实验报告

|  |  |
| --- | --- |
| 实验名称：基本报文分析 | |
| 实验台号：2 | 实验时间：2019年11月17日 |
| 实验小组：第2组  成员及本次实验分工:於文卓 | |
| 实验目的：   1. 理解IP层的作用以及IP地址的分类方法 2. 理解子网的划分和子网掩码的作用 3. 掌握IP数据包的组成和网络层的基本功能 4. 学习使用Wireshark如何对报文作分析 5. 通过Wireshark了解TCP三次握手过程 | |
| 实验环境说明：  笔记本电脑一台(Win10系统)，Wireshark(Version 3.0.3) | |
| 实验过程、步骤（可另附页、使用网络拓扑图等辅助说明）及结果：   1. 原理分析   网际协议 IP 是 TCP/IP 协议栈的心脏，也是网络层中最重要的协议。目前几乎所有的上层网络协议都是基于 IP 协议。在接收数据的时候，网络层接收由数据链路层发送的数据包进行解封装，并把该数据包发送到更高层——传输层，在发送数据的时候，网络层接受由传输层发送的数据包进行 IP 封装，然后把数据报交给下层——数据链路层。  IP 协议处于 TCP/IP 协议栈的网际层，用于管理数据通信中源端和目的端之间的报文传送，是互联网最重要的网际协议。IP 地址是也叫逻辑地址，用于在网络中标识主机。在 IP网络中，主机之间进行通信时使用 IP 地址来指定接收端的主机地址。数据进行封装过程中，IP层负责将数据封装成 IP包，IPv4数据包报文格式如下图所示。     1. Wireshark抓包对应的OSI模型      1. Wireshark抓到的包对应的TCP中的每个字段      1. 实例分析TCP三次握手   首先打开Wireshark，再在浏览器中输入www.hdu.edu.cn 在Wireshark中进行http过滤后，选中GET / HTTP/1.1的那条记录，右键然后点击追踪流🡪TCP流，从而得到与浏览器打开网站相关的数据包    从图中可以看到Wireshark截获了三次握手的三个数据包。第四个包才是HTTP，说明HTTP是使用TCP建立连接的。    第一次握手：  客户端发起一个TCP，标志位为SYN，序列号为0，代表客户端请求连接    第二次握手：  服务器发回确认包，标志位为SYN，ACK，将确认序号设置为客户端的ISN+1    第三次握手  客户端再次发送确认包（ACK），SYN标志位为0，ACK标志位为1，并且把服务器发来ACK的序号字段+1，放在确定字段中发给对方，并且数据字段放些ISN的+1 | |
| 实验总结（遇到的问题及解决办法、体会）：  问题：IP 数据包在从源主机出发到达目的主机的过程中，IP首部中的I源地址和目的地址字段是否发生变化？  回答：没有变化。在数据封装的过程中 是包含协议端口等其他标识应用程序的字段或者协议，以便应用层能够区分，在internet层（OSI中的网络层）完成对IP地址的封装之后数据交到数据链路层 打上帧头 帧尾 之后交下一层进行传输在传输过程中不变化 | |
| 器材、工具领用及归还负责人：於文卓 | 实验记录人：於文卓 |
| 实验执笔人：於文卓 | 报告协助人：於文卓 |
| 小组成员签名：於文卓 | |
| 验收人： | 成绩评定： |