

免责声明：

1. 在根据本教程进行实际操作时，如因您操作失误导致出现的一切意外，包括但不限于路由器变砖、故障、数据丢失等情况，概不负责；
2. 该技术仅供学习交流，请勿将此技术应用于任何商业行为，所产生的法律责任由您自行承担；
3. 部分学校明令禁止使用路由器上网，相关文件请点击[广东工业大学校园网责任书](#)、[厦门大学校园网责任书](#)查看。本教程仅用于交流使用，安装路由器的行为完全是您个人意志所决定的，如您已成功安装，请在 24 小时内重置路由器至原出厂状态；
4. 请按照学校推荐的方式连接到互联网，如因个人问题受到相关校规追责，由您自行承担。

前言

本教程教您如何在[Drcom](#)下使用路由器上校园网(以广东工业大学、极路由1S HC5661A为例)

本教程适合使用[Drcom](#)进行拨号上网的用户，同时，要求您的路由器支持刷入第三方系统，如openwrt。由于是针对新手的教程，所以叙述部分可能会比较冗杂，您可自行跳到不同的章节。

本教程以极路由1S HC5661A为例，不同型号路由器所对应的教程略有不同，请您注意。

本教程非原创，在以下开发者的基础上进行改进：

[GJXS](#)、[NickHopps](#)、[陈浩南](#)

准备工作

- 一款支持刷入第三方系统([openwrt](#))的路由器
- 该路由器已联网并获得开发者(**root**)权限
- 一根网线
- 下载软件[WinSCP](#)
- 下载软件putty，32位操作系统请下载[putty32](#)，64位系统请下载[putty64](#)

步骤一：获取路由器root权限

以 极路由1S HC5661A 为例，在您购买满14天后，请先登录极路由器后台，然后依次开通、安装开发者插件

☒ 开通开发者模式：“云插件”>“路由器信息”>“高级设置”>“开通”

☒ 安装开发者插件：“云插件”>“全部插件”>“开发者模式”>“确定”

其他路由器可查看其他教程获取root权限。

步骤二：刷入不死Breed

下载Breed

[Breed](#)是一个路由器的Bootloader（Bootloader 意为引导加载器，即为用于加载操作系统的程序。它是一大类此类功能程序的统称。现在的 BIOS、UEFI、GRUB、RedBoot、U-Boot、CFE等都是 Bootloader），装它的目的是为了下一步刷入固件（ROM）。以 [极路由1S HC5661A](#) 为例，不同型号下载不同的Breed，请务必对号入座，下载[breed-mt7628-hiwifi-hc5661a.bin](#)

上传到指定目录

使用WinSCP登入你的路由器后台，其中：

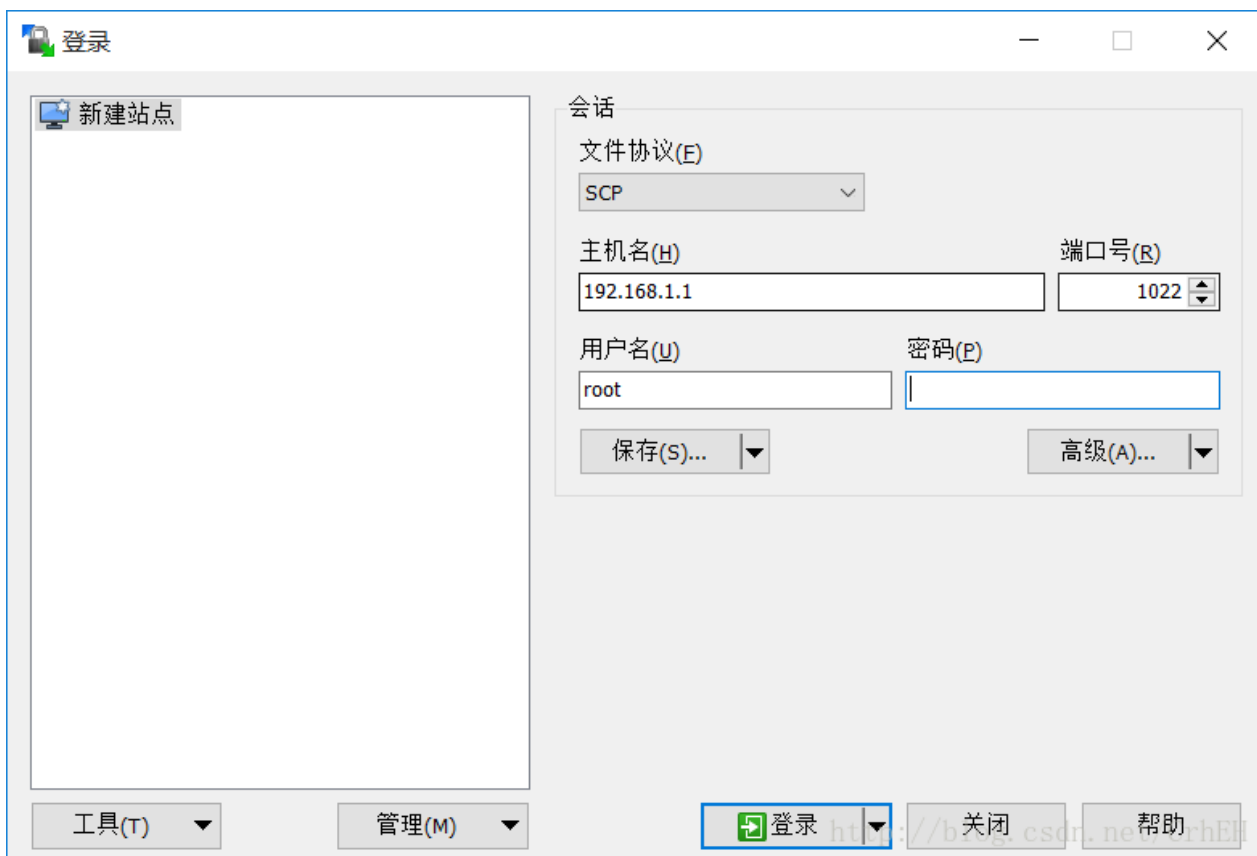
主机名：你的后台管理地址(比如192.168.1或者192.168.1.199)

账号：root

密码：你的后台管理密码

端口：1022或者22(自行测试)

模式：SCP

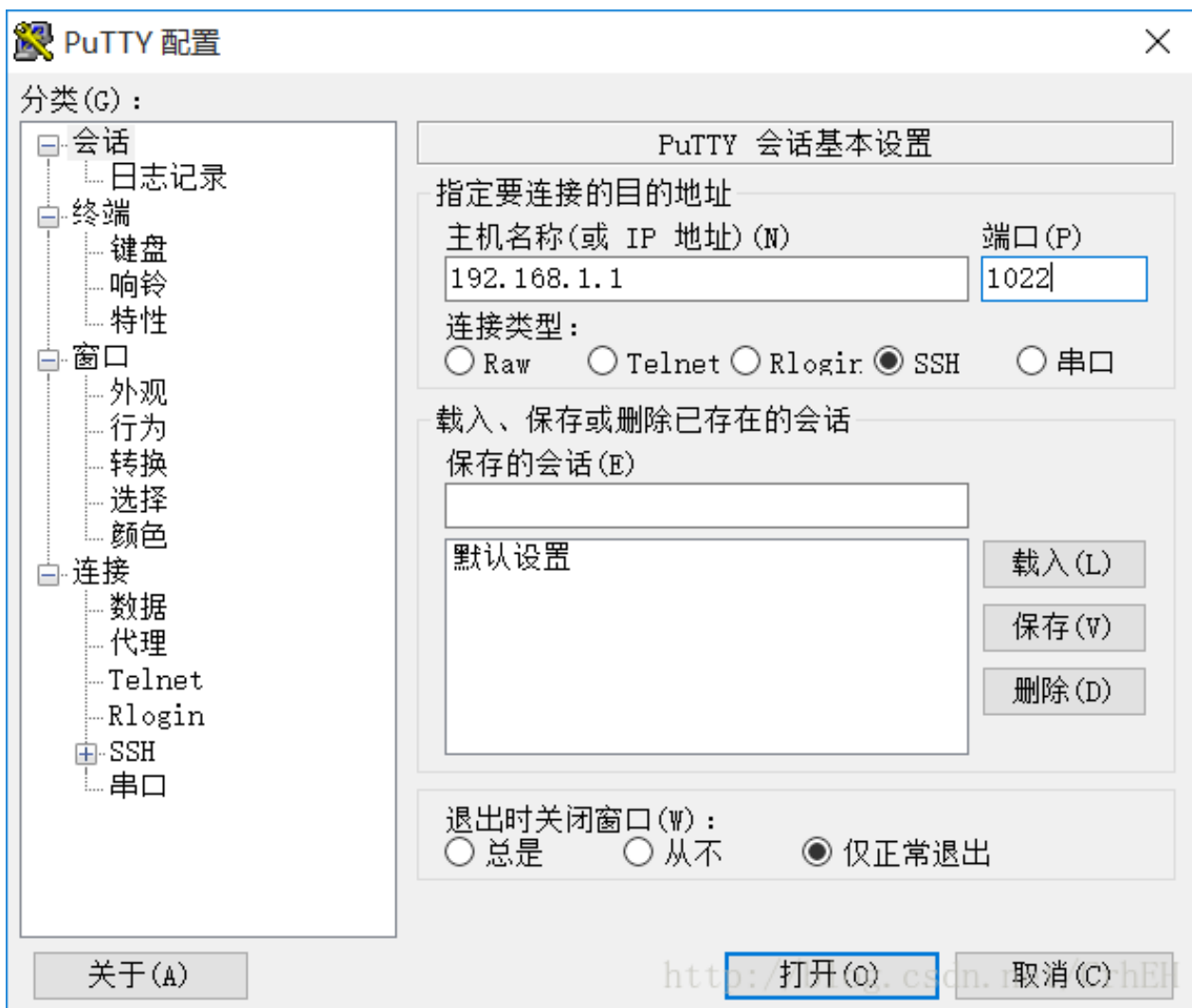


登陆成功后进入 `/tmp` 目录，将刚才下载的 [breed-mt7628-hiwifi-hc5661a.bin](#) 上传到这个目录

刷入Breed

使用 [putty64](#) 登入你的路由器后台，主机名、账号、密码、端口均与上述相同，登入成功后键入以下命令

```
mtd -r write /tmp/breed-mt7628-hiwifi-hc5661a.bin u-boot
```



显示rebooting后等待路由重启完成，不死uboot就完成了刷入了。（注意，为了确定百分百刷入成功，建议此时什么都不要动，等待5分钟后再进行其他操作）

步骤三：刷入OpenWrt 系统固件

下载对应的OpenWrt 系统固件

键入以下命令查看 路由器CPU的型号，以确定我们要刷什么版本的固件

```
cat /proc/cpuinfo
```

点击[这里OpenWrt Downloads](#)下载对应型号的OpenWrt固件，以 极路由1S HC5661A 为例,点击下载[openwrt-18.06.2-ramips-mt76x8-hc5661a-squashfs-sysupgrade.bin](#)

如下图:

Index of (root) / releases / 18.06.2 / targets / ramips / mt76x8 /

Image Files

These are the image files for the **ramips/mt76x8** target. Check that the sha256sum of the file you downloaded matches the sha256sum listed below. Shortened image file names below have the same prefix: `openwrt-18.06.2-ramips-mt76x8-...`

Image for your Device	sha256sum
LinkIt7688-squashfs-sysupgrade.bin	<code>aff3f0d25fe400f080f3cb86a96a4b6752e5049c54b450a7f68aa084</code>
alfa-network_auwusfree1-squashfs-sysupgrade.bin	<code>3c00a5fcb557d99f01f9fa75b1df7f1e0813d0968cfee761987d5f47</code>
dusun-dm06-squashfs-sysupgrade.bin	<code>dc1d13b799358d15477298b16add6fd48505ebb614c6536aea2c4d67</code>
ql-mt300n-v2-squashfs-sysupgrade.bin	<code>bc3b2bf6a142ddb985d01685bb2ca8477aff6ad3aabaafd214927df1a</code>
hc5661a-squashfs-sysupgrade.bin	<code>ba2688055af37dc32f6f445735761193ab6888d994eaacff902e2904</code>
mac1200r-v2-squashfs-sysupgrade.bin	<code>73e112f6f685db1d26c2e7b3b2e277ba5d54bf8efd00e2004f37cb4c</code>
miwifi-nano-squashfs-sysupgrade.bin	<code>1d31151c1a2c00efa5e4c0f68b22323e85fba6701f11bf43f82f2e35</code>
omega2-squashfs-sysupgrade.bin	<code>719e5161d4133c0cdb53ce12b7246794c0c82aa01586bf620602afc8</code>
omega2p-squashfs-sysupgrade.bin	<code>c810cd2306de793fd71d618a7d73080c1e54689623b30b8f2a2a2b02</code>
pbr-d1-squashfs-sysupgrade.bin	<code>d2a8bb6b5b7848dc85139c7cb744ec15aa9a26b6e97b68280c1c8cc3</code>
tama_w06-squashfs-sysupgrade.bin	<code>388a55c48d58b709a5d9c32b0cd95f925f299a2f705b992bc3a6ecb0</code>
tl-wr840n-v4-squashfs-sysupgrade.bin	<code>5ad41492eee85b0d0462d6114a8ffe7c48338c8dd3f618629949d733</code>
tl-wr840n-v4-squashfs-tftp-recovery.bin	<code>8dd1bfff77c22463928417d4b1bd67415a926ab49fbc91dcde2894e89</code>

开始刷入OpenWrt固件

本小节的步骤请严格按照先后顺序操作。

1. 用网线让路由器的LAN口与电脑的网口相连接；
2. PC设置为自动获取IP(一般默认自动获取IP)；
3. 路由器断电(就是拔插头)；
4. 首先按住reset不放！，确保没有松开reset键后，然后，插入路由器电源；
5. 保持按住reset 3-4秒左右，路由器灯开始一闪一闪的时候，松开reset；
6. PC网卡获取到192.168.1.x的地址（如未获取到手工设置），一般是192.168.1.1；
7. 浏览器访问 192.168.1.1，接着你就会看到一个uboot控制台的界面。

为了保险起见，首先进行固件备份，以备不时之需。严重强烈建议极路由用户刷Breed后，第一次进入后台就备份一次，这样以后想要重新刷回官方系统时原有功能不会受到影响，仍然能够访问云平台。

Breed Web 恢复控制台

系统信息

固件更新

固件备份

频率设置

恢复出厂设置

固件启动设置

MAC 地址修改

环境变量设置

重启

关于

单击按钮备份相应的数据

EEPROM

固件

编程器固件

极路由 Key

小米 Mini bdata

小米 Mini SN

最好三个备份

<http://www.cnblogs.com/xuliangxing>

现在正是开始刷入OpenWrt固件，依次点击固件更新→勾选固件→点击选择文件，选择我们刚刚下载的[openwrt-18.06.2-ramips-mt76x8-hc5661a-squashfs-sysupgrade.bin](#)，然后耐心等待固件刷入完成。

Breed Web 恢复控制台

系统信息

固件更新

固件备份

频率设置

恢复出厂设置

固件启动设置

MAC 地址修改

环境变量设置

重启

关于

常规固件

编程器固件

☐ Bootloader

选择文件

未选择任何文件

☒ 固件

选择文件

RT-AC54U-GPIO-1-PSG1218-64M_3.4.3.9-099.trx

☐ EEPROM

选择文件

未选择任何文件

闪存布局

公版 (0x50000)

☒ 自动重启

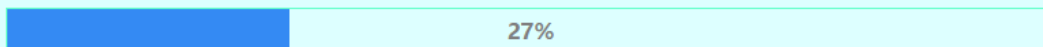
上传

<http://www.cnblogs.com/xuliangxing>

Breed Web 恢复控制台

操作正在进行

您选择的操作正在进行
正在更新固件，请耐心等待至进度条完成



警告：在操作进行过程中请不要断开电源

<http://www.cnblogs.com/xuliangxing>

安装完成后会自动重启，这时可以不断刷新浏览器，直到管理界面显示出来，如果没有显示，建议稍后使用192.168.1.1访问管理页面。

账号:root

密码:默认为admin

OpenWrt

未设置密码!

尚未设置密码。请为 root 用户设置密码以保护主机并启用 SSH。

[跳转到密码配置页...](#)

需要授权

请输入用户名和密码。

用户名

密码

登录

复位

Powered by LuCI openwrt-18.06 branch (git-18.228.31946-f64b152) / OpenWrt 18.06.1 r7258-5eb055306f

步骤四：安装Dr.com插件

这里以 广工 (广东工业大学) 校园网为例，其他学校请自行获得相应的Dr.com插件，如果您愿意折腾的话，可以[点击这里](#)自行编译合适自己的学校的Dr.com插件(需要较强的编程基础，建议还是找现成的)

以下是 广工 (广东工业大学) 校园网 各个路由器相应版本Dr.com插件下载

路由器版本	下载链接
GDUT-极路由HC5661、HC5761和HC5861	下载链接
GDUT-极路由HC5661A和HC5861B	下载链接
GDUT-极路由HC5962	下载链接
GDUT-极路由HC6361	下载链接
GDUT-斐讯K2T	下载链接
GDUT-斐讯K2P	下载链接
GDUT-斐讯K1-PSG1208、K2-PSG1218和K2G	下载链接

说明：由于路由器版本太多，若您上面没有找到对应的路由器型号，建议选择自己编译(难度很低)

将下载的 `Dr.com` 插件用 `WinSCP` 传到路由器 `/tmp` 文件夹下(WinSCP的使用方式上面已经阐述过)。

打开并登录putty，进行安装Dr.com，请键入以下命令：

```
cd /tmp
opkg install gdut-drcom_6.0-4_mipsel_24kc.ipk
```

至此，Dr.com插件安装完毕。

对于没有上述对应型号路由器的 `广工` (广东工业大学) 同学，可进行以下步骤进行编译生成自己的Dr.com插件。

1.首先 路由器CPU的型号，键入以下命令查看 `cat /proc/cpuinfo`

2.然后进入 [OpenWrt 18.06](#)，根据自己路由器的 路由器型号 进入相应的网站, 以极路由HC5661A为例, 进入 [ramips/mt76x8](#)，找到 [openwrt-sdk-18.06.0-ramips-mt76x8_gcc-7.3.0_musl.Linux-x86_64.tar.xz](#) 并下载

3.打开并登录putty，键入以下命令：


```
#解压文件夹
tar xjf openwrt-sdk-18.06.0-ramips-mt76x8-gcc-7.3.0-musl.Linux-x86_64.tar.xz
cd ~/openwrt-sdk-18.06.0-ramips-mt76x8-gcc-7.3.0-musl.Linux-x86_64.tar.xz/

#进入package下载软件包
cd package && git clone https://github.com/GJXS1980/ODP.git

#编译
cd .. && make package/ODP/compile
```

4.最后编译完的软件包在 `/bin/packages/xxxx/base/` 目录下,到这里你也有一个适合自己路由器的 drcom插件了,回到[步骤四](#)安装Dr.com客户端

步骤五：配置上网

1.点击 Network（网络）-> Interfaces（接口），点击“WAN”对应的 Edit(编辑) 按钮。

- Protocol（通信协议）：改选为 `PPPoE`，然后点击出现的 Switch Protocol（切换协议）按钮。
- PAP/CHAP username（PAP/CHAP 用户名）：学号
- PAP/CHAP password（PAP/CHAP 密码）：校园网密码

点击 Save & Apply（保存并应用）。这时，路由器本身和有线网已经可以上网了。

2.点击 Network -> Wireless（无线）。如果提示 Disabled（已禁用）就点击 Enable（启用）。可能只有一个 2.4G 的，也可能有一个 2.4G 的、一个 5G 的。点 2.4G 的 Edit(编辑) 按钮。

- ESSID：填 WiFi 的名字。

3.点击 Wireless Security（无线安全）

- Encryption（加密）：改选为 `WPA2-PSK`
- Key（密码）：填 WiFi 密码
- 点击 Save & Apply（保存并应用）

这时，WiFi 就可以正常联网啦。

4.配置dr.com客户端，这里以 `广工(广东工业大学)` 为例，进行如下配置：

- 点击 Network（网络）-> Interfaces（接口），查看LAN的MAC地址并复制

WAN6

eth0.2

运行时间: 1h 56m 38s

MAC 地址: 98

接收: 1.58 GB (1365417 数据包)

发送: 148.68 MB (1005585 数据包)

连接

关闭

修改

删除

修改Dr.com客户端的配置

OpenWrt 状态 系统 服务 网络存储 VPN 网络 带宽监控 退出

Dr.com客户端

Dr.com认证

☒

认证拨号

☒

接口名称

eth0.2

选择eth0.2

校园网帐号

3115000xxx

帐号为你端口对应的学号

密码

•••••

端口对应学号的密码

MAC拨号

9

使用eth0.2的MAC，随意修改后2位数字
格式：00:11:22:AA:BB:CC

IP

大学城校区

对应你所在校区选择

Dr.com版本

5.2.1(P版)或6.0.0(P版)

如无需更改，请保持默认

配置完成后，重启路由器，耐心等待若干分钟（15分钟内），查看是否拨号成功。

接口

<div>LAN</div> <div>br-lan</div>	<div>协议: 静态地址</div> <div>运行时间: 19h 22m 39s</div> <div>MAC: [REDACTED]</div> <div>接收: 187.20 MB (1293893 数据包)</div> <div>发送: 1.99 GB (1739190 数据包)</div> <div>IPv4: [REDACTED]</div> <div>IPv6: [REDACTED]</div>	<div>重启</div> <div>关闭</div> <div>编辑</div> <div>删除</div>
<div>WAN</div> <div>pppoe-wan</div>	<div>协议: PPPoE</div> <div>运行时间: 19h 22m 19s</div> <div>MAC: [REDACTED]</div> <div>接收: 1.97 GB (1865094 数据包)</div> <div>发送: 182.50 MB (1329471 数据包)</div> <div>IPv4: [REDACTED]</div>	<div>重启</div> <div>关闭</div> <div>编辑</div> <div>删除</div>
<div>WAN6</div> <div>eth0.2</div>	<div>协议: DHCPv6 客户端</div> <div>MAC: [REDACTED]</div> <div>接收: 1.99 GB (1972991 数据包)</div> <div>发送: 214.04 MB (1403219 数据包)</div>	<div>重启</div> <div>关闭</div> <div>编辑</div> <div>删除</div>

添加新接口...

步骤六：配置防检测

同步时间

NTP 就是用来同步两台电脑上的时钟的协议。接下来先启用 OpenWrt 自带的 NTP 服务器，然后将局域网内所有时钟校正的请求都发给路由器上的 NTP 服务器（也就是说，无视局域网内的电脑原本想要和哪台服务器同步时间，而强制将路由器上的时钟作为标准），这样局域网内所有的电脑上的时间都会变得一致。

点击 System（系统）->System（系统），只需要在管理页面中修改几个设置就可以了。

- 配置 NTP 服务。点击 System -> System。
 - 勾选 Enable NTP client（启用 NTP 客户端）和 Provide NTP server（作为 NTP 服务器提供服务）。
 - NTP server candidates（候选 NTP 服务器）四个框框分别填写

cn.pool.ntp.org、pool.ntp.org、time.apple.com。

点击 Save & Apply 按钮。

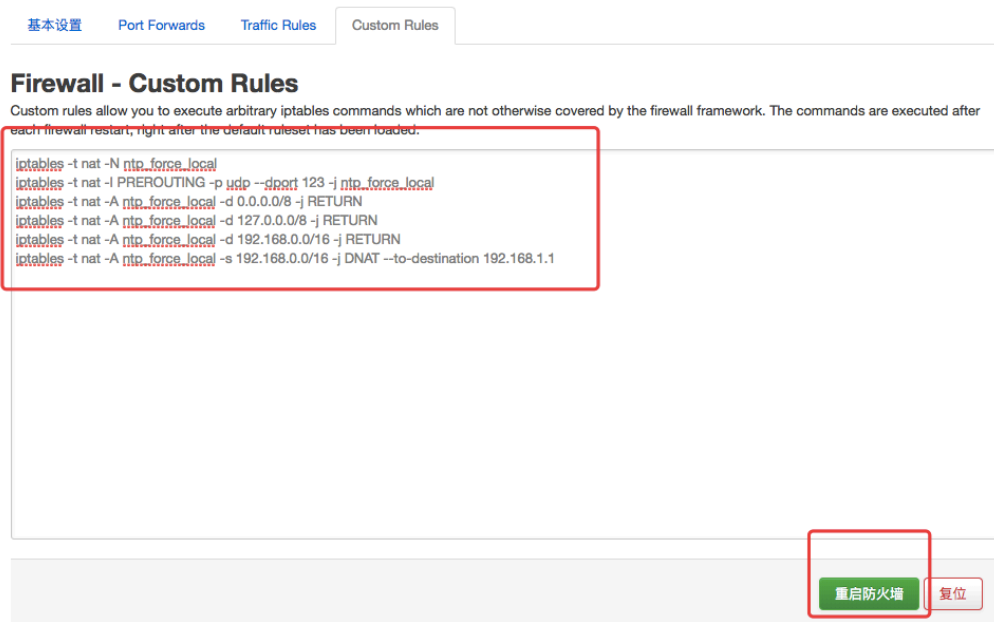
- 配置防火墙转发。点击 Network -> Firewall（防火墙），然后点击 Custom Rules 标签，在大框框里另起一行，添加下面的代码：

```
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
```

第六行最后的 192.168.1.1 需要修改为你的路由器的管理页面地址。例如，你的管理页面地址是 192.168.10.1，那么这一行代码需要修改为：

```
iptables -t nat -A ntp_force_local -s 192.168.0.0/16 -j DNAT --to-destination 192.168.10.1
```

然后点击 Restart Firewall（重启防火墙）。



修改 HTTP 头的 UA 标志

UA 中包含了操作系统版本等信息，而 HTTP 协议没有对这些信息加密，因此别人可以从这里看到这个数据包发自 Windows 电脑还是安卓手机等(所以根据这个原理，能够实现检测到超过1台设备立即强制断网的效果)。接下来把所有 HTTP 头中的 UA 都改得一样(伪装成只有一台设备，所以就不会被强制断网了)。

接下来，需要安装好 Privoxy 并正确配置，然后将所有 HTTP 流量转发给 Privoxy 代理，并在 Privoxy 中替换 UA。

- 安装 Privoxy。进入路由器管理页面，点击 System(系统) -> Software（软件包）。
 - 点击 Update lists（刷新列表）按钮，等待几分钟。如果提示好几条“Signature check passed”那么这一步执行成功；如果卡死了，几分钟后再进入这个页面，看到了很长很长的软件列表，那也是成功了。
 - 在 Filter（过滤器）中填写 `luci-app-privoxy`，点击 Find package（查找软件包）按钮。点击下方“luci-app-privoxy”对应的 Install（安装）按钮。如果提示好几条“Configuring xxxx”，那么就是执行成功了；如果卡死后再进入管理页面，看到有一个 Services（服务）菜单，菜单里有 Privoxy WEB proxy（Privoxy 网络代理），那也是成功了。

下载并安装软件包:

确认

过滤器:

luci-app-privoxy

查找软件包

状态

可用软件包 (luci-app-privoxy)

已安装软件包 (luci-app-privoxy)

软件包名称	版本	大小 (.ipk)	描述	
luci-app-privoxy	1.0.6-2	12991	LuCI Support for Privoxy WEB proxy	安装
luci-i18n-privoxy-de	1.0.6-2	5640	Translation for luci-app-privoxy - Deutsch (German)	安装
luci-i18n-privoxy-pt-br	1.0.6-2	6138	Translation for luci-app-privoxy - Português do Brasil (Brazilian Portuguese)	安装
luci-i18n-privoxy-ru	1.0.6-2	6848	Translation for luci-app-privoxy - Русский (Russian)	安装
luci-i18n-privoxy-sv	1.0.6-2	3086	Translation for luci-app-privoxy - Svenska (Swedish)	安装
luci-i18n-privoxy-zh-cn	1.0.6-2	5601	Translation for luci-app-privoxy - 中文 (Chinese)	安装

- 配置 Privoxy 设置。点击 Services -> Privoxy WEB proxy。
 - Files and Directories（文件和目录）：Action Files 删除到只剩一个框，填入 `match-all.action`。Filter files 和 Trust files 均留空。
 - Access Control（访问控制）：Listen addresses 填写 `0.0.0.0:8118`，Permit access 填写 `192.168.0.0/16`。Enable action file editor 勾选。
 - Miscellaneous（杂项）：Accept intercepted requests 勾选。
 - Logging（日志）：全部取消勾选。

点击 Save & Apply。

Privoxy WEB proxy

Privoxy is a non-caching web proxy with advanced filtering capabilities for enhancing privacy, modifying web page data and HTTP headers, controlling access, and removing ads and other obnoxious Internet junk.

For help use link at the relevant option

系统

Documentation

Files and Directories

Access Control

Forwarding

Miscellaneous

日志

Log File Viewer

Start / Stop

PID: 29280

Start/Stop Privoxy WEB Proxy

已启用

Enable/Disable autostart of Privoxy on system startup and interface events

Boot delay

10

Delay (in seconds) during system boot before Privoxy start
During delay ifup-events are not monitored !

保存并应用

保存

复位

Action Files +

The actions file(s) to use. Multiple actionsfile lines are permitted, and are in fact recommended!
match-all.action := Actions that are applied to all sites and maybe overruled later on.
default.action := Main actions file
user.action := User customizations

Filter files +

The filter files contain content modification rules that use regular expressions.

Trust file

The trust mechanism is an experimental feature for building white-lists and should be used with care.
It is NOT recommended for the casual user.

保存并应用

保存

复位

系统 Documentation Files and Directories Access Control Forwarding Miscellaneous 日志 Log File Viewer

his tab controls the security-relevant aspects of Privoxy's configuration.

Listen addresses +

The address and TCP port on which Privoxy will listen for client requests.
Syntax: IPv4:Port / [IPv6]:Port / Host:Port

Permit access +

Who can access what.
Please read Privoxy manual for details!

Deny Access +

Who can access what.
Please read Privoxy manual for details!

Buffer Limit

Maximum size (in KB) of the buffer for content filtering.
Value range 1 to 4096, no entry defaults to 4096

Toggle Status ☒

Enable/Disable filtering when Privoxy starts.
Disabled == Transparent Proxy Mode

Enable remote toggle ☐

Whether or not the web-based toggle feature may be used.

Enable remote toggle via HTTP ☐

Whether or not Privoxy recognizes special HTTP headers to change toggle state.
This option will be removed in future releases as it has been obsoleted by the more general header taggers.

Enable action file editor ☒

Whether or not the web-based actions file editor may be used.

Privoxy WEB proxy

Privoxy is a non-caching web proxy with advanced filtering capabilities for enhancing privacy, modifying web page data and HTTP headers, controlling access and removing ads and other obnoxious Internet junk.

For help use link at the relevant option

系统 Documentation Files and Directories Access Control Forwarding Miscellaneous 日志 Log File Viewer

Accept intercepted requests ☒

Whether intercepted requests should be treated as valid.

Allow CGI request crunching ☐

Whether requests to Privoxy's CGI pages can be blocked or redirected.

Split large forms ☐

Whether the CGI interface should stay compatible with broken HTTP clients.

Privoxy WEB proxy

Privoxy is a non-caching web proxy with advanced filtering capabilities for enhancing privacy, modifying web page data and HTTP headers, controlling access, and removing ads and other obnoxious Internet junk.

For help use link at the relevant option

系统 Documentation Files and Directories Access Control Forwarding Miscellaneous 日志 Log File Viewer

Single Threaded ☐

Whether to run only one server thread.
This option is only there for debugging purposes. It will drastically reduce performance.

Debug 1 ☐

Log the destination for each request Privoxy let through. See also 'Debug 1024'.

Debug 2 ☐

Show each connection status

Debug 4 ☐

Show I/O status

Debug 8 ☐

Show header parsing

- 配置防火墙转发。点击 Network -> Firewall（防火墙），然后点击 Custom Rules 标签，在大框里另起一行(注意，之前已经添加了6行代码，不要把刚刚添加的几行代码给删除了)，添加下面的代码：

```
iptables -t nat -N http_ua_drop
iptables -t nat -I PREROUTING -p tcp --dport 80 -j http_ua_drop
iptables -t nat -A http_ua_drop -m mark --mark 1/1 -j RETURN
iptables -t nat -A http_ua_drop -d 0.0.0.0/8 -j RETURN
iptables -t nat -A http_ua_drop -d 127.0.0.0/8 -j RETURN
iptables -t nat -A http_ua_drop -d 192.168.0.0/16 -j RETURN
iptables -t nat -A http_ua_drop -p tcp -j REDIRECT --to-port 8118
```

点击 Restart Firewall（重启防火墙）按钮。

Firewall - Custom Rules

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

```
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

iptables -t nat -N http_ua_drop
iptables -t nat -I PREROUTING -p tcp --dport 80 -j http_ua_drop
iptables -t nat -A http_ua_drop -m mark --mark 1/1 -j RETURN
iptables -t nat -A http_ua_drop -d 0.0.0.0/8 -j RETURN
iptables -t nat -A http_ua_drop -d 127.0.0.0/8 -j RETURN
iptables -t nat -A http_ua_drop -d 192.168.0.0/16 -j RETURN
iptables -t nat -A http_ua_drop -p tcp -j REDIRECT --to-port 8118
```

重启防火墙

复位

- 使用 Privoxy 替换 UA。打开 <http://config.privoxy.org/edit-actions-list?f=0>，如果打不开，请重启路由器多测试几遍。点击 Edit 按钮。在 Action 那一列中，hide-user-agent 改选为 Enable（绿色），在右侧 User Agent string to send 框中填写以下内容：

```
(Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.81 Safari/537.36
```

其它全部选择为 No Change（紫色）。最后点击 Submit 按钮，再次重启路由器

Actions:

Edit

```
+client-header-tagger{css-requests}
+client-header-tagger{image-requests}
+client-header-tagger{range-requests}
+hide-user-agent{Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.81 Safari/537.36}
```

URL patterns:

/ (Matches all requests)

Advanced:

Insert new section below

<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<i>hide-referrer</i>	at least in theory the If-Modified-Since header could help prevent tracking by not sending the URL of the original document.
<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<i>hide-user-agent</i>	Pretend to be using a different web browser. (May be useful for bypassing some security checks.)
				User Agent string to send: Mozilla/5.0 (Windows NT 6.3; WOW64) App
<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<i>limit-connect</i>	Limit which ports are allowed in HTTP CONNECT proxies.
<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<i>limit-cookie-lifetime</i>	Limit the cookie lifetime specified in Set-Cookie headers.
				Lifetime limit in minutes (or 0 to behave like session cookies).
				60
<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<i>overwrite-last-modified</i>	Remove or randomize the Last-Modified header.

- 验证防检测效果。

手机连接到该路由器的WIFI，使用手机(注意关闭为x屁x后再测试)在浏览器打开 <http://www.atool.org/useragent.php>，查看结果是否为Windows NT 6.3，而不是android或者iphone。

注意关闭为x屁x后再测试！注意关闭为x屁x后再测试！注意关闭为x屁x后再测试！



您的UserAgent:

Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit

您的IP地址为:

浏览器系统信息 | Browser & System

浏览器	版本	内核
Chrome 69	69.0.3497.81	WebKit 537.36
系统	CPU	设备
Windows 8.1	amd64	undefined undefined un

UserAgent分析, 访问IP地址 - aTool在线工具

1. UserAgent、浏览器、系统、IP信息集合；也可以解析自己的ua信息。

您的UserAgent :

Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.81 Safari/537.36

您的IP地址为: 中国 广东 广州 教育网



概览 显示器 储存空间 支持 服务



macOS Sierra

版本 10.12.6

MacBook Air (13-inch, Early 2015)

处理器 1.6 GHz Intel Core i5

内存 8 GB 1600 MHz DDR3

启动磁盘 Macintosh HD

图形卡 Intel

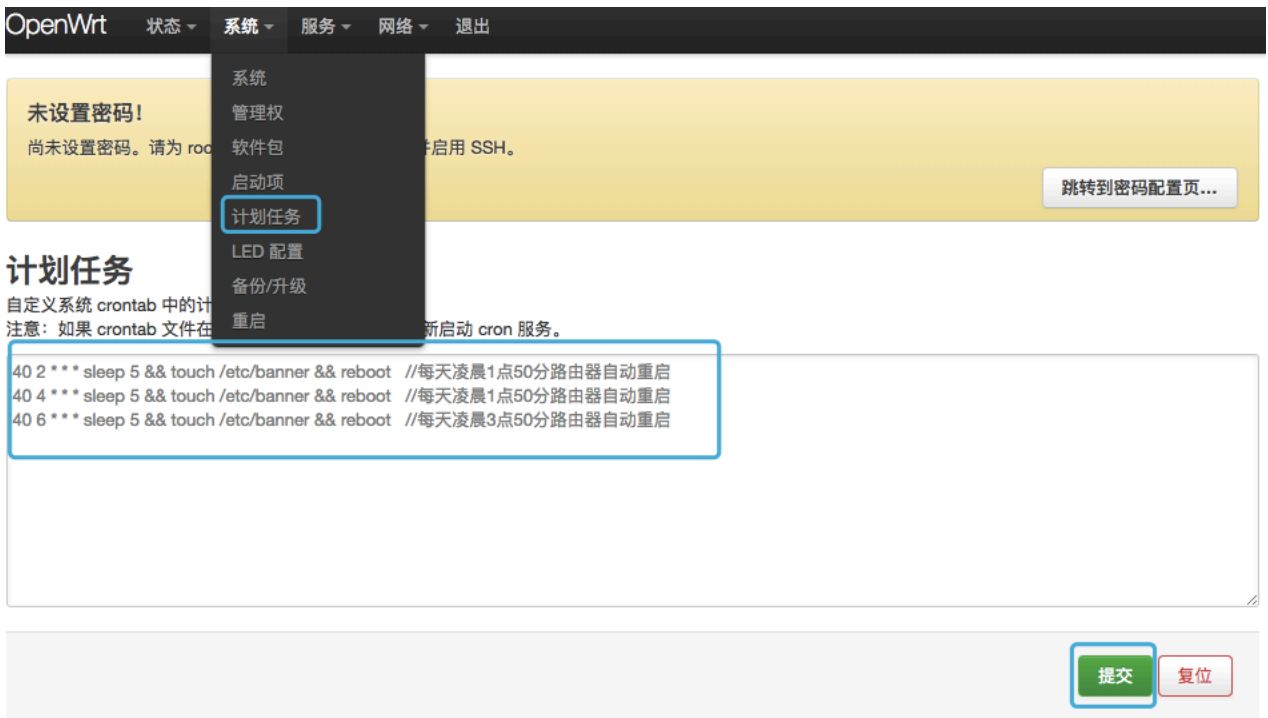


设置定时重启

由于使用了Privoxy代理，会使得所有的http流量均被转发到Privoxy，时间一旧，网络会变成异常慢。为了保证良好的网络，可以每天凌晨让路由器自动重启一遍以恢复路由器系统响应速度。

打开以下页面，键入以下代码(具体时间可自行更改)：

```
40 2 * * * sleep 5 && touch /etc/banner && reboot //每天凌晨2点40分路由器自动重启
40 4 * * * sleep 5 && touch /etc/banner && reboot //每天凌晨4点40分路由器自动重启
40 6 * * * sleep 5 && touch /etc/banner && reboot //每天凌晨6点40分路由器自动重启
```



提交后，然后打开以下页面，重启 cron 服务

OpenWrt					状态 ▾	系统 ▾	服务 ▾	网络 ▾	退出
						系统			
						管理权			
						软件包			
						启动项			
						计划任务			
						LED 配置			
						备份/升级			
						重启			
20	network	已启用	开始	重启	关闭				
35	odhcpd	已启用	开始	重启	关闭				
50	cron	已启用	开始	重启	关闭				
50	dropbear	已启用	开始	重启	关闭				
50	uhttpd	已启用	开始	重启	关闭				
80	ucitrack	已启用	开始	重启	关闭				

至此，所有步骤均已配置完毕，可以安心上网了。

补充

完整版 请点击[这里](#)打开[GitHub项目地址](#)

欢迎您[star本项目](#)

如有疑问，请发送邮件至sqzhang77@gmail.com