

Palm pre 新机入门傻瓜篇

2009 年 10 月 7 日

第一步：准备阶段

需要下载安装的软件列表如下：

1. **MS NET Framework 3.5**:[http://www.microsoft.com/download... 31-508d977d32a6&](http://www.microsoft.com/download...31-508d977d32a6&)
2. **Java6**: <http://java.sun.com/javase/downloads/index.jsp>(下载 x86 适用的版本):
3. **python 2.6**:<http://www.python.org/ftp/python/2.6.2/python-2.6.2.msi>
4. **putty**:<http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>
5. **Novacom**Installer_x86.rar
6. **qxdm3.11.36.rar**（注：会被误当病毒被杀毒软件删除）
7. **CDMA Workshop 2.7** 破解版（注：会被误当病毒被杀毒软件删除）
8. PalmPreCentroTreo800w_**DiagDrivers**
9. **qpst-2.7_264**
10. **novaproxy.py**
11. sun **VirtualBox**
12. **PalmPre_Rom_qinray_1.0.3.jar**（注：还有 1.1，1.2 等 rom 版本，都要在 1.03 上弄好了再更新其他的新版本）
13. **Evdo.prl**

另外在新开机注册阶段需要 wifi 网络环境，否则将无法注册你的 profile。

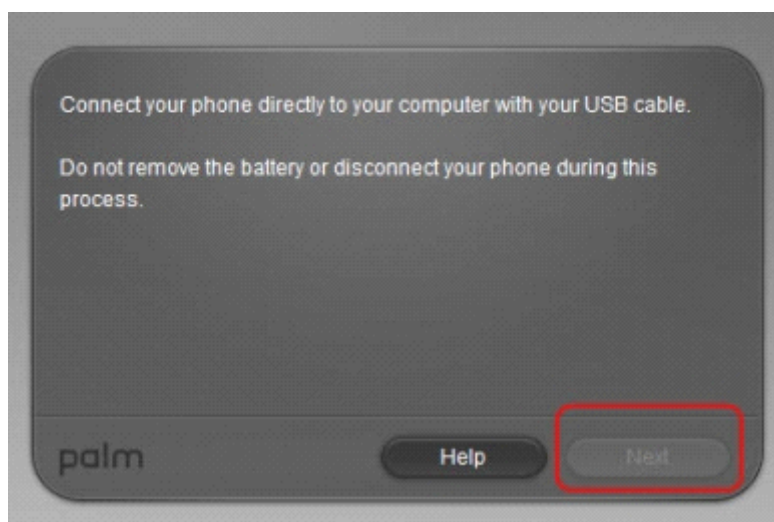
第二步：激活阶段

这里所使用的激活方法是通过刷 qinray 定制的 1.03rom，在这刷机前请先安装好 NovacomInstaller，以便 pre 连接到电脑时能够找到相关的驱动。同时还要安装上上述的大部分软件，特别是 python、java6、putty、workshop、qxdm 等。

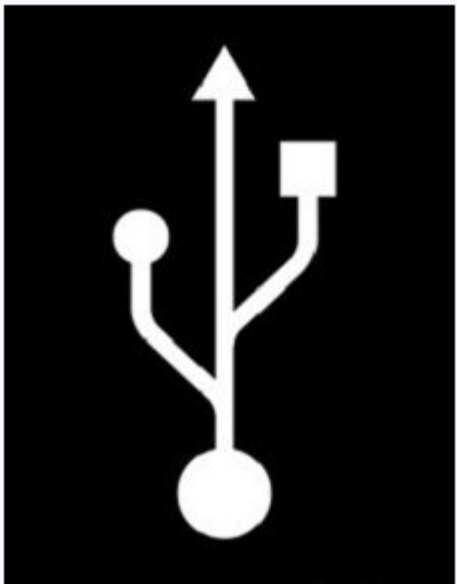
在安装好 java 环境后，可双击 **PalmPre_Rom_qinray_1.0.3.jar**，出现以下页面开始顺序操作：



经多次点击 Next 后，出现：



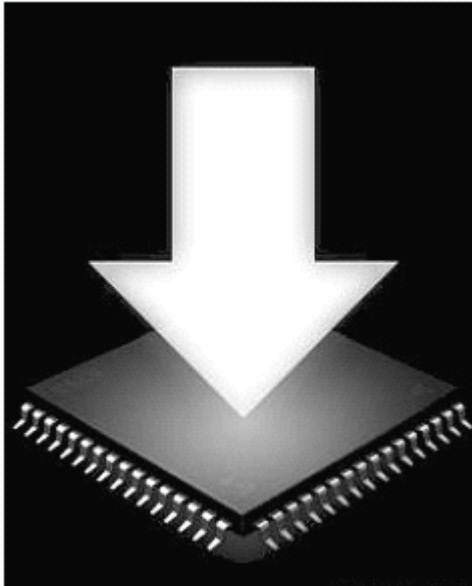
确保 Palm Pre 的电源是关闭的情况下，持续按住 Palm Pre 的音量向上键，同时将 USB 线插入手机，估计几秒钟后手机出现如下界面：



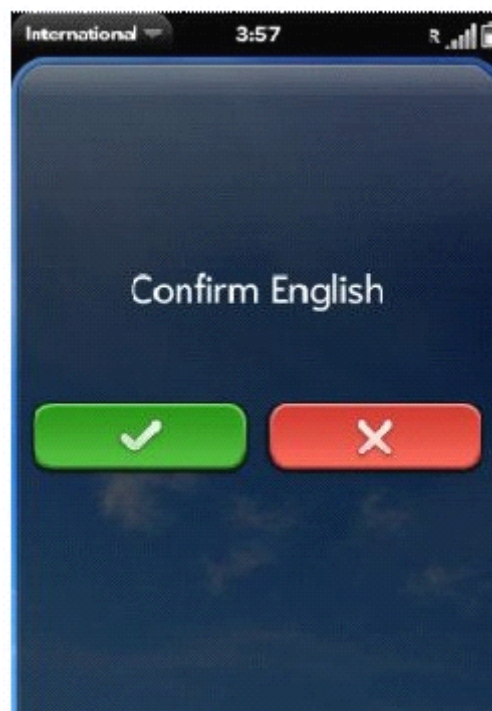
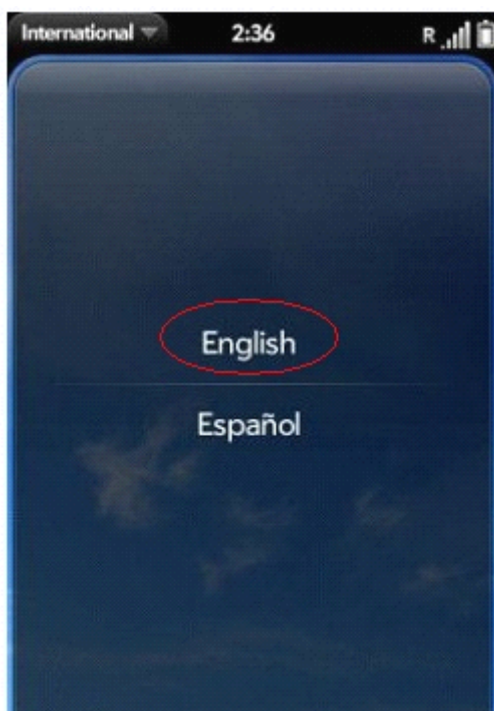
同时电脑上的界面如下的 Next 按钮将置亮状态，这时可松开向上音量的按键，即可顺利“NEXT”：

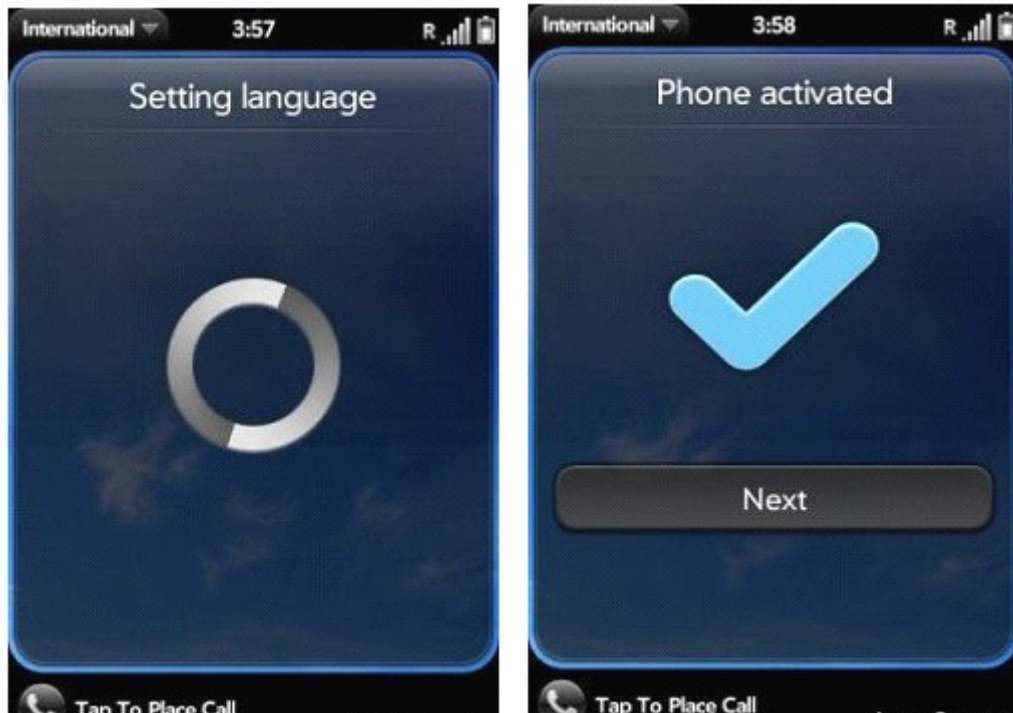


之后 Palm 手机上将进行一些界面切换，最后会停留在如下界面中：



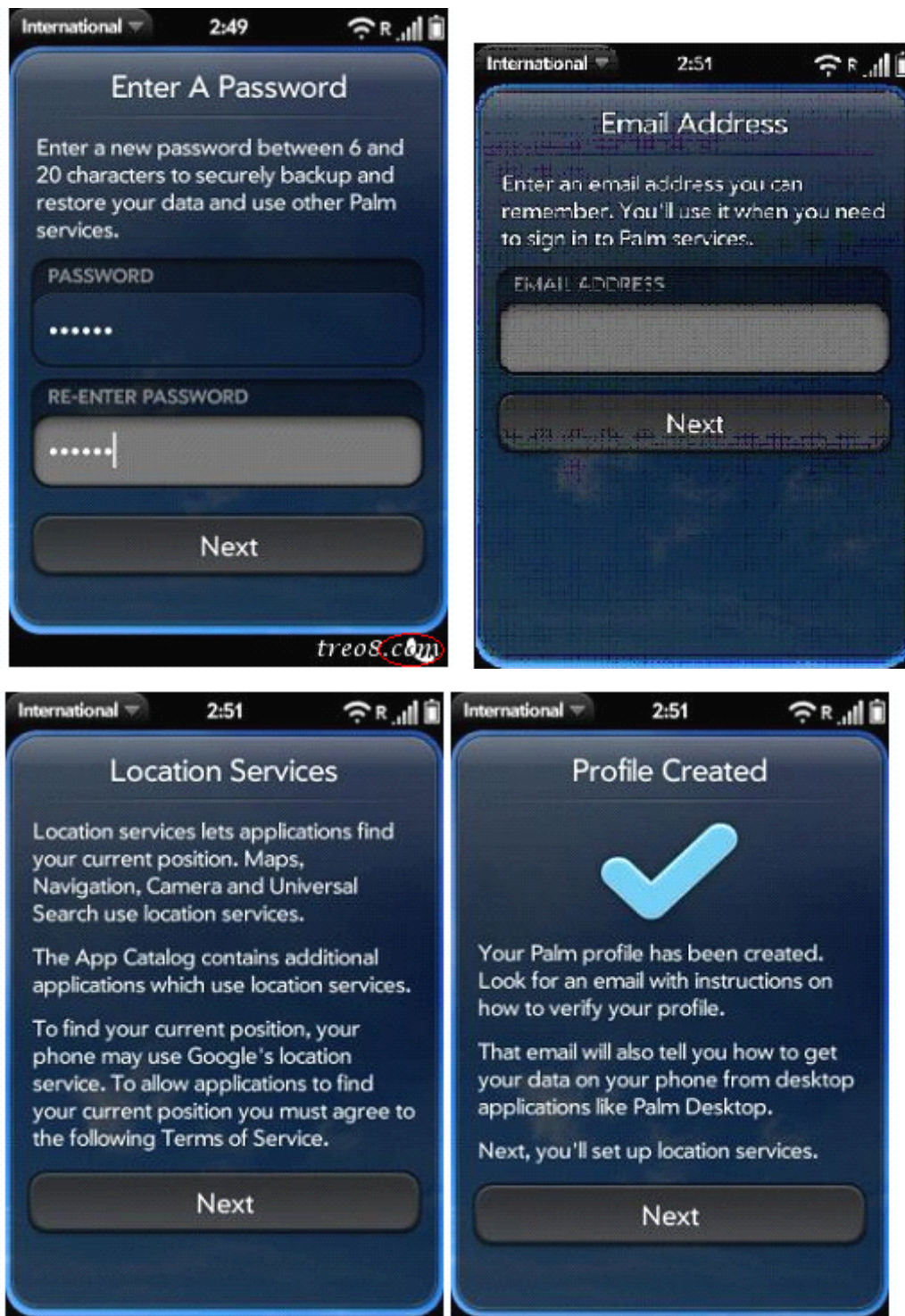
在刷机完成后, 经 Palm 重启, 手机界面进入如下界面, 选择 “English” :





经上述几个步骤后，手机已被激活，这时 Palm 要求进行用户注册，在屏幕中选择“Accept”，并点击屏幕右下角的电话图标，选择“Enable WiFi”，开启 WiFi。

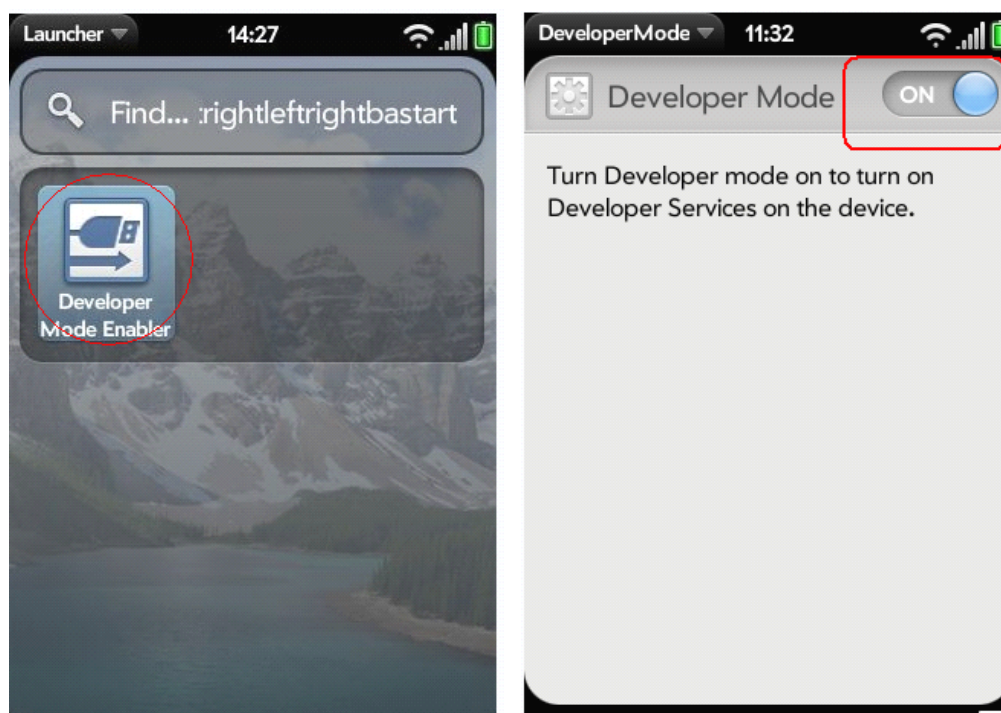
以拔出电板方式重新开机后，点击“Create new profile”，建立 Pre 个人账户。



以上完成了激活以及个人账号创建的工作。

第三步：连接与备份

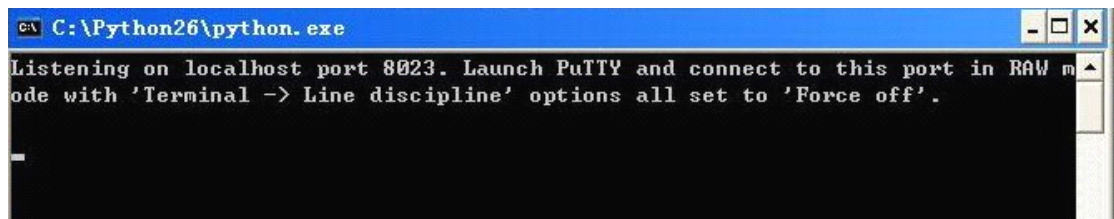
在完成激活后，需要连接 Palm 手机完成各种的写码，这要求手机要处于“开发者模式”下，进入该模式的方式是：在标准的待机界面下输入“魂斗罗秘笈”：“**upupdownndownlefttrightlefttrightbastart**”，在升级 1.1 ROM 后，新增加了一个秘笈“**webos20090606**”：



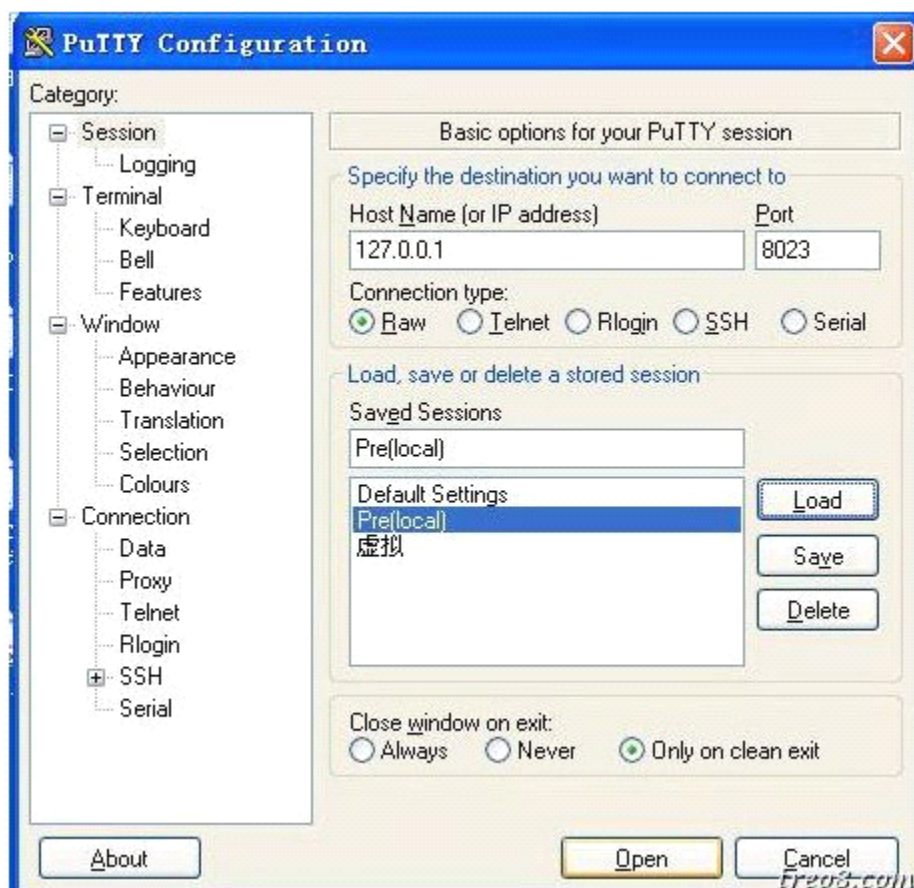
第一次进入该界面是默认的开发模式是 OFF 状态，需要将按钮置成 ON，确认后 Palm 会进行一次重启，重启完成后再输入秘笈进入开发者模式。打开 Pre 上的 developer 模式后，在打开机器的情况下连上数据线，Pre 上会弹出一个窗口来选择同步多媒体、当 U 盘使用以及充电等三种模式，选择 Just Charge 即可开始后续的操作。

在确保电脑上安装装了 java6, python, 并下载到了 putty 软件和端口监听脚本 novaproxy。

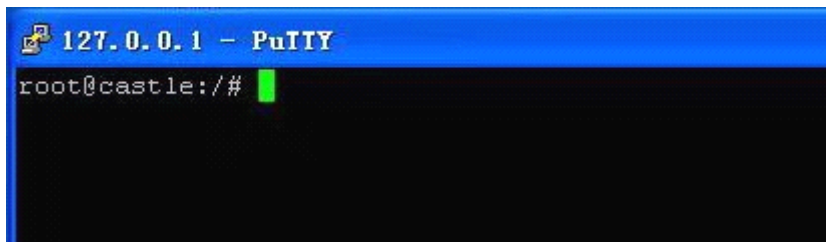
运行监听脚本 novaproxy.py，该脚本有 python 负责执行，直接双击运行后会有个 DOS 窗口，请保持该窗口一直开着状态。



然后双击 Putty.exe 程序，首先在 putty 的窗口下设置到 Pre 的连接，IP 是 127.0.0.1，Port 是 8023，登录方式选择 raw，可将该配置信息保存起来，方便下次直接双击“Saved sessions”中的列表：



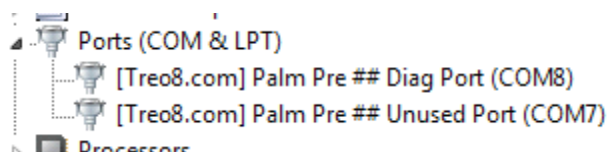
从这登录到 Pre 后，即是 root 用户登录：



对于所要执行的操作，见具体的各操作说明进行操作，在写码前有个常用的命令，用于设置 Palm pre 连接到电脑的端口，在 root 连接到 Palm 手机后，请执行：

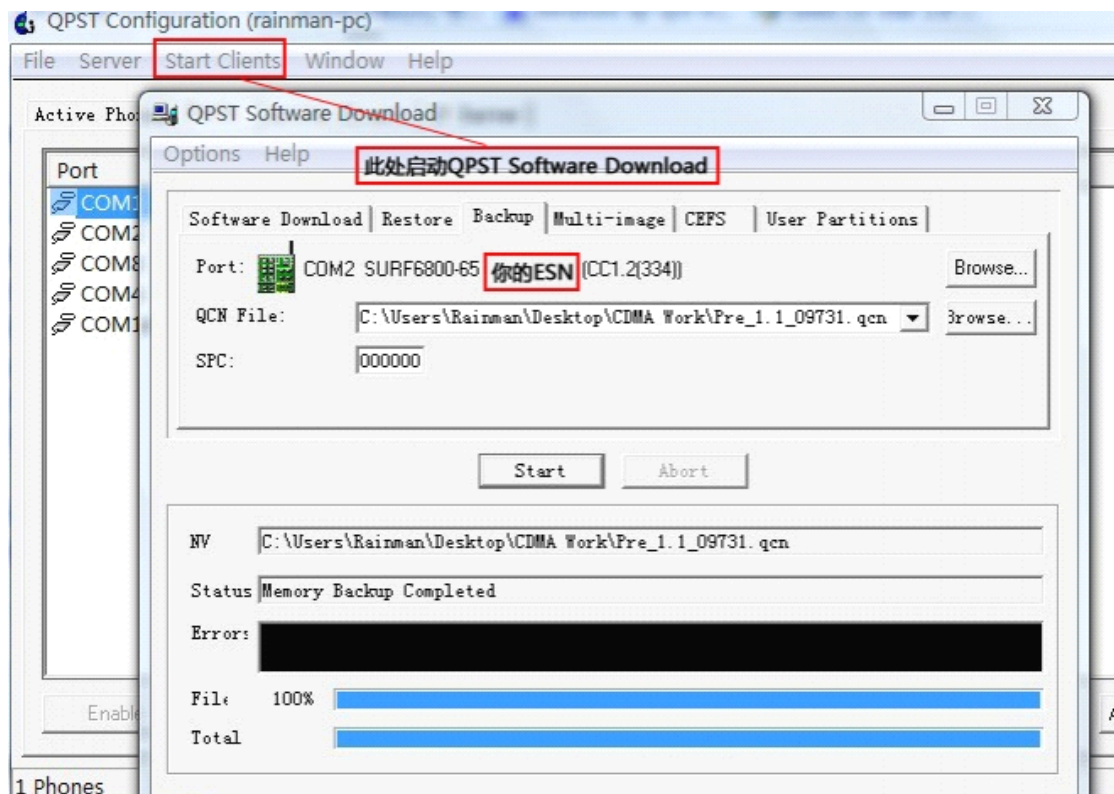
/usr/bin/mpt diag

进入电脑设备管理器中可见到两个同 Palm pre 有关的端口号，一般情况下需要更新这设备中的驱动，相关驱动程序可从 PalmPreCentroTreo800w_ **DiagDrivers** 压缩包中获取，手工进行安装即可，完成后有如下的界面结果显示：



为避免写码失败需要复用 Pre 原始 MV 内存状态，可采用 QPST 工具进行内存备份，操作如下：

从 QPST configuration 中运行 QPST 的 Software download 客户端，如图选择 Backup 选项卡，备份修改 ESN 前的内存状态，以便在话机出现问题时进行恢复。



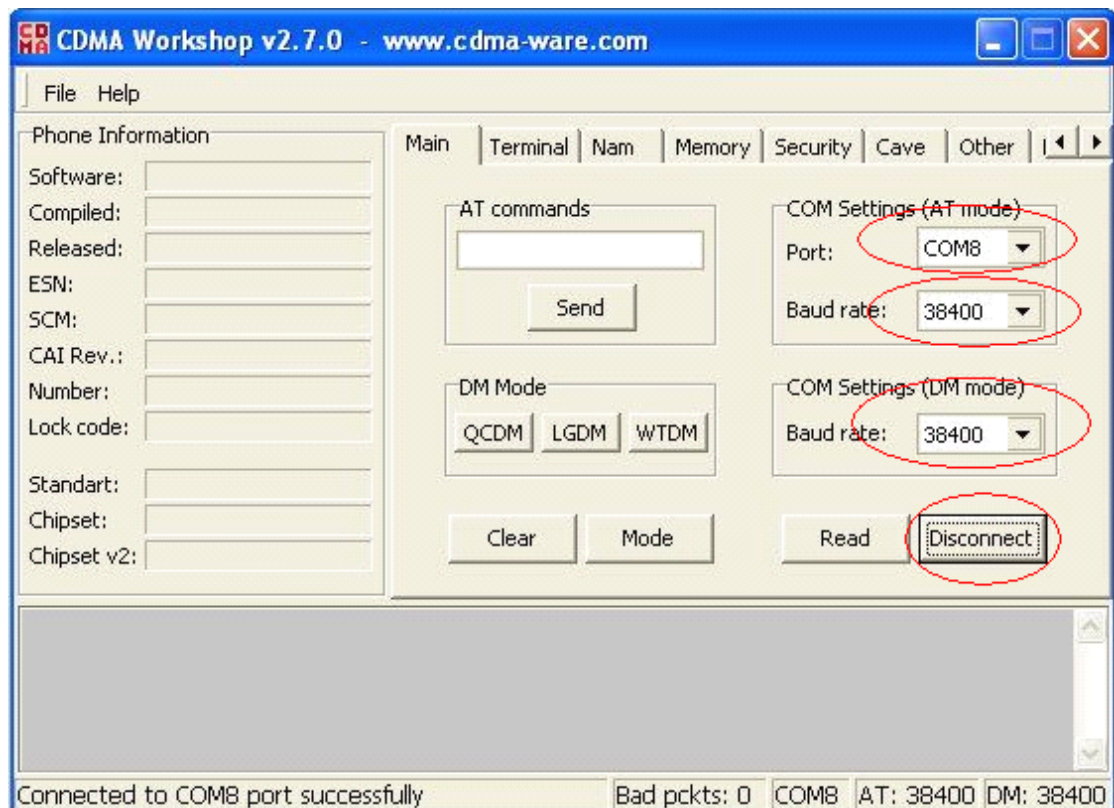
由于备份的信息主要是 MEID 和 ESN，可通过查询获得到这两值记录下来也可起备份效果，而不用通过 QPST 进行相关备份：

- 记录 ESN：输入“##3282#”后，系统出现相关的信息，并选择界面中右下角的“MENUADVANCE”，进入新页面的第一行既是本机的 ESN。
- 记录 MEID：在包装盒上有登记着 MEID HEX，在取下手机电池后机身中也有登记。

第四步：扫描 SPC

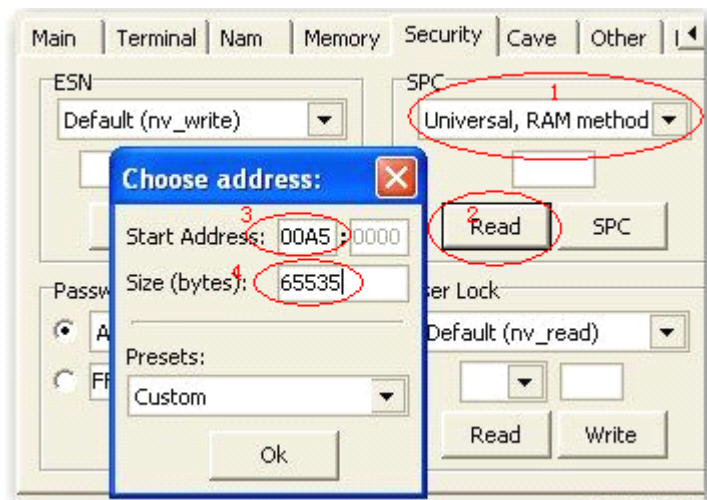
SPC 是访问 Palm pre 的密钥口令，需要通过工具读取并进行修改，一般修改成“000000”，具体扫描方式如下：

通过上述连接方式，到设备管理器中找到 Palm pre 的连接端口，将该端口号设置到 Workshop 界面中：



点击“Connect”后，若连接成功则出现“Disconnect”按钮。同时点击“Read”按钮可以查询出当前机器的相关信息。

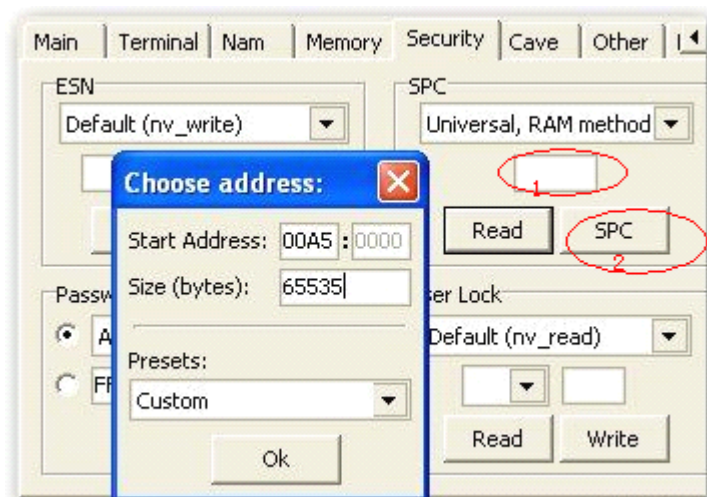
进入“Security”界面，通过选择 SPC 访问方式，点击“Read”后出现“Choose address”界面，设置相关参数后点击“OK”，开始扫描 SPC 密码，有可能一次扫描不能完成出现异常，可以多试几次。



扫描成功后出现如下界面：



一般未改过 SPC 前不会是“000000”的，需要进行 SPC 修改，首先将获得的 SPC 写入如下界面 1 中，然后点击“SPC\send”进行验证，会提示 phone unlock 字样，这时将“000000”填入如下界面 1 中，点击“SPC\write”，完成后提示修改成功。



第五步：写 IMSI

点击 Workshop 界面中的“Nam” sheet，进入 IMSI 修改界面，可点击“Read”获取当前 IMSI 的相关信息，然后根据一下进行信息修改，对于未提到的信息请勿做调整。

通过从电信中查询到的 UIM 卡 IMSI 信息，取其后 10 位填入 1 中，一般是“659*****”，并将：

- MCC 设置成 460，
- MNC 设置成 03，
- SID 设置为福州的 ID，为 14136，
- NID 设置为 65535.

Main | Terminal | **Nam** | Memory | Security | Cave | Other | ◀ ▶

Nam Programming

MIN: 0300001234 Dir_Number: 0000001234 Name:

MCC: 460 SID: 0 0 0 0 0 0 0

MNC: 03 NID: 0 0 0 0 0 0 0

P CH: 283 384 SCM: SCI: 2 Accolc: 1 Nam: 1

S CH: 691 777 IMSI: Banner: CTC

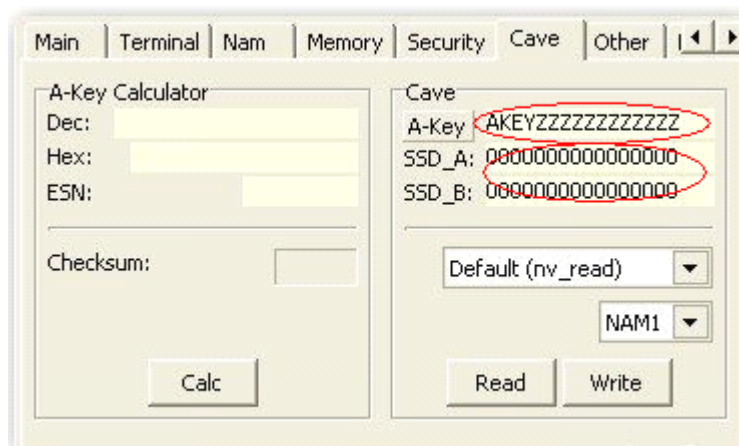
PRL: Enabled System: Otapa: Disabled

NAM1 Load Save 0 Read 6 Write

填写完成后点击“Write”，有可能会提示 Palm 无响应，可以多点几次。

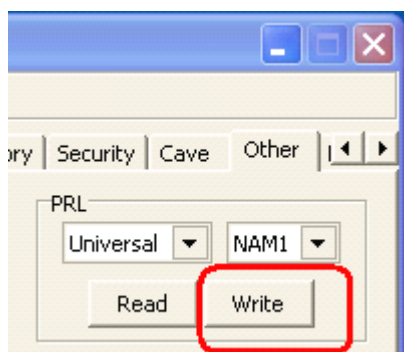
第六步：写 AKEY

点击 Workshop 界面中的“Cave” sheet，进入 AKEY 修改界面，可将从电信中查询到的 AuthenticationKey 写入 A-KEY 中，SSD-A、SSD-B 都填 0 即可，然后点击“Write”。

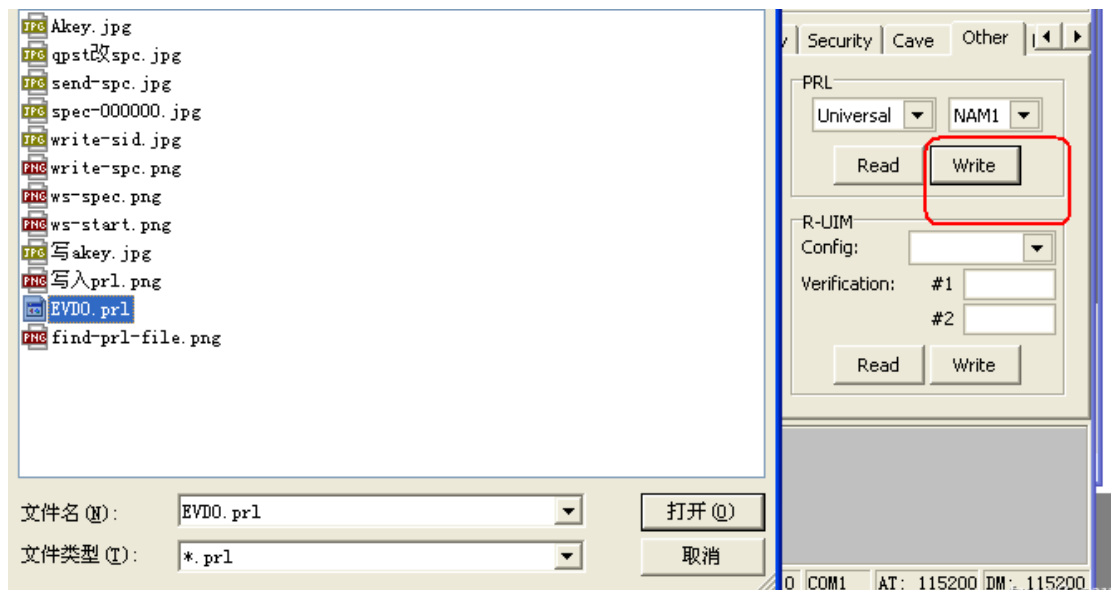


第七步：写 Prl

点击 Workshop 界面中的“Other” sheet，进入 Prl 修改界面，直接点击 PRL 中的“Write”：



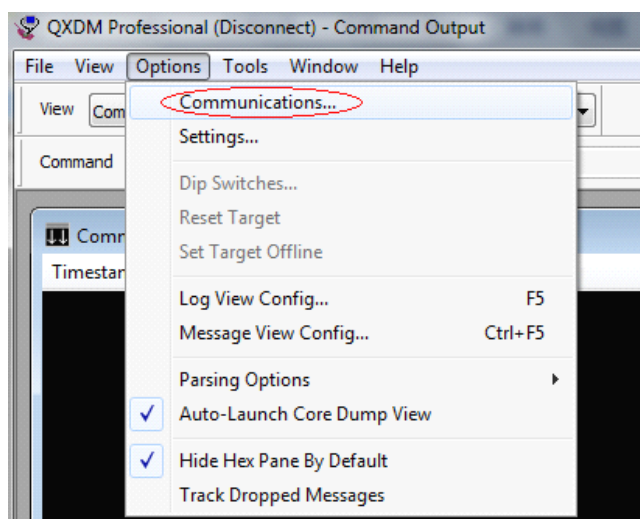
系统弹出“evdo.prl”文件的选择界面，选择好后系统就启动写 Prl 的操作：



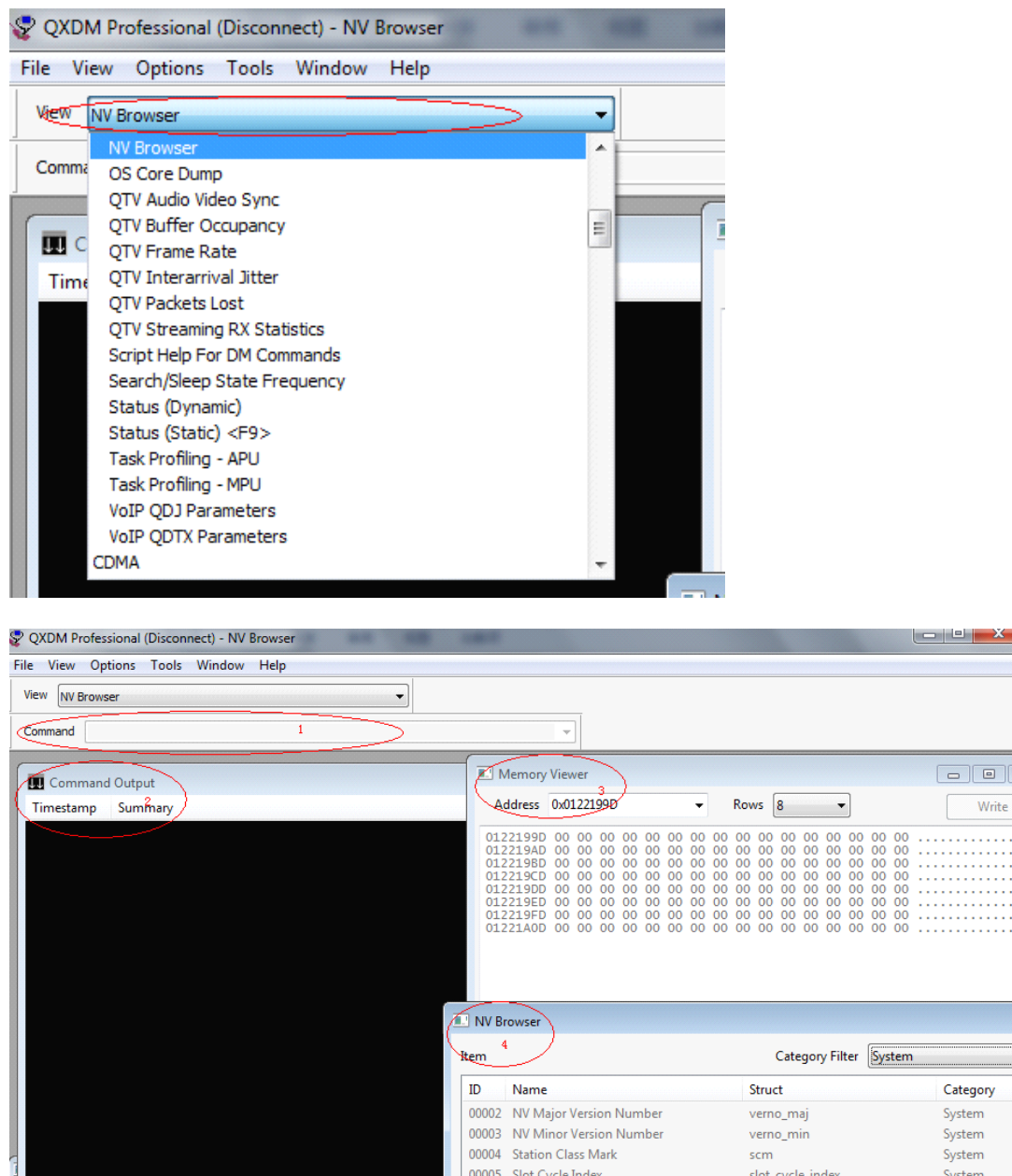
第八步：改 meid、esn

该步骤适用于无法修改局端 ESN 的模式。

启动 qdxm professional，设置中选择 communication，选择 pre 连接的 com 口，连接开发者模式下的 Pre。



开启 qdxm 中的 Memory Viewer 窗口、Command 和 Command Output 窗口



在 Command 输入以下命令，可看到 TX 的数据是"00000000000"之类.....tx 是发送请求的数据,比如读取,RX 则是返回的值：

```
spc 000000
RequestNVItemRead meid
RequestNVItemRead esn
RequestNVItemRead scm
```

在 QXDM 中选择 View--New--Common--NV Brower，找出 meid_cd 项，写入值“1”后 “Write”。

按顺序验证以下地址（注：以下地址仅适用 1.0.3 版本的，对其他新版本不适用），依次在 Memory Viewer 中输入上面地址，将对应的 MEID、ESN 顺序清零并 write，即在 Memory Viewer 窗口对应地址位，写入相同长度“00”，后点 write 键写入。注意其中格式为逐字节反序，即本机 ESN 为 1A2B3C4D，则 Viewer 中显示 4D 3C 2B 1A。

MEID addresses

0x00A5C340
0x00F28B20
0x00F2D899
0x0102DC34
0x0102DD04
0x010373AC
0x01221609

ESN addresses:

0x00A5BEC4
0x00A5C358
0x00A62618
0x00A63560
0x00A86188
0x00AAD0FC
0x00AACF40
0x0109B2AC
0x0122199D

再次在 Command 行输入命令，分别读取 MEID、ESN、SCM 等数据，如确认 MEID、ESN 已清零后方可继续下一步操作：

```
RequestNVItemRead meid  
RequestNVItemRead esn  
RequestNVItemRead scm
```

以命令模式写入 MEID、ESN、SCM：

```
RequestNVItemWrite scm 0x2A  
RequestNVItemWrite esn 0x1A2B3C4D(你要写入的 ESN)
```


RequestNVItemWrite meid 0x0000000000000000(此时写入是会报错，可以继续往下)

通常 ESN 已写入关键地址，需核查以上 ESN 地址列表中的每个地址，未写入数据的请写入你的 ESN 地址。同时检查 0x01221609 等地址的 MEID 通常都会有反复，如已改变，需再次清零、写入。

在 QXDM 中选择 View--New--Common--NV Brower，找出 meid_cd 项，写入值“0”后 “Write”。

重启 Palm 后可试着拨打 10000 等号码，正常情况可以开始通话了，为方便 Palm 对中文的支持，需要对其 1.0.3 版本进行升级。

第九步：升级 ROM

当前 Webos 已提供 1.2.1, qinray 所提供的也有 1.2 版本，在完成 1.0.3 安装后，需要在关机的状态下重新进行刷 ROM，即重复文中“第二步”的刷机部分。

在刷机完成后需要拔掉后盖电池的方式重启机器，重启完成进入开发者模式，进入 Workshop，先查询以下参数是否同之前设置的一致，若不一致请根据以下值重新设置：

- MCC 设置成 460，
- MNC 设置成 03，
- SID 设置为福州的 ID，为 14136，

- NID 设置为 65535
- AKEY 设置为电信查询到的 AuthenticationKey
- PRL 设置为 evdo.prl

进入 QXDM professional 界面中，

```
spc 000000
RequestNVItemRead meid
RequestNVItemRead esn
RequestNVItemRead scm
```

检查 scm 是否为 0x2A，若不是则执行如下：

在 QXDM 中选择 View--New--Common--NV Brower，找出 meid_cd 项，写入值“1”后 “Write”。

```
RequestNVItemWrite scm 0x2A
```

在 QXDM 中选择 View--New--Common--NV Brower，找出 meid_cd 项，写入值“0”后 “Write”。

上述都设置完成后重启 Palm，即可实现版本升级。

以 USB 的模式访问 Pre，更改当前路径下的 config.ini 文件，将其中的 meid 设置为原厂本机所带的 meid 值。

第十步：写 1X EVDO

在写 EVDO 前，请确保 Palm 开启开发者模式，并将 ROM 升级至 1.1/1.2 版本 ROM，建议直接采用 qinray 的 ROM 定制版，并自行配置好 config.ini 文件。

出于对手机的安全考虑，不管是否使用 qinray 定制的 rom，检查 /etc/event.d/ 路径下的 LunaSysMgr 文件，用 vi 命令编辑该文件。

以下为原文件内容：

```
pre-start script
    echo "1" > /proc/sys/vm/overcommit_memory
    mkdir -p /var/luna/preferences
    if [ ! -f /var/luna/preferences/ran-first-use ]
    then
        echo " -u minimal -a com.palm.app.firstuse" >
/var/luna/preferences/sysmgr-args
    else
        echo "" > /var/luna/preferences/sysmgr-args
    fi
end script
```

以下为修改后的文件内容，请注意红色“#”内容，若检查文件已为以下内容，那无需再做调整：

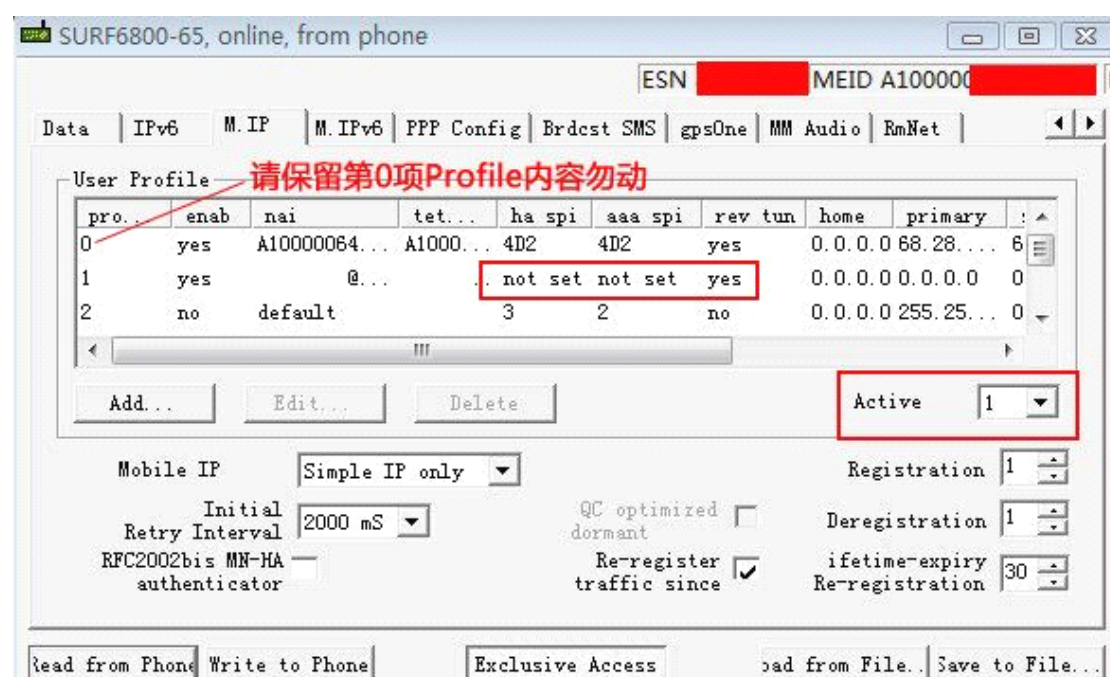
```
pre-start script
    echo "1" > /proc/sys/vm/overcommit_memory
    mkdir -p /var/luna/preferences
    # if [ ! -f /var/luna/preferences/ran-first-use ]
    # then
    #     echo " -u minimal -a com.palm.app.firstuse" >
/var/luna/preferences/sysmgr-args
    # else
    #     echo "" > /var/luna/preferences/sysmgr-args
    # fi
end script
```

务必记住之后不要轻易关闭开发者模式，它能让你在可能无法正常登入 Palm Pre 主界面时，有机会以终端模式连接电脑恢复数据和修复软件故障，

启动 Python 监听脚本，将 Putty 连接至 pre，并在终端窗口输入“mpt d”，启动 QPST 并连接上所选串口，确认选择连接了 pre 后，进入 Service

Programming 界面，读取话机数据，检查 CDMA/CDMA2 中使用的数据是否与你当前写号配置一致。升级 1.1/1.2 后 MCC 和 MNC 会发生变化请在此重新写入。在 SYSTEM 选项卡中，检查输入你的 Home SID/NID。

进入“M.IP” Sheet 界面，这里将是能否通过数据验证并 EV 的关键。数据需如图填写，Mobile IP 项一定要选择 **Simple IP only**。对于第 0 项数据，请勿做改动。



在“M.IP” Sheet 界面选择列表中第二项进行编辑，参照图片内容修改数据。此处 NAI 的填写与真正的 PPP 拨号密码及 EV 的 AN/AAA 无关，请按图示格式以确保能通过认证。确保清空 MN-HA SPI、MN-AAA SPI、DMU Mobile Authenticator 三项。此处请反复读写确认。

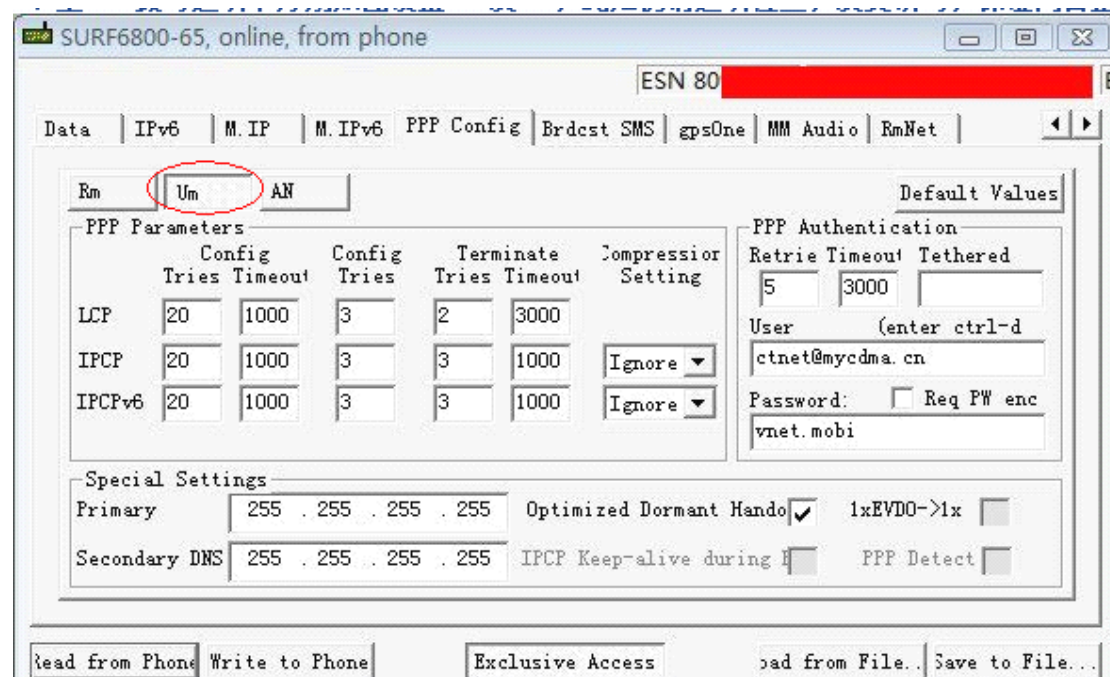
在 NAI 和 Tethered 输入框中，将“[ESN 号@sprintpcs.com](#)”填入 NAI，将“[ESN 号@modem.sprintpcs.com](#)”填入 Tethered。



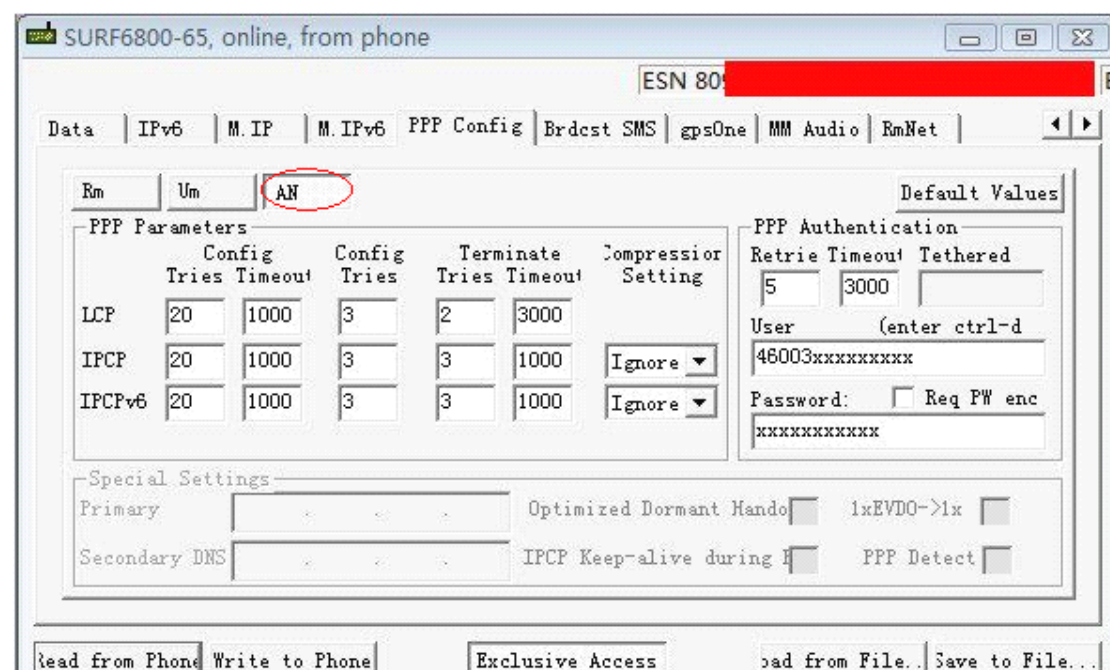
PPP 拨号选项卡分别如图设置 UM 及 AN，此处仍请逐项检查，反复读写，保证内容正确，将 UM 和 AN 两界面都调整后一次性提交“Write to Phone”写入手机。

填写 User: “ctnet@mycdma.cn”、Password: “vnet.mobi”；

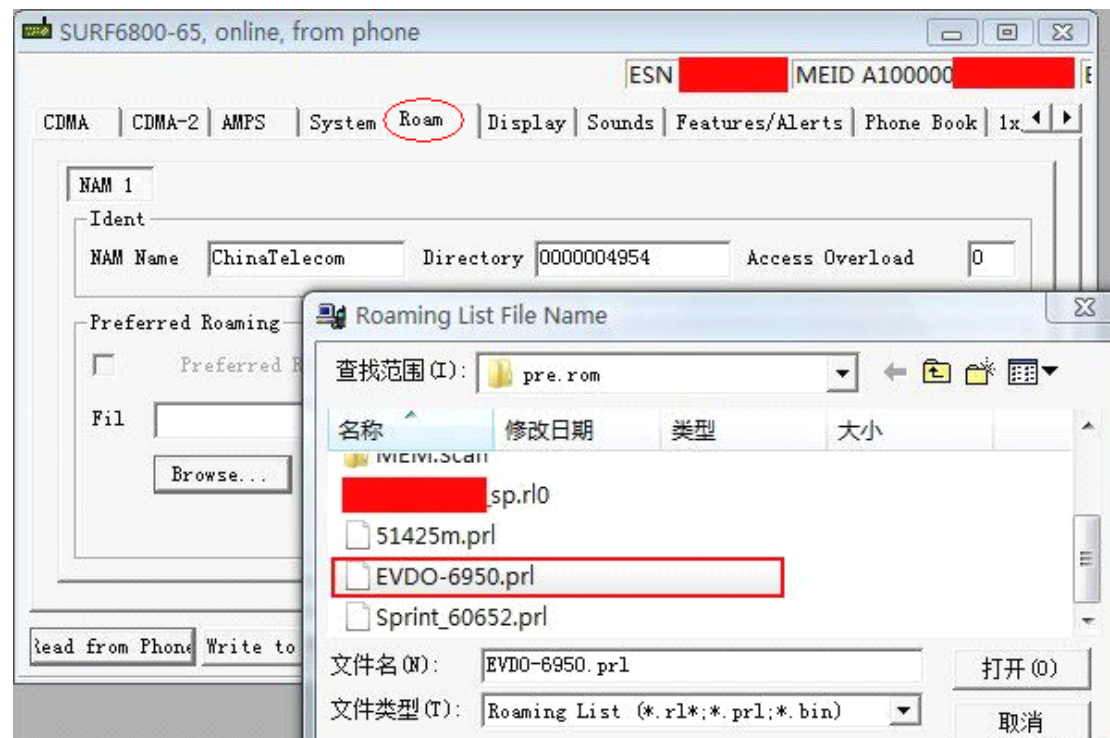
填写 Special Settings 中的 Primary 和 secondary DNS，都为“255.255.255.255”；



填写 User 和 Password，将通过电信所查询到的 EVDO 上网账号和密码分别填入输入框，若原先给的账号含“@mycdma.cn”的，可将这部分去掉。



至 Roam 选项卡，Browse 选择你下载的 PRL 文件，升级 PRL。



上述步骤后，将机器重启后部分用户可能至此为止，手机已经在搜索信号，稍后即出现 1X 或 EV 标识，那么恭喜，你已经通过了数据认证，可以上网了。

若没有出现可尝试通过开启/关闭 WIFI、在拨号盘界面进入 Preferences 中关闭/开启“data usage”，过会儿一般会出现 EV 的图标。

附录一：各地 SID 值

北京	13824	双鸭山	13985	青岛	13945
上海	13840	牡丹江	13979	河北沧州	14001
广州	13828	大庆	13981	南京	14174
深圳	13844	吉林市	13966	呼和浩特	14120
湛江	13848	合肥市	14151	包头	14118
长春	13965	广西南宁	14225	湖北宜昌	13890
阜新	13866	福建泉州	14140	武汉	13884
抚顺	13861	辽宁朝阳	13869	广西玉林	14228
淄博	13943	唐山	13995	青岛	13945
杭州	14121	吉林松原	13970	海口	14148
沈阳	13858	安徽芜湖	14153	秦皇岛	13997
广东中山	13850	山东菏泽	13954	浙江金华	14129
吉林通化	13969	湖南湘潭	14207	盐城	14183
哈尔滨	13977	江苏无锡	14176	山东烟台	13946
大连	13859	陕西西安	13938	唐山	13995
鞍山	13860	湖南郴州	14216	济南	13942
辽宁抚顺	13861	浙江宁波	14124	东营	13950
本溪	13862	长沙	14206	滨州	13952
丹东	13863	安徽淮北	14161	葫芦岛	13871
营口	13865	株洲	14208	日照	13958
荆州	13888	江苏镇江	14178	顺德	13851
常州	14177	汕尾	13843	佛山	13832
潍坊	13944	太原	14091	南海	13851
吉林市	13966	吕梁	14093	广东江门	13835
延边	13967	武汉	13884	河南新乡	14014
昆明	14253	山东枣庄	13957	云南保山	14266
保定	13996	聊城	13953	山东威海	13947
天津市	13940	盘锦	13870	河南洛阳	14010
江苏南通	14179	贵州毕节	14249	山东泰安	13948
佳木斯	13980	广东肇庆	13849	福州	14136
鹤岗	13984	浙江台州	14126		