**实验三、传输层TCP协议分析实验报告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 组号： |  |  |  |  |  |
| 姓名： |  | 学号： |  | 班级： |  |
| 姓名： |  | 学号： |  | 班级： |  |
|  |  |  |  |  |  |

1. 实验目的
2. 理解TCP报文首部格式和字段的作用，TCP连接的建立和释放过程，TCP数据传输中的编号与确认的过程。
3. 理解TCP的错误恢复的工作原理和字节流的传输模式，分析错误恢复机制中TCP双方的交互情况。
4. 理解TCP的流量控制的工作原理，分析流量控制中TCP双方的交互情况。
5. 理解TCP的拥塞控制的工作原理，分析拥塞控制中TCP双方的交互情况。
6. 实验内容
7. 使用基于TCP的应用程序（如浏览器下载文件）传输文件，在**客户端和服务器均要捕获TCP报文**。
8. 分析TCP报文首部信息、TCP连接的建立和释放过程、TCP数据的编号与确认机制。观察几个典型的TCP选项：MSS、SACK、Window Scale、Timestamp等，查资料说明其用途。
9. 观察和估计客户机到服务器的RTT，双方各自的MSS，计算丢包率及重传的流量。
10. 观察TCP的流量控制过程，和拥塞控制中的慢启动、快速重传、拥塞避免，快速恢复等过程【观察拥塞控制的难度较大，观察到两个过程即可】。

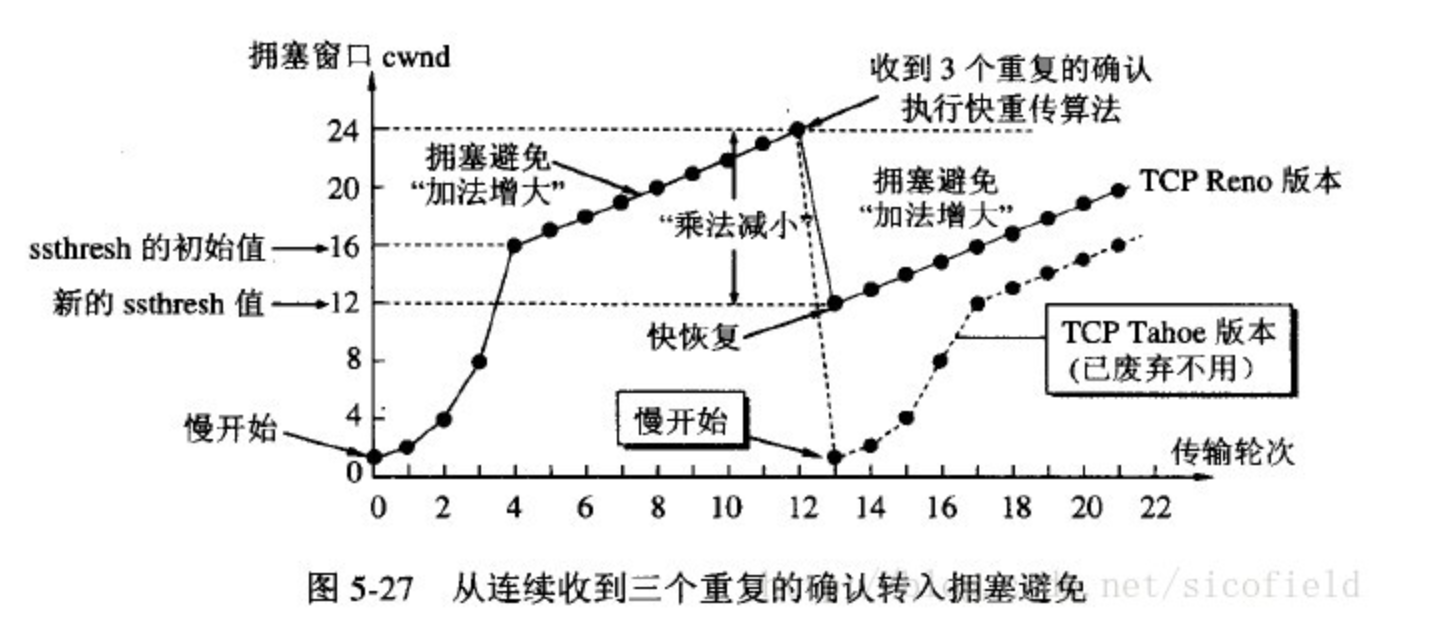


图4-0 典型的TCP 拥塞控制过程图例

1. \*（可选）注意观察初始的cwnd是多少，看看不同的操作系统初始cwnd的差别。观察有没有Delay ACK的应答模式，注意不同操作系统的差异。

【可以增加题目规定以外的分析】

1. 实验环境与分组

1）云服务器一台，启动Apache2服务（或其他服务器程序）。

2）每2名同学一组，各自在电脑上运行客户端程序（浏览器或其他客户端程序）。

3）使用客户端程序下载数据，运行Wireshark软件捕获报文。【注意：可以关闭Wireshark的HTTP协议分析，专注在TCP协议上，关闭方法是：菜单‘分析’—>‘启用的协议’中，取消‘HTTP’的选择。】

1. 实验组网

下图是本实验的组网图，图中参数请根据实际情况标注。



1. 实验过程及结果分析

【过程记录应当详尽，截图并加以说明。以下过程和表格仅供参考。】

步骤1：PC2通过ssh登录到服务器Z上，在云服务器Z上启动合适的服务器程序。

步骤2：在PC1和Z上启动报文捕获软件，开始截获报文【注意加过滤器，比如host w.x.y.z；不熟悉tcpdump的可以用 tcpdump -n -s 500 tcp and host A.B.C.D and port P -w server.pcap选项，把报文记录到文件中，传输到客户端用Wireshark分析。其中A.B.C.D是客户端的**公网地址，P是服务端口，如80**】。

步骤3：在PC1上运行客户端软件，发送和接收一个约500KB的文件。文件传输完成后，停止报文截获。

步骤4：对比观察客户端和服务器截获的报文，分析TCP协议的建立过程的三个报文并填写表3-1。分析TCP连接的释放过程，选择TCP连接撤销的四个报文并填写表3-2。

tcpdump -n -s 500 tcp and port 80 -w server.pcap

表3-1 TCP连接建立过程的三个报文信息【如果有多条，全部列出】

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名称 | 第1条报文 | 第2条报文 | 第3条报文 |
| 报文序号NO. |  |  |  |
| Seq # |  |  |  |
| Ack # |  |  |  |
| ACK Flag |  |  |  |
| SYN Flag |  |  |  |

表3-2 TCP连接撤销的四个报文信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 首条报文 | 二条报文 | 三条报文 | 四条报文 |
| 报文捕获序号NO. |  |  |  |  |
| Seq # |  |  |  |  |
| Ack # |  |  |  |  |
| ACK |  |  |  |  |
| FIN |  |  |  |  |

步骤5：分析TCP数据传送阶段的报文，分析其错误恢复和流量控制机制，并填表。【注：出现明显的流量控制的地方，Wireshark会有[TCP Window Full]标记。如果没有观察到明显的流量控制过程，可以再单独设计实验测试。比如编程设计接收端缓慢接收数据。】

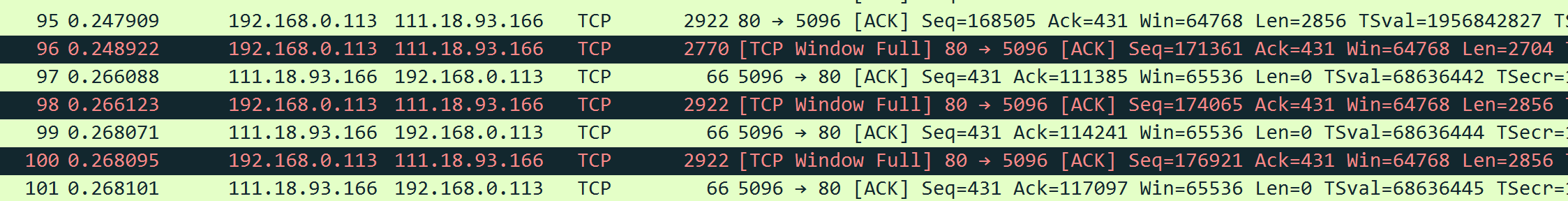


表3-3 记录TCP数据传送阶段的报文

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 报文序号 | 报文种类 (数据/确认) | 序号字段Seq Number | 确认号Ack Number | 数据长度 | 确认到哪条报文（填序号） | 窗口大小 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

步骤6、分析客户机和服务器两边各自捕获到的分组，分析整个TCP流，估计双方的RTT，重传率和重传流量，平均传输速度等参数。

步骤7、分析整个TCP流的拥塞控制，找到拥塞控制的几个典型过程（即慢启动、快速重传、拥塞避免，快速恢复），计算各个时期发送数据平均传输速度。

步骤8、如果拥塞控制的相关过程不明显，请设计合适的方法再次测试。

步骤9、完成其他可选的实验步骤。

1. 互动讨论主题

1）TCP的流量控制和拥塞控制有什么不同？

2）TCP的流量控制是哪一方（接收、发送）来主导的？什么情况下会发生流量控制？

3）讨论传输层与其上下相邻层的关系；

4）讨论TCP协议在传输实时语音流方面的优缺点。