# 实验三 传输层的TCP协议分析

## 实验目的

1. 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。
2. 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。
3. 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。
4. 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。

## 实验内容

1. 使用基于TCP的应用程序（比如浏览器下载文件）传输文件，在客户端和服务器均要捕获TCP报文。
2. 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。
3. 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。
4. 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】。

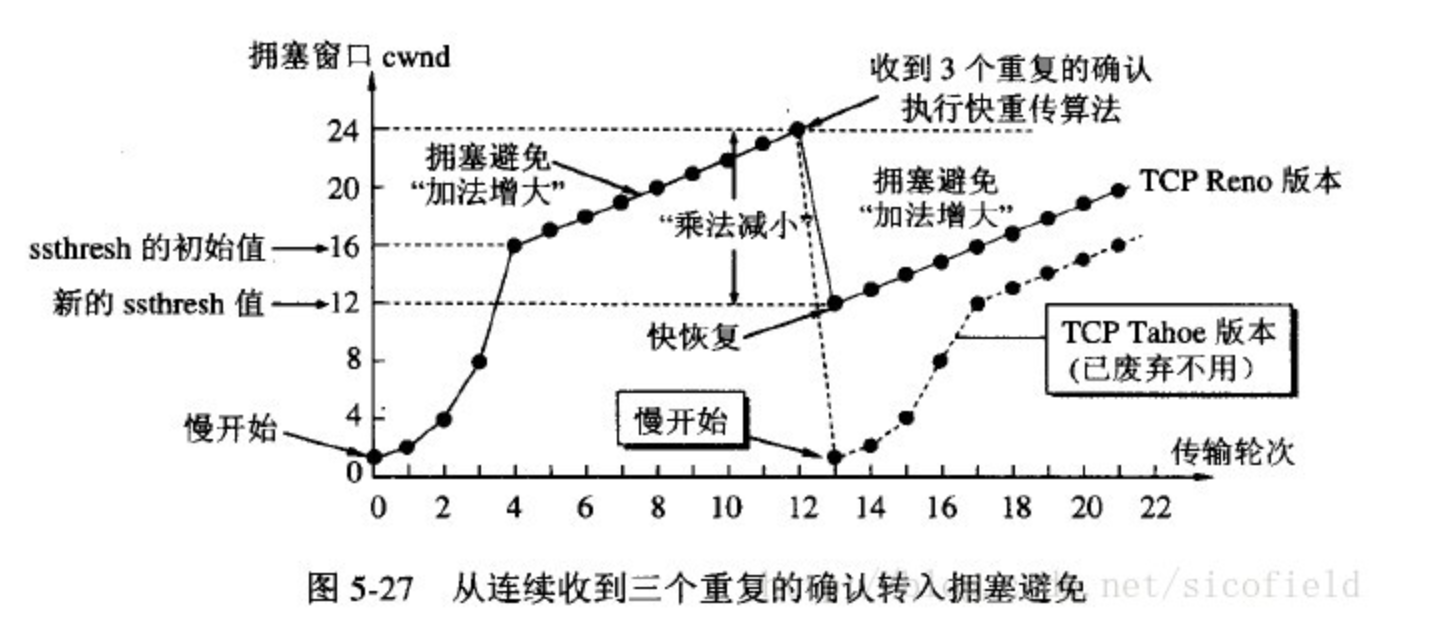


图3-0 典型的TCP 拥塞控制过程图例

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。

## 实验原理

### TCP协议报文格式

TCP协议工作在网络层之上，是一个面向连接的、端到端的、可靠的传输层协议。TCP的报文格式如图3-1，详细地规范参阅RFC 793。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 16 32 | | | | | | | | |
| 源端口Source port | | | | | | | | 目的端口Destination port |
| 顺序号Sequence number | | | | | | | | |
| 确认号Acknowledgement number | | | | | | | | |
| Data Offset | Resrvd | **U**  **R**  **G** | **A**  **C**  **K** | **P**  **S**  **H** | **R**  **S**  **T** | **S**  **Y**  **N** | **F**  **I**  **N** | 窗口大小Window |
| 校验和Checksum | | | | | | | | 紧急指针Urgent pointer |
| 选项和填充Option + Padding | | | | | | | | |
| 数据Data | | | | | | | | |

图3-1 The TCP header structure

1）源端口号，标识主机上发起传送的应用程序；目的端口标识主机上传送要到达的应用程序。源端和目的端的端口号，用于寻找发端和收端应用进程。这两个值加上I P包首部中的源端I P地址和目的端I P地址唯一确定一个T C P连接。

2）顺序号字段：占32比特。用来标识从TCP源端向TCP目标端发送的数据字节流，它表示在这个报文段中的第一个数据字节序号。

3）确认号字段：占32比特。只有ACK标志为1时，确认号字段才有效。它包含目标端所期望收到源端发送的下一个数据字节号。

4）Data Offset字段：占4比特。给出头部占32比特的数目，同时也指出数据的开始位置。没有任何选项字段的TCP头部长度为20字节；最多可有60字节的TCP头部。

5）Resrvd预留：由跟在数据偏移字段后的6位构成，预留位通常为0.

6）控制标志位（U、A、P、R、S、F）：占6比特。各比特的含义如下：

URG：紧急指针（urgent pointer）值有效；

ACK：确认号Acknowledgement number值有效；

PSH：接收方应该尽快将这个报文段交给应用层；

RST：重建连接；

SYN：发起一个连接；

FIN： 释放一个连接。

7）窗口大小字段：占16比特。此字段用来进行流量控制。单位为字节数，这个值是本机期望一次接收的字节数。

8）TCP校验和字段：占16比特。对整个TCP报文段，即TCP头部和TCP数据进行校验和计算，并由目标端进行验证。

9）紧急指针字段：占16比特。URG设置时有效，它是一个正偏移量，和序号字段中的值相加指向数据包中的第一个重要数据字节。

10）选项字段：占32比特。可能包括"窗口扩大因子"、"时间戳"等选项。

### TCP连接的建立与撤销

TCP连接的建立采用了三次握手方式，连接的撤销则是四次握手，TCP连接的建立和撤销的过程如图3-2所示：



图3-2 TCP 连接的建立的三次握手

## 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。】

## 实验组网

图3-3是本实验的组网图，图中参数仅供参考。



图3-3 TCP协议分析组网图

## 实验过程及结果分析

步骤1：PC2通过ssh（或远程桌面）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。

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。】

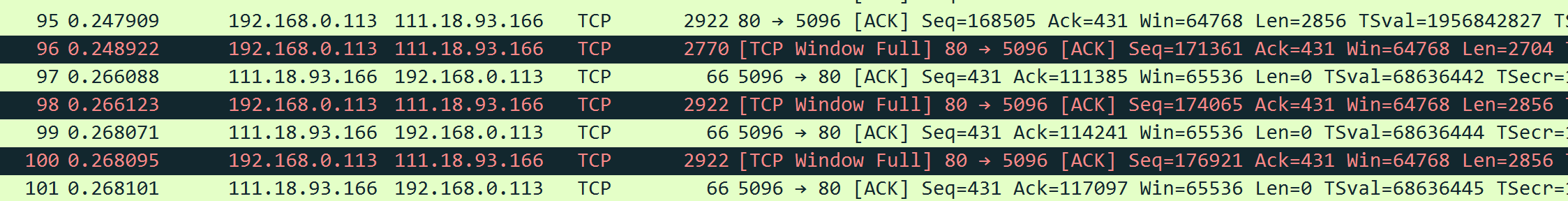


表3-3 记录TCP数据传送阶段的报文

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

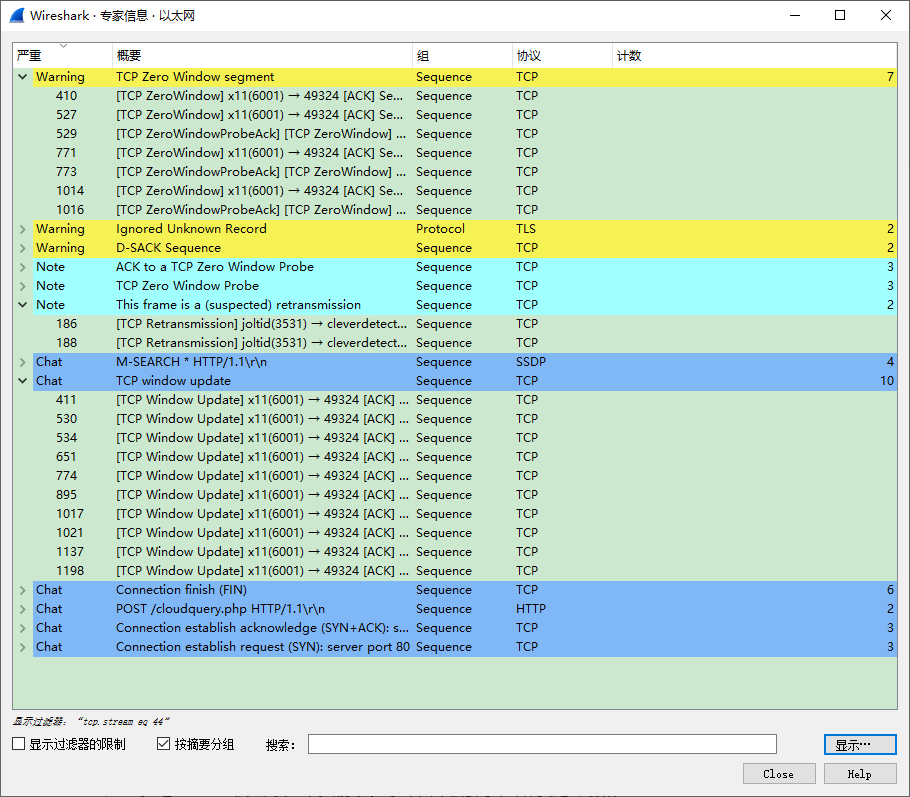
步骤6、分析客户机和服务器两边各自捕获到的分组，分析整个TCP流，估计双方的RTT，重传率和重传流量，平均传输速度等参数。

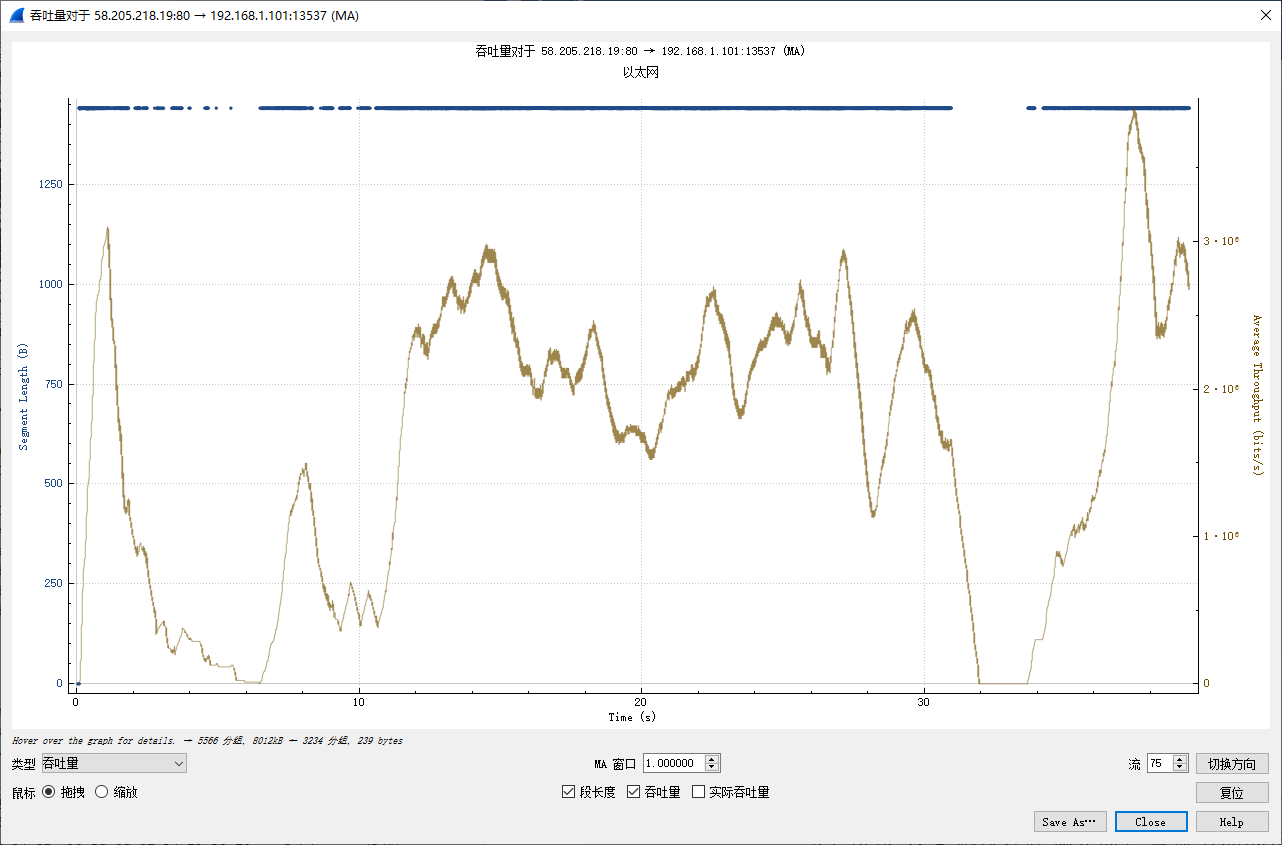
步骤7、分析整个TCP流的拥塞控制，找到拥塞控制的几个典型过程（即慢启动、快速重传、拥塞避免，快速恢复），计算各个时期发送数据平均传输速度。

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。

**注：**在做统计分析的时候，可以利用Wireshark自带的分析/统计工具，如“分析->专家信息”，“统计->TCP流图形”，“统计->流量图”等。注意观察特殊数据包： [TCP Window Full]、[TCP ZeroWindow]、[TCP Window Update]、 [TCP Retransmission]、[TCP Dup ACK] 、[ [TCP Fast Retransmission]等。





## 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。