



软件说明书

RobustOS Pro 软件说明书





广州鲁邦通物联网科技有限股份公司

www.robustel.com.cn

版权所有©2022 广州鲁邦通物联网科技股份有限公司
保留一切权利。

商标许可

 &  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

未经版权所有者允许，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



目录

第一章 产品概述.....	6
第二章 网页配置前准备.....	7
2.1 配置计算机.....	7
2.2 出厂默认设置.....	11
2.3 登录 WEB 配置页面.....	11
2.4 控制面板.....	12
第三章 网页 UI 说明.....	14
3.1 系统状态.....	14
3.1.1 总览.....	14
3.1.2 蜂窝网.....	14
3.1.3 以太网.....	15
3.1.4 互联网状态.....	15
3.1.5 局域网状态.....	15
3.1.6 系统资源.....	16
3.1.7 系统信息.....	16
3.1.8 模块状态.....	16
3.2 网络.....	17
3.2.1 广域网.....	17
3.2.2 局域网.....	21
3.2.3 路由.....	24
3.2.4 策略路由.....	25
3.2.5 防火墙.....	27
3.2.6 QoS.....	33
3.3 接口.....	37
3.3.1 以太网.....	37
3.3.2 蜂窝网络.....	38
3.3.3 网桥.....	43
3.3.4 Wi-Fi.....	44
3.3.5 USB.....	53
3.3.6 VLAN.....	54
3.3.7 DI/DO.....	55
3.3.8 串口.....	59
3.3.9 Packet Forwarder (LG5100 支持).....	64
3.3.10 LoRaWAN 基站 (LG5100 支持).....	69
3.4 虚拟专用网.....	71
3.4.1 IPsec.....	71
3.4.2 OpenVPN.....	78
3.4.3 GRE.....	86
3.4.4 PPTP.....	88
3.4.5 L2TP.....	92
3.5 服务.....	96
3.5.1 系统日志.....	96
3.5.2 事件.....	98
3.5.3 NTP.....	103

3.5.4	短信	104
3.5.5	Email	106
3.5.6	DDNS	107
3.5.7	VRRP	109
3.5.8	SSH	110
3.5.9	GPS	110
3.5.10	SNMP	114
3.5.11	Web 服务器	118
3.5.12	高级	118
3.6	系统	120
3.6.1	调试	120
3.6.2	证书管理器	122
3.6.3	资源图	125
3.6.4	应用中心	127
3.6.5	工具	128
3.6.6	参数文件	131
3.6.7	用户管理	133
3.6.8	DEB 管理	134
第四章	配置示例	135
4.1	Cellular 蜂窝网	135
4.1.1	蜂窝 APN 手动设置和蜂窝拨号	135
4.1.2	短信远程控制	138
4.2	VPN 配置示例	140
4.2.1	IPsec VPN	140
4.2.2	OpenVPN	144
4.2.3	GRE VPN	146
第五章	CLI 简介	149
5.1	什么是 CLI	149
5.2	如何配置 CLI	150
5.3	常用命令	150
5.4	配置示例	151
	术语表	154

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	固件版本	文档版本	详细说明
2022 年 7 月 7 日	2.0.0	1.0.0	首次编写。

第一章 产品概述

本用户手册适用于所有基于 RobustOS Pro 的网关产品，提供了网关产品网页端的配置及操作说明。因为不同产品的硬件配置或接口有所不同，相应的配置及操作说明请参考特定章节。

相关产品	EG5100	LG5100	EG5120															
SIM 卡槽	2	2	2															
以太网口	2	2	2															
PoE-PD	-	*	-															
Wi-Fi	*	-	*															
蓝牙	*	-	*															
GNSS	*	*	*															
DI/DO	4	4	4															
AI	-	-	-															
RS-232	√	√	√															
RS-485	√	√	√															
USB	√	√	√															

注：√ = 支持，- = 不支持，* = 可选

关于 RobustOS Pro

RobustOS Pro由鲁邦通自主开发的边缘网关系统。本系统基于标准的Debian 11（bullseye）版本，具有增强的网络安全特性，支持高级GUI和Docker容器，并支持C、C++、Java、Python、Node.js等编程语言，便于用户在系统上自主开发及部署其应用程序。另外用户同时可以在鲁邦通的RCMS网关云管理平台上下载最新的通用APP，也可以下载Debian生态应用APP，充分满足碎片化的物联网应用需求。


第二章 网页配置前准备

网关支持网页配置，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。连接网关的方式有多种，既可通过外部中继器/集线器连接，也可以直接连接到电脑。网关直接连接到电脑的以太网口时，如果网关作为 DHCP 服务器，那么电脑可以直接从网关获取 IP；电脑也可以设置和网关同在一网段的静态 IP，这样电脑与网关就构成了一个小型的局域网。电脑与网关已成功建立连接后，在电脑浏览器上输入设备的默认登录地址，即可进入网关的 Web 登录界面。

2.1 配置计算机

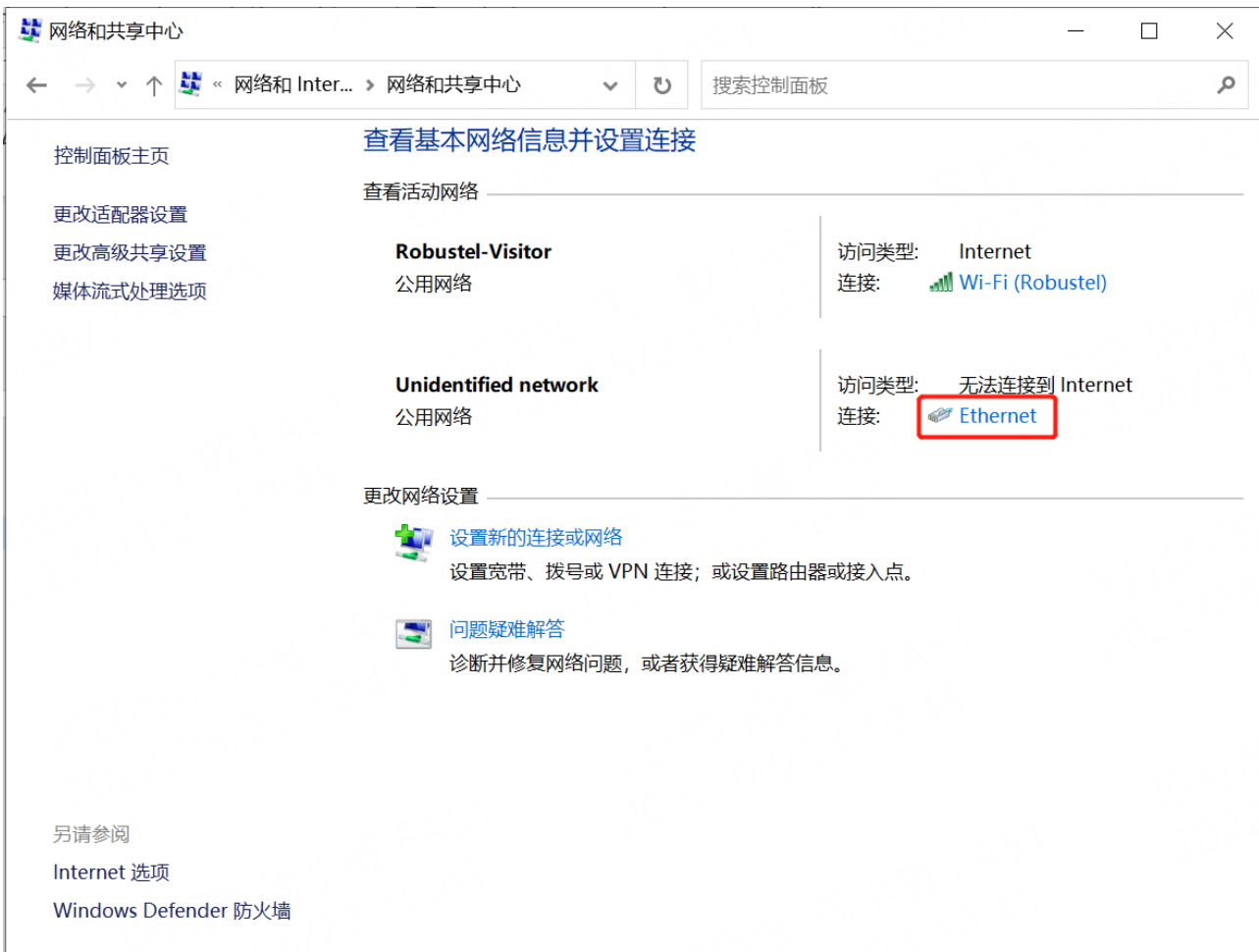
在 PC 端，有两种方法配置其 IP 地址：一是在 PC 端的本地连接上开启自动获取 IP 地址，二是在 PC 端的本地连接上配置一个跟网关在同一个子网的静态 IP 地址。

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配置一个跟网关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。

选项	描述
用户名	admin
密码	请参阅产品标签
ETH 0	WAN 模式 或 192.168.0.1/255.255.255.0, LAN 模式
ETH 1/2 (*)	192.168.0.1/255.255.255.0, LAN 模式
DHCP 服务器	开启

* 注：不同型号的以太网口数量可能存在差异，具体数量请参阅对应型号的产品规格书。

2.3 登录 WEB 配置页面

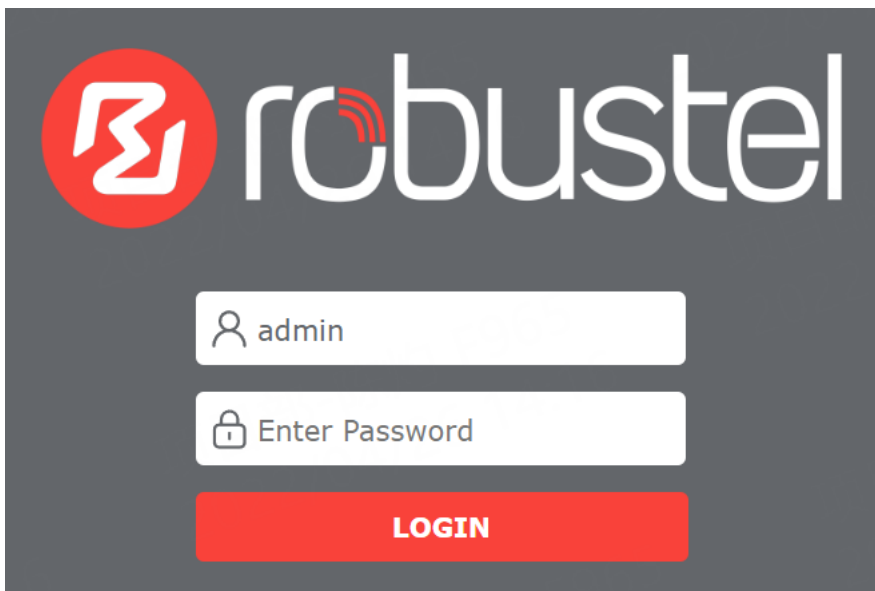
要登录管理页面并查看设备的配置状态，请按照以下步骤操作。

1. 在 PC 上，打开浏览器，如 IE、谷歌等；
2. 在 Web 浏览器中，在地址栏中键入设备的 IP 地址，然后按 Enter 键。设备的默认 IP 地址 <http://192.168.0.1/>，但实际地址可能会有所不同。

注：如果在设备中插入了具有公网 IP 地址的 SIM 卡，请在浏览器的地址栏中输入此相应的公网 IP 地址，即可无线访问设备。

3. 在登录页面，输入用户名和密码，然后单击“登录”。在产品阅读标签上查看默认用户名和密码。

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。








2.4 控制面板




登录后，将显示产品 Web 管理界面的主页，这里以 EG5120 为例。



在首页，用户可以浏览产品具体信息，并可以执行保存配置、重启设备、注销等操作。

选项	描述	标志
保存&生效	默认情况下，该图标为灰色，如果对配置进行任何修改，将变为红色，然后单击该按钮，使提交的所有配置更改生效。	 or 
重启应用	单击以重新启动所有应用程序，然后切换到登录页面。	
重启设备	单击以重新启动网关，然后切换到登录页面。	
注销	单击此项可安全注销当前用户。注销后，它将切换到登录页面。直接关闭网页而不注销，下一位用户在超时之前无需密码即可在此浏览器上登录网页。	

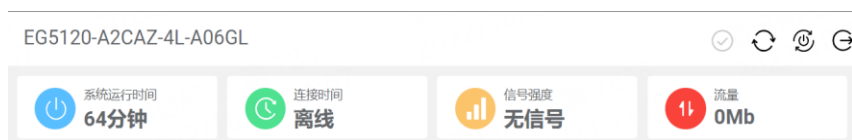
注意：修改配置的步骤如下：

1. 在一个页面中修改
2. 点击 
3. 在另一页修改
4. 点击 
5. 完成所有修改
6. 点击  保存修改及使其生效

第三章 网页 UI 说明

3.1 系统状态

3.1.1 总览



选项	描述
系统运行时间	显示网关当前已通电的时间。
连接时间	显示网关当前已连接到互联网的时间。
信号强度	显示当前信号强度。
流量	显示数据流量使用量。

3.1.2 蜂窝网

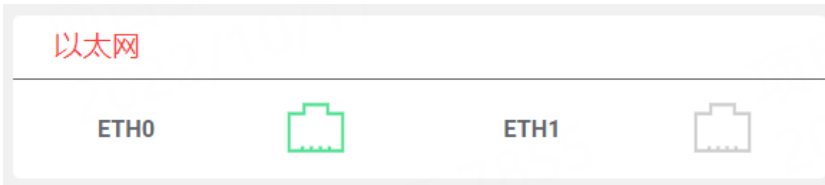
此页面显示 SIM 卡的状态。





选项	描述
	未连接。
	信号弱。
	信号良好。
	信号强。

3.1.3 以太网

此页面显示网关的以太网状态



图标	说明
	未连接。
	已连接，在工作状态下。

3.1.4 互联网状态

此页面显示网关的互联网状态信息。

互联网状态	
活动连接	wwan
IP地址	10.239.215.92
网关	10.239.215.93
DNS	120.80.80.80 221.5.88.88

选项	描述
活动链接	显示当前联机链接：WWAN1、WWAN2 或 WAN。
IP 地址	显示当前链接的地址。
网关	显示当前链路的网关地址。
DNS	显示当前 DNS 服务器。

3.1.5 局域网状态

此页面显示网关的 LAN 状态

局域网状态	
IP地址	192.168.0.2
MAC地址	34:FA:40:04:B9:C7

选项	描述
IP 地址	显示网关的 IP 地址。
MAC 地址	显示网关的 MAC 地址。

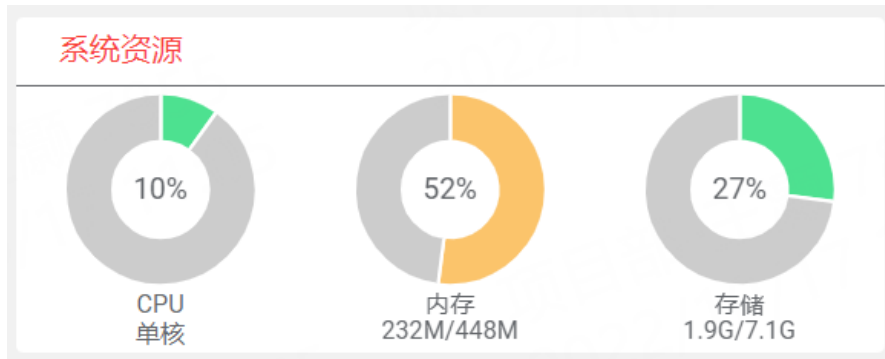
3.1.6 系统资源

系统资源此页显示网关的系统资源使用情况信息。

当使用量超过 65% 时，图标将显示为红色。

当使用率低于 30% 时，图标将显示为绿色。

当使用率介于 30% 和 65% 之间时，图标将为黄色。



3.1.7 系统信息

此页显示网关的系统信息。

系统信息	
操作系统	Debian GNU/Linux 11.3
系统时间	Thu Jul 7 16:47:33 2022
固件版本	2.0.0 (d6ad1c5)
硬件版本	0.0
内核版本	5.4.70-gc5eab33ca
序列号	08270122070019

选项	描述
操作系统	显示操作系统信息。
系统时间	显示当前系统时间。
固件版本	显示网关上运行的固件版本
硬件版本	显示当前硬件版本
内核版本	显示当前内核版本
序列号	显示设备的序列号。

3.1.8 模块状态

此页面显示网关的模块状态。

Cellular Status

Modem Vendor	quectel
Modem Model	EG25
Network Registration	Registered to home network
IMEI	865167060963973
IMSI	460015726101417

选项	描述
Modem Vendor	显示蜂窝模块供应商信息。
Modem Model	显示蜂窝模块的型号。
Network Registration	显示当前网络注册信息。
IMEI	显示蜂窝模块的IMEI（国际移动设备标识）号。
IMSI	显示当前 SIM 卡的 IMSI。

3.2 网络

3.2.1 广域网


WAN 代表广域网，提供与互联网的连接。您可以基于以太网、蜂窝调制解调器或 WiFi（如果支持）配置 WAN。

链路

链路	状态																		
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px; margin-bottom: 5px;">^ 设置</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>名称</th> <th>类型</th> <th>描述</th> <th>权重</th> <th>防火墙区域</th> <th style="text-align: right;">+</th> </tr> </thead> <tbody> <tr> <td>WWAN</td> <td>蜂窝网</td> <td>default wan</td> <td style="text-align: center;">0</td> <td style="text-align: center;">external</td> <td style="text-align: right;">⋮ □ ×</td> </tr> <tr> <td>Robustel</td> <td>以太网</td> <td></td> <td style="text-align: center;">0</td> <td style="text-align: center;">external</td> <td style="text-align: right;">⋮ □ ×</td> </tr> </tbody> </table> </div>		名称	类型	描述	权重	防火墙区域	+	WWAN	蜂窝网	default wan	0	external	⋮ □ ×	Robustel	以太网		0	external	⋮ □ ×
名称	类型	描述	权重	防火墙区域	+														
WWAN	蜂窝网	default wan	0	external	⋮ □ ×														
Robustel	以太网		0	external	⋮ □ ×														

单击  添加新的 WAN 链路

单击  删除链路

拖动  调整链路的优先级，顶部的链路具有更高的优先级。

单击  编辑链接

用户可以在此部分中管理链接连接。它提供四种类型的互联网连接，包括蜂窝网，以太网，VLAN 和 Wi-Fi。

^ 链路设置	
名称	<input type="text" value="WWAN"/> ?
类型	<input type="text" value="蜂窝网"/> v
接口	<input type="text" value="wwan"/> v
描述	<input type="text" value="default wan"/>
权重	<input type="text" value="0"/> ?
防火墙区域	<input type="text" value="external"/> v

^ 链路设置	
名称	<input type="text" value="Robustel"/> ?
类型	<input type="text" value="以太网"/> v
接口	<input type="text" value="eth0"/> v
描述	<input type="text" value=" "/>
权重	<input type="text" value="0"/> ?
防火墙区域	<input type="text" value="external"/> v

^ 链路设置	
名称	<input type="text" value="Robustel"/> ?
类型	<input type="text" value="VLAN"/> v
接口	<input type="text"/> v
描述	<input type="text"/>
权重	<input type="text" value="0"/> ?
防火墙区域	<input type="text" value="external"/> v

^ 链路设置

名称	<input style="width: 90%;" type="text" value="Robustel"/>	?
类型	<input style="width: 90%;" type="text" value="WIFI"/>	v
接口	<input style="width: 90%;" type="text" value="wlan0"/>	v
SSID	<input style="width: 90%;" type="text" value="router"/>	
密码	<input style="width: 90%;" type="password"/>	
描述	<input style="width: 90%;" type="text" value="Wi-Fi"/>	
权重	<input style="width: 90%;" type="text" value="0"/>	?
防火墙区域	<input style="width: 90%;" type="text" value="external"/>	v

选项	描述	默认值
名称	链路的名称	--
类型	<ul style="list-style-type: none"> 连接类型。 蜂窝网：通过蜂窝网络连接。 以太网：通过以太网有线网络连接。 VLAN：通过VLAN网络连接。 WIFI：通过无线网络连接。 	空
接口	设置相关接口。 如果类型是调制解调器，请参阅 3.3.2 蜂窝网络 如果类型是以太网，请参阅 3.3.1 以太网 如果类型为 VLAN，请参阅 3.3.6 VLAN 如果类型为 Wi-Fi，请参阅 3.3.4 Wi-Fi	空
描述	链接的说明。	空
SSID	无线网络的名称。	0
密码	无线网络的密码。	0
权重	此链接在所有链接中的权重。	0
防火墙区域	所选的防火墙规则集，请参见 3.2.5 防火墙	0

^ IPv4设置

IPv4连接类型	<input style="width: 90%;" type="text" value="DHCP"/>	?
----------	---	---

^ IPv6设置

IPv6连接类型	<input style="width: 90%;" type="text" value="自动"/>	v
----------	---	---

^ 链路检测设置
?

启用 ON OFF

IPv4 首选服务器

IPv4 备用服务器

IPv6 首选服务器

IPv6 备用服务器

间隔 ?

超时 ?

失败次数上限 ?

成功次数下限 ?

选项	描述	默认值
IPv4 连接类型	IPv4 连接的类型。 <ul style="list-style-type: none"> DHCP。 PPPoE。 手动。 不启动。 选择相应的类型。 *注：现在不支持基于 PPPoE 的 IPv6，因此如果在此处选择 PPPoE，请禁用 IPv6。	DHCP
IPv6 连接类型	IPv6 连接的类型。 <ul style="list-style-type: none"> 自动。 手动。 不启动。 选择相应的类型。	自动

选项	描述	默认值
启用	单击切换按钮以启用/禁用Ping检测机制	OFF
IPv4 首选服务器	网关Ping IPv4主地址/域名来检测当前网络连接是否正常。	8.8.8.8
IPv4 备用服务器	网关Ping IPv4备用地址/域名来检测当前网络连接是否正常。	114.114.114.114
IPv6 首选服务器	网关Ping IPv6主地址/域名来检测当前网络连接是否正常。	2001:4860:4860::8888
IPv6 备用服务器	网关Ping IPv6备用地址/域名来检测当前网络连接是否正常。	2400:3200:baba::1
间隔	设置Ping的间隔时间。	30
超时	设置Ping的超时时间。	3

选项	描述	默认值
失败次数上限	在连续探测不成功的情况下尝试重新连接此链接。	3
成功次数下限	在连续探测成功的情况下，恢复此链接。	3

状态

此窗口用于查看网关的链路状态。

链路	状态			
^ 链路状态				
接口	状态	MAC地址	IPv4地址	IPv6地址
wwan	Disconnected			
eth0	Connected	8A:AE:E4:18:17:20	172.16.19.29	


3.2.2 局域网


局域网（LAN）将逻辑第 2 层网络中的网络设备（如以太网或网桥）连接在一起。默认链接（br_lan）始终可用。

链路

名称	类型	描述	防火墙区域	
LAN1	网桥	default lan	internal	+
				✕

单击  添加新的局域网链路

单击  删除局域网链路

单击  编辑局域网链路

用户可以在此部分中管理链接连接。它提供三种连接类型，包括网桥，以太网和 VLAN。

^ 链路设置

名称	<input type="text" value="LAN1"/>	?
类型	<input type="text" value="网桥"/>	v
接口	<input type="text" value="br_lan"/>	v
描述	<input type="text" value="default lan"/>	
防火墙区域	<input type="text" value="internal"/>	v

选项	描述	默认值
名字	局域网链路的名称。	--
类型	连接类型。从“网桥”、“以太网”和“VLAN”中进行选择。 <ul style="list-style-type: none"> 网桥：通过网桥网络连接。 以太网：通过以太网有线网络连接。 VLAN：通过VLAN网络连接。 	空
接口	设置相关接口。 如果类型为网桥，请参阅 3.3.3 网桥 。 如果类型是以太网，请参阅 3.3.1 以太网 。 如果类型为 VLAN，请参阅 3.3.6 VLAN 。	空
描述	链路的说明。	空
防火墙区域	所选的防火墙规则集，请参见 3.2.5 防火墙 。	0

^ ip4设置

IPv4地址	<input type="text" value="192.168.0.1/24"/>	+
--------	---	---

^ DHCPv4设置

起始IPv4地址池	<input type="text" value="192.168.0.2"/>	
结束IPv4地址池	<input type="text" value="192.168.0.100"/>	
首选DNS服务器	<input type="text"/>	
备用DNS服务器	<input type="text"/>	
租约时间	<input type="text" value="120"/>	?

选项	描述	默认值
IPv4 地址	输入LAN的地址。格式“IP/掩码”例如192.168.0.1/24	--
起始 IP 地址池	定义给DHCP客户端分配地址的IP地址池开端。	空
结束 IP 地址池	定义给DHCP客户端分配地址的IP地址池结尾。	空

选项	描述	默认值
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主要DNS服务器。	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

^ IPv6设置

地址模式

^ IPv6设置

地址模式

IPv6地址转换

IPv6地址 ?

选项	描述	默认值
地址模式	委托或静态。	委托
IPv6 地址转换	在静态模式下开启或关闭 IPv6 地址转换。	ON
IPv6 地址	在静态模式下输入具有 64 位网络前缀的 IPv6 地址。	--

状态

此窗口用于查看局域网链路的状态。

^ 接口状态

接口	MAC地址	IPv4地址	IPv6地址
br_lan	34:FA:40:1B:5C:91	192.168.0.1	fe80::611f:333d:e8b...

^ 已连接设备

索引	IP地址	MAC地址	接口	无活动时间
1	192.168.0.73	00:E0:4C:10:00:57	br_lan	0s
2	fe80::70bb:1ab:461f:1d37	00:E0:4C:10:00:57	br_lan	20s

^ DHCP租约表

索引	IP地址	MAC地址	接口	使用时间
----	------	-------	----	------

3.2.3 路由

路由确保网络流量能够找到通往目标网络的路径。静态路由是路由表中的固定路由条目。

静态路由

静态路由
状态

^ 静态路由表

索引	描述	目的点	子网掩码	网关	Interface	
+						

单击 + 添加静态路由。最多支持配置 20 条。

^ 静态路由

索引	<input style="width: 90%;" type="text" value="1"/>
描述	<input style="width: 90%;" type="text"/>
目的点	<input style="width: 90%;" type="text"/>
子网掩码	<input style="width: 90%;" type="text"/>
网关	<input style="width: 90%;" type="text"/>
路由度量	<input style="width: 90%;" type="text" value="0"/>
MTU	<input style="width: 90%;" type="text" value="1500"/>
Interface	<input style="border-bottom: 1px solid #ccc;" type="text" value="br_lan"/> v

选项	描述	默认值
索引	指示列表的序号。	--
描述	输入此静态路由的说明。	空
目的点	输入目标主机或目标网络的 IP 地址。	空
子网掩码	输入目标主机或目标网络的网络掩码。	空
网关	定义目标的网关。	空
路由度量	输入度量值。度量值用于衡量路由的优先级。值越小，路径越优。	0
MTU	输入 MTU 值 1280~1500。	1500
Interface	选择路由所要配置的链路接口。	--

状态

此窗口用于查看路由的状态。

静态路由		状态			
^ 路由表					
索引	目的地	子网掩码	网关	接口	度量
1	0.0.0.0	0.0.0.0	172.16.19.1	eth0	200
2	172.16.19.0	255.255.255.0	0.0.0.0	eth0	200
3	192.168.0.0	255.255.255.0	0.0.0.0	br_lan	425

3.2.4 策略路由

在此窗口中，您可以根据报文中的 IP 地址、端口号来设置策略路由。

策略路由

策略路由						
^ 匹配设置						
索引	名称	协议	源地址	目的地址	绑定接口	+

单击 **+** 添加策略路由。最多支持配置 20 条。

^ 匹配设置

索引	<input type="text" value="1"/>	
名称	<input type="text"/>	
协议	<input type="text" value="TCP-UDP"/>	v
钩子	<input type="text" value="PREROUTING"/>	v
源端口	<input type="text"/>	?
源MAC地址	<input type="text"/>	?
目的地址	<input type="text"/>	?
目的端口	<input type="text"/>	?

选项	描述	默认值
索引	指示列表的序号。	--
名称	策略路由的名称。	--
协议	网络协议的类型。	TCP-UDP
钩子	固定设置。	PREROUTING
源地址	输入源 IP 地址。格式: x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x, 0.0.0.0/0 表示任意。	--
源端口	选择 TCP, UDP 或 TCP-UDP 类型后, 输入源端口。	--
源 MAC 地址	输入源 MAC 地址。	--
目的地址	输入访问源所要访问的目标地址。格式: x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x, 0.0.0.0/0 表示任意。	--
目的端口	选择 TCP, UDP 或 TCP-UDP 类型后, 输入目标端口。	--

^ 路由规则

目的地址	<input type="text"/>	
子网掩码	<input type="text"/>	
网关地址	<input type="text"/>	
绑定接口	<input type="text" value="br_lan"/>	v

选项	描述	默认值
目的地址	输入目标主机或目标网络的 IP 地址。	--
子网掩码	输入目标主机或目标网络的网络掩码。	--
网关地址	输入目标主机或目标网络的网关地址。	--
绑定接口	选择绑定的接口。	--

3.2.5 防火墙

防火墙使用 Linux iptables 来控制进出设备的流量。

常规设置

^ 常规设置

启用 SYN-flood 保护 ON OFF

输出链 接受

输出链 接受

转发链 丢弃

选项	描述	默认值
启用 SYN-flood 保护	单击切换按钮启用/禁用防范 SYN-flood 攻击。	ON
输入链	输入链的默认操作，如果数据包与该链上的任何现有规则都不匹配 <ul style="list-style-type: none"> 接受：数据包继续到下一个链 丢弃：停止并删除数据包 	接受
输出链	输出链的默认操作，如果数据包与该链上的任何现有规则都不匹配 <ul style="list-style-type: none"> 接受：数据包继续到下一个链 丢弃：停止并删除数据包 	接受
转发链	转发链的默认操作，如果数据包与该链上的任何现有规则都不匹配 <ul style="list-style-type: none"> 接受：数据包继续到下一个链 丢弃：停止并删除数据包 	丢弃

注： 除非指定，否则常规设置将用作默认防火墙设置。

^ 安全区域
?

名称	输入链	输出链	转发链	
external	丢弃	接受	丢弃	+ <input type="checkbox"/> <input checked="" type="checkbox"/>
internal	接受	接受	接受	+ <input type="checkbox"/> <input checked="" type="checkbox"/>

区域是一组防火墙规则，用户可以定义自己的防火墙区域。

单击 + 添加一个防火墙区域。最多支持配置 50 条。

^ 安全区域

名称	<input style="width: 90%;" type="text"/>
输入链	<input style="width: 90%;" type="text" value="接受"/> v
输出链	<input style="width: 90%;" type="text" value="接受"/> v
转发链	<input style="width: 90%;" type="text" value="接受"/> v
伪装	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
MSS协商	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF

选项	描述	默认值
名字	防火墙区域的名称。	---
输入链	输入链的默认操作，如果数据包与该链上的任何现有规则都不匹配 <ul style="list-style-type: none"> 接受：数据包继续到下一个链 丢弃：停止并删除数据包 	接受
输出链	输出链的默认操作，如果数据包与该链上的任何现有规则都不匹配 <ul style="list-style-type: none"> 接受：数据包继续到下一个链 丢弃：停止并删除数据包 	接受
转发链	转发链的默认操作，如果数据包与该链上的任何现有规则都不匹配 <ul style="list-style-type: none"> 接受：数据包继续到下一个链 丢弃：停止并删除数据包 	接受
伪装	单击切换按钮以启用/禁用。MASQUERADE 是一个 iptables 目标，当在编写规则时网络接口的外部 IP 未知时（当接口动态获取外部 IP 时），可以使用它来代替 SNAT（源 NAT）目标。	ON
MSS 协商	单击切换按钮以启用/禁用。MSS 协商是一种解决方法，用于更改通过 MTU 低于以太网默认值 1500 的链路的所有 TCP 连接的最大段大小（MSS）。	ON

^ DMZ设置

启用DMZ	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
主机IP地址	<input style="width: 90%;" type="text"/>
源IP地址	<input style="width: 90%;" type="text"/> ?
目的地址	<input style="width: 90%;" type="text"/>

DMZ（隔离区），也称为非军事化区。它是非安全系统与安全系统之间的缓冲区，旨在解决访问外部网络的用户在安装防火墙后无法访问内部网络服务器的问题。DMZ 主机是一种 Intranet 主机，其中所有端口都对指定地址开放，但被占用和转发的端口除外。

选项	描述	默认值
启用 DMZ	单击切换按钮以启用/禁用 DMZ。DMZ 主机是内部网络上公开所有端口（以其他方式转发的端口除外）的主机。	ON
主机 IP 地址	输入内部网络上 DMZ 主机的 IP 地址。	空
源 IP 地址	设置可以与 DMZ 主机通信的地址。空表示任何地址。	空
目标 IP 地址	设置 DMZ 主机可以与的地址。空表示任何地址。	空

^ 访问控制设置

启用SSH访问 ON OFF

启用HTTP访问 ON OFF

启用HTTPS访问 ON OFF

响应Ping请求 ON OFF ?

选项	描述	默认值
启用 SSH 访问	单击切换按钮以启用/禁用此选项。启用后，互联网用户可以通过 SSH 访问网关。	ON
启用 HTTP 访问	单击切换按钮以启用/禁用此选项。启用后，互联网用户可以通过 HTTP 访问网关。	ON
启用 HTTPS 访问	单击切换按钮以启用/禁用此选项。启用后，互联网用户可以通过 HTTPS 访问网关。	ON
启用 Ping 响应	单击切换按钮以启用/禁用此选项。启用后，网关将响应其他主机的 Ping 请求。	ON

端口转发

常规设置
端口转发
通行规则
自定义规则
状态

^ 端口转发规则

索引	名称	协议	源安全区域	目的安全区域	+

此窗口用于查看端口转发规则。端口转发是一种将传入连接重定向到另一个 IP 地址、端口或两者的组合的方法。

单击 + 添加一个端口转发规则。最多支持配置 50 条。

端口转发规则

索引	<input type="text" value="1"/>
名称	<input type="text"/>
IPv4源地址	<input type="text"/> +
协议	TCP-UDP v
源安全区域	external v
外部端口	<input type="text"/> ?
目的安全区域	external v
内部IP地址	<input type="text"/>
内部端口	<input type="text"/> ?

选项	描述	默认值
索引	指示列表的序号。	--
名称	规则的名称。	空
IPv4 源地址	连接主机所使用的 IP 地址或网段。该规则只适用于从该字段中指定的 IP 地址连接的主机	空
协议	从“TCP”、“UDP”或“TCP-UDP”中选择您的应用相匹配的协议	TCP-UDP
源安全区域	第三方将连接到的区域。选择已配置的 ZONE。	external
外部端口	匹配定向到此主机上给定目标端口或端口范围的传入流量。选择已配置的 ZONE。	空
目标安全区域	传入连接将重定向到的区域。	external
内部 IP 地址	传入连接将重定向到的 IP 地址。	空
内部端口	传入连接将重定向到的端口号。	空

通信规则

常规设置 端口转发 **通行规则** 自定义规则 状态

通信规则

索引	名称	地址族	协议	源安全区域	动作	+

此窗口可查看通信规则。单击 **+** 添加一条通信规则。最多支持配置 50 条。

^ 通信规则

索引	<input type="text" value="1"/>	
名称	<input type="text"/>	
地址族	<input type="text" value="IPv4-IPv6"/>	v
协议	<input type="text" value="TCP-UDP"/>	v
源安全区域	<input type="text" value="device_output"/>	v
IPv4源地址	<input type="text"/>	?
IPv6源地址	<input type="text"/>	
源端口	<input type="text"/>	?
源MAC地址	<input type="text"/>	?
目的安全区域	<input type="text" value="any_forward"/>	v
IPv4目的地址	<input type="text"/>	?
IPv6目的地址	<input type="text"/>	
目的端口	<input type="text"/>	?
动作	<input type="text" value="丢弃"/>	v

选项	描述	默认值
索引	指示列表的序号。	--
名字	规则的名称。	空
地址族	根据您的应用要求，从“IPv4”、“IPv6”或“IPv4-IPv6”中进行选择。	IPv4-IPv6
协议	根据您的应用要求，从“TCP”、“UDP”或“TCP-UDP”中进行选择。	TCP-UDP
源安全区域	第三方将连接到的 ZONE。	device_output
IPv4 源地址	连接主机所使用的 IPv4 地址或网段。 该规则只适用于从该字段中指定的 IP 地址连接的主机	空
IPv6 源地址	连接主机使用的 IPv6 地址或网段。 该规则将仅适用于从此字段中指定的 IP 地址进行连接的主机。	空
源端口	连接主机使用的端口号。 该规则会将连接主机使用的源端口与此字段中指定的端口号进行匹配。将空放置以使规则跳过源端口匹配。	空
源 MAC	连接主机的 MAC 地址。	空

选项	描述	默认值
	该规则将仅适用于与此字段中指定的 MAC 地址匹配的主机。留空以使规则跳过 MAC 地址匹配。	
目的安全区域	传入连接将重定向到的 ZONE。	any_forward
IPv4 目标地址	传入连接将重定向到的 IP 地址。	空
IPv6 目标地址	传入连接将重定向到的 IP 地址。	空
目标端口	传入连接将重定向到的端口号。	空
动作	根据您的应用要求，从“接受”、“丢弃”中进行选择	空

自定义规则

常规设置
端口转发
通行规则
自定义规则
状态

^ 自定义规则

索引	描述	地址族	规则	+

此窗口用于查看自定义规则。单击 + 添加规则。最多支持配置 50 条。

^ 自定义防火墙规则

索引	<input style="width: 60%;" type="text" value="1"/>
描述	<input style="width: 60%;" type="text"/>
地址族	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; text-align: right; font-size: small; color: #666; padding-right: 5px;" type="text" value="IPv4"/> v
规则	<input style="width: 60%;" type="text"/> ?

选项	描述	默认值
索引	指示列表的序号。	--
描述	输入对此自定义防火墙规则的描述。	空
地址族	根据您的应用要求，从“IPv4”、“IPv6”或“IPv4-IPv6”中进行选择。	IPv4
规则	输入自定义的规则。如：-I INPUT -s 192.168.0.2 -j ACCEPT	空

状态

此窗口用于查看防火墙状态。

常规设置
端口转发
通行规则
自定义规则
状态

^ IPv4 Filter

```

314 30172 input_internal_rule all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
33 1584 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:443
4 256 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 8
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 ctstate DNAT
477 34332 zone_internal_src_ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain zone_internal_output (1 references)
pkts bytes target prot opt in out source destination
7 2064 output_internal_rule all -- * * 0.0.0.0/0 0.0.0.0/0
7 2064 zone_internal_dest_ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0
      
```

3.2.6 QoS

QoS 可提供基于主机、端口号或服务的网络优化，也可以限制选定接口的下载与上传速率。

常规设置

^ 常规设置

启用QoS

ON OFF

上传带宽

10000

?

下载带宽

10000

?

选项	描述	默认值
启用 QoS	单击切换按钮启用或禁用，建议启用 QoS。	OFF
上传带宽	输入上传带宽的值，单位为 kbit。	1000
下载带宽	输入下载带宽的值，单位为 kbit。	1000

优先级定义

^ 优先级定义 ?				
索引	优先级	带宽	借用空闲带宽	
1	最高	20	true	
2	较高	20	true	
3	正常	20	true	
4	较低	20	true	
5	最低	20	true	

单击 设置优先级

^ 优先级定义	
索引	<input type="text" value="1"/>
优先级	<input type="text" value="最高"/> v
带宽	<input type="text" value="20"/> ?
借用空闲带宽	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF ?

选项	描述	默认值
带宽	占总带宽的百分比。所有优先级的带宽总和不能大于 100。	20
借用空闲带宽	启用借用时，与此优先级关联的流量将从其他优先级借用未使用的带宽，并在禁用借用时限制为指定的带宽。	ON

IPv4 QoS 规则

^ IPv4 QoS规则							
索引	源地址	源端口	目的地址	目的端口	协议	优先级	+

单击 添加 1 条规则。最多支持配置 10 条。

^ QoS规则

索引	<input type="text" value="1"/>	
源地址	<input type="text"/>	?
源端口	<input type="text"/>	?
源MAC地址	<input type="text"/>	?
目的地址	<input type="text"/>	?
目的端口	<input type="text"/>	?
协议	<input type="text" value="全部"/>	v
优先级	<input type="text" value="正常"/>	v

选项	描述	默认值
索引	显示列表的序号。	--
源地址	源主机 IP 地址或网络地址。	空
源端口	源主机端口。	空
源 MAC	源主机 MAC 地址。	空
目标地址	目标主机 IP 地址或网络地址。	空
目标端口	目标主机端口。	空
协议	根据您的应用要求，从“TCP”、“UDP”或“ICMP”中进行选择。	全部
优先权	根据您的应用要求，从“最高”、“最高”、“正常”、“最低”或“最低”中进行选择。	正常

IPv6 QoS 规则

^ IPv6 QoS规则

索引	源地址	源端口	目的地址	目的端口	协议	优先级	+

单击 + 添加 1 条规则。最多支持配置 10 条。

^ QoS规则

索引	<input style="width: 90%;" type="text" value="1"/>	
源地址	<input style="width: 90%;" type="text"/>	?
源端口	<input style="width: 90%;" type="text"/>	?
源MAC地址	<input style="width: 90%;" type="text"/>	?
目的地址	<input style="width: 90%;" type="text"/>	?
目的端口	<input style="width: 90%;" type="text"/>	?
协议	<input style="width: 90%;" type="text" value="全部"/>	v
优先级	<input style="width: 90%;" type="text" value="正常"/>	v

选项	描述	默认值
索引	显示列表的序号。	--
源地址	源主机 IP 地址或网络地址。	空
源端口	源主机端口。	空
源 MAC 地址	源主机 MAC 地址。	空
目的地址	目标主机 IP 地址或网络地址。	空
目的端口	目标主机端口。	空
协议	根据您的应用要求，从“TCP”、“UDP”或“ICMP”中进行选择。	全部
优先级	根据您的应用要求，从“最高”、“最高”、“正常”、“最低”或“最低”中进行选择。	正常



3.3 接口


3.3.1 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。设备中的所有以太网端口都可以配置为 WAN 端口或 LAN 端口。所有以太网端口的默认设置均为 lan0，其默认 IP 为 192.168.0.1/255.255.255.0。

注：LG5100 ETH 0 支持 POE-PD 功能。

端口

端口		状态	
^ 端口设置			
名称	端口	MTU	MAC地址
port1	eth0	1500	
port2	eth1	1500	

单击  以配置其参数，并在弹出窗口中修改端口分配参数。

^ 端口设置	
名称	<input type="text" value="port1"/> 
端口	<input type="text" value="eth0"/> v
端口速率	<input type="text" value="自动"/> v
MTU	<input type="text" value="1500"/> 
MAC地址	<input type="text"/> 

选项	描述	默认值
名称	端口的名称。	--
端口	显示编辑的端口	--
端口速度	从“自动”，“10M 半双工”，“10M-全双工”，“100M 半双工”，“100M 全双工”，“1000M 半双工”，“1000M 全双工”中选择。	自动
MTU	输入最大传输单位（maximum transmission unit）的值。	1500
MAC 地址	指定端口的 MAC 地址。	--
启用 POE (可选)	点击切换按钮来启用或禁用 POE 功能。当 POE 功能启用后，它将支持使用 POE 供电。	ON

状态

此页面用于查看以太网端口的状态。

^ 端口状态		
索引	端口	连接状态
1	eth0	Up
2	eth1	Down

3.3.2 蜂窝网络

本节用于设置蜂窝网络的相关参数。

蜂窝网络

蜂窝网
状态
AT调试

^ 蜂窝网常规设置

主SIM卡 ?

开启SIM卡自动切换功能 ON OFF ?

选项	描述	默认值
主 SIM 卡	选择一张 SIM 卡作为主 SIM 卡	SIM1
开启 SIM 卡自动切换功能	启用自动切换后，默认情况下，当 SIM 卡错误或连接错误或 ping 失败时，SIM 卡将自动切换到另一张 SIM 卡。	ON


^ 附加的切换规则

基于信号强度切卡 ON OFF ?

当漫游时切卡 ON OFF ?

选项	描述	默认值
基于信号强度切卡	当信号较差时，切换到另一个 SIM 卡。仅适用于双 SIM 卡备份。	OFF
当漫游时切卡	漫游时切换到另一张 SIM 卡。仅适用于双 SIM 卡备份。	OFF

^ 蜂窝网高级设置					
索引	SIM卡	电话号码	网络类型	频段选择	
1	SIM1		自动	全部	
2	SIM2		自动	全部	

单击  以在弹出窗口中配置其参数。

^ 常规设置	
索引	<input type="text" value="1"/>
SIM卡	<input type="text" value="SIM1"/> v
自动匹配APN	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
电话号码	<input type="text"/>
PIN码	<input type="text"/> ?
额外的AT命令	<input type="text"/> ?
Telnet端口	<input type="text" value="0"/> ?

选项	描述	默认值
索引	显示列表的序号。	--
SIM 卡	显示当前正在编辑的 SIM 卡。	SIM1
自动匹配 APN	单击切换按钮以启用/禁用“自动 APN 选择”选项。启用后，设备将自动识别接入点名称。用户可以禁用此选项并手动添加接入点名称。	ON
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 4-8 个字符的 PIN 码。	空
额外的 AT 命令	输入用于蜂窝初始化的 AT 命令。	空
Telnet 端口	指定 Telnet 服务的端口侦听，用于通过 Telnet 进行 AT。	0

当“自动 APN 选择”处于关闭状态时，用户可以指定自己的 APN 设置。

自动匹配APN	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
APN	<input type="text" value="internet"/>
用户名	<input type="text"/>
密码	<input type="text"/>
鉴权方式	<input type="text" value="无鉴权"/> v
电话号码	<input type="text"/>
PIN码	<input type="text"/> ?
额外的AT命令	<input type="text"/> ?
Telnet端口	<input type="text" value="0"/> ?

项目	描述	默认值
APN	输入由本地 ISP 提供的蜂窝拨号连接的接入点名称。	internet
用户名	输入由本地 ISP 提供的蜂窝拨号连接的用户名。	空
密码	输入由本地 ISP 提供的手机网络拨号连接的密码。	空
鉴权方式	选择身份验证类型。从“None”, “CHAP”, “PAP”中进行选择。 <ul style="list-style-type: none"> None: 无鉴权。 CHAP: 挑战握手认证协议。 PAP: 密码验证协议。 	无鉴权

^ 网络设置

网络类型	<input type="text" value="自动"/> v ?
频段选择	<input type="text" value="全部"/> v ?

选项	描述	默认值
网络类型	选择蜂窝移动网络类型，即网络访问顺序。从“自动”，“仅2G”，“优先2G”，“仅3G”，“优先3G”，“仅4G”，“优先4G”，“仅5G”中选择。 <ul style="list-style-type: none"> 自动: 自动连接到最佳信号网络 仅限2G: 仅连接2G网络 优先2G: 优先使用2G网络 仅限3G: 仅连接3G网络 优先3G: 优先使用3G网络 仅限4G: 仅连接4G网络 优先4G: 优先使用4G网络 	自动

	<ul style="list-style-type: none"> • 仅限5G: 仅连接5G网络 <p>注: 由于蜂窝模块不同, 可能会有一些不同的可选网络类型。</p>	
频段选择	<p>从“全部”或“指定”中进行选择。如果选择“指定”, 您可以选择某些频段。</p> <p>注: 由于蜂窝模块不同, 频段设置可能存在一些差异。</p>	全部

^ 高级设置

启用调试 ON OFF

启用详细调试 ON OFF

网络注册超时时间 ?

选项	描述	默认值
启用调试	单击切换按钮以启用/禁用此选项。启用调试信息输出。	ON
启用详细调试	单击切换按钮以启用/禁用此选项。启用详细调试信息输出。	OFF
网络注册超时时间	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

状态

此页面用于查看蜂窝移动网络连接的状态。

^ 蜂窝网信息

索引	模块状态	模块型号	IMSI	注册状态
1	Initializing	EG25		

单击状态行，详细的状态信息将显示在行下。

^ 蜂窝网信息				
索引	模块状态	模块型号	IMSI	注册状态
1	Ready	EG25	[REDACTED]	Registered to home network
<p>索引 1</p> <p>模块状态 Ready</p> <p>模块型号 EG25</p> <p>当前SIM卡 SIM1</p> <p>电话号码 [REDACTED]</p> <p>IMSI [REDACTED]</p> <p>ICCID [REDACTED]</p> <p>注册状态 Registered to home network</p> <p>运营商 CHINA MOBILE</p> <p>网络类型 LTE</p> <p>频段 39</p> <p>信号强度 17 (-79dBm)</p> <p>参考信号接收功率 -109 dBm</p> <p>参考信号接收质量 -8 dB</p> <p>信号与干扰加噪声比 17 dB</p> <p>位误码率 99</p> <p>运营商识别号 46000</p> <p>位置区码 FFFE</p> <p>小区号 02A21102</p> <p>物理扇区ID 205</p> <p>IMEI [REDACTED]</p> <p>固件版本 EG25GGBR07A08M2G_01.002.01.002</p> <p>模块厂家 quectel</p>				

选项	描述
索引	显示列表的序号。
模块状态	显示蜂窝模块的状态。
模块型号	显示蜂窝模块的型号。
当前 SIM 卡	显示网关正在使用的 SIM 卡。
电话号码	显示当前 SIM 卡的电话号码。
IMSI	显示当前 SIM 卡的 IMSI。
ICCID	显示当前 SIM 卡的 ICCID。
注册状态	显示当前网络状态。
运营商	显示网络提供商的名称。

选项	描述
网络类型	显示当前网络服务类型。
频段	显示频段信息。
信号强度	显示网关检测到的信号强度。
参考信号接收功率	注册到网络时显示当前 RSRP。
参考信号接收质量	注册到网络时显示当前 RSRQ。
信号干扰加噪声比	注册到网络时显示当前 SINR。
位误码率	显示当前误码率。
PLMN ID	显示当前 PLMN ID。
位置区码	显示用于标识不同区域的当前本地区域代码。
小区号	显示用于定位网关的当前小区 ID。
物理小区标识	显示用于定位网关的当前物理单元 ID。
IMEI	显示蜂窝模块的 IMEI（国际移动设备标识）号。
固件版本	显示蜂窝模块的当前固件版本。
模块厂家	显示蜂窝模块的厂家名称。

AT 调试

此页用于 AT 命令调试。

蜂窝网
状态
AT调试

^ AT命令调试

命令

结果

发送

3.3.3 网桥

网桥用于创建由多个设备组成的单个网络。默认网桥（br_lan）始终可用。


设置

^ 接口

接口	描述	+
br_lan	default bridge	✕

单击 + 添加新的网桥。

单击  以删除网桥。

单击  单击以在弹出窗口中配置网桥的参数。

^ 接口

接口	br_lan	?
描述	default bridge	
子接口	<input checked="" type="checkbox"/> eth0 <input checked="" type="checkbox"/> eth1	

选项	描述
接口	接口的名称
描述	桥的说明。
子接口	选择并启用相关的以太网端口。

3.3.4 Wi-Fi

本节用于配置 Wi-Fi AP 模式的参数。网关支持 Wi-Fi AP 模式或客户端模式。

地区

国别
无线射频
状态

^ 地区

地区	SE	?
----	----	---

选项	描述
地区	请使用 ISO 3166-1 alpha-2 标准中定义的两字母的国家代码。

无线射频

射频设置

Wi-Fi 支持 2.4 GHz 和 5 GHz，但不能同时支持两者

2.4 GHz: 11 bgn 混合模式，仅 11b，仅 11g，仅 11n

5 GHz: 11an & 11a/an/ac 混合模式

^ 射频设置

启用

无线模式

通道

ON
OFF

11bgn混合模式
v

自动
v
?

选项	描述	默认值
启用	单击切换按钮以启用/禁用 Wi-Fi 接入点选项。	OFF
无线模式	<p>从“11bgn 混合模式”、“仅 11b”、“仅 11g”，“仅 11n”，“11a/an/ac 混合模式或仅 11an 中进行选择。</p> <ul style="list-style-type: none"> • 11bgn 混合模式: 混合 IEEE 802.11b/g/n 三种协议, 用于向后兼容 • 仅 11b: IEEE 802.11b • 仅 11g: IEEE 802.11g • 仅 11n: IEEE 802.11n • 11a/an/ac 混合模式: IEEE 802.11a/an/ac. • 仅 11an: 仅 IEEE 802.11an. 	11bgn 混合模式

选项	描述	默认值
通道	<p>从“自动”、“1”、“2”……“13”,或“36”,“40”、“44”、“48”、“149”、“153”、“157”、“161”、“165”中选择频道</p> <ul style="list-style-type: none"> 1~13 网关将固定与此通道配合使用 自动: 设备会一直扫描所有的频率,直到找到一个可用的 其他: 网关将固定与此通道配合使用 <p>2.4 GHz:</p> <ul style="list-style-type: none"> 20/40 MHz 带宽可用信道对应的 1~13 频道的频率 <ul style="list-style-type: none"> 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 <p>5 GHz:</p> <ul style="list-style-type: none"> 20/40/80 MHz 带宽可用信道对应的 36~165 频道的频率 (80 MHz 仅无线模式为 11ac 使用): <ul style="list-style-type: none"> 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 <p><i>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存在差异,需要 WEB 页面配置区域。</i></p>	自动
带宽 (11a/ac/an or 11an)	从“80MHz”,“40MHz”,“20MHz”或者“40MHz”,“20MHz”中选择	11a/an/ac: 80MHz 11an: 40MHz

射频高级设置

^ 射频高级设置

信号间隔	<input style="width: 90%;" type="text" value="100"/>	?
DTIM周期	<input style="width: 90%;" type="text" value="2"/>	?
RTS/CTS阈值	<input style="width: 90%;" type="text" value="2347"/>	?
分片阈值	<input style="width: 90%;" type="text" value="2346"/>	?
发射功率	<input style="width: 90%;" type="text" value="最大"/>	v
启用WMM	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	
启用Short GI	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	?
带宽	<input style="width: 90%;" type="text" value="自动"/>	v ?
传输速率	<input style="width: 90%;" type="text" value="自动"/>	
11N传输速率	<input style="width: 90%;" type="text" value="自动"/>	

选项	描述	默认值
信号间隔	设置网关 AP 广播用于无线网络身份验证的信标的时间间隔。	100
DTIM 周期	设置投递流量指示消息周期，AP 将根据该时间段对数据进行多播。	2
RTS/CTS 阈值	设置“请求发送”阈值。当阈值设置为 2347 时，AP 在发送数据之前不会发送检测信号。当阈值设置为 0 时，AP 会在发送数据之前发送检测信号。	2347
分片阈值	设置 Wi-Fi 接入点的分段阈值。建议您使用默认值 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	注意：40 MHz 信道宽度提供更高的可用数据速率，是 20 MHz 信道宽度的两倍。	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
带宽	从“自动”、“20MHz” or “40MHz”.中进行选择 注：40 MHz 信道宽度提供更高的可用数据速率，是 20 MHz 信道宽度的两倍。	自动
传输速率	设置传输速率。您可以选择“自动”或指定传输速率，包括 1Mbps、2Mbps、5.5Mbps、6Mbps、11Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps 和 54Mbps。	自动
11n 传输速率	指定 IEEE 802.11n 模式下的传输速率。您可以选择“自动”或指定传输速率，包括 MCS0、MCS1、MCS2、MCS3、MCS4、MCS5、	自动

选项	描述	默认值
	MCS6 和 MCS7、MCS8、MCS9、MCS10、MCS11、MCS12、MCS13、MCS14、MCS15。	

射频 VAP 设置

^ 射频VAP设置

启用	广播SSID	SSID	安全模式	+
				+

单击 + 添加接入点。最多支持配置 2 条。

单击 □ 配置接入点。

^ 常规设置

启用	<input type="checkbox"/> ON <input type="checkbox"/> OFF
接口	br_lan v
广播SSID	<input type="checkbox"/> ON <input type="checkbox"/> OFF
SSID	router
安全模式	公开 v ?

将安全模式设置为“WPA-个人”时，窗口显示如下。

^ 常规设置

启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
接口	br_lan v
广播SSID	<input type="checkbox"/> ON <input type="checkbox"/> OFF
SSID	router
安全模式	WPA-个人 v ?
WPA版本	自动 v
加密	自动 v ?
PSK密码	<input type="text"/> ?
组密钥更新间隔	3600

将安全模式设置为“WPA-企业”时，窗口显示如下。

^ 常规设置

启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
接口	<input type="text" value="br_lan"/> v
广播SSID	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
SSID	<input type="text" value="router"/>
安全模式	<input type="text" value="WPA-企业"/> v ?
WPA版本	<input type="text" value="自动"/> v
加密	<input type="text" value="自动"/> v ?
Radius认证服务器地址	<input type="text"/>
Radius认证服务器端口	<input type="text" value="1812"/>
Radius认证服务器共享密钥	<input type="text"/>
组密钥更新间隔	<input type="text" value="3600"/>

将安全模式设置为“WEP”时，窗口显示如下。

^ 常规设置

启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
接口	<input type="text" value="br_lan"/> v
广播SSID	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
SSID	<input type="text" value="router"/>
安全模式	<input type="text" value="WEP"/> v ?
WEP密钥	<input type="text"/> ?

选项	描述	默认值
启用	单击切换按钮以启用/禁用 Wi-Fi 接入点选项。	OFF
接口	选择一个接口。	br_lan
广播 SSID	单击切换按钮以启用/禁用正在广播的 SSID。启用后，客户端可以扫描您的 SSID。禁用后，客户端将无法扫描您的 SSID。如果要连接到 AP，则需要在 Wi-Fi 客户端手动输入 AP 的 SSID。	ON

选项	描述	默认值
SSID	输入服务集标识符，即无线网络名称。客户端的 SSID 和 AP 的 SSID 必须相同，客户端和 AP 才能相互通信。输入 1 到 32 个字符。	router
安全模式	<p>可选“公开”、“WPA-个人”、“WPA-企业”或“WEP”</p> <ul style="list-style-type: none"> 公开：用户可以无密码访问 AP，无需身份验证和数据加密 注：出于安全考虑，强烈建议您不要选择这种模式。 WPA-个人：Wi-Fi 保护访问仅提供一个用于身份验证的密码 WPA-Enterprise：为 EAP 提供认证接口，可通过 Radius 认证服务器或其他扩展认证进行验证。 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	<p>从“自动”、“WPA”或“WPA2”中进行选择。</p> <ul style="list-style-type: none"> 自动：网关会自动选择最适合的 WPA 版本 WPA2 是比 WPA 更强的安全功能 	自动
加密	<p>从“自动”、“TKIP”或“AES”中进行选择。</p> <ul style="list-style-type: none"> 自动：网关会自动选择最适合的加密方式 TKIP：时态密钥完整性协议（TKIP）加密使用无线连接。TKIP 加密可用于 WPA-PSK 和 WPA 802.1x 身份验证 注：不建议在 802.11n 模式下使用 TKIP 加密。 AES：AES 加密使用无线连接。AES 可用于 CCMP WPA-PSK 和 WPA 802.1x 身份验证。AES 是比 TKIP 更强的加密算法 	自动
PSK 密码@WPA-个人	输入预共享密钥密码。当网关作为 AP 模式工作时，输入主密钥以生成用于加密的密钥。PSK 密码用作 WLAN 连接中加密方法（或密码类型）的基础。PSK 密码应该很复杂，并且尽可能长。出于安全原因，此 PSK 密码应仅披露给需要它的用户，并应定期更改。输入 8 到 63 个字符。	空
组密钥更新间隔	输入组密钥更新的时间间隔。	3600
Radius 认证服务器的地址@WPA-企业	输入 Radius 认证服务器的地址。	空
Radius 认证服务器的端口@WPA-企业	输入 Radius 认证服务器的端口。	1812
Radius 服务器共享密钥@WPA-企业	输入 Radius 认证服务器的共享密钥。	空
WEP 密钥	输入 WEP 密钥。密钥长度应为 10 或 26 位十六进制数字，具体取决于所使用的 WEP 密钥，即 64 位或 128 位。	空

^ 高级设置

最大接入点个数	64
启用AP隔离	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
调试等级	none v

选项	描述	默认值
最大接入点个数	设置允许访问网关 AP 的最大客户端数。	64
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	从“详细”、“调试”、“信息”、“通知”、“警告”或“无”中进行选择。	none

射频 ACL 设置

^ 射频ACL设置

启用ACL	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
ACL模式	接受 v ?

选项	描述	默认值
启用 ACL	单击切换按钮以启用/禁用此选项。	OFF
ACL 模式	从“接受”或“拒绝”中进行选择。 <ul style="list-style-type: none"> 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保存在访问控制列表里的设备。	接受

射频访问控制列表

^ 射频访问控制列表

索引	描述	MAC地址

+

单击 + 以添加访问控制列表。最多支持配置 64 条。

^ 访问控制列表

索引	1
描述	
MAC地址	

选项	描述	默认值
索引	显示列表的序号。	--
描述	输入此访问控制列表的描述。	空
MAC 地址	添加 MAC 地址。	空

状态

本节用于查看 AP 的状态。

^ VAP1状态						
索引	状态	SSID	通道	带宽	MAC地址	
1	COMPLETED	phy0				

^ VAP1接入点		
索引	MAC地址	信号

^ VAP2状态						
索引	状态	SSID	通道	带宽	MAC地址	
1	COMPLETED	phy0				

^ VAP2接入点		
索引	MAC地址	信号

^ STA状态						
		SSID				
		IP地址				
		BSSID				
		WPA状态	INACTIVE			
		安全模式				

Wi-Fi 客户端

注意：用户可以通过以下步骤将设备配置为 Wi-Fi 客户端。

单击“网络>链路>设置”，单击 **+** 以添加新的 WAN 链接，然后配置相关参数。

^ 链路设置

名称	<input type="text"/>	?
类型	<input type="text" value="WIFI"/>	v
接口	<input type="text" value="wlan0"/>	v
SSID	<input type="text" value="router"/>	
密码	<input type="text"/>	
描述	<input type="text"/>	
权重	<input type="text" value="0"/>	?
防火墙区域	<input type="text" value="external"/>	v

3.3.5 USB

本节可用于配置 USB 参数。网关的 USB 接口可用于升级固件和升级配置。

USB

密钥

^ 常规设置

启用USB	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
启用USB自动升级	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

选项	描述	默认值
启用 USB	单击切换按钮以启用/禁用 USB 选项。	ON
启用 USB 自动升级	单击切换按钮以启用/禁用此选项。启用此选项可在插入具有网关固件的 USB 存储设备时自动更新网关的固件。	OFF

USB

密钥

^ 密钥

USB自动升级密钥
生成密钥

选项	描述	默认值
USB 自动升级密钥	单击 生成密钥 生成文件，单击 下载密钥 以下载密钥。	--

注：使用 USB 自动升级功能时，LED 开始逐个闪烁，表示升级正在进行中。当 LED 停止逐个闪烁，并且用户指示灯亮起时，表示升级已完成。升级后，设备不会自动重新启动。如果没有 LED 一直逐个开始闪烁，则表示存在异常，并且不会进入自动升级过程。

3.3.6 VLAN

VLAN 代表虚拟 LAN，允许将单个物理 LAN 拆分为单独的虚拟 LAN，以减少 LAN 上的广播流量。

设置

^ 接口

名称	描述	VLAN标记
+		

单击 + 以添加新的 VLAN。最多支持配置 10 条。

^ 接口





名称	<input type="text"/>	?
描述	<input type="text"/>	
VLAN标记	<input type="text" value="1"/>	
父接口类型	<input type="text" value="以太网"/>	v
父接口	<input type="text" value="eth0"/>	v


选项	描述	默认值
名称	VLAN 的名称。	空
描述	输入此 VLAN 的说明。	空
VLAN 标记	输入此 VLAN 的标记。	1
父接口类型	从“以太网”或“网桥”中选择。	以太网
父接口	选择相关的父接口。	eth0

3.3.7 DI/DO

本节可用于设置 DI/DO 参数。DI 接口可用于触发报警，而 DO 可用于控制从设备，从而实现实时监控。在某些设备中，用户可以将 IO 配置为 DI 或 DO。

DIDO

DIDO			状态
^ DIDO设置			
索引	PHY模式	启用	
1	DI	false	
2	DI	false	
3	DO	false	
4	DO	false	

单击  以在弹出窗口中配置参数。

DI

^ 常规设置	
索引	<input type="text" value="1"/>
PHY模式	<input type="text" value="DI"/>
启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
模式	<input type="text" value="计数"/>
反向	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
门限值	<input type="text" value="0"/>
告警触发内容	<input type="text" value="Alarm On"/>
告警消除内容	<input type="text" value="Alarm Off"/>

选项	描述	默认值
索引	显示列表的序号。	--
PHY 模式	DI。	--
启用	单击切换按钮以启用/禁用数字输入功能。	OFF

选项	描述	默认值
模式	从“电平”或“计数”中选择。 <ul style="list-style-type: none"> 电平：DI接入开-关时可触发报警模式。 计数：处于事件计数器模式 	ON-OFF
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	当模式为 Count 时，阈值是唯一参数。设置阈值，在计数值达到阈值时触发 DI 告警。	0
告警触发内容	警报打开时显示内容。	Alarm On
告警消除内容	警报关闭时显示内容。	Alarm Off

注：默认高电平告警，开启“反向”之后变成低电平告警。

DO

^ 常规设置

索引	<input type="text" value="3"/>
PHY模式	<input style="border: 1px solid #ccc;" type="text" value="DO"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
告警触发行为	<input style="border: 1px solid #ccc;" type="text" value="高电平"/>
告警消除行为	<input style="border: 1px solid #ccc;" type="text" value="低电平"/>
初始状态	<input style="border: 1px solid #ccc;" type="text" value="上一次"/>
延时	<input style="border: 1px solid #ccc;" type="text" value="0"/> ?
保持时间	<input style="border: 1px solid #ccc;" type="text" value="0"/> ?
由DI触发	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
告警源	<input style="border: 1px solid #ccc;" type="text" value="NONE"/>

选项	描述	默认值
索引	显示列表的序号。	--
PHY 模式	DO	--
启用	单击切换按钮以启用/禁用此 DO。	OFF
告警触发行为	数字输出在有警报时启动。从“高电平”、“低电平”或“脉冲”中选择。 <ul style="list-style-type: none"> 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规定的方波 	高电平
告警消除行为	数字输出在警报解除时启动。从“高电平”、“低电平”或“脉冲”中选择。 <ul style="list-style-type: none"> 高：高电平输出 低：低电平输出 脉冲：触发时生成脉冲模式参数中指定的方波 	低电平

选项	描述	默认值
初始状态	指定上电时的数字输出状态。从“上一次”、“高电平”或“低电平”中选择。 <ul style="list-style-type: none"> 最后：DO 的状态将包括上次断电状态 高：DO 接口处于高电平 低：DO 接口处于低电平 	上一次
延时 (单位: 100ms)	设置 DO 警报启动的延迟时间。第一个脉冲将在“延迟”后产生。输入从 0 到 3000 (0=无延迟生成脉冲)。	0
保持时间 (单位: s)	设置 DO 状态的保持时间 (报警操作/警报关闭操作)。当操作时间达到此指定时间时, DO 将停止操作。输入从 0 到 3000 秒。(0=保持打开, 直到下一个操作)	0
由 DI 触发	DO 的状态通过 DI 触发	OFF
告警源	数字输出激活可通过此警报激活。	None
低电平脉宽 (单位: ms)	设置低电平脉宽。它在启用脉冲为 "报警开动作/报警关动作 "时可用。在脉冲输出模式下, 选定的数字输出通道将产生脉冲模式参数中指定的方波。低电平宽度在此指定。从 1000 到 3000 输入。	1000
高电平脉宽 (单位: ms)	设置高电平脉宽。它在启用脉冲为 "报警开动作/报警关动作 "时可用。在脉冲输出模式下, 选定的数字输出通道将产生脉冲模式参数中指定的方波。高电平宽度在此指定。从 1000 到 3000 输入。	1000

状态

此窗口用于查看 DI/DO 接口的状态。它还可以清除此处 DI 的计数器警报。单击 **清除** 按钮以清除 DI 1 或 DI 2 使用情况统计信息，以进行计数器警报。单击 **切换** 按钮以切换电平输出。

DIDO

状态

^ DI状态

索引	Name	电平	状态	计数
1	DI1	Low	Alarm off	
2	DI2	Low	Alarm off	

^ DI计数器

	DI 1计数器告警	清除
	DI 2计数器告警	清除

^ DO状态

索引	Name	电平	低电平脉宽	高电平脉宽
1	D03	Low		
2	D04	Low		

^ DO控制器


	D03 电平	切换
	D04 电平	切换

3.3.8 串口

本节用于设置串口参数。设备可能支持两个串口，可以根据需要配置为 RS232 或 RS485。串行数据可以转换为 IP 数据或通过 IP 数据转换为串行数据，然后通过有线或无线网络进行传输，从而实现数据透明传输的功能。

串口

串口		状态			
^ 串口设置					
索引	端口	启用	Type	波特率	应用模式
1	COM1	false	RS232	115200	透传 
2	COM2	false	RS485	115200	透传 

单击  在弹出窗口中配置参数。

^ 串口应用设置	
索引	<input type="text" value="1"/>
端口	<input type="text" value="COM1"/> v
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Type	<input type="text" value="RS232"/> v
波特率	<input type="text" value="115200"/> v
数据位	<input type="text" value="8"/> v
停止位	<input type="text" value="1"/> v
校验位	<input type="text" value="无"/> v
流控	<input type="text" value="无"/> v

选项	描述	默认值
索引	显示列表的序号。	--
端口	显示当前序列号的名称	COM1
启用	单击切换按钮以启用/禁用此串行端口。当状态为 OFF 时，串行端口不可用。	OFF
Type	从“RS232”，“RS485”中选择。	RS232

选项	描述	默认值
波特率	从“300”、“600”、“1200”、“2400”、“4800”、“9600”、“19200”、“38400”、“57600”或“115200”中选择。	115200
数据位	从“7”或“8”中选择。	8
停止位	从“1”或“2”中选择。	1
校验位	从“无”、“奇校验”或“偶校验”中进行选择。	无
流控	从“无”、“软件”或“硬件”中进行选择。	无

^ 数据打包

打包超时时间	<input type="text" value="50"/>	?
打包数据长度	<input type="text" value="1200"/>	

选项	描述	默认值
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。当指定介于 1 和 3000 字节之间的数据包长度时，缓冲区中的数据将在达到指定长度后立即发送。	1200

在“服务器设置”列中，当选择“透传”作为应用程序模式，选择“TCP 客户端”作为协议时，窗口如下：

^ 服务器设置

应用模式	<input type="text" value="透传"/>
协议	<input type="text" value="TCP客户端"/>
服务器地址	<input type="text"/>
服务器端口	<input type="text"/>

当选择“透传”作为应用程序模式，选择“TCP 服务器”作为协议时，窗口如下所示：

^ 服务器设置

应用模式	<input type="text" value="透传"/>
协议	<input type="text" value="TCP服务器"/>
本地IP	<input type="text"/>
本地端口	<input type="text"/>

当选择“透传”作为应用程序模式并使用“UDP”作为协议时，窗口如下：

^ 服务器设置	
应用模式	<input type="text" value="透传"/> v
协议	<input type="text" value="UDP"/> v
本地IP	<input type="text"/>
本地端口	<input type="text"/>
服务器地址	<input type="text"/>
服务器端口	<input type="text"/>

当选择“Modbus RTU 网关”作为应用程序模式，选择“TCP 客户端”作为协议时，窗口如下：

^ 服务器设置	
应用模式	<input type="text" value="Modbus RTU网关"/> v
协议	<input type="text" value="TCP客户端"/> v
服务器地址	<input type="text"/>
服务器端口	<input type="text"/>

当选择“Modbus RTU 网关”作为应用程序模式，选择“TCP 服务器”作为协议时，窗口如下：

^ 服务器设置	
应用模式	<input type="text" value="Modbus RTU网关"/> v
协议	<input type="text" value="TCP服务器"/> v
本地IP	<input type="text"/>
本地端口	<input type="text"/>

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

^ 服务器设置	
应用模式	Modbus RTU网关 v
协议	UDP v
本地IP	<input type="text"/>
本地端口	<input type="text"/>
服务器地址	<input type="text"/>
服务器端口	<input type="text"/>

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

^ 服务器设置	
应用模式	Modbus ASCII网关 v
协议	TCP客户端 v
服务器地址	<input type="text"/>
服务器端口	<input type="text"/>

选择“Modbus ASCII 网关”作为应用程序模式，选择“TCP 服务器”作为协议时，窗口如下：

^ 服务器设置	
应用模式	Modbus ASCII网关 v
协议	TCP客户端 v
服务器地址	<input type="text"/>
服务器端口	<input type="text"/>

选择“Modbus ASCII 网关”作为应用程序模式，选择“UDP”作为协议时，窗口如下：

^ 服务器设置

应用模式	<input style="width: 90%;" type="text" value="Modbus ASCII网关"/>
协议	<input style="width: 90%;" type="text" value="UDP"/>
本地IP	<input style="width: 90%;" type="text"/>
本地端口	<input style="width: 90%;" type="text"/>
服务器地址	<input style="width: 90%;" type="text"/>
服务器端口	<input style="width: 90%;" type="text"/>

选项	描述	默认值
应用模式	从“透传”，“Modbus RTU 网关”或“Modbus ASCII 网关”中进行选择。 <ul style="list-style-type: none"> • 透传：网关将透明地传输未用任何协议封装的串行数据 • Modbus RTU网关：网关将Modbus RTU数据转换为Modbus TCP数据并发送出去，反之亦然 • Modbus ASCII 网关：网关会将Modbus ASCII数据转换为Modbus TCP数据并发送出去，反之亦然 	透传
协议	从“TCP 客户端”、“TCP 服务器”或“UDP”中进行选择。 <ul style="list-style-type: none"> • TCP客户端：网关作为TCP客户端，启动TCP服务器TCP连接。服务器地址同时支持 IP 和域名 • TCP服务器：网关作为TCP服务器，监听来自TCP客户端的连接请求 • UDP：网关用作 UDP 客户端 	TCP 客户端
服务器地址	输入将接收从网关串行端口发送的数据的服务器的地址。IP 地址或域名将可用。	空
服务器端口	输入用于接收串行数据的服务器的指定端口。	空
本地 IP@ Transparent	输入网关的 LAN IP，该 IP 将转发到网关的互联网端口。	空
本地端口@ Transparent	输入网关局域网 IP 的端口。	空
本地 IP @ Modbus	在 Modbus 模式下输入 的本地 IP。	空
本地端口 @ Modbus	在 Modbus 模式下输入 的本地端口。	空

状态

单击“状态”列以查看当前的串行端口状态。

串口		状态		
^ 串口状态				
索引	类型	发送	接收	连接状态
1	RS232	0B	0B	
2	RS485	0B	0B	

3.3.9 Packet Forwarder（LG5100 支持）

数据包转发器是一个运行在网关上的程序，它的作用是：1）与 LoRa 芯片互动，接收和传输 LoRa 数据包；2）与网络互动，为应用传输数据。

常规设置

通用设置		状态
^ 网关设置		
LoRa 模式	US915	v
使能	ON OFF	
网关 ID	001234567890ABCD	
服务器地址	127.0.0.1	
服务器上行端口	1700	
服务器下行端口	1700	

项目	描述	默认值
LoRa 模式	支持的 LoRa 频段，固定在设备中。	--
使能	点击切换按钮，启用或禁用该功能。	OFF
网关 ID	将网关ID设置为LoRaWAN网络服务器。	001234567890ABCD
服务器地址	设置LoRaWAN网络服务器地址。	127.0.0.1

项目	描述	默认值
服务器上行端口	设置上行链路端口至LoRaWAN网络服务器	1700
服务器下行端口	设置下行链路端口到LoRaWAN网络服务器。	1700

^ SX1302 板级设置

LoRaWAN 公共模式 ON OFF

全双工 ON OFF

时钟源 v

接口类型 v

设备节点路径 v

项目	描述	默认值
LoRaWAN 公共模式	启用或关闭使用公共的 LoRaWAN。	ON
全双工	点击切换按钮来启用或禁用该功能。	OFF
时钟源	时钟源，从 "0" 和 "1" 中选择。	--
接口类型	通信接口。	SPI 接口
设备节点路径	通信设备节点。	Spidev1.0

^ SX1302 射频链路0设置

链路0使能 ON OFF

射频频率

RSSI 偏移

无线芯片型号 v

发送链路使能 ON OFF

发送链路最小频率

发送链路最大频率

发送链路增益表 v

项目	描述	默认值
链路 0 使能	点击切换按钮来启用或禁用该功能。	ON
射频频率	LoRa通道0的中心频率。	100000000
RSSI 偏移	RSSI偏移值。	0

项目	描述	默认值
无线芯片型号	无线芯片选择, 从 "无"、"SX1250"、"SX1255"、"SX1257"、"SX1272"、"SX1276 "中选择。	SX1250
发送链路使能	点击切换按钮, 启用或禁用该功能。	ON
发送链路最小频率	传输最小频率。	100000000
发送链路最大频率	传输最大频率。	100000000
发送链路增益表	传输增益表。	EU433


^ SX1302 射频链路1设置

链路1使能	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
射频频率	<input type="text" value="100000000"/>
RSSI 偏移	<input type="text" value="0"/>
无线芯片型号	<input type="text" value="SX1250"/> v
发送链路使能	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
发送链路最小频率	<input type="text" value="100000000"/>
发送链路最大频率	<input type="text" value="100000000"/>
发送链路增益表	<input type="text" value="EU433"/> v

项目	描述	默认值
链路 1 使能	点击切换按钮来启用或禁用该功能。	ON
射频频率	LoRa通道1的中心频率。	100000000
RSSI 偏移	RSSI偏移值。	0
无线芯片型号	无线芯片选择, 从 "无"、"SX1250"、"SX1255"、"SX1257"、"SX1272"、"SX1276 "中选择。	SX1250
发送链路使能	点击切换按钮, 启用或禁用该功能。	ON
发送链路最小频率	传输最小频率。	100000000
发送链路最大频率	传输最大频率。	100000000
发送链路增益表	传输增益表。	EU433

^ SX1302 Multi Channels Settings

Index	RF Chain	IF Frequency	+

单击  以在弹出窗口中配置参数。

^ 多通道设置

索引	<input style="width: 90%;" type="text" value="1"/>
使能	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
射频链路	<input style="width: 90%;" type="text" value="射频链路0"/>
接口频率	<input style="width: 90%;" type="text" value="0"/>

项目	描述	默认值
索引	显示列表的序号。	--
使能	点击切换按钮，启用或禁用该功能。	ON
射频链路	选择链路0或链路1作为射频链路。	RF Chain 0
接口频率	特定通道的中心频率和射频链路 0/1 的中心频率之间的偏移量。例如：选择射频链路 0，偏移值：-200000，表示通道的中心频率是 $86300000=868500000-200000$ 。	0

^ SX1302 标准通道设置

使能	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
射频链路	<input style="width: 90%;" type="text" value="射频链路0"/>
接口频率	<input style="width: 90%;" type="text" value="0"/>
带宽	<input style="width: 90%;" type="text" value="500KHz"/>
扩频因子	<input style="width: 90%;" type="text" value="SF9"/>

项目	描述	默认值
使能	单击切换按钮以启用/禁用此功能。	OFF
射频链路	选择射频链路 0 或射频链路 1。	RF Chain 0
接口频率	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
带宽	选择可选的带宽，单位是 KHz。	500KHz
扩频因子	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

^ SX1302 FSK 通道设置

使能	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
射频链路	<input type="text" value="射频链路0"/> v
接口频率	<input type="text" value="0"/>
带宽	<input type="text" value="500KHz"/> v
数据速率	<input type="text" value="250000"/>

项目	描述	默认值
使能	点击切换按钮来启用/禁用该选项。	OFF
射频链路	选择链路0或链路1作为射频链路。	Chain 0
接口频率	输入中心频率，数值从-500000到500000，单位为Hz。特定通道的中心频率和射频链路的中心频率之间的偏移是0/1。	0
带宽	选择可选择的带宽，单位为KHz。	500KHz
数据速率	输入数据速率，从500到250000，单位为Bit。	250000

状态

此节可用于查看分组转发器的状态。

通用设置
状态

^ 基本信息

运行状态	initial successful
安装包版本 (协议)	1.0.4 (2)
硬件库版本	2.1.0

项目	描述
运行状态	显示你的网关的LoRaWAN状态。
安装包版本 (协议)	显示Packet forwarder的版本。
硬件库版本	显示网关内LoRaWAN芯片组的驱动版本。

3.3.10 LoRaWAN 基站（LG5100 支持）

LoRa 基站是一个 LoRaWAN 网关软件的实现，它在处理数据包流、管理频谱接入和 LNS 回程连接等方面提供这一核心功能。

常规设置

通用设置
状态

^ 网关设置

LoRa 模式

使能
 ON OFF

使能加密
 ON OFF

服务器地址

服务器端口

项目	描述	默认值
LoRa 模式	显示当前 LoRa 模式	US915
使能	启用应用程序	OFF
使能加密	启用 TLS 加密传输	OFF
服务器地址	服务器地址	127.0.0.1
服务器端口	服务器端口	3001

状态

本节可用于查看基站的状态。

通用设置

状态

^ 基本信息

运行状态 connected

软件版本 2.0.6

安装包版本 (协议) 2.0.4 (2)

硬件库版本 5.0.1

项目	描述
运行状态	平台连接状态
软件版本	应用程序版本
安装包版本 (协议)	应用程序包版本
硬件库版本	LoRaWAN HAL 库版本

3.4 虚拟专用网

3.4.1 IPsec

本节可用于设置 IPsec 和相关参数。互联网协议安全（IPsec）是用于安全互联网协议（IP）通信的协议套件，它的工作原理是对通信会话的每个 IP 数据包进行身份验证和加密。

常规设置

常规
隧道
状态

^ 常规设置

存活时间	<input style="width: 90%;" type="text" value="20"/>	?
优化DH指数大小	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	?
输出调试信息	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	
启用备份网关	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	

选项	描述	默认值
存活时间	设置存活时间，单位为秒。网关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。启用 IPsec VPN 信息输出到调试端口。	OFF
启用备份网关	单击切换按钮以启用/禁用此选项。	OFF

隧道

常规
隧道
状态

^ 隧道设置

索引	启用	描述	网关	本地子网	远端子网	+

单击 + 以添加 IPsecVPN 隧道。最多支持配置 6 条。

常规设置

^ 常规设置

索引	<input type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
描述	<input type="text"/>
链路绑定	<input type="text" value="v"/>
网关	<input type="text"/> ?
协议	<input style="width: 100%;" type="text" value="ESP"/>
模式	<input style="width: 100%;" type="text" value="隧道"/>
本地子网	<input type="text"/> ?
远端子网	<input type="text"/> ?
IKE类型	<input style="width: 100%;" type="text" value="IKEv1"/>
协商模式	<input style="width: 100%;" type="text" value="主模式"/>
初始模式	<input style="width: 100%;" type="text" value="保持连接"/>

选项	描述	默认值
索引	指示列表的序号。	--
启用	单击切换按钮以启用/禁用此 IPsec 隧道。	OFF
描述	输入此 IPsec 隧道的说明。	空
链路绑定	选择链接以生成IPSec。	不绑定
网关	输入远程端 IPsec VPN 服务器的地址。0.0.0.0 表示任何地址。	空
模式	可选“隧道”或“传输”。 <ul style="list-style-type: none"> • 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，如在工作站到网关之间建立加密的 Telnet 连接 	隧道
协议	可选“ESP”或“AH”作为安全协议。 <ul style="list-style-type: none"> • ESP：使用 ESP 协议 • AH：使用 AH 协议 	ESP
本地子网	输入受 IPsec 保护的掩码的本地子网地址，例如 192.168.1.0/24	空
远端子网	输入受 IPsec 保护的掩码的远程子网地址，例如 10.8.0.0/24	空
IKE 类型	从“IKEv1”和“IKEv2”中进行选择。	IKEv1
协商模式	从阶段 1 中的 IKE 协商模式的“主要”和“主动”中进行选择。如果 IPsec 隧道一端的 IP 地址是动态获取的，则 IKE 协商模式必须具有主动性。在这种情况下，只要用户名和密码正确，就可以建立 SA。	主模式

初始模式	从“始终打开”和“按需”中进行选择。	保持连接
------	--------------------	------

IKE 设置

^ IKE设置

启用压缩	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	
启用强制封装	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?	
备份网关	<input type="text"/>	?
专家选项	<input type="text"/>	?

选项	描述	默认值
启用压缩	点击切换按钮来启用/禁用该选项。启用以压缩IP数据包的内部头信息。	OFF
启用强制封装	即使没有检测到NAT情况，也强制对ESP数据包进行UDP封装，这可能有助于克服限制性防火墙。	OFF
备份网关	用于启动连接的远程对等体的备份地址，空意味着禁用。	空
专家选项	在这里添加更多的PPP配置选项，格式为： <code>config-desc; config-desc</code> ，例如： <code>protostack=netkey; plutodebug=none</code>	空

SA 设置

选择“PSK”作为身份验证类型时，窗口显示如下。

^ SA设置

认证方法	<input type="text" value="3DES"/>	v
加密算法	<input type="text" value="SHA1"/>	v
IKE DH分组	<input type="text" value="DHgroup2"/>	v
认证类型	<input type="text" value="PSK"/>	v
PSK密钥	<input type="text"/>	
本地ID类型	<input type="text" value="默认"/>	v
远程ID类型	<input type="text" value="默认"/>	v
IKE存活时间	<input type="text" value="86400"/>	?

选择“CA”作为身份验证类型时，窗口显示如下。

^ SA设置	
认证方法	3DES
加密算法	SHA1
IKE DH分组	DHgroup2
认证类型	CA
本地证书	None
对端证书(Optional)	None
私钥	None
根证书	None
密匙密码	
IKE存活时间	86400

选择“PKCS#12”作为身份验证类型时，窗口显示如下。

^ SA设置	
认证方法	3DES
加密算法	SHA1
IKE DH分组	DHgroup2
认证类型	PKCS#12
对端证书(Optional)	None
PKCS#12证书	None
密匙密码	
IKE存活时间	86400

选择“xAuth PSK”作为身份验证类型时，窗口显示如下。

^ SA设置	
认证方法	3DES v
加密算法	SHA1 v
IKE DH分组	DHgroup2 v
认证类型	xAuth PSK v
PSK密钥	<input type="text"/>
本地ID类型	默认 v
远程ID类型	默认 v
用户名	<input type="text"/> ?
密码	<input type="text"/> ?
IKE存活时间	86400 ?

选择“xAuth CA”作为身份验证类型时，窗口显示如下。

^ SA设置	
认证方法	3DES v
加密算法	SHA1 v
IKE DH分组	DHgroup2 v
认证类型	xAuth CA v
本地证书	None v
对端证书(Optional)	None v
私钥	None v
根证书	None v
密匙密码	<input type="text"/>
用户名	<input type="text"/> ?
密码	<input type="text"/> ?
IKE存活时间	86400 ?

选项	描述	默认值
加密算法	从“3DES”、“AES128”、“AES192”、“AES256”、“AES128-GCM8”、“AES192-GCM8”、“AES256-GCM8”、“AES128-GCM12”、“AES192-GCM12”、“AES256-GCM12”、“AES128-GCM18”、“AES192-GCM18”和“AES256-GCM18”中进行选择。	3DES
认证方法	从“MD5”、“SHA1”、“SHA2 256”、“SHA2 384”或“SHA2 512”中选择。	SHA1
IKE DH 分组	从“DHgroup1”、“DHgroup2”、“DHgroup5”、“DHgroup14”、“DHgroup15”、“DHgroup16”、“DHgroup17”或“DHgroup18”中选择。	DHgroup2
认证类型	从“PSK”、“CA”、“xAuth PSK”、“PKCS#12”和“xAuth CA”中选择用于 IKE 协商。 PSK: 预共享密钥 CA: 证书颁发机构 xAuth: 将身份验证扩展到 AAA 服务器 PKCS#12: 交换数字证书身份验证	PSK
PSK 密钥	输入预共享密钥。	空
本地 ID 类型	从“默认”、“地址”、“FQDN”和“用户 FQDN”中进行选择。 默认值: 在 IKE 协商中使用 IP 地址作为 ID FQDN: 在 IKE 协商中使用 FQDN 类型作为 ID。如果选择此选项, 请键入本地安全网关的名称, 不带任何 at 符号 (@), 例如, test.robustel.com 用户 FQDN: 使用用户 FQDN 类型作为 IKE 协商中的 ID。如果选择此选项, 请键入一个带有符号“@”的名称字符串, 表示本地安全网关, 例如, test@robustel.com	默认
远程 ID 类型	从“默认”、“FQDN”和“用户 FQDN”中进行选择以进行 IKE 协商。 默认值: 在 IKE 协商中使用 IP 地址作为 ID FQDN: 在 IKE 协商中使用 FQDN 类型作为 ID。如果选择此选项, 请键入本地安全网关的名称, 不带任何 at 符号 (@), 例如, test.robustel.com 用户 FQDN: 使用用户 FQDN 类型作为 IKE 协商中的 ID。如果选择此选项, 请键入一个带有符号“@”的名称字符串, 表示本地安全网关, 例如, test@robustel.com	默认
IKE 存活时间	在 IKE 协商中设置生存期。在 SA 到期之前, IKE 协商一个新的 SA。设置新的 SA 后, 它将立即生效, 旧 SA 将在过期时自动清除。	86400
私钥	在“CA”和“xAuth CA”身份验证类型下输入私钥。	空
用户名	输入用于“xAuth PSK”和“xAuth CA”身份验证类型的用户名。	空
密码	输入用于“xAuth PSK”和“xAuth CA”身份验证类型的密码。	空

高级设置

^ 高级设置

加密算法	<input style="width: 100%;" type="text" value="3DES"/>	v
认证方法	<input style="width: 100%;" type="text" value="SHA1"/>	v
PFS组	<input style="width: 100%;" type="text" value="PFS(N/A)"/>	v
SA存活时间	<input style="width: 100%;" type="text" value="28800"/>	?
DPD间隔	<input style="width: 100%;" type="text" value="30"/>	?
DPD失败时间	<input style="width: 100%;" type="text" value="150"/>	?

选项	描述	默认值
加密算法	当您在“协议”中选择“ESP”时，从“3DES”、“AES128”、“AES192”、“AES256”、“AES128-GCM8”、“AES192-GCM8”、“AES256-GCM8”、“AES128-GCM12”、“AES192-GCM12”、“AES256-GCM12”、“AES128-GCM18”、“AES192-GCM18”和“AES256-GCM18”中进行选择。更高的安全性意味着更复杂的实施和更低的速度。DES 足以满足一般要求。当需要高机密性和安全性时，请使用 3DES。	3DES
认证方法	从“MD5”、“SHA1”、“SHA2 256”或“SHA2 512”中选择用于 SA 协商。	SHA1
PFS 组	从“PFS(N/A)”、“DHgroup1”、“DHgroup2”、“DHgroup5”、“DHgroup14”、“DHgroup15”、“DHgroup16”、“DHgroup17”或“DHgroup18”中选择用于 SA 协商。	DHgroup2
SA 存活时间	设置 IPsec SA 生存期。协商设置 IPsec SA 时，IKE 使用本地设置的生存期与对等方建议的生存期之间的较小一个。	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 包回传时间间接个内未接收到 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 失败时间	设置 DPD（失效对等体检测）数据包的超时。单位：秒	150

状态

此节用于查看 IPsec 隧道的状态。

常规	隧道	状态
----	----	----

^ IPsec隧道状态

索引	描述	状态	运行时间

3.4.2 OpenVPN

此节用于设置 OpenVPN 相关参数。OpenVPN 是一个开源的软件应用程序，可以创建安全的点对点或站点对站点的连接。

OpenVPN

OpenVPN	状态
---------	----

^ 隧道设置

索引	启用	描述	模式	对端地址	+

^ 用户密码管理

索引	用户名	+

^ 客户端管理

索引	启用	常用名	客户端IP地址	+

隧道设置

单击 **+** 以添加 OpenVPN 隧道设置。最大计数为 6。当选择不同的模式时，配置页面可能会有所不同，而认证类型可能会在特定模式下固定使用。默认情况下，模式为“P2P”。选择“P2P”作为模式时，窗口显示如下。

常规设置

索引	<input type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
启用IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
描述	<input type="text"/>
模式	<input type="text" value="P2P"/> ?
TLS模式	<input type="text" value="无"/> ?
协议	<input type="text" value="UDP"/>
对端地址	<input type="text"/>
对端端口	<input type="text" value="1194"/>
监听地址	<input type="text"/>
监听端口	<input type="text" value="1194"/>
接口类型	<input type="text" value="TUN"/>
验证方式	<input type="text" value="无"/> ?
本地IP	<input type="text" value="10.8.0.1"/>
远端IP	<input type="text" value="10.8.0.2"/>
保活间隔时间	<input type="text" value="20"/> ?
保活超时时间	<input type="text" value="120"/> ?
隧道MTU	<input type="text" value="1500"/>
数据分片	<input type="text"/>
启用压缩	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
启用NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
日志信息级别	<input type="text" value="0"/> ?

选择“客户端”作为模式时，窗口显示如下。

常规设置

索引	<input type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
描述	<input type="text"/>
模式	<input type="text" value="客户端"/> ?
协议	<input type="text" value="UDP"/>
对端地址	<input type="text"/>
对端端口	<input type="text" value="1194"/>
接口类型	<input type="text" value="TUN"/>
验证方式	<input type="text" value="无"/> ?
重新协商间隔	<input type="text" value="86400"/> ?
保活间隔时间	<input type="text" value="20"/> ?
保活超时时间	<input type="text" value="120"/> ?
隧道MTU	<input type="text" value="1500"/>
数据分片	<input type="text"/>
启用压缩	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
启用NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
接收DNS推送	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
日志信息级别	<input type="text" value="0"/> ?

选择“服务器”作为模式时，窗口显示如下。

常规设置

索引	<input type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
启用IPv6	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
描述	<input type="text"/>
模式	<input type="text" value="服务器"/> ?
协议	<input type="text" value="UDP"/>
监听地址	<input type="text"/>
监听端口	<input type="text" value="1194"/>
接口类型	<input type="text" value="TUN"/>
启用IP地址池	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
客户端网络	<input type="text" value="10.8.0.0"/>
客户端网络掩码	<input type="text" value="255.255.255.0"/>
重新协商间隔	<input type="text" value="86400"/> ?
最大客户端数量	<input type="text" value="10"/>
保活间隔时间	<input type="text" value="20"/> ?
保活超时时间	<input type="text" value="120"/> ?
隧道MTU	<input type="text" value="1500"/>
数据分片	<input type="text"/>
启用压缩	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
启用默认网关	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
启用NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
日志信息级别	<input type="text" value="0"/> ?

选择“无”作为身份验证类型时，窗口显示如下。

监听地址	<input type="text"/>
监听端口	<input type="text" value="1194"/>
接口类型	<input type="text" value="TUN"/>
验证方式	<input type="text" value="无"/> ?
启用IP地址池	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
客户端网络	<input type="text" value="10.8.0.0"/>
客户端网络掩码	<input type="text" value="255.255.255.0"/>
重新协商间隔	<input type="text" value="86400"/> ?

选择“预共享”作为身份验证类型时，窗口显示如下。

监听地址	<input type="text"/>
监听端口	<input type="text" value="1194"/>
接口类型	<input type="text" value="TUN"/>
验证方式	<input type="text" value="预共享密钥"/> ?
预共享密钥	<input type="text" value="None"/>
启用IP地址池	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
客户端网络	<input type="text" value="10.8.0.0"/>
客户端网络掩码	<input type="text" value="255.255.255.0"/>
加密算法	<input type="text" value="BF"/>
验证算法	<input type="text" value="SHA1"/>

选择“密码”作为身份验证类型时，窗口显示如下。

监听地址	<input type="text"/>
监听端口	<input type="text" value="1194"/>
接口类型	<input type="text" value="TUN"/>
验证方式	<input type="text" value="密码"/> ?
启用IP地址池	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
客户端网络	<input type="text" value="10.8.0.0"/>
客户端网络掩码	<input type="text" value="255.255.255.0"/>
加密算法	<input type="text" value="BF"/>
验证算法	<input type="text" value="SHA1"/>
重新协商间隔	<input type="text" value="86400"/> ?

选择“X509CA”作为身份验证类型时，窗口显示如下。

监听地址	<input type="text"/>
监听端口	<input type="text" value="1194"/>
接口类型	<input type="text" value="TUN"/>
验证方式	<input type="text" value="X509证书"/> ?
根证书	<input type="text" value="None"/>
证书文件	<input type="text" value="None"/>
私钥	<input type="text" value="None"/>
DH	<input type="text" value="None"/>
私钥密码	<input type="text"/>
启用IP地址池	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

选项	描述	默认值
索引	显示列表的序号。	--
启用	单击切换按钮以启用/禁用此 OpenVPN 隧道。	ON
启用 IPv6	单击切换按钮以启用/禁用 IPv6。	OFF
描述	输入此 OpenVPN 隧道的描述。	空
模式	从“P2P”，“客户端”或“服务器”中选择。	P2P
TLS 模式	从“无”、“客户端”或“服务器”中进行选择。	None
协议	从“UDP”、“TCP 客户端”或“TCP 服务器”中进行选择。	UDP
对端地址	输入远程 OpenVPN 服务器的端到端 IP 地址或域。	空
对端串口	输入 OpenVPN 服务器的端到端侦听器端口或侦听器端口。	1194
监听地址	输入 IP 地址或域名。	空
监听端口	在此端输入侦听器端口。	1194
接口类型	从“TUN”，“TAP”中选择，这是 OpenVPN 的两种不同类型的设备接口。TUN 和 TAP 设备之间的区别在于，TUN 设备是网络上的点对点虚拟设备，而 TAP 设备是以太网上的虚拟设备。	TUN
私钥	在“X509CA”和“X509CA 密码”身份验证下输入私钥密码。	空
本地 IP	输入本地虚拟 IP。	10.8.0.1
远端 IP	输入远程虚拟 IP。	10.8.0.2
加密算法	从“BF”，“DES”，“DES-EDE3”，“AES-128”，“AES-192”和“AES-256”中选择。 <ul style="list-style-type: none"> • BF: 在 CBC 模式下使用 128 位 BF 加密算法 • DES: 在 CBC 模式下使用 64 位 DES 加密算法 • DES-EDE3: 在 CBC 模式下使用 192 位 3DES 加密算法 • AES128: 在 CBC 模式下使用 128 位 AES 加密算法 • AES192: 在 CBC 模式下使用 192 位 AES 加密算法 • AES256: 在 CBC 模式下使用 256 位 AES 加密算法 	BF
身份认证	从“MD5”，“SHA1”，“SHA256”或“SHA512”中进行选择。	SHAI
保活间隔时间	设置保持活动（ping）间隔以检查隧道是否处于活动状态。	20
保活超时时间	设置保持活动超时。在 n 秒过去后触发 OpenVPN 重新启动，而不会收到来自远程的 ping 或其他数据包。	120
隧道 MTU	设置隧道的 MTU。	1500
数据分片	设置要通过隧道传输的数据的分片大小。	空
启用压缩	单击切换按钮以启用/禁用此选项。启用后，此功能将压缩 IP 数据包的标头。	ON
启用 NAT	单击切换按钮以启用/禁用 NAT 选项。启用后，网关后面的主机的源 IP 地址将在访问远程 OpenVPN 客户端之前被伪装。	OFF
日志信息级别	选择输出日志的级别和值（从 0 到 11）。 <ul style="list-style-type: none"> • 0: 除致命错误外无输出 • 1~4: 正常使用范围 • 5: 将每个数据包的读写输出到控制台 • 6~11: 调试信息范围 	0

^ 高级设置

专家选项



选项	描述	默认值
专家选项	在此字段中输入 OpenVPN 的其他一些选项。每个表达式都可以用“;”分隔。	空

客户端管理

^ 客户端管理


索引

启用

常用名

客户端IP地址



单击  以添加客户端信息。最多支持配置 20 条。

^ 常规设置

索引

启用

 ON OFF

常用名



客户端IP地址

选项	描述	默认值
索引	显示列表的序号。	--
启用	单击切换按钮以启用/禁用此选项。	ON
常用名	指定客户端的公用名。	空
客户端 IP 地址	指定客户端的虚拟 IP 地址。	空

状态

本节用于查看 OpenVPN 隧道的状态。

OpenVPN		状态				
^ 隧道状态						
索引	描述	状态	模式	运行时间	本地IP	本地IPv6地址
^ 客户端列表						
索引	常用名	真实IP地址	端口号	虚拟IP地址	虚拟IPv6地址	

3.4.3 GRE

本节用于设置 GRE 参数。通用路由封装（GRE）是一种隧道协议，可以在互联网协议网络的虚拟点对点链接内封装各种网络层协议。GRE 协议有两个主要用途：内部协议封装和私有地址封装。

GRE

^ GRE隧道				
索引	启用	描述	远端IP地址	+

单击  以添加隧道。最多支持配置 6 条。

^ 隧道设置	
索引	<input type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
描述	<input type="text"/>
远端IP地址	<input type="text"/>
本地虚拟IP地址	<input type="text"/>
本地虚拟子网掩码	<input type="text"/> 
远端虚拟IP地址	<input type="text"/>
启用默认路由	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

启用NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
密码	<input type="text"/>
链路绑定	<input type="text" value="v"/>

选项	描述	默认值
索引	显示列表的序号。	--
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	输入此 GRE 隧道的描述。	空
远端 IP 地址	设置 GRE 隧道的远程真实 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 隧道的本地虚拟网络掩码。	空
远程虚拟 IP 地址	设置 GRE 隧道的远程虚拟 IP 地址。	空
启用默认路由	单击切换按钮以启用/禁用此选项。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/禁用此选项。在 NAT 环境下进行网关时，必须启用此选项。	OFF
密码	设置 GRE 隧道的密钥。	空
链路绑定	选择绑定的链路	空

状态

本节可用于查看 GRE 隧道状态。

^ GRE隧道状态					
索引	描述	状态	本地IP地址	远端IP地址	运行时间

3.4.4 PPTP

本节用于设置 PPTP 的参数, PPTP 是一种 VPN 协议, 它使用 TCP 控制通道和通用路由封装隧道来封装 PPP 数据包。

常规设置

常规	PPTP服务器	PPTP客户端	状态
----	---------	---------	----

^ 常规设置

启用户LED ON OFF 

选项	描述	默认值
启用户 LED	单击切换按钮以启用/禁用用户 LED。如果在此处启用户 LED, 它将具有更高的优先级。	OFF

PPTP 服务器

常规

PPTP服务器

PPTP客户端

状态

^ PPTP服务器配置

启用 ON OFF

用户名 ?

密码 ?

本地IP地址

地址池起始IP地址

地址池结束IP地址

认证类型 v

使能NAT ON OFF

专家选项


输出调试信息 ON OFF

^ 静态路由

索引	对端子网	对端子网掩码	对端IP地址	
				+

选项	描述	默认值
启用 PPTP 服务器	单击切换按钮以启用/禁用 PPTP 服务器。	OFF
用户名	输入 PPTP 服务器的名称。	空
密码	输入 PPTP 服务器的密码。	空
本地 IP 地址	此 PPTP 网络接口的 IP 地址。	空
地址池起始 IP 地址	PPTP IP 地址租约将从此字段中指定的地址开始。	空
地址池结束 IP 地址	PPTP IP 地址租约将以此字段中指定的地址结束。	空
认证类型	从“pap”，“chap”，“mschap v1”，“mschap v2”中选择。	pap
使能 NAT	单击切换按钮以启用/禁用 NAT。	ON
专家选项	在此字段中输入 PPTP 的其他一些选项。每个表达式都可以用“;”分隔。	空
输出调试信息	单击切换按钮以启用/禁用调试。	OFF

^ 静态路由			
索引	对端子网	对端子网掩码	对端IP地址

单击  为 PPTP 服务器添加静态路由。最多支持配置 20 条。

^ 静态路由	
索引	<input type="text" value="1"/>
描述	<input type="text"/>
对端子网	<input type="text"/>
对端子网掩码	<input type="text"/>
对端IP地址	<input type="text"/> 

选项	描述	默认值
索引	指示列表的序号。	--
描述	输入此静态路由的说明。	空
对端子网	输入远程子网的地址。	空
对端子网掩码	输入子网地址的远程掩码。	空
对端 IP 地址	输入客户端 IP，空表示任何地方。	空

PPTP 客户端

常规	PPTP服务器	PPTP客户端	状态
----	---------	----------------	----

^ PPTP客户端配置						
索引	启用	描述	服务器地址	认证类型	对端子网	对端子网掩码

单击 **+** 以添加 PPTP 客户端。最多支持配置 6 条。

^ PPTP客户端配置

索引	<input style="width: 90%;" type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
描述	<input style="width: 90%;" type="text"/>
服务器地址	<input style="width: 90%;" type="text"/>
用户名	<input style="width: 90%;" type="text"/> ?
密码	<input style="width: 90%;" type="password"/> ?
认证类型	<input style="width: 90%;" type="text" value="pap"/> v
使能NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
此接口作为默认网关	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
对端子网	<input style="width: 90%;" type="text"/>
对端子网掩码	<input style="width: 90%;" type="text"/>
专家选项	<input style="width: 90%;" type="text" value="noaccomp nopcomp nodeflate nobsdcomp n"/>

选项	描述	默认值
索引	显示列表的序号。	--
启用	单击切换按钮以启用/禁用 PPTP 客户端。	ON
服务器地址	输入 PPTP 服务器的 IP 地址或主机名。	
用户名	输入 PPTP 服务器的名称	空
密码	输入 PPTP 服务器的密码	空
认证类型	从“pap”，“chap”，“mschap v1”，“mschap v2”中选择。	pap
启用 NAT	单击切换按钮以启用/禁用 NAT。	ON
此接口作为默认网关	单击切换按钮以启用/禁用此功能。	OFF
远程子网地址	输入远程子网地址。	空
远程子网地址掩码	输入远程子网地址掩码。	空
专家选项	在此字段中输入 PPTP 的其他一些选项。每个表达式都可以用“;”分隔。	空

状态

状态栏用于查看 PPTP 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下方。

常规
PPTP服务器
PPTP客户端
状态

^ PPTP服务器状态

索引	对端IP地址	在线时间

^ PPTP客户端状态

索引	描述	状态	本地IP地址	对端IP地址	在线时间

3.4.5 L2TP

L2TP 是一种用于支持虚拟专用网络的隧道协议。它比 PPTP 更安全，因为它将传输的数据封装两次，但它的速度较慢，并且使用更多的 CPU 功率。

常规设置

常规
L2TP服务器
L2TP客户端
状态

^ 常规设置

启用户LED

 ON
 OFF
 ?

选项	描述	默认值
启用户 LED	单击切换按钮以启用/禁用用户 LED。如果在此处启用户 LED，它将具有更高的优先级。	OFF

L2TP 服务器

常规
L2TP服务器
L2TP客户端
状态

^ L2TP服务器配置

启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	
用户名	<input type="text"/>	?
密码	<input type="password"/>	?
本地IP地址	<input type="text"/>	
地址池起始IP地址	<input type="text"/>	
地址池结束IP地址	<input type="text"/>	
隧道密钥	<input type="text"/>	
认证类型	<input type="text" value="pap"/>	v
端口号	<input type="text" value="1701"/>	
使能NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	
专家选项	<input type="text" value="noaccomp nopcomp nodeflate nobsdcomp n"/>	
输出调试信息	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	

选项	描述	默认值
启用 L2TP 服务器	单击切换按钮以启用/禁用 L2TP 服务器。	OFF
用户名	输入 L2TP 服务器的名称	空
密码	输入 L2TP 服务器的密码	空
本地 IP 地址	此 L2TP 网络接口的 IP 地址。	
地址池起始 IP 地址	L2TP IP 地址租约将从此字段中指定的地址开始。	
地址池结束 IP 地址	L2TP IP 地址租约将以此字段中指定的地址结束。	
隧道密钥	输入隧道密码。	
认证类型	从“pap”，“chap”，“mschap v1”，“mschap v2”中选择。	pap
端口号	输入此隧道的端口。	1701
使能 NAT	单击切换按钮以启用/禁用 NAT。	ON
专家选项	在此字段中输入 L2TP 的其他一些选项。每个表达式都可以用“;”分隔。	空
输出调试信息	单击切换按钮以启用/禁用调试。	OFF

^ 静态路由			
索引	对端子网	对端子网掩码	对端IP地址
+			

单击 **+** 为 L2TP 服务器添加静态路由。最多支持配置 20 条。

^ 静态路由	
索引	<input type="text" value="1"/>
描述	<input type="text"/>
对端子网	<input type="text"/>
对端子网掩码	<input type="text"/>
对端IP地址	<input type="text"/> ?

选项	描述	默认值
索引	指示列表的序号。	--
描述	输入此 L2TP 服务器的描述。	空
对端子网	输入远程子网地址	空
对端子网掩码	输入远程子网地址掩码	空
对端 IP 地址	输入客户端 IP	空

L2TP 客户端

常规	L2TP服务器	L2TP客户端	状态				
^ L2TP客户端配置							
索引	启用	描述	服务器地址	认证类型	对端子网	对端子网掩	
+							

单击 **+** 以添加 L2TP 客户端。最多支持配置 3 条。

^ L2TP客户端配置

索引	<input style="width: 90%;" type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
描述	<input style="width: 90%;" type="text"/>
服务器地址	<input style="width: 90%;" type="text"/>
用户名	<input style="width: 90%;" type="text"/> ?
密码	<input style="width: 90%;" type="text"/> ?
认证类型	<input type="text" value="pap"/> v
隧道密钥	<input style="width: 90%;" type="text"/>
端口号	<input style="width: 90%;" type="text" value="1701"/>
使能NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
此接口作为默认网关	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
对端子网	<input style="width: 90%;" type="text"/>
对端子网掩	<input style="width: 90%;" type="text"/>
专家选项	<input style="width: 90%;" type="text" value="noaccomp nopcomp nodeflate nobsdcomp n"/>

选项	描述	默认值
索引	指示列表的序号。	--
启用	单击切换按钮以启用/禁用 PPTP 客户端。	ON
描述	输入此 L2TP 客户端的描述。	空
服务器地址	输入 L2TP 服务器的 IP 地址或主机名。	空
用户名	输入 PPTP 服务器的名称	空
密码	输入 PPTP 服务器的密码	空
认证类型	从“pap”，“chap”，“mschap v1”，“mschap v2”中选择。	pap
隧道密码	输入隧道密码。	空
启用 NAT	单击切换按钮以启用/禁用 NAT。	ON
此接口作为默认网关	单击切换按钮以启用/禁用此功能。	OFF
远程子网地址	输入远程子网地址。	空
远程子网地址掩码	输入远程子网地址掩码。	空
专家选项	在此字段中输入 PPTP 的其他一些选项。每个表达式都可以用“;”分隔。	空

状态

状态栏用于查看 L2TP 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下方。

常规	L2TP服务器	L2TP客户端	状态												
<div style="background-color: #333; color: white; padding: 2px;">^ L2TP服务器状态</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">索引</th> <th style="width: 40%;">对端IP地址</th> <th style="width: 50%;">在线时间</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>				索引	对端IP地址	在线时间									
索引	对端IP地址	在线时间													
<div style="background-color: #333; color: white; padding: 2px;">^ L2TP客户端状态</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">索引</th> <th style="width: 15%;">描述</th> <th style="width: 10%;">状态</th> <th style="width: 15%;">本地IP地址</th> <th style="width: 20%;">对端IP地址</th> <th style="width: 30%;">在线时间</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>				索引	描述	状态	本地IP地址	对端IP地址	在线时间						
索引	描述	状态	本地IP地址	对端IP地址	在线时间										

3.5 服务

3.5.1 系统日志

本节用于设置系统日志参数。网关的系统日志可以保存在本地，也支持发送到远程日志服务器和指定的应用程序调试。默认情况下，“记录到远程”选项处于禁用状态。

系统日志								
<div style="background-color: #333; color: white; padding: 2px;">^ 系统日志设置</div> <table style="width: 100%;"> <tr> <td style="width: 30%;">启用</td> <td><input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF</td> </tr> <tr> <td>系统日志级别</td> <td><input style="width: 100%;" type="text" value="调试"/></td> </tr> <tr> <td>保存位置</td> <td><input style="width: 100%;" type="text" value="RAM"/> ?</td> </tr> <tr> <td>记录到远程</td> <td><input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?</td> </tr> </table>	启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	系统日志级别	<input style="width: 100%;" type="text" value="调试"/>	保存位置	<input style="width: 100%;" type="text" value="RAM"/> ?	记录到远程	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF							
系统日志级别	<input style="width: 100%;" type="text" value="调试"/>							
保存位置	<input style="width: 100%;" type="text" value="RAM"/> ?							
记录到远程	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?							

启用“记录到远程”选项时，窗口显示如下。

系统日志

^ 系统日志设置

启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	
系统日志级别	<input type="text" value="调试"/>	v
保存位置	<input type="text" value="RAM"/>	v ?
记录到远程	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	?
添加标识符	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	?
远程IP地址	<input type="text"/>	
远程端口	<input type="text" value="514"/>	

选项	描述	默认值
启用	单击切换按钮以启用/禁用系统日志设置选项。	ON
系统日志级别	从“调试”，“信息”，“通知”，“警告”或“错误”中选择，从低到高。较低级别将详细输出更多系统日志。	调试
保存位置	从“RAM”，“NVM”或“控制台”中选择保存位置。重新启动后，选择“RAM”时，数据将被清除。	RAM
记录到远程	单击切换按钮以启用/禁用此选项。启用此选项可允许网关将系统日志发送到远程系统日志服务器。您需要输入系统日志服务器的 IP 和端口。	OFF
添加标识符	单击切换按钮以启用/禁用此选项。启用后，您可以将序列号添加到用于将系统日志加载到 RCMS 的系统日志消息中。	OFF
远程 IP 地址	启用“记录到远程”选项时，输入系统日志服务器的 IP 地址。	空
远程端口	启用“记录到远程”选项时，输入系统日志服务器的端口。	514

3.5.2 事件

本节用于设置事件参数。事件功能提供了在发生某些系统事件时通过短信或电子邮件发送警报的功能。

事件

事件
通知
查询

^ 常规设置

信号质量门限

0

?

温度门限

0

?

选项	描述	默认值
信号质量门限	设置信号质量的阈值。当实际阈值小于指定的阈值时，网关将生成日志事件。0 表示禁用此选项。	0
温度门限	设置温度阈值。当实际阈值小于指定的阈值时，网关将生成日志事件。0 表示禁用此选项。	0

通知

事件
通知
查询

^ 事件通知群组设置

索引	描述	发送SMS	发送Email	DO控制	保存到NVM	+

单击  按钮添加事件参数。

^ 常规设置

索引	<input style="width: 100%;" type="text" value="1"/>
描述	<input style="width: 100%;" type="text"/>
发送SMS	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
发送Email	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DO控制	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
保存到NVM	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?

选项	描述	默认值
索引	显示列表的序号。	--
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。启用后，如果发生事件，网关将通过短信向指定的电话号码发送通知。在“3.21 服务>短信”中设置相关电话号码，并使用“;”以分隔每个数字。	OFF
发送 Email	单击切换按钮以启用/禁用此选项。启用后，如果发生事件，网关将通过电子邮件向指定的电子邮箱发送通知。在“3.21 服务>电子邮件”中设置相关电子邮件地址。	OFF
DO 控制	单击切换按钮以启用/禁用此选项。打开后，事件网关会以低/高级别的形式将其发送到相应的 DO。	OFF
保存到 NVM	单击切换按钮以启用/禁用此选项。启用此选项可将事件保存到非易失性存储器。	OFF

^ 事件选择 ?

系统启动	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
系统重启	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
系统时间更新	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
参数变化	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
蜂窝网络类型变化	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
蜂窝统计数据清除	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
蜂窝网超流量	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
信号质量差	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN数据统计清除	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN数据流量溢出	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
链路切换	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN连接成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN连接断开	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WLAN连接成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WLAN连接断开	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WWAN连接成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WWAN连接断开	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
IPSec连接成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
IPSec连接断开	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

OpenVPN连接成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
OpenVPN连接失败	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LAN端口Link Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LAN端口Link Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
USB设备插入	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
USB设备移除	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DDNS更新成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DDNS更新失败	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
收到短信	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
收到并执行短信管理命令	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 1 告警	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 1 告警消除	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 1计数器溢出	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 2 告警	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 2 告警消除	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 2 计数器溢出	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
高温告警	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

选项	描述	默认值
事件	单击切换按钮以启用此选项以生成事件。	OFF

查询

在以下窗口中，您可以查询各种类型的事件记录。单击 **清除** 查询已过滤的事件，同时单击 **刷新** 清除窗口中的事件记录。

事件
通知
查询

^ 事件记录

储存位置 RAM v

过滤

```

Jan 01 03:06:16, switch link, from WWAN1 to WWAN2
Jan 01 03:09:20, switch link, from WWAN2 to WWAN1
Jan 01 03:12:13, LAN port link up, eth0
Jan 01 03:12:23, switch link, from WWAN1 to WWAN2
Jan 01 03:15:26, switch link, from WWAN2 to WWAN1
Jan 01 03:18:29, switch link, from WWAN1 to WWAN2
Jan 01 03:21:32, switch link, from WWAN2 to WWAN1
Jan 01 03:24:35, switch link, from WWAN1 to WWAN2
Jan 01 03:24:47, LAN port link down, eth0
Jan 01 03:27:38, switch link, from WWAN2 to WWAN1
Jan 01 03:28:00, LAN port link up, eth0
Jan 01 03:30:41, switch link, from WWAN1 to WWAN2
Jan 01 03:33:44, switch link, from WWAN2 to WWAN1
Jan 01 03:36:47, switch link, from WWAN1 to WWAN2
Jan 01 03:39:50, switch link, from WWAN2 to WWAN1
Jan 01 03:42:53, switch link, from WWAN1 to WWAN2
Jan 01 03:45:56, switch link, from WWAN2 to WWAN1
Jan 01 03:48:59, switch link, from WWAN1 to WWAN2
Jan 01 03:52:02, switch link, from WWAN2 to WWAN1
Jan 01 03:55:05, switch link, from WWAN1 to WWAN2
          
```

清除
刷新

选项	描述	默认值
储存位置	从“RAM”或“NVM”中选择事件的保存位置。 RAM: 随机存取存储器 NVM: 非易失性存储器	RAM
过滤	根据用户设置的关键字输入过滤消息。单击“刷新”按钮，过滤后的事件将显示在下面的框中。使用“&”分隔多个筛选器消息，例如 message1&message2。	空

3.5.3 NTP

本节用于设置相关的 NTP（网络时间协议）参数。

NTP

NTP	状态
<div style="background-color: #333; color: white; padding: 5px;">^ 时区设置</div> <div style="padding: 10px;"> 时区 <input type="text" value="亚洲-上海"/> </div>	

选项	描述	默认值
时区地址	单击下拉列表以选择您所在的时区。	亚洲-上海

^ NTP客户端设置	
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
首选NTP服务器	<input type="text" value="pool.ntp.org"/>
备用NTP服务器	<input type="text"/>
NTP更新间隔	<input type="text" value="0"/> ?

选项	描述	默认值
启用	单击切换按钮以启用/禁用此选项。启用此选项可与 NTP 服务器同步时间。	ON
首选 NTP 服务器	输入主 NTP 服务器的 IP 地址或域名。	pool.ntp.org
备用 NTP 服务器	输入辅助 NTP 服务器的 IP 地址或域名。	空
NTP 更新间隔	输入将 NTP 客户端时间与 NTP 服务器的客户端时间同步的时间间隔（分钟）。等待下一次更新的分钟数，0 表示仅更新一次。	0

^ NTP服务器设置	
启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

选项	描述	默认值
启用	单击切换按钮以启用/禁用 NTP 服务器选项。	OFF

状态

此窗口用于查看网关的当前时间，还可以同步网关时间。单击按钮 **同步** 将网关时间与 PC 的时间同步。

NTP
状态

^ 系统时钟

系统时间	2022-07-12 17:42:45
电脑时间	2022-07-12 17:43:04 同步
上次更新时间	未更新

3.5.4 短信

本节用于设置 SMS 参数。网关支持短信管理，用户可以通过发送短信来控制 and 配置自己的网关。有关短信控制的更多详细信息，请参阅 [4.1.2 短信远程控制](#)。

短信

短信
短信测试

^ 短信管理设置
?

启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
认证类型	<input type="text" value="密码"/> ?
电话号码	<input type="text"/> + ?

选项	描述	默认值
启用	单击切换按钮以启用/禁用短信管理选项。 注： 如果禁用此选项，则 SMS 配置无效。	ON
认证类型	从“密码”，“电话号码”或“两者都要”中选择身份验证类型。 密码：使用与 Web 管理器相同的用户名和密码进行身份验证。例如，短信的格式应为“用户名：密码;cmd1;cmd2;...” 注： 在“系统>用户管理”部分中设置 Web 管理器密码。 电话号码：使用电话号码进行身份验证，用户应设置允许用于短信管理的电话号码。短信的格式应为“cmd1;cmd2;...” 并且：同时使用“密码”和“电话号码”进行身份验证。用户应设置允许用于短信管理的电话号码。短信的格式应为“用户名：密码;cmd1;cmd2;...”	密码

电话号码	设置用于短信管理的电话号码，然后单击 + 添加新的电话号码。 注：当选择“密码”作为身份验证类型时，它可以为空。	空
------	--	---

短信测试

用户可以测试当前 SMS 服务是否可用。

短信
短信测试

^ 短信测试

电话号码

信息

结果

发送

选项	描述	默认值
电话号码	输入可以从网关接收短信的指定电话号码。	空
信息	输入网关将发送到指定电话号码的消息。	空
结果	SMS 测试的结果将显示在结果框中。	空
发送	单击该按钮以发送测试消息。	--

3.5.5 Email

电子邮件功能支持通过电子邮件方式将事件通知发送给指定的收件人。

Email

^ Email设置

启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
启用TLS/SSL	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
启用 STARTTLS	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
发件服务器	<input type="text"/>
服务器端口	<input type="text" value="25"/>
超时	<input type="text" value="10"/> ?
认证登陆 启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
用户名	<input type="text"/>
密码	<input type="password"/>
发件人	<input type="text"/>
主题	<input type="text"/>

选项	描述	默认值
启用	单击切换按钮以启用/禁用电子邮件选项。	OFF
启用 TLS/SSL	单击切换按钮以启用/禁用 TLS/SSL 选项。	OFF
启用 STARTTLS	单击切换按钮以启用/禁用STARTTLS加密。	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	设置向 SMTP 服务器发送电子邮件的最长时间。当服务器在这段时间内没有收到电子邮件时，它将尝试重新发送。	10
认证登陆启用	如果邮件服务器支持 AUTH 登录，则必须启用此按钮并设置用户名和密码。	OFF
用户名	输入已从 SMTP 服务器注册的用户名。	空
密码	输入上述用户名的密码。	空
发件人	输入电子邮件的源地址。	空
主题	输入此电子邮件的主题。	空

3.5.6 DDNS

本节用于设置 DDNS 参数。动态 DNS 功能允许您将动态 IP 地址别名为静态域名，允许您的 ISP 不为其分配静态 IP 地址以使用域名。这对于通过您的连接托管服务器特别有用，因此任何希望连接到您的人都可以使用您的域名，而不必使用您的动态 IP 地址，该地址会不时更改。此动态 IP 地址是网关的 WAN IP 地址，由您的 ISP 分配给您。服务提供商默认为“DynDNS”，如下所示。

DDNS

DDNS		状态			
^ DDNS设置					
索引	启用	服务提供商	主机名	链路绑定	+

单击 **+** 以添加新的动态域名服务器。

^ DDNS设置	
索引	<input type="text" value="1"/>
启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
服务提供商	<input type="text" value="DynDNS"/> v
主机名	<input type="text"/>
用户名	<input type="text"/>
密码	<input type="text"/>
链路绑定	<input type="text"/> v
最大尝试次数	<input type="text" value="3"/> ?

选择“自定义”服务提供商后，窗口显示如下。

^ DDNS设置

索引	<input style="width: 80%;" type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
服务提供商	<input style="border-bottom: 1px solid #ccc;" type="text" value="自定义"/>
URL	<input style="width: 80%;" type="text"/>
最大尝试次数	<input style="width: 80%;" type="text" value="3"/> ?

选项	描述	默认值
启用	单击切换按钮以启用/禁用 DDNS 选项。	OFF
服务提供商	从“DynDNS”，“NO-IP”，“3322”或“自定义”中选择DDNS服务。 注： DDNS服务只有在相应服务商注册后才能使用。	DynDNS
主机名	输入DDNS服务器提供的主机名。	空
用户名	输入DDNS服务器提供的用户名。	空
密码	输入DDNS服务器提供的密码。	空
URL	输入用户自定义的URL。	空
最大尝试次数	输入最大尝试次数	3

状态

此窗口用于查看 DDNS 的状态。

DDNS
状态

^ DDNS状态

索引	状态	最后一次更新时间

选项	描述
状态	显示 DDNS 的当前状态。
最后一次更新时间	显示上次成功更新 DDNS 的日期和时间。

3.5.7 VRRP

本节用于设置 VRRP 参数。VRRP 代表虚拟网关冗余协议，是设备冗余和故障转移的标准，用于创建具有浮动 IP 地址的虚拟网关。

VRRP 设置

VRRP

^ VRRP设置

启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
接口	<input type="text" value="br_lan"/>
组ID	<input type="text" value="1"/>
优先级	<input type="text" value="100"/>
间隔	<input type="text" value="1"/> ?
虚拟IP地址	<input type="text"/>

选项	描述	默认值
启用	单击切换按钮以启用/禁用 VRRP 选项。	OFF
接口	选择 VRRP 运行的接口。	--
组 ID	虚拟网关标识符。具有相同 ID 的网关将分组到同一 VRRP 群集中。	1
优先级	虚拟网关的 VRRP 优先级。值越高等于优先级越高。	100
间隔	间隔值（以秒为单位）对于 VRRP 组中的所有路由平台必须相同。	1
虚拟 IP 地址	网关的 VRRP 群集的虚拟 IP 地址。	空

Ping 检测设置

^ Ping检测设置

启用	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
服务器	<input type="text" value="8.8.8.8"/>
间隔	<input type="text" value="300"/> ?

选项	描述	默认值
启用	单击切换按钮以启用/禁用该选项。	OFF

服务器	ping 检测服务器地址。	8.8.8.8
间隔	ping 检测的间隔值（以秒为单位）。	300

3.5.8 SSH

网关支持 SSH 密码访问和密钥访问。

SSH

^ SSH设置

启用

端口

禁用密码登陆

公开密钥

ON OFF

ON OFF

v

选项	描述	默认值
启用	单击切换按钮以启用/禁用此选项。启用后，您可以通过 SSH 访问网关	ON
端口	设置 SSH 访问的端口。	22
禁用密码登录	单击切换按钮以启用/禁用此选项。启用后，您不能使用用户名和密码通过 SSH 访问网关。在这种情况下，只有密钥可用于登录。	OFF

3.5.9 GPS

本节用于配置 GPS 的参数。网关的 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。

GPS

GPS
状态
地图

^ 常规设置

启用

同步GPS时间

ON OFF

ON OFF

^ RS232上报数据设置

通过RS232上报数据	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
上报GGA信息	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
上报VTG信息	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
上报RMC信息	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
上报GSV信息	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

^ GPS服务器

索引	启用	协议	本地地址	本地端口	服务器地址	服务器端口	
							+

单击 **+** 以添加新的 GPS 服务器。

^ 服务器设置

索引	<input type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
协议	<input type="text" value="TCP客户端"/> v
服务器地址	<input type="text"/>
服务器端口	<input type="text"/>
发送GGA信息	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
发送VTG信息	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
发送RMC信息	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
发送GSV信息	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

选项	描述	默认值
索引	显示列表的序号。	--
启用	单击切换按钮以启用/禁用服务器。	ON
协议	从“TCP客户端”、“TCP服务器”、“UDP”中进行选择。	TCP 客户端
服务器/本地 IP 地址	服务器或本地IP地址。	空
服务器/本地 IP 端口	服务器或本地IP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

添加SN到GPSID

ON

OFF

?

自定义GPSID的前缀

?

选项	描述	默认值
添加 SN 到 GPSID	单击切换按钮以启用/禁用此选项。	OFF
自定义 GPSID 的前缀	自定义GPSID前缀，四个大写字母。	空

状态

此窗口用于查看 GPS 的状态。

GPS

状态

地图

^ GPS状态

状态

世界标准时间

最后定位时间

卫星使用数量

可见卫星数量

纬度

经度

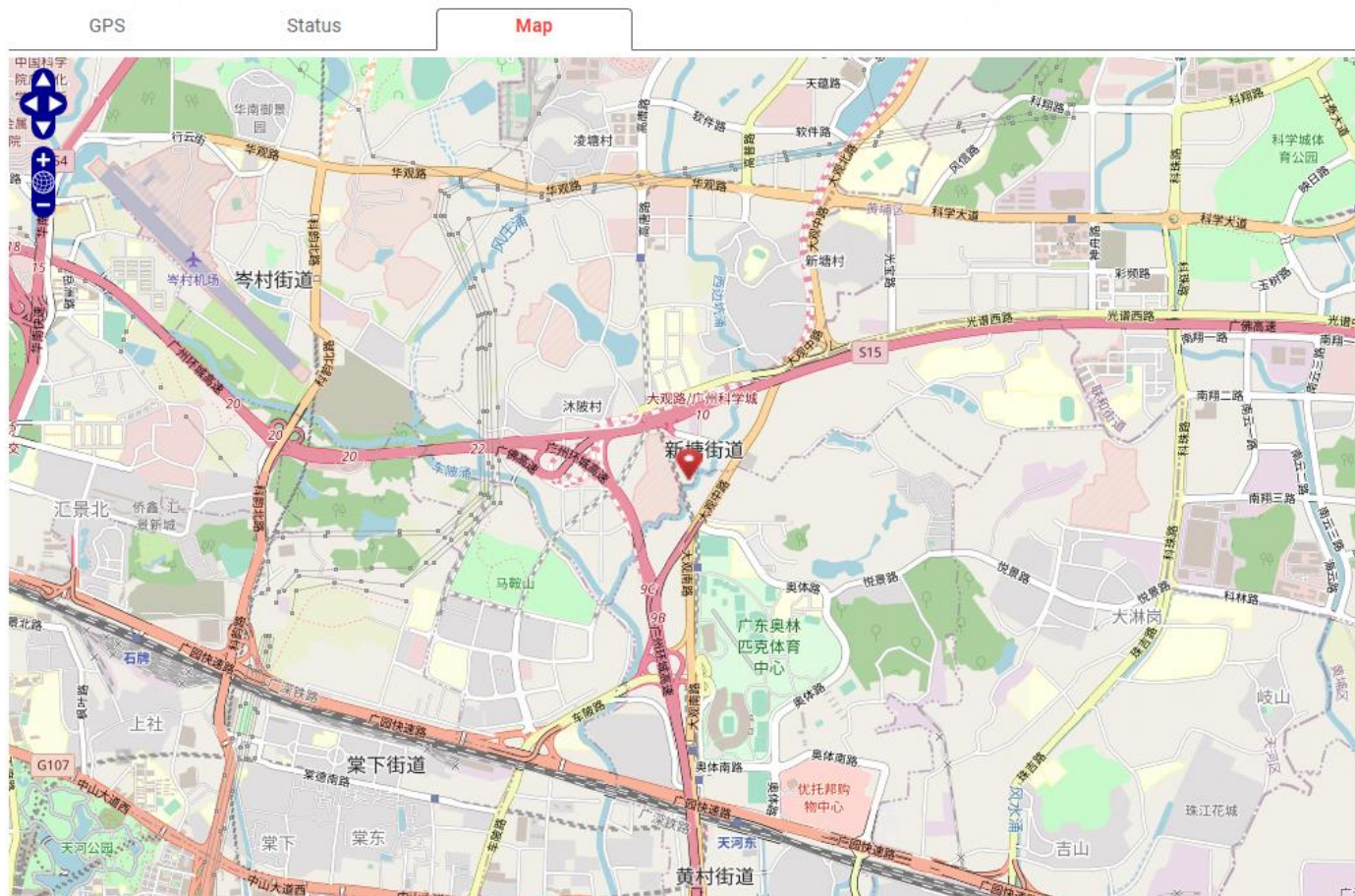
高度

速度

选项	描述
状态	显示网关的当前 GPS 状态。
世界标准时间	显示卫星的 UTC。 注： UTC 是世界的统一时间，而不是本地时间。
最后定位时间	上次成功定位的时间。
卫星使用数量	使用的卫星数量
可见卫星数量	可见卫星数量
纬度	显示网关的纬度信息。
经度	显示网关的经度信息。
高度	显示网关的高度信息。
速度	显示网关的速度信息。

Map

“地图”页面在地图上显示设备的当前坐标和位置。要在地图上查看设备的位置，请确保在设备上连接 GPS 天线，并在 GPS 页面中启用 GPS。



[在新标签页查看](#)

单击 [在新标签页查看](#) 按钮在新选项卡中查看。

3.5.10 SNMP

本节用于设置 SNMP 参数。简单网络管理协议是用于收集信息和配置网络设备的网络管理协议。

SNMP 代理服务器

SNMP代理服务器
SNMP上报
管理数据库

^ SNMP代理服务器设置

启用SNMP代理服务器设置	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
端口	<input type="text" value="161"/>
启用OEM	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
OEM企业	<input type="text"/>
OEM Platform	<input type="text"/>
版本	<input type="text" value="SNMPv3"/> v
本地信息	<input type="text"/>
联系信息	<input type="text"/>
系统名称	<input type="text"/>
认证算法	<input type="text" value="MD5"/> v
私有算法	<input type="text" value="DES"/> v

选项	描述	默认值
启用 SNMP 代理服务器设置	单击切换按钮以启用/禁用此选项。	OFF
端口	SNMP服务的端口。	161
启用 OEM	单击切换按钮以启用/禁用此选项。	OFF
OEM 企业	输入OEM信息。	空
OEM Platform	输入OEM平台信息。	空
版本	SNMP 版本，从“SNMPv3”或“SNMPv1v2v3”中进行选择。	SNMPv3
本地信息	系统位置信息。	空
联系信息	系统联系信息。	空
系统名称	系统名称。	空
认证算法	从“MD5”，“SHA”中选择。	MD5
私有算法	从“DES”，“AES”中选择。	DES

SNMP 上报

SNMP Trap 规则是在发生某些用户指定的事件时触发的警报。当触发事件发生时，SNMP Trap 将通知已知的 SNMP 主机。

SNMP代理服务器

SNMP上报

管理数据库

^ SNMP上报设置

启用SNMP上报	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
版本	SNMPv3 <input type="button" value="v"/>
接收服务器地址	<input type="text"/>
接收服务器端口	162 <input type="text"/>

^ SNMPv3认证

用户名	<input type="text"/>
认证算法	MD5 <input type="button" value="v"/>
认证密码	<input type="text"/>
私有算法	DES <input type="button" value="v"/>
私有密码	<input type="text"/>

选项	描述	默认值
启用 SNMP 上报	单击切换按钮以启用/禁用此选项。	OFF
版本	SNMP 版本，从“SNMPv3”或“SNMPv2c”或“SNMPv1”中进行选择。	SNMPv3
接收服务器地址	要将 SNMP 流量传输到的主机名或 IP 地址。	空
接收服务器端口	捕获主机的端口号。	162
用户名	对 SNMP 的用户名访问。	空
认证算法	从“MD5”，“SHA”中选择。	MD5
认证密码	输入身份验证密码。	空
私有算法	从“DES”，“AES”中选择。	DES
私有密码	输入隐私密码。	空

单击启用或禁用相关事件的切换按钮。

^ 事件选择 ?

系统启动	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
系统重启	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
系统时间更新	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
参数变化	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
蜂窝网络类型变化	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
蜂窝统计数据清除	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
蜂窝网超流量	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
信号质量差	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
链路切换	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN连接成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN连接断开	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WWAN连接成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WWAN连接断开	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
IPSec连接成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
IPSec连接断开	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
OpenVPN连接成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
OpenVPN连接失败	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LAN端口Link Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LAN端口Link Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

USB设备插入	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
USB设备移除	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DDNS更新成功	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DDNS更新失败	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
收到短信	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
收到并执行短信管理命令	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 1 告警	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 1 告警消除	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 1 计数溢出告警	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 2 告警	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 2 告警消除	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 2 计数溢出告警	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
高温告警	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

管理数据库

MIB 代表管理信息库，MIB 包含受管设备维护的变量，可由代理查询或设置。MIB 定义受管设备的属性，包括名称、状态、访问权限和数据类型。

SNMP代理服务器 SNMP上报 **管理数据库**

^ SNMP管理数据库

SNMP管理数据库	<input type="button" value="生成"/>
SNMP管理数据库	<input type="button" value="下载"/>

Item	Description	Default
SMMP 管理数据库	单击 <input type="button" value="生成"/> 生成文件，然后单击 <input type="button" value="下载"/> 下载设备的 MIB 文件。	--

3.5.11 Web 服务器

本节可用于修改 Web 服务器的参数。

Web服务器

^ 常规设置

HTTP端口	<input type="text" value="80"/>	?
HTTPS端口	<input type="text" value="443"/>	?
HTTPS CA证书	<input type="text" value="None"/>	v
HTTPS私钥	<input type="text" value="None"/>	v

选项	描述	默认值
HTTP 端口	输入您想在网关的 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 端口号配置网关而不是用 80，那么您只要加上端口号就可以登录网关的 Web 服务器。	80
HTTPS 端口	输入您想在网关的 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 端口号配置网关而不是用 443，那么您只要加上端口号就可以登录网关的 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。出于这个原因，HTTP 是由 Netscape 公司开发的，用以保证授权和安全交易。	443
HTTPS CA 证书	导入证书后选择一个，请参阅 3.6.2 证书管理器	
HTTPS 私钥	导入证书后选择一个，请参阅 3.6.2 证书管理器	

3.5.12 高级

本节用于设置高级参数。高级网关设置包括系统设置和重新启动。

系统
重启

^ 系统设置

设备名称	<input type="text" value="router"/>	?
自定义LED灯类型	<input type="text" value="无"/>	v ?

选项	描述	默认值
设备名称	设置设备名称以区分已安装的不同设备;有效字符为 a-z、A-Z、0-9、@、.、-、_	router

	#、\$和*。	
自定义 LED 灯类型	<p>指定 USR LED 的显示类型。从“无”、“OpenVPN”或“IPsec”中进行选择。</p> <ul style="list-style-type: none"> 无：选择此选项后，USR指示灯灭，无意义 SIM卡：选择此类型后，网关的USR指示灯显示的是SIM 卡的状态 OpenVPN：选择此类型后，网关的USR指示灯显示的是OpenVPN的状态 IPsec：选择此类型后，网关的USR指示灯显示的是IPsec的状态 	无

系统

重启

^ 定期重启设置

定期重启	<input type="text" value="0"/>	?
每天重启时间	<input type="text"/>	?

^ 紧急重启设置。

当网络不可用重启。	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	?
-----------	---	---

定期重启设置		
选项	描述	默认值
定期重启	设置网关的重启周期。0 代表不启用定期重启。	0
每天重启时间	设置每天重启网关的时间点，格式为 HH:MM（24 小时制）。否则数据将无效。此项为空时代表关闭定时重启。	空
当前网络不可重启	单击切换按钮以启用/禁用此选项。	OFF

3.6 系统

3.6.1 调试

本节用于检查和下载系统日志详细信息。单击“系统日志>服务>系统日志设置”以启用系统日志。

系统日志

^ 日志记录

日志等级

调试

过滤

?

```

Jul 06 09:45:35 Router systemd[1]: fstrim.service: Succeeded.
Jul 06 09:45:35 Router systemd[1]: Finished Discard unused blocks on filesystems from /etc/fstab.
Jul 06 09:45:36 Router nm_wrapper[1114]: [D] nmw_get_modem: found no modems!
Jul 06 09:45:37 Router systemd[1]: apt-daily.service: Succeeded.
Jul 06 09:45:37 Router systemd[1]: Finished Daily apt download activities.
Jul 06 09:45:37 Router systemd[1]: apt-daily.service: Consumed 2.181s CPU time.
Jul 06 09:45:37 Router systemd[1]: Starting Daily apt upgrade and clean activities...
Jul 06 09:45:39 Router ModemManager[22982]: <info> [base-manager] couldn't check support for device
'/sys/devices/soc0/soc/2100000.aips-bus/20b4000.ethernet': not supported by any plugin
Jul 06 09:45:39 Router ModemManager[22982]: <info> [base-manager] couldn't check support for device
'/sys/devices/soc0/soc/2100000.aips-bus/2188000.ethernet': not supported by any plugin
Jul 06 09:45:39 Router systemd[1]: apt-daily-upgrade.service: Succeeded.
Jul 06 09:45:39 Router systemd[1]: Finished Daily apt upgrade and clean activities.
Jul 06 09:45:39 Router systemd[1]: apt-daily-upgrade.service: Consumed 1.774s CPU time.
Jul 06 09:45:40 Router systemd[1]: exim4-base.service: Succeeded.
Jul 06 09:45:40 Router systemd[1]: Finished exim4-base housekeeping.
Jul 06 09:45:40 Router systemd[1]: Starting Rotate log files...
Jul 06 09:45:41 Router systemd[1]: logrotate.service: Succeeded.
Jul 06 09:45:41 Router systemd[1]: Finished Rotate log files.
Jul 06 09:45:42 Router rospam[23149]: pam_unix(login:session): session opened for user admin(uid=1000) by (uid=0)
Jul 06 09:45:42 Router rospam[23149]: pam_unix(login:session): session closed for user admin
Jul 06 09:45:42 Router nm_wrapper[1114]: [D] nmw_get_modem: found no modems!
Jul 06 09:45:45 Router ModemManager[22982]: <info> [base-manager] couldn't check support for device
'/sys/devices/soc0/soc/2100000.aips-bus/20b4000.ethernet': not supported by any plugin
Jul 06 09:45:45 Router ModemManager[22982]: <info> [base-manager] couldn't check support for device
'/sys/devices/soc0/soc/2100000.aips-bus/2188000.ethernet': not supported by any plugin
Jul 06 09:45:46 Router ModemManager[22982]: <info> [modem0] state changed (unknown -> locked)
Jul 06 09:45:46 Router ModemManager[22982]: <warn> [modem0] modem couldn't be initialized: Couldn't check unlock status: QMI
operation failed: GW primary session index unknown
Jul 06 09:45:46 Router ModemManager[22982]: <info> [modem0] state changed (locked -> failed)
Jul 06 09:45:46 Router NetworkManager[811]: <info> [1657071946.5013] manager: (cdc-wdm0): new Broadband device
(/org/freedesktop/NetworkManager/Devices/600)
Jul 06 09:45:46 Router NetworkManager[811]: <info> [1657071946.5155] device (cdc-wdm0): state change: unmanaged -> unavailable
(reason 'managed', sys-iface-state: 'external')
Jul 06 09:45:46 Router NetworkManager[811]: <info> [1657071946.5277] device (cdc-wdm0): modem state 'failed'
Jul 06 09:45:46 Router NetworkManager[811]: <info> [1657071946.5480] device (cdc-wdm0): old_state: unmanaged, state: unavailable,
concheck_now: false
Jul 06 09:45:46 Router NetworkManager[811]: <warn> [1657071946.5494] device (cdc-wdm0): concheck_update_interval[IPv4]:
applicable interval is 0
Jul 06 09:45:46 Router NetworkManager[811]: <info> [1657071946.5507] device (cdc-wdm0): concheck_update_state[IPv4], state: NONE,
old state: UNKNOWN, dev state: unavailable, continuous success count: 0, continuous failure count: 1
Jul 06 09:45:46 Router NetworkManager[811]: <warn> [1657071946.5538] device (cdc-wdm0): concheck_update_interval[IPv6]:
applicable interval is 0
                    
```

手动更新

v

清除

刷新

选项	描述	默认值
日志级别	从“调试”，“信息”，“通知”，“警告”，“错误”中选择从低到高。较低的级别将详细输出更多的系统日志。	Debug
过滤	根据关键字输入过滤消息。使用“&”分隔多个筛选器消息，例如“关键字1&关键字2”。	空
手动更新	从“手动更新”，“5秒”，“10秒”，“20秒”或“30秒”中进行选择。您可以选择这些间隔来刷新以下框中显示的日志信息。如果选择“手动刷新”，则应单击刷新按钮以刷新系统日志。	手动刷新

清除	单击该按钮以清除系统日志。	--
刷新	单击该按钮以刷新系统日志。	--

^ 日志文件

系统日志文件 **产生**

系统日志文件 **下载**

选项	描述	默认值
系统日志文件	单击 产生 生成系统日志文件 单击 下载 下载系统日志文件。	--

^ 系统诊断数据

系统诊断数据 **生成**

系统诊断数据 **下载**

选项	描述	默认值
系统诊断数据	单击 生成 生成系统诊断数据单击 下载 下载系统诊断数据文件。	--

3.6.2 证书管理器


本节用于在此处管理所有证书。如果要管理自定义应用程序的证书，可以通过“其他”选项卡对其进行管理。

OpenVPN

^ X509设置
?

根证书	<input type="button" value="选择文件"/> 未选择文件	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/>
证书文件	<input type="button" value="选择文件"/> 未选择文件	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/>
私钥	<input type="button" value="选择文件"/> 未选择文件	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/>
Diffie-Hellman密钥	<input type="button" value="选择文件"/> 未选择文件	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/>
TLS-Auth密钥	<input type="button" value="选择文件"/> 未选择文件	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/>
证书吊销列表	<input type="button" value="选择文件"/> 未选择文件	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/>
PKCS#12证书	<input type="button" value="选择文件"/> 未选择文件	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/>
预共享密钥	<input type="button" value="选择文件"/> 未选择文件	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/>
Ovpn配置文件	<input type="button" value="选择文件"/> 未选择文件	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/>

选项	描述	默认值
根证书	单击 <input type="button" value="选择文件"/> 找到根证书文件，然后单击 <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/> 将此文件导入网关。	--
证书文件	单击 <input type="button" value="选择文件"/> 找到证书文件，然后单击 <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/> 将此文件导入网关。	--
私钥	单击 <input type="button" value="选择文件"/> 找到私钥文件，然后单击 <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/> 将此文件导入网关。	--
DH 密钥	单击 <input type="button" value="选择文件"/> 找到 DH 密钥文件，然后单击 <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/> 将此文件导入网关。	
TLS-Auth 密钥	单击 <input type="button" value="选择文件"/> 找到 TLS-Auth 密钥文件，然后单击 <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/> 将此文件导入网关。	--
证书吊销列表	单击 <input type="button" value="选择文件"/> 找到证书吊销列表文件，然后单击 <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/> 将此文件导入网关。	
PKCS#12 证书	单击 <input type="button" value="选择文件"/> 找到 PKCS#12 证书文件，然后单击 <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/> 将此文件导入网关。	--
预共享密钥	单击 <input type="button" value="选择文件"/> 找到预共享密钥文件，然后单击 <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="image"/> 将此文件导入网关。	






Ovpn 配置文件	单击 <input type="button" value="选择文件"/> 找到 Ovpn 配置文件，然后单击  将此文件导入网关。
-----------	---

IPsec

OpenVPN	IPsec	SSH	Web	系统证书	其它
---------	--------------	-----	-----	------	----

^ X509设置 ?

本地证书	<input type="button" value="选择文件"/> 未选择文件	
对端证书	<input type="button" value="选择文件"/> 未选择文件	
私钥	<input type="button" value="选择文件"/> 未选择文件	
根证书	<input type="button" value="选择文件"/> 未选择文件	
PKCS#12证书	<input type="button" value="选择文件"/> 未选择文件	

选项	描述	默认值
本地证书	单击 <input type="button" value="选择文件"/> 找到本地证书文件，然后单击  将此文件导入网关。	--
对端证书	单击 <input type="button" value="选择文件"/> 找到对端证书文件，然后单击  将此文件导入网关。	--
私钥	单击 <input type="button" value="选择文件"/> 找到私钥文件，然后单击  将此文件导入网关。	--
根证书	单击 <input type="button" value="选择文件"/> 找到根证书文件，然后单击  将此文件导入网关。	
PKCS#12 证书	单击 <input type="button" value="选择文件"/> 找到 PKCS#12 证书文件，然后单击  将此文件导入网关。	--

SSH


OpenVPN	IPsec	SSH	Web	系统证书	其它
---------	-------	------------	-----	------	----

^ 密钥管理 ?

公有密钥	<input type="button" value="选择文件"/> 未选择文件	
------	---	---

^ 公有密钥

索引	文件名	文件大小	最后修改时间

选项	描述	默认值
公有密钥	单击 <input type="button" value="选择文件"/> 找到公有密钥文件，然后单击  将此文件导入网关。	--

Web

OpenVPN
IPsec
SSH
Web
系统证书
其它

^ HTTPS证书管理 ?

HTTPS私钥 未选择文件 



HTTPS CA证书 未选择文件 

^ HTTPS私钥

索引	文件名	文件大小	最后修改时间

^ HTTPS CA证书

索引	文件名	文件大小	最后修改时间


选项	描述	默认值
HTTPS 私钥	单击 <input type="button" value="选择文件"/> 找到公有密钥文件，然后单击  将此文件导入网关。	--
HTTPS CA 证书	单击 <input type="button" value="选择文件"/> 找到公有密钥文件，然后单击  将此文件导入网关。	

系统证书

OpenVPN
IPsec
SSH
系统证书
其它

^ 证书安装

文件 未选择文件 导入

选项	描述	默认值
系统证书	单击 <input type="button" value="选择文件"/> 找到系统证书文件，然后单击  将此文件导入网关。	--

其它

OpenVPN
IPsec
SSH
Web
系统证书
其它

^ 其它证书管理 ?

其它证书

选择文件
未选择文件

↑

^ 其它证书

索引	文件名	文件大小	最后修改时间

选项	描述	默认值
其他证书管理	单击 选择文件 找到其他证书文件，然后单击 ↑ 将此文件导入网关。	

3.6.3 资源图

本节用于查看最近 3 分钟、过去一小时或最近一天的系统资源，例如 CPU 使用率或蜂窝信号强度。

处理器使用情况

CPU使用率
内存使用率
SIM流量
SIM信号

∨ 最近三分钟CPU使用率

∨ 最近1小时CPU使用率

∨ 最近1天CPU使用率

内存使用情况



SIM 流量



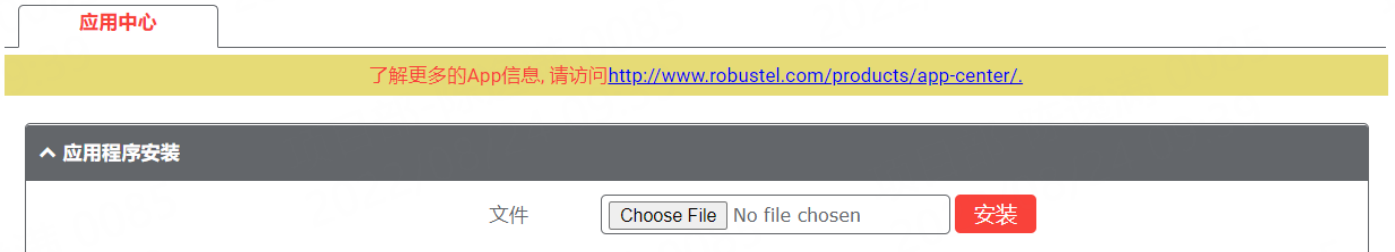
SIM 信号



3.6.4 应用中心

网关支持 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:将应用程序导入网关后，由于浏览器缓存的原因，页面显示可能会有轻微延迟。建议您先清除浏览器缓存，然后重新登录网关。



选项	描述	默认值
文件	单击“选择文件”以从PC中找到应用程序文件，然后单击 安装 将此文件导入网关。	--

成功安装的应用将显示在以下列表中。单击 **×** 以卸载应用程序。

^ 已装应用程序				
索引	名称	版本	状态	描述
1	linux-image-5.4.24-2.0.0	2.0.0	Running	Linux kernel, version 5.4.24-2.0.0
2	rosp-core	2.0.0mes202...	Running	ros pro core deb

选项	描述
索引	指示列表的序号。
名称	显示应用的名称。
版本	显示应用程序的版本。
状态	显示应用的状态。
描述	显示此应用的说明。

3.6.5 工具

本节为用户提供了三个工具：**Ping**，路由跟踪和嗅探器。

Ping

Ping
路由跟踪
嗅探器

^ Ping

IP地址

请求数量

超时时间

接口

|

开始

停止

选项	描述	默认值
IP 地址	输入 ping 的目标 IP 地址或目标域。	空
请求数	指定 ping 请求的数量。	5
超时时间	指定 ping 请求的超时。	1
本地 IP	指定来自蜂窝 WAN、以太网 WAN 或以太网 LAN 的本地 IP。Null 代表从这三个地址中自动选择本地 IP 地址。	空
开始	单击此按钮启动ping请求，日志将显示在下面的框中。	--
停止	单击此按钮可停止 ping 请求。	--

路由跟踪

Ping
路由跟踪
嗅探器

^ 路由跟踪

目标地址

跳数

超时时间

接口

开始
停止

选项	描述	默认值
目标地址	输入目标 IP 地址或目标域。	空
跳数	指定最大跳数。如果跳数已达到最大值，则无论是否到达目标，网关都将停止跟踪。	30
超时时间	指定跟踪路由请求的超时。	1
接口	选择目标接口。	
开始	单击此按钮启动ping请求，日志将显示在下面的框中。	--
停止	单击此按钮可停止 ping 请求。	--

嗅探器

Ping 路由跟踪 **嗅探器**

^ 嗅探器

接口 v

主机地址

抓包数量

协议 v

状态

开始 停止

选项	描述	默认值
接口	根据您的以太网配置选择接口。	All
主机	筛选包含指定 IP 地址的数据包。	空
抓包数量	设置网关可以一次嗅探的数据包编号。	1000
协议	从“全部”、“IP”、“TCP”、“UDP”和“ARP”中进行选择。	All
状态	显示嗅探器的当前状态。	--
开始	单击此按钮可启动嗅探器。	--
停止	单击此按钮可停止嗅探器。单击此按钮后，将在以下列表中显示一个新的日志文件。	--

^ 抓包文件

索引	文件名	文件大小	最后修改时间

选项	描述	默认值
抓包文件	每次嗅探器日志都将自动保存为新文件。您可以从此嗅探器流量数据列表中找到该文件，然后单击 下载日志 下载日志，单击以删除日志文件。它最多可以缓存5个文件。	--

3.6.6 参数文件

本节用于导入或导出配置文件，或者将网关回滚到以前的配置。

参数文件

参数文件

参数回滚

^ 导入配置文件

将其他参数恢复到默认设置 ON OFF ?

忽略非法配置 ON OFF ?

XML配置文件 未选择文件

选项	描述	默认值
将其他参数恢复到默认设置	单击切换按钮作为“ON”，将其他参数返回到默认设置。	OFF
忽略非法设置	单击切换按钮为“OFF”以忽略无效设置。	OFF
XML 配置文件	单击 Choose File 从 PC 中找到 XML 配置文件，然后单击 导入 将此文件导入网关。	--

^ 导出配置文件

忽略未启用的参数 ON OFF ?

添加详细信息 ON OFF ?

XML配置文件

选项	描述	默认值
忽略未启用的参数	单击切换按钮为“关闭”以忽略禁用的功能。	OFF
添加详细信息	单击切换按钮作为“开”以添加详细信息。	OFF
加密机密文件	单击切换按钮为“ON”以加密机密数据。	ON
XML 配置文件	单击 生成 按钮生成 XML 配置文件，然后单击 导出 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 保存 ?

出厂配置 恢复

选项	描述	默认值
保存当前运行的参数为默认配置	单击 保存 按钮将当前正在运行的参数保存为默认配置。	--
出厂配置	单击 恢复 按钮以恢复出厂默认设置。	--

参数回滚

参数文件 参数回滚

^ 回滚设置

保存为回滚配置档案 保存 ?

^ 配置文件档案

索引	文件名	文件大小	修改时间

选项	描述	默认值
保存为回滚配置档案	手动创建保存点。此外，如果配置发生更改，系统将每天自动创建一个保存点。	--
配置文件档案	查看有关配置归档文件的相关信息，包括名称、大小和修改时间。	--

3.6.7 用户管理

本节用于更改用户名和密码，以及创建或管理用户帐户。一个网关只有一个超级用户，该用户具有修改、添加和管理其他常见用户的最高权限。

超级用户
普通用户

^ 超级用户设置 ?

新用户名

?

旧密码

?

新密码

?

确认密码

选项	描述	默认值
新用户名	输入您要创建的新用户名;有效字符为 a-z、A-Z、0-9、@,., -, #、\$和 *。	空
旧密码	输入网关的旧密码。默认值为“管理员”。	空
新密码	输入要创建的新密码;有效字符为 a-z、A-Z、0-9、@,., -, #、\$和 *。	空
确认密码	再次输入新密码进行确认。	空

超级用户
普通用户

^ 普通用户设置 ?

UserId	角色	用户名	
			+

单击 + 按钮以添加新的普通用户。最多支持配置 5 个用户。。

^ 普通用户设置

UserId

?

角色

只读用户
v

用户名

?

密码

?

选项	描述	默认值
索引	指示列表的序号。	--
角色	从“只读用户”和“编辑者”中选择。 只读用户：用户只能查看此级别下的网关配置 编辑者：用户可以在此级别下查看和设置网关的配置	只读用户
用户名	设置用户名;有效字符为 a-z、A-Z、0-9、@、.、-、#、\$和*。	空
密码	设置至少包含 5 个字符的密码;有效字符为 a-z、A-Z、0-9、@、.、-、#、\$和*。	空

3.6.8 DEB 管理

本节用于管理自己的 Debian 软件包。

^ DEB包管理

Apt行为

包名称

额外参数

?

选项	描述	默认值
Apt 行为	从“update”, “install”, “clean”, “remove”, “show”.中进行选择 update: 更新 apt。 Install: 安装 apt。 Remove: 移除 apt。 Clean: 清除 apt。 Show: 显示 apt 列表。	update
包名称	输入要实现的包名称。	--
额外参数	更多“apt”命令参数，例如“--清除”等。。	空

第四章 配置示例

4.1 蜂窝网

4.1.1 蜂窝 APN 手动设置和蜂窝拨号

本节介绍如何为移动网络拨号配置 APN。正确连接网关并插入 SIM 卡，然后打开 Web 配置页面。在主页菜单下，单击“接口>蜂窝>蜂窝”以转到蜂窝配置页面。

蜂窝网
状态
AT调试

^ 蜂窝网常规设置

主SIM卡

v
?

开启SIM卡自动切换功能

ON

OFF

?

^ 附加的切换规则

基于信号强度切卡

ON

OFF

?

当漫游时切卡

ON

OFF

?

^ 蜂窝网高级设置

索引	SIM卡	电话号码	网络类型	频段选择	
1	SIM1		自动	全部	☑
2	SIM2		自动	全部	☑

单击 根据当前 ISP 设置其参数。

^ 常规设置

索引	<input type="text" value="1"/>
SIM卡	<input type="text" value="SIM1"/> v
自动匹配APN	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
APN	<input type="text" value="internet"/>
用户名	<input type="text"/>
密码	<input type="password"/>
鉴权方式	<input type="text" value="无鉴权"/> v
电话号码	<input type="text"/>
PIN码	<input type="text"/> ?
额外的AT命令	<input type="text"/> ?
Telnet端口	<input type="text" value="0"/> ?

然后单击“网络>WAN>链接”转到WAN配置页面。

链路

状态

^ 设置

名称	类型	描述	权重	防火墙区域	+
WWAN	蜂窝网	default wan	0	external	⋮ □ ×

单击 + 若要为蜂窝拨号添加一个链接，请选择“调制解调器”作为链接类型，然后单击 提交 提交

链路设置

名称

类型

接口

描述

权重

防火墙区域

链路检测设置

启用 ON OFF

提交 关闭

保存并应用后，新的蜂窝 WAN 链接将生效。

名称	类型	描述	权重	防火墙区域	
WWAN	蜂窝网	default wan	0	external	  

4.1.2 短信远程控制

EG51xx 支持通过短信进行远程控制。您可以使用以下命令获取网关的状态，并设置网关的所有参数。

SMS 命令具有以下结构：

SMS 命令具有以下结构：

1. 密码模式—用户名：密码;cmd1;cmd2;cmd3;...cmdn（适用于每个电话号码）。
2. 电话模式—密码;cmd1;cmd2;cmd3;...cmdn（使用网关的电话组中的电话号码发送短信时可用）。
3. 两种模式—用户名：密码;cmd1;cmd2;cmd3;...cmdn（使用网关的电话组中的电话号码发送短信时可用）。

注：所有命令符号都必须以英语输入法的半角模式输入。

短信命令说明：

用户名和密码：使用与 WEB 管理器相同的用户名和密码进行身份验证。

cmd1, cmd2, cmd3 到 cmdn, 命令格式与 CLI 命令相同，有关 CLI cmd 的更多详细信息请参阅 [5.1 什么是 CLI](#)。

注：从配置的 Web 浏览器下载配置 XML 文件。SMS 控制命令的格式可以参考 XML 文件的数据。

转到“系统>配置文件>导出配置文件”，单击 **生成** 生成 XML 文件，然后单击 **导出** 以导出 XML 文件。

参数文件
参数回滚

^ 导入配置文件

将其他参数恢复到默认设置 ON OFF ?

忽略非法配置 ON OFF ?

XML配置文件 未选择文件

^ 导出配置文件

忽略未启用的参数 ON OFF ?

添加详细信息 ON OFF ?

XML配置文件

XML配置文件

XML 命令：

```
<lan>
<network max_entry_num="5">
<id>1</id>
<interface>lan0</interface>
<ip>172.16.24.24</ip>
<netmask>255.255.0.0</netmask>
<mtu>1500</mtu>
```

短信 cmd:

```
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
```

1. 分号字符 (;) 用于分隔打包在单个SMS中的多个命令
2. 例:

admin:admin;status system

在此命令中，用户名为“admin”，密码为“admin”，控制命令为“status system”，命令的功能是获取系统状态。

SMS received:

```
firmware_version = 2.0.0
firmware_version_full = "2.0.0 (60b55c0)"
kernel_version = 5.4.24-2.0.0
hardware_version = 0.0
operation_system = "Debian GNU/Linux 11.3"
device_model = ""
serial_number = 2204190667030003
temperature_interval = 53.0
uptime = "0 days, 00:12:06"
system_time = "Thu May 19 16:52:22 2022"
ram_usage = 392M/448M
cpu_usage = "22569s Idle/71405s Total /1 cpus"
disk_usage = 1.9G/7.1G
```

admin:admin;reboot

在此命令中，用户名为“admin”，密码为“admin”，该命令用于重启网关。

SMS received:

OK

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

在此命令中，用户名为“admin”，密码为“admin”，该命令用于禁用 remote_ssh 并 remote_telnet 访问权限。

SMS received:

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

在此命令中，用户名为“admin”，密码为“admin”，命令用于配置 LAN 参数。

SMS received:

OK

OK

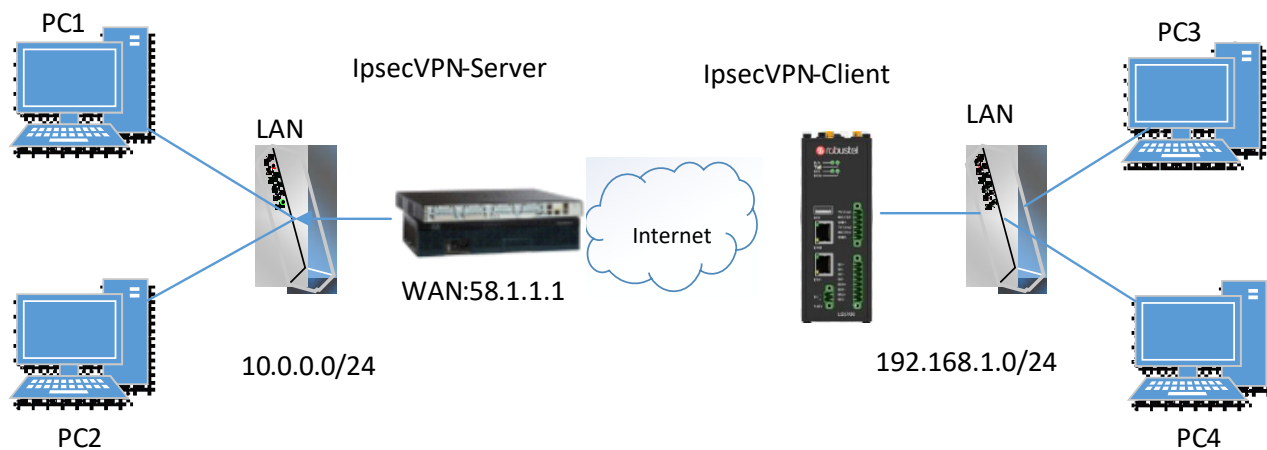
OK

OK

4.2 VPN 配置示例

4.2.1 IPsec VPN

IPsec VPN 拓扑（服务器端和客户端 IKE 和 SA 参数必须配置相同）。



IPsecVPN 服务器:

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

```

IPsec VPN 客户端:

The window is displayed as below by clicking “虚拟专用网 > IPsec > 隧道.”

索引	启用	描述	网关	本地子网	远端子网	
						+

单击按钮 **+** 然后按如下方式设置 IPsec 客户端的参数。

^ 隧道设置

索引	启用	描述	网关	本地子网	远端子网	
1	ON OFF					+

^ 常规设置

索引	<input type="text" value="1"/>	
启用	<input type="checkbox"/> ON <input type="checkbox"/> OFF	
描述	<input type="text"/>	
链路绑定	<input type="text" value="v"/>	
网关	<input type="text"/>	?
协议	<input type="text" value="ESP"/>	v
模式	<input type="text" value="隧道"/>	v
本地子网	<input type="text"/>	?
远端子网	<input type="text"/>	?
IKE类型	<input type="text" value="IKEv1"/>	v
协商模式	<input type="text" value="主模式"/>	v
初始模式	<input type="text" value="保持连接"/>	v

^ 高级设置

加密算法	<input type="text" value="3DES"/>	v
认证方法	<input type="text" value="SHA1"/>	v
PFS组	<input type="text" value="PFS(N/A)"/>	v
SA存活时间	<input type="text" value="28800"/>	?
DPD间隔	<input type="text" value="30"/>	?
DPD失败时间	<input type="text" value="150"/>	?

^ SA设置

认证方法	<input type="text" value="3DES"/>	▼
加密算法	<input type="text" value="SHA1"/>	▼
IKE DH分组	<input type="text" value="DHgroup2"/>	▼
认证类型	<input type="text" value="PSK"/>	▼
PSK密钥	<input type="text"/>	
本地ID类型	<input type="text" value="默认"/>	▼
远程ID类型	<input type="text" value="默认"/>	▼
IKE存活时间	<input type="text" value="86400"/>	?

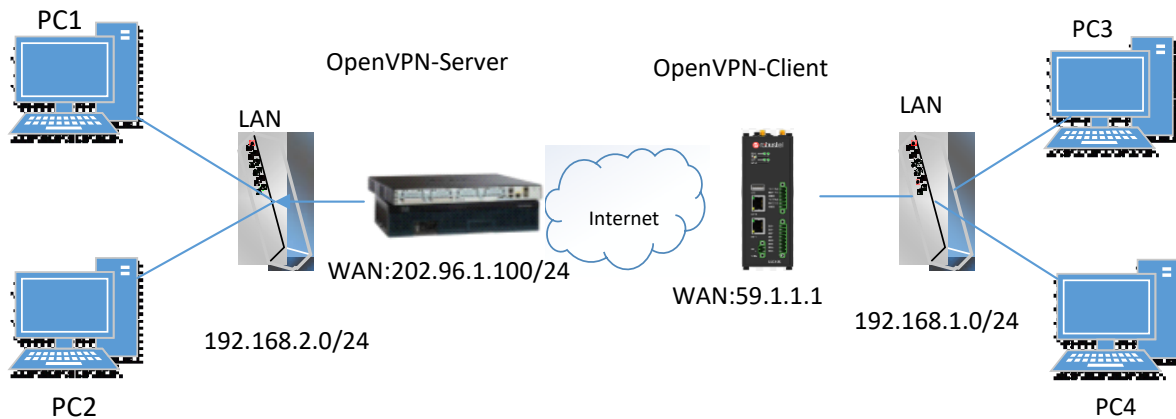
^ 高级设置

加密算法	<input type="text" value="3DES"/>	▼
认证方法	<input type="text" value="SHA1"/>	▼
PFS组	<input type="text" value="PFS(N/A)"/>	▼
SA存活时间	<input type="text" value="28800"/>	?
DPD间隔	<input type="text" value="30"/>	?
DPD失败时间	<input type="text" value="150"/>	?

完成后，单击 **提交** 提交并单击  使配置生效。

4.2.2 OpenVPN

OpenVPN 支持客户端和 P2P 两种模式。以下以客户端模式作为例子。



OpenVPN 服务器:

首先在服务器端生成相关的 OpenVPN 证书，并参考以下命令配置服务器:

```
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: 如需要有关配置详细信息，请联系您的技术支持工程师。

OpenVPN_Client:

单击“VPN>OpenVPN>OpenVPN”，如下所示。

索引	启用	描述	模式	对端地址	
					+

单击 + 以配置 Client01，如下所示。

^ 常规设置	
索引	<input type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
启用IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
描述	<input type="text"/>
模式	<input type="text" value="P2P"/> ?
TLS模式	<input type="text" value="无"/> ?
协议	<input type="text" value="UDP"/>
对端地址	<input type="text"/>
对端端口	<input type="text" value="1194"/>
监听地址	<input type="text"/>
监听端口	<input type="text" value="1194"/>
接口类型	<input type="text" value="TUN"/>
验证方式	<input type="text" value="无"/> ?
本地IP	<input type="text" value="10.8.0.1"/>
远端IP	<input type="text" value="10.8.0.2"/>
保活间隔时间	<input type="text" value="20"/> ?
保活超时时间	<input type="text" value="120"/> ?
隧道MTU	<input type="text" value="1500"/>

数据分片	<input type="text"/>
启用压缩	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
启用NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
日志信息级别	0 <input type="text"/> <input type="button" value="v"/> <input style="color: red;" type="button" value="?"/>

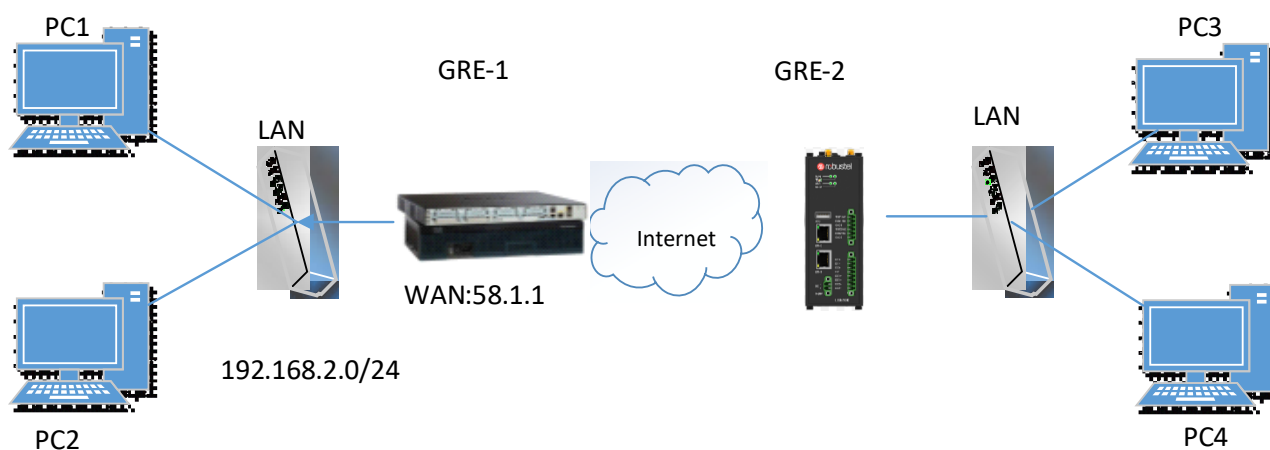
^ 高级设置

专家选项	<input type="text"/> <input style="color: red;" type="button" value="?"/>
------	---

完成后，单击 提交 提交，然后单击 使配置生效。

4.2.3 GRE VPN

GRE VPN 拓扑



GRE-1:

通过单击“VPN > GRE > GRE”，窗口显示如下。

虚拟专用网/GRE

GRE是通用路由封装协议，它是一种IP报文封装协议，允许网络和路由从一个网络设备发布到另一个网络设备。

GRE
状态

^ GRE隧道

索引	启用	描述	远端IP地址	+

单击 + 按钮，然后按如下方式设置 GRE-1 的参数。

GRE	
索引	<input type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
描述	<input type="text" value="GRE-1"/>
远端IP地址	<input type="text" value="58.1.1.1"/>
本地虚拟IP地址	<input type="text" value="10.8.0.1"/>
本地虚拟子网掩码	<input type="text" value="255.255.255.0"/> ?
远端虚拟IP地址	<input type="text" value="10.8.0.2"/>
启用默认路由	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
启用NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
密码	<input type="password" value="....."/>

完成后，单击 提交，然后单击 使配置生效。

GRE-2:

在远程端，点击按钮 设置 GRE-2 的参数，如下所示。

GRE	
索引	<input type="text" value="1"/>
启用	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
描述	<input type="text" value="GRE-2"/>
远端IP地址	<input type="text" value="59.1.1.1"/>
本地虚拟IP地址	<input type="text" value="10.8.0.2"/>
本地虚拟子网掩码	<input type="text" value="255.255.255.0"/> ?
远端虚拟IP地址	<input type="text" value="10.8.0.1"/>
启用默认路由	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
启用NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
密码	<input type="password" value="....."/>

完成后，单击 **提交** 提交，然后单击 使配置生效。

GRE-1 和 GRE-2 的对比如下。

The screenshot shows two side-by-side configuration panels for GRE instances. The left panel is for GRE-1 and the right panel is for GRE-2. Red annotations provide the following information:

- Remote IP Address:** GRE-1 has 58.1.1.1, GRE-2 has 59.1.1.1. An annotation states: "另一个GRE实例的外部IP地址，用于建立组之间的初始连接。" (External IP address of another GRE instance, used for initial connection between groups).
- Local Virtual IP Address:** GRE-1 has 10.8.0.1, GRE-2 has 10.8.0.2. An annotation states: "远程GRE隧道网络接口的IP地址。" (IP address of the remote GRE tunnel network interface).
- Local Virtual Subnet Mask:** GRE-1 has 255.255.255.0, GRE-2 has 255.255.255.0. An annotation states: "为GRE组使用相同的密码。" (Use the same password for GRE groups).
- Remote Virtual IP Address:** GRE-1 has 10.8.0.2, GRE-2 has 10.8.0.1.
- Other settings:** Both instances have "启用" (Enabled) checked, "启用默认路由" (Enable default routing) set to OFF, and "启用NAT" (Enable NAT) set to OFF. The password field is masked with dots.

Buttons for "提交" (Submit) and "关闭" (Close) are located at the bottom right of the configuration area.

第五章 CLI 简介

5.1 什么是 CLI

命令行界面（CLI）是一种软件界面，提供了从 SSH 或通过 telnet 网络连接设置设备参数的另一种方法。与网关建立 Telnet 或 SSH 连接后，输入登录帐户和密码（默认管理员/管理员）以进入网关的配置模式，如下所示。

网关登录：

Router login: admin

Password: admin

#

CLI 命令：

?

!	注释
add	添加配置的列表条目
clear	清除统计信息
config	配置操作
debug	将调试信息输出到控制台
del	删除配置的列表条目
do	设置执行的级别状态
exit	退出CLI
help	显示 CLI 语法的概述
ovpn_cert_get	通过 http 或 ftp 下载 OpenVPN 证书文件
ping	向网络主机发送消息
reboot	暂停并执行冷重新启动
set	设置系统配置
show	显示系统配置
status	显示正在运行的系统信息
tftpupdate	使用 tftp 更新固件或配置文件
traceroute	将路由数据包跟踪打印到网络主机
trigger	触发操作
urlupdate	通过 http 或 ftp 更新固件
ver	固件版本

5.2 如何配置 CLI

下表介绍了帮助的描述，在配置程序中应该会遇到错误。

命令/提示	描述
?	键入问号“?”将显示帮助信息。 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	同时按下这两个键，除了它的“复制”功能外，还可以用于“打破”出设定程序。
语法错误：命令未完成	命令未完成。
勾选空格键+制表键	它可以帮助您完成命令。 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	设置完成后，您应该输入这些命令以使设置在设备上生效。 注：提交和 save_and_apply 起着相同的作用。

5.3 常用命令

命令	句法	描述
调试	调试参数	打开或关闭调试功能
显示	显示参数	显示每个函数的当前配置，如果需要查看所有内容请使用“显示运行”
设置	设置参数	所有函数参数都是通过命令设置和添加来设置的，不同之处在于设置是针对单个参数的，而 add 是针对列表参数的
加	添加参数	

注： 从配置的 Web 浏览器下载配置.XML 文件。命令格式可以引用配置.XML 文件格式。

5.4 配置示例

掌握 CLI 的最好和最快的方法是首先从网页查看所有功能，然后一次读取所有 CLI 命令，最后学习使用一些参考示例进行配置。

示例 1：查看当前版本

```
# status system
firmware_version = 2.0.0
firmware_version_full = "2.0.0 (60b55c0)"
kernel_version = 5.4.24-2.0.0
hardware_version = 0.0
operation_system = "Debian GNU/Linux 11.3"
device_model = ""
serial_number = 2204190667030003
temperature_interval = 53.0
uptime = "0 days, 00:12:06"
system_time = "Thu May 19 16:52:22 2022"
ram_usage = 392M/448M
cpu_usage = "22569s Idle/71405s Total /1 cpus"
disk_usage = 1.9G/7.1G
#
```

示例 2：设置移动网络的CLI

```
# 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
```

```
// 保存应用当前的配置，让配置生效
```

术语表

缩写	解释参照
AC	Alternating Current
APN	Access Point Name
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	Evolution-Data Optimized
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 Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
kbps	kbits per second

缩写	解释参照
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

缩写	解释参照
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

地址： 广州市黄埔区永安大道 63 号 2 栋 501

邮箱： info@robustel.com

网址： www.robustel.com.cn