**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：周玉川 学 号：2017221302006 指导教师：赵洋**

**实验地点： 信软楼303 实验时间：2019/11/05**

**一、实验室名称：信软楼303**

**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**

（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：

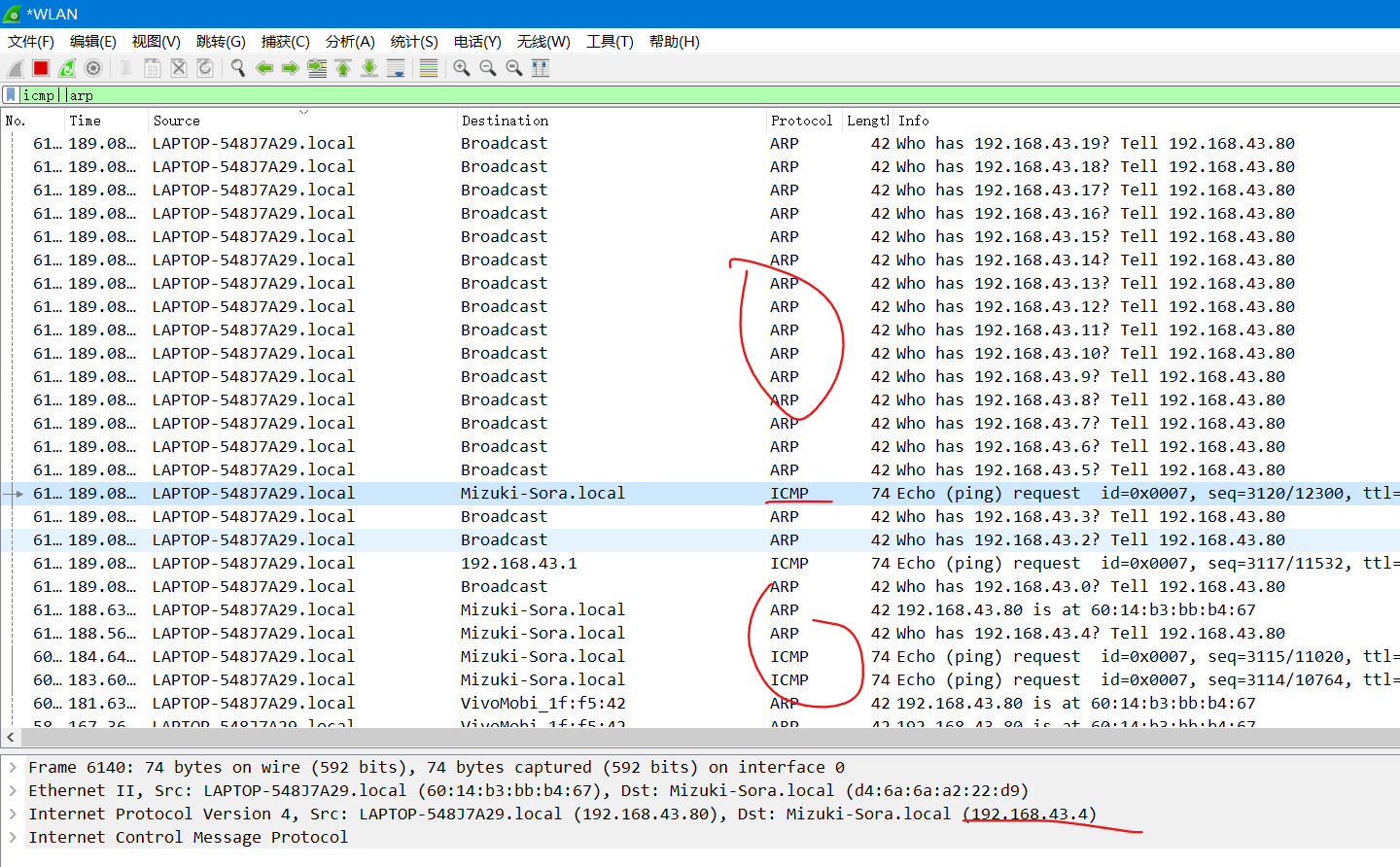
Advanced：Protocol = ARP，ICMP

（2） 清空A、B主机上的ARP缓存表（命令：arp -d \*）。

结果如图1-1

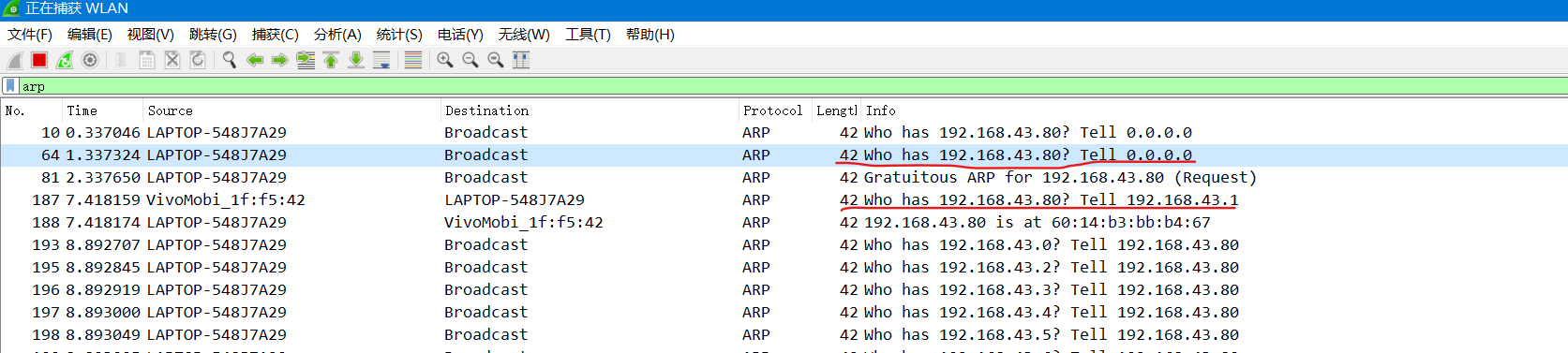
（3） 在A、B主机上启动Sniffer的捕获过程。首先由A主机PING B主机。PING结束以后，停止A、B主机的Sniffer捕获过程，保存捕获数据。

**ICMP协议前会使用ARP协议，说明ping之前会通过arp获得目的ip的mac地址，符合逻辑。**

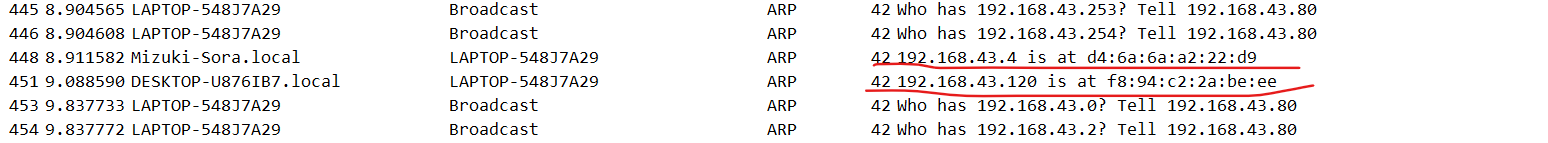


**arp协议大概过程**

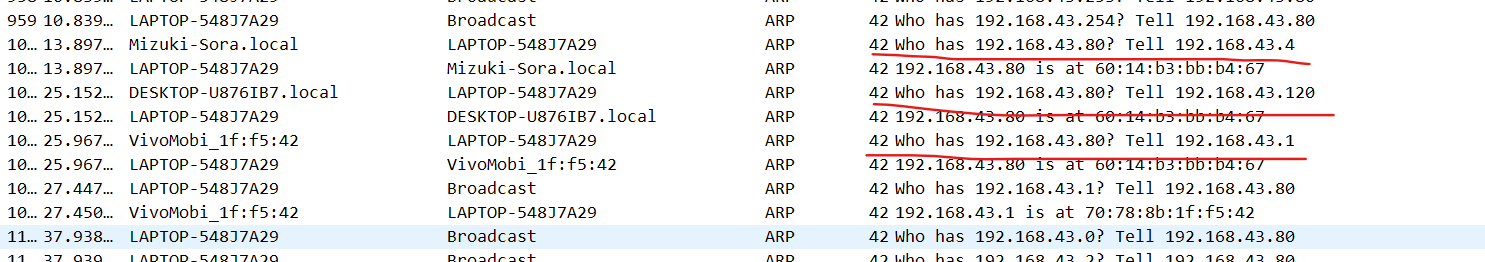
1.首先广播告诉0.0.0.0自己ip的mac地址，然后局域网内广播查询局域网内ip对应的mac地址。



2.得到局域网中两台主机的返回信息，获得mac地址。



3.其他主机开始广播获得本机的mac地址。



（4） 查看A、B主机上的ARP缓存表（命令：arp -a）。

结果如图1-1

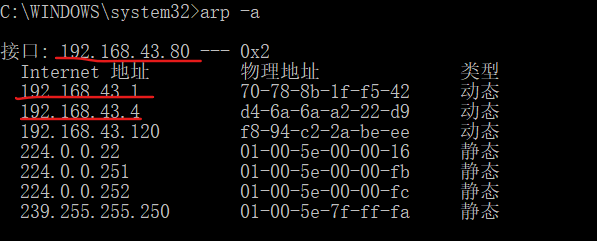
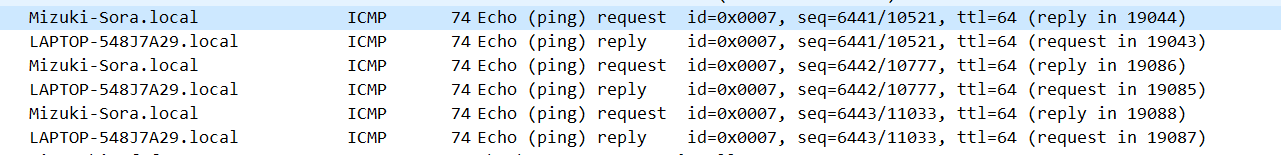
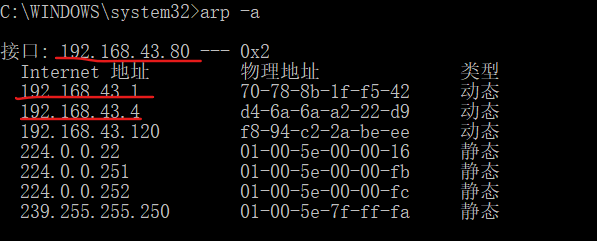


图1-1

（5） 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。



（6） 查看A、B主机上的ARP缓存表（命令：arp -a）。



（7） 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。

**对比步骤三和步骤五，步骤3中ICMP报文之前有大量arp报文，步骤5中抓到的大部分是是ICMP报文。说明ping之前如果没用arp表无法得到目标地址的mac地址，会通过arp协议获得目的ip的mac地址，然后才会进行ping操作，符合逻辑。**

（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：

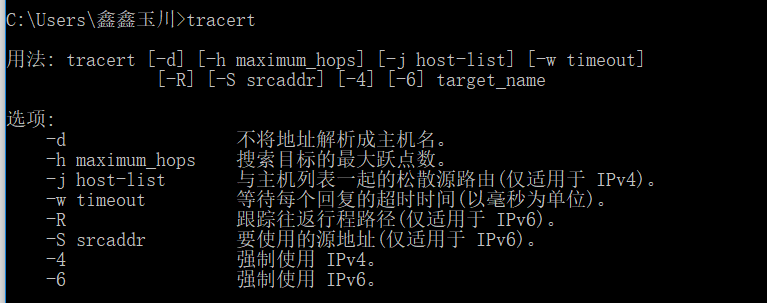
Advanced：Protocol = ICMP

（2） 计算子网A、B的子网地址和子网广播地址。

|  |  |  |  |
| --- | --- | --- | --- |
|  | ip/子网掩码 | 子网地址 | 广播地址 |
| A | 113.54.247.214/23 | 113.54.246.0 | 113.54.247.255 |
| B |  |  |  |

（3） 路径跟踪——TRACE

（A） 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。



（B） 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。

（C） 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。

（D） 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。

（E） 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

（2） 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.

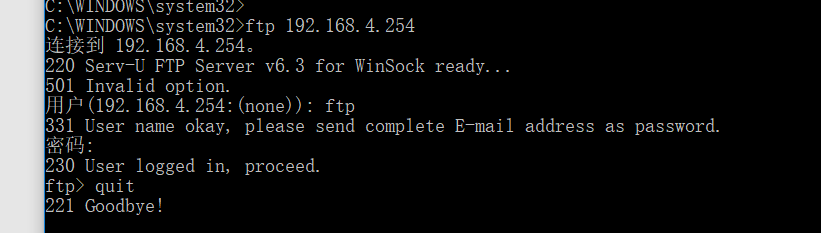
Password: ftp@

230 User logged in, proceed.

ftp> quit

221 Goodbye!

cmd中结果如图所示

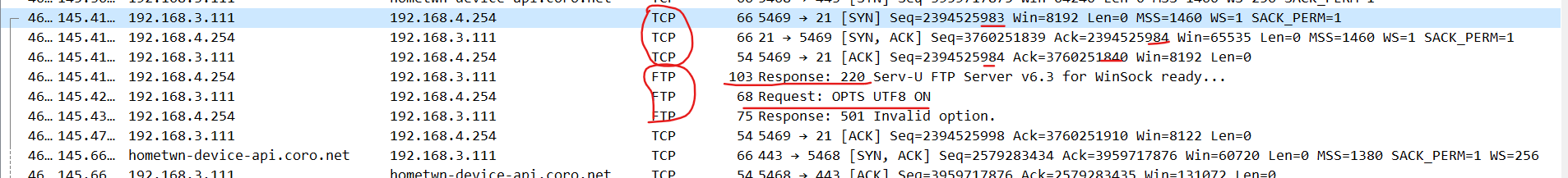


（3） 停止Sniffer的捕获过程，保存捕获数据。

wireShark抓包结果如图

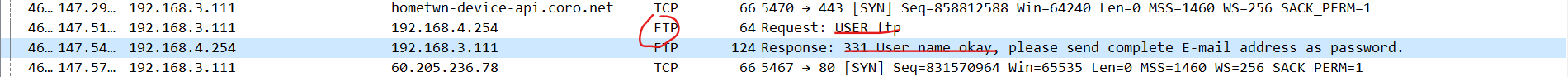
首先三次握手建立tcp连接，然后通过该连接建立ftp应答。

**客户端通知服务器I am coming。ftp服务器回应I am ready,come on。**



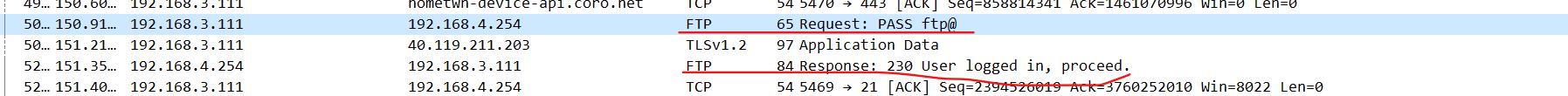
输入用户名，ftp回应。

**客户端说我的名字是ftp。ftp服务器回应现在有230个用户登陆。**

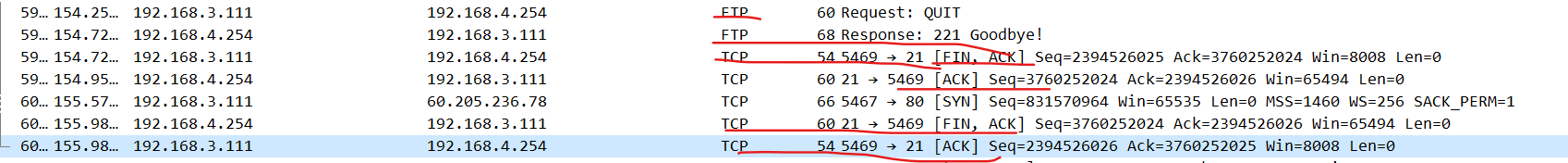


输入密码，ftp服务器回应。

**客户端说我的密码是ftp@。ftp服务器回应现在有290个用户登陆。**

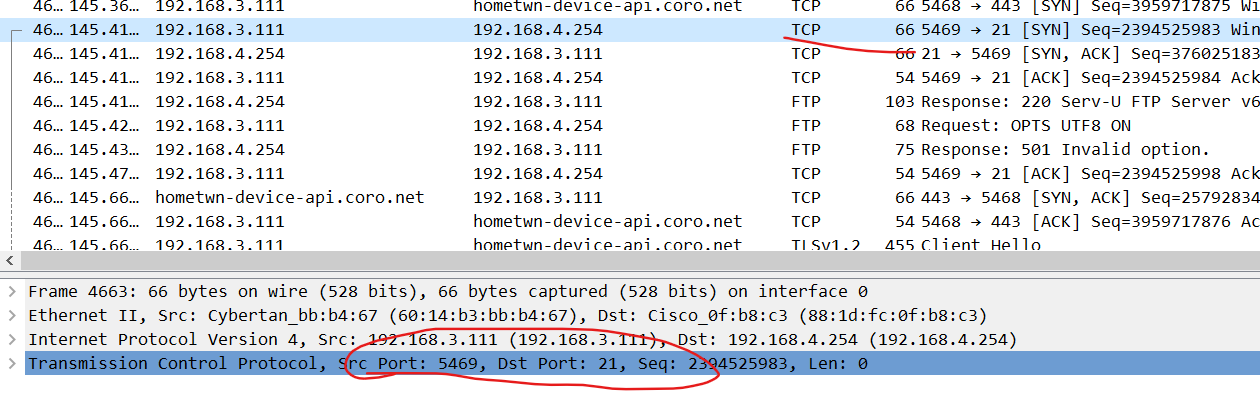


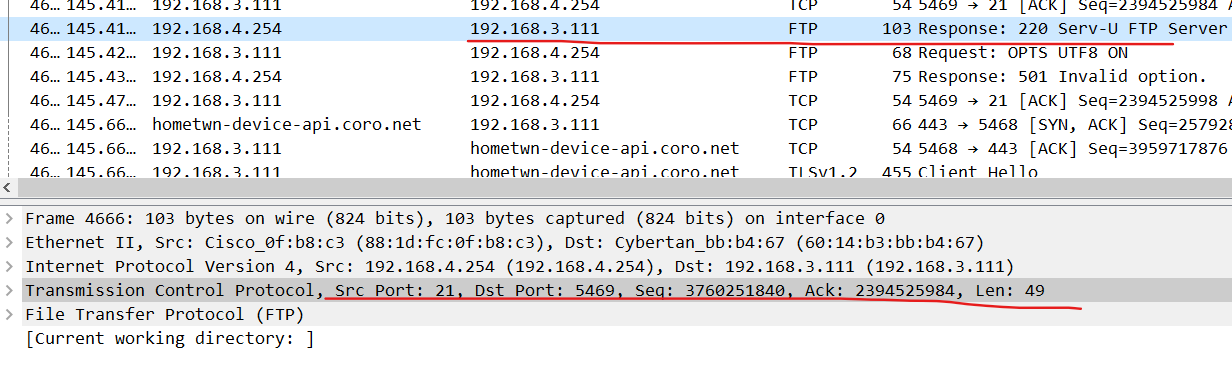
最后主动断开ftp数据传输，进行4次分手断开tcp连接。



（4） 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。

**ftp依托tcp协议使用同一个端口，主机5469端口到ftp服务器21端口**



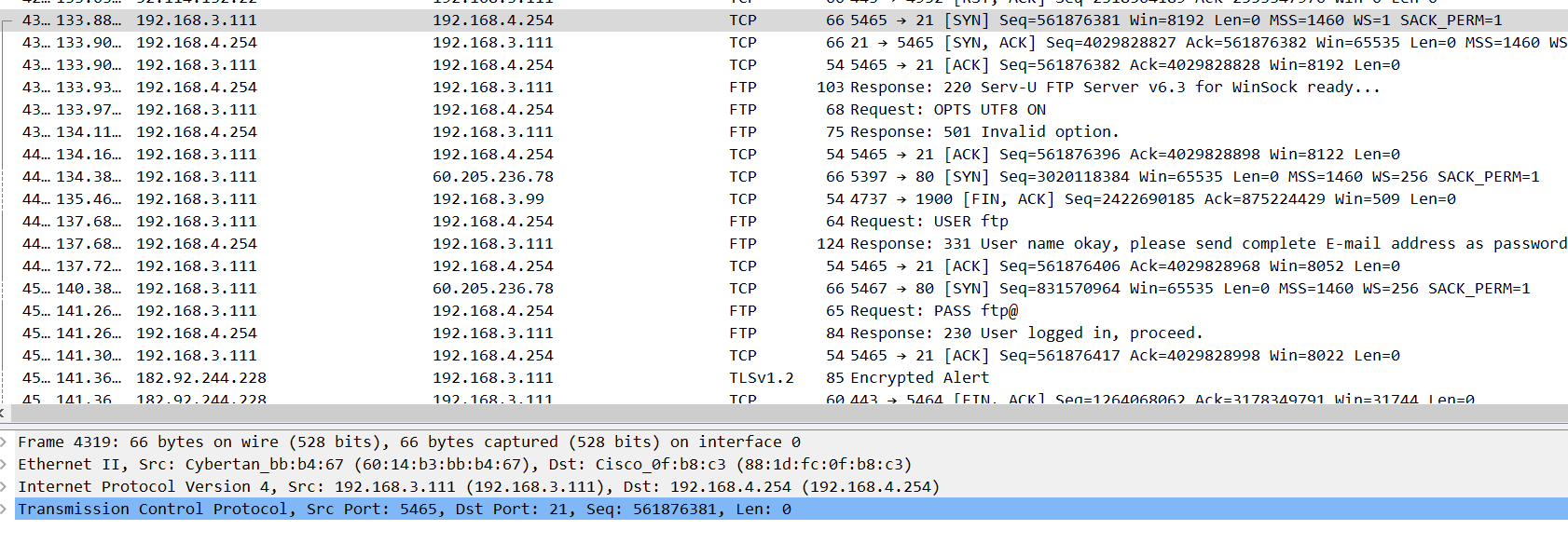


可以发现TCP主机初始序列号是2394525983，f服务器tcp初始序列号是3760251839，

ftp的序号是紧接着tcp的序号的。

（5） 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。

通过这次观察如图，连接端口是5465->21,服务器tcp初始序列号是4029828827，客户端初始序列号是561876381。而ftp的端口号和tcp是相同的，序列号也是紧接着tcp的序列号。



**与步骤4的结果相比较，可以发现，两次连接的初始序列号差别很大，查阅资料了解到序列号是随机的，所以才如此。ftp的序列号总是紧接着tcp的序列号，可以得出结论应用层协议ftp是依靠于tcp协议的。**

**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？

答：当终端中存在arp表而且arp表中可以找到对应ip的mac地址时不会发送arp请求，否则会发送arp请求。

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？

答：这是系统自动搜索捕获的ARP映射表项因为系统每隔一段时间就会自动搜索可用的ARP，用ap-d\*可暂时清除，随后又会出现。

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？
3. 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？
4. 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？

**（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？

答：trace的功能是用于探索源地址到目标地址当中所经过的路线。可能返回中间经过的ip地址，也可能返回超时，也会返回最终到达的地址。

1. 分析步骤3中捕获的TRACE报文，阐述TRACE的工作原理。

而每到达一个点，就会向源地址返回一个信号。例如A要访问D，那么当中经过B，再经过C。当经过B时，会向A返回一个信号，当经过C时，再向A返回一个信号，最后到达D时，返回信号，结束整个过程。在这当中需要注意的是两点，经过的节点需要有IP地址才能返回信号，像普通交换机或hub，没有IP地址，是不可能有信号返回的。二是，网络都是双向的，像上面的例子，如果我们发现tracert D，但到了C已经没有信号返回了，并不能说明信号到不了D，也有可能是信号到了，但中途有节点无法返回信号而已。

**（3）TCP连接实验**

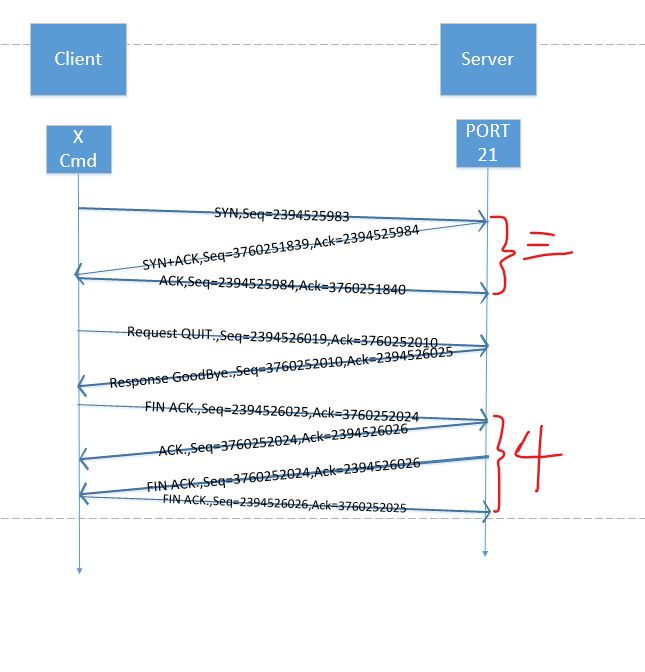
1. 一条TCP连接需要用哪些参数来标识？实验步骤2和实验步骤5中的TCP连接是否是同一条连接？请根据实验记录分别写出其连接标识。

答：一条tcp连接可以用源ip地址和源端口，目的IP地址和目的IP地址以及tcp序列号的范围判断。

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？

答：第一次握手是为了确认客户端tcp初始序列号，报文文中包括源ip和端口以及初始序列号。第二次握手为了确认服务端tcp初始序列号，报文中包括服务端初始序列号，期望收到的客户端报文的序列号。第三次握手代表客户端收到服务端回复，客户端已经准备好。

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**

实验很棒，通过实践深入理解理论，老师很棒，辛苦了。

**报告评分：**

**指导教师签字：**