

## 北京联通光猫华为 HN8346V5 破解方法介绍

北京联通的华为 HN8346V5 是因为 2020 年初刚上 1000M 宽带换上的光猫。此光猫端口为路由模式，客户只能使用普通用户权限，里面的设置就是供你看看，想加点常用的诸如端口映射、开 UPnP 等都是不行，于是决定破解。

### 北京联通华为 HN8346V5 固件基本的情况

固件版本为 V5R019C30S020，硬件版本 1960A。

准备软件：

- 1、华为光猫 ONT 维修使能工具.exe：开设备端口 Telnet 功能
- 2、华为光猫 ONT 组播配置工具.exe：补全设备 shell 命令
- 3、tftpd32.exe：用于备份配置文件
- 4、putty.exe：远程登陆设备工具
- 5、华为配置文件解密和加密工具.exe：这个工具可以在 Windows 下对华为 hw\_ctree.xml 进行处理，可以解密解压缩成为明文的形式，同时也可以加密压缩还原为原始的形式。相当于华为光猫中的 aescrypt2 命令。

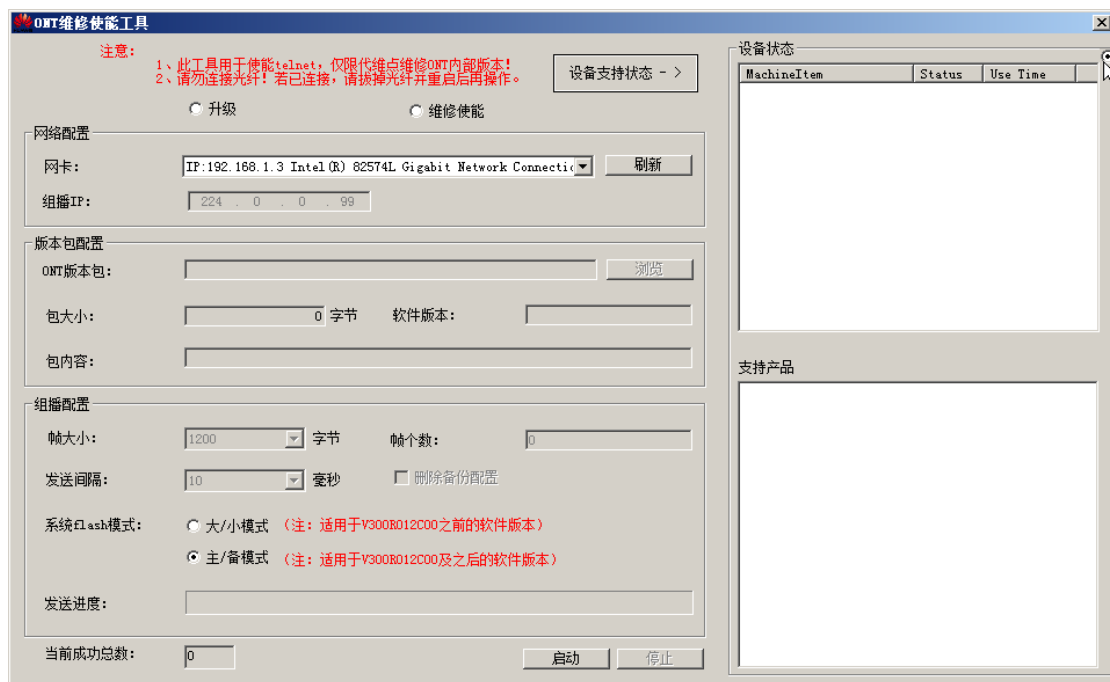
### 破解步骤：

- 1、使用“华为光猫 ONT 维修使能工具.exe”打开 Telnet 功能



选择“维修使能”，点击“启动”，此时光猫所有指示灯闪烁，等到所有指示灯灭后，点击“停止”按钮，关闭工具程序，重新启动光猫。

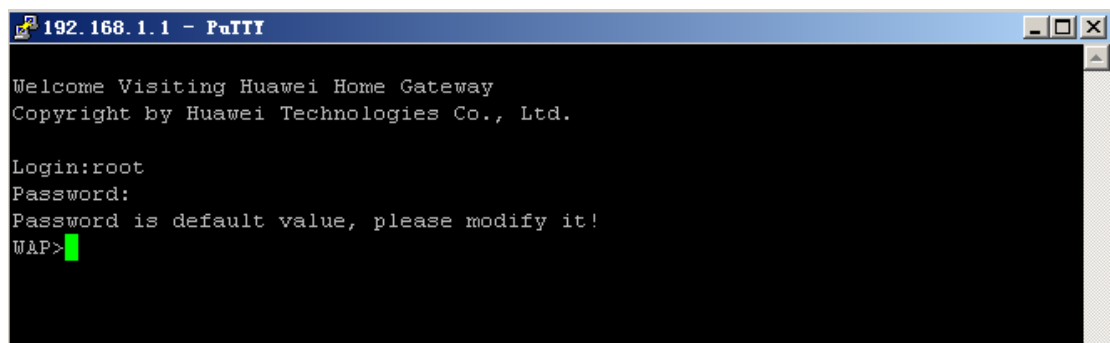
## 2、使用“华为光猫 ONT 组播配置工具.exe”补全设备 shell 命令



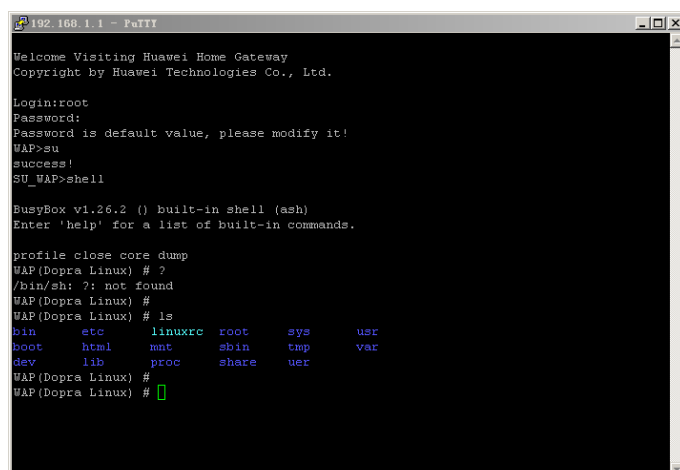
注意选择右上角那个点，点击“启动”，此时光猫所有指示灯闪烁，等到所有指示灯一直亮后，点击“停止”按钮，关闭工具程序，重新启动光猫。

## 3、备份设备配置文件

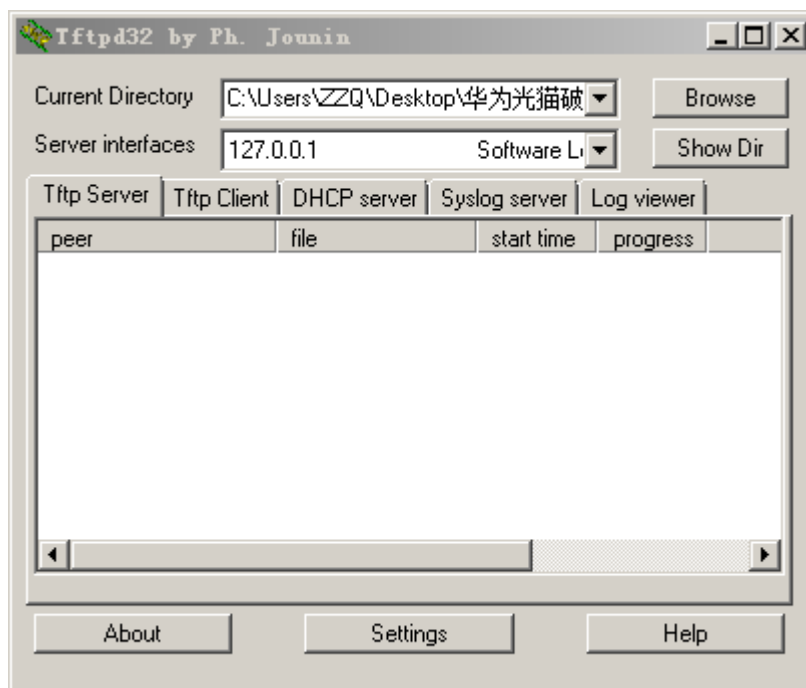
通过“putty.exe”进入 Telnet 后（用户名：root，密码：adminHW）



然后输入“su”回车，输入“shell”回车，输入“ls”回车，看是否能看到路径



进入目录/mnt/jffs2，复制原配置文件“hw\_ctree.xml”到“myconfig.xml.gz”中  
输入“cp hw\_ctree.xml myconfig.xml.gz”回车  
这个文件是 AES 加密的，所以先解密，  
输入“aescrypt2 1 myconfig.xml.gz tmp”回车  
解密后的文件还是被压缩了的，所以要用 gunzip 命令展开压缩文件“myconfig.xml.gz”，  
得到“myconfig.xml”。  
输入“gunzip myconfig.xml.gz”回车  
把生成的 XML 文件用 TFTP 传回来  
先打开“tftp32.exe”  
然后输入“tftp -p -l myconfig.xml -r myconfig.xml 你机器的 IP 地址”



#### 4、恢复华为登录界面

输入“restorehwmode.sh”命令回车，光猫将恢复为华为界面。看到提示“successful”后，重启光猫，就会转为华为原厂界面。光猫的 IP 地址将变为 192.168.100.1，超级账户名：telecomadmin，密码：admintelecom。SSID：WirelessNET，密码：eeeeeeee。

5、重新启动光猫后，已经恢复为华为登录界面，并且有 telecomadmin 超级用户权限，登录进去以后，使用配置文件导入功能将上面生成的“myconfig.xml”配置文件导入即可。光猫重新启动后，以前的所有设置全部恢复回来了。  
恢复到华为界面后功能强大（同时比联通界面下超级管理员的功能还多一些）。路由和桥接可以自由选择。

欢迎使用华为ONT，让您轻松完成网络设置！

用户名：

密码：

登 录

