红米 ax3000 CR880X 系列免拆机刷机教程

1、永久固化 ssh 密码

想要永久固化的话，在/etc/rc.local 最后一行上面加一行

```
echo -e 'root\nroot' | passwd root
```

修改好的配置文件，我们还需要把它重新上传到路由器的原文件夹下。覆盖掉原文件。这样固化密码的步骤就完成了。

2、 刷写固件

openWRT 固件下载链接：

https://github.com/hzyitc/openwrt-redmi-ax3000/releases

我们先用 SSH 的方式登录到路由器。然后键入命令查看路由器的分区情况，

```
cat /proc/mtd
```

```
dev: size erasesize name
mtd0: 00080000 00020000 "0:SBL1"
mtd1: 00080000 00020000 "0:MIBIB"
mtd2: 00040000 00020000 "0:BOOTCONFIG"
mtd3: 00040000 00020000 "0:BOOTCONFIG1"
mtd4: 00100000 00020000 "0:QSEE"
mtd5: 00100000 00020000 "0:QSEE_1"
mtd6: 00040000 00020000 "0:DEVCFG"
mtd7: 00040000 00020000 "0:DEVCFG_1"
mtd8: 00040000 00020000 "0:CDT"
mtd9: 00040000 00020000 "0:CDT_1"
mtd10: 00080000 00020000 "0: APPSBLENV"
mtd11: 00140000 00020000 "0:APPSBL" #u-boot
mtd12: 00140000 00020000 "0:APPSBL_1"#u-boot
mtd13: 00100000 00020000 "0:ART"
mtd14: 00080000 00020000 "0:TRAINING"
mtd15: 00080000 00020000 "bdata"
mtd16: 00080000 00020000 "crash"
mtd17: 00080000 00020000 "crash_log"
mtd18: 02400000 00020000 "rootfs" #系统分区 1
mtd19: 02400000 00020000 "rootfs_1"#系统分区 2
mtd20: 01f00000 00020000 "overlay"
mtd21: 00d80000 00020000 "data"
mtd22: 00364000 0001f000 "kernel"
mtd23: 0158e000 0001f000 "ubi_rootfs"
mtd24: 01b20000 0001f000 "rootfs_data"
mtd25: 00a2c000 0001f000 "data_ignor_reset"
```

这些就是目前路由器的分区情况

这里简单的介绍一下小米路由器的分区，第 11 和 12 分区是存放 uboot 的地方，这个有点类似电脑上的 efi 分区。而 mtd18 和 mtd19 实际上就是系统分区。

然后执行这段代码查看反馈结果：

```
nvram get flag_last_success
```

如果反馈结果是 0 说明目前的系统在 mtd18。我们就需要把启动分区切换到另外一个分区。如果反馈结果是 1 的话，我们就跳过这步。

我们看到反馈结果是 0，我们去执行下面代码。

```
nvram set flag_last_success=1
nvram set flag_boot_rootfs=1
nvram commit
reboot
```

运行代码之后等待系统重启，然后 ssh 登陆。再次输入查询代码查看反馈

```
nvram get flag_last_success
```

我们看到这回的反馈结果就是 1 了

我们继续下一步

接下来把要刷机的固件上传到路由器的 tmp 文件夹下。

然后运行这段代码就可以进行刷机了

```
ubiformat /dev/mtd18 -y -f
/tmp/openwrt-ipq50xx-arm-redmi_ax3000-squashfs-nand-factory.
ubi
```

注意看这里的完整的固件文件名是：

（openwrt-ipq50xx-arm-redmi_ax3000-squashfs-nand-factory.ubi）

大家在运行之前要注意核对一下代码里的固件的文件名。要和你所刷的固件文件

名需要一致。

固件刷写完毕之后

我们再去执行这段代码，把启动分区改回 mtd18

#修改启动分区为 0(rootfs_1 为 1，原厂的 rootfs 为 0)

```
nvram set flag_last_success=0
nvram set flag_boot_rootfs=0
nvram commit
reboot
```

耐心等待机器重启完毕。然后用 192.168.1.1 的 ip 登录到 op 系统。

这个系统默认是没有密码的，也没有任何的中文包和插件。相当于是一个毛坯房。

我在这里简单演示一下，中文包的安装方法。

我们 ssh 登录后可以用这个命令进行一键换源

```
sed -i 's_downloads.openwrt.org_mirrors.aliyun.com/openwrt_' /etc/opkg/distfeeds.conf
```

换源之后，再来到 network-interfaces 里把 WAN 口设置一下。让路由器可以连接网络。我这里是直接把它挂在我的主路由下面。

做完这些之后，我们再来到 system——software 下点击一下这个 update lists（更新列表）

这样就可以把插件列表更新出来了。

然后依次搜索这三个软件包进行安装。

安装中文包

点——system/software/update list

然后搜索 base-zh-cn、opkg-zh-cn、firewall-zh-cn，安装三个软件包。

软件包更新完了以后系统就会自动显示为中文了。

因为路由器里有两个分区，刷好了 op 系统之后，我们还可以在 ssh 里输入以下命令进行启动分区的切换。用回到小米的原系统，这样就可以使用双系统了。

执行了切换分区的代码之后，我们再重启一下路由器。

然后就可以用 192.168.10.1 的 ip 地址登录另一个分区里的小米原系统了。

```
fw_setenv  flag_last_success 1
fw_setenv flag_boot_rootfs 1
reboot
```

另外如果你要想保留这个双系统，记得要小米系统中把系统里的自动更新功能关闭掉。

想要再切换回 openWRT 的分区则要用以下这段代码，注意在不同系统的切换命令会有所不同。

所以从 op 系统切换到小米原系统，和从小米系统切换回 op 系统的代码是不同的。

```
nvram set flag_last_success=0
nvram set flag_boot_rootfs=0
nvram commit
reboot
```

还有就是以上刷机方法刷坏了也不要紧，可以利用小米的救砖工具直接救回。还是挺方便的。

救砖以后再用这个解锁神器解锁一次路由器就 OK 了