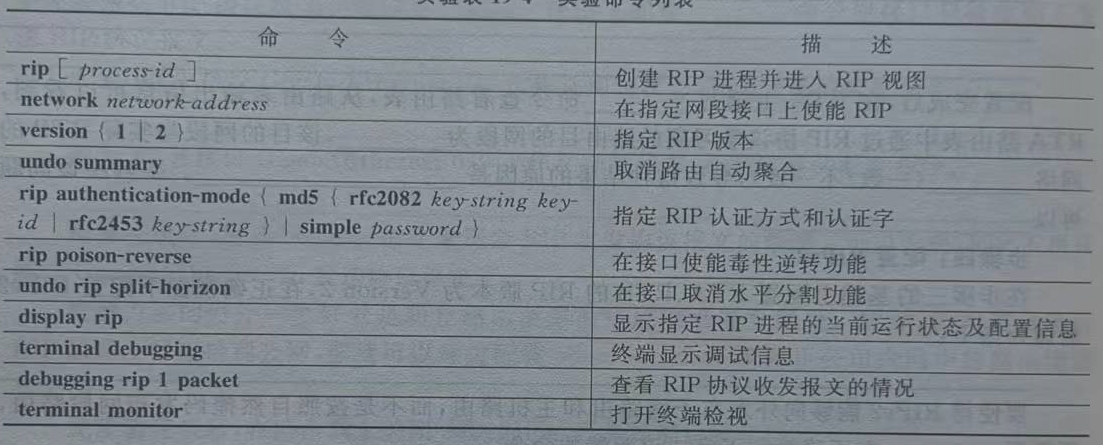
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名： | | 学号： | 专业年级：软件工程2020 | 班级： 卓越班 |
| 分组： | | 实验室： | 指导教师：郭念 | 实验日期：2022.06.09 |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **计算机网络与安全** | | |
| **实验名称** | **实验七 UDP和TCP协议分析** | | |
| **实验目的** | 1. 掌握常见网络协议数据包的结构和首部字段。 2. 理解MAC地址、IP地址和端口号在网络通信中的作用。 3. 掌握TCP、UDP协议的报文格式 4. 理解 TCP 的工作过程，掌握 TCP 工作原理与实现。 | | |
| **实验内容** | 启动 Wireshark，捕捉网络活动中的报文并按要求分析。   1. 分析Ethernet II帧结构。 2. 分析IP数据报的报文格式。 3. 分析ICMP数据报的报文格式。 4. 分析ARP报文格式分析。 5. 分析TCP报文段格式。 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | 1. TCP连接管理 | | |
| **实验环境** | 运行Windows 操作系统PC机， 在本地连接-属性对话框，去掉IPv6设置，如下图所示： | | |
| **实验的实施阶段** | **实验步骤及实验结果** | **1、捕获并分析以太帧。**  1.1删除浏览器中的历史记录。  1.2启动Wireshark进行抓包，开始分组捕获。  1.3在命令行窗口ping：192.168.1.200  1.4停止抓包，对抓取的数据进行分析，在 Wireshark 监视器中设置过滤条件。例如图1.2–3设置过滤条件为 icmp，则显 示出所捕获的 ICMP 数据包。  选取以太网帧进行分析，可以看到该帧的到达时间，帧编号，帧长度，帧的长度等等。  1.5 分析以太帧结构  **抓包截图：**  057a48d43bdb47845c39695bf763931  结果分析   1. 源地址是： 78:eb:14:6e:92:28   (2) 目的 MAC 地址为30:c9:ab:46:c6:8b ，它（不是）Web服务器的MAC地址？若不是，它是\_\_\_\_本机\_\_\_\_\_\_\_ 的MAC地址。  (3) 类型字段是：\_\_\_0x0800\_\_\_\_\_\_ 包含\_\_IPv4 \_\_\_。 例如，以太类型值为 0x0800 指示了该帧包含了 IPv4 数据报，0x0806 表明指示了该帧包含了 ARP 帧， 0x8100 指示了该帧包含了 IEEE 802.1Q 帧。  **2、捕获并分析IP数据包。**  点击 Internet Protocol Version 4 展开（如图1.2–4），查看 IP 数据报，特别观察 IP 数据报的首部字段ࣿ其内容。  **抓包截图：**  057a48d43bdb47845c39695bf763931    **结果分析：**  版本号：4  首部长度：20 bytes  总长度：60  标识：0x5b10  标志位：0x00  片偏移：20 bytes  生存时间(TTL) 协议：ICMP  首部校验和：0xc3c7  源IP地址：101.87.62.129  目的IP地址：192.168.1.105  **3、分析ICMP报文**  点击 Internet Control Message Protocol 展开，查看 ICMP 报文，并解释回显（Echo Request 和 Echo Reply）报文的首部字段。  **抓包截图：**  057a48d43bdb47845c39695bf763931    **结果分析：**  Type：3  Code：3  **4、ARP 协议分析**  使用arp -d 命令，清空本机的 ARP 缓存，清空抓捕记录后重启抓包， ping 本机的同网段地址，停止抓包。在显示过滤器条框中输入“arp”，观察捕获的 ARP 报 文的各个字段，分析请求/响应的过程。    **抓包截图：**    分别指出请求报文和响应报文。  请求报文：其中1、2帧等是请求报文  响应报文：3帧等是响应报文  **5、TCP报文段分析**  5.1 启动Wireshark进行抓包，ftp连接192.168.1.200，并用stu登录，上传文件，然后关闭ftp连接窗口，停止抓包，在显示过滤器条框中输入“tcp”，观察捕获的 TCP报文段的各个字段，分析请求/响应的过程。  5.2 观察 TCP 三次握手与四次挥手报文，注意报文收发过程中，观察 TCP 状态的变化。  5.3 选择其中一个 TCP 报文，配合 Wireshark 截图，分 析该报文 TCP 首部各字段的定义、值ࣿ含义。  **抓包截图：**        结果分析：  tcp报文由tcp header和tcp数据组成。tcp header 的最大长度为60字节，而必须要有的固定长度也就是图一的前5层的20字节，每层占有32bit，也就是32/8=4字节，5层，5\*4 = 20字节，那么第六层的可选项和填充也就是Tcp Options字段最大为60-20=40字节。填充是为了使TCP首部为4字节（32bit）的整数倍。  图中一个tcp报头的详细信息，其中的1011........Header Length = 44字节（11），即11\*4 = 44，下面有header的所有数据，两行共计44字节。  源 端 口 ：443  目 的 端 口：3424  序 号：9017  确认号：5929  窗 口 校 验 和：0xfeb3 | | |
| **Echo (ping) request id=0xca2b, seq=1906/29191, ttl=64 (reply in 884)实验结果的处理阶段** | **实验结果的分析与总结** | 分析与总结：  本次的实验任务已完成，在本次试验中，我通过Wireshark软件进行抓包，并对一些MAC地址、IP地址进行分析。通过本次实验，我根据自己所学知识分析了常见网络协议数据包的结构和首部字段，并通过实践观察、理解了MAC地址、IP地址和端口号在网络通信中的作用，也掌握TCP、UDP协议的报文格式，理解了 TCP 的工作过程，掌握 TCP 工作原理与实现。虽然在实验过程中也遇到了一些困难与错误，通过向同学咨询、上网查询等方式，终于将遇到的问题解决掉，并从错误中学到了相关的知识，增强了自己的动手实践能力。 | | |

**注意：**

1. **实验关键步骤和结果需要截图后粘贴到相应位置，截图要注明学号和姓名。**
2. **提交实验报告时，文档名改为：学号-姓名-实验名称.docx。**

****