|  |  |  |  |
| --- | --- | --- | --- |
| **《计算机网络》实验报告** | | | |
| **实验编号** | 实验七 | **实验名称** | TCP |
| **姓名** | 叶俊 | **学号** | 202200201151 |
| **班级** | 菁英班 | **成绩** |  |
| 1. **实验目的**   学习TCP协议是如何工作的,TCP是互联网上使用的主要传输协议 | | | |
| 1. **实验要求**   Wireshark:本实验使用Wireshark软件工具捕获和检测数据包的踪迹。  weget: 这个实验室使用wget（Windows）获取web资源。 | | | |
| 1. **实验内容** 2. Capture a Trace 3. Inspect the Trace 4. TCP Segment Structure 5. TCP Connection Setup/Teardown 6. TCP Data Transfer | | | |
| 1. **实验过程** 2. Step1 Capture a Trace 捕获追踪   数据包信息如下：     1. Step2 Inspect the Trace检查跟踪   选择一个数据包，展开其TCP协议部分：    TCP各字段解释：   1. 端口号范围：0-65535 2. 源端口号：是客户端进程随机生成的，源端口号是发送方（客户端）的端口号，用于标识发送方的进程。 3. 目标端口号：一般是服务器固定的。目标端口号是接收方（服务器）的端口号，用   于标识服务器上的特定服务或应用程序。例如，HTTP服务通常使用端口80。   1. 序列号seq：TCP为每个字节都进行了编号。序列号是TCP报文段中第一个字节的序列号。TCP使用序列号来保证数据的有序传输，并对每个字节进行编号。 2. 确认号ack：确认号是期望从对方收到的下一个TCP报文段的第一个字节的序列号。通过确认号，接收方告诉发送方已经成功接收了哪些数据。 3. 首部长度header length 给出了TCP报头的长度，以32位字（4字节）为单位。这个字段允许TCP头具有可变长度。 4. 标记flags 有多个标志位，包括紧急位、确认位、推送位、复位位、同步位、终止位。 5. SYN：请求建立连接位 6. FIN：请求断开连接位 7. RST：重置位，强制对方断开连接，释放会话 8. PSH：推送位，推送数据到应用层，为1时为有应用层数据 9. ACK：确认位，该位为开关，为1时ack号有效，为0时无效。 10. URG：紧急位，为1时，代表有些字节为紧急数据， 11. 窗口大小：win窗口，用于通知发送方自己的缓存大小。 12. 校验和：校验和字段用于检测TCP头和数据部分的错误。校验范围是首部和数据两部分。 13. Step3: CP Segment Structure TCP段结构   如下图（单位：字节）   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 源端口 | 目的端口 | seq | ack | 头部长度 | 标识位 | 窗口大小 | | 2 | 2 | 4 | 4 | 2 | | 2 |  |  |  |  |  | | --- | --- | --- | --- | | 校验和 | 紧急指针 | 选项 | 载荷 | | 2 | 2 | 12 | 14 |  1. Step4：TCP Connection Setup/Teardown TCP连接建立/释放   过滤器表达式“tcp.flags.syn==1”搜索SYN标志为on的数据包。“SYN数据包”是三方握手的开始。远程服务器应使用设置了SYN和ACK标志的TCP段或“SYN ACK数据包”进行应答。    三次握手的时间序列图:  1735555944912  回答以下问题：   1. 在SYN数据包上，TCP包含了哪些选项字段以供跟踪。   ACK和SYN。  **连接释放**：最后，在下载完成后关闭TCP连接。这通常在FIN 环节中完成。每一方向另一方发送FIN，并确认收到FIN;这类似于三次握手。或者，当一端发送RST (Reset)时，连接可能突然断开。此报文不需要被对方确认。  1735556010017   1. TCP Data Transfer TCP数据传输      1. 当TCP连接正常的时候，下载方向的粗略数据速率(以包/秒或位/秒为单位)是多少？   答：大约是1.3Mbps   1. 内容占下载率的百分比是多少?展示你的计算。   答：整体大小为1466字节，其中TCP载荷大小为1368字节，下载速率中下载内容占93.3%。   1. 由于ACK报文，上传方向的粗略速率(比特/秒)是多少？   答：250bits/s   1. 如果最近从服务器接收到的TCP段的序列号是X，那么下一个传输的TCP段携带的ACK号是什么?   答：如果最近接收到的分段Seq为X，则下次发送包的Ack应为X+对应包的分段长度。 | | | |
| **四．实验心得**  本次实验的主要目标是深入探究TCP（传输控制协议），涵盖了理论知识的学习和实际操作的体验。起初，我通过对TCP原理的深入研究，逐步构建了对这一网络基础协议的全面认识。在理论铺垫之后，我运用了Wireshark这一专业的网络分析软件来捕获和分析TCP数据包。通过对实际传输中的TCP数据包的观察，我掌握了如何截取和分析TCP段，并对每个组成部分的功能和意义有了深入的认识。我特别对TCP段的结构进行了细致的研究，包括各个字段的作用和含义，并通过图表的形式将这些抽象概念具象化，从而加深了对TCP段结构的理解。  接着，我亲自实践了TCP连接的建立与终止过程，重点关注了TCP的三次握手和四次挥手机制。我借助时间序列图对这一过程进行了详尽的分析，这不仅丰富了我的理论知识，也让我对TCP连接的完整生命周期有了更清晰的认识。此外，我还探索了Wireshark的IO图功能，这一功能以直观的方式展示了TCP数据传输的动态过程。通过这种分析，我对TCP在不同场景下的行为和性能特点有了更深入的了解，对网络数据传输的本质有了更深刻的洞察。  总结来说，这次实验不仅增强了我对TCP协议的理论理解，也提高了我在实际操作中使用网络分析工具的技能。通过将理论与实践相结合的学习方式，我更加明确了TCP在现代网络通信中的核心地位，并学会了如何利用网络分析工具来诊断和解决网络问题。这次宝贵的实验经历无疑为我未来在网络技术领域的进一步学习和职业发展打下了坚实的基础。 | | | |