|  |
| --- |
|  |

|  |
| --- |
|  |
|  | C:\Users\ADMINI~1\AppData\Local\Temp\ksohtml7476\wps3.jpg |

实验报告

（\_\_2022\_\_/\_\_2023\_\_学年第二学期）



|  |  |
| --- | --- |
| 课程名称： | 计算机网络原理实验 |
| 学 院： | 信息科学与工程学院 |
| 教 研 室： | 计算机系 |
| 专业班级： | 计算机21-5 |
| 姓 名： | 孔令杰 |
| 指导教师： | 冯龛 |

**实验七：传输控制协议（TCP）**

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

一. TCP协议简介

TCP（传输控制协议）协议是TCP/IP协议族中的面向连接的、可靠的传输层协议。TCP与UDP不同，它允许发送和接收字节流形式的数据。为了使服务器和客户端以不同的速度发送和接收数据，TCP提供了发送和接收两个缓冲区。TCP提供全双工服务，数据同时能双向流动。通信的每一方都有发送和接收两个缓冲区，可以双向发送数据。TCP在报文中加上一个递增的确认序列号来告诉发送端，接收端期望收到的下一个报文，如果在规定时间内，没有收到关于这个包的确认响应，则重新发送此包，这保证了TCP是一种可靠的传输层协议。

TCP的常用熟知端口如下表所示：

表7-1 TCP常用熟知端口

二. TCP报文格式

TCP报文的格式如下图所示：

图7-1 TCP报文格式

TCP报文包括20～60字节的首部，接着是应用程序的数据部分。首部在没有选项时是20字节，而当有选项时长度会增加，但是最大不会超过60字节。

● 源端口：该字段定义了在主机中发送这个报文的应用程序端口号。

● 目的端口：该字段定义了数据报发往的主机中接收这个报文的应用程序的端口号。

● 序列号：该字段定义了指派给本报文第一个数据字节的一个序号。TCP是流式传输协议，为了保证连通性，要在发送的每一个字节上编号。序号指定了这个序列中的哪一个字节是报文的第一个字节。在连接建立时，双方使用随机数产生器产生初始序号，通常每一方的初始序号都是不同的。

● 确认号：该字段定义了报文的接收端期望从对方接收的序号。如果报文的接收端成功地接收了对方发来的序号为x的报文，它就把确认号定义为x+1。确认可以和数据一起发送。

● 首部长度：该字段指定TCP首部的长度，以4字节为单位。首部长度可以在20～60字节之间。因此，这个字段的值可以在5至15之间。

● 保留：这是6位字段，保留为今后使用。

● 控制：这个字段定义了8种不同的标志。如下图所示。在同一时间可设置一位或多位标志。

图7-2 控制字段

这些标志用在TCP的流量控制、连接建立和终止以及数据传送的方式等方面。下表给出了每一位的简要说明。

表7-2 TCP标志位

● 窗口大小：该字段定义对方必须维持的窗口值（以字节为单位）。这个字段的长度是16位，因此窗口值的最大长度是65535字节。这个值通常是作为接收窗口，并由接收端来确定。这时，发送端必须服从接收端的决定。

● 校验和：该字段的校验范围包括伪首部、TCP首部和TCP数据部分。

● 紧急指针：只有当紧急标志置位时，这个16位字段才有效，这时的报文中包括紧急数据。

● 选项：在TCP首部中可以有多达40字节的可选信息。

三. 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：

图7-3 TCP封装

四. 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：

图7-4 伪首部加到TCP报文上

五. TCP连接建立与释放

1. 连接建立

TCP以全双工方式传送数据。当两个进程建立了TCP连接后，它们能够同时向对方发送数据。在传送数据之前，双方都要对通信进行初始化，得到对方的认可。

2. 三次握手(动画演示)

TCP的连接建立过程叫做三次握手。服务器程序首先准备好接受TCP连接，这个过程叫做被动打开请求。这时，服务器的TCP就已准备好接受任何一台主机的TCP连接了。

客户程序发出TCP连接请求的过程叫做主动打开。然后服务器与客户端就开始三次握手过程，如下图所示（在图中客户端与服务器端各使用一条时间线，并给出每个阶段的几个重要字段，包括序号、确认号、控制标志以及非零的窗口值）。这个过程有以下3个步骤。

图7-5 使用三次握手的连接建立

（1）客户发送第一个报文，这是一个SYN报文，在这个报文中只有SYN标志置为1。这个报文的作用是使序号同步。

（2）服务器发送第二个报文，即SYN+ACK报文，其中SYN和ACK标志被置为1。这个报文有两个目的。首先，它是一个用来和对方进行通信的SYN报文。服务器使用这个报文同步初始序号，以便从服务器向客户发送字节。服务器还使用ACK标志确认已从客户端收到了SYN报文，同时给出期望从客户端收到的下一个序号。另外，服务器还定义了客户端要使用的接收窗口的大小。

（3）客户发送第三个报文。这仅仅是一个ACK报文。它使用ACK标志和确认号字段来确认收到了第二个报文。

3. 连接终止

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。

4. 三次握手方式终止连接

使用三次握手的TCP终止过程如下图所示：

图7-6 使用三次握手的连接终止

（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。

5. 半关闭的四次握手方式终止连接(动画演示)

在TCP连接中，一方可以终止发送数据，但仍然保持接收数据，这就叫做半关闭。半关闭通常是由客户端发起的。图7-7描绘了半关闭的过程。客户发送FIN报文，半关闭了这个连接。服务器发送ACK报文接受这个半关闭。但是，服务器仍然可以发送数据。当服务器已经把所有处理的数据都发送完毕时，就发送FIN报文，客户端发送ACK报文给予确认。

在半关闭一条连接后，客户端仍然可以接收服务器发送的数据，而服务器也可以接收客户端发送的确认。但是，客户端不能传送数据给服务器。

实验步骤

各主机打开工具区的“拓扑验证工具”，选择相应的网络结构，配置网卡后，进行拓扑验证，如果通过拓扑验证，关闭工具继续进行实验，如果没有通过，请检查网络连接。

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。

1. 主机B启动协议分析器捕获数据，并设置过滤条件（提取TCP协议）。

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。

2. 主机A启动TCP工具连接主机B。

主机A启动实验平台工具栏中的“TCP工具”。选中“客户端”单选框，在“地址”文本框中填入主机B的IP地址，在“端口”文本框中填入主机B的一个TCP端口，点击[连接]按钮进行连接。

3. 察看主机B捕获的数据，填写下表。

表7-3 实验结果

● 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。

4. 主机A断开与主机B的TCP连接。

5. 察看主机B捕获的数据，填写下表。

表7-4 实验结果

● 结合步骤3、5所填的表，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。

实验结果与数据

思考题

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。

2. 解释TCP协议的释放过程？