红米 AX6000 保姆级刷机教程以及排坑指南

AX6000 路由器简介

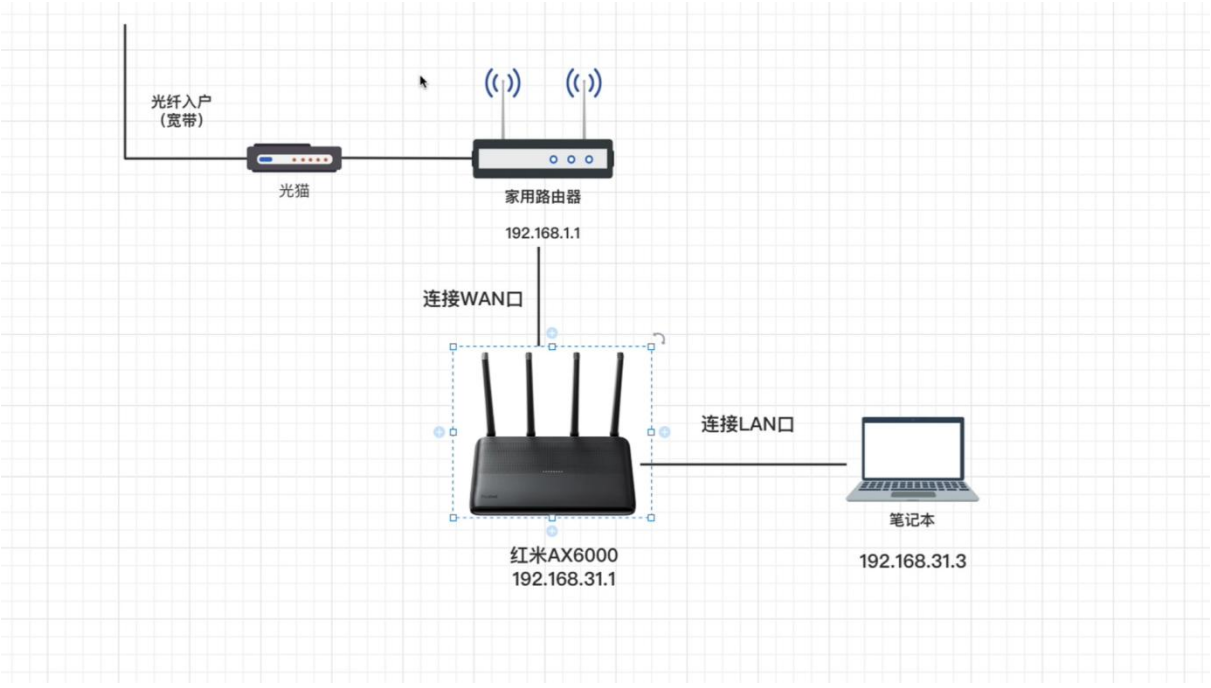
CPU：联发科 FiLogic 830 系列的 MT7986A，四核 A53 架构，12nm 工艺制程，2.0GHz 主频；
内存：512mb+128MB 的存储组合 ；
优点：性价比很高，参数到位。PPD 不到 400 大洋能买到，性能强劲；加上可以刷机，可玩性高。WiFi 信号覆盖还不错，一朵承重墙还能接近跑满 1000M。不过两朵承重墙就会出现断连了。
缺点：散热部分做得比较差，没有 USB 接口，也缺少了 2.5G 网口，希望下一代产品补齐遗憾。

以下是搬运+整理其他大佬的教程得出的保姆级刷机教程

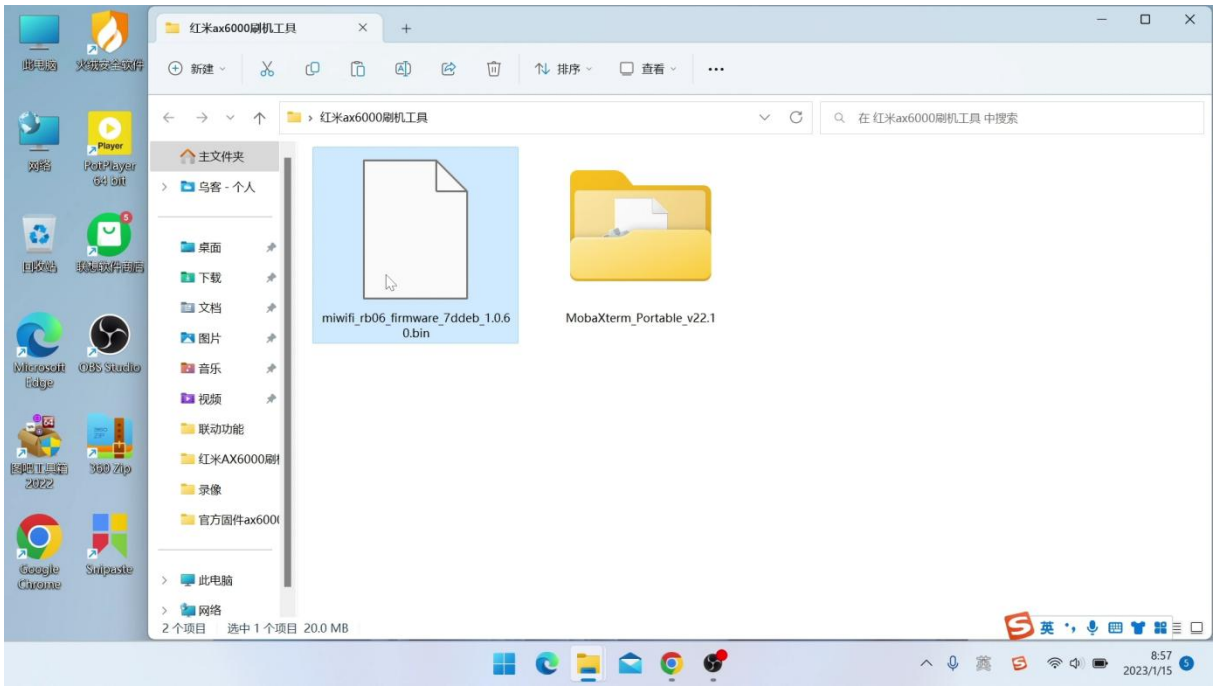
整体思路是 1.解锁 telnet 2. 开启 SSH 3.刷入过度固件 4.升级科学固件 标红处注意一下

1、SSH 解锁

刷机前的准备工作，我们需要把红米 ax6000 的 wan 口连接到现有网络中。并且在 ax6000 的 lan 口上连接上一台电脑。建议用网线将电脑和路由器连接起来，这样刷机会更稳定一些。（连 wifi 刷也问题不大，尽量选有线）



软件方面，我们需要准备一个能连接 ssh 和 **Telnet 的工具。我这里用的 mobaxterm。还需要一个支持解锁的官方固件，这里推荐 1.6.0 这个版本。**

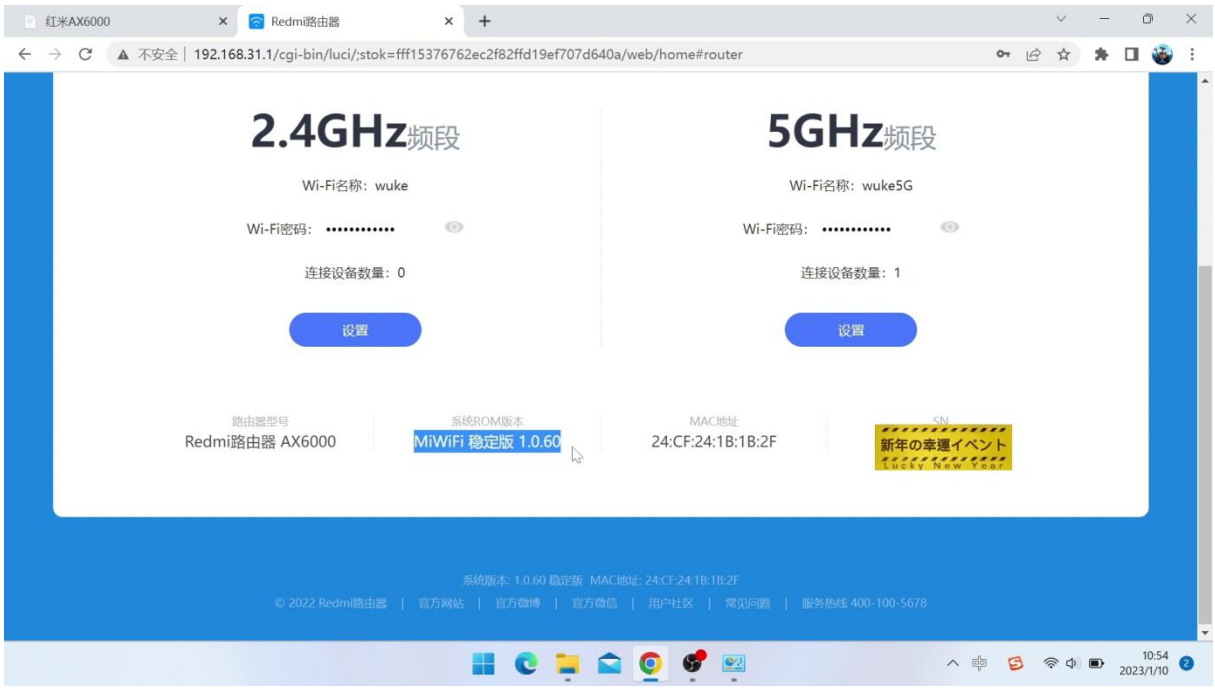


然后是解锁 ssh 代码

一、系统降级

首先要确定下路由器系统的版本，如果不是可以解锁的版本，那么需要在“系统设置”里，把当前系统版本手动降级为 1.6.0。

上传固件，如果提示不成功，则把浏览器地址栏最后面一个数字 0 改为 1，再回车，如果最后一个数字是 1 则改为 2，再回车，就可以降级了

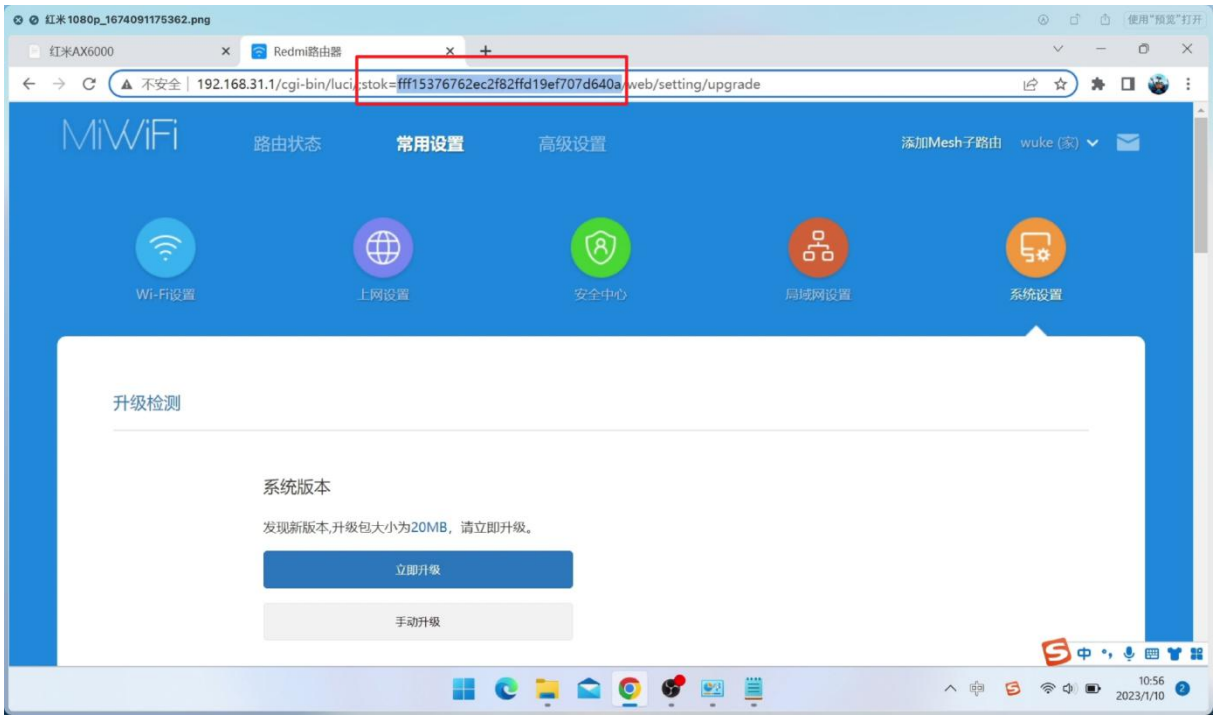


如果当前版本已经是可解锁的则可以忽略这一步。目前可解锁的版本号有 1.0.60; 1.0.48; 1.0.28

路由器在刷机之前最好能初始化一次，并且设置成路由模式。

二、获取 stok

登录到路由器的后台，在地址栏上方会生成一串 stok 的数值。我们需要把 stok 等于后的这串数字复制下来, 这串数字是解锁 ssh 的关键, 不过在每个机器上生成的值都不同, 而且每次重启路由器以后这个值都会改变。



所以每次路由器重启后，我们都需要重新复制一下这串代码。

三、打开红米 AX6000 的开发者模式

首先我们需要解锁下 ax6000 的开发者模式
1、复制以下代码

```
http://192.168.31.1/cgi-bin/luci/;stok={token}/api/misystem/set_sys_time?timezone=%20%27%20%3B%20zz%3D%24%28dd%20if%3D%2Fdev%2Fzero%20bs%3D1%20count%3D2%202%3E%2Fdev%2Fnull%29%20%3B%20printf%20%27%A5%5A%25c%25c%27%20%24zz%20%24zz%20%7C%20mtd%20write%20-%20crash%20%3B%20
```

注意把 stok={token} 的字符{token}替换为路由器生成的 stok 值。

然后把代码复制到浏览器的地址栏里再回车，看到返回过来这样一串字符就表示代码注入成功了。

2、粘贴命令重启路由器

```
http://192.168.31.1/cgi-bin/luci/;stok={token}/api/misystem/set_sys_time?timezone=%20%27%20%3b%20reboot%20%3b%20
```

同样需要替换 stok=后边的字符。
代码注入成功之后，网页同样会返回这样一串字符并且开始重启路由器。

四、设置路由器的 Bdata 参数

1、我们稍等两分钟等路由器重启好了之后，再次登录到路由器的后台。这时需要重新复制一下 stok，因为此时路由器重启后 stok 的值已经改变。
接下来的步骤是设置 Bdata 参数来永久开启 telnet，在新打开的浏览器地址栏中输入以下代码。

```
http://192.168.31.1/cgi-bin/luci/;stok={token}/api/misystem/set_sys_time?timezone=%20%27%20%3B%20bdata%20set%20telnet_en%3D1%20%3B%20bdata%20set%20ssh_en%3D1%20%3B%20bdata%20set%20uart_en%3D1%20%3B%20bdata%20commit%20%3B%20
```

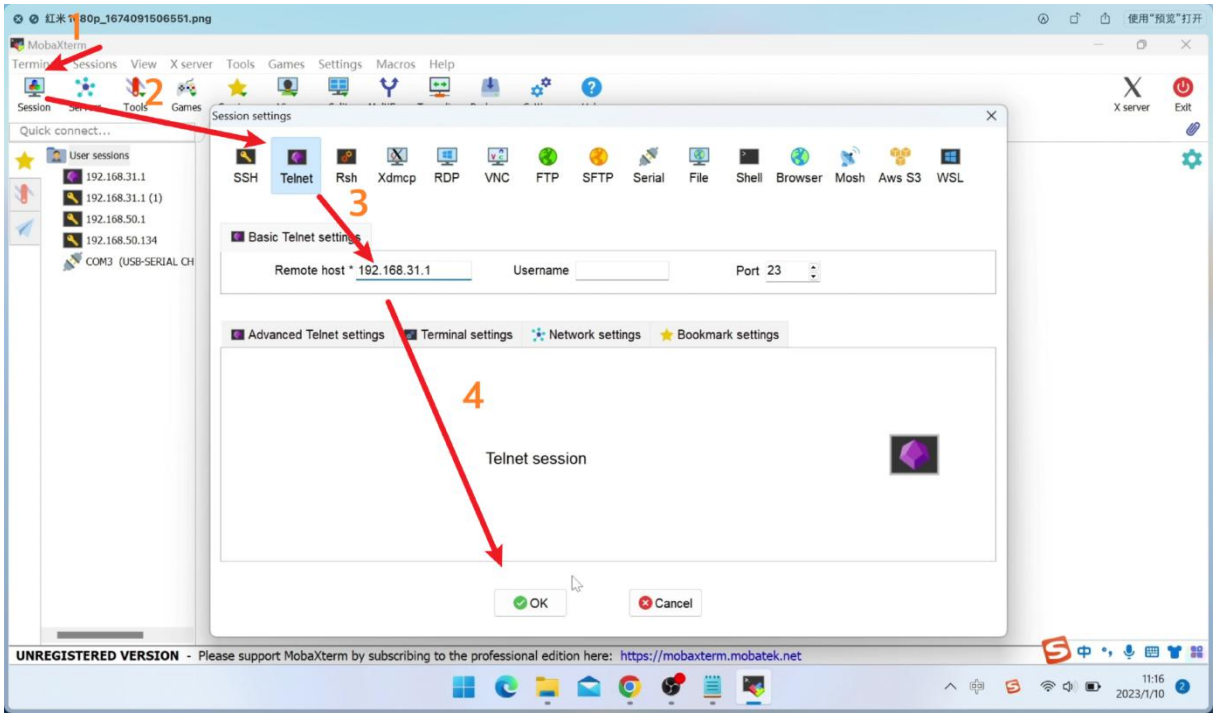
同样将 stok=token 中的{token}替换成路由器新的 stok 即可

2、再次在浏览器里输入以下代码来重启路由器:

```
http://192.168.31.1/cgi-bin/luci/;stok=token/api/misystem/set_sys_time?timezone=%20%27%20%3b%20reboot%20%3b%20
```

五、登录 telnet 开启 ssh

现在我们已经开启了 telnet，可以用 telnet 登录到路由器的后台。
我们打开 mobaxterm，选择 telnet 登录的方式。输入路由器 ip 地址 默认是 192.168.31.1（这里是不用输入用户和密码）点击 ok 登录到 telnet。



接下来我们需要复制粘贴一些代码到 telnet 里执行即可。

1. 修改 root 密码为 admin（不修改也可以通过 SN 计算默认密码)这里我们修改一下

```
echo -e 'admin\nadmin' | passwd root
```

2、固化 SSH

```
bdata set boot_wait=on
bdata commit
nvram set ssh_en=1
```

```
nvram set telnet_en=1
nvram set uart_en=1
nvram set boot_wait=on
nvram commit
sed -i 's/channel=.*/channel="debug"/g' /etc/init.d/dropbear
/etc/init.d/dropbear restart
```

输入命令后没有反馈信息，不用担心，已经执行成功了。

3、永久开启 SSH 的代码（这样即使路由器重启也不会影响 SSH）注意这步需要路由器能够联网。

```
mkdir /data/auto_ssh && cd /data/auto_ssh
```

以下命令二选一，方式一虽然便捷，但是大概率会出现网络问题无法下载失败报错

一、

```
curl -O https://cdn.jsdelivr.net/gh/lemoeo/AX6S@main/auto_ssh.sh
```

二、

使用 winscp 工具把 auto_ssh.sh 上传到/data/auto_ssh 文件夹

```
chmod +x auto_ssh.sh
uci set firewall.auto_ssh=include
uci set firewall.auto_ssh.type='script'
uci set firewall.auto_ssh.path='/data/auto_ssh/auto_ssh.sh'
uci set firewall.auto_ssh.enabled='1'
uci commit firewall
```

4、接下来还需要修改时区设置，输入：

```
uci set system.@system[0].timezone='CST-8'
uci set system.@system[0].webtimezone='CST-8'
uci set system.@system[0].timezoneindex='2.84'
uci commit
```

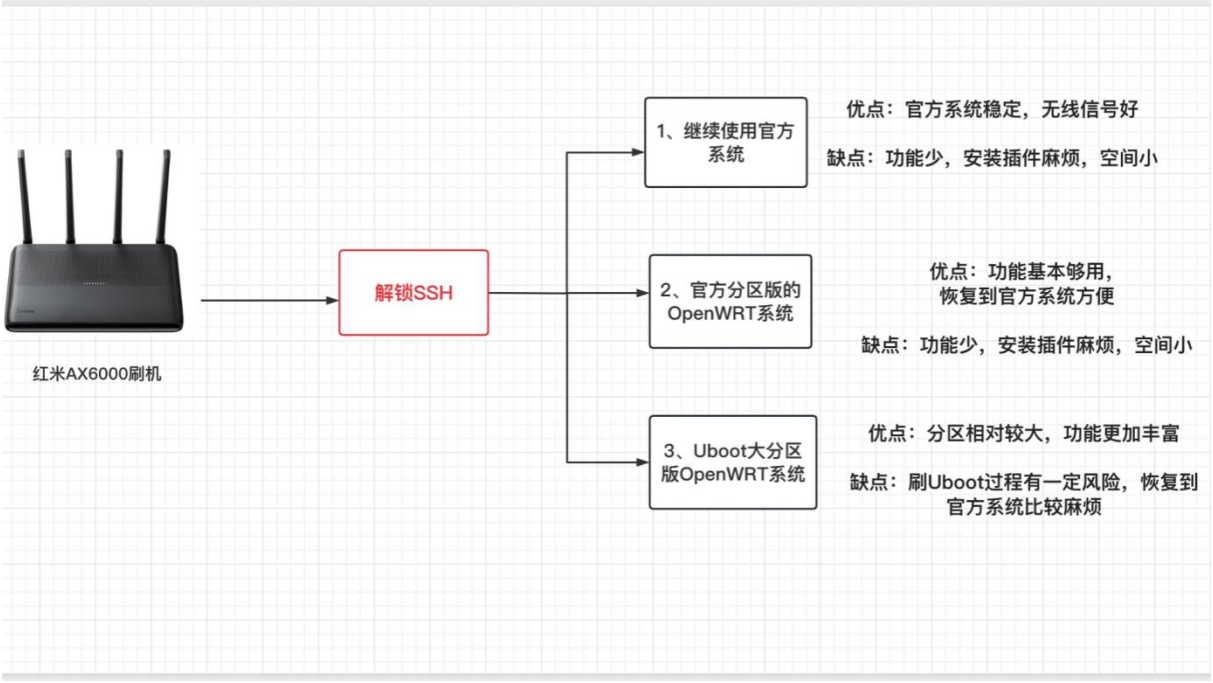
5、最后一步，关闭开发/调试模式。在提示符后输入:

```
mtd erase crash
```

6、然后输入 reboot 重启路由

```
reboot
```

成功登录 ssh 之后，我们就相当于获取了路由器的最高权限。



解锁 ssh 之后我们就有三种刷机方案选择，第一种是继续沿用目前小米路由器官方固件。我们可以通过 ssh 的命令行的方式来安装需要插件。恩山论坛里有安装各类插件的方法，大家参考教程去做就可以。

相对来说官方的固件稳定，无线信号好，而且可以享受官方的固件更新。缺点是用 ssh 的方式安装插件有点太麻烦了，而且官方的原版固件的功能太少了。完全不能发挥 MT7986A 这颗 soc 强大的性能。

所以就有了后两者刷机方案：刷一个版本的 openWRT 系统：
我们到论坛里下载红米 ax6000 的 openWRT 固件时会看到楼主一般会发布两个版本固件。一个是官方分区版，另一个是 uboot 大分区版本。这里我简单解释下两个版本的区别：
红米 AX6000 的实际 ROM 大小是 128M，不过小米官方的固件功能非常少，根本用不到这么大的空间。官方默认的固件分区大小只有 30M 左右。
所以如果不改变官方分区大小的情况下，官方分区版本的 openWRT 固件最大就只能有 30 多 M 体积。 这么点容量的固件能安装的插件就少的可怜，只能够最基本日常使用。

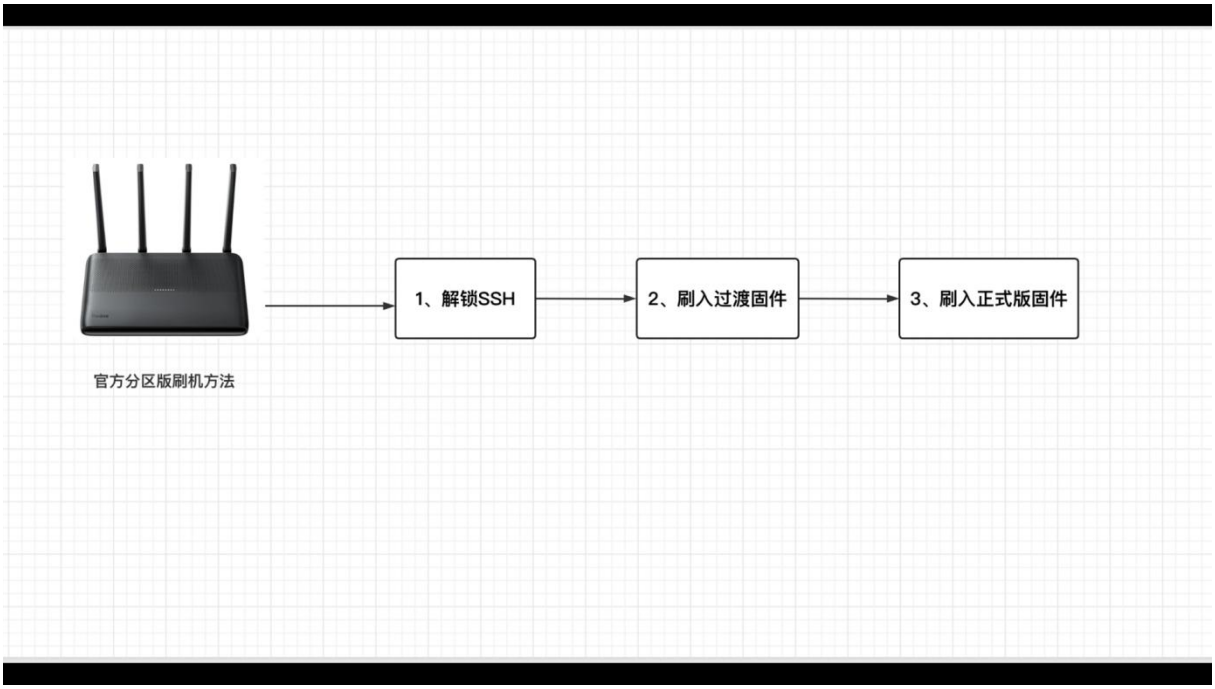
官方分区版优点是可以很方便的恢复到官方版本，一旦你觉得系统不稳定或者用不惯 op 系统，随时都可以用官方的救砖工具恢复到官方版本。

不过既然路由器实际 ROM 大小有 128M，为了更好的利用空间，就有大神开发出了大分区的 uboot 版本。这样就能安装体积更大大固件，还能预留更多的空间给用户折腾。而且刷好了 uboot 以后，刷不同版本第三方的固件就非常方便，也不用担心设备会变砖。但是刷了 uboot 版本就要官方固件说再见了，而且刷写 uboot 的的过程会存在本身一定风险，刷写过程中是不能断电的。
下面我会依次介绍两种 openwrt 固件的刷写方法，如果你只是想尝试下第三方固件，那么刷官方分区版比较合适。如果想最大程度挖掘这款路由器的性能还是推荐用大分区的

uboot 版本。虽然刷机有风险，但相信很多小伙伴和我一样买这款路由器就是为了折腾的。

3、官方分区版刷机教程

我们先来介绍下官方分区版的刷写方法，大致过程是先刷入一个过渡固件，再从过渡固件刷成 openwrt 固件。



先用 ssh 的方式登录到路由器。
一、刷入过渡固件
输入代码：

```
cat /proc/cmdline
```

查看 firmware（固件版本）=1 或者 0，如果结果是 0 就执行代码：

```
nvram set boot_wait=on
nvram set uart_en=1
nvram set flag_boot_rootfs=1
nvram set flag_last_success=1
nvram set flag_boot_success=1
nvram set flag_try_sys1_failed=0
nvram set flag_try_sys2_failed=0
nvram commit
cd /tmp
curl -L http://sebs.oss-cn-shanghai.aliyuncs.com/initramfs-factory.ubi -o initramfs-factory.ubi--此命令下载文件已经失效故改用 winscp 手动上传 initramfs-factory.ubi 到 tmp 文件夹
ubiformat /dev/mtd9 -y -f /tmp/initramfs-factory.ubi
reboot -f
```

如果结果是 1 就执行：

```
nvram set boot_wait=on
nvram set uart_en=1
nvram set flag_boot_rootfs=0
nvram set flag_last_success=0
nvram set flag_boot_success=1
nvram set flag_try_sys1_failed=0
nvram set flag_try_sys2_failed=0
nvram commit
cd /tmp
curl -L http://sebs.oss-cn-shanghai.aliyuncs.com/initramfs-factor
y.ubi -o initramfs-factory.ubi--此命令下载文件已经失效故改用 winscp 手动
上传 initramfs-factory.ubi 到 tmp 文件夹
ubiformat /dev/mtd8 -y -f /tmp/initramfs-factory.ubi
reboot -f
```

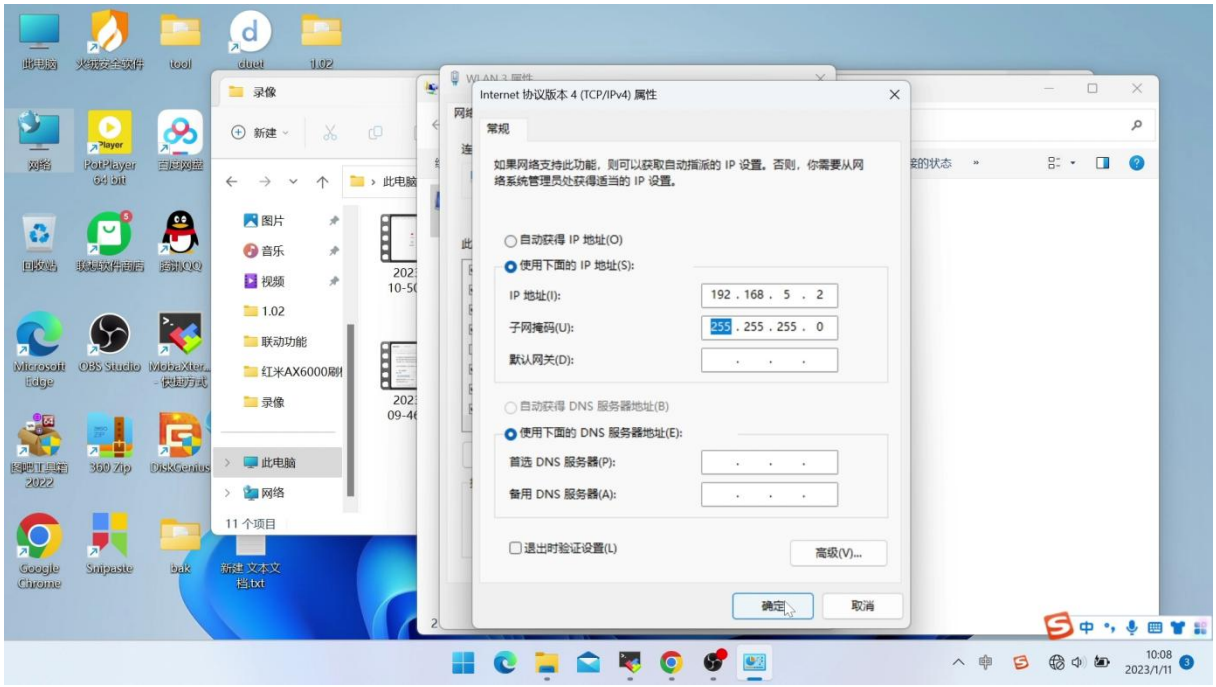
执行完毕后，路由器被自动刷入一个过渡固件。注意执行这步需要路由器可以联网。

固件无线默认名称：X-WRT_XXXX，密码：88888888

固件管理界面：http://192.168.15.1/

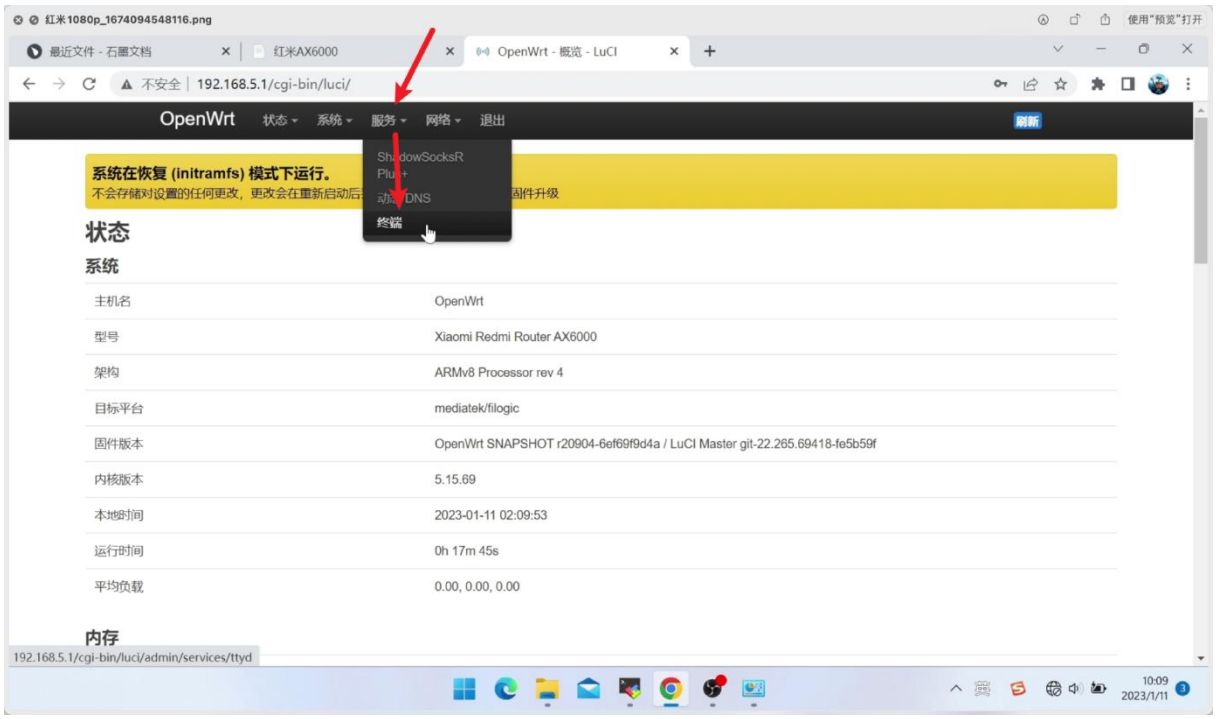
管理界面账户/密码：admin/admin

SSH 登录账户/密码：root/admin 需要**进入界面-系统-管理权页面-开启 SSH 登录**这里有一个小坑，我的过渡固件刷好以后。连接到路由器并没有自动分配 IP 地址，我手动设置电脑的 IP 为：192.168.15.2 就可以成功连上。



进入过渡系统之后，我们需要打开**服务里的终端选项，然后用 root 登录，密码是：**

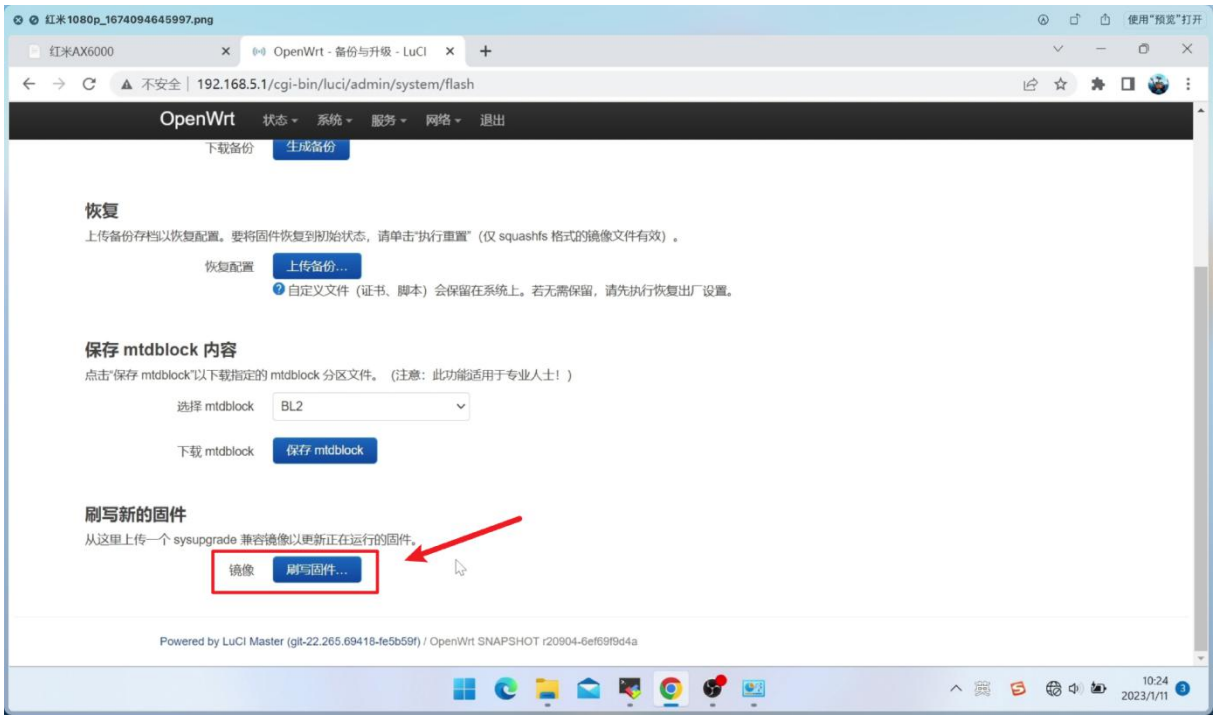
admin



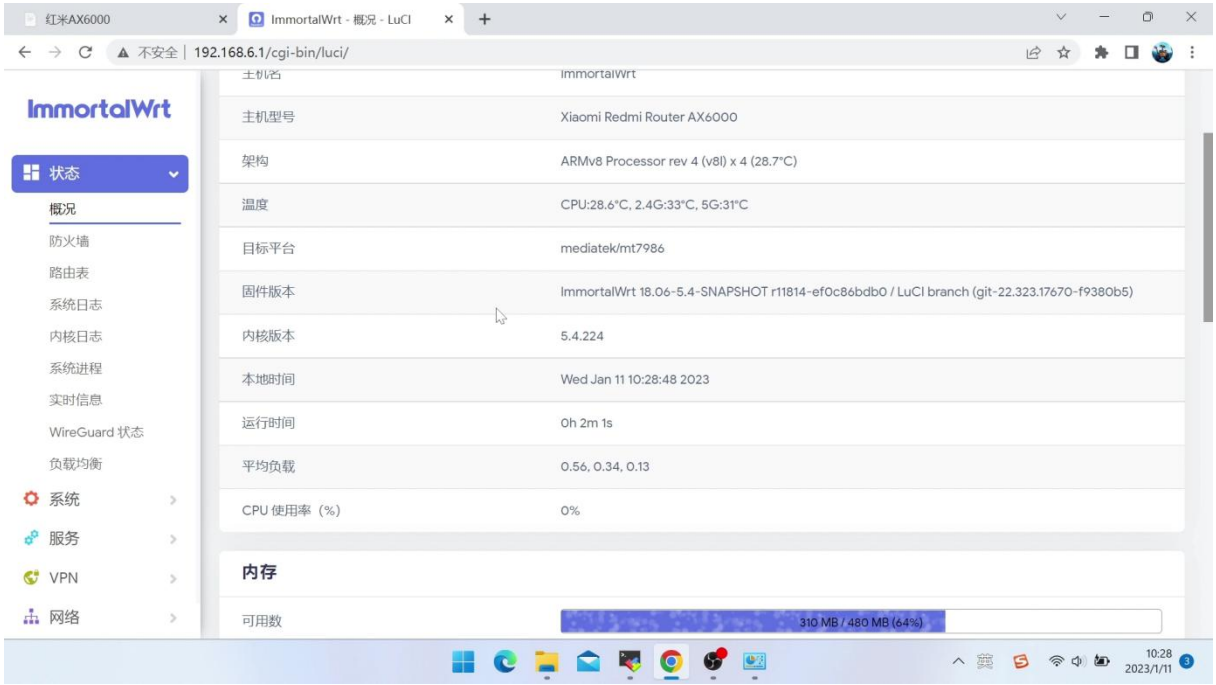
再终端里粘贴运行以下代码：

```
fw_setenv boot_wait on
fw_setenv uart_en 1
fw_setenv flag_boot_rootfs 0
fw_setenv flag_last_success 1
fw_setenv flag_boot_success 1
fw_setenv flag_try_sys1_failed 8
fw_setenv flag_try_sys2_failed 8
```

接下来我们可以选择一个官方分区版 openwrt 固件刷入。我这里推荐 237 大神制作的闭源固件。当然用别的版本固件也是可以的，不过一定要下载带官方分区版的字样的固件。



打开系统 > 备份 > 升级，选择最后一项：刷写新的固件。然后选择准备好固件点击上传。
上传完之后记得取消"保留当前配置"再点击继续。



等待刷写完毕并自动重启后，就进入正式版的 openWRT 系统了。

正式版的 openWRT 系统后台地址是 192.168.6.1 用户名和密码依然

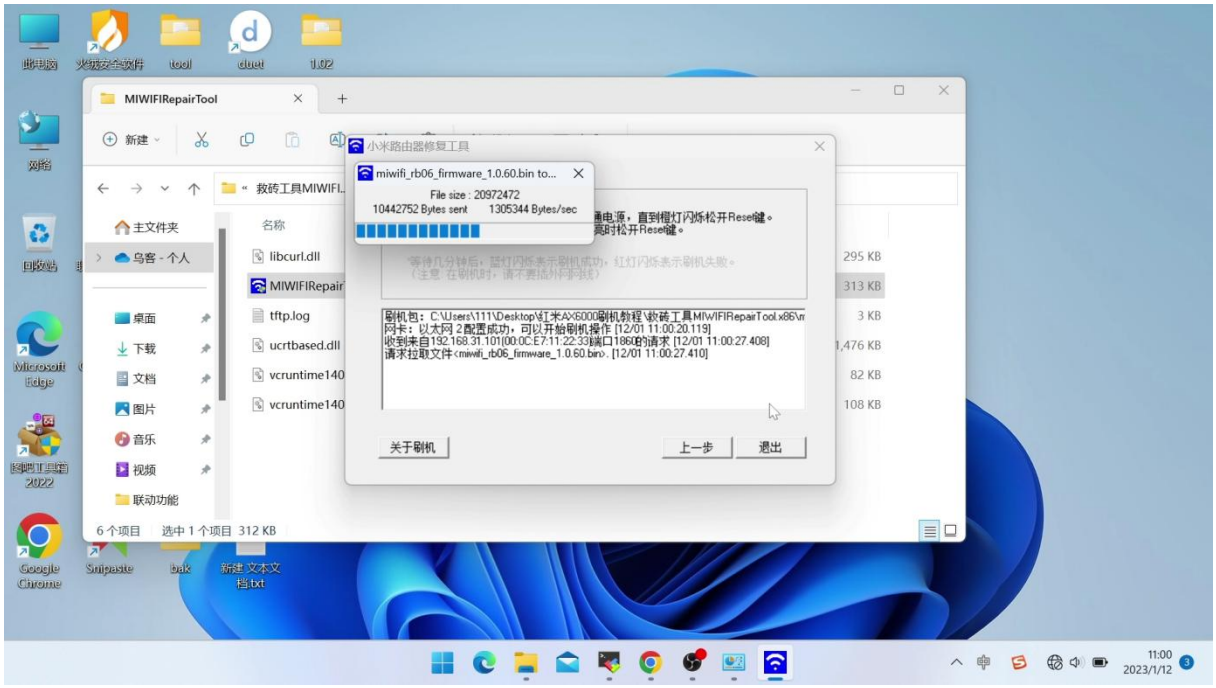
是 root 和 password，默认的网口 1 是 wan 口，剩下的都是 lan 口。

至此我们已经成功红米 AX6000 上刷入了官方分区 openwrt 系统。237 大神已经为固件做了比较完善的闭源驱动。无论是系统的稳定性还是无线信号的强度都已经非常接近官方系统了。
接下来我们再演示下如何从 openwrt 系统刷回官方固件

前面说了官方分区版的优点是可以非常方便的刷回小米官方的系统。如果你不想用 openwrt 系统，或者在刷机过程中出现任何问题。
我们都可以用小米的救砖工具加官方固件就可以恢复到最初的路由器系统，固件可选择文件夹中 降级固件 1.0.60;或者从官方下载最新固件
巨坑三次提醒
Win 系统一定要关闭自带防火墙等杀毒软件
Win 系统一定要关闭自带防火墙等杀毒软件
Win 系统一定要关闭自带防火墙等杀毒软件

方法是用卡针顶住路由器 reset 恢复按钮，再插上电源。持续按住 reset 按键 8s 左右，看到指示灯闪烁。

这时我们可以用电脑的有线网口连接路由器的 234 口。打开官方救砖工具。



并上传一个小米官方固件。上传成功后等待几分钟，看路由器的蓝灯闪烁。就可以手动断电重启路由，这时路由器就恢复到官方系统了。

救砖后恢复 ssh 权限
刷回官方系统后，我们还是可以通过 telnet 来恢复 SSH 权限。
不过此时的 telnet 密码会被重置，我们需要通过这个网页里分享文件中 route.html 输入路由器的 SN 来计算出登录的初始密码。

成功登录到 telnet 之后，执行一下命令：

```
sed -i 's/channel=.*/channel="debug"/g' /etc/init.d/dropbear
/etc/init.d/dropbear restart
echo -e 'admin\nadmin' | passwd root
```

这样我们就能重新登录到 ssh 了，ssh 的登录账号和密码分别为 root 和 admin。

登录之后可以再执行以下命令：

```
mkdir /data/auto_ssh && cd /data/auto_ssh
curl -O https://cdn.jsdelivr.net/gh/lemoeo/AX6S@main/auto_ssh.sh
chmod +x auto_ssh.sh 参照之前的做法
uci set firewall.auto_ssh=include
uci set firewall.auto_ssh.type='script'
uci set firewall.auto_ssh.path='/data/auto_ssh/auto_ssh.sh'
uci set firewall.auto_ssh.enabled='1'
uci commit firewall
```

到这里我们就完成了循环，接下来我们就介绍如何刷写 uboot 大分区版本。

4、uboot 大分区版本

好了接下来我们来介绍 uboot 大分区版的刷写方法：
需要准备的工具有，H 大神编译的红米 AX6000 的 uboot 文件，uboot 大分区版的 openwrt 固件，还有上传下载文件的工具 winscp。
我们需要先刷入 uboot，再通过启动 uboot 来刷入 openwrt 系统。
值得一提的恩山论坛里的大分区版 uboot 与 openwrt 社区提供 ubootmod 又所不同。我这里是参考了恩山论坛的的教程，大家在刷入固件时要加以区分。

我们先介绍两条命令 分别可以查看路由器分区和分区大小：
查看路由器分区

```
cat /proc/mtd
```

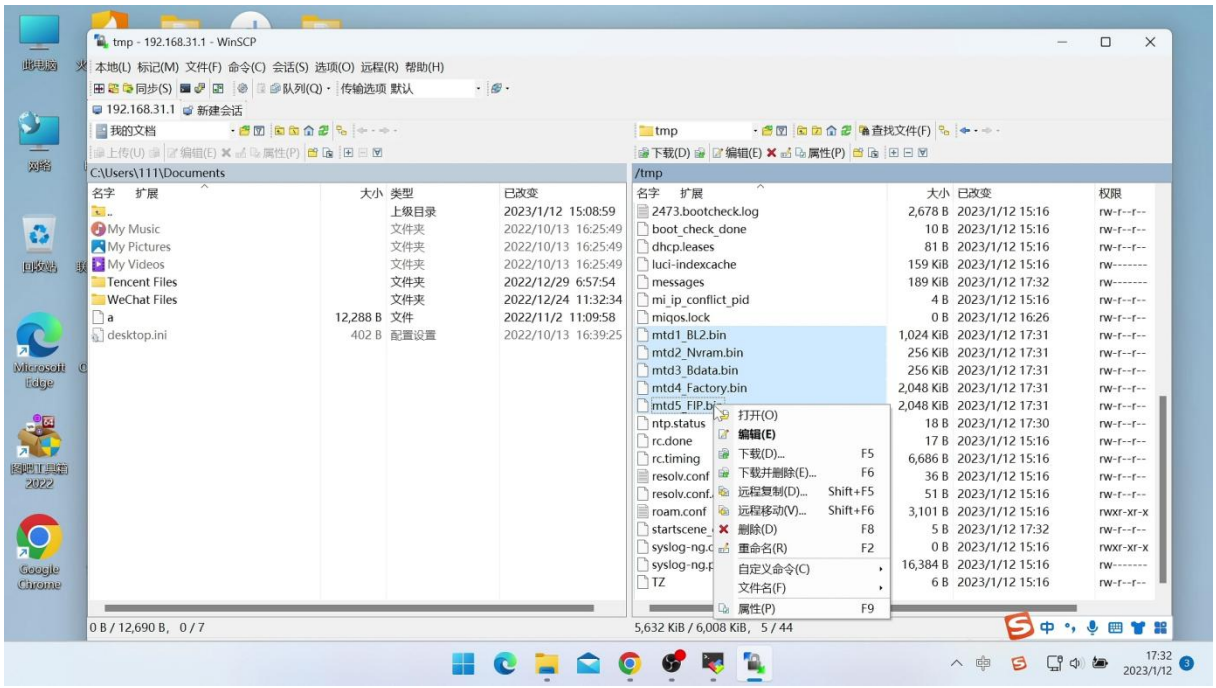
查看路由器分区的大小

```
cat /proc/partitions
```

刷机之前我们可以用命令行备份几个原厂的分区，这样以后还可以通过备份恢复到官方固件。
我们登录到 ssh，复制并运行以下命令，分区备份就会被复制 tmp 文件夹下：

```
dd if=/dev/mtd1 of=/tmp/mtd1_BL2.bin
dd if=/dev/mtd2 of=/tmp/mtd2_Nvram.bin
dd if=/dev/mtd3 of=/tmp/mtd3_Bdata.bin
dd if=/dev/mtd4 of=/tmp/mtd4_Factory.bin
dd if=/dev/mtd5 of=/tmp/mtd5_FIP.bin
```

然后用软件 winscp 登录到路由器，打开 tmp 文件夹，下载这些备份文件到电脑做保存。
winscp 的登录 ip 账号和密码都与 ssh 登录内容相同。
登录到 tmp 文件夹后，先把刚刚复制出来的五个分区备份下载到电脑。



上传完毕后关闭 winscp，再次用 ssh 登录。

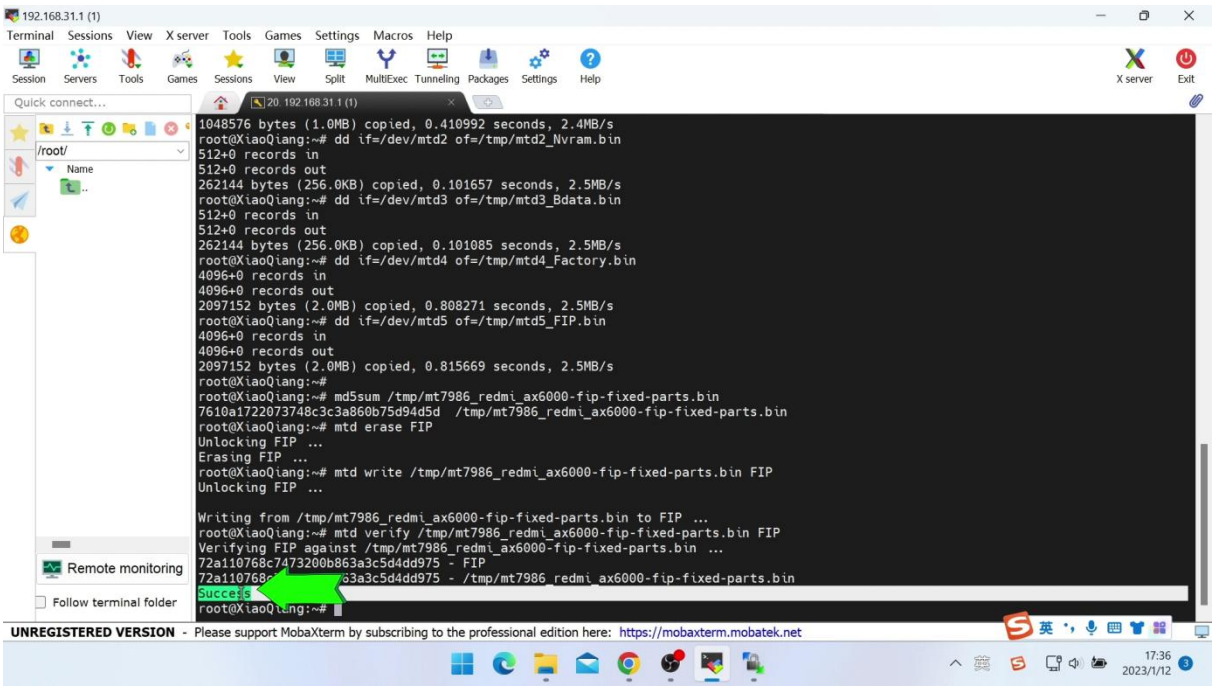
备份好分区以后顺便把 uboot 文件上传到 tmp 文件夹下 (注意这里上传的是 uboot 文件，而不是 openwrt 系统固件，它的大小只有 775k) 、然后逐条输入以下命令，把 uboot 刷入到 FIP 分区：

```
md5sum /tmp/mt7986_redmi_ax6000-fip-fixed-parts.bin
mtd erase FIP
mtd write /tmp/mt7986_redmi_ax6000-fip-fixed-parts.bin FIP
mtd verify /tmp/mt7986_redmi_ax6000-fip-fixed-parts.bin FIP
```

注意：擦除和写入 FIP 分区时不能断电、重启，不然路由器就会直接变砖。只能用 tll 或者编程器救砖。会非常麻烦。

刷入.bin 文件时为了确保万无一失，最好先验证下文件的 md5 值与作者发布的一致。

md5 值：7610a1722073748c3c3a860b75d94d5d



当我们看到输出 success 字样就说明 uboot 已经刷入成功了。
进入 uboot 的方法按住路由器的 reset 键再通电。一直按住状态等待 15 秒以后再松开。注意 uboot 目前还不能支持指示灯所以只能在心里默数 15 秒。

手动电脑的 IP 地址设置为 192.168.31.2，然后我们在浏览器里输入 192.168.31.1，就能见到 uboot 的 ui 界面了。

以后我们就可以直接在 uboot 界面里上传和安装固件就可以了。提示刷机成功之后我们只需要耐心等待两分钟，等到固件初始化完成就能进到 openWRT 系统界面。
即使上传的固件不对或者刷机失败，也不要紧。我们只需要按照同样的步骤再次进入 uboot 界面重新上传固件就可以了，刷过了 uboot 以后的路由器是刷不死的。

这里我刷的是 237 大神发布的 uboot 大分区版 openwrt 固件，后台管理地址

192.168.6.1 用户名和密码是 root 和 password，默认的网口 1 是 wan 口，

剩下的都是 lan 口。

链接：https://pan.baidu.com/s/1qO5TmyrMdmXxvHqSoXAM7Q?pwd=6666
提取码：6666
--来自百度网盘超级会员 V6 的分享本文参考的资料：
解锁 ssh 教程：https://www.right.com.cn/FORUM/thread-8253125-1-1.html
官方分区版的刷机教程：https://www.right.com.cn/forum/thread-8255378-1-1.html
uboot 大分区版刷机教程及救砖方法：
https://www.right.com.cn/forum/thread-8265832-1-1.html
237 大神的 op 固件：https://www.right.com.cn/forum/thread-8261104-1-1.html
另一个 uboot 教程以及 H 大的 uboot：
https://www.right.com.cn/forum/thread-6352752-1-1.html
另一个大佬编译的 op 固件：https://www.right.com.cn/forum/thread-8255594-1-1.html

网友整理的红米 ax6000 教程合集：
https://www.right.com.cn/forum/thread-8270115-1-1.html