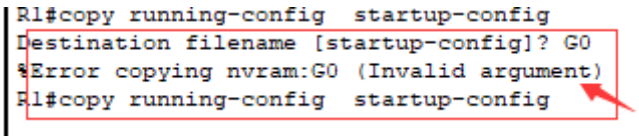
实验二

1. 基本信息

姓名	学号	班级	本次是否有抄袭	所选协议
庄佳强	202121331104	计算2114	否	TCP

2. 使用Cisco Packet Tracer遇到的问题及解决方法

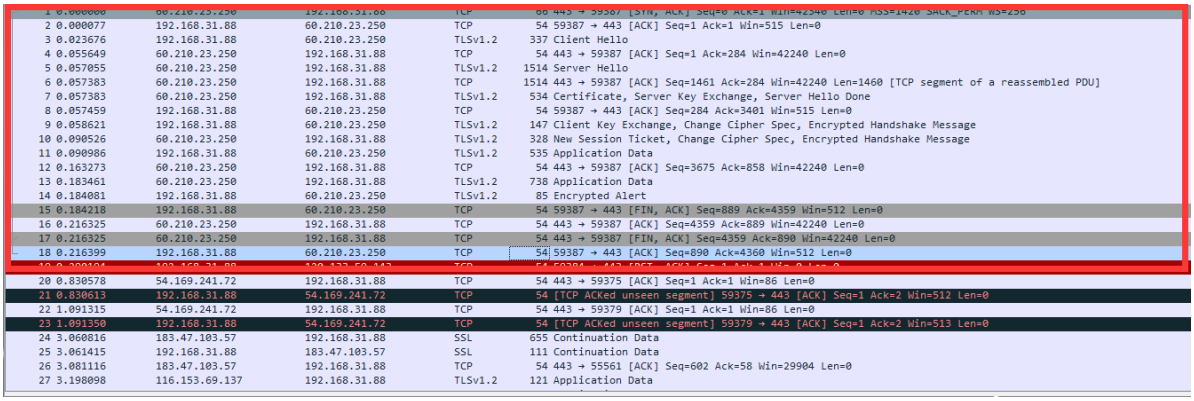


路由器搭设中:

跟着步骤走时，出现了这个问题，一开始以为是要确认就输入了Yes,但出现bug,后面看来报错才知道要输入的是文件名，但我也不知道文件名是什么，以为是自己建立一个文件，就以为命名为Go，但依然错误，不知所措。

解决方法：百度才知道其实是用已有的文件，默认为startup-config,输入后就完成了。

3. Wireshark抓取报文



（1）如何抓取到你所选择的协议报文

我是通过抓取所有的报文，再通过筛选得到自己的报文。

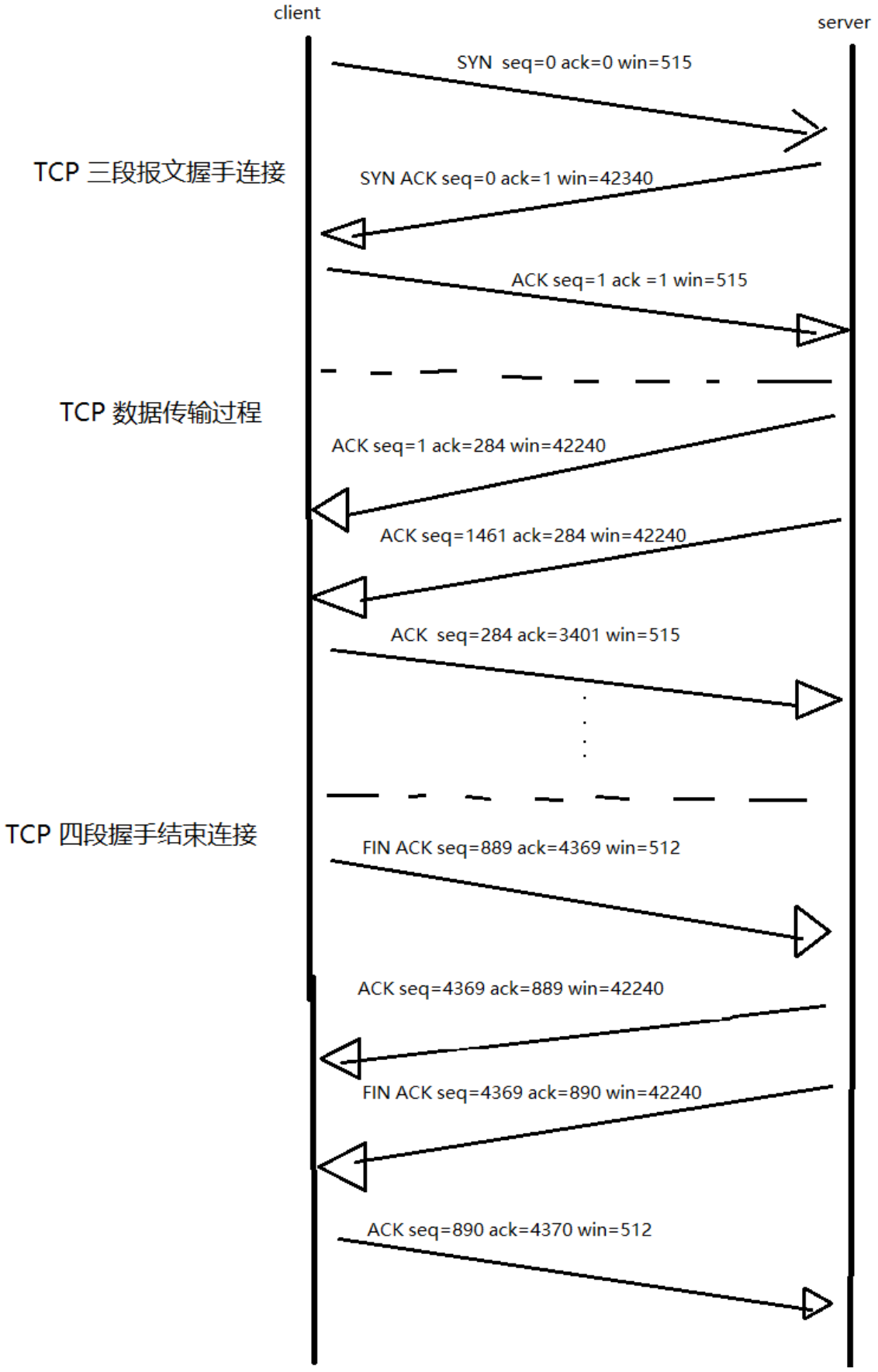
ps:可能不是一个好方法。

（2）Wireshark出来很多报文，你是如何过滤出与你所选协议相关的报文

我是通过先抓取一堆报文，再通过用筛选器筛选出TCP报文部分来查看，从而实现抓取特定的协议。

框中为比较完整的一次TCP通信，用来重点分析。

4. 协议时序图



5. 分析协议工作原理

一次完整的TCP通信包括了三段式握手连接，数据传输，四段握手接受连接。

三段式握手连接：在通信双方建立连接之前，需要进行三次握手，即主机发送SYN（同步）报文、收到SYN+ACK（同步确认）报文、再发送ACK（确认）报文。

seq：表示的是我方（发送方）这边，这个packet的数据部分的第一位应该在整个data stream中所在的位置。

ack：表示的是期望的对方（接收方）的下一次sequence number是多少。

SYN中同步报文中：seq=0为序号，ack=0为确认号，win为缓冲区大小（分析非重点）。

SYN+ACK中：ack=1为确认发来的报文，seq为服务端序号。

ACK中：发送了对TCP连接的确认。

自从TCP通信连接上了。

数据传输：连接建立后，数据通过TCP分段传输。每个数据包都有序号和确认号，以确保数据的可靠传输。发送方发送数据包后，等待接收方的确认。如果接收方没有收到数据包，或者数据包损坏，就会发送一个重传请求。

再发出ACK确认报文后,服务器发出了ACK确认收到报文，其中ack为之前收到的seq1+确认报文中的数据长度337-54表头长度=284字节，表示希望接受284字节开始的数据。其后同理可得。

四段握手接受连接：当数据传输完毕后，需要拆除连接。拆除连接也需要进行四次握手，即主机发送FIN（结束）报文、收到ACK报文、再收到FIN报文、发出ACK报文。收到ACK报文中在这期间服务器还可以向主机传递信息。

6. 遇到的问题及解决方法

1.在分析seq序号和ack确认号时啊，有时候会发现seq和ack怎么都对不上，反复查看tcp连接部分也没有看出什么错误，陷入了苦思。

解决方法:在查询资料后得知：

果接收方收到了乱序的数据包，它会发送一个带有已经收到的最后一个有序数据包序号的ACK报文，这个序号可能会比之前的序号大，导致ack字段的值突然增加。 -bychatGPT

从而得知其实可能是数据包乱序到达，导致全部抛弃，重新发送导致。

2.一开始不知道用什么画图，也不知道怎么画图。

解决方案：在反复查看群里的图片后，依葫芦画瓢，结合画图软件模仿着来，但也没有达到很好的效果。