**实验8 运输层**

**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。

**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。
2. 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。
3. 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 |
|  |  |  |  |

接收的UDP包报头：

|  |  |  |  |
| --- | --- | --- | --- |
| 源端口 | 目的端口 | 长度 | 校验和 |
|  |  |  |  |

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？
2. 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？
3. 校验和计算时包括哪些部分？
4. 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？
5. 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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 源端口 | | | | | | | | | 目的端口 | |
|  | | | | | | | | |  | |
| 序号 | | | | | | | | | | |
|  | | | | | | | | | | |
| 确认号 | | | | | | | | | | |
|  | | | | | | | | | | |
| 数据偏移 | 保留 | URG | ACK | PSH | RST | SYN | | FIN | | 窗口 |
|  |  |  |  |  |  |  | |  | |  |
| 校验和 | | | | | | | 紧急指针 | | | |
|  | | | | | | |  | | | |

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？
2. 序号的大小是多少？观察连续的多个TCP包，序号有何变化？
3. 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？
4. 在固定长度首部的情况下，数据偏移的取值是多少？为什么？
5. 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？
6. 窗口的取值是多少？窗口值用于什么用途？
7. 紧急指针字段在什么情况下会起作用？有什么作用？
8. 思考：请根据今天实验的所有实验结果
9. 分析UDP与TCP协议功能上相同与不同之处？
10. 从报头来看，TCP协议除了复用与分用外，还应该有哪些功能？
11. 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？

**二、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。
2. 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 |
|  |  |  |  |
| 第二次握手 | 序号 | 确认号 | SYN标志 | ACK标志 |
|  |  |  |  |
| 第三次握手 | 序号 | 确认号 | SYN标志 | ACK标志 |
|  |  |  |  |

四报文挥手：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 第一次挥手 | 序号 | 确认号 | FIN标志 | ACK标志 |
|  |  |  |  |
| 第二次挥手 | 序号 | 确认号 | FIN标志 | ACK标志 |
|  |  |  |  |
| 第三次挥手 | 序号 | 确认号 | FIN标志 | ACK标志 |
|  |  |  |  |
| 第四次挥手 | 序号 | 确认号 | FIN标志 | ACK标志 |
|  |  |  |  |

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？
2. 分析SYN标志位与FIN标志位是如何设置的？说明了什么？
3. 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?
4. 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？