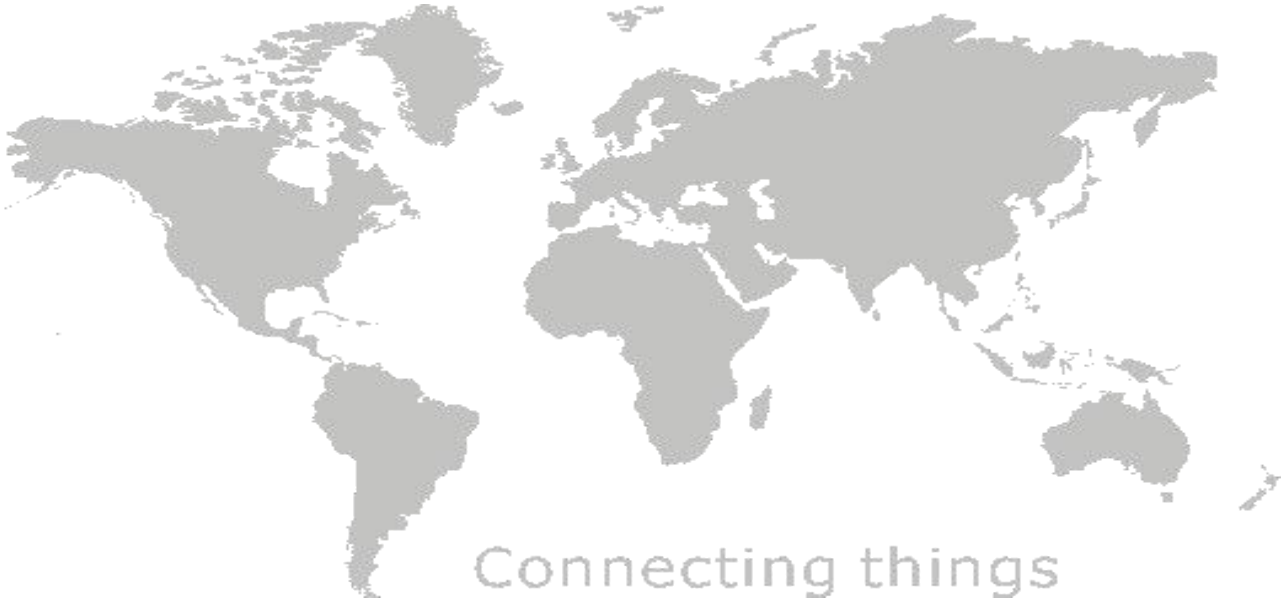
使用说明书

工业智能网关

宏电 Hongdian



深圳市宏电技术股份有限公司为客户提供全方位的技术支持，用户可直接与公司总部联系。

深圳市宏电技术股份有限公司

地址： 深圳市龙岗区布澜大道中海信科技园总部中心14A栋16层

网址： http://www.hongdian.com

技术专线： 400-00-64288拨2

投诉热线： 400-00-64288拨3

传真： 0755-83644677

邮政编码： 518112

前 言

前言

工业智能网关/5G CPE 是宏电面向工业领域推出的带边缘计算能力的新一代 5G 工业网关产品。

本文档的主要功能在于：帮助读者了解本产品功能特点及典型应用方式、熟悉本产品安装部署及配置操作方法、掌握使用过程中常见故障处理。

读者对象

本文档适用于以下人员：

- 研发工程师
- 技术支持工程师
- 客户

如果是初次接触和使用工业网关产品，建议从第一章开始，阅读本文档全部内容，以便获得相应的产品了解和正确使用。

如果已经了解或使用过宏电工业网关产品，建议可通过文档结构导航选择性阅读想了解的章节内容。

内容简介

本文档对工业智能网关产品的使用进行了以下描述。

章节	内容
1 产品介绍	本章介绍工业智能网关及其功能特点、产品定位。
2 产品结构	本章介绍工业智能网关软件、硬件结构。
3 产品安装	本章介绍如何安装工业智能网关。
4 环境配置	本章介绍工业智能网关配置前准备工作。
5 产品配置	本章介绍工业智能网关功能配置操作。
6 其他功能	本章介绍工业智能网关的 RESET 功能。
7 异常处理	本章介绍工业智能网关使用过程中常见故障原因及处理方法。
0 参数规范表	介绍本文档中各类参数输入规范。
0 术语	介绍本文档中出现的术语。
0 缩略语	介绍本文档中出现的缩略语。

约定

符号约定

文中出现的下列标志所代表含义如下。

符号	说明
	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
	以本标志开始的文本能帮助解决某个问题或节省的时间。
	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

通用格式约定

格式	说明
宋体	正文采用宋体表示。
黑体	一级、二级、三级标题采用黑体。
楷体	警告、提示等内容一律用楷体，并且在内容前后增加线条与正文隔离。
“TerminalDisplay”格式	“Terminal Display”格式表示屏幕输出信息。此外，屏幕输出信息中夹杂的用户从终端输入的信息采用加粗字体表示。

图形界面元素引用约定

格式	意义
“”	带双引号“”的格式表示各类界面控件名称和数据表，如单击“确定”。
>	多级菜单用“>”隔开。如选择“文件>新建>文件夹”，表示选“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。

键盘操作约定

格式	意义
加“”的字符	表示键名。如“Enter”、“Tab”、“Backspace”、“a”等分别表示回车、制表、退格、小写字母 a。
“键 1+键 2”	表示在键盘上同时按下几个键。如“Ctrl+Alt+A”表示同时按下“Ctrl”、“Alt”、“A”这三个键。
“键 1，键 2”	表示先按第一键，释放，再按第二键。如“Alt，F”表示先按“Alt”键，释放后再按“F”键。

鼠标操作约定

格式	意义
单击	快速按下并释放鼠标的一个按钮。
双击	连续两次快速按下并释放鼠标的一个按钮。
拖动	按住鼠标的一个按钮不放，移动鼠标。

修改记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本	修订时间	修订人	修订说明
V1.0.0.0	2020-03-20	王攀	初稿

目 录

表格目录

插图目录

1 产品介绍

1.1 功能与特点

基本功能

网络接入

- 支持 WAN、WLAN、4G/5G 等多网同时在线、多网备份切换
- 支持 WLAN AP/station 客户端功能，实现最高 1200Mbps 的无线局域网传输速率
- 支持 3 个千兆 LAN，1 个千兆 WAN 口
- 支持宏电自主研发多参数多功能组合切换功能，实现多服务器的灵活快速通信切换和单卡多运营商切换
- 支持 VPDN、APN 专网接入
- 支持 IPSec、GRE、IPIP、PPTP、L2TP、OpenVPN 支持 CA 数字证书

智能管理

- 支持 QoS，可针对业务、IP 网段进行多种方式的 QoS 带宽智能管理
- 支持静态路由、支持 RIPv2 和 OSPF 动态路由、支持源地址策略路由
- 支持定时管理，支持定时下线或者数据空闲下线
- 支持 M2M 平台管理，可实时统计设备流量、监控设备网络状态
- 支持 LCP 检测、ICMP 检测、心跳包检测等链路检测功能，保障无线网络稳定可靠
- LED 状态监测（显示系统、4G/5G 网络类型和信号强度等状态）

网络监控

- 支持 M2M 平台管理，可实时统计设备流量、监控设备网络状态
- 支持 SNMP 网络管理功能
- 提供系统本地日志和远程日志发送，实现网络实时监控
- 支持 NR、LTE、HSPA+、CDMA 2000 EV-DO Rev.A、WCDMA（HSDPA，HSUPA）、TD-SCDMA 等网络，同时向下兼容 GPRS/EDGE 或 CDMA 1X 网络

运维管理

- 支持本地或远程进行固件或补丁升级
- 支持 WEB、CLI、平台多种参数管理方式
- 支持参数备份及导入，支持使用私钥导入导出参数配置
- 支持 TF 卡进行系统升级维护
- 支持设备内部存储，支持 SATA 硬盘、TF 卡扩展存储

其他功能

- 支持 NTP 网络对时功能
- 支持 RTC 实时时钟功能

2 产品结构

关于本章

章节	内容简介
2.1 硬件结构	本节简要介绍工业智能网关硬件结构。
2.2 功能结构	本节简要介绍工业智能网关产品功能结构。

2.1 硬件结构

2.1.1 设备外观与尺寸

外观图

宏电工业智能网关外观实物图如图 2-1 所示。

图 2-1 工业智能网关外观实物图

尺寸

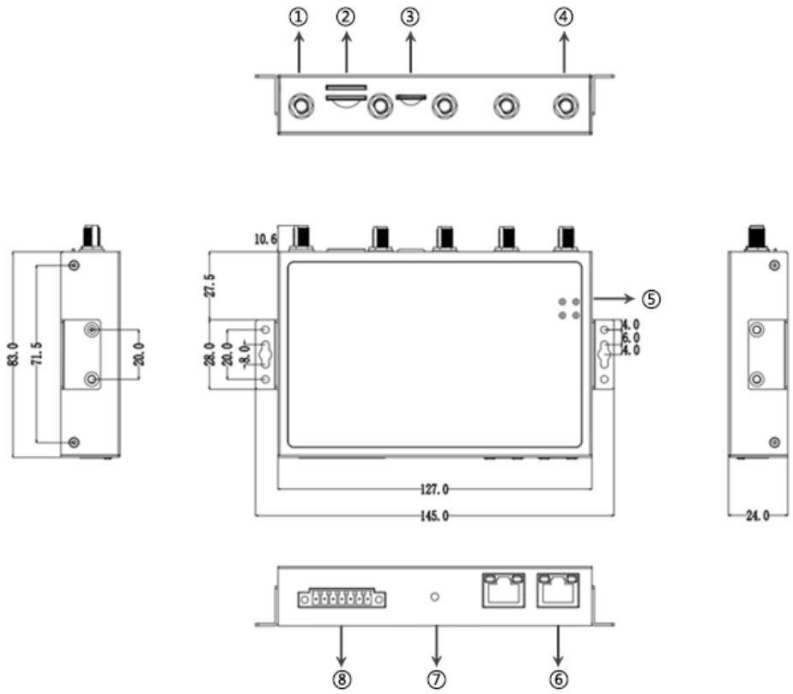


图 2-2 工业智能网关结构尺寸图

2.1.2 设备的配置以及配件

配件说明

表 2-1 工业智能网关配件清单

配件名称	数量	备注
标配		
工业智能网关主机	1 个	据用户订货情况包装
标准 RJ45 接口网线	1 个	1.5m
天线盒子	1 个	1*WiFi+4*5G
安装固定件	1 个	无
合格证和保修卡	1 份	无

工业智能网关支持外置防水套管，防护等级可达 IP66,。若有防水需求，可联系我司销售或技术支持人员。

3 产品安装

关于本章

章节	内容简介
3.1 开箱	本节简要介绍工业智能网关产品安装时开箱操作及需要检查的设备清单。

3.2 安装与接线	本节简要介绍工业智能网关产品 SIM/UIM 卡的安装和以太网连接、串口线连接等。
3.3 供电电源	本节简要介绍工业智能网关的供电要求及供电方法。
3.4 安装检查	本节简要介绍工业智能网关安装后检查操作。

3.1 开箱

设备到达现场后，需要开箱并检验配件是否齐全。正常情况下，整套设备应包含的配件如表 2-2 所示。开箱后保管好包装材料，以备二次转运过程中需要使用。

3.2 安装与接线

3.2.1 SIM 卡的安装

工业智能网关支持双 SIM 卡，在正常安装使用过程中需要分别为两个 SIM 卡槽安装 SIM。

注意

在进行 SIM 卡安装时，请确保产品处于断电状态。

步骤 1 SIM1：用 SIM 卡芯片朝向下方插入 SIM 卡槽中靠上方的卡槽即可

步骤 2 SIM2：用 SIM 卡芯片朝向上方插入 SIM 卡槽中靠下方的卡槽即可。

---结束

3.2.2 以太网线连接

工业智能网关配置使用简单，通过以太网网线连接即可进行正常的配置管理和数据通信。以太网连接可以分为单设备直连方式和多设备局域网连接方式。

单设备直连方式

使用 RJ-45 类型接头的以太网线将配置电脑与工业智能网关的 LAN 口中的任何一个直接连接。

以太网线的连接

工业智能网关支持 3 个 LAN 口和 1 个 WAN 口的局域网/广域网的连接，可以使用 RJ45 网线将网线的一端插入网关的 LAN 接口，另一端连接其他设备即可。

3.3 供电电源

工业智能网关产品使用+9V～+24V 直流供电。

3.4 安装检查

安装并准备上电前，查看一下 SIM 卡，检查卡有没有插紧。插上电后检查网关工作状态指示灯，在插上电的一瞬间所有灯都会亮起，接下来，SYS 灯会亮，过一段时间，连接 PC 的 LAN 灯会亮起，表示系统已经启动并和 PC 建立了连接。

上电前务必连接天线，以免射频部分阻抗失配，导致信号差而无法拨号上线。

操作步骤

步骤 1 检查天线连接是否正确。

步骤 2 检查 SIM 卡是否安装无误，并确认 SIM 卡是否有效。

步骤 3 给工业智能网关供电，下面仅以内部的 SIM 卡来说明网关的拨号情况，外部的 SIM 相同。

- 供电后如果工业智能网关上接有下位机的 LAN 口灯亮，表示网关供电正常。
- 供电 10s 后，工业智能网关 SYS 指示灯亮，表示网关系统已启动。
- 在 SYS 指示灯亮一段时间后，NET 指示灯亮并快闪，表示网关已找到模块并开始拨号。
- 网关在拨号过程中，SIG 灯会亮，表示网关已获得 SIM 卡信号强度。详情请参见“4.1 终端面板指示灯状态”。
- 网关拨号结束后，若 NET 灯常亮，则表示拨上的网络是 4G/5G。若慢闪，表示拨上的网络为 2G/3G 网络。

说明

对于不同的模块，网关找到模块的时间不一致，且因网络不同，拨号的时间也不同；所以对于不同的模块，网关拨号并获得 IP 地址的时间可能不一致，但网关拨号流程则严格按照上面所述。

---结束

4 环境配置

关于本章

章节	内容简介
4.1 终端面板指示灯状态	本节简要介绍工业智能网关终端面板指示灯状态。
4.2 本地连接配置	本节简要介绍工业智能网关安装后本地连接配置过程。

4.1 终端面板指示灯状态

工业智能网关前面板上有 4 个 LED 指示灯，指示工业智能网关的工作状态和网络状态。指示灯状态说明如表 4-1 所示。

表 4-1 指示灯说明表

指示灯	指示灯名称	状态说明

SYS	系统状态指示灯（绿色）	常亮：表示系统正常 闪烁：表示正在初始化 灭：系统异常
WiFi	无线指示灯（绿色）	常亮：同时开启 2.4GHz 和 5GHz WiFi 慢闪：只启用 2.4GHz WiFi 灯 快闪：只启用 5GHz WiFi 灯 灭：2.4GHz 和 5GHz Wi-Fi 都不启用
NET	网络连接指示灯（绿色）	常亮：拨号成功，接入 4G/5G 网络 慢闪（2s 闪）：拨号成功，接入 2G/3G 网络 快闪（0.5s 闪）：正在拨号 灭：不能正常通讯（未找到模块或者禁用拨号）
SIG	信号强度指示灯（绿色）	常亮：信号强（CSQ>20） 闪烁：信号弱（0<CSQ≤20） 灭：没有信号（CSQ=0）

4.2 本地连接配置

前提条件

智能网关供电。

- 已经通过以太网网线连接工业智能网关网口。

以太网连接具体操作请参见“3.2.2 以太网线连接”。工业智能网关本地连接配置包含指定 IP 方式和 DHCP 自动获取 IP 方式，下文分别对这两种配置方式做详细说明。

指定 IP 方式

步骤 1 单击“开始>控制面板>网络和 Internet>网络共享中心”，如图 4-1 所示。

图 4-1 网络连接窗口

步骤 2 单击“本地连接”，打开“本地连接状态”窗口，如图 4-2 所示。

图 4-2 本地连接状态

步骤 3 在“本地连接状态”窗口中单击“属性”，打开“本地连接属性”窗口，如图 4-3 所示。

图 4-3 Internet 协议（TCP/IPv4）

后面的配置存在两种配置方法，即常规方法配置和高级配置。

- 常规方法配置

  1. 在“本地连接属性”窗口中双击“Internet 协议（TCP/IP）”，打开 Internet 协议（TCP/IP）属性窗口。在“常规”选项卡中修改常规网络配置。如图 4-4 所示。

注意

由于工业智能网关出厂默认参数中，

- IP 地址：192.168.8.1
- 子网掩码：255.255.255.0

因此，“Internet 协议（TCP/IP）属性”窗口中，“默认网关”和“子网掩码”配置为工业智能网关出厂默认值。

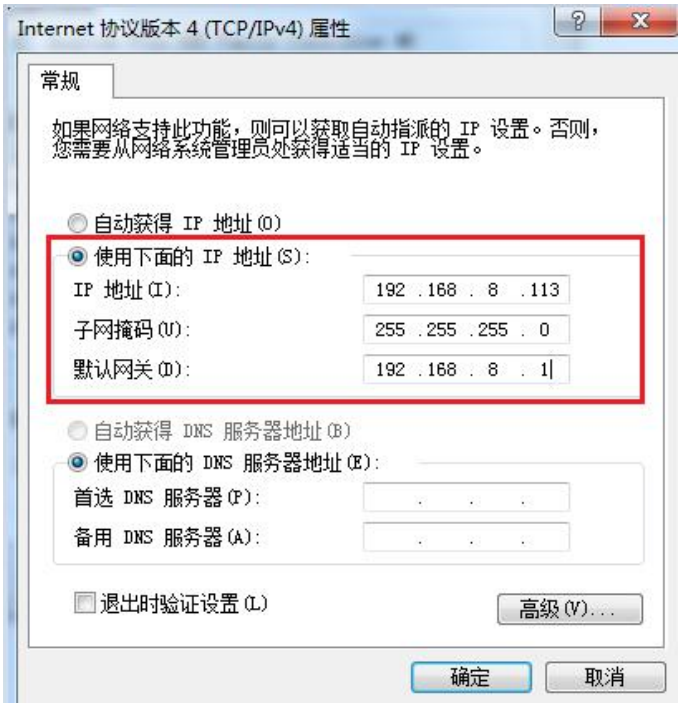


图 4-4 Internet 协议（TCP/IPv4）属性窗口 3

注：IP 地址可以为 192.168.8.*（其中*表示 2～254 的任意整数）。

2. 单击“确定”，完成配置。

- 高级配置

  该方法即在原有网络环境配置（步骤 1～步骤 3）下不希望中断本地 PC 机继续局域网通信，又能对工业智能网关进行配置时，可考虑添加高级配置。

  1. 单击“高级”，打开“高级 TCP/IP 设置”，如图 4-5 所示。

图 4-5 高级 TCP/IP 设置

2. 单击“IP 地址(R)”中的“添加”，填写需要配置的 IP 地址，如图 4-6 所示。

图 4-6 TCP/IP 地址

3. 单击“添加”，完成配置。

---结束

DHCP 自动获取 IP 方式

工业智能网关内置 DHCP（Dynamic Host Configuration Protocol）服务器，自动按照预先设定的参数对连接在其上的终端(或 PC 等)分配 IP（Internet Protocol）地址。

说明

工业智能网关内置的 DHCP 服务在出厂时处于开启状态，在没有对该功能进行配置之前，DHCP 服务都是开启的。

步骤 1 单击“开始>控制面板>网络和 Internet>网络连接”，如图 4-7 所示。

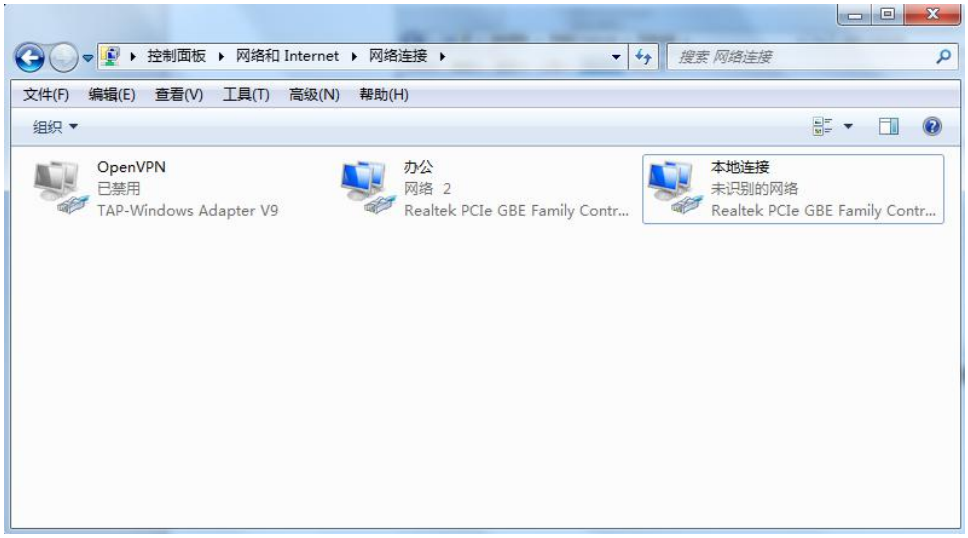


图 4-7 网络连接窗口

步骤 2 右键单击“本地连接”并在弹出的菜单中单击“属性”，打开“本地连接窗口”，如图 4-8 所示。

图 4-8 本地连接属性

步骤 3 在“此连接使用下列项目(0):”中，选择“Internet 协议版本 4（TCP/IPv4）”并双击进入“Internet 协议版本 4（TCP/IPv4）属性”窗口，如图 4-9 所示。

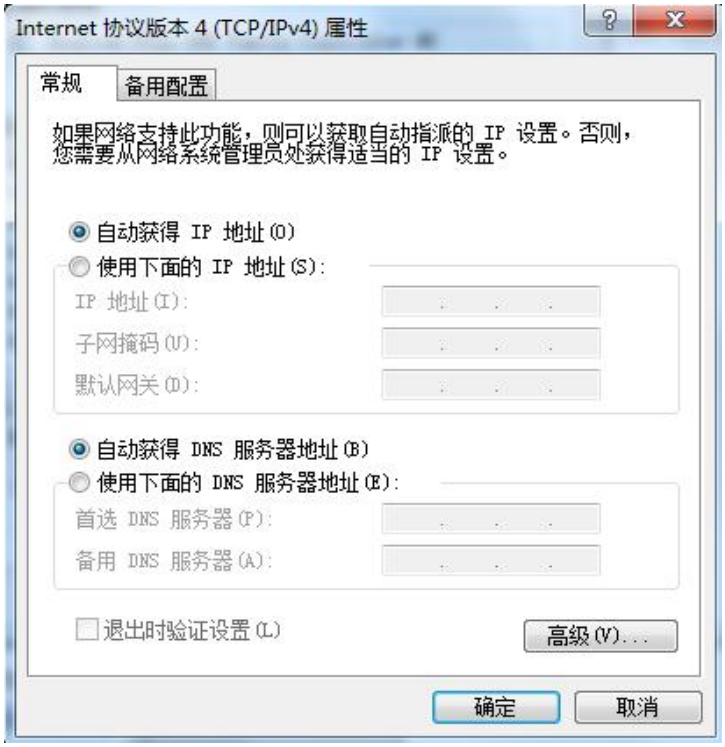


图 4-9 Internet 协议版本 4（TCP/IP）属性

步骤 4 如果 Internet 协议版本 4（TCP/IPv4）属性如图 4-9 所示，则无需改动；如果 Internet 协议版本 4（TCP/IPv4）属性不是图 4-9 所示，则在“常规”中选择“自动获得 IP 地址”。

步骤 5 单击“确定”完成配置。

---结束

配置检查

步骤 6 单击“开始>运行”，在“运行”输入框中输入“**cmd**”命令后按回车键。打开“运行”窗口，如图 4-10 所示。

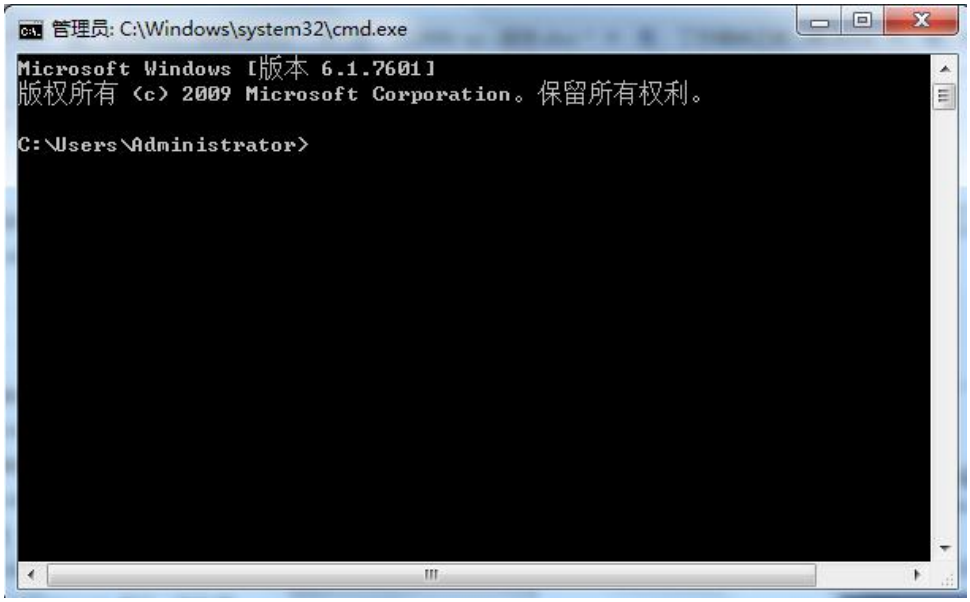


图 4-10 “运行”窗口

步骤 7 在“运行”窗口中输入命令“**ipconfig**”，对上述两种连接的配置方法，“ipconfig”窗口中显示的 IP Address 是不一样的：指定 IP 方式的配置方法中 IP Address 显示的是输入的图 4-6 中的 IP 地址，如图 4-11 所示；以网关 DHCP 自动获取 IP 的配置方法中 IP Address 显示的“2～254”的随机数字，如图 4-12 所示。窗口显示如图 4-13 所示信息表示 IP 配置正常。

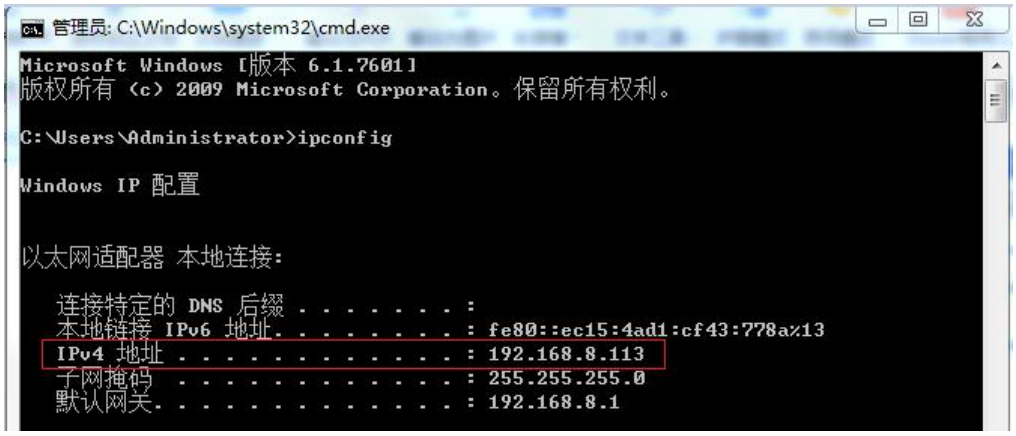


图 4-11 指定 IP 方式的“ipconfig”执行结果

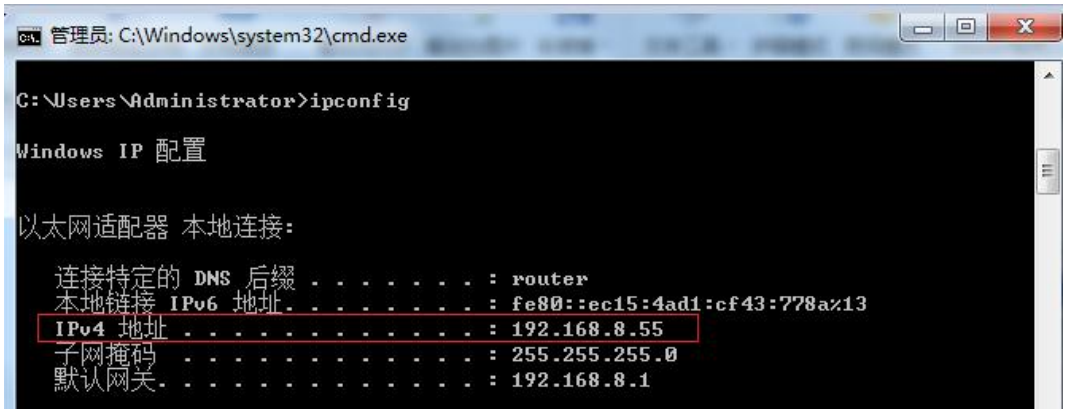


图 4-12 DHPC 自动获取 IP 方式“ipconfig”执行结果

步骤 8 在命令行窗口中输入如下命令确认连通性是否正常。

ping *192.168.8.1*

如果出现如图 4-13 所示界面，表示本地计算机与工业智能网关连通性正常。

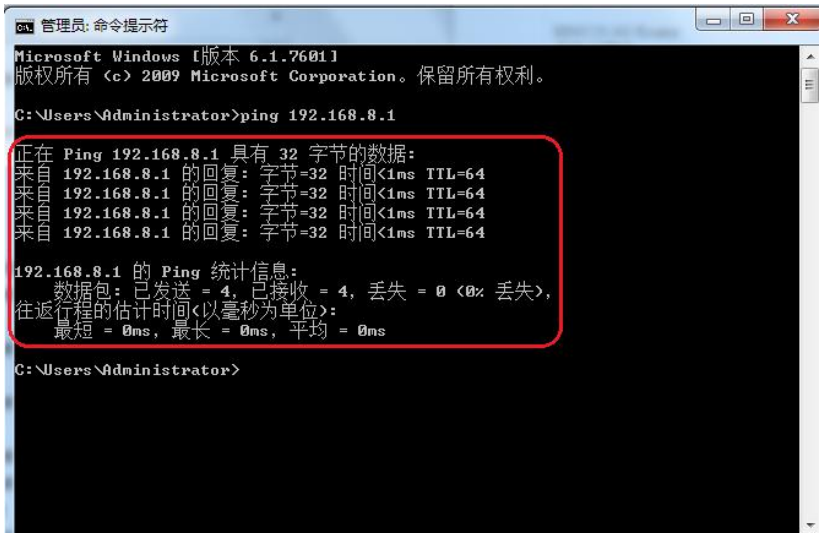


图 4-13 连通性验证结果

---结束

5 产品配置

关于本章

章节	内容简介
5.1 概述	本节简要介绍工业智能网关如何连接以及配置。
5.2 登录配置	本节简要介绍工业智能网关如何配置登录 WEB 页面。
5.3 运行状态	本节简要介绍工业智能网关网络的运行状态。
5.4 网络设置	本节简要介绍工业智能网关网络配置包含哪些，以及具体配置操作方法。
5.5 应用设置	本节简要介绍工业智能网关应用程序配置包含哪些，以及具体配置操作方法。
5.6 运维管理	本节简要介绍工业智能网关运维管理包含哪些，以及具体配置操作方法。
5.7 平台管理	本节简要介绍工业智能网关平台管理包含哪些，以及具体配置操作方法。
5.8 系统管理	本节简要介绍工业智能网关系统管理配置包含哪些，以及具体的配置操作方法。

5.1 概述

工业智能网关可采用 WEB 方式进行配置操作，该方式具有操作简便、直观等特点。按照“本地连接配置”完成 PC 机和工业智能网关的本地连接配置后可在 PC 机上启动 Internet Explorer 或者其他浏览器，登录到工业智能网关进行配置操作。

- 支持 IE11 浏览器
- 支持 Google Chrome 浏览器
- 支持 Firefox 浏览器
- 支持 Edge 浏览器

5.2 登录配置

打开配置电脑 IE 浏览器，在地址栏内输入“http://192.168.8.1/”。进入工业智能网关设备登录界面，如图 5-1 所示，输入用户名和密码，进入 WEB 配置页面。

图 5-1 工业智能网关设备登录界面

说明

用户初次登录系统时，须使用缺省用户名和密码。缺省用户名为“admin”、密码为“admin”。如需修改密码，请参见“5.7.5 用户管理”。

---结束

5.3 运行状态

工业智能网关提供状态显示信息。通过运行状态页面能快速查看路由器的的基本信息、网络状态以及路由表信息。运行状态主要完成设备的运行状态展示，包含上网速率、无线上网时长、稳定运行时间、终端连接数量、CPU/内存占用、流量统计等功能，可以查看设备的各项参数配置是否正确及设备是否正常运行。

5.3.1 运行状态

图 5-2 运行状态

表 5-1 运行状态参数说明

参数名称	含义	如何配置
上网速率	显示设备通过 WAN 口、modem、WiFi 上网时的上下行速率。	单位：bps，自动刷新。
WiFi/LAN	WiFi：WiFi ap、station 模式打开，且有终端通过 WiFi 连接此 AP（或已连接上其他 AP）时，线条为绿色，否则线条为灰色； LAN：有终端通过设备 LAN 口接入时，线条为绿色，否则为灰色。	请留意线条颜色，自动刷新。
无线上网时长	通过 modem 或 WiFi station 上网的时长，多种方式同时上网时，时长为根据默认路由来判断及统计。	自动刷新。
稳定运行时间	显示设备从上电开始的时长。	自动刷新。
终端连接数量	显示当前通过 LAN 和 WiFi 连接的终端数量。	自动刷新。

运行状态页面实时 2s 刷新一次，如果显示有问题，请清除浏览器缓存后重新刷新。

5.3.2 路由器

点击运行状态页面上方路由器图标，切换到路由器状态页面。显示路由器的工作状态，包含系统信息、路由信息两部分。

系统信息

显示设备的产品型号、软件版本、硬件版本以及、序列号，当前 CPU 占用、内存占用比率以及拨号上网的流量统计、终端的流量统计。如图 5-3 所示。

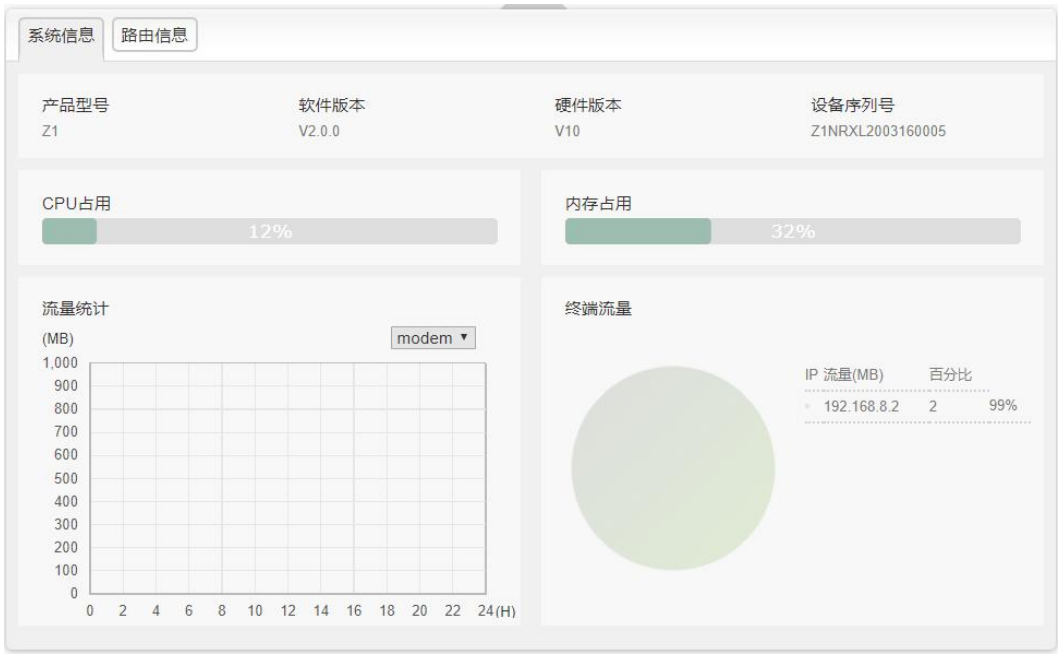


图 5-3 系统信息

表 5-2 系统信息参数说明

参数名称	含义	如何配置
设备序列号	设备的序列号信息	不可配
流量统计	统计模块 modem 上网的流量。	（1）横坐标时间（小时：H），纵坐标流量（单位：MB）；双模时可选择 modem/modem2； （2）时间为从设备上电后开始计算的时长。
终端流量	统计通过 LAN 或者 WiFi 接入设备的终端流量，以 IP 地址来统计。	扇形图只显示占用前四的终端流量占比以及“其他”终端占用的流量总和占比，右边显示流量值及占比。

路由信息

显示设备运行时的静态路由和策略路由情况。如图 5-4 所示。

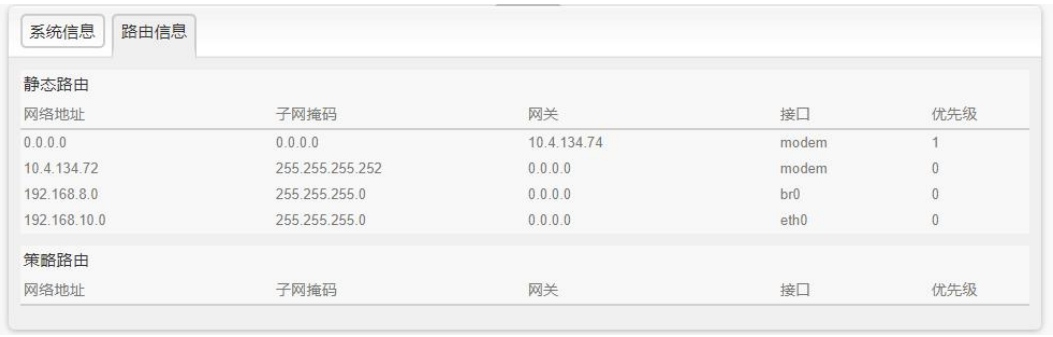


图 5-4 静态路由信息

表 5-3 路由信息参数说明

参数名称	含义	如何配置
静态路由		
目的 IP	路由器可达的 IP 地址	不可配
子网掩码	路由器可达的 IP 网络，与目的地址一起使用	不可配
网关	路由器要到达目的 IP 的下一条地址	不可配
接口	路由器到网关经过的接口	不可配
度量	路由器到达目的 IP 讲过的路由器条数	不可配
策略路由		
优先级	路由器选择路由的优先级	不可配

5.3.3 互联网

点击运行状态页面上方互联网图标，切换到互联网状态页面。显示设备上网的状态信息，包含 Modem 状态、SIM 状态、WAN 状态。

Modem 状态

显示设备拨号模块的运行状态及基本信息，包含联网状态、网络类型、在线时间、信号强度、域名服务器、接口 IP 地址、接口网关地址、MAC 地址、模块 IMEI 号、基站 LAC、小区 ID。

点击修改配置，可跳转到网络设置-移动网络，如图 5-5 所示。

图 5-5 Modem 状态

表 5-4 Modem 信息参数说明

参数名称	含义	如何配置
网络类型	当前移动网络拨号的 Modem 网络类型。	不可配
在线时间	显示拨号上线后的的在线时长。	不可配
信号强度	当前拨号的 Modem 网络的信号强度。	不可配
网络类型	当前生效的 SIM 卡对应的网络类型。	不可配
信号强度	无线网络的信号强度。 取值范围：1～31 若没有信号时，则无法成功拨号。	不可配
IP 地址	拨号时获取的外网 IP 地址。	不可配
域名服务器	拨号时获取的首选 DNS 地址。	不可配

SIM 状态

显示设备当前所插入的 SIM 卡状态，包含 SIM 卡状态、SIM 卡位置、ICCID、IMSI。如图 5-6 所示。

图 5-6 SIM 状态

表 5-5 SIM 信息参数说明

参数名称	含义	如何配置
位置	当前 SIM 插入的卡槽位置。	不可配
状态	X2 4G Router 当前使用的卡槽对应的 SIM 的工作状态。	不可配

WAN 状态

显示设备当前 WAN 口状态，包含连接类型、IP 地址、子网掩码、MAC；

点击-修改配置，可跳转到网络设置-WAN。如图 5-7 所示。

图 5-7 WAN 状态

表 5-6 WAN 信息参数说明

参数名称	含义	如何配置
WAN 口类型	显示当前 WAN 接口的类型。	不可配
IP 地址	显示 WAN 口配置的本地 IP 地址。	不可配
子网掩码	显示配置的 WAN 接口所在的网络地址号。	不可配
MAC	显示 LAN 网口卡物理地址，此地址一般情况下固定且唯一。	不可配

5.3.4 下位机

点击运行状态页面上方下位机图标，切换到下位机状态页面。显示当前接入网关设备的下位机状态信息，包含 LAN 状态、WiFi2.4G 状态、WiFi5.8G 状态。

LAN 状态

显示 LAN 口状态及通过 LAN 接入的下位机信息，包含连接状态、IP 地址、子网掩码、MAC 地址，终端的 IPV4 地址、IPV6 地址、MAC 地址、流量值。

点击-修改配置，可跳转到网络设置-LAN。如图 5-8 所示。

图 5-8 LAN 状态

表 5-7 LAN 信息参数说明

参数名称	含义	如何配置
连接状态	显示当前 LAN 接口的连接状态。	不可配
IP 地址	显示 LAN 口配置的本地 IP 地址。	不可配
子网掩码	显示配置的 LAN 接口所在的网络地址号。	不可配
MAC	显示 LAN 网口卡物理地址，此地址一般情况下固定且唯一。	不可配

WiFi2.4G 状态

显示 WiFi2.4G 状态及通过 WiFi2.4G 接入的下位机信息，包含连接状态、工作模式、SSID、IP 地址、网关地址，终端的 IPV4 地址、IPV6 地址、MAC 地址、流量值。

点击-修改配置，可跳转到网络设置-WiFi2.4G。如图 5-9 所示。

图 5-9 WiFi2.4G 状态

表 5-8 WiFi2.4G 信息参数说明

参数名称	含义	如何配置
连接状态	显示当前 WiFi2.4G 接口的连接状态。	不可配
工作模式	WLAN 的工作模式。	不可配
SSID	AP 的表示。	不可配
IP 地址	显示 WiFi2.4G 的 IP 地址。	不可配
网关地址	设备的物理地址。	不可配

WiFi5.8G 状态

显示 WiFi5.8G 状态及通过 WiFi5.8G 接入的下位机信息，包含连接状态、工作模式、SSID、IP 地址、网关地址，终端的 IPV4 地址、IPV6 地址、MAC 地址、流量值。

点击-修改配置，可跳转到网络设置-WiFi5.8G。如图 5-10 所示。

图 5-10 WiFi5.8G 状态

表 5-9 WiFi2.4G 信息参数说明

参数名称	含义	如何配置
连接状态	显示当前 WiFi2.4G 接口的连接状态。	不可配
工作模式	WLAN 的工作模式。	不可配
SSID	AP 的表示。	不可配
IP 地址	显示 WiFi2.4G 的 IP 地址。	不可配
网关地址	设备的物理地址。	不可配

5.4 网络设置

网络设置主要完成 LAN、WAN、WiFi、移动网络、参数切换以及网络连接、链路备份、VPN 设置、DHCP 服务器等配置。配置完成后可满足基本网络通信需要。

5.4.1 LAN

LAN 口配置主要用于网关与下位机连接，使下位机可以通过网关访问外网，同时保证连接在网关上的各个网段之间能够正常通信。

步骤 1 登录工业智能网关的 WEB 配置界面。

步骤 2 单击“网络设置> LAN”。

打开“LAN”页签，如图 5-11 所示。

图 5-11 LAN 页签

步骤 3 配置 LAN 口连接参数，参数说明如表 5-10 所示。

表 5-10 LAN 口连接类型参数说明

参数名称	含义	如何配置
主机名	网关的名称。	手动输入，最大长度不超过 32 位的一般 WORD 型字符串，输入规范请参见“参数规范表”。
IP1～4	用于划分子网，这些子网之间能够相互通信，IP1～4 代表了 4 个子网。	手动输入。 格式：A.B.C.D/M 接口型，输入规范请参见“参数规范表” IP1 默认值：192.168.8.1/24，IP2～4 按上述格式输入，但两两之间的内容不能相同。
回环地址	网关的虚拟接口地址，配置之后不会因 LAN 接口关闭而消失。	手动输入。 格式：A.B.C.D/M 接口型，输入规范请参见“参数规范表”。

步骤 4 单击“保存”，完成 LAN 口连接类型的配置。

说明

用户在修改 IP1 地址时，如果页面没有自动跳转，请确保用户的电脑上有与修改后的 LAN 地址在同一网段的地址，或者设置电脑为自动获取 IP，然后在浏览器中输入新的 IP1 地址。

---结束

5.4.2 WAN

WAN 主要用于通过以太网连接 Internet，连接方式有静态 IP、DHCP、PPPoE 三种方式。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“网络设置> WAN”。

打开“WAN”页签，如图 5-12 所示。

图 5-12 WAN 页签

步骤 3 配置 WAN 口连接类型。

参数说明如表 5-11 所示。

表 5-11 WAN 口连接类型参数说明

参数名称	含义	如何配置
连接类型	广域网的连接类型。	下拉框选择，包含： • 静态 IP：手动配置接口 IP，若需要通过 WAN 上网则需要在网络连接类型中补充网关、DNS、默认路由等配置。 • DHCP：DHCP 客户端自动获取 IP 方式，若需要通过 WAN 上网，则需在网络连接类型中补充默认路由配置。 • PPPoE：PPPoE 拨号获取 IP 方式（通常是外接 ADSL 猫进行 ADSL 拨号上网），若需要通过 WAN 上网，则需要在网络类型类型中补充默认路由配置。
IP：**“连接类型”选择“静态 IP”时显示**		

参数名称	含义	如何配置
IP	当“连接类型”选择“静态 IP”时需配置。	接口型 A.B.C.D/M， 输入规范请参见“参数规范表” 例如：192.168.10.1/24
基本设置：**“连接类型”选择“PPPoE”时显示**		
接口名称	接口的唯一标识名，用于其他功能调用或者关联本接口时使用，如配置该接口的路由、控制该规则接口的禁用、启用。	PPPoE 不可配置项。 网页配置的 PPPoE 接口名由系统指定，其接口名是：pppoe
服务名称	配置 PPPoE 服务名，通常是用于客户端与服务端之间的身份识别与判断，通常由服务端提供，ADSL 拨号时由 ISP 提供。	一般 WORD 类型，最大 64 字节，不能为空，输入规范请参见“参数规范表”。
用户名/密码	PPPoE 拨号所用用户名/密码，通常由服务器端提供，ADSL 拨号时由 ISP 提供。	一般 WORD 类型/CODE 类型，各最大长度 64 字节，均非空，输入规范请参见“参数规范表”。
高级设置	高级参数在特殊情况下使用，通常不建议配置，“高级设置”的参数说明，请参见表 5-3 中的相关参数。	单击“显示”即可显示高级设置参数。

步骤 4 单击“保存”，完成 WAN 口连接类型配置。

---结束

5.4.3 WiFi2.4G

工业智能网关提供 WiFi AP 和 Station 客户端，通过 AP 功能，工业智能网关可以为提供无线局域网热点；通过 Station 客户端功能，可以让工业智能网关接入其他的 AP 设备，这样工业智能网关的下位机可以通过连接的 AP 设备访问外网。

步骤 1 登录工业智能网关的 WEB 配置界面。

步骤 2 单击“网络设置>WiFi2.4G”。

打开“WiFi2.4G”页签，当选择不同工作模式（AP、Station）时，显示页面分别如图 5-17、图 5-18 所示。当 WiFi 工作模式选择 Station 时，需要扫描周围 AP，以选择一个 AP 接入，如图 5-19 所示。

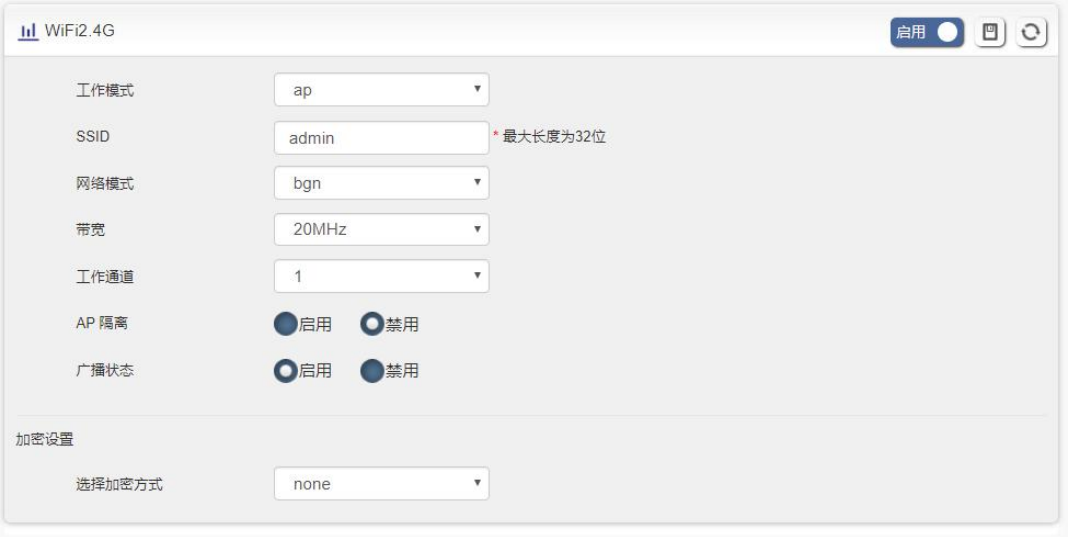


图 5-13 AP 模式配置页签

图 5-14 Station 模式配置页签

图 5-15 选择 station 时的扫描页签

步骤 3 单击“网络设置>WiFi5.8G”。WiFi5.8G 配置页签如图 5-20。

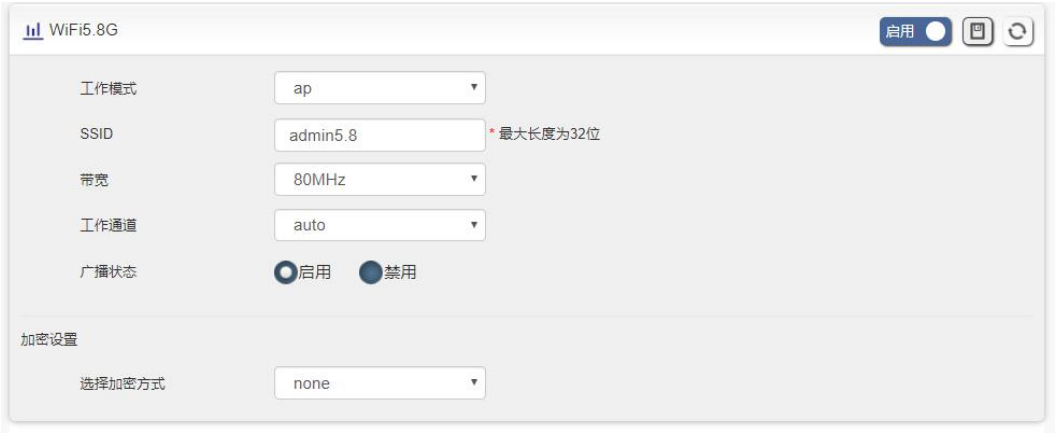


图 5-16 WiFi5.8G 配置页签

步骤 4 配置“WiFi”相关参数。

参数说明如表 5-12 所示。

表 5-12 WiFi 参数说明

参数名称	含义	如何配置
WiFi 状态	使能 WiFi 功能	按钮选择，当前按钮为“启用”时，表示当前 WiFi 功能已开启；当前显示为“禁用”时，表示当前 WiFi 功能已禁用。 • 启用 • 禁用
基本信息		
SSID	WiFi 服务端身份标识。	一般 WORD 类型，最大 32 字节，输入规范请参见“参数规范表”。

参数名称	含义	如何配置
工作模式	WiFi 工作模式，支持 ap/station 模式。	下拉框选项 • ap • station
网络模式	WiFi 网络模式，不同网络模式传输速率有较大差异，默认 bgn 混合模式。当工作模式选择 AP 时，需要手动设置 AP 的网络模式；当工作模式选择 station 时，网络模式为选择的 AP 的网络模式，不可手动修改。	下拉框选项 • n 表示 WiFi 的速率为 400Mbps • bg 表示 WiFi 速度为 11Mbps、54Mbps 自适应 • bgn 表示可支持 11Mbps、54Mbps、400Mbps 的混合模式，根据接入的 WiFi 客户端自适应
工作通道	WiFi 的工作信道，根据网络环境具体需求配置，默认 auto。	下拉框选项 WiFi_2.4G • auto • 1～13 WiFi_5.8G • auto • 149～165 auto 表示信道自适应
带宽	WiFi 工作在 802.11b/g/n 和 802.ac 模式下的带宽配置。	下拉框选项 WiFi_2.4G • 20MHz • 40MHz 40MHz 表示 802.11n 的高速模式 WiFi_5G • 20MHz • 40MHz • 80MHz
AP 隔离	将接入 AP 的 WiFi 客户端进行隔离，使各客户端之间相互不能访问。	单选按钮选择 • 启用 • 禁用
广播状态	用于配置 WiFiSSID 是否广播出去以便客户端能搜索到该 SSID，通常在不希望其他人搜索并使用 WiFi 功能时禁用，禁用则表示在网络环境中隐藏 SSID 功能，用户若要连接，需手动添加该 SSID。	单选框选择 • 启用 • 禁用
IP 分配（当工作模式选择 station 时需要配置）	当工业智能网关做 station 连接到 AP 时与 AP 通信的地址。	下拉框选项 • dhcp：通过 AP 的 DHCP 功能获得 IP 地址 • static：手动设置 IP 地址
IP(当工作模式	当“IP 分配”选择 static 时需要	格式：A.B.C.D 型，输入规范请参

参数名称	含义	如何配置
选择 station 时需要配置）	配置，与 AP 建立通信的地址。	见“参数规范表”
WiFi 加密		
加密方式	配置 WiFi 的加密方式，当不需要加密验证时可以 disable。	下拉框选项 • none • wpa • wpa2
wpa/wpa2（WiFi Protected Access，WiFi 网络安全存取）		
加密算法	加密采用算法 • tkip • aes	下拉框选项选择。
无线密码	WiFi 的加密密钥，用于连接指定 SSID。	字母数字 WORD 项，输入规范请参见“参数规范表”。

说明

当工作模式选择 station 时，工业智能网关会根据选择的 AP 自动匹配相应的加密方式和算法（以保持与 AP 的加密方式一致）；无线密码与更新时间间隔则需填写连接 AP 的密钥和间隔。

---结束

5.4.4 移动网络

移动网络是 Z1 工业智能网关最核心功能之一，工业智能网关支持单模单卡拨号、单模双卡备份拨号两种移动网络拨号方式，为用户提供高速无线宽带上网功能。

步骤 1 登录工业智能网关的 WEB 配置界面。

步骤 2 单击“网络设置>移动网络”。

打开“移动网络”页签，如图 5-13 所示。

图 5-17 移动网络页签

步骤 3 对“移动网络参数”的“添加”、“编辑”、“删除”、“启用”和“禁用”操作。

- 添加

  1. 单击“添加”，显示移动网络配置添加界面，如图 5-14 所示。

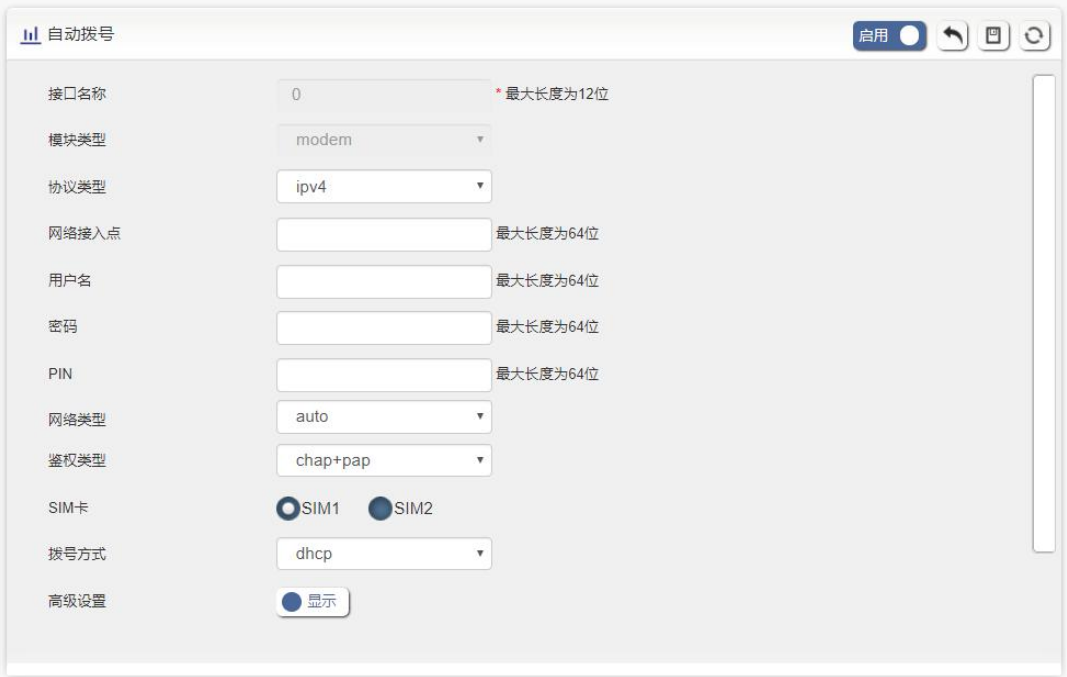


图 5-18 移动网络配置页面

2. 对“移动网络”参数进行添加操作。“移动网络”参数说明如表 5-13 所示。

表 5-13 移动网络参数说明

参数名称	含义	如何配置
接口名称	接口的唯一标识名，用于其他功能调用或者关联本接口时使用，如配置该接口的路由、控制该规则接口的禁用、启用。	字母数字型 WORD 类型，最大 12 字节，非空，输入规范请参见“参数规范表”。
模块类型	选择模块类型。	不可配置项，为 modem。
协议类型	选择拨号的协议类型，表示通过此协议拨号及获取相应的 IP 地址。	可选择 ipv4、ipv6、ipv4&ipv6。
网络接入点	接入运营商网络的一个标识信息，通常用于表示接入到运营商网络的类型，专网业务情况通常按照专网的业务类型来命名，由运营商或 ISP 提供。通常情况下 G 网运营商才有接入点配置。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。
用户名/密码	接入运营商网络身份标识，专网业务情况下用于接入到不同的专网业务中来隔离不同的专用网络。通常情况下 C 网运营商才有用户名密码，现在很多 G 网运营商也开始使用。	WORD 类型/CODE 类型，各最大长度 64 字节，同时存在或同时为空。

参数名称	含义	如何配置
PIN	Personal Identification Number，SIM 卡的识别密码，用户可以使用 PIN 码对 SIM 卡进行解锁和加锁，防止非法用户使用。	字母数字 WORD 型，输入规范请参见“参数规范表”。
网络类型	通过该选项将所需接入网络类型强制为 4G 或者 5G，或者自动拨号 auto。通常某一网络不稳定或者只希望工作在某一网络情况下使用。	下拉框选项 2G、3G 在本版本上没有强制网络类型；auto 表示 2G/3G/4G/5G 自适应，但如果有 5G 信号，会首先拨上 5G。
鉴权类型	选择拨号所采用的鉴权、认证协议类型。	默认 chap+pap。下拉框可选： • chap+pap • chap • pap • none
SIM 卡	单模双卡模式下配置选项，用于指定拨号时选择 SIM 卡。	单选框选择 • SIM1 • SIM2
拨号方式	用于选择拨号方式。	当前版本只支持 DHCP 拨号。
高级设置	用于配置 PPP 拨号的高级参数，通常情况下不建议配，通常在专网业务服务端有对应匹配要求情况下使用，本产品 VPDN、PPPoE 的拨号高级选项与 modem 高级选项一致，如图 5-8 所示。	单击即可显示高级设置。
认证&加密（配置时需要与服务端匹配，默认全部为协商）		
CHAP	挑战握手协议（Challenge-Handshake Authentication Protocol），是一种加密验证方式，能够避免建立连接时传送用户的真实密码。主要针对 PPP 的，认证时密钥信息不需要在通信信道中发送，而且每次认证所交换信息都不一样，可以很有效地避免监听攻击，安全性较高。	单选框选择 • 禁用 • 协商 **说明** 协商表示与服务器协商是否使用该认证，全部认证选择协商时优先使用 CHAP 先协商。
PAP	密码认证协议（Password Authentication Protocol）是一种简单的明文验证方式，要求将密钥信息在通信信道中明文传输，因此容易被网络窃听软件如 sniffer 等监听而泄漏。	单选框选择 • 禁用 • 协商 协商表示与服务器协商是否使用该认证。
MS-CHAP	MS-CHAP（MicrosoftChallenge-Handshake Authentication Protocol）也是一种加密验	单选框选择 • 禁用 • 协商

参数名称	含义	如何配置
	证机制，使用基于 MPPE 数据加密。	协商表示与服务器协商是否使用该认证。
MS2-CHAP	MS-CHAP 的第二个版本，也是一种加密验证机制。	单选框选择 • 禁用 • 协商 协商表示与服务器协商是否使用该认证。
EAP	PPP 扩展认证协议（Extensible Authentication Protocol）是一个用于 PPP 认证的通用协议，可以支持多种认证方法。EAP 并不在链路建立阶段指定认证方法，而是把这个过程推迟到认证阶段。这样认证方就可以在得到更多信息以后再决定使用什么认证方法。这种机制还答应 PPP 认证方简单地把收到的认证报文透传给后方认证服务器，由后方认证服务器来真正实现各种认证方法。	单选框选择 • 禁用 • 协商 协商表示与服务器协商是否使用该认证。
压缩&控制协议（配置时需要与服务端匹配，默认全部为禁用）		
压缩控制协议	负责在 PPP 链路上的两端配置并协商采用哪种压缩算法。并且用可靠方式来标志压缩和解压缩机制的失败。	单选框选择 • 接受 • 禁用
地址/控制压缩	是否允许进行 IP 地址和控制压缩设置。	单选框选择 • 接受 • 禁用
协议域压缩	是否启用协议域压缩。	单选框选择 • 接受 • 禁用
VJ TCP/IP 头部压缩	是否允许 TCP/IP 数据包进行 VJ 头部压缩。	单选框选择 • 接受 • 禁用
连接 ID 压缩	是否允许进行连接 ID 压缩。	单选框选择 • 接受 • 禁用
其它		
调试	使能 PPP 拨号时链路交互的调试日志，主要用于分析 PPP 拨号协商过程，默认打开，当设备可以正常运行又不希望看到过多调试信息可以关闭，默认为打开，不建议禁用。	单选框选择 • 启用 • 禁用
对端 DNS	使能 PPP 拨号时获取对端 DNS，DNS 是	单选框选择

参数名称	含义	如何配置
	上网时访问域名必备参数，当不希望下端设备访问域名是可以禁用，默认为打开，不建议禁用。	• 启用 • 禁用
LCP 间隔时间/LCP 重试次数	PPP 拨号成功之后需要通过 LCP 来维持 PPP 拨号链路，一方面维持连接，另一方面可以在异常的时候快速发现链路故障并且恢复。根据网络的实际情况可以适当调整，通常不建议修改该值。	取值范围：1～512 单位：秒 缺省值：30/5
最大传输单元	PPP 接口发送单个数据报的报文最大长度，通常拨号过程中与运营商协商得到。下位机有报文大小传输要求时配置，通常金融数据交互有此要求的较多。	取值范围：128～16364 单位：byte
最大接收单元	PPP 接口接收单个数据报的报文最大长度，通常拨号过程中与运营商协商得到，通常金融数据交互有此要求的较多。	取值范围：128～16364 单位：byte
本地 IP	PPP 拨号时指定本地 IP，以便使得本地获得的 IP 地址一直是固定的，通常在专网业务有此配置，需要运营商提供该服务才能配置。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：10.10.10.1
远端 IP	PPP 拨号协商 IP 地址时对端的身份识别，现大多数网络已经不使用该参数，通常指定本地 IP 即可，需要运营商提供该服务才能配置。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：10.10.10.254
专家选项	• nomppe：禁用微软点对点加密。 • mppe required：启用带状态微软点对点加密。 • mppe stateless：启用无状态微软点对点加密。 • nodeflate：禁用 Deflate 压缩。 • nobsdcomp：禁用 BSD-Compress 压缩。 • default-asyncmap：禁用 asyncmap 协商。 这里只列举了“专家选项的一部分”，更多专家选项请联系宏电技术支持工程师，在其指导下使用。	LINE 类型，输入规范请参见“参数规范表”。 配置时每一个协议换行区分，通常不建议使用该选项，如需使用需联系我司技术人员。

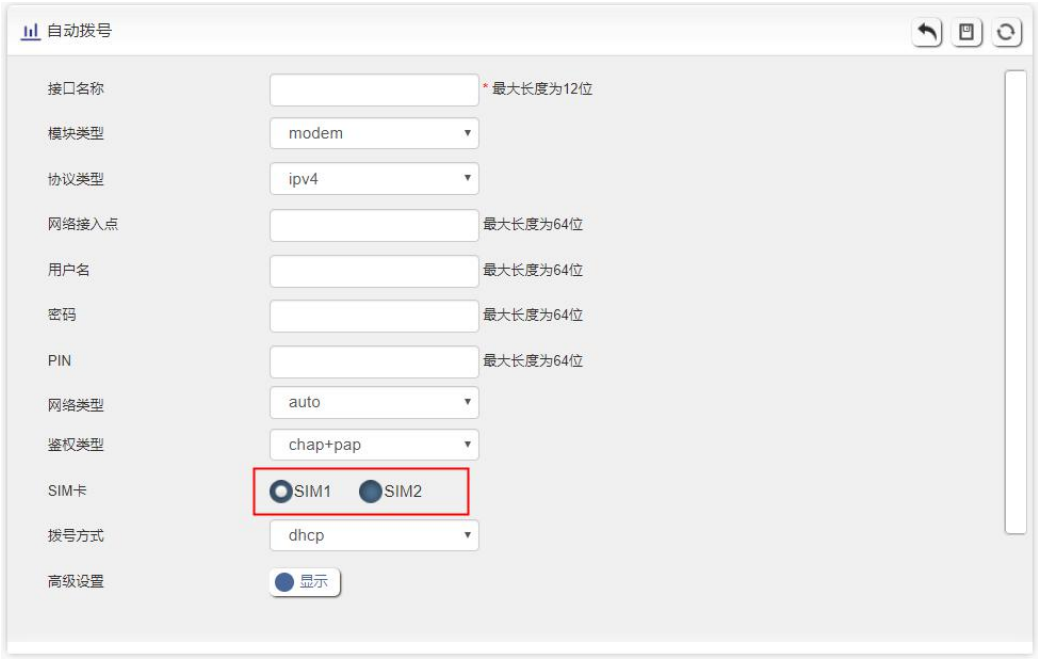


图 5-19 单模双卡模式配置页面

图 5-20 高级选项配置页面

3. 单击“保存”，完成对“移动网络”的参数配置。

- 编辑

  如图 5-13 中确定某一条参数配置记录，单击“编辑”，即可对该条参数记录进行编辑操作。参数说明如表 5-5 示。

- 删除

如图 5-13 中确定某一条参数配置记录，单击“删除”，即可删除该条参数记录。

- 启用

  如图 5-13 中确定某一条参数配置记录，单击“启用”，即可启用该条参数配置。

- 禁用

  如图 5-13 中确定某一条参数配置记录，单击“禁用”，即可禁用该条参数配置生效。

- 刷新

  单击“刷新”，刷新当前页面。

说明

当按钮为“启用”时，表示对应动作已经处于生效状态；“启用”按钮变成“禁用”，表示目前该功能或者参数处于禁用状态。

---结束

5.4.5 参数切换

工业智能网关参数切换功能是我司自主研发的备份切换功能，具备多功能组合的备份与切换。其主要应用场景是：多服务端互备份，多运营商备份（很多国家一个 SIM 卡支持多个运营商，某一运营商网络异常则切换到另外一个运营商）等相互冲突的组网但又需要相互间备份切换的应用场景。

步骤 1 登录工业智能网关的 WEB 配置界面。

步骤 2 单击“网络设置>参数切换”。

打开“参数切换”页签，如图 5-21 所示。

图 5-21 参数切换页签

步骤 3 配置“参数切换”相关参数。

可以“添加”、“编辑”、“删除”、“启用”、“删除”对应的“参数规则”。

- 添加

  1. 单击“添加”，显示“参数切换配置”页面，如图 5-22 所示。

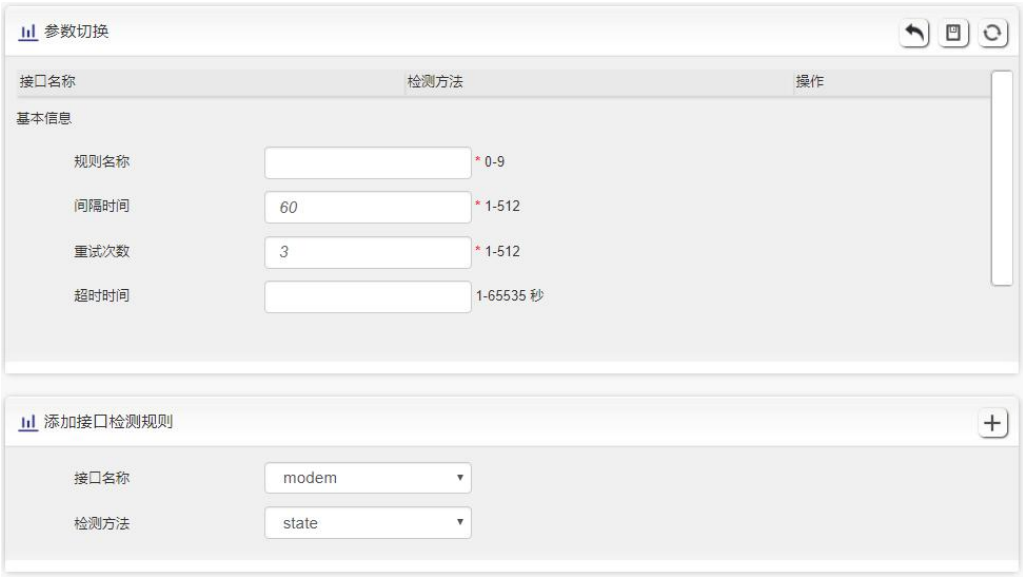


图 5-22 参数切换配置页面

2. 添加一条“参数备份”规则。

参数说明如表 5-14 所示。

表 5-14 参数切换参数说明

参数名称	含义	如何配置
状态	使能当前规则。所有使能规则同时只有一个规则在运行，所有禁用规则中关联接口都为禁用状态。如：rule0 中选择 modem0、ipsec1、vpdn2，若 rule0 禁用则 modem0、ipsec1、vpdn2 则都被禁用。	按钮选择 • 启用 • 禁用
基本信息		
规则名称	参数切换规则名称标识，用于区分不同的规则。	取值范围：[0,9]
间隔时间/重试次数	检测的时间间隔和最大失败次数。若失败次数达到配置的次数则切换到下一条规则进行工作。	取值范围：1～512 单位：秒/次数 默认值：60/3
超时时间	用于限定当前规则最大工作时间，rule0 中该参数无效，其他规则中配置该参数并且到达最大工作时间后切换到 rule0，不配置则按 rule 的顺序切换。通常没有严格主备要求时不建议配置。	取值范围：1～65535 单位：秒
添加接口检测规则		

参数名称	含义	如何配置
接口名称	规则关联参数接口名称，如 modem 接口名称：modem。	下拉框选项，取决于当前系统配置接口名称个数，自动生成。
检测方法	检测方法分为接口状态检测和 ICMP 检测，通过检查状态或者链路来判定是否需要切换到下一条规则（达到最大失败次数后切换）。	下拉框选项 • state • icmp
目的 IP	选择 icmp 检测方法时才需要配置，用于配置 icmp 检测目的地址。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.8.2

3. 单击“添加”完成规则添加。

- 删除

  单击“删除”，删除选中的“参数切换规则”。

- 启用

  单击“启用”，启动并应用该“参数切换规则”。

- 禁用

  单击“禁用”，禁用该“参数切换规则”。

- 刷新

  单击“刷新”，刷新当前页面。

说明

在同时使用参数切换和链路备份功能时，请确保两个功能使用接口类别不同。如需使用，请联系我司技术支持人员。

---结束

5.4.6 网络连接

为用户提供默认路由配置页面。

步骤 1 登录工业智能网关的 WEB 配置界面。

步骤 2 单击“网络设置>网络连接”。

打开“网络连接”页签，如图 5-23 所示。

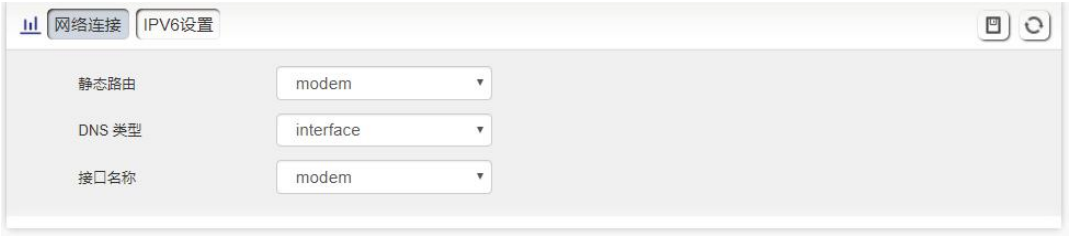


图 5-23 网络连接页签

步骤 3 配置“网络连接”相关参数。

参数说明如表 5-15 所示。

表 5-15 网络连接参数说明

参数名称	含义	如何配置
静态路由	网关数据包默认的转发路径。根据具体需要配置默认路由，当需要多网切换可以参见链路备份功能。	下拉框选项根据需要进行配置。
网关	默认路由选择 wan 口并且 wan 为静态 IP 时，需要配置 wan 口地址的下一跳网关地址，如果需要访问域名则还需要自定义配置 DNS。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.10.254
DNS 类型	配置网关的 DNS 类型，选择接口时则使用接口拨号等方式自动的获取 DNS，若为 WAN 静态 IP 时必须手动定义设置 DNS。	下拉框选项 • interface • custom
DNS1/DNS2	DNS 类型选择 custom 时配置，手动配置 DNS 地址，最多可配置两个。	接口型 A.B.C.D 例如：8.8.8.8
接口名称	DNS 类型选择 interface 时配置，配置后网关使用 DNS 关联接口获得的 DNS，所以需要特别注意该接口是否能获取 DNS。	下拉框选项 • modem • lan • wan • wifi2.4 • wifi5.8 wan 表示关联 WAN 口 PPPoE 拨号或者 DHCP 获取的 DNS，特别注意 WAN 静态 IP 时选择 wan 无效，PPP 拨号配置禁用对端 DNS 时选择 modem 无效，wifi2.4/wifi5.8 表示 WiFi 获得的 DNS。

步骤 4 单击“保存”，完成网络连接的配置。

说明

当“默认路由”选择“wan”接口，且 WAN 口形式从 DHCP 或静态 IP 切换至 PPPoE 时，网关默认路由需要点击“网络连接”页面的“保存”按钮才会显示并生效。

---结束

5.4.7 链路备份

工业智能网关结合客户实际需要实现了多网链路备份功能，能实现无线与无线、无线与有线链路之间的互备切换，能在某一链路故障时能快速切换到备份链路，保障下位机通讯链路的联通性和稳定性，从而保障用户数据业务不受影响。工业智能网关支持冷、热两种主备份模式，热备份优点是链路切换后直接可以通讯，但不足之处是会在备份链路实时在线的情况下产生通讯费用，增加成本开支。

步骤 1 登录工业智能网关的 WEB 配置界面。

步骤 2 单击“网络设置>链路备份”。

打开“链路备份”页签，如图 5-24 所示。

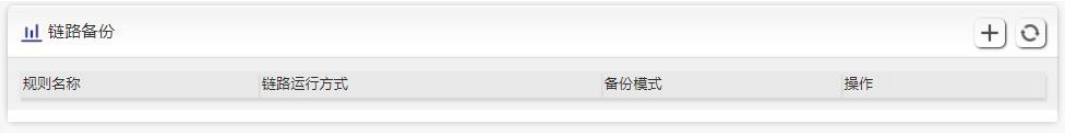


图 5-24 链路备份页签

步骤 3 单击“添加”，打开添加“链路备份”规则页面，如图 5-25 所示。

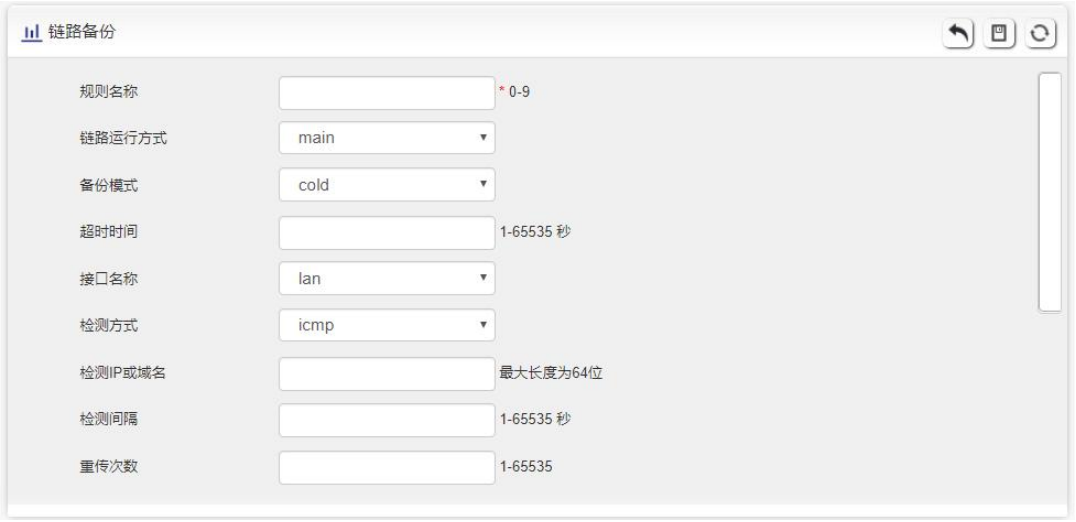


图 5-25 链路备份规则添加页面

步骤 4 配置“链路备份”相关参数。

参数说明如表 5-16 所示。

表 5-16 链路备份参数说明

参数名称	含义	如何配置
状态	使能链路备份功能。	按钮 • 启用 • 禁用
规则名称	链路备份规则名称标识 **说明** 0 可以为主链路，也可以为备份链路；1～9 只能为备份链路； 备份链路 1～9 之间根据数字大小决定优先级，数字越小，优先级越高。	取值范围：0～9
链路运行方式	备份方式，包含： • main：链路模式为主链路。 • backup：链路模式为备份链路。	下拉框选择。
备份模式	备份模式，有冷备份和热备份。热备份是指对应的链路处理启用状态，热备份的优点是切换速度快，不足之处是当链路在线时将会增加网络开销和资费成本。冷备份是指只有当前工作链路的接口处于启用状态。其他处于非工作链路的接口处于下线状态。	下拉框选项 • cold • hot
超时时间	• 如果当前链路为主链路，表示主链路稳定时间。 • 如果当前链路为备份链路，表示该链路最短工作时间。 **说明** 超时时间仅适用于主备切换。	取值范围：1～65535 单位：秒
接口名称	用于链路切换的接口。	有如下可选项： • modem • lan • wan • wifi2.4 • wifi5.8
检测 IP 或域名	通过 ping 包方式检测 IP 地址或域名，ping 不通则判定检测失败。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。
检测间隔/重传次数	链路正常检测时间间隔和最大失败次数。最大失败次数到达则切换链路。	取值范围：1～65535 单位：秒/次数

步骤 5 单击“保存”，完成链路备份配置。

说明

当启用链路备份功能后，网关的默认路由为链路备份规则的默认路由；
链路备份为主备切换时，只要主链路检测成功，则立即切换到主链路上；

---结束

5.4.8 VPN 设置

概述

VPN（Virtual Private Network）即虚拟专用网，是基于 Internet 的一种安全局域网，目前工业智能网关不仅支持 L2TP/PPTP/GRE/IPIP/IPSEC 五种 VPN 协议的单独使用，同时也支持在 VPN 上再架设 VPN 服务，即 VPN OVER VPN，如 GRE over IPSec、IPSec over PPTP/L2TP/GRE/IPIP 等。多层 VPN 的设置能够更好的报数用户通信数据的安全性。

VPDN 配置

VPDN 英文为 Virtual Private Dial-up Networks，又称为虚拟专用拨号网，是 VPN 业务的一种，是基于拨号用户的虚拟专用拨号网业务。即以拨号接入方式上网，是利用 IP 网络的承载功能结合相应的认证和授权机制建立起来的安全的虚拟专用网，是近年来随着 Internet 的发展而迅速发展起来的一种技术。

VPDN 支持 L2TP 和 PPTP 两种协议。

PPTP（Point to Point Tunneling Protocol）点对点隧道协议是一种支持多协议虚拟专用网络的网络技术，它也是第二层协议。通过该协议，远程用户能够通过 Windows 主流操作系统以及其它装有点对点协议的系统安全访问公司网络，并能拨号连入本地 ISP，通过 Internet 安全连接到公司网络。

L2TP（Layer Two Tunneling Protocol）第二层通道协议的缩写，它是 VPDN（虚拟专用拨号网络）技术的一种，专门用来进行第二层数据的通道传送。L2TP 提供了一种远程接入访问控制的手段，其典型的应用场景是：某公司员工通过 PPP 拨入公司本地的网络访问服务器（NAS），以此接入公司内部网络，获取 IP 地址并访问相应权限的网络资源。该员工拨入公司网络如同在公司局域网一样安全方便。

步骤 1 登录工业智能网关的 WEB 配置界面。

步骤 2 单击“网络设置>VPN 设置>VPDN 设置”，打开“VPDN 设置”页签，如图 5-26 所示。

图 5-26 VPDN 配置页签

步骤 3 单击“添加”，添加一条新 VPDN 规则。如图 5-27 所示。

图 5-27 VPDN 配置页面

步骤 4 配置 VPDN 规则参数。参数说明如表 5-17 所示。

表 5-17 VPDN 规则参数说明

参数名称	含义	如何配置
VPDN 服务	启用/禁用该条 VPDN 规则。	单击“启用”即可启用该条规则。
基本设置		
接口名称	该条 VPDN 规则的名称。	建议采用易于识别的名称。如城市-城市、特定事件（出差）等。 保存后不允许修改。
协议	VPDN 采用的协议，包括： • L2TP • PPTP	下拉列表选择。 根据实际情况设置，设置后不允许修改。
服务地址	用于接入访问的服务器 IP 地址或域名。	填入用于接入访问的服务器 IP 地址或域名即可。
用户名	接入服务器已授权的合法访问用户。	填入接入服务器已授权的合法访问用户名即可。
密码	接入服务器已授权的合法的访问用户密码。	填入接入服务器已授权的合法的访问用户密码即可。
高级配置	PPP 链路协商建立的高级参数设置,详情请参考“移动网络”高级参数配置。	单击后展开。

步骤 5 单击“保存”，完成该条 VPDN 规则配置。

在完成一条 VPDN 规则配置后，网关将自动与服务地址取得联系并建立 VPN 通信。与服务地址建立连接后，网关将会自动添加到对端子网的网关，而不要手动添加静态路由，更不需要添加 MASQ，较大的减少了用户的操作量。若想查看某条 VPDN 隧道状态，单击该条隧道对应的“查看”按钮，结果如图 5-28 所示。

图 5-28 L2TP 隧道状态页面

---结束

Tunnel 配置

隧道技术是一种通过互联网络基础设施在网络之间传递数据的方式。整个传递过程中，被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。

Tunnel 配置支持 GRE 和 IPIP 两种模式。

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

IPIP 隧道是在两个网关间对 IP 数据包进行封装的简单协议，IPIP 隧道接口会像一个物理接口出现在接口列表中，许多网关包括 Cisco，基本都支持该协议。这个协议使多个网络分布成为可能。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“网络设置>VPN 设置>Tunnel 配置”，打开“Tunnel 配置”页签，如图 5-29 所示。

图 5-29 Tunnel 配置页面

步骤 3 单击“添加”，添加一条新 Tunnel 规则。参数说明如表 5-18 所示。

表 5-18 Tunnel 规则参数说明

参数名称	含义	如何配置
隧道服务	启用/禁用 IP 隧道服务。	单击“启用”即可启用该条隧道规则。
基本设置		
隧道名称	该隧道的名称，保存后不能修改。	填入要设置的隧道名称，建议采用易于识别的名称。保存后不允许修改。
隧道模式	隧道工作模式，分为： • gre • ipip	下拉列表选择。 根据实际需求设置，保存后不能修改。
接口虚拟 IP	本地隧道的虚拟 IP 地址。	填入本地 GRE 隧道的虚拟 IP 地址。 格式：接口型 A.B.C.D/M，输入规范请参见“参数规范表”。
对端接口虚拟 IP	对端隧道的虚拟 IP 地址	填入对端 GRE 隧道的虚拟 IP 地址。 格式：接口型 A.B.C.D/M，输入规范请参见“参数规范表”
接口类型	对外接口类型，选择为“接口”或者“静态 IP”。	下拉列表选择。 根据自身需求选择为“接口”

参数名称	含义	如何配置
		或者“静态 IP”。
本端接口	“接口类型”选择“接口”后出现的下拉框选项，可以选择任意已建立连接的接口作为本地对外接口（VPDN 设置中建立的接口和 modem）。	下拉列表选择。 从下拉列表中选择隧道本端网络的对外接口皆可。
本端地址	“接口标识”选择“静态 IP”后出现的下拉框选项。设置本地对外的 IP 地址。	填入隧道本端网络的对外接口 IP 即可。 格式：A.B.C.D 接口型，输入规范请参见“参数规范表”。
对端地址	隧道对端网络的对外接口 IP，常为公网 IP（Internet）地址，也可为企业不同内网 IP。	填入隧道对端网络的对外接口 IP 即可。 格式：A.B.C.D 接口型，输入规范请参见“参数规范表”。

步骤 4 单击“保存”，完成该条 Tunnel 规则配置。

---结束

IPSec 设置

IPSec（IP_SECURITY）是一种建立在 Internet 协议(IP)层之上的协议。它能够让两个或更多主机以安全的方式来通讯。IPSec 是安全联网的长期方向。它通过端对端的安全性来提供主动的保护以防止专用网络与 Internet 的攻击。工业智能网关中的 IPSec 采用公用的 phase1，可以与大部分 IPSec 服务器进行连接协商，同时工业智能网关也支持通过其他接口拉起 IPSec（如通过 modem 拉起），省去用户手动操作。IPSec 有两种模式：隧道模式和传输模式。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“网络设置>VPN 设置>IPSec 配置”，打开“IPSec 配置”页签，如图 5-30 所示。

图 5-30 IPSec 配置页签

步骤 3 单击“添加”，添加一条新的 IPSec 规则。本 IPSec 页面分为三个阶段的配置，配置方法如下：

1. 第一阶段参数配置。

   第一阶段配置页面，如图 5-31 所示。

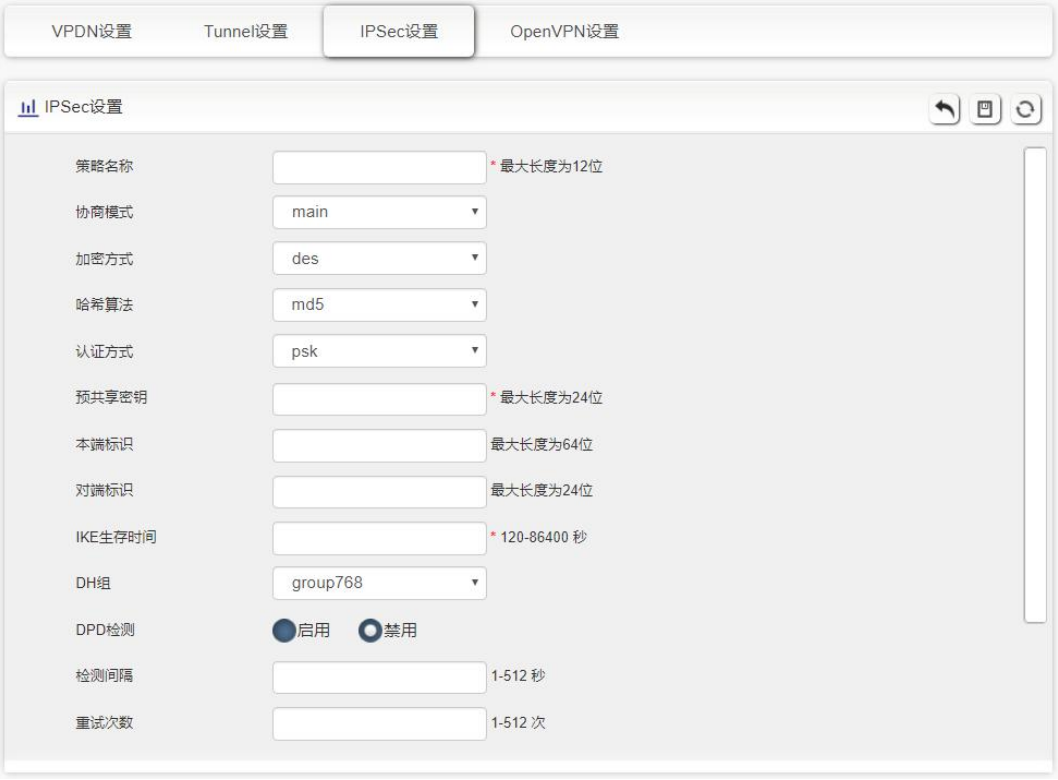


图 5-31 IPSec 第一阶段配置页面

IPSec 规则第一阶段参数说明如表 5-19 所示。

表 5-19 IPSec 规则第一阶段参数说明

参数名称	含义	如何配置
基本设置		
策略名称	该阶段的名称，主要用于第三阶段的匹配。	填入该阶段的名称。保存后不能修改。
协商模式	IPSec 第一阶段的协商模式，包括“main”（主模式）和“aggr”（野蛮模式）。	下拉列表选择。 从下拉列表中选择要设置的启动模式，一般两端有经过 NAT 且使用 USERID 的方式建议“野蛮模式”。
加密方式	支持 des、3des、aes128/aes192/aes256 加密方式。	下拉列表选择。 从下拉列表中选择要设置的加密方式。
哈希算法	支持 md5、sha1、sha2_256 加密算法。	下拉列表选择。 从下拉列表中选择要设置的加密算法。
认证方式	支持预共享密钥方式认证。	下拉列表选择。 • psk • rsasig
预共享密钥	设置预共享密钥。	填入 IPSec 对端服务器预置的预共享密钥。 最大长度为 64 位的字母数字型字符串，输入规范请参见“参数规范表”。
本端标识	配置 IPSEC 本端标识以标明本端身份，不配置则以 IP 为标识。	填入 IPSec 本端标识即可，需与 IPSec 对端服务器预置的对端标识一致。 一般 WORD 型，输入规范请参见“参数规范表”；另外，本端表述支持空格输入。
对端标识	配置 IPSEC 对端标识以标明对端身份，不配置则以 IP 为标识。	填入 IPSec 对端标识即可，需与 IPSec 对端服务器预置的本端标识一致。 一般 WORD 型，输入规范请参见“参数规范表”；另外，本端表述支持空格输入。
IKE 生存时间	IKE 密钥生存时间。	填入合适的密钥生命周期。 取值范围：120～86400 单位：秒

参数名称	含义	如何配置
DH 组	此处配置为第一阶段 IKE 协商的密钥长度。	下拉列表选择。 从下拉列表选择合适的组名即可。
DPD 检测	使能 DPD 检测，DPD 对端检测需要对端服务器支持，它用于检测 IKE 环境是否正常，若不正常则立刻重新协商 IKE 环境，以达到保障 IPSec 环境的安全和连接的稳定性和连通性。	单击按钮选择。 单击“启用”即可启用对端检测服务。
检测间隔	设置 DPD 检测间隔时间。	手动输入 取值范围：1～512 单位：秒
重试次数	连续 DPD 检测失败的最大次数。	手动输入 取值范围：1～512 单位：次

单击“保存”，完成该条 IPSec 第一阶段规则配置。

2. 第二阶段参数配置。

第二阶段参数配置页面如图 5-32 所示。

注意

上述参数中，协商模式、加密方式、哈希算法、认证方式、预共享密钥、IKE 生存时间、DH 组要与 IPSec 服务器设置的一致。本端标识与对端标识要与 IPSec 服务器中的对端标识与本端标识一致。

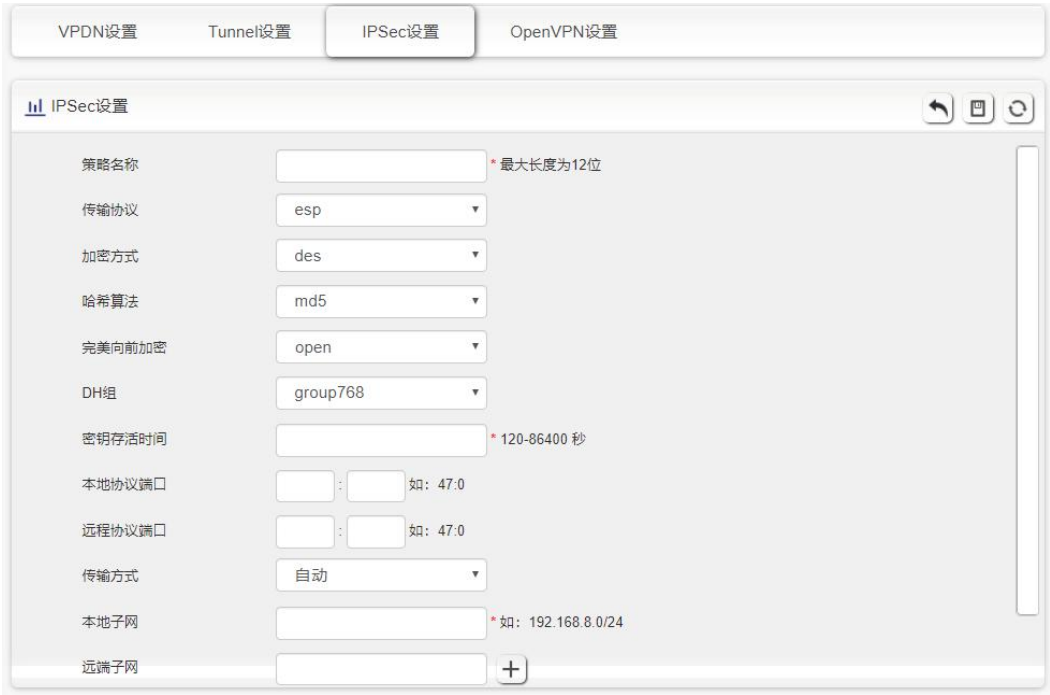


图 5-32 IPSec 第二阶段配置页面

IPSec 规则第二阶段参数说明如表 5-20 所示。

表 5-20 IPSec 规则第二阶段参数说明

参数名称	含义	如何配置
基本设置		
策略名称	该阶段的名称，主要用于第三阶段的匹配。	填入该阶段的名称。保存后不能修改。
加密方式	支持 des、3des、aes128/aes192/aes256 加密方式。	下拉列表选择。 从下拉列表中选择要设置的加密方式。
哈希算法	支持 md5、sha1、sha2_256 加密算法。	下拉列表选择。 从下拉列表中选择要设置的加密算法。
完美向前加密	启用或禁用完美向前加密，启用完美向前加密会增加系统开销，但可以增加 IPSec 的安全性。	下拉列表选择。 根据对端 IPSec 服务器的设置，选择 open 或 close。
DH 组	启用完美向前加密时使用，此处配置为 IPSec 第二阶段 SA 协商的密钥长度。	下拉列表选择。 从下拉列表选择合适的组名。

参数名称	含义	如何配置
密钥存活时间	IPSec SA（IPSec 安全联盟）密钥存活时间。	填入合适的密钥生命周期。 取值范围：120～86400 单位：秒
本地协议端口	配置本端需要加密的协议及端口	手动输入，前框输入协议代码，后框输入端口。
远程协议端口	配置对端需要加密的协议及端口	手动输入，前框输入协议代码，后框输入端口。
传输方式	支持隧道模式、传输模式或者自动选择。	下拉列表选择。 从下拉列表选择需要的传输方式。
本地子网	本地子网配置。	传输模式下不用配置子网，自动和隧道模式下需配置。填入本地子网地址。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。
远端子网	远端子网配置。	传输模式下不用配置子网，自动和隧道模式下需配置。填入远端子网地址。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。

单击“保存”，完成该条 IPSec 第二阶段规则配置。

注意

上述参数中，传输协议、加密方式、哈希算法、DH 组、完美向前加密、密钥存活时间等要与 IPSec 服务器配置一致；如果传输方式设置为自动或者隧道模式，则本地子网与远端子网要与 IPSec 服务器中的远端子网和本地子网的配置一致。

本地协议端口及远端协议端口的协议代码必须一致，表示对一种协议加密；当配置了本地协议端口及远端协议端口后，表示 IPSec 进对该协议及端口加密，其他通信不加密；当未配置该参数时，表示 IPSec 对所有的通信都加密。

3. 匹配阶段参数配置。

匹配阶段配置页面如图 5-33 所示。

图 5-33 IPSec 匹配阶段配置页面

配置 IPSec 规则匹配阶段参数，配置完后单击“保存”。

说明

当加密接口选择 br0 且 br0 接口有多个地址时，IPSec 选择的地址为 br0 的 IP1 地址。

IPSec 规则匹配阶段参数说明如表 5-21 所示。

表 5-21 IPSec 规则匹配阶段参数说明

参数名称	含义	如何配置
基本设置		
接口名称	该阶段的名称，主要用于第三阶段的匹配。	最大允许输入 12 位字符串。 填入该阶段的名称。保存后不能修改。
匹配 Phase1	选择需要与之相匹配的 IPSec 第一阶段配置的策略名称。	下拉框选项。 选择第一阶段配置的策略名称。
匹配 Phase2	选择需要与之相匹配的 IPSec 第二阶段配置的策略名称。	下拉框选项。 选择第二阶段配置的策略名称。
服务地址	IPSec 对端服务器 IP 或域名。	填入 IPSec 对端服务器 IP 或域名。 最大允许输入 64 位字符串。
加密接口	选择 IPSec 的绑定接口，绑定 VPDN/modem/br0 接口作为 IPSec 协商的本端，可实现支持 IPSecOVER VPDN 等组网应用，另外绑定接口后 IPSec 规则将随绑定的接口状态变化而变化，能最快速度的恢复 IPSec 在拨号接口上的连接，保障 IPSec 连通性。	下拉列表选择。 从下拉列表选择合适的接口。

---结束

Open VPN 设置

Open VPN 是一个基于 OpenSSL 库的应用层 VPN 实现。和传统 VPN 相比，它的优点是简单易用。Open VPN 所有的通信都是基于一个单一的 IP 端口，默认且推荐使用 UDP 协议通信，同时 TCP 也被支持。Open VPN 连接能通过大多数的代理服务器，并且能够在 NAT 的环境中很好的工作。服务端具有向客户端“推送”某些网络配置信息的功能，这些信息包括：IP 地址、路由设置等。Open VPN 提供了两种虚拟网络接口：通用 Tun/Tap 驱动，通过它们，可以建立三层 IP 隧道，或者虚拟二层以太网，后者可以传送任何类型的二层以太网络数据。IANA（Internet Assigned Numbers Authority）指定给 Open VPN 的官方端口为 1194。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“网络设置>VPN 设置>OpenVPN 设置”，打开“OpenVPN 配置”页签，如图 5-34 所示。

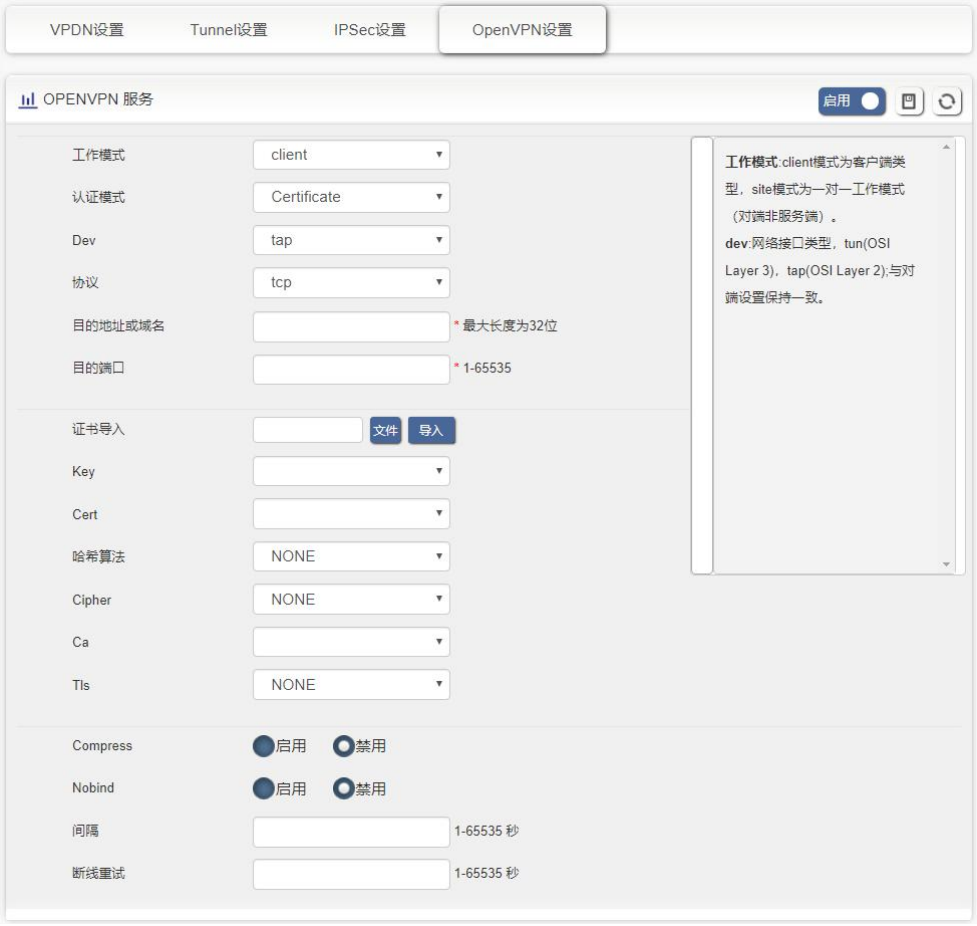


图 5-34 OpenVPN 配置页面

步骤 3 配置 Open VPN 参数，参数如表 5-22 所示。

表 5-22 OpenVPN 参数说明

参数名称	含义	如何配置
OPENVPN 服务	使能 OPENVPN 服务。	单选按钮选择。 • 启用 • 禁用
基本设置		
工作模式	支持 client 和 site-to-site 两种工作模式 • Client 模式为客户端类型模式 • Site-to-site 模式为一对一工作模式（对端为非服务端）	下拉列表选择。 从下拉列表选择需要的工作模式。
Dev	Dev 表示网络接口类型。支持 tun 和 tap 两种类型 • tun（OSI Layer 3）：tun 模拟了网络层设备，操作第三层数据包，比如 IP 数据包。 • tap（OSI Layer 2）：tap 等同于一个以太网设备，操作第二层数据包，比如以太网数据帧。	下拉列表选择。 从下拉列表选择需要的工作模式。 要求保持与对端保持一致。
协议	数据传输协议类型设置。 • TCP：TCP 协议是一种面向连接的可靠传输协议，适用于对可靠性要求较高、对通讯效率敏感程度不高的场合。 • UDP：UDP 协议是一种非连接的不可靠传输协议，适用对效率要求相对高、对可靠性要求相对低的场景。	下拉列表选择。 从下拉列表选择需要的传输协议 要求保持与对端保持一致。
目的地址或域名	指定连接的服务器地址。	WORD 类型，最大 32 个字节，输入规范请参见“参数规范表”。 要求保持与对端保持一致。
目的端口	指定连接服务器的端口。	取值范围：1～65535 • 缺省：1194 要求保持与对端保持一致。
证书导入	导入证书。	点击文件，选择相应证书，导入。
Ca	指定客户端 CA 证书的文件路径。	WORD 类型，最大 32 个字节，输入规范请参见“参数规范表”。

参数名称	含义	如何配置
Key	指定当前客户端的私钥路径。	WORD 类型，最大 32 个字节，输入规范请参见“参数规范表”。
Cert	指定当前客户端的证书文件路径。	WORD 类型，最大 32 个字节，输入规范请参见“参数规范表”。
Tls	开启 TLS，如果服务器开启，客户端也必须开启。 TLS：安全传输层协议（TLS）用于两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成：TLS 记录协议（TLS Record）和 TLS 握手协议（TLS Handshake）。	WORD 类型，最大 32 个字节，输入规范请参见“参数规范表”。
Compress	压缩协议：配置是否开启 VPN 连接压缩。 若服务器开启，则客户端必须开启。	单选按钮选择。 • 启用 • 禁用
nobind	配置是否绑定特定的本地端口号。	单选按钮选择。 • 启用 • 禁用
Cipher	SSL 的加密算法系统。	下拉框选项 • NONE • BF-CBC • DES-CBC • DES-EDE-CBC • DES-EDE3-CBC • DESX-CBC • RC2-40-CBC • CAST5-CBC • RC2-64-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • SEED-CBC

步骤 4 单击“保存”，完成 Open VPN 配置。

---结束

5.4.9 DHCP 服务

动态主机设置协议（Dynamic Host Configuration Protocol,DHCP）是一个局域网的网络协议。启用 DHCP 功能之后，下位机能自动获取动态 IP。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“网络设置>DHCP 服务”。

打开“DHCP 服务”页签，如图 5-35 所示。

图 5-35 DHCP 服务页签

步骤 3 配置“DHCP 服务器设置”。

DHCP 服务器设置参数如表 5-23 所示。

表 5-23 DHCP 服务器设置参数说明

参数名称	含义	如何配置
DHCP 服务	DHCP 服务使能按钮，用于启用/禁用 DHCP 服务。	按钮选择设置。 • 启用 • 禁用
基本设置（DHCP 在无特殊组网要求的情况下不建议配置）		
标识名	DHCP 服务的标识名。	最大长度为 32 位。
地址池	DHCP 客户端获取 IP 地址的范围。选择接口时则表示关联接口的网段。该选项通常在需要指定下位机可分配的地址范围时配置，例如：只希望最多四台机器能自动获取 IP。	下拉框选项 • lan • custom
起始 IP	地址池选择 custom 时配置，配置 DHCP 地址池的起始 IP 地址。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.8.2
结束 IP	地址池选择 custom 时配置，配置 DHCP 地址池的结束 IP 地址。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.8.254

参数名称	含义	如何配置
网关类型	DHCP 客户端获取的网关 IP 来源，分为 default、lan、wan、custom 四类，关联接口时则将接口的 IP 分配给 DHCP 客户端作为网关。	下拉框选项 默认值：default
网关	网关类型选择 custom 时配置，通常需要指定下位机网关 IP 时使用。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.8.1
DNS 类型	DHCP 客户端获取的 DNS IP 的来源，有 default、modem、wan、lan、custom 等方式，通常不建议修改该配置，特别是双模应用场景下不建议配置。	下拉框选项 • default • modem • wan • lan • custom • wifi2.4 • wifi5.8 配置为 default 则根据网关本身的 DNS 地址来分配。
DNS1/DNS2	DNS 类型选择 custom 时配置，配置 DHCP 客户端获取 DNS 的 IP 地址。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：8.8.8.8
租约时间	DHCP 客户端获取 IP 后对 IP 租用时间，客户端通常在租约时间过半的时候重新协商获取 IP 地址。租约时间主要是用于释放空闲的 IP，避免 DHCP 客户端关机之后还占用 IP 地址资源。	取值范围：120～86400 单位：秒 默认值为 3600
IP、MAC 绑定，用于为指定范围内的机器分配的固定的 IP 地址		
IP 地址	与指定的 MAC 配对，当被绑定 MAC 的 DHCP 客户端发起 DHCP 请求时则会与该 MAC 地址绑定的 IP 地址分配给它。该 IP 地址即使没有被占用也不会分配给其他 MAC 地址。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.8.2
MAC	配置需要指定 DHCP 获取 IP 的 DHCP 客户端的 MAC 地址。	WORD 类型 MAC 格式 例如：00:1A:4D:34:B1:8E

---结束

5.5 应用设置

工业智能网关根据多年用户应用场景，除了常用的 SNMP、DDNS 等功能之外还自主研发了很多适用于无线网络产品的功能，主要有链路检测、任务管理、转发设置、安全设置、DDNS 设置、SNMP 设置功能等。

5.5.1 链路检测

无线网络存在假链接（拨号获得 IP 在，但是链路不通）等异常现象，通常通过 LCP 等方式进行维护，工业智能网关除了支持这种检测方式外还提供更为可靠的 ICMP 链路检测功能。ICMP 检测主要通过 ping 包检测方式检测通讯链路，当检测链路异常时执行用户设置的动作，实现链路和系统的快速恢复。ICMP 链路检测在设计之初主要用于检测无线链路，工业智能网关支持对 VPN 等隧道链路进行检测，支持多规则同时检测，最大支持 10 条 ICMP 检测规则。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用设置>链路检测”。

打开“链路检测”页签，如图 5-36 所示。

图 5-36 链路检测页面

步骤 3 对“链路检测”进行“添加”、“编辑”、“删除”、“启用”和“禁用”操作。

- 添加

  1. 单击“添加”，显示“链路检测”的添加界面，如图 5-37 所示。

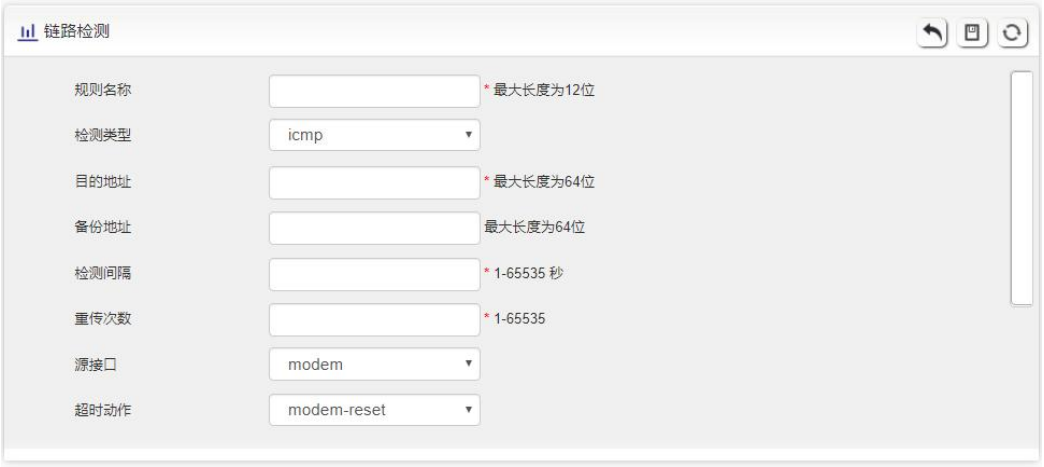


图 5-37 链路添加页面

  2. 配置 ICMP 检测服务参数。

     参数说明如表 5-24 所示。

表 5-24 ICMP 检测规则参数说明

参数名称	含义	如何配置
检测服务	使能 ICMP 检测规则。多条规则可同	按钮

参数名称	含义	如何配置
	时运行，也可禁用某一条规则。	• 启用 • 禁用
基本设置		
规则名称	ICMP 检测规则名称标识，没有特定意义，仅用于区分不同规则。	WORD 类型，最大 12 字节，输入规范请参见“参数规范表”。
目的地址	ICMP 检测目的地址，可以是 IP 也可以是域名，设置为域名时需要确保网关配置正确的 DNS。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。
备份地址	ICMP 检测备份目的地址，主地址检测不通时检测备份地址，若备份地址检测不通则判定检测失败。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。
检测间隔/重传次数	链路正常时检测时间间隔和最大失败次数。最大失败次数到达则执行 ICMP 规则对应的动作任务，例如：modem 重新拨号等。	取值范围：1～65535 单位：秒/次
源接口	网关发送 ICMP 检测包的源地址	下拉框选项 • lan • modem
超时动作	当检测失败达到最大失败次数时执行的动作，主要有重拨号、自定义动作。	下拉框选项。 • modem-reset：modem 重拨号 • custom：自定义动作
执行命令	超时动作选择 custom 时配置，命令为后台操作命令，通常不建议使用。如有配置需要请联系我司技术人员。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。

3. 单击“保存”，完成一条 ICMP 检测规则的添加。

ICMP 正常按照 ICMP 检测间隔发送，如出现异常则立刻按照异常 ICMP 检测连续发送 ICMP 包，若检测目的地址不通，则开始检测备份地址。若检测备份地址不通的次数也到达重传次数，则网关执行“超时动作”。

- 编辑

  如图 5-36 中确定某一条参数配置记录，单击“编辑”，即可对该条参数记录进行编辑操作。参数说明如表 5-24 所示。

- 删除

  如图 5-36 中确定某一条参数配置记录，单击“删除”，即可删除该条参数记录。

- 启用

如图 5-36 中确定某一条参数配置记录，单击“启用”，即可启用该条参数配置。

- 禁用

  如图 5-36 中确定某一条参数配置记录，单击“禁用”，即可禁用该条参数配置生效。

- 刷新

  单击“刷新”，刷新当前页面。

---结束

5.5.2 任务管理

工业智能网关任务管理能够为用户提供网关在线时长、定时任务执行等功能。客户可以根据需求配置多个在线时间段（如某天的某几个小时），设置某时间点的任务执行等（如每天凌晨零点重新拨号或重启系统）。最大支持 10 条任务规则。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用设置>任务管理”。

打开“任务管理”页签，图 5-38 所示。

图 5-38 时间段管理设置页签

步骤 3 若需添加新的任务管理规则，请单击“添加”，进入任务管理规则设置界面，如图 5-39 所示。

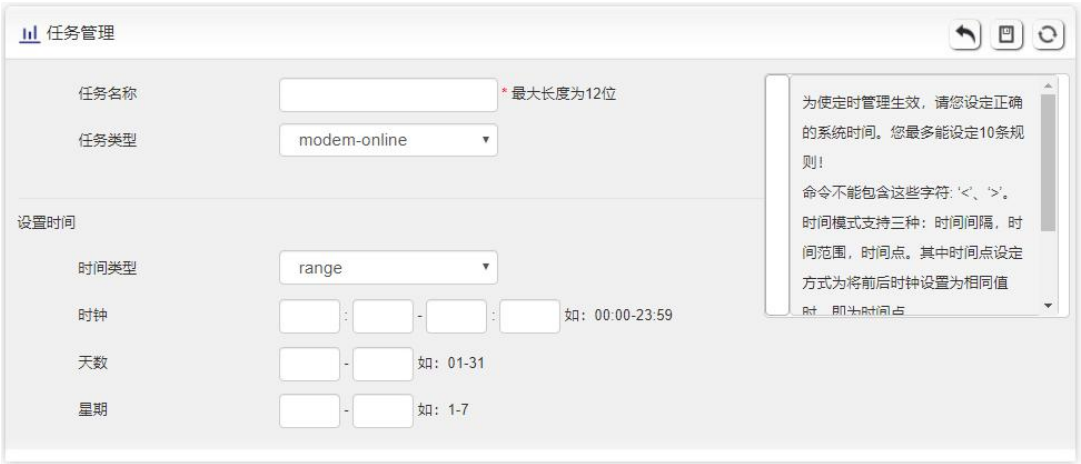


图 5-39 任务管理配置界面

步骤 4 配置任务管理规则参数。

参数说明如表 5-25 所示。

表 5-25 任务管理规则参数说明

参数名称	含义	如何配置
状态	使能定时规则。多条规则可同时运行，也可禁用某一条规则。本功能除了时间间隔类型动作任务外，其他任务需要配合 NTP 服务一起使用，否则很难达到合理的时间任务控制。	单选框选择。 • 启用 • 禁用
基本设置		
任务名称	任务管理规则名称标识，仅用于区分不同的规则。	最大长度为 12 位，输入规范请参见“参数规范表”。
任务类型	任务主要有动作类任务和状态类任务，动作类任务配置为时间点或者时间间隔，状态类任务则配置为时间段，状态类任务只有在线，它表示所配置时间区域 modem 处于上线状态（掉线自动重拨号），其他时间区域时保持下线（不拨号）。	下拉框选项 • modem-online • reboot • custom 选择“自定义”，则显示“命令”参数，需要用户输入命令（可以是 diaup 等命令，也可以是一些其他的命令）。 最大长度为 64 位字符串，输入规范请参见“参数规范表”。
设置时间		
时间类型	分为时间范围和时间间隔，分别对应状态任务和动作任务。	下拉框选项 • range • interval
当“时间类型”选择“range”时		
时钟	配置小时、分钟，，当时间间隔前后一致则表示时间点，适用于动作类任务。	取值范围：[00:00,23:59] 格式：HH:mm-HH:mm
天数	任务执行的天数，表示一个月中的某天的某个时间段或时间点执行任务。	取值范围：[01,31] 格式：XX-XX
星期	动作执行的星期设置。 代表一个星期中某天的某个时间段或时间点执行任务。当天数和星期都配置时表示两个时间条件同时满足时执行任务。	取值范围：[1,7] 格式：X-X 1 表示星期一

参数名称	含义	如何配置
当“时间类型”选择“interval”时		
时间间隔	动作类任务除了可以配置时间点执行外，还可以配置为每隔一段时间执行一次。	取值范围：1～65535 单位：分钟

步骤 5 单击“保存”，完成任务管理服务配置。

当任务管理的时间类型为“range”时，则必须先开启“系统时间”，即 NTP 服务（任务管理暂时不支持手动对时）；若时间类型为“interval”，则不需要开启“系统时间”。要使用“系统时间”，请参见“5.8.1 系统时间”。

因考虑到 modem 的稳定性，网关有多个对 modem 操作的功能，如任务管理、参数切换、链路备份、ICMP 检测、触发设置等，其中任务管理是改变保持 modem 状态，而其它功能则是改变 modem 状态但并不保持，故在使用任务管理时请兼顾其它功能，如有需要，可联系我司技术人员。

---结束

5.5.3 转发设置

工业智能网关转发功能包括 NAT、路由、动态路由（RIP、OSPF）和 QoS。

NAT

NAT（Netword Address Translation），网络地址转换，一般用于将私网（局域网）IP 地址替换成公网 IP 地址。

DNAT 规则配置

DNAT 是目的地址替换，用于将外网访问网关内部的目的地址替换成用户设置的地址。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用设置>转发设置>NAT”，打开“NAT”页签，如图 5-40 所示。

图 5-40 NAT 页签

步骤 3 单击“添加”按钮，选择转换类型为“DNAT”新建一条 DNAT 规则，如图 5-41 所示。

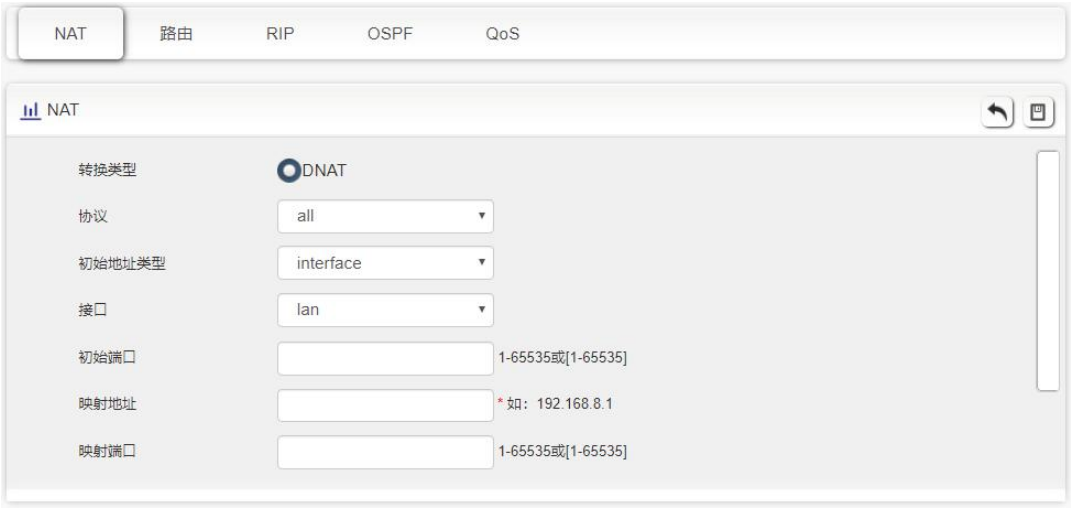


图 5-41 NAT 规则配置页面

步骤 4 配置 DNAT 规则参数。参数说明如表 5-26 所示。

表 5-26 DNAT 参数说明

参数名称	含义	如何配置
基本设置		
协议	针对哪种协议数据包做目的地址转换。	下拉列表选择： • all • tcp • udp • icmp

参数名称	含义	如何配置
初始地址类型	需要转换的 IP 数据包的目的地址类型。	下拉列表框选择： • interface • static
接口（当初始地址类型选择 interface 时需要配置）	表示 IP 数据包的目的地址为网关的某个接口。	下拉列表框选择： • lan • modem • wan • wifi2.4 • wifi5.8
初始地址（当初始地址类型选择 static 时需要配置）	表示进入网关的 IP 数据包的目的地址，该目的地址需要转换。	A.B.C.D 接口型或 A.B.C.D/M；接口型，输入规范请参见“参数规范表”
初始端口	IP 数据包中目的地址使用的端口。	取值范围：1～65535 或[1～65535]；可以是范围，也可以是单个端口。
映射地址	原目的地址替换后的地址。	A.B.C.D 接口型，输入规范请参见“参数规范表”
映射端口	初始端口替换后的端口。	取值范围：1～65535 或[1～65535]；可以是范围，也可以是单个端口。

步骤 5 单击“保存”，完成该条 DNAT 规则配置。

说明

当 DNAT 规则中配置了端口时，协议选择“all”表示选择“tcp”、“udp”两种协议；当 DNAT 规则中没有配置端口时，协议选择“all”表示选择“tcp”、“udp”、“icmp”三种协议。

---结束

SNAT 配置

SNAT 是源地址转换，其作用是将 IP 数据包的源地址转换成另外一个地址。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用设置>转发设置> NAT”，打开“NAT”页签，如图 5-40 所示。

步骤 3 选择“转换类型”为“SNAT”后，配置界面如图 5-42 所示。

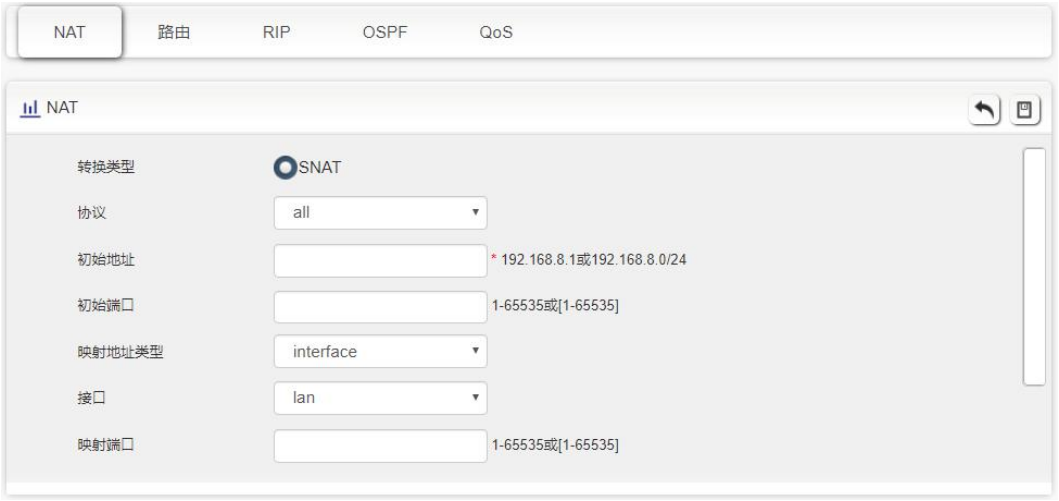


图 5-42 SNAT 规则配置界面

步骤 4 配置 SNAT 规则参数。参数说明如表 5-27 所示。

表 5-27 SNAT 规则参数说明

参数名称	含义	如何配置
协议	针对哪种协议数据包做目的地址转换。	下拉列表选择： • all • tcp • udp • icmp
初始地址	需要替换的源地址	A.B.C.D 接口型或 A.B.C.D/M；接口型，输入规范请参见“参数规范表”。
初始端口	需要替换的源地址端口	取值范围：1～65535 或[1～65535]；可以是范围，也可以是单个端口。
映射地址类型	源地址替换后的新源地址类型	下拉列表选择： • interface • static
接口（当映射地址类型选择 interface 时需要配置）	选择网关的某个接口作为替换后的源地址	下拉列表选择： • lan • modem • wan • wifi2.4 • wifi5.8
映射地址	源地址替换后的新源地址	A.B.C.D 接口型，输入规范请参见“参数规范表”
映射端口	替换之后的源地址端口	取值范围：1～65535 或[1～65535]；可以是范围，也可

参数名称	含义	如何配置
		以是单个端口。

步骤 5 单击“保存”，完成该条路由模式规则配置。

说明

当 SNAT 规则中配置了端口时，协议选择“all”表示选择“tcp”、“udp”两种协议；当 SNAT 规则中没有配置端口时，协议选择“all”表示选择“tcp”、“udp”、“icmp”三种协议。

---结束

MASQ 配置

MASQ 也就是 MASQUREADE，地址伪装，将所有经过网关转发的数据包的源 IP 地址转换成用户设置的 IP 地址。工业智能网关支持将数据包的源 IP 转换成网关的某个接口地址。

步骤 1 登录工业智能网关的 WEB 配置界面。

步骤 2 单击“网络设置>转发设置> NAT”，打开“NAT”页签，选择“转换类型”为“MASQ”，如图 5-43 所示。

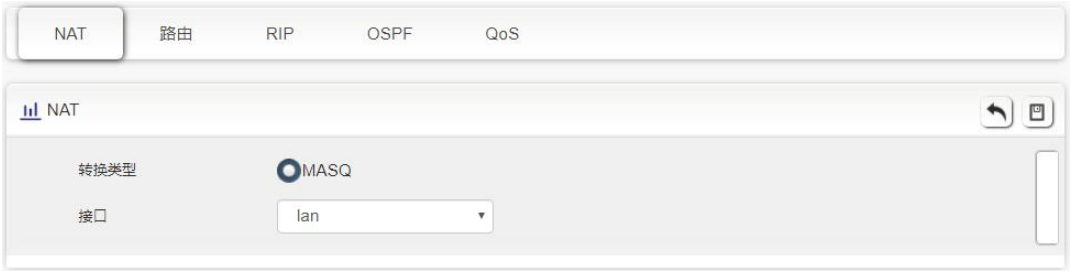


图 5-43 MASQ 规则配置界面

步骤 3 配置 MASQ 规则参数。参数说明如表 5-28 所示。

表 5-28 MASQ 规则参数说明

参数名称	含义	如何配置
接口	接口包含： • lan：以 LAN 口地址作为网关及局域网与外部通信地址 • modem：以 modem 口地址作为网关及局域网与外部通信地址 • wan：以 WAN 地址作为网关及局域网与外部通信地址 • wifi2.4/wifi5.8：以 WiFi 地址作为网关及局域网与外部通信地址	下拉列表选择。 建议根据自身需要从下拉列表中选择需要的接口即可。

步骤 4 单击“保存”，完成该条路由模式规则配置。

说明

MASQ 规则：将所有从局域网中发出的数据包的源地址改成网关指定接口的 ip 地址，这样从局域网侧的 PC 机才能将数据包发送出去；若在网关页面将 MASQ 规则删除，则网关 LAN 侧的 PC 不能与外部进行通信。

---结束

路由配置

静态路由是为网关转发数据包提供具体的转发路径，须由用户手动配置。静态路由形式分为静态路由和策略路由，静态路由是以目的地址作为选择依据的路由；而策略路由是以源地址为选择依据的路由（网关检测接收到的转发包的源地址，然后根据源地址选择相应的策略路由转发），且策略路由优先级，以 3～252 数字来区分，数字越小，优先级越高。而静态路由和策略路由之间也有优先级：策略路由的优先级高于静态路由。

步骤 1 登录工业智能网关的 WEB 配置界面。

步骤 2 单击“应用设置>转发设置>路由”。打开“路由”页签，如图 5-44 所示。

图 5-44 静态路由页签

步骤 3 单击“添加”按钮，新建一条静态路由规则。配置界面如图 5-45 所示和图 5-46 所示。

图 5-45 静态路由配置页面

图 5-46 策略路由配置页面

参数说明如表 5-29 所示。

表 5-29 静态路由参数说明

参数名称	含义	如何配置
基本设置		
路由类型	选择是“静态路由”还是“策略路由”。	下拉框选项
当“路由类型”选择“静态路由”时		
网络地址	设置静态路由的目标地址和子网掩码位数。	填入目的地址和子网掩码位数即可。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。
网关类型	指定静态路由所作用的网关类型。包含： • 接口 • 静态 IP	下拉列表选择。 可以从下拉列表选择需要的接口标识，分别是静态 IP 和接口。
网关	设置静态路由的下一跳 IP 地址，即相邻网关的端口地址。	下拉列表选择 • 若网关类型选择静态 IP，则网关需要手动是输入，格式：A.B.C.D • 若网关类型选择接口，则网关需要下拉列表选择。
当“路由类型”选择“策略路由”时		
源类型	设置策略路由的源地址类型。 • 静态 IP • 接口	下拉框选项。

参数名称	含义	如何配置
网络地址	当源类型选择“静态 IP”时需要配置，手动添加网络地址。	填入目的地址和子网掩码位数即可。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。
源接口	当源地址选择“接口”时需要配置，选择策略路由的源地址。 • modem	下拉框选项。 当网关创建有其它如 vpdn、IPSec 接口时，也会有接口名称在“源接口”列表中显示。
网关类型	设置策略路由的下一条地址。 • 静态 IP • 接口	下拉框选项。
网关	当网关类型选择“静态 IP”时需要填写 IP 地址，当网关类型选择“接口”时，需要选择相应接口做网关。	格式：A.B.C.D/M，输入规范请参见“参数规范表”。
优先级	设置策略路由的优先级，优先级数字越小，则优先级越高。	取值范围：[3,252]

步骤 4 单击“保存”，完成该条静态路由配置。

静态路由是指网关根据接收到的转发包的目的地址选择路由然后再将数据包转发出去，如网关接收到源地址为 1.1.1.1/目的地址为 2.2.2.2 的包，则网关在路由表中选择符合目的地址 2.2.2.2 的路由并将该数据包发送到下一跳。

而策略路由是指网关根据收到的转发包的目的地址选择路由再转发出去，如网关接收到源地址为 1.1.1.1/目的地址为 2.2.2.2 的包，则网关在路由表中选择符合源地址 1.1.1.1 的路由并将该数据包转发到下一跳。

策略路由的优先级高于静态路由，无论策略路由的优先级是多少。

---结束

QoS 配置

QoS（Quality of Service）服务质量，是网络的一种安全机制，是用来解决网络带宽分配和网络优先级等问题的一种技术。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行，我司工业智能网关支持定制 QoS 业务。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用设置>转发设置> QoS”，打开“QoS”页签，如图 5-47 所示。

图 5-47 QoS 页签

步骤 3 单击“添加”，新建一条 QoS 规则。配置界面如图 5-48 所示

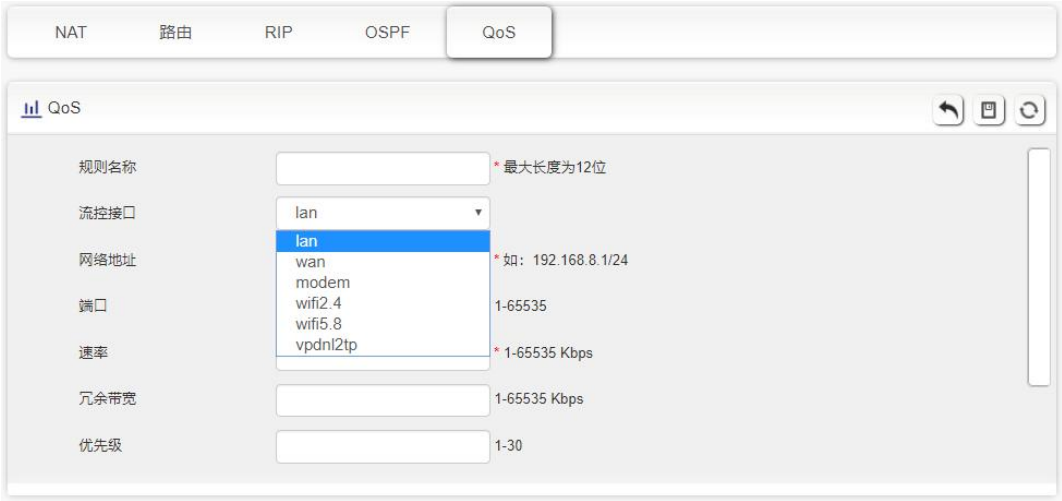


图 5-48 QoS 配置界面

步骤 4 配置 QoS 参数。QoS 的参数说明如表 5-30 所示。

表 5-30 QoS 参数说明

参数名称	含义	如何配置
状态	启用/禁用 QoS 功能。	单击“启用”/“禁用”按钮选择。
基本设置		
规则名称	QoS 的规则名称。	最大允许输入 12 个字符。 只能在添加新规则的时候设定，后续不能修改。 规则名称不能重复，否则后添加的规则将覆盖前面添加的规则。
流控接口	进行流量控制的接口类型，包含： • lan：流控的接口为 LAN 口 • wan：流控的接口为 WAN 口 • wifi2.4/wifi5.8：流控的接口为 wifi • modem：流控的接口为 modem	下拉选项： • lan • wan • modem • wifi2.4 • wifi5.8

参数名称	含义	如何配置
网络地址	进出流控接口的网络地址，限速的对象。	填入目的地址和子网掩码位数即可。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。
端口	需要进行流控的网络端口。	取值范围：1～65535 该端口可以不配置，若不配置则代表所有端口。
速率	对网络地址设置的传输速率。	取值范围：1～1024000 单位：Kbps
冗余带宽	在保证基本速率且带宽有空余的情况下，该网络地址通信可以获得的最大带宽，优先级高的将会优先获得冗余带宽。	取值范围：1～1024000 单位：Kbps
优先级	设置该规则的优先级。	取值范围：[1,30]

步骤 5 单击“保存”完成参数配置。

说明

QoS 主要用于网关给上网的用户平均分配路由或优先某个上网用户使用带宽。如网关下接有两个子网：192.168.8.1/24 和 192.168.9.1/24，则网关可以通过 QoS 来控制这两个子网的速率；若网关的带宽比较宽裕，则网关可以根据两个子网的优先级和冗余带宽先满足优先级高的冗余带宽，再满足优先级低的子网的冗余带宽。

---结束

RIP 配置

RIP（Route Information Protocol，路由信息协议）协议是最广泛使用的 IGP(Interior Gateway Protocol，内部网关协议)之一，被设计用于使用同种技术的小型网络，因此适应于大多数的校园网和使用速率变化不是很大的连续线的地区性网络，工业智能网关支持 RIP v2 协议。对于更复杂的环境，一般不使用 RIP 协议。RIP 业务可在工业智能网关出厂时根据用户是否需要进行配置。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用设置>转发设置>RIP”，打开“RIP”页签，如图 5-49 所示。

图 5-49 RIP 页签

参数说明如表 5-31 所示。

表 5-31 RIP 参数说明

参数名称	含义	如何配置
RIP 服务	启用/禁用 RIP 服务	单选按钮选择。
发布连接路由	是否允许发布连接路由	单选按钮选择。 根据自身需求选择是否允许发布连接路由。
发布静态路由	是否允许发布静态路由	单选按钮选择。 根据自身需求选择是否允许发布静态路由。
发布内核路由	是否允许发布内核路由	单选按钮选择。 根据自身需求选择是否允许发布内核路由。

步骤 3 单击“添加”按钮，新建一条 RIP 规则。配置界面如图 5-50 所示。.

图 5-50 RIP 规则配置页面

步骤 4 配置路由模式规则参数。参数说明如表 5-32 所示。

表 5-32 RIP 参数说明 II

参数名称	含义	如何配置
基本设置		

参数名称	含义	如何配置
通告类型	添加 RIP 路由的类型。	单选按钮选择。 选择需要的类型即可。 • 当选择为“网络”时，需要配置目的网络地址（一般为网关直连的网络）。 • 当选择为“邻居”时，需要配置邻居的 IP 地址（与网关相连的网关的 IP 地址）。
网络（与网关直接相连的网络才能添加）	添加 RIP 路由的目的网络。	填入需要添加 RIP 路由的目的网络地址。 格式：A.B.C.D/M，输入规范请参见“　　参数规范表”。
邻居（与网关直接相连的网关）	添加 RIP 路由的邻居的 IP 地址。	填入需要添加 RIP 路由的邻居的 IP 地址即可。 格式：A.B.C.D/M，输入规范请参见“　　参数规范表”。

步骤 5 单击“保存”，完成该条 RIP 规则配置。

说明

路由信息协议（RIP）是一种在网关与主机之间交换路由选择信息的标准。RIP 是一种内部网关协议。在国家性网络中（如当前的因特网），拥有很多用于整个网络的路由选择协议。

- 仅和相邻的网关交换信息。如果两个网关之间的通信不经过另外一个网关，那么这两个网关是相邻的。RIP 协议规定，不相邻的网关之间不交换信息。
- 网关交换的信息是当前本网关所知道的全部信息。即自己的路由表。
- 按固定时间交换路由信息（如每隔 30 秒），然后网关根据收到的路由信息更新路由表。

RIP 协议的“距离”也称为“跳数”(hop count)，因为每经过一个网关，跳数就加 1。RIP 认为好的路由就是它通过的网关的数目少，即“距离短”。RIP 允许一条路径最多只能包含 15 个网关。因此“距离”等于 16 时即相当于不可达。可见 RIP 只适用于小型互联网。

---结束

OSPF 配置

OSPF（Open Shortest Path First，开放式最短路径优先）协议是最广泛使用的 IGP（Interior Gateway Protocol，内部网关协议）之一，用于在单一自治系统(autonomous System,AS)内决策路由，适用于大型网络。OSPF 业务可在工业智能网关出厂时根据用户是否需要进行配置

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用设置>转发设置>OSPF”，打开“OSPF”页签，如图 5-51 所示。

图 5-51 OSPF 页签

参数说明如表 5-33 所示。

表 5-33 OSPF 参数说明 I

参数名称	含义	如何配置
OSPF 服务	启用/禁用 OSPF 服务	单选按钮选择。
发布连接路由	是否允许发布连接路由	单选按钮选择。 根据自身需求选择是否允许发布连接路由。
发布静态路由	是否允许发布静态路由	单选按钮选择。 根据自身需求选择是否允许发布静态路由。
发布内核路由	是否允许发布内核路由	单选按钮选择。 根据自身需求选择是否允许发布内核路由。

步骤 3 单击“添加”，新建一条 OSPF 规则。配置界面如图 5-52 所示。

图 5-52 OSPF 规则配置页面

步骤 4 配置路由模式规则参数。参数说明如表 5-34 所示。

表 5-34 OSPF 规则参数说明 II

参数名称	含义	如何配置
通告类型	添加 OSPF 路由类型。	单选按钮选择。 选择需要的类型即可。 • 网络 • 邻居 • 接口
当“通告类型”选择“网络”时		
网络	设置某个网段作为网关 OSPF 发送地址。	格式：A.B.C.D/M 接口型，输入规范请参见“参数规范表”。
域地址	用于标识网络（只有域地址相同的网关之间才会使用 OSPF 协议来交换路由信息）。	手动输入，取值范围：[0,65535]
当“通告类型”选择“邻居”时		
邻居	网关可以一跳到达的设备地址。	手动输入，格式：A.B.C.D/M 接口型，输入规范请参见“参数规范表”。
当“通告类型”选择“接口”时		
接口名称	网关的某个接口	下拉列表选择： • lan • modem • wifi2.4 • wifi5.8 • wan
接口属性	配置网关接口的属性，包括开销和网络两种属性	单击按钮选择 • 开销 • 网络
开销	配置网关接口的开销，用于 OSPF 路由表的学习	手动输入，取值范围：1～65535
网络类型（接口属性选择“网络”时需配置）	配置网关接口的网络类型。	下拉列表选择： • broadcast • non-broadcast • point-to-multipoint • point-to-point

步骤 5 单击“保存”，完成该条 OSPF 规则配置。

说明

OSPF 路由协议是一种典型的链路状态（Link-state）的路由协议，一般用于同一个路由域内。在这里，路由域是指一个自治系统，它是指一组通过统一的路由政策或路由协议互相交换路由信息的网络。在这个 AS 中，所有的 OSPF 网关都维护一个相同的描述这个 AS 结构的数据库，该数据库中存放的是路由域中相应链路的状态信息，OSPF 网关正是通过这个数据库计算出其 OSPF 路由表的。

作为一种链路状态的路由协议，OSPF 将链路状态广播数据 LSA（Link State Advertisement）传送给在某一区域内的所有网关，这一点与距离矢量路由协议不同。距离矢量路由协议是将部分或全部的路由表传递给与其相邻的网关。

---结束

5.5.4 安全设置

安全设置是指网关的防火墙功能。工业智能网关支持 IP 过滤、域名过滤和 MAC 地址过滤等三种安全设置。用户通过分析进入网关数据包的 IP 地址/端口、MAC 地址、域名，与用户添加的防火墙规则进行对比，并对与防火墙规则匹配的数据包执行接收或丢弃动作来达到如允许/禁止某些网段访问外网、允许/禁止其他用户访问网关等目的。

IP 过滤

IP 过滤是指网关通过滤 IP 地址规则来判定是否允许外部设备访问网关以及是否允许数据包经过网关转发，IP 过滤通常用来实现只允许某一部分主机访问外网或禁止某一部分主机访问特定网络。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用设置>安全设置>IP 过滤”，打开“IP 过滤”页签，如图 5-27 所示。

图 5-53 IP 过滤页签

输入/转发过滤规则中，

- 黑名单：默认允许数据包转发，符合名单中“丢弃”规则的数据包不能经过网关转发。

- 白名单：默认拒绝数据包转发，符合名单中“接受”规则的数据包可以经过网关转发出去。

步骤 3 单击“添加”，添加一条新的 IP 过滤规则，配置 IP 过滤参数。IP 过滤有两种过滤类型：“输入”和“转发”，规则配置页面如图 5-54 和图 5-55 所示。

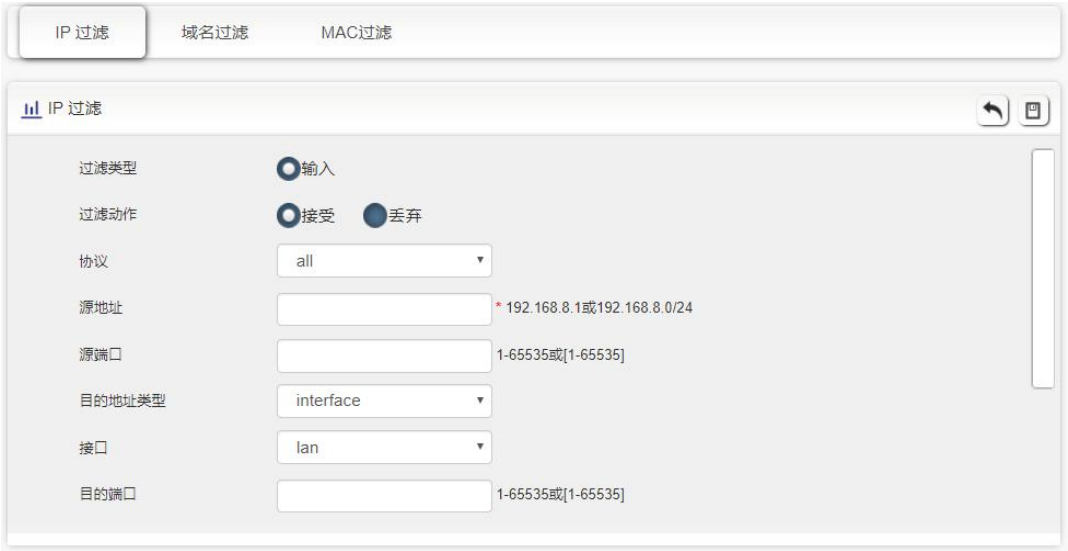


图 5-54 输入过滤规则页面

图 5-55 转发过滤规则页面

参数说明如表 5-35 所示。

表 5-35 IP 过滤参数说明

参数名称	含义	如何配置
过滤类型	选择一种过滤类型，可以根据自身需求选择“输入”或者“转发”。 • 输入：是否允许访问网关。 • 转发：是否允许经过网关转发。	单选按钮选择。
过滤动作	该条规则的默认动作。可以选择“接受”或“丢弃”。 • 接受：防火墙接受这个包，即可以通过。 • 丢弃：防火墙对这个包直接做丢弃处理。	单选按钮选择。 根据自身需求选择“接受”或“丢弃”即可。
镜像规则	当过滤类型选择“转发”时需要配置 • 启用：在所配置规则基础上额外添加一条源地址/端口与目的地址/端口反向的规则； • 禁用：不做任何处理。	单选按钮选择。
协议	IP 数据包使用的协议	下拉列表选择。 • all • tcp • udp • icmp
源地址	IP 数据包的源地址。	格式：A.B.C.D 型，输入规范请参见“参数规范表”。 例如：192.168.8.1 或 192.168.8.1/24
源端口	IP 数据包的源端口，当协议选择“icmp”时，不需要配置。	取值范围：1～65535 或 [1-65535]；可以是范围，也可以是单个端口。
当过滤类型选择“输入”时		
目的地址类型	指定 IP 数据包访问的网关接口。	下拉列表选择。 • interface • any
接口	目的地址类型选择“interface”时需要配置，表示 IP 数据包访问的网关端口（若目的地址类型选择的是“any”，则表示网关的所有接口）。	下拉列表选择。 • lan • modem • wan • wifi2.4 • wifi5.8
目的端口	IP 数据包访问的网关端口（当协议选择“icmp”时，不需要配置）	取值范围：1～65535 或 [1-65535]；可以是范围，也可以是单个端口。

参数名称	含义	如何配置
当过滤类型选择“转发”时		
目的地址	IP 数据包中的目的地址。	格式：A.B.C.D 型，输入规范请参见“参数规范表”。
目的端口	IP 数据包中的目的端口	取值范围：1～65535 或[1-65535]；可以是范围，也可以是单个端口。

步骤 4 单击“保存”，完成该条 IP 过滤规则配置。

说明

IP 输入规则表示是否允许其他设备访问网关，该规则中的目的地址只能选择网关的接口；IP 转发规则表示是否允许 IP 数据包经过网关转发出去，该规则中的目的地址可以是除网关接口地址外的其他所有 IP 地址。

当规则中配置了端口后，选择“all”协议表示同时选择“tcp”和“udp”两种协议；当规则中未配置端口，选择“all”协议表示同时选择“tcp”、“udp”和“icmp”三种协议。

--结束

域名过滤

域名过滤支持黑白名单，主要目的是禁止局域网内主机访问某些域名或者只允许访问指定域名。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用设置>安全设置>域名过滤”，打开“域名过滤”页签，如图 5-56 所示。

图 5-56 域名过滤页签

- 黑名单：默认允许访问任何域名，符合名单中动作为“丢弃”规则的数据包会被丢弃。
- 白名单：默认拒绝访问任何域名，符合名单中动作为“接受”规则的数据包会被接受并转发。

步骤 3 单击“添加”按钮，添加一条新的域名过滤规则，配置域名过滤参数。规则配置页面如图 5-57 所示。

图 5-57 域名过滤规则配置页面

参数说明如表 5-36 所示。

表 5-36 域名过滤规则配置参数说明

参数名称	含义	如何配置
域名关键字	需过滤域名的关键字。	WORD 型，最大长度为 64 位，输入规范请参见“参数规范表”。 如 www.baidu.com 的域名关键字是“baidu”。
过滤动作	对域名关键字执行的动作。	单击按钮选择。 • 接受：对域名关键字为输入的字符串的包的动作为接受并进行转发 • 丢弃：对域名关键字为输入的字符串的包的动作为丢弃

步骤 4 单击“保存”，完成该条域名过滤规则配置。

---结束

MAC 过滤

MAC 过滤也同样支持黑白名单，它通常用来控制主机对网关的接入访问。工业智能网关除了实现该功能外，还能限制特定 MAC 主机的外网访问权限，或者只允许特定 MAC 地址的主机访问外网。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用设置>安全设置>MAC 过滤”，打开“MAC 过滤”页签，如图 5-58 所示。

图 5-58 MAC 过滤页签

参数说明如表 5-37 所示。

表 5-37 MAC 过滤页签说明

参数名称	含义	如何配置
MAC 输入过滤规则配置		
动作	启用 MAC 输入过滤黑名单/白名单。	单选按钮选择。 • 黑名单：默认允许访问网关，符合名单中的“丢弃”规则的设备访问网关的数据包会被丢弃。 • 白名单：默认拒绝访问网关，符合名单中的“接受”规则的设备访问网关的数据包会被接受。 同一时间，黑名单、白名单只有一个名单生效。
MAC 转发过滤规则配置		
动作	启用 MAC 转发过滤黑名单/白名单。	单选按钮选择。 • 黑名单：默认接受数据包的转发，符合名单中“丢弃”规则的数据包会被丢弃。 • 白名单：默认拒绝数据包的转发，符合名单中“接受”规则的数据包会被接受并转发。 • 同一时间，黑名单、白名单只有一个名单生效。

步骤 3 单击“添加”，添加一条新的 MAC 过滤规则，配置 MAC 过滤参数。规则配置页面如图 5-59 所示。

图 5-59 MAC 过滤规则配置页面

参数说明如表 5-38 所示。

表 5-38 MAC 过滤规则配置参数说明

参数名称	含义	如何配置
基本设置		
MAC	需过滤的 MAC 地址。	WORD 类型 MAC 格式：XX:XX:XX:XX:XX:XX

参数名称	含义	如何配置
过滤动作	该规则的默认动作，可以是接受”或“丢弃”。 • 接受：接受所有从该 MAC 地址发出的包。 • 丢弃：对所有从该 MAC 地址发出的包做丢弃处理。	单选按钮选择。 根据自身需求选择“接受”或者“丢弃”。
过滤模式	该规则的过滤模式，可以是“输入”、“转发”或“输入和转发”。 • 输入：所有访问网关的包。 • 转发：所有经过网关转发的包。 • 输入和转发：所有访问网关的包和所有经过网关转发的包。	单选按钮选择。 根据自身需求选择“输入”、“转发”或“输入或转发”。

步骤 4 单击“保存”，完成该条 MAC 过滤规则配置。

---结束

5.5.5 DDNS 设置

DDNS 是动态域名系统的缩写，DDNS 协议提供动态 IP 和域名之间的对应查询功能。DDNS 可以让用户在任何可以连上公网的 PC 机通过域名访问网关的页面。当然，网关使用的 SIM 卡对应的网络必须是公网可访问地址，这样才能保证输入域名就可以访问网关。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用程序设置>DDNS 设置”。

打开“应用设置>DDNS 设置”页签，如图 5-60 所示。

图 5-60 DDNS 设置页签

步骤 3 配置 DDNS 服务参数。

参数说明如表 5-39 所示。

表 5-39 DDNS 服务参数说明

参数名称	含义	如何配置
DDNS 服务	使能 DDNS 服务。	按钮 • 启用 • 禁用
基本设置		
服务提供商	申请的域名对应域名提供商选项，目前我司暂不支持列表之外的域名提供商的 DDNS 服务。	下拉框选项 • 3322 • 88ip • Dnsexit • Dyndns • Zoneedit • changeip • custom
服务地址	服务提供商选择 custom 时配置，当自建 DDNS 服务器时配置，自定义默认为标准 DDNS 协议，如有配置需要可联系我司技术人员定制协议。	一般 WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。
服务端口	域名服务提供商的 DDNS 服务器端口号，默认一般都为 80 端口，通常在自定义 DDNS 服务时会使用非 80 端口。	取值范围：1～65535 不配置时表示端口为 80。
用户名/密码	注册 DDNS 服务提供商域名时的用户名、密码。	一般 WORD 类型/CODE 类型，最大 64 个字节。
用户域名	DDNS 服务提供商提供的域名，它与网关的 IP 相对应，通常通过访问该域名来访问网关的 IP。	一般 WORD 类型，最大 64 字节。
更新间隔	网关向 DDNS 域名服务提供商更新 IP 地址的间隔时间，若设置该参数，则网关按照“更新间隔”上报 IP 地址；若不设置，则当 IP 地址发生变化时，才向域名提供商上报 IP 地址。	取值范围：120～86400 单位：秒

步骤 4 单击“保存”，完成 DDNS 服务配置。

说明

- 国内的 DDNS 服务商：88IP（www.88ip.net）、3322（www.3322.org）
- 国外的 DDNS 服务商：DNSEXIT(www.dnsexit.com)、ZONEEDIT(www.zoneedti.com)、CHANGEIP(www.changeip.com)、DYNDNS(www.members.dyndns.org)
- 每次网关重启时，从 SIM/UIM 卡服务提供商那里得到的 IP 地址都会改变。如果用户在远程登录网关时使用的是申请到的 DDNS 域名，那么不管网关 modemIP 地址怎么改变，用户都可以登录到网关页面。

---结束

5.5.6 SNMP 配置

SNMP（Simple Network Management Protocol）简单网络管理协议，启用该功能之后，可以使用 SNMP 管理工具对设备进行远程监测，查看设备的运行状态（支持 VPN 等状态查看需要导入我司 MIB 库）。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用程序设置>SNMP 配置”。

打开“应用设置>SNMP 配置”页签，如图 5-61 所示。

图 5-61 SNMP 配置页签

步骤 3 配置 SNMP 参数。

参数说明如表 5-40 所示。

表 5-40 SNMP 参数说明

参数名称	含义	如何配置
SNMP 服务	使能 SNMP 服务。	单选按钮选择。 • 启用 • 禁用
基本设置		
服务端口	SNMP 服务侦听端口，建议配置为其默认端口 161。	取值范围：1～65535 缺省：161

参数名称	含义	如何配置
共同体	SNMP 客户端连接网关 SNMP 服务的共同体密码，用于身份识别。	WORD 类型，最大 16 个字节，输入规范请参见“参数规范表”。
Trap IP	网关链路状态上报的服务器地址。	格式：A.B.C.D 接口型，输入规范请参见“参数规范表”。
Trap 端口	网关链路状态上报的服务器端口。	取值范围：1～65535 缺省：162
回环标识状态	与“LAN”页面中的回环地址对应：在“回环标识状态”为“启用”，如果回环地址配置成功，则网关 Trap 上报的 IP 包源地址就是回环地址；若“回环标识状态”为“禁用”，则网关 Trap 上报的 IP 包源地址为 LAN 口地址。	单选按钮选择 • 启用 • 禁用

步骤 4 单击“保存”，完成 SNMP 配置。

说明

Trap：SNMP 协议 5 个数据类型中的一个，指被管理设备上报的陷阱报文，表明设备发生故障或变更的通知。工业智能网关上报 Trap 的类型和内容包括：modem 的连接状况及哪个接口、哪张 SIM 卡拨号，VPDN/TUNNEL/IPSec 接口的连接和断开等。
与 SNMP 对应的 MIB 库可以在我司公网上下载，如有需要，请联系我司技术人员。

---结束

5.6 运维管理

工业智能网关系统管理功能主要是对系统进行一些日常的维护操作。例如：网络诊断、通过日志分析系统的运行情况等。

5.6.1 网络诊断

PING 功能

网络诊断，包括了常用的 Ping 功能和 Tracert 功能，具体使用步骤如下：

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“运维管理>网络诊断”。

打开“网络诊断”页签，如图 5-62 所示。

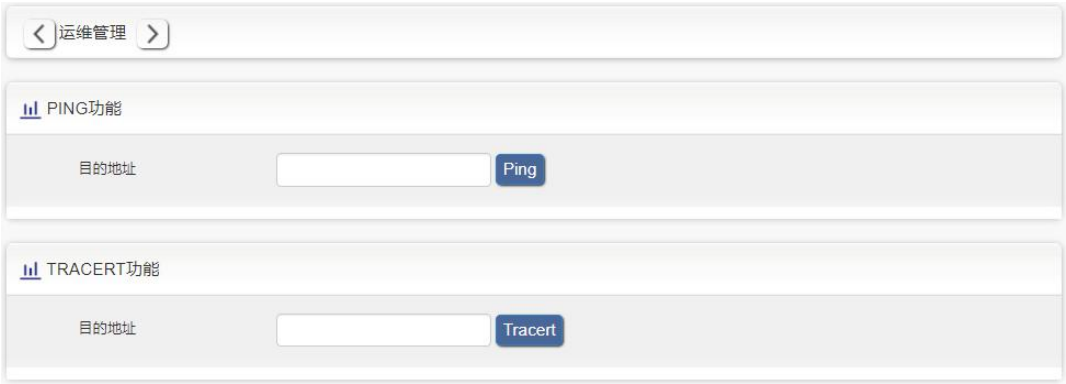


图 5-62 网络测试配置页面

步骤 3 在“目的地址”框中输入要测试 IP 地址或域名，单击“Ping”，测试网关与目的地址的连通性。

参数和按钮说明如表 5-41 所示。

表 5-41 网络诊断参数说明

参数名称	含义	如何配置
目的地址	设置用于测试的目的 IP 地址或域名。	填入要用于测试的目的 IP 地址或域名即可。
Ping	使用 Ping 命令测试网络连接连通性。	单击“Ping”。
Tracert	使用 Tracert 命令测试网关到达目的地址的跳数。	单击该按钮即可使用 Tracert 命令。
检查结果	网络测试的结果。	无。

说明

Tracert：即 traceroute，通过 Traceroute 我们可以知道信息从计算机到互联网另一端的主机是走的什么路径；通过发送小的数据包到目的设备直到其返回，来测量其需要多长时间。一条路径上的每个设备 Traceroute 要测 3 次。输出结果中包括每次测试的时间(ms)和设备的名称（如有的话）及其 IP 地址。

---结束

5.6.2 本地日志

本地日志是指通过在工业智能网关管理界面直接查看系统运行、操作配置等信息。通过这些信息，能够查找系统异常状况，并准确的定位问题和采取有效的预防或补救措施。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“运维管理>本地日志”，打开“本地日志”页签，如图 5-63 所示。

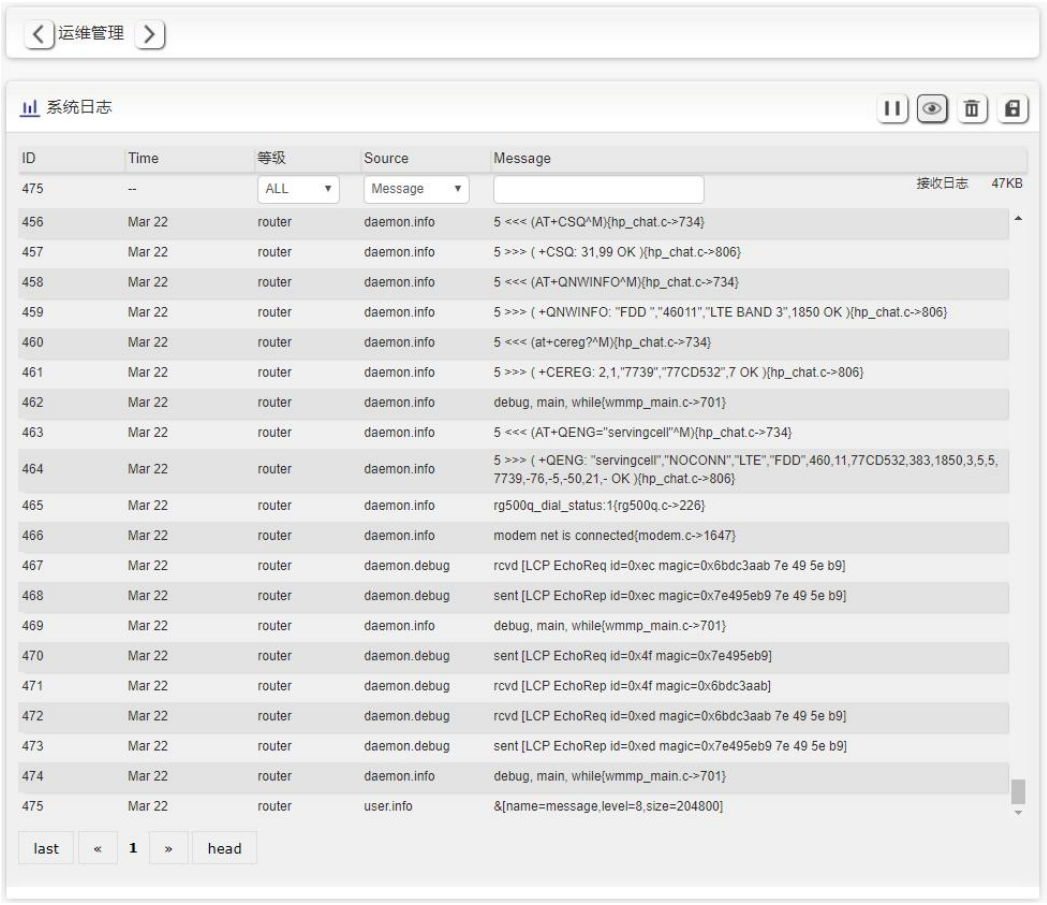


图 5-63 本地日志页签

步骤 3 在“系统日志”中选择要查询的日志的类型，单击“查看”，则在“日志列表”中显示查询到的日志。

还可以单击“清空”清除“日志列表”中的日志信息；单击“导出”导出日志信息到本地。

日志分类包含三种类型：

- message：系统日志，记录网关运行日志，用户一般只适用系统日志。
- application：应用程序日志，记录网关进程的开启或关闭等信息。
- kernel：程序内核日志，打印内核信息，一般由研发人员查看参考。

---结束

5.6.3 远程日志

“远程日志”主要用于连接远程日志服务器，网关可以将本地日志上传到远程日志服务器，配置步骤如下：

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“系统管理>远程日志”，打开“远程日志”页签，如图 5-64 所示。

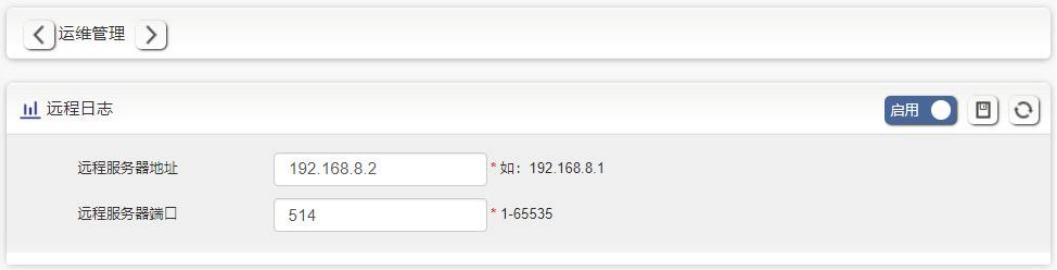


图 5-64 系统日志页签

步骤 3 配置系统日志参数。参数说明如表 5-42 所示。

表 5-42 系统日志参数说明

参数名称	含义	如何配置
日志状态	启用/禁用远程日志。	单击“启用”即可启用系统日志功能。
远程日志服务器地址	远端日志服务器的 IP 地址（既可以是 LAN 侧 PC 的 IP 地址，又可以是公网地址）。	填入接收日志信息的 PC 机的 IP 地址即可。
远程日志服务器端口号	远端日志服务器的端口号。	填入远端日志服务器的端口号，默认为 514。

步骤 4 单击“保存”，完成系统日志参数配置。

说明

在网关将系统日志发送至远程日志服务器地址后，将使用 Syslog 工具进行接收；通过 Syslog 工具，可以区分来至不同网关、不同功能的日志，便于用户查看日志。
Syslog 工具可以在深圳宏电技术股份有限公司官网上进行下载。

---结束

5.7 平台管理

5.7.1 M2M 设置

工业智能网关通过 WMMP 协议（Wireless Machine-to-Machine Protocol）实现与 M2M（Machine-to-Machine）平台通信功能，可通过平台实现对设备的远程维护管理和现场网络状态的监控管理，如查看设备信息、升级补丁、升级固件、配置参数等，查看设备网络信号强度、时延、流量等。具体设置说明如下。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“应用程序设置>M2M 配置”。

打开“M2M 配置”页签，如图 5-65 所示。

图 5-65 M2M 配置页签

步骤 3 配置 M2M 参数。

参数说明如表 5-43 所示。

表 5-43 M2M 参数说明

参数名称	含义	如何配置
M2M 服务	使能 M2M 服务，该功能需要配合我司 M2M 终端管理平台使用。	按钮 • 启用 • 禁用
基本设置		
服务 IP 或域名	设备云平台服务器的 IP 地址或域名。	WORD 类型，最大 64 个字节，输入规范请参见“参数规范表”。
服务端口	设备云平台服务器 WMMP 服务所使用的端口号，与服务器匹配即可。	取值范围：1～65535

步骤 4 单击“保存”，完成 M2M 配置。

---结束

5.8 系统管理

5.8.1 系统时间

工业智能网关支持 NTP（Network Time Protocol）网络协议对时。进行 NTP 网络对时可以保证网关的系统时间与实际时间对应，可以保证任务管理等功能在正确的时间执行。具体步骤如下。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“系统管理>系统时间”，打开“系统时间”页签，根据“时间同步类型”不同，展示的页面分别如图 5-66 和图 5-67 所示。

图 5-66 网络时间同步方式

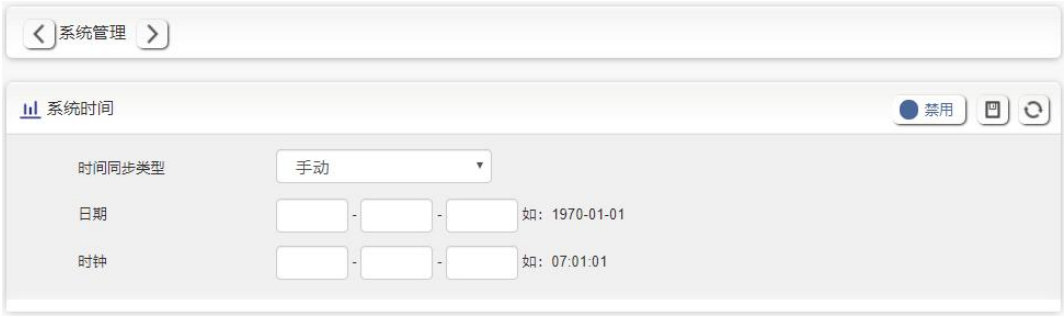


图 5-67 手动方式同步时间

步骤 3 配置系统时间参数。参数说明如表 5-44 所示。

表 5-44 系统时间参数说明

参数名称	含义	如何配置
状态	“启用”或“禁用”系统时间同步。	• 单击“启用”即可启用系统时间同步功能。 • 单击“禁用”即禁止系统时间同步功能。
时间同步类型	进行系统时间校验的时间同步类型。	下来列表框选择。 • 采用 NTP 网络时间校对 • 采用手动方式进行校对
当“时间同步类型”选择“网络时间”时		
主服务器地址	NTP 时钟服务器域名。	从下拉列表中选择合适的 NTP 时钟服务器域名即可。
备用服务器地址	备用的 NTP 服务器域名或 IP 地址，主服务器不通或者不能同步到时间时使用，一般不需要配置。	手动输入服务器域名或 IP 地址。

参数名称	含义	如何配置
同步间隔	NTP 与服务器时间同步频率，如每隔 10 分钟（600 秒）进行一次自动对时。	取值范围：1～65535 单位：秒 缺省值：600
时区	地理时区。	从下拉列表中选择网关所在的时区。
当“时间同步类型”选择“手动”时（本页只显示配置的时间，系统时间在页面上方）		
日期	校验的标准日期。	格式为 YYYY-MM-DD 如 1970-01-01
时钟	校验的标准时间。	格式为 HH:MM:mm 如 07:01:01

步骤 4 单击“保存”，完成系统日志参数配置。

---结束

5.8.2 用户管理

用户管理提供用户修改用户名/密码的功能。同时，用户管理可以修改网关的 WEB 访问端口，屏蔽其他用户访问路由。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“系统管理>用户管理”，打开“用户管理”页签，如图 5-68 所示。

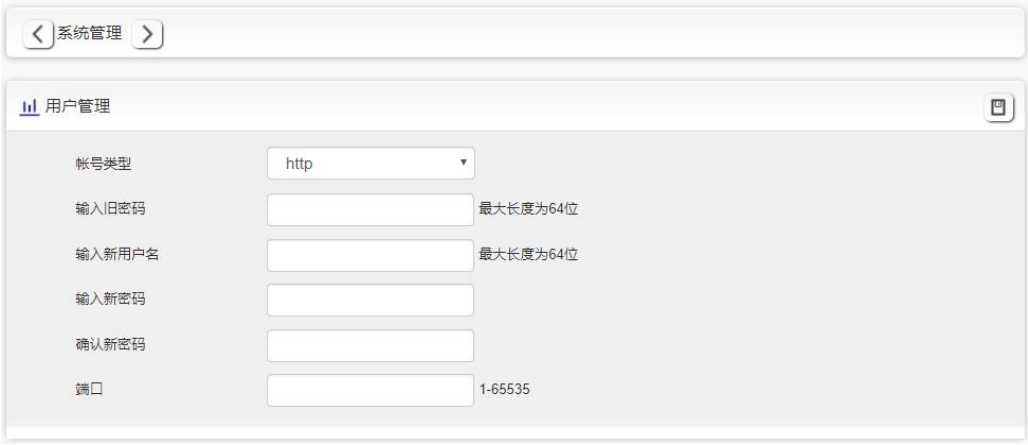


图 5-68 用户管理配置页面

步骤 3 配置用户管理参数。参数说明如表 5-45 所示。

表 5-45 用户管理参数说明

参数名称	含义	如何配置
帐号类型	通过 WEB 页面登录网关。	下拉列表选择。
输入旧密码	当前登录用户的登录密码。	输入当前登录用户的登录密码。
输入新用户名	用户修改后的用户名。	手动输入，最大长度为 64 位的 word 字符串，输入规范请参见“参数规范表”。
输入新密码	用户修改后的密码。	手动输入，最大长度为 64 位的 word 字符串，输入规范请参见“参数规范表”。
确认新密码	用户修改后的密码，修改后的确认密码。	手动输入，最大长度为 64 位的 word 字符串，输入规范请参见“参数规范表”。
端口	用户登录网关页面端口。	手动输入 取值范围 1～65535 默认：80

说明

用户管理只提供用户的修改功能，不提供添加、删除等功能。
若没有修改过“端口”参数，则直接输入网关的 IP 地址就可以登录网关页面；若端口修改为其他数字且修改成功，则需要输入网关的“IP：端口”才能登录网关页面。

步骤 4 修改完毕后单击“保存”。保存成功之后，页面或自动跳转到登录界面，用户需要输入修改之后的用户名/密码才能进入。

---结束

5.8.3 证书管理

证书管理提供导入证书的功能。可以导入 VPN 证书等。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“系统管理>证书管理”，打开“证书管理”页签，如图 5-69 所示。

图 5-69 证书管理配置页面

步骤 3 点击“文件”选择本地证书，点击“导入”上传证书。

可以对证书进行保存、删除操作。

5.8.4 文件升级

升级设置

工业智能网关支持本地网络方式升级系统文件，在升级之前请确定你已获得系统更新的目标文件，并将更新文件已经存放置局域网的计算机上。

步骤 1 登录工业智能网关 WEB 配置界面。

步骤 2 单击“系统管理>文件升级”。

显示“文件升级”界面，如图 5-70 所示。

图 5-70 文件升级页面

步骤 3 单击“文件”，在本地选择升级文件，单击“升级”系统开始进行升级。选中“恢复默认”则在升级补丁或者程序后，网关的配置将恢复到出厂设置；不选中，则表示仅升级补丁或程序，网关的参数配置将会保持。

---结束

备份设置

工业智能网关支持配置文件的备份和恢复，如图 5-71 所示。

- 单击“文件”，浏览本地需要导入的配置文件，单击“导入”完成文件的导入。若网关参数发生错误或文件丢失，可以使用“导入”功能实现参数的还原。
- 单击“导出”，即可导出配置文件到本地，实现文件/参数的备份功能。

图 5-71 备份功能

说明

导入备份文件后，系统自动重启，在重启系统之后才能生效。
密钥：当导出一份文件时添加密钥，那在导入该份文件时需要输入该密钥，否则会导致网关乱码；该密钥可以不填写。若在导入时，密钥输入错误，则会导致无法进入网关页面。
若输出密钥，则密钥必须为八位。

查看补丁信息

工业智能网关具备了查看补丁信息功能，可以查看补丁文件夹下的补丁信息和删除所有补丁文件功能。如图 5-72 所示。

图 5-72 补丁文件操作

- 删除：删除所有补丁文件。

TF 卡升级

- 拷贝升级的 roofs，kernel，boot 和配置文件到 TF 卡，配置文件默认
- 插上 TF 卡，设备上电

---结束

5.8.5 复位重启

出厂设置

工业智能网关具备常用的出厂设置功能，可以根据需要恢复到出厂设置状态。也可以将现有的配置设为默认配置，并在网关中生成一个默认配置文件，用户可以单击“恢复默认”随时将配置恢复到这个默认配置。若该默认配置文件或被删除，则网关会恢复至最初的出厂设置。如图 5-73 所示。

图 5-73 出厂设置页面

- 设为默认：将当前配置保存为默认出厂配置。
- 恢复默认：恢复出厂配置。

重启设备

单击“重启设备”按钮可以重新启动系统。如图 5-73 所示。

6 其他功能

关于本章

章节	内容简介
6.1 RESET 功能	本节简要介绍工业智能网关的 RESET 功能。

6.1 RESET 功能

“RESET”键位于设备前面板 USB 接口旁，可在设备正常运行时使用和设备上电时使用。

设备正常运行时使用包含如下功能：

- 轻压“RESET”键 0~5 秒左右，则重启系统。
- 轻压“RESET”键 5 秒以上，则重启系统，同时系统配置将恢复到默认出厂状态。

7 异常处理

关于本章

章节	内容简介
7.1 硬件类	本节简要介绍工业智能网关在使用过程中可能发生的硬件类故障的产生原因及处理方法。
7.2 拨号类问题	本节简要介绍工业智能网关在使用过程中可能发生的拨号类故障的产生原因及处理方法。
7.3 VPN 连接类问题	本节简要介绍工业智能网关在使用过程中可能发生的 VPN 连接类故障的产生原因及处理方法。
7.4 WEB 配置操作类问题	本节简要介绍工业智能网关在使用过程中可能发生的 WEB 配置类故障的产生原因及处理方法。

7.1 硬件类问题

7.1.1 所有指示灯均不亮

问题现象

工业智能网关所有指示灯均不亮。

原因分析

可能原因如下：

- 供电电源不符合要求
- 供电电源与网关电源口没有连上

解决方法

- 如果是供电电源不符合要求，请确保电源的供电范围为+9V～24V。
- 如果是网关电源口与供电电源连接上，请将电源线插入电源口。

7.1.2 SIM 卡座连接问题

问题现象

SIM 卡槽无法正常插入 SIM 卡。

原因分析

- SIM 卡槽已经损坏
- SIM 卡的插入方向错了

解决方法

- 如果是 SIM 卡槽损坏，请联系我司技术支持工程师是否需要报修。
- 如果是 SIM 卡的插入方向错了，请确认 SIM 卡插入时芯片朝上且切角后插入卡座。

7.1.3 TF 卡槽连接问题

问题现象

TF 卡槽无法正常插入 TF 卡。

原因分析

工业智能网关的 TF 卡槽在设备内部，需拆掉外壳后检查 TF 卡情况。

- TF 卡槽已经损坏
- TF 卡的插入方向错了

解决方法

- 如果是 TF 卡槽损坏，请联系我司技术支持工程师是否需要报修。
- 如果是 TF 卡的插入方向错了，请确认 TF 卡插入时有金属片方向朝上插入卡座。

7.1.4 网口连接问题

问题现象

LAN 口指示灯不亮，且无法访问网关 WEB 页面。

原因分析

- 网线安装不正确
- 网线已损坏
- PC 端网卡工作异常

解决方法

- 如果是网线安装不正确，请重新安装网线。
- 如果是网线已损坏，请更换网线。

- 如果是 PC 端网卡工作异常，请更换网卡。

7.2 拨号类问题

7.2.1 拨号中断

问题现象

工业智能网关拨号过程中断，拨号失败。

原因分析

- SIM 卡网络类型不符合要求
- SIM 卡已欠费
- 供电电源不符合要求
- Modem 拨号配置不正确

解决方法

- 如果是 SIM 卡网络类型不正确，请根据模块更换相应类型的 SIM 卡。
- 如果是 SIM 卡欠费，请到指定的 ISP 处为 SIM 卡充值。
- 如果是供电电源不符合要求，请更换符合要求的供电电源。
- 如果是 Modem 拨号配置有误，请参见“移动网络”进行正确的配置。

7.2.2 无法找到 SIM/UIM 卡

问题现象

工业智能网关移动网络状态页面显示无法找到 SIM 卡。

原因分析

- SIM 卡已损坏
- SIM 卡松动、接触不正常或安装不正确

解决方法

- 如果是 SIM 卡已损坏或无效，请更换 SIM 卡。
- 如果是 SIM 卡松动、接触不正常或安装不正确，请重新安装。

7.2.3 通信信号薄弱

问题现象

工业智能网关移动网络状态页面显示无信号或信号差。

原因分析

- 天线未安装好或者已损坏
- 设备所在区域网络覆盖和信号强度较弱

解决方法

- 如果是天线未正确安装，请正确安装天线。
- 如果是天线已损坏，请更换天线。
- 如果是设备所在区域网络覆盖和信号强度较弱，联系网络运营商进行合理解决。

7.2.4 压缩协议不匹配

问题现象

工业智能网关拨号失败，日志显示压缩协议不匹配。

原因分析

Modem 压缩协议配置与服务器对端不匹配。

解决方法

请修改 Modem 压缩协议配置，具体操作方法请参见“移动网络”。

7.3 VPN 连接类问题

7.3.1 VPDN 无法连接

问题现象

状态页面显示 VPDN 无法连接。

原因分析

可能原因如下：

- VPDN 连接使用的接口工作不正常
- VPDN 配置参数不正确
- VPDN 对端服务器工作不正常

解决方法

- 如果是 VPDN 连接所使用的接口工作不正常，请重新正确配置所使用的接口。如果是 Modem 接口工作不正常，请参见“移动网络”。
- 如果是 VPDN 接口工作不正常，请参见“5.4.8 VPDN 配置”。
- 如果是 VPDN 配置参数不正确，请参见“5.4.8 VPDN 配置”进行正确的配置。
- 如果是 VPDN 对端服务器工作不正常，请检查 VPDN 对端服务器的配置和工作状态。

7.3.2 VPN 无法通信

问题现象

VPN 页面显示已连接，但无法进行通信。

原因分析

可能原因如下：

- 路由表中配置的路由信息不正确
- VPN 对端服务器配置不正确

解决方法

- 如果是路由不正确，请添加正确的路由。
- 如果是 VPN 对端服务器配置不正确，请更改 VPN 对端服务器的配置。

7.3.3 路由可通信但子网不可通信

问题现象

路由可通信，但子网不可通信

原因分析

- VPN 对端服务器配置不正确
- 本端的网关没有做 MASQ
- 本地路由不正确

解决方法

- 如果是 VPN 对端服务器配置不正确，请正确修改 VPN 对端服务器的配置。
- 本端网关没有做 MASQ，请手动添加 VPN 接口的 MASQ，具体操作方法请参见“5.5.3 NAT”。
- 如果是本地路由不正确，请手动更改路由配置，具体配置方法请参见“5.5.3 路由配置”。

7.4 WEB 配置操作类问题

7.4.1 升级固件失败

问题现象

升级固件发现没有升级成功。

原因分析

- 升级时工业智能网关受其他功能影响而重启（如 Modem 拨不上号自动重启）
- 供电电源不符合要求
- 升级固件的型号、格式不正确
- 升级过程中网关断电

解决方法

- 如果是升级时受其他功能影响而重启造成的升级失败，请关闭其他功能，并重新升级。
- 如果是供电电源不符合要求，请更换符合要求的供电电源。
- 如果是升级固件型号、格式不正确，请更换格式正确、与工业智能网关相匹配的升级固件。
- 如果是升级过程中网关断电，请确保在升级过程中网关供电在正常。

7.4.2 恢复参数失败

问题现象

网关恢复参数失败。

原因分析

- 参数文件格式不正确
- 恢复参数后未重启网关

解决方法

- 如果是参数文件格式错误，请更换正确格式的参数文件。
- 恢复参数后必须重启网关，恢复参数才能生效。

7.4.3 升级补丁失败

问题现象

升级补丁后用查看补丁功能，发现没有补丁，补丁升级失败。

原因分析

- 检查补丁格式不正确。
- 补丁的名称不符合规定。

解决方法

- 如果是补丁格式不正确，请更换格式正确的补丁文件。
- 如果是补丁的名称不符合规定，请将补丁的名称改为规定的名称。

7.4.4 页面升级失败

问题现象

用页面升级时，显示升级失败，断电重启后，无法进入页面。

原因分析

升级的程序太大，导致升级失败。

解决办法

直接采用 TF 卡升级。若通过该方法无法进行升级，请联系我司工作人员。

7.4.5 忘记网关登录密码

问题现象

登录网关页面时忘记密码。

原因分析

用户在系统管理的用户管理页面修改过密码。

解决办法

在网关启动的情况下，需要通过按 RESET 键 10～11 秒后松开，将系统配置恢复到出厂状态（用户名：admin，密码：admin）；“设为默认”的配置将会被清除，恢复到最初的默认配置，但补丁将会被保留。

在网关启动的情况下,若按住 RESET 键 1s 左右后松手,网关将会重启,且不会更改任何配置。

参数规范表

参数类型	取值范围
一般 WORD 型	包含数字、字母、特殊字符（@、.、\、/、-、_、:），其他类型均为非法字符，如 username
字母数字 WORD 型	包含字母、数字，其他均为非法字符，如 modem 接口名称
首字字母一般 WORD 型	首字为字母的字母数字型：如 hostname
CODE 型	除空格以外的任意字符，如 svc-code
LINE 型	可包含空格的任意字符，如 description、password（不允许空格的 password 则为 CODE 型）
A.B.C.D 型	0.0.0.0～255.255.255.255，ABCD 为 0～255，如 IP 地址的配置
A.B.C.D 接口型	0.x.x.x、127.x.x.x、169.254.x.x、255.x.x.x、224.x.x.x、x.x.x.255、x.x.x.0 均为非法
A.B.C.D/M 型	0.0.0.0/0～255.255.255.255/32，ABCD 为 0～255，M 为 0～32，如子网配置
A.B.C.D/M 接口型	0.x.x.x、127.x.x.x、169.254.x.x、255.x.x.x、224.x.x.x。x.x.x.255，x.x.x.0 均为为非法，M 为 0 和 32 时非法，如接口 IP 地址的配置
数字范围型	如 1～512，表示该值是 1～512 中的任意数字（包含 1 和 512）
指定范围型（下拉或单选按钮）	指定字符型参数，如 vpdn 中的协议配置：pptp、l2tp

术语

I

IPSEC	Internet 协议安全性 (IPSec)是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议 (IP) 网络上进行保密而安全的通讯。

L

L2TP	L2TP（Layer 2 Tunneling Protocol）是一种工业标准的 Internet 隧道协议，功能大致和 PPTP 协议类似，比如同样可以对网络数据流进行加密。不过也有不同之处，比如 PPTP 要求网络为 IP 网络，L2TP 要求面向数据包的点对点连接；PPTP 使用单一隧道，L2TP 使用多隧道；L2TP 提供包头压缩、隧道验证，而 PPTP 不支持。
网关	为信息流或数据分组选择路由的设备。

M

Modem	调制器和解调器合在一起的总称。使数字数据能在模拟信号传输线上传输的转换接口。

R

RIP2	（RIP/RIP2/RIPng：Routing Information Protocol）作为一种内部网关协议或 IGP（内部网关协议），路由选择协议应用于 AS 系统。 RIP 主要设计来利用同类技术与大小适度的网络一起工作。因此通过速度变化不大的接线连接，RIP 比较适用于简单的校园网和区域网，但并不适用于复杂网络的情况。RIP 2 由 RIP 而来，属于 RIP 协议的补充协议，主要用于扩大 RIP 2 信息装载的有用信息的数量，同时增加其安全性能。RIP 2 是一种基于 UDP 的协议。在 RIP2 下，每台主机通过路由选择进程发送和接受来自 UDP 端口 520 的数据包。RIP 协议默认的路由更新周期是 30 秒。

W

WMMP	WMMP（Wireless M2M Protocol）协议是为实现 M2M 业务中 M2M 终端与 M2M 平台之间、M2M 终端之间、M2M 平台与应用平台之间的数据通信过程而设计的应用层协议。

缩略语

A		
ATM	Auto Table Machine	自动柜员机
C		
CDMA	Code Division Multiple Access	码分多址
D		
DDNS	Dynamic Domain Name Server	动态域名服务
DHCP	Dynamic Host Configuration Protocol	动态主机设置协议
DMZ	Demilitarized Zone	隔离区
DNS	Domain Name RUNtem	域名系统
E		
EDGE	Enhanced Data Rate for GSM Evolution	增强型数据速率 GSM 演进技术
G		
GPRS	General Packet Radio Service	通用分组无线业务
GPS	Global Positioning RUNtem	全球定位系统
GRE	Generic Routing Encapsulation	通用路由封装
GSM	Global RUNtem for Mobile Communications	全球移动通信系统
H		
HSDPA	High Speed Downlink Packet Access	高速下行分组接入
HSUPA	High Speed Uplink Packet Access	高速上行链路分组接入
I		
IP	Internet Protocol	互联网协议
ICMP	Internet Control Message Protocol	Internet 控制报文协议
L		
LAN	Local Area Network	局域网
LCP	Link Control Protocol	链路控制协议
M		
MAC	Media Access Control	媒体存取控制
N		
NR	New Radio	全球性 5G 标准
NAT	Network Address Translation	网络地址转换
O		
OSPF	Open Shortest Path First	开放式最短路径优先

P		
PPTP	Point to Point Tunneling Protocol	点对点隧道协议
S		
SIM	Subscriber Identify Module	用户标识模块
SNMP	Simple Network Management Protocol	简单网络管理协议
SOHO	Small Office Home Office	在家里办公、小型办公
T		
TCP	Transmission Control Protocol	传输控制协议
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access	时分同步码分多址
U		
UDP	User Datagram Protocol	用户自带寻址信息协议
UIM	User Identity Module	用户标识模块
V		
VPN	Virtual Private Network	虚拟专用网络
W		
WAN	Wide Area Network	广域网
WCDMA	Wideband Code Division Multiple Access	宽带码分多址
WWW	World Wide Web	环球信息网,万维网