**计算机网络实验报告**

**课程名称： 计算机网络**

**实验名称： 课程实验1**

**学 号： 71118415**

**姓 名： 叶宏庭**

**成文日期： 2020年4月24日**

**1 实验目的及目标**

通过实践，熟悉本机网络参数的获取，掌握抓包工具的使用，加深对因特网上协议数据单元及其封装的理解。

**2 实验过程**

1. 提取本机网络参数：包括协议地址配置，MAC地址，IP地址，子网掩码，及子网地址。

**具体操作：**

* 1. 在cmd窗口中输入Ipconfig/all命令，查看结果；
  2. 通过计算得到子网地址；

1. 下载/安装/运行抓包工具(嗅探器)，捕获协议数据包并分析，包括以太网帧，IP报文，TCP或者UDP报文等。

**具体操作：**

* 1. 在Wireshark官网下载，Wireshark抓包工具；
  2. 运行Wireshark软件进行抓包；
  3. 对照报文格式对抓到的数据包进行分析；

**3 实验结果**

1. 通过cmd命令得到本机网络参数如下：

协议地址配置：本机为自动获取IP地址；

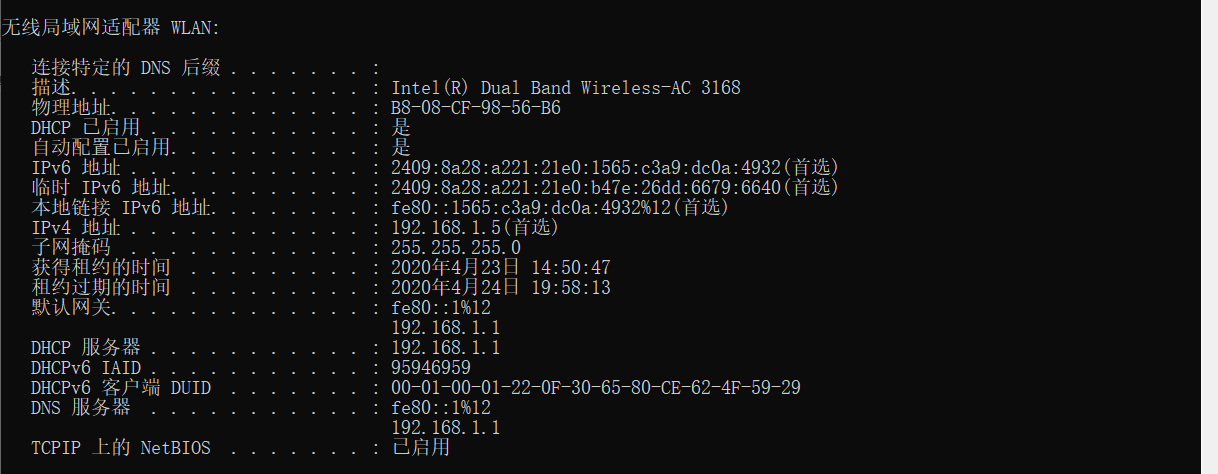
MAC地址（物理地址）：B8-08-CF-98-56-B6；

IP地址（IPv4）：192.168.1.5；

子网掩码：255.255.255.0；

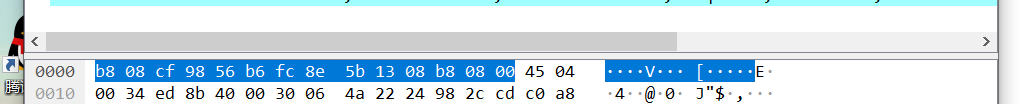
经计算子网地址：192.168.1.0

附图1



1. 下载运行Wireshark软件抓包并分析

**1以太网帧**（图中蓝色部分为以太帧数据包）：





根据以太帧结构可知：

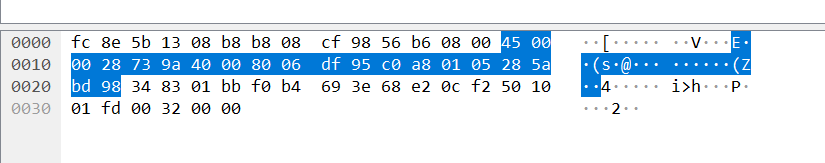
DA：b8 08 cf 98 56 b6 即为宿MAC地址

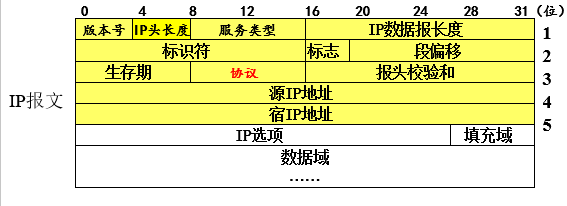
SA：fc 8e 5b 13 08 b8 即为源MAC地址

L/T：08 00 代表IPv4类型

注：抓包软件已过滤了前八个字节前序码及后四个字节FCS。

**2 IP报文**（图中蓝色部分为IP报文）：





根据IP报文格式可知：

版本号(0-3bit)：4 可知为IPv4

IP头长度(4-7bit)：5 表示头长度为20字节

服务类型(8-15bit)：00 前6位表示Default的Differentiated Services Codepoint，

后2位表示Explicit Congestion Notification: Not ECN-Capable Transport

IP数据报长度(16-31bit)：00 28 代表IP数据报长度为40

标识符(32-47bit)：73 9a 标识符0x739a (29594)

标志(48-51bit)：4

段偏移(52-63bit)：000 段偏移为0

生存期(64-71bit)：80 生存期为128

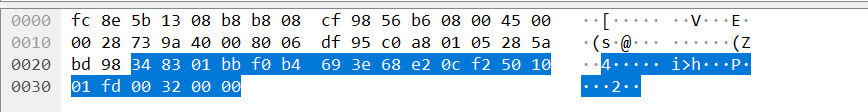
协议(72-79bit)：06 代表协议为TCP

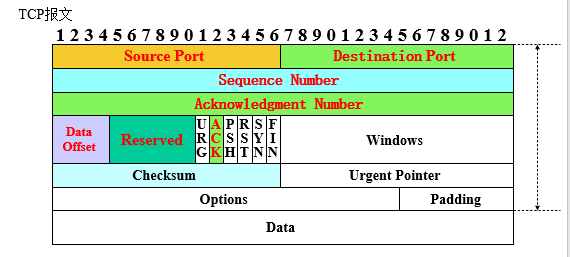
报头校验和(80-85bit)：df 95 代表validation disabled 校验无效

源IP地址(86-117bit)：c0 a8 01 05 源IP地址192.168.1.5

宿IP地址(118-139bit)：28 5a bd 98 宿IP地址40.90.189.152

**3 TCP报文**（图中蓝色部分为TCP报文）：





根据TCP报文格式可知：

源端口：34 83 端口13443

宿端口：01 bb 端口 443

序列号：f0 b4 69 3e 序列号为861 行号为4038355262

确认号：68 e2 0c f2 确认号为3481 行号为1759644914

Data Offset：5 数据偏移为5

Reserved：0b000 Not set

URG：0b0 Not set

ACK：0b1 Set

PSH：0b0 Not set

RST：0b0 Not set

SYN：0b0 Not set

FIN：0b0 Not set

Windows：01 fd 窗口大小为509

Checksum：00 32 未核实

Urgent Pointer：00 00

**4 实验小结**

通过本次实验，掌握了如何获取本机网络参数，以及如何使用抓包软件抓包，并进行数据包分析，掌握了这些基本操作，才能顺利的进行后续的其他实验，总的来说，这个实验还是很有意义的，初步入门了网络抓包这项技术。