**步骤1**

首先安装wireshark。建议采用缺省安装。

然后安装perl。推荐安装strawperl

**步骤2**

在防火墙上抓包。最好是用ssh方式，因为telnet和串口速度太慢，容易丢掉部分数据包。在命令行工具里设置记录文件，比如“secureCRT”的“log session”。



然后在命令行窗口抓包，选择“3”来输出抓包的头和内容。

dump sniff pack port1 'tcp and port 80 and host 192.168.6.168' 3

1: print header of packets

2: print header and data from ip of packets

3: print header and data from ethernet of packets

**步骤3**

1. 将apw2eth.pl文件中的

 my $text2pcapdirwin = "c:\\Progra~1\\wireshark";

中的"c:\\Progra~1\\Ethereal"改为你wireshark的安装目录，比如你安装的wireshark在D:\，则如下：

 my $text2pcapdirwin = "d:\\Ethereal";

(缺省就不用管了)

2. 到C:\strawberry\perl\bin>目录下，运行

perl apw2eth.pl -in session.log 得到output.eth文件，然后在Ethereal中打开即可。

其中session.log是你在防火墙上抓的包形成的text文件。

