

**实验报告**

**课程名称： 计算机网络原理**

**学生姓名： 朱方灏钧 学号： 210111316**

**年级专业： 19级软件工程 班级： 19.11**

**指导教师： 张毅**

**开课学期： 2021 年— 2022 年 1 学期**

**宜宾学院人工智能与大数据学部实验教学中心**

**宜宾学院人工智能与大数据学部**

**实验报告**

**年级：19级**  **专业：软件工程** **上课日期： 2021**年 12月12日

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **实验名称** | **运输层报头结构** | | | | | |
| **学生姓名** | **朱方灏钧** | **学号** | **210111316** | **实验合作者 姓名** | **无** | |
| **指导教师(签名)** |  | **评 阅 日 期** | |  | **实验报告分** |  |
| **实验报告基本内容：**一、实验目的；二、实验内容；三、实验原理；四、实验步骤及结果；五、实验遇到问题及解决方法；六、实验结论 | | | | | | |
| 1. 实验目的：   1、掌握运输层UDP与TCP协议内容；  2、掌握运输层TCP协议建立连接与释放连接过程。   1. 实验内容：   **一、运输层UDP与TCP的报头结构**   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。   IMG_256   1. 运行wireshark抓包分析工具，做如下操作：1、使用qq与其他同学进行语音或视频通话，2、打开浏览器访问任意网站。过一段时间后停止捕获，观察捕获到的数据包。        1. 在过滤栏中，设置过滤条件过滤从本机ip地址发送和接收的UDP数据包，查看捕获数据包的UDP报头，并记录下表   发送的UDP包报头：   |  |  |  |  | | --- | --- | --- | --- | | 源端口 | 目的端口 | 长度 | 校验和 | | 59446 | 18001 | 154 | 0x4539 |   接收的UDP包报头：   |  |  |  |  | | --- | --- | --- | --- | | 源端口 | 目的端口 | 长度 | 校验和 | | 18001 | 59446 | 91 | 0xabe7 |   根据捕获的数据包信息思考并回答以下问题：   1. 根据发送与接收时不同报头内容分析，qq在语音或视频通话时可能使用了哪个固定端口？哪个临时端口？   答：固定端口有443，临时端口有18001,59446,7882   1. 根据捕获的数据包判断UDP数据包报头内的长度字段是以什么为单位的？   答：是以byte为单位的   1. 校验和计算时包括哪些部分？   答：包括头部和数据两个部分   1. 捕获的数据包是一对一传输的还是一对多的？UDP支持广播么？   答：是一对一传输的，支持广播   1. 在过滤栏中，设置过滤条件过滤从本机ip地址发送和接收的TCP数据包，查看捕获数据包的TCP报头，并记录下表   1   |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 源端口 | | | | | | | | | 目的端口 | | | 7882 | | | | | | | | | 443 | | | 序号 | | | | | | | | | | | | 1 | | | | | | | | | | | | 确认号 | | | | | | | | | | | | 1 | | | | | | | | | | | | 数据偏移 | 保留 | URG | ACK | PSH | RST | SYN | | FIN | | 窗口 | | 20bytes | 000 | 0 | 1 | 0 | 0 | 0 | | 0 | | 516 | | 校验和 | | | | | | | 紧急指针 | | | | | 0x059a | | | | | | | 0 | | | |   根据捕获的数据包信息回答以下问题：   1. 分析TCP报头内的端口与UDP报头内的端口是否是统一的一套端口号？   答：不是统一的一套，UDP是关于QQ语音的端口，TCP是关于浏览器网页的端口   1. 序号的大小是多少？观察连续的多个TCP包，序号有何变化？   答：序号的大小为1，序号在根据TCP的三次握手来回传值变化   1. 确认号是否与同一个数据包里的序号有关系？应该与什么序号有关？   答：下一个确认号和上一个传出来的序号向对应，对应TCP的三次握手   1. 在固定长度首部的情况下，数据偏移的取值是多少？为什么？   答：是数据首部的长度加1，因为数据的第一个字符在数据首部之后   1. 记录根据六个标志位的取值来分析这是一个什么作用的tcp报文？   答：这是一个用于发送连接请求的报文   1. 窗口的取值是多少？窗口值用于什么用途？   答：是516，用于规定单个报文段的最大传输数据大小   1. 紧急指针字段在什么情况下会起作用？有什么作用？   答：但当有时一些应用程序在某些紧急情况下（如在某些连接中进行强制中断）  要求在接收方在没有处理完数据之前就能够发送一些紧急数据  这就使得发送方将CODE字段的URG置为1 即紧急指针字段有效  这样可以不必考虑你发送的紧急数据在数据流中的位置  也就是相当于优先级最高  紧急指针指出的是紧急数据在报文段中结束的位置   1. 思考：请根据今天实验的所有实验结果 2. 分析UDP与TCP协议功能上相同与不同之处？   答：UDP和TCP一样是数据传输协议，UDP是不可靠的，可以多播，TCP是可靠的，只能点对点，需要三次握手   1. 从报头来看，TCP协议除了复用与分用外，还应该有哪些功能？   答：还有传输控制，传输数据，确认报文送达，分配到相应端口等功能   1. 从捕获的报文首部来看，三类端口分别是什么情况下被使用的？   答：是在发送数据，接受数据等情况下呗使用  **TCP的三报文握手与四报文挥手**   1. 运行wireshark抓包分析工具，做如下操作：打开浏览器访问任意网站（使用ping查询该网站的ip地址）然后关闭浏览器。过一段时间后停止捕获，观察捕获到的数据包。        1. 在过滤栏中，设置过滤条件过滤从网站ip地址发出和接收的TCP数据包，找到后使用追踪流的功能，查看捕获数据包的TCP首部结构，并记录下表   三报文握手：   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 第一次握手 | 序号 | 确认号 | SYN标志 | ACK标志 | | 1 | 1 | 1 | 1 | | 第二次握手 | 序号 | 确认号 | SYN标志 | ACK标志 | | 1 | 518 | 1 | 1 | | 第三次握手 | 序号 | 确认号 | SYN标志 | ACK标志 | | 518 | 2921 | 0 | 1 |   四报文挥手：   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 第一次挥手 | 序号 | 确认号 | FIN标志 | ACK标志 | | 1 | 1 | 1 | 0 | | 第二次挥手 | 序号 | 确认号 | FIN标志 | ACK标志 | | 1 | 518 | 0 | 1 | | 第三次挥手 | 序号 | 确认号 | FIN标志 | ACK标志 | | 1 | 518 | 1 | 1 | | 第四次挥手 | 序号 | 确认号 | FIN标志 | ACK标志 | | 518 | 2921 | 0 | 1 |   根据捕获的数据包信息思考并回答以下问题：   1. 三报文握手与四报文挥手中，序号与确认号是如何发生变化的？说明了什么？   答：把序号传到对方主机后，对方主机作为确认号，反之亦然   1. 分析SYN标志位与FIN标志位是如何设置的？说明了什么？   SYN标志表明这是一个TCP连接请求确认报文段，FIN标志表明这是一个TCP连接请求确认报文段   1. 分析三报文握手与四报文挥手过程中，双方是如何建立连接与释放连接的?   答：主机向对方转送建立连接请求，对方收到后就开始建立连接，然后发送已建立的回复请求，再开始传输数据。释放连接也是如此   1. 为什么建立连接是三报文握手而释放连接需要四报文挥手？   答：因为释放连接需要等待主机释放完成后再发送确认报文，这一步多了一个步骤   1. 实验原理：   利用wireshark的软件功能实现   1. 实验步骤及结果 2. 实验遇到问题及解决方法   无   1. 实验结论   通过wireshark的使用，把课堂上学到的理论知识用到了实践中，真正理解了什么是TCP和UDP数据包的知识 | | | | | | |
| **指**  **导**  **教**  **师**  **评**  **语** | | | | | | |