# 网络协议分析及编程

# 实验报告

学　　院：计算机学院·网络空间安全学院

专　　业：2019级计算机科学与技术2班

学　　号：201905556608

姓　　名：姜德琛

时　　间：2021.11.22

指导老师：周维

# 实验报告 1

课程 网络协议分析及编程 实验地点 信息楼 6 楼网络安全实验室

姓　　名 姜德琛 实 验 日 期： 2021.10.29
学　　号 201905556608 实验报告日期： 2021.11.28
同组人姓名 王文海 报 告 退 发：（订正 、 重做 ）
同组人学号 201805821012 教师审批签字：

---

## 一. 实验名称

以太网链路层帧格式分析实验

## 二. 环境（详细说明运行的操作系统，网络平台，机器的 IP 地址）

1、 操作系统：Windows7 操作系统
2、网络平台：PC1，PC2，交换机*1
3、PC1 的 ip：172.22.10.8
PC2 的 ip：172.22.10.9

## 三. 实验目的

了解 EthernetV2 标准规定的 MAC 帧结构，初步了解 TCP/IP 的主要协议和协议的层次结构.

## 四. 实验内容及步骤

1. 连接好设备，配置 PC1 和 PC2 的 IP 地址，PC1 为：172.22.10.10，PC2 为 172.22.10.11，如图 4.1.1 所示，网络拓扑图如图 4.1.2 所示。

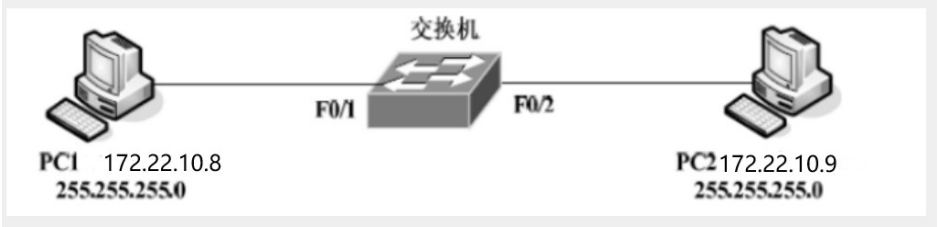



图 4.1.2

2. 在 PC1 和 PC2 上运行 wireshark 截获报文，为了只截获和实验内容有关的报文，将 wireshark 的 Captrue Filter 设置为“No Broadcast and

no Multicast ”，如图 4.2.1 过滤器设置所示。

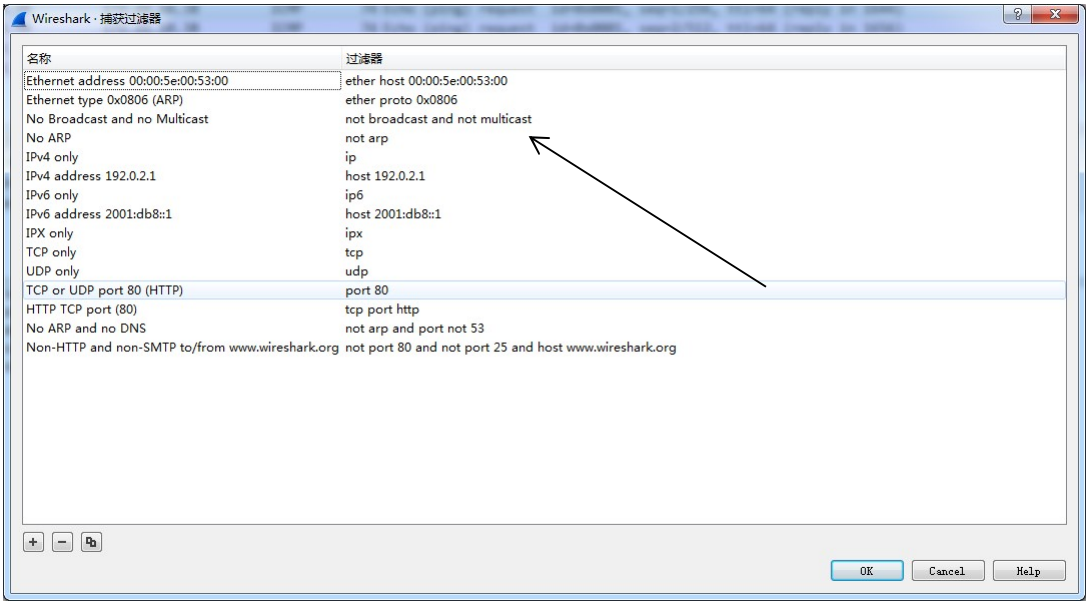



图 4.2.1 过滤器设置

3. 在 PC1 的 cmd 控制终端中输入命令 “Ping 172.22.10.09”，键入回车，如图 4.3.1cmd 界面所示

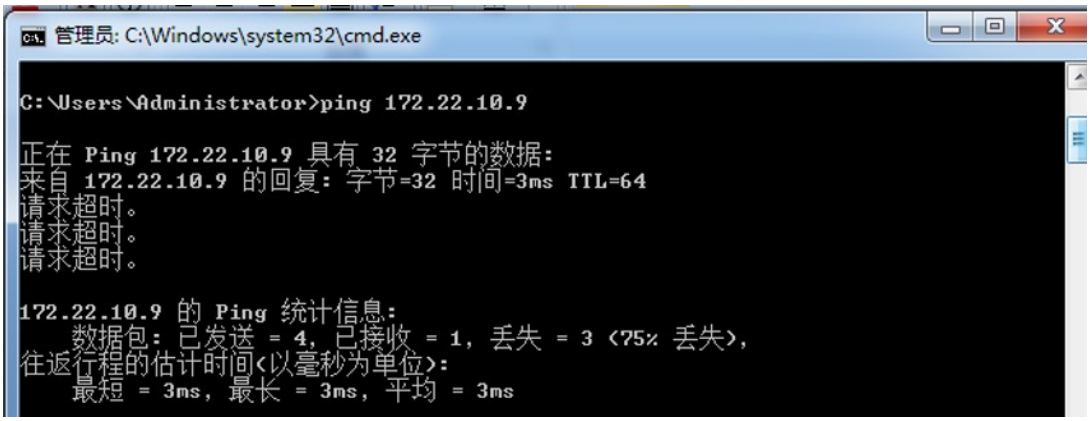



图 4.3.1cmd 界面

4. 停止截获报文：将结果保存为 MAC-201905556608，并设置过滤条件 ip. src eq 172.22.10.8 and ip.dst eq 172.22.10.9，对截获的报文进行分析，报文如图 4.4.1 截获报文所示

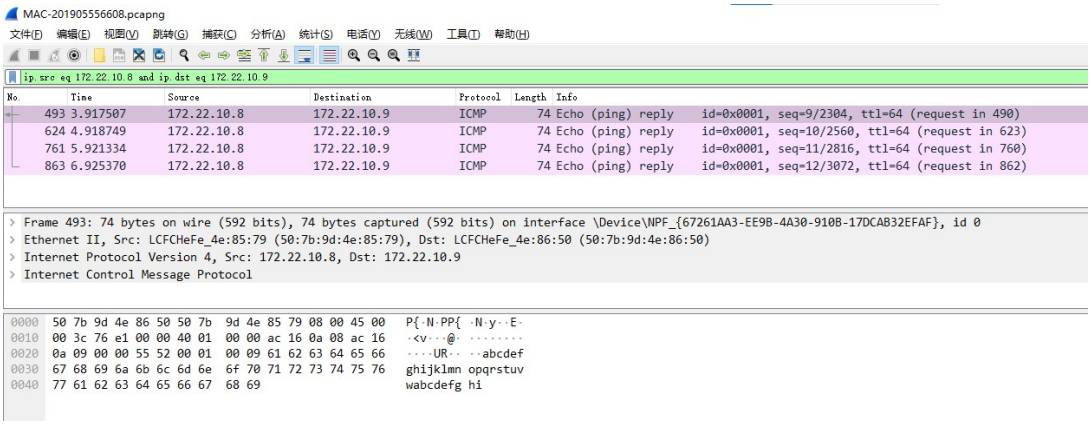



图 4.4.1 截获报文

5. 在 PC1 和 PC2 上运行 wireshark 截获报文，然后进入 PC1 的 Windows 命令行窗口，执行如下命令：

net send 172.22.10.9 Hello

这是 PC1 向 PC2 发送消息的命令，等到 PC2 显示器上显示收到消息后，终止截获报文。注意 PC1 和 PC2 的信使服务应启动。

但是实际操作过程中，由于 win7 系统没有 net send 的命令，故此执行命令更改为：

MSG/server：172.22.10.9 *“Hello”

①打开注册表编辑器，修改里面的 AllowRemoteRPC 的值如图所示，数值数据由 0 改为 1。如图 4.5.1，图 4.5.2 所示。

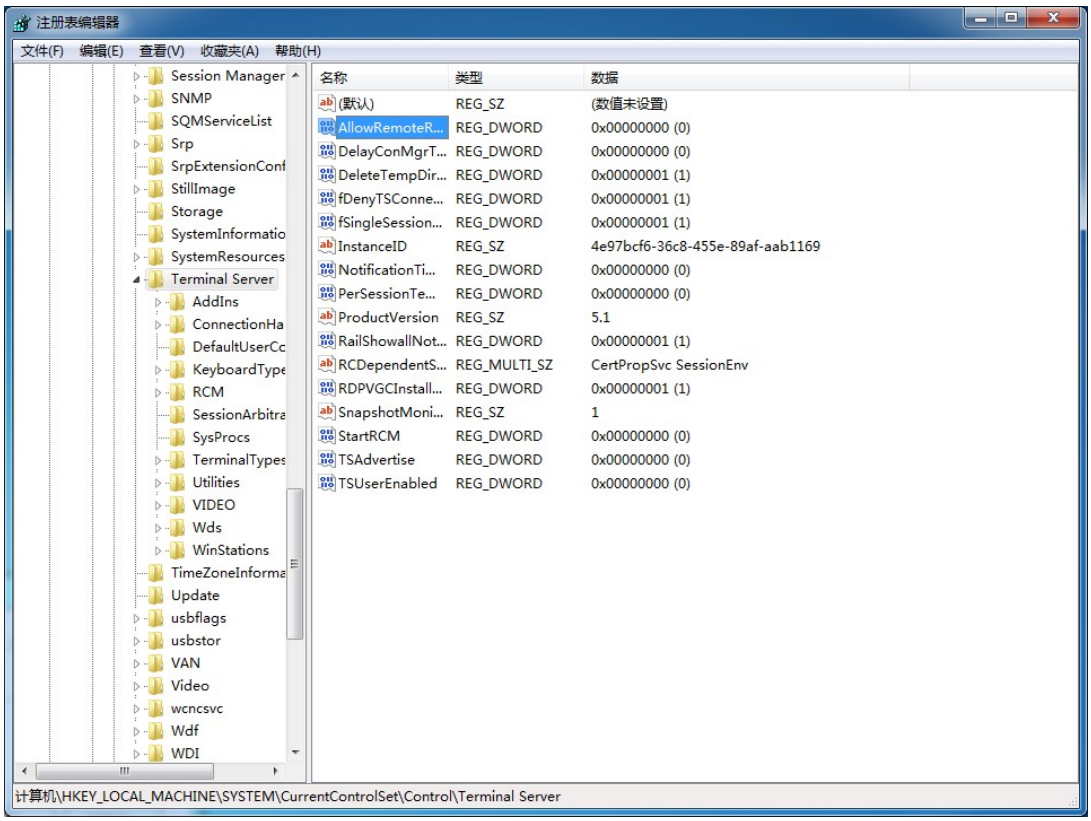


图 4.5.1


图 4.5.2

②修改凭据管理器，设置用户名及密码，如图 4.5.3，图 4.5.4 所示。

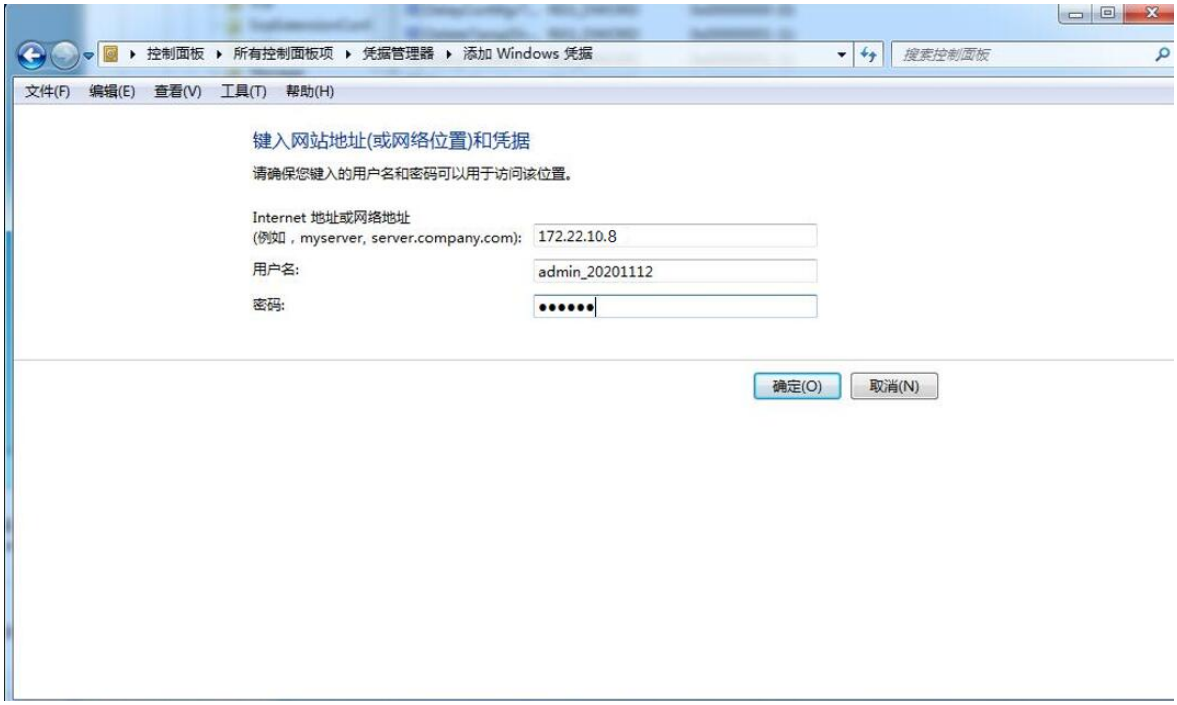



图 4.5.3


图 4.5.4

③在 PC2 上修改管理员密码，如图 4.5.5 所示。

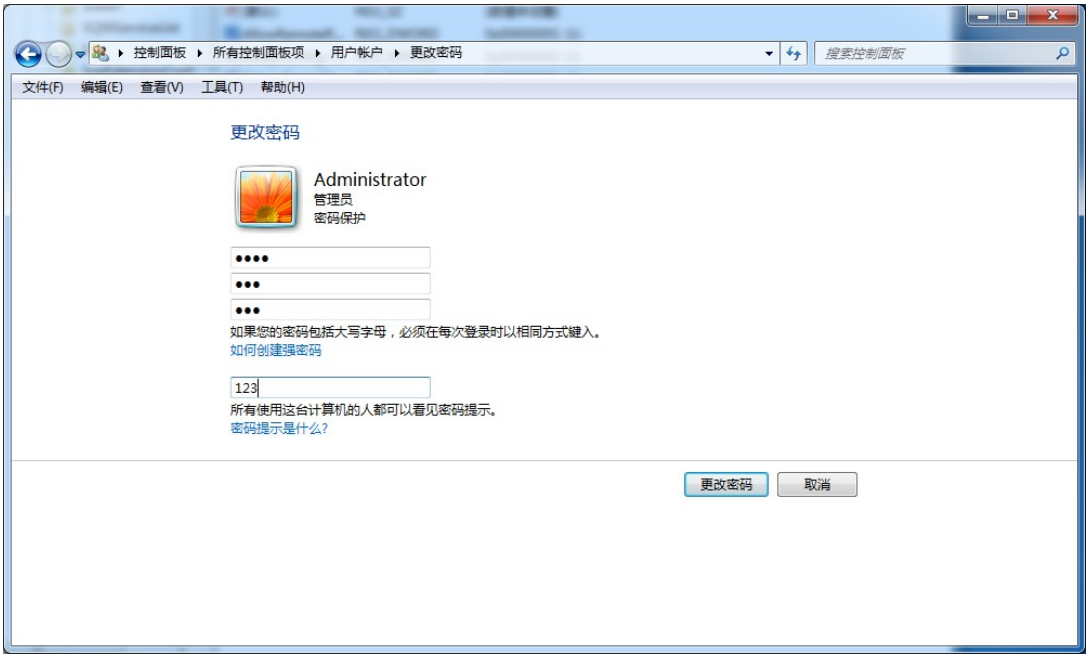



图 4.5.5

④由 PC1 向 PC2 传递信息，消息接受界面如图 4.5.6 所示。

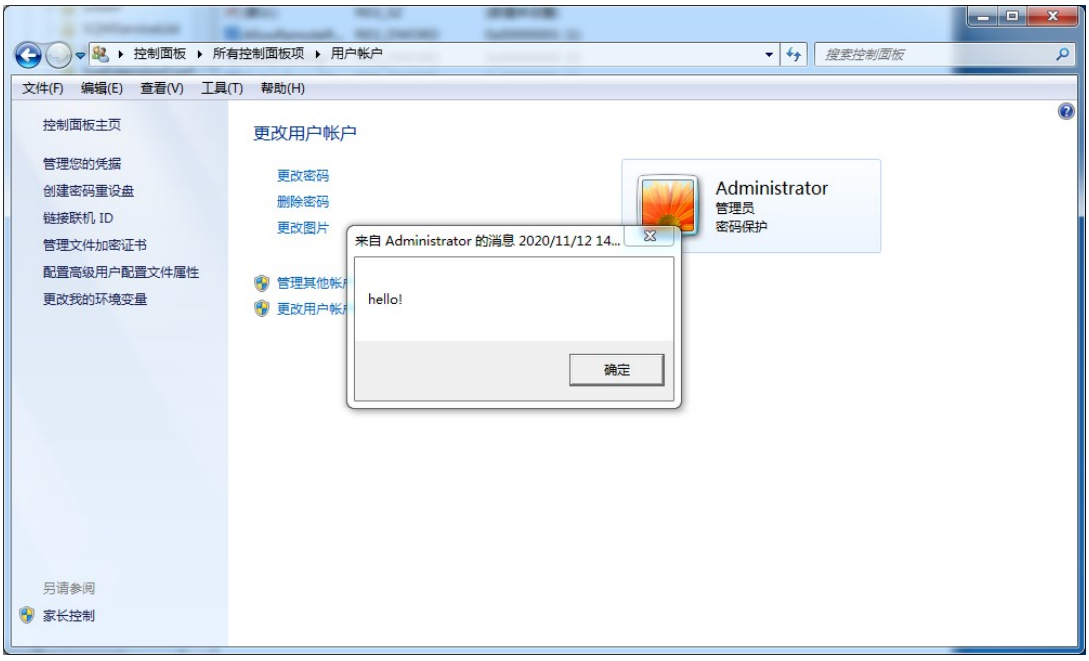



图 4.5.6

⑤捕捉到的报文如图 4.5.7 所示。

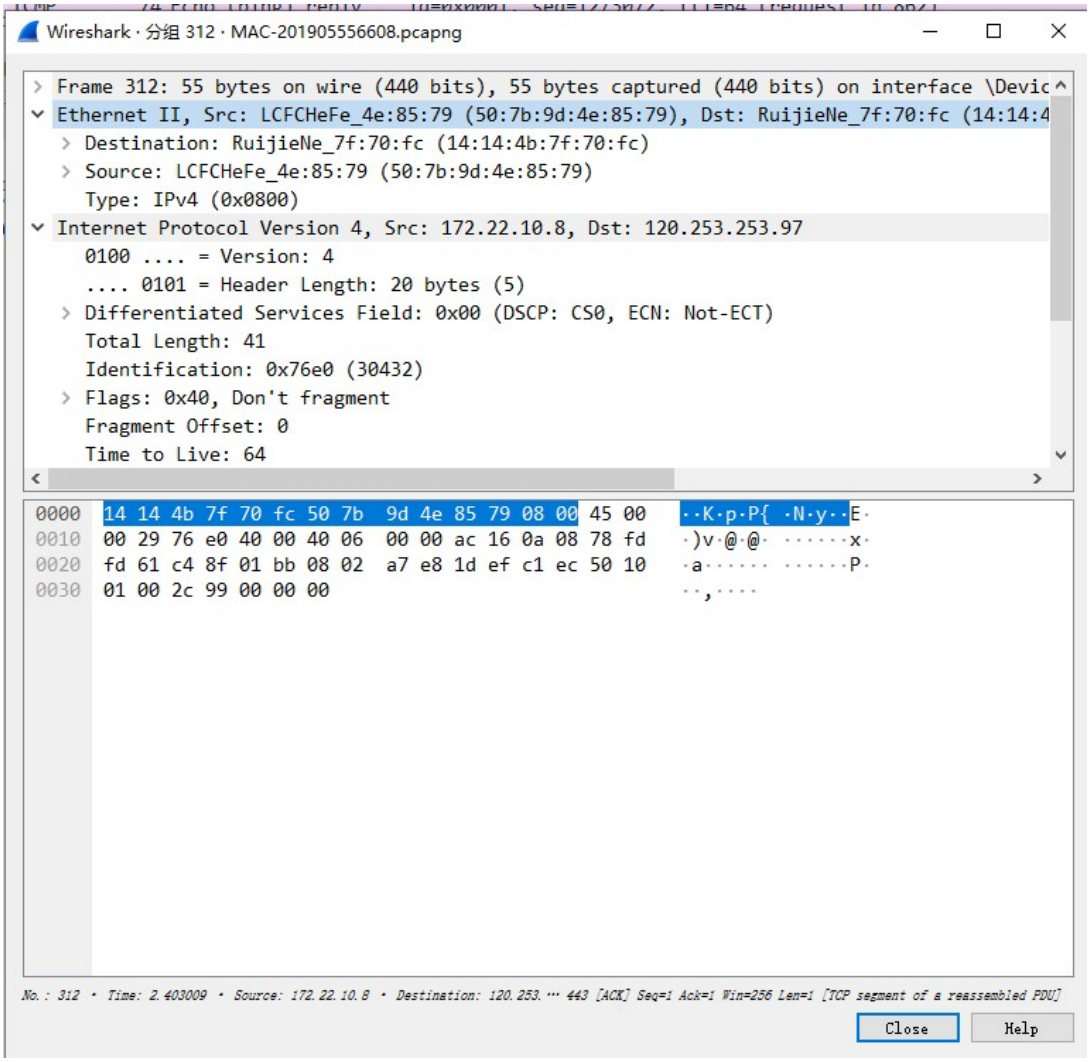


图 4.5.7

## 五.实验结果

1、列出截获的报文中的协议类型，观察这些协议之间的关系。

答：捕获到的有 arp 报文，tcp 报文，icmp 报文。

①arp：地址解析协议，是根据 IP 地址获取物理地址的一个 TCP/IP 协议。主机发送信息时将包含目标 IP 地址的 ARP 请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址。

②tcp：传输控制协议，是一种面向连接的、可靠的、基于字节流的传输层通信协议。

③icmp：Internet 控制报文协议。它是 TCP/IP 协议簇的一个子协议，用于在 IP 主机、路由器之间传递控制消息。

报文中的协议类型有 IP 协议,ICMP 协议。协议之间是倒向的树形结构，依次是链路层，网络层，传输层和应用层。数据链路层显示的 Ethertype=0800，可知网络层使用的是 IP 协议。网络层中还有 ICMP 协议，将在执行过程中的出错报告，报文分组封装成 IP 分组，送给链路层。

2、在网络课程学习中，EthernetV2 规定以太网的 MAC 层的报文格式分为 7 字节的前导符、1 字节的帧首定界、6 字节的目的 MAC 地址、6 字节的源 MAC 地址、2 字节的类型、46～1500 字节的数据字段和 4 字节的帧尾校验字段。分析一个 Ethernet V2 帧，查看这个帧由几部分组成，缺少了哪几部分？为什么？

答:一个 Ethernet V2 帧由 6 字节的目的 MAC 地址、6 字节的源 MAC 地址，2 字节的类型、46-1500 字节的数据字段四个部分组成，少了 7 字节的前导符、1 字节的帧首定界和 4 字节的帧尾校验字段。这是因为 Wireshark 的设计原理，能捕捉数据链路层上的包，是已经校验正确的，就不再显示帧尾的 4 字节的 FCS 校验

3、报文分析

| 此报文类型 | | ICMP |
|---|---|---|
| 此报文的基本信息（数据报文列表窗口中的 Information 项的内容） | | Echo (ping) request id=0x1bb2, seq=37/9472, ttl=64 (reply in 1160) |
| Ethernet II 协议树中 | Source 字段值 | 50:7b:9d:4e:85:79 |
| | Destination 字段值 | 50:7b:9d:4e:86:50 |
| Internet Protocol 协议树中 | Source 字段值 | ac 16 0a 08 |
| | Destination 字段值 | ac 16 0a 09 |
| Internet Control Message Protocol 协议树 | Checksum 字段值 | 0x5552 |
| | Identifier (LE)字段值 | 0x0100 |

## 六. 实验中的问题及心得

这是第一次的网络协议实验，主要是进行网络抓包软件的使用以及对所抓到的包进行，网络链路层上的协议分析。在整个过程中，遇到了 win 7 不支持 net send 系统命令的困难，查资料来找到了另一个替代命令 msg，然后为了正常使用这些命令，我们来修改了一些系统参数，所以总的来说本次实验的体验还是不错的。在跟随实验指导的步骤进行下，整个过程十分顺利，通过本次实验，我对 wireshark 抓包软件的使用流程有了进一步了解，比起上个学期的计算机网原理实验的点到为止，我觉得这次的实验让我收获更多，期待后面的实验。

# 实验报告 2

课程 网络协议分析及编程 实验地点 信息楼 6 楼网络安全实验室

姓　　名 姜德琛 实 验 日 期： 2021.10.29
学　　号 201905556608 实验报告日期： 2021.11.28
同组人姓名 王文海 报 告 退 发： （订正 、 重做 ）
同组人学号 201805821012 教师审批签字：

---

## 一．实验名称

IP 协议分析实验

## 二．环境（详细说明运行的操作系统，网络平台，机器的 IP 地址）

1.操作系统：Windows7 操作系统

2.网络平台：PC1，PC2，交换机*1

3.PC1 的 ip：172.22.10.8
PC2 的 ip：172.22.10.9

## 三．实验目的

使用 Ping 命令在两台计算机之间发送发送大于 MTU 的数据报，验证分片过程，加深对 IP 协议的理解.

## 四．实验内容及步骤

1.连接好设备，配置 PC1 和 PC2 的 IP 地址，网络拓扑图如图 4.1.1 所示。

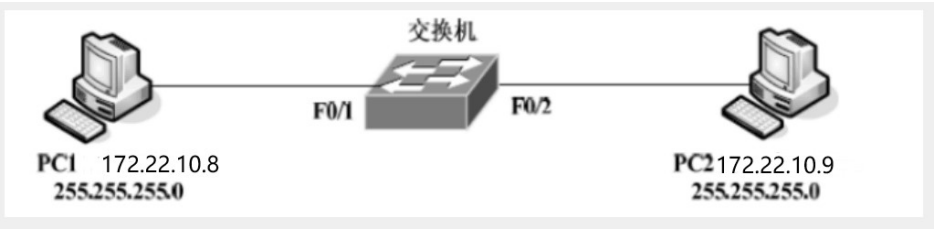



图 4.1.1

2. 完成路由器和 PC1、PC2 的相关配置；

3. 在 PC1、PC2 两台计算机上运行 Ethereal，为了只截获和实验有关的数据报，设置 Ethereal 的截获条件为对方主机的 IP 地址，开始截获报文，截获的报文如图 4.3.1 所示。

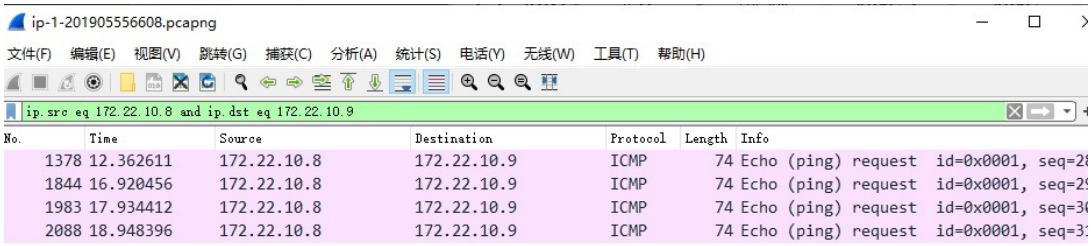



图 4.3.1

4. 任取一个数据报，分析 IP 协议的报文格式，截获的数据报报文如图 4.3.2 所示。

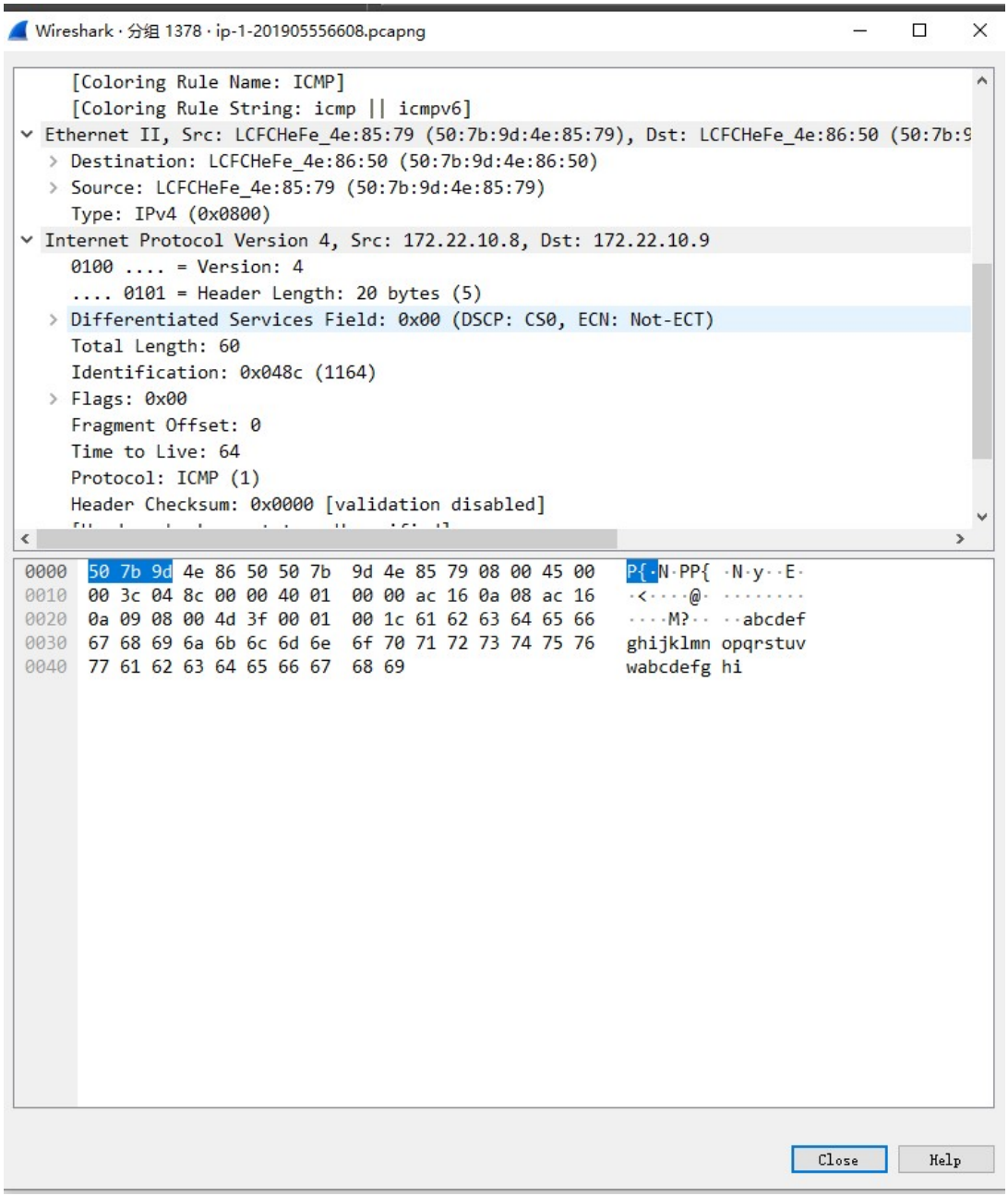



图 4.3.2

## 五．实验结果

1.IP 协议报报文分析表

| 字段 | 报文信息 | 说明 |
|---|---|---|
| 版本 | 4 | IP 协议的版本 |
| 头长 | 20 字节 | 头部总长度 |
| 服务类型 | 0x00 | |
| 总长度 | 60 字节 | 总长度指首部和数据之和的长度 |
| 标识 | 0x048c(1164) | 需要分片时将该字段复制到所有分片中，用以标识 |
| 标志 | 0x00 | 最后一位标志是否还有分片，首位标志是否可以分片 |
| 片偏移 | 0 | 分片后，某片再原分组中的相对位置 |
| 生存周期 | 64 | 数据报在网络中的寿命 |
| 协议 | ICMP（1） | 指出此数据报携带的数据是使用何种协议 |
| 校验和 | 0x0000 | 检验数据报的首部，不包括数据部分 |
| 源地址 | 172.22.10.8 | 发送 IP 数据报的 PC 机 |
| 目的地址 | 172.22.10.9 | 接受该 IP 数据报的 PC 机 |

2.查看该数据报的源 IP 地址和目的 IP 地址，他们分别是哪类地址？体会 IP 地址的编址方法。

答：源 IP 地址：172.22.10.8　属于 B 类地址

目的 IP 地址：172.22.10.9 属于 B 类地址

IP 地址的编址方法：

1、IP 地址

是给每个连接在 Internet 上的主机分配的一个 32bit 地址。IP 地址分为网络 IP 和主机 IP，地址有两部分组成，一部分为网络地址，另一部分为主机地址。IP 地址分为 A、B、C、D、E 5 类。网络地址的位数直接决定了可以分配的网络数；主机地址的位数则决定了网络中最大的主机数。主机 ID 不能全为 0 或全为 1，全为 0 用于网络地址，全为 1 用于广播。D、E 类 IP 不分网络 ID 和主机 ID。如图 5.2.1 所示

（1）A 类地址： 网络位 8（7）位+主机位 24 位，IP 范围：1.0.0.0--126.255.255.255

（2）B 类地址：网络位 16（14）位+主机位 16 位,IP 范围：128.0.0.0--191.255.255.255

（3）C 类地址：网络位 24（21）位+主机位 8 位，IP 范围：192.0.0.0--223.255.255.255

（4）D 类地址：用于组播，IP 范围：224.0.0.0——239.255.255.255

（5）E 类地址：用于研究，IP 范围：240.0.0.0——255.255.255.255


| 网络类别 | 第一个可指派的网络号 | 最后一个可指派的网络号 | 最大可指派的网络数量 | 每个网络中的最大主机数量 | 不能指派的网络号 | 占总地址空间 |
|---|---|---|---|---|---|---|
| A | 1 | 126 | 126 ($2^{(8-1)}-2$) | 16777214 ($2^{24}-2$) | 0和127 | 1/2 ($2^{(32-1)}/2^{32}$) |
| B | 128.0 | 191.255 | 16384 ($2^{(16-2)}$) | 65534 ($2^{16}-2$) | 无 | 1/4 ($2^{(32-2)}/2^{32}$) |
| C | 192.0.0 | 223.255.255 | 2097152 ($2^{(24-3)}$) | 254 ($2^{8}-2$) | 无 | 1/8 ($2^{(32-3)}/2^{32}$) |

| 网络类别 | 作 用 | 第一个地址 | 最后一个地址 | 地址数量 | 占总地址空间 |
|---|---|---|---|---|---|
| D | 多播地址 | 224.0.0.0 | 239.255.255.255 | 268435456 ($2^{28}$) | 1/16 ($2^{(32-4)}/2^{32}$) |
| E | 保留为今后使用 | 240.0.0.0 | 255.255.255.255 | 268435456 ($2^{28}$) | 1/16 ($2^{(32-4)}/2^{32}$) |

| 一般不使用的特殊IP地址 | | | | |
|---|---|---|---|---|
| 网络号 | 主机号 | 作为源地址 | 作为目的地址 | 代表的意思 |
| 0 | 0 | 可以 | 不可 | 在本网络上的本主机（DHCP协议） |
| 0 | host-id | 可以 | 不可 | 在本网络上的某台主机host-id |
| 全1 | 全1 | 不可 | 可以 | 只在本网络上进行广播（各路由器均不转发） |
| net-id | 全1 | 不可 | 可以 | 对net-id上的所有主机进行广播 |
| 127 | 非全0或全1 | 可以 | 可以 | 用于本地软件环回测试 |

图 5.2.1

在 IP 地址 3 种主要类型里，各保留了 3 个区域作为私有地址，其地址范围如下：

A 类地址：10.0.0.0～10.255.255.255

B 类地址：172.16.0.0～172.31.255.255

C 类地址：192.168.0.0～192.168.255.255

回送地址：127.0.0.1 也是本机地址，等效于 localhost 或本机 IP。一般用于测试使用。例如：ping 127.0.0.1 来测试本机 TCP/IP 是否正常。

2、子网掩码

它是一种用来指明一个 IP 地址的哪些位标识的是主机所在的子网，以及哪些位标识的是主机的位掩码。子网掩码不能单独存在，它必须结合 IP 地址一起使用。子网掩码只有一个作用，就是将某个 IP 地址划分成网络地址和主机地址两部分。 子网掩码是一个 32 位地址，用于屏蔽 IP 地址的一部分以区别网络标识和主机标识，并说明该 IP 地址是在局域网上，还是在远程网上。子网掩码——屏蔽一个 IP 地址的网络部分的“全 1”比特模式。对于 A 类地址来说，默认的子网掩码是 255.0.0.0；对于 B 类地址来说默认的子网掩码是 255.255.0.0；对于 C 类地址来说默认的子网掩码是 255.255.255.0。通过子网掩码，就可以判断两个 IP 在不在一个局域网内部，可以看出有多少位是网络号，有多少位是主机号，如图 5.2.2 所示。

| 类别 | 默认子网掩码 |
|---|---|
| A类 | 255.0.0.0 |
| B类 | 255.255.0.0 |
| C类 | 255.255.255.0 |

图 5.2.2

3.IP 协议的工作模式

IP 协议提供了一种分层的、与硬件无关的寻址系统，它可以在复杂的路由式网络中传递数据所需的服务，可以将多个交换网络连接起来，在源地址和目的地址之间传送数据包。同时，它还提供数据重新组装功能，以适应不同网络对数据包大小的要求。

在一个路由式网络中，源地址主机向目标地址主机发送数据时，IP 协议是如何将数据成功发送到目标主机上的呢？

由于网络分同网段和不同网段两种情况，工作方式如下：

a）同网段

如果源地址主机和目标地址主机在同一网段，目标 IP 地址被 ARP 协议解析为 MAC 地址，然后根据 MAC 地址，源主机直接把数据包发给目标主机。

b）不同网段

如果源地址主机和目标地址主机在不同网段，数据包发送过程如下：网关（一般为路由器）的 IP 地址被 ARP 协议解析为 MAC 地址。根据该 MAC 地址，源主机将数据包发送到网关。

网关根据数据包中的网段 ID 寻找目标网络。如果找到，将数据包发送到目标网段；如果没找到，重复步骤（1）将数据包发送到上一级网关。数据包经过网关被发送到正确的网段中。目标 IP 地址被 ARP 协议解析为 MAC 地址。根据该 MAC 地址，数据包被发送给目标地址的主机。

## 六．实验中的问题及心得

这是网络协议终端编程的第二次实验课，这次我们是对网络层的协议进行分析。上个学期的计算机网络原理实验里我们用抓包软件对 tcp 协议进行过分析，但是当时没有着重分析 ip 报文，这次不只是 ppt 上的内容了，同时这次也对分析过程总结如下：

分析 IP 报文各部分的作用，如下所述：

IP 报头的最小长度为 20 字节，上图中每个字段的含义如下：

(1) 版本（version）

占 4 位，表示 IP 协议的版本。通信双方使用的 IP 协议版本必须一致。目前广泛使用的 IP 协议版本号为 4，即 IPv4。

(2) 首部长度（网际报头长度 IHL）

占 4 位，可表示的最大十进制数值是 15。这个字段所表示数的单位是 32 位字长（1 个 32 位字长是 4 字节）。因此，当 IP 的首部长度为 1111 时（即十进制的 15），首部长度就达到 60 字节。当 IP 分组的首部长度不是 4 字节的整数倍时，必须利用最后的填充字段加以填充。数据部分永远在 4 字节的整数倍开始，这样在实现 IP 协议时较为方便。首部长度限制为 60 字节的缺点是，长度有时可能不够用，之所以限制长度为 60 字节，是希望用户尽量减少开销。最常用的首部长度就是 20 字节（即首部长度为 0101），这时不使用任何选项。

(3) 区分服务（tos）

也被称为服务类型，占 8 位，用来获得更好的服务。这个字段在旧标准中叫做服务类型，但实际上一直没有被使用过。1998 年 IETF 把这个字段改名为区分服务（Differentiated Services，DS）。只有在使用区分服务时，这个字段才起作用。

(4) 总长度（totlen）

首部和数据之和，单位为字节。总长度字段为 16 位，因此数据报的最大长度为

2^16-1=65535 字节。

(5) 标识（identification）

用来标识数据报，占 16 位。IP 协议在存储器中维持一个计数器。每产生一个数据报，计数器就加 1，并将此值赋给标识字段。当数据报的长度超过网络的 MTU，而必须分片时，这个标识字段的值就被复制到所有的数据报的标识字段中。具有相同的标识字段值的分片报文会被重组成原来的数据报。

(6) 标志（flag）

占 3 位。第一位未使用，其值为 0。第二位称为 DF（不分片），表示是否允许分片。取值为 0 时，表示允许分片；取值为 1 时，表示不允许分片。第三位称为 MF（更多分片），表示是否还有分片正在传输，设置为 0 时，表示没有更多分片需要发送，或数据报没有分片。

(7) 片偏移（offsetfrag）

占 13 位。当报文被分片后，该字段标记该分片在原报文中的相对位置。片偏移以 8 个字节为偏移单位。所以，除了最后一个分片，其他分片的偏移值都是 8 字节（64 位）的整数倍。

(8) 生存时间（TTL）

表示数据报在网络中的寿命，占 8 位。该字段由发出数据报的源主机设置。其目的是防止无法交付的数据报无限制地在网络中传输，从而消耗网络资源。路由器在转发数据报之前，先把 TTL 值减 1。若 TTL 值减少到 0，则丢弃这个数据报，不再转发。因此，TTL 指明数据报在网络中最多可经过多少个路由器。TTL 的最大数值为 255。若把 TTL 的初始值设为 1，则表示这个数据报只能在本局域网中传送。

(9) 协议

表示该数据报文所携带的数据所使用的协议类型，占 8 位。该字段可以方便目的主机的 IP 层知道按照什么协议来处理数据部分。不同的协议有专门不同的协议号。例如，TCP 的协议号为 6，UDP 的协议号为 17，ICMP 的协议号为 1。

(10) 首部检验和（checksum）

用于校验数据报的首部，占 16 位。数据报每经过一个路由器，首部的字段都可能发生变化（如 TTL），所以需要重新校验。而数据部分不发生变化，所以不用重新生成校验值。

(11) 源地址

表示数据报的源 IP 地址，占 32 位。

(12) 目的地址

表示数据报的目的 IP 地址，占 32 位。该字段用于校验发送是否正确。

(13) 可选字段

该字段用于一些可选的报头设置，主要用于测试、调试和安全的目的。这些选项包括严格源路由（数据报必须经过指定的路由）、网际时间戳（经过每个路由器时的时间戳记录）和安全限制。

(14) 填充

由于可选字段中的长度不是固定的，使用若干个 0 填充该字段，可以保证整个报头的长度是 32 位的整数倍。

(15) 数据部分

表示传输层的数据，如保存 TCP、UDP、ICMP 或 IGMP 的数据。数据部分的长度不固定。

期待下次的实验。

# 实验报告 3

课程 网络协议分析及编程　　实验地点 信息楼 6 楼网络安全实验室

| | | | |
|---|---|---|---|
| 姓　　名 | 姜德琛 | 实　验　日　期： | 2021.11.05 |
| 学　　号 | 201905556608 | 实验报告日期： | 2021.11.28 |
| 同组人姓名 | 王文海 | 报　告　退　发： | （订正 、 重做） |
| 同组人学号 | 201805821012 | 教师审批签字： | |

---

## 一．实验名称

传输层协议分析

## 二．实验环境（详细说明运行的操作系统，网络平台，机器的 IP 地址）

1. 操作系统：Windows7 操作系统
2. 网络平台：PC1，PC2，交换机*1
3. PC1 的 ip：172.22.10.20
   PC2 的 ip：172.22.10.21

## 三．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。

## 四．实验内容及步骤

1、连接好设备，配置 PC1 和 PC2 的 IP 地址，网络拓扑图，验证连接。

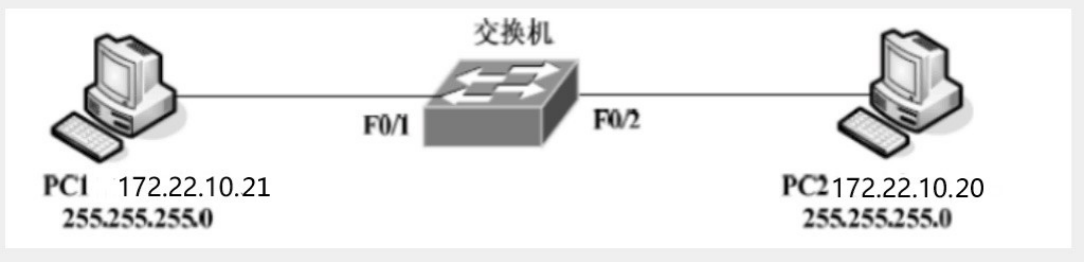



图 1

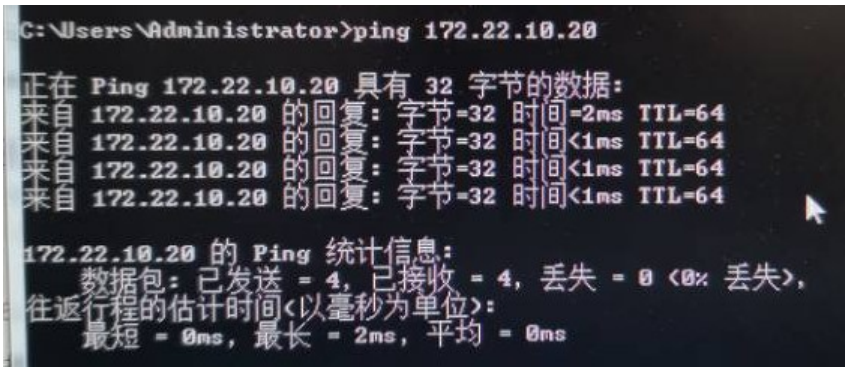



图 2

2、按照 3CDaemon 软件的介绍方法在 PC1 上建立 FTP 服务器。

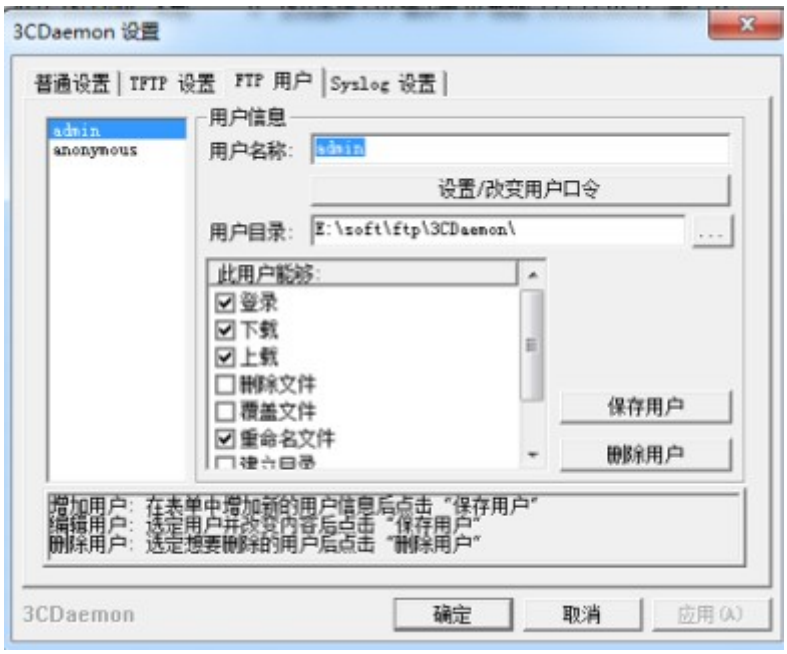



图 3

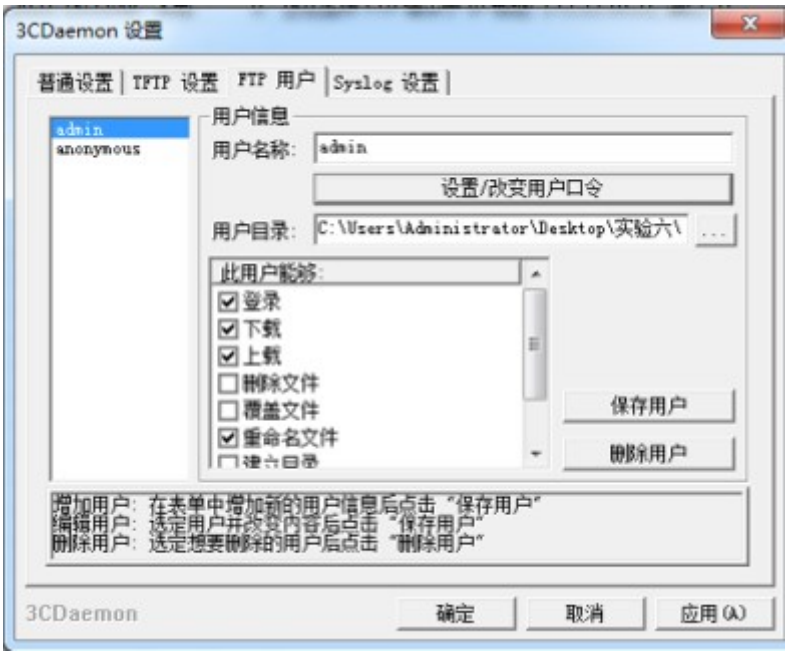



图 4

3、在 PC1 和 PC2 中运行 Ethereal，开始截获报文，为了只截获到与我们实验有关的内容，将截获条件设置为对方主机的 IP 地址，如 PC1 的截获条件为“host 172.22.10.20”。

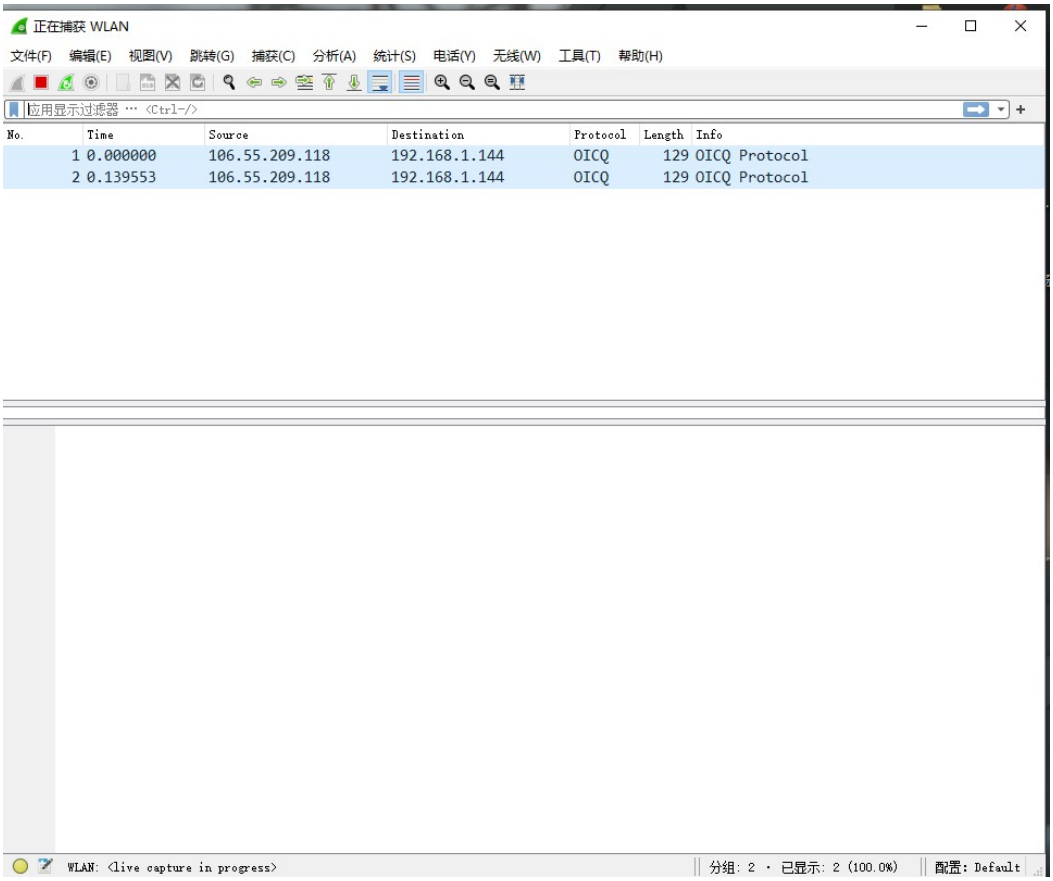



图 5

4、在 PC1 上打开命令行窗口，执行如下操作：

```
C:\Documents and Settings\Administrator>ftp
ftp> open
To 172.22.10.20
Connected to 172.22.10.20.
220 3Com 3CDaemon FTP Server Version 2.0
User (172.22.10.20:(none)): anonymous
331 User name ok, need password
Password:
230 User logged in
ftp> quit
221 Service closing control connection
```

5、停止截获报文，将截获的结果保存为 FTP-201905556608，其中三次握手如图 4.5.1，所示，四次挥手如图 3.9 所示。

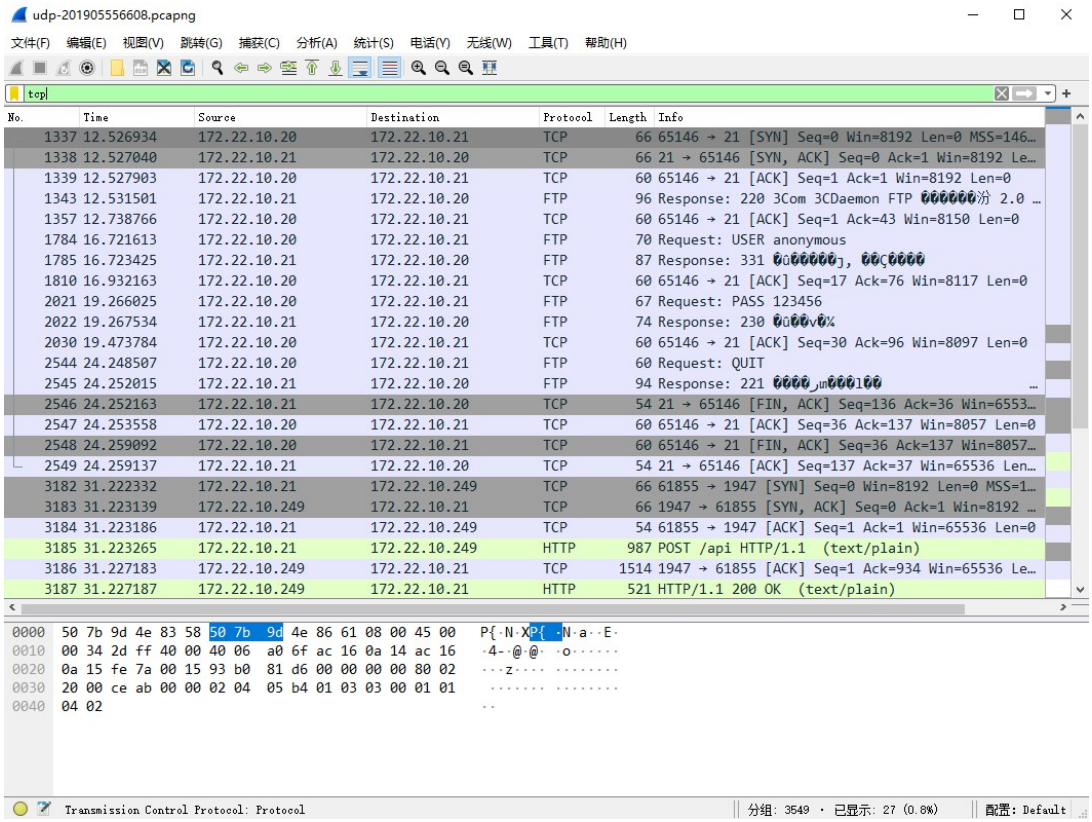



图 6

## 五． 实验结果

1. 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 |
|---|---|---|---|---|---|---|---|
| 46123 | 主机到客户端 | 65146 | 21 | 0 | 0 | 1 | 0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 46126 | 客户端到主机 | 21 | 56738 | 0 | 1 | 1 | 1 |
| 46127 | 主机到客户端 | 65146 | 21 | 1 | 1 | 0 | 1 |

2. TCP 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 | 同步位 SYN | 确认位 ACK | 终止位 |
|---|---|---|---|---|---|---|---|---|
| 51210 | 客户端到主机 | 21 | 65146 | 136 | 32 | 0 | 1 | 1 |
| 51211 | 主机到客户端 | 65146 | 21 | 32 | 137 | 0 | 1 | 0 |
| 51215 | 客户端到主机 | 65146 | 21 | 32 | 137 | 0 | 1 | 1 |
| 51216 | 主机到客户端 | 21 | 65146 | 137 | 33 | 0 | 1 | 0 |

3. TCP 报文格式详解

TCP 报文是 TCP 层传输的数据单元，也称为报文段。TCP 报文中每个字段如图 3.10 所示。

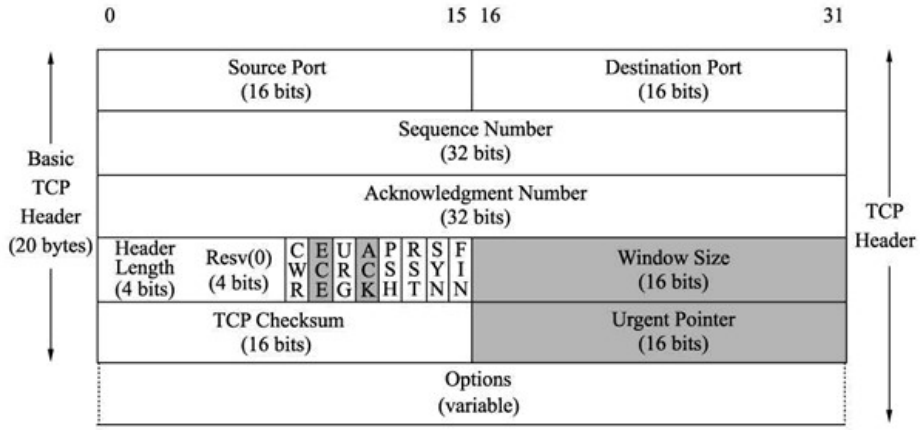



图 3.10

上图中 TCP 报文中每个字段的含义如下：

源端口和目的端口字段

TCP 源端口（Source Port）：源计算机上的应用程序的端口号，占 16 位。

TCP 目的端口（Destination Port）：目标计算机的应用程序端口号，占 16 位。

序列号字段

CP 序列号（Sequence Number）：占 32 位。它表示本报文段所发送数据的第一个字节的编号。在 TCP 连接中，所传送的字节流的每一个字节都会按顺序编号。当 SYN 标记不为 1 时，这是当前数据分段第一个字母的序列号；如果 SYN 的值是 1 时，这个字段的值就是初始序列值（ISN），用于对序列号进行同步。这时，第一个字节的序列号比这个字段的值大 1，也就是 ISN 加 1。

确认号字段

TCP 确认号（Acknowledgment Number，ACK Number）：占 32 位。它表示接收方期望收到发送方下一个报文段的第一个字节数据的编号。其值是接收计算机即将接收到的下一个序列号，也就是下一个接收到的字节的序列号加 1。

数据偏移字段

TCP 首部长度（Header Length）：数据偏移是指数据段中的“数据”部分起始处距离 TCP 数据段起始处的字节偏移量，占 4 位。其实这里的“数据偏移”也是在确定 TCP 数据段头部分的长度，告诉接收端的应用程序，数据从何处开始。

保留字段

保留（Reserved）：占 4 位。为 TCP 将来的发展预留空间，目前必须全部为 0。

标志位字段

CWR（Congestion Window Reduce）：拥塞窗口减少标志，用来表明它接收到了设置 ECE 标志的 TCP 包。并且，发送方收到消息之后，通过减小发送窗口的大小来降低发送速率。

ECE（ECN Echo）：用来在 TCP 三次握手时表明一个 TCP 端是具备 ECN 功能的。在数据传输过程中，它也用来表明接收到的 TCP 包的 IP 头部的 ECN 被设置为 11，即网络线路拥堵。

URG（Urgent）：表示本报文段中发送的数据是否包含紧急数据。URG=1 时表示有紧急数据。当 URG=1 时，后面的紧急指针字段才有效。

ACK：表示前面的确认号字段是否有效。ACK=1 时表示有效。只有当 ACK=1 时，前面的确认号字段才有效。TCP 规定，连接建立后，ACK 必须为 1。

PSH（Push）：告诉对方收到该报文段后是否立即把数据推送给上层。如值为 1，表示应当立即把数据提交给上层，而不是缓存起来。

RST：表示是否重置连接。如果 RST=1，说明 TCP 连接出现了严重错误（如主机崩溃），必须释放连接，然后再重新建立连接。

SYN：在建立连接时使用，用来同步序号。当 SYN=1，ACK=0 时，表示这是一个请求建立连接的报文段；当 SYN=1，ACK=1 时，表示对方同意建立连接。SYN=1 时，说明这是一个请求建立连接或同意建立连接的报文。只有在前两次握手中 SYN 才为 1。

FIN：标记数据是否发送完毕。如果 FIN=1，表示数据已经发送完成，可以释放连接。

窗口大小字段

窗口大小（Window Size）：占 16 位。它表示从 Ack Number 开始还可以接收多少字节的数据量，也表示当前接收端的接收窗口还有多少剩余空间。该字段可以用于 TCP 的流量控制。

TCP 校验和字段

校验位（TCP Checksum）：占 16 位。它用于确认传输的数据是否有损坏。发送端基于数据内容校验生成一个数值，接收端根据接收的数据校验生成一个值。两个值必须相同，才能证明数据是有效的。如果两个值不同，则丢掉这个数据包。Checksum 是根据伪头 + TCP 头 + TCP

数据三部分进行计算的。

紧急指针字段

紧急指针（Urgent Pointer）：仅当前面的 URG 控制位为 1 时才有意义。它指出本数据段中为紧急数据的字节数，占 16 位。当所有紧急数据处理完后，TCP 就会告诉应用程序恢复到正常操作。即使当前窗口大小为 0，也是可以发送紧急数据的，因为紧急数据无须缓存。

可选项字段

选项（Option）：长度不定，但长度必须是 32bits 的整数倍。

## 六． 实验中的问题及心得

这是网络协议编程的第三次实验，我们这次是对传输层的 tcp 协议进行分析，整个过程除了新软件的使用时有些费时间之外，别的都还很顺利，tcp 协议三次握手，四次挥手的原理也借这个机会总结如下。

**1、TCP 三次握手原理**

第一次握手：建立连接。客户端发送连接请求报文段，并将 syn(标记位)设置为 1，Squence Number(数据包序号)(seq)为 x,接下来等待服务端确认，客户端进入 SYN_SENT 状态(请求连接)；

第二次握手：服务端收到客户端的 SYN 报文段，对 SYN 报文段进行确认，设置 ack(确认号)为 x+1(即 seq+1 ；同时自己还要发送 SYN 请求信息,将 SYN 设置为 1, seq 为 y。服务端将上述所有信息放到 SYN+ACK 报文段中，一并发送给客户端，此时服务器进入 SYN_RECV 状态。SYN_RECV 是指,服务端被动打开后,接收到了客户端的 SYN 并且发送了 ACK 时的状态。再进一步接收到客户端的 ACK 就进入 ESTABLISHED 状态。

第三次握手：客户端收到服务端的 SYN+ACK(确认符) 报文段；然后将 ACK 设置为 y+1,向服务端发送 ACK 报文段，这个报文段发送完毕后，客户端和服务端都进入 ESTABLISHED(连接成功)状态，完成 TCP 的三次握手。

三次挥手过程如下图 3.11 所示：

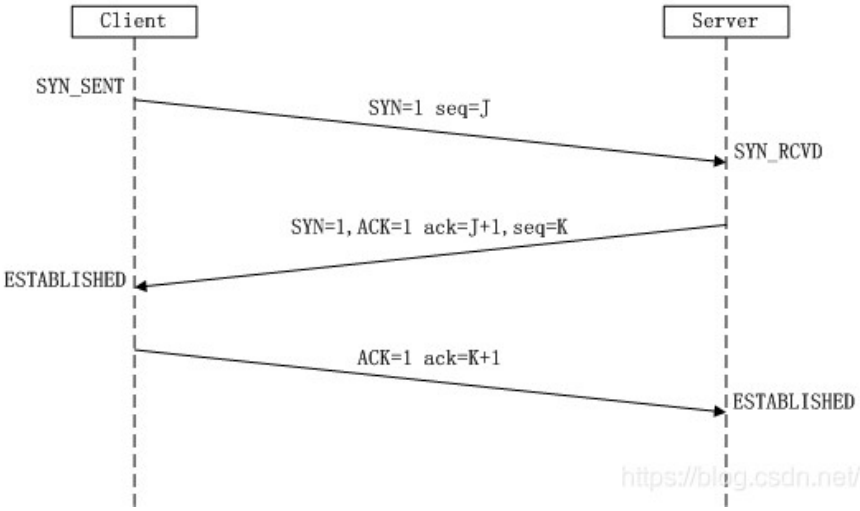




图 3.11

## 2、TCP 四次挥手原理

当客户端和服务端通过三次握手建立了 TCP 连接以后,当数据传送完毕,断开连接就需要进行 TCP 的四次挥手。其四次挥手如下所示：

第一次挥手:客户端设置 seq 和 ACK ,向服务器发送一个 FIN(终结)报文段。此时，客户端进入 FIN_WAIT_1 状态，表示客户端没有数据要发送给服务端了。

第二次挥手:服务端收到了客户端发送的 FIN 报文段，向客户端回了一个 ACK 报文段。

第三次挥手:服务端向客户端发送 FIN 报文段，请求关闭连接，同时服务端进入 LAST_ACK 状态。

第四次挥手:客户端收到服务端发送的 FIN 报文段后，向服务端发送 ACK 报文段,然后客户端进入 TIME_WAIT 状态。服务端收到客户端的 ACK 报文段以后，就关闭连接。此时，客户端等待 2MSL（指一个片段在网络中最大的存活时间）后依然没有收到回复，则说明服务端已经正常关闭，这样客户端就可以关闭连接了。

四次挥手过程如下图 3.12 所示：

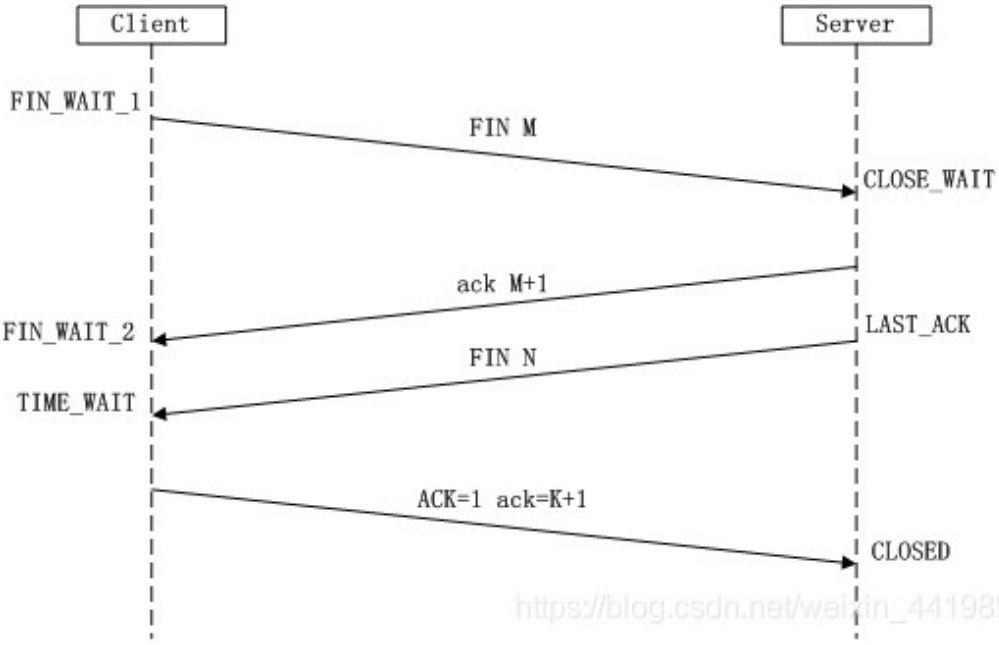




图 3.12

整个过程如图 3.13 所示：

建立连接（三次握手）

数据传输

释放连接（四次挥手）

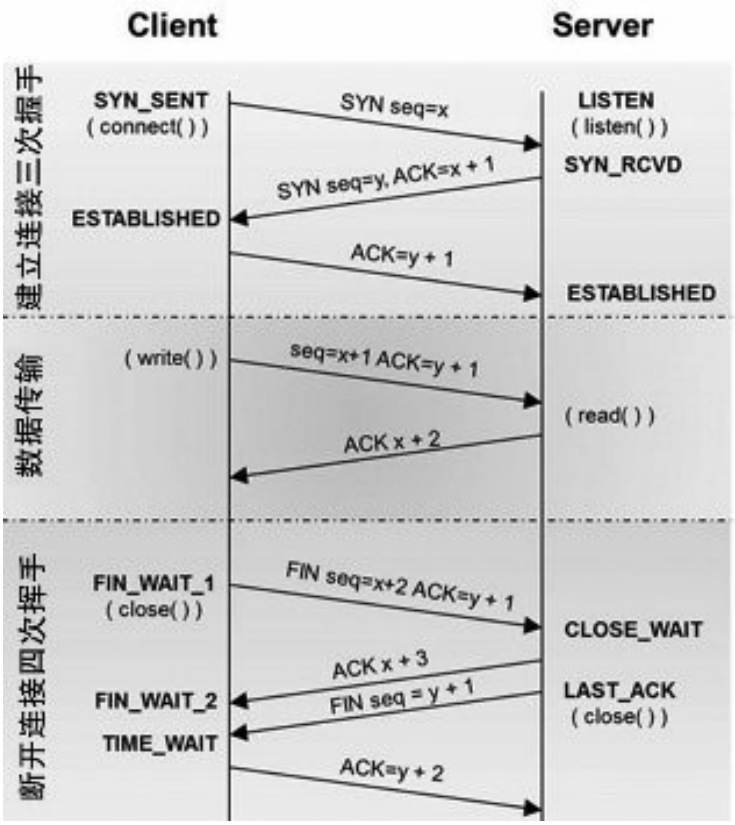



图 3.13

# 实验报告 4

课程_ 网络协议分析及编程 _ 实验地点 信息楼 609 _

姓　　名_�姜德琛_____ _____ 实　验　日　期：
学　　号_201905556608_____ 实验报告日期：
同组人姓名_王文海_____ 报　告　退　发：（订正 、 重做 ）
同组人学号_201805821012_____ 审 批 签 字：

---

## 一. 实验名称

HTTP 协议分析实验

## 二. 环境（详细说明运行的操作系统，网络平台，机器的 IP 地址）

1、 操作系统：Windows 7
2、 机器的 IP 地址：172.22.10.20 和 172.22.10.21

## 三. 实验目的

在 PC 机 上访问 RCMS 的 Web 页面，截获报文，分析 HTTP 协议的报文格式和 HTTP 协议的工作过程。

## 四. 实验内容及步骤

1、网络拓扑图
网络拓扑图如图 4.1.1 所示。

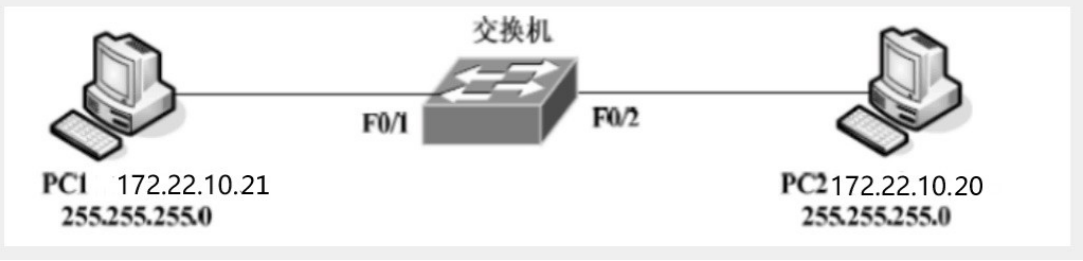



图 4.1.1

2、软件设置过程
(1) 在 PC 机上运行 Ethereal，开始截获报文，为了只截获和我们要访

问的网站相关的数据报，将截获条件设置为“not broadcast ad not multicast”。过程如图 4.2.1 所示。

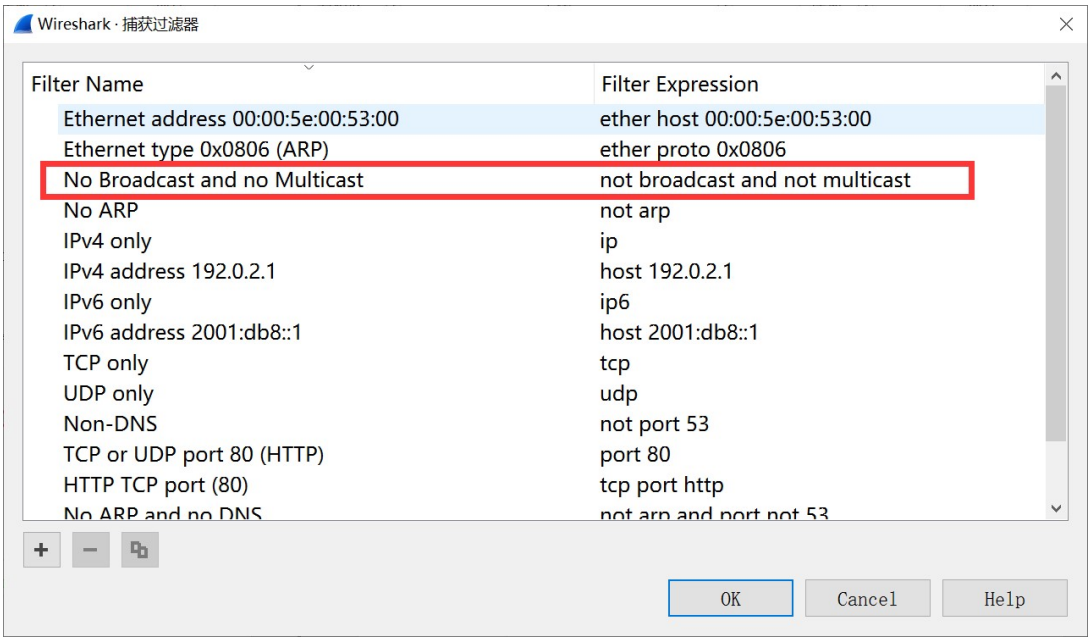


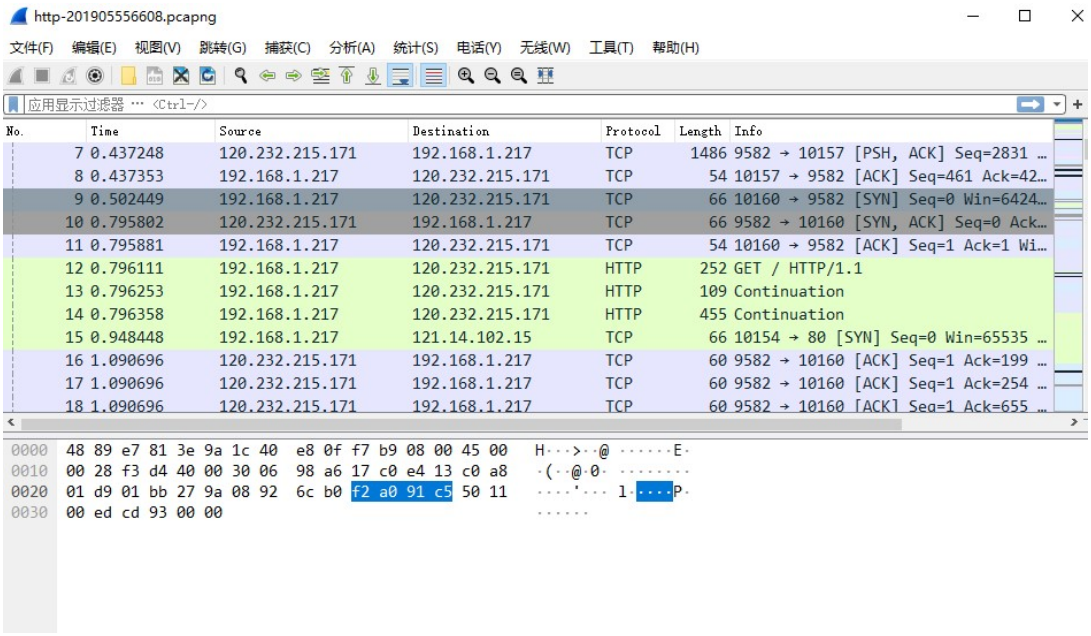

图 4.2.1

(2) 从浏览器上访问在线翻译_有道 (youdao.com)界面。打开网页，待浏览器的状态栏出现“完毕“信息后关闭网页。过程如图 4.2.2 所示。


图 4.2.2

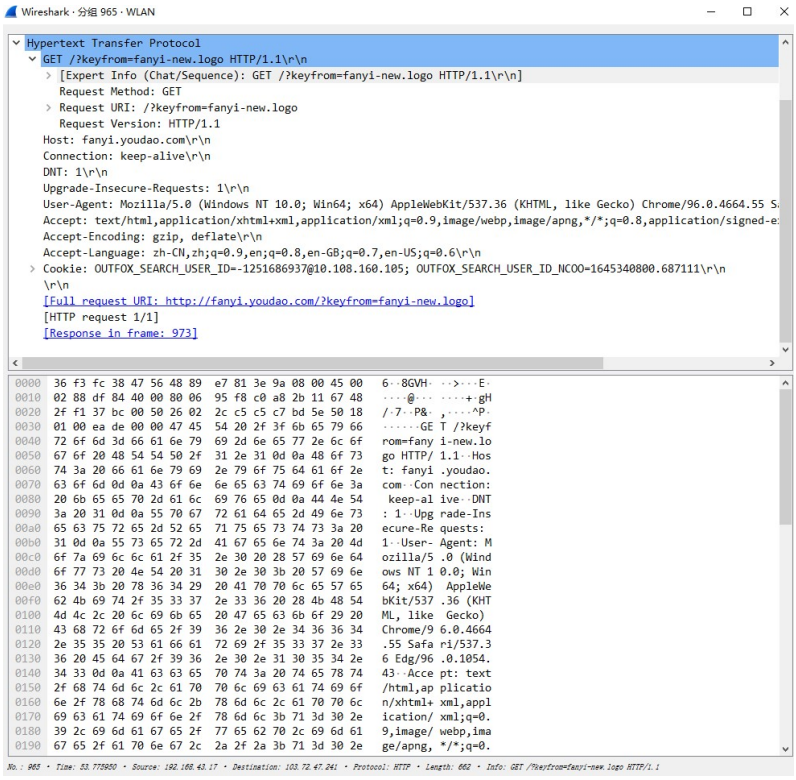
3、捕获分析

停止截获报文，将截获的报文命名为 http-201905556608 保存。

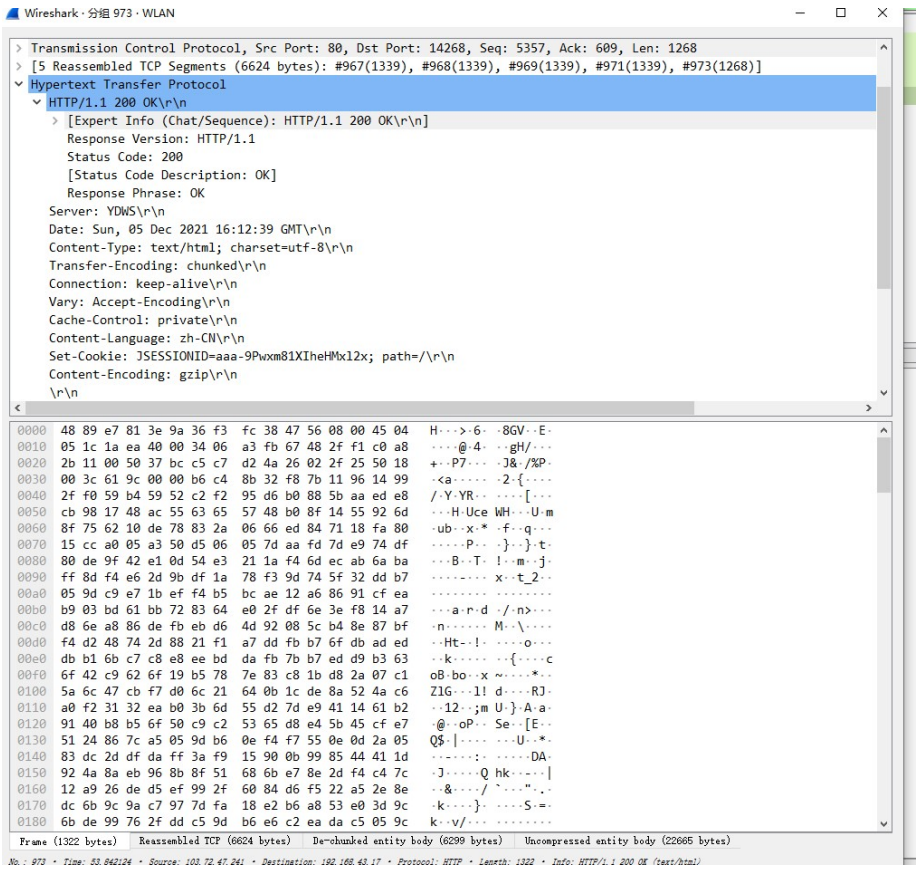



# 五． 实验结果

1. 请求报文




2、HTTP 应答报文

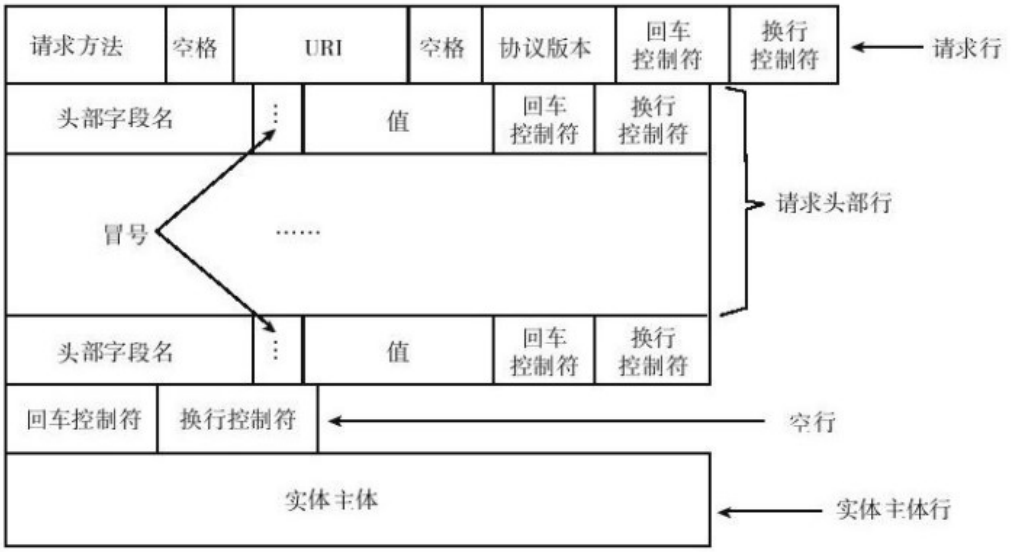

Wireshark · 分组 973 · WLAN
Transmission Control Protocol, Src Port: 80, Dst Port: 14268, Seq: 5357, Ack: 609, Len: 1268
[5 Reassembled TCP Segments (6624 bytes): #967(1339), #968(1339), #969(1339), #971(1339), #973(1268)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Server: YDWS\r\n
Date: Sun, 05 Dec 2021 16:12:39 GMT\r\n
Content-Type: text/html; charset=utf-8\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
Vary: Accept-Encoding\r\n
Cache-Control: private\r\n
Content-Language: zh-CN\r\n
Set-Cookie: JSESSIONID=aaa-9Pwxm81XIheHMxl2x; path=/\r\n
Content-Encoding: gzip\r\n
\r\n
0000 48 89 e7 81 3e 9a 36 f3 fc 38 47 56 08 00 45 04
0010 05 1c 1a ea 40 00 34 06 a3 fb 67 48 2f f1 c0 a8
0020 2b 11 00 50 37 bc c5 c7 d2 4a 26 02 2f 25 50 18
0030 00 3c 61 9c 00 00 b6 c4 8b 32 f8 7b 11 96 14 99
0040 2f f0 59 b4 59 52 c2 f2 95 d6 b0 88 5b aa ed e8
0050 cb 98 17 48 ac 55 63 65 57 48 b0 8f 14 55 92 6d
0060 8f 75 62 10 de 78 83 2a 06 66 ed 84 71 18 fa 80
0070 15 cc a0 05 a3 50 d5 06 05 7d aa fd 7d e9 74 df
0080 80 de 9f 42 e1 0d 54 e3 21 1a f4 6d ec ab 6a ba
0090 ff 8d f4 e6 2d 9b df 1a 78 f3 9d 74 5f 32 dd b7
00a0 05 9d c9 e7 1b ef f4 b5 bc ae 12 a6 86 91 cf ea
00b0 b9 03 bd 61 bb 72 83 64 e0 2f df 6e 3e f8 14 a7
00c0 d8 6e a8 86 de fb eb d6 4d 92 08 5c b4 8e 87 bf
00d0 f4 d2 48 74 2d 88 21 f1 a7 dd fb b7 6f db ad ed
00e0 db b1 6b c7 c8 e8 ee bd da fb 7b b7 ed d9 b3 63
00f0 6f 42 c9 62 6f 19 b5 78 7e 83 c8 1b d8 2a 07 c1
0100 5a 6c 47 cb f7 d0 6c 21 64 0b 1c de 8a 52 4a c6
0110 a0 f2 31 32 ea b0 3b 6d 55 d2 7d e9 41 14 61 b2
0120 91 40 b8 b5 6f 50 c9 c2 53 65 d8 e4 5b 45 cf e7
0130 51 24 86 7c a5 05 9d b6 0e f4 f7 55 0e 0d 2a 05
0140 83 dc 2d df da ff 3a f9 15 90 0b 99 85 44 41 1d
0150 92 4a 8a eb 96 8b 8f 51 68 6b e7 8e 2d f4 c4 7c
0160 12 a9 26 de d5 ef 99 2f 60 84 d6 f5 22 a5 2e 8e
0170 dc 6b 9c 9a c7 97 7d fa 18 e2 b6 a8 53 e0 3d 9c
0180 6b de 99 76 2f dd c5 9d b6 e6 c2 ea da c5 05 9c
Frame (1322 bytes)
Reassembled TCP (6624 bytes)
De-chunked entity body (6299 bytes)
Uncompressed entity body (22665 bytes)

六.　　实验中的问题及心得

这次的网络协议实验主要进行应用层的 http 协议进行分析。

遇到的主要问题就是一直抓不到目标网站的包。查询资料之后发现可能是因为相关的连接在抓包之前就已经建立好了，所以更换一个抓包的目标网站就可以解决这个问题了。最后选择的是有道翻译网站，成功完成了抓包实验。

请求报文格式如下：




应答报文格式如下：