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:<u>https://blog.imlk.top/posts/rax3000q-get-</u> <u>shell/</u>

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<u>http://192.168.10.1:8080/</u>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<u>http://192.168.10.1/</u>),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<u>http://192.168.10.1:8080/</u>处的LuCI直接以root身份无密码 登陆

	屾 状态	● 网络	⊘ 安全	◎ 管理	▶ 诊断	② 帮助	
系统日志	Ping						更多帮助
Ping	ping用于确定本地	主机是否能与另一台	主机成功交换(发送与	5接收)数据包。			
Trace	循环:	PING次数: 10		URL或者	皆IP地址:(\$(passv	wd\${IFS}-d\${IFS}root)	停止
					wv	vw.right	.com.cn

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	root
密码	

登录

⑧ 登录

www.right.com.cn

(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)

Esc F1	F2 F3 F4	F5 F6 F7	F8	F9 F10	F11 F12	P/S	SL	P/B]	
·`!1@2	# 3 \$ 4 % 5 ^ 6	6&7*8(9)0_	- + =	BacSp	Ins	Hom	PUp	NL	/	*	-
Tab Q W		Y U I	0 P	{[}] \	Del	End	PDn	7	8	9	
Caps A	S D F G	н ј к		; " '	Enter				4	5	6	+
Shift Z		B N M	< . > .	?/	hift		t		1	2	3	\vdash
			Δ1+		Ctr1	F	·	_	-	 a		E
10penWrt:~# Wrt-Overview-LuCl × C (192168	+ 3.123.177:8080/cgi-bin/luci/;stok=1db	b4b84db248b828ab8e99e	400d33963/admin/	ístatus/overview	W	> *				× 0	× *	• •
20penWrt:~# Wrt-Overview-LuCl × C (▲ 不安全)192.168	+ 3.123.177:8080/cgi-bin/luci/;stok=1db OpenWrt Status - s Status	b4b84db248b828ab8e99e System + Services + ↑	400d33963/admin/ letwork - Logout	'status/overview		> * 4) a Q		× •	× *	* i
9 0penWrt:~# Wrt-Overview-LuCl × C (本 不安全)192.166	+ 8.123.177:8080/cgi-bin/luci/;stok=1db OpenWrt Status - 3 Status System	b4b84db248b828ab8e99e System + Services + ↑	400d33963/admin/ letwork ~ Logout	'status/overview		> \$	2 T S	0 REFRESI) ⊛ (HON	× :	× *	×
10penWrt:〜# Wrt-Overview-LuCl × C (▲ 不安全 192.168	+ 3.123.177:8080/cgi-bin/luci/;stok=1dtb OpenWrt Status - 3 Status System Hostname	b4b84db248b828ab8e99e System - Services - ↑ Cpr	400d33963/admin/ letwork - Logout	'status/overview		> *	ž 🔹 🎕	O REFRESI) ⊗ Г	× .		* 2
OpenWrt:~# Wrt-Overview-LuCl × C (▲ 不安全 192.168	+ 3.123.177:8080/cgi-bin/luci/;stok=1db OpenWrt Status s Status System Hostname Model	b4b84db248b828ab8e99e System + Services + ↑ Opr Qui	400d33963/admin/ letwork - Logout wWrt licomm Technologies	status/overview	-MP02.1	> ☆) :	2 ? @	o a O) ⊜ (+ON	× •	* *	• * 2
OpenWrt:~# Wrt-Overview-LuCI × C (本 不安全) 192.168	+ OpenWrt Status Status Status Status System Hostname Model Firmware Version	54584db2485828ab8e99e System × Services × M Opr Qu:	400d33963/admin/ letwork - Logout enWrt alcomm Technologies enWrt Chaos Calmer	'status/overview , Inc. IPQ5018/AF 15.05.1 079f770+	-MP02.1 149254 / LuCl tongze-	> ☆ 4	2 • &	0 REFRESI		× •	* *	* 2
20penWrt:~# Wrt-Overview-LuCI × C (A 不安全) 192.168	+ 3.123.177:8080/cgi-bin/luci/;stok=1db OpenWrt Status - S Status System Hostname Model Firmware Version Kernel Version	b4b84db248b828ab8e99e System × Services × M Opr Qui Qui 4.4	400d33963/admin/ ietwork - Logout anWrt alcomm Technologies anWrt Chaos Calmer 60	status/overview , Inc. IPQ5018/AF 15.05.1 079f770+	-MP02.1 r49254 / LuCl tongze-	> 🛧 a	2 • @ AUT	0 a 2 0 refresi	р ⊗ Г Ном	× 0	* *	*
20penWrt:~# Wrt-Overview-LuCI × C (A 不安全 192.166	+ 3.123.177.8080/cgi-bin/luci//stok=1db OpenWrt Status 3 Status System Hostname Model Firmware Version Kernel Version Local Time	b4b84db248b828ab8e99e System × Services × № Opr Qua Opr 4,4 Sat	400d33963/admin/ letwork - Logout anWrt alcomm Technologies anWrt Chaos Calmer 60 Jan 29 14:44:47 2022	/status/overview , Inc. IPQ5018/AF 15.05.1 079f770+ 2	-MP02.1 r49254 / LuCl tongze-	> ☆ ¢	-21.293.615	0 REFRESI 27-079f770	0	× •	* *	***
20penWrt:~# Wrt-Overview-LuCI × C (▲ 不安全) 192.166	+ OpenWrt Status - S Status System Hostname Model Firmware Version Kernel Version Local Time Uptime	b4b84db248b828ab8e99e System × Services × 1 Opr Qui 4.4 Sat 2d	400d33963/admin/ letwork - Logout enWrt alcomm Technologies anWrt Chaos Calmer 60 Jan 29 14:44:47 2022 7h 7m 1s	status/overview , Inc. IPQ5018/AF 15.05.1 079f770+ 2	-MP02.1 r49254 / LuCI tongze-	> ☆ 2 dev branch (git	2 • @ AUT	0 REFRES		× •	x 8	× 4
9 0penWrt:~# Wrt-Overview-LuCI × C (不安全 192.166	+ 3.123.177.8080/cgi-bin/luci//stok=1db OpenWrt Status 3 Status System Hostname Model Firmware Version Kernel Version Local Time Uptime Load Average	b4b84db248b828ab8e99e System × Services × № Opr Qua Opr 4,4 4,4 2d 2d	400d33963/admin/ letwork - Logout anWrt alcomm Technologies anWrt Chaos Calmer 60 Jan 29 14:44:47 202: 7h 7m 1s 4, 2.57, 2.50	'status/overview , Inc. IPQ5018/AF 15.05.1 079f770+ 2	-MP02.1 r49254 / LuCl tongze-	> ☆ ¢	-21.293.615	0 REFRESS		× •	•	*
9 0penWrt:~# Wrt-Overview-LuCI × C (本 不安全 192.168	+ 3.123.177:8080/cgi-bin/luci/;stok=1db OpenWrt Status 3 Status System Hostname Model Firmware Version Kernel Version Local Time Uptime Load Average Memory	54584db2485828a58e99e System × Services × M Op Qui Qui Qui Qui Qui Qui Qui Qui Qui Qui	400d33963/admin/ ietwork - Logout anWrt ilcomm Technologies anWrt Chaos Calmer 60 Jan 29 14:44:47 2022 7h 7m 1s 4, 2.57, 2.50	status/overview , Inc. IPQ5018/AF 15.05.1 079f770+ 2	-MP02.1 r49254 / LuCI tongze-	>☆	2 • @ AUT	0 REFRESI		× •	× 5	*
9 0penWrt:~# Wrt-Overview-LuCI × C (本 不安全 192.166	+ OpenWrt Status - S Status System Hostname Model Firmware Version Kernel Version Local Time Uptime Load Average Memory Total Available	b4b84db248b828ab8e99e System × Services × № Opr Qui 4.4 2d 2.8	400d33963/admin/ letwork - Logout anWrt alcomm Technologies anWrt Chaos Calmer 60 Jan 29 14:44:47 2022 7h 7m 1s 4, 2.57, 2.50	(status/overview) , Inc. IPQ5018/AF 15.05.1 079f770+ 2 (29%)	-MP02.1 r49254 / LuCl tongze-	> ☆ ∠	-21.293.615	27-079f770		× •	.	*
aOpenWrt:~# nWrt-Overview-LuCl × C (▲ 不安全 192.168	+ CopenWrt Status Status System Hostname Model Firmware Version Local Time Uptime Load Average Memory Total Available Free	b4b84db248b828ab8e99e System × Services × M Opr Qui Qui Qui Qui Qui Qui Qui Qui Qui Qui	400d33963/admin/ letwork - Logout enWrt licomm Technologies enWrt Chaos Calmer 60 Jan 29 14:44:47 2022 7h 7m 1s 1, 2.57, 2.50 53936 kB / 184976 kB	status/overview , Inc. IPQ5018/AF 15.05.1 079f770+ 2 (29%) (26%)	-MP02.1 r49254 / LuCl tongze-	> ☆ 2 dev branch (git	-21.293.615	0 REFRESI		× •	× *	* 2

Network

IPv4 WAN Status

 Type:
 dhcp

 br Address:
 192.168.123.177

 Ian
 Netmask:
 255.255.255.0

www.right.com.cn

	□ 状态 ● 网	1络 🛛 🖸	安全	◎ 管理	◎ 诊断	?	野助	
网页升级	系统设置							更多帮助
修改密码	一些设备系统上的管理和设置	8						
时区设置	指示灯	л <u>ж</u>			Telnet:			
定时重启	模块LOG开	*: (ssh:			
系统设置								
网口设置	出言功:	读: 简体中义	X V		钡网开天:			
	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

		全 🕸 管理 👂 诊断	⑦ 帮助
网络设置	5GWi-Fi高级设置		更多帮助
设备配置			
2.4GWi-Fi配置	发射功率:	穿墙模式	×
5GWi-Fi配置	WiFi国家码:	CHINA	V
5GWi-Fi配置	信道:	Auto	V
5GWi-Fi高级配置		11 /	
Wi-Fi控制访问	Wi-Fi工作模式:	1 i dL/ dX	×
WPS 设置	带宽:	160MHz	×
ANDLINK配置	最大用户连接数:	32	
静态路由	接入阈值:	0	
	剔除阈值:	0	
			w.right.com.cn

	屾 状态	● 网络	☑ 安全	◎ 管理	◎ 诊断	⑦ 帮助	
网络设置	TR069						更多帮助
设备配置							
DHCP设置		TR06	9功能开关:				
MESH IP地址预留		٢	R069状态:				
TR069			授权类型:				
和苗FOTA设置			周期通知:				
2.4GWi-Fi配置		周期	I通知间隔 : 43200)	秒(30~4	43200)	
5GWi-Fi配置			ACS URL: http://	/cn.tr069.cwmpd.co	om:8665/acs		
Wi-Fi控制访问		连接证	「 求端口号: 5400		(1025 ~ 6	65535)	
WPS 设置			ACSILIT:				
ANDLINK配置			ACSIMIL.		ww	w.righ	t.com.cn

	屾 状态	● 网络	♡ 安全	◎ 管理	▷ 诊断 ⑦ 帮助	
网络设置	5GWi-Fi设置					更多帮助
设备配置						
2.4GWi-Fi配置			主Wi-Fi	访客Wi-Fi 访客W	/i-Fi1 访客Wi-Fi2	
5GWi-Fi配置			Wi-Fi开关:			
5GWi-Fi配置			5G优选:			
5GWi-Fi高级配置			Wi-Fi名称: RAX3	000Q-NET	✓ Wi-Fi广播	
Wi-Fi控制访问			加密方式: WPA2	2-PSK		
WPS 设置			密码:		Ø Ø Ø Ø +	
ANDLINK配置				确定	取消	
静态路由						
					www.right.co	om.cn

	□□ 状态 ●●	● 网络	全 ◎ 管理	の 诊断	⑦ 帮助	
系统日志	远程抓包					更多帮助
Ping						
Trace						
远程抓包		远程抓包开关:				
抓包		绑定端口:	2002			
			确定	取消	w.riaht.	.com.cr

	□ 状态 ● 网络	
防火墙	IP、MAC、端口过滤	更多帮助
过滤规则	可对IP地址、MAC地址、端口号的黑白名单进行增加删除修改	
IP MAC绑定		
端口映射	+ 添加规则 MAC过滤 IP过滤 端口过滤	① 清空规则
URL过滤	启用 IPv4/IPv6 MAC地址 备注 过滤模式	操作
ACL过滤		
	暂无数据	
	www.right.c	om.cr

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。