robustel | 软件说明书

RobustOS

软件说明书

robustOS

广州鲁邦通物联网科技股份有限公司

www.robustel.com.cn

关于文档

本文档提供基于 RobustOS 的 DTU、路由器和网关产品的 Web 界面信息，包括功能介绍和操作配置。

商标许可

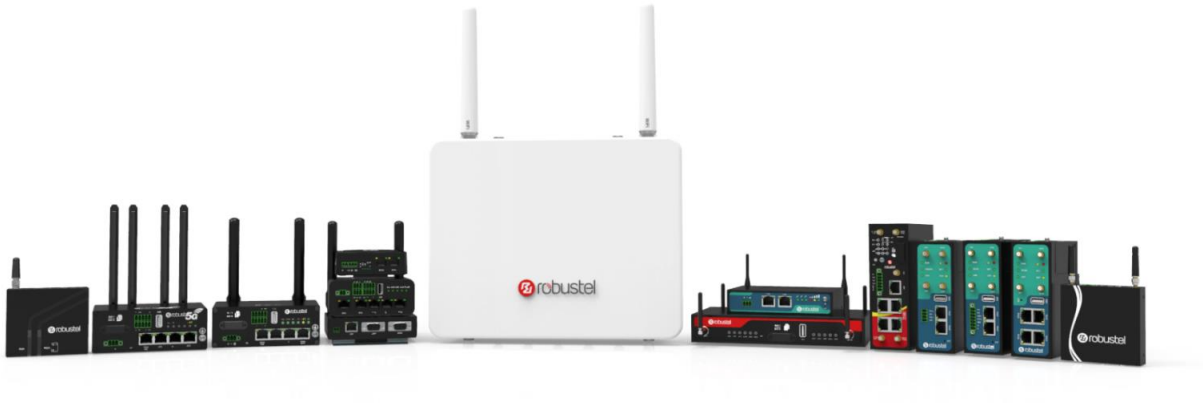
robustel、robustOS是广州鲁邦通物联网科技股份有限公司的商标。本手册中提及的其他商标和商业名称均属于各自持有者。

免责声明

未经版权拥有者允许，不得以任何形式复制该文档的任意部分。由于方法、设计、生产工艺的不断改进，文档内容可能在未预先通知的情况下进行更新或修订。因未使用该文档导致任何错误或损坏，鲁邦通概不负责。

技术支持

电话：+86-20-82321505
传真：+86-20-82321505
邮件：support@robustel.com
网址：www.robustel.com.cn



版本历史

这里不断累积文档版本的更新记录。因此，最新版本的文档包含了所有历史版本的更新记录。

更新日期	文档版本	详细说明
2022 年 8 月 1 日	V.1.0.0	首次编写。
2022 年 10 月 18 日	V.1.1.0	适配 RobustOS V5.1；

目录

第 1 章 产品概念 6

1.1 产品概述 6

第 2 章 网页配置前准备 7

2.1 配置 PC 端 7
2.2 出厂默认设置 10
2.3 恢复出厂配置 10
2.4 登录 WEB 配置页面 11
2.5 控制面板 12

第 3 章 路由器配置 14

3.1 状态 14
3..1.1 系统信息 14
3.1.2 互联网状态 15
3.1.3 Modem 状态 15
3.1.4 局域网状态 16
3.2 接口 16
3.2.1 链路管理 16
3.2.2 局域网 29
3.2.3 以太网 34
3.2.4 蜂窝网 37
3.2.5 Wi-Fi 44
3.2.6 USB 57
3.2.7 DI/DO 57
3.2.8 AI 62
3.2.9 串口 64
3.2.10 LoRa 70
3.3 Packet Forwarders 77
3.3.1 Basic Station 77
3.3.2 Semtech UDP Forwarder 78
3.4 网络 80
3.4.1 路由 80
3.4.2 防火墙 82
3.4.3 IP Passthrough 93
3.5 虚拟专用网 94
3.5.1 IPsec 94
3.5.2 WireGuard 105
3.5.3 OpenVPN 108
3.5.4 GRE 119
3.6 服务 121
3.6.1 系统日志 121
3.6.2 事件 122

3.6.3 NTP 126
3.6.4 短信 127
3.6.5 Email 129
3.6.6 DDNS 130
3.6.7 SSH 132
3.6.8 电话 132
3.6.9 Ignition 134
3.6.10 GPS 134
3.6.11 Web 服务器 139
3.6.12 高级 140
3.6.13 Smart Roaming V2 141
3.7 系统 148
3.7.1 调试 148
3.7.2 软件更新 149
3.7.3 应用中心 150
3.7.4 工具 151
3.7.5 参数文件 153
3.7.6 用户管理 155
3.7.7 角色管理 156

第 4 章 配置示例 159

4.1 蜂窝网 159
4.1.1 蜂窝网拨号 159
4.1.2 短信远程控制 161
4.2 VPN 配置示例 164
4.2.1 IPsec VPN 164
4.2.2 OpenVPN 170
4.2.3 GRE VPN 172

第 5 章 CLI 命令介绍 175

5.1 CLI 介绍 175
5.2 命令帮助 176
5.3 常用命令 177
5.4 CLI 配置示例 177

术语表 184

第1章 概述

1.1 产品概述

本软件说明书适用于所有基于 RobustOS 的产品，包括 DTU、路由器和网关产品，提供 Web 界面信息（配置和操作）。

因为硬件配置或接口因产品而异，请根据产品的接口情况参考具体章节。

产品型号	M1200	M1201	R1510	R1510 Lite	R1511	R1520	ET8013	R2000	R2000 Dual	R2000 Ent	R2010	R2011	R2110	R3000	R3000 Lite	R3000 Quad	R3000 LG	R3010	R5020
SIM 卡	2	1	1	1	1	2	1	2	2	2	2	2	2	2	2	2	2	1	2
以太网口	-	-	2	1	2	5	2	2	5	5	2	5	4	2	1	4	2	2	4
PoE PD	-	-	-	-	-	*	-	*	-	*	*	*	*	-	-	-	-	-	*
PoE PSE	-	-	-	-	-	-	-	-	√	-	-	-	-	-	-	-	-	-	-
Wi-Fi	-	-	√	-	√	√	-	*	√	√	√	√	√	*	-	*	-	-	√
蓝牙	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-
GNSS	-	-	-	-	-	*	-	-	-	-	-	-	*	*	-	*	*	-	*
DI	2	-	√	-	-	√	-	-	√	-	√	-	√	2	-	-	2	-	√
DO	√	-	√	-	-	√	-	-	-	-	√	-	√	2	-	-	-	-	√
AI	-	-	-	-	-	√	-	-	-	-	-	-	-	-	-	-	-	-	-
RS232	√	*	-	-	*	√	-	-	-	*	*	-	√	√	√	*	*	√	√
RS485	√	*	-	-	*	√	√	-	-	*	*	-	√	√	√	*	*	√	√
USB 主设备	-	-	-	-	-	√	-	-	-	√	-	-	√	√	√	√	√	√	√
RS422	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CAN	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	√	-
语音	-	-	-	-	-	-	√	-	-	*	-	-	-	-	-	-	-	√	-
MicroSD	-	-	-	-	-	-	-	-	-	-	-	-	√	√	-	√	√	-	√

注: *√ = 支持, - = 不支持, * = 可选*

RobustOS 基于 Linux 系统上开发，适用于公司大部分路由器设备。除基本的网络功能和协议外，系统带给客户更多样、更方便、更实用的自定义体验。与此同时，鲁邦通将为合作伙伴和客户提供 SDK，允许用户使用 C、C++自行开发功能。另外，还提供丰富的运行于 RobustOS 上的 App 应用程序，满足碎片化的物联网应用市场需求。

第2章 网页配置前准备

设备支持网页配置，支持使用的浏览器有 Microsoft Edge、Google Chrome 和 Firefox 等，而支持使用的操作系统包括 Ubuntu，macOS，Window 7/8/10/11 等。连接设备的方式有多种，既可通过外部中继器/集线器连接，也可以直接连接到电脑。设备直接连接到电脑的以太网口时，如果设备作为 DHCP 服务器，那么电脑可以直接从设备获取 IP；电脑也可以设置和设备同在一网段的静态 IP，这样电脑与设备就构成了一个小型的局域网。电脑与设备已成功建立连接后，在电脑浏览器上输入设备的默认登录地址，即可进入设备的 Web 登录界面。

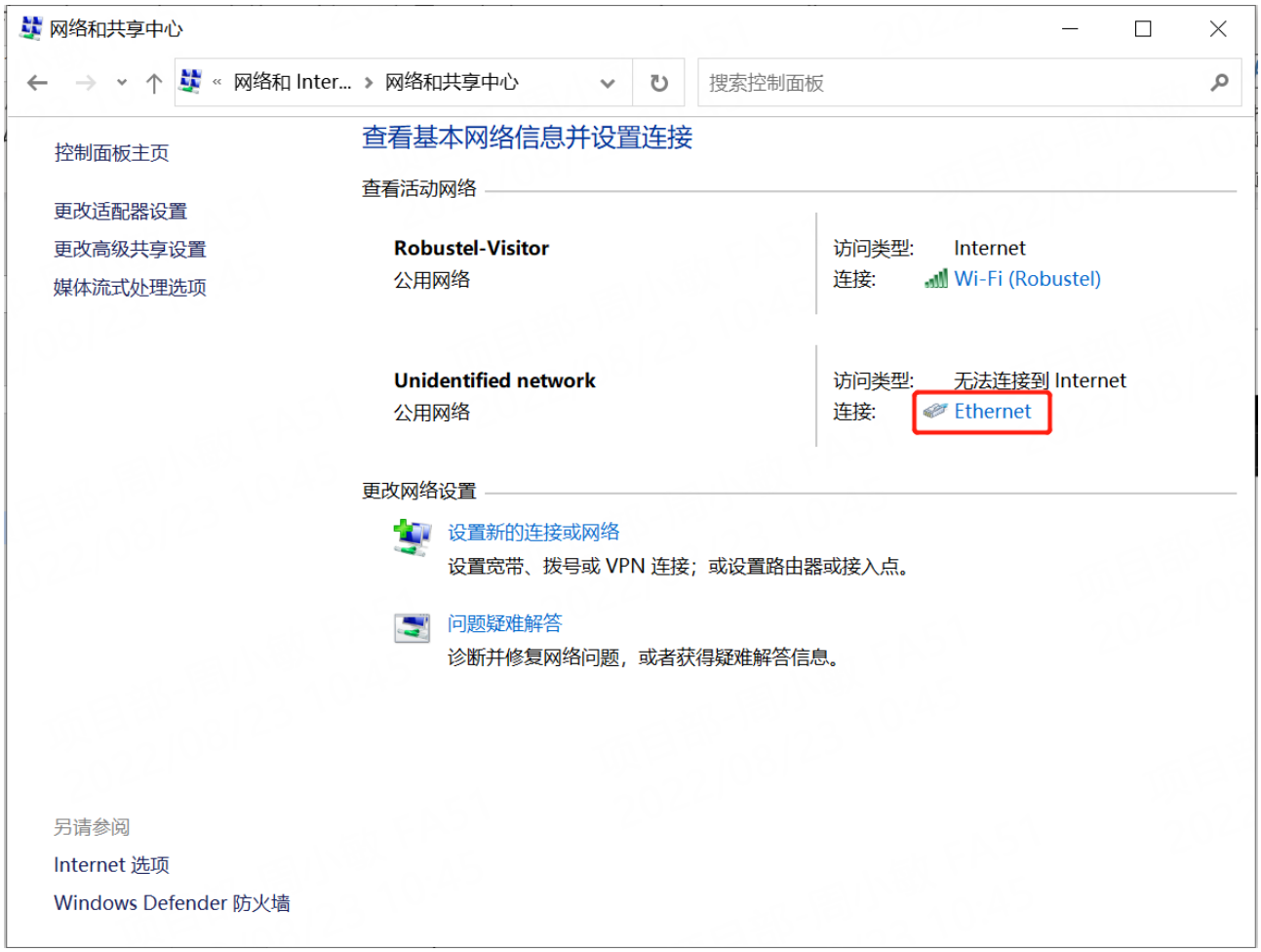
2.1 配置 PC 端

在 PC 端，有两种方法配置其 IP 地址；一是在 PC 端的本地连接上开启自动获取 IP 地址，二是在 PC 端的本地连接上配置一个跟设备在同一个子网的静态 IP 地址。

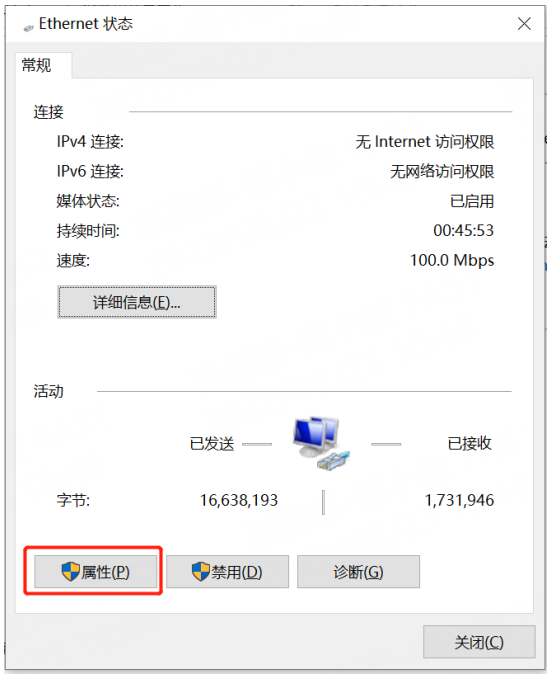
本节以配置 **Windows 10** 系统为例。Windows 7/8/11 系统的配置方式均相似。

1. 寻找键盘的Windows徽标键  （后文简称Win键），按下**Win键 + R**，输入“**Control**”，运行控制面板。打开控制面板后，左键单击“**查看网络状态和任务**”。

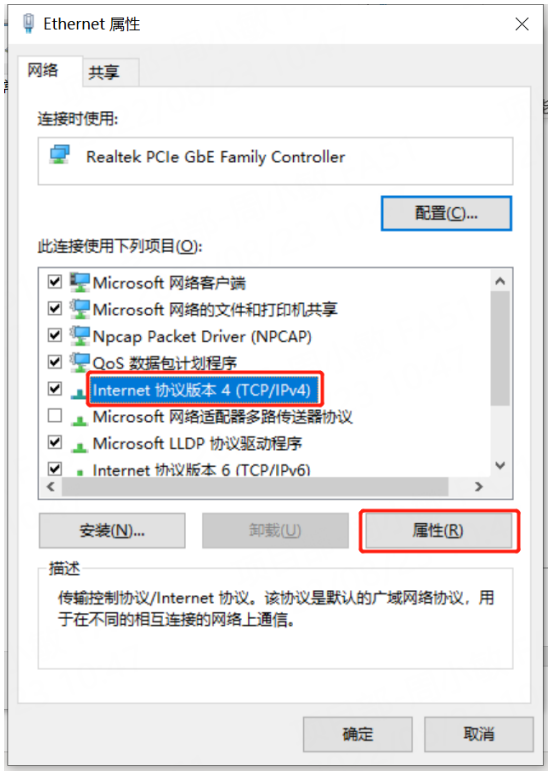
2. 单击“控制面板 > 网络和共享中心”，点击“**以太网**“；



3. 在“本地连接 状态”窗口中，单击“**属性**”；



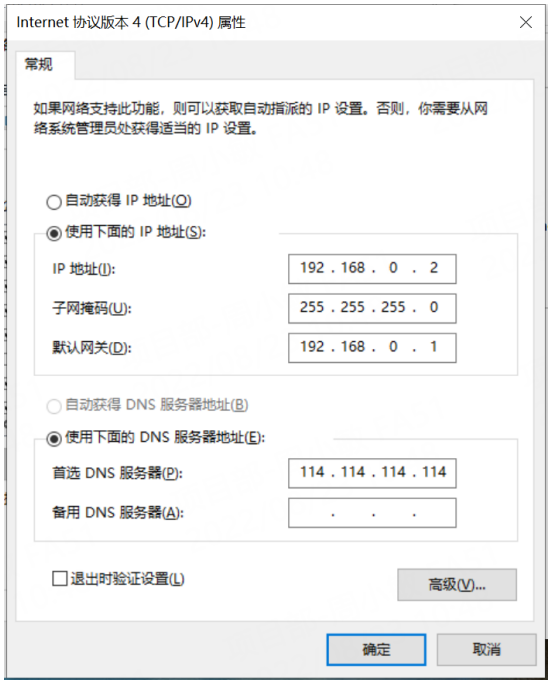
4. 选择“**Internet 协议版本 4（TCP/IPv4）**”，并单击“**属性**”；



5. 两种方法配置PC的IP地址：

（1）自动从 DHCP 服务器获取 IP 地址，单击“**自动获得 IP 地址**”；

（2）手动给PC配置一个跟设备地址在同一个子网的静态IP地址，单击并配置“**使用下面的IP地址**”；



6. 单击“**确定**”以完成配置。

2.2 出厂默认设置

登录配置页面前，您有必要了解以下的默认设置。

项目	描述
用户名	admin
密码	admin
ETH0	WAN 模式或则 192.168.0.1/255.255.255.0，LAN 模式
ETH1/2/3/4(*)	192.168.0.1/255.255.255.0，LAN 模式
DHCP 服务器	开启

** 不同设备的 ETH 接口数量存在差异，详情请参阅设备的产品规格书。*

2.3 恢复出厂配置

功能	操作
重启	在工作状态下，按住 RST 按钮 2~5 秒。
恢复默认设置	在工作状态下，按住 RST 按钮 5~10 秒。RUN LED 指示灯快速闪烁后，释放 RST 按钮，设备即可恢复到默认设置。
恢复默认出厂设置	在一分钟内操作“恢复默认设置”两次，设备即可恢复到默认出厂设置。

2.4 登录 WEB 配置页面

1. 在 PC 上，打开浏览器，如 Microsoft Edge、Google Chrome 和 Firefox 等；

2. 在浏览器的地址栏上输入设备的 IP 地址 http://192.168.0.1/以进入用户登录身份认证界面；

3. 在登录页面输入“用户名”、“密码”，选择语言为“简体中文”，再单击“登录”按钮。
注：如果连续 6 次输入错误的用户名或密码，登录页面将被锁定 5 分钟。

2.5 控制面板

成功登录设备后，主页如下图所示（这里以 R1520 为例）：

在主页内，用户可以执行保存配置，重启设备，注销登录等操作。
使用默认用户名和密码登录设备时，页面会有以下窗口提示：

单击 × 符号以关闭弹窗。如需修改密码，请参阅“3.7.6 用户管理”。

项目	说明	按钮
应用	单击该按钮，使提交的所有配置更改生效。	应用
重启	重启设备。	重启

注销	单击安全退出配置页面，并返回登录页面。	注销
提交	单击该按钮，提交当前页面修改的内容。	提交
取消	单击该按钮取消当前页面的内容修改。	取消

注：*修改配置的步骤如下：*

1) *在一个页面中修改；*
2) *单击页面下方的* 提交 *；*
3) *在另一个页面中修改；*
4) *单击页面下方的* 提交 *；*
5) *完成所有页面的修改；*
6) *单击* 应用 *。*

第3章 设备配置

3.1 状态

3.1.1 系统信息

本节显示设备的系统状态信息。

系统信息	
项目	**说明**
设备型号	显示设备的型号。
系统运行时间	显示系统从启动到当前的运行时长。
系统时间	显示当前的系统时间。
内存使用情况	显示当前的内存使用情况和总内存容量。
固件版本	显示当前的固件版本。
硬件版本	显示当前的硬件版本。
内核版本	显示当前的内核版本。
序列号	显示设备出厂的序列号。从序列号里可以获取设备的出厂时间等信息。

3.1.2 互联网状态

本节显示设备的互联网状态信息。

互联网状态	
项目	**说明**
链路描述	显示当前在线的链路：WWAN1，WWAN2，WAN或WLAN。
连接时间	显示当前链路工作了多长时间。
IP 地址	显示当前获取到的蜂窝网IP地址。
网关	显示当前的网关地址。
DNS	显示当前的DNS服务器。

3.1.3 Modem 状态

Modem状态	
项目	**说明**
Modem 型号	显示无线模块的型号。
注册状态	显示当前的网络状态。
运营商	显示当前注册网络的运营商。

Modem状态	
项目	**说明**
网络类型	显示当前的网络服务类型。
信号强度	显示当前的信号强度。

3.1.4 局域网状态

本节显示设备的局域网状态信息。

局域网状态	
项目	**说明**
IP 地址	显示设备在当前局域网的IP地址和掩码。
MAC 地址	显示设备的 MAC 地址。

3.2 接口

3.2.1 链路管理

用户可以在本节中管理链路连接，链路管理功能支持选择单/双链路。同时，每条链路支持配置链路检测功能，使网络连接一直保持在线。

常规设置@链路管理		
项目	**说明**	**默认**
主链路	可选择“WWAN1”、“WWAN2”、“WAN”或“WLAN”。 • WWAN1：选择SIM1作为主要的无线链路。 • WWAN2：选择SIM2作为主要的无线链路。	WWAN1

常规设置@链路管理		
项目	**说明**	**默认**
	• WAN：使用WAN作为主要的有线链路。 • WLAN：选择WLAN作为主要的无线链路。 ***注：****WLAN链路仅当开启Wi-Fi的Client模式后才可用，详情请参阅“3.2.5 Wi-Fi”。*	
备份链路	可选择“WWAN1”、“WWAN2”、“WAN”或“None”。 • WWAN1：使用SIM1作为备份的无线链路。 • WWAN2：使用SIM2作为备份的无线链路。 • WAN：使用WAN作为备份的有线链路。 • WLAN：使用WLAN作为备份的无线链路。 ***注：****WLAN链路仅当开启Wi-Fi的Client模式后才可用，详情请参阅“3.2.5 Wi-Fi”。* • None：代表不设置备份链路。	None
备份模式	可选择“冷备份”、“热备份”或“负载均衡”。 • 冷备份：备份链路在切换时才拨号上线。 • 热备份：备份链路一直保持在线。 ***注：****热备份不适用于双SIM卡备份。* • 负载均衡：同时使用两条链路。 • 此功能仅当备份链路不为None时才显示。	冷备份
恢复间隔	当备份链路在冷备份模式下使用时，指定等待多少分钟后切回主链路以检测主链路是否恢复正常。0表示不主动回切。 ***注：****此功能仅当选择冷备份模式时才显示。*	0
异常重启	单击切换按钮以启用/禁用异常重启功能。启用后，当没有可用链路时整个系统将重新启动。	OFF

注：*单击 以寻求帮助。*

链路设置用于配置链路连接的参数，包括 WWAN1，WWAN2，WAN 和 WLAN。
建议启用 Ping 检测，以保持设备的网络连接一直在线。Ping 检测提高了网络连接的可靠性。

单击 WWAN1/WWAN2/WAN/WLAN 最右侧的 以进入配置窗口。

WWAN1/WWAN2

启用“自动选择 APN”时，窗口显示如下：

禁用“自动选择 APN”时，窗口显示如下：

链路设置（WWAN）		
项目	**说明**	**默认**
常规设置		
索引	显示表序号。	--
类型	显示链路类型。	WWAN1
描述	输入链路描述，可以为空。	空
WWAN 设置		
自动选择 APN	单击切换按钮以启用/禁用自动选择 APN 选项。开启自动选择 APN 后，设备会自动获取当前网络的 APN，无需手动输入；关闭该功能后，则需手动添加 APN。	ON
APN	输入由本地互联网服务供应商提供的蜂窝网拨号连接的接入点。	internet

链路设置（WWAN）		
项目	**说明**	**默认**
用户名	输入由本地互联网服务供应商提供的蜂窝网拨号连接的用户名。	空
密码	输入由本地互联网服务供应商提供的蜂窝网拨号连接的密码。	空
拨号号码	输入由本地运营商所提供的网络拨号号码。	*99***1#
认证类型	根据本地 ISP 选择“自动”，“PAP”或“CHAP”。	自动
PPP 优先	优先使用 PPP 拨号。	OFF
流量限制切卡	单击切换按钮以启用/禁用流量限制切卡功能。启用后，当数据流量到达限制值时会切换到另一张卡。 *注：仅用于双 SIM 卡备份。*	OFF
流量限制额度	设置每月的数据流量限制。当指定数据流量限度时，系统会记录数据流量统计；流量记录将显示在**“接口 > 链路管理 > 状态 > WWAN 使用数据统计”**中；“0”表示禁用数据流量记录。	0
结算日	指定每个月的数据流量结算日。该数据流量将在这一天被清零重新计算。如不设置，不会统计流量。	1
Ping 检测设置		
启用	单击切换按钮以启用/禁用 Ping 检测机制，其为设备的一项保留策略。	ON
首选服务器	设备 Ping 主地址/域名来检测当前网络连接是否正常。	8.8.8.8
备用服务器	设备 Ping 备用地址/域名来检测当前网络连接是否正常。	114.114.114.114
Ping 间隔	设置 Ping 的间隔时间。	300
Ping 重试间隔	设置 Ping 的重试间隔时间。当 ping 失败后，设备每隔一个 Ping 重试间隔再重新 ping。	5
Ping 超时	设置 Ping 的超时时间。	3
Ping 超时单位	设置 Ping 超时的单位。单位：秒或者毫秒	秒
最大尝试次数	设置 Ping 的最大尝试次数。如果达到最大的连续 Ping 尝试次数，请切换到另一条链路或采取紧急行动。	3
高级设置		
启用 NAT	单击切换按钮以启用/禁用 NAT 功能。	ON
Auto MTU For WWAN	设置 WWAN 的 MTU 为 AUTO 模式。AUTO 模式下自动同步通信模块的 MTU 值。	ON
MTU	设置最大传输单元。 **注：**只有“Auto MTU For WWAN”处于 OFF 状态时，MTU 才可用。	1500
上传带宽	设置用于 QoS 的上传带宽，单位为 kbps。	10000

链路设置（WWAN）		
项目	**说明**	**默认**
下载带宽	设置用于 QoS 的下载带宽，单位为 kbps。	10000
指定首选 DNS 服务器	定义 DHCP 服务器分配给客户端的主要 DNS 服务器。	空
指定备用 DNS 服务器	定义 DHCP 服务器分配给客户端的备选 DNS 服务器。	空
启用调试	单击切换按钮以启用/禁用调试选项。开启：输出链路管理调试信息。	ON
启用详细调试	单击切换按钮以启用/禁用详细调试选项。开启：输出链路管理详细调试信息。	OFF

WAN

当“连接类型”选择“DHCP”时，设备将会从 DHCP 服务器自动获取 IP。

当“连接类型”选择“静态 IP”时，出现下拉列表如下所示：

当“连接类型”选择“PPPoE”时，出现下拉列表如下所示：

链路设置（WAN）		
项目	**说明**	**默认**
常规设置		
索引	显示表序号。	--
类型	显示链路类型。	WAN
描述	输入链路的描述，支持留空。	空
连接类型	可选“DHCP”，“静态 IP”或“PPPoE”。	DHCP
静态地址设置		
IP 地址设置	设置可以访问互联网的带子网掩码的 IP 地址，如 192.168.1.1/24。	空
网关	设置 WAN 口 IP 的网关。	空
首选 DNS 服务器	设置首选的 DNS 服务器。	空
备用 DNS 服务器	设置备用的 DNS 服务器。	空

PPPoE 设置		
用户名	输入由您的互联网服务供应商提供的用户名。	空
密码	输入由您的互联网服务供应商提供的密码。	空
认证类型	根据本地互联网服务供应商来选择“自动”,“PAP”或“CHAP”。	自动
PPP 专家选项	输入用于 PPPoE 拨号的 PPP 专家选项。您可以添加其他关于 PPP 拨号初始化的字符串，多个字符串请用 “;” 分隔开。	空
WAN 设置		
流量统计	设置每月的数据流量限制。当指定数据流量限度时，系统会记录数据流量统计；流量记录将显示在**“接口 > 链路管理 > 状态 > WAN 使用数据统计”**中；“0”表示不统计数据流量。	0
结算日	指定每个月的数据流量结算日。该数据流量将在这一天被清零重新计算。	1
Ping 检测设置		
启用	单击切换按钮以启用/禁用 Ping 检测机制，其为设备的一项保留策略。	ON
首选服务器	设备 Ping 主地址/域名来检测当前网络连接是否正常。	8.8.8.8
备用服务器	设备 Ping 备用地址/域名来检测当前网络连接是否正常。	114.114.114.114
Ping 间隔	设置 Ping 的间隔时间。	300
Ping 重试间隔	设置 Ping 的重试间隔时间。当 Ping 失败后，设备每隔一个 Ping 重试间隔再重新 ping。	5
Ping 超时	设置 Ping 的超时时间。	3
Ping 超时单位	设置 Ping 的超时单位。单位：秒或者毫秒。	秒
最大尝试次数	设置 Ping 的最大尝试次数。如果达到最大的连续 Ping 尝试次数，请切换到另一条链路或采取紧急行动。	3
高级设置		
启用 NAT	单击切换按钮以启用/禁用 NAT 功能。NAT 是 Network Address Translation，即网络地址转换。	ON
MTU	设置最大传输单元。	1500
上传带宽	设置用于 QoS 的上传带宽，单位为 kbps。	10000
下载带宽	设置用于 QoS 的下载带宽，单位为 kbps。	10000
指定首选 DNS 服务器	定义 DHCP 服务器分配给客户端的主要 DNS 服务器。	空
指定备用 DNS 服务器	定义 DHCP 服务器分配给客户端的备选 DNS 服务器。	空
启用调试	单击切换按钮以启用/禁用调试选项。开启：输出链路管理调试信息。	ON
启用详细调试	单击切换按钮以启用/禁用详细调试选项。开启：输出链路管	OFF

	理详细调试信息。	

WLAN

当“连接类型”选择“DHCP”时，设备将会从 WLAN AP 自动获取 IP。请在下面窗口中完成 SSID 的参数配置。

当“连接类型”选择“静态 IP”时，请在下面静态地址设置的窗口中输入相关的参数：

注：*WLAN 连接类型不支持“PPPoE”。*

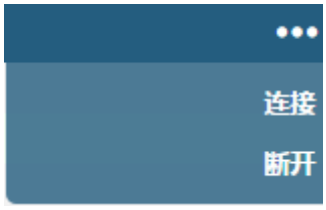
链路设置（WLAN）		
项目	**说明**	**默认**
常规设置		
索引	显示表序号。	--
类型	显示链路类型。	WLAN
描述	输入链路描述，可以为空。	空
连接类型	可选“DHCP”或“静态 IP”。	DHCP
WLAN 设置		
SSID	输入设备想要访问的接入点的 SSID。SSID（服务集标识）是指 WLAN 的网络名字，请输入 1~32 个字符。	router
连接到隐藏 SSID	单击切换按钮以启用/禁用“连接到隐藏 SSID”功能。当设备作为 WiFi Client 模式且需要连接已对外隐藏 SSID 的任何接入点时，这里必须要开启该功能。	OFF

链路设置（WLAN）		
项目	**说明**	**默认**
密码	输入设备想要访问的接入点的密码。请输入 8~63 个字符。	空
静态地址设置		
IP 地址设置	设置可以访问到互联网的 IP 加掩码，如 192.168.1.1/24。	空
网关	输入 WiFi AP 的 IP 地址作为设备的网关地址。	空
首选 DNS 服务器	设置首选的 DNS 服务器。	空
备用 DNS 服务器	设置备用的 DNS 服务器。	空
Ping 检测设置		
启用	单击切换按钮以启用/禁用 Ping 检测机制，其为设备的一项保留策略。	ON
首选服务器	设备 Ping 主地址/域名来检测当前网络连接是否正常。	8.8.8.8
备用服务器	设备 Ping 备用地址/域名来检测当前网络连接是否正常。	114.114.114.114
Ping 间隔	设置 Ping 的间隔时间。	300
Ping 重试间隔	设置 Ping 的重试间隔时间。当 Ping 失败后，设备重新 Ping 的时间间隔。	5
Ping 超时	设置 Ping 的超时时间。	3
Ping 单位	设置 Ping 的单位。单位：秒或者毫秒。	秒
最大尝试次数	设置 Ping 的最大尝试次数。如果达到最大的连续 ping 尝试次数，请切换到另一条链路或采取紧急行动。	3
高级设置		
启用 NAT	单击切换按钮以启用/禁用 NAT 功能。NAT 是 Network Address Translation，即网络地址转换。	ON
MTU	设置最大传输单元。	1500
上传带宽	设置用于 QoS 的上传带宽，单位为 kbps。	10000
下载带宽	设置用于 QoS 的下载带宽，单位为 kbps。	10000
指定首选 DNS 服务器	定义 DHCP 服务器分配给客户端的主要 DNS 服务器。	空
指定备用 DNS 服务器	定义 DHCP 服务器分配给客户端的备选 DNS 服务器。	空
启用调试	单击切换按钮以启用/禁用调试选项。开启：输出链路管理调试信息。	ON
启用详细调试	单击切换按钮以启用/禁用详细调试选项。开启：输出链路管理详细调试信息。	OFF

状态

本节用于查看当前链路的状态。

单击链路状态窗口右侧的•••，可选择当前链路的连接状态。



单击其中一行，将会显示链路连接的详细信息。

WWAN 使用数据统计和 WAN 使用数据统计分别统计蜂窝模块和 WAN 的数据包流量。

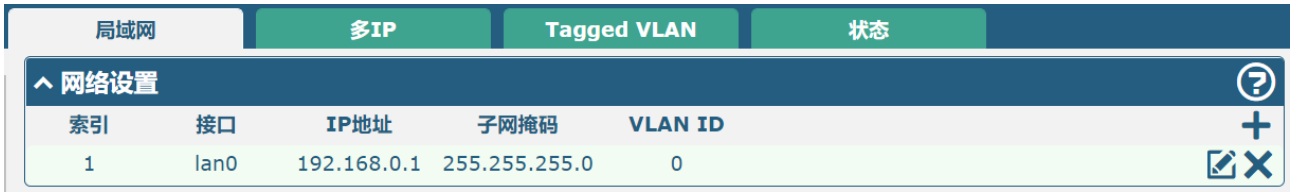
单击 清除 按钮即可清除 SIM1 或 SIM2 或 WAN 每月数据流量的使用统计信息。只有当启用**“接口 > 链路管理 >链路设置 > WWAN1/WWAN2/WAN”**设置中的“流量限制额度”功能或“流量统计”功能，此项数据统计才会显示。

3.2.2 局域网

本节用于配置局域网及相关参数。设备中可能有多个以太网端口，必须至少将一个 LAN 端口分配为 lan0，其默认 IP 为 192.168.0.1/255.255.255.0。

注：
1） R3000 Lite 只有一个以太网端口，只能分配为 LAN。
2） R2000 Lite 只有一个以太网端口，只能分配为 LAN。
3） R1510 Lite 只有一个以太网端口，只能分配为 LAN。

局域网



注：lan0 无法删除。

单击 以添加一个新的 LAN 口；单击 以删除当前的 LAN 口；单击 以编辑当前 LAN 口的配置。

常规设置@局域网		
项目	**说明**	**默认**
索引	显示表序号。	--
接口	显示当前编辑的接口。 ***注：****只有在“以太网 > 端口 > 端口设置”中选择 ETH1，ETH2，ETH3 或 ETH4 中的一个为 lan1 时，lan1 才可配。*	lan0
IPv4 地址	设置 LAN 口的 IP 地址。	192.168.0.1
子网掩码	设置 LAN 口的子网掩码。	255.255.255.0
MTU	设置最大传输单元。	1500

当“模式”选择“服务器”时，窗口如下所示：

当“模式”选择“中继”时，窗口如下所示：

局域网		
项目	**说明**	**默认**
DHCP 设置		
启用	单击切换按钮以启用/禁用 DHCP 功能。	ON
模式	选择 DHCP 的模式为“服务器”或“中继”。 • 服务器：租赁 IP 地址给连接上 LAN 口的 DHCP 客户端。 • 中继：设备可以成为 DHCP 中继，这将为解决 DHCP 客户端与 DHCP 服务器不在同一子网中的问题提供一条中继隧道。	服务器

起始 IPv4 地址池	定义给 DHCP 客户端分配地址的 IP 地址池开端。	192.168.0.2
结束 IPv4 地址池	定义给 DHCP 客户端分配地址的 IP 地址池结尾。	192.168.0.100
子网掩码	定义 DHCP 客户端从 DHCP 服务端获取的 IP 地址的子网掩码。	255.255.255.0
DHCP 中继代理	输入 DHCP 中继服务器的 IP 地址。	空
DHCP 高级设置		
网关	定义 DHCP 服务器分配给客户端的网关，必须与 DHCP 地址池在相同的网段。	空
首选 DNS 服务器	定义 DHCP 服务器分配给客户端的主要 DNS 服务器。	空
备用 DNS 服务器	定义 DHCP 服务器分配给客户端的备份 DNS 服务器。	空
WINS 服务器	输入 WINS 服务器的地址。Windows 系统因特网命名服务（WINS）管理局域网中的所有设备，可以为空。	空
租约时间	设置租约时间，单位为分钟。租约时间是指动态 IP 地址的网络用户占用 IP 地址的租约周期。	120
静态租约	通过 MAC 地址绑定租约，使其对应一个 IP 地址。 格式为 MAC,ip;MAC,ip;...，例如： FF:ED:CB:A0:98:01,192.168.0.200	空
专家选项	输入关于 DHCP 的高级选项。格式为 config-desc;config-desc，例如 log-dhcp;quiet-dhcp。	空
启用调试	单击切换按钮以启用/禁用调试功能。开启：输出 DHCP 信息到调试口。	OFF

多 IP

本节用于配置 LAN 口多 IP 地址

单击 以编辑 LAN 口的多 IP；单击 以删除 LAN 口的多 IP；单击 以添加一个新的多 IP。

IP 地址设置		
项目	**说明**	**默认**
索引	显示表序号。	--
接口	显示当前编辑的接口。	--
IP 地址	设置 LAN 口的 IP 地址。	空
子网掩码	设置 LAN 口的子网掩码。	空

VLAN 标记

本节用于配置 VLAN

单击 以编辑 LAN 口的 VLAN 标记 IP；单击 以删除 LAN 口的 VLAN 标记 IP；单击 以添加一个新的 LAN 口的 VLAN 标记 IP。

VLAN 设置		
项目	**说明**	**默认**
索引	显示表序号。	--
启用	单击切换按钮以启用/禁用 VLAN 功能。	ON
接口	显示当前编辑的接口。	--
VID	设置 VLAN ID，取值范围 从 1 到 4094。	100
IP 地址	设置 VLAN 的 IP 地址。	空

VLAN 设置		
项目	说明	默认
子网掩码	设置 VLAN 的子网掩码。	空

状态

本节用于显示局域网的连接状态等信息。

单击其中一行，其详细的状态信息将显示于当前行的下面。

3.2.3 以太网

本节用于设置以太网的相关参数。设备中可能有多个以太网端口。设备中的 ETH0 可以配置为 WAN 端口或 LAN 端口，而其他以太网端口只能配置为 LAN 端口。所有以太网端口的默认设置为 lan0，其默认 IP 为 192.168.0.1/255.255.255.0。

注:

1) R2000 Dual 可以通过 ETH1 ~ ETH4 向后面的设备供电（在端口设置中启用 POE）。

2) R3000 Lite 只有一个以太网端口，只能配置为 LAN。

3) R2000 Lite 只有一个以太网端口，只能配置为 LAN。

4) *R1510 Lite 只有一个以太网端口，只能配置为 LAN。*

端口

本节用于配置端口的类型。

单击 eth0 最右侧的，在弹出的端口窗口中修改网口的参数。

注:

1） R3000 Quad 和 R2000 系列设备不支持“端口启用”功能。

2） 仅 R3000 系列产品支持指定端口速率。

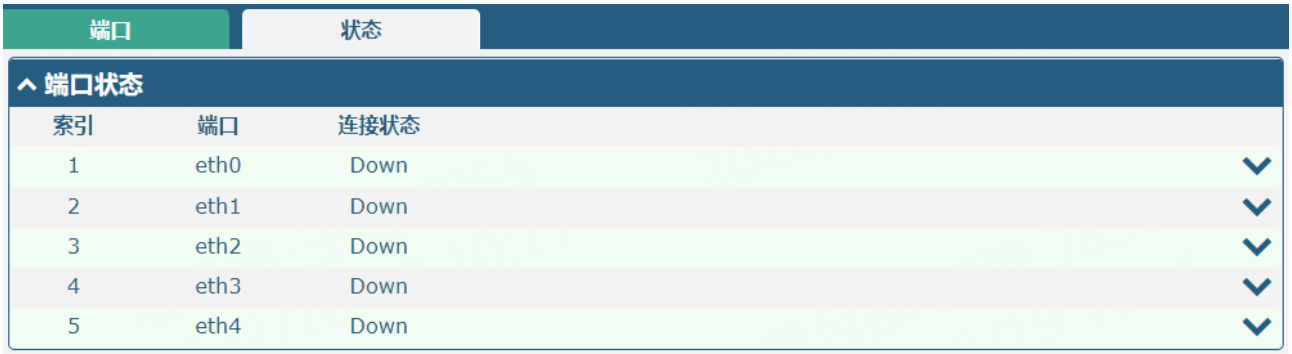
端口设置		
选项	**说明**	**默认**
索引	显示表序号。	--
端口	显示当前编辑的端口，无法编辑。	--
端口分配	选择网口的类型，WAN口或者LAN口。当在“接口 > 局域网 > 局域网 > 网络设置 > 常规配置”里设置其为LAN口时，可以下拉框选择lan0或lan1或lan2或lan3。	lan0
端口启用	单击以启用或禁用端口。	ON
端口速率（可选）	设置以太网端口速率。	
POE 启用（可选）	单击以启用或禁用POE功能。当POE功能启用时，它将连接POE电压。	ON

高级设置		
选项	**说明**	**默认**
启用转发加速引擎	单击以启用或禁用转发加速引擎功能。 转发加速引擎可以提高以太网端口速率，但会影响 QoS。	OFF

注：仅 R5020 支持“转发加速引擎”功能。

状态

本节用于查看端口连接的状态。



单击其中一行，其详细的状态信息将显示于当前行的下面。

3.2.4 蜂窝网

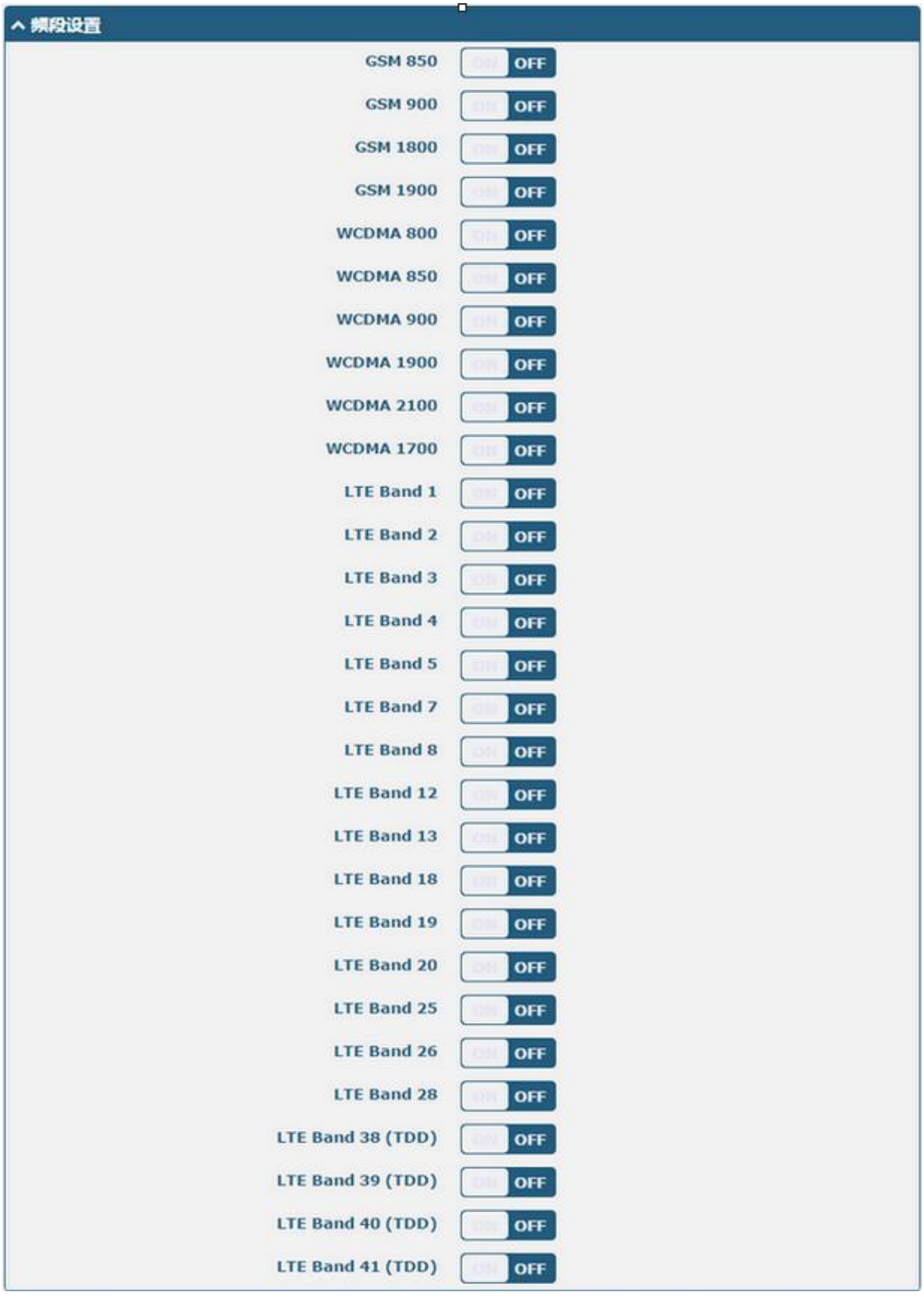
设置蜂窝网和相关参数。不同的设备会有一或两个 SIM 卡槽。

单击 SIM1 最右侧的 以编辑参数：

当“网络类型”选择“自动”时，窗口如下所示：

当“频段选择”选择“指定”时，窗口如下所示：

注：由于蜂窝模块的不同，频段设置可能存在一些差异。


频段设置
GSM 850 OFF
GSM 900 OFF
GSM 1800 OFF
GSM 1900 OFF
WCDMA 800 OFF
WCDMA 850 OFF
WCDMA 900 OFF
WCDMA 1900 OFF
WCDMA 2100 OFF
WCDMA 1700 OFF
LTE Band 1 OFF
LTE Band 2 OFF
LTE Band 3 OFF
LTE Band 4 OFF
LTE Band 5 OFF
LTE Band 7 OFF
LTE Band 8 OFF
LTE Band 12 OFF
LTE Band 13 OFF
LTE Band 18 OFF
LTE Band 19 OFF
LTE Band 20 OFF
LTE Band 25 OFF
LTE Band 26 OFF
LTE Band 28 OFF
LTE Band 38 (TDD) OFF
LTE Band 39 (TDD) OFF
LTE Band 40 (TDD) OFF
LTE Band 41 (TDD) OFF

蜂窝网		
项目	**说明**	**默认**
常规设置		
索引	显示表序号。	--
SIM 卡	显示当前编辑的SIM卡。	SIM1
电话号码	输入SIM卡的电话号码。	空
PIN 码	输入用于解锁 SIM 卡的 PIN 代码，4~8 位。	空
MCC+MNC 码	用于锁定设备使用指定运营商的 SIM 卡。SIM 卡的 IMSI 与设备配置不匹配时，无法使用该 SIM 卡。必须使用分号结尾，5~6 位	空
额外的 AT 命令	输入用于无线模块初始化的额外AT命令，提供给专家使用。	空
Telnet 端口	指定一个端口。用户通过Telnet连接设备此端口发送AT命令到蜂窝网模块。	0
等待更新 APN	连接网络后自动更新APN的时间间隔。单位：秒。 Modem需要支持自动更新APN。 例如：HL7618RD	90
蜂窝网网络设置		
网络类型	选择蜂窝网络类型，即网络访问顺序。可选“自动”，“仅用2G”，“2G优先”，“仅用3G”，“3G优先”，“仅用4G”或“4G优先”。 • 自动：自动连接到最佳信号网络 • 仅2G：仅连接2G网络 • 2G优先：优先接入2G网络 • 仅3G：仅连接3G网络 • 3G优先：优先接入3G网络 • 仅4G：仅连接4G网络 • 4G优先：优先接入4G网络 ***注：*** *1) 由于蜂窝模块的不同，可能存在一些不同的可选网络类型。* *2) 点击“？”帮助查看详细信息的菜单中的字符。*	自动

蜂窝网		
项目	**说明**	**默认**
频段选择	可选“全部”或“指定”。当选择“指定”时，用户可以选择某些特定频段。	全部
高级设置		
启用调试	单击切换按钮以启用/禁用调试选项。开启：输出链路管理调试信息。	ON
启用调试	单击切换按钮以启用/禁用此选项。开启：输出调试信息。	ON
启用详细调试	单击切换按钮以启用/禁用详细调试选项。开启：输出链路管理详细调试信息。	OFF
网络注册超时	模块注册到网络所需的超时时间。单位：秒。 0 表示使用默认设置。	0
首选 CID3	有些运营商需要使用 APN3 才能正常上网，就像 Verizon 一样，可根据实际情况开启。	OFF
启用自定义 APN 列表	启用客户自定义导入的 APN 列表	ON

状态

本节用于查看蜂窝网的状态信息。

单击其中一行，其详细的状态信息将显示于当前行的下面。

蜂窝网信息	
项目	**说明**
索引	显示表序号。
Modem 状态	显示无线模块的运行状态。
Modem 型号	显示无线模块的型号。
当前 SIM 卡	显示设备当前使用的SIM卡：SIM1或者SIM2。
电话号码	显示当前SIM卡的电话号码。 ***注：****此选项需在“**蜂窝网 > 高级蜂窝网设置 > SIM1/SIM2 > 电话号码**”中手动填入。*

蜂窝网信息	
项目	**说明**
IMSI	显示当前SIM卡的IMSI码。
ICCID	显示当前SIM卡的ICCID码。
注册状态	显示当前的网络状态。
运营商	显示当前注册网络的运营商。
网络类型	显示当前的网络服务类型。
5G 架构	显示当前5G的类型。SA或则NSA。该选项仅在5G的产品上显示。
频段	显示当前使用的频段。
信号强度	显示当前的信号强度。（适用于2G, 3G和4G网络。5G网络请参阅5G网络的RSRP）
参考信号接收功率	显示当前参考信号接收功率。（仅适用于4G网络或5G网络）
参考信号接收质量	显示当前参考信号接收质量。（仅适用于4G网络或5G网络）
载干比	注册到3G网络时显示载干比
运营商识别号	显示当前运营商识别号。
位置区码	显示当前的位置区码，用于标识不同的位置区。
小区号	显示当前的小区号，用于定位设备。
IMEI	显示无线模块的IMEI码。
固件版本	显示当前无线模块的固件版本。
信号与干扰加噪声比	显示当前信号与干扰加噪声比。（仅适用于4G网络或5G网络）
物理小区号	显示物理小区标识。

AT 调试

本节用于 AT 命令调试。

AT 命令调试		
项目	说明	默认
命令	在文本框中输入您要发送给蜂窝网模块的AT命令。	空
结果	设备在该文本框中显示移动通信模块回应的AT命令。	空
发送	单击该按钮以发送AT命令。	--

3.2.5 Wi-Fi

本节用于配置 Wi-Fi AP 和 Wi-Fi 客户端的参数。设备支持 Wi-Fi AP 和 Wi-Fi 客户端功能，出厂默认为 Wi-Fi AP。

Wi-Fi AP

设置设备作为 Wi-Fi AP，选择“AP”作为模式，然后单击“提交”。

仅支持 2.4 GHz Wi-Fi：

支持 2.4 GHz 和 5 GHz Wi-Fi：

注：

1) R5020/R2110 支持 2.4GHz 和 5 GHz Wi-Fi。

*2) 完成配置后，请单击“**提交**”和“**应用**”，配置方可生效。*

接入点 2.4G

单击“接入点 2.4G”栏以配置 Wi-Fi AP 的参数，其“安全模式”默认为“公开”。

当“安全模式”选择“WPA-个人”时，窗口显示如下：

当“安全模式”选择“WEP”时，窗口显示如下：

常规设置@接入点 2.4G		
项目	**说明**	**默认**
启用	单击切换按钮以启用/禁用 Wi-Fi AP 功能。	OFF
无线模式	可选“11bgn 混合模式”、“仅 11B”、“仅 11g”或“仅 11n”。 • 11bgn 混合模式：三个协议混合，为了向后兼容。 • 仅 11b：IEEE 802.11b，11 Mbps，2.4GHz。 • 仅 11g：IEEE 802.11g，54 Mbps，2.4GHz。 • 仅 11n：IEEE 802.11n，300 Mbps。	11bgn 混合模式
带宽	可选信道宽度为“20MHz”或“40MHz”。 ***注：****40MHz 信道带宽提供的可用数据传输速率是单条 20MHz 信道的两倍多。*	20MHz
通道	不同带宽可选的通道如下： • 自动：设备会一直扫描所有的频率，直到找到一个可用的接入点或者可以接入的无线网络 • 20MHz 带宽可用信道对应的 1~13 频道的频率： 1–2412 MHz 2–2417 MHz 3–2422 MHz 4–2427 MHz 5–2432 MHz 6–2437 MHz 7–2442 MHz 8–2447 MHz 9–2452 MHz 10–2457 MHz 11–2462 MHz 12–2467 MHz 13–2472 MHz	自动

	• 40MHz 带宽可用信道对应的 1~13 频道的频率： 1–2412 MHz 2–2417 MHz 3–2422 MHz 4–2427 MHz 5–2432 MHz 6–2437 MHz 7–2442 MHz 8–2447 MHz 9–2452 MHz 10–2457 MHz 11–2462 MHz 12–2467 MHz 13–2472 MHz	
SSID	输入 SSID（服务集标识），即 WLAN 的网络名字。客户端和 AP 的 SSID 必须完全一致以使它们可以相互通信。当设备作为客户端模式时，键入其要连接的接入点 SSID。请输入 1-32 的字符。	RBT-XXXX-2.4G
广播 SSID	单击切换按钮以启用/禁用广播 SSID 功能。当开关切换为“OFF”时，其它无线设备不能自动发现这个无线接入点。用户必须在其它无线设备上手动键入 SSID 让它们可以接入设备 AP 发出的无线网络。	ON
安全模式	可选“公开”、“WPA-个人”、“WEP”。 • 公开：用户可以无密码访问 AP，无需身份验证和数据加密。 ***注：****为了安全起见，尽量不要设置安全模式为“公开”。* • WPA-个人：Wi-Fi 访问保护，只能提供一个密码用于身份认证。 • WEP：Wired Equivalent Privacy 有线等效保密，为无线设备提供加密的数据传输。	公开
WPA 版本	可选“自动”、“WPA”和“WPA2”和“WPA3*”。 • 自动：设备会自动选择最合适的 WPA 模式。 • WPA2 的安全特性比 WPA 更强。 *** 注：**R151x 和 R201x 支持 WPA3。	自动
加密	可选“TKIP”和“AES”。 • TKIP：临时密钥完整性协议（TKIP）加密使用无线连接。TKIP 加密可以用于 WPA-PSK 和 WPA 802.1 x 认证。 • AES：AES 加密使用无线网络。可以使用 CCMP WPA-PSK 和 WPA 802.1 x 认证。AES 是一种比 TKIP 更强的加密算法。 ***注：****加密模式会影响到无线速率，不同的无线模式对加密模式支持不一样。如 802.11n 不支持 WEP 安全模式，也不支持 TKIP 算法，如强制使用，无线速率会降到 54Mbps，即切换到了 802.11g 模式。在 802.11n 的模式下推荐使用 AES 加密*	AES

	算法。	
PSK 密码	输入预共享密钥。请输入 8~63 字符。	空
组密钥更新间隔	输入组密钥更新间隔。	3600
WEP 密钥	输入 WEP 密钥。密钥长度应该是 10 或 26 个 16 进制字符，这取决于使用的是 64 位还是 128 位的 WEP。	空

高级设置@接入点 2.4G		
项目	**说明**	**默认**
最大接入点个数	设置允许接入设备 AP 的最大客户端个数。（0 值代表没有限制）	0
信号间隔	设置设备 AP 广播 Beacon 报文的信号间隔，用于声明某个无线网络的存在。	100
DTIM 周期	设置 Delivery Traffic Indication Message 周期，即交付传输指示信息的周期。DTIM 用于省电模式中，设备 AP 会根据这个时间间隔来组播流量。	2
启用 Short GI	单击切换按钮以启用/禁用 Short Guard Interval，即短保护间隔。其为两个符号之间的空白时间段，给信号延迟提供了缓冲时间。使用短的保护间隔可以增加 11%的数据率，但也会导致更高的包出错率。	ON
启用 AP 隔离	单击切换按钮以启用/禁用 AP 隔离选项。启用后，隔离所有连接的无线设备，使各个无线设备之间无法互相访问。	OFF
调试等级	选择调试等级。可选“verbose”、“debug”、“info”、“notice”、“warning”或“none”。	none

单击➕以添加 MAC 地址到访问控制列表中，最多可添加 64 个 MAC 地址。

ACL 设置@接入点 2.4G		
项目	**说明**	**默认**
启用 ACL	单击切换按钮以启用/禁用访问控制列表。	OFF
ACL 模式	选择 ACL 模式。可选“接受”或“拒绝”。 • 接受：只有在访问控制列表里面的地址才能访问设备 AP。 • 拒绝：在访问控制列表里的地址都被拒绝访问设备 AP。 ***注：****设备只能接受或拒绝存在于访问控制列表里的设备。*	接受
访问控制列表@接入点 2.4G		
索引	显示表序号。	--
描述	输入对此访问控制列表的描述。	空
MAC 地址	在此添加 MAC 地址。	空

接入点 5G

单击“接入点 5G”栏以配置 Wi-Fi AP 的参数，其“安全模式”默认为“公开”。

当“安全模式”选择“WPA-个人”时，窗口显示如下：

当“安全模式”选择“WEP”时，窗口显示如下：

常规设置@接入点 5G		
项目	**说明**	**默认**
启用	单击切换按钮以启用/禁用 Wi-Fi AP 功能。	OFF
无线模式	可选“11a/n”或“11/a/n/ac”。 • 11a/n：兼容 IEEE 802.11a(最高速率为 54 Mbps)和 IEEE 802.11n(最高速率为 300Mbps)。 • 11a/n/ac：兼容 IEEE 802.11a(最高速率为 54 Mbps)、IEEE802.11n(最高速率为 300 Mbps)和 802.11ac(最高速率为 867 Mbs)。	11a/n
带宽	可选信道宽度为“20MHz”，“40MHz”或“80MHz”。 ***注：****40MHz 信道带宽提供的可用数据传输速率是单条 20MHz 信道的两倍多；80MHz 信道带宽提供的可用数据传输速率是单条 20 MHz 的四倍多。*	20MHz
通道	不同带宽可选的通道如下： • 20MHz 带宽可用信道对应的 36~165 频道的频率： 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz • 40MHz 带宽可用信道对应的 36~165 频道的频率： 36–5180 MHz 40–5200 MHz 44–5220 MHz	36

	48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz • 80MHz 带宽可用信道对应的 36~165 频道的频率（仅无线模式为 11ac 使用）： 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz ***注：****以上列出了 5GHz Wi-Fi 在不同频宽的所有可用信道，不同国家和地区可用的信道不一样，需要 WEB 页面配置区域。*	
SSID	输入 SSID（服务集标识），即 WLAN 的网络名字。客户端和 AP 的 SSID 必须完全一致以使它们可以相互通信。当设备作为客户端模式时，键入其要连接的接入点 SSID。请输入 1-32 的字符。	RBT-XXXX-5G
广播 SSID	单击切换按钮以启用/禁用广播 SSID 功能。当开关切换为“OFF”时，其它无线设备不能自动发现这个无线接入点。用户必须在其它无线设备上手动键入 SSID 让它们可以接入设备 AP 发出的无线网络。	ON
安全模式	可选“公开”、“WPA-个人”或“WEP”。 • 公开：用户可以无密码访问 AP，无需身份验证和数据加密。 ***注：****为了安全起见，尽量不要设置安全模式为“公开”*。 • WPA-个人：Wi-Fi 访问保护，只能提供一个密码用于身份认证。 • WEP：Wired Equivalent Privacy 有线等效保密，为无线设备提供加密的数据传输。	公开
WPA 版本	可选“自动”、“WPA”和“WPA2”。 • 自动：设备会自动选择最合适的 WPA 模式。 • WPA2 的安全特性比 WPA 更强。	自动
加密	可选“TKIP”和“AES”。 • TKIP：临时密钥完整性协议（TKIP）加密使用无线连接。TKIP 加密可以用于 WPA-PSK 和 WPA 802.1 x 认证。 • AES：AES 加密使用无线网络。可以使用 CCMP WPA-PSK 和 WPA 802.1 x 认证。AES 是一种比 TKIP 更强的加密算法。 ***注：****加密模式会影响到无线速率，不同的无线模式对加密模*	AES

	式支持不一样。如 802.11n 不支持 WEP 安全模式，也不支持 TKIP 算法，如强制使用，无线速率会降到 54MBps，即切换到了 802.11g 模式。在 802.11n 的模式下推荐使用 AES 加密算法。	
PSK 密码	输入预共享密钥。请输入 8~63 字符。	空
组密钥更新间隔	输入组密钥更新间隔。	3600
WEP 密钥	输入 WEP 密钥。密钥长度应该是 10 或 26 个 16 进制字符，这取决于使用的是 64 位还是 128 位的 WEP。	空

高级设置@接入点 5G		
项目	**说明**	**默认**
最大接入点个数	设置允许接入设备 AP 的最大客户端个数。（0 值代表没有限制）	0
信号间隔	设置设备 AP 广播 Beacon 报文的信号间隔，用于声明某个无线网络的存在。	100
DTIM 周期	设置 Delivery Traffic Indication Message 周期，即交付传输指示信息的周期。DTIM 用于省电模式中，设备 AP 会根据这个时间间隔来组播流量。	2
RTS/CTS 阀值	设置 Request To Send 阀值，即请求发送阀值。当阈值设置为 2347，设备 AP 在送出数据之前不会发送检测信号；当阈值设置为 0 时，设备 AP 在送出数据前一定会发送检测信号。	2347
分片阀值	设置 Wi-Fi AP 数据包的分包阈值。建议默认为 2346。	2346
发射功率	选择发射功率级别。可选“最大”、“高”、“中”或“低”。	最大
启用 WMM	单击切换按钮以启用/禁用 WMM 选项。	ON

启用 Short GI	单击切换按钮以启用/禁用 Short Guard Interval，即短保护间隔。其为两个符号之间的空白时间段，给信号延迟提供了缓冲时间。使用短的保护间隔可以增加 11%的数据率，但也会导致更高的包出错率。	ON
启用 AP 隔离	单击切换按钮以启用/禁用 AP 隔离选项。启用后，隔离所有连接的无线设备，使各个无线设备之间无法互相访问。	OFF
调试等级	选择调试等级。可选“verbose”、“debug”、“info”、“notice”、“warning”或“none”。	none

单击➕以添加 MAC 地址到访问控制列表中，最多可添加 64 个 MAC 地址。

访问控制列表设置@接入点 5G		
项目	**说明**	**默认**
启用 ACL	单击切换按钮以启用/禁用访问控制列表。	OFF
ACL 模式	选择 ACL 模式。可选“接受”或“拒绝”。 • 接受：只有在访问控制列表里面的地址才能访问设备 AP。 • 拒绝：在访问控制列表里的地址都被拒绝访问设备 AP。 ***注：****设备只能接受或拒绝存在于访问控制列表里的设备。*	接受
访问控制列表		
索引	显示表序号。	--
描述	输入对此访问控制列表的描述。	空
MAC 地址	在此添加 MAC 地址。	空

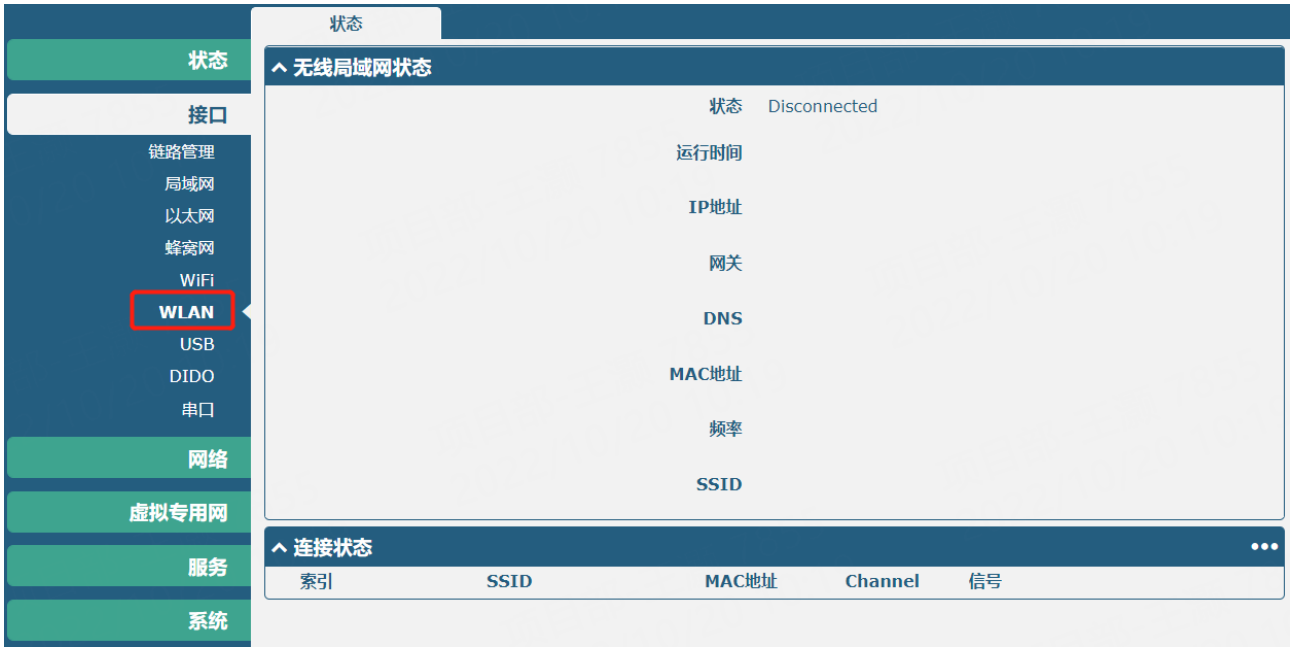
单击“状态”栏以查看 AP 的连接状态。

Wi-Fi 客户端

配置设备作为 Wi-Fi 客户端

选择“客户端”作为模式，根据连接 AP 类型选择相应的客户端模式，并单击“提交”。

随后“接口”列表会出现“WLAN”一栏，显示如下：



单击“**接口 > 链路管理 > 链路设置**”，并单击 WLAN 的编辑按钮，在弹出的“**WLAN 设置**”窗口内配置 Wi-Fi 客户端的参数。

单击“**接口 > WLAN**”以查看 Wi-Fi 客户端的参数。

3.2.6 USB

本节用于配置 USB 的参数。设备的 USB 接口可以用于升级固件和更新配置。

密钥

本节用于 USB 的密钥生成和下载。

USB		
项目	**说明**	**默认**
常规设置		
启用 USB	单击切换按钮以启用/禁用USB功能。	ON
启用 USB 自动升级	单击切换按钮以启用/禁用该选项。在插入带有设备固件与其它相关文件的USB存储设备后，设备会自动升级固件。	OFF
密钥		
USB 自动升级密钥	单击 生成密钥 按钮，即可生成密钥。单击 下载密钥 按钮，即可下载密钥。	--

注：*使用 USB 自动升级功能时，当出现跑马灯效果时，表示正在升级中，当跑马灯效果停止，USER 灯亮起时表示升级完成。升级后，设备不会自动重启。如一直没有出现跑马灯效果表示存在异常，没有进入到自动升级流程。*

3.2.7 DI/DO

本节用于设置数字输入（DI）和数字输出（DO）的参数。数字输入可用来触发告警，数字输出可用来控制下端设备，以此达到实时监控设备的目的。

DI

单击 DI 索引 1 最右边的按钮，其“模式”默认为“电平”，显示如下：

当“模式”选择为“计数”时，显示如下：

DI（数字输入）		
项目	**描述**	**默认值**
索引	显示表序号。	--
启用	单击切换按钮为“ON”以开启数字输入功能。	OFF
模式	可选择“电平”或“计数”。 • 电平：处于DI接入电平即可触发告警模式。	电平

	• 计数：处于事件计数器模式。	
反向	计数分为电平的上升沿计数或者是下降沿计数两种。如果当前是上升沿计数，开启反向之后就是下降沿计数。	OFF
门限值	门限值是模式为计数时特有的参数。设置门限值，当计数值到达门限值时触发DI告警。	0
告警触发内容	触发DI告警时发送的信息内容。	Alarm On
告警消除内容	消除DI告警时发送的信息内容。	Alarm Off

注：*默认高电平告警，开启“反向”之后变成低电平告警。*

DO

单击 DO 索引 1 最右边的按钮，显示如下：

当“告警触发动作”选择为“脉冲”时，窗口显示如下：

当“告警消除动作”选择为“脉冲”时，窗口显示如下：

DO（数字输出）		
项目	**描述**	**默认值**
索引	显示表序号。	--
启用	单击切换按钮为“ON”以开启数字输出功能。	OFF

告警触发动作	当告警触发时，数字输出启动。可选择“高电平”，“低电平”或“脉冲”。 • 高：高电平输出。 • 低：低电平输出。 • 脉冲：触发时产生脉冲模式参数中指定的方波。	高电平
告警消除动作	当告警消除后，数字输出启动。可选择“高电平”，“低电平”或“脉冲”。 • 高电平：高电平输出。 • 低电平：低电平输出。 • 脉冲：触发时产生脉冲模式参数中指定的方波。	低电平
初始状态	指定上电时的数字输出状态。可选择“上一次”，“高电平”或“低电平”。 • 上一次：DO 的状态将与上次断电的状态一致。 • 高电平：DO 接口处于高电平。 • 低电平：DO 接口处于低电平。	上一次
延时	设置数字输出告警启动的延时。输入0-3000（0=直接生成脉冲，没有delay）。单位：100ms。	0
保持时间	输入数字输出状态保持的时间。当数字输出产生“告警触发动作”或“告警消除动作”状态为“高电平”时可用。输入 0-3000 秒（0：一直保持当前状态直到下一个动作出现）。单位：秒。	0
低电平脉宽	指定低电平的宽度。在脉冲输出模式下，选定的数字输出通道将生成一个预先定义好的方波。输入 1000-3000。单位：ms。	1000
高电平脉宽	指定高电平的宽度。在脉冲输出模式下,选定的数字输出通道将生成一个预先定义好的方波。输入 1000-3000。单位：ms。	1000
告警源	数字输出启动可以由该告警激活。	DI1

状态

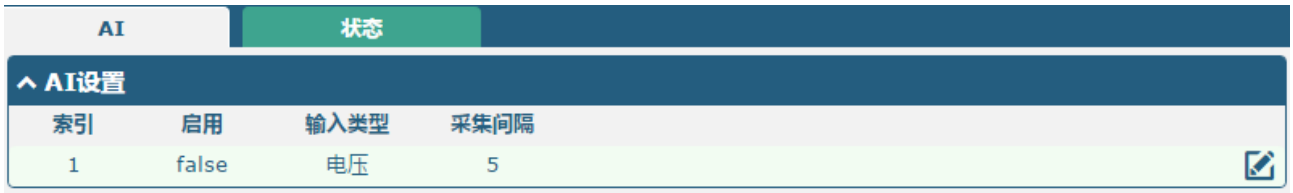
本节用于查看 DI/DO 的状态。单击 清除 按钮即可清除 DI 1 或 DI 2 每月计数器告警的使用统计信息。

3.2.8 AI

本节用于设置模拟输入（AI）的参数。模拟输入用于对一定量程范围内的模拟信号进行采集，常用于采集传感器的电压、电流、温度、压力等连续变化的值。模拟输入所用到的 ADC 位数精度越高，模拟量化就越精细，结果就越准确。

注：

1） R1520 支持 AI 接口



单击 AI 索引 1 最右边的按钮，其“输入类型”默认为“电压”，显示如下：

当“输入类型”选择为“电流”，显示如下：

AI（模拟输入）		
项目	**描述**	**默认值**
索引	显示表序号。	--
启用	单击切换按钮为“ON”以开启模拟输入功能。	OFF
输入类型	可选择“电压”或“电流”。 • 电压：采集到的数据为电压。 • 电流：采集到的数据为电流。	电压
最小电压门限	设置最小电压门限，当AI接口采集到的电压小于最小电压门限时，会激发事件通知。单位：V。	3
最大电压门限	设置最大电压门限，当AI接口采集到的电压大于最小电压门限时，会激发事件通知。单位：V。	20
最小电流门限	设置最小电流门限，当AI接口采集到的电流小于最小电压门限时，会激发事件通知。单位：mA。	4

最大电流门限	设置最大电流门限，当AI接口采集到的电流大于最小电压门限时，会激发事件通知。单位：mA。	16
采集间隔	每隔多少秒采集一次最新的数据。单位：秒。	5

状态

本节用于查看 AI 的状态。

3.2.9 串口

本节用于设置串口参数。可以将串口数据转换成 IP 数据或者通过 IP 数据转换成串口数据，然后通过有线或无线网络传送数据，从而实现数据透明传输的功能。COM1 表示 RS232，COM2 表示 RS485。

注：

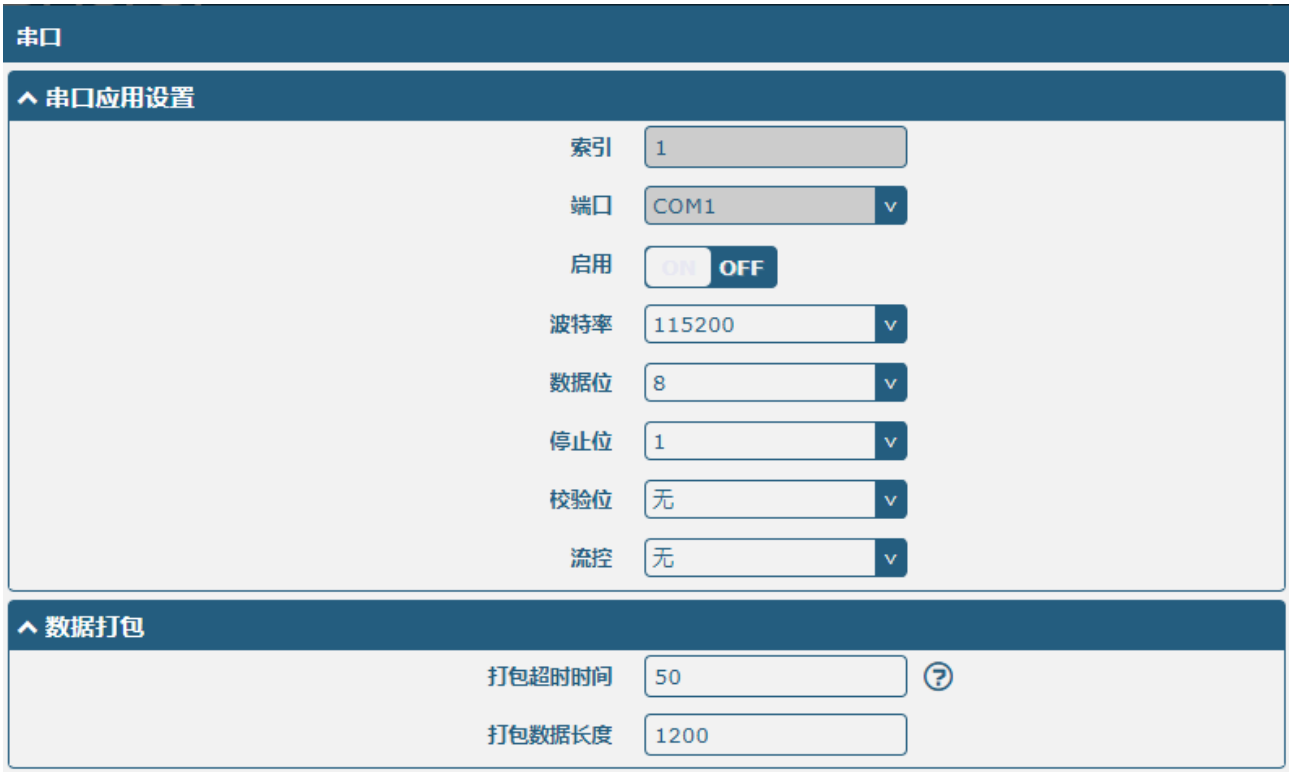
1） R2010，R3000-Quad 串行端口支持配置为 RS232 或 RS485。

串口		
项目	**描述**	**默认值**
串口类型	支持RS485或RS232	RS485

串口

本节用于配置串口。

单击 COM1 最右端的 按钮，弹出窗口如下：

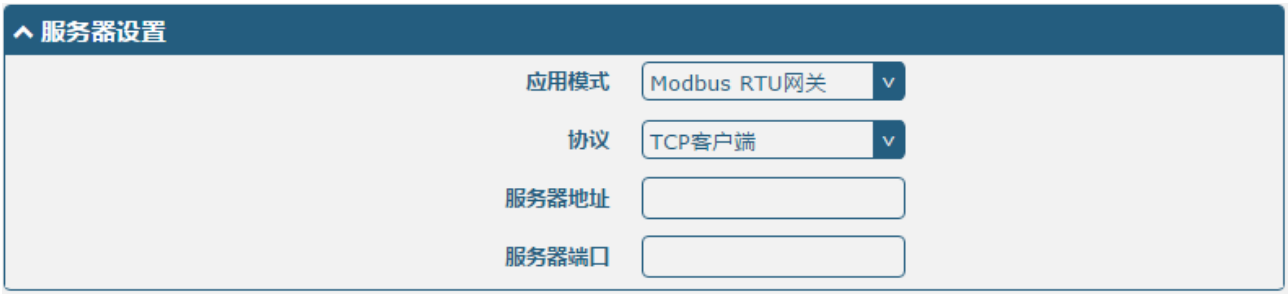


在“服务器设置”一栏，当选择“透传”作为应用模式，“TCP 客户端”作为协议时，窗口如下所示：

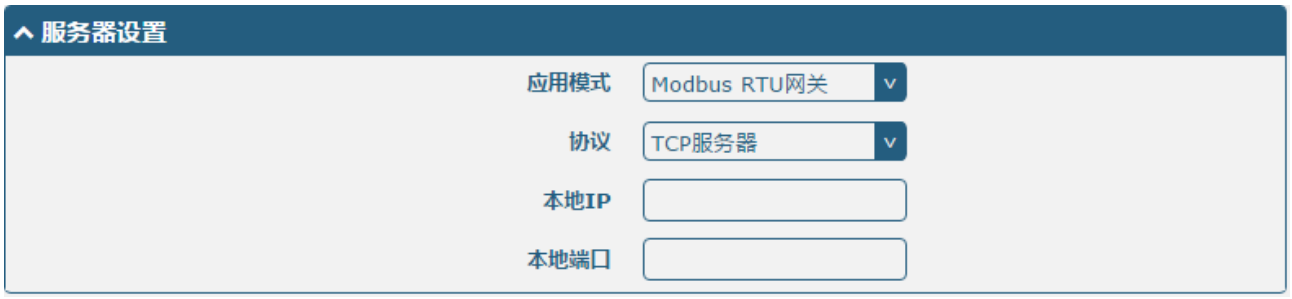
当选择“透传”作为应用模式，“TCP 服务器”作为协议时，窗口如下所示：

当选择“透传”作为应用模式，“UDP”作为协议时，窗口如下所示：

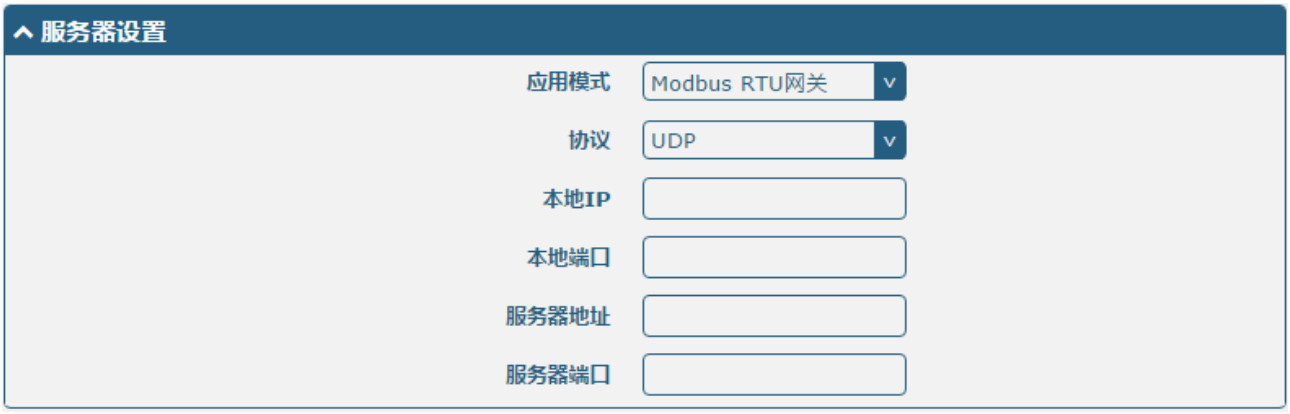
当选择“Modbus RTU 网关”作为应用模式，“TCP 客户端”作为协议时，窗口如下所示：



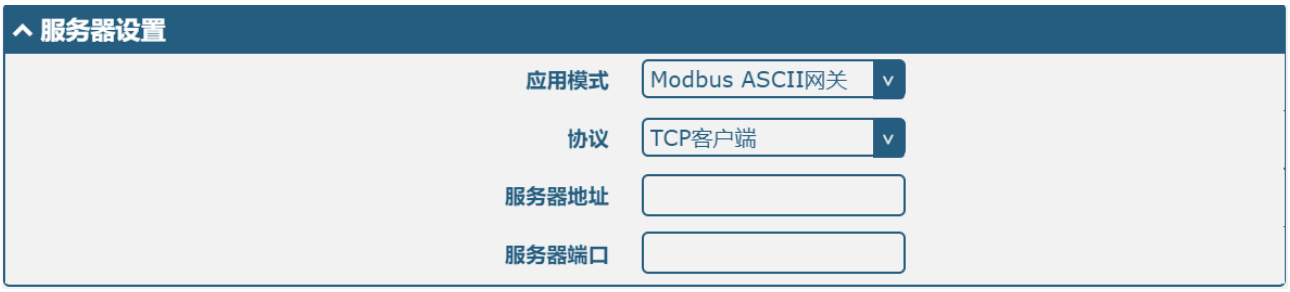
当选择“Modbus RTU 网关”作为应用模式，“TCP 服务器”作为协议时，窗口如下所示：



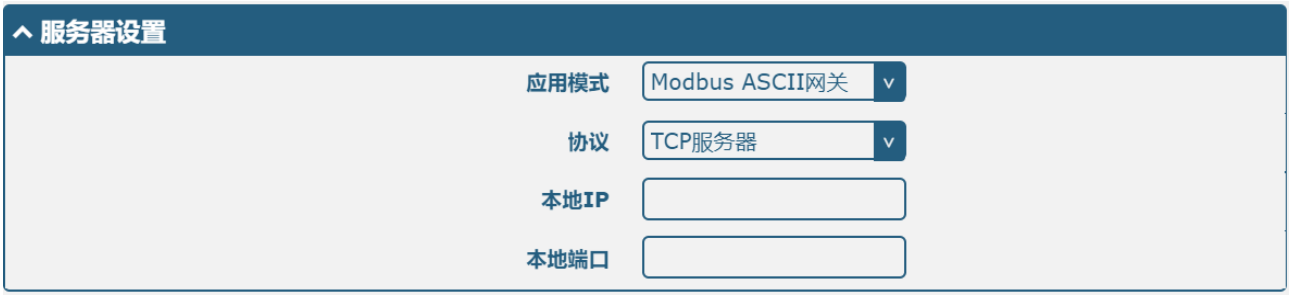
当选择“Modbus RTU 网关”作为应用模式，“UDP”作为协议时，窗口如下所示：



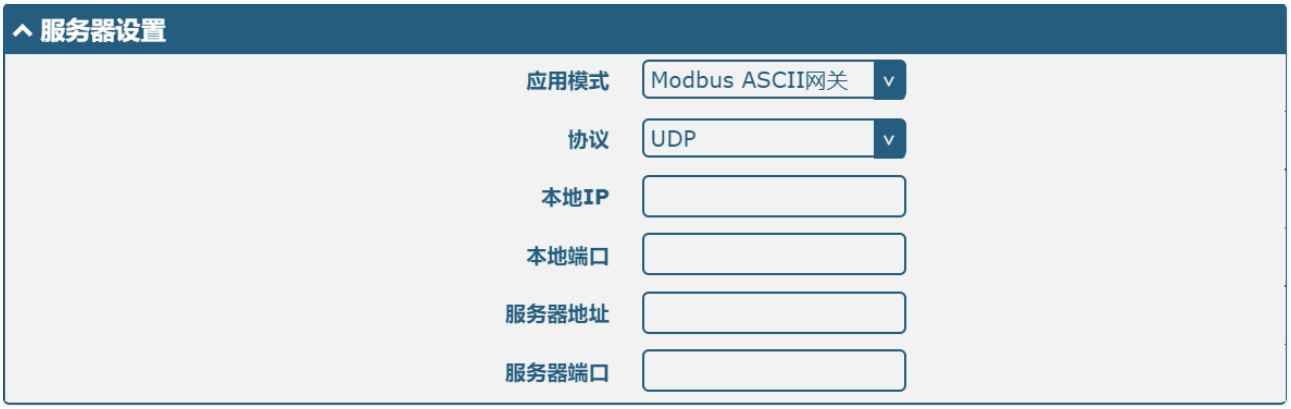
当选择“Modbus ASCII 网关”作为应用模式，“TCP 客户端”作为协议时，窗口如下所示：



当选择“Modbus ASCII 网关”作为应用模式，“TCP 服务器”作为协议时，窗口如下所示：



当选择“Modbus ASCII 网关”作为应用模式，“UDP”作为协议时，窗口如下所示：



串口		
项目	**说明**	**默认**
串口应用设置		
索引	显示表序号。	--
端口	显示当前串口的名字，无法编辑。	COM1
启用	单击切换按钮以启用/禁用此端口。当选项为 OFF 时，表示串行端口不可用。	OFF
波特率	支持“300”，“600”，“1200”，“2400”，“4800”，“9600”，“19200”，“38400”，“57600”，“115200”。	115200
数据位	支持选择“7”和“8”。	8
停止位	支持选择“1”和“2”。	1
校验位	支持选择“无”，“奇校验”和“偶校验”。	无
流控	支持选择“无”，“硬件”和“软件”。	无
数据打包		
打包超时时间	设置打包超时时间。串口把数据排列在缓冲区，当达到间隔超时时间时，它就会把数据发送到移动广域网/以太网广域网。单位为毫秒。 ***注：****即使未达到间隔超时时间，当与被指定包长度或设置的定界符一样时，数据也会被发送。*	50
打包数据长度	设置打包数据长度。包长度设置指的是在发送之前，串口缓冲区允许积累的最大数据量。当包长度设置为 0 时，没有指定最大数据量；当达到指定的间隔超时时间时，检测到设定的定界符时或缓冲区满时，缓冲区的数据就会被发送出去；当包长度指定为 1 到 3000 字节之间时，缓冲区数据达到指定长度时会被发送出去。 ***注：****即使没达到预设的包长度，当达到指定的间隔超时时间或设置的定界符，数据也会被发送出去。*	1200
服务器设置		
应用模式	从“透传”、“Modbus RTU 网关”、“Modbus ASCII 网关”中选择。 • 透传：设备将透明地传输未用任何协议封装的串行数据 • Modbus RTU 网关：设备将 Modbus RTU 数据转变为 Modbus TCP 数据，反之亦然。 • Modbus ASCII 网关：设备将 Modbus ASCII 数据转变为 Modbus TCP 数据，反之亦然。	透传
协议	从“TCP 客户端”，“TCP 服务器”，“UDP”中选择。 • TCP 客户端：设备作为 TCP 客户端，发起到 TCP 服务器端的 TCP 连接。服务器地址既可以是 IP 地址又可以是域	TCP 客户端

	名。 • TCP 服务器：设备作为 TCP 服务器端，监听来自 TCP 客户端的连接请求。 • UDP：设备作为 UDP 的客户端。	
服务器地址	输入对端服务器的地址。	空
服务器端口	输入对端服务器的端口。	空
本地 IP@透传	输入设备的 IP 地址。	空
本地端口@透传	输入 TCP 或 UDP 的本地端口。	空
本地 IP@Modbus 网关	输入设备的 IP 地址。	空
本地端口@ Modbus 网关	输入 Modbus 的本地端口。	空

状态

本节用于查看当前串口的状态。

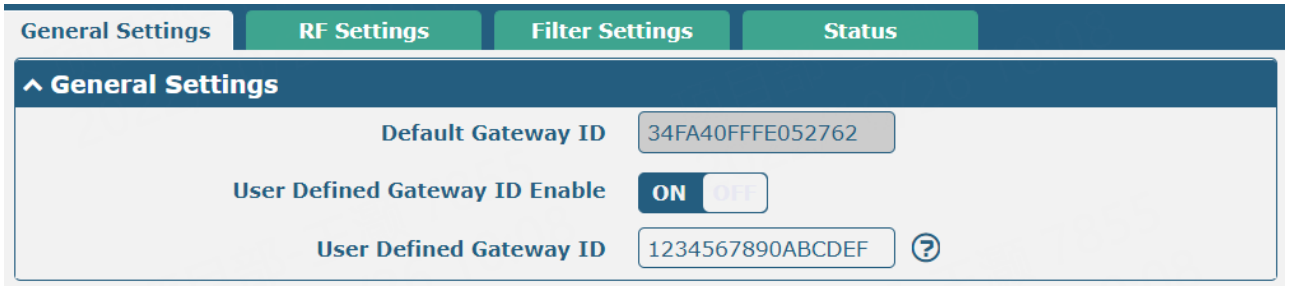
项目	状态
TX	发送数据到串口
RX	接收到串口数据

3.2.10 LoRa

此节用于设置 LoRaWAN 参数。仅适用于 R3000-LG。

General Settings

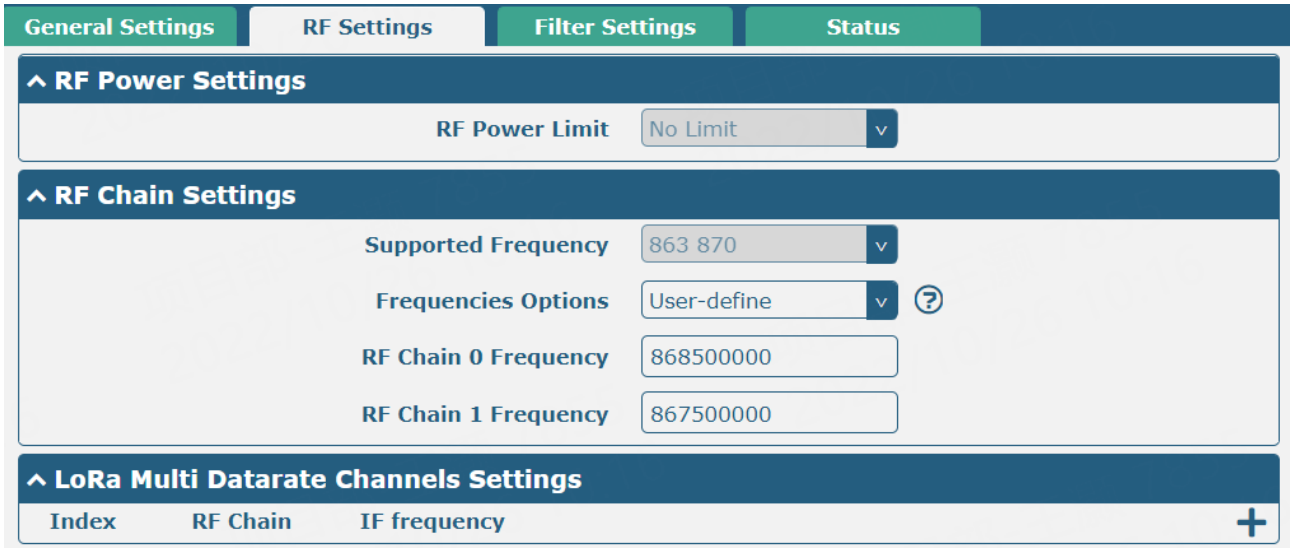
本节用于配置网关 ID 。如下所示。



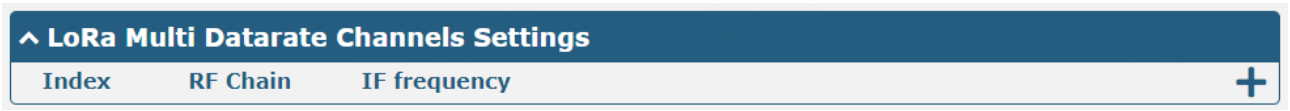
General Settings		
项目	**说明**	**默认值**
Default Gateway ID	设置默认网关ID或自定义一个唯一的64位的序列号。	空
User Defined Gateway ID Enable	单击切换按钮以启用/禁用此选项。	OFF
User Defined Gateway ID	输入自定义的网关ID。	空

RF Settings

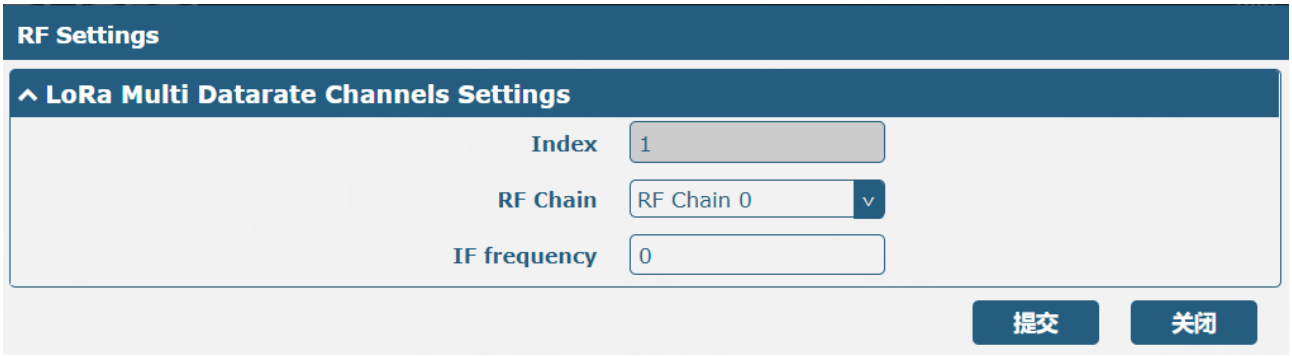
本节用于修改射频设置。



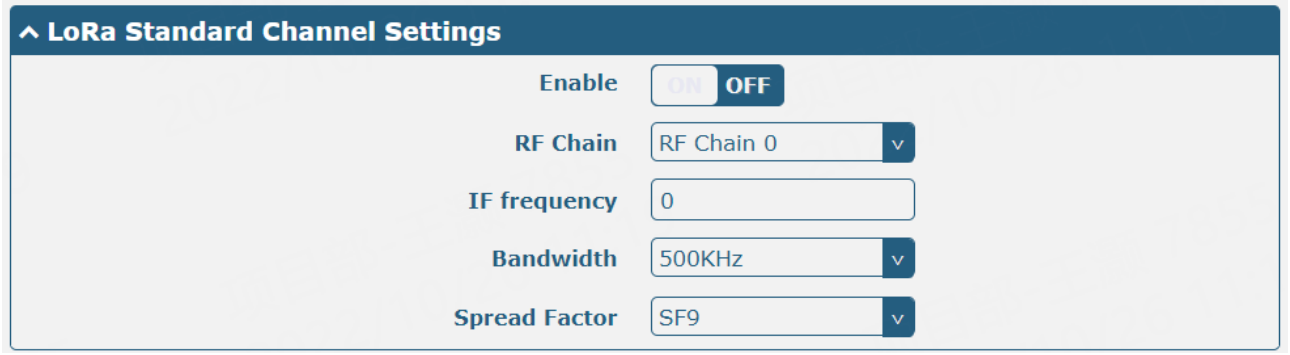
RF Settings		
项目	说明	默认值
RF Power Settings		
RF Power Limit	显示射频功率限制。	No Limit
RF Chain Settings		
Support Frequency	显示支持的频率。	863 870
Frequencies Options	设置链路频率。 EU868: 868.1,868.3,868.5,867.1,867.3,867.5,867.7,867.9, STD 868.3 and FSK 868.8; RU868: RF Chain 0:869000000,RF Chain 1:864500000, 868.9,869.1,869.3,864.1,864.3,864.5,864.7,864.9; KZ868: RF Chain 0:865300000,RF Chain 1:867500000, 865.1,865.3,865.5,867.1,867.3,867.5,867.7,867.9.	User-define
RF Chain 0 Frequency	设置射频链路0的频率。	868500000
RF Chain 1 Frequency	设置射频链路1的频率。	867500000



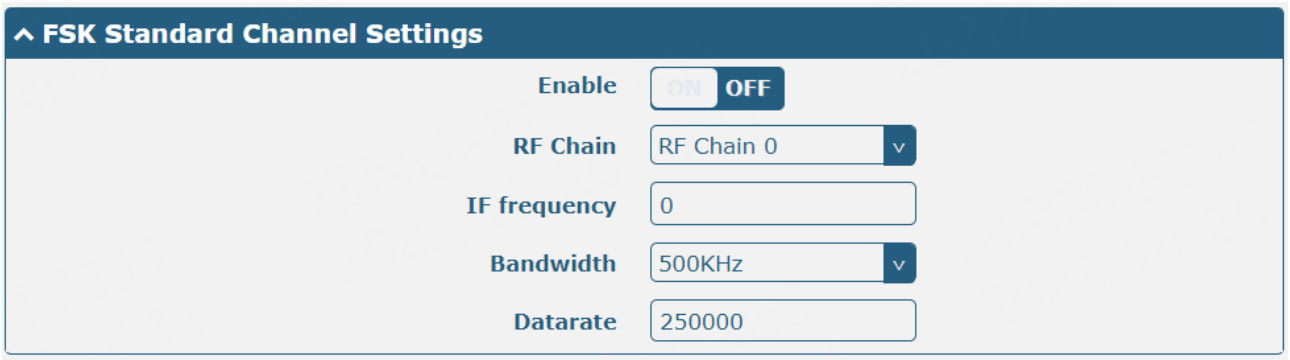
单击+以添加 LoRa 多数据速率通道设置。



LoRa Multi Datarate Channels Settings@RF Settings		
项目	说明	默认值
Index	显示表序号。	1
RF Chain	选择射频链路。	RF Chain 0
IF frequency	输入中心频率，数值为-500000-500000，单位为 Hz。特定通道的中心频率与射频链路 0/1 的中心频率之间的偏移。	0



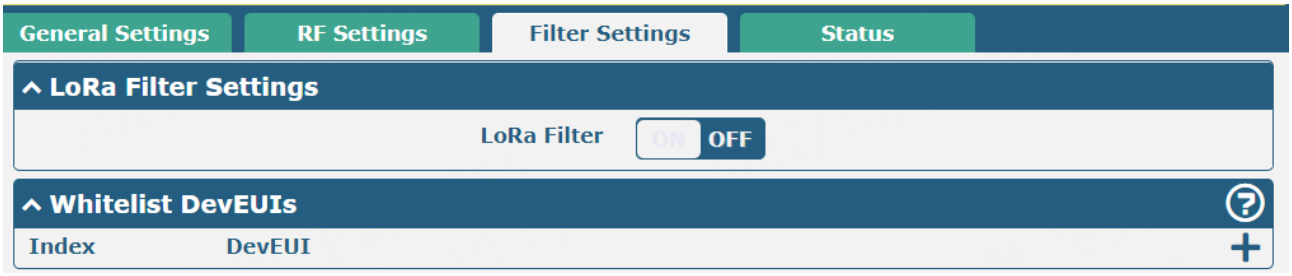
LoRa Standard Channel Settings@RF Settings		
项目	说明	默认值
Enable	单击切换按钮以启用/禁用此选项。	OFF
RF Chain	选择射频链路。	RF Chain 0
IF frequency	输入中心频率，数值为-500000-500000，单位为 Hz。特定通道的中心频率与射频链路 0/1 的中心频率之间的偏移。	0
Bandwidth	选择可选的带宽，单位是KHz。	500KHz
Spread Factor	输入可选的扩频因子。大扩频因子对应低速率，小扩频因子对应高速率。	SF9



FSK Standard Channel Settings@RF Settings		
项目	说明	默认值
Enable	单击切换按钮以启用/禁用此选项。	OFF
RF Chain	选择射频链路。	RF Chain 0
IF frequency	输入中心频率，数值为-500000-500000，单位为 Hz。特定通道的中心频率与射频链路 0/1 的中心频率之间的偏移。	0
Bandwidth	选择可选的带宽，单位是KHz。	500KHz
Datarate	输入数据速率，从500到250000，单位为Bit。	250000

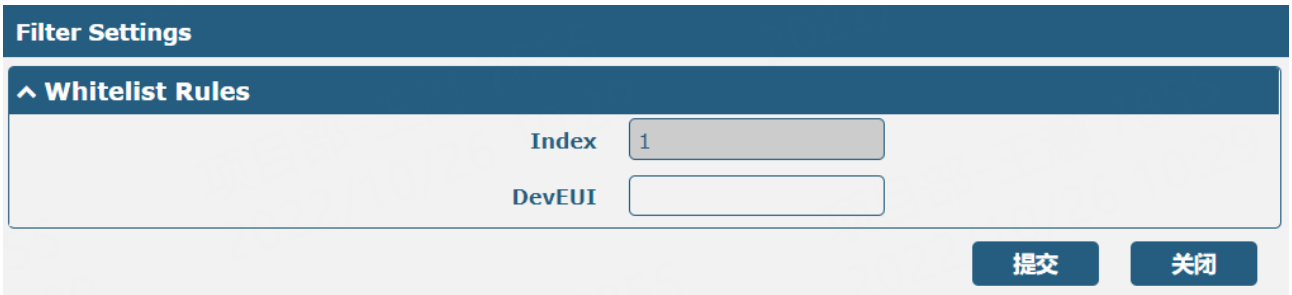
Filter Settings

本节用于修改 LoRa 过滤器设置。



Filter Settings		
项目	说明	默认值
LoRa Filter	单击切换按钮以启用/禁用此选项。	OFF

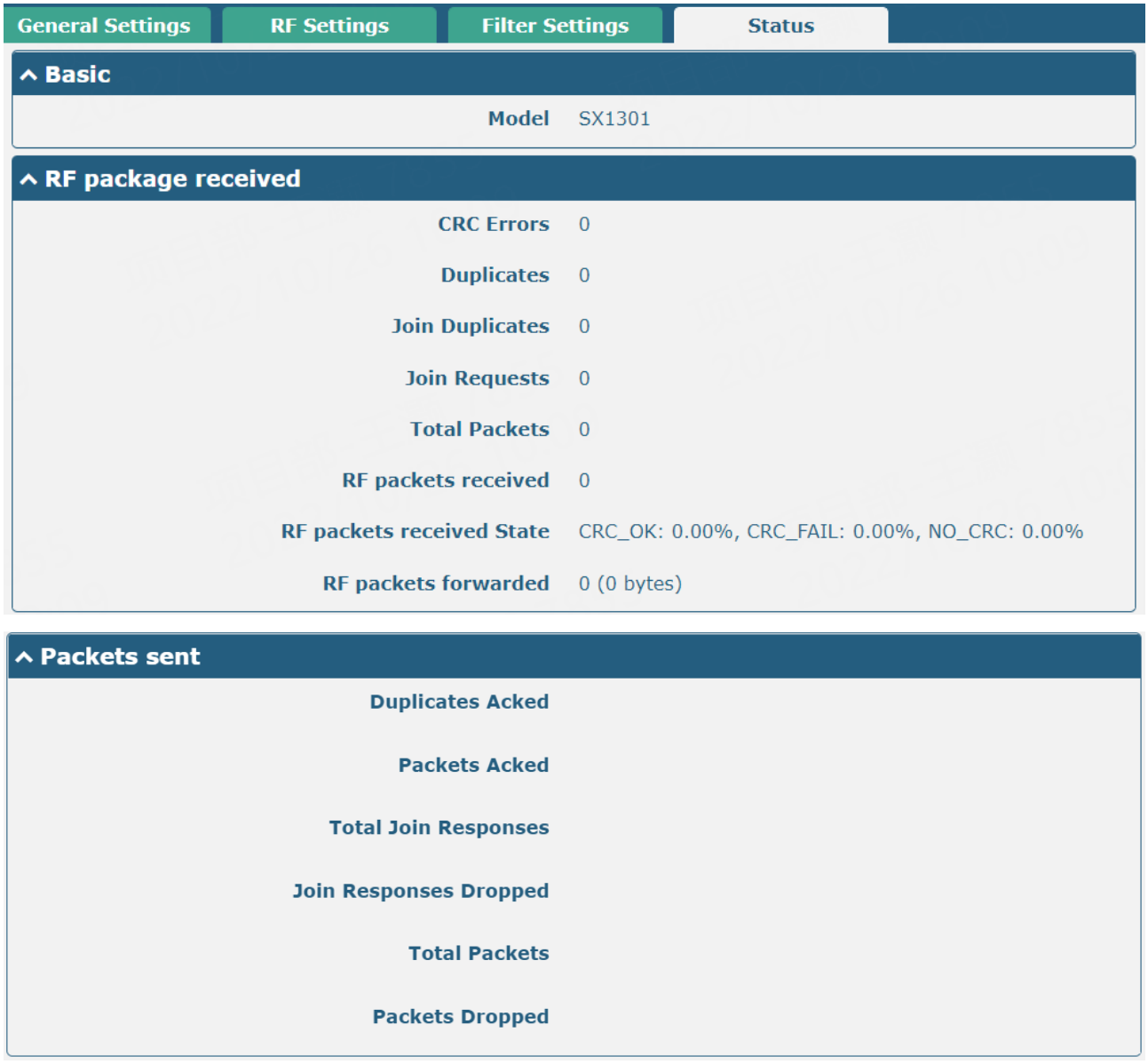
单击➕以添加白名单规则。



Whitelist Rules@Filter Settings		
项目	说明	默认值
Index	显示表序号。	1
DevEUI	输入设备的唯一标识符。开启该功能后，设备会基于 lora 节点发送的入网请求的 DevUI 进行过滤。	空

Status

本节用于查看当前节点状态。



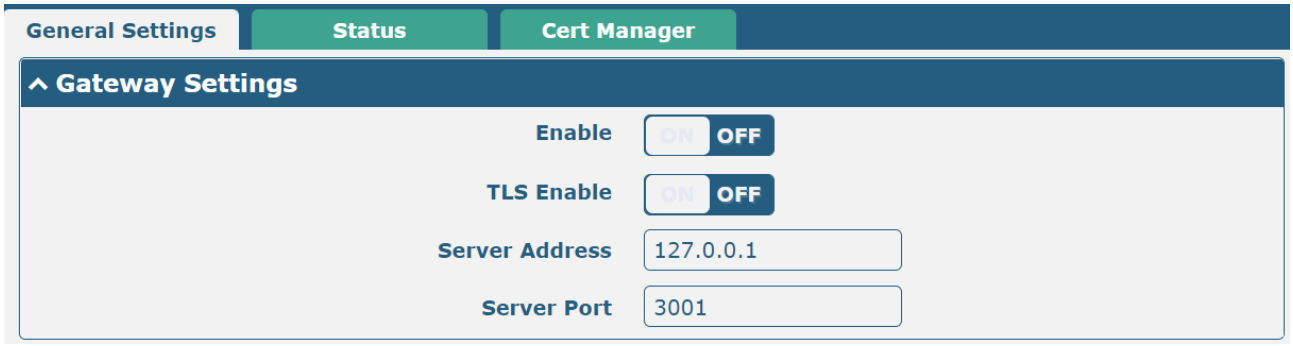
Status	
项目	说明
Basic	
Model	显示 LoRa 模块型号。
RF Packets received	
CRC Errors	显示接收到的CRC错误的射频数据包数量。
Duplicates	显示接收到的重复射频数据包的数量。
Join Duplicates	显示接收到的重复射频加入请求数据包数量。
Join Requests	显示接收到的射频加入请求数据包数量。
Total Packets	显示接收到的总射频数据包数量。
RF Packets Received	显示从节点发送到网关的数据包数量。
RF Packets Received State	显示射频数据包的接收状态。 • CRC_OK: CRC校验成功的数据包的百分比。 • CRC_Fail: CRC校验失败的数据包的百分比。 • NO_CRC: 没有经过CRC校验的数据包的百分比。
RF Packets Forwarded	从网关发送到服务器的经过CRC校验的数据包。
Packets sent	

Duplicates Acked	显示发送重复响应的射频数据包数量。
Packets Acked	显示发送响应的射频数据包数量。
Total Join Responses	显示发送重复加入响应射频数据包的总数量。
Join Responses Dropped	显示发送加入失败响应射频数据包数量。
Total Packets	显示发送射频数据包总数量。
Packets Dropped	显示丢弃的射频数据包数量。
Center Frequency	
RF Chain 0 Frequency	LoRa 信道 0 的中心频率。
RF Chain 1 Frequency	LoRa信道1的中心频率。
LoRa Multi Datarate Channels	
RF Chain	LoRa信道索引。
IF Frequency	LoRa信道的中频频率。
LoRa standard Channel	
RF Chain	LoRa标信道索引。
IF frequency	LoRa标准信道的中频频率。
Bandwidth	LoRa标准信道带宽。
Spread Factor	LoRa标准信道的传播因子。
FSK Standard Channel	
RF Chain	FSK标准频道索引。
IF frequency	FSK标准信道的中频频率。
Bandwidth	FSK标准信道带宽。
Data Rate	FSK标准通道数据速率。

3.3 Packet Forwarders

3.3.1 Basic Station

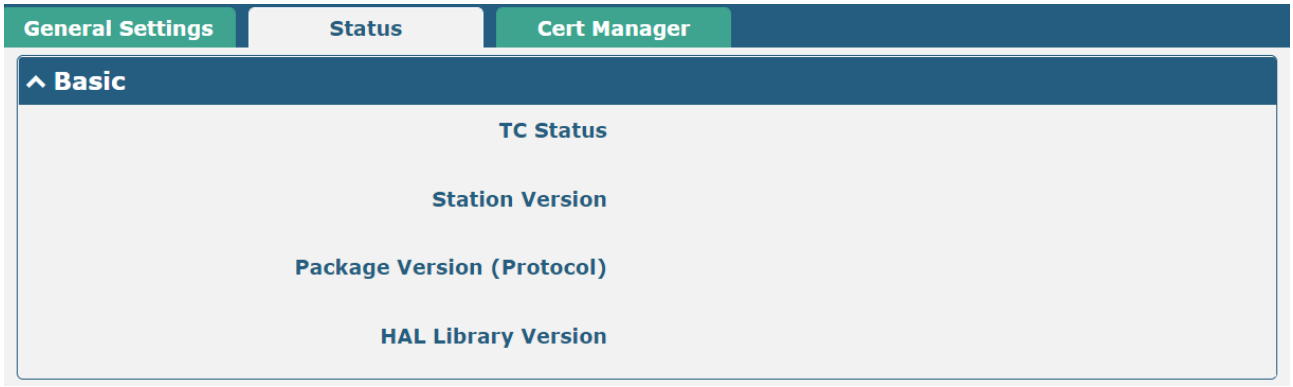
General Settings



常规设置		
Gateway Settings		
项目	说明	默认值
Enable	启用或关闭应用。	OFF
TLS Enable	启用或关闭 TLS 加密传输。	OFF
Server Address	设置服务器地址。	127.0.0.1
Server Port	设置服务器端口。	3001

状态

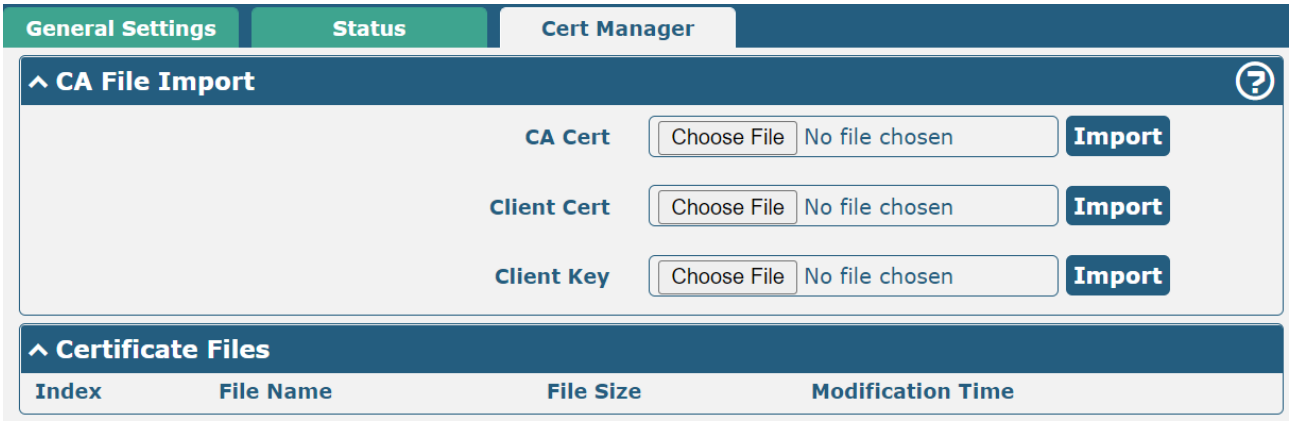
本节用于查看当前 Basic Station 状态。



项目	说明
TC Status	平台的连接状态。
Station Version	应用程序版本。
Package Version (Protocol)	应用程序包版本。
HAL Library Version	显示网关集成的 LoRaWAN 芯片的驱动版本。

Cert Manager

本节用于导入证书和查看当前证书信息。

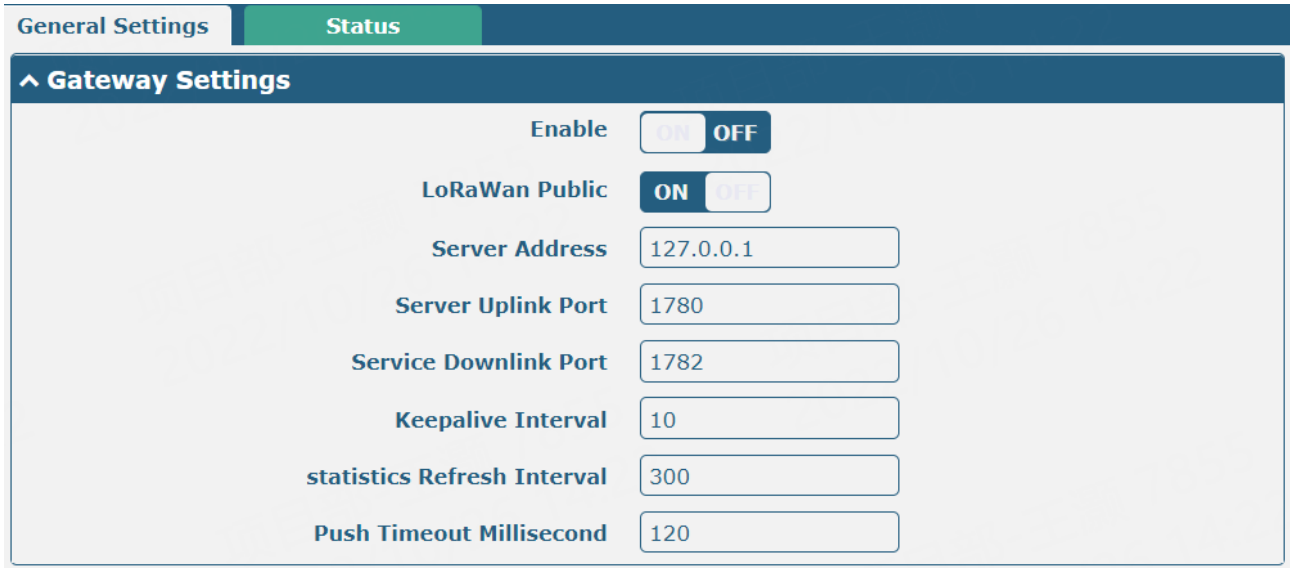


Cert Manager		
CA File Import		
项目	说明	默认值
CA Cert	服务器 CA 证书。	Null
Client Cert	服务器分配给客户端的证书。	Null
Client Key	服务器分配给客户端的私钥。	Null

3.3.2 Semtech UDP Forwarder

General Settings

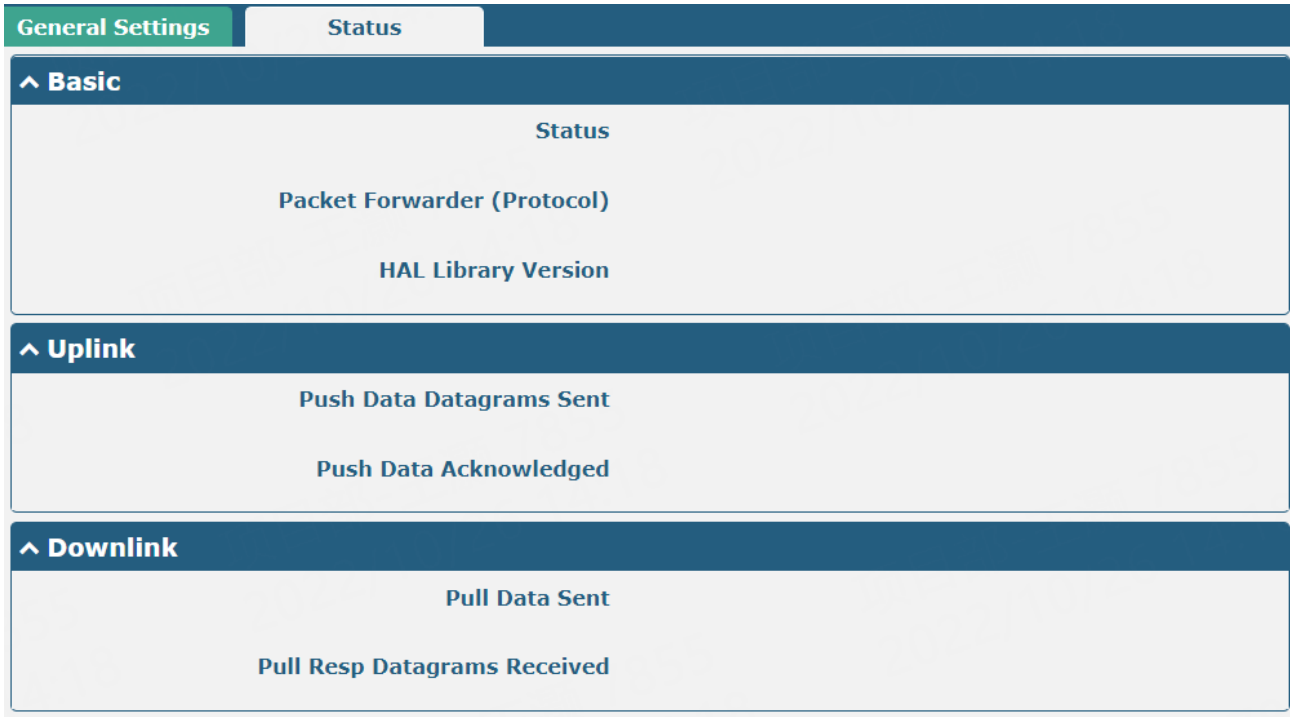
本节用于配置连接 LoRaWAN 服务器。



General Settings		
Gateway Settings		
项目	说明	默认值
Enable	启用或关闭应用。	OFF
LoRaWan Public	启用或关闭使用公共的 LoRaWan。	ON
Server Address	设置服务器地址。	127.0.0.1
Server Uplink Port	设置 UDP 上行连接端口。	1780
Service Downlink Port	设置 UDP 下行连接端口。	1782
Keepalive Interval	设置获取下行数据的时间间隔。	10
Statistics Refresh Interval	设置统计间隔、USI 更新间隔。	300
Push Timeout Millisecond	设置上行数据超时时间。	120

Status

本节用于查看当前 Packet Forwarder 的状态。



Status	
项目	说明
Basic	
Status	显示网关的LoRaWAN状态。
Status	显示数据包转发器的状态。
Packet Forwarder (Protocol)	显示数据包转发器的版本。
HAL Library Version	显示网关集成的LoRaWAN芯片的驱动版本。
Uplink	
Push Data Datagrams Sent	从网关发送到服务器的数据包的总数量，包括转发的射频数据包和统计数据包。
Push Data Acknowledged	推送数据后所发送的响应数据包的百分比。
Downlink	
Pull Data Sent	显示发送到服务器的数据包的数量，以及接收到服务器的数据包的响应数据包的百分比。
Pull Resp Datagrasms Received	显示从服务器发送到网关的数据包的数量和大小。

3.4 网络

3.4.1 路由

本节用于设置静态路由。静态路由是当设备使用手动配置的路由条目而不是来自动态路由流量的信息时发生的一种路由形式。路由信息协议（RIP）广泛应用于小型网络，使用率稳定。开放最短路径优先（OSPF）是在单个自治系统内的设备，用于大型网络。

静态路由

单击+，在弹出窗口里添加静态路由。最多可添加 20 条。

静态路由		
选项	**说明**	**默认**
索引	显示表序号。	--
描述	输入该静态路由的描述。	空
目的点	输入目的主机或目的网络的 IP 地址。	空
子网掩码	输入目的主机或目的网络的子网掩码。	空
网关	输入该静态路由规则网关的 IP 地址。设备将会把与该目的地址和子网掩码相匹配的全部数据转发给该网关。	空
接口	选择当前所要配置的链路的接口。	wwan
VID	输入 VLAN ID。0 表示没有 VLAN ID。	0

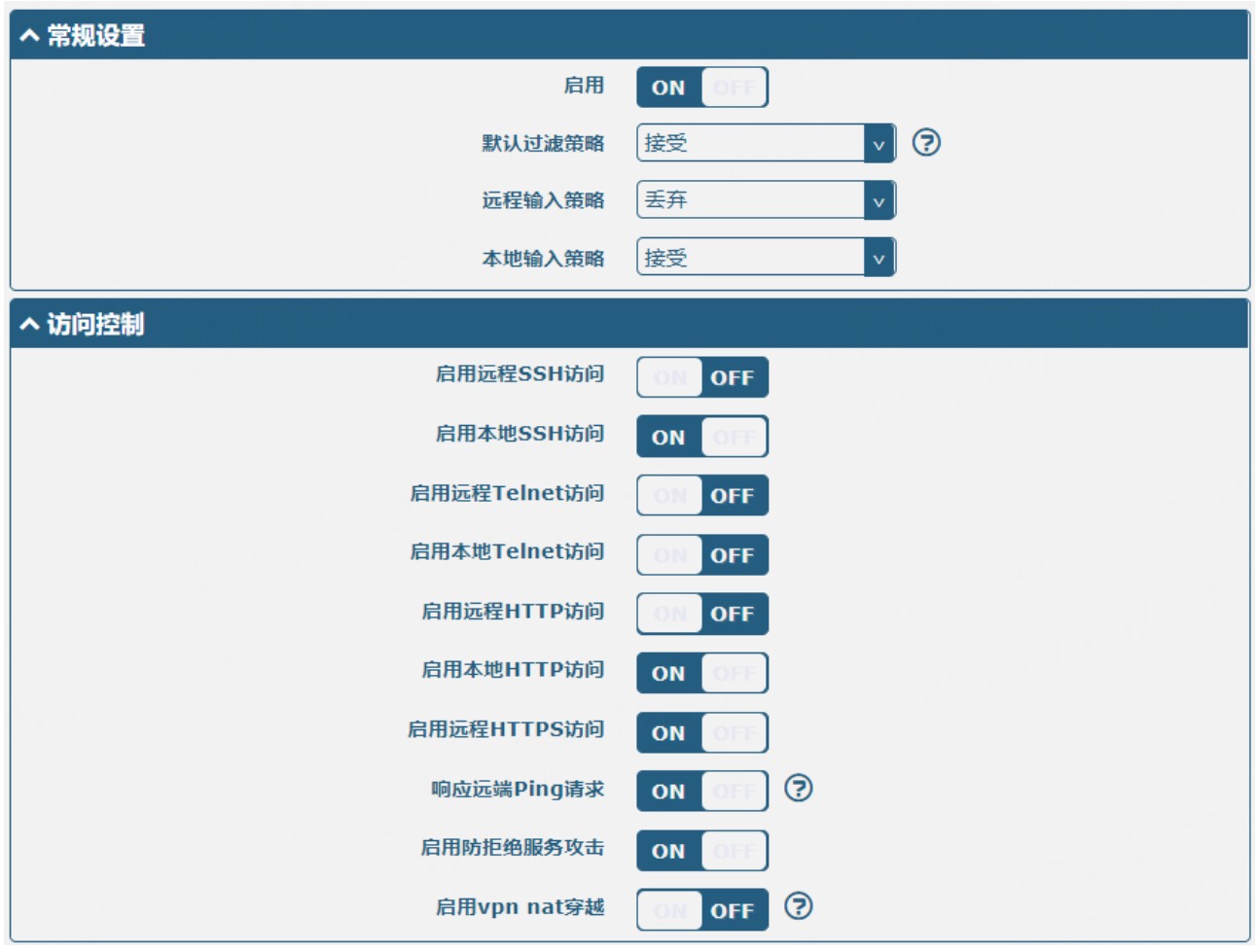
状态

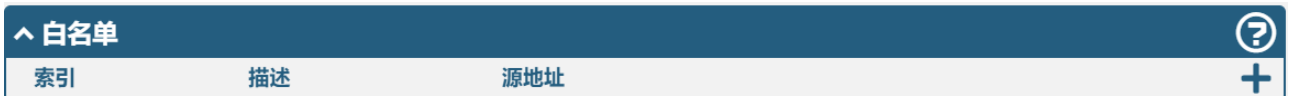
本节用于查看当前路由的状态。

3.4.2 防火墙

本节用于设置防火墙参数，包括设置访问控制以及添加过滤规则。过滤规则允许用户自定义接受或丢弃指定的访问源，对其 IP 地址或 MAC 地址进行过滤。

单击**“网络 > 防火墙 > 过滤”**显示如下：





单击 添加白名单，最多可添加 50 条。

单击➕添加过滤规则，最多可添加 50 条。当协议默认为“全部”或选择为“ICMP”时，窗口显示如下（以“全部”协议为例）：

当选择“TCP”，“UDP”或“TCP-UDP”作为协议时，窗口显示如下（以“TCP”协议为例）：

过滤		
选项	**说明**	**默认**
常规设置		
启用	单击切换按钮以启用/禁用默认过滤规则。	ON
默认过滤策略	可选择“接受”或“丢弃”。 • 接受：除了过滤规则表设置为丢弃的访问连接请求，其它的访问都被允许 • 丢弃：除了过滤规则表设置为接受的访问连接请求，其它的访问都被丢弃	接受

远程输入策略	当数据包通过防火墙链时，它将与远程输入链的所有规则进行匹配。如果没有规则与所述数据包匹配，则执行相应的操作（丢弃、拒绝或接受）： • 接受 – 数据包继续进入下一条链。 • 丢弃 – 数据包已停止并删除。 • 拒绝 – 数据包被停止、删除，与丢弃不同，拒绝消息将发送到数据包的来源。	丢弃
本地输入策略	当数据包通过防火墙链时，它将与远程输入链的所有规则进行匹配。如果没有规则与所述数据包匹配，则执行相应的操作（丢弃、拒绝或接受）： • 接受 – 数据包继续进入下一条链。 • 丢弃 – 数据包已停止并删除。 • 拒绝 – 数据包被停止、删除，与丢弃不同，拒绝消息将发送到数据包的来源。	接受
访问控制		
启用远程 SSH 访问	单击切换按钮以启用/禁用此选项。启用后，允许互联网上的用户通过 SSH 远程访问本设备。	OFF
启用本地 SSH 访问	单击切换按钮以启用/禁用此选项。启用后，允许局域网内的用户通过 SSH 本地访问本设备。	ON
启用远程 Telnet 访问	单击切换按钮以启用/禁用此选项。启用后，允许互联网上的用户通过 Telnet 远程访问本设备。	OFF
启用本地 Telnet 访问	单击切换按钮以启用/禁用此选项。启用后，允许局域网内的用户通过 Telnet 本地访问本设备。	OFF
启用远程 HTTP 访问	单击切换按钮以启用/禁用此选项。启用后，允许互联网上的用户通过 HTTP 远程访问本设备。	OFF
启用本地 HTTP 访问	单击切换按钮以启用/禁用此选项。启用后，允许局域网内的用户通过 HTTP 本地访问本设备。	ON
启用远程 HTTPS 访问	单击切换按钮以启用/禁用此选项。启用后，允许互联网上的用户通过 HTTPS 远程访问本设备。	ON
响应远端 Ping 请求	单击切换按钮以启用/禁用此选项。启用后，本设备会回复互联网上其他主机发来的 Ping 请求。	ON
启用防拒绝服务攻击	单击切换按钮以启用/禁用此选项。启用后，本设备拒绝服务攻击。拒绝服务攻击目的是企图让预期用户不能使用一台机器或网络资源。	ON
启用 vpn_nat 穿越	单击切换按钮以启用/禁用此选项。启用后，本设备自动将 WAN/WWAN 收到的 VPN 报文目的 IP 地址修改为 LAN 口下挂设备的 IP 地址并发送出去。	OFF
白名单		
索引	显示表序号。	--
描述	输入对此白名单的描述。	空
源地址	指定一个访问源，输入其源地址。	空
过滤规则		

索引	显示表序号。	--
描述	输入对此过滤规则或 MAC 绑定规则的描述。	空
源地址	指定一个访问源，输入其源地址。	空
源端口	指定一个访问源，输入其源端口。	空
源 MAC 地址	指定一个访问源，输入其源 MAC 地址。	空
目标地址	输入访问源所要访问的目标地址，可以是本设备下接的 IP 设备。	空
目标端口	输入访问源所要访问的目标端口，可以是本设备下接的 IP 设备。	空
协议	选择访问所用的协议，可选“全部”、“TCP”、“UDP”、“ICMP”或“TCP-UDP”。 ***注：****如果您不清楚当前的访问协议，建议选择“全部”。*	全部
动作	设置对访问的过滤规则，可选“接受”或“丢弃”。 • 接受：当默认过滤策略为删除时，本设备将删除符合此接受过滤列表的主机之外的所有连接请求。 • 丢弃：当默认过滤策略为“接受”时，本设备将接受除符合此删除过滤列表的主机之外的所有连接请求	丢弃

NAT

本节用于设置与 NAT 相关的功能，包括 DMZ、端口映射和 NAT。

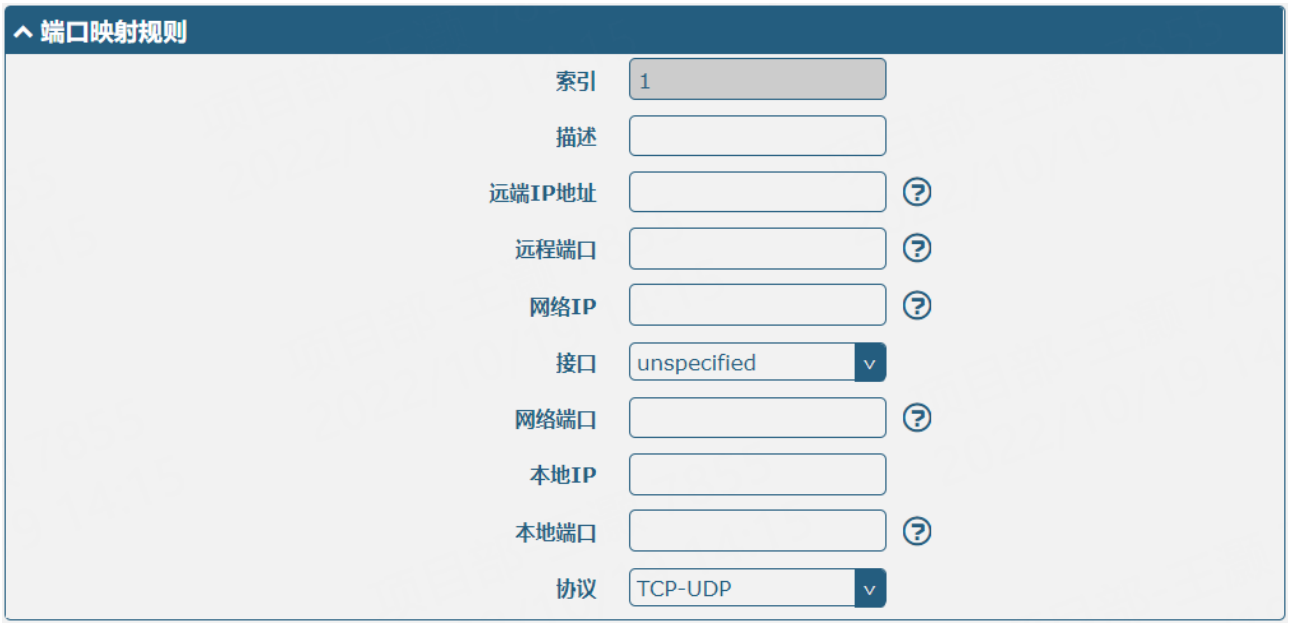
DMZ（Demilitarized Zone），即隔离区，也称非军事区。它是为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。DMZ 主机是除了被占用和转发的端口外，其他所有端口都对指定地址开放访问的内网主机。

选择**“网络>防火墙>NAT>DMZ”**。将显示以下信息：

DMZ 设置		
选项	**说明**	**默认**
启用	单击切换按钮以启用/禁用 DMZ 功能。	OFF
主机 IP 地址	输入内网隔离区主机的 IP 地址。	空
源 IP 地址	设置可以和 DMZ 主机通话的主机。0.0.0.0 代表所有的地址都能与 DMZ 通话。	空

端口映射是指在本设备中手动定义，从公网某些端口收到的数据全部转发到内网的某个 IP 的某个端口。单击**“网络 > 防火墙 > NAT > NAT 设置”**显示如下：

单击 添加端口映射规则，最多可添加 50 条。



端口映射规则		
项目	**说明**	**默认**
索引	显示表序号。	--
描述	输入对此端口映射的描述。	空

端口映射规则		
项目	**说明**	**默认**
远端 IP 地址	定义允许访问本地 IP 地址的主机或网络，空为不限制。 例如：10.10.10.10/255.255.255.255 or 192.168.1.0/24	空
远程端口	定义允许访问本地 IP 地址的端口，空为不限制。 格式：port[:port]	空
网络 IP	如果该参数设置为空，则网络 IP 地址不受限制。例如，10.10.10.10/255.255.255 或 192.168.1.0/24	空
接口	选择要配置的链路的相应接口。	
网络端口	输入外网访问本设备的对外端口。	空
本地 IP	输入想把数据转发到内网的设备的 IP 地址。	空
本地端口	输入想把数据转发到内网的设备的端口号。	空
协议	根据应用从“TCP”，“UDP”或“TCP-UDP”中选择。	TCP-UDP

NAT 设置，即自定义 NAT 规则。单击**“网络>防火墙>NAT>NAT 规则”**以显示以下内容。

单击 添加自定义规则。

NAT Settings		
项目	**说明**	**默认**
索引	指示列表的序号。	--
描述	输入此 NAT 规则的描述。	空
源地址	输入格式为 x.x.x.x、x.x.x.x/xx、x.x.x.x-x.x.x.x 的源地址，或 null 表	空

	示任何地址。	
输出接口	选择输出接口。选择未指定表示任何输出接口。	unspecified
目的地址	以 x.x.x.x，x.x.x.x/xx，x.x.x.x-x.x.x.x.x.x 的格式输入目标地址。	空
NAT 地址	以 x.x.x.x 格式输入 NAT 地址。	空

高级

Ipset 是 Linux 内核中的一个框架，可以由 Ipset 实用程序管理。根据类型的不同，IP 集可以存储 IP 地址、网络、（TCP/UDP）端口号、MAC 地址、接口名称或它们的组合，从而确保在将条目与集进行快速匹配。单击**“网络>防火墙>高级”**。将显示以下信息：

单击 ➕ 以添加 MAC 列表。最多添加 50 条。

单击➕以添加 IP 列表。最多添加 50 条。

单击➕以添加网络列表。最多添加 50 条。

Advanced		
项目	**说明**	**默认**
General Settings		
启用 Ipset	单击切换按钮以启用/禁用 Ipset 选项。	ON
默认输入策略	从“接受”或“拒绝”中进行选择。 • 接受 ：本设备将接受所有输入连接请求，但符合MAC / IP端口/ 网络下拉列表的主机除外。 • 拒绝：本设备将丢弃所有输入连接请求，但符合MAC / IP端口/ Net接受列表的主机除外。	接受
MAC 列表名称	输入 MAC 列表的名称。不支持输入纯数字。	MAC
MAC 列表操作	从“接受”或“拒绝”中进行选择。 • 接受：当默认输入策略为拒绝时，本设备将拒绝所有连接请求，但是符合MAC列表中主机除外。 • 拒绝：当默认输入策略为接受时，本设备将接受所有连接请求，但是符合MAC列表中主机除外。	拒绝
IP 端口名称	输入IP端口列表的名称。不支持输入纯数字。	ip-port
IP 端口操作	从“接受”或“拒绝”中进行选择。 • 接受：当默认输入策略为拒绝时，本设备将拒绝所有连接请求，但是符合IP端口列表中主机除外。 • 拒绝：当默认输入策略为接受时，本设备将接受所有连接请求，但是符合IP端口列表中主机除外。	拒绝
网络列表名称	输入网络列表的名称。不支持输入纯数字。	net
网络列表操作	从“接受”或“拒绝”中进行选择。	拒绝

	• 接受：当默认输入策略为拒绝时，本设备将拒绝所有连接请求，但是符合网络列表中主机除外。 • 拒绝：当默认输入策略为接受时，本设备将接受所有连接请求，但是符合网络列表中主机除外。	
MAC 列表		
索引	显示表序号。	--
MAC	输入 MAC 地址。格式：XX：XX：XX：XX：XX：XX。	空
IP 端口列表		
索引	显示表序号。	--
协议	从“TCP”，“UDP”中选择。	TCP
IP	输入 IP 地址。	空
端口	输入端口号。	空
网络列表		
索引	显示表序号。	--
网络	输入域名/IP/IP 网段。	空

自定义规则

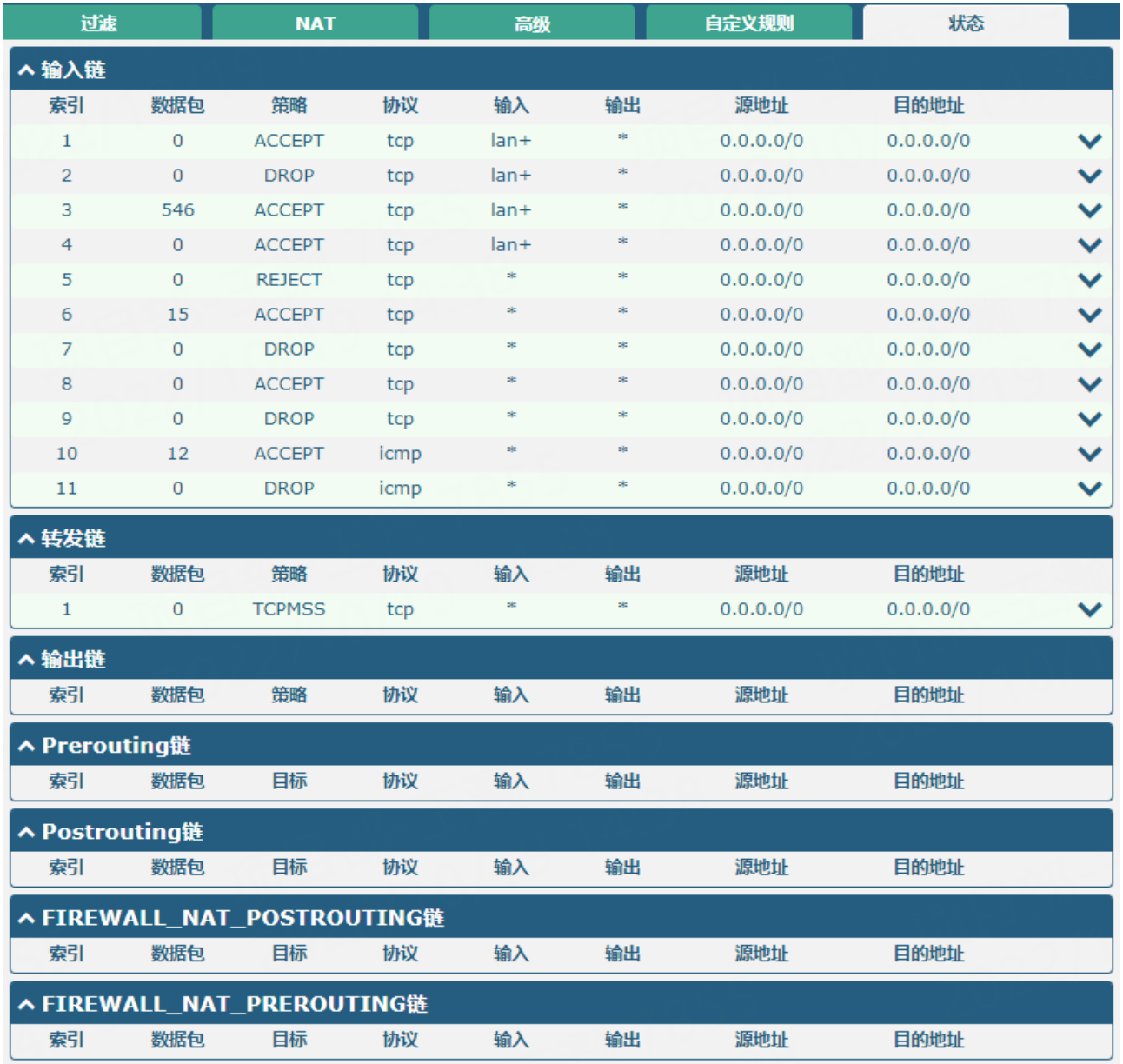
本节用于配置自定义防火墙规则。

单击 + 添加自定义规则。最多添加 50 条。

自定义防火墙规则		
选项	**说明**	**默认**
索引	显示表序号。	--
描述	输入对此自定义防火墙规则的描述。	空
规则	输入自定义的规则。	空

状态

本节用于查看当前设备的防火墙状态。



3.4.3 IP Passthrough

本节用于设置 IP Passthrough 功能。当本设备开启 IP Passthrough 功能时，终端设备（如 PC）将开启 DHCP Client 模式然后连接到本设备的 LAN 口。当本设备成功拨上号后，PC 将自动获取到运营商分配的 IP 地址和 DNS 服务器地址。

注：

1）*IP Passthrough 功能功能只能分配一个网络提供商地址。*

2）*使用该功能，主链路需要设置为 WWAN，备份链路需要设置为 None。*

*单击“**网络 > IP Passthrough > IP Passthrough**”，以配置 **IP Passthrough** 功能。*

注：请确保主要链接是 WWAN，备份链接配置成无。

3.5 虚拟专用网

3.5.1 IPsec

IPsec（Internet Protocol Security）是一种建立在 Internet 协议层上的协议，能够让两个主机以安全的方式来通讯。IPsec 是安全联网的方向，它通过端对端的安全性来提供主动的保护以防止专用网络与 Internet 的攻击。

单击**“虚拟专用网 > IPsec > 常规”**以设置 IPsec 参数。

常规设置@常规		
项目	**说明**	**默认**
存活时间	设置存活时间，单位为秒。本设备每隔一段时间就会发送保活数据包到 NAT（网络地址转换）服务器，避免 NAT 表上的记录消失。	20
优化 DH 指数大小	单击切换按钮以启用/禁用此选项。启用后，能缩短生成密钥的时间。	OFF
输出调试信息	单击切换按钮以启用/禁用此选项。开启 IPsec VPN 的调试信息输出到调试口。	OFF
启用备份网关		
Monitor Interval	输入监视器间隔。单位：秒。	30
Monitor Times	输入未应答的 IPsec 主网关的最大次数。	5

隧道

单击➕添加 IPsec 隧道，最多可添加 6 条。

常规设置@隧道		
项目	**说明**	**默认**
索引	显示表序号。	--
启用	单击切换按钮以启用/禁用此IPsec隧道。	ON
描述	输入关于此IPsec隧道的描述。	空
网关	输入远端IPsec VPN服务器地址。0.0.0.0表示任何地址。	空
备份网关	输入远端IPsec VPN备份服务器地址。0.0.0.0表示任何地址。	空
模式	可选“隧道”或“传输”。 • 隧道：一般用于设备之间或终端到设备之间，设备作为身后主机的代理。 • 传输：用于终端之间或终端到设备之间的通讯，如在工作站到本设备之间建立加密的Telnet连接。	隧道
协议	可选“ESP”或“AH”作为安全协议。 • ESP：使用ESP协议 • AH：使用AH协议	ESP
本地子网	输入IPsec协议的本地子网地址和掩码。本地子网掩码，例如192.168.1.0/24。	空
本地协议端口	输入IPsec协议的本地端口，例如 tcp/443;udp/1701 如果两者都不为空，本地协议端口和远端协议端口必须相同。	空
远端子网	输入IPsec保护的远端子网地址和掩码。远端子网掩码，例如10.8.0.0/24。	空

常规设置@隧道		
项目	**说明**	**默认**
远端协议端口	输入IPsec协议的远端端口，例如 tcp/443;udp/1701 如果两者都不为空，本地协议端口和远端协议端口必须相同。	空
链路绑定	选择要建立IPsec的链路。	不绑定

在 IKE 设置窗口中，当认证类型选择“PSK”时，窗口显示如下：

当认证类型选择“CA”时，窗口显示如下：

当认证类型选择“PCKS#12”时，窗口显示如下：

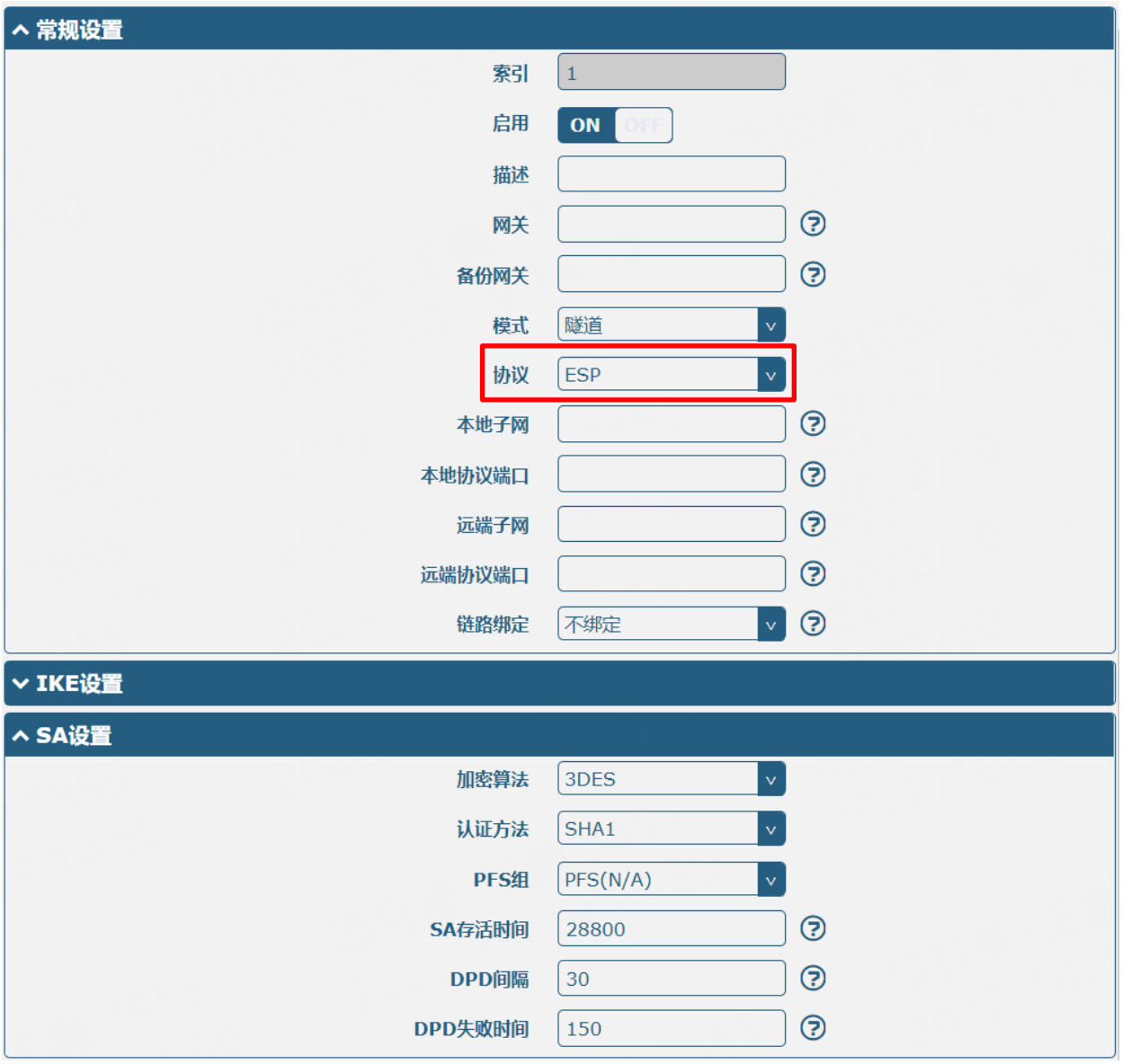
当认证类型选择“xAuth PSK”时，窗口显示如下：

当认证类型选择“xAuth CA”时，窗口显示如下：

IKE 设置		
项目	**说明**	**默认**
IKE类型	从“IKEv1”和“IKEv2”中选择。	IKEv1
协商模式	从“主模式”和“野蛮模式”中选择IKE（网络密钥交换）的协商模式。如果IPsec隧道一端的IP地址是自动获取的，必须选择“野蛮模式”为IKE（网络密钥交换）协商模式；在这种情况下，只要用户名和密码正确，就能够建立SA协商。	主模式
认证方法	从“MD5”、“SHA1”、“SHA2 256”和“SHA2 512”中选择认证算法应用于IKE（网络密钥交换）协商。	SHA1
加密算法	从“3DES”、“AES128”、“AES192”和“AES256”中选择加密算法应用在IKE（网络密钥交换）协商中。 • 3DES：使用168位的3DES加密算法。 • AES128：使用128位的AES加密算法。 • AES192：使用192位的AES加密算法。 • AES256：使用256位的AES加密算法。	3DES
IKE DH分组	选择DH分组应用于IKE（网络密钥交换）协商。可选“DHgroup1”、“DHgroup2”、“DHgroup5”、“DHgroup14”、“DHgroup15”、“DHgroup16”、“DHgroup17”或“DHgroup18”。	DHgroup2
认证类型	从“PSK”、“CA”、“xAuth PSK”、“PKCS#12”和“xAuth CA”选择认证类型应用于IKE协商。 • PSK：预共享密钥。 • CA：x509证书认证。 • xAuth：对AAA服务器的扩展认证。 • PKCS#12：交换数字证书认证。	PSK

PSK密钥	输入PSK密钥。	空
本地ID类型	可选“默认”、“FQDN”或“用户FQDN”。 • 默认：默认选择IP地址。 • FQDN：Fully Qualified Domain Name，即正式域名，在IKE协商中用FQDN作为本地ID；如果选择这一选项，要把域名中@去掉后再输入，如test.robustel.com。 • 用户FQDN：在IKE协商中把用户FQDN作为本地ID；如果选择这一选项，输入域名时要带上@，如test@robustel.com。	默认
远程ID类型	可选“默认”、“FQDN”或“用户FQDN”。 • 默认：默认选择IP地址。 • FQDN：Fully Qualified Domain Name，即正式域名，在IKE协商中用FQDN作为远程ID；如果选择这一选项，要把域名中@去掉后再输入，如test.robustel.com。 • 用户FQDN：在IKE协商中把用户FQDN作为远程ID；如果选择这一选项，输入域名时要带上@，如test@robustel.com。	默认
IKE存活时间	设置在IKE协商中的生存时间。在SA过期之前，IKE协商出新的SA；新的SA建立，它会立即生效；旧的那一个过期后会立即清除。	86400
私匙密码	输入CA和xAuth CA认证下的私匙密码。	空
用户名	输入xAuth PSK和xAuth CA认证下的用户名。	空
密码	输入xAuth PSK和xAuth CA认证下的密码。	空

当“**虚拟专用网 > IPsec > 隧道 > 常规设置**”中的协议选择“ESP”时，SA 设置显示如下：



当“虚拟专用网 > IPsec > 隧道 > 常规设置”中的协议选择**“AH”**时，SA 设置显示如下：

SA设置		
项目	**说明**	**默认**
加密算法	当在“协议”中选择“ESP”时，可选“3DES”、“AES128”、“AES192”或“AES256”。更高的安全性意味着更复杂的实现和更低的速率。DES能满足一般性需求，安全	3DES

	和机密性要求更高是则选用3DES。	
认证方法	从“MD5”、“SHA1”、“SHA2 256”和“SHA2 512”中选择认证算法应用于SA协商阶段。	SHA1
PFS组	从“PFS（N/A）”，“DHgroup1”，“DHgroup2”，“DHgroup5”，“DHgroup14”，“DHgroup15”，“DHgroup16”，“DHgroup17”或“DHgroup18”中选择。	DHgroup2
SA存活时间	设置IPsec SA的存活时间。当协商建立IPsec SAs时，IKE将在本地设定生存时间和对端提出的生存之间选择较小的那一个。	28800
DPD间隔	设置间隔时间。如果从对端接收不到IPsec保护包，过了该间隔时间后，DPD将会被触发。DPD是失效对等体检测，其会不定期地检测IKE（因特网密钥交换）的对端是否失效。本地终端接收到IPsec包时，DPD检测上一次从对端收到IPsec包的时间。如果时间超过DPD间隔时间，它将发送DPD hello包给对端。如果本地终端在DPD包回传时间内未接收到DPD确认，它将重传DPD hello包。如果本地终端发送DPD hello包超过最大重传尝试次数，仍未收到DPD确认，就认为对端已经无效，将清除IKE SA和基于IKE SA的IPsec SAs。	30
DPD失败次数	设置DPD（失效对等体检测）包的超时时间。	150
高级设置		
启用压缩	单击切换按钮以启用/禁用该选项。启用后，该功能会压缩IP数据包的头部。	OFF
启用强制封装	单击切换按钮以启用/禁用该选项。启用后，即使未检测到NAT情况，也强制对esp数据包进行UDP封装。这有助于克服限制性防火墙。	OFF
清除数据流	启用或关闭该功能。建立IPsec后清除conntrack。	OFF
专家选项	添加更多关于PPP的配置选项。格式：config-desc;config-desc，如protostack=netkey;plutodeBug=none	空

状态

本节用于查看 IPsec 的连接状态。

X509

本节用于查看和导入证书。

x509		
选项	**说明**	**默认**
X509 设置		
隧道名	选择一条有效的隧道。从“隧道1”，“隧道2”，“隧道3”，“隧道4”、“隧道5”、“隧道6”中选择。	隧道 1
导入方式	选择导入方式，从“Default”、“Manual-Import”中选择。	Default
本地证书	从本地选择正确的证书文件导入到本设备中。	--
对端证书	从远端选择正确的证书文件导入到本设备中。	--
私钥	选择正确的私钥文件导入到本设备中。	--
CA 证书	选择正确的CA证书导入到本设备中。	--
PKCS#12 证书	选择PKCS#12证书文件导入到本设备中。	--
证书文件		
索引	显示表序号。	--
文件名	显示已导入本设备的证书名称。	空
文件大小	显示当前文件的大小。	空
最后修改时间	显示上一次修改证书的时间。	空

3.5.2 WireGuard

本节用于设置 WireGuard VPN 的参数，WireGuard VPN 是一种基于 SSL 的开源 VPN 系统。本设备的无线保护功能可以支持点对点和点对多点 VPN 通道。

单击“VPN>WireGuard”设置 WireGuard 参数。

常规设置@WireGuard		
选项	**描述**	**默认值**
启用 WireGuard	启用或禁用WireGuard。	OFF
私钥	输入本地私钥。可以通过X509设置自动生成或手动导入，但不能为空。	Null
IP 地址	输入虚拟接口的IP地址。它不能为空。	Null
侦听端口	输入虚拟接口侦听端口。它不能为空。	51820
MTU	输入虚拟接口切片大小。	1472
启用 NAT	启用/禁用 NAT 功能。启用后，IP 地址将转换为接口虚拟 IP 地址。	ON

注：*单击* *以获取帮助。*

单击 以添加对等设置。最大计数为 20。

对端设置@WireGuard		
选项	**描述**	**默认值**
指数	显示索引	--
描述	输入对端的描述。	空
公钥	输入公钥。公钥不能为空。	空
预共享密钥	输入预共享密钥。它不能为空。	空
终结点主机	输入对等 IP 地址。空值不会启动连接请求。	空
端点端口	输入对等端口。空值不会启动连接请求。	空
允许的 IP	输入允许的 IP 地址，该地址不能为空。	空
路由允许 IP	启用/禁用功能。启用后，将为此对等网络允许的网络创建路由。如果允许的网络为 0.0.0.0/0，则该对等方将被设置为默认路由。	ON
持久保持活力	输入发送持续保留消息的间隔（秒）。0 表示禁用该功能。	0

状态

本节用于查看查看 WireGuard 的连接状态。单击其中一行，其链接连接的详细信息将显示在当前行的下方。

X509

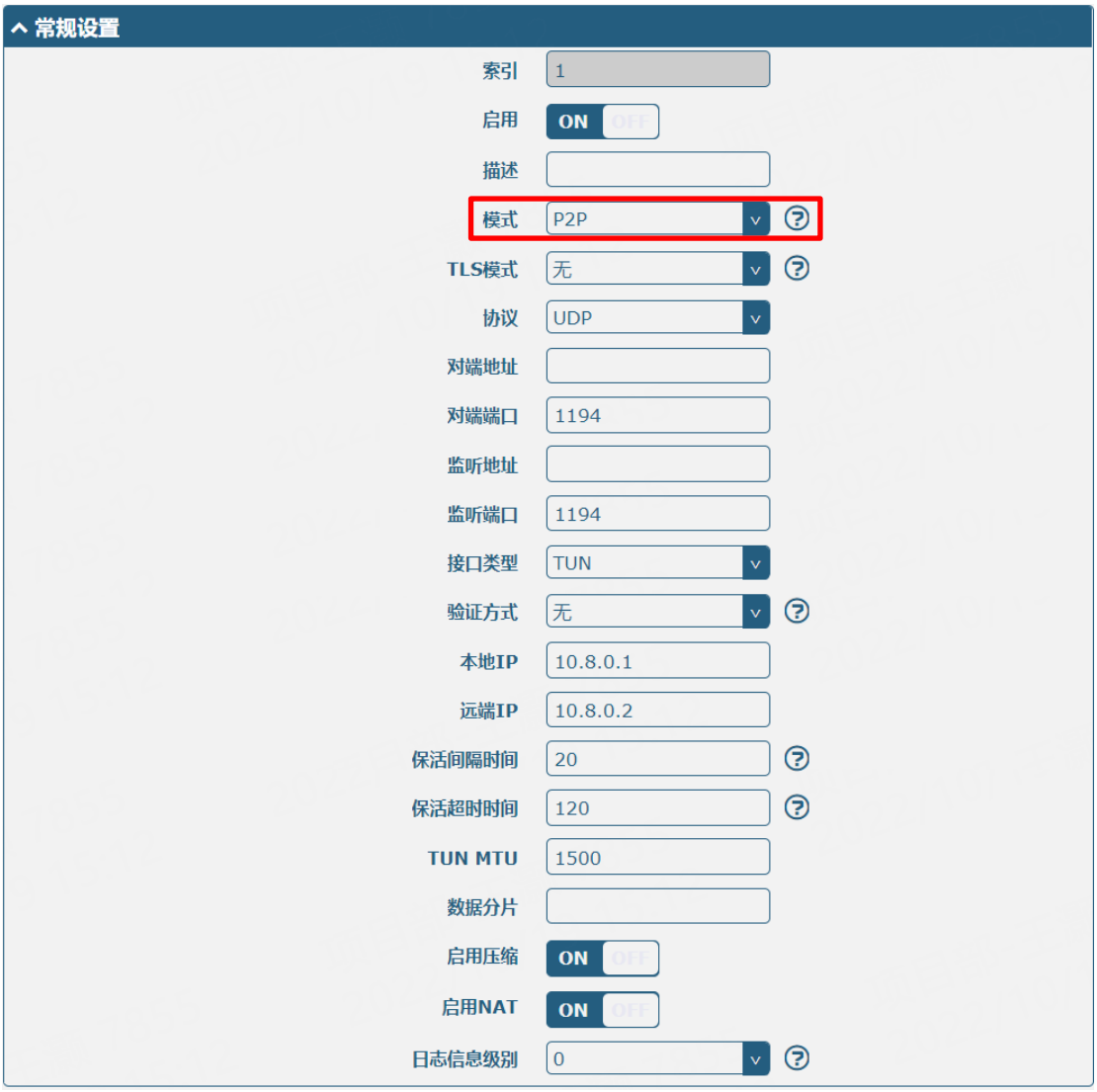
本节用于生成或导入私钥和公钥。

x509		
选项	**描述**	**默认值**
X509 设置		
私钥	单击 生成 以生成私钥文件	--
私钥	单击 选择文件 按钮从您的计算机中找到私钥，然后单击 导入 按钮从电脑上导入私钥文件到本设备中。	--
公钥	单击 生成 以生成公钥文件	--
配置文件	单击 生成 以生成配置文件	--
配置文件	单击 选择文件 按钮从您的计算机中找到配置文件，然后单击 导入 按钮从电脑上导入私钥文件到本设备中。	--

3.5.3 OpenVPN

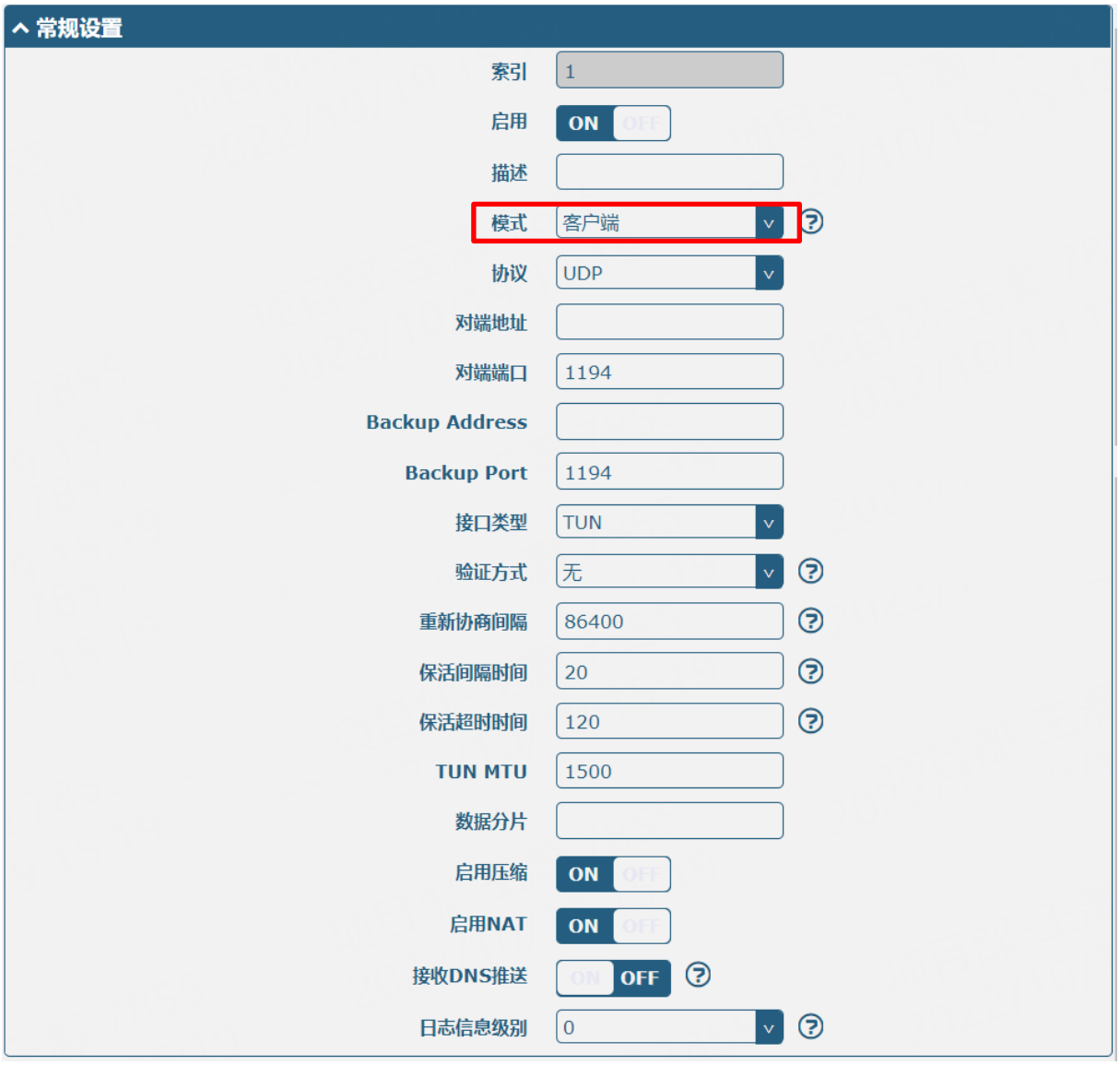
本节用于设置 Open VPN 的参数。OpenVPN 是一个开放源码的基于 SSL 的 VPN 系统。本设备的 OpenVPN 功能可以支持点对点和点对多点（客户端）的 VPN 通道。
单击“虚拟专用网 > OpenVPN > OpenVPN”显示如下：

单击隧道设备里的 + 以添加 OpenVPN 隧道，最多可添加 5 条。其模式默认为“P2P”，显示如下：



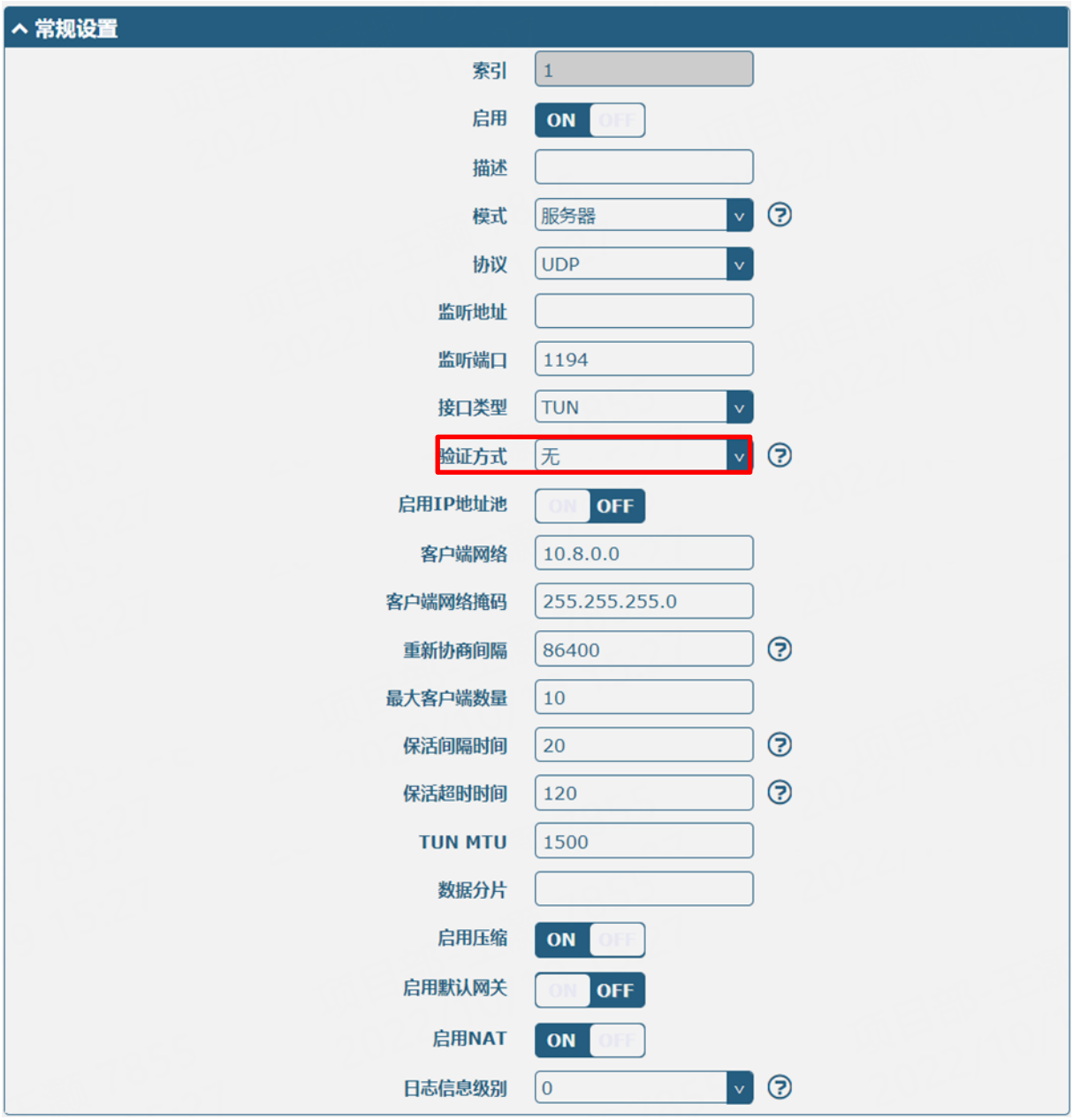
当模式选择“自动”时，窗口显示如下：

当模式选择“客户端”时，窗口显示如下：



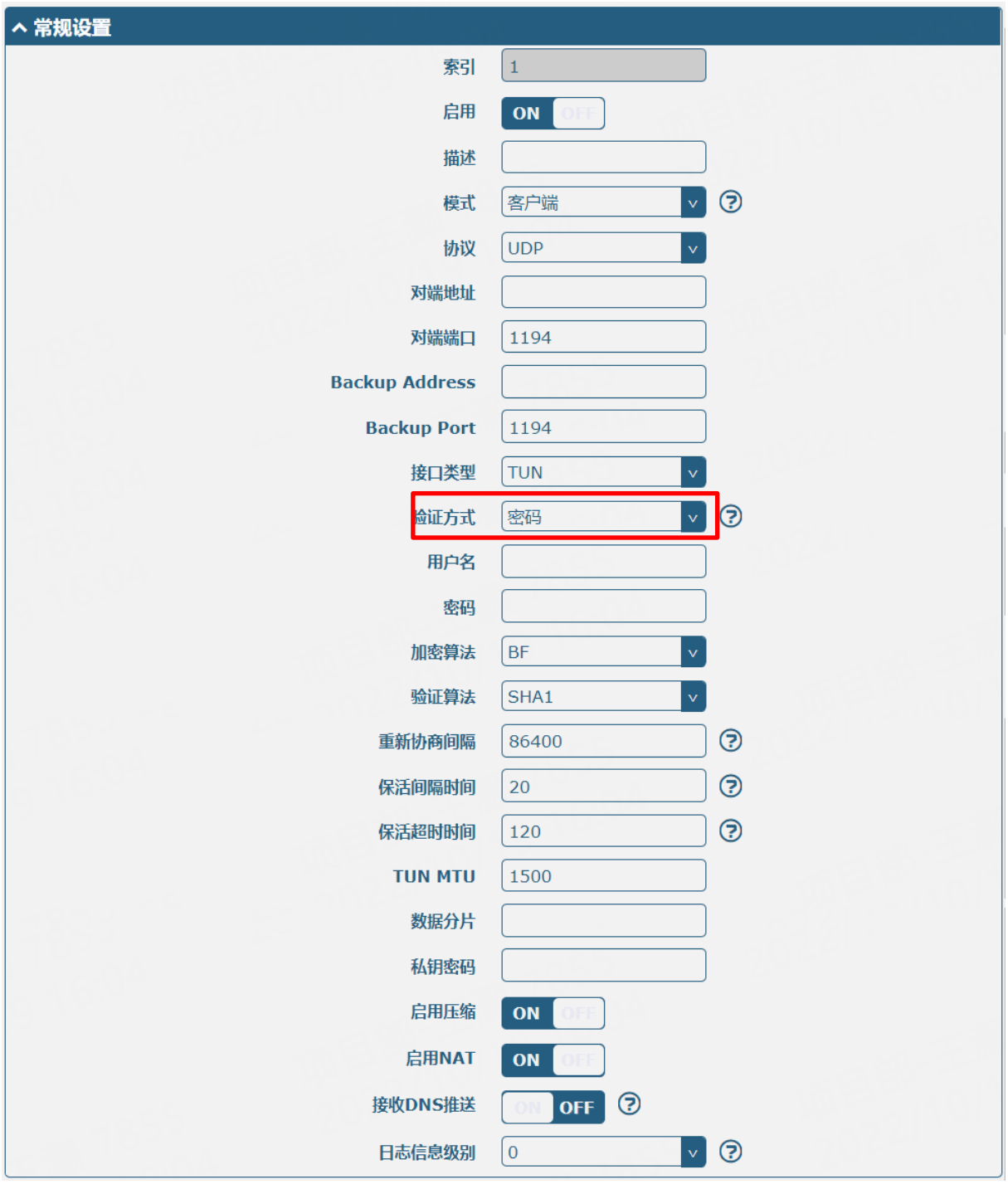
当模式选择“服务器”时，窗口显示如下：

当验证方式选择“无”时，窗口显示如下：



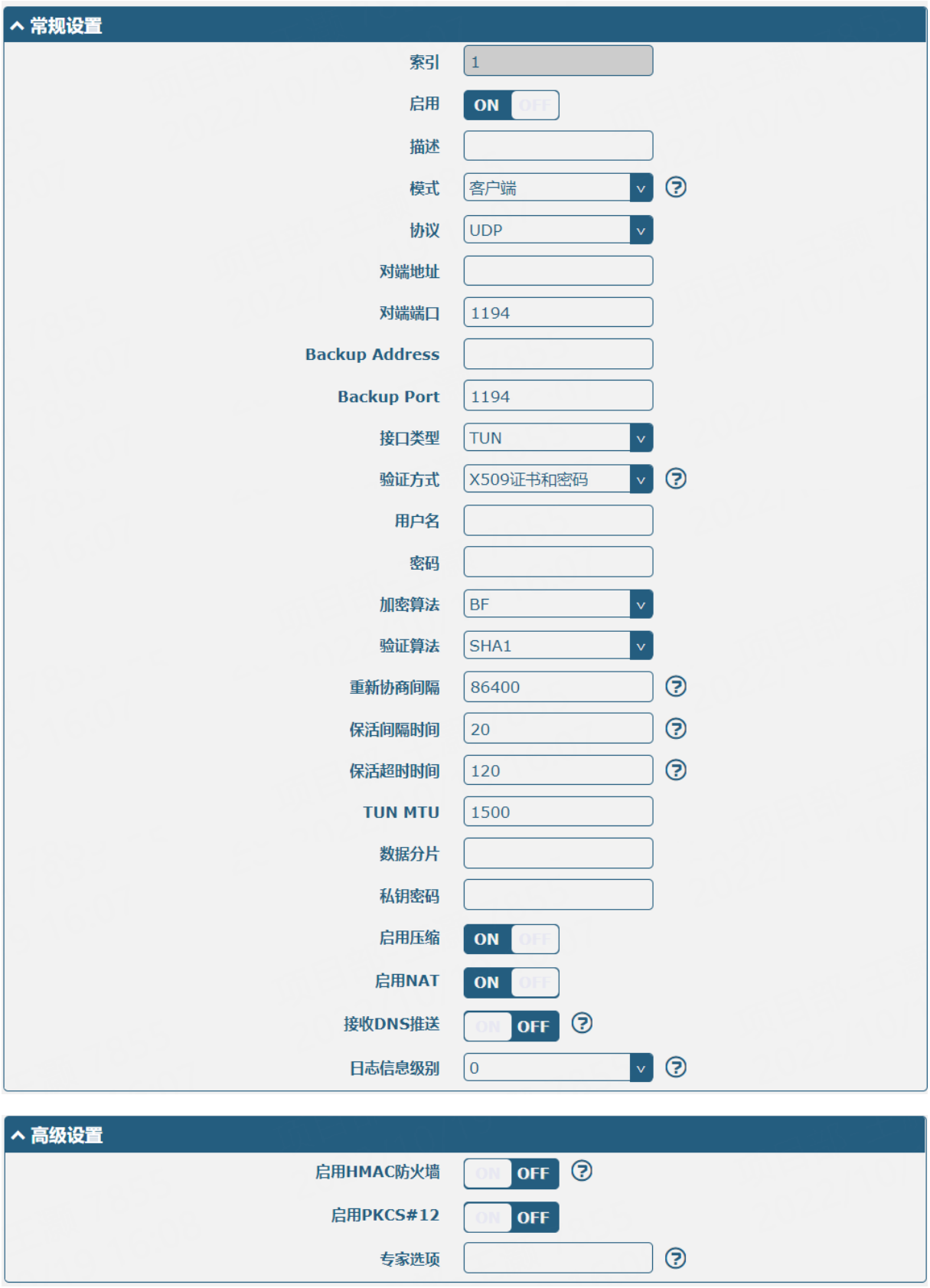
当“验证方式”选择“预共享密钥”时，窗口显示如下：

当验证方式选择“密码”时，窗口显示如下：


常规设置
索引
1
启用
ON
描述
模式
客户端
协议
UDP
对端地址
对端端口
1194
Backup Address
Backup Port
1194
接口类型
TUN
验证方式
密码
用户名
密码
加密算法
BF
验证算法
SHA1
重新协商间隔
86400
保活间隔时间
20
保活超时时间
120
TUN MTU
1500
数据分片
私钥密码
启用压缩
ON
启用NAT
ON
接收DNS推送
OFF
日志信息级别
0

当“验证方式”选择“X509 证书”时，窗口显示如下：

当“验证方式”选择“X509CA 证书和密码”时，窗口显示如下：



常规设置 @ OpenVPN		
项目	**说明**	**默认**
常规设置		
索引	显示表序号。	--
启用	单击切换按钮以启用/禁用OpenVPN客户端。	ON
描述	输入该OpenVPN的描述。	空
模式	选择“自动”或“P2P”或“客户端”或“服务器”。	客户端
协议	根据应用需求，从“UDP”、“TCP客户端”或“TCP服务器”中选择。	UDP
服务器地址	输入对端IP地址或远端OpenVPN服务器的域名。	空
服务器端口	输入对端或者OpenVPN服务器的监听端口。	1194
Backup Address @客户端模式	输入对端IP地址或远端OpenVPN备份服务器的域名。	空
Backup port @客户端模式	输入对端或者OpenVPN备份服务器的监听端口。	1194
监听地址@服务器模式	输入本端IP地址或域名。	空
监听端口@服务器模式	输入本端的监听端口。	1194
接口类型	选择“TUN”或“TAP”。TUN与TAP的不同之处是TUN设备是网络层点到点的虚拟设备，而TAP是以太链路层的虚拟设备。	TUN
用户名	输入用于“密码”或“X509CA密码”两种验证方式的用户名。	空
密码	输入用于“密码”或“X509CA密码”两种验证方式的密码。	空
验证方式	从“无”、“预享密钥”、“密码”、“X509CA”和“X509CA密码”中选择。 ***注：****“无”和“预享密钥”仅适用于P2P模式。在使用带有密码验证的服务器模式时，必须从用户管理添加帐户。*	无
启用 IP 地址池	单击切换按钮以启用/禁用该选项。启用后，客户端会从地址池中获取虚拟IP。	OFF
本地 IP	输入本地虚拟IP。	10.8.0.1
远程 IP	输入远端虚拟IP。	10.8.0.2
客户端网络	客户端虚拟IP网络地址。	10.8.0.0
客户端网络掩码	客户端虚拟IP网络地址掩码。	255.255.255.0
加密算法	从“BF”、“DES”、“DES-EDE3”、“AES-128”、“AES-192”和“AES-256”中选择。	BF
验证算法	从“MD5”、“SHA1”、“SHA256”和“SHA512”中选择。	SHA1

最大客户数量	设置服务器模式下，最大客户端连接的数量。	10
重新协商时间	设置隧道断开后重新协商的时间间隔。	86400
保活间隔时间	设置检查隧道是否断开的ping时间间隔。	20
保活超时时间	设置保活超时时间。如果在这段时间内一直连接超时，将重新建立OpenVPN隧道。	120
TUN MTU	设置隧道的MTU。	1500
数据分片	设置隧道传输数据的分片大小。	空
私钥密码	输入在“X509CA”以及“X509CA密码”验证方式下的私钥密码。	空
启用压缩	单击切换按钮以启用/禁用该选项。启用后，该功能会压缩IP数据包的头部。	ON
接收 DNS 推送	单击切换按钮以启用/禁用该选项。启用后，会接收服务器推送的DNS作为本端DNS服务器。	OFF
启用虚拟接口与 LAN0 桥接	单击切换按钮以启用/禁用该选项。启用后，可以实现虚拟接口和Lan0进行桥接。	ON
启用默认网关	单击切换按钮以启用/禁用该选项。启用后，会接收服务器推送的网关作为本端网关。	OFF
启用客户端状态	单击切换按钮以启用/禁用该选项。用于服务器启用后，可显示已连接的客户端状态信息。	OFF
启用 NAT	单击切换按钮以启用/禁用NAT（网络地址转换）功能。开启后，本设备身后的主机IP将会被封装起来。	OFF
日志信息级别	选择输出log信息级别，取值0~11。 • 0：仅输出致命错误信息 • 1~4：正常使用范围 • 5：输出数据包收发信息 • 6~11：调试信息范围	0
高级设置 @ OpenVPN		
启用 HMAC 防火墙	单击切换按钮以启用/禁用此选项。在 TLS 控制通道顶端添加额外的 HMAC（Hash Message Authentication Code）认证，以保护链路防止 DoS 攻击。	OFF
启用 PKS#12	单击切换按钮以启用/禁用 PKCS#12 证书。PKS#12，一种数字证书加密标准，用于标识个人身份信息。	OFF
启用 nsCertType	单击切换按钮以启用/禁用 nsCertType，即指定采用服务器校验方式。服务器开启 nsCertType，OpenVPN 客户端也需配置一致。	OFF
专家选项	在此字段中输入一些其他PPP初始化的字符串。每个字符串用空格分开。	空

状态

本节用于查看 OpenVPN 当前的连接状态。

X509

本节用于导入证书和查看证书。

x509		
项目	**说明**	**默认**
X509 设置		
隧道名字	选择一条有效的隧道，可从“隧道1”，“隧道2”，“隧道3”，“隧道4”，“隧道5”和“隧道6”选择。	隧道 1
隧道模式	所选择隧道所设置的隧道模式。	客户端模式
导入文件方式	选择导入文件的方式，可从“Default”和“Manual-Import”选择。	Default
根证书	选择根证书文件导入到本设备中。	--
证书文件	选择证书文件导入到本设备中。	--
私钥	选择私钥文件导入到本设备中。	--

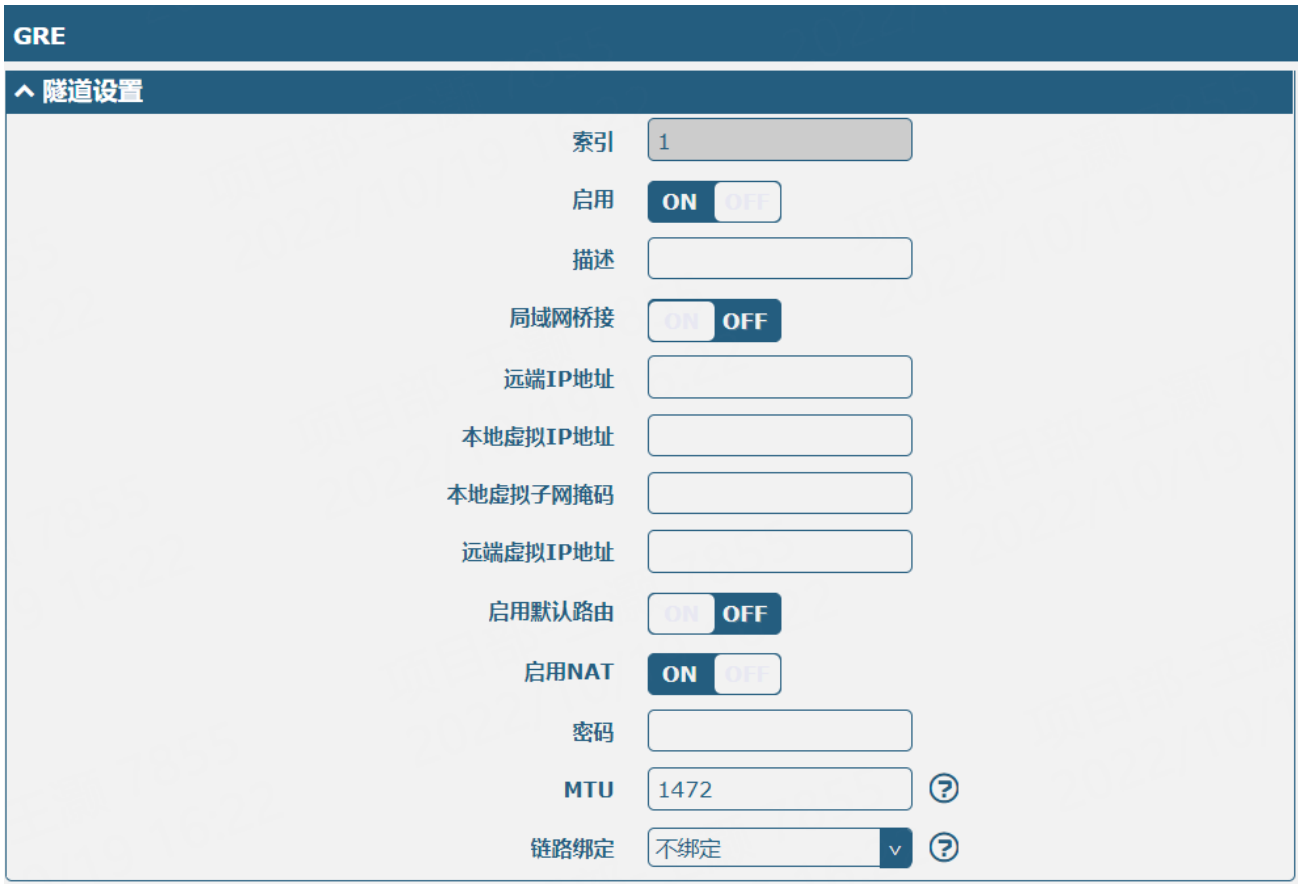
TLS-Auth 密钥	选择TLS-Auth密钥文件导入到本设备中。	--
PKCS#12 证书	选择PKCS#12证书文件导入到本设备中。	--
证书文件		
索引	显示表序号。	--
文件名	显示已导入本设备的证书名称。	空
文件大小	显示当前文件的大小。	空
最后修改时间	显示上一次修改证书的时间。	空

3.5.4 GRE

本节用于设置 GRE 参数。GRE（Generic Routing Encapsulation），即通用路由协议封装，规定了如何用一种网络协议去封装另一种网络协议的方法。GRE 协议的主要用途有两个：企业内部协议封装和私有地址封装。

GRE

单击 ➕ 以添加 GRE 隧道，最多可添加 5 条。



隧道设置@GRE		
项目	**说明**	**默认**
索引	显示表序号。	--
启用	单击切换按钮以启用/禁用GRE。GRE（通用路由封装）是封装数据包协议以便能够在IP网络中路由其他协议的数据包。	ON
描述	输入对此GRE隧道的描述。	空
局域网桥接	单击切换按钮以启用/禁用桥接到LAN	OFF
远端 IP 地址	设置GRE隧道的远端真实IP地址。	空
本地虚拟 IP 地址	设置GRE隧道的本地虚拟IP地址。	空
本地虚拟子网掩码	设置GRE隧道的本地虚拟子网掩码。	空
远程虚拟 IP 地址	设置GRE隧道远端的虚拟IP地址。	空
启用默认路由	单击切换按钮以启用/禁用该选项。启用后，所有数据流量都会通过GRE隧道发送。	OFF
启用 NAT	单击切换按钮以启用/禁用NAT（网络地址转换）遍历。在NAT（网络地址转换）环境中，必须启用这个选项。	OFF
密码	设置GRE隧道密钥。	空

MTU	设置最大传输单元。	1472
链接绑定	选择绑定的链接。例如：WWAN1, WWAN2, WLAN, WAN。	Unbound

X509

本节用于查看 GRE VPN 的连接状态。

3.6 服务

3.6.1 系统日志

本节用于设置系统日志参数，其“记录到远程”功能默认为关闭。本设备的系统日志可以保存在本地，支持发送系统日志到远程日志服务器的功能，也支持指定应用程序调试。

当启用“记录到远程”时，窗口显示如下：

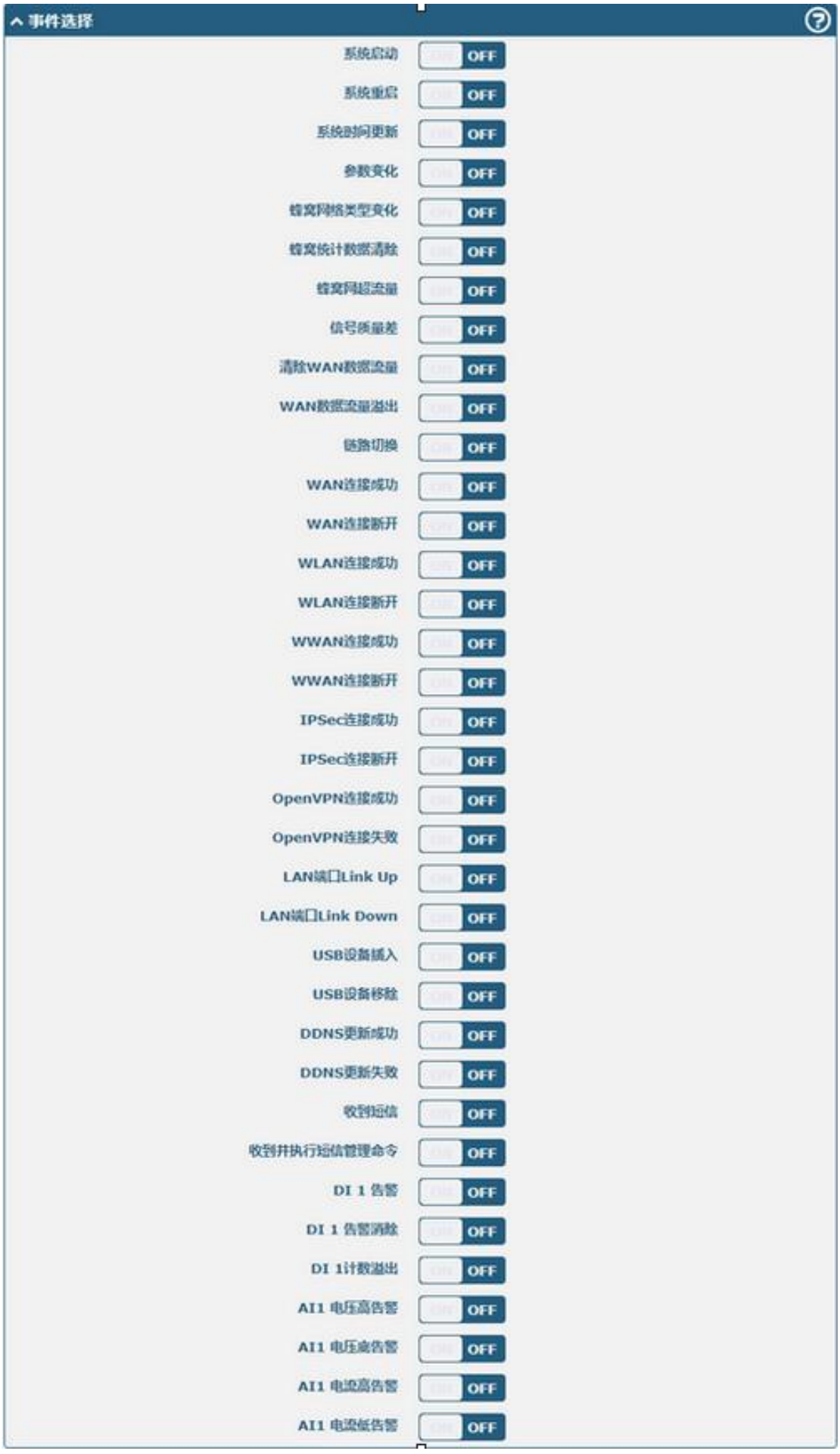
系统日志设置		
项目	**说明**	**默认**
启用	单击切换按钮以启用/禁用系统日志设置功能。	ON
系统日志级别	选择“调试”、“信息”、“通知”、“警告”或“错误”。越低级别输出的信息越多，即调试输出的信息更详细。	调试
保存位置	可选“RAM”、“NVM”或“控制台”以指定保存系统日志的地方。 ***注：****不建议长时间保存系统日志到NVM。*	RAM
记录到远程	单击切换按钮以启用/禁用“记录到远程”功能。启用后，本设备可以发送系统日志到远程日志服务器。	OFF
添加标识符	单击切换按钮以启用/禁用此选项。启用后，添加序列号到日志信息，用于上传 Syslog 到 RCMS。	OFF
远程 IP 地址	当开启“记录到远程”功能时，输入系统日志服务器的 IP 地址。	空
远程端口	当开启“记录到远程”功能时，输入系统日志服务器的端口号。	514

3.6.2 事件

本节用于设置本设备通知。可以配置为短信发送事件告警，也可以通过 SMS 或电子邮件发送警报。

单击+以添加事件。

常规设置@通知		
项目	**说明**	**默认**
索引	显示表序号。	--
描述	输入对此事件通知的描述。	空
发送 SMS	单击切换按钮以启用/禁用此选项。开启后，事件发生本设备会以SMS形式将通知发送到指定的电话号码。指定电话号码在“3.6.4 短信”里设置。	OFF
电话号码	输入用于接收事件提醒的电话号码。多个电话号码请用分号（;）分隔开。	空
发送 Email	单击切换按钮以启用/禁用此选项。开启后，事件发生本设备会以Email形式将通知发送到指定的电子邮箱。指定电子邮箱在“3.6.5 Email”里设置。	OFF
Email 地址	输入用于接收事件通知的邮箱地址，多个邮箱地址请用空格分隔开。	空
DO 控制	单击切换按钮以启用/禁用此选项。开启后，触发DO输出。	OFF
保存到 NVM	单击切换按钮以启用/禁用此选项。启用后，将事件保存到非易失存储器。	OFF


事件选择
系统启动 OFF
系统重启 OFF
系统时间更新 OFF
参数变化 OFF
蜂窝网络类型变化 OFF
蜂窝统计数据清除 OFF
蜂窝网超流量 OFF
信号质量差 OFF
清除WAN数据流量 OFF
WAN数据流量溢出 OFF
链路切换 OFF
WAN连接成功 OFF
WAN连接断开 OFF
WLAN连接成功 OFF
WLAN连接断开 OFF
WWAN连接成功 OFF
WWAN连接断开 OFF
IPSec连接成功 OFF
IPSec连接断开 OFF
OpenVPN连接成功 OFF
OpenVPN连接失败 OFF
LAN端口Link Up OFF
LAN端口Link Down OFF
USB设备插入 OFF
USB设备移除 OFF
DDNS更新成功 OFF
DDNS更新失败 OFF
收到短信 OFF
收到并执行短信管理命令 OFF
DI 1 告警 OFF
DI 1 告警消除 OFF
DI 1计数溢出 OFF
AI1 电压高告警 OFF
AI1 电压底告警 OFF
AI1 电流高告警 OFF
AI1 电流低告警 OFF

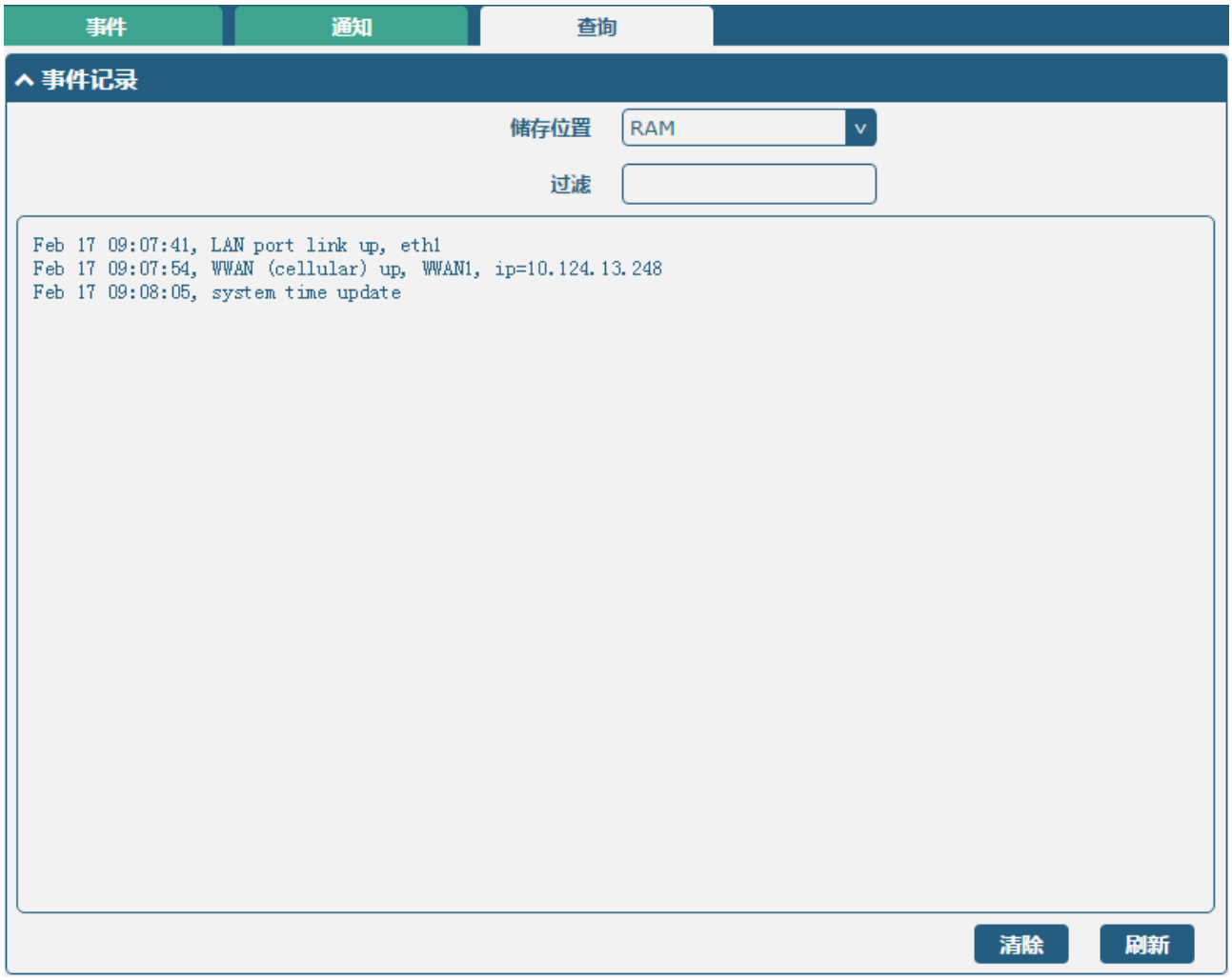
事件

本节用于配置信号质量门限。

常规设置 @ Event		
项目	**说明**	**默认**
信号质量阈值	设置信号质量阈值。当实际阈值小于指定阈值时，本设备将生成日志事件。0 表示禁用此选项。	0

查询

“查询”栏中可以查询各类事件发生记录。选择存储位置，在过滤项里输入关键词筛选事件，用分隔符“&”分隔两个或两个以上的关键词。单击 刷新 即可查询事件记录，单击 清除 即可清除窗口的事件记录。



事件记录		
项目	**说明**	**默认**
储存位置	可选“RAM”或“NVM”。 • RAM：Random-Access Memory 随机存取存储器。 • NVM：Non-Volatile Memory固定存储器。	RAM
过滤	输入基于客户设置的关键字过滤事件信息。单击 刷新 按钮，过滤事件被会显示于下列表格中；使用“&”符号以分隔关键字，如信息1&信息2。	空

3.6.3 NTP

本节用于设置本设备的时钟和 NTP（Network Time Protocol）网络时间协议。

NTP		
项目	**说明**	**默认**
时区设置		
时区	选择您本地时区。例如中国：UTC+08:00。	UTC+08:00
专家设置	按TZ环境变量格式指定时区和夏令时，此时时区参数设置将会被忽略。不支持设置特殊字符，例如“~”。	空
NTP 客户端设置		
启用	单击切换按钮以启用/禁用此选项。开启NTP客户端模式后，本设备与NTP服务器在时间上将会实现同步。	ON
首选 NTP 服务器	输入首选NTP服务器的IP地址或者域名。	pool.ntp.org

NTP		
项目	**说明**	**默认**
备用 NTP 服务器	输入备用NTP服务器的IP地址或者域名。	空
NTP 更新间隔	输入NTP客户端和NTP服务器的时间进行同步的间隔时间。等待一个NTP更新间隔后进行下一次更新，0表示只更新一次。	0
请求网络端口	选择“默认”或“lan”。	默认
NTP 服务器设置		
启用	单击切换按钮以启用/禁用本设备的NTP服务器功能。启用后，NTP客户端即可与本设备在时间上实现同步。	OFF

状态

本节用于查看本设备的系统时间和连接本设备的电脑时间。单击 同步 即可使本设备的时间与电脑同步。

3.6.4 短信

本节用于设置短信参数。本设备支持短信管理，用户可以发送短信来控制和配置本设备。更多关于短信控制的内容，请参阅“4.1.2 短信远程控制”。

短信管理设置		
项目	**说明**	**默认**
启用	单击切换按钮以启用/禁用短信管理配置。 ***注：****若关闭此功能，短信配置本设备则无效。*	ON
认证类型	该选项指定短信管理的身份验证类型，可以选择“密码”、“电	密码

短信管理设置		
项目	**说明**	**默认**
	话号码”或“两者都要”。 • 密码：使用与WEB网管相同的用户名和密码进行验证。短信格式为“用户名：密码; 命令1; 命令2; ...” ***注：****在“系统 > 用户管理”中设置网管的密码。* • 电话号码：只允许指定的电话号码，不需要密码。短信格式为“命令1; 命令2; ...” • 两者都要：只允许指定的电话号码，同时需要密码。短信格式为“用户名：密码; 命令1; 命令2; ...”	
电话号码	输入用于短信管理的号码，用分号（;）分隔多个号码。 ***注：****认证类型选择“密码”时，可以不填。*	空
数据编码方案	选择“GSM-7”或“ucs2”	GSM-7

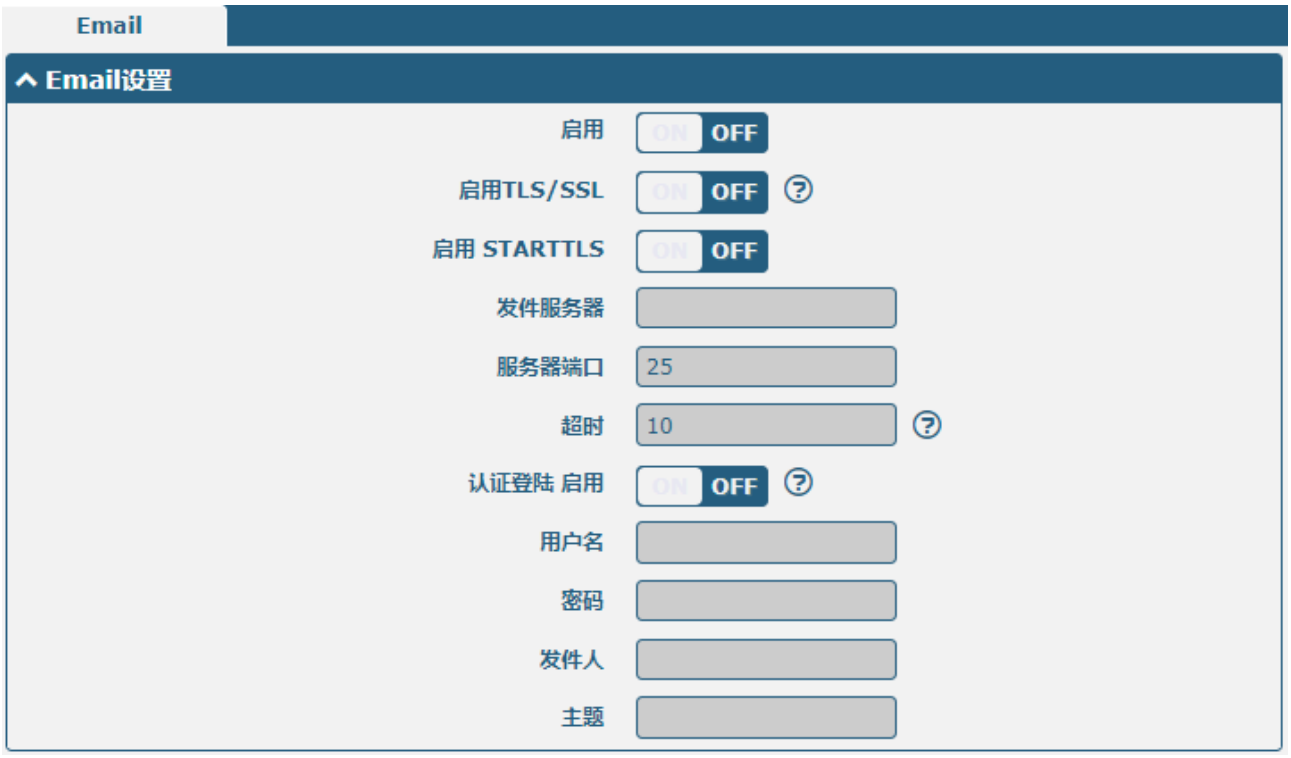
短信测试

本节用于测试当前短信服务是否可用。

短信测试		
项目	**说明**	**默认**
电话号码	输入一个可以接收本设备发送短信的号码。	空
信息	输入测试信息。	空
结果	显示短信的测试结果。例如短信发送成功，此结果框则会显示“OK”。	空
发送	单击该按钮以发送测试短信内容。	--

3.6.5 Email

本设备的电子邮件功能支持将事件推送以电子邮件的方式发送到指定的收件人。



Email 设置		
项目	**说明**	**默认**
启用	单击切换按钮以启用/禁用Email功能。	OFF
启用 TLS/SSL	单击切换按钮以启用/禁用TLS/SSL加密。	OFF
启用 STARTTLS	单击切换按钮以启用/禁用STARTTLS加密传输方式。	OFF
发件服务器	输入SMTP服务器IP地址或域名。	空
服务器端口	输入SMTP服务器端口。	25
超时	输入超时时间。	10
认证登陆 启用	使用用户名密码认证。	OFF
用户名	输入 SMTP 服务器已注册的用户名。	空
密码	输入SMTP服务器已注册的用户名的密码。	空
发件人	输入该邮件的源地址。	空
主题	输入该邮件的主题。	空

3.6.6 DDNS

DDNS，全称 Dynamic Domain Name Server，即动态域名服务。DDNS 服务允许将一个动态 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，即 DDNS 服务允许您为主机动态的 WAN IP 分配一个固定的域名，其他用户则可以直接通过此固定的域名访问您的主机，而不是通过动态 WAN IP 地址。本设备的动态 WAN IP 地址由 ISP 直接分配。单击“**服务 > DDNS**”以设置 DDNS 的相关参数，其服务提供商默认为“DynDNS”。

DDNS

当“服务提供商”选择“自定义”时，窗口显示如下：

当“服务提供商”选择“NO-IP”时，窗口显示如下：

当“服务提供商”选择“3322”时，窗口显示如下：

DDNS 设置		
项目	**说明**	**默认**
启用	单击切换按钮以启用/禁用DDNS设置。	OFF
服务提供商	可选“DynDNS”，“NO-IP”，“3322”或“自定义”。 ***注：****在相应的服务提供商注册后，才可以使用动态域名解析服务。*	DnyDNS
主机名	输入由DDNS提供的主机名。	空
用户名	输入由DDNS提供的用户名。	空
密码	输入由DDNS提供的密码。	空
URL	输入用户自定义URL。	空
Max tries	输入最大尝试次数	3

状态

本节用于查看当前 DDNS 的状态。

DDNS 状态	
项目	**说明**
状态	显示当前DDNS的状态。
上次更新时间	显示上次成功更新DDNS的时间。

3.6.7 SSH

本设备支持 SSH 密码访问和密钥访问。

SSH 设置		
项目	**说明**	**默认**
启用	单击切换按钮以启用/禁用“SSH访问本设备”功能。	OFF
端口	输入想要访问的端口。	22
禁用密码登陆	单击切换按钮以启用/禁用该选项。启用后，用户不能使用用户名和密码通过SSH访问本设备。倘若禁用密码登陆后想要SSH访问本设备，只能使用密钥登录。	OFF

导入公有密钥	
项目	**说明**
公有密钥	当启用禁用密码登录时，此项有效。从电脑导入一个正确的公钥到本设备，用户不用密码也可直接SSH访问本设备。

3.6.8 电话

本节用于设置语音接口的参数。若本设备带语音，则此“电话”页面可配。

注：

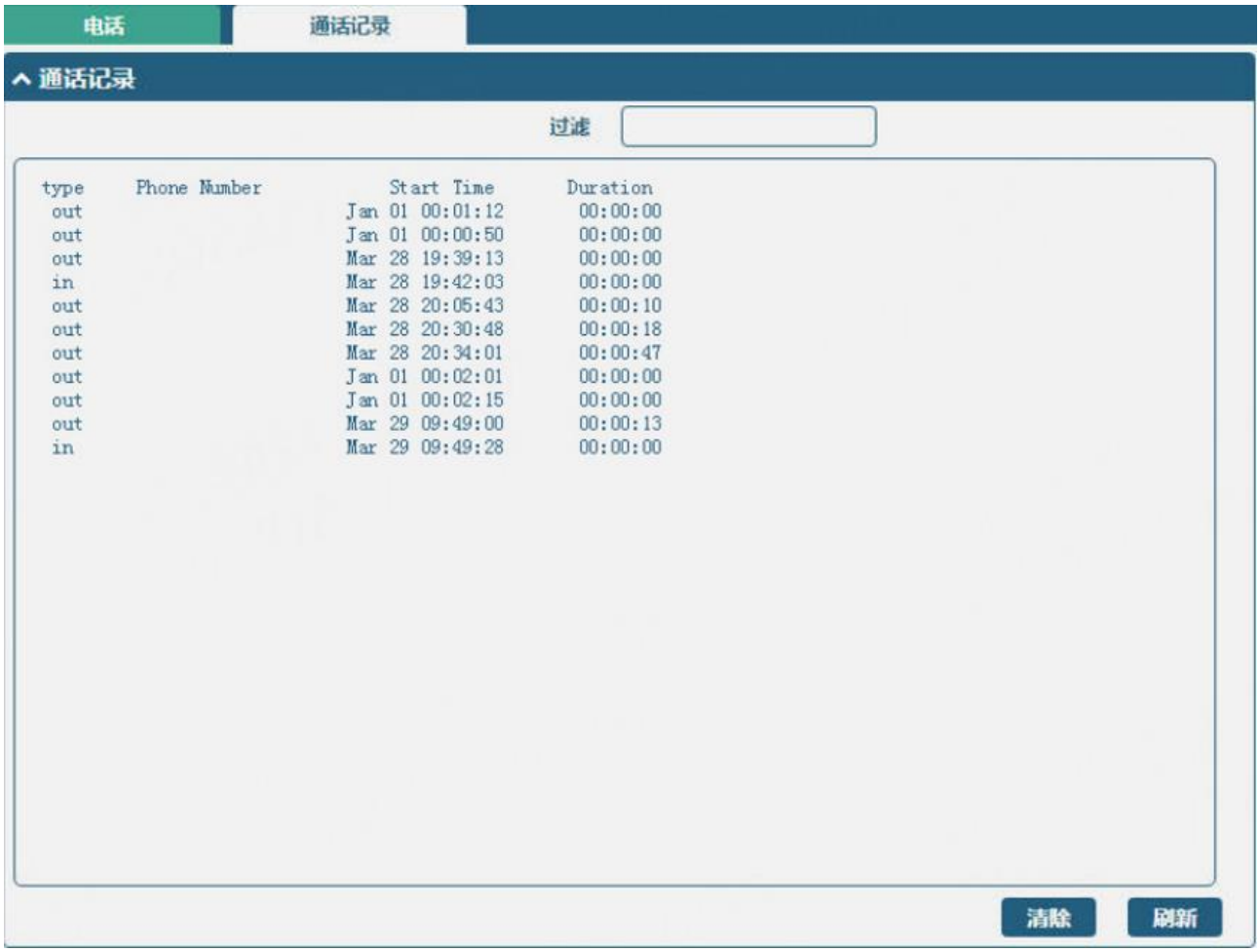
1) 蜂窝网的语音通话和数据服务能否同时进行取决于您的运营商网络。

2) R2000-Ent ， R3010 和 ET8013 支持电话功能。

常规设置@拨号策略		
项目	**说明**	**默认**
等待拨号超时	设置等待拨号超时时间，单位为秒。	5
数图	数图用于匹配电话输入的电话号码。当输入的电话号码与数图规则完全匹配时，系统会立即呼叫此号码，不匹配这等待超时拨号。此功能用于快速拨号。	空

通话记录

本节用于查看通话的记录。



通话记录		
项目	**说明**	**默认**
过滤	输入用于过滤通话记录的关键词。	空
清除	单击按钮以清除通话记录。	--
刷新	单击按钮以刷新通话记录。	--

3.6.9 Ignition

本节用于配置 Ignition 参数。

注：

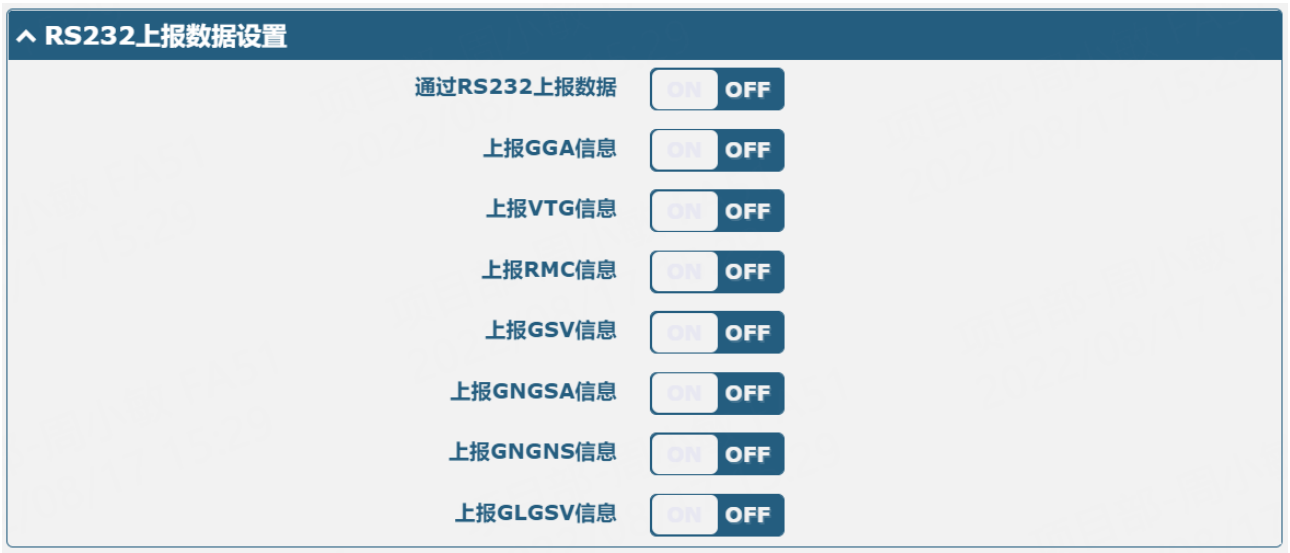
1）R5020 和 R2110 支持该选项。

常规设置		
项目	**说明**	**默认值**
Delay Shutdown	输入要延迟断电的时间（以秒为单位）。延迟断电的超时时间为 60 秒至 3600 秒。	60

3.6.10 GPS

本节用于配置 GPS 的参数。本设备的 GPS 功能可以定位和获取设备的位置信息，并且上报给指定的服务器。

注：R1520 无独立的 GPS 模块，定位数据来源于蜂窝模块，是否支持 GPS 功能取决于蜂窝模块。



GPS		
项目	说明	默认
常规设置		
启用	单击切换按钮到“ON”以启用GPS功能。	OFF
同步 GPS 时间	单击切换按钮到“ON”以同步GPS时间。	OFF
RS232 上报数据设置		
通过 RS232 上报数据	通过RS232的方式上报GPS信息。	OFF
上报 GGA 信息	上报GGA信息。	OFF
上报 VTG 信息	上报VTG信息。	OFF
上报 RMC 信息	上报RMC信息。	OFF
上报 GSV 信息	上报GSV信息。	OFF
上报 GNGSA 信息	上报GNGSA信息。	OFF
上报 GNGNS 信息	上报GNGNS信息。	OFF
上报 GLGSV 信息	上报GLGSV信息。	OFF

单击 添加 GPS 服务器。

项目	说明	默认
索引	显示序号。	--
启用	单击切换按钮到“ON”以启用GPS数据转发设置。	ON
协议	可选“TCP客户端”，“TCP服务器”或“UDP”作为协议。 • TCP客户端：网关作为TCP客户端时，启动与TCP服务器（GPS服务器），服务器的地址同时支持IP和域名。 • TCP服务器：网关作为TCP服务器（GPS服务器），监听TCP客户端的连接请求。 • UDP：网关作为UDP客户端。	TCP 客户端
服务器/本地地址	服务器或本地地址。	空
服务器/本地端口	服务器或本地端口。	空
发送 GGA 信息	单击切换按钮以启用/禁用此选项。	OFF
发送 VTG 信息	单击切换按钮以启用/禁用此选项。	OFF
发送 RMC 信息	单击切换按钮以启用/禁用此选项。	OFF
发送 GSV 信息	单击切换按钮以启用/禁用此选项。	OFF

高级设置		
项目	**说明**	**默认**
删除 LF 字符	单击切换按钮以启用/禁用此选项。	ON
自定义 GPSID	自定义GPSID在传输前附加到 NMEA 消息中。可选择“无”、“前缀”、“后缀”。	无
GPSID 标题	输入GPSID标题，通常为7个大写字母	空
添加 SN 到 GPSID	单击切换按钮以启用/禁用此选项。	OFF

状态

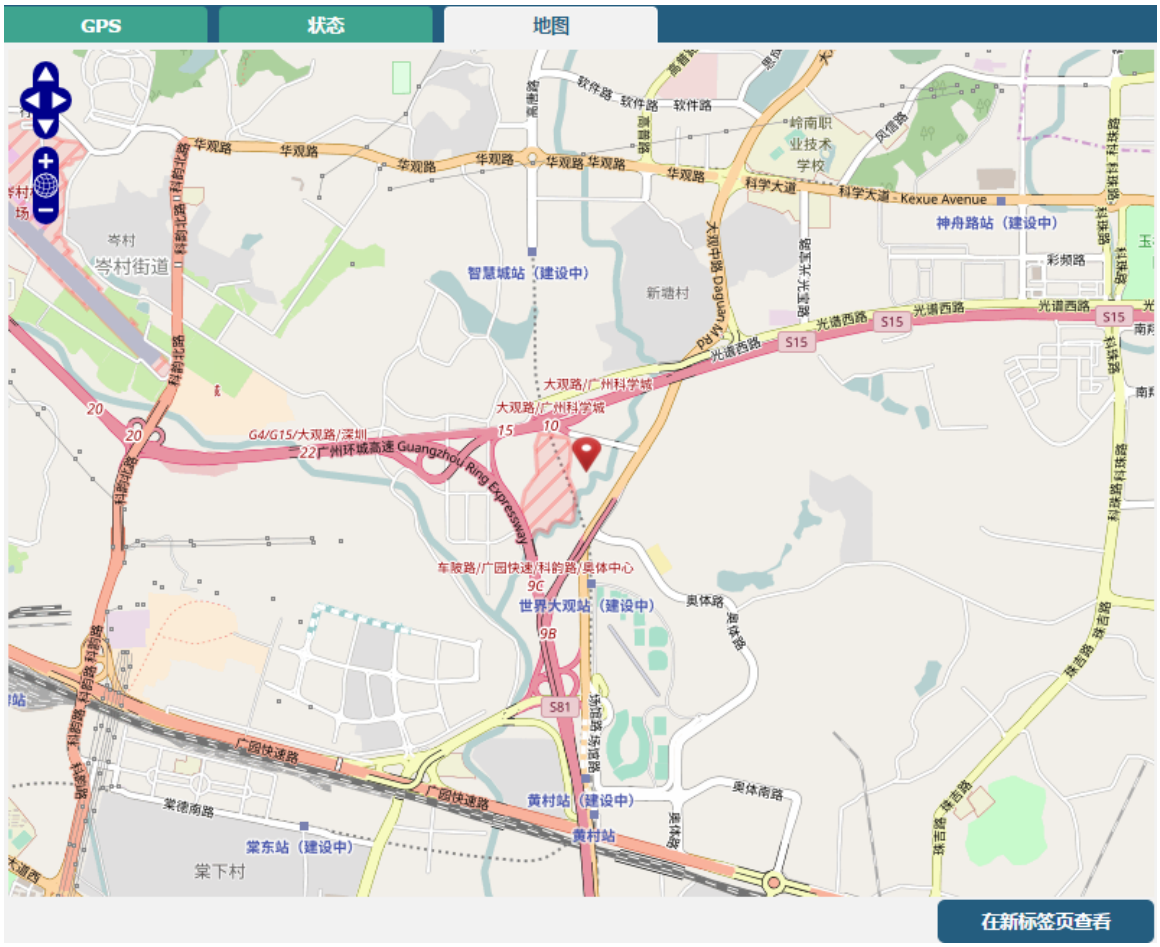
本节用于查看本设备当前的 GPS 状态；

GPS 状态	
项目	**说明**
状态	显示本设备的当前GPS状态。
世界标准时间	显示卫星的UTC。 ***注：****UTC是世界统一时间，而不是当地时间。*
最后定位时间	最后一次定位成功的时间。
卫星使用数量	使用的卫星数量。
可见卫星数量	可见的卫星数量。
纬度	显示本设备的纬度信息。
经度	显示本设备的经度信息。

高度	显示本设备的高度信息。
速度	显示本设备的移动速度。

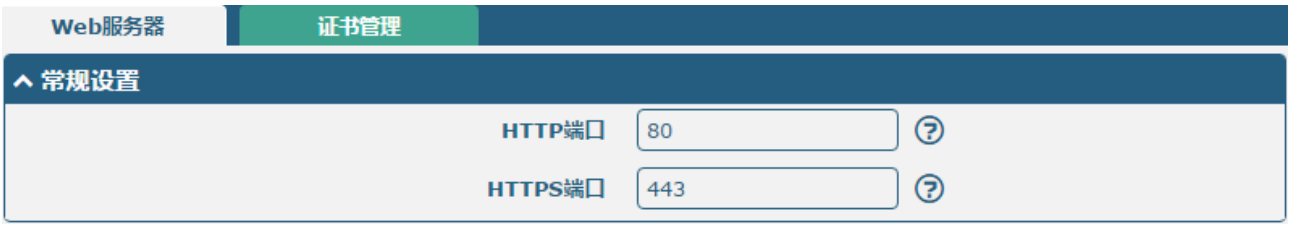
地图

本节用于查看本设备当前的地理定位。



3.6.11 Web 服务器

本节用于配置 Web 服务器的参数。



常规设置@Web 服务器		
项目	**说明**	**默认**
HTTP 端口	输入您想在本设备的 Web 服务器使用的 HTTP 端口号。在 Web 服务器上，80 端口是服务器监听或从 Web 客户端接收数据的端口。如果您用其他的 HTTP 端口号配置本设备而不是用 80，那么您只要加上端口号就可以登录本设备的 Web 服务器。	80
HTTPS 端口	输入您想在本设备的 Web 服务器使用的 HTTPS 端口号。在 Web 服务器上，443 端口是服务器监听或从 Web 客户端接收数据的端口。如果您用其他的 HTTPS 端口号配置本设备而不是用 443，那么您只要加上端口号就可以登录本设备的 Web 服务器。 ***注：****HTTPS 比 HTTP 更安全。在许多案例中，客户端和服务器之间要交换机密数据，要做好安全禁止非法入侵。*	443

X509

本节用于用户将证书文件导入到本设备中。

导入证书文件		
项目	**说明**	**默认**
导入类型	可选“CA”或“私有密钥”。 • CA：CA 中心签发的数字证书。 • 私有密钥：私钥文件。	CA
HTTPS 证书文件	单击“选择文件”从电脑中选择证书文件，再单击“导入”从电脑中导入文件到本设备。	--

3.6.12 高级

本设备高级设置包括系统设置和重启。

系统设置		
项目	**说明**	**默认**
设备名字	设置本设备的名字，以区分其它已安装的设备。	router
自定义 LED 灯类型	可选“无”、“SIM”、“OpenVPN”或“IPsec”。 • 无：选择此选项后，USR指示灯灭，无意义。 • SIM：选择此类型后，本设备的USR指示灯显示的是SIM卡的状态。 • OpenVPN：选择此类型后，本设备的USR指示灯显示的是OpenVPN的状态。 • IPsec：选择此类型后，本设备的USR指示灯显示的是IPsec的状态。	无

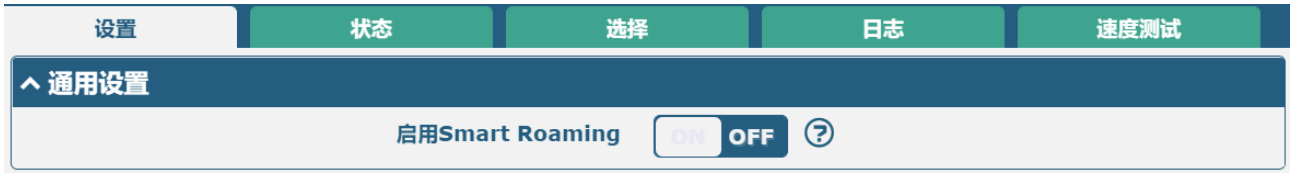
X509

本节用于设置重启设备的类型。

定期重启设置		
项目	**说明**	**默认**
定期重启	设置本设备重启的周期。0代表不启用定期重启。	0
每天重启时间	设置每天重启本设备的时间点，格式为HH：MM（24小时制）。此项为空时代表关闭定时重启。	空

3.6.13 Smart Roaming V2

Smart Roaming 设置包括常用设置、健康检查、PING 设置和高级设置。



常用设置		
项目	说明	默认
启用 Smart Roaming	单击切换按钮以启用/禁用“Smart Roaming”功能。	OFF

健康检查设置		
项目	**说明**	**默认**
健康检查间隔	当前连接的健康检查间隔时间，单位分钟。如果健康检查失败，Smart Roaming 会尝试切换到其他运营商网络。注意不要把所有的检查条件都设置为理论上无法达到的值。	5 分钟
RSSI 质量检查	单击切换按钮以启用/禁用“RSSI质量检查”功能。	OFF
RSSI 阈值（3G）	2G网络的信号强度阈值。	-85 dBm
RSSI 阈值（3G）	3G网络的信号强度阈值。	-95 dBm
RSSI 阈值（4G）	4G网络的信号强度阈值。	-100 dBm
RSRP 质量检查	单击切换按钮以启用/禁用“RSRP质量检查”功能。	OFF
RSRP 阈值（4G）	4G网络的参考信号接收功率阈值。	-100 dBm
RSRQ 质量检查	单击切换按钮以启用/禁用“RSRQ质量检查”功能。	OFF
RSRQ 阈值（4G）	4G 网络的参考信号接收质量阈值。	-20 dBm
网络延时检查	单击切换按钮以启用/禁用“网络延时检查”功能。	ON
RTT 超时时间阈值	往返时延超时时间。	3000 ms
丢包率检查	单击切换按钮以启用/禁用“丢包率检查”功能。	ON
丢包率阈值	设置丢包率阈值。	70 %

PING 设置		
项目	**说明**	**默认**
首选服务器	本设备ping主地址/域名来检测当前连接是否一直存在。	8.8.8.8
备用服务器	本设备ping备用地址/域名来检测当前连接是否一直存在。	114.114.114.114
Ping 超时时间	设置Ping的超时时间。	5 秒
Ping 尝试次数	每次健康检查时的ping尝试次数。每个ping尝试默认都会发送3个ping报文，因此每次健康检查时发送的总的ping报文数量为（3*ping尝试次数）。	3 次

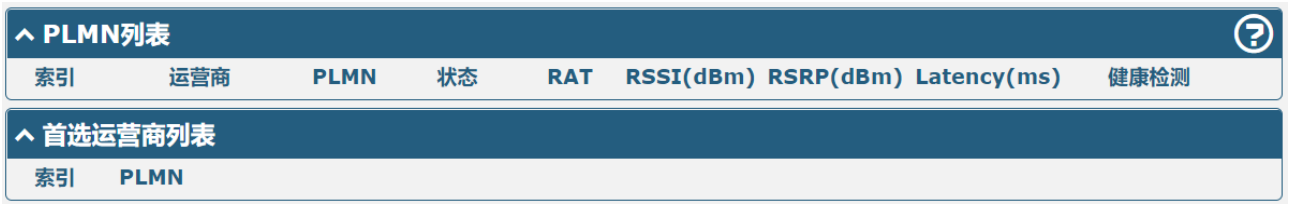
高级设置		
项目	说明	默认
使用降级网络	单击切换按钮以启用/禁用“使用降级网络”功能。降级网络的定义是可以联网，但是网络质量不满足健康检查的阈值。	OFF
定期重启	设置重启“Smart Roaming”功能的周期，以小时为单位。0代表不启用定期重启。重启“Smart Roaming”会重新搜索可用的运营商网络和重置当前状态，因为搜索可用的运营商网络耗时较长，重启可能会耗时3到5分钟。	0
每天重启时间	设置每天重启“Smart Roaming”的时间点，格式为HH：MM（24小时制）。此项为空时代表关闭定时重启。	空
首选运营商列表	通过PLMN设置首选运算符列表。如果需要多个运算符，请使用分号分隔，例如46000；46001	空

状态

本节用于查看当前连接的状态。

状态	
项目	说明
状态	显示当前“Smart Roaming”的状态。包括 Scanning、Connecting、Connected、Inactive 等状态，分别表明正在搜索可用网络、正在连接网络、网络已连接、功能未启动。
运营商选择模式	显示当前按照何种方式选择运营商网络。包括 Automatic 和 Manual 两种方式，分别指按照标准规范的自动选择和软件根据网络质量进行选择，软件会循环在这两种方式间进行切换。

从上次搜索可用网络开始经过的时间	显示从上次搜索可用网络开始经过的时间。“Smart Roaming”重启会刷新此时间。



PLMN 列表	
项目	**说明**
索引	PLMN 列表索引。
PLMN	PLMN = MCC + MNC，即移动国家代码和移动网络代码的组合。
状态	当前网络状态，包括 Current、Visible、Forbidden、Unknown 等状态，分别表明当前使用此网络、可用网络、禁止网络和未知网络。
RAT	当前无线接入技术，包括 3G/4G/5G。
RSSI	当前信号质量，用于 3G、4G 网络。
RSRP	当前参考信号接收功率，用于 4G、5G 网络。 （连接 5G 时，不能看信号强度 RSSI，只能看信号功率 RSRP）
延时	当前网络延时。
丢包率	当前网络丢包率。
健康检查情况	当前健康检查情况，包括 Pending、Good、Degraded、Failed 等，分别表明当前网络还未进行健康检查、网络质量良好、降级网络、网络质量差（包括网络断开或者不满足健康检查阈值）。
首选运营商列表	
索引	PLMN 列表索引。
PLMN	PLMN = MCC + MNC，即移动国家代码和移动网络代码的组合。

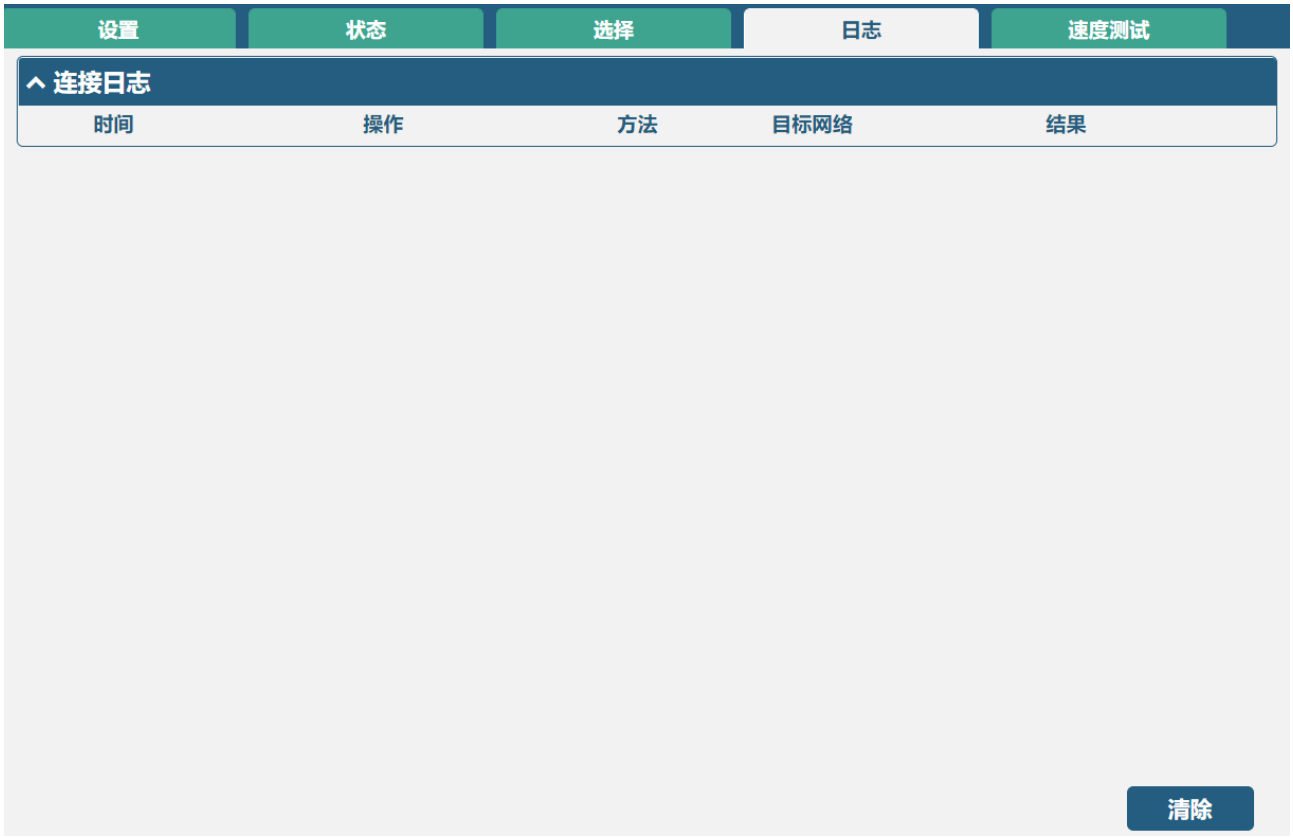
选择

本节用于配置网络选择。

运营商选择		
项目	**说明**	**默认值**
用户指定的网络选择	选择指定的网络。	--
Forget RPLMN	强制从 SIM 中删除所有位置信息。	--
Rescan	重新扫描运营商网络列表	--
提交	提交用户指定的网络选择	--

日志

本节用于查看连接日志。



日志		
清除	单击按钮以清除连接日志。	--

速度测试

本节用于查看测试当前网络的速度。

速度测试		
Speedtest	单击按钮开始网络速度测试。	--
清除	单击按钮以清除速度测试日志。	--

3.7 系统

3.7.1 调试

本节用于查看、生成本设备的系统运行日志和诊断数据。单击**“服务 > 系统日志 > 系统日志设置”**以开启系统日志。

系统日志		
项目	**说明**	**默认值**
日志记录		
日志等级	可选择“调试”、“信息”、“通知”、“警告”或“错误”作为日志级别。	Debug

过滤	输入基于关键字过滤日志信息，可使用“&”分隔关键字。	空
手动更新	可选“手动更新”，“5秒”，“10秒”，“20秒”或“30秒”作为刷新日志信息的时间间隔。	手动更新
清除	单击清除窗口内的系统日志。	--
刷新	单击刷新窗口内的系统日志。	--
日志文件		
日志文件	列表中最多可以显示5个系统日志文件，文件名从message0到message4不等。最新的系统日志文件将放在列表的顶部。	--
系统诊断数据		
生成	单击生成系统诊断数据。当设备出现问题时，可以生成系统诊断数据并发送给鲁邦通技术支持代表来获取协助。	--

3.7.2 软件更新

本节用于升级本设备系统，以导入和更新固件文件的方式实现系统更新。从电脑导入固件文件到本设备，单击 更新 ，并根据系统提示重启设备以完成固件更新。

注：*如需最新的固件文件，请联系我司的技术支持工程师。*

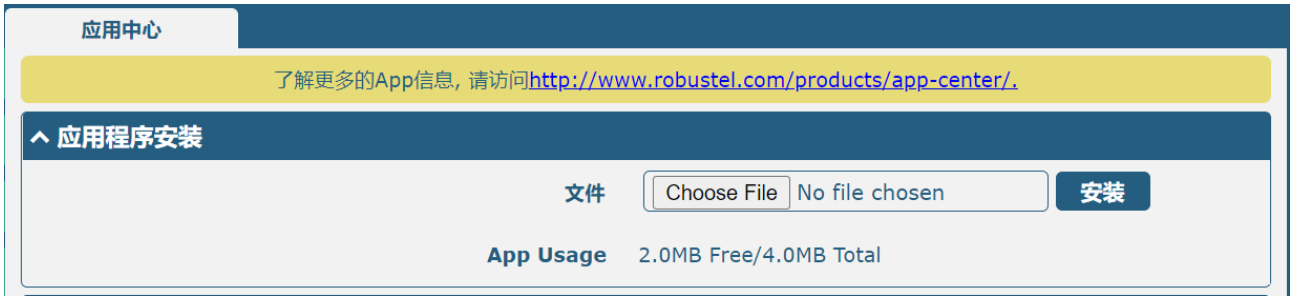
软件更新	
选项	**描述**
固件更新	
文件	单击 选择文件 按钮从您的计算机中找到文件，然后单击 更新 进行系统更新。
文件上传@上传自定义文件	
文件	单击 选择文件 按钮从您的计算机中找到文件，然后单击 导入 进行导入自定义文件操作。

文件上传@自定义文件列表	
索引	显示自定义文件序号。
文件名	显示自定义文件名称。
文件大小	显示自定义文件大小。
最后修改时间	显示自定义文件最后修改时间。

3.7.3 应用中心

本设备支持 App 导入。在此应用中心里直接导入并安装 App，根据系统提示重启设备即可。安装成功后的 App 会在“服务”栏中显示，而其他的 VPN App 安装后则会显示于“VPN”栏中。

注：*由于浏览器缓存原因，导入 App 到本设备并重启后，页面显示会有延迟；此情况下，建议先清理浏览器的缓存再重新登录本设备。*



成功安装的 App 会在以下列表里显示，单击✕即可卸载该 App。

应用中心	
项目	**说明**
应用程序安装	
文件	从您的电脑中选择想要安装的应用程序，单击“安装”按钮以导入到本设备中。 文件格式：xxx.rpk。
已装应用程序	
索引	显示表序号。
名字	显示应用程序的名字。
版本	显示应用程序的版本。
状态	显示应用程序的状态。

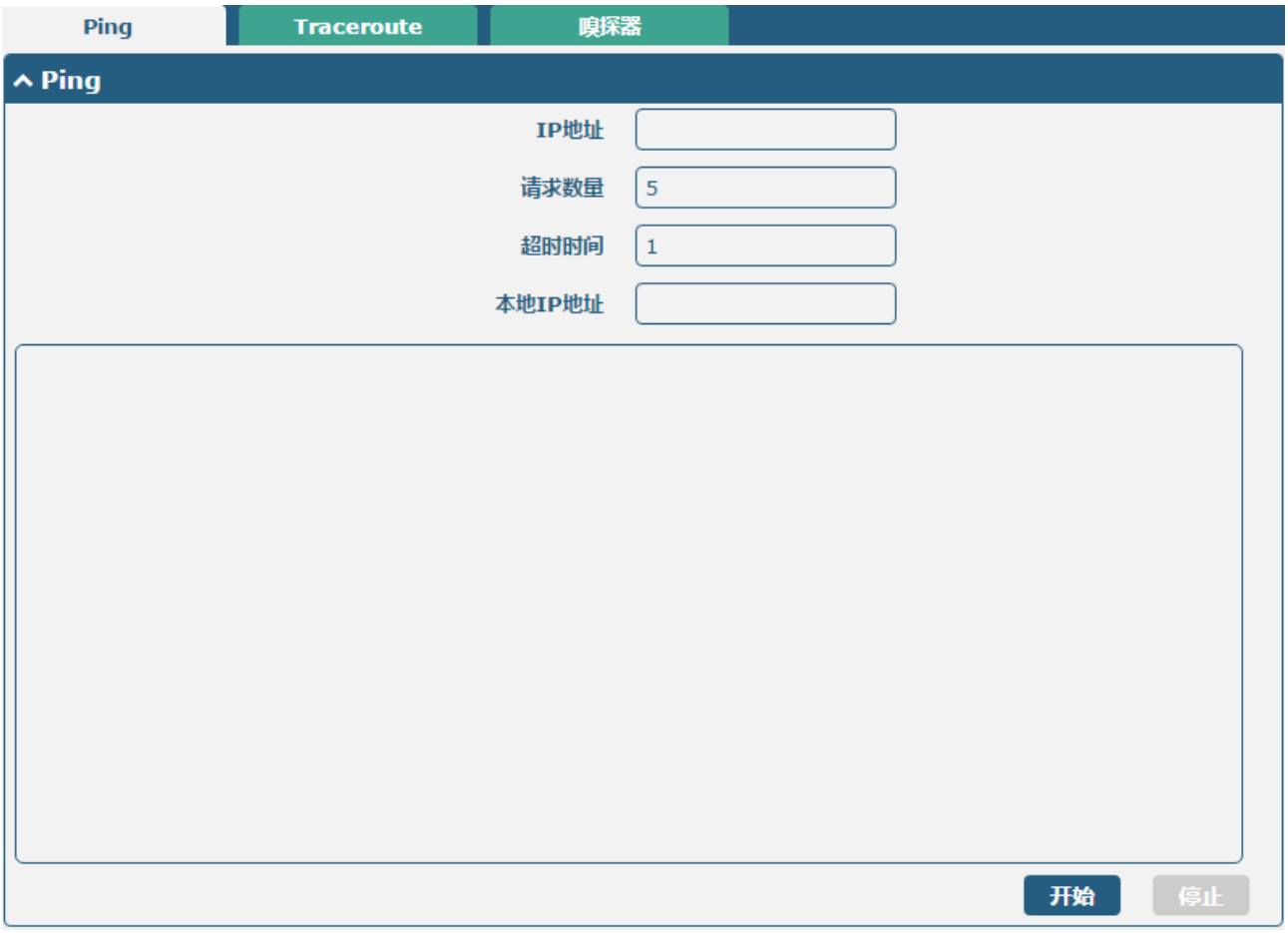
描述	显示应用程序的描述。

3.7.4 工具

用户可以在本节中使用三种工具：Ping、Traceroute 和嗅探器。Ping 工具用来检测本设备的网络连通性。

Ping

本节用于配置 Ping 检测工具。

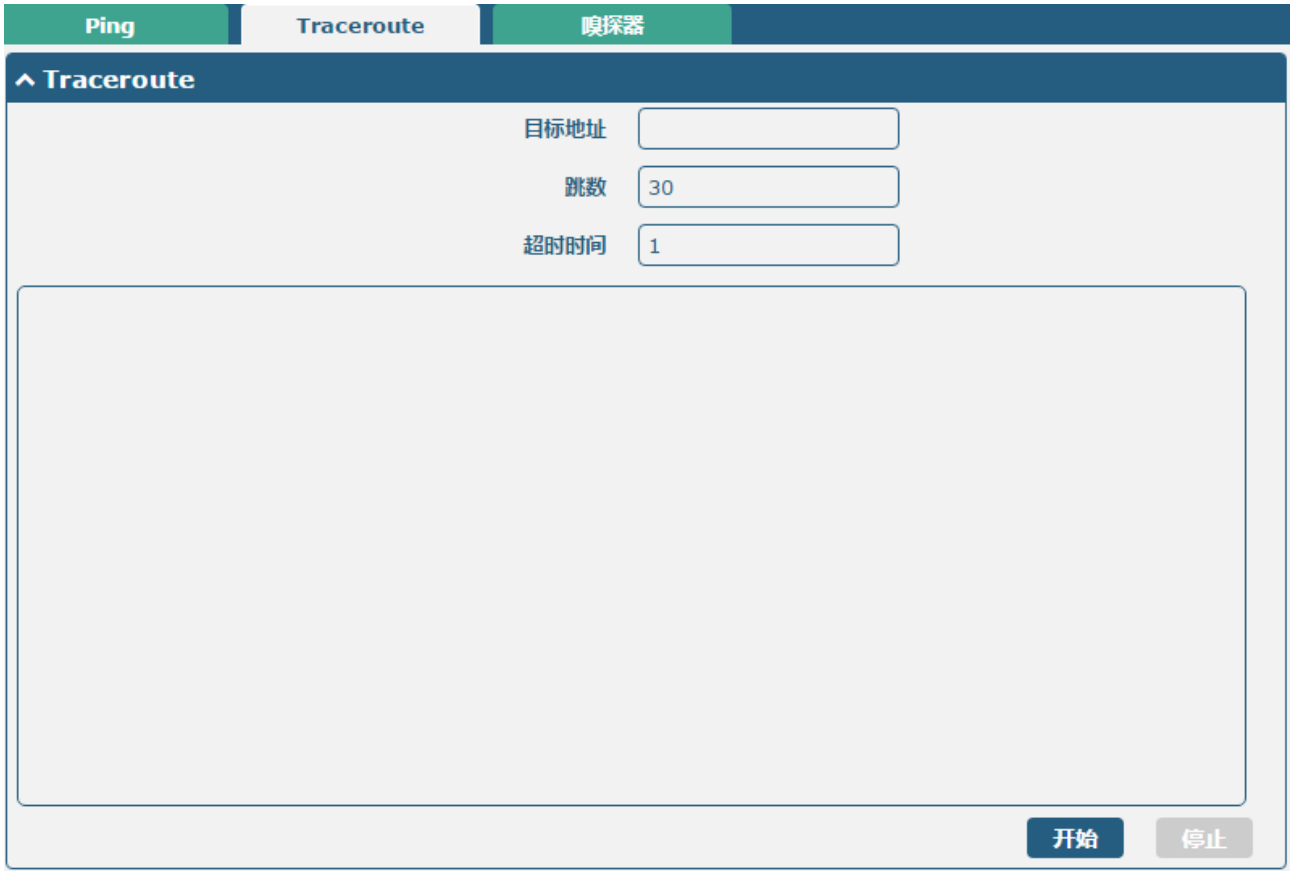


Ping		
项目	**说明**	**默认**
IP 地址	输入Ping的目的IP地址或域名。	空
请求数量	指定Ping请求次数。	5
超时时间	指定Ping请求超时时间。	1

本地 IP 地址	从移动广域网，以太广域网或以太局域网中指定本地IP。不填代表自动从这三者中选择。	空
开始	单击该按钮开始Ping请求，日志会在下面的文本框中显示。	--
停止	单击停止Ping操作。	--

Traceroute

本节用于配置 Traceroute 检测工具。



Traceroute		
选项	**说明**	**默认**
目标地址	输入跟踪的目的地址或域名。	空
跳数	指定最大的跟踪跳数。不管是否到达目的地，到达跳数最大值时，本设备会停止跟踪。	30
超时时间	指定追踪路由请求超时时间。	1
开始	单击该按钮开始跟踪路由请求，日志信息会在下面的文本框中显示。	--
停止	单击该按钮停止跟踪路由请求。	--

嗅探器

本节用于设置抓包工具。

嗅探器		
项目	**说明**	**默认**
接口	根据“以太网”配置选择接口。	All
主机地址	过滤包含指定IP地址的数据包。	空
抓包数量	设置抓包数量，取值范围从10到40000。	1000
协议	从“全部”，“IP”，“TCP”，“UDP”和“ARP”中选择。	全部
状态	显示嗅探器的当前状态。	--
开始	单击该按钮开始抓包。抓包文件会在窗口里显示，单击下载抓包文件，单击删除该抓包文件。	--
停止	单击此按钮以停止抓包。一旦单击停止按钮，一个新的日志文件将显示在下面清单中。	--
抓包文件	每次嗅探器的日志将会自动保存为新文件。您可以从“抓包文件”中找到这个文件，单击下载该日志，或单击删除该日志文件。它最多能缓存 5 个文件。	--

3.7.5参数文件

本节用于导入或导出配置文件，使本设备恢复出厂设置。

参数文件		
项目	**说明**	**默认**
导入配置文件		
将其他参数恢复到默认设置	单击为“ON”以将其他参数恢复到默认的设置。	OFF
忽略非法设置	单击为“ON”以忽略非法设置。	OFF
XML 配置文件	单击 **导入** 按钮从电脑上导入XML配置文件到本设备中。	--
导出配置文件		
忽略未启用的参数	单击为“ON”以忽略未启用的参数。	OFF
添加详细信息	单击为“ON”以添加详细信息。	OFF
XML 配置文件	单击 **生成** 以生成XML配置文件；单击 **导出** 以导出XML配置文件	--
出厂配置		
保存当前运行的参数为默认配置	单击 **保存** 按钮以保存当前运行的参数为默认配置。	--
出厂配置	单击 **恢复** 按钮以恢复出厂配置。	--

参数回滚

本节用于回滚设备参数。

参数回滚		
项目	**说明**	**默认**
回滚设置		
保存为回滚配置档案	手动创建一个可用于配置回滚的配置档案。如果系统参数被修改，系统会每天自动保存一个配置档案。	--
配置文件档案		
配置文件档案	查看相关配置文件档案的名字，大小和修改时间。	--

3.7.6 用户管理

本节用于修改或添加管理用户账户。一个本设备只有一个管理员用户帐号。

单击 以编辑管理员用户信息。

管理员设置		
项目	**说明**	**默认**
用户名	输入超级用户的新用户名。如果不修改用户名，请留空不填。5-32字符，有效字符: a-z, A-Z, 0-9, @, #, $, ., *, !, -。	空

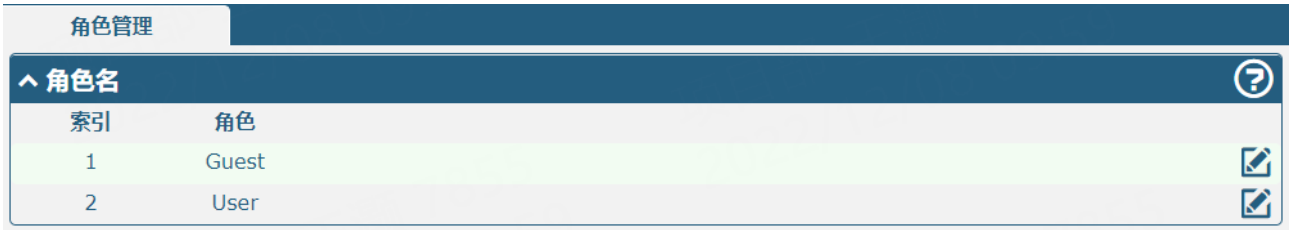
旧密码	输入超级用户旧密码。5-32字符，有效字符: a-z, A-Z, 0-9, @, #, $, ., *, !, -。	空
新密码	输入超级用户新密码。5-32字符，有效字符: a-z, A-Z, 0-9, @, #, $, ., *, !, -。	空
确认密码	再一次输入新密码以确认。	空

单击+以添加普通用户信息。

普通用户设置		
项目	**说明**	**默认**
索引	显示表序号。	
用户名	输入用户名。如果不修改用户名，请留空不填。5-32字符，有效字符: a-z, A-Z, 0-9, @, #, $, ., *, !, -。	空
角色	可以选择“User”或 “Guest”	User
密码	输入用户密码。5-32字符，有效字符: a-z, A-Z, 0-9, @, #, $, ., *, !, -。	空
确认密码	再一次输入密码以确认。	空

3.7.7 角色管理

本节用于管理用户角色，对不同角色的用户进行权限管理。



单击以编辑角色权限，显示如下图。


角色管理
设置
索引
1
角色
Guest
保存并运用,重启..
访问
接口
串口
访问
蜂窝网
访问
局域网
访问
链路管理
访问
USB
访问
以太网
访问
VPN
防火墙
访问
IP Passthrough
访问
路由
访问
网络
OpenVPN
访问
WireGuard
访问
GRE
访问
IPsec
访问

设置@角色管理	
项目	**说明**
无	该角色无法访问、编辑此选项。
访问	该角色能够访问，无法编辑此选项。
编辑	该角色能够访问、编辑此选项。

注：

1. 使用 Guest/User 角色账号登录时，“参数文件”功能不可用。
2. 当 Guest 角色权限“保存并应用，重启…”设置为访问时，以 Guest 角色账号登录将不会显示“保存并应用”、“重启”按钮。

第4章 配置示例

4.1 蜂窝网

4.1.1 蜂窝网拨号

本节将向用户展示如何配置本设备主备链路以及对本设备进行拨号。正确插入两张 SIM 卡并连接好本设备后，通过网页登陆本设备，并打开配置页面；单击**“接口 > 链路管理 > 链路管理 > 常规设置”**，选择“WWAN1”作为主链路，“WWAN2”作为备份链路，并设置“冷备份”为备份模式；再单击“提交；

注：*冷备份模式下，当 WWAN1 作为主链路时，所有数据会选择 WWAN1 来传输，而 WWAN2 会一直离线作为备份链路；当 WWAN1 断开时，数据会切换到 WWAN2 进行传输。*

单击 WWAN1 最右端的，并根据当前的 ISP 来设置 WWAN1 的参数。

配置完成后，单击**“提交 > 应用”**使配置生效。

单击“**界面>蜂窝>高级蜂窝设置**”，窗口显示如下：

单击 SIM1 最右端的，并根据应用要求来设置 SIM1 卡的参数。

配置完成后，单击“**提交 > 应用**”使配置生效。

4.1.2 短信远程控制

R2011支持手机短信远程控制。用户可以使用以下命令来查看本设备的状态，并且能够配置本设备的所有参数。

短信控制命令有三种模式，结构如下：

1. 密码模式—**用户名:密码; cmd1; cmd2; cmd3; … cmdn**（任何电话号码均有效）
2. 电话号码模式—**密码; cmd1; cmd2; cmd3; … cmdn**（发送到指定的电话号码才有效）
3. 密码加电话号码模式—**用户名:密码; cmd1; cmd2; cmd3; … cmdn**（发送到指定的电话号码才有效）

注：*所有命令符号必须在英文输入法半角模式下进行输入。*

短信命令的解释：

1. 密码：短信控制密码默认为超级用户的登录密码或者有读写权限的普通用户的登录密码。
2. **cmd1; cmd2; cmd3; … cmdn** 即跟 CLI 控制命令的格式一样。更多细节请参阅“5.1 CLI 介绍”。

注：*从本设备的配置页面下载XML配置文件，控制短信的格式也可以参考XML配置文件里的命令。*

单击**“系统 > 参数文件 > 导出配置文件”**，选择导出类型为“完整”，单击 生成 按钮以生成XML文件，再单击 导出 按钮以导出XML文件。

XML命令：

```
<lan>
<network max_entry_num="2">
<id>1</id>
<interface>lan0</interface>
<ip>172.16.24.24</ip>
<netmask>255.255.0.0</netmask>
<mtu>1500</mtu>
```

SMS命令：

set lan network 1 interface lan0

set lan network 1 ip 172.16.24.24

set lan network 1 netmask 255.255.0.0

set lan network 1 mtu 1500

3. 分号字符（“;”）用于分隔同一个短信里的多个命令。
4. 示例命令：

   密码模式—**admin:admin;status system**

此命令中用户名为admin，密码为admin，控制命令为status system，发此条短信到本设备则可以获取系统状态。

SMS接收到以下内容：

hardware_version = 1.1

firmware_version = 3.1.0

firmware_version_full = "3.1.0 (Rev 3199)"

kernel_version = 4.9.152

device_model = R1520

serial_number = ""

uptime = "0 days, 00:02:55"

system_time = "Thu May 14 05:51:56 2020 (NTP not updated)"

ram_usage = "75M Free/128M Total"

admin:admin;reboot

此命令中用户名为admin，密码为admin，控制命令为reboot。发送此短信到本设备可以重启本设备。

SMS接收到以下内容：

OK

admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet_access false

此命令中用户名为admin，密码为admin，控制命令为set firewall remote_ssh_access false;set firewall remote_telnet_access false。发送此短信到本设备可以关闭防火墙远程SSH登录和远程Telnet访问功能。

SMS接收到以下内容：

OK

OK

admin:admin; set lan network 1 interface lan0;set lan network 1 ip 172.16.24.24;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500

此命令中用户名为admin，密码为admin，控制命令为set lan network 1 interface lan0;set lan network 1 ip 172.16.24.24;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500。发送此短信到本设备配置LAN口。

SMS接收到以下内容：

OK

OK

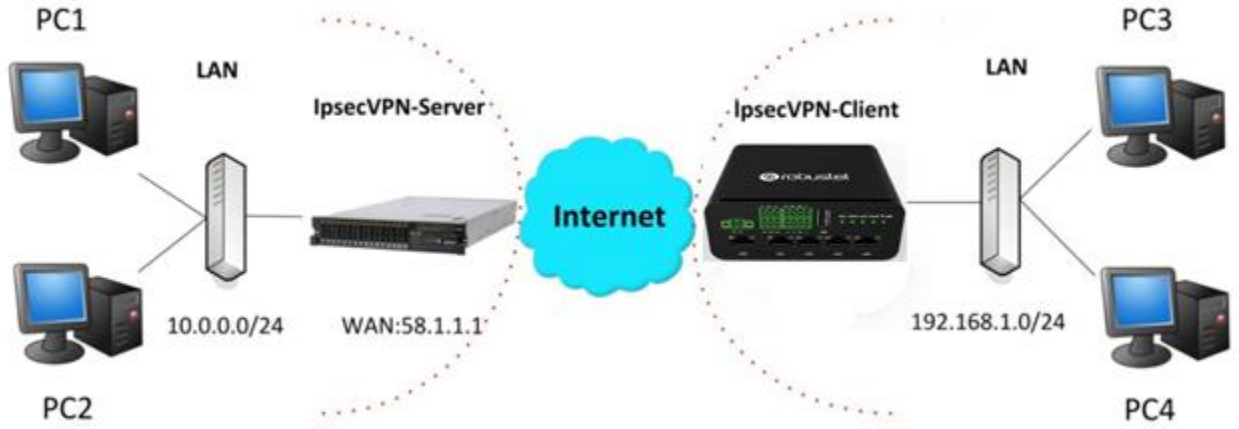
OK

OK

4.2 VPN 配置示例

4.2.1 IPsec VPN

IPsec VPN 示例拓扑（服务器端与客户端的 IKE 与 SA 参数配置必须一致）：



IPsecVPN_Server 配置

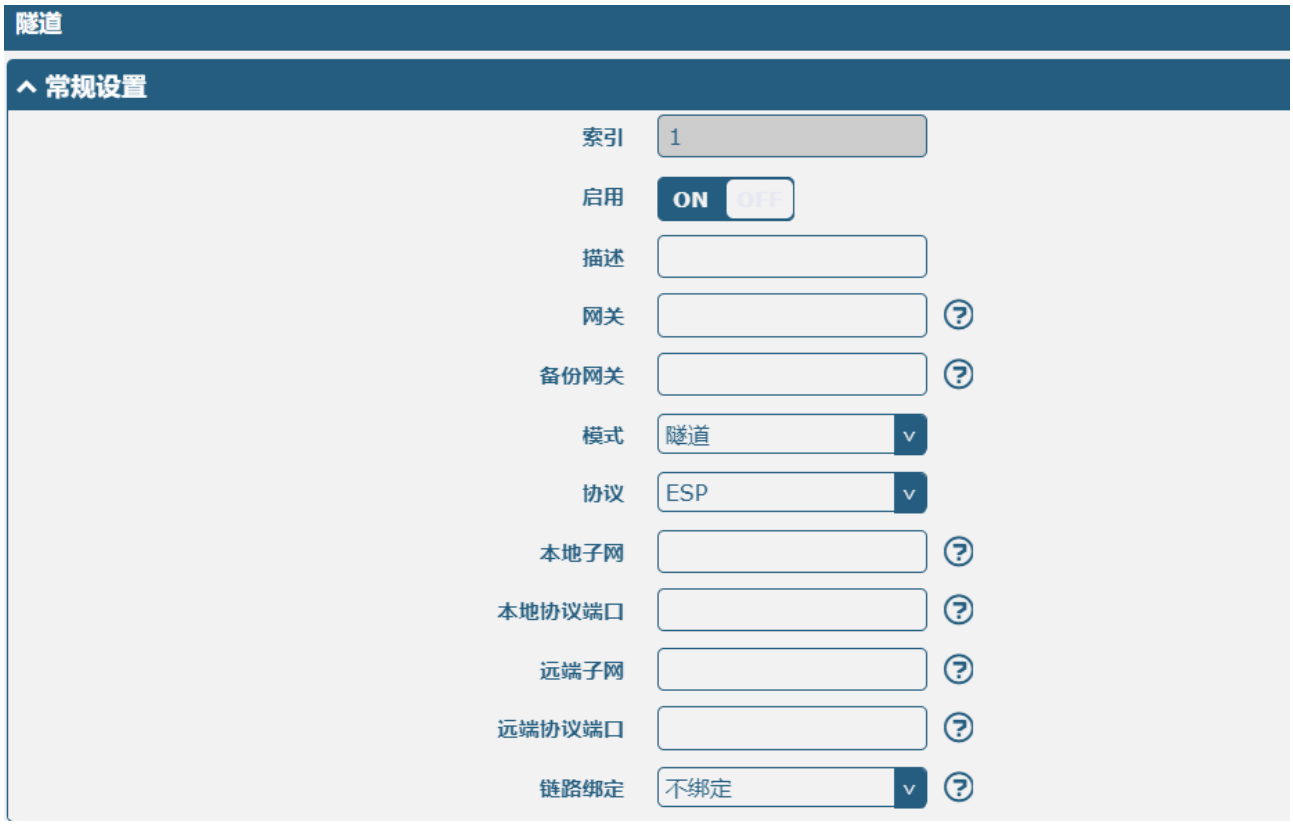
Cisco 2811：

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0


Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac


Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit

Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit



Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

IPsecVPN_Client 配置

单击“虚拟专用网 > IPsec > 隧道”，窗口如下所示：

单击+，并参照下图的配置完成 IPsec Client 的参数配置。



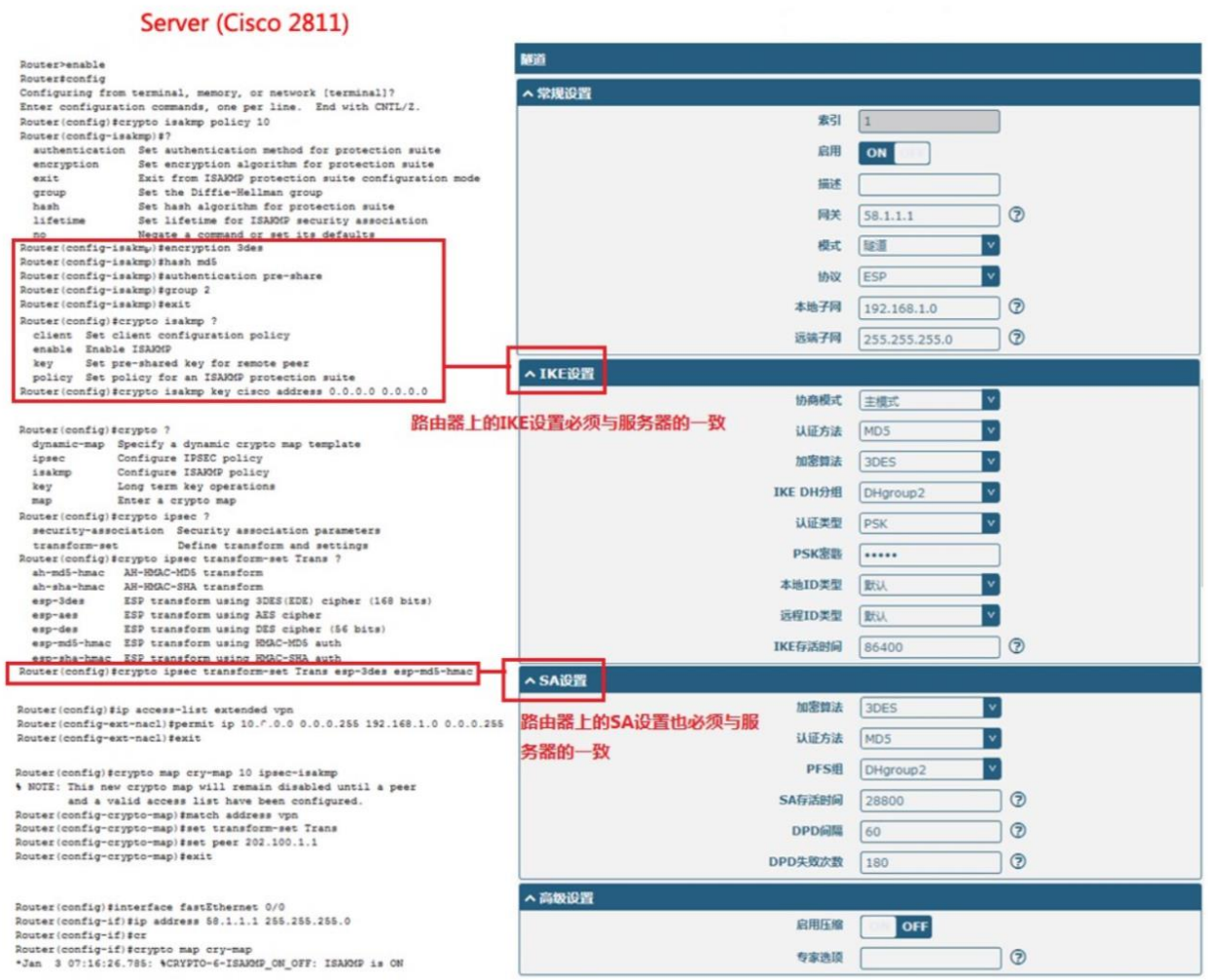
配置完成后，单击*“提交 > 应用”*使配置生效。

IPsecVPN_Server:

IPsec Server 与 Client 之间的配置对比如下图所示：

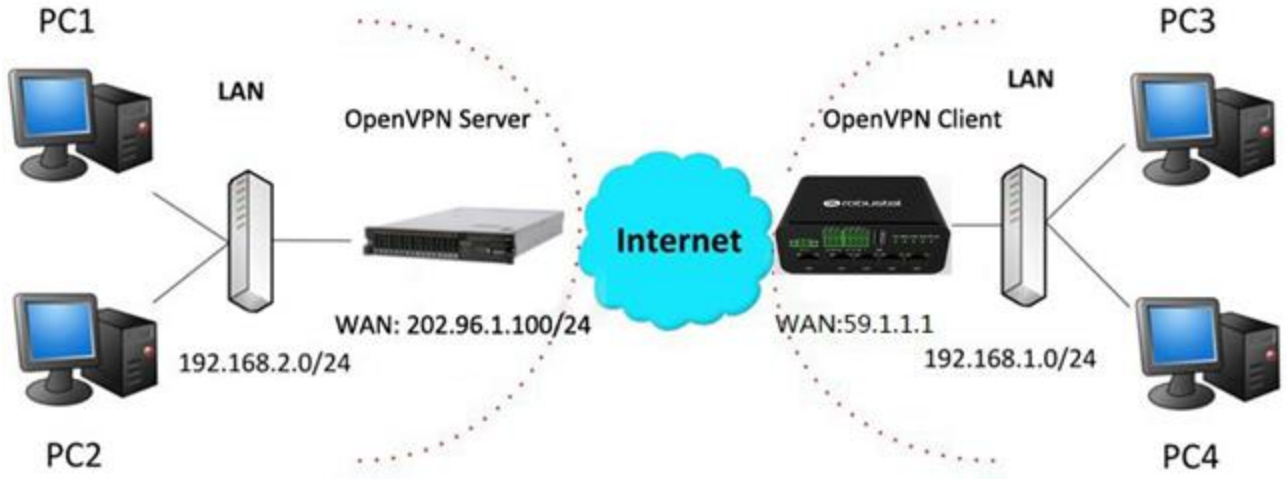
Cisco 2811:

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0


Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac


Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit

Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit


Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```


Server (Cisco 2811)
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
authentication Set authentication method for protection suite
encryption Set encryption algorithm for protection suite
exit Exit from ISAKMP protection suite configuration mode
group Set the Diffie-Hellman group
hash Set hash algorithm for protection suite
lifetime Set lifetime for ISAKMP security association
no Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
client Set client configuration policy
enable Enable ISAKMP
key Set pre-shared key for remote peer
policy Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
Router(config)#crypto ?
dynamic-map Specify a dynamic crypto map template
ipsec Configure IPSEC policy
isakmp Configure ISAKMP policy
key Long term key operations
map Enter a crypto map
Router(config)#crypto ipsec ?
security-association Security association parameters
transform-set Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
ah-md5-hmac AH-HMAC-MD5 transform
ah-sha-hmac AH-HMAC-SHA transform
esp-3des ESP transform using 3DES(EDE) cipher (168 bits)
esp-aes ESP transform using AES cipher
esp-des ESP transform using DES cipher (56 bits)
esp-md5-hmac ESP transform using HMAC-MD5 auth
esp-sha-hmac ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac
Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
路由器上的IKE设置必须与服务器的一致
路由器上的SA设置也必须与服务器的一致
常规设置
索引
1
启用
ON
描述
网关
58.1.1.1
模式
隧道
协议
ESP
本地子网
192.168.1.0
远端子网
255.255.255.0
IKE设置
协商模式
主模式
认证方法
MD5
加密算法
3DES
IKE DH分组
DHgroup2
认证类型
PSK
PSK密钥
本地ID类型
默认
远程ID类型
默认
IKE存活时间
86400
SA设置
加密算法
3DES
认证方法
MD5
PFS组
DHgroup2
SA存活时间
28800
DPD间隔
60
DPD失效次数
180
高级设置
启用压缩
OFF
专家选项

4.2.2 OpenVPN

OpenVPN 可支持客户端和 P2P（点对点）两种模式，此处以客户端为例。示例拓扑如下图所示：



OpenVPN_Server 配置

先在服务端生成 OpenVPN 相关证书，参考以下命令配置 Server:

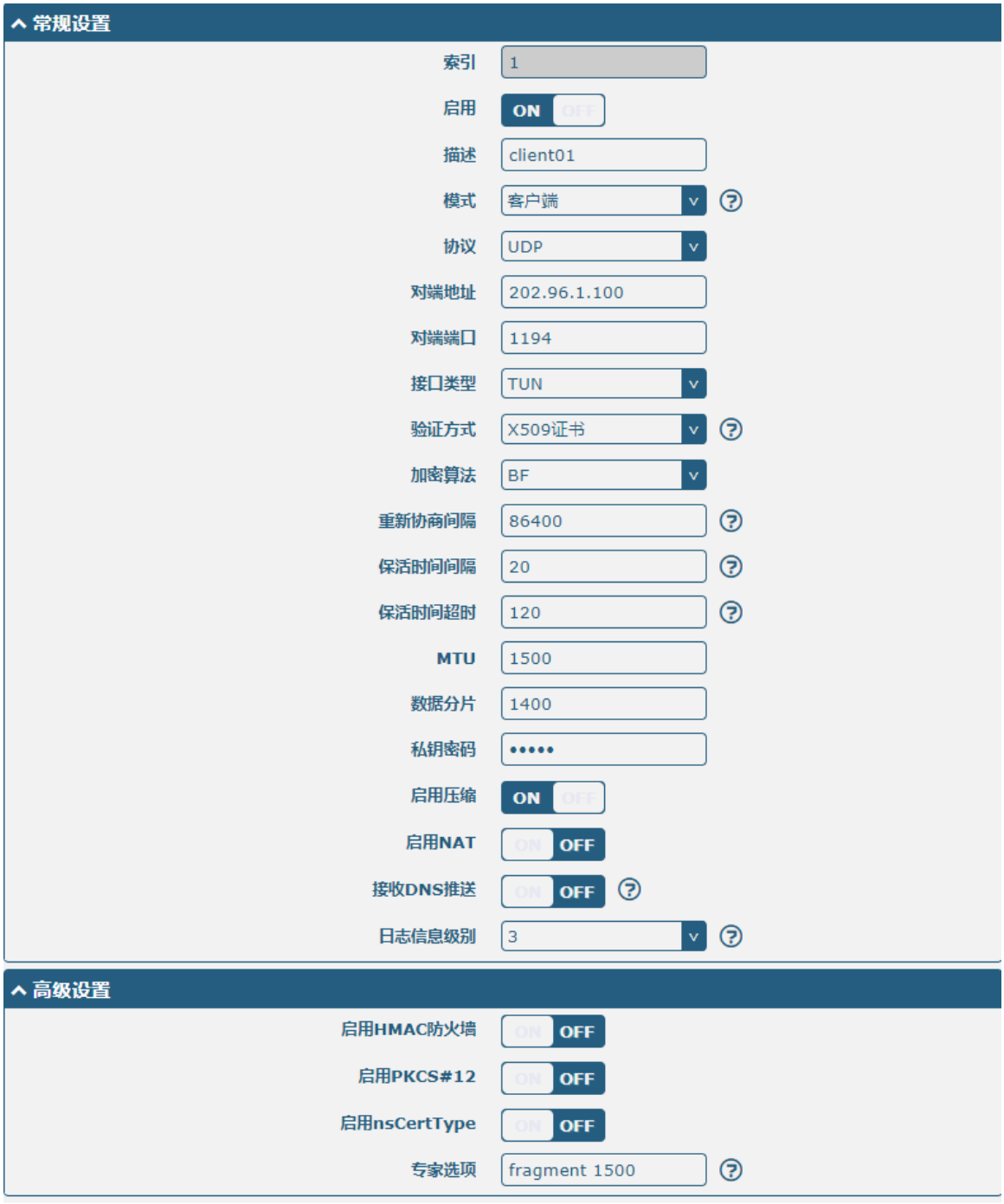
```
local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verB 3
```

注：*如需了解更多配置细节，请联系我司的技术支持工程师。*

OpenVPN_Client 配置

单击“**虚拟专用网 > OpenVPN > OpenVPN**”，窗口如下所示：

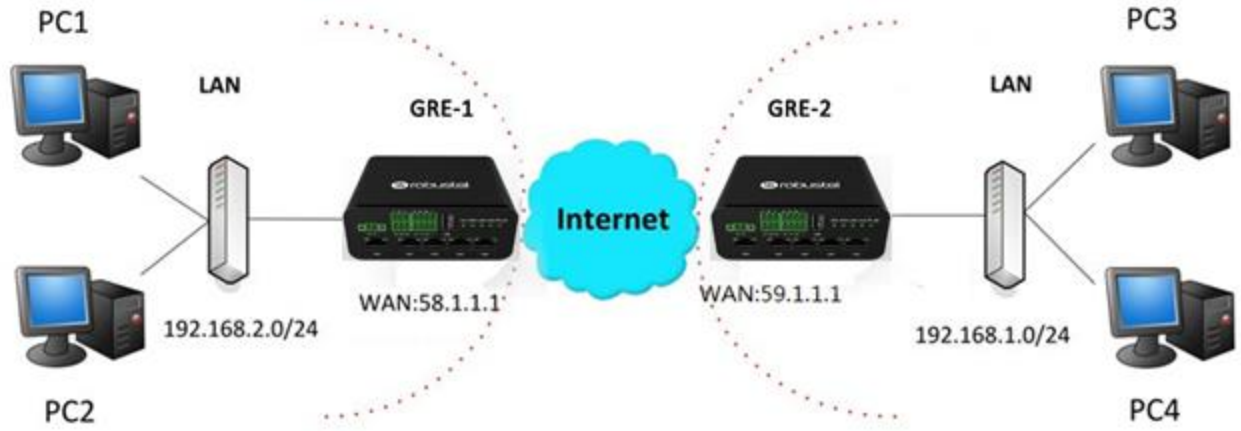
单击+，并参照下图的配置完成 Client01 的配置。



配置完成后，单击“**提交 > 应用**”使配置生效。

4.2.3 GRE VPN

GRE VPN 示例拓扑：



GRE-1 配置

单击“**虚拟专用网 > GRE > GRE**”，窗口如下所示：

单击+，并参照下图配置完成对 GRE-1 的配置。

配置完成后，单击“**提交 > 应用**”使配置生效。

GRE-2 配置

单击➕，并参照下图配置完成对 GRE-2 的配置。

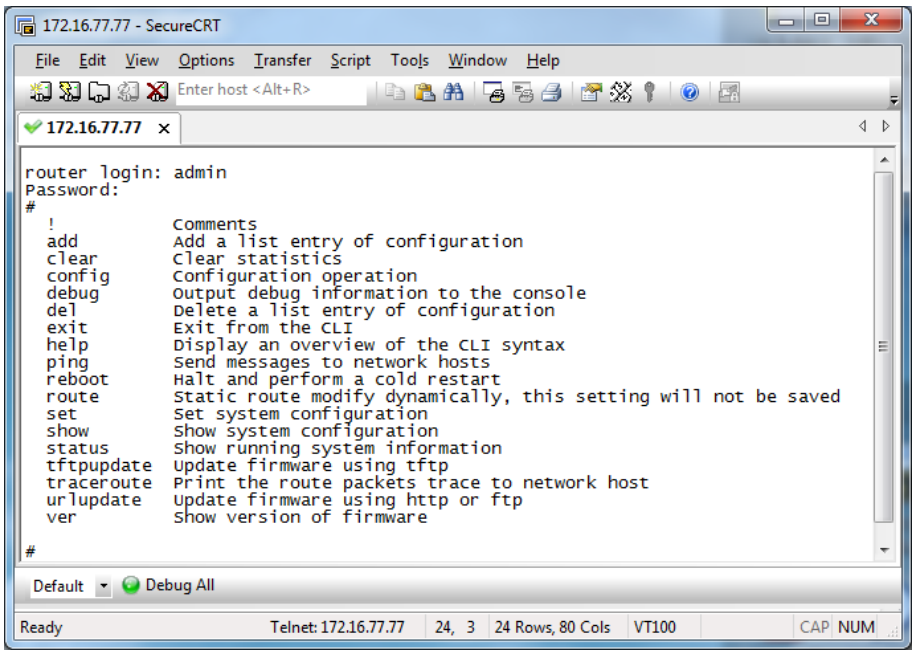
配置完成后，单击**“提交 > 应用”**使配置生效。

GRE-1 与 GRE-2 之间的配置对比如下图：

第5章 CLI 命令介绍

5.1 CLI 介绍

命令行接口（CLI）是一组软件界面，它提供另一种配置设备参数的方式。用户可以通过 SSH 或 telnet 来连接本设备，从而对其进行 CLI 命令配置。与本设备建立 Telnet 或者 SSH 连接后，输入登录账号和密码（默认 admin/admin），进入本设备的配置模式，如下图。



登录本设备：

Router login: admin

Password: admin

#

CLI命令：

#？（“?”问号不会显示出来）

!	Comments
add	Add a list entry of configuration
add_preferred	smart roaming add preferred plmn list
clear	Clear statistics
config	Configuration operation
debug	Output debug information to the console
del	Delete a list entry of configuration
delete_preferred	smart roaming remove all preferred operators
do	Set the level state of the do

exit	Exit from the CLI
force_rescan	smart roaming network rescan
forget_rplmn	smart roaming forget rplmn
help	Display an overview of the CLI syntax
ipsec_cert_get	Download IPSec certificate file via http or ftp
ovpn_cert_get	Download OpenVPN certificate file via http or ftp
ping	Send messages to network hosts
reboot	Halt and perform a cold restart
saveConfig	Save Running Configuration as Default
select	smart roaming select operator
set	Set system configuration
show	Show system configuration
show_networks	show networks that scanf
speedtest	speedtest
status	Show running system information
tftp_upload_diagnostic	Generate diagnostic files and upload them using TFTP
tftpupdate	Update firmware or configuration file using tftp
traceroute	Print the route packets trace to network host
trigger	Trigger action
uninstall	Uninstall App
UploadConfig	Upload Current UCI Config to FTP Server
urlupdate	Update firmware via http or ftp
ver	Show version of firmware

5.2 命令帮助

下面列表是查看帮助信息命令和配置过程中遇到的错误命令的描述。

命令/指示	描述
?	输入一个问号“?”会出现帮助信息。 例： # config（按‘?’） config Configuration operation # config（按空格键+’?’） commit Save the configuration changes and take effect changed configuration save_and_apply Save the configuration changes and take effect changed configuration loaddefault Restore Factory Configuration

Ctrl+c	同时按住这两个键，除了可以用来“复制”，还可以用于中断并强迫退出的当前设置。
Syntax error: The command is not completed	当前命令不完整。
敲空格键+Tab 键	帮助您完成当前未完整的命令。 例： # config（按 Enter 键） Syntax error: The command is not completed # config（按空格键+Tab 键） commit save_and_apply loaddefault
#config commit # config save_and_apply	当完成所有的配置，必须要输入这两条命令令配置生效 ***注：committ 和 save_and_apply 作用一样***

5.3 常用命令

命令	命令语法	描述
Debug	Debug *parameters*	开启或关闭 debug 功能。
Show	Show *parameters*	查看每个功能的当前配置。
Set	Set *parameters*	所有功能的参数都是由命令“set”和“add”设置的，不同的是“set”是针对单个参数的，而“add”是用在参数列表里的。
Add	Add *parameters*	

注：更多关于 CLI 的命令，请参考 CLI 指导手册。

5.4 CLI 配置示例

最好和最快掌握 CLI 配置的方法是首先网页登录本设备查看其所有的功能，然后阅读所有 CLI 命令，最后参考一些例子来学习配置。

示例 1：查看当前版本

```
# status system
hardware_version = 1.1
firmware_version =3.1.0
firmware_version_full = "3.1.0 (Rev 3199)"
kernel_version = 4.9.152
device_model = R1520
serial_number = ""
uptime = "0 days, 00:06:51"
system_time = "Thu May 14 05:55:52 2020 (NTP not updated)"
ram_usage = "74M Free/128M Total"
```

示例 2：用 tftp 更新固件

```
# tftpupdate （space+?）
  firmware    New firmware
# tftpupdate firmware （space+?）
  String    Firmware name
# tftpupdate firmware r1520-firmware-3.1.0.ruf host 192.168.100.99 //输入新固件的名字
  Downloading
r1520-firmware-s 100% |*******************************|   5018k   0：00：00 ETA
Flashing
Checking 100%
Decrypting 100%
Flashing 100%
Verifying 100%
Verfify Success
upgrade success                                    //更新成功
# config save_and_apply
OK                                                 //应用后，配置生效
```

示例 3：设置链路管理

```
# set
# set (space+?)
   cellular             Cellular
   ddns                  DDNS
   dido                  DIDO
   email                 Email
   ethernet              Ethernet
   event                 Event Management
   firewall             Firewall
   gre                    GRE
   ip_passthrough        IP Passthrough
   ipsec                 IPSec
   lan                    Local Area Network
   link_manager           Link Manager
   ntp                    NTP
   openvpn               OpenVPN
   reboot                Automatic Reboot
   route                 Route
   serial_port            Serial
   sms                   SMS
   ssh                   SSH
   syslog                 Syslog
   system                 System
   user_management    User Management
```

```
   web_server            Web Server

# set link_management
   primary_link          Primary Link
   Backup_link           Backup Link
   Backup_mode           BackSup Mode
   emergency_reBoot      Emergency ReBoot
   link                  Link Settings
# set link_management primary_link（space+?）
Enum    Primary Link （wwan1/wwan2/wan/wlan）
# set link_management primary_link wwan1                    //选择“wwan1”作为主链路
OK                                                          //设置成功
set link_manager link 1
   type                  Type
   desc                  Description
   connection_type       Connection Type
   wwan                  WWAN Settings
   static_addr           Static Address Settings
   pppoe                 PPPoE Settings
   ping                  Ping Settings
   nat_enable            NAT Enable
   mtu                   MTU
   weight                Weight
   upload_bandwidth          Upload Bandwidth
   download_bandwidth        Download Bandwidth
   dns1_overrided            Overrided Primary DNS
   dns2_overrided            Overrided Secondary DNS
   debug_enable              Debug Enable
   verbose_debug_enable      Verbose Debug Enable

# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
   auto_apn                  Automatic APN Selection
   apn                       APN
   username                  Username
   password                  Password
   dialup_numBer             Dialup NumBer
   auth_type                 Authentication Type
   data_allowance            Data Allowance
   Billing_day               Billing Day
# set link_manager link 1 wwan switch_By_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100           //通过数据流量打开蜂窝网开关
```

```
OK                                                          //设置成功
# set link_manager link 1 wwan Billing_day 1                //设置每月指定的计费日
OK                                                          //设置成功
…
# config save_and_apply
OK                                          //保存并应用当前的配置，使更改生效
```

示例 4：设置以太网

```
# set Ethernet port_setting 2 port_assignment lan0          //设置表2（eth1）为lan0
OK
# config save_and_apply                                     //使配置生效
OK
```

示例 5：设置局域网 IP 地址

```
# show lan all
network {
        id = 1
        interface = lan0
        ip = 192.168.0.1
        netmask = 255.255.255.0
        mtu = 1500
        dhcp {
                180umber = true
                mode = server
                relay_server = “”
                pool_start = 192.168.0.2
                pool_end = 192.168.0.100
                netmask = 255.255.255.0
                router = “”
                primary_dns = “”
                secondary_dns = “”
                wins_server = “”
                lease_time = 120
                expert_options = “”
                debug_enable = false
    }
        vlan_id = 0
}
#
# set lan（space+?）
    network             Network Settings
    multi_ip      Multiple IP Address Settings
# set lan network 1(space+?)
```

```
   interface    Interface
   ip           IP Address
   netmask      Netmask
   mtu          MTU
   dhcp         DHCP Settings
   Vlan_id      VLAN ID
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.24.24                    //为局域网配置 IP 地址
OK                                                     //设置成功
# set lan network 1 netmask 255.255.0.0
OK
#
…
# config save_and_apply
OK                                                     //保存并应用当前的配置，使更改生效
```

示例 6：设置蜂窝网

```
# show cellular all
sim {
        id = 1
        card = sim1
        phone_number = ""
        pin_code = ""
        extra_at_cmd = ""
        telnet_port = 0
        network_type = auto
        band_select_type = all
        band_settings {
                gsm_850 = false
                gsm_900 = false
                gsm_1800 = false
                gsm_1900 = false
                wcdma_800 = false
                wcdma_850 = false
                wcdma_900 = false
                wcdma_1900 = false
                wcdma_2100 = false
                wcdma_1700 = false
                wcdma_band19 = false
                lte_band1 = false
                lte_band2 = false
                lte_band3 = false
                lte_band4 = false
```

```
            lte_band5 = false
            lte_band7 = false
            lte_band8 = false
            lte_band13 = false
            lte_band17 = false
            lte_band18 = false
            lte_band19 = false
            lte_band20 = false
            lte_band21 = false
            lte_band25 = false
            lte_band28 = false
            lte_band31 = false
            lte_band38 = false
            lte_band39 = false
            lte_band40 = false
            lte_band41 = false
        }
        telit_band_settings {
            gsm_band = 900_and_1800
            wcdma_band = 1900
        }
        debug_enable = true
        verbose_debug_enable = false
}
# set(space+space)
cellular            ddns                dido                email               ethernet
event               firewall            gre                 ip_passthrough      ipsec
l2tp                lan                 link_manager        ntp                 openvpn
pptp                reboot              route               serial_port         sms
ssh                 syslog              system              user_management     web_server
# set cellular(space+?)
  sim    SIM Settings
# set cellular sim(space+?)
  Integer    Index (1..1)
}
# set cellular sim 1(space+?)
    card                        SIM Card
    phone_number                Phone Number
    pin_code                    PIN Code
    extra_at_cmd                Extra AT Cmd
    telnet_port                 Telnet Port
    network_type                Network Type
    band_select_type            Band Select Type
    band_settings               Band Settings
    telit_band_settings         Band Settings
```

```
    debug_enable                Debug Enable
    verbose_debug_enable        Verbose Debug Enable
# set cellular sim 1 phone_number 18620435279
OK
…
# config save_and_apply
OK                                          // 保存并应用当前的配置，使更改生效
…
```

术语表

缩写	解释参照
AC	Alternating Current
APN	Access Point Name of GPRS Service Provider Network
ASCII	American Standard Code for Information Interchange
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface for Batch scripting
CSD	Circuit Switched Data
CTS	Clear to Send
dB	DeciBel
dBi	DeciBel Relative to an Isotropic radiator
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DCS 1800	Digital Cellular System, also referred to as PCN
DI	Digital Input
DO	Digital Output
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready
EDGE	Enhanced Data rates for GloBal Evolution of GSM and IS-136
EMC	Electromagnetic CompatiBility
EMI	Electro-Magnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
EVDO	European Telecommunications Standards Institute
FDD LTE	Frequency Division Duplexing Long Term Evolution
GND	Ground
GPRS	General Packet Radio Service
GRE	generic route encapsulation
GSM	GloBal System for MoBile Communications
HSPA	High Speed Packet Access
ID	identification data
IMEI	International MoBile Equipment Identification
IP	Internet Protocol
IPsec	Internet Protocol Security
kBps	kBits per second

L2TP	Layer 2 Tunneling Protocol
LAN	local area network
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	Subscriber identification module
SMA antenna	Stubby antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct Current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

广州鲁邦通物联网科技股份有限公司

Guangzhou Robustel Co., Ltd.

地址：广州市黄埔区永安大道 63 号 2 栋 501

热线：+86-4009-873-791

邮箱：info@robustel.com

网址：www.robustel.com.cn