**重庆科技大学校园网认证以及防多设备检测的教程文档**

本文档包含两个部分：

1. **极路由4增强版刷机教程**（注意：此路由器处理器太老，我已经更换新的路由器：新路由3，newwifi3。若已经有一台处理器新的路由器且刷好openwrt固件请跳跃至防多设备检测教程处，若需要刷机教程，可参考极路由4刷机教程，各路由器刷机流程几乎相同。）
2. **防多设备检测教程**（适用于校园网认证环境，此处以重庆科技大学校园网认证为例，认证方式为锐捷）
3. **自动认证脚本**

**一、极路由4增强版刷机教程**

**1. 获取local\_ssh程序**

* **背景说明**：由于厂商倒闭关服，我们需要自行通过算法基于uuid以及local\_token生成cloud\_token，然后才能获取local\_ssh。
* **操作**：下载获取local\_ssh的程序。

**2. 开启SSH服务**

* 获取成功后，端口22开启，此时可通过终端工具选择ssh2协议进行连接。  
  **注意**：此时需要将ssh连接变为永久，因为通过算法开启的端口号只会维持5分钟。
* 通过终端工具连接成功后，使用命令：/etc/init.d/dropbear enable
* 将SSH设置为永久。（这里我使用的终端工具是SecureCRT）
* 图片参考：  
  图片1，图片2

**3. 备份路由器固件及相关数据**

* **目标**：我们开启SSH的目的是给此路由器刷上第三方固件，因此需要先备份路由器的MAC地址以及原始固件。
* **备份MAC地址**：在终端中输入

css

复制编辑

ifconfig -a

将打印出来的所有内容全部备份在txt中（此处不贴图，较为简单）。

* **备份原始固件**：
  1. 在终端中输入命令：

bash

复制编辑

cat /proc/mtd

可看到我们需要备份的内容。

* 1. 创建备份文件夹（路径在/tmp下），具体命令如下：

bash

复制编辑

cd /tmp

mkdir firmwarebackup

cd firmwarebackup

* 1. 在此文件夹内开始备份，具体命令如下：

bash

复制编辑

dd if=/dev/mtd0 of=/tmp/firmwarebackup/u-boot.bin

dd if=/dev/mtd1 of=/tmp/firmwarebackup/debug.bin

dd if=/dev/mtd2 of=/tmp/firmwarebackup/Factory.bin

dd if=/dev/mtd3 of=/tmp/firmwarebackup/firmware.bin

dd if=/dev/mtd4 of=/tmp/firmwarebackup/kernel.bin

dd if=/dev/mtd5 of=/tmp/firmwarebackup/rootfs.bin

dd if=/dev/mtd6 of=/tmp/firmwarebackup/hw\_panic.bin

dd if=/dev/mtd7 of=/tmp/firmwarebackup/bdinfo.bin

dd if=/dev/mtd8 of=/tmp/firmwarebackup/backup.bin

dd if=/dev/mtd9 of=/tmp/firmwarebackup/overlay.bin

dd if=/dev/mtd10 of=/tmp/firmwarebackup/firmware\_backup.bin

dd if=/dev/mtd11 of=/tmp/firmwarebackup/oem.bin

dd if=/dev/mtd12 of=/tmp/firmwarebackup/opt.bin

**检查备份是否成功**：  
在Windows中打开PowerShell或者命令行，输入命令：

ruby

复制编辑

scp -r -o HostKeyAlgorithms=+ssh-rsa root@192.168.199.1:/tmp/firmwarebackup ./

**注意**：由于新版取消了ssh-rsa，而极路由4仅支持较旧的ssh-rsa主机密钥类型，我们可以采取临时启用ssh-rsa，安全的同时且仅单次命令有效。

 开启SSH的程序源于：  
<https://www.right.com.cn/FORUM/thread-8268438-1-1.html>  
图片参考：图片x4  
参考文档：  
<https://blog.csdn.net/u010102747/article/details/124639593>

**二、防多设备检测教程**

**1. 定制固件及所需软件包**

* 访问网址：<https://openwrt.ai/>  
  定制所需固件和固件内软件包，软件包参考如下：

rust

复制编辑

luci-app-autotimeset luci-app-ttyd luci-theme-argon luci-app-broadbandacc kmod-rkp-ipid iptables-mod-filter iptables-mod-ipopt iptables-mod-u32 iptables-nft kmod-ipt-ipopt iptables-mod-conntrack-extra

**2. 安装ShellClash**

* 从jsDelivrCDN源安装ShellClash，执行命令：

bash

复制编辑

export url='https://fastly.jsdelivr.net/gh/juewuy/ShellCrash@master' && sh -c "$(curl -kfsSl $url/install.sh)" && source /etc/profile &> /dev/null

* 此处结合网上大多教程填充细节，例如crash作者github。  
  crash添加#用于UA3F的Clash配置（无外部代理）  
  配置文件地址：  
  <https://cdn.jsdelivr.net/gh/SunBK201/UA3F@master/clash/ua3f-cn.yaml>

**3. 从URL安装UA3F**

* 执行命令：

bash

复制编辑

opkg update

opkg install curl libcurl luci-compat

export url='https://blog.sunbk201.site/cdn' && sh -c "$(curl -kfsSl $url/install.sh)"

service ua3f reload

* **注意**：此处安装UA3F的命令，opkg或许可能出现failed download错误，请更新openwrt源！可更换国内源：

swift

复制编辑

src/gz openwrt\_core https://mirrors.tuna.tsinghua.edu.cn/openwrt/releases/22.03.4/targets/x86/64/packages

src/gz openwrt\_base https://mirrors.tuna.tsinghua.edu.cn/openwrt/releases/22.03.4/packages/x86\_64/base

src/gz openwrt\_luci https://mirrors.tuna.tsinghua.edu.cn/openwrt/releases/22.03.4/packages/x86\_64/luci

src/gz openwrt\_packages https://mirrors.tuna.tsinghua.edu.cn/openwrt/releases/22.03.4/packages/x86\_64/packages

src/gz openwrt\_routing https://mirrors.tuna.tsinghua.edu.cn/openwrt/releases/22.03.4/packages/x86\_64/routing

src/gz openwrt\_telephony https://mirrors.tuna.tsinghua.edu.cn/openwrt/releases/22.03.4/packages/x86\_64/telephony

具体命令可参考如下：

bash

复制编辑

vi /etc/opkg/distfeeds.conf

**4. 配置启动项**

* 添加到启动项的本地启动脚本如下：

nginx

复制编辑

# 启动 UA3F

uci set ua3f.enabled.enabled=1

uci commit ua3f

service ua3f enable

service ua3f start

# 防火墙规则：

iptables -t nat -A PREROUTING -p udp --dport 53 -j REDIRECT --to-ports 53

iptables -t nat -A PREROUTING -p tcp --dport 53 -j REDIRECT --to-ports 53

# 防 IPID 检测

iptables -t mangle -N IPID\_MOD

iptables -t mangle -A FORWARD -j IPID\_MOD

iptables -t mangle -A OUTPUT -j IPID\_MOD

iptables -t mangle -A IPID\_MOD -d 0.0.0.0/8 -j RETURN

iptables -t mangle -A IPID\_MOD -d 127.0.0.0/8 -j RETURN

# 由于本校局域网是 A 类网，所以我将这一条注释掉了，具体要不要注释结合你所在的校园网内网类型

iptables -t mangle -A IPID\_MOD -d 10.0.0.0/8 -j RETURN

#iptables -t mangle -A IPID\_MOD -d 172.16.0.0/12 -j RETURN

iptables -t mangle -A IPID\_MOD -d 192.168.0.0/16 -j RETURN

iptables -t mangle -A IPID\_MOD -d 255.0.0.0/8 -j RETURN

iptables -t mangle -A IPID\_MOD -j MARK --set-xmark 0x10/0x10

# 防时钟偏移检测

iptables -t nat -N ntp\_force\_local

iptables -t nat -I PREROUTING -p udp --dport 123 -j ntp\_force\_local

iptables -t nat -A ntp\_force\_local -d 0.0.0.0/8 -j RETURN

iptables -t nat -A ntp\_force\_local -d 127.0.0.0/8 -j RETURN

iptables -t nat -A ntp\_force\_local -d 192.168.0.0/16 -j RETURN

iptables -t nat -A ntp\_force\_local -s 192.168.0.0/16 -j DNAT --to-destination 192.168.1.1

# 通过 iptables 修改 TTL 值

iptables -t mangle -A POSTROUTING -j TTL --ttl-set 64

# iptables 拒绝 AC 进行 Flash 检测

iptables -I FORWARD -p tcp --sport 80 --tcp-flags ACK ACK -m string --algobm --string " src=\"http://1.1.1." -j DROP

**5. 修改添加OpenWrt的NTP时间服务器**

* **NTP服务器**（作为NTP服务器提供服务）：

css

复制编辑

ntp.aliyun.com

time1.cloud.tencent.com

time.ustc.edu.cn

cn.pool.ntp.org

**6. 注意事项及问题解决**

* 启动crash服务时可能会出现一堆报错，此时可将防火墙应用改成iptables。  
  相关网址参考：<https://github.com/SunBK201/UA3F/issues/7>  
  （从叶小姐与github user 2107010424的对话得知，由2107010422提出此解决方法）

**三、重庆科技大学校园网自动化认证脚本部署**

**1. 环境说明**

* 大部分防多设备检测已经构建完毕，此时可根据自身校园网认证进行自动化脚本部署。
* **本人校园网认证环境**：重庆科技大学，认证方式为锐捷。  
  参考文档：[https://blog.csdn.net/u010102747/article/details/124639593](https://blog.csdn.net/u010102747/article/details/124639593" \t "_new)  
  启发于该文档，结合教程以及自身部署环境进行部署。

**2. 部署步骤**

* **步骤一**：首先下载所需文件脚本，其次记录自己的校园网认证网页的wanuserip数据。  
  假设，我的验证地址是：

arduino

复制编辑

http://1.1.1.1/eportal/index.jsp?wlanuserip=

需要将wlanuserip=及后面所有内容都复制保存。

* **步骤二**：更改脚本内容
  + 打开脚本文件中的ruijie\_template.sh，只需修改以下两项：
    - **service**：修改为运营商urlencode编码（不需要填写则需要手动注释）。
    - **queryString**：修改为刚刚复制的wlanuserip=地址。
* **步骤三**：上传脚本到路由器
  + 使用winscp软件建立与路由器之间的通信，将脚本放在/etc/ruijie目录下并给予足够的权限：755。
  + 随后启用终端软件例如SecureCRT或者openwrt内的终端，测试脚本是否有效：

bash

复制编辑

/etc/ruijie/ruijie\_template.sh 登录账号 密码

* + 若出现permission denied，则权限不够，可直接添加执行权限：

bash

复制编辑

chmod +x /etc/ruijie/ruijie\_template.sh

* **步骤四**：测试认证
  + 测试返回内容为success，则说明认证脚本成功运行。
  + 随后添加进OpenWrt启动项：

bash

复制编辑

# 联网

/etc/ruijie/ruijie\_template.sh 登录账号 密码

* + 保存并重启路由器，即可享受你的防多设备检测自动认证的网络环境！
* **3. 个人吐槽**
* 在此我要吐槽一下重庆科技大学的校园网速度，50M带宽，敷衍谁呢，当然不是说学校不好哈（害怕.jpg）