# 实验报告 1

课 程 TCP/IP网络编程 实验地点 信息楼601

姓 名 王 康 实 验 日 期：2018.05.14

学 号 2015551621 实验报告日期：

同组人姓名 曾碧霄 报 告 退 发： ( 订正 、 重做 )

同组人学号 2015551634 教 师 审 批 签 字：

1. 实验名称

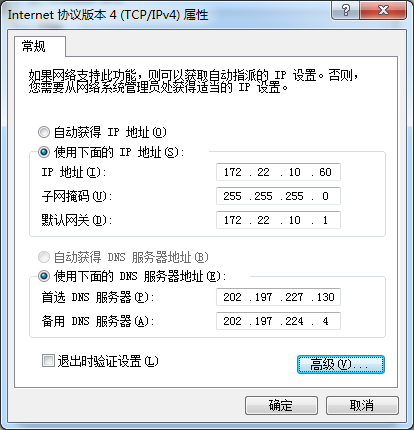
以太网链路层帧格式分析实验

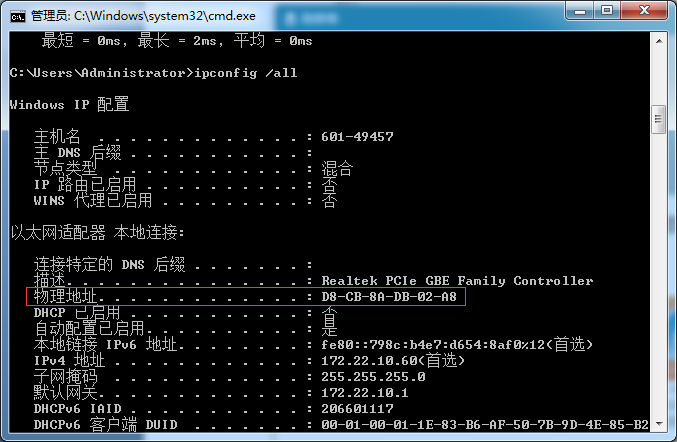
1. 环境

操作系统：Win7

网络平台：以太网

机器的IP地址：172.22.10.60



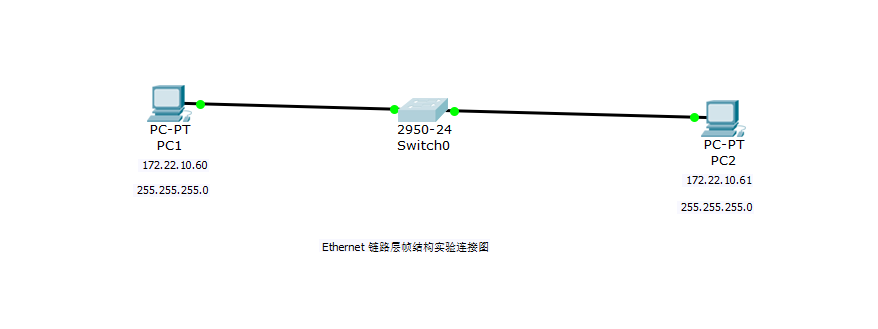


1. 实验目的

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。

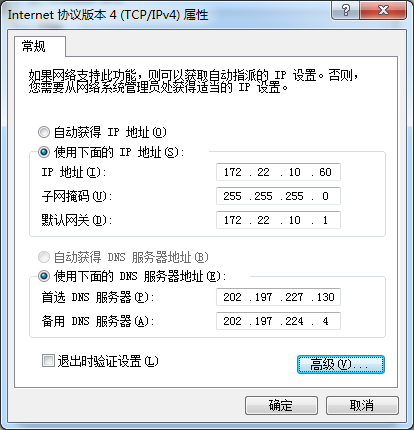
1. 实验内容及步骤

网络拓扑图：

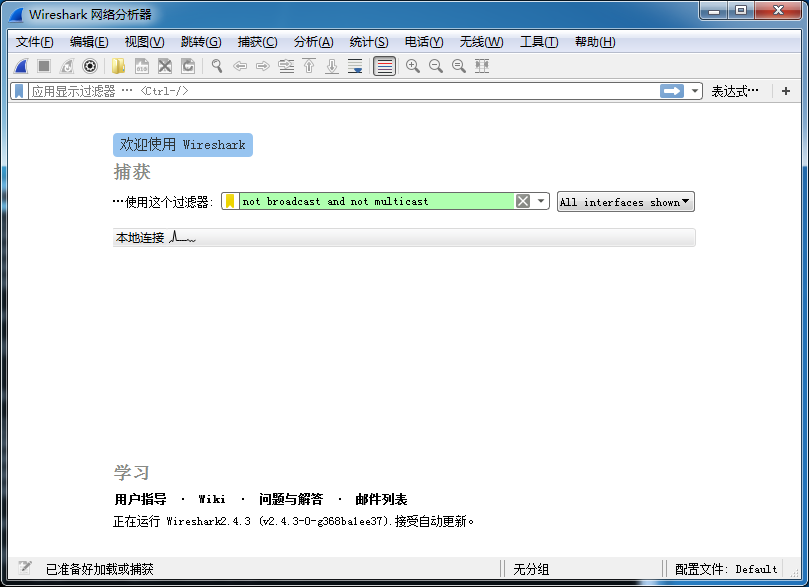


配置及捕获分析：

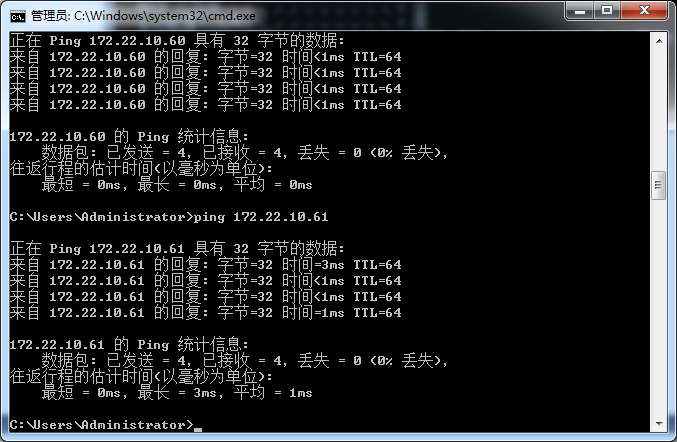
步骤1：配置PC1和PC2的IP地址；（编者注：实验室中任何一台PC都可以作为模型中的PC1或PC2。）



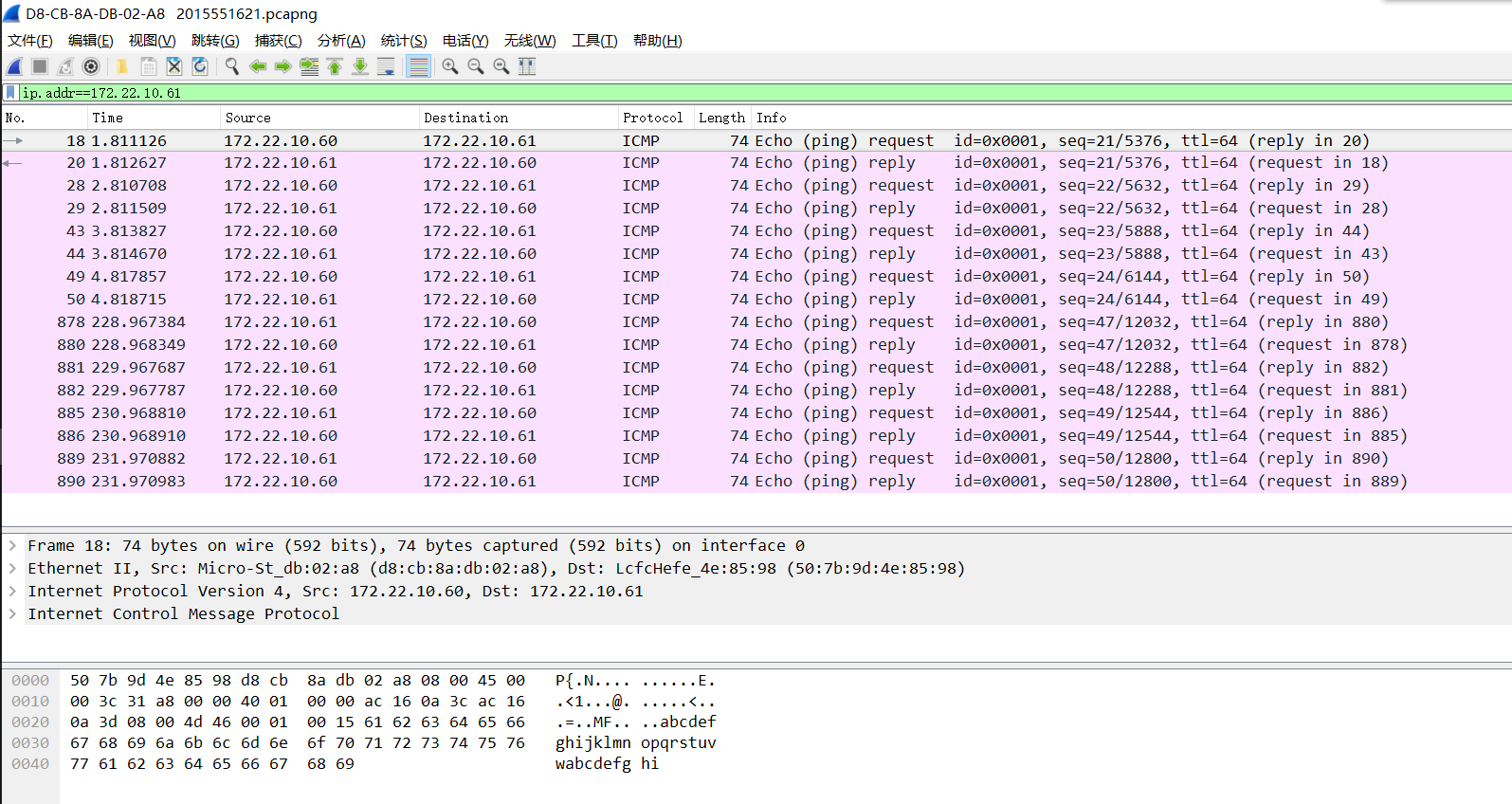
步骤2：在：PC1和PC2 上运行Ethereal截获报文，为了只截获和实验内容有关的报文，将Ethereal的CaptrueFilter设置为“NoBroadcastandnoMulticast”；



步骤3：在：PC1的“运行”对话框中输入命令“Ping172.22.10.61”，单击“确定”按钮；



步骤4：停止截获报文：将结果保存为MAC-学号，并对截获的报文进行分析：（见实验结果）

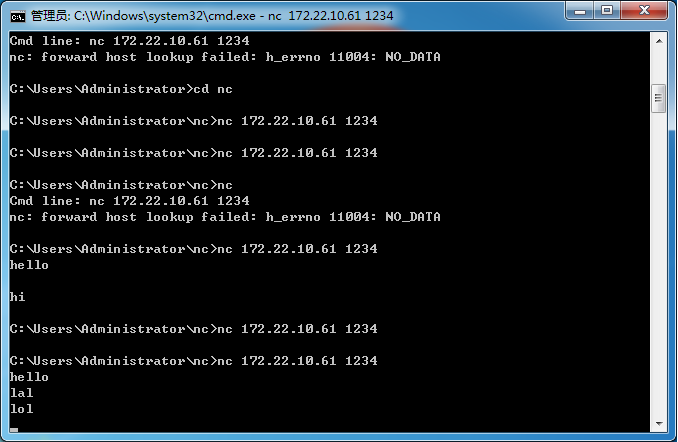


步骤5：在：PC1和PC2上运行Ethereal截获报文，然后进入PC1的Windows命令行窗口，执行如下命令：

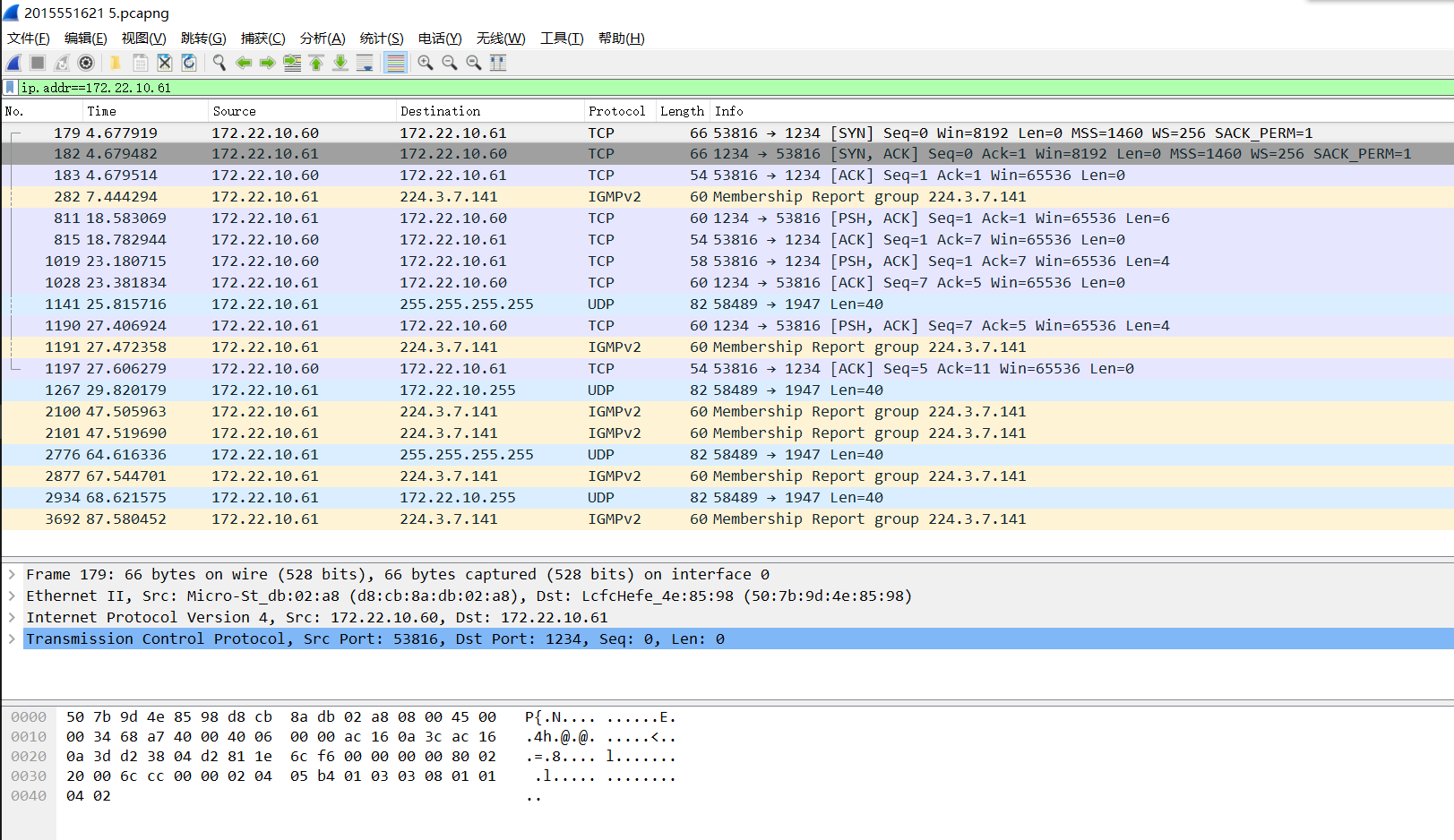
netsend172.16.1.102Hello

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。



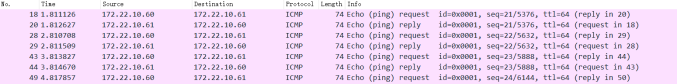
找到发送消息的报文并进行分析，查看主窗口中数据报文列表窗口和协议树窗口信息，填表（见实验结果）



1. 实验结果

**步骤4：报文分析**

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。



协议类型：ICMP UDP ARP HTTP

ICMP：（Internet Control Message Protocol ）Internet控制报文协议。它是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网咯本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

UDP：用户数据包协议，它和TCP一样位于传输层，和IP协议配合使用，在传输数据时省去包头，但它不能提供数据包的重传，所以适合传输较短的文件。

ARP：地址解析协议，实现通过IP地址得知其物理地址。在TCP/IP网络环境下，每个主机都分配了一个32位的IP地址，这种互联网地址是在网际范围标识主机的一种逻辑地址。为了让报文在物理网路上传送，必须知道对方目的主机的物理地址。这样就存在把IP地址变换成物理地址的地址转换问题。

HTTP：超文本传输协议（HyperText Transfer Protocol），是互联网上引用最为广泛的一种网络协议。所有的WWW文件都必须遵守这个标准。设计HTTP最初的目的是为了提供一种发布和接收HTML页面的方法。

其中截获Ping命令数据包均为ICMP报文，ping一次共8个报文，其中4个请求报文，4个应答报文，大小默认为32字节，当目标主机收到请求后回复，本地主机就可以收到ICMP回复报文，说明网络连通。

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EthernetV2帧，查看这个帧由几部分组成，缺少了哪几部分？为什么？

组成部分：

6字节源主机物理地址（d8:cb:8a:db:02:a8）

6字节目的主机物理地址(50:7b:9d:4e:85:98)

46～1500字节的数据字段

2字节的类型

缺少部分：

7字节的前导符

1字节的帧首定界

4字节的帧尾校验字段

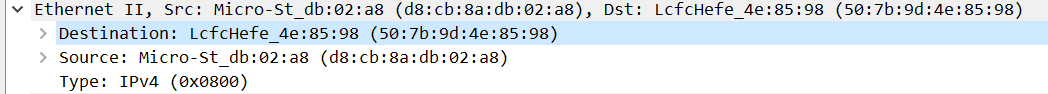
原因：

7字节的前导符是用来使接收端的适配器在接收MAC帧时能迅速调整其时钟频率，使它和发送端实现位同步。

1字节的帧首定界前6位的作用和前同步码一样，后2位表示数据到来。

4字节的帧尾校验字段（FCS）用来快速检验帧有没有出现比特差错。

这三部分用过后都会在适配器上被丢弃，不会提交给上一层。因此截获的包中没有这些信息。



**步骤5：报文分析**

|  |  |  |
| --- | --- | --- |
| 报文类型 | | TCP报文 |
| 报文的基本信息（数据报文列表窗口中的 Information 项的内容） | | 53816->1234 [PSH,ACK] Seq=1 Ack=7 Win=65536 Len=6 |
| EthernetII协议树中 | Source字段值 | d8:cb:8a:db:02:a8 |
| Destination字段值 | 50:7b:9d:4e:85:98 |
| Internet Protocol协议树中 | Source字段值 | 172.22.10.60 |
| Destination字段值 | 172.22.10.61 |
| UserDatagramProtocol协议树中 | Source字段值 | 53816 |
| Destination字段值 | 1234 |
| 应用层协议树 | 协议名称 | TCP |
| 包含Hello的字段值 | Data：68656c6c6f0a |

1. 实验中的问题及心得

通过本次实验，对MAC帧，TCP、ICMP协议有了进一步的了解，同时加深了主机间通讯过程的理解。用抓包软件对数据包进行分析，对帧的整体格式更加熟悉，同时了解到TCP三次握手的具体流程。也知道win7系统没有信使功能，所以需要自己下载netcat并配置监听端口，实现简单的聊天功能。

问题：应用层协议树中应该不包括TCP协议，但是里面只看到TCP协议。