暨南大学本科实验报告专用纸

课程名称 《计算机网络实验》 成绩评定

实验项目名称 TCP 协议分析实验 指导教师雷小林 、魏林锋

实验项目编号 实验项目类型 综合 实验地点 N117

学生姓名 陈宇 学号 2020101642

学院 信息科学技术学院 系 计算机 专业 软件工程

实验时间 2022 年 10 月 25 日下午～10 月 25 日 下午 温度 ℃湿度

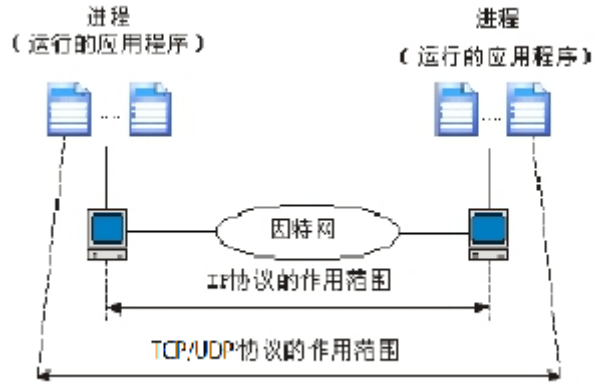
实验目的

1. 掌握 TCP 协议的报文格式
2. 掌握 TCP 连接的建立和释放过程
3. 掌握 TCP 数据传输中编号与确认的过程
4. 掌握 TCP 协议校验和的计算方法
5. 理解 TCP 重传机制

实验原理

1. 进程到进程的通信

在学习 TCP/UDP 协议之前，首先应该了解主机到主机的通信和进程到进程的通信，以及这两种通信之间的区别。IP 协议负责主机到主机的通信。作为一个网络层协议，IP 协议只能把报文交付给目的主机。这是一种不完整的交付，因为这个报文还没有送交到正确的进程。像 TCP/UDP 这样的传输层协议负责进程到进程的通信。TCP/UDP 协议负责把报文交付到正确的进程。下图描绘了 IP 协议和 TCP/UDP 协议的作用范围。



在网络中，主机是用 IP 地址来标识的。而要标识主机中的进程，就需要第二个标识符，这就是端口号。在 TCP/IP 协议族中，端口号是在 0～65535 之间的整数。

在客户/服务器模型中，客户程序使用端口号标识自己，这种端口号叫做短暂端口号，短暂的意思是生存时间比较短。一般把短暂端口取为大于 1023 的数，这样可以保证客户程序工作得比较正常。

TCP常用熟知端口

端口	协议	端口	协议
20	FTP Data	80	HTTP
21	FTP Control	110	POP3
23	TELNET	143	IMAP
25	SMTP		

服务器进程也必须用一个端口号标识自己。但是这个端口号不能随机选取。如果服务器随机选取端口号，那么客户端在想连接到这个服务器并使用其服务的时候就会因为不知道这个端口号而无法连接。TCP/IP 协议族采用熟知端口号的办法解决这个问题。每一个客户进程都必须知道相应的服务器进程熟知端口号。

在一个 IP 数据包中，目的 IP 地址和端口号起着不同的寻址作用。目的 IP 地址定义了在世界范围内惟一的一台主机。当主机被选定后，端口号定义了在这台主机上运行的多个进程中的一个。

2．TCP 协议介绍

TCP 是传输控制协议 （Transmission Control Protocal）的缩写，提供面向连接的可靠的传输服务。在 TCP/IP 体系中，HTTP、FTP、SMTP 等协议都是使用 TCP 传输方式的。

（1）TCP 报文格式

图 28 TCP 报文段格式

TCP 报文分为首部和数据两个部分。如图 28 所示，TCP 报文段首部的前 20 字节是固定的，后面有 4 ×n 字节是可选项。其中：

* 源端口和目的端口：各 2 字节，用于区分源端和目的端的多个应用程序；

* 序号：4 字节，指本报文段所发送的数据的第一字节的序号；

* 确认序号：4 字节，是期望下次接收的数据的第一字节的编号，表示该编号以前的数据已安全接收。

* 数据偏移:4 位,指数据开始部分距报文段开始的距离,即报文段首部的长度,以 32bit 为单位。

* 标志字段：共有六个标志位：

① 紧急位 URG=1 时，表明该报文要尽快传送，紧急指针启用；

② 确认位 ACK=1 时，表头的确认号才有效；ACK=0，是连接请求报文；

③ 急迫位 PSH=1 时，表示请求接收端的 TCP 将本报文段立即传送到其应用层，而不是等到整个缓存都填满后才向上传递；

④ 复位位 RST=1 时，表明出现了严重差错，必须释放连接，然后再重建连接；

⑤ 同步位 SYN=1 时，表明该报文段是一个连接请求或连接响应报文，

⑥ 终止位 FIN=1 时，表明要发送的字符串已经发送完毕，并要求释放连接。

标志	说明
CWR	拥塞窗口减小（用来表明发送主机接收到了设置 ECE 标志的 TCP 包。拥塞窗口是被 TCP 维护的一个内部变量，用来管理发送窗口大小）
ECE	经历拥塞回送（用来在 TCP3 次握手时表明一个 TCP 端是具备 ECN 功能的，并且表明接收到的 TCP 包的 IP 头部的 ECN 被设置为 11）
URG	紧急指针字段值有效
ACK	确认字段值有效
PSH	推送数据
RST	连接必须复位
SYN	在连接建立时对序号进行同步
FIN	终止连接

* 窗口：2 字节，指该报文段发送者的接收窗口的大小，单位为字节；

* 校验和：2 字节，对报文的首部和数据部分进行校验；

* 紧急指针：2 字节，指明本报文段中紧急数据的最后一个字节的序号，和紧急位 URG 配合使用；

* 选项：长度可变，若该字段长度不够四字节，有填充补齐。

（2）TCP 连接的建立

TCP 连接的建立采用 “三次握手”的方法。

一般情况下，双方连接的建立由其中一方发起。如图 29(a)所示：

* 主机 A 首先向主机 B 发出连接请求报文段，其首部的 SYN 同步位为 1，同时选择一个序号 x；

* 主机 B 收到此连接请求报文后，若同意建立连接，则向主机 A 发连接响应报文段。在响应报文段中，SYN 同步位为 1，确认序号为 x+1，同时也为自己选择一个序列号 y；

* 主机 A 收到此确认报文后，也向主机 B 确认，这时，序号为 x+1，确认序号为 y+1。当连接建立后，A、B 主机就可以利用 TCP 进行数据传输了。

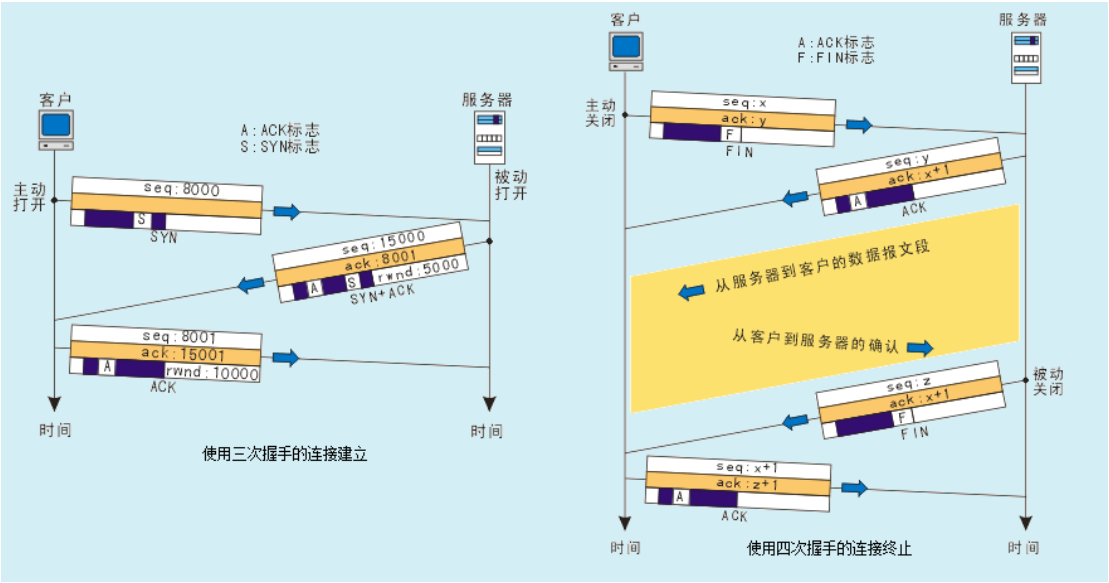


图 29 TCP 的连接和释放

（3）TCP 连接的释放

通信双方中的任何一方都可以关闭连接。当一方的连接被终止时，另一方还可继续向对方发送数据。TCP 的连接终止有两种方式：三次握手和具有半关闭的四次握手。

四次握手如图 29(b)所示，假如主机 A 首先向主机 B 提出释放连接的请求，其过程如下：

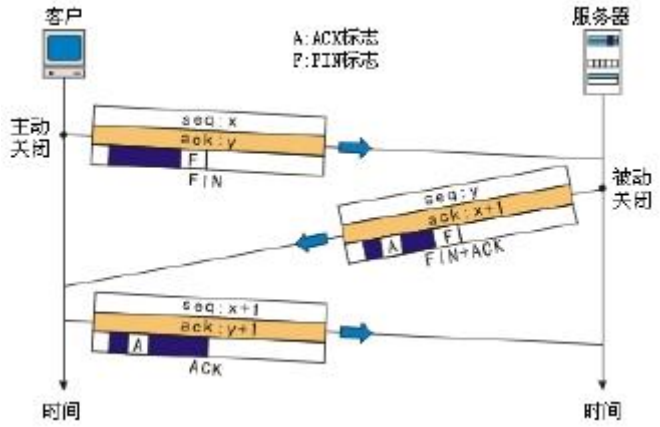
* 主机 A 向主机 B 发送释放连接的报文段，其中，FIN 终止位为 1，序号 x 等于前面已经发送数据的最后一个字节的序号加 1；

* 主机 B 对释放连接请求进行确认，其序号等于 x+1。这时从 A 到 B 的连接已经释放，连接处于半关闭状态，以后主机 B 不再接收主机 A 的数据。但主机 B 还可以向主机 A 发送数据，主机 A 在收到主机 B 的数据时仍然向主机 B 发送确认信息。

* 当主机 B 不再向主机 A 发送数据时，主机 B 也向主机 A 发释放连接的请求；

* 同样主机 A 收到该报文段后也向主机 B 发送确认。

使用三次握手的 TCP 终止过程如下图所示：



(1) 当客户端想关闭 TCP 连接时，它发送一个 TCP 报文，把 FIN 标志位设置为 1。

(2) 服务器端在收到这个 TCP 报文后，把 TCP 连接即将关闭的消息发送给相应的进程，并发送第二个报文——FIN+ACK 报文，以证实从客户端收到了 FIN 报文，同时也说明，另一个方向的连接也关闭了。

(3) 客户端发送最后一个报文以证实从 TCP 服务器收到了 FIN 报文。这个报文包括确认号，它等于从服务器收到的 FIN 报文的序号加 1。

（4 ）TCP 数据传输

TCP 可以通过检验序号和确认号来判断丢失、重复的报文段，从而保证传输的可靠性。TCP 将要传送的报文看成是由一个个字节组成的数据流，对每个字节编一个序号。在连接建立时，双方商定初始序号（即连接请求报文段中的 SEQ 值）。TCP 将每次所传送的第一个字节的序号放在 TCP 首部的序号字段中，接收方的 TCP 对收到每个报文段进行确认，在其确认报文中的确认号字段的值表示其希望接收的下一个报文段的第一个数据字节的序号。

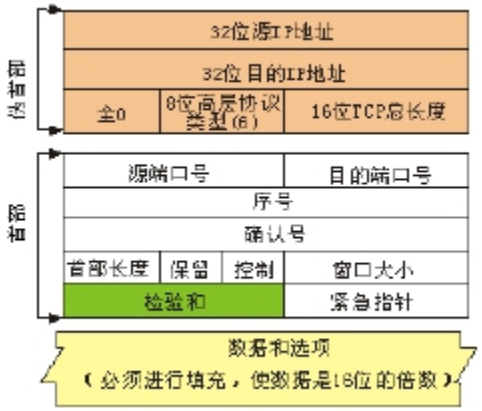
由于 TCP 能提供全双工通信，因此，通信中的每一方不必专门发送确认报文段，而可以在发送数据时，捎带传送确认信息，以此来提高传输效率。

（4 ）TCP 封装

TCP 报文封装在 IP 数据报中，然后再封装成数据链路层中的帧，如下图所示：

（5）TCP 校验和

TCP 的校验和与 UDP 的校验和计算过程是一样的。但是，UDP 是否使用校验和是可选的，而 TCP 是否使用校验和则是强制性的。在计算 TCP 校验和时也要在报文上添加伪首部。对于 TCP 的伪首部，高层协议类型字段的值是 6。如下图所示：



3．实验环境与说明

（1）实验目的

学习 3CDaemon FTP 服务器的配置和使用，分析 TCP 报文格式，理解 TCP 的连接建立、和连接释放的过程。

（2）实验设备和连接

实验设备和连接图如图 32 所示，一台锐捷 S2126G 交换机连接了 2 台 PC 机，分别命名为主机 A、主机 B，交换机命名为 Switch。

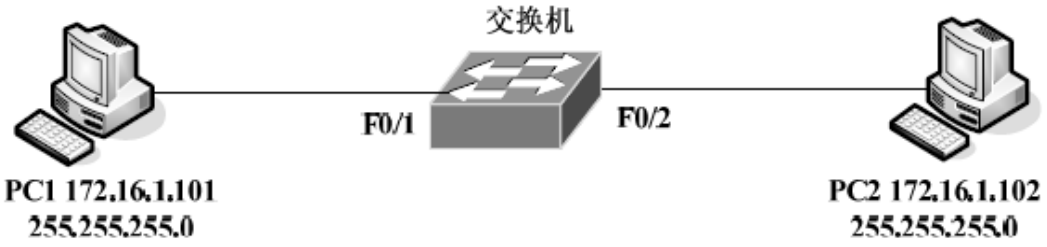


图 32 TCP 协议分析实验连接图

（3）实验分组

每六名同学为一组，其中每两人一小组，每小组各自独立完成实验。将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。

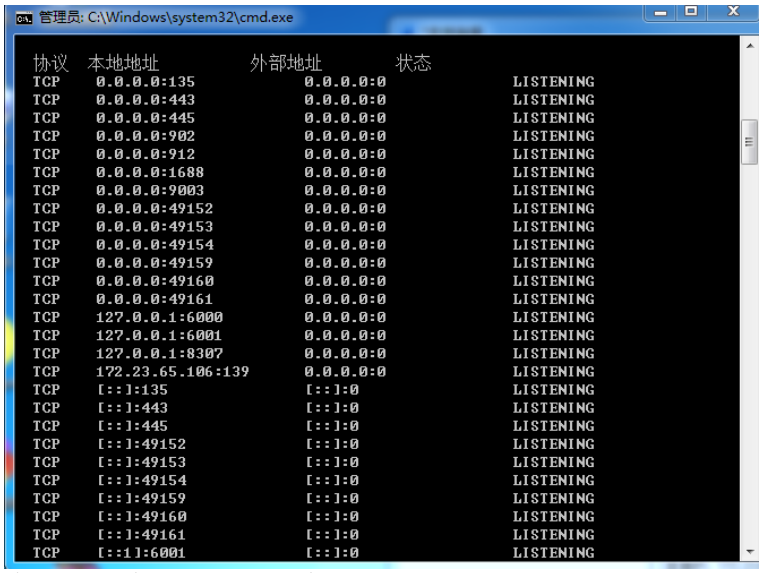
实验步骤

练习一、察看 TCP 连接的建立和释放

本练习将主机A和B作为一组，主机C和D作为一组，主机E和F作为一组。现仅以主机A、B为例，其它组的操作参考主机A、B的操作。

步骤1：主机B运行Wireshark截获报文，并设置过滤条件（提取TCP协议）。

步骤2：主机B在命令行下输入：netstat -a -n命令来查看主机B的TCP端口号。

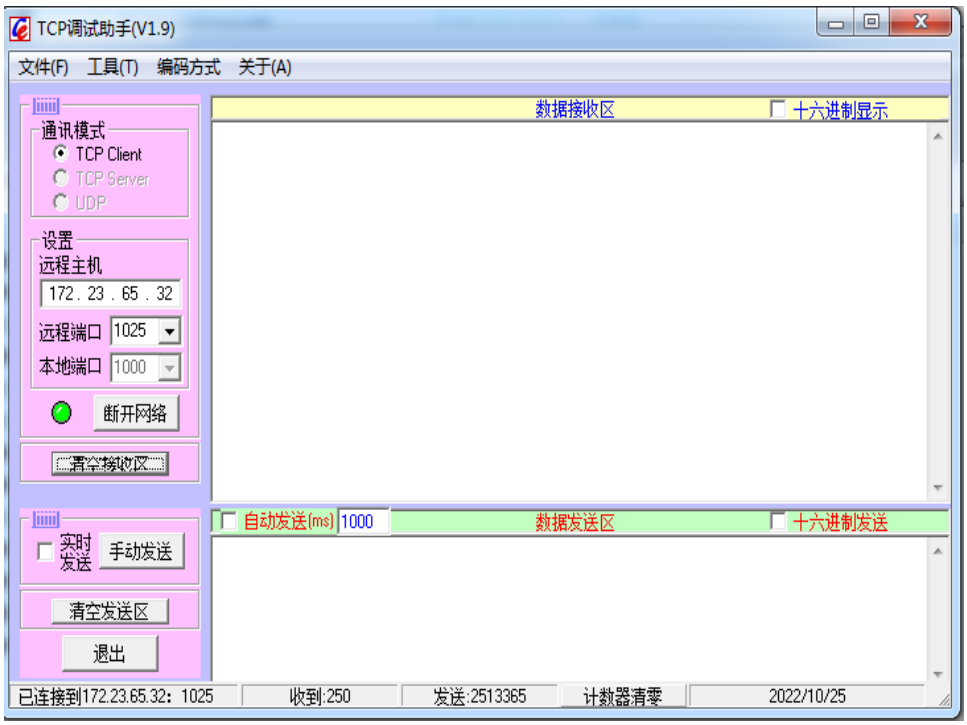


步骤3：主机A，B上分别启动TCP工具。

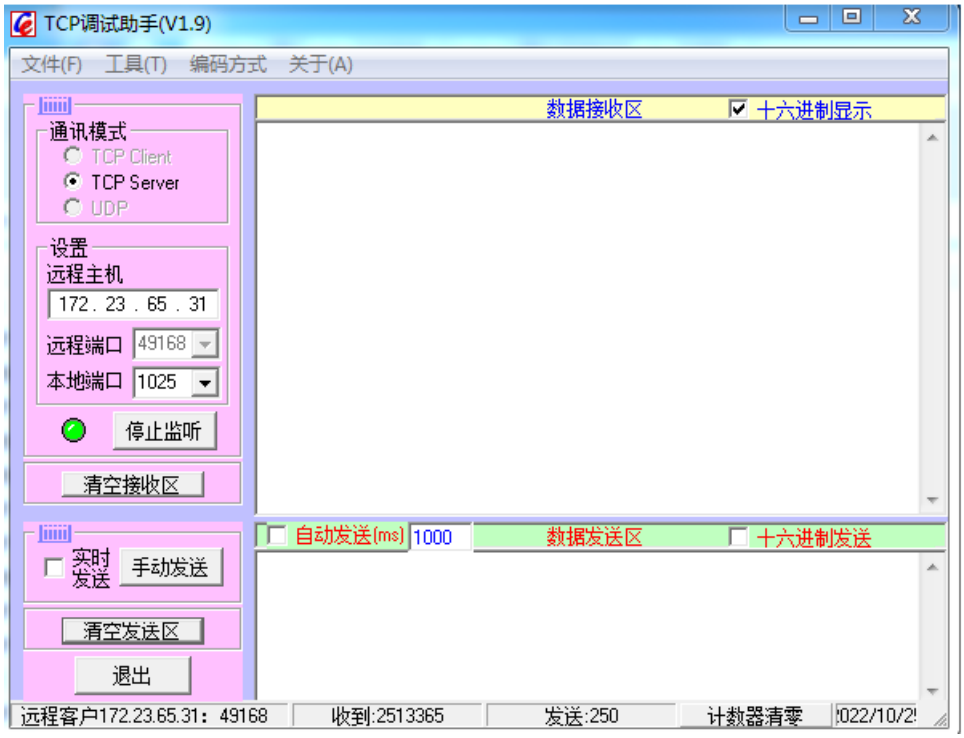
步骤4：启动后的界面如下图：

a. 主机B选中“TCP Server”单选框，在“远程主机”文本框中填入主机A的IP地址，在“本地端口”文本框中填入主机B的一个TCP监听端口，点击[开始监听]按钮进行监听。

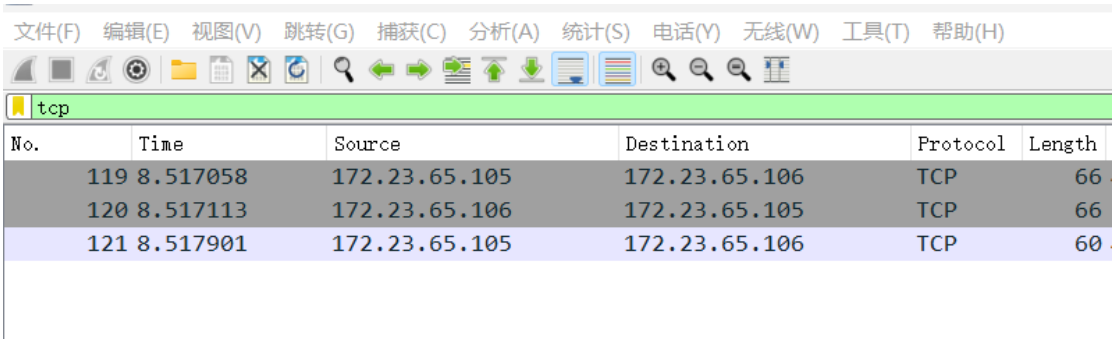
b. 主机A选中“TCP Client”单选框，在“远程主机”文本框中填入主机B的IP地址，在“远程端口”文本框中填入主机B的同一个TCP监听端口，点击[连接网络]按钮进行连接。



主机A 充当客户端



主机B充当服务器端



步骤5：网络连接正常后，察看主机B捕获的数据，结合本节TCP 协议介绍部分的内容，分析TCP 连接建立的 “三次握手”过程，找到对应的报文，填写表12（传输方向填写主机B=>主机A 或主机B<=主机A ）。

表 12 TCP 连接建立报文分析

报文号	传输方向	源端口	目的端口	序　号	确认序号	同步位 SYN	确认位 ACK
1	a=>b	49168	1688	808540248	0	1	0
2	b=>a	1688	49168	935405101	808540249	1	1
3	a=>b	49168	1688	808540249	935405101	0	0

● TCP 连接建立时，前两个报文的首部都有一个“最大字段长度”字段，它的值是多少？作用是什么？结合 IEEE802.3 协议规定的以太网最大帧长度分析此数据是怎样得出的。

答：最大字段=1460bytes； 作用表示在一个帧中数据长度最长为 1460，不能发出更长的帧。以太网中规定发出的帧长度不能超过 1500，而 ip 首部长度为 20 字节，tcp 首部长度为 20 字节。所以 tcp 字段长度不能超过 1460 字节。

步骤6：主机 A 断开与主机 B 的 TCP 连接。

步骤7：察看主机 B 捕获的数据，填写下表。

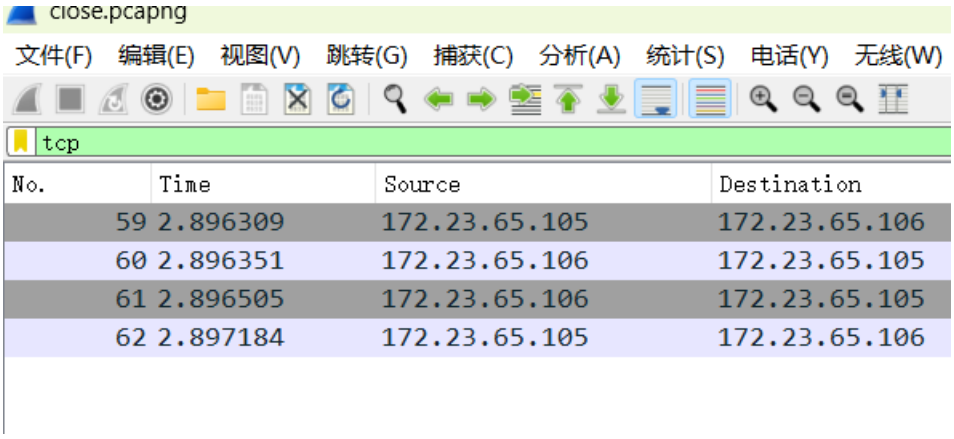


表 13 TCP 连接连接释放报文分析

报文号	传输方向	源端口	目的端口	序　号	确认序号	终止位 FIN	同步位 SYN	确认位 ACK
1	A=>b	49169	1688	3597594204	2218887512	1	0	1
2	B=>a	1688	49169	2218887512	3597594205	0	0	1
3	B=>a	1688	49169	2218887512	3597594205	1	0	11
4	A=>b	49169	49169	3597594205	2218887513	0	0	

结合上述两表所填写的内容，理解 TCP 的三次握手建立连接和四次握手的释放连

接过程，理解序号、确认号等字段在 TCP 可靠连接中所起的作用。

思考问题：

1. 为什么在 TCP 连接过程中要使用三次握手？如不这样做可能会出现什么情况。

答：通过三次握手才能阻止重复历史连接的初始化；通过三次握手才能对通信双方的初始序列号进行初始化；TCP 建立连接时通过三次握手可以有效地避免历史错误连接的建立，减少通信双方不必要的资源消耗，三次握手能够帮助通信双方获取初始化序列号，它们能够保证数据包传输的不重不丢，还能保证它们的传输顺序，不会因为网络传输的问题发生混乱，

2. 解释 TCP 协议的释放过程以及为什么要使用四次挥手？

释放过程：

第一次挥手：A->B，A 向 B 发出释放连接请求的报文，其中 FIN（终止位） = 1，seq（序列号）=u；在 A 发送完之后，A 的 TCP 客户端进入 **FIN-WAIT-1**（终止等待 1）状态。此时 A 还是可以进行收数据的

第二次挥手：B->A：B 在收到 A 的连接释放请求后，随即向 A 发送确认报文。其中 ACK=1，seq=v，ack（确认号） = u +1;在 B 发送完毕后，B 的服务器端进入 **CLOSE_WAIT**（关闭等待）状态。此时 A 收到这个确认后就进入 **FIN-WAIT-2**（终止等待 2）状态，等待 B 发出连接释放的请求。此时 B 还是可以发数据的。

第三次挥手：B->A：当 B 已经没有要发送的数据时，B 就会给 A 发送一个释放连接报文，其中 FIN=1，ACK=1，seq=w，ack=u+1，在 B 发送完之后，B 进入 **LAST-ACK**（最后确认）状态。

第四次挥手：A->B；当 A 收到 B 的释放连接请求时，必须对此发出确认，其中 ACK=1，seq=u+1,ack=w+1;A 在发送完毕后，进入到 **TIME-WAIT** （时间等待）状态。B 在收到 A 的确认之后，进入到 **CLOSED**（关闭）状态。在经过时间等待计时器设置的时间之后，A 才会进入 **CLOSED** 状态。

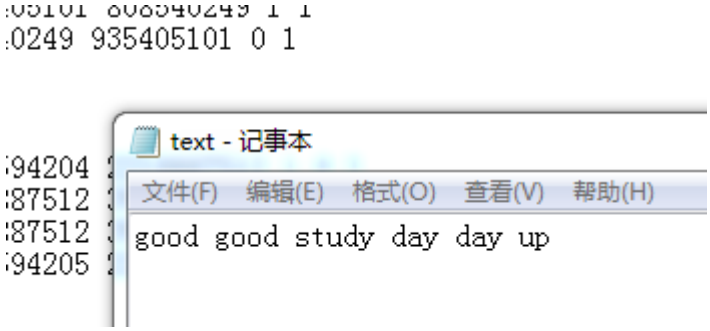
答：其实是客户端和服务端的两次挥手，也就是客户端和服务端**分别释放**连接的过程。

练习二、察看 TCP 数据传输过程

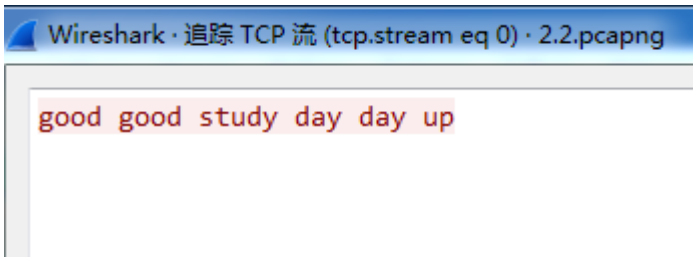
步骤1：根据练习一的操作步骤建立TCP连接，然后在主机A、B上输入框里输入发送内容，点击“手动发送”按钮分别向对方发送数据。

步骤 2：察看主机 B 捕获的数据，回答下列问题：

发送内容：



接收内容：



1）TCP 协议如何保证数据传输的可靠性？具体是通过哪些字段来实现的？

答：TCP 协议主要通过以下七点来保证传输可靠性：连接管理，校验和，序列号，确认应答，超时重传，流量控制，拥塞控制。

校验和：发送方对发送数据的二进制求和取反，然后将值填充到 TCP 的校验和字段中，接收方收到数据之后，以相同的方式计算校验和并进行对比。如果结果不符合预期，则将数据包丢弃。

序列号：TCP 将每个字节的数据都进行了编号，这就是序列号。序列号的具体作用如下：能够保证可靠性，既能防止数据丢失，又能避免数据重复。能够保证有序性，按照序列号顺序进行数据包还原。能够提高效率，基于序列号可实现多次发送，一次确认。

确认应答：接收方接收数据之后，会回传 ACK 报文，报文中带有此次确认的序列号，用于告知发送方此次接收数据的情况。在指定时间后，若发送端仍未收到确认应答，就会启动超时重传。

超时重传：具体来说，超时重传主要有两种场景：数据包丢失：在指定时间后，若发送端仍未收到确认应答，就会启动超时重传，向接收端重新发送数据包。确认包丢失：当接收端收到重复数据(通过序列号进行识别)时将其丢弃，并重新回传 ACK 报文。

流量控制：接收端处理数据的速度是有限的，如果发送方发送数据的速度过快，就会导致接收端的缓冲区溢出，进而导致丢包……为了避免上述情况的发生，TCP 支持根据接收端的处理能力，来决定发送端的发送速度。这就是流量控制。流量控制是通过在 TCP 报文段首部维

护一个滑动窗口来实现的。

拥塞控制：拥塞控制就是当网络拥堵严重时，发送端减少数据发送。拥塞控制是通过发送端维护一个拥塞窗口来实现的。可以得出，发送端的发送速度，受限于滑动窗口和拥塞窗口中的最小值。

步骤 3：点击菜单栏里的“工具”，选择“发送文件”菜单项，发送一个 TXT 文件，察看主机 B 捕获的数据，回答下列问题：

1）简述发送文件数据的过程。

答：程序分为发送端和接收端。首先在传输文件数据之前，发送端会把将装有文件名称和文件长度等，信息的数据包发送至接收端。接收端收到文件名称和文件长度信息后会创建好空白文件。接着开始传输文件数据。

2）观察报文的序号和确认号是如何变化的，有什么样的规律。

答：1. a=>b 序号：1888286325 确认号：69920749

2. b=>a 序号：69920749 确认号：1888286351

差为数据长度

步骤4：选中一个数据报文，在右键菜单里选择“跟踪流”->“TCP流”，观察数据是否与TXT文件内容一致。

实验总结

通过实验我掌握了 TCP 协议的报文格式，

掌握了 TCP 连接的建立和释放过程，

掌握了 TCP 数据传输中编号与确认的过程，

掌握了 TCP 协议校验和的计算方法，

理解了 TCP 重传机制。