# 星际宝盒CM520刷机教程（TTL）

前言：本刷机教程完全参考的M大的，仅为像我这样的小白做点优化。

首先我们看看原厂固件

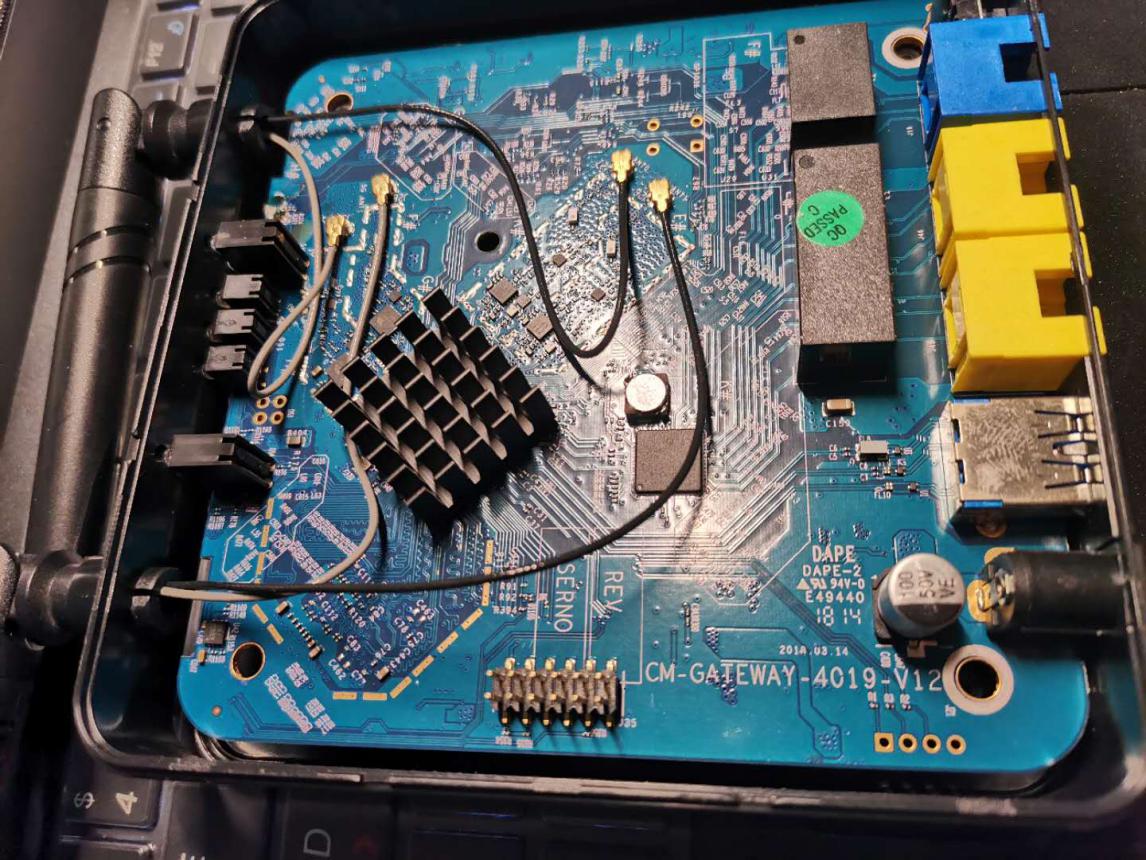
原版固件仅适合挖矿用，有可能包含挖矿后门，功能非常少，IPQ4019不支持的频段竟然也能设置？



## 拆机方法

1. 用刀片或者最小的一字起“挑”开底部四个硬塑料
2. 十字螺丝刀拆掉4颗螺丝
3. 拆掉上下壳子，拆掉天线，取出主板。

（这路由也是奇葩，明明4条天线却合到两个天线外壳里面）



准备

TTL转接线，淘宝随便买个几块钱包邮的就可以

网线一根

文件下载地址：关注微信公众号“WIFI物联网”，往期内容——新年首发——文章最下面随便打赏即可获得。

或者下载我的集成包（2020.2.29更新）

链接：https://pan.baidu.com/s/1yii-XJeiJ0cWwHSdRvNiNA

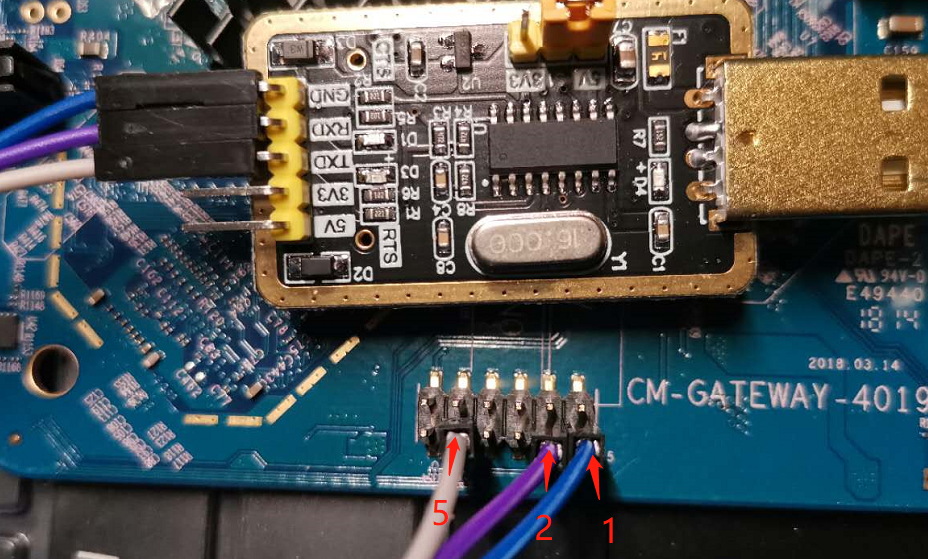
提取码：ock0

## TTL刷机方法（感谢mleaf大神的教程）

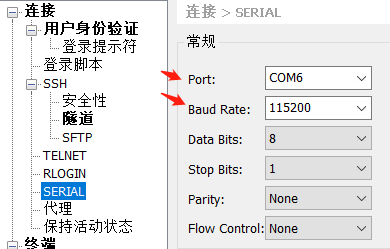
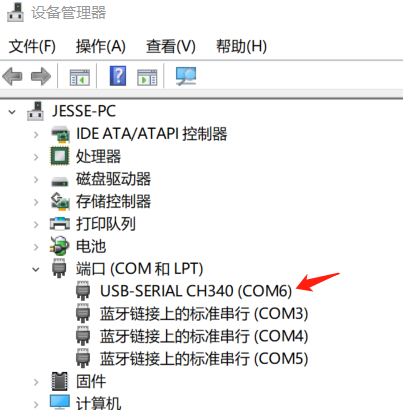
1. TTL线连接

原教程用CP2102模块转接器，接线顺序是1-2-5分别为GND-TXD-RXD我尝试N次未成功（可能是我对发送和接收理解错误）。

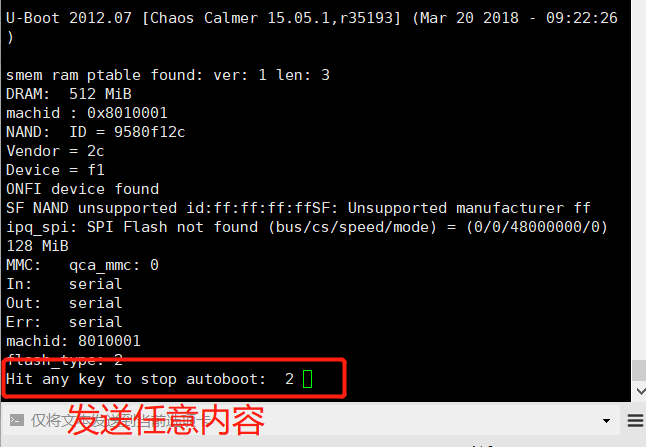
我买的是CH340G模块，WIN10自动安装的驱动，1-2-5接转换器GND-RXD-TXD，测试正常。



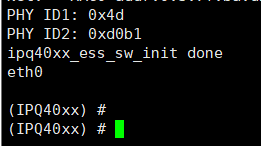
1. 使用xshell连接路由，波特率115200，串口号查看方法：win键+X-》设备管理器-》端口



1. xshell连接后，路由器插电启动，大约2秒后出现如下显示，发送任意内容。



1. 出现（IPQ40XX）即进入恢复模式，此时可以输入OpBoot



1. 宝盒直接设置网卡IP为192.168.1.188（使用print命令查看当前uboot环境变量，查看serverip，然后将电脑ip固定为所查询到的ip。）

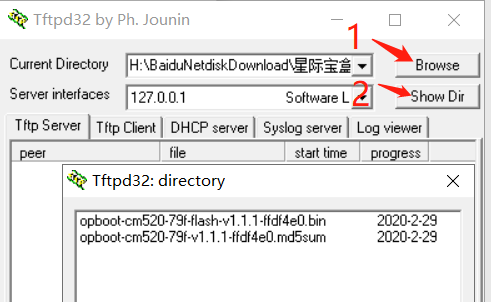


1. 在tftpd32指定OpBoot路径【opboot-cm520-79f-flash-v1.1.1-ffdf4e0.bin】

注意：请务必使用MD5校验工具校验

opboot-cm520-79f-flash-v1.1.1-ffdf4e0.bin

的MD5值，是否和opboot-cm520-79f-v1.1.1-ffdf4e0.md5sum中的值一样。

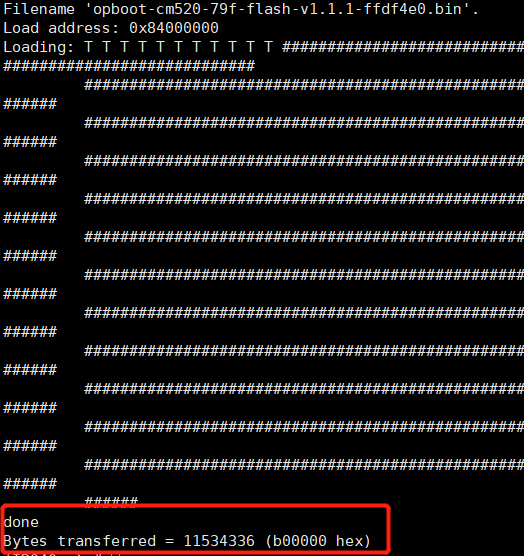


1. 传opboot到路由，在终端中输入：

tftpboot opboot-cm520-79f-flash-v1.1.1-ffdf4e0.bin

(tftpboot opboot-cm520-79f-flash-v1.1.2-cd881f4.bin)更新 3.17日

Loading正常显示“#”，如一直显示的是“T”,请先关闭电脑防火墙，检查网卡IP设置，网卡连接，检查Tftpd32设置



1. 擦除原版uboot，在终端中输入：

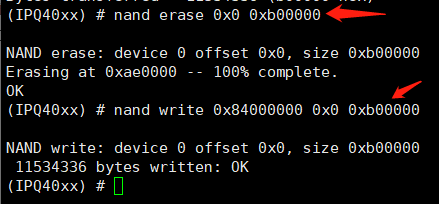
nand erase 0x0 0xb00000

注意：此命令极其危险，如果输入此命令后断电必然成砖，请严格按照教程指引操作。

1. 将OpBoot写入星际宝盒，在终端中输入：

nand write 0x84000000 0x0 0xb00000

（注意：此处的0x84000000是刚刚的tftpboot下载到内存中的地址，每个人机器不一样可能这个地址也不一样，请查看第七步Load address: 后面的地址，将教程中的0x84000000修改为对应的Load address: 后面的地址即可。）



1. 刷opboot完成。网卡改回自动获ip，长按reset键插电进入opboot刷机模式。页面地址192.168.1.1
2. 首次需要刷入ubi格式固件(chrome浏览器左下角显示上传进度）



1. 刷机完成。注意openwrt常见密码，用户名基本是root，密码admin或者password或koolshare



如实在进不去也可以TTL直接改密码，输入passwd修改。

