### 实验3: 分析EthernetII帧

### 一、实验目的

1：深入理解Ethernet II帧结构。

2：基本掌握使用Wireshark分析捕获的跟踪文件的基本技能。

### 二、实验内容和要求

1：深入理解Ethernet II帧结构。

2：基本掌握使用Wireshark分析捕获的跟踪文件的基本技能。

3：PC 具有以太网卡一块，通过双绞线与网络相连。

### 三、实验环境

1：运行网络模拟器软件的Windows 7 操作系统PC机。

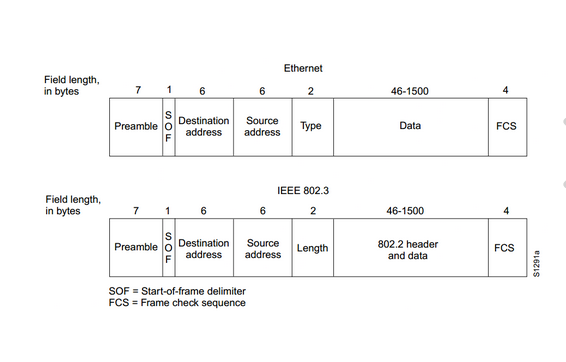
2：去FTP服务器下载Wireshark软件以及使用它进行抓包然后对抓包结果进行分析。

3：PC 具有以太网卡一块，通过双绞线与网络相连。

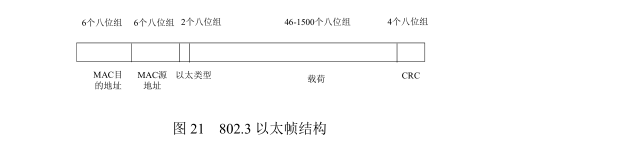
**四、操作方法与实验步骤概念**

以太帧的相关知识。

IEEE 802.3以太帧结构。



Ethernet II帧结构。



第一：捕获并分析以太帧。

1.1删除浏览器中的历史记录。

1.2启动Wireshark进行抓包，开始分组捕获。

1.3在浏览器中输入<http://www.henu.edu.cn/>

1.4停止抓包，对抓取的数据进行分析。

选取一个目的地址为进行分析，可以看到该帧的到达时间，帧编号，帧长度，帧的长度等等。

第二：分析以太帧结构

将计算机连网路，然后抓包。最后回答下面的问题：

1：本地连接的48比特以太网MAC地址是什么？

98:90:96:d3:91:29

2：以太帧中目的MAC 地址是什么？它是你选定的远地Web 服务器的MAC 地址吗？(提示：不是)那么，该地址是什么设备的MAC 地址呢？

目的 MAC 地址为01:00:5e:01:04:56 不是 是路由器网关的 MAC地址 01:00:5e:01:04:56的地址。

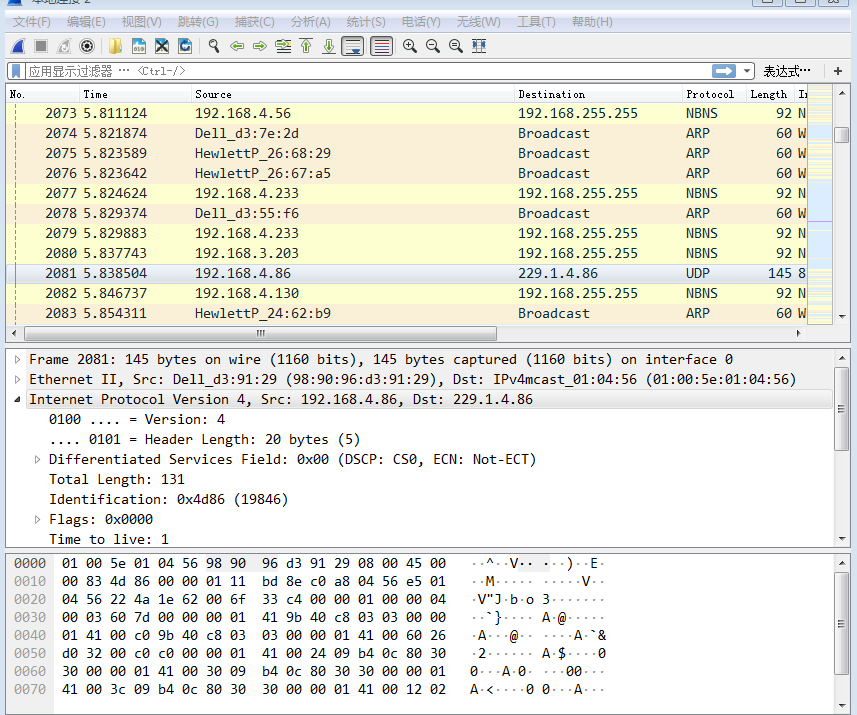
(3) 给出2 字节以太类型字段的十六进制的值。它表示该以太帧包含了什么样的协议？

值：0800 包含TCP协议

### 五、实验数据记录和结果分析

为了进一步分析以太帧结构，点击以太帧的信息，然后显示如图1的部分。其中看到源 MAC 地址为\_\_\_\_98:90:96:d3:91:29\_\_\_\_，目的 MAC 地址为\_\_\_\_01:00:5e:01:04:56\_\_\_；以太类型字段中值为 \_\_\_0x0800\_\_\_，表示该帧封装了 \_\_IP数据报\_\_；以及 MAC 地址分配的相关信息。

**抓包分析截图：**



1：源地址是：\_\_\_\_98:90:96:d3:91:29\_\_\_\_。

2：目的 MAC 地址为\_01:00:5e:01:04:56\_ ，它是路由器网关的

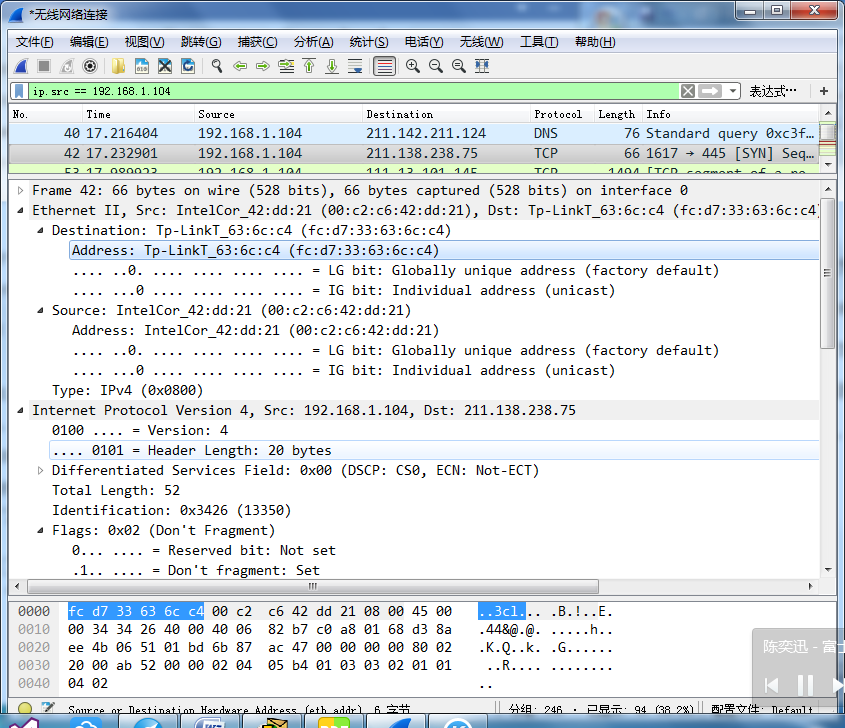
MAC地址 \_\_\_01:00:5e:01:04:56\_\_\_ 的地址。

3：值：\_\_\_\_0800\_\_\_\_ 包含TCP协议 例如，以太类

型值为 0x0800 指示了该帧包含了 IPv4 数据报，0x0806 表明指示了该帧包含了 ARP 帧， 0x8100 指示了该帧包含了 IEEE 802.1Q 帧。

Ipv6的值：86DD

具体信息参考图2：



### 六、实验体会、质疑和建议

通过此次试验，进一步分析了解了Ethernet II帧的结构,以及自己所抓取的包分组的信息，以及重点是知道了MAC地址实际上是路由器网关的NAC地址。