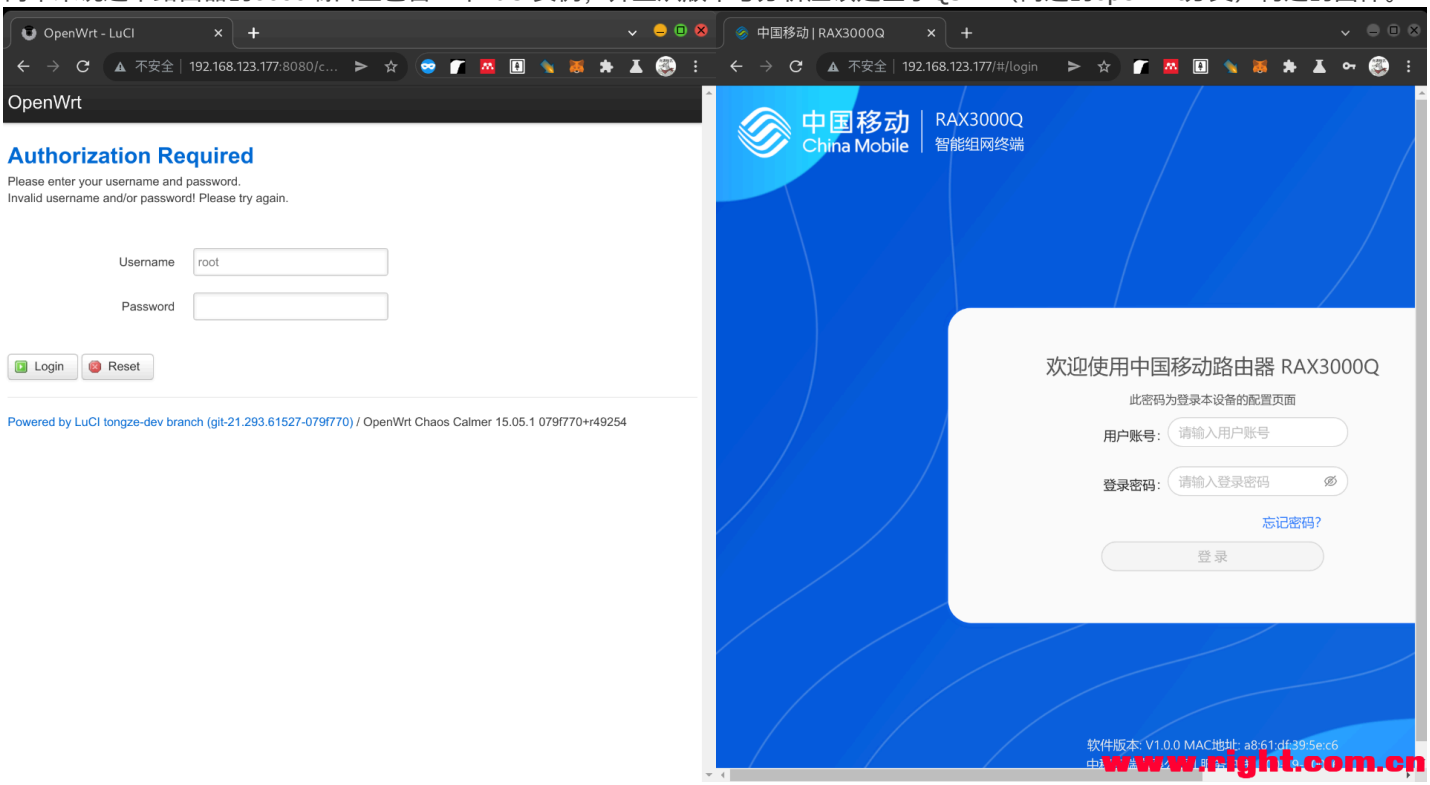
过年在家没事研究了下新买的中国移动RAX3000Q，为什么选它实际上是因为几乎同配置wifi6的H3C RC3000和RT3000太贵了，买不起。虽然自带web面板肯定不如H3C，但是人家便宜啊。淘宝150拿下后，一开始做AP用，在我的卧室里的wifi链路速率从200多M升到了576M，凑到路由器旁边则是1200M，wifi6感知还是很强的。后来折腾了一下，发现已经可以替换我的新3路由了。

在这里把折腾的经历分享给大家，我就简单说一说了，具体的细节可以看我的博客：https://blog.imlk.top/posts/rax3000q-get-shell/

文章一共两篇，这是第一篇，第二篇介绍怎么编译QSDK源码，构建自己需要的软件包ipk文件。
（图上有些ip是192.168.123.177，这是因为当时折腾的时候这台路由器还不是主路由，这都不影响，把它看作192.168.10.1即可）

简单来说这个路由器的8080端口上包含一个LuCI实例，并且从版本号分析应该是基于QSDK（高通的openwrt分支）构建的固件。



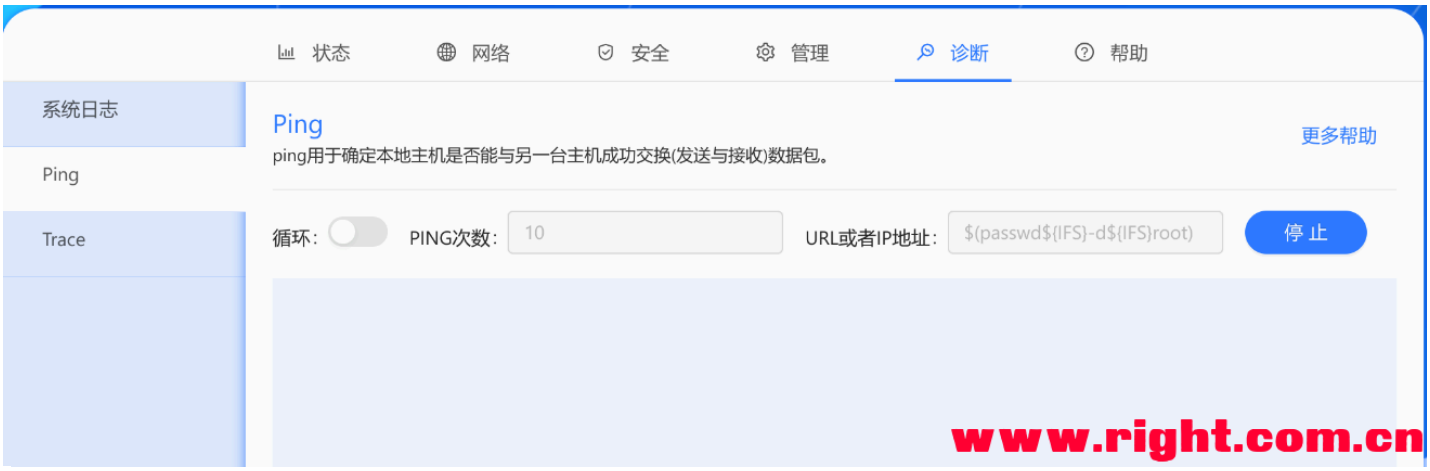
从http://192.168.10.1:8080/可以进入这个页面（其中192.168.10.1是你路由器ip）。

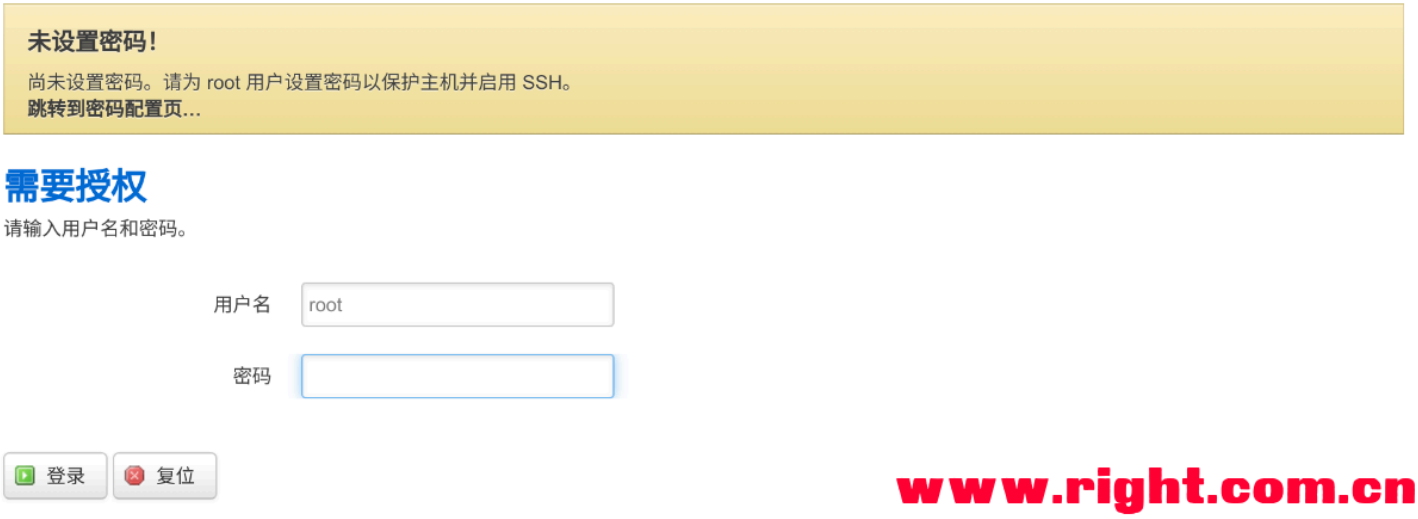
相当于这个路由器自带一个完整的QSDK固件，并且LuCI都直接暴露出来了，后面进一步分析发现opkg也是能用的（只不过得自己编译ipk文件，如果直接用openwrt仓库里的很容易遇到兼容性问题）

但是root用户的密码不知道，我们得从其他地方入手。

接下来介绍如何开启telnet/ssh，并进入这个LuCI面板

1. 登陆LuCI的方法：
首先登陆中国移动的web面板（就是默认的那个80端口的http://192.168.10.1/），在「更多 --> 诊断 --> ping」页面的ip地址输入框填入以下内容后点击「开始」按钮：
$(passwd${IFS}-d${IFS}root)
点完之后不会有结果显示，但是此时root用户的密码已经清除。可以在http://192.168.10.1:8080/处的LuCI直接以root身份无密码登陆



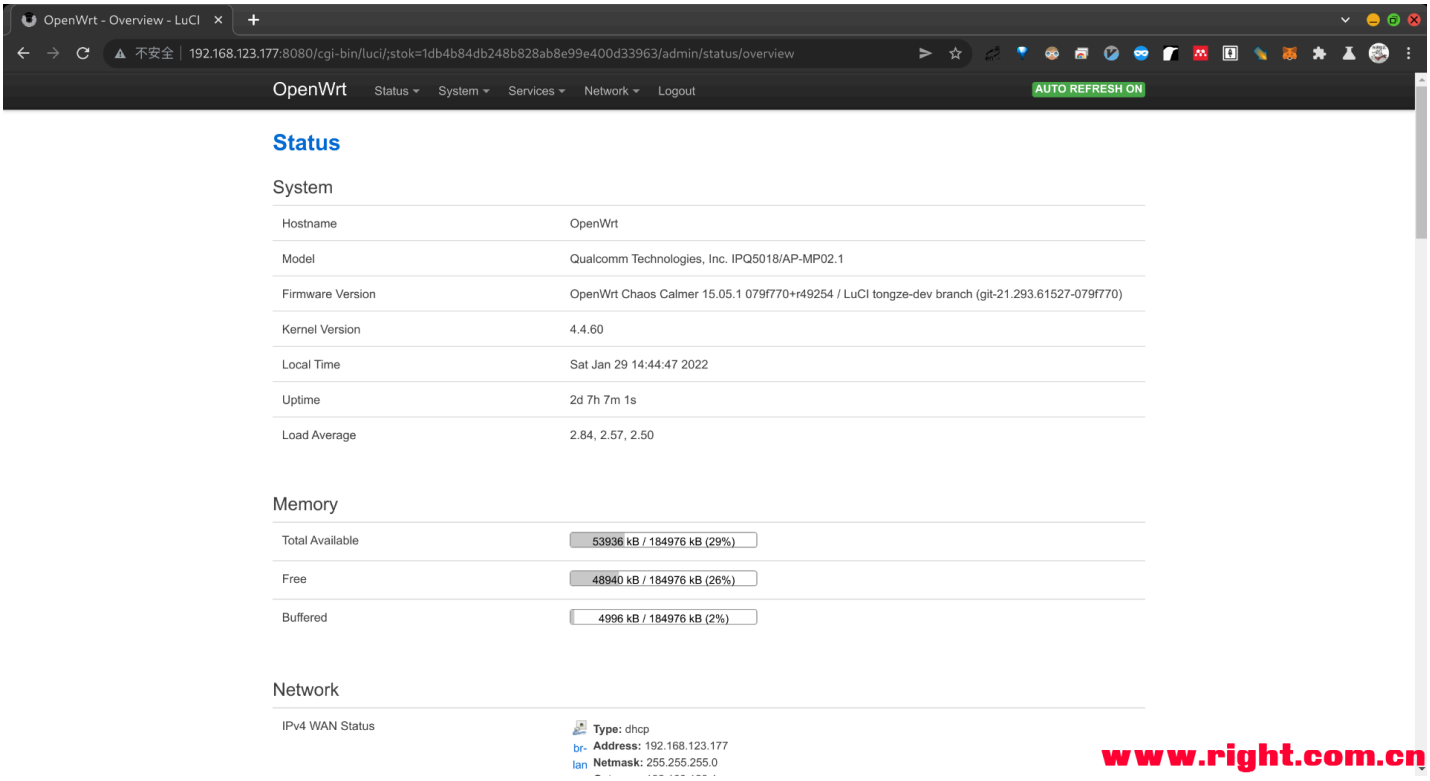


(这里第二张图只是演示，我已经进去改过了所以已经是中文了)

2.开启telnet/ssh
这个更简单，只介绍稳定telnet的开启方法，自带的ssh服务有点麻烦暂时不管自己折腾（都有luCI了，方法肯定多的去了）
这个路由器中国移动的web面板有3个账户，权限依次提高（后面两个账户密码我猜测在其他中国移动的路由器上也能用）：
user: <路由器背面的密码>
senior：123456
superadmin：83583000
所以我们回到web面板，直接以帐号superadmin，密码83583000登陆，在「管理 - 系统设置」页面可开启telnet**注意telnet端口号为4719，应使用telnet 192.168.10.1 4719登陆，用户名为root，密码已经清除**
开启ssh的按钮是坏的，不过没有关系，可以telnet登陆进去执行dropbear -p 22手动开启ssh

最后放几张图结尾


~ ssh root@192.168.123.177
root@192.168.123.177's password:
BusyBox v1.30.1 () built-in shell (ash)
For those about to rock... (Chaos Calmer, 079f770+r49254)
root@OpenWrt:~#
www.right.com.cn


OpenWrt - Overview - LuCI
192.168.123.177:8080/cgi-bin/luci/;stok=1db4b84db248b828ab8e99e400d33963/admin/status/overview
OpenWrt
Status
System
Services
Network
Logout
AUTO REFRESH ON
Status
System
Hostname OpenWrt
Model Qualcomm Technologies, Inc. IPQ5018/AP-MP02.1
Firmware Version OpenWrt Chaos Calmer 15.05.1 079f770+r49254 / LuCI tongze-dev branch (git-21.293.61527-079f770)
Kernel Version 4.4.60
Local Time Sat Jan 29 14:44:47 2022
Uptime 2d 7h 7m 1s
Load Average 2.84, 2.57, 2.50
Memory
Total Available 53936 kB / 184976 kB (29%)
Free 48940 kB / 184976 kB (26%)
Buffered 4996 kB / 184976 kB (2%)
Network
IPv4 WAN Status
Type: dhcp
Address: 192.168.123.177
Netmask: 255.255.255.0
www.right.com.cn


状态
网络
安全
管理
诊断
帮助
网页升级
修改密码
时区设置
定时重启
系统设置
网口设置
系统设置
一些设备系统上的管理和设置
更多帮助
指示灯开关
Telnet:
模块LOG开关:
ssh:
语言切换:
简体中文
锁网开关:
导出日志:
导出日志
导出配置:
导出配置
升级配置:
选择文件
上传文件
导入配置:
选择文件
导入配置
www.right.com.cn


状态
网络
安全
管理
诊断
帮助
网络设置
设备配置
2.4GWi-Fi配置
5GWi-Fi配置
5GWi-Fi配置
5GWi-Fi高级配置
Wi-Fi控制访问
WPS 设置
ANDLINK配置
静态路由
5GWi-Fi高级设置
更多帮助
发射功率:
穿墙模式
WiFi国家码:
CHINA
信道:
Auto
Wi-Fi工作模式:
11ac/ax
带宽:
160MHz
最大用户连接数:
32
接入阈值:
0
剔除阈值:
0
www.right.com.cn


状态
网络
安全
管理
诊断
帮助
网络设置
设备配置
DHCP设置
MESH
IP地址预留
TR069
和苗FOTA设置
2.4GWi-Fi配置
5GWi-Fi配置
Wi-Fi控制访问
WPS 设置
ANDLINK配置
TR069
更多帮助
TR069功能开关:
TR069状态: -----
授权类型: -----
周期通知:
周期通知间隔: 43200 秒(30 ~ 43200)
ACS URL: http://cn.tr069.cwmpd.com:8665/acs
连接请求端口号: 5400 (1025 ~ 65535)
ACS认证:
www.right.com.cn


状态
网络
安全
管理
诊断
帮助
网络设置
设备配置
2.4GWi-Fi配置
5GWi-Fi配置
5GWi-Fi配置
5GWi-Fi高级配置
Wi-Fi控制访问
WPS 设置
ANDLINK配置
静态路由
5GWi-Fi设置
更多帮助
主Wi-Fi
访客Wi-Fi
访客Wi-Fi1
访客Wi-Fi2
Wi-Fi开关:
5G优选:
Wi-Fi名称: RAX3000Q-NET
Wi-Fi广播
加密方式: WPA2-PSK
密码: ••••••••
中
确 定
取 消
www.right.com.cn

讲道理，哪怕没有登进去openwrt，直接用superadmin账户登中国移动的web面板，功能也已经很全面了，个人感觉绝对不比H3C的差

可惜就是IPQ50XX还没有官方的openwrt，所以这个里面也是QSDK，缺点就是包少了，不方便下载包。下一篇介绍如何从QSDK源码构建自己想要的软件包。