

4G/5G 聚合工业路由器 USR-G810-33



说明书

联网找有人,靠谱

可信赖的智慧工业物联网伙伴



目	录
H	氺

1.	产品简	简介	. 4
	1.1.	产品特点	. 4
	1.2.	技术参数	. 5
	1.3.	状态指示灯	.6
	1.4.	产品选型	. 6
	1.5.	尺寸描述	. 7
2.	系统基	基本功能	. 7
	2.1.	Web 页面设置	.7
	2.2.	系统	. 8
		2.2.1. 主机名设置	.8
		2.2.2. 时间参数	. 9
		2.2.3. NTP 校准	.9
		2.2.4. 日志	10
	2.3.	用户名密码设置	11
	2.4.	参数备份与上传	12
	2.5.	恢复出厂设置	13
	2.6.	固件升级	13
	2.7.	重启	14
	2.8.	定时重启	15
3.	聚合朋	服务	15
	3.1.	开启并设置聚合服务	16
	3.2.	聚合规则设置(白名单)	17
		3.2.1. 规则添加	17
		3.2.2. 选择聚合服务器	18
	3.3.	聚合服务黑名单设置	19
	3.4.	状态与日志	20
		3.4.1. 状态	20
		3.4.2. 日志	20
4.	网络排	安口功能	21
	4.1.	蜂窝网设置	21
		4.1.1.4G 接口	21
		4.1.2. APN 配置	23
		4.1.3. 保活探测配置	24
		4.1.4. SIM 卡信息显示	24
	4.2.	无线配置	25
	4.3.	LAN 接口	27
		4.3.1. DHCP 功能	28
	4.4.	DHCP/DNS	29
	4.5.	WAN []	30
		4.5.1. DHCP 客户端	30
		4.5.2. 静态 IP	31

📌 क्dda www.usr.cn 🛛 联网找有人

USR-G810-33 说明书

	4.5.3. PPPoE	31
	6. 网络切换	32
	7. 主机名	33
	8. 静态路由	34
	9. 网络诊断功能	35
	.10. QoS	36
	4.10.1. 接口限速	36
	4.10.2. 分类规则	37
	.11. 负载均衡	38
5. VF	N 功能	39
	1. PPTP Client	40
	2. L2TP Client	41
	3. IPSec	43
	4. OpenVPN	44
	5. GRE	45
6. 防	火墙功能	46
	1. 基本设置	46
	2. 通信规则	47
	6.2.1. IP 地址黑名单	48
	6.2.2. IP 地址白名单	50
	3. NAT 功能	52
	6.3.1. IP 地址伪装	52
	6.3.2. SNAT	53
	6.3.3. 端口转发	56
	6.3.4. NAT DMZ	57
	4. 访问限制	58
	6.4.1. 域名黑名单	59
	6.4.2. 域名白名单	59
7. 高	及服务	60
	1. 云服务	60
	7.1.1. 监控大屏	61
	7.1.2. 设备管理	62
	7.1.3. 报警联动	66
	7.1.4. 数据中心	70
	7.1.5. 设备运维	71
	.2. 动态域名解析(DDNS)	76
	7.2.1. 已支持服务商	76
	7.2.2. 自定义的服务商	78
8. 兌	责声明	80
9. 更	新历史	80





1. 产品简介

USR-G810-33 是一款和阿里云合作推出的一款双 4G 聚合工业 CPE,采用高性能嵌入式双核 CPU,工作频率高达 880MHz, 搭载双高通 4G 模组,并具备丰富的软硬件功能:多链路聚合服务、负载均衡、2.4GHz 和 5.8GHz 双频 WiFi、千兆 LAN/WAN 口、5 种 VPN 加密传输以及免费云管理平台。它在弱网环境以及高速移动场景尤其能够凸显其不断网的优势,为您的数据传输提 供稳定可靠的网络组网解决方案。

本产品具有可靠性高、高网络稳定性、零断网等特性以及操作简单的优势,可广泛应用在商超监控、无人车、机器人、ATM 机、自动售货机、充电站等领域。

1.1. 产品特点

稳定可靠

- 全工业设计,金属外壳,防护等级 IP30;
- 支持水平桌面放置、挂壁式、导轨式安装方式;
- 宽电压 DC 9-36V 输入,具备电源反向保护;
- 工业级宽温-20℃~+70℃宽温设计、EMC 3 级防护;
- 内置硬件看门狗、故障自检测、自修复,固件备份还原功能,确保系统稳定。

组网灵活

- 提供高速率、低时延、高稳定的多链路聚合网络;
- 支持双高通 4G 全网通,支持 APN/VPDN 专网接入,可定制 eSIM;
- 支持4个千兆网口,提供高速连接能力;
- 支持 2.4G 和 5.8G 双频 wifi, 提供稳定的 wifi 网络;
- 支持 VPN (PPTP、L2TP、IPSec、OpenVPN、GRE),并支持 VPN 加密功能;
- 可定制双 5G+有线聚合版/4G+5G+有线聚合版/WIFI+蜂窝网+有线聚合版。

功能强大

- 支持多种 WAN 连接方式,包括静态 IP、DHCP、PPPoE、3G/4G;
- 支持免费云管理:可实现远程打开内置网页、掉电报警、批量可视化配置;
- 支持多路聚合功能、保持设备零断网、低延时网络传输性能;
- 支持负载均衡、QoS、DDNS、静态路由功能;
- 支持防火墙、NAT、访问控制的黑白名单;
- 支持 ssh、telnet、Web 多平台管理配置方式;
- 支持配置参数导入/导出,极大提升大批量应用下的配置效率;
- 支持 NTP、支持一键恢复出厂设置;
- 支持 LED 状态监测(PWR、WLAN、NET1、NET2),直观查看当前状态;
- 支持链路探测功能,提供防掉线机制,确保数据终端长久在线。



1.2. 技术参数

表 1 基本参数

项目		型号/规格		
	无线模块	工业级无线模块		
		LTE:B1/B3/B5/B8/B38/B39/B40/B41		
蜂窒网标准	标准频段	TD-SCDMA:B34/B39		
	1.0000000	WCDMA:B1/B8		
		CDMA/GSM:900/1800MHz		
	理论速率	LTE :150Mbps (DL) /50Mbps (UL)		
		WCDMA :42Mbps (DL) /5.76Mbps (UL)		
	无线标准	支持 IEEE802.11b/g/n/ac		
	理论带宽	2.4G:最高速度 300Mbps		
		5.8G:最高速度 867Mbps		
WIFI 标准	认证类型	WPA-PSK、WPA2-PSK、WPA3-PSK		
	安全加密	支持 TKIP、AES 加密算法		
		室外空旷/无阻拦,覆盖半径可达 200 米		
	復皿屸內	室内办公环境/障碍物,覆盖半径可达 40 米(受环境影响)		
	工作温度	-20℃~ +70℃		
	存储温度	-40°C ~ +125°C		
	工作湿度	5%~95%RH(无凝露)		
	存储湿度	1%~95%RH(无凝露)		
物理特性	供电电压	DC 9-36V		
	适配器	12V/3A		
	平均功耗	12V@260mA		
	尺寸	200.0*140.0*35.0mm(L*W*H,不含导轨挂耳、天线座以及安装件)		
	安装方式	导轨式安装、挂壁式安装、水平桌面放置		
	EMC 等级	3级		
	WAN 🗆	1个10/100/1000M 以太网口,自适应 MDI/MDIX,具备1.5KV 电磁隔离保护		
	LAN 🗆	3 个 10/100/1000M 以太网口,自适应 MDI/MDIX,具备 1.5KV 电磁隔离保护		
	SIM 卡接口	2*(3 V/1.8 V)标准自弹式 SIM 卡槽(双卡可定制内置 eSIM)		
	天线接口	蜂窝: 2 个标准 SMA 天线接口(外螺内孔)		
		WiFi: 2 个标准 SMA 天线接口(外螺内孔)		
	指示灯	PWR、WLAN、NET1、NET2		
	电源接口	直流电源:筒式 5.5*2.1mm 圆插座或者工业端子供电,具备反极性保护		
	Reload 按键	长按 5-15s 松开恢复出厂		



	TBD 接口	调试接口
	接地保护	接地螺丝

<功耗参数>

表 2 功耗表			
工作方式	供电电压	平均电流	最大电流
空载运行	DC12V	310mA	480mA
满载运行	DC12V	260mA	600mA

1.3. 状态指示灯

共有4个状态指示灯,含义如下

	表 3 指示灯说明表	
名称	状态	说明
PWR	常亮	上电状态
电源指示灯	灭	未上电状态
WLAN	常亮	WIFI 开启状态
WIFI 指示灯	灭	WIFI 关闭状态
NET1/2	灭	未插卡/联网异常
SIM1/2 指示灯	绿色	4G
	双色	3G
	红色	2G

1.4. 产品选型

USR-G810 系列选型表					
选型 功能	双 4G 聚合版	高通单 5G 版			
产品图					
蜂窝网	4G 双卡双模	5G 单卡单模			
阿里聚合	双 4G 聚合,如插入有线支持有线+双 4G 三路聚合				
负载均衡	支持				
免费云平台	支持,远程打开网页、硬件断电报警、可视化批量配置	远程管理平台			
网络灾备	双卡无缝切换,零断网	5G/有线自动切换			
网口	千兆 1WAN+3LAN	千兆 1WAN+3LAN			
WIFI	双频 WIFI5	双频 WIFI5			
eSIM	可定制				
可定制多链路方式聚合	双 5G 聚合版/4G+5G 聚合版/WIFI+蜂窝网聚合版				





1.5. 尺寸描述



图 1 尺寸图

- 钣金外壳,两侧固定孔,兼容导轨安装件;
- ▶ 长宽高分别为 200.0*139*35mm(L*W*H,不含导轨挂耳、天线座以及安装件)。

2. 系统基本功能

2.1. Web 页面设置

首次使用 USR-G810-33 设备时,可以通过 PC 连接 USR-G810-33 的 LAN 口或者连接 G810-33 WIFI, 然后用 web 管理页 面配置。SSID、IP 地址和用户名、密码如下:

表 4 USR-G810-3	33 网络默认设置表
----------------	------------

参数	默认设置
2.4G SSID	USR-G810-XXXX
5.8G SSID	USR-G810-XXXX_5G
LAN 口 IP 地址	192.168.1.1
用户名	root
密码	root
无线密码	12345678

<u><说明></u>



➢ XXXX 代表设备 MAC 后四位。

首先用 PC 的无线网卡或者以太网卡, USR-G810-33 的默认 SSID 为 USR-G810-33-xxxx, 操作 PC 加入这个无线网络。等 无线连接好后, 打开浏览器, 在地址栏输入 192.168.1.1 回车。填入用户名和密码(均为 root), 然后点击确认登录。网页会出 现 USR-G810-33 的管理页面。USR-G810-33 管理页面默认中文。

		i ∞ english
<u>.</u>		
90 01	要授权	
	n de fa Yanda IV	
请输入户	月尸名和密码。	
田白夕· root		
व्हेल्यच.		
登录	复位	

图 2 首页页面

2.2. 系统

2.2.1. 主机名设置

G810-33 路由器可自定义主机名(默认 USR-G810), 配置如下:

		自动刷新开 中文 English
	配置路由器的部分基础信息。	A
TEST		
	系统属性	
> 状态	基本设置 远程日志	本地日志 主題
肥久		
	主机名	TEST
》聚合网络	时区	Asia/Beijing
> 网络		
> VPN	本地时间	2023-05-05 18:30:58 Fri 🔲 同步浏览器时间
> 防火墙		
✓ 系统		
系统	时间同步	
管理权	启用NTP客户端	
中叶带白		
正 山 里/口	NTP服务器	
备份/升级	候选NTP服务器	ntp1.aliyun.com
重启		time1.cloud.tencent.com
> 退出		time.ustc.edu.cn
		cn.pool.ntp.org



图 3 主机名设置页面

2.2.2. 时间参数

可通过"同步浏览器时间"同步本地时间,可设置路由器默认时区。

			自动刷新开 中文 English
TEST	基本设置 远程日志	本地日志 主題	
	主机名	TEST	
> 状态			(
> 服务	DIX	Asia/ beijing	
> 聚合网络	本地时间	2023-05-05 18:31:23 Fri 🔲 同步浏览器时间	
> 网络			
> VPN			
> 防火墙	时间同步		
✓ 系统	启用NTP客户端		
系统	I NTDBR& 58		
管理权	N 1 P 80 35 8H		
定时重启	候选NTP服务器	ntp1.aliyun.com	
备份/升级		time.ustc.edu.cn	
電白		cn.pool.ntp.org	
単山			
Ц			
	图 4	时区与本地时间同步设置	

2.2.3. NTP 校准

路由器可以进行网络校时,默认启动 NTP 客户端功能。

			自动感新开 中文 English
	土が石	IESI	
TEST	时区	Asia/Beijing	v
	*****	2022 OF OF 19:21:22 Fri	
> 状态	لبا (1997-14) ال	2023-05-05 16.51.25 FIL	
> 服务			
> 聚合网络	时间同步		
> 网络			
> VPN	启用NTP客户端		
> 防火墙	NTP服务器		
✓ 系统	候选NTP服务器	ntp1.aliyun.com	×
系统	1	time1.cloud.tencent.com	m 🗵
管理权		time.ustc.edu.cn	*)
白柱市白		cn.pool.ntp.org	
<u> たい里 向 </u>			
备份/升级			
重启		र्यत	应用 保存
> 退出			
		15 NTP 页	页面





2.2.4. 日志

<远程日志>

- ▶ 远程 log 服务器:远端 UDP 服务器的 IP,当 IP 为 0.0.0.0 时不启用远程日志;
- ▶ 远程 log 服务器端口:远端 UDP 服务器端口。

тест	
тест	
TEST	1
家统	
■ 記置路由器的部分基础信息。	
→ 一 > 服务 ■ SA属性	
> 聚合网络 基本设置 远程日志 主题	
シ VPN 近程log蔵务器 0.0.0.0 () IPv4地址,使用udp传输协议,留空或为0.0.0°时为禁用	
> 防火墙 远程log服务器端口 514	
▲ 公式 2000 (20165535,留空时为款用)	
定时重启 时间间步 · · · · · · · · · · · · · · · · · ·	
备份/升级 启用NTP客户端 I	
重启 NTP服务器 □	
> 退出 模选NTP服务器 ntp1.aliyun.com 图	
time1 claud tancent com	

图 6 远程日志

<u><本地日志></u>

- ▶ 内核/应用日志等级:支持调试/信息/注意/警告/错误/致命错误/警戒/紧急,共8个等级;按顺序调试最低,紧急最高;
- ▶ 日志(内核、应用、VPN)支持即时查看、清空,支持日志文件导出。

	内核日志等级 调试 >	
> 状态	应用日志等级 调试 🗸	
> 服务		
> 聚合网络		
> 网络	May 5 18:28:01 uhttpd[3710]: uci: Entry not found May 5 18:28:01 uhttpd[3710]: uci: Entry not found	î
> VPN	May 5 18:28:01 uhttpd[3710]: uci: Entry not found May 5 18:28:01 uhttpd[3710]: Failed to find log object: Not found	
> 防火墙	May 5 18:28:01 unttpd[3/10]; wc: /proc/net/nf_conntrack: No such file or directory May 5 18:28:06 uhttpd[3/10]: uci: Entry not found May 5 19:29:06 ubttpd[3/10]: uci: Entry not found	•
✓ 系统	May 5 18:28:06 uhttpd[3710]: uci: Entry not found May 5 18:28:06 uhttpd[3710]: uci: Entry not found	
云统	May 5 18:28:06 uhttpd[3710]: Failed to find log object: Not found May 5 18:28:06 uhttpd[3710]: wc: /proc/net/nf_conntrack: No such file or directory	
20090	May 5 18:28:07 uhttpd[3710]: Failed to find log object: Not found May 5 18:28:08 uhttpd[3710]: Failed to find log object: Not found	
管理权	May 5 18:28:09 uhttpd[3710]: Failed to find log object: Not found	
定时重启	May 5 18:28:11 uhttpd[3710]: uci: Entry not found	
夕 /// 川/昭	May 5 18:28:11 uhttpd[3710]: uci: Entry not found May 5 18:28:11 uhttpd[3710]: uci: Entry not found	
田177/71-9 X	May 5 18:28:11 uhttpd[3710]: uci: Entry not found	
重启	May 5 18:28:11 uhttpd[3710]: wc: /proc/net/nf_conntrack: No such file or directory	
(日山)	May 5 18:28:16 uhttpd[3710]: uci: Entry not found May 5 18:28:16 uhttpd[3710]: uci: Entry not found	
	May 5 18:28:16 uhttpd[3710]: uci: Entry not found	

图 7 log 查看



		自动刷新开 中文 English
TEST	May 5 18:28:01 uhttpd[3710]: ucl: Entry not found May 5 18:28:01 uhttpd[3710]: ucl: Entry not found May 5 18:28:01 uhttpd[3710]: ucl: Entry not found May 5 18:28:01 uhttpd[3710]: edite to find log object: Not found	Î
 > 状态 > 服务 > 取ら四句 	May 5 18:28:01 uhttpd[3710]: wc: /proc/net/nf_contrack: No such file or directory May 5 18:28:06 uhttpd[3710]: wc: /proc/net/nf_contrack: No such file or directory May 5 18:28:06 uhttpd[3710]: uc: Entry not found May 5 18:28:06 uhttpd[3710]: uc: Entry not found May 5 18:28:06 uhttpd[3710]: uc: Entry not found May 5 18:28:06 uhttpd[3710]: uc: Chtry not found May 5 18:28:06 uhttpd[3710]: railed to find log object: Not found May 5 18:28:06 uhttpd[3710]: railed to find log object: Not found May 5 18:28:06 uhttpd[3710]: railed to find log object: Not found	
> 家百两曲 > 网络 > VPN	May 5 18:28:07 uhttpd[3710]; Rei Jposten Content Contract, No Such and Oracedory May 5 18:28:07 uhttpd[3710]; Failed to find log object: Not found May 5 18:28:09 uhttpd[3710]; Failed to find log object: Not found May 5 18:28:10 uhttpd[3710]; Failed to find log object: Not found May 5 18:28:11 uhttpd[3710]; Icailed to find log object: Not found May 5 18:28:11 uhttpd[3710]; uci: Entry not found May 5 18:28:11 uhttpd[3710]; uci: Entry not found	
 > 防火墙 > 系统 系统 	May 5 18:28:11 uhttpd[3710]: uci: Entry not found May 5 18:28:11 uhttpd[3710]: uci: Entry not found May 5 18:28:11 uhttpd[3710]: ici: Entry not found May 5 18:28:10 uhttpd[3710]: wc: /proc/net/nf_conntrack: No such file or directory May 5 18:28:16 uhttpd[3710]: uci: Entry not found May 5 18:28:16 uhttpd[3710]: uci: Entry not found May 5 18:28:16 uhttpd[3710]: uci: Entry not found May 5 18:28:16 uhttpd[3710]: uci: Entry not found	
管理权定时重启	May 5 18:28:16 uhttpd[3710]: uci: Entry not found May 5 18:28:16 uhttpd[3710]: aliel to find log object: Not found May 5 18:28:16 uhttpd[3710]: wc: /proc/net/nf_conntrack: No such file or directory May 5 18:28:17 uhttpd[3710]: Failed to find log object: Not found May 5 18:28:18 uhttpd[3710]: Failed to find log object: Not found	
· 面份/升级 重启	may 3 10:20:19 unttpa[3/10]: Falled to find log object: Not found 日志文件: 日志文件:	8
→ 退出		Ţ

图 8 log 下载

<u><说明></u>

- ▶ 先生产日志,然后下载日志。
- 2.3. 用户名密码设置

		中文 English
TEST	主机密码	
> 状态	修改访问设备的管理员密码	
> 服务	配置	
> 聚合网络	****	
> 网络	(2) 密码支持:数字、字母和非中文符号。不大于16个字符	
> VPN	确认密码	
> 防火墙		
✓ 系统		
系统管理权	应用 傑存	
定时重启		
备份/升级		
重启		
> 退出		

默认密码可以设置,默认密码为 root,用户名不可设置。本密码为管理密码(网页登录密码)。

图 9 用户名密码设置页面





2.4. 参数备份与上传

TEST 留份/开感 》 妖感 > 妖感 > 聚合网络 > 聚合网络 > 聚合网络 > 聚合网络 > 聚合网络 > 聚合网络 > 水感 ● <th></th> <th></th> <th></th>			
TEST 备份/开您 》 然感 AG// 快愿 》 感容 AG// 使愿 》 K感 ● 如金 》 KN ● 如金 》 KN ● 如金 》 KN ● 如金 》 KN ● 如金 ● 加合 ● 如金 ● 加合 ● 加合			
TEST 备份/开级 > 状态 > 形态 > 影合网络 > 影合网络 > 网络 > 网络 > VPN > 防火油 上作备份存档以应复配量。 上作备份存档以应复配量。 水路 溶解 溶解 管理权 方的力强 广告公的国作儿 上行合适的国作儿吸斯当前系统。选择 保留设置 未维持原有设置。 正常 通路			
> 状态 > 販务 > 販务 > 緊合网络 > 网络 > NPN > 防火塩 ● 方 医外/恢复当前系统配置文件。 - 下载金份: □ 生成金份 - 放船 - 反執合 - 反射 - 反由 - 成品 - 「成品	TEST	7	
氷 各份/恢复 服务 备份/恢复当前系统配置文件。 原合网络 予数备份: ■ 生成备份 网络 万载备份: ■ 生成备份 网络 恢复到出厂设置: ● 执行 > 防火墙 上代备份存出以恢复配置。 人名 水 AM / AM 上代备份存出以恢复配置。 / AM 人名 / 方統 上代备份存出以恢复配置。 / 方統 日 / 通出 通知面中文件: 「通過項文件」 / 通路 通知国际在,			
NBS GG//代复当前系统配置文件. NGK FtGG//L SK FtGG//L SK FtGG//L SK FtGG//L SMB FtGG//L FtGI/IE MISMINIE SMB FtGG//L Staff FtGG//L	> 状态 备份/恢复	j	
家合网络 下載品行: 重 生成品份 > 网络 · · · · · · · · · · · · · · · · · · ·	> 服务 备份/恢复	当前系统配置文件。	
> 网络 施复到出厂说罢: ● 执行 > 防火站 上传备份存档以恢复配置。 > 防火站 上传备份存档以恢复配置。 > 然久 火复配置: 」 直然建文件: ● 浏戏: ● 上传备份… 系统 修理収 管理収 定时面启 刷写新的固件 备份开级 上传合适的固件以喝新当前系统、选择 保留设置 未维持原有设置。 面合 通常配置: □ 通出 面件文件: 」 直 浏戏: ● 解写面件…	> 聚合网络	下载备份: 🔲 生成备份	
> VPN > 防火塩 上传备份存档以恢复配置。 > 家统 「炊复配置: 」」該選擇文件: ② 浏览 ③ 上传备份 系统 管理収 定时重启 月写新的固件 备份/升级 上传台道的圆件以刷新当前系统、选择 保留设置 来维特原有设置。 重启 L任台道的圖件以刷新当前系统、选择 保留设置 来维特原有设置。 通出 圖件文件: 」」」」」」」」」」」	> 网络	恢复到出厂设置: 🕲 执行	
防火端 上传备份存档以优复配置。 依复配置: 通 浏览 上传备份/// 系统 通 浏览 上传备份/// 通 浏览 上传备份/// 序时重启 月写折的固件 通 通 <th< th=""> <th< th=""> <th< th=""></th<></th<></th<>	> VPN		
系统 恢复配置: 通选择文件 通 浏览 重 上传备份…	> 防火墙 上传备份存	邦以恢复配置。	
系统 管理权 定时重启 刷写新的固件 备份/开级 上传合适的固件以刷新当前系统,选择 保留设置 来维持原有设置。 重启 保留配置: 退出 固件文件: [請选择文件]	◇ 系统	恢复配置: 请选择文件 💽 浏览	
管理权 定时重启 刷写新的固件 备份/开级 上传合适的固件以刷新当前系统,选择 保留设置 来维持原有设置。 重启 保留配置: 退出 圖件文件: 」 透览 』 過览 』 副写圆件…	系统		
定时重启 刷写幼形D卤件 备份/升级 上传合适的固件以刷新当前系统,选择 保留设置 来维持原有设置。 重启 保留配置: 退出 圖件文件: 请选择文件 2 浏览	管理权		_
备份/升级 上传台道的回杆以喇嘛当前系统,选择 傑留说童 来维持顺有说童。 重启 保留配置: 退出 圖件文件: 请选择文件 2 浏览	定时重启		
重启 中間配置. □ > 退出 固件文件: 両选择文件 3 浏览 副写固件	备份/升级	」回什以刷新当則系统,选择 保留设置 米雅持原有设置。	
> 退出 圖件文件: 请选择文件 □ 浏览 □ 刷写圖件	重启		
	> 退出	固件文件: 请选择文件 词 浏览 圆 刷写固件	

图 10 备份/恢复页面

参数备份:点击"下载备份"按钮,可以将当前参数文件,备份为压缩包文件,比如 backup- USR-G810-2022-04-20.tar.gz , 并保存到本地。

тест	
1231	备份/升级
> 状态	
> 服务	备份/恢复 每份/恢复当前系统配置文件
> 聚合网络	下载备份: 2 生成备份
> 网络	
> VPN	
> 防火墙	上传备份存档以恢复配置。
◇ 系统	恢复配置: 请选择文件 圆 浏览 圆 上传备份
系统	
管理权	
定时重启	刷与新的运行
音份/升级 重户	
里□ > 退出	
APPERT -	

图 11 参数备份上传页面

<u><说明></u>

- > 必须是 USR-G810-33 的配置文件进行导入,否则将有可能出现配置混乱现象;
- > 尽可能是同一版本固件进行导入配置,版本跨越较大有可能出现配置混乱现象。



2.5. 恢复出厂设置

通过网页可以恢复出厂参数设置。

		中文 English
TEST	备份/恢复	
	备份/恢复当前系统配置文件。	
> 状态	下載备份: 📴 生成备份	
> 服务	恢复到出厂设置: 🥘 执行	
> 聚合网络		
) 网络	上传备份存档以恢复配置。	
VPN NGV/抽	恢复配置: 请选择文件 🔲 浏览 🔟 上传备份	
✓ 药体		
系统	副写新的团件	
管理权	上传台适的固件以刷新当前系统,选择 保留设置 来维持原有设置。	
定时重启	保留配置: □	
备份/升级	固件文件: 请选择文件 🚺 浏览 🚺 剧骂固件	
重启		
> 退出		

图 12 恢复出厂页面

<u><说明></u>

- ▶ 在设备正常运行时,长按 Reload 按钮 5-15s 然后松开,路由器将自行恢复出厂参数设置,并自动重启;
- 重启生效瞬间,所有指示灯都将闪亮一下,然后灭掉(电源灯不灭);
- 在路由器内置网页界面,点击按钮恢复出厂设置,本功能与硬件的 Reload 按键功能一致;
- ▶ 恢复出厂过程持续 3 分钟,期间请不要给设备断电。

2.6. 固件升级

USR-G810-33 模块支持 web 方式的在线固件升级。



TEST
·
留於 1 名 名 合 的 / 次复当前系统配置文件。
状态 下戦备份: 🔟 生成备份
服务 佐毎利山口20年・ 👩 歩伝
聚合网络 2月11日 2日 2月11日 2日 2月11日 2日
网络
蒸 猝
入外が
管理权 上传合适的固件以刷新当前系统,选择保留设置来维持原有设置。
定时重启 保留配置: □
备份/升级 国件文件: 请选择文件 🔲 浏览 🔲 刷写固件
重启
退出

图 13 升级页面

<说明>

- > 固件升级过程会持续 3-4 分钟左右,请在 4 分钟后再次登录网页;
- > 可以选择是否"保留配置",如版本跨越较大不建议"保留配置"升级;
- 固件烧录过程中请不要断电或者拔网线。

2.7. 重启

点击按钮重启路由器。	重启时间与路由器的上电启动时间一致,	约为1分钟后完全启动成功。
------------	--------------------	---------------

		中文 English
TEST	系统	
	重新启动设备的操作系统]
> 状态		
1版方	重局	
> 紫台网站	<i>凤</i> 出行審白	
—————————————————————————————————————		
VPIN Nrivita		
○ 조倅		
系统		
管理权		
定时重启		
备份/升级		
重启		
> 退出		





2.8. 定时重启

可以按照每日、每周、每月任意时间的方式对路由器进行定时重启的管理,定期清除运行缓存,提高路由器运行稳定性。页 面设置如下。

				中文 Englis
TECT				
TEST	 定时重启			
	重新启动设备的操作系统			
〉 状态				
> 服务	参数配置			
> 聚合网络	开启	v		
> 网络	704	-		
> VPN	重启周期	每周 ~		
> 防火墙	星期	星期三 ~		
✓ 系统	().Brt	4		
系统				
答理权	分钟	44 ~		
	-		-	
之心可见				
首1577T级		应用	目保存	
重启				
> 退出				
	 图 15	定时重启设置		

3. 聚合服务

本服务是和阿里云合作推出的核心服务,开启聚合可以让多 WAN 网速叠加(包括双蜂窝网、有线、WIFI),让业务传输更加的稳定。在弱网或高速移动场景能够持续保持稳定高速联网。

聚合路由和普通路由器对比优势 弱网场景实测:加速后不丢包,低抖动 高速移动场景实测:加速后低延时,不掉帧 聚合立方 友商聚合竟品 延迟对比图 帧率对比图 600 单卡CPE测试一小时 云聚测试一小时 ●
单卡CPE 掉线次数 掉线时长 : 23 掉线次数 0 W. MAN THE MARAN APPROVA MAN A MANA MANANA 500 掉线时长总丢包率 : 73s 0s ----聚合立方 : 4% 总丢包率 : 0% 400 平均延迟 : 87.8ms 平均延迟 : 41.93ms 延迟标准差: 205.42 延迟标准差: 6.53 300 一聚合立方 一友商聚合产品 时延对比图 200 8000 100 6000 0 10 15 20 25 5 30 40 45 60 35 50 55

图 16 弱网以及移动环境下对比

<u><说明></u>

📌 क्dd www.usr.cn | 联网找有人

- > 常规出货 WIFI 支持 AP 功能,如需 WIFI WAN 多链路聚合功能需定制;
- 如您需体验聚合服务,可直接联系销售,我司将免费提供试用;
- 如需正式部署聚合服务批量使用,需联系销售购买聚合服务;
- ▶ 聚合服务支持 TCP/UDP 协议;
- 开启聚合服务时,负载均衡功能将自动关闭,再次关闭聚合服务时负载均衡自动打开;
- 聚合服务开启时,不影响网络切换功能;
- ▶ 服务优先顺序: QoS>聚合服务>负载均衡。
- 3.1. 开启并设置聚合服务

设置聚合服务请顺序执行:开启聚合服务->设置聚合规则(聚合规则内数据将走聚合服务)->如您需设置聚合黑名单请至聚合网络-黑名单进行设置(黑名单内规则将不走聚合服务)->查看聚合网络-状态与日志查看是否聚合建立成功。

TEST	뿔					
						_
> 状态	聚合网络	开启		~		
> 服务	设备ID	01600322	2093000000128			
✓ 聚合网络	用户名					
配置	ate 7.7					
聚合规则	當時			167		
黑名单	聚合网卡	• •	デ VLAN接口: "eth).2" (wan_wired)		
状态与日志		• 🖾	➢ 以太网适配器: "e ➢ 以太网活配器: "e	th1" (wan_4g1) th2" (wan_4g2)		
> 网络			64 W W W W	(
> VPN						
> 防火墙	服冬哭	H# tut			服冬哭烘口	
> 系统	加大力量	ACT AT			א וויינאר כלאח	
> 退出						
			尚	尤任何配置		

图 17 聚合配置页面

表 5 聚合配置参数表

名称	含义	默认值
聚合网络	开启:开启聚合服务	禁用
	禁用:禁用聚合服务	
用户名/密码	使用聚合服务,需要设置用户名密码	空
	免费体验版请联系销售提供	
	正式购买服务需填写正确的用户名密码	
聚合网卡	选择聚合服务使用的链路,可多选	eth1+eth2 双 SIM 聚合
	eth0.2:有线	
	eth1:SIM1	
	eth2: SIM2	
	如您定制 WIFI,聚合网卡将会新增 WIFI 网卡,可将双卡+有线+WIFI	
	四路聚合上传	



服务器地址	聚合服务器的地址: 域名或 IP	空
	免费体验版请联系销售提供	
	正式购买服务需填写正确的服务器地址	
服务器端口	聚合服务器的端口	空
	免费体验版请联系销售提供	
	正式购买服务需填写正确的服务器端口	

<u><说明></u>

- ▶ 服务器地址端口可最多可填写 10 条,填写多个服务器可实现聚合多 Server 优选、多 Server 灾备;
- ▶ 设置多个服务后设备会根据 RTT 值智能选路,选择最佳服务器进行聚合;
- 如最优聚合服务器异常,会自动再您设置的其他多个服务器中再选择最佳服务进行聚合;
- 聚合服务是否设置成功,请至聚合网络-状态与日志进行查看;
- 如您开启了聚合服务,但是未设置聚合规则,所有数据将不走聚合服务;
- ▶ 此界面点击应用将重启聚合服务。
- 3.2. 聚合规则设置(白名单)

3.2.1. 规则添加

TEST					
	聚合规则				
> 状态	聚合规则				
> 服务	目地IP地址	目的端口	源IP地址	源端口	协议
◇ 聚合网络					
配置			尚无任何配置		
聚合规则					
黑名单	新建规则:				
状态与日志	目地IP地址	目的端口	源IP地址	源端口 协议	(注解
> 网络	新建规则			ТСР	✔ 🚵 添加
> VPN					
> 防火墙					
> 系统			应用保存		
> 退出					

图 18 聚合规则页面

表 6 聚合配置参数表

名称	含义	默认值
目的 IP 地址	访问的目标 IP 地址经过聚合服务	空
	如您需要所有数据都经过聚合,可将目的 IP 地址设置为 0.0.0.0/0	
目的端口	访问的目标端口经过聚合服务	空



	如您无需限制端口,可直接填空	
源 IP 地址	某子网设备经过聚合服务	空
	如您无需限制具体子网设备可设置为: 0.0.0.0/0	
源端口	某子网设备限制端口经过聚合路由	空
	如您无需限制端口, 可直接填空	
协议	可选择的协议: tcp/udp	tcp

3.2.2. 选择聚合服务器

下图规则解析:所有子网设备无限制,访问所有目标网络并且协议是 tcp 或 udp 均走聚合服务。

点击选择服务器,可为该规则选择需要使用的服务器,对应服务器才会添加该规则,不选中任何服务器时,则该规则不生效。

TEST	TO A HORA					
	家古规则					
状态	聚合规则					
服务	目地IP地址	目的端口	源IP地址	源端口	协议	1
聚合网络						¥
配置	0.0.0/0	*	0.0.0/0	*	tcp	🛃 选择服务器 💉 删除
聚合规则	0.0.0/0	*	0.0.0/0	*	udp	🛃 选择服务器 💌 删除
黑名单						
状态与日志	新建规则:					
网络	目地IP挑扯	B	的端口	源IP地址		源端口 协议 注解
VPN						
防火墙	新建规则					TCP ~ 添加
系统						
退出				应用	保存	

图 19 聚合规则页面

<说明>

▶ 聚合规则最多可添加 30 条。



		中文 English
TEST	聚合规则 - 0.0.0.0/0:* - 0.0.0.0/0:* - tcp	
> 状态> 服务	服务器地址 • □ 階 服务器 • □ 階 服务部	
 	■ 返回至戦況 应用 候存	
繁音规则 黑名单 状态与日志		
> 网络 > VPN		
 > 防火端 > 系统 > 退出 		

图 20 勾选选择聚合服务器页面

<说明>

- > 聚合规则如不设置(或删除规则后),相当于未开启聚合服务,所有数据将不走聚合服务器,走原有路由通道;
- > 在"聚合网络-配置"界面中配置了几个服务器,在此处选择时,便有几个服务器可以选择,可全选;
- ▶ 该规则勾选哪个服务器,哪个服务器才会添加该规则,未勾选的服务器该规则将失效;
- > 聚合规则设置完成点击"应用"后仅重新配置规则,不重启聚合服务。

TEST			
	▲百半 甲名曲		
版务	而 日地IP地址	目的端口	注解
聚合网络		1/ 1/ / 1/1 T	
配置 聚合规则		回花社的監査	
梁名单	新建规则:		
伏态与日志	目地IP地址	目的端口	主解
	新建规则		21 添加
()			
充		应用 保存	
1			

3.3. 聚合服务黑名单设置



名称	含义	默认值
目的 IP 地址	聚合服务器黑名单 IP 地址	空
目的端口	聚合服务器黑名单端口号	空
	端口为空表示目标黑 IP 的所有端口所有协议数据均不走聚合服务	
注释	此规则备注	空

<说明>

- > 黑名单优先级比聚合规则高,如聚合规则和黑名单 IP 端口冲突时,以黑名单优先;
- ▶ 黑名单最多可添加 30 条;
- > 黑名单设置完成点击"应用"后仅重新配置规则,不重启聚合服务。

3.4. 状态与日志

3.4.1. 状态

如聚合功能开启成功后,状态将显示"已建立",也可以看到每个服务器的 RTT 值以及实时速率。

									目刻刷新井中文
TEST									
	状态与日志								
状态	状态日志								
服务		+							
聚合网络	第 百四始各户 调 切	验 追打中							
配置	通道状	态 共4条通道							
聚合规则	通道状态								
	通道	监听端口	类型	状态	RTT	客户端统计	上行吞吐量	下行吞吐量	
秋心与口 応 國络		20001	ТСР	已建立	21	0	0KB/s	OKB/s	
VPN		20000	TCP	已建立	33	28	0KB/s	OKB/s	
防火墙		10001	UDP	已建立	21	0	0KB/s	OKB/s	
系统		10000	UDP	已建立	33	0	0KB/s	OKB/s	
退出									
						_			
					<u></u> 逾用 6	247			

图 22 聚合服务状态显示页面

3.4.2. 日志

可通过日志查看聚合的状态和异常信息,也可在此处下载聚合日志包到电脑。





				自动刷新开 中文 English
	状态与日志			^
TEST				
	状态日志			_
状态	信息日志	开启	~	
> 服务	调试日志	禁用	~	
◇ 聚合网络				
配置	日志	□ 查看 □ 下载日志		
聚合规则				
黑名单				
状态与日志				
> 50人国				
> 退出				
	L			*

图 23 聚合服务 log 页面

<说明>

- 开启调试日志,日志更加详细;
- 可通过"下载日志"下载到电脑分析;
- 此界面点击应用将重启聚合服务。

4. 网络接口功能

4.1. 蜂窝网设置

4.1.1. 4G 接口

本路由器支持二路 4G 通信模块接口,用来访问外部网络。网页界面如下。



TEST	接口			
状态	接口总览			
服务	网络	状态	动作	
聚合网络 网络 接口	LAN ළුම් (දුණී) br-lan	运行时间: 24h 0m 31s MAC-地址: D4:AD:20:42:8A:A7 接收: 894.72 MB (1480463 数据包) 发送: 2.89 GB (2213889 数据包) IP44: 192.168.1.1/24	當 连接 ▲ 修改	
蜂窝网网络切换	WAN_4G1	MAC-地址: 00:00:00:00:00:00 接收: 0.00 B (0 数据包) 发送: 0.00 B (0 数据包)	连接 道修改	
无线配置 DHCP/DNS 主机名	WAN_4G2	运行时间: 23h 59m 26s MAC-地址: 32:53:41:FD:FB:09 接徵: 406.46 MB (318339 数据包) 发觉: 225.35 MB (221802 数据包) IPv4: 10.134.239.9/30	愛 连接 ▲ 修改	
静态路由 网络诊断 QoS	WAN_WIRED	运行时间: 0h 21m 53s MAC-地址: D4:AD:20:42:8A:A8 接收: 216.21 MB (257034 数据包) 发送: 243.57 MB (229209 数据包) [Py4: 172.16.11.25:27.23	💈 连接	
布裁均衡				

图 24 4G 接口设置页面

对于状态栏的显示如下,如果运行时间为0,代表本网卡未能联网。

表 8 状态表

名称	含义
运行时间	本接口在网时间
MAC 地址	本网卡接口的 MAC 地址
接收/发送	本网卡累计的接收与发送数据统计
IPv4	代表本网卡使用 IPv4 协议

<说明>

▶ 路由器默认优先使用有线 WAN 口, 可设置 4G1/4G2/WAN 优先。





4.1.2. APN 配置

				中文 English
TEST	配置移动网络IDAPN参数。网络 配置网络搜索优先级,可以减少	8优先级、SIM卡PIN码、网络探测 P网络搜索时间	等功能	Â
> 状态> 服务	修改 APN配置 保活探测配置	信息展示		
> 聚合网络	APN名称	自动检测	×	
✓ 网络		🔞 填写APN名称, 0-62 个字符		
接口	用户名	ADN(約田白夕 0.63 公式/		
蜂窝网		W APPROPRIA, 0-02 11-3-13		
网络切换	密码	④ APN的用户密码, 0-62 个字符		
无线配置	4- 	-		
DHCP/DNS	金权力丸	 APN的鉴权方式 	•	
主机名	网络横式	AUTO	~	
静态路由				
网络诊断	网络搜索优先级	AUTO	×	
QoS	DTNJ#F48			
负载均衡	PIN使能	U 🥘 如果SIM卡井启PIN码。需	第二日の日本での日本である「日本市である」	

图 25 配置页面

表 9 4GAPN 配置表

名称	含义	默认值
APN 名称	如您使用 APN 卡,请设置正确 APN	自动检测
	如您使用普通物联网卡,默认值即可	
用户名	如 APN 卡需要用户名,请正确填写	空
密码	如 APN 卡需要密码,请正确填写	空
鉴权方式	如 APN 需要设置鉴权,请正确填写	无
网络模式	可锁 2G/3G/4G	AUTO
	默认自动模式,自动模式当现场无 4G 情况会选择 2G 或 3G 驻网	
网络搜索优先级	驻网搜网时的优先顺序	AUTO
	可设置 AUTO/4G/3G/2G	
PIN 使能	如 SIM 卡设置了 PIN 码,请开启 PIN 使能并设置正确 PIN 码	关闭
PIN 码	如 SIM 卡设置了 PIN 码,请开启 PIN 使能并设置正确 PIN 码	1234

<说明>

> 路由器 APN 设置界面上面是 SIM1 的设置, 往下拉有一样的配置界面为 SIM2 配置界面。







4.1.3. 保活探测配置

		中文 English
	A	
TEST	APN記答	
> 状态	配置時初网始的JAPN姿数、网络优先级、SIM卡FINeb、网络探测等功能 配置网络搜索优先级,可以减少网络搜索时间	
> 服务		
> 聚合网络	修改	
✓ 网络	APN配置 保活探測配置 信息展示	
接口		
蜂窝网	开启 □ 🥘 勾选店,使用ping碰鱼网络	
网络切换	探测时间间隔 10 @ 西次班际 in child 如此: 10 5,85400	
无线配置	M หลังการสงๆจาก และเป็นสายาสระบาย, #102.87, 5-00400	
DHCP/DNS	探测地址1 223.6.6.6 V	
主机名		
	环期地址2 8.8.8.8	
网络诊断	473001/2018/r	
	7年25/142 ~ 7 (2) 连续失敗达到此次敗后,重新进行拨号,1-100	
Qos		
<u></u>	¥	

图 26 保活探测配置页面

表 10 保活探测配置表

名称	含义	默认值
开启	勾选:开启	自动检测
探测时间间隔	ping 的时间间隔,单位:s	10
探测地址 1	ping 探测的地址	223.6.6.6
	其中一个探测地址能 ping 通则表示网络通畅	
探测地址 2	ping 探测的地址	8.8.8.8
	其中一个探测地址能 ping 通则表示网络通畅	
探测次数	ping 的次数	AUTO

<u><说明></u>

▶ 路由器保活探测配置界面上面是 SIM1 的设置,往下拉有一样的配置界面为 SIM2 配置界面;

> 当界面填写的 2 个探测地址和内部预留的 ping 探测地址都不通时则认为网络异常,将重新驻网拨号。

4.1.4. SIM 卡信息显示

SIM 卡信息显示会详细得显示出 SIM 卡的配置信息,如果联网出现问题可以在此查看问题的原因。





图 27 SIM 卡信息显示

4.2. 无线配置

USR-G810 具备双频 WiFi 功能: 2.4GHz 和 5.8GHz 无线网络。可以在基本设置、高级设置里面对双频 WiFi 的参数进行修改。如不需要 WiFi 功能,可直接选择禁用。

теѕт		
	无线概况	
状态	WIFI-2.4G-AP	
》服务	Work mode: AP Driver version: 5.0.4.0	🥏 重载 📝 高级设置
聚合网络	Interface: rax0 Type: AP SSID: USR-G810-8AA7 Channel: 0	(2) 禁田 (2) 基础设置
✓ 网络	BSSID: 02:0c:43:38:05:c0 Mode: B/G/GN mode	
接口		
蜂窝网	WIFI-5G-AP Work mode: AP	🥏 重载 🗾 高级设置
网络切换	Driver version: 5.0.4.0	
无线配置	Interface: rau type: AP SSID: USR-G810-8AA / SG Channel: 0 BSSID: 00:0c:43:28:05:c0 Mode: A/AC/AN mixed	🥹 禁用 🗹 基础设置
DHCP/DNS		
主机名		
静态路由		
网络诊断		
QoS		
各封均衡		

图 28 无线配置界面

<u><说明></u>

➢ G810 路由器本身是一个 AP,其它无线终端可以接入到它的 WLAN 网络。支持最多 24 个无线 STA 连接;



> 本 WLAN 局域网与有线 LAN 口互为交换方式;

> WiFi 最大覆盖范围为空旷地带 200m, 办公室等有障碍物地受环境影响可在 40m 内覆盖。

			中文 English
тгет			
IESI	拉口石架 W/EL24	C AD@rav0	
45-	按口的道"WIFI-2.44	S-AP@Idx0	
1.122	基本设置 客户端列	表	
服力			
	WIFI名称	USR-G810-8AA7 character (1 ~ 32)	
接口	认证模式	WPA2PSK 🗸	
蜂室网	加密	TKIPAES V	
网络切换	密码	12345678	
无线配置	隐藏		
DHCP/DNS	WMM多媒体加速		
主机名			
静态路由			
网络诊断			
QoS			
负载均衡			

图 29 无线-SSID 设置页面

默认参数	说明	默认值
WIFI 名称	WIFI 名称	2.4G:USR-G810-XXXX
		5G: USR-G810-XXXX_5G
		(最后为 MAC 地址后 4 位)
认证模式	WIFI 的认证模式,可设置	WPA2PSK
	Disable/WPA2PSK/WPA3PSK/WPAPSKWPA2	
	PSK/WPA2PSKWPA3PSK	
加密	TKIP/TKIPAES/AES	TKIPAES
密码	WIFI 密码	12345678
隐藏	勾选后客户端搜索不到本 WIFI 名称	未勾选
	连接时需要输入正确 WIFI 名称和密码才可连接	

表 11 无线 WiFi 基本设置参数表

在"无线配置→WiFi-2.4G-AP(WiFi-5G-AP)→基础设置→无线客户端"查看客户端的列表信息。



â										
TEST										
	接口配置 - WIFI-2	.4G-AP@rax	0							
> 状态	基本设置 客户端	列表								
> 服务	<u> </u>									
> 聚合网络	MAC Addr	Aid I	PSM PS) TX Rate	TxBF	RSSI	Stream SNR	Snd Rsp SNR	Last RX Rate	Connect Time
✓ 网络				MCS 79		-41	0.0	-	MCS 72	
接口	C F7	1 (D 3	20M, LGI OFDM,		-34 -127	0.0	-	20M, LGI MM, STBC	00:00:25
蜂窝网				_						
网络切换				Σ.	VA C	呆存				
无线配置										
DHCP/DNS										
主机名										
静态路由										
网络诊断										
QoS										
负载均衡										
VPN										

图 30 无线-客户端列表

在"无线配置→WiFi-2.4G-AP(WiFi-5G-AP)→高级设置"修改信道、带宽、发射功率。

TEST	
	设备配置 - WIFI-2.4G-AP
状态	日本设置 高級
服务	
聚合网络	区域代码 US (United States) >
网络	区域街道 0: Ch1~11 学期的选项不受支持 US 国家码 9 - B/G/GN mode 无线模式
接口	工作模式 Mixed Mode >
网络切换	信道须选 20/40 MHz ▼ 禁用的选项不受支持 WIFI-2.4G-AP 设备 9 - B/G/GN mode 无线或者信道 0
无线配置	发射功率 100 %(范围 1-100, 默认 100)
DHCP/DNS	
主机名	<i>加</i> 用 保存
静态路由	
网络诊断	
QoS	
〕 载均衡	
/PN	
0.00000000	

图 31 无线-信道设置页面

4.3. LAN 接口

LAN 口为千兆局域网络,本设备具备 3 个有线 LAN 口。





				自动
∧				
TEST	接口			
				_
状态	接口总览			
服务	网络	状态	动作	
聚合网络	LAN	运行时间: 5h 15m 4s		
/ 网络	5º (<u></u>)	接收: 55.87 MB (135327 数据包)	🥔 连接 🛃 修改	
接口	br-lan	友達: 125.52 MB (113426 数组信息) IPv4: 192.168.1.1/24		
蜂窝网	WAN_4G1	MAC-地址: 00:00:00:00:00		
网络切换	eth1	接收: 0.00 B (0 数据包) 发送: 0.00 B (0 数据包)	🐉 连接	
无线配置		运行时间: 5h 13m 58s		
DHCP/DNS	WAN_4G2	MAC-地址: F6:8F:50:66:07:48		
主机名	eth2	发送: 10.52 MB (31447 数据包)		
静态路由		IPv4: 10./1.241.52/29 远行时间: 5h 15m 0s		
网络诊断	WAN_WIRE	D MAC-地址: D4:AD:20:42:8A:A8	All starter	
	eth0.2	发送: 51.05 MB (104702 数据包)		
Q03		IPv4: 172.16.11.225/23		
贝轼均衡				
VPN				
防火墙				

图 32 LAN 口设置页面

<说明>

- ▶ 3个LAN口;
- ▶ 默认静态的 IP 地址 192.168.1.1,子网掩码 255.255.255.0。本参数可以修改,比如静态 IP 修改为 192.168.2.1;
- ▶ WIFI 桥接到了 LAN 口,和 LAN 同网段;
- ▶ 默认开启 DHCP 服务器功能,所有接入到路由器 LAN 口的设备均可自动获取到 IP 地址;
- 具备简单的状态统计功能。

4.3.1. DHCP 功能

LAN 口的 DHCP Server 功能默认开启(可以选择关闭),所有接入 LAN 口的网络设备,可以自动获取到 IP 地址。





				自动場新开 中文 Englis
TEST	IPv4地址	192.168.1.1		
	IPv4子网拖码	255.255.255.0 🗸		
> 状态	IPv4广播			
> 服务	使用自完义的DNS服务器			
> 聚合网络	אר לאנגייטינעצבאבורטו			
✓ 网络				
接口	り日の服务界			
蜂窝网				-
网络切换	基本设置			
无线配置	关闭DHCP	② 2 禁用本接口的DHCP。]	
DHCP/DNS	記念地址	2		
		2		
主机名		2 ② 网络地址的起始分配基址。		
主机名	客户数	2 网络地址的起始分配基址。 253		
主机名 静态路由 网络诊断	客户数	2 3 网络地址的起始分配基址。 253 3 最大地址分函数量。		
主机名 静态路由 网络诊断 QoS	客户数 租用时间	 2 2 2 (2) 网络地址的起始分配基址。 2 53 3 (2) 日本(1) 日本(2) 11 日本(2) 11 日本(2) 11 11 11 11 11 11 11 11 11 11 11 11 11		
 主机名 静态路由 网络诊断 QoS 负载均衡 	客产数 租用时间	2 网络地址的起始分和基础。 253 ② 最大地址分前数量。 12h ④ 地址相同,最小公分钟(2m)。		
主机名 静志路由 网络诊断 QoS 负载均衡 > VPN	客户数 租用时间	2 网络地址加加显动分和温祉。 253 ④ 最大地址分前波量。 12h ④ 地址相明,最小之分钟(2m)。		

图 33 DHCP 设置页面

<说明>

- > 可以调整 DHCP 池的开始地址,以及地址租用时间;
- > DHCP 默认分配范围从 192.168.1.2 开始;
- 默认租期 12 小时。
- 4.4. DHCP/DNS

静态地址分配(IP-MAC 绑定):该功能是 LAN 接口 DHCP 设置的延伸,用于给 DHCP 客户端分配固定的 IP 地址和主机标识。

â				
TEST	DHCP/DNS			
	DHCP 客户端列表及静态IP地址分配			
状态	静态地址分配用于给DHCP客户端分配	配固定的IP地址和主机标识。只有指定的	主机才能连接,并且接口须为非动态副	記置。
服务	已分配的DHCP租约			
漱百四增 网络	主机名	IPv4地址	MAC-地址	剩余租期
接口	?	192.168.1.11	c8:9 5:f7	9h 40m 38s
全 案 网	USR-NDVSZNHNEZD	192.168.1.198	c 57:14	11h 50m 13s
各切换				
5线配置	静态地址分配			
DHCP/DNS	主机名	<u>MAC</u> -地址		<u>IPv4</u> -地址
机名				
争态路由		尚	无任何配置	
网络诊断				
QoS	新建规则:			
负载均衡	主机名	MAC-地址	IP	<u>v4</u> -地址
PN .	新建规则		~	► 🚵 添加
▶/墙				







	表 12 DHCP/DNS 参数	2表
默认参数	说明	默认值
主机名	子网设备的名称	空
MAC 地址	子网设备的 MAC 地址	空
IPv4 地址	设置的 IPv4 地址	空

<说明>

- ۶ 最多可添加 20 条 DHCP/DNS 规则;
- IPv4 地址请和 LAN 口设置同网段,否则无法正常通信。 ≻

4.5. WAN 口

				自动局新开中
TEST				_
	接口			
状态	接口总览			
服务	网络	状态	动作	
聚合网络	LAN	运行时间: 10h 25m 40s		
/ 网络	මුළු (දූක) br-lan	地域-地址: 04:AD:20:42:0A:A/ 接收: 65.73 MB (214714 数据包) 发送: 183.34 MB (186870 数据包)	🌮 连接	
按口	WAN 4G1	IPV4: 192.168.1.1/24		
蜂篱网 网络切换	eth1	MAC-地加:0000000000000000 接收:0.00 B (0 数据包) 发送:0.00 B (0 数据包)	🌮 连接	
无线配置	WAN 4G2	运行时间: 10h 24m 34s		
DHCP/DNS 主机名	eth2	MAC-地址 Fr6381:50/5650/748 接收: 112.28 MB (131443 数据包) 发送: 17.22 MB (75833 数据包) IPv4: 10.71 241 52/29	连接 谨按 修改	
静态路由		运行时间: 10h 25m 36s		
网络诊断 OoS	eth0.2	MAC-地址: D4:AD:20:42:8A:A8 接收: 200.06 MB (955516 数据包) 发送: 59.33 MB (164177 数据包)	② 连接 ▲ 修改	
① 载均衡		IPv4: 1/2.16.11.225/23		
VPN				
防火墙				

图 35 WAN 口设置页面

<说明>

- \triangleright 1 个有线 WAN 口,WAN 口为广域网接口;
- 支持 DHCP 客户端,静态 IP, PPPOE 模式; \triangleright
- ⊳ 默认 DHCP 客户端;
- WAN 口 IP 不可与 LAN 口 IP 同网段。 \triangleright

4.5.1. DHCP 客户端

上级路由器必须开启 DHCP 服务,用网线插入上级路由器 LAN 和本路由器 WAN, G810-33 才可获取 IP。





		自动刷新开;
TEST		
	接口 - WAN_WIRED	
J 1	配置网络接口信息。	
大会		
》 紫台网络	基本设置 物理设置 防火堵设置	
	状态 运行时间: 10h 28m 52s	
一接口	MAC-地址: D4:AD:20:42:84:A8 tellfo: 20, 20, 10, 10, 06:1002 #51(日本)	
蜂窝网	eth0.2	
网络切换	IPV4; 1/2.16.11.225/23	
无线配置	thuy DHCPse 白迷 く	
DHCP/DNS		
主机名	请求DHCP的发送的主机名 USR-G810	
静态路由		
网络诊断	◎ 返回至概况	
QoS		
负载均衡		
VPN		
and the first		

4.5.2. 静态 IP

填写和上级路由器同网段 IP, IP、网关和子网掩码需要正确填写,如是专线公网网线,需按照运营商给出的 IP、子网掩码、网关 以及 DNS 服务器正确填写。

		目式加制数
тет		
IESI	接口 - WAN_WIRED	
华大	配置网络接口信息。	
服务		
聚合网络		
网络	基本设置 物理设置 防火電设置	
接口	状态 运行时间: 10h 29m 17s MAC-地址: D4:AD:20:42:84:A8	
蜂窝网	接触: 200.77 MB (962919 数据包) eth0.2 发送: 59.39 MB (164650 数据包)	
网络切换	IPv4: 172.16.11.225/23	
无线配置	14 MA 1924-1011	
DHCP/DNS		
主机名	IPv4提加	
静态路由	IPv4子网编码 请选择 🔸	
网络诊断	IPv4网关	
QoS	10-40-56	
负载均衡		
VPN	使用自定义的DNS服务器	
防火墙		

图 37 WAN 口设置-静态 IP

4.5.3. PPPoE

需按照运营商给出的正确用户名和密码填写。

.



		自动局新开 中文 English
TEST		_
	接口 - WAN_WIRED	_
> 状态	配置网络接口信息。	
> 服务	一般设置	
> 聚合网络		_
✓ 网络		
接口	状态 运行助间: 10h 34m 37s MAC-地址: D4:AD:20:42:8A:A8	
蜂窝网	推載: 201.91 MB (974180 数据包) eth0.2 发送: 59.48 MB (165389 数据包)	
网络切换	IPv4: 172.16.11.225/23	
无线配置		
DHCP/DNS	协议 PPPoE Ý	
主机名	PAP/CHAP用户名	
静态路由	PAP/CHAP密码 Ø	
网络诊断		
QoS		
负载均衡		
> VPN		
> 防火墙		

图 38 WAN 口设置-PPPoE

4.6. 网络切换

				中父	z English
TEST					Î
1231	网络切换				
	配置网络优先级检测规则				
> 状态					
> 服务	配置				
> 聚合网络	优先级	有线网络优先	~		
✓ 网络		la ann			
接口	参考模式	自定义	~		
蜂窝网	参考地址 1	223.6.6.6	~		
网络切换		② IP地址或域名,如"223.6.	6.6"或者"baidu.com"		
天线配置	参考地址 2	119.29.29.29	v		
DHCP/DNS		IP地址或域名,如"223.6.	6.6"或者"baidu.com"		
======================================	参考地址 3	8.8.8.8	~		
土机名		(2) IP地址或域名, 如*223.6.	6.6"或者"baidu.com"		
静态路由	检查时间周期	10			
网络诊断		(2) 1-600秒			
QoS	Ping包大小	100			
负载均衡		32-1024Byte			
> VPN	Ping超时	2000			
> 防火墙		@ 100-20000達秒			
					*
		— •• —			
		图 39 网	內谷切换配直		
		主 12 12	网络切场和罢		
		π 13 μ	小名刘沃巴旦		
名称	描述			默认参数	



优先级	有线网络优先	有线网络优先
	4G1 网络优先	
	4G2 网络优先	
	禁用:禁用网络切换功能,使用当前上网方式上网	
参考模式	自定义:根据自定义参考地址确定网络状态	自定义
	网关:参考网关确定网络状态	
参考地址 1	可设置 IP/域名	223.6.6.6
参考地址 2	可设置 IP/域名	119.29.29.29
参考地址 3	可设置 IP/域名	8.8.8.8
检测间隔(单位:s)	设置链路检测间隔:可设置1-600s	10
ping 包大小(单位:字节)	检测链路时包大小:可设置 32-1024 字节	100
Ping 超时(单位:ms)	设置 ping 超时时间:可设置 100-20000ms	2000

<说明>

- > 配置网络优先级检测规则,默认启用,默认切网顺序:有线网络优先;
- > 设定 3 组检测联网状态的 IP 地址(也可以设定域名),如能够 ping 通其一,则判断网络正常,不进行任何切网配置;
- ▶ 如 3 组检测规则均无法 ping 通,则执行切网操作,继续进行 ping 包检测;
- > 如有线网络、蜂窝网络均无法 ping 通,则判断路由器无法连接外网。

4.7. 主机名

主机名功能为自定义挟持域名功能,可将自定义域名对应 IP(需要客户端 DNS 指向本路由生效)。

A			
	主机名		
	为内网主机设置主机名,配置重启生效		
	主机目录		
	主机名	IP地址	
		尚无任何配置	
	象话建规则:		
	主机名	IP地址	
	新强制规则	~	1 添加
		应用 保存	

图 40 主机名配置

<u><说明></u>

▶ 主机名最多可设置 20 条。



4.8. 静态路由

静态路由有如下几个参数。

名称	描述	默认参数
接口	lan、wan_4g1、wan_4g2、wan_wired 、vpn 接口	lan
对象(目标地址)	要访问的对象的地址或地址范围	空
子网掩码	要访问的对象网络的子网掩码	空
网关(下一跳)	要转发到的地址	空
跃点数(Metric)	包跳跃个数	空

表 14 静态路由参数表

静态路由描述了以太网上数据包的路由规则。

测试示例:测试环境,两个平级路由器 A 和 B,如下图。



图 41 静态路由表实例图

路由器 A 和 B 的 WAN 口都接在 192.168.0.0 的网络内,路由器 A 的 LAN 口为 192.168.2.0 子网,路由器 B 的 LAN 为 192.168.1.0 子网。

现在,如果我们要在路由器 A 上做一条路由,使我们访问 192.168.1.x 地址时,自动转给路由器 B。



	路由表				
	路由表描述了数据包试 请为静态IPv4路由选择 当添加或者制除路由机	0可达路径。 彰IPv4接口, 如: wan_wired, wan_4 则后, 需要点击应用来保证工作正	4g1, wan_4g2 二常		
	静态IPv4路由				
ł	接口	目标	IPv4-子网掩码	<u>IPv4</u> -网关	跃点数
			尚无任何配益	Ŧ	
	新建规则:				
	接口	目标	IPv4-子网掩码	<u>IPv4</u> -网关	跃点数
		主机IP或网络	如果对象是一个网络		
	wan_wired 🛩	192.168.1.0	255.255.255.0	192.168.0.202 0	🎽 添加
				-	
			应用(保	3	

图 42 路由表添加页面

<u><说明></u>

▶ 静态路由最多可添加 20 条规则。

4.9. 网络诊断功能

				中文 English
TEST	501000 M			
	网络诊断			
> 状态	网络工具			
> 服务	223.6.6.6	8.8.8.8	www.baidu.com	
> 聚合网络	I Ping	Traceroute	Nslookup	
~ 网络				
接口				
蜂窝网				
网络切换				
无线配置				
DHCP/DNS				
主机名				
静态路由				
网络诊断				
QoS				
负载均衡				
> VPN				
> 防火墙				
> 系统				
》退出				

图 43 网络诊断页面

<u><说明></u>

- 在线诊断功能,包括 Ping 工具,路由解析工具,DNS 查看工具;
- Ping 是 Ping 工具,可以直接在路由器端,对一个特定地址进行 ping 测试;



Traceroute 是路由解析工具,可以获取访问一个地址时,经过的路由路径;

> Nslookup 是 DNS 查看工具,可以将域名解析为 IP 地址。

4.10. QoS

QoS(Quality of Service)即服务质量。在有限的带宽资源下,QoS为各种业务分配带宽,为业务提供端到端的服务质量保证。 例如,语音、视频和重要的数据应用在网络设备中可以通过配置 QoS 优先得到服务。

<u><说明></u>

- 开启聚合服务时,负载均衡功能将自动关闭,再次关闭聚合服务时负载均衡自动打开;
- ▶ 聚合服务开启后,不影响网络切换功能;
- ▶ 服务优先顺序: QoS>聚合服务>负载均衡。

TEST	接口													删除
狀态	WA	N												
				开启)								
聚合网络				分类组	默认	L.			~					
网络			t	算开销)								
接口				半双工	C)								
(两网) I络切换		下载	速度(kbit/s)	10)24								
线配置		上传	速度(kbit/s)	12	28								
DHCP/DNS														
主机名					1	添加								
静态路由	分类	规则				-								
各诊断	目标	源主	n.	目的主	ŧî.	服务	;	协议	端口	穷	步数	注解	排序	
负载均衡														
PN	最~	全部	~	全部	~	全部	~	全部 🖌	22,53	~	SS	h, dns		▶ 删除
火墙	最~	全部	~	全部	~	全部	~	ICMP 🗸	全部	~	pir	ng	•	制除
č	普~	全部	~	全部	~	全部	~	тср 🗸	20,21,25,80,110,443,993,995	~	ftp	o, smtp, h		▶ 删除
3	×.	~PR	~	498		今朝	~		5100			01 IChat		

图 44 QoS 设置页面

4.10.1. 接口限速

可以新建立一个接口限速,此处的接口与下列一致,添加接口使用小写即可,添加后会自动显示大写格式。

名称	网卡名						
LAN 接口	lan						
有线 WAN 接口	wan_wired						
蜂窝 SIM1	wan_4g1						
蜂窝 SIM2	wan_4g2						

表 15 接口表

举例:将 WAN 口限速上下行 100kbit/s 左右。




	#X1					
USR-G810	下翻译度 (Unit/e)	1024				
		L Sector				
> 狀态	上传速度 (kbit/s)	128				
) IB-8-						
1100						删除
× 网络	WAN WIRED					
接口						
(A)	开启					
网络扫描	分类组	默认	•			
于任初罢	计算开销					
DUCD/DNC	3430 T					
+切々	TAL	0				
主切内	下载速度 (kbit/s)	100				
IPO208日	上传速度 (kbit/s)	100				
Q05		៉ 添加				
贝轼内衡	八半切回山					
VPN		0 8247 44539		, 100 Hillson	1+07	19-14
> 防火増	HAN WEAR HUTD	Ni 88295 1976X	Line	子印叙	11.84	ALLA
熟玩		マ 今照 マ 今照 マ 22	50	~	eeb, doe	
退出	W. Th. Th.	aller EBP * 22	100		531, 013	
	最✓ 全部 ✓ 全部	✓ 全部 ✓ ICMP✓ 全部	ß	~	ping	• • 💌 副除

图 45 接口限速设置页面

<说明>

▶ 开启:是否在此接口启用 QoS,勾选则启用;

- > QoS 接口限速如和聚合路由选择的接口并用,首先"接口限速"会作用在该接口,其次"分类规则"也会作用在该接口;
- ▶ 上传速度: 会将上传的速度限制在此速率附近, 单位为 kbit/s, (注意:网上的文章表明此处仅限 TCP);
- > 下载速率: 会将下载的速度限制在此速率附近, 单位为 kbit/s。

4.10.2. 分类规则

		计算	开销	2							
		¥	双工								
	下载	東度 (kb	it/s)	100							
	上传	東度 (kb	it/s)	100							
				🖆 添加							
分割	き规则										
目标	源主机	i (目的主机	服务	协议	X	端口	字节数	注解	排序	
•	全部	→ 全	部 、	全部	✓ 全部	~	22,53 ~		ssh, dns		▶ ■ 删除
最~	全部	✓ 全	# v	全部		~	全部 🗸		ping	•	
普~	全部	✓ 全	部 ¥	全部	✓ TCP	~	20,21,25,80,110,443,993,995		ftp, smtp, h	tel.	
高~	全部	✓ 全	部 、	全部	✓ 全部	~	5190 🗸		AOL, iChat,		制除
任人	全部	v 4	en 🗸	全部		~	0000 0008 0007 0006 0005 0004 0003 0007 00 🗸				
100.2	al er		-	all her	- ODI						En auror
(1) 活	iba										
							<u>应用</u> 保存				

图 46 分类规则设置页面

📌 👬 WWW.usr.cn 🛛 联网找有人

<说明>

- > 目标:一种分类标记,可选项:最高/高/普通/低,QoS会将符合条件的数据包加上对应的标记;
- > 源主机:数据包的源地址,填写 IP 地址;
- ▶ 目标主机:数据包的目的地址,填写 IP 地址;
- ▶ 服务:可选针对某种网络服务,可选项 aim/bittorrent/edonkey/fasttraclk/ftp...
- ▶ 协议: TCP/UDP/ICMP/自定义;
- 端口:可选针对不同端口,多个端口使用逗号隔开;
- 包大小:定义需要匹配的字节数大于等于该数值,单位 bytes,如需设置最大长度,匹配小于 50000 字节的包(:50000),匹配 500-3000 字节内的包(500:3000);
- ▶ 注释: 解释文字, 用来给人员方便查看的。

4.11. 负载均衡

本设备采用 mwan3 软件, 它的作用是把路由器的流量, 做路由表级别的负载均衡, 按照设置的优先级和权重分配到不同的 WAN 口上, 从而起到网速叠加的作用。

<说明>

- 当开启聚合服务时,负载均衡将自动关闭;
- 默认禁用负载均衡,如使用负载均衡功能请正确配置;
- 开启聚合服务时,负载均衡功能将自动关闭,再次关闭聚合服务时负载均衡自动打开;
- ▶ 当 QoS 具备接口限速,优先 QoS 限速功能,负载均衡功能仍旧生效,QoS 限速接口数据包速率低;
- ▶ 服务优先顺序: QoS>聚合服务>负载均衡。

名称	网卡名
有线 WAN 接口	wan_wired
蜂窝 SIM1	wan_4g1
蜂窝 SIM2	wan_4g2

表 16 各 WAN 接口表



05K-0010		
> 状态		
> 服务		
> 聚合网络		
✓ 网络	MWAN负载均衡 接口状态	
接口	wan 4g1 (eth1) wan 4g2 (eth2)	wan_wired (eth0.2)
蜂窝网	Online (tracking active)	Online
网络切换		
无线配置	L	
DHCP/DNS		
主机名		
静态路由		
网络诊断		
QoS		
负载均衡		
> VPN		
> 防火墙		

图 47 负载均衡设置页面

5. VPN 功能

VPN(Virtual Private Network)虚拟专用网,在协议上又分为 PPTP、L2TP、IPSec、OpenVPN、GRE 等。接下来分别介 绍一下这几种协议创建 VPN 的原理。

PPTP:

是一种点对点的隧道协议,使用一个 TCP(端口 1723)连接对隧道进行维护,使用通用的路由封装(GRE)技术把数据封装成 PPP 数据帧通过隧道传送,在对封装 PPP 帧中的负载数据进行加密或压缩。其中 MPPE 将通过由 MS-CHAP V2 身份验证过程所生成 的加密密钥对 PPP 帧进行加密。

L2TP:

是第二层隧道协议,与 PPTP 类似。目前 G810-33 支持隧道密码认证、用户名密码认证方式,支持 L2TP OVER IPSec 的预 共享密钥加密。

IPSec:

协议不是一个单独的协议, 它给出了应用与 IP 层上网络数据安全的一整套体系结构, 包括网络认证协议 ESP、IKE 和用于网路认证及加密的一些算法等。其中 ESP 协议用于提供安全服务, IKE 协议用于密钥交换。

OpenVPN:

支持基于证书的双向认证,也就是说客户端需认证服务端,服务端也要认证客户端。

GRE:

GRE(Generic Routing Encapsulation、通用路由封装)协议是对某些网络层协议(如 IP 和 IPX)的数据报文进行封装,使 这些被封装的数据报文能够在另一个网络层协议(如 IP)中传输。GRE 采用了 Tunnel(隧道)的技术,是 VPN(Virtual Private Network)的第三层隧道协议。

注意:

这几种协议都可以搭建出 VPN,具体可以根据自己的需求来选择比较适合的协议来搭建。

下面是这几种协议的版本号和具体搭建过程:

序号	协议	版本号
----	----	-----





1	РРТР	V1.10.0
2	L2TP	V1.3.15
3	IPSec	V5.3.3
4	OpenVPN	V2.4.7

5.1. PPTP Client

应用前需要获取到 VPN 服务器地址、账户、密码和加密方式,然后启用 PPTP 客户端,其他参数依次写入。

			中文 English
	PP1P 麥欸		A
USR-G810	PPTP 客户端	● 开启 ○ 禁用	
	服务器地址	192.168.0.2	
> 状态	接口	自动	
> 服务		(2) "自动"表示使用默认路由接口连接	
> 聚合网络	用户名		
> 网络	密码	2	
~ VPN	对端子网	192.168.55.0	
PPTP		2 eg: 192.168.10.0	
L2TP	对端子网掩码	255.255.255.0	
IPSec		@ eg: 255.255.0	
OpenVPN	NAT		
GRE	MPPE加密		
VPINA/22	МТО	1450	
四人個		6 00~1450	
〉退出	额外配置		
- Parameters		▲ 通加pppd参数,非专业人员,禁止操作	
	使能静态隧道IP地址		
			· · · · · · · · · · · · · · · · · · ·

图 48 路由器添加 VPN 操作图一

<说明>

- ▶ 服务器地址:填写要连接的 VPN 服务器 IP 或者域名;
- ➢ 接口:根据联网方式的不同可选择 wan_4g1、wan_4g2、wan_wired、自动;
- ▶ 用户名/密码:从 VPN 服务器处获取;
- ▶ 加密方式: MPPE 加密、无加密,从 VPN 服务器端获取,根据实际情况选择打勾或不打勾;
- > MTU 设置:设置通道的 MTU 值,默认 1450,本项设置需和 VPN 服务器对应;
- NAT 设置:该功能默认开启。当内容需要和外部通讯时,将内部地址替换成公用地址。关闭该项,则无法实现网络地址转换 功能;
- ➢ 对端子网、掩码:填写正确后,在 NAT 功能开启下,可直接实现 VPN 下的子网互通功能;
- ▶ 使能静态隧道 IP 地址:默认未使能,服务器端自动分配 IP。可于此处填写静态隧道 IP;
- > 额外配置:追加 PPPD 参数、魔术字等,默认不需要进行任何操作;
- > 使能 ping:实时 VPN 在线检测及重连机制。通过 ping 自定义 IP 的方式,保证连接稳定。默认未启用。



		中文 English
	MPPEbase	
	MTU	1450
\		600~1450
10.05	额外配置	
影合网络		◎ 追加pppd参数非专业人员禁止操作
> 网络	(市会)総合大計算(第10十年日)	
✓ VPN	UCHORPS ARELES IF ACAL	
PPTP	默认网关	□ ③ 所有流量主VPN除WANHitV5pPPPOE外
L2TP	使船ping	🖾 🥥 ping失败将撤连VPN
IPSec	ping地址	
OpenVPN		Standard, while 10.0.1.2
GRE	ping周期	10
VPN状态	nina)定勝7	3
> 防火墙	pm.goox	
> 系统		
> 退出		放用 保存

图 49 路由器启用 VPN 状态检测

PPTP 连接成功:完成相关参数的填入后,保存&应用,进入到 VPN--VPN 状态处查看连接状态。

		#1 5
USR-G810		
	VPN	
状态	VPN状态	
服务		
聚合网络	类型: PPTP	
网络	IP地址: 192.168.154.105	
VPN	子网海码: 255.255.255.255	
РРТР	网关: 192.168.154.100	
L2TP	這接时间: 3s	
IPSec		
OpenVPN		
GRE		
VPN状态		
防火墙		
系统		
退出		

图 50 路由器 VPN 连接状态

5.2. L2TP Client

L2TP 是第二层隧道协议,与 PPTP 类似。目前 G810-33 支持隧道密码认证,支持 L2TP OVER IPSec 的预共享密钥加密方式。进入 VPN--L2TP 界面中,选择启用 L2TP 客户端,依次填入参数。



USR-G810			
	L2TP 设直		
d h-+-	L2TP 参数		
17.63	L2TP 客户端		-
> 服务		- 70L - 2070	
> 聚合网络	服务器地址	192.168.0.2	
	埼口	白动	
P.G. H	382	 (3) '自动'表示使用默认路由接口送 	车接
✓ VPN			
PPTP	用户名		
L2TP	密码		-
IPSec			
il occ	隧道名称	g810	
OpenVPN	議道宗紀		1
GRE	HEDE LEAN-J	(2) 字符(0-50)	
VPN状态		-	
) 防火樓	IPSec加密	U	
	对端子网	192.168.55.0	
> 系统		eg: 192.168.10.0	
> 退出	7.11米乙的东西	255 255 255 0	
	Entertion enterty	(2) eg: 255.255.255.0	
		-	
	NAT		

图 51 L2TP 客户端启用设置界面

<说明>

- L2TP 支持隧道密码认证、L2TP OVER IPSec 加密;
- ▶ 服务器地址:填写要连接的 VPN 服务器 IP 或者域名;
- ➢ 接口:根据联网方式的不同可选择 wan_4g1、wan_4g2、wan_wired、自动;
- ▶ 用户名/密码:从 VPN 服务器处获取;
- ▶ 加密/认证:隧道密码认证、IPSec 加密,从 VPN 服务器端获取后正确填入;
- ▶ 使能静态隧道 IP 地址:默认未使能,服务器端自动分配 IP。可于此处填写静态隧道 IP;
- > 额外配置:追加 PPPD 参数、魔术字等,默认不需要进行任何操作;
- NAT 设置:该功能默认开启。当内容需要和外部通讯时,将内部地址替换成公用地址。关闭该项,则无法实现网络地址转换 功能;
- ➢ 对端子网、掩码:填写正确后,在 NAT 功能开启下,可直接实现 VPN 下的子网互通功能;
- ▶ 使能 ping:实时 VPN 在线检测及重连机制。默认未启用。打勾代表 ping 失败将重连 VPN;
- > L2TP 连接成功:完成相关参数的填入后,保存&应用,进入到 VPN--VPN 状态处查看连接状态。



5.3. IPSec

				中文 English
	IPSec 参数			· · · · · · · · · · · · · · · · · · ·
USR-G810	IPSec	● 开启 ○ 禁用		
	接口	自动	•	
> 状态		(a) '自动'表示使用默认路由	白接口连接	
> 服务	对端地址	192.168.0.2		
> 聚合网络		 IP地址/现名或者%any,eg: 	10.10.1.88, eg:%any	
> 网络	协商方法	主模式	~	
V VPN	隧道类型	子网到子网	·	
РРТР	本端子网	192.168.1.0/24		
L2TP		@ eg: 192.168.10.0/24		
IPSec	对端子网	192.168.55.0/24		
OpenVPN		eg: 192.168.20.0/24		
GRE	IKE加密算法	3DES	~	
VPN状态	IKE校验算法	MD5	v	
> 防火墙	Diffie-Hellman组	Group2(1024bits)	~	
> 系统		f manage		
> 退出	IKE生存时间	28800 28800 seconds		
	认证类型	预共享密钥	~	
				Ţ



<说明>

- ▶ 接口:根据联网方式的不同可选择 wan_4g1、wan_4g2、wan_wired、自动;
- ➢ 对端地址:可以分为 VPN 客户端和 VPN 服务器。填入对端的 IP/域名;
- 协商方式:主模式、积极模式(野蛮模式),默认主模式;
- 隧道类型:子网到子网、子网到主机、主机到子网、主机到主机。根据实际应用方式选择;
- > 本端子网: IPSec 本端子网及子网掩码;
- > 对端子网: IPSec 对端子网及子网掩码;
- ➤ 本端标识符:通道本端标识,可以为 IP 或 FQDN,注意在域名自定义名时加@;
- ▶ 对端标识符:通道对端标识,可以为 IP 或 FQDN,注意在域名自定义名时加@;
- ▶ IKE 的加密: 第一阶段包括 IKE 阶段的加密方式、完整性方案、DH 交换算法;
- ➢ IKE 生命周期:设置 IKE 的生命周期,单位为秒,默认:28800;
- ➢ IKE 加密算法: 3DES/AES-128/AES-192/AES-256;
- ➢ IKE 校验算法: SHA-1/SHA2-256/SHA2-512/MD5;
- Diffie-Hellman 组: Group1/2/5/14;
- 认证方式:目前支持预共享密钥的认证方式;
- ➢ ESP 加密:第二阶段包括 ESP 对应的加密方式、完整性方案;
- ➢ ESP 生命周期:设置 ESP 生命周期,单位为秒,默认:3600;
- ➢ ESP 加密算法: 3DES/AES-128/AES-192/AES-256;
- ▶ ESP 校验算法: SHA-1/SH2-256/MD5;
- 会话密钥向前加密(PFS): None/DH1/DH2/DH5;
- ➢ 启动 DPD 检测:当 DPD 声明对等点为死时,应该采取什么行动;
- > DPD 检测周期:设置连接检测(DPD)的时间间隔;
- ▶ DPD 超时时间:设置连接检测(DPD)超时时间;





▷ DPD 操作:设置连接检测的操作。包括重启、拆除、保持、无,默认重启;

> IPSec 连接成功:和对端通过 IPSec 连接成功后,进入到 VPN--VPN 状态处查看连接状态。

5.4. OpenVPN

启用 OpenVPN 搭建 VPN, 内部可选 TUN(路由模式)或 TAP(网桥模式):

				中文 English
	OpenvPN 参 <u>叙</u>			
USR-G810	OpenVPN	● 开启 ○ 禁用		
	拓扑	组网~		
> 状态	角色	客户端		
> 服务	14.57			
> 聚合网络	9742	UDP V		
> 网络	端口	1194		
V VPN	设备类型	TUN ~		
РРТР	OpenVPN服务地址	192.168.0.2		
L2TP	10 F	白动		
IPSec	381	 (2) '自动'表示使用默认路由接口连接 	ġ.	
OpenVPN	认证类型	证书 ~		
GRE	CA2T+2	洗择文件 未洗择文件		
VPN状态	CAILTS			
> 防火墙	CRT公开证书	123年又14 未23年又14		
> 系统	私钥	选择文件未选择文件		
〉退出	TLS密钥	选择文件未选择文件		
	NAT			
	中田Kaapaliya	1		

图 53 OpenVPN 启用设置界面

<u><说明></u>

- ▶ 设备类型:可选择 TUN(路由模式)或 TAP(网桥模式);
- ➢ 通道协议: UDP 或 TCP;
- 端口: OpenVPN 客户端的监听端口;
- ➢ VPN 服务器地址: OpenVPN 服务器的 IP/域名;
- ▶ 接口:根据联网方式的不同可选择 wan_4g1、wan_4g2、wan_wired、自动;
- CA 证书:服务器和客户端公共的 CA 证书;
- CRT 公开证书:客户端证书;
- 客户端私钥:客户端的密钥;
- TLS 认证密钥:安全传输层的认证密钥;
- ▶ 加密算法:无/Blowfish-128/DES-128/3DES-192/AES-128/AES-192/AES-256;
- ▶ 哈希算法:无/SHA1/SHA256/SHA512/MD5;
- ▶ 加密和哈希算法均需和 VPN 服务器保持一致;
- ▶ 使用 LZO 压缩: 启用或禁用传输数据使用 LZO 压缩;
- NAT 设置:该功能默认开启。当内容需要和外部通讯时,将内部地址替换成公用地址。关闭该项,则无法实现网络地址转换 功能;
- 启用 Keepalive: 默认启用, 默认配置为 keepalive 10 120。本项设置需和 VPN 服务器对应;
- > MTU 设置:设置通道的 MTU 值,默认 1500,本项设置需和 VPN 服务器对应;
- ➤ TLS 方式: tls-auth/tls-crypt;
- ▶ 使能 ping 功能:设定 Ping 检测的地址后,可以保证 vpn 在异常断开下进行重连;



- OpenVPN 连接成功:和 VPN 服务器连接成功后,进入到 VPN--VPN 状态处查看连接状态。
- ▶ 注意:
- ▶ 客户端与服务器连接前, CA 证书、客户端证书、客户端密钥、TLS 认证密钥, 这几个需要服务器提供;
- > 得到的证书文件后,将不同的证书内容分别添加到配置界面接口。
- 附: linux下 OpenVPN 服务端配置

```
port 1194
proto udp
dev tun
user nobody
group nogroup
persist-key
persist-tun
keepalive 10 120
topology subnet
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
push "redirect-gateway defl bypass-dhcp"
crl-verify crl.pem
ca ca.crt
cert server_Jz40qi4AWJnZuN8X.crt
key server_Jz40qi4AWJnZuN8X.crt
key server_Jz40qi4AWJnZuN8X.key
tls-auth tls-auth.key 0
dh dh.pem
auth SHA256
cipher AES-256-CBC
#tls-server
#tls-version-min 1.2
#tls-cipher TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
status openvpn.log
verb 3
```



5.5. GRE

USR-G810 GRE 设置	
> 状态 GRE 参数 GRE	
> 服务	● 开启 ○ 禁用
> 聚合网络 GRE名称	gre1
> 网络	Inused,eg: gre1
本地WAN IP	192.168.0.151
	192 168 0 10
hh h	10010101
L2TP 远端隧道IP	10.10.10.1
IPSec 20世界中的	192.168.55.0/24
OpenVPN	@ eg:192.168.1.0/24
GRE	10.10.10.2
V FINA AGA	255
防火墙	W 1~255
> 系统 MTU	1450
> 退出	600~1450
NAT	
使能ping	□ 👩 ping失败将重连VPN

图 55 GRE 基本配置



<说明>

- ➢ 远程地址:对端 GRE 的 WAN □ IP 地址;
- > 本端地址:本端的 wan_wired、5G 或者 STA 的地址,根据联网方式不同输入相应本段地址;
- ▶ 远端隧道地址:对端的 GRE 隧道 IP;
- 对端子网:对于设置子网掩码可以按照如下规定表示: 255.255.255.0 可以写成 IP/24、255.255.255.255 可以写成 IP/32。
 例如: 172.16.10.1/24,对应着 IP为 172.16.10.1,子网掩码为 255.255.255.0;
- ➤ 本端隧道 IP:本地 GRE 隧道 IP 地址;
- > NAT: 该功能默认开启。当内容需要和外部通讯时,将内部地址替换成公用地址。关闭该项,则无法实现网络地址转换功能;
- TTL 设置:设置 GRE 通道的 TTL,默认 255;
- ➢ 设置 MTU:设置 GRE 通道的 MTU,默认 1450。

6. 防火墙功能

6.1. 基本设置

默认两条防火墙规则。

										中文 Eng
TEST	基本设置									
	启用SYN-flood防御									
 > 状态 > 服务 	丢弃无效数据包									
> 聚合网络	入站数据	接受	~							
> 网络	出始数据	接受	~							
→ VPN → 防火墙	转发	接受	~							
基本设置										
端口转发	区域									
访问限制		区域⇒转发		入站数据	出站数据	转发	IP动态伪装	MSS钳制		
> 系統	lan	: lan: ﷺ ⇒ wan		接受 🖌	接受 🗸	接受 🗸			🛃 修改	
> 退出	wan: wan_wired: 📰 v	wan_4g1: 🗾 wan_4g2: 🗾	$\Rightarrow \left[ACCEPT \right]$	接受 🖌	接受 🖌	接受 🗸	2		🛃 修改	
			应用(呆存						

图 56 防火墙设置页面

<名词介绍>

- ➢ 入站:访问路由器 IP 的数据包;
- ➤ 出站:路由器 IP 要发出的包;
- ▶ 转发:接口之间的数据转发,不经过路由自身;
- > IP 动态伪装: 仅对 WAN 口与 5G 口有意义, 访问外网时 IP 地址的伪装;
- > MSS 钳制:限制报文 MSS 大小,一般是 1460。

<规则 1>

📌 🚛 🖞 👬 👫 👫 👫 👫

- ▶ LAN 口到有线 WAN 口的入站,以及转发,均为接受;
- ▶ 如果有数据包来自于 LAN 口,要去访问 WAN 口,那么本条规则允许数据包从 LAN 口转发到 WAN 口,这属于转发;
- ▶ 您也可以在 LAN 口下,打开路由器的网页,这属于"入站";
- ▶ 路由器自身去连接外网,比如同步时间,这属于"出站"。

<规则 2>

- ▶ 有线 WAN 口与 5G 口,接受"入站",接受"出站",允许"转发";
- ▶ 如果有"入站"数据包,比如有人打算从 WAN 口登录路由器网页,那么将会被允许;
- ▶ 如果有"出站"数据包,比如路由器通过 WAN 口或者 5G 口访问外网,此动作被允许;
- ▶ 如果有"转发"数据包,比如从 WAN 口来的数据包想转发到 LAN 口,此动作被允许。

6.2. 通信规则

通信规则可以选择性的过滤特定的 Internet 数据类型,以及阻止 Internet 访问请求,通过这些通信规则增强网络的安全性。 防火墙的应用范围很广,下面简单介绍下常见的几种应用。

名称	描述	默认参数
启用	显示 🧐 禁用 表示启用状态 显示 🗐 启用 表示禁用状态	启用
名字	此条规则名字,字符类型	-
限制地址	限制 IPv4 地址	仅 IPv4 地址
协议	限制规则的协议类型,可选择: TCP+UDP/TCP/UDP/ICMP	TCP+UDP
匹配 ICMP 类型	匹配的 ICMP 规则,选择 any 即可	Any
源区域	数据流源区域,可选择:任意区域,WAN,LAN LAN:表示子网访问外网规则 WAN:表示外网访问内网规则	LAN
源 MAC 地址	需要匹配规则的源 MAC 空:代表匹配所有 MAC 说明:匹配源 MAC 地址时需将源 IP 地址设置为空	空
源 IP 地址	需要匹配规则的源 IP 空:代表匹配所有 IP 说明:匹配源 IP 地址时需将源 MAC 地址设置为空	空
源端口	需要匹配规则的源端口 空:代表匹配所有端口	空
目标区域	数据流目标区域,可选择:任意区域,WAN,LAN LAN:表示子网访问外网规则 WAN:表示外网访问内网规则	WAN
目标地址	访问的目标 IP 地址 空:代表所有地址	空

表 17 通信规则参数表



目标端口	访问的目标端口号	空
	空:代表所有	
动作	接受到此类数据包可选择:丢弃,接受,拒绝,无动作	接受
	丢弃: 收到此规则数据包将丢弃	
	接受: 收到此规则数据包将接受	
	拒绝: 收到此规则数据包将拒绝	
	无动作: 收到此规则数据包将无动作	

6.2.1. IP 地址黑名单

首先在新建转发规则中输入规则的名字,然后点击"添加并编辑按钮"

TECT	名字	匹配规则	动作	开启 排序	
TEST > 状态	Allow- Ping	IPv4-ICMP 和 type echo-request 来目 所有主机位于 wan 到 所有語由地址位于本设备	Accept input		改善删除
> 服务	打开路由器端口:				
> 聚合网络	名字	协议 外部端□			
> VPN	新建进入规则	TCP+UDP 🗸			
∨ 防火墙					
基本设置	新建转发规则:				
端口转发	名字	源区域 目标区域	_		
通信规则	test	lan v wan v 🖻 添加并编辑			
50回版制 > 系统	Course NAT				
〉退出	Source NAT 名字	匹置法规则	_	动作	开启 排序
		尚无任何配置			
	1030				
	新班至Source NAT:				

图 57 防火墙黑名单图一

在跳转的页面中, 源区域选择 lan, 源 MAC 地址和源地址都选择所有 (如果是只限制局域网内的特定 IP 访问外网的特定 IP, 则此处需填写 IP 地址或是 MAC 地址), 如下图:





		中文 English
		<u>۸</u>
TEST	规则使能	◎ 禁用
	-	had
> 状态	5 7	
> 服务	限制地址	₹ZIPv4 ~
> 聚合网络	协议	TCP+UDP v
> 网络	匹表引CMD 幾年	any
> VPN	EBUCON	un y
> 防火墙	源区域	
基本设置		Ian:
端口转发		O wan: wan_wired: 👷 wan_4g1: 🧝 wan_4g2: 👰
通信规则		
访问限制	源MAC地址	
> 系统		Reserved Origination/Inco (Higoday 1)
> 退出	源地址	192.168.2.133 · · · · · · · · · · · · · · · · · ·
	3年3第二	7:19 第二次の時期には、1000年間の前期には、1000年間の前期に、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期に、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期には、1000年間の前期に
	目标区域	0 195 (44))
	and SURE200	

图 58 防火墙黑名单图二

在目标区域选择 WAN,目标地址填写禁止访问的 IP,动作选择"拒绝"设置完成后,点击"应用"。如下图。

		中文 English
		◎ 需要匹配入站流量的源MACs (可以为多个)
IEST	源地址	192.168.2.133
		② 需要匹配入站流量的源P-动P范围
> 状态	海洋口	所有
> 服务	i - Tursiow	《 需要匹配入站流量的源端口或端口范围
》聚合网络	日短区は	
网络		○ 设备(输入)
Mari		○ 任意区域(转发)
> VPN		O lan: lan: 🖤
◇ 防火墙		
基本设置		wan: wan_wired: wan_4g1: wan_4g2:
端口转发	目标挑計	所有 Y
通信规则		@ 重定向匹配的人站流量到的内部主机
访问限制	目标端口	所有
> 系统		◎ 重定向匹配的人站流星到内部主机的端口
> 退出	动作	拒绝
	📄 返回至概況	应用 保存
		Y

图 59 防火墙黑名单图三



	名字	p	匹税则		动作	开启 排序	
TEST							
	Allow-	IPv4-ICMP 和 来自 所] type <i>echo-request</i> 有主机位于 wan		Accept input	eg 🔹 🔹 📝	修改 🔊 删除
> 状态	Ping	到 <i>所有路</i> 。	由地址位于本设备				(.
> 服务		IPv-	4-TCP,UDP		Defens forward		14734 D 00160
> 聚合网络	test	米目 IP 192 到 所有	.168.2.133 位于 Ian 注机位于 wan		Refuse forward		15°DX 🗾 1100pt
> 网络	LTTTR: L WALCO						
VPN	打开路田 都 端口:						
防火墙	*A-7-	19MX	外的面上				
基本设置	新建进入规则	TCP+UDP	~	1	际力口		
端口转发							
通信规则	新建转发规则:						
访问限制	名字	源区域	目标区域				
系统	新建转发规则	lan	Ƴ wan	✓ ☑ 添加并编辑			
退出							
	Source NAT						
	名字		匹配规则			动作	开启 排序
				※平江(司憲)業			

图 60 防火墙黑名单图四

这样设置完成后,就实现了黑名单的功能。即实现子网设备 IP 为 192.168.2.133 的 IP 禁止访问所有外网。

6.2.2. IP 地址白名单

首先添加要加入白名单的 IP 或 MAC 地址的通信规则,在新建转发规则中输入规则的名字,然后点击"添加并编辑按钮"。

	名字	区面出现现	动作	开启 排序	
TEST _{状态}	Allow- Ping	IPv4-ICMP 和 type echo-request 来目 所有差別 位于 wan 到 所有語曲地址 位于本设备	Accept input		修改 💌 删除
员务	打开路由器端口:				
聚合网络	名字	协议 外部端口			
网络					
VPN	新建进入规则	TCP+UDP V	500		
防火墙					
基本设置	新建转发规则:				
端口转发	名字	源区域 目标区域			
通信规则	test	lan v wan v 🖻 添加并编辑			
系统	Course NAT				
退出	Source NAI	11. 51 to 01		-b/w	
	AT.	V -Dac/ARAD		5/J11F	开启 排序
		尚无任何配置			
	新建Source NAT:				

图 61 防火墙白名单图一

在跳转的页面中, 源区域选择 lan, 源 MAC 地址和源地址都选择所有(如果是允许局域网内的特定 IP 访问外网的特定 IP, 则此处需填写 IP 地址或是 MAC 地址), 如下图





		中文 English
TEST		
	我也可以使用品	
> 状态	名字	test
> 服务	限制地址	₫IPν4 ∽
> 聚合网络	协议	TCP+UDP v
> 网络	LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL	
> VPN	EBUCON	un y
∨ 防火墙	源区域	〇 任章区域
基本设置		Ian:
端口转发		O wan: wan_wired: 👷 wan_4g1: 🔔 wan_4g2: 🛃
通信规则		
访问限制	源MAC地址	所有 ② 需要匹配入站流單的網MACs (可以为多个)
> 系统	2004 Later	103 468 3 422
> 退出	2442342	192.160.2.153 @ 需要匹配入法流量的潮P动户范围
	源端口	所有
		② 需要匹配人均流量的骤端口前满口范围
	目标区域	〇 设路 (输入)

图 62 防火墙白名单图二

在目标区域选择 WAN,目标地址填写允许访问的 IP,动作选择"接受"设置完成后,点击"保存并应用"。如下图。

		中文 English
TEST	 ◎ 需要匹配入38流型分類MACs(可以35多个) // 第時地計 / 192,165,2,133 	
 > 状态 > 距条 	 (2) 務務理(2012.) とお前、借金が期(2016) (第5) (第5) (第5) (第5) (第5) (第5) (第5) (第5)	
 聚合网络 > 网络 	目标区域 ○ 设备(输入) ○ 打意区域 (毛友)	
 > VPN > 防火墙 基本设置 	 Ian: generation in the second seco	
端口转发通信规则	目标地址 所有 。 《 重加回匹莱约入A4的建到的内部主机	
> 系统> 退出	目标编印 所行 ④ 重加的匹配的人为处理量的内部主印的编口 初作 接受 ✓	
	● 返回至輕況	
		Ť

图 63 防火墙白名单图三

接下来再设置一条所有的通信都拒绝的规则, 源地址设置为"所有", 目标地址设置为"所有", 动作选择"拒绝"。注意 两条规则的先后顺序, 一定是允许的规则在前, 拒绝的规则在后。总体设置完成后如下图



中文 | English

ESI	防火墙 - 通信规则	l.				
大态	通信规则定义了不同证 Source NAT是一种特	K域间的流量传送,例如:拒绝一些主机之间的通信、排 殊形式的封包伪装,它允许精细的控制传出流量的源时	丁开到WAN的端口。 ,例如,将多个WAN地址映射到	则内部子网。		
6务 SAmto	通信规则					
	名字	匹配规则	动作	开启	排序	
· /PN 方火墙	Allow- Ping	IPv4-ICMP和 type echo-request 来目 所有主机位于wan 到 所有路由地址位于本设备	Accept inpu	rt 🖸	•	✓ 修改 ■ 删除
→ 以直 端口转发 重信规则	test	IPv4-TCP,UDP 来自 IP <i>192.168.2.133</i> 位于 Ian 到 <i>所有主机</i> 位于 wan	Accept forwa	rd 🗹	•	🖉 修改 💌 删除
方问限制	-	IPv4-TCP,UDP 来自 <i>所有主机</i> 位于 <i>Ian</i> 到 <i>所有主机</i> 位于 <i>wan</i>	Refuse forwa	rd 🗹	• •	🖉 修改 💌 删除
昆出	打开路由器端口:					
	名字	协议 外部端口				
	新建进入规则	TCP+UDP 🗸	1 添加			

图 64 防火墙白名单图三

<说明>

- ▶ 最多可添加 20 条通信规则。
- 6.3. NAT 功能

6.3.1. IP 地址伪装

IP 地址伪装, 将离开数据包的源 IP 转换成路由器某个接口的 IP 地址, 如图勾选 IP 动态伪装, 系统会将流出路由器的数据 包的源 IP 地址修改为 WAN 口的 IP 地址。

注意:WAN 接口必须开启 IP 动态伪装和 MSS 钳制, lan 接口禁止开启 IP 动态伪装和 MSS 钳制。



.



T 基本设置
基本设置
启用SYN-floor(防御 2
入 法 数据 接受 く
出始数据接受
報发 接受 ◆
_定
区域→转发 入站数据 出站数据 转发 IP初态伪装 MSS钳制
wan: wan_wired: 要 wan_4g1: 是 wan_4g2: 是 ⇒ ACCEPT 接受 ∨ 接受 ∨ 接受 ∨ ☑ ☑ ☑ 修改
应用 · 保存

图 65 IP 地址伪装设置

6.3.2. SNAT

名称	描述	默认参数
启用按钮	显示 《 禁用 表示启用状态 显示 》 启用 表示禁用状态	启用
名字	此条防火墙规则的名称	-
协议	可设置: TCP+UDP/TCP/UDP/ICMP	TCP+UDP
源 IP 地址	需要匹配入站流量的源 IP 例如一个 IP:192.168.1.100 为空表示匹配所有源 IP	空
源端口	需要匹配入站流量的源端口 例如一个端口:9999 为空表示匹配所有源端口	空
目标 IP	需要匹配入站流量的目标 IP 例如一个 IP:192.168.2.100 为空表示匹配所有目标 IP	空
目标端口	需要匹配入站流量的目标端口 例如一个端口:9999 为空表示匹配所目标端口	空
SNAT IP 地址	将匹配流量的源地址改成此地址	添加时自定义的 IP

表 18 SNAT 参数表



SNAT 端口

将匹配流量的源端口改为此端口 为空表示使用源端口 空

Source NAT 是一种特殊形式的封包伪装,改变离开路由器数据包的源地址,使用时首先将 wan 口的 IP 动态伪装关闭

TEST						TXT English
TEST 基本位置 ● 技术 単成 ● 技术 ● 展示 ● 展示 ● 展示 ● 原示 ● 原示 ● 原示 ● 原示 ● 原示 ● 原示						
131 ENISTING CostSHE 2 55 ENISTING CostSHE		基本设置				
A the is probable is proba	IESI					
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	*44	后用SYN-flood防御				
· · · · · · · · · · · · · · · · · · ·	1/Jon 18-48-	丢弃无效数据包				I
> NK > NK > KK > KK > BK BK BK BK BK BK BK BK BK BK BK BK BK BK	聚合网络	入站数据	接受 🗸			
* VN #20 #20 * * KK #20 #20 * * KK #20 #20 * * KK * KK	> 网络	出站数据	接受 🗸			
● が火油 ● 広花 ● 広信	> VPN	转发	接受 🗸			
● 林说用 ● 「「「」」」」」 ● 「「」」」」 ● 「「」」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● □」 ● □」 ● □」 ● □」 ● □」 ● □」 ● □」	> 防火墙					
Implify Implify Implify Implify <t< td=""><td>基本设置</td><td></td><td></td><td></td><td></td><td></td></t<>	基本设置					
通信規则 访问限制 <td>端口转发</td> <td>区域</td> <td></td> <td></td> <td></td> <td></td>	端口转发	区域				
第純 通出 ● Watt wan_wired: 愛 wan_4g2: ② ● ACCEPT ● 愛 ● 愛 ● 愛 ● @ ● @ @ @ @ 第冊 ● Watt ● Watt wan_wired: 愛 wan_4g2: ② ● ACCEPT ● 愛 ● 愛 ● @ ● @ @ @ ● Matt wan_wired: 愛 wan_4g2: ② ● ACCEPT ● 愛 ● @ @ ● @ @ ★后设置 Source NAT #xx [English	通信规则		区域 ⇒ 转发	入站数据 出站数据 转发	IP动态伪装 MSS钳制	
> 新航	访问限制	lan	: lan: *** ⇒ wan	花泉 へ 花泉 く 花沢 く		
》 提出 Want: Wan.wired: 愛 Wan.4g1: @ Wan.4g2: @ = ACCEPT 按弦 ★ 接弦 ★ 接弦 ★ 正 ▲ 体弦 MH G47 太后设置 Source NAT #文 [English TEST	> 系统					
★后设置 Source NAT #文 English	〉退出	wan: wan_wired: 🕎 v	wan_4g1: 🛃 wan_4g2: 🛃 ⇒ ACCEPT	接受 > 接受 > 接受 >	□	
★后设置 Source NAT #文 English						
朱后设置 Source NAT #文 English			应用	保存		
★后设置 Source NAT #文 English TEST						
大后设置 Source NAT 中文 English TEST						·
朱后设置 Source NAT 中文 English TEST						
中文 English TEST	然后设置 Source NAT	Г — — — — — — — — — — — — — — — — — — —				
新能地入规则 TCP+UDP マ						中文 English
新設法入规则 TCP+UDP V 2 添加 A						
新建进入规则 TCP+UDP V 2 添加						
	TEST	新建进入规则	TCP+UDP V	~ 添加		*

IESI			
	杂衍建性与发现则 :		
状态	名字 源区域 目标区域		
服务			
聚合网络			
> 网络			
VPN	Source NAT		
/ 防火墙	名字	动作	开启 排序
基本设置			
端口转发	尚无任何配置		
通信规则			
访问限制	额建Source NAT:		
系统	名字 源区域 目标区域 到源IP 到源端口		
退出	test lan v wan v 192.168.9.1 v 不填写= (角	所有端口) 💽 添加好	+编辑
	<u> </u> 应用 供		

图 66 NAT 设置一

点击添加并编辑



		中文 English
		A
TEST	协议	ICMP 👻
	源区域	Ian: lan: 整整
> 状态		○ wan: wan_wired: 🕎 wan_4g1: 🤔 wan_4g2: 🤔
服务		
> 网络	源旧地址	所有 素要匹配入
> VPN	源端口	所有
∨ 防火墙		新要UEC人站流量的源端口或端口范围
基本设置	目标区域	O lan: lan: 📰
端口转发		🖲 wan: wan_wired: 🕎 wan_4g1: 🚑 wan_4g2: 🚑
通信规则	目标IP#地址	
访问限制		自病Pa以P范围 日前Pa以P范围
》 乐班	目标端口	所有 日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本
18th		
	SNAT IP地址	192.168.9.1 · · · · · · · · · · · · · · · · · · ·
	SNAT 端口	不填写= (所有端口)
		 将四弦流量的源就口波写成指定进口。也可以留空,只次写P地址。

图 67 NAT 设置二

若源 IP、源端口和目的 IP、目的端口不填,默认所有 ip 与端口。设置完之后保存。

TEST 新建进入规则 TCP+UDP V 简 添加
> 状态 航建转发规则:
> 服务 名字 源区域 目标区域
> 聚合网络 新建转发现则 lan ▼ wan ▼ ● 添加并编辑…
→ 网络
> VPN Source NAT
> 防火墙
端口转发 任何交通 源地址次写成 IP 東 ・ 2 修改 w 細陸
通信初期 到 所有主的位于 wan 192.168.9.1 ■ 192.4 (8.9.1
新建Source NAT:
名字 源区域 目标区域 到期中 到源满口
新建SNAT规则 Ian v wan v - 満选择 - v 不填写=(所有端口) 通 添加并编辑
ALCH TANT

图 68 NAT 设置三

如图将离开路由器的数据包的源 IP 地址改变为 192.168.9.1,如图可以看到,到 192.168.13.4 的 ICMP 包的源地址是 192.168.9.1,而不是 192.168.1.114。

验证用路由器下的设备(IP:192.168.1.114)ping 与路由器在同一个交换机下的 PC(IP:192.168.13.4), 在 PC 上抓包的数据 如下:



过滤:	ip.addr == 1	92.168.13.4		▼ 表达式	清除 应用		
No.	Time	Source	Destination	Protocol	Info		
	1 0.000000	192. 168. 13. 4	220. 195. 22. 209	TCP	50379 > http [FIN, A	CK] Seq=1 Ack=1 Win=64708 Len=0	
	2 0. 689352	192. 168. 9. 1	192. 168. 13. 4	ICMP	Echo (ping) request	(id=0x1d3c, seq(be/le)=57/14592,	ttl=64)
	3 0. 689426	192. 168. 13. 4	192. 168. 9. 1	ICMP	Echo (ping) reply	(id=0x1d3c, seq(be/le)=57/14592,	ttl=128)
	6 1.689615	192. 168. 9. 1	192. 168. 13. 4	ICMP	Echo (ping) request	(id=0x1d3c, seq(be/le)=58/14848,	ttl=64)
	7 1.689687	192. 168. 13. 4	192. 168. 9. 1	ICMP	Echo (ping) reply	(id=0x1d3c, seq(be/le)=58/14848,	ttl=128)
	8 1.823459	192. 168. 18. 4	192. 168. 4. 69	<u>SMD2</u>	Create Request File.		
	9 1.825746	192. 168. 4. 63	192. 168. 13. 4	SMB2	Create Response File	: · · · · · · · · · · · · · · · · · · ·	
	0 1.826091	192. 168. 13. 4	192. 168. 4. 63	SMB2	Create Request File:		

<说明>

▶ 最多可添加 20 条 SNAT 规则。

6.3.3. 端口转发

端口转发允许来自 Internet 的计算机访问私有局域网内的计算机或服务, 即将 WAN 口地址的一个指定端口映射到内网的一台主机。

内容 第二目地 2013日期10月前4 有局域网内的计算机或服务 第二日本2013日期 第文型 第二日本2013日期 第文型 第二日本2013日期 第文型 第二日本2013日期 第文型 第二日本2013日期 第文型 第二日本2013日期 第文型 第二日本2013日期 第二日本2013日期 第二日本2013日 第二日本2013日期 第二日本2013日 第二日本2013日第三日本2013日 第二日本2013日 第二日本2013日 第二日本2013日	TEST	防火墙 - 端口知	\$ \$		
第合网络 医学 医型 化 学校组 作程 他 中 中 中 中 中 中 中 中 中 中 中 中 中 中 中 中 中 中	状态	端口转发允许来自 端口转发	internet的计算机访问私有周城网内的计算机或服务		
▼ 防火塩 基本设置 端口转发 諸信規则 访问限制 ● 系统 選出	> 聚合网络 > 网络 > VPN	名字	U-TA-24000	转发到	开启 排序
	防火墙 基本设置 端口结发	新建端口转发:		0927542 03204H5 09294C	
> 終航 2 週出 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	通信规则	test	TCP+UDP v wan v 81	lan ∨ 192.168.2.1 ∨ 80	🎦 添加
	 > 糸統 > 退出 		应用	B (Biter	

图 70 端口设置页面一

<说明>

- 设置好转发规则后,需要点击右侧的添加按钮,然后本条规则会显示在规则栏内;
- 然后点击右下角的"应用"按钮,使设置生效;
- 以下的设置,192.168.2.1:80为路由器自身的网页服务器。如果我们想从外网去访问局域网内的某个设备,那么需要设置 外网到内网的映射,比如设置外网端口为 81,内网 IP 为 192.168.2.1,内网端口为 80;
- ▶ 当我们从 WAN 口访问 81 端口时,访问请求将会被转移到 192.168.2.1:80 上面。



TEST	防火墙 - 端口	转发		
dhata	端口转发允许来自	自Internet的计算机访问私有局域网内的计算机或服务		
2 次念	港口社会			
聚合网络		匹百法规则	转发到开	合 排序
网络				
> VPN	test	IPv4-TCP, UDP 来自 <i>所有主机</i> 位于 wan	IP 192.168.2.1. port 80 位于 lan	
防火墙		通过 所有路由地址 at port 81	· · · · · · · · · · · · · · · · · · ·	
基本设置				
端口转发	新建端口转发:			
通信规则	名字	协议 外部区域外部端口	内部区域 内部IP地址 内部端口	
访问限制	新建端口转发	TCP+UDP 🖌 wan 🖌	lan 🗸 🗸	🎦 添加
系统				
〉退出				
		λ <u>ν</u> .	用【保存】	

图 71 端口设置页面二

表 19 端口转发参数表

名称	描述	默认参数
名字	此条端口转发规则名称,字符类型	空
协议	协议类型,可设置:TCP+UDP/TCP/UDP	TCP+UDP
外部区域	包括有线 wan、5G、VPN、STA	wan
外部端口	可设置端口范围,例如:8000-9000	空
	说明:当外部端口以及内部端口为空时为 DMZ 功能	
内部区域	路由器子网区域	lan
内部 IP	路由器 LAN 区域 IP 地址	空
内部端口	可设置端口范围,例如:8000-9000	空
	说明:当外部端口以及内部端口为空时为 DMZ 功能	

<说明>

▶ 最多可添加 20 条端口转发规则。

6.3.4. NAT DMZ

端口映射是将 WAN 口地址的一个指定端口映射到内网的一台主机, DMZ 功能是将 WAN 口地址的所有端口都映射到一个主机上, 设置界面和端口转发在同一个界面, 设置时外部端口不填, 点击"添加"即可。





TEST 防火墙 - 端口转发 端口转发允许来自Internet的计算机访问私有局域网内的计算机或服务 状态 服务 端口转发 聚合网络 名字 匹配规则 转发到 开启 排序 网络 VPN 尚无任何配置 基本设置 新建端口转发: 端口转发 名字 外部区域外部端口 内部区域 内部IP地址 内部端口 协议 通信规则 1 添加 新建端口转发 TCP+UDP ₩ 192.168.2.1 Ƴ wan 访问限制 系统 应用 保存 〉退出 无需设置

图 72 DMZ 设置一

TEST な な た な た な た な た な た た は し た た た し た た し た し た し た し た し た し た し た し た し た し た し し し し た し し た し し た し し た し し た し し た し し た し し た し し た し し た し し た し し た し し し し し し し し し し し し し					
TEST KK KK </th <th></th> <th></th> <th></th> <th></th> <th></th>					
Itsi KKa KKa <th></th> <td></td> <td></td> <td></td> <td></td>					
第二日総券抗学株値Internetishi 算机以前時机構構構成例的設計算机成器分 第26 网络 第26 网络 内容 VPN 第26 個名 第26 個名 第26 個名 第27 回日総合、(194-102, UDP) 第28 所得描述地位 第28 所得描述地位 第28 個名 第18 所得描述地位 第18 所有法 第18 所得描述地位 第18 所得描述地位 第18 所用	IESI	防火墙 - 端口	转发		
加合 加合 加合 第合 加合 加合 <	d N-de-	端口转发允许来问	自Internet的计算机访问私有局域网内的计算机或服务		
加合 1422 加合 1422 第合 网络 名字 通知 (新 4 年 4 年 4 年 4 年 4 年 4 年 4 年 4 年 4 年 4	- 天心 - 昭年	进口结告			
対化 IPA-1CP, UDP IP 192.168.2.1位于 Ian ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	影合网络	300日代文 名字	匹配规则	转发到	开启 排序
VPN IP4-TCP, UDP #IB ######20/GF wan BdJ.####################################	> 网络				
防火信 通ご 所務額地地址 正 いいいいい いいいいいいいいいいいいいいいいいいいいいいいいいいいいいい	> VPN		IPv4-TCP, UDP 来自 <i>所有主机</i> 位于 wan	IP 192.168.2.1 位于 Ian	
第注第二件经 所建第二件经: 下本 物文 外部区域 外部時回 内部区域 内部時間回 の前 第2 第3 第3 <td< td=""><th>∨ 防火墙</th><td></td><td>通过 所有路由地址</td><td></td><td></td></td<>	∨ 防火墙		通过 所有路由地址		
第日转送 第日转送 第日第三年後: 第日第三年8日第三年8日第三年8日第三年8日第三年8日第三年8日第三年8日第三年	基本设置				
通信規則 名字 协议 外韶区域 外韶端口 内韶域 内阁中地址 内韶端口 访问限制 新诺德口经过 TCP+UDP v van v Ian v v 通 添加 選出 近川 《文字	端口转发	新建端口转发:			
访问限制 新建論□142 TCP+UDP v van v lan v v 微微 微微 系统 追出 成別 保存	通信规则	名字	协议 外部区域外部端口	内部区域 内部IP地址 内部	尚口
系统 退出 取用 保存	访问限制	新建端口转发	TCP+UDP 🖌 wan 🖌	lan 🗸 🗸	🎦 添加
退出 (好存)	系统				
	> 退出				
			AV.		

图 73 DMZ 设置二

如图, WAN 口地址的所有端口都映射到内网 192.168.2.133 这台主机上。

<u><注意></u>

- 端口映射和 DMZ 功能不能同时使用;
- DMZ 功能仅可建立一条规则使用。

6.4. 访问限制

访问限制实现对指定域名的访问限制,支持域名地址的黑名单和白名单设置,选择黑名单时,连接路由器的设备无法访问黑





名单的域名,其它域名地址可以正常访问,选择白名单时,连接路由器的设备除白名单设置的域名地址可以访问外,其它域名地址都不能够正常访问,黑名单和白名单都可以设置多条,此功能默认关闭。

6.4.1. 域名黑名单

首先,在方式选项中选择黑名单,点击添加输入该条规则的名称和正确的域名,然后点击报保存,规则立即生效,连接路由器的设备将无法访问该域名。如果选择黑名单,而未添加规则,默认黑名单为空,即所有域名都可以访问。如图,除百度外,其他域名均可以正常访问。

		中文 Engli
TEST	访问限制	
、华杰	宽松匹配模式,主要限制网页等数据。不支持主机名的访问限制,输入域名关键字,如:baidu.com。	
1/1/201	2 2 3 3	
> 聚合网络		
> 网络	方式 黒名単 ・	
> VPN		
∨ 防火墙	名称 域名 开启	
基本设置		
端口转发	test1 baidu.com 💟 💌 删除	
通信规则		
初門財政制	約(建防火)帶規則:	
》退出	名称	
ACTION	新建规则	
	应用 保存	

图 74 域名黑名单

6.4.2. 域名白名单

首先,在方式选项中选择白名单,点击添加输入该条规则的名称和正确的域名,然后点击报保存,规则立即生效,连接路由器的设备除规则中的域名可以访问外,其他域名都不能够访问。如果选择白名单,而未添加规则,默认白名单为空,即所有域名都不能够访问。如图,设备能够访问百度。



TEST	访问限制			
	宽松匹配模式,主要限制网页等数	居。不支持主机名的访问限制,输入域名:	关键字, 如: baidu.com。	
状态				
服务	配置			
聚合网络	方式	1名単 🖌		
网络 MPN				
VPN Phaluta				
基本沿電	名称	域名	开启	
端门转发	tort1	baidu com		- mite
通信规则	testi	baldu.com		Trainin N
访问限制	众元之为史之、七八中之间 前川。			
系统	evizeral A reverse.	zŧk	10°2	
退出	-	240		
	新建城			添加
		应	保存	

图 75 域名白名单

<说明>

- 最多可添加 20 条访问限制规则。
- 7. 高级服务

7.1. 云服务

路由器远程管理平台服务地址:路由器远程管理平台,可以将路由器设备在路由器远程管理平台进行:监控、控制、批量配置、 统计、硬件断电报警等高效率、统一化的管理。

<说明>

- USR-G810-33 默认未开启云服务功能。路由器 Web 界面可以配置统计流量、网络状态、心跳包的上报参数;同时支持数据 上报到私有部署。
- ▶ 设备如需上路由器管理平台,请将私有化部署勾选,并设置私有云设备接入地址: 106.14.191.33,端口设置: 7100;
- ▶ 请登录路由器远程管理平台,注册账号,添加设备后管理。



		中文 English
	1000000000000000000000000000000000000	
TEST		1
	配置	l .
> 状态	流量记录时间(分钟) 10	
∨ 服务	◎ 受買时长不可大于12小时	
云服务	流量上版时间(分钟) 30	
动态DNS	₩ 経営的水中以大「12191日本日大」407100000000	
> 聚合网络	网络状态记录时间(分钟) 5 ② 设置时长不可大于12小时	
> 网络		
> VPN	 P3-487-V34-Linke-JP3 (217) ② 设置时长不可大于12小时且不可大于40个网络块态统计周期 	
> 防火墙	在國心戰包開開 30秒 🖌	
> 系统		
> 退出		
	UDP配置	1 1
	UDP心跳起周期 20秒	
	私有化部署	i I
	使用私有部署的云服务 🛛	
	私有云设备接入统计 106.14.191.33	
	HE 7100	
	2011 V100	Ŧ

图 76 USR-G810-33 有人云服务界面

7.1.1. 监控大屏

监测大屏,可以按照项目以及设备系列展示设备在线情况、位置信息等信息。



图 77 监测中心



7.1.2. 设备管理

7.1.2.1. 添加设备

点击"添加设备"

ē	大屏管理	~	设备管理	> 联网设备	÷							
୯	设备管理	^	联网设	备								
[联网设备		请选择	單组织		01600322093000000	请选择设备状态 🛛 🗸	请选择标签	→ 查询	添加设备 启用设备 禁用设备	批量删除	高级设置
	变量模板			设备状态		设备名称	SN	设备型号	所属组织	设备地址	启用状态	标签
₫	报警联动	~		在线		TEST	01600322093000000128	USR-G810	根组织	山东省济南市历下区龙奥南路		
ш	数据中心	~									_	
∞	设备运维	~ -								共1条 10条/页 × <	1 〉前往	1 页
		<										
	V1.0.0											

图 78 有人云—添加设备界面一

USR-G810-33 出厂标签上提供设备的 MAC、SN;有人云添加设备时需要填入这些参数。

ē	大屏管理	~	设备管理 > 联网设备 > 添加设备
୯	设备管理	^	添加设备 批量添加设备
	联网设备		
	交量模板		基本信息
≞	报警联动	~	• 设备合称 未命名_设备名称_33 上传图片
<u>111</u>	数据中心	~	* 所篇组织 前选修组织 ~
Æ	设备运维	~	仪支持ipg、gif、png楷式;大小为6Mi以内
		Ĩ	*SN 時能入 SN SN不支持,点这里
			* MAC / IMEI ② 诺给入MAC/IMEI/NID码
			设备配置
			· 交量模板/透传 送播模板 送播模板 ○ 自动定位 ○ 自动定位
			网络监测 🚺 设备地图 山东督济南市历下区龙奥南路 地图
	V1.0.0		

图 79 有人云—添加设备

表 20 有人云添加设备参数表

名称	描述	默认参数
	I	



设备名称	给此设备设置一个名称,必填项	未命名_设备名称_XX
所属组织	设备所属于的分组,可作为设备查询筛选项,必选项	无
	例如:此设备属于山东-济南	
SN	设备 SN 号,必填项	无
	路由器可通过查看小标签 SN 填入	
MAC/IMEI	可通过田 MAC/IMEI/NID,必填项	无
	路由器可通过查看小标签 MAC 或者 IMEI 填入	
变量模板/透传	可设置变量模板	无
网络监测	开启:网络监测开启	开启
	关闭: 将不再监测此设备	
上传图片	可以上传设备或者现场图片	无
设备标签	可以给此设备设置标签,可通过标签筛选同一标签设备	无
设备位置	手动定位: 可通过"设备地图"设置此设备的具体位置	手动定位
	自动定位:需要设备支持基站定位或 GPS 定位功能	
设备地图	可手动设置设备具体位置	山东省济南市历下区龙奥南
		路

<说明>

设备亦可批量添加,需按照指定格式将信息填写正确;

- ▶ 批量添加模板可在批量添加设备处"下载 Excel 模板";
- ▶ USR-G810-33 不支持基站和 GPS 定位,如需支持需沟通定制。

7.1.2.2. 数据查看

在"设备管理"-"联网设备"-"设备列表"下,找到相应设备,点击"数据查看"可查看设备基本信息。

2	大屏管理	~	设备管理 > 联网设备 > 数据查看			í
୯	设备管理	^	设备概况 连接用户			I
	联网设备		设备信息		设备地图	I
	变量模板		TEST			I
≞	报警联动	~	016003220930	00000128		I
ш	数据中心	~	所屋组织: 设备型号:	根组织 USR-G810		l
Ð	设备运维	~ ~	面件扳本: 空量模板 设备地址: 标选:	V1.0.11.4g.06 山东省济南市历下区龙奥南路	◎ 2223 Baidu - GS(2021)6026号 - 甲则资学11111342 - 东ICP证030173	
			变量概况			I
			请选择从机	> 请输入变	品名称音向 雪海	I
					该设备没有变量	
	V1.0.0					
				医 20	有人二一物坦本毛	

图 80 有人云—数据查看





7.1.2.3. 设备运维

在	"设备管	理"-	- "毦	关网设备"	-"设备运维	挂"下,找到 [;]	相应设备,	点击"设备运约	隹"可查看设备	基本信息	以及发	送 AT 团	記置。	
	大屏管理	~	设备管	理 > 联网设备										
୯	设备管理	^	联网词	段备										
	联网设备		请送	「「「「」」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」	01600322093000000	请选择设备状态 >	请选择标签 ·	~ 音调	添加设备	i 启用设备	禁用设备	批量靜除	高级设置	
	交量模板			设备状态	设备名称	SN	设备型号	所属组织	设备地址	启用状态	标签	操作		
Ē	报警联动	Ň		在线	TEST	01600322093000000128	USR-G810	根组织	山东省济南市历下区龙奥南路			数据查看	设备运维	8
<u>111</u>	数据中心	Ň	_							共1条 10条/页	× < 1	> 前往	1 页	
Ð	设备运维	~												
		<												
	V1.0.0	100												
						图 81	有人	云—设备运维						

7.1.2.4. 设备概况

1 12	旦省以	. щ з	三坐中口心	, xiei	-//J/.				
2	大屏管理	~	设备管理 > 联网设备	> 设备运维					
G	设备管理	^	设备概况	数据调试	参数配置				
١	联网设备		设备信息						
	变量模板		-	TEST					
≞	报警联动	~		01600322093000	000128				
al	数据中心	~	F	所属组织	根组织	设备型号:	USR-G810	电池电量:	-
_			ì	设备模板: 辺をまままと	-	MAC:	D4AD20428AA7	ICCID_1网络类型	2 -
÷	设备运维	~	1	标签:	MARKING THE WART T REPARAMENT	IMEL_1:	867018061355230	ICCID_2内由史生	
			i l			ICCID_1:	=,	ICCID_2信号强度	12 极强
		<				ICCID_2:	89860122801405773834		
						面件版本: 硬件版本:	V1.0.11.4g.06		
			设备流量监测 ② 2023-05-11 10	6:19:04 至 2	023-05-12 16:19:04 查询				
			字节数/kb 210			-0-1	ccid1 -O- iccid2		
			180						
	V1.0.0		150						0

可以查看设备一些基本信息,如图所示:

图 82 设备概况

<说明>



> 设备如使用 SIM 卡上网,设备流量监测和信号质量监测将生效。

7.1.2.5. 参数配置

在参数配置界面,可以输入 AT 指令来进行配置设备的某些参数,或者读取设备的某些参数,并且参数的返回也会显示在平台上面。本款路由器支持批量可视化配置以及远程打开内置网页,无需复杂的 AT 配置查看路由器参数。

ē	大屏管理	 · ·	理 〉 联网词	268 > 设备运维										
Ċ	设备管理	~ 设备	概况	数据调试	参数配置									
	联网设备	基	本信息											
	变量模板	ig	备名称: TES	т			设备编号: 0160	0032209 <mark>3000000</mark> 1	128					
₾	报警联动	~ 所	属组织: 根组 件版本: V1.0	织 .11.4g.06			设备型号: USR	-G810						
<u>ш</u>	数据中心	*	数调试											
	₩ <u>₽</u> ₩	× ×	① 日本	+VER V1 0 11 4	g 06	AT+VER 恢复出厂设置				5-				
	V1.0.0									发送				
							冬	83	参数配	置				

7.1.2.6. 配置网页

G810-33 支持有人云配置远程登录设备网页进行配置操作。

	大屏管理	~	设备管理 > 联网设备									
G	设备管理	^	联网设备									
	联网设备		请选择组织 ~	01600322093000000	请选择设备状态 🛛 🗸	请选择标签	➤ 查询	添加设备	a 启用设备	第用设备 批集	in the second	級设置
	变量模板		设备名称	SN	设备型号	所属组织	设备地址	启用状态	标签 操作			
₾	报警联动	~	TEST	01600322093000000128	USR-G810	根组织	山东省济南市历下区龙奥南路		数据查看	设备运输 编	编设备 更多	
<u>111</u>	数据中心	~										
ß	设备运维	~							共1条 10条/页	× < 1	配置网页	页
											重启设备	
											删除设备	
	V1.0.0	81										



	图 84 配置网页(一)	
C 【▲ 不安全 f230267034b9c61ae2351a4875b46d92f25170c6	lagdev.usr.cn:18000/cgi-bin/luci	A () 😘 🖆 🕼 🦉
TEST		中文 English
	需要授权	
	请输入用户名和密码。	
	用户名: root	
	密码:	
	登录 复位	
	图 85 配置网页(二)	

<u><说明></u>

- > 点击配置网页弹出本设备网页如上图,登录网页进行配置;
- > 如出现链接打不开内置网页情况请在有人云,选择对应设备的"配置网页"直接打开。
- 7.1.3. 报警联动

7.1.3.1. 配置报警联系人

2	大屏管理	~	报警联动 〉报警联系人							
୯	设备管理	~	联系人							
≞	报警联动	^	→ 講选择组织 ~ 単	系人姓名、手机号或邮箱		查询				添加 批星删除
	设备监测触发器		联系人姓名	所属组织	手机	自即百	备注	添加人	更新时间	操作
	报警配置					智无数据				
<u>ш</u>	数据中心	~						共0条 10条/页	~ 上一页 1	下一页前往 1 页
	设备运输	× ×								
					图 86	添加报警联系人	(-)			



3	入井昌珪	报警联动 > 报警联系人							
Ċ	设备管理 🗸 🗸	联系人							
≞	报警联动 へ	请选择组织 ~ 联系人姓名。手机	新增联系人			×			添加 批星删除
	设备监测触发器	联系人姓名 所属	•联系人姓名	test		关联用户	添加人	更新时间	操作
	报警配置								
	报警联系人		* 请选择组织	根组织					
Ш	数据中心 🗸			联系方式至少填写手机、邮箱的其中一种			共0条 10条/页	上一页 1	下一页前往 1 页
~	设备运维 🗸 🎽		手机	请输入手机号					
			手机验证码	请输入验证码	获取验证码				
			邮箱	清输入邮箱					
			邮箱验证码	请输入验证码	获取验证码				
			备注	谚脑入酱注					
					取消	保存			
	V1.0.0								
			冬	87 添加报警	联系人(二)			

7.1.3.2. 设置监控触发器

路由器出发什么条件会报警的配置界面。

ē	大屏管理	~	报警联动 > 设备监测触发器							
G	设备管理	~	设备监测触发器							
۵	报警联动	^	请选择组织 ~ 触	发器名称	请输入联网设备名称或SN		查询			添加 批星删除
	设备监测触发器		触发器名称	所属组织	关联设备数量	状态	创建人	更新时间	操作	
	报警配置		未命名_触发器名称_99	根组织	1		test	2023-03-24 10:43:02	查看 编辑 关联设备	删除
	报警联系人							#1条	10条/面 > 上一面	1 下一页 前往 1 页
<u>111</u>	数据中心	ř						20130		
R	设备运维	~ <mark>></mark> <								
		-								
	V1.0.0									

图 88 添加设备监测触发器(一)



.....

Ċ		设备监测航发器
₾		
	设备监测触发器	■ 純炭器名称 所属组织 * 就发储名称 test 摄作
	报警配置	□ 未命名_就发展名称_99 根据织 *所思组织 根组织 ✓ 24 10.43.02 查看 编辑 关联设备 删除
<u>111</u>	数据中心 ~	报警规则描述 INAANSTRATING 社 其1条 10条/页 · 上一页 和社 1 页
æ		* 新田和RD/ 図 设施商総計的> 5 分钟
		☑ 设施 10 分钟外5, 种能比对的组织过 5 次
		SIMt 无线管罚提生 弱 ~
		2 SIM2无线信号强度 s 转
		☑ SIM1:当月远意用解≥ 1024 MB(1G8=1024MB)
		✓ SIM2:当月活型消耗 > 1024 MB(1G8=1024MB)
		2 设备接电报整(仅支持部分产品型号,详情清查看产品出明书或高词相关人员)
	V1.0.0	

图 89 添加设备监测触发器(二)

关联设备,那些设备触发以上条件会报警的配置。

	大屏管理 ~	报警联动 > 设备监测触发器		
୯	设备管理 >	设备监测触发器		
₾	报警联动 へ	请选择组织 >> 触发器名称 请输入联网设备名称	otsN	添加 批量調除
	设备监测触发器	触发器名称 所属组织 关联设	备数量 状态 创建人	更新时间 操作
	报警配置	test 相組织 0	test	2023-05-12 16:33:51 查看 编辑 关联设备 删除
	报警联系人	未命名_截发器名称_99 根组织 1	test	2023-03-24 10:43:02 查看 编辑 关联设备 删除
<u></u>	数据中心			共2条 10条/页 > 上一页 1 下一页 能往 1 页
Ð	设备运维 🗸 🗸	< Comparison of the second sec		
	V1.0.0			
			图 90 关联设备	

7.1.3.3. 报警配置

将设备检测触发器和报警联系人关联,某台设备触发了某些触发条件将报警信息发给那位报警联系人。



ē	大屏管理 >	报警联动 〉报警配置								
୯	设备管理 🛛 🗡	报警配置								
₽	报警联动 ^	请选择组织 ~	请输入报警配置名称	Tia -						添加 批星 那除
	设备监测触发器	报警配置名称	所属组织	推送类型	推送主体	推送方式	推送机制	状态	创建人 更新时间	操作
	报警配置					婚子粉屉				
	报警联系人					H/L905				
<u>ıll</u>	数据中心 🗸 🗸							共0条	10条/页 > 上一页	1 下一页 前往 1 页
	₩ 2% 运生 ~	¢								
	V1.0.0									

配置报警

报警联动 > 报警配置 *报警配置名称 test 报警配置 *所属组织 根组织 添加 批型服除 * 推送类型 触发器 报警配置名称 选择刚刚设置的设备检测触发器 操作 🗸 🛛 test 🗙 🌽 报警配置 *选择触发器 设备监测触发器 报警联系 * 推送机制 变量值达到触发条件时 共0条 10条/页 · 上一页 1 下一页 前往 1 页 ○ 仅第一次推送 ○ 报警沉默时间 分钟 🕤 * 推送方式 🗹 短信 🗹 邮件 🔶 短信和邮件都推进 * 推送人 ✓ 全选 推送给刚刚设置的报警联系人 ✓ test(根组织) 共1条 〈 **1** 〉 图 92 配置报警

图 91

以硬件断电举例

7.1.3.4. 报警验证





cloudmonitor 发给 意双双	三部 (14) (14) (14) (14) (14) (14) (14) (14)
尊敬的用户 test 、您好	
检测到您的设备 <test> 的掉电状态 已触发报警, 当前值为: 已掉电 以下为详情:</test>	
设备名称: TEST	
设备编号: 01600322093000000128	
当前值:已掉电	
触发条件: 设备已掉电	
报警/恢复时间: 2023年05月12日 16:40:04	
此为系统邮件请勿回复	

图 93 邮件报警信息举例

7.1.4. 数据中心

7.1.4.1. 设备上下线

可 SN 查询某台设备一段时间的上下线情况。

「空大用管理 >	数据中心 > 设备上下线				
	设备上下线				
① 报警联动 ~	请选择联网设备	· 2023-05-05 16:43:35	Ē 2023-05-12 16:43:35	查询	下载数据
山数据中心 ^	设备名称	SN	时间	状态	下线原因
设备上下线	TEST	01600322093000000128	2023-05-12 16:43:34	上线	-
设备报警记录	TEST	01600322093000000128	2023-05-12 16:40:07	下线	设备掉电
▶ 设备运维 >	TEST	01600322093000000128	2023-05-12 16:13:14	上线	-
	TEST	01600322093000000128	2023-05-12 15:36:42	下线	心到过程时
	TEST	01600322093000000128	2023-05-12 15:34:34	上线	-
	TEST	01600322093000000128	2023-05-12 12:30:20	下线	设备掉电
	TEST	01600322093000000128	2023-05-12 10:34:38	上线	-
	TEST	01600322093000000128	2023-05-12 10:21:04	下线	设备掉电
	TEST	01600322093000000128	2023-05-12 09:53:20	上线	-
	样机1	01600322093000000117	2023-05-11 19:33:30	下线	心跳起时
				共53条 10条/页 > 上一页 1	2 3 4 5 6 下一页 前往 1 页
V1 0.0					
V1.0.0					
		图 94	设备上下线	统计	

7.1.4.2. 设备报警记录

看查看所有的设备报警记录,也可通过时间、SN 等精确查看报警记录。



2	大屏管理	~	数据中心 > 设备报警记录							
୯	设备管理	~	设备报警记录							
₾	报警联动	~	请选择联网设备 >>	请选择报警状态 >	请选择处理状态 ~ © 2	023-04-11 16:45:24 至 2023-05-12 1	6:45:24 Ē	in		
щ	数据中心	^	设备名称	所属组织	报警内容	报警时间	报警状态	处理状态	操作	
	设备上下线		TEST	根组织	设备已掉电	2023-05-12 16:40:04	报警	未处理	处理	
	设备报警记录							共1条 10条/页 🗸		1 0
⊵	设备运维	~								
		_ <	l I							
		Ī								
	V1.0.0									
							1			

图 95 设备报警记录统计

7.1.5. 设备运维

7.1.5.1. 远程配置

路由	器远程管理平台								Q 服务支持	\$ • 用>>权限
e ē	大屏管理 > 设备管理 >	设备运维 > 远程配置 远程配置	l							
₫	报警联动 >	请选择组织	~ 全部状态	~ ©	开始日期	至结束日	明 请输入任务名称 直询			批星關除 添加配置任务
<u>ul</u>	数据中心 ~	状态	所属组织	任务名称	配置进度	设备型号	任务时间	操作 🕘		
∞	设备运维 ^	 已結束 	根组织	wu聚合	1/1	USR-G810	2023-04-21 14:30:20 - 2023-04-22 14:30:20	配置详情	终止任务删除	
	远程配置	□ ■已结束	根组织	test	1/1	USR-G810	2023-04-17 15:24:57 - 2023-04-18 15:24:57	配置详情	终止任务删除	
	固件升级	 已结束 	根组织	test	1/1	USR-G810	2023-04-17 14:57:20 - 2023-04-18 14:57:20	配置详情	终止任务删除	
		• 已结束	根组织	123	1/1	USR-G810	2023-03-30 15:24:05 - 2023-03-31 15:24:05	配置详情	终止任务删除	
			根组织	11	1/1	USR-G810	2023-03-30 15:11:38 - 2023-03-31 15:11:38	配置详情	终止任务 删除	
		 已結束 	根组织	123	1/1	USR-G810	2023-03-30 15:08:57 - 2023-03-31 15:08:57	配置详情	终止任务删除	
		□ ■已結束	根组织	12	1/1	USR-G810	2023-03-30 14:59:06 - 2023-03-31 14:59:06	配置详情	终止任务删除	
		 已结束 	根组织	123	1/1	USR-G810	2023-03-24 11:04:41 - 2023-03-25 11:04:41	配置详情	终止任务删除	
		□ ■已結束	根组织	1	1/1	USR-G810	2023-03-24 11:01:57 - 2023-03-25 11:01:57	配置详情	终止任务删除	
		•已结束	根组织	11	1/1	USR-G810	2023-03-24 10:56:04 - 2023-03-25 10:56:04	配置详情	终止任务删除	
							共 12 条	10条/页 ~	上—页 1 :	2 下一页前往 1 页
	V1.0.0									

G810-33 支持远程可视化批量配置路由器,无需繁琐 AT 批量配置。轻松快速完成配置任务。可视化的平台批量配置,免去繁琐的配置每台设备,也免去您需定制默认参数的烦恼,高效运维。

图 96 远程配置(一)



如下,点击进行下一步。可以看到当前设备型号下,已经存在的设备,并选择需要对其进行配置的设备,然后点击下一步。

路由器远程管理平台		○ 服务支持 ● 用户权限
☑ 大屏管理 > 设备运维 > 远程定置 > 添加配置任务		
C 设备管理 ~ 配置任务		
▲ 报程器模长动 ~	1.任务信息 2.选择设备 3.进行配置 4.完成	
	*所還組织 模組织 >>	
	* 任务名称 test	
远程直置	* 设备带号 USR-G10 ~	
<u></u>	*任务时间 ③ 2023-05-12 16:52:36 至 2023-05-13 16:52:36	
	下一步	
V1.0.0 -	图 07 注印和军(一)	

路由器远程管理平台				○ 服务支持 ● 用户权限 ●
「空大用管理 >	设备运维》远程配置》添加配置任务			Í
C 设备管理 ~	配置任务			
① 报警联动 ∨		1.任务信息 2.选择设备	3.进行配置 4.完成	
山数调中心 ~	全部状态 ∨ 请输入SN或设备名称	查询		
子 设备运维 ^	设备名称	SN	当前版本	状态
远程配置	TEST	01600322093000000128	V1.0.11.4g.06	在线
固件升级	未命名_设备名称_53	01600322093000000125	V1.0.11.4g.06	高线
	< 未命名_设备名称_50	01600322101200000333	V1.0.11.4g.02	潮线
	未命名_设备名称_38	01600322093000000121	V1.0.11.4g.04	高线
	未命名_设备名称_41	01600322093000000199	V1.0.11.4g.04	商线
	cesshi2	0160032209300000127	V1.0.11.4g.03	商线
	聚合路由测试	01600322093000000120	V1.0.11.4g.04	离线
	未命名_设备名称_11	01600322093000000133	V1.0.11.4g.05	测线
	↓¥初1	01600322093000000117	V1.0.11.4g.05	高线
			共9条 105	い クレーズ 1 下一页 前往 1 页
V1.0.0	8	98 远程配置-选择排	⊪⊭ 比量的设备	

可以进行常用参数配置,也可在高级设置中进行设置其他参数,设置完成后点击"确认"。




路由	日器远程管理平台		O 服务支持 💿 用户权限 🌗
ē	大屏管理 ~	设施运输 > 远程和置 > 海 加和面面任务	Î
Ċ	设备管理 >	配置任务	
₾	报警联动 >	1.任务信息 2.远岸设备 3.进行配置 4.完成	
<u>111</u>	数据中心 🗸	~ 简单配置顶	
⊡	设备运维 ^	* 登录密码 root	
	远程配置	* WI-FI4名称 ④	
	固件升级	*Wi-Fi4密码 12345678	
		* Wi-Fiら名称 ④ 4GRoute-F7E9_5G	
		* WI-FI08569 12345678	
		* 子琬LAN口IP ③ 192.168.1.1	
		* 子网晚码 255.255.255.0	
		* 定时重启时间 🕚 報周 🗸 星期三 🔨 04 🗸 时 44 🗸 分	
	V1.0.0	高级设置	
		图 99 远程配置-可以设置基本的参数	Ť

将您需要设置的参数设置好后,任务添加完成,会将您在平台设置的参数,在您勾选的所有设备进行配置。配置完成后路由器将 自动重启。

路由器远程管理平台		○ 服务支持 ♥ 用户収限
	设备运维 > 远程处置 > 添加配置任务	
C 设备管理 ~	配置任务	
▲ 振警联动 >	1.任务信息 2.选择设备 3.进行管置 4.完成	
山 数据中心 ~		
▶ 设备运性 ∧	18006870	
远程配置		
固件升级	861.	
V1.0.0		

图 100 远程配置任务添加成功

7.1.5.2. 固件升级

平台支持对路由器自身设备进行固件升级。注意:这里的固件升级不是给下端客户设备升级。 在"设备管理""联网设备"-"更多"下,找到想要进行固件升级的设备,选择"固件升级"。



路由	器远程管I	理平台								Q 服务支持	• 用户权限 🌗	
⊵	大屏管理	~	设备管理 > 联网设备									
୯	设备管理	^	联网设备									
	联网设备		请选择组织 ~	01600322093000000	请选择设备状态 ~	请选择标签 🗸	查询	添加	し しょうしょう しゅうしょう しゅうしょう しゅうしょう しゅうしゅう しゅう	用设备 禁用设备	批星剧除	高级设置
	变量模板		设备名称	SN	设备型号	所属组织	设备地址	启用状态	标签	操作		
₾	报警联动	~	TEST	01600322093000000128	USR-G810	根组织	山东省济南市历下区龙奥南路			数据查看 设备运维	编辑设备更多	
ш	数据中心	~									お常知市	
⊡	设备运维	~							关于派	1038/00	固件升级	W
		-	<								重启设备	
		Ī									删除设备	
	V1.0.0											

图 101 固件升级(一)

也可以在"设备运维"-"固件升级"下,点击"添加升级任务"。

路由器远程管理平台		○ 服务支持 ● 用户权限
□ 大麻管理 ∨	役金送準 > 国件升级	
C 设备管理 ~	固件升级	
① 报警联动 ∨	· 通過詳細訳 → 全部状态 → ○ 开始日期 至 括甲日期 - 清输入任务名称 - 直向	添加升级任务
山数据中心 ~	状态 所属组织 任务名称 升级进度 设备型号 升级版本 任务时间	操作 🎯
➡ 设备运维 ∧	韬无政损	
远程配置	共0条 1	10条/页 > 上一页 1 下一页 前往 1 页
固件升级		
V100		
V1.0.0		

图 102 固件升级(二)

填写上本次固件升级的"任务名称",选择"固件升级版本",填写"任务时间",点击"确认"后进行下一步。





路由器远程管理平台 • ① 殿技持 • 即响限 👘 🛄								
		设备运维 > 固件升级						
		固件升级						
		请选择组织 全計	×	添加升级任务				
		状态 所属组织	1.任务信息 2.选择设备 3.完成	操作 0				
		*所属组	Real V					
远程配置	า	*任务各种	test	10条/页 >> 上一页 1 下一页 前往 1 页				
		* 设备型(v v					
		* 固件升级版本	VI.0.11.4g.03 V					
		* 任务时间	· 2023-05-12 17:01:48 至 2023-05-13 17:01:48 ·					
			10月 下一步					

图 103 有人云—固件升级(三)



路由器远程管理平				O 服务支持 💿 用户权限 🌗
2 大麻管理	₩ 设备运维 > 固件升级			
C 设备管理	~ 固件升级			
	~ 请选择组织 ~	固件升级		× 18307148699
山 数据中心	* 状态 所属组织	1.任务信息 2	2选择设备 3.完成	istr 🛛
🖸 设备运维	^.	全部状态 > 遺选择组织 >	翰諭入SN或设备名称 直询	
远程置		□ 设备名称 SN 当前版本	目标版本 状态 所属组织	10条/页 ~ 上一页 1 下一页 前往 1 页
固件升级		TEST 01600322093 V1.0.11.4	g.06 V1.0.11.4g.03 在线 根组织	
		未命名_设备名 01600322093 V1.0.11.4	g.06 V1.0.11.4g.03 高线 根组织	
		未命名_设备名 01600322101 V1.0.11.4	g.02 V1.0.11.4g.03 高线 根组织	
		□ 未命名_设备名 01600322093 V1.0.11.4	g.04 V1.0.11.4g.03 高线 根组织	
		未命名_设备名 01600322093 V1.0.11.4	g.04 V1.0.11.4g.03 高线 根组织	
		cesshi2 01600322093 V1.0.11.4	g.03 V1.0.11.4g.03 商线 根组织	
		聚合路由测试 01600322093 V1.0.11.4	g.04 V1.0.11.4g.03 商线 根组织	
		未命名_设备名 01600322093 V1.0.11.4	g.05 V1.0.11.4g.03 高线 根组织	
			g.05 V1.0.11.4g.03 阐述 根组织	
V100		共9条	10条/页 > 上一页 1 下一页 前往 1 页	

图 104 固件升级(四)

在"升级详情"里面查看当前固件升级进度,并且可以在"查看日志"里面查看详细信息。





路由器远程管理平台 ①											
		设备运维 > 西	牛升级								
		固件升级									
		请选择组织	~ 全	升级详情					×		添加升级任务
		状态	所属组织	待升级(0)	升级中(0)	升级失败(0)	升级成功(1)			操作 🔍	
		■已結束	根组织	设备名称	SN		原版本	目标版本	操作日志	升级详情 终止任务	##Re
远程配置				TEST	01600	0322093000000128	V1.0.11.4g.06	V1.0.11.4g.03	查看日志 ~	10条/页 > 上一页	1 下一页 前往 1 页
固件升级		L		2023-05-12 17:04:0)1: 下发指令						
		<		2023-05-12 17:04:0	12: 设置权到指令 13: 下载完成						
				2023-05-12 17:09:4	16: 成功						
							共1条 10祭/页	> 上一页 1 下一页	前往 1 页		
V1.0.0											

图 105 固件升级(五)

7.2. 动态域名解析 (DDNS)

DDNS(Dynamic Domain Name Server, 动态域名服务)是将用户的动态 IP 地址映射到一个固定的域名解析服务上,用 户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序,服务器程序 负责提供 DNS 服务并实现动态域名解析。动态域名的使用分为两种情况.

7.2.1. 已支持服务商

第一种,路由器自身支持这种服务商(在"服务提供商"下拉框中查看并选择,这里使用花生壳 ddns.oray.com),设置 方法如下:

.



TEST			
状态	开启		
<u>4</u>	生效接口	wan_wired	~
		ODNS生效的网络接口	
云服务	10.44	hard the second s	
动态DNS	服务	ddns.oray.com	•
2008			
	主机名	fe26203015.zicp.vip	
网络		② 填写对应的域名	
VPN	田白夕	vss0520	
防火墙		,	
14	密码	•••••	8
200	TO MILLI AN WE		
3出	IP地址来源	後日 (2) 通过法院大切ID地址	
		ANALASIA ANALASIA	
	接口	eth0.2	~
	检查IP变动的时间间隔	10	
	时间单位	分	~
	131 34 LL		
	强制更新间隔	72	
		~	
	5 TO 10 BE ALL DOUGHT ALL DO 17		

图 106 DDNS 设置页面

表 21 DDNS 参数列表

功能	内容	备注	
开启	勾选使能 DDNS 功能	默认不开启,请开启以生效	
事件接口	根据需求选择哪个 WAN 口	举例:选择 wan_wired	
肥久/1101	请填写 DDNS 的服务地址(这里以花生壳为例,服务	举例:ddps.oray.com	
服务/URL	地址选择 ddns.oray.com)	举例. duris.oray.com	
主机名	请填写您申请号的域名	举例: fe26203015.zicp.vip	
用户名	花生壳账户名	举例: yss0520	
密码	花生壳密码	举例: *****	
IP 地址来源	这里选择接口	选择接口	
按口	<u> </u>	举例:这里选择 eth0.2	
按口	选择按口右 	也就是有线 WAN 口	
检查 IP 变动的时间间	检测 IP 地址变动的时间间隔, 域名指向的 IP 可能会经	举/问,1 八	
隔 / 时间单位	常变动,数值越小检测越频繁	华例. 1 万 世	
强制更新间隔 / 强制	22.4.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	※例・72 小时	
更新时间单位	当 " " " " " " " " " " " " " " " " " " "	平別, 72 小切	

测试申请的域名地址如下。



C:\Users\Adminis	trator>
C:\Users\Adminis	trator>ping fe26203015.zicp.vip
正在 Ping fe2620 来自 60 来自 60 来自 60 来自 60 来自 60	3015.zicp.vip [6 38] 具有 32 字节的数据: 38 的回复: 字节=32 时间<1ms TTL=127 38 的回复: 字节=32 时间<1ms TTL=127 38 的回复: 字节=32 时间<1ms TTL=127 38 的回复: 字节=32 时间<1ms TTL=127
⁹ 6()的	9 Ping 统计信息:
数据包:已发	送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时	间(以毫秒为单位):
最短 = Oms, 1	最长 = Oms, 平均 = Oms

图 107 DDNS 测试图

7.2.2. 自定义的服务商

第二种情况,路由器自身不支持的 DDNS 服务商(需要在"服务提供商"下拉框中,选择"自定义",我们这里仍然填写 ddns.oray.com),使用方法如下:

TEST			
	8 🛛		
广 杰	T wan wired		
	② DDNS生效的网络接口		
「服务	F 目定义 ♥ ② 提供域名解析服务的服务商		
b态DNS			
《合网络 自定义更新UF	L http://yss052()@dc		
主机	g fe26203015.zicp.vip		
PN	2 填写对应的域名		
用户	gyss0520		
·····	ی ۱۰۰۰۰۰۰ <i>و</i>	1	
444			
IP地址来			
接	□ eth0.2 ~		
检查IP变动的时间间	稿 10		
Brijaja	☆ 分 ×		
	ш ¹³		
强制更新间	幕 72		

图 108 DDNS 自定义服务参数设置页面

表 22 DDNS 自定义服务参数表

功能	内容	备注
开启	勾选使能 DDNS 功能	默认不开启,请开启以生效
事件接口	根据需求选择哪个 WAN 口	举例:选择 wan_wired
服务/URL	请填写 DDNS 的服务地址(这里以花生壳为例,	举例:
	服务选择自定义),需要以	http://yss0520:***@ddns.oray.c
	http://username:password@ddns.oray.co	om/ph/update?hostname=fe26
	m/ph/update?hostname=花生壳的动态域名	203015.zicp.vip
	的格式填写	



〒 招索工具

主机名	请填写您申请号的域名	举例:fe26203015.zicp.vip
用户名	花生壳账户名	举例: yss0520
密码	花生壳密码	举例:***
IP 地址来源	这里选择接口	选择接口
接口	选择接口名	举例:这里选择 eth0.2,也就是
		WAN 接口
检查 IP 变动的时间	检测 IP 地址变动的时间间隔,域名指向的 IP 可能	举例:1分钟
间隔	会经常变动,数值越小检测越频繁	
强制更新间隔 / 强	强制更新时间间隔	举例・72 小时
		+ /// / = // - /

下面确认 DDNS 设置是否生效(路由器必须重启才可以使设置生效)。首先我们先看一下自己所在网络的公网 IP 地址。

 P地址查询

 本机IP:123.101.125.124
 山东省济南市 联通

 資源
 重源

 本机P室看方法
 P地址设置方法

 图 109
 DDNS 测试图二

然后,我们在 PC 上 ping 域名 1a516r1619.iask.in ,可以 ping 通,说明 DDNS 已经生效。

百席为您找到相关结果约100.000.000个

C: Wsers Administrator>ping 1a516r1619.iask.in 正在 Ping 1a516r1619.iask.in [123.101.125.124.] 具有 32 字节的数据: 来自 123.101.125.124 的回复: 字节=32 时间<1ms TTL=254 来自 123.101.125.124 的回复: 字节=32 时间<1ms TTL=254 来自 123.101.125.124 的回复: 字节=32 时间<1ms TTL=254 来自 123.101.125.124 的回复: 字节=32 时间=1ms TTL=254 [123.101.125.124 的Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 <0% 丢失>, 往返行程的估计时间<以毫秒为单位>: 最短 = 0ms, 最长 = 1ms, 平均 = 0ms

图 110 DDNS 测试图三

<说明>

- 修改设置后,请重启路由器确保生效;
- ▶ 请按照表格说明严格填写参数,服务/URL、申请的域名、用户名密码、接口等参数确保正确;
- 即便作为子网下的路由器,本功能也应可以使动态域名生效;
- > DDNS + 端口映射可以实现异地访问本路由器内网;
- > 如果路由器所在的网络,没有分配到独立的公网 IP,那么本功能无法使用。



8. 免责声明

本文档未授予任何知识产权的许可,并未以明示或暗示,或以禁止发言或其它方式授予任何知识产权许可。除在其产品的销售条款和条件声明的责任之外,我公司概不承担任何其它责任。并且,我公司对本产品的销售和/或使用不作任何明示或暗示的担保,包括对产品的特定用途适用性,适销性或对任何专利权,版权或其它知识产权的侵权责任等均不作担保。本公司可能随时对产品规格及产品描述做出修改,恕不另行通知。

9. 更新历史

说明书版本	更新内容	更新时间
V1.0.0	创立文档,完成相关功能描述	2023-05-12



可信赖的智慧工业物联网伙伴

天猫旗舰店: https://youren.tmall.com 京东旗舰店: https://youren.jd.com 官方网站: www.usr.cn 技术支持工单: im.usr.cn 战略合作联络: ceo@usr.cn 软件合作联络: console@usr.cn 电话: 4000 255 652



地址:山东省济南市历下区茂岭山三号路中欧校友产业大厦 12、13 层有人物联网