**电子科技大学信息与软件工程学院**

**标 准 实 验 报 告**

**（实验）课程名称 网络安全技术**

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：陈奎 学 号：2017221303023 指导教师：赵洋**

**实验地点：信软楼西304 实验时间：19.11.5**

**一、实验室名称：信软楼西304**

**二、实验项目名称：网络侦听实验**

**三、实验学时： 4 学时**

**（一）实验目的**

通过使用Sniffer（嗅探）工具，实现捕捉ARP、ICMP、FTP等协议的数据包，以理解TCP/IP协议栈中多种协议的数据结构、会话连接建立和终止的过程、TCP序列号、应答序号的变化规律。并且通过实验了解FTP、HTTP等协议明文传输的特性，以建立安全意识，防止FTP、HTTP等协议由于传输明文密码造成的泄密。

**（二）实验内容**

1. 地址解析协议（ARP）实验
2. 网络路径跟踪（TRACE）实验
3. TCP连接实验

**四、实验原理：**

1. **地址解析协议（ARP）实验**

本实验中，所有计算机位于一个物理网络中：所有计算机通过以太网交换机连接在一个以太网中。该物理网络中没有连接路由器。同时，所有计算机也位于同一个IP网络中。

IP分组在以太网中发送时，除了要有接收站的IP地址（IP分组中的目的IP地址）外，还需要接收站的MAC地址（以太网帧中的目的MAC地址）。ARP协议将IP地址（逻辑地址）动态映射为MAC地址（物理地址）。

实验中两人一组，在“**未知**”（使用命令***arp -d \**** 清空ARP缓存表）和“**已知**”IP网络内通信时所需地址映射（目的IP地址，目的MAC地址）这两种情况下，先后使用计算机上的通信测试命令（***ping***）发起一次通信过程，并通过使用Sniffer软件捕获通信过程中通信双方的交互信息。比较两次通信过程中所捕获的分组数量、分组类型和分组内容，分析ARP协议的工作原理，包括：ARP分组（ARP请求分组和ARP应答分组）的产生条件、具体内容和传输方式。

每个实验者使用计算机上的ARP缓存表查看命令（***arp -a***），查看本小组的ARP协议操作结果和ARP缓存表内容，了解ARP缓存表的形成及其在ARP协议操作过程中的作用。

1. **网络路径跟踪（TRACE）实验**

本实验中，每个实验小组中的计算机分别连接在两个以太网中，每个以太网被配置为一个IP子网。

ICMP协议作为IP协议的辅助协议，提供差错报告和查询机制。

实验者在计算机上使用路径跟踪命令（***tracert***）查看子网A和子网B之间的通信路径，理解并掌握命令的用途和使用方法，结合IP协议、ICMP协议分析命令的工作原理。

实验者通过更改***tracert***命令参数，结合Sniffer软件所捕获的数据报文和ICMP的差错报告机制，考察IP分组生存时间（TTL）的含义及其对网络间IP分组交付的影响，了解并体会***tracert***命令的工作原理。

1. **TCP连接实验**

本实验中，所有计算机位于一个物理网络中：所有计算机通过以太网交换机连接在一个以太网中。该物理网络中没有连接路由器，有一台FTP服务器。所有计算机和FTP服务器位于同一个IP网络中。

TCP协议是一个面向连接的、可靠的运输层协议，通过连接建立和连接终止这两个过程完成面向连接的传输。

FTP协议是一个用于文件传输的应用层协议，采用客户/服务器模式实现文件传输功能，使用TCP协议提供的面向连接的可靠传输服务。FTP客户和服务器之间需要建立两条FTP连接：控制连接（端口21）和数据连接（端口20）。

实验者的计算机作为FTP客户，通过***ftp***命令与FTP服务器进行一次FTP会话活动。使用Sniffer软件捕获通信双方的交互信息，考察TCP协议的连接建立过程和连接终止过程。

分析TCP连接建立和连接终止过程中所捕获的TCP报文段，掌握TCP报文段首部中的端口地址、序号、确认号和各个码元比特的含义和作用。结合FTP操作，体会网络应用程序间的交互模式——客户/服务器（C/S）模式。

**五、实验器材（设备、元器件）**

* 1. 实验人数50～80人，每人1台计算机；2人一组配合完成本实验。
  2. 拓扑：（A、B范围中的主机分别简称为A主机和B主机）



**A**

**B**

* 1. 设备：以太网交换机2～4台；计算机50～80台
  2. 软件：Sniffer软件（捕获网络上传输的数据报文）

**六、实验步骤**

**（一）地址解析协议（ARP）实验**

1. 在A、B主机上运行Sniffer软件，设置捕获条件：

Address：Type = Hardware，Mode = Include，

Station 1 = <本机MAC地址>，Station 2 = any：

Advanced：Protocol = ARP，ICMP

1. 清空A、B主机上的ARP缓存表（命令：***arp -d \****）。
2. 在A、B主机上启动Sniffer的捕获过程。首先由A主机PING B主机。PING结束以后，停止A、B主机的Sniffer捕获过程，保存捕获数据。
3. 查看A、B主机上的ARP缓存表（命令：***arp -a***）。
4. 在A、B主机上再次启动Sniffer的捕获过程，由B主机PING A主机。PING结束以后，停止A、B主机的Sniffer捕获过程，保存捕获数据。
5. 查看A、B主机上的ARP缓存表（命令：***arp -a***）。
6. 查看并比较步骤3和步骤5中A、B主机上Sniffer软件所捕获的数据报文数量和类型。

**（二）网络路径跟踪（TRACE）实验**

1. 根据实验拓扑要求设置主机上的TCP/IP协议配置参数。运行Sniffer软件，设置捕获条件：

Address：Type = IP，Mode = Include，

Station 1 = <本机IP地址>，Station 2 = any：

Advanced：Protocol = ICMP

1. 计算子网A、B的子网地址和子网广播地址。
2. 路径跟踪——TRACE
3. 在主机的cmd窗口键入“***tracert***”命令，查看并分析选项***-d***、***-h***的含义和作用。
4. 启动Sniffer捕获过程，子网A、B中的主机TRACE对方子网中的1个主机IP地址。TRACE结束以后，停止Sniffer的捕获过程，保存捕获数据，查看并解释本主机上显示的通信结果。
5. 启动Sniffer捕获过程，使用***-d***选项TRACE步骤3-2中的目的主机。TRACE结束后，停止Sniffer的捕获过程，保存捕获数据，查看本主机上显示的通信结果，并与步骤3-2的结果相比较。
6. 启动Sniffer捕获过程，使用***-d***和***-h***选项重新TRACE步骤3-2中的目的主机，***-h***选项取值分别为***1***、***2***、***3***。TRACE结束以后，停止Sniffer的捕获过程，保存捕获数据，查看本主机上显示的通信结果。
7. 启动Sniffer捕获过程，使用***-d***和***-h***选项TRACE对方子网中1个不存在的主机IP地址，***-h***选项取值为***6***。TRACE结束以后，停止Sniffer的捕获过程，保存捕获数据，查看本主机上所显示的通信结果。

**（三）TCP连接实验**

* 1. 在主机上运行Sniffer软件，设置捕获条件：

Address：Type = IP，Mode = Include，

Station 1 = <本机IP地址>，Station 2 = 192.168.3.254：

Advanced：Protocol = FTP

* 1. 启动Sniffer的捕获过程，并在主机的cmd窗口中以命令行的方式启动FTP客户进程，过程如下：

（***黑斜体***表示输入内容，其它为系统显示信息）

C:\> ***ftp 192.168.4.254（或ftp 192.168.3.254）***

Connected to 192.168.4.254.

220 Serv-U FTP Server v4.0 for WinSock ready…

User (192.168.3.254:(none)): ***ftp***

331 User name okay, please send complete E-mail address as password.

Password: ***ftp@***

230 User logged in, proceed.

ftp> ***quit***

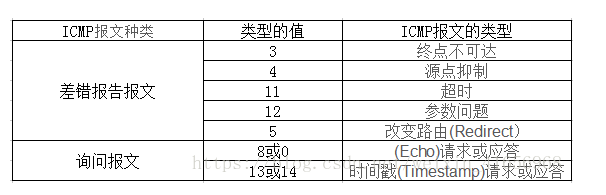
221 Goodbye!

* 1. 停止Sniffer的捕获过程，保存捕获数据。
  2. 查看捕获报文中的本机FTP进程端口号、FTP服务器进程端口号、本机TCP初始序号和服务器TCP初始序号。
  3. 重复步骤2和3，查看捕获报文中的本机FTP进程端口号、FTP服务器进程端口号、本机TCP初始序号和服务器TCP初始序号，并与步骤4的查看结果相比较。

**七、实验数据及结果分析**

**做实验前需关闭防火墙，否则会失败**

**几种常见的ICMP报文类型：**



**（一）地址解析协议（ARP）实验**

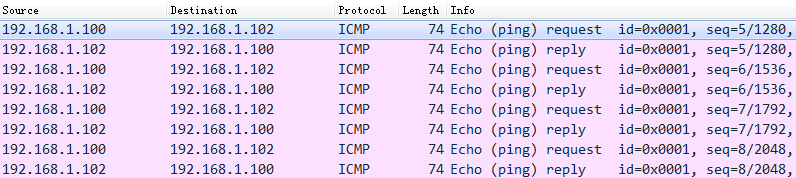
1.清空缓存表

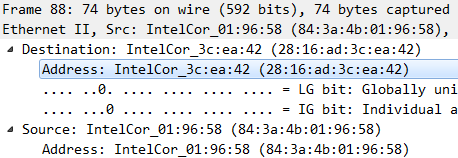


2.A主机pingB主机

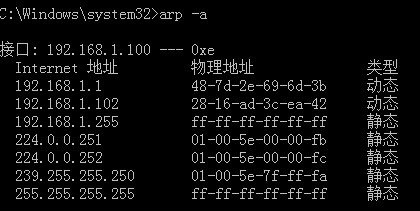


主机A抓包记录

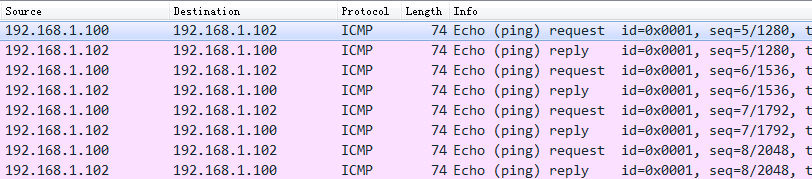




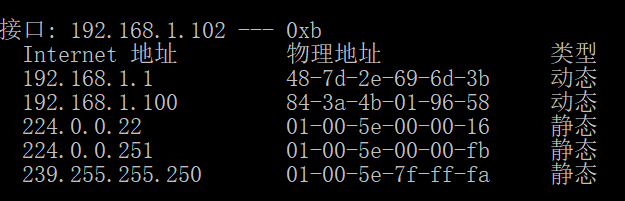
主机A的ARP缓存表



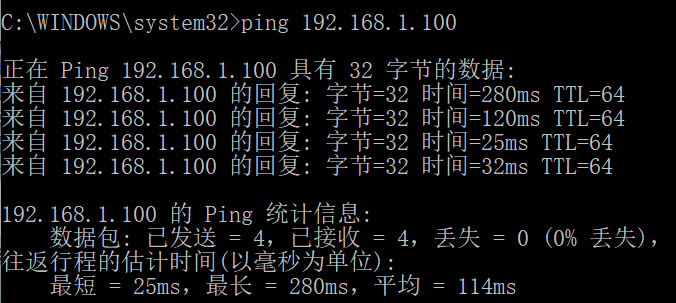
主机B抓包记录



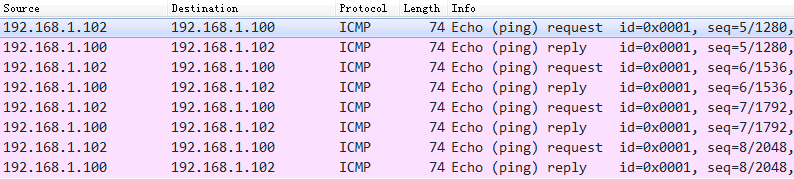
主机B的ARP缓存表



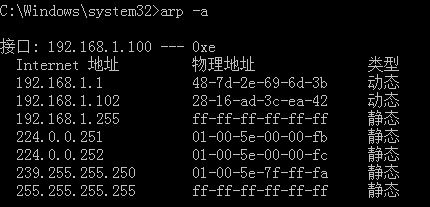
3.B主机pingA主机



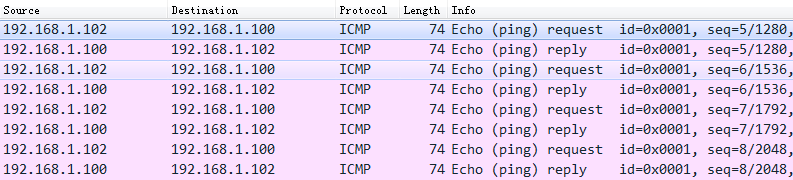
主机A的抓包记录



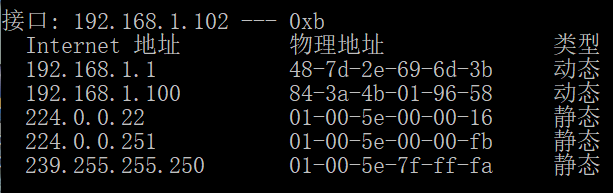
主机A的ARP缓存表



主机B抓包记录



主机B的ARP缓存表

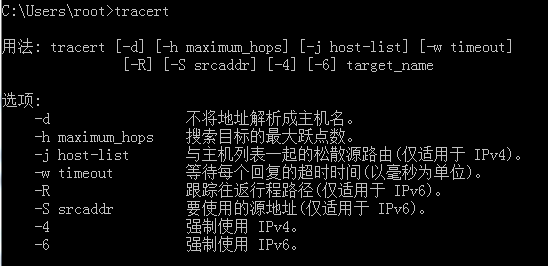


整个ICMP包的长度是74个字节。前面的14个字节为以太网帧头。跟着的20字节为IP帧头。报文由IP首部（20字节）加ICMP报文（40）字节组成。再后面8个字节是ICMP信息头，最后32个字节是ICMP数据。ICMP信息头包括：类型（8或0）、代码（0）、检验和、标示符、序号。请求报文的类型为8，应答报文的类型为0。

**（二）网络路径跟踪（TRACE）实验**

主机A连接UESTC-WiFi，B连接UESTC-Guest-WiFi。用A tracert B

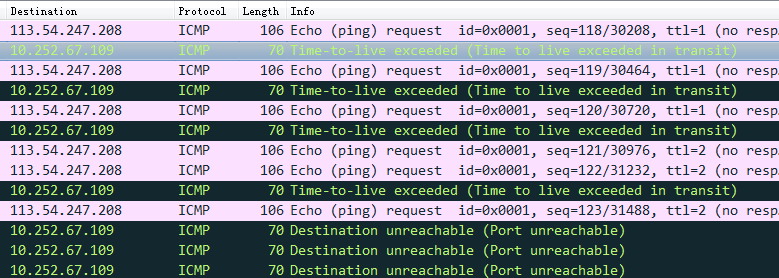
1.tracert命令

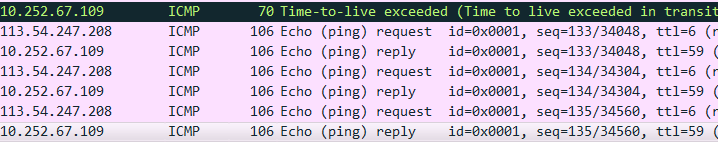


2.tracert对方子网IP



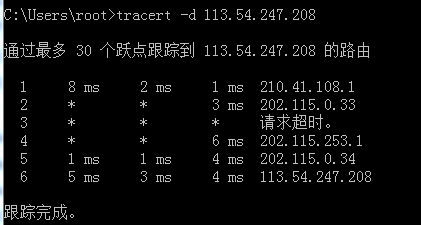
源地址向目的地址113.54.247.208发送UDP数据包，每跳默认发送3个，TTL设置为1；数据包遇到路由器之后，被丢弃，返回Time tolive exceeded超时通知，解析出路由器IP地址210.41.108.1。源地址再发数据包，设置TTL=2，从而解析出第二跳路由10.2.30.1。数据包从seq=118开始每次加1，tracert能够通过seq来唯一识别返回的包。



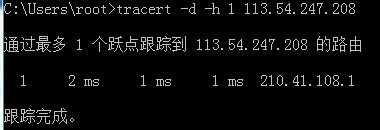


TTL=6时，源地址收到了目的地址的ICMP回应答复（ICMP Echo Reply），说明源地址经过了6跳到达目的地址，与终端显示信息相符。

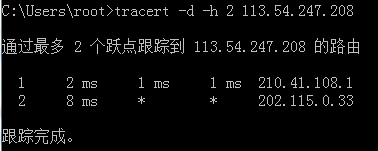
3. tracert –d IP



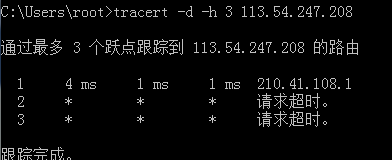
4. tracert –d –h 1 IP



tracert –d –h 2 IP

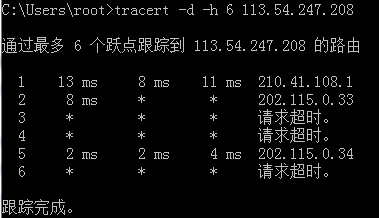


tracert –d –h 3 IP



5. tracert –d –h 6 IP

此时主机B断开网络连接，子网中的IP不存在



**(三）TCP连接实验**

**FTP 响应码**

客户端发送FTP命令后，服务器返回响应码，响应码用三位数字编码表示：

第一个数字给出了命令状态的一般性指示，第二个数字是响应类型的分类，第三个数字提供了更加详细的信息。

第一个数字的含义如下：

1 表示服务器正确接收信息，还未处理。

2 表示服务器已经正确处理信息。

3 表示服务器正确接收信息，正在处理。

4 表示信息暂时错误。

5 表示信息永久错误。

第二个数字的含义如下：

 0 表示语法。

1 表示系统状态和信息。

2 表示连接状态。

3 表示与用户认证有关的信息。

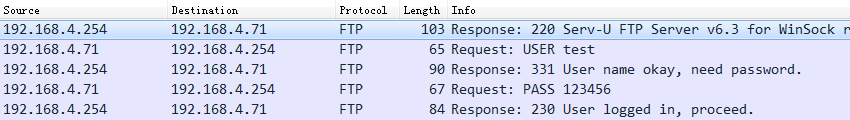
4 表示未定义。

5 表示与文件系统有关的信息。

1. 首次ftp抓包



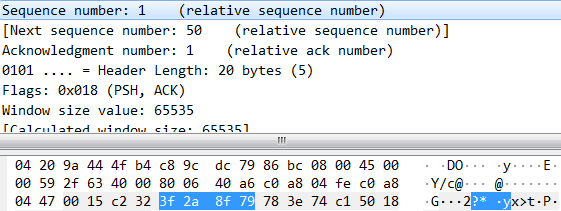
抓包结果



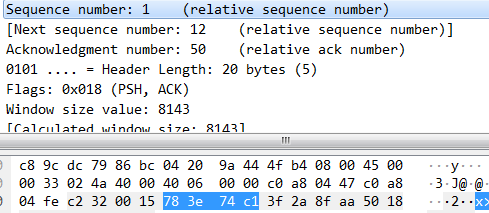


本机ftp进程端口号：21

FTP服务器进程端口号：49714

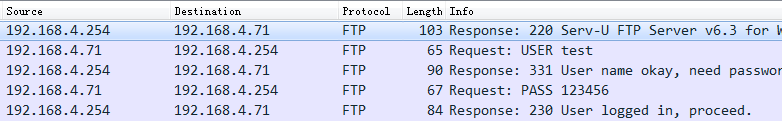


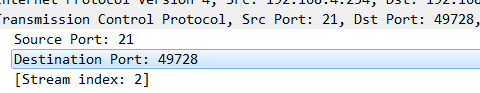
本机TCP初始序号：0x3f2a8f79



服务器TCP初始序号：0x783e74c1

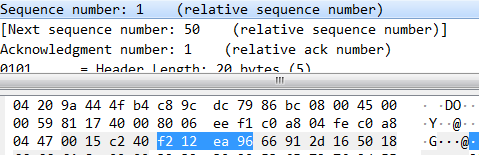
2. 再次抓包



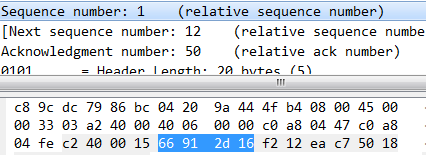


本机ftp进程端口号：21

FTP服务器进程端口号：49728



本机TCP初始序号：0xf212ea96



服务器TCP初始序号：0x66912d16

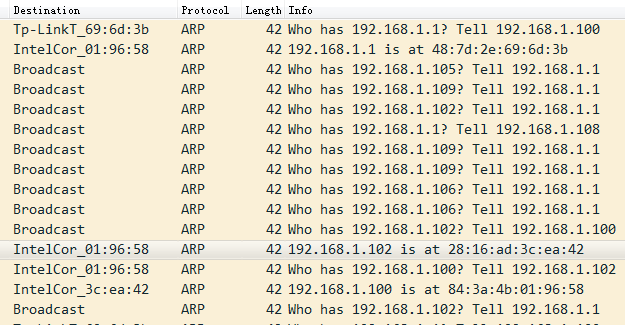
**八、实验结论、心得体会**

**（一）地址解析协议（ARP）实验**

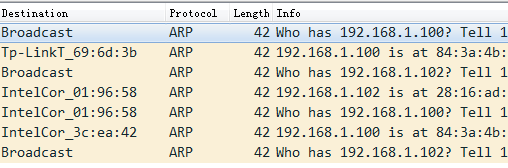
1. **计算机在通信过程中，什么情况下要发送ARP请求分组？什么情况下不发送ARP请求分组？**

在源主机的ARP高速缓存中已经有了该目的IP地址的项目，源主机发送的是广播分组，源主机和目的主机使用点对点链路，就不需要再发送ARP请求分组了。

首次抓包结果：可以看到ARP包头很多



第二次抓包：ARP结果大为减少



1. **如果步骤4或步骤6中显示A主机或B主机上有多余一条的ARP映射表项，请根据实验中的数据报文捕获结果，解释为什么会获得这些ARP映射表项？**

这是系统自动搜索获取的ARP映射表项，因为系统每隔一段时间都会自动搜索可用的ARP

1. **请分析本实验中关于Sniffer软件捕获条件的设置问题：**
2. **Address Type捕获条件是否能设置成为*IP*？为什么？**

能，因为Filter是过滤器，具有筛选功能

1. **如果Station2的地址设置成为对方主机的地址，对实验的捕获操作会有什么影响？**

只捕获当前主机的数据通信信息

1. **如果Station1和Station2的地址均设置成为*any*，对实验的捕获操作会有什么影响？**

可能会有很多别的ARP请求被监听到以致抓包结果混乱

**（二）网络路径跟踪（TRACE）实验**

1. **TRACE的功能是什么？有哪些可能的响应？产生这些响应的原因是什么？**

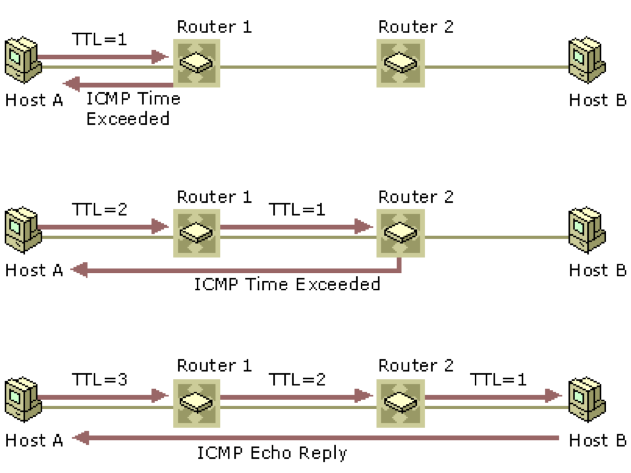
Tracert是一个探测路由的程序，可以让我们看见IP数据报到达目的地经过的路由。

可能的响应：ICMP超时通知（ICMP Time Exceeded Message）、ICMP回应答复（ICMPEcho Reply）

Windows系统使用ICMP请求回显（ICMP Echo Request）数据包进行探测，源地址以目的地址返回的ICMP回应答复（ICMP Echo Reply）作为跟踪结束标志。

1. **分析步骤3中捕获的TRACE报文，阐述TRACE的工作原理。**

**Tracert实现原理**

****

1. 从源地址发出一个ICMP请求回显（ICMP Echo Request）数据包到目的地址，并将TTL设置为1；

2. 到达路由器时，将TTL减1；

3. 当TTL变为0时，包被丢弃，路由器向源地址发回一个ICMP超时通知（ICMP Time Exceeded Message），内含发送IP包的源地址，IP包的所有内容及路由器的IP地址；

4. 当源地址收到该ICMP包时，显示这一跳路由信息；

5. 重复1～5，并每次设置TTL加1；

6. 直至目标地址收到探测数据包，并返回ICMP回应答复（ICMPEcho Reply）；

7. 当源地址收到ICMP Echo Reply包时停止tracert。

**（三）TCP连接实验**

1. **一条TCP连接需要用哪些参数来标识？实验步骤2和实验步骤5中的TCP连接是否是同一条连接？请根据实验记录分别写出其连接标识。**

需要源、目的IP地址及其端口号来标识

不是同一条连接，用的是不同的端口号

步骤2：

源IP：192.168.4.254；目的IP：182.168.4.71；源端口：21；目的端口：49714

步骤5：

源IP：192.168.4.254；目的IP：182.168.4.71；源端口：21；目的端口：49728

1. **本实验中用来建立TCP连接的3个TCP报文段的详细作用分别是什么？每个报文段中包含了哪些用于连接建立的信息？**

A与B建立TCP连接时：首先A向B发SYN（同步请求），然后B回复SYN +ACK（同步请求应答），最后A回复ACK确认，这样TCP的一次连接（三次握手）的过程就建立了！

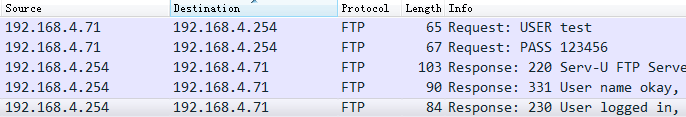
第一次握手：建立连接时,客户端发送syn包(syn=j)到服务器,并进入SYN\_SEND状态,等待服务器确认；

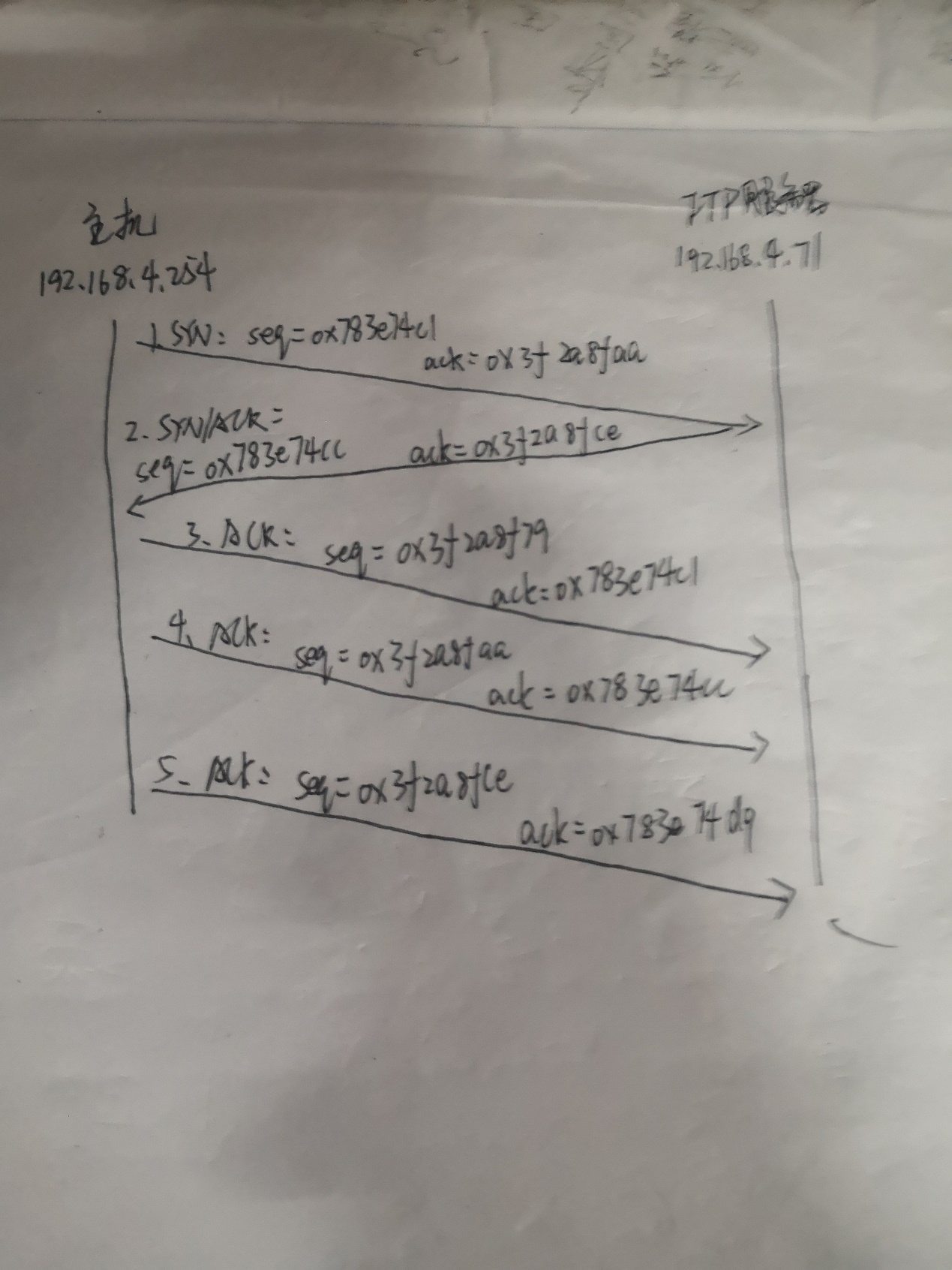
SYN：同步序列编号(Synchronize Sequence Numbers)

第二次握手：服务器收到syn包,必须确认客户的SYN（ack=j+1）,同时自己也发送一个SYN包（syn=k）,即SYN+ACK包,此时服务器进入SYN\_RECV状态；

第三次握手：客户端收到服务器的SYN＋ACK包,向服务器发送确认包ACK(ack=k+1),此包发送完毕,客户端和服务器进入ESTABLISHED状态,完成三次握手。

1. **利用步骤3中保存的捕获数据，画出主机与FTP服务器之间的TCP连接建立过程和TCP连接终止过程的时序交互图，并在图中注明每个TCP报文段的类型、序号和确认号。**



****

**九、对本实验过程及方法、手段的改进建议**

无

**报告评分：**

**指导教师签字：**