

使用说明书

H61XX 工业智能网关



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： 深圳市龙岗区平湖街道山厦社区华宝路100号宏达大厦A座2301

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

版权所有 ©2025 深圳市宏电技术股份有限公司。保留一切权利。

本使用说明书包含的所有内容均受版权法的保护，未经深圳市宏电技术股份有限公司的书面授权，任何组织和个人不得以任何形式或手段对整个说明书和部分内容进行复制和转载。

商标声明

、DTU 是深圳市宏电技术股份有限公司的商标，本说明书中提及到的其他商标由拥有该商标的机构所有，宏电公司并无拥有其它商标的权利。

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

前言

本文档的主要功能在于帮助读者了解 H61XX 工业智能网关产品功能特点及典型应用方式、熟悉各功能及配置操作方法、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
- ☒ 现场应用工程师

如果是初次接触和使用 H61XX 工业智能网关，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 H61XX 工业智能网关，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 H61XX 工业智能网关产品的使用进行以下描述。

章节	内容
1 配置前准备	本章介绍 H61XX 工业智能网关配置前准备工作。
2 H61XX 工业智能网关配置	本章介绍 H61XX 工业智能网关功能配置操作。
3 业务场景	本章介绍 H61XX 工业智能网关几种典型应用方式。
4 FAQ/异常处理	本章介绍 H61XX 工业智能网关使用过程中常见故障原因及处理方法。

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
 注意	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。
 窍门	以本标志开始的文本能帮助解决某个问题或节省的时间。
 说明	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。

格式	意义
“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	2026-04-21	邹高俊	基于 OSDT 标准说明书修改

目录

1. 配置前准备	11
1.1. 本地连接配置	11
2. H61XX 工业智能网关配置	19
2.1. 概述	19
2.2. 登录 WEB 配置界面	20
2.3. 运行状态	20
2.3.1. 运行状态	20
2.3.2. 网关	21
2.3.3. 互联网	23
2.3.4. 下位机	26
2.4. 网络设置	29
2.4.1. 接口管理	29
2.4.2. 移动网络	33
2.4.3. WAN	39
2.4.4. WLAN 服务	41
2.4.5. VPN 服务	44
2.4.6. DHCP 服务	63
2.4.7. 智能链路	65
2.4.8. 路由设置	70
2.4.9. QoS	78
2.4.10. DDNS 设置	80
2.4.11. 负载均衡	83
2.4.12. VLAN	88
2.4.13. 双发选收	90
2.5. 安全设置	93
2.5.1. 概述	93
2.5.2. 黑白名单	93
2.5.3. NAT 设置	97
2.5.4. 端口禁用	102
2.5.5. DDOS 防御	104
2.6. 应用中心	106
2.6.1. 插件	106
2.6.2. 容器	106
2.6.3. DTU	109
2.6.4. 国密 SSL	116
2.6.5. LBS	118
2.6.6. Dedgebus 配置	120

2.6.7.	工业协议	122
2.7.	运维管理	124
2.7.1.	网络诊断	124
2.7.2.	本地日志	125
2.7.3.	远程日志	126
2.8.	系统管理	127
2.8.1.	云平台	127
2.8.2.	TR069	128
2.8.3.	SNMP	130
2.8.4.	硬件配置	131
2.8.5.	计划管理	133
2.8.6.	用户管理	135
2.8.7.	系统时间	137
2.8.8.	证书管理	138
2.8.9.	系统升级	139
2.8.10.	配置管理	140
2.8.11.	复位重启	140
2.9.	按键重启	141
3.	业务场景	142
3.1.	SDN	142
3.1.1.	SDN 功能简介	142
3.1.2.	M2M 组网应用	144
3.1.3.	平台实际配置	144
3.2.	VXLAN	149
3.2.1.	VXLAN 功能简介	149
3.2.2.	VXLAN 组网应用	150
3.2.3.	VXLAN 配置说明	151
3.3.	双发选收	152
3.3.1.	使用场景	152
3.3.2.	应用组网	153
3.4.	负载均衡	153
3.5.	链路参数备份	155
4.	FAQ/异常处理	162
4.1.	硬件类问题	162
4.1.1.	所有指示灯均不亮	162
4.1.2.	SIM 卡座连接问题	163
4.1.3.	网口连接问题	163
4.1.4.	天线连接问题	163
4.2.	拨号类问题	164

4.2.1.	拨号中断.....	164
4.2.2.	无信号显示.....	164
4.2.3.	无法找到 SIM 卡.....	165
4.2.4.	通信信号薄弱.....	165
4.3.	VPN 连接类问题.....	165
4.3.1.	VPDN 无法连接.....	165
4.3.2.	VPN 无法通信.....	166
4.3.3.	路由可通信但子网不可通信.....	166
4.4.	WEB 配置操作类问题.....	167
4.4.1.	升级固件失败.....	167
4.4.2.	恢复参数失败.....	167
4.4.3.	升级补丁失败.....	168
4.4.4.	忘记登录密码.....	168
5.	参数规范表.....	170
6.	术语.....	171
7.	缩略语.....	172

表格目录

表 2-1 运行状态参数说明.....	21
表 2-2 系统信息参数说明.....	22
表 2-3 路由信息参数说明.....	23
表 2-4 移动网络状态信息参数说明.....	24
表 2-5 SIM 卡状态信息参数说明.....	25
表 2-6 WAN 信息参数说明.....	26
表 2-7 LAN 信息参数说明.....	27
表 2-8 Wlan_0/Wlan_1 信息参数说明.....	28
表 2-9 VXLAN 信息参数说明.....	28
表 2-10 GPS 信息参数说明.....	29
表 2-11 接口管理参数说明.....	30
表 2-12 桥接口参数说明.....	31
表 2-13 “移动网络”拨号规则参数说明.....	34
表 2-14 规则管理说明	35
表 2-15 “移动网络”拨号规则参数说明.....	36
表 2-16 WAN 口连接类型参数说明.....	40
表 2-17 wlan2g/5g 参数说明.....	42
表 2-18 VPDN 规则参数说明.....	45
表 2-19 IPSec 规则第一阶段参数说明.....	51
表 2-20 IPSec 规则第二阶段参数说明.....	53
表 2-21 IPSec 规则匹配阶段参数说明.....	55
表 2-22 OpenVPN 参数说明.....	57
表 2-23 Tunnel 规则参数说明.....	60
表 2-24 VXLAN 配置参数说明.....	62
表 2-25 DHCP 服务器设置参数说明.....	64
表 2-26 链路检测规则参数说明.....	66
表 2-27 链路备份参数说明.....	68
表 2-28 路由参数说明	72
表 2-29 RIP 参数说明	74
表 2-30 RIP 参数说明 II	75
表 2-31 OSPF 参数说明.....	76
表 2-32 OSPF 参数说明 II	77
表 2-33 QoS 参数说明	79

表 2-34 DDNS 服务参数说明.....	81
表 2-35 负载均衡规则的参数说明.....	86
表 2-36 VLAN 配置参数说明.....	90
表 2-37 双发选收配置项说明.....	92
表 2-38 IP 过滤规则参数说明：	94
表 2-39 MAC 过滤规则参数说明：	95
表 2-40 域名过滤规则参数说明：	97
表 2-41 DNAT 参数说明.....	98
表 2-42 SNAT 参数说明.....	100
表 2-43 MASQ 参数说明.....	102
表 2-44 端口禁用参数说明.....	103
表 2-45 DDOS 防御参数说明.....	104
表 2-46 添加容器参数说明.....	108
表 2-47 容器操作参数说明.....	109
表 2-48 DTU 配置参数说明.....	110
表 2-49 DTU 高级设置配置说明.....	112
表 2-50 服务端参数说明.....	113
表 2-51 SM2 配置参数说明.....	117
表 2-52 SM2 配置参数说明.....	118
表 2-53 LBS 配置参数说明.....	119
表 2-54 Dedgebus 配置参数说明.....	121
表 2-55 工业协议业务配置配置参数说明.....	122
表 2-56 网络诊断参数说明.....	125
表 2-57 系统日志参数说明.....	126
表 2-58 云平台参数说明.....	128
表 2-59 TR069 配置参数说明.....	129
表 2-60 SNMP 配置参数说明.....	130
表 2-61 硬件配置参数说明.....	132
表 2-62 任务管理规则参数说明.....	133
表 2-63 用户管理参数说明.....	136
表 2-64 系统时间参数说明.....	137

插图目录

图 1-1 网络连接窗口	11
图 1-2 本地连接状态	12
图 1-3 Internet 协议 (TCP/IP)	12
图 1-4 Internet 协议 (TCP/IP) 属性窗口	13
图 1-5 高级 TCP/IP 设置.....	14
图 1-6 TCP/IP 地址.....	14
图 1-7 网络连接窗口	15
图 1-8 本地连接 2 属性.....	15
图 1-9 Internet (TCP/IP) 属性	16
图 1-10 “运行”窗口	17
图 1-11 指定 IP 方式的“IPConfig”执行结果	17
图 1-12 DHCP 自动获取 IP 方式“IPConfig”执行结果	18
图 1-13 连通性验证结果.....	18
图 2-1 用户登录身份认证界面.....	20
图 2-2 运行状态界面	20
图 2-3 系统信息界面	22
图 2-4 路由信息	23
图 2-5 移动网络状态信息页面.....	24
图 2-6 SIM 卡状态显示	25
图 2-7 WAN 状态显示	26
图 2-8 LAN 状态信息	27
图 2-9 WiFi 状态	27
图 2-10 VXLAN 状态.....	28
图 2-11 GPS 状态	29
图 2-12 接口管理页签	30
图 2-13 “桥接口”配置页签	31
图 2-14 移动网络通用配置页签.....	34
图 2-15 规则管理页签	35
图 2-16 拨号规则配置页签.....	36
图 2-17 多 DNN 配置显示.....	37
图 2-18 bridge 拨号方式显示	37
图 2-19 桥接口添加移动网络接口显示.....	38
图 2-20 5glan 配置显示.....	38

图 2-21 协议配置 ethernet 显示	39
图 2-22 锁频配置显示	39
图 2-23 WAN 页签	40
图 2-24 AP 模式配置页签	42
图 2-25 Station 模式配置页签	42
图 2-26 VPDN 配置页签	45
图 2-27 VPDN 服务配置页面	45
图 2-28 高级设置页签	49
图 2-29 L2TP 隧道状态页面	50
图 2-30 IPSec 服务配置页签	50
图 2-31 IPSec 第一阶段配置页面	51
图 2-32 IPSec 第二阶段配置页面	53
图 2-33 IPSec 匹配阶段配置页面	55
图 2-34 OpenVPN 服务配置页签	57
图 2-35 Tunnel 服务配置页面	60
图 2-36 VXLAN 页签	61
图 2-37 VXLAN 配置页面	62
图 2-38 默认桥添加 vxlan 接口	62
图 2-39 DHCP 服务页签	64
图 2-40 链路检测页面	65
图 2-41 链路检测添加页面	66
图 2-42 链路参数备份页签	68
图 2-43 链路参数备份规则添加页面	68
图 2-44 静态路由页签	71
图 2-45 添加静态路由规则页签	71
图 2-46 策略路由页签	71
图 2-47 添加策略路由规则页签	72
图 2-48 RIP 页签	74
图 2-49 RIP 配置页签	74
图 2-50 OSPF 页签	76
图 2-51 OSPF 配置页签	76
图 2-52 QoS 页签	78
图 2-53 QoS 配置页签	78
图 2-54 DDNS 页签	80
图 2-55 DDNS 设置页签	81

图 2-56 接口列表	83
图 2-57 新增接口检测规则.....	84
图 2-58 成员规则列表	84
图 2-59 新增成员规则	85
图 2-60 策略规则列表	85
图 2-61 新增策略规则	85
图 2-62 负载均衡的规则列表.....	86
图 2-63 新增负载均衡规则.....	86
图 2-64 VLAN 设置页面	89
图 2-65 新增 VLAN	89
图 2-66 选择 VLAN 绑定的 port.....	89
图 2-67 双发选收配置页面.....	91
图 2-68 黑白名单基本页面.....	93
图 2-69 IP 过滤规则添加.....	94
图 2-70 MAC 过滤规则添加	95
图 2-71 域名过滤规则添加.....	96
图 2-72 NAT 页签.....	98
图 2-73 DNAT 配置页签.....	98
图 2-74 NAT 配置页签.....	100
图 2-75 MASQ 配置页签	101
图 2-76 端口禁用界面	102
图 2-77 端口禁用参数设置页面.....	103
图 2-78 DDOS 防御配置页面.....	104
图 2-79 应用中心页签	106
图 2-80 插件安装页签	106
图 2-81 本地容器安装页签.....	107
图 2-82 仓库容器安装页签.....	107
图 2-83 容器安装页签	109
图 2-84 DTU 配置页签	110
图 2-85 DTU 高级设置页签	112
图 2-86 单中心透明方式参数配置.....	113
图 2-87 TCP 通道数据收发	114
图 2-88 DDP 服务端参数配置.....	115
图 2-89 DDP 封装通道数据收发.....	116
图 2-90 SM2 配置页签.....	117

图 2-91 DTU 中启用 SM 加密.....	117
图 2-92 SM4 配置页签.....	118
图 2-93 LBS 配置页签	119
图 2-94 Dedgebus 配置页签.....	120
图 2-95 Dedgebus 配置与云平台配置.....	121
图 2-96 工业协议业务配置页签.....	122
图 2-97 历史数据导出	123
图 2-98 配置文件导入导出.....	123
图 2-99 协议库更新	124
图 2-100 协议库删除	124
图 2-101 网络诊断配置页签.....	125
图 2-102 本地日志页签.....	126
图 2-103 远程日志页签.....	126
图 2-104 云平台配置页签.....	127
图 2-105 TR069 配置页签	129
图 2-106 SNMP 配置页签.....	130
图 2-107 硬件配置页签.....	131
图 2-108 串口参数配置页签.....	131
图 2-109 动态识别串口显示.....	133
图 2-110 计划管理配置页签.....	133
图 2-111 用户管理页签.....	135
图 2-112 用户管理配置页签.....	136
图 2-113 网络时间同步方式.....	137
图 2-114 手动方式同步时间.....	137
图 2-115 证书管理页签.....	139
图 2-116 文件升级页签.....	139
图 2-117 补丁文件操作页签.....	139
图 2-118 备份设置页签.....	140
图 2-119 出厂设置页签.....	140
图 2-120 默认设置页签.....	141
图 2-121 重启设备页签.....	141
图 3-1 接口-wan 口配置.....	153
图 3-2 接口-移动网络配置.....	154
图 3-3 成员配置	154
图 3-4 策略配置	154

图 3-5 规则配置 154

图 3-6 默认路由为 wan..... 154

图 3-7 后台 mwan3 status 查看负载均衡状态 155

图 3-8 主链路-wan 156

图 3-9 备份链路-移动网络..... 156

图 3-10 链路状态 156

图 3-11 主链路-L2TP 158

图 3-12 备份链路-移动网络..... 158

图 3-13 链路状态 158

图 3-14 主链路-移动网络+L2TP..... 160

图 3-15 备份链路-wan+PPTP..... 160

图 3-16 链路状态 160

1. 配置前准备

关于本章

章节	内容简介
本地连接配置	本节简要介绍 H61XX 工业智能网关安装后本地连接配置过程。

1.1. 本地连接配置

前提条件

- ☑ 已为 H61XX 工业智能网关供电。
- ☑ 已通过以太网网线连接网口。

H61XX 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”，在打开的窗口中双击“网络连接”。

图1-1 网络连接窗口



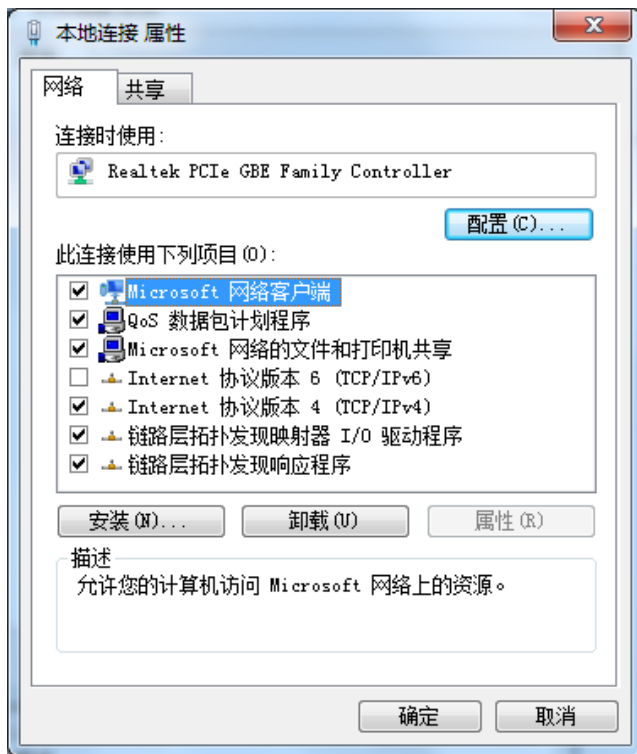
步骤 2 双击“本地连接”，打开“本地连接状态”窗口。

图1-2 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。

图1-3 Internet 协议（TCP/IP）



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

步骤 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。点击“确定”，完成配置。



注意

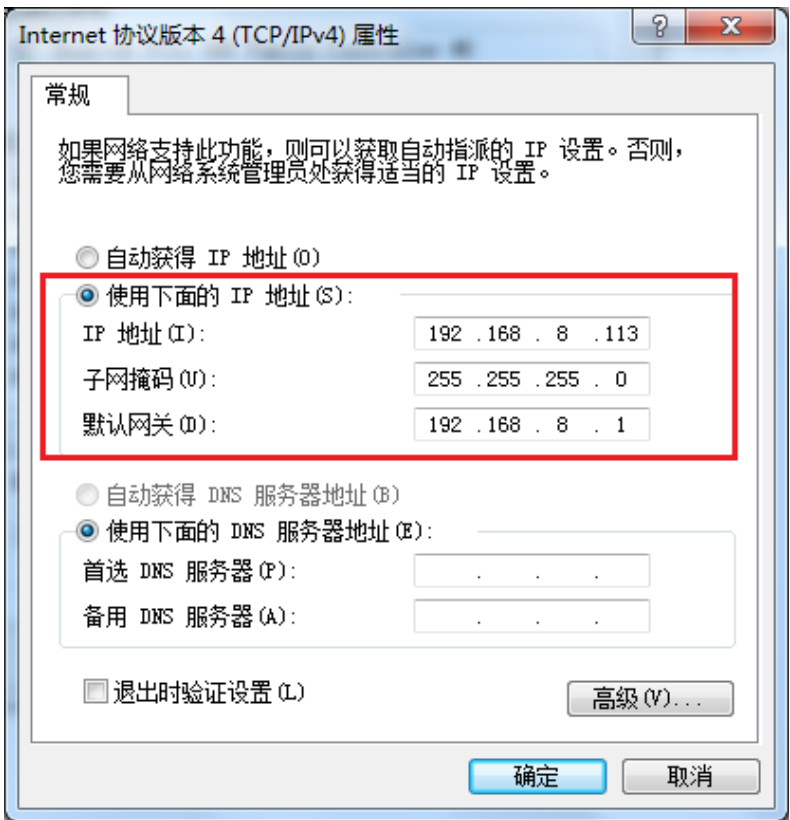
由于 H61XX 工业智能网关出厂默认参数中，

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”配置为出厂默认值。

图1-4 Internet 协议（TCP/IP）属性窗口



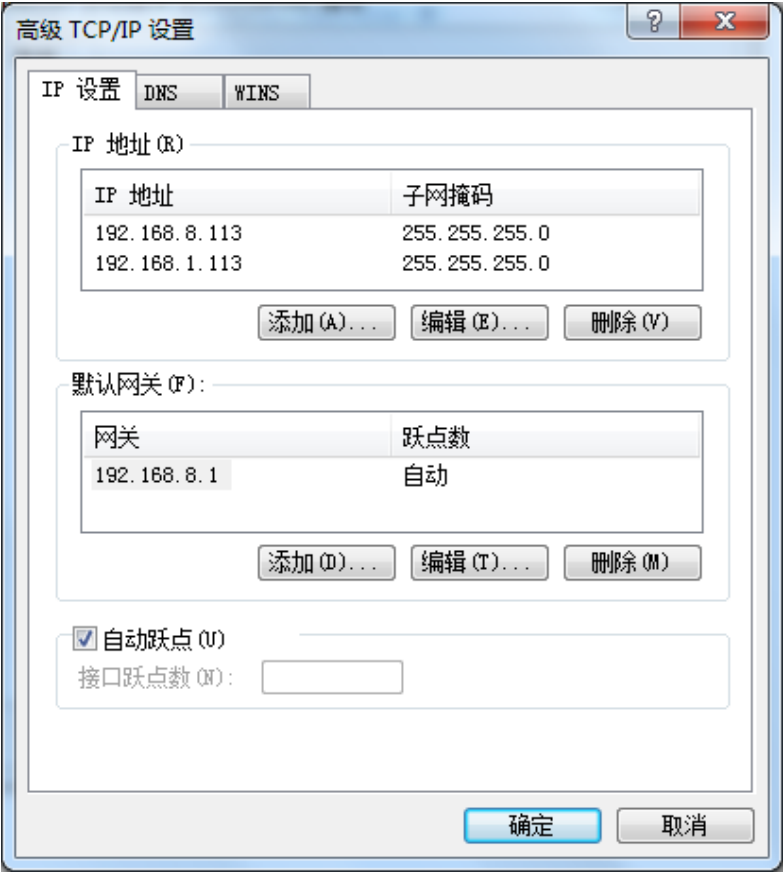
注：IP 地址可以为 192.168.8.*（其中*表示 2~254 的任意整数）。

● 高级配置

该方法即在原有网络环境配置（～）下不希望中断本地 PC 机继续局域网通信，又能对 H61XX 工业智能网关进行配置时，可考虑添加高级配置。

步骤 1 在单击“高级”，打开“高级 TCP/IP 设置”。

图1-5 高级 TCP/IP 设置



步骤 2 单击“IP 地址(R)”中的“添加”，填写需要配置的 IP 地址。

图1-6 TCP/IP 地址



步骤 3 单击右上角“添加”，完成配置。

——结束

DHCP 自动获取 IP 方式

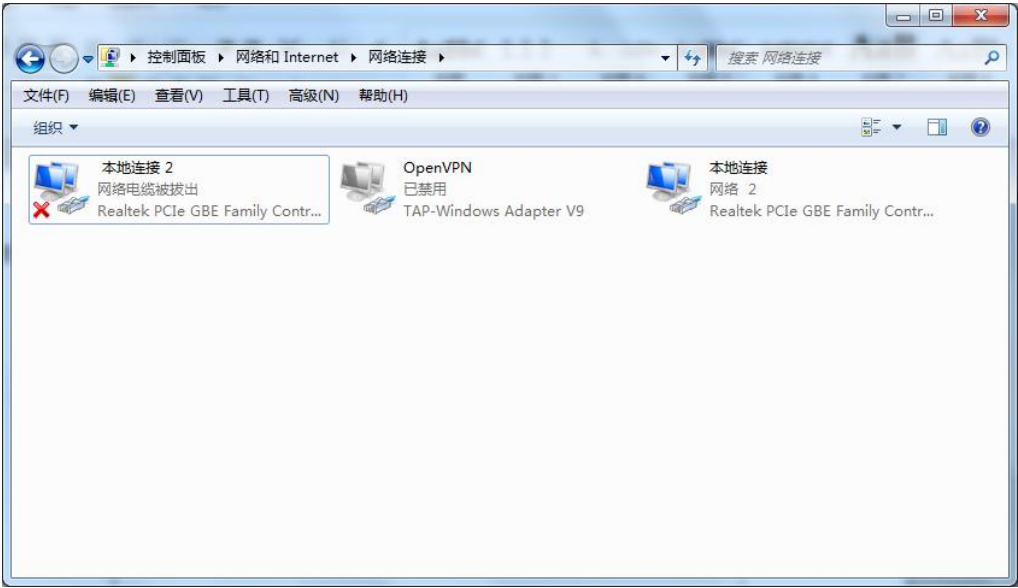
H61XX 工业智能网关内置 DHCP（Dynamic Host Configuration Protocol）服务器，自动按照预先设定的参数对连接在其上的终端(或 PC 等)分配 IP（Internet Protocol）地址。



H61XX 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。

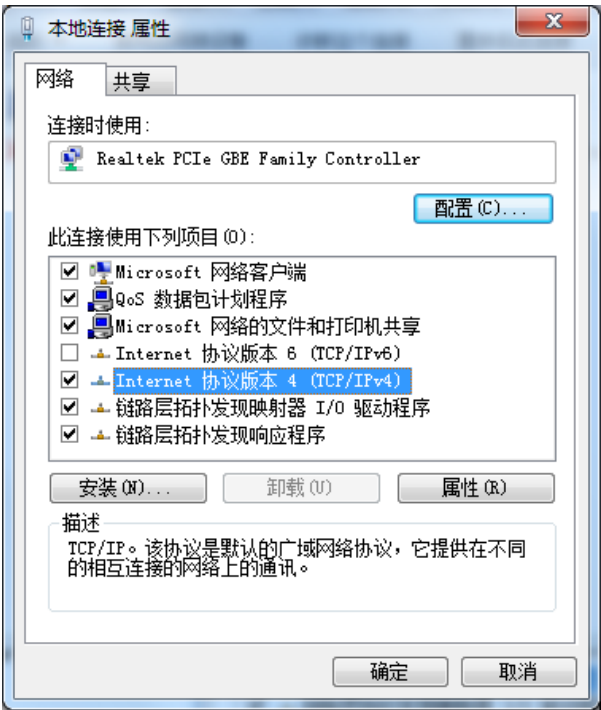
步骤 1 单击“开始>控制面板”，在打开的窗口中双击“网络连接”。

图1-7 网络连接窗口



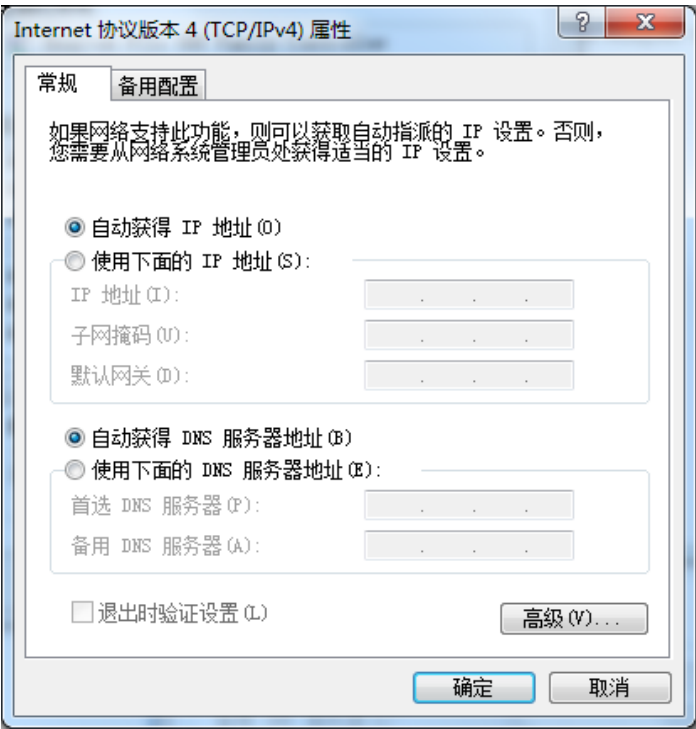
步骤 2 右键单击“本地连接 2”并在弹出的菜单中单击“属性”，打开“本地连接 2 窗口”。

图1-8 本地连接 2 属性



步骤 3 在“此连接使用下列项目 (0):”中，选择“Internet 协议 (TCP/IP)”并双击进入“Internet (TCP/IP) 属性”窗口。

图1-9 Internet（TCP/IP）属性



步骤 4 如果 Internet 协议（TCP/IP）属性，则无需改动；如果 Internet 协议（TCP/IP）属性不是所示，则在“常规”中选择“自动获得 IP 地址”。

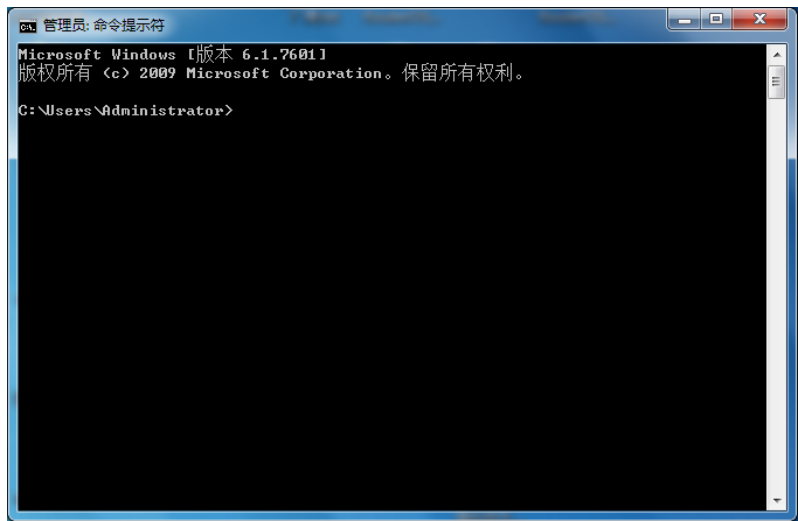
步骤 5 单击“确定”完成配置。

——结束

配置检查

步骤 1 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。

图1-10 “运行” 窗口



步骤 2 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 显示的是中的 IP 地址，；以 H61XX 工业智能网关 DHCP 自动获取 IP 的配置方法中 IP Address 显示的为“2~254”的随机数字。窗口显示信息表示 IP 配置正常。

图1-11 指定 IP 方式的“IPConfig”执行结果

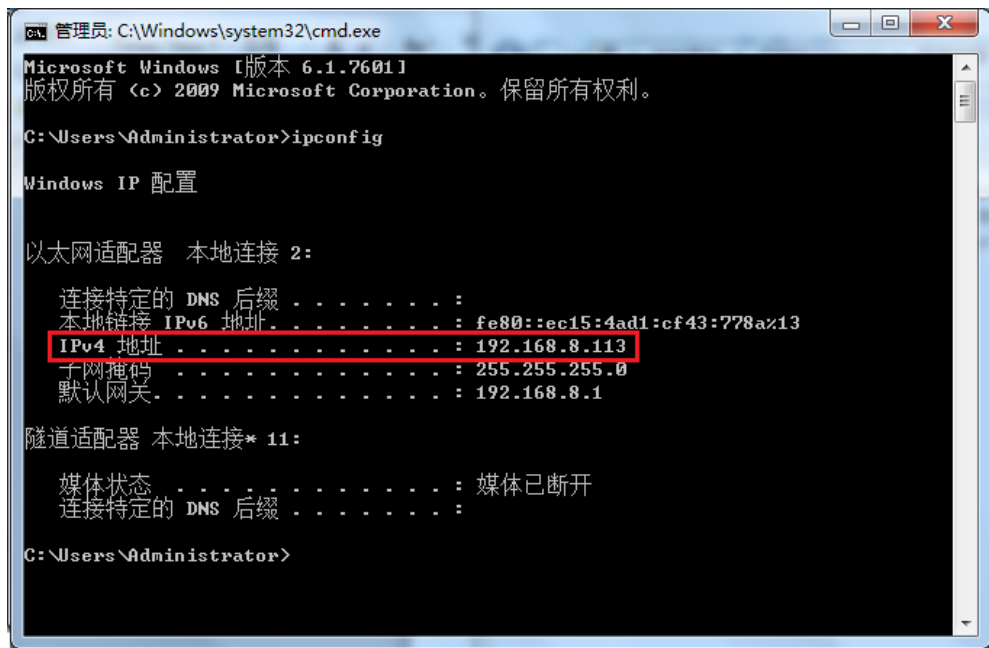
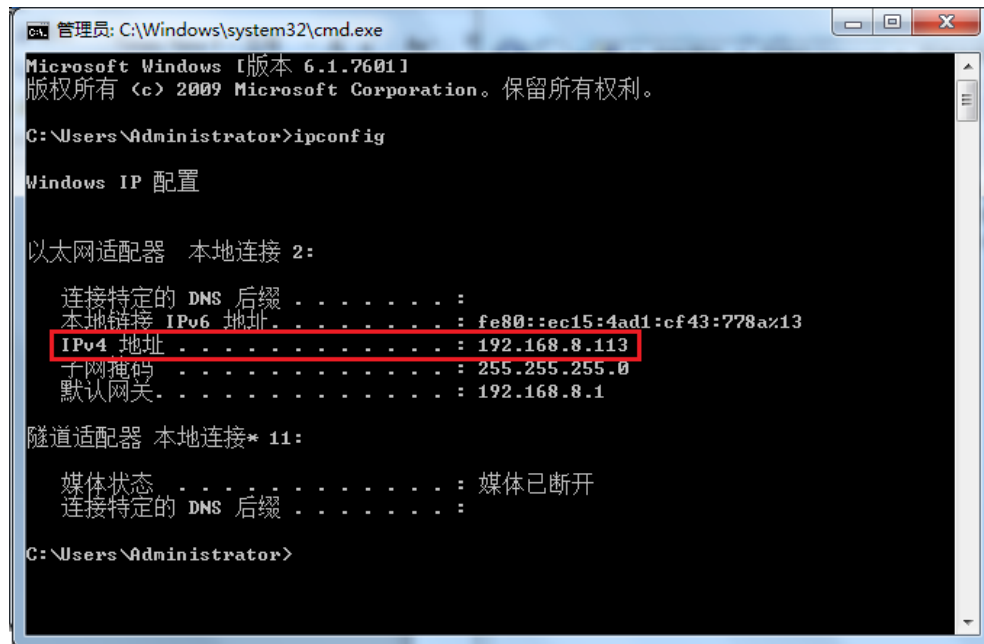


图1-12 DHCP 自动获取 IP 方式“IPConfig”执行结果

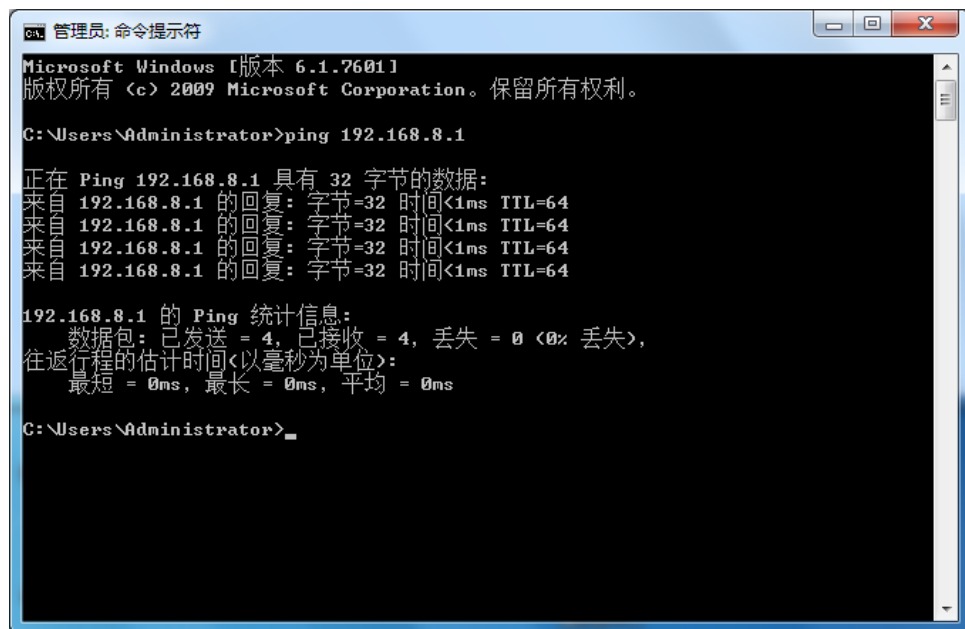


步骤 3 在命令行窗口中输入如下命令确认连通性是否正常。

```
ping 192.168.8.1
```

如果出现界面，表示本地计算机与 H61XX 工业智能网关连通性正常。

图1-13 连通性验证结果



---结束

2. H61XX 工业智能网关配置

关于本章

章节	内容简介
2.1 概述	本节简要介绍 H61XX 工业智能网关采用 WEB 方式进行配置操作。
2.2 登录 WEB 配置界面	本节简要介绍 H61XX 工业智能网关如何登陆 WEB 配置界面。
2.3 运行状态	本节简要介绍 H61XX 工业智能网关的运行状态包含哪些，以及状态查询方法。
2.4 网络设置	本节简要介绍 H61XX 工业智能网关网络设置包含哪些，以及具体配置操作方法。
2.5 安全设置	本节简要介绍 H61XX 工业智能网关安全设置包含哪些，以及具体配置操作方法。
2.6 应用中心	本节简要介绍 H61XX 工业智能网关应用设置包含哪些，以及具体配置操作方法。
2.7 运维管理	本节简要介绍 H61XX 工业智能网关运维管理配置包含哪些，以及具体配置操作方法。
2.8 系统管理	本节简要介绍 H61XX 工业智能网关系统管理配置包含哪些，以及状态查询方法。
2.9 按键重启	本节简要介绍 H61XX 工业智能网关 RST 键功能包含哪些，以及使用方法。

2.1. 概述

H61XX 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“”完成 PC 机和 H61XX 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 H61XX 工业智能网关进行配置操作。

2.2. 登录 WEB 配置界面

步骤 1 打开配置电脑 Internet Explorer 浏览器，在地址栏内输入“http://192.168.8.1/”。进入运行状态页面，修改运行状态页面配置或者进入其他页面需要用户登录，用户登录身份认证界面。

图2-1 用户登录身份认证界面



步骤 2 输入“用户名”、“密码”，单击“确定”。即可登录到 H61XX 工业智能网关的 WEB 配置界面。



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“2.8.6 用户管理”。

---结束

2.3. 运行状态

H61XX 工业智能网关提供状态信息显示。通过“运行状态”页面能快速查看 H61XX 工业智能网关的基本信息、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、移动网络在线时长、稳定运行时间、终端连接数量及详细信息、CPU/内存占用率、流量统计、移动网络状态、SIM 卡状态、各接口状态等，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。

2.3.1. 运行状态

图2-2 运行状态界面



表2-1 运行状态参数说明

参数名称	含义	如何配置
上网速率	显示设备通过移动网络上网时的上下行速率。	单位: bps, 自动刷新。
WLAN/LAN	LAN: 有终端通过设备 LAN 口接入时, 线条为绿色, 否则为灰色; WLAN: WiFi AP 模式打开, 且有终端通过 WiFi 连接此 AP 时, 线条为绿色, 否则线条为灰色。(选配 WiFi 版本才有 WLAN 功能)	请留意线条颜色, 自动刷新。
移动网络在线时长	通过移动网络上网的时长, 移动网络和移动网络 2 同时上网时, 时长根据默认路由来判断及统计。	自动刷新。 说明: 仅表示模块在线时间。
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 WLAN 连接的终端数量。	自动刷新。



说明

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。
选配带 WiFi 功能的版本才有 WLAN 模式和参数。

--结束

2.3.2. 网关

点击“运行状态”页面上方“网关”图标, 切换到 H61XX 工业智能网关状态页面, 显示 H61XX 工业智能网关的工作状态, 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、硬件版本及序列号，当前 CPU、内存占用率，以及拨号上网的流量统计。

图2-3 系统信息界面



表2-2 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	统计各接口的流量。	(1) 横坐标时间（小时：H），纵坐标流量（单位：MB）； (2) 时间为从设备上电后开始计算的时长。

路由信息

显示设备运行时的静态路由和策略路由情况。

图2-4 路由信息

系统信息

路由信息

静态路由

网络地址	子网掩码	网关	接口	度量
0.0.0.0	0.0.0.0	10.146.24.1	modem.0	0
10.146.24.0	255.255.255.0	0.0.0.0	modem.0	0
10.150.175.0	255.255.255.0	0.0.0.0	modem.1	0
172.17.0.0	255.255.0.0	0.0.0.0	docker0	0
192.168.8.0	255.255.255.0	0.0.0.0	lan	0
:::0	-	fe80::211:9ff:fe64:101	modem.0	1
:::0	-	fe80::211:9ff:fe64:101	modem.0	1024

策略路由

协议	源信息	目的信息	动作
协议	路由表ID	目的地址	网关
			接口

表2-3 路由信息参数说明

参数名称	含义	如何配置
网络地址	H61XX 工业智能网关接口当前获取的 IP 地址或配置的默认 IP 地址	不可配
子网掩码	H61XX 工业智能网关可达的 IP 网络，与目的地址一起使用	不可配
网关	H61XX 工业智能网关要到达目的 IP 的网关	不可配
接口	H61XX 工业智能网关到网关经过的接口	不可配
度量	H61XX 工业智能网关到达该地址的度量值，直连时度量值为 0。	不可配

2.3.3. 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，包含移动网络状态、SIM 状态、WAN 状态。

移动网络状态

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、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”。

图2-5 移动网络状态信息页面



表2-4 移动网络状态信息参数说明

参数名称	含义	如何配置
联网状态	当前移动网络拨号的网络连接状态。	不可配
网络类型	当前拨号成功的网络对应的网络类型。	点击“修改配置”进入配置页面进行配置
在线时间	显示拨号上线后的在线时长。	不可配
信号强度	无线网络的信号强度。 取值范围：1~31 信号值 0~10：信号较弱 信号值 11~20：信号一般 信号值 21~30：信号较强 若没有信号，则无法成功拨号。	不可配
域名服务器	拨号时获取的首选 DNS 地址。	不可配
接口 IP 地址	拨号时获取的外网 IP 地址。	不可配

参数名称	含义	如何配置
接口网关地址	拨号时获取的外网 IP 地址的网关地址。	不可配
模块 IMEI 号	模块的唯一设备识别码。	不可配
运营商	当前拨号的运营商。	不可配
Cell 信息	显示当前附上网的主小区信息	不可配
NeighborCell 信息	显示当前邻区信息	不可配



说明

邻区信息显示当前仅部分模组支持，如展锐（RG200U/RM500U）、高通（RM500Q/RM520）、Redcap（MT5700/MT5711/MT5710）。

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。

图2-6 SIM 卡状态显示

移动网络状态

SIM 状态

WAN 状态

状态

Ready

位置

sim 2

ICCID

89860119801508239308

IMSI

460014336651797

表2-5 SIM 卡状态信息参数说明

参数名称	含义	如何配置
状态	设备当前使用的卡槽对应的 SIM 卡的工作状态。	不可配
位置	当前 SIM 插入的卡槽位置。	不可配
ICCID	当前生效的 SIM 卡卡号。	不可配
IMSI	拨号所在基站中对应的 SIM 卡的识别码。	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 地址；

点击“修改配置”，可跳转到“网络设置”>“WAN”。

图2-7 WAN 状态显示



表2-6 WAN 信息参数说明

参数名称	含义	如何配置
名称	当前 WAN 类型接口的名称	不可配
连接类型	显示当前 WAN 接口的类型，有 static、pppoe、dhcp 三种类型。	点击“修改配置”进入配置页面进行配置
IP 地址	显示 WAN 口配置的本地 IP 地址。	点击“修改配置”进入配置页面进行配置
子网掩码	显示配置的 WAN 接口所在的网络地址号。	不可配
MAC	显示网口卡物理地址，此地址一般情况下固定且唯一。	不可配

2.3.4. 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。显示当前接入路由设备的下位机状态信息，包含 LAN 状态、wlan_0 状态、wlan_1 状态。

LAN 状态

显示 LAN 口状态及通过 LAN 接入的下位机信息，包含名称、IP 地址、子网掩码、MAC 地址，终端的 IPv4 地址、MAC 地址。

点击“修改配置”，可跳转到“网络设置”>“接口管理”设置“桥接口”下 LAN IP。

图2-8 LAN 状态信息



表2-7 LAN 信息参数说明

参数名称	含义	如何配置
名称	显示当前 LAN 接口所在桥的名称。	不可配
IP 地址	显示 LAN 口配置的本地 IP 地址。	点击“修改配置”进入配置页面进行配置
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

wlan_0/wlan_1 状态

显示 wlan_0 和 wlan_1 的状态及通过 WLAN 接入的下位机信息，包含连接状态、工作模式、SSID、IP 地址、工作通道、带宽。

点击“修改配置”，可跳转到“网络设置”>“WLAN 服务”。

图2-9 WiFi 状态



表2-8 Wlan_0/Wlan_1 信息参数说明

参数名称	含义	如何配置
连接状态	显示当前 WLAN 接口的连接状态。	不可配
工作模式	WLAN 的工作模式。	点击“修改配置”进入配置页面进行配置
SSID	AP 端身份标识。	点击“修改配置”进入配置页面进行配置
IP 地址	显示 WLAN 的 IP 地址。	不可配
工作通道	WLAN 工作通道。	点击“修改配置”进入配置页面进行配置
带宽	设备当前配置的 WLAN 带宽。	点击“修改配置”进入配置页面进行配置



说明

Wlan 应用需要选配支持 WiFi 2.4g 和 5.8g 功能版本，无 WiFi 功能就没有 wlan 选项。

VXLAN 状态

显示 VXLAN 接口的状态，包含 VXLAN 接口名、MAC 地址、接收数据、发送数据和 VXLAN 状态。

图2-10 VXLAN 状态

LAN 状态 WLAN 状态 WLAN2 状态 VXLAN 状态 GPS 状态				
接口信息				
VXLAN接口名	MAC	接收	发送	VXLAN状态
vxlan123	6A:75:3C:3D:DB:A7	0 B	648 B	Up

表2-9 VXLAN 信息参数说明

参数名称	含义	如何配置
VXLAN 接口名	显示当前 VXLAN 接口的名称	不可配
MAC	VXLAN 接口的 MAC 地址	不可配
接收	VXLAN 接口的接收流量	不可配
发送	VXLAN 接口的发送流量	不可配

参数名称	含义	如何配置
VXLAN 状态	VXLAN 接口的状态	不可配

GPS 状态

显示 GPS 的状态，包含 GPS 状态、经度、纬度、地面速度、地面航向和日期时间。

图2-11 GPS 状态



表2-10 GPS 信息参数说明

参数名称	含义	如何配置
状态	显示当前 GPS 的状态	不可配
经度	显示当前定位的经度坐标	不可配
纬度	显示当前定位的纬度坐标	不可配
地面速度	显示当前地面速度	不可配
地面航向	显示当前地面航向	不可配
日期时间	显示当前日期和时间	不可配



GPS 状态需要开启 LBS 功能才会显示，无定位芯片则无此状态。

2.4. 网络设置

网络设置主要完成物理接口及桥接口管理、WLAN、VPN、DHCP、智能链路、路由设置、安全设置、QoS、DDNS 等配置。配置完成后可满足基本网络通信需要。

2.4.1. 接口管理

接口管理部分包含对所有的物理接口和桥接口的配置查询管理，如 WAN 接口的管理和 LAN 口桥接管理。

桥接口的作用是将多个物理接口连接起来形成网桥互相通信。默认的桥接口可以删除，新增加的桥接口可以删除。

- 步骤 1 登录 H61XX 工业智能网关的 WEB 配置界面。
登录方法请参见“2.2 登录 WEB 配置界面”。
- 步骤 2 单击“网络设置>接口管理”。
打开“接口管理”页签。

图2-12 接口管理页签



- 步骤 3 配置接口管理参数，参数说明。

表2-11 接口管理参数说明

参数名称	含义	如何配置
名称	接口的名称。	不可配
模式	接口的业务模式。	WAN 支持配置 LAN 和 WAN 两种模式
协议	接口所采用的协议类型，如 WAN 支持 Static、DHCP 和 PPPoE 三种类型。	可进入对应接口的配置页面进行更改。
信息	接口 IP。	“移动网络”的信息为当前拨号 IP，不可配；“WAN”、“WLAN”和“LAN”为配置的物理接口的 IP。
操作	对接口进行使能、编辑操作。	默认接口均使能。 单击“编辑”按钮可进入对应接口的配置页面。

- 步骤 4 点击“桥接口”右上角“添加”或某一桥接口右侧的“编辑”，进入桥接口配置界面，桥接口配置参数说明。

图2-13 “桥接口”配置页签

网络设置

lan

模式

LAN

协议

Static

桥接口

lan2 wlan

IPv4 地址

192.168.8.1/24

-

+ * 如: 192.168.8.1/24

最大传输单元

ipv4:68-1500 ipv6:1280-1500 字节

DNS

+

IPv6 地址

如: 2001:D0B0:3000:3001::1/64

DHCP服务

DHCPV6

禁用

☐ 关闭此接口 DHCP (IPv4&IPv6) 功能

起始地址

192.168.8.

100

* 网络地址的起始分配基址

客户端数

150

* 最大地址分配数量

租期

43200

* 120-86400秒

表2-12 桥接口参数说明

参数名称	含义	如何配置
名称	桥接口的名称，便于区分多个桥接口，默认有一个桥接口 lan。	右上角“添加”按钮新增桥接口时可编辑，默认桥接口 lan 的名称不可编辑。
协议	桥接口所采用的协议类型。	下拉框选项 • static 目前仅支持 static 静态 IP。
桥接口	网桥内包含的物理接口，默认桥接口 bridge0 内包含接口 lan2、移动网络、wlan_0 和 wlan_1。	单击“编辑”进入桥接口的配置页面进行下拉框选项，多项选择。 下拉框选项 ☒ lan2 ☒ 移动网络 ☒ Wlan_0 ☒ Wlan_1 说明：接口 wlan_0、wlan_1 仅对应的 WiFi 版本才有

参数名称	含义	如何配置
IPv4 地址	桥接口所在网段，可以添加或者删除，由于默认跟 LAN 进行桥接，因此 IPv4 地址为 LAN 口 IP 地址。	单击“编辑”进入桥接口的配置页面进行 IPv4 地址的手动输入，最多可支持 4 个网段划分。 格式：A.B.C.D/M 接口型，输入规范请参见“5. 参数规范表” IP1 默认值：192.168.8.1/24， IP2~4 按上述格式输入，各个网段不能配置同一子网。
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：46~1500 单位：byte
DNS	如果需要访问域名则需要自定义配置 DNS，最多可配置两个。	接口型 A.B.C.D 例如：8.8.8.8
“DHCP 服务”启用时显示		
起始地址	DHCP 服务 IP 地址池的起始 IP 地址。	接口型 A.B.C.D, 输入规范请参见“5. 参数规范表”。 例如：192.168.8.2
客户数	DHCP 服务最大地址分配数量。	手动输入 取值范围：1~155
租期	DHCP 客户端获取 IP 后对 IP 的租用时间，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
“DHCPV6”		
路由通告	用于定义 DHCPv6 服务器路由通告的工作方式	下拉列表 ☒ “禁用” ☐ “服务器模式” 默认是禁用

参数名称	含义	如何配置
DHCPV6 服务	用于定义 DHCPv6 服务器的工作方式	下拉列表 ☒ “禁用” ☐ “服务器模式” 默认是禁用
DHCPV6 模式	DHCPV6 地址的分配方式 无状态：设备通过 SLAAC 自动生成，不依赖 DHCPv6 服务器 有状态：完全由 DHCPv6 服务器分配	下拉列表 ☐ “无状态” ☐ “有状态” ☒ “无状态+有状态” 默认是无状态+有状态
强制通告默认路由	确保客户端设备自动将本路由器设置为 IPv6 流量的默认网关	复选框，默认不勾选
DNS	DHCP client 获取到的 DNS	手动输入 比如：2003::1, 这时 DHCP client 获取到的 dns 是 2003::1

步骤 5 点击右上角“保存”，完成桥接口的配置。



说明

用户在修改 IPv4 地址的第一个 IP 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 IPv4 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该 IP 地址。
WiFi 和硬件有关系，系统会自动获取具体的 WIFI 接口，在页面会动态更新。

---结束

2.4.2. 移动网络

移动网络是 H61XX 工业智能网关最核心功能之一，H61XX 工业智能网关支持单模单卡拨号，单模双卡自动切卡，双模双卡拨号，为用户提供高速无线宽带上网功能。

2.4.2.1. 通用配置

步骤 1 登录 H61XX 工业智能网关的 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“网络设置>移动网络”，可看到通用配置。

图2-14 移动网络通用配置页签



表2-13 “移动网络” 拨号规则参数说明

参数名称	含义	如何配置
网络类型	强制下发的网络制式。	下拉框选择 Auto 5G 4G
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“5. 参数规范表”。
网络频段	5G 锁频段配置。	下拉框选项（按照具体要锁的频段进行选择）
SA 开关	启用则支持拨号 SA、禁用则拨号 NSA	下拉框选择 启用 禁用
SIM 卡（单模双卡模式下才有的配置项）	单模双卡模式下配置选项，用于指定拨号时选择 SIM 卡；选定 AUTO 为自动切换 SIM 卡拨号	单选框选择 ☒ SIM1 ☒ SIM2 ☒ AUTO

步骤 3 点击“上图界面”中的移动网络接口的“编辑”按钮，可支持对“拨号规则”进行“添加”、“编辑”、“删除”操作。

图2-15 规则管理页签

规则管理

接口名称

移动网络-0

拨号方式

dhcp

MTU

范围: 128~15360

子网掩码

如: 255.255.255.0

使用通告DNS

☒

添加拨号规则

规则名称

网络接入点

用户名

操作

表2-14 规则管理说明

参数名称	含义	如何配置
接口名称	显示对应的接口名称,可用于区分多DNN的接口。	不可配
拨号方式	定义不同的拨号方式进行拨号,其中选择 5g-lan 时需要选择协议类型为 ethernet。	下拉框选择 DHCP Bridge 5g-lan
MTU	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: 128~15360 单位: byte
子网掩码	可用于修改通过Modem接口获取的 IP 地址的子网掩码	标准掩码地址, 如: 255.255.255.0
使用通告 DNS	使用服务器端下发的 DNS 服务器。	手动勾选。 默认勾选。

步骤 4 点击添加拨号规则，可看到规则相关配置，拨号规则参数说明。点击“保存”，完成对“移动网络拨号规则”的参数配置

图2-16 拨号规则配置页签

||| 拨号规则

↶

🏠

规则名称

* 最大长度为64位

协议类型

IPv4

▼

网络接入点

最大长度为64位

切片信息

▼

最大长度为64位

用户名

最大长度为64位

密码

最大长度为64位

鉴权类型

none

▼

表2-15 “移动网络” 拨号规则参数说明

参数名称	含义	如何配置
点击“添加拨号规则”按钮或拨号规则右侧“编辑”按钮，对拨号规则进行编辑		
规则名称	拨号规则的唯一标识名，用于其他功能调用或者关联本规则时使用，如配置该规则的路由、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。
协议类型	当前规则拨号获取的 IP 所属协议类型，如 IPv4、IPv6、Ethernet。	下拉框选项 ☒ IPv4 ☒ IPv6 ☒ IPv4&IPv6 ☒ Ethernet
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。	WORD 类型，最大 64 字节，输入规范请参见“5. 参数规范表”。
切片信息	5G 网络中，Modem 处理和管理网络切片相关数据的能力。这些信息包括用户路由选择策略（URSP）、网络切片选择辅助信息（NSSAI）等，用于确保终端设备能够连接到适当的网络切片，以满足特定业务需求	下拉框选项（根据具体环境扫描到的切片信息选择）
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。	WORD 类型/CODE 类型，各最大长度 64 字节，同时存在或同时为空。
鉴权类型	选择拨号时所采用的鉴权方式、认证协议类型。	下拉框选项 ☒ chap+pap ☒ chap ☒ pap ☒ none

● 编辑

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。

- 删除

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

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。

2.4.2.2. 多 DNN

步骤 1 点击移动网络接口的“+”按钮，可以添加新的 modem 接口，不支持多 DNN 的模块无法添加，同时根据不同的模块可支持配置多路 DNN，最大支持 4 路 DNN。

图2-17 多 DNN 配置显示



接口名称	使用通告DNS	规则数	操作
移动网络-0	启用	0	 
移动网络-1	启用	0	  

步骤 2 编辑不同的 modem 接口，可以单独配置对应的拨号规则，APN、用户名和密码。

2.4.2.3. Bridge 拨号

步骤 1 进入移动网络页面，点击移动网络接口的编辑按钮，选择拨号方式为 Bridge，点击保存。

图2-18 bridge 拨号方式显示



接口名称	移动网络-0
拨号方式	bridge
MTU	范围:128~15360
子网掩码	如: 255.255.255.0
使用通告DNS	☒

[添加拨号规则](#)

规则名称	网络接入点	用户名	操作
default			  

步骤 2 进入网络设置--接口管理页面，选择桥接口，勾选移动网络接口-0，同时禁用 DHCP 功能，即勾选关闭此接口 DHCP（IPv4&IPv6）功能，如。此时下位机自动获取 IP 可获取 Modem 接口的 IP 地址。

图2-19 桥接口添加移动网络接口显示

网络设置

lan

模式

LAN

协议

Static

桥接口

lan2 移动网络-0

IPv4 地址

192.168.8.1/24

+

如: 192.168.8.1/24

最大传输单元

ipv4:68-1500 ipv6:1280-1500 字节

DNS

+

IPv6 地址

如: 2001:D0B0:3000:3001::1/64

DHCP服务

DHCPV6

禁用

☒ 关闭此接口 DHCP (IPv4&IPv6) 功能

服务IP或域名

中继接口

2.4.2.4. 5GLAN 拨号

步骤 1 进入移动网络页面，点击移动网络接口的编辑按钮，选择拨号方式为 5glan，点击保存。

图2-20 5glan 配置显示

规则管理

接口名称

移动网络-0

拨号方式

5glan

VLANID

请选择

MTU

范围:128~15360

子网掩码

如: 255.255.255.0

使用通告DNS

☒

添加拨号规则

规则名称

网络接入点

用户名

操作

default

步骤 2 若需要结合 VLAN 划分，则需要 在 VLAN 页面配置对应 LAN 口的 VLAN ID，详细配置见：配置完成后，VLANID 下拉框会显示当前已配置的 VLAN ID，根据需求选择即可。相同 VLAN 的下位机才可互通。

步骤 3 编辑 default 规则名称，选择协议为 ethernet。

图2-21 协议配置 ethernet 显示

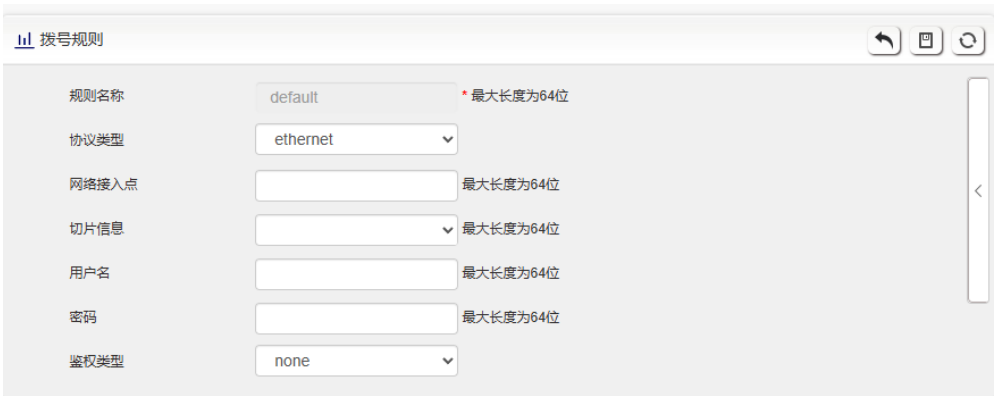


图2-21展示了“拨号规则”配置界面。该界面包含以下配置项：

配置项	当前值	备注
规则名称	default	* 最大长度为64位
协议类型	ethernet	
网络接入点		最大长度为64位
切片信息		最大长度为64位
用户名		最大长度为64位
密码		最大长度为64位
鉴权类型	none	

步骤 4 需在桥接口添加移动网络接口，同时禁用 LAN 口 DHCP 服务，具体步骤同 2.4.2.3 的步骤 2

2.4.2.5. 小区锁定

步骤 1 进入移动网络页面，选择网络类型为 5G，并选择具体的网络频段，可配置 PCID 和频点的对应关系。

图2-22 锁频配置显示



图2-22展示了“通用配置”界面。该界面包含以下配置项：

配置项	当前值	备注
网络类型	5G	
PIN		最大长度为31位
网络频段	78	
PCID		0-1007,多组配置时以分隔，并与频点一一对应
频点		0-4294967295,多组配置时以分隔，并与PCID一一对应
SCS	30	
SA开关	☒ 启用 ☐ 禁用	
SIM卡	☒ SIM1 ☐ SIM2 ☐ AUTO	

步骤 2 若要配置多小区，需要以“,”分隔，并且 PCID 与频点需要一一对应

 说明

当按钮显示为“启用”时，表示对应动作已经处于生效状态。如单击“启用”后，“启用”按钮变成灰色，表示目前该功能或者参数处于禁用状态。

---结束

2.4.3. WAN

WAN 主要用于通过以太网连接 Internet，连接方式有静态 IP、DHCP、PPPoE、DHCPv6、DHCPv4v6 三种方式。

步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“网络设置>接口管理”。

步骤 3 点击“WAN”右侧“编辑”按钮，
打开“WAN”页签。

图2-23 WAN 页签

步骤 4 配置 WAN 口连接类型。
参数说明。

表2-16 WAN 口连接类型参数说明

参数名称	含义	如何配置
协议	广域网的连接协议类型。	下拉框选项，包含： ☒ static：手动配置接口 IP。 ☒ dhcp：dhcp 客户端自动获取 IPV4-IP 方式。 ☒ dhcpv6：dhcp 客户端自动获取 IPV6-IP 方式。 ☒ dhcpv4v6：dhcp 客户端自动获取 IPV4 和 IPV6-IP 方式。 ☒ 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“路由设置”中补充静态路由接口、网络地址、子网掩码等配置，并在“安全设置”中补充“NAT 规则”配置。
“协议”选择“static”时显示		
IPv4 地址	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“5. 参数规范表” 例如：192.168.10.1/24
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	取值范围：ipv4:68-1500 ipv6:1280-1500 字节 单位：byte

参数名称	含义	如何配置
	输要求时配置，通常金融数据交互有此要求的较多。	
DNS	如果需要访问域名则需要自定义配置 DNS，最多可配置两个。	接口型 A.B.C.D 例如：8.8.8.8
“协议”选择“pppoe”时显示		
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“5. 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“5. 参数规范表”。
使用通告 DNS	使用服务器端下发的 DNS 服务器。“协议”选择“pppoe”、“dhcp”、“dhcpv6”、“dhcpv4v6”时均需选择	手动勾选。 默认勾选。
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 Web 中的相关说明。	单击“显示”即可显示高级设置参数。

步骤 5 点击“保存”，完成 WAN 口连接类型配置。

---结束

2.4.4. WLAN 服务

H61XX 工业智能网关 WiFi 版本支持 wlan，且提供 AP、Station 两种功能模式。通过 AP 功能，H61XX 工业智能网关可以提供无线局域网热点；通过 Station 客户端功能，可以让 H61XX 工业智能网关接入其他的 AP 设备，这样 H61XX 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 H61XX 工业智能网关的 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“网络设置>WLAN 服务”。

打开“wlan”页签，当选择不同 WLAN 工作模式（AP、Station）时，会进入不同页签。当 WLAN 工作模式选择 Station 时，需要扫描周围 AP，以选择一个 AP 接入。

图2-24 AP 模式配置页签

< 网络设置 >

WLAN服务

wlan

无线特性

802.11AX Wi-Fi6

工作频段

2.4G

国家码

CN

工作通道

1

带宽

20/40MHz

工作模式

AP

桥接口

lan

SSID

Hongdian_test24

* 最大长度为32位

广播状态

启用

禁用

认证方式

wpa2-psk

加密算法

ccmp(aes)

无线密码

* 长度为8到63位

高级设置

图2-25 Station 模式配置页签

WLAN服务

wlan

wlan2

工作模式

Station

SSID

* 最大长度为32位

连接类型

DHCP

BSSID

认证方式

none

步骤 3 配置“WLAN”相关参数。
参数说明。

表2-17 wlan2g/5g 参数说明

参数名称	含义	如何配置
工作模式	WLAN 工作模式, 支持 AP/Station 模式。	下拉框选项 ☒ AP ☒ Station 默认值: AP
“工作模式” 选择 AP 时		
桥接口	选择当前 WiFi 是否桥接到某一接口。	下拉框选项。
SSID	WLAN 服务端身份标识。AP 模式时为当前服务端的名称 ID;	☒ 字母数字 WORD 项, 输入规范请参见“5. 参数规范表”。

参数名称	含义	如何配置
	Station 模式时为所接入的 AP 设备的名称 ID。	
认证方式	配置 WLAN 的加密方式，当不需要加密验证时可以 none。	下拉框选项 ☒ none ☐ wpa-psk ☐ wpa2-psk ☐ wpa3-sae ☐ wpa2-psk/wpa3-sae 默认值: none
无线密码	WLAN 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“5. 参数规范表”。
高级设置：当“工作模式”选择“AP”时显示		
国家码	国家码设置，不同的国家码对应的信道不一样	下拉框选项 支 持 AE/BH/BR/CA/CN/DE/ES/FR/G B/HK/ID/IT/JP/KW/SA/SE/SG /TH/TR/TW/US/ZA 默认值 CN
工作通道	WLAN 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 ☒ auto ☒ 1~13 (wlan_0 时可选) auto 表示信道自适应，无干扰时默认使用信道 6，当相同信道干扰则自动跳转到干扰较小的信道工作。
功率	用于配置 WLAN 的发射功率。	下拉框选项 ☐ 弱 ☐ 中 ☒ 强 默认值强
带宽	WLAN 工作在 802.11n 模式下的带宽配置。	下拉框选项 ☒ 20MHz ☐ 40MHz 40MHz 表示 802.11n 的高速模式
广播状态	用于配置 WLAN SSID 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 WLAN 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	单选按钮选择 ☒ 启用 ☐ 禁用 默认启用。

参数名称	含义	如何配置
	SSID。	
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 默认启用。
加密算法	加密采用算法	下拉框选项 ☒ ccmp(aes) ☒ tkip ccmp(aes)
“工作模式”选择 Station 时		
连接类型	当 H61XX 工业智能网关做 Station 连接到 AP 时，与 AP 通信的 IP 地址获取方式。	下拉框选项 ☐ 静态 IP ☒ DHCP 默认值 DHCP
BSSID	选择的 AP 的 MAC 地址。	WORD 型 MAC 地址格式： XX:XX:XX:XX:XX:XX；根据选择的 AP 自动填写，也可手动输入。



说明

WLAN 根据支持的芯片不一样，页面上也会存在一点差异性。

---结束

2.4.5. VPN 服务

2.4.5.1. 概述

VPN (Virtual Private Network) 即虚拟专用网，是基于 Internet 的一种安全局域网，H61XX 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。

2.4.5.2. VPDN 服务

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 H61XX 工业智能网关的 WEB 配置界面。
- 登录方法请参见“2.2 登录 WEB 配置界面”。

- 步骤 2 单击“网络设置>VPN 服务>VPDN 服务”。
- 打开“VPDN 服务”页签。

图2-26 VPDN 配置页签



- 步骤 3 单击右上角“添加”，添加一条新 VPDN 规则。

图2-27 VPDN 服务配置页面



- 步骤 4 配置 VPDN 规则参数。
- 参数说明。

表2-18 VPDN 规则参数说明

参数名称	含义	如何配置
启用/禁用	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		
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。

参数名称	含义	如何配置
协议	VPDN 采用的协议，包括：l2tp、pptp。	下拉框选项 ☒ l2tp ☒ pptp 根据实际情况设置，设置后点击“编辑”进行修改。
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名。	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。
通道密钥	当前链路的通道密钥。“协议”选择“l2tp”时填写。	输入与服务器配置一样的通道密钥。
使用通告 DNS	使用服务器端下发的 DNS 服务器。	手动勾选 默认勾选
高级配置	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，配置。	单击后展开。
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。

参数名称	含义	如何配置
MS-CHAP	MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol) 也是一种加密验证机制, 使用基于 MPPE 数据加密。	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。
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		

参数名称	含义	如何配置
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。	单选框选择 ☒ 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“5. 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“5. 参数规范表”。 例如：10.10.10.254

参数名称	含义	如何配置
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“5. 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2-28 高级设置页签

认证 & 加密

CHAPPAPMS-CHAPMS2-CHAPEAP

其它

调试对端DNS

压缩 & 控制协议

压缩控制协议地址/控制压缩协议域压缩

VJ TCP/IP 头部压缩连接ID压缩

专家选项

nomppemppe requiredmppe statelessnodeflate

nobsdcompdefault-asyncmap

LCP间隔时间30

LCP重试次数51-512

最大传输单元128-16384 字节

最大接收单元128-16384 字节

本地IP如: 192.168.8.1

远端IP如: 192.168.8.254

步骤 5 点击“保存”，完成该条 VPDN 规则配置。

在完成一条 VPDN 规则配置后，H61XX 工业智能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，H61XX 工业智能网关将会自动添加到对端子网的 H61XX 工业智能网关，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。

图2-29 L2TP 隧道状态页面

VPN设置	
接口名称	1
状态	connected
协议	l2tp
本地IP	192.168.120.50
远端IP	192.168.120.1

---结束

2.4.5.3. IPSec 服务

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。H61XX 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 H61XX 工业智能网关也支持通过其他接口拉起 IPSec（如通过移动网络拉起），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 H61XX 工业智能网关 WEB 配置界面。
登录方法请参见“2.2 登录 WEB 配置界面”。
- 步骤 2 单击“网络设置>VPN 服务>IPSec 服务”。
- 打开“IPSec 服务”页签。

图2-30 IPSec 服务配置页签

< 网络设置 >				
VPN服务 Tunnel服务 IPSec服务 OpenVPN服务				
Phase1				
策略名称	加密方式	哈希算法	认证方式	操作
Phase2				
策略名称	加密方式	哈希算法	远端子网	操作
IPSec接口				
接口名称	加密接口	服务地址	操作	

- 步骤 3 单击右上角“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。

图2-31 IPSec 第一阶段配置页面

IPSec服务

策略名称

* 最大长度为12位

协商模式

main

加密方式

des

哈希算法

md5

认证方式

psk

预共享密钥

* 最大长度为24位

IKE

ikev1

本端标识

最大长度为64位

对端标识

最大长度为64位

IKE生存时间

* 120-86400 秒

DH组

group768

检测间隔

1-512 秒

重试次数

1-512 次

IPSec 规则第一阶段参数说明。

表2-19 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）。	下拉框选项。 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。	下拉框选项。 从下拉列表中选择要设置的加密方式。
哈希算法	支持 md5、sha1 和 sha2_256 三种加密算法。	下拉框选项。 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。	下拉框选项 ☒ psk ☒ rsasig ☒ xauth

参数名称	含义	如何配置
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“5. 参数规范表”。
IKE	网络密钥交换复合协议。	下拉选择 ☒ ikev1 ☒ ikev2
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“5. 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“5. 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
DH 组	此处配置为第一阶段 IKE 协商的密钥长度。	下拉框选项。 从下拉框选项合适的组名即可。
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

点击“保存”，完成该条 IPSec 第一阶段规则配置。



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。

2. 第二阶段参数配置

第二阶段参数配置页面。

图2-32 IPSec 第二阶段配置页面

IPSec 规则第二阶段参数说明。

表2-20 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。
传输协议	支持 esp 认证加密协议。	下拉框选项。 从下拉列表中选择要设置的认证加密协议。
加密方式	支持 des、3des、aes128、aes192、aes256 加密方式。	下拉框选项。 从下拉列表中选择要设置的加密方式。
哈希算法	支持 md5、sha1 和 sha2_256 三种加密算法。	下拉框选项。 从下拉列表中选择要设置的加密算法。

参数名称	含义	如何配置
完美向前加密	选择完美向前加密密钥或禁用完美前向加密。使用完美向前加密会增加系统开销，但可以增加 IPSec 的安全性。	下拉框选项 ☒ close ☒ group768 ☒ group1024 ☒ group1536 ☒ group2048 ☒ group3072 ☒ group4096 根据对端 IPSec 服务器的设置，选择加密密钥或 close。
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。	下拉框选项。 从下拉框选项需要的传输方式。
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。填入本地子网地址和子网掩码位数。 格式：A.B.C.D/M，输入规范请参见“5. 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。填入远端子网地址和子网掩码位数。 格式：A.B.C.D/M，输入规范请参见“5. 参数规范表”。

点击“保存”，完成该条 IPSec 第二阶段规则配置。



上述参数中，传输协议、加密方式、哈希算法、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。

图2-33 IPSec 匹配阶段配置页面

配置 IPSec 规则匹配阶段参数，配置完后点击“保存”。

 说明

当加密接口选择 bridge0（即以太网接口）且 bridge0 接口有多个地址时，IPSec 选择的地址为 bridge0 的 IP1 地址。
IPSec 规则匹配阶段参数说明。

表2-21 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/移动网络/bridge0/wan 接口作为 IPSec 协商的本端，可实现支持 IPSec over VPDN 等组网应用；	下拉框选项。 从下拉框选项合适的接口。

参数名称	含义	如何配置
	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 的连通性。	

——结束

2.4.5.4. OpenVPN 服务

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 H61XX 工业智能网关 WEB 配置界面。登录方法请参见“2.2 登录 WEB 配置界面”。
- 步骤 2 单击“网络设置>VPN 服务>OpenVPN 服务”，打开“OpenVPN 服务”页签。

图2-34 OpenVPN 服务配置页签

OpenVPN

状态未连接

虚拟接口IP

工作模式client

认证模式Certificate&User

接口类型tun

协议udp

目的地址或域名192.168.1.236

目的端口1194

Key

Cert

用户名test

密码

哈希算法RSA-MD5

CipherAES-128-CBC

Ca

TlsNONE

Compress

Nobind

心跳间隔10

工作模式: client模式为客户端类型, site模式为一对一工作模式(对端非服务端)。

接口类型: 网络接口类型, tun(OSI Layer 3), tap(OSI Layer 2): 与对端设置保持一致。

步骤 3 配置 OpenVPN 参数，参数。

表2-22 OpenVPN 参数说明

参数名称	含义	如何配置
启用/禁用	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 工作模式和 site-to-site 模式。 • client 模式为客户端模式 • site-to-site 模式为端对端互访模式	下拉框选项。 从下拉框选项需要的工作模式。
认证模式	支持 Certificate、Certificate&User 和 User/Pwd 两种认证模式。	下拉框选项。 从下拉框选项需要的工作模式。
接口类型	支持 tun 和 tap 两种类型 • tun (OSI Layer 3)：tun 模	下拉框选项。 从下拉框选项需要的工作模式。

参数名称	含义	如何配置
	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。	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。	下拉框选项。 从下拉框选项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“5. 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 要求保持与对端保持一致。
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“5. 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“5. 参数规范表”。
用户名/密码	注册 OpenVPN 服务提时的用户名/密码	WORD 类型/CODE 类型,最大 64 字节,输入规范请参见“5. 参数规范表”。
哈希算法	支持 md5、sha1 等多种加密算法。	下拉框选择
Cipher	SSL 的加密算法系统。	下拉框选项 ☒ NONE ☒ BF-CBC ☒ DES-CBC ☒ RC2-CBC ☒ DES-EDE-CBC ☒ DES-EDE3-CBC ☒ DESX-CBC ☒ RC2-40-CBC ☒ CAST5-CBC ☒ RC2-64-CBC ☒ AES-128-CBC ☒ AES-192-CBC

参数名称	含义	如何配置
		☒ AES-256-CBC ☒ SEED-CBC
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“5. 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“5. 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
心跳间隔	TCP 模式下 keepalive 包进行链路检测时间间隔	手动输入 取值范围：1~65535 单位：秒

步骤 4 点击“保存”，完成 Open VPN 配置。

2.4.5.5. Tunnel 服务

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 H61XX 工业智能网关间对 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 H61XX 工业智能网关包括 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 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“网络设置>VPN 服务>Tunnel 服务”。

打开“Tunnel 服务”页签。

步骤 3 单击右上角“添加”，添加一条新 Tunnel 规则。

图2-35 Tunnel 服务配置页面

< 网络设置 >

VPDN服务

Tunnel服务

IPSec服务

OpenVPN服务

Tunnel服务

名称

*最大长度为8位

协议

ipip

接口虚拟IP

*如: 10.1.1.1

对端接口虚拟IP

*如: 10.1.1.2

接口类型

静态IP

本端地址

*如: 192.168.8.1

对端地址

*如: 192.168.8.1

步骤 4 配置 Tunnel 规则参数。

参数说明。

表2-23 Tunnel 规则参数说明

参数名称	含义	如何配置
启用/禁用	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。
隧道协议	隧道工作模式，分为 gre 和 ipip。	下拉框选项 ☒ gre ☒ ipip 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“5. 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“5. 参数规范表”

参数名称	含义	如何配置
接口类型	对外接口类型，选择为“接口”或者“静态 IP”。	下拉框选项 ☒ 静态 IP ☒ 接口
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“5. 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“5. 参数规范表”。

步骤 5 点击“保存”，完成该条 Tunnel 规则配置。

——结束

2.4.5.6. VXLAN

VXLAN（Virtual Extensible LAN）是一种网络虚拟化技术，用于在现有三层网络（如 IP 网络）上构建 虚拟的二层局域网。

典型组网： PC1-----R1-----R2-----PC2

R1 和 R2 之间具有连通性，R1 和 R2 之间配置 VXLAN，分别将 VXLAN 接口桥接到默认桥下面，在 PC1 和 PC2 之间建立起一个虚拟的二层局域网。

步骤 1 登录 H61XX 工业智能网关 WEB 配置界面，登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“网络设置>VPN 服务”，打开“VXLAN”页签。

图2-36 VXLAN 页签



步骤 3 单击+，新添加 VXLAN 规则。

图2-37 VXLAN 配置页面

< 网络设置 >

VPDN服务Tunnel服务IPSec服务OpenVPN服务VXLAN

VXLAN设置

VXLAN ID

* 范围:1~16777214

端口号

* 如:4789

远端IP

* 如:192.168.8.1

网络接口

[pptp] 1

VXLAN接口MTU

128-15360

UDP校验和

☒启用☐禁用

- 步骤 4 配置完成后，点击保存。
- 步骤 5 在默认桥页面，将 VXLAN 接口绑定到桥。

图2-38 默认桥添加 vxlan 接口

< 网络设置 >

lan

模式

LAN

协议

Static

桥接口

lan2 wlan vxlan_1

*

IPv4 地址

192.168.8.1/24

—

+

* 如: 192.168.8.1/24

最大传输单元

ipv4:68-1500 ipv6:1280-1500 字节

DNS

+

IPv6 地址

2003::1/64

如: 2001:D0B0:3000:3001::1/64

DHCP服务

DHCPV6

禁用

☐关闭此接口 DHCP (IPv4&IPv6) 功能

起始地址

192.168.8.

100

* 网络地址的起始分配基址

客户数

150

* 最大地址分配数量

租期

43200

* 120-86400秒

- 步骤 6 路由器两端都按照上述操作执行，整个 VXLAN 配置完成。

表2-24 VXLAN 配置参数说明

参数名称	含义	如何配置
VXLAN ID	VXLAN ID 号，两端需要一致	手工输入

参数名称	含义	如何配置
		范围：1-16777214 0 和 16777215 保留，不予设置
端口号	VXLAN 数据包的外层 UDP 目标端口号，两端需要一致	手工输入 范围：1-65535
远端 IP	对端 VTEP（VXLAN Tunnel Endpoint）的 IP 地址，用于建立隧道	手工输入 如 200.1.1.2
网络接口	建立 VXLAN 隧道的物理接口	下拉框 下拉框的值为当前设备的接口列表
MTU	VXLAN 虚拟接口的最大传输单元	手工输入 范围：128-15360 此处需要结合实际物理接口 MTU 的范围来设置，默认值是 1500
UDP 校验和	是否启用外层 UDP 校验和（用于检测数据包传输错误）	单选框 默认开启



说明

VXLAN 数据包的传输封装会增加 50 字节 开销（外层 IP/UDP/VXLAN 头），因此在进行大包传输的时候，需要计算好 MTU，根据实际情况合理设置 MTU 值，防止数据出现分包，影响业务性能。

---结束

2.4.6. 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 H61XX 工业智能网关 WEB 配置界面，登录方法请参见“2.2 登录 WEB 配置界面”。
- 步骤 2 单击“网络设置>DHCP 服务”，打开“DHCP 服务”页签。

图2-39 DHCP 服务页签

< 网络设置 >

DHCP服务

域名

OpenSDT

最大长度为32位

DNS

+

IP&MAC绑定规则

名称	MAC	IP地址	租约时间	操作
最大长度为64位	*	*	秒	

步骤 3 配置“DHCP 服务器设置”。DHCP 服务器设置参数。

表2-25 DHCP 服务器设置参数说明

参数名称	含义	如何配置
启用/禁用	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）		
域名	DHCP 客户端向 DNS 服务器请求解析时的“连接特定的 DNS 后缀”，当主要后缀连接失败时，下位机用主机名+“连接特定的后缀”向 DNS 服务器请求 IP 地址。	WORD 类型，最大 32 字节，输入规范请参见“5. 参数规范表”。
DNS	DHCP 客户端获取的 DNS IP。最多可配置 10 个。	接口型 A.B.C.D，输入规范请参见“5. 参数规范表”。 例如：8.8.8.8
IP、MAC 绑定，用于为指定范围内的机器分配的固定的 IP 地址		
名称	IP、MAC 绑定的规则名称标识，没有特定意义，仅用于区分不同规则。	WORD 类型，最大 64 字节，输入规范请参见“5. 参数规范表”。以字母开头，且不能设置特殊字符。
IP	与指定的 MAC 配对，当被绑定 MAC 的 DHCP 客户端发起 DHCP 请求时则会将与该 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分配不会分配给其他 MAC 地址。	接口型 A.B.C.D，输入规范请参见“5. 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：

参数名称	含义	如何配置
		00:1A:4D:34:B1:8E
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

步骤 4 点击“保存”，完成 DHCP 服务配置。

---结束

2.4.7. 智能链路

2.4.7.1. 链路检测

无线网络存在假链接（拨号 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，H61XX 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，H61XX 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 H61XX 工业智能网关 WEB 配置界面，登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“网络设置>智能链路>链路检测”。

打开“链路检测”页签。

图2-40 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. 单击右上角“添加”，显示“链路检测”的添加界面。

图2-41 链路检测添加页面

< 网络设置 >

链路检测

链路备份

链路检测

规则名称

* 最大长度为12位

检测类型

icmp

目的地址

* 最大长度为64位

备份地址

最大长度为64位

检测间隔

* 1-65535 秒

重传次数

* 1-65535

源接口

[dhcp] wan

超时动作

重置 移动网络

2. 配置链路检测服务参数。

参数说明。

表2-26 链路检测规则参数说明

参数名称	含义	如何配置
启用/禁用	使能 ICMP 检测规则。多条规则可同时运行，也可禁用某一条规则。	单选按钮选择。 ☒ 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“5. 参数规范表”。
检测类型	检测类型支持 ICMP 方式。	下拉框选项 ☒ icmp
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 H61XX 工业智能网关配置正确的 DNS。	WORD 类型，最大 64 字节，输入规范请参见“5. 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“5. 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 规则对应的超时动作任务，例如：重置移动网络等。	取值范围：1～65535 单位：秒/次
源接口	H61XX 工业智能网关发送 ICMP 检测包的源地址	下拉框选项 ☒ [brideg]lan ☒ [dhcp]wan

参数名称	含义	如何配置
		☒ [modem]移动网络 ☒ [modem]移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） ☒ wlan2g/5g (WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)
超时动作	当检测失败达到最大失败次数时执行的动作，主要有重置移动网络、重启。	下拉框选项。 ☒ 重置移动网络 ☒ 重启

3. 点击“保存”，完成一条 ICMP 检测规则的添加。



说明

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 H61XX 工业智能网关执行“超时动作”。

- 编辑
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。
 - 删除
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
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
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

2.4.7.2. 链路参数备份

H61XX 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，能实现物理链路、物理链路+虚拟链路、虚拟链路组合的互备切换，能在某一链路故障时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。H61XX 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 H61XX 工业智能网关的 WEB 配置界面。
- 登录方法请参见“2.2 登录 WEB 配置界面”。
- 步骤 2 单击“网络设置>智能链路>链路参数备份”。
- 打开“链路参数备份”页签。

图2-42 链路参数备份页签

< 网络设置 >

链路检测

链路参数备份

规则管理

+

📄

🔄

主链路稳定时间

60

1-65535 秒

备份链路最短工作时间

30

1-65535 秒

规则名称	优先级	链路运行方式	备份模式	接口规则项	当前规则	操作
0	0	main	hot	4g	yes	
1	1	backup	cold	wan		

步骤 3 对“链路参数备份”进行“添加”、“编辑”、“删除”、“启用”和“禁用”操作。

●添加

1. 单击右上角“添加”，显示“链路参数备份”的添加界面。

图2-43 链路参数备份规则添加页面

< 网络设置 >

链路检测

链路参数备份

智能链路

↶

📄

🔄

规则名称

* 最大长度为12位

优先级

* 0-9

链路运行方式

backup

▼

备份模式

cold

▼

检测间隔

1-65535 秒

失败间隔

1-65535 秒

重传次数

1-65535

接口名字

[static] lan2

▼

检测方法

none

▼

检测地址

接入规则

▼

+

2. 配置链路参数备份参数。

参数说明。

表2-27 链路备份参数说明

参数名称	含义	如何配置
主链路稳定时间	从备链切回主链时，主链需保持稳定在线的最短时间。 说明： 当链路运行方式为“主备”（有规则 0）时生效，互备模式不生效。 若不配置，则主链恢复后从备链立即切回主链。	取值范围：1~65535 单位：秒

备份链路最短工作时间	主链恢复从备链切回主链时，备链需要保持的已工作的最短时间。 说明： 当链路运行方式为“主备”（有规则 0）时生效，互备模式不生效。 若不配置，则主链恢复后从备链立即切回主链。	取值范围：1~65535 单位：秒
启用/禁用	使能链路备份功能。	单选按钮选择。 ☒ 启用 ☒ 禁用
规则名称	链路备份规则名称标识，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“5. 参数规范表”。
优先级	备份链路规则的优先级。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	链路的备份方式，包含：主链路和备份链路。主链路发生异常后，通过备份机制将下一跳流量切换至备份链路。	下拉框选项 ☒ main：链路模式为主链路。 ☒ backup：链路模式为备份链路。
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于启用状态，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。 主链路必须为热链路。	下拉框选项 ☒ cold ☒ hot
接口名称	用于链路切换的接口。	下拉框选项 ☒ [brideg]lan ☒ [dhcp]wan ☒ [modem]移动网络 ☒ [modem]移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） wlan2g/5g(WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)

检测方法	检测链路连通状态的方式。	下拉框选项 ☒ none--表示不检测该接口 ☒ state--表示检测接口存在即可 ☒ icmp--表示通过 icmp 方式检测该接口联通指定地址 ☒ http--表示通过 http 方式检测该接口联通指定地址
检测地址	通过 icmp 或 http 方式检测指定 IP 地址或域名，不通则判定检测失败。	WORD 类型，最大 64 字节，输入规范请参见“5. 参数规范表”。
接入规则	当检测接口为移动网络时，可选择指定的拨号规则进行检测。	默认无拨号规则。
检测间隔	链路正常检测时间间隔。	取值范围：1~65535 缺省值为 10 单位：秒
失败间隔	链路检测失败后下一次检测的间隔。	取值范围：1~65535 缺省值为 5 单位：秒
重传次数	链路正常检测的最大失败次数。	取值范围：1~65535 缺省值为 5 单位：次数

3. 点击“保存”，完成链路备份配置。



说明

链路参数切换功能，与负载均衡、双发选收功能冲突，三者不能同时启用；
当启用链路参数备份功能后，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且持续主链路稳定时间，则切换到主链路上；
如需检测虚拟链路，必须所有规则都为虚拟链路，或者物理链路+虚拟链路的组合；
虚拟链路的检测地址，为虚拟接口的对端地址；
虚拟链路的服务器地址，不能为相同地址。

--结束

2.4.8. 路由设置

2.4.8.1. 路由

路由是为 H61XX 工业智能网关转发数据包提供具体的转发路径，须由用户配置。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（H61XX 工业智能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。

2.4.8.2. 静态路由

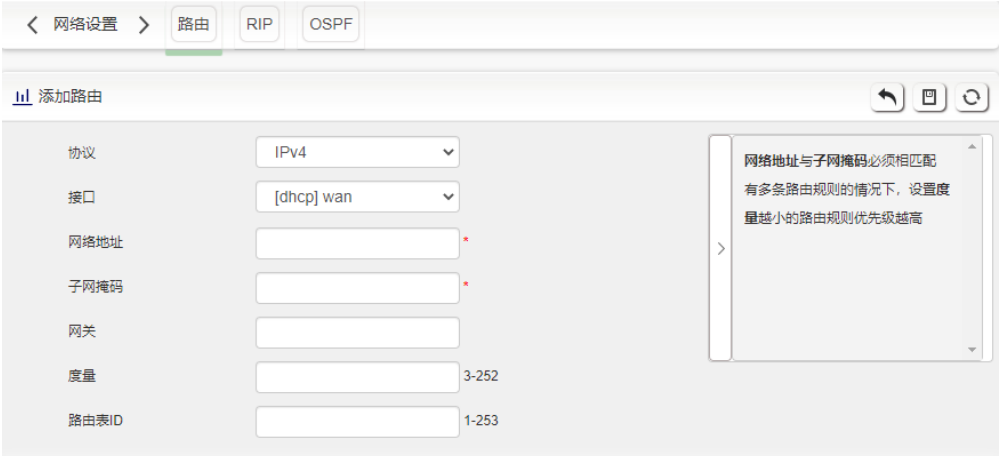
步骤 1 单击“网络设置>路由设置>路由”。打开“路由”页签，默认进入静态路由显示页面。

图2-44 静态路由页签



步骤 2 点击右上角“添加”按钮，新建一条静态路由规则。配置界面。

图2-45 添加静态路由规则页签

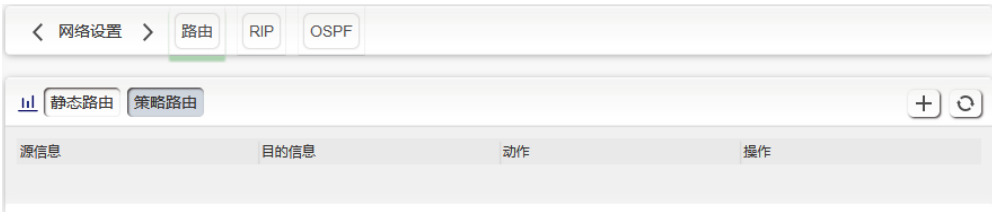


步骤 3 点击“保存”，完成该条路由配置。

2.4.8.3. 策略路由

步骤 1 单击“网络设置>路由设置>路由”。打开“路由”页签，单击“策略路由”，进入策略路由显示页面。

图2-46 策略路由页签



步骤 2 点击右上角“添加”按钮，新建一条策略路由规则。配置界面。

图2-47 添加策略路由规则页签

< 网络设置 >

路由RIPOSPF

添加路由

源接口,目的接口: 设定后, 当前规则需依赖其正常, 策略路由才会生效。

协议IPv4

源接口空

源地址192.168.8.1或192.168.8.0/24

目的地址192.168.8.1或192.168.8.0/24

路由表ID1-253

步骤 3 点击“保存”，完成该条路由配置。

表2-28 路由参数说明

参数名称	含义	如何配置
当选择“静态路由”时		
协议	路由的 IP 地址类型，目前仅支持 IPv4 类型。	下拉框选项 ☒ IPv4
接口	静态路由所作用的接口。	下拉框选项 ☒ [bridge]lan ☒ [dhcp]wan ☒ [modem]移动网络 ☒ [modem]移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） ☒ wlan2g/5g(WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)
网络地址	设置静态路由的目标地址。	接口型 A.B.C.D，输入规范 请参见“5. 参数规范表”。 例如：192.168.8.2。
子网掩码	设置静态路由的目标地址所匹配的子网掩码。	接口型 A.B.C.D，输入规范 请参见“5. 参数规范表”。 例如：255.255.255.0。
网关	设置静态路由的下一跳 IP 地址，即相邻 H61XX 工业智能网关的端口地址。	接口型 A.B.C.D，输入规范 请参见“5. 参数规范表”。 例如：192.168.8.1。
度量	路由表的度量值。度量值越小，路由策略的优先级越高。	取值范围：3~252

参数名称	含义	如何配置
路由表 ID	路由策略的路由表标识号，便于策略路由和静态路由进行策略匹配。	取值范围：1~253
当选择“策略路由”时		
协议	路由的 IP 地址类型，目前仅支持 IPv4 类型。	下拉框选项 ☒ IPv4
源接口	策略路由的源接口。 说明： 当源接口和源地址为一一对应时，源地址和源接口可以不都配置，如移动网络的接口和 IP。	下拉框选项 ☒ 空 ☒ [bridge]lan ☒ [dhcp]wan ☒ [modem]移动网络 ☒ [modem]移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） ☒ wlan2g/5g(WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)
源地址	策略路由的源 IP 地址。	接口型 A.B.C.D，输入规范请参见“5. 参数规范表”。 例如：192.168.8.2。
目的地址	策略路由的目的地址。当目的地址为空时，其路由可达地址与对应源接口、源地址或路由表一致。	接口型 A.B.C.D，输入规范请参见“5. 参数规范表”。 例如：192.168.8.2。
路由表 ID	路由策略的路由表标识号，便于策略路由和静态路由进行策略匹配。 当源接口和源地址为空，配置路由表 ID 后，其路由策略与该路由表中静态路由一致。	取值范围：[1, 253]



说明

静态路由是指 H61XX 工业智能网关根据接收到的转发包的目的地地址选择路由然后再将数据包转发出去，如 H61XX 工业智能网关接收到源地址为 1.1.1.1/目的地地址为 2.2.2.2 的包，则 H61XX 工业智能网关在路由表中选择符合目的地地址 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 H61XX 工业智能网关根据收到的转发包的源地址选择路由再转发出去，如 H61XX 工业智能网关接收到源地址为 1.1.1.1/目的地地址为 2.2.2.2 的包，则 H61XX 工业智能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

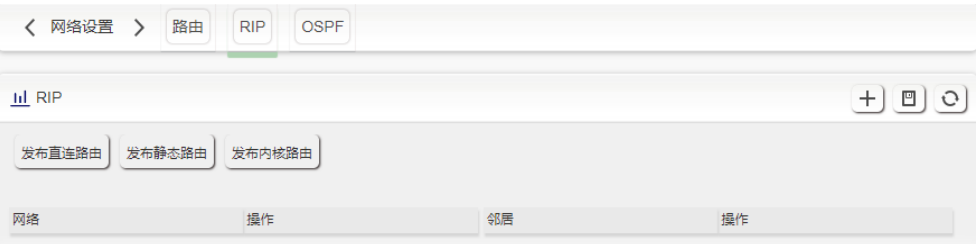
2.4.8.4. RIP 配置

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, H61XX 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 H61XX 工业智能网关出厂时根据用户是否需要进行配置。

步骤 2 单击“网络设置>路由设置>RIP”。

打开“RIP”页签。

图2-48 RIP 页签



RIP 的参数说明。

表2-29 RIP 参数说明

参数名称	含义	如何配置
发布直连路由	是否允许发布直连路由。	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 点击右上角“添加”按钮, 新建一条 RIP 规则。配置界面。

图2-49 RIP 配置页签



步骤 4 配置 RIP 规则参数。

RIP 规则的参数说明。

表2-30 RIP 参数说明 II

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。 ☒ 当选择为“网络”时，需要配置目的网络地址（一般为 H61XX 工业智能网关直连的网络）。 ☒ 当选择为“邻居”时，需要配置邻居的 IP 地址（与 H61XX 工业智能网关相连的 H61XX 工业智能网关的 IP 地址）。
网络（与 H61XX 工业智能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及子网掩码位数。 格式：A.B.C.D/M，输入规范请参见“5. 参数规范表”。
邻居（与 H61XX 工业智能网关直接相连的 H61XX 工业智能网关）	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，输入规范请参见“5. 参数规范表”。

步骤 5 点击“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 H61XX 工业智能网关交换信息。如果两个 H61XX 工业智能网关之间的通信不经过另外一个 H61XX 工业智能网关，那么这两个 H61XX 工业智能网关是相邻的。RIP 协议规定，不相邻的 H61XX 工业智能网关之间不交换信息。

H61XX 工业智能网关交换的信息是当前本 H61XX 工业智能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 H61XX 工业智能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 H61XX 工业智能网关，跳数就加 1。RIP 认为好的路由就是它通过的 H61XX 工业智能网关的数目少，即“距离短”。RIP 允许一条路径最多只能包含 15 个 H61XX 工业智能网关。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

2.4.8.5. 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 H61XX 工业智能网关出厂时根据用户是否需要配置

步骤 1 单击“网络设置>路由设置>OSPF”。

打开“OSPF”页签。

图2-50 OSPF 页签



OSPF 的参数说明。

表2-31 OSPF 参数说明

参数名称	含义	如何配置
启用/禁用	启用/禁用 OSPF 服务。	单选按钮选择。 ☒ 启用 ☒ 禁用
发布直连路由	是否允许发布直连路由。	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 2 单击右上角“添加”，新建一条 OSPF 规则。配置界面。

图2-51 OSPF 配置页签



步骤 6 配置路由模式规则参数。

OSPF 的参数说明。

表2-32 OSPF 参数说明 II

参数名称	含义	如何配置
当“通告类型”选择“网络”时		
网络	设置某个网段作为 H61XX 工业智能网关 OSPF 发送地址。	格式：A.B.C.D/M 接口型，输入规范请参见“5. 参数规范表”。
域地址	用于标识网络（只有域地址相同的 H61XX 工业智能网关之间才会使用 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	H61XX 工业智能网关可以一跳到达的设备地址。	手动输入，格式：A.B.C.D 接口型，输入规范请参见“5. 参数规范表”。
当“通告类型”选择“接口”时		
接口名称	H61XX 工业智能网关的某个接口。	下拉框选项 ☒ [bridge]lan ☒ [dhcp]wan ☒ [modem] 移动网络 ☒ [modem] 移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） ☒ wlan2g/5g (WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)
接口属性	配置 H61XX 工业智能网关接口的属性，包括网络和邻居两种属性。	单击按钮选择 ☒ 网络 ☒ 邻居
开销	配置 H61XX 工业智能网关接口的开销，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 H61XX 工业智能网关接口的网络类型。	下拉框选项 ☒ broadcast ☒ non-broadcast ☒ point-to-multipoint ☒ point-to-point

步骤 7 点击“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 H61XX 工业智能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 H61XX 工业智能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 H61XX 工业智能网关，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 H61XX 工业智能网关。

——结束

2.4.9. QoS

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，H61XX 工业智能网关支持定制 QoS 业务。

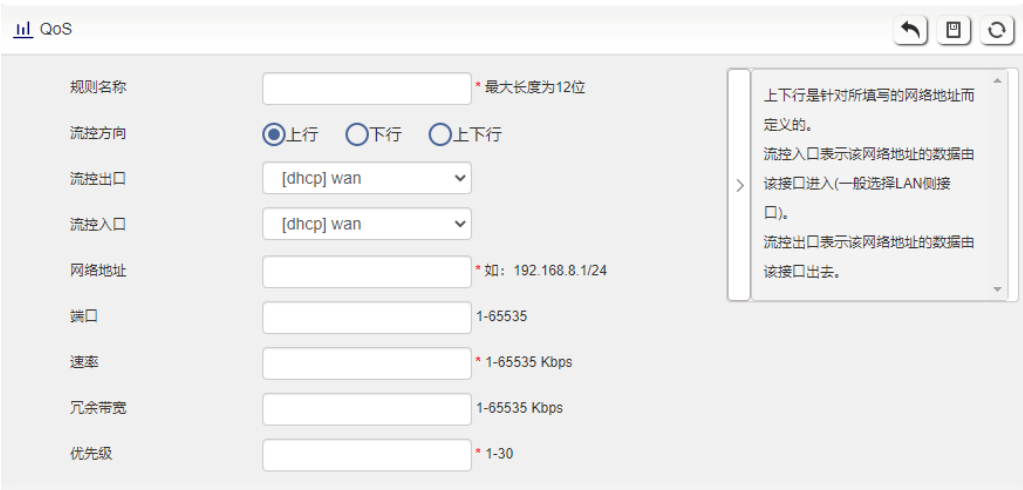
- 步骤 1 单击“网络设置>QoS”。
- 打开“QoS”页签。

图2-52 QoS 页签



- 步骤 2 点击右上角“添加”，新建一条 QoS 规则。配置界面。

图2-53 QoS 配置页签



- 步骤 3 配置 QoS 参数。
- QoS 的参数说明。

表2-33 QoS 参数说明

参数名称	含义	如何配置
规则名称	QoS 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“5. 参数规范表”。 说明： 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。
流控方向	进行流量控制的流量方向。上下行方向是针对所填写的网络地址而定义的。	单击按钮选择 ☒ 上行 ☒ 下行 ☒ 上下行
流控出口	进行流量控制的网络地址的数据由该接口出去。	下拉框选项 ☒ [brideg]lan ☒ [dhcp]wan ☒ [modem] 移动网络 ☒ [modem] 移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） ☒ wlan2g/5g (WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)
流控入口	进行流量控制的网络地址的数据由该接口进入（一般选择[brideg]lan 侧接口）	下拉框选项 ☒ [brideg]lan ☒ [dhcp]wan ☒ [modem] 移动网络 ☒ [modem] 移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） ☒ wlan2g/5g (WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)
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“5. 参数规范表”。

参数名称	含义	如何配置
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：1~65535 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：1~65535 单位：Kbps 冗余带宽可以不配置，若不配置则代表不对带宽进行限制。
优先级	设置该规则的优先级。	手动输入 取值范围：1~30

步骤 4 点击“保存”完成参数配置。



说明

QoS 主要用于 H61XX 工业智能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 H61XX 工业智能网关下接有两个子网：192.168.8.1/24 和 192.168.9.1/24，则 H61XX 工业智能网关可以通过 QoS 来控制这两个子网的速率；若 H61XX 工业智能网关的带宽比较宽裕，则 H61XX 工业智能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。

一结束

2.4.10. 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 H61XX 工业智能网关的页面。当然，H61XX 工业智能网关使用的 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 H61XX 工业智能网关。

步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。
登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“网络设置>DDNS 设置”。
打开“DDNS”页签。

图2-54 DDNS 页签



步骤 3 点击右上角“添加”，新建一条 DDNS 规则。配置界面。

图2-55 DDNS 设置页签

DDNS

规则名

* 最大长度为12位

主机名

* 最大长度为64位

源接口

[dhcp] wan

协议版本

IPv4

服务提供商

zoneedit.com

用户域名

* 最大长度为64位

用户名

* 最大长度为64位

密码

* 最大长度为64位

更新间隔

300-86400 秒

用户名/密码：用户名和密码由您的服务提供商提供。

更新间隔：每隔一定时间向服务器发送更新信息的时间。

步骤 4 配置 DDNS 服务参数。

参数说明。

表2-34 DDNS 服务参数说明

参数名称	含义	如何配置
启用/禁用	使能 DDNS 服务。	单选按钮选择 ☒ 启用 ☒ 禁用
基本设置		
规则名	DDNS 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“5. 参数规范表”。 说明： 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。
主机名	DDNS 规则的主机名。	WORD 类型，最大 12 字节，输入规范请参见“5. 参数规范表”。

参数名称	含义	如何配置
源接口	配置 DDNS 规则的源接口。应用该规则的接口可通过该规则进行域名解析。	下拉框选项 ☒ [brideg]lan ☒ [dhcp]wan ☒ [dhcp]SPF1 ☒ [dhcp]SPF2 ☒ [modem]移动网络 ☒ [modem]移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） ☒ wlan2g/5g(WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)
协议版本	IP 地址类型，目前仅支持 IPv4 类型。	下拉框选项 ☒ IPv4
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 ☒ zoneedit.com ☒ ns1.dipns.com ☒ dnsexit.com ☒ changeip.com ☒ 3322.com ☒ dyndns.org ☒ oray.com ☒
用户域名	DDNS 服务提供商提供的域名，它与 H61XX 工业智能网关的 IP 相对应，通常通过访问该域名来访问 H61XX 工业智能网关的 IP。	一般 WORD 类型，最大 64 字节，输入规范请参见“5. 参数规范表”。
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，输入规范请参见“5. 参数规范表”。
更新间隔	H61XX 工业智能网关向 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 H61XX 工业智能网关按照“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。	手动输入 取值范围：120~86400 单位：秒

步骤 5 点击“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.zoneedit.com)、CHANGEIP(www.changeip.com)、DYNDNS(www.members.dyndns.org)
- 每次 H61XX 工业智能网关重启时，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 H61XX 工业智能网关时使用的是申请到的 DDNS 域名，那么不管 H61XX 工业智能网关移动网络 IP 地址怎么改变，用户都可以登录到 H61XX 工业智能网关页面。

---结束

2.4.11. 负载均衡

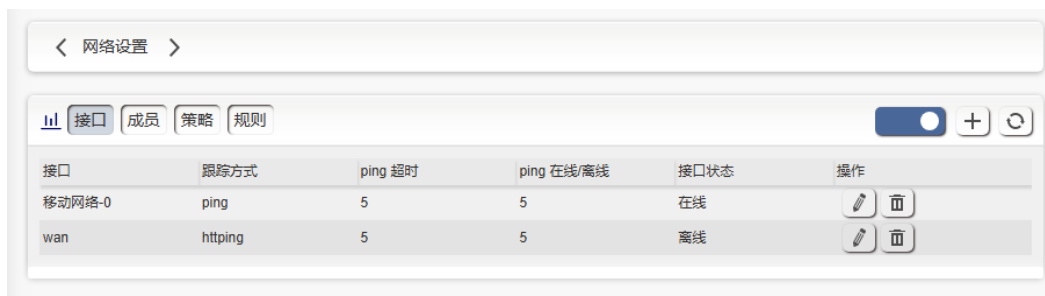
H61XX 工业智能网关的负载均衡功能，是采用 MWAN3 解决方案实现的。MWAN3 是一个用于 Linux 系统的负载均衡和故障切换解决方案，特别适用于多 WAN（广域网）环境。其主要功能是通过在多个网络接口间分配出站连接数来优化网络性能和可靠性。即 H61XX 工业智能网关如有多个 WAN 口，MWAN3 可以同时利用外网连接的带宽，或者在一个连接失败时自动切换到另一个，确保网络连接的连续性。此外，它还支持基于策略的路由，允许用户根据特定规则选择数据包通过哪个接口发送，从而实现更精细的连接数控制。

负载均衡需要依次对接口、成员、策略、规则依次配置，才能实现精细的、基于连接数的均衡。

2.4.11.1. 接口

步骤 1 单击“网络设置>负载均衡”，打开“接口”页签，配置外 WAN 口检测规则，

图2-56 接口列表



< 网络设置 >					
	接口	成员	策略	规则	  
接口	跟踪方式	ping 超时	ping 在线/离线	接口状态	操作
移动网络-0	ping	5	5	在线	 
wan	httping	5	5	离线	 

步骤 2 点击右侧“+”图标，可进入新增接口检测规则页面。

图2-57 新增接口检测规则

负载均衡-接口

接口

[modem] 移动网络-0

跟踪方式

ping

跟踪地址

8.8.8.8

www.baidu.com

ping 超时

5

秒

ping 间隔

3

秒

ping 失败间隔

5

秒

ping 在线/离线

5

次

说明

突，负载均衡的接口和网络接口存在关联。
跟踪地址：可以配置多个地址，通过跟踪方式检测地址是否连通，只要有其中一个地址连通就认为接口正常。
ping 在线/离线：只要检测地址连续达到的次数达到配置次数，就认为接口在线/离线。

步骤 3 接口规则支持新增、编辑、删除操作。

说明

- 负载均衡仅针对外网接口，如 wan、移动网络、WiFi station；
- 一个外网接口仅能使用一条接口检测规则；
- 操作接口规则后，负载均衡功能立即自动重启生效。

2.4.11.2. 成员

步骤 1 单击“网络设置>负载均衡”，打开“成员”页签，配置每个接口的权重、跃点数。

图2-58 成员规则列表

接口 成员 策略 规则

+

刷新

成员	接口	跃点数	权重	操作
modem_m1_w3	移动网络-0	1	3	编辑 删除
wan_m1_w3	wan	1	3	编辑 删除

步骤 2 点击右侧“+”图标，可新增成员规则。

图2-59 新增成员规则



图2-59展示了“新增成员规则”的界面。该界面包含以下配置项：

- 成员**：输入框，提示“* 最大长度为64位”。
- 接口**：下拉菜单，当前选择为“[dhcp] wan”。
- 跃点数**：输入框，提示“* 1-256”。
- 权重**：输入框，提示“* 1-1000”。

步骤 3 成员规则支持新增、编辑、删除操作。

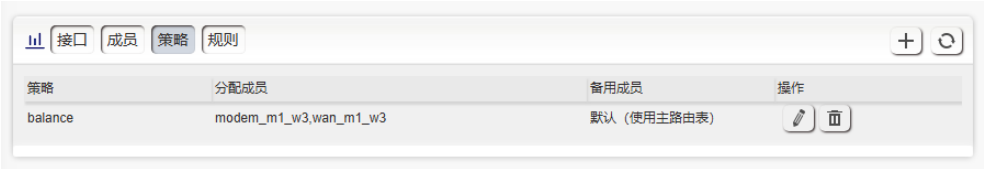
 说明

- 成员命名规则一般为：[外网接口]_m[跃点数]_w[权重]，如 modem_m1_w3，表示该成员为跃点数为 1、权重为 3 的 modem 接口；
- 每个外网接口可以有不同权重、跃点数的规则；
- 跃点数越小，优先级越高；
- 权重值越大，均衡的连接数越多；
- 操作成员规则后，负载均衡功能立即自动重启生效。

2.4.11.3. 策略

步骤 1 单击“网络设置>负载均衡”，打开“策略”页签，配置成员组合的策略。

图2-60 策略规则列表



策略	分配成员	备用成员	操作
balance	modem_m1_w3,wan_m1_w3	默认（使用主路由表）	 

步骤 2 点击右侧“+”图标，可新增策略规则。

图2-61 新增策略规则



图2-61展示了“新增策略规则”的界面。该界面包含以下配置项：

- 策略**：输入框，提示“* 最大长度为64位”。
- 分配成员**：下拉菜单，当前选择为“modem_m1_w3”，右侧有“-”按钮。
- 备用成员**：下拉菜单，当前选择为“wan_m1_w3”，右侧有“+”按钮。
- 备用成员**：下拉菜单，当前选择为“默认（使用主路由表）”。

右侧提示框内容：

“策略”把成员进行分组，在分配规则中使用这一策略的流量。最多32条策略。拥有较低跃点数的成员将会被优先。

步骤 3 策略规则支持新增、编辑、删除操作。



说明

- 拥有较低跃点数的成员将会被优先使用；
- 拥有相同跃点数的成员把流量进行负载均衡；
- 进行负载均衡的成员之间拥有较高比重的成员将会被分配到更多流量；
- 操作策略规则后，负载均衡功能立即自动重启生效。

2.4.11.4. 规则

步骤 1 单击“网络设置>负载均衡”，打开“规则”页签，配置负载均衡规则优先顺序。

图2-62 负载均衡的规则列表

规则	分配的策略	协议	源地址	源端口	目的地址	目的端口	操作
rule_default	balance	all					

步骤 2 点击右侧“+”图标，可新增策略规则。

图2-63 新增负载均衡规则

规则 * 最大长度为14位

协议

源地址

目的地址

域名

分配的策略

规则用于指定哪些流量将使用特定的 MWAN 策略，最多32条规则。规则可基于 IP 地址，端口或协议。每条规则至上而下进行匹配。如果匹配中了某条规则，则其下方的规则将被忽略。不符合任何规则的流量将使用主路由进行转发。

参数说明如下：

表2-35 负载均衡规则的参数说明

参数名称	含义	如何配置
规则	自定义规则名称	WORD 类型，最大 14 位，输入规范请参见“5. 参数规范表”。 说明： 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。

参数名称	含义	如何配置
协议	支持的连接协议类型，指定的协议匹配规则	下拉框选项 ☒ ALL ☒ TCP ☒ UDP ☒ ICMP 默认 TCP。
源地址	发起连接的源地址	IP 地址格式
目的地址	连接访问的目的地址	IP 地址格式
分配策略	在“策略”页面的策略列表	下拉框选项

步骤 3 负载均衡的规则支持新增、编辑、删除操作。



说明

- 每条规则至上而下进行匹配，如匹配中了某条规则，则其下方的规则将被忽略；
- 不符合任何规则的流量将使用主路由表进行路由；
- 负载均衡是针对连接数进行均衡，并不针对流量；
- 操作规则后，负载均衡功能立即自动重启生效；
- 负载均衡与链路参数切换、双发选收功能重启，三者不能同时使用。

典型应用场景

基于 MWAN3 的负载均衡功能，H61XX 支持以下典型应用场景：

带宽叠加

场景描述：将多条 WAN 链路的带宽进行叠加，提升总出口带宽。适用于需要大带宽传输的应用场景，如视频监控回传。

配置要点：在策略配置中，将多个成员（如 WAN 和移动网络）加入同一策略，设置相同的跃点数（metric），MWAN3 将按权重比例分配新建连接到不同链路，实现带宽叠加效果。

示例：H61XX 同时使用 WAN 口（300Mbps）和移动网络（100Mbps），配置负载均衡策略后，总可用带宽可达到约 400Mbps（实际效果取决于各链路实时状况）。

验证方法：使用电脑开启迅雷等多线程下载工具下载一个大文件，或同时用多台设备看高清视频。在 MWAN3"状态"页，会看到两个接口同时有持续的流量流出。使用测速网站可能无法体现叠加效果（因为测速通常是单线程），但实际多任务下载速度会接近两条宽带之和。

主备热备

场景描述：主链路正常时使用主链路，主链路故障时自动切换到备份链路。适用于对网络可靠性要求高的场景。

配置要点：在策略配置中，主链路成员设置较小的跃点数，备份链路成员设置较大的跃点数。MWAN3 优先使用跃点数小的成员转发流量，当该成员故障时自动切换到跃点数较大的备份成员。

示例：将 WAN 口跃点数设为 10（主链路），移动网络跃点数设为 20（备份链路）。WAN 口正常时所有流量走 WAN；WAN 口故障时自动切换到移动网络。

验证方法：在持续 ping 一个公网 IP（如 8.8.8.8）时，断开主链路，观察到 1-3 个 ping 包超时（切换时间）后恢复连通。后台 mwan3 status 查看备份链路权重变为 100%。恢复主链路后，流量自动迁回。

互备延迟

场景描述：两条链路互为主备，根据链路质量（延迟）动态选择最优链路。适用于两条链路质量相近、需要动态优化的场景。

配置要点：所有接口配置中需选择 ping 检测方式，勾选“检查连接质量”并配置最大延迟和最小延迟。MWAN3 实时检测各接口连接质量，延迟连续大于配置最大延迟 5 次后，接口被判定离线/延时大。

验证方法：双接口质量良好时，上网按接口权重比例分配流量。当一条链路延迟过高时，流量自动切换到另一条链路。

策略分流

场景描述：根据数据包特征（源/目的 IP、端口、协议等）将不同业务流量分配到指定链路。适用于不同业务有不同出口需求的场景。

示例：将视频监控流量路由到 WAN 口，将业务数据流量路由到移动网络，实现业务隔离和链路优化。具体配置：

1. 配置接口：添加 WAN、移动网络-0、移动网络 2-0 接口并分别配置检测地址。
2. 创建成员：为每个接口创建成员，跃点数相同，权重按带宽比设置。
3. 制定策略：创建多个策略分别用于不同出口。
4. 定义规则：rule_wan 规则目的地址填写办公网网段走 WAN；rule_modem2 填写访问平台域名走 modem2；rule_modem 承担其他流量，规则放在最后作为默认。
5. 点击使能按钮，启用功能。

验证方法：后台输入“contrack -L |grep icmp”命令查看流量链接，可以看到不同目的地址的数据从不同的出口出去。

注：以上场景可通过后台命令“mwan3 status”查看当前负载均衡状态，包括各接口状态、权重、策略和规则信息。

2.4.12. VLAN

H61XX 工业智能网关的 VLAN 功能是基于端口的 VLAN 绑定功能，支持端口配置 tag 和 untag 两种类型；默认所有端口均属于 vlan1（vlan1 为默认管理 vlan，不可编辑）

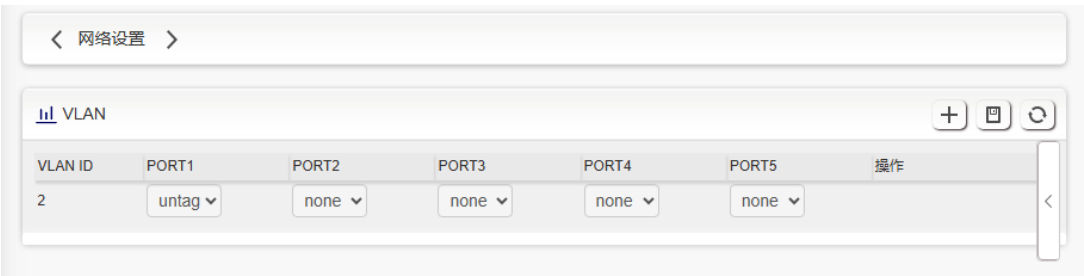
步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“网络设置>VLAN 设置”。

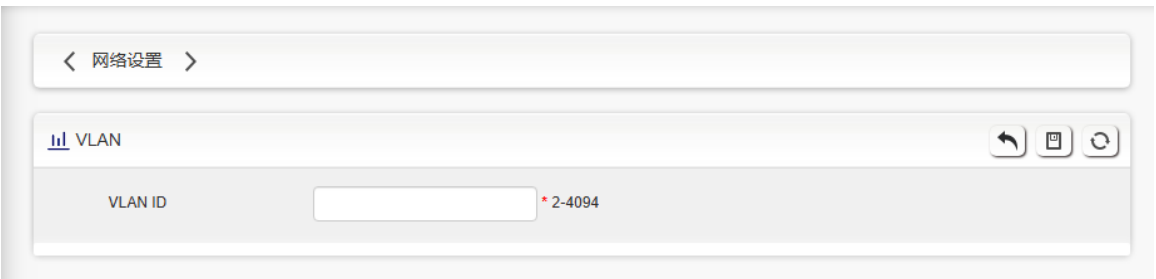
打开“vlan”页签。

图2-64 VLAN 设置页面



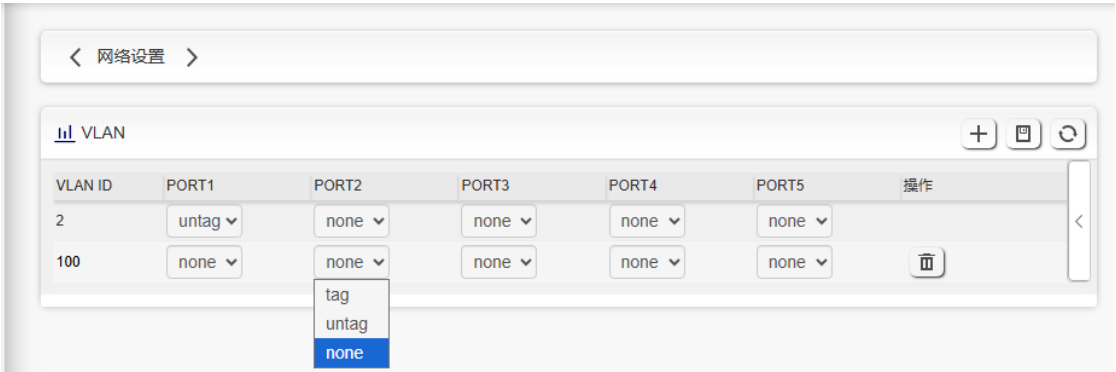
步骤 3 点击右上角添加按钮，新增一条 vlan 配置：

图2-65 新增 VLAN



步骤 4 选择 vlan 绑定的 port。

图2-66 选择 VLAN 绑定的 port



对应端口下拉框选择该接口是否加入 vlan，以及使用哪种端口类型加入；
VLAN 配置参数如下表：

表2-36 VLAN 配置参数说明

参数名称	含义	如何配置
Vlan ID	添加 vlan 配置，配置 Vlan ID	数字类型；支持 2-4094
Port	1. 选择端口是否加入该 vlan； 2. 当前端口绑定该 vlan 时的端口类型	下拉框选择： ● None 不绑定 vlan ● Tag 端口为 tag 类型 ● Untag 端口为 untag 类型

步骤 5 点击保存，完成 vlan 配置添加。



说明

- 所有 LAN 口默认属于 vlan1，vlan1 为默认管理 vlan，不可编辑；WAN 口默认属于 vlan2
- 至少保留一个端口属于 vlan1 且为 untag 类型，保证管理 IP 可以访问

---结束

2.4.13. 双发选收

双发选收（也称为冗余路径或冗余传输）是一种提高数据传输可靠性的技术，特别是在网络通信和存储系统中。这种机制通过在发送端同时经由两条独立的路径发送相同的数据，接收端则从这两条路径中选择质量更好、到达更快或者更可靠的那一条数据进行处理，从而确保数据能够成功、及时地到达目的地。这种方法主要用于对抗网络中的丢包、延迟和抖动等问题，尤其适用于对可靠性要求极高的应用场合。

步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“网络设置>双发选收设置”。

图2-67 双发选收配置页面

< 网络设置 >

双发选收

基础设置

类型

FRER

接口选择

入口

br-lan

出口1

[dhcp] wan

默认转发出口

出口2

[dhcp] wan

关键流源MAC匹配

MAC地址

+

如: 00:1A:4D:34:B1:8E

高级选项

消冗窗口

512

256-1024

序号号按源MAC流独立

☐

步骤 3 启用功能，选择对应的配置

表2-37 双发选收配置项说明

参数名称	含义	如何配置
基础设置		
类型	选择双发选择的协议类型	下拉框选择： ● FRER ● PRP
接口选择		
入口	选择终端的数据入口	下拉框选择： ● Br-lan
出口 1	选择双发选收的数据出接口	● WAN ● 移动网络-0 ● 移动网络 2-0
出口 2	选择双发选收的数据出接口	● WAN ● 移动网络-0 ● 移动网络 2-0
关键流源 MAC 匹配		
MAC 地址	配置从双发选收转发的数据源 MAC； 最多可添加 10 个	WORD 类型 MAC 格式 例如： 00:1A:4D:34:B1:8E
高级选项		
消冗窗口	主要用于处理由双发选收带来的重复 数据问题	数据类型格式： 范围：256-1024
序列号按源 MAC 流独立	每个具有不同源 MAC 地址的数据流都 有自己独立的一套序列号系统	勾选框配置 ● 勾选 启用 ● 去勾选 禁用

步骤 4 点击保存，完成双发选收配置添加。

---结束

2.5. 安全设置

2.5.1. 概述

H61XX 工业智能网关的安全功能包括黑白名单、NAT 设置、端口禁用、DDOS 防御四个部分的配置。其中黑白名单是基于转发规则对数据进行限制；NAT 设置包括常用的 NAT 配置，包括 SNAT/DNAT/MASQ 配置；端口禁用针对 input 规则，用户可以基于设备上的接口设置基于 TCP 和 UDP 接口的访问控制；DDOS 防御主要基于常见的 DDOS 攻击进行防御，用户可以根据自身的安全要求开启不同类型的防护。

2.5.2. 黑白名单

黑白名单针对的是 iptables 里面的转发规则，分为 ip 过滤、MAC 过滤、域名过滤 3 种场景，黑名单表示拒绝访问，白名单表示允许访问，白名单的最后会添加一条 deny all 的规则。

图2-68 黑白名单基本页面



2.5.2.1. IP 过滤

基于源 IP、源端口、目的 IP、目的端口进行配置，规则可以应用到 TCP 和 UDP 协议上。用户可以灵活的根据条件进行组合。黑名单和白名单同时只能一个生效，不能同时既有黑名单和白名单。

IP 过滤规则配置步骤如下：

步骤 1 单击“安全设置>黑白名单>IP 过滤”。选择+添加黑白名单规则；

图2-69 IP 过滤规则添加

< 安全设置 >

IP 过滤

MAC过滤

域名过滤

IP 过滤

规则名称

1

* 最大长度为64位

过滤模式

黑名单

协议

TCP

源地址

192.168.8.0/24

192.168.8.1或192.168.8.0/24

源端口

合法的格式为'xx-xx'， 或者 'xx xxxx ...'， 或者'xx'！

目标地址

8.8.8.8

192.168.8.1或192.168.8.0/24

目标端口

合法的格式为'xx-xx'， 或者 'xx xxxx ...'， 或者'xx'！

步骤 2 单击保存，规则添加成功

表2-38 IP 过滤规则参数说明：

参数名称	含义	如何配置
规则名称	IP 过滤规则名称	手动输入 最大支持 64 个字符
过滤模式	IP 过滤规则模式设置	下拉框选项 ☒ 黑名单 ☒ 白名单 选择黑名单，添加的时候默认显示黑名单；选择白名单添加时，默认显示白名单
协议	Socket 协议设置	下拉框选项 ☒ TCP ☒ UDP ☒ TCP+UDP 默认选择 TCP
源地址	匹配报文源地址设置，不设置的时候表示 any，任意源地址都能匹配成功	手动输入 支持输入 IP 地址和网络地址
源端口	匹配报文源端口设置	手动输入 范围 1-65535
目标地址	匹配报文源地址设置，不设置的时候表示 any，任意目标地址都能匹配成功	手动输入 支持输入 IP 地址和网络地址

目标端口	匹配报文目标端口设置	手动输入 范围 1-65535
------	------------	--------------------



说明

- 白名单下面必须配置一条规则，因为白名单最后有一条 deny any 的规则，否则会影响正常的业务运行

2.5.2.2. MAC 过滤

可以基于源 MAC 地址进行转发过滤，这里只要 MAC 地址匹配上了，TCP 和 UDP 协议都会生效。

MAC 过滤规则配置步骤如下：

步骤 1 单击“安全设置>黑白名单>MAC 过滤”。选择+添加黑白名单规则；

图2-70 MAC 过滤规则添加

步骤 2 单击保存，规则添加成功

表2-39 MAC 过滤规则参数说明：

参数名称	含义	如何配置
规则名称	IP 过滤规则名称	手动输入 最大支持 64 个字符

参数名称	含义	如何配置
过滤模式	IP 过滤规则模式设置	下拉框选项 ☒ 黑名单 ☒ 白名单 选择黑名单，添加的时候默认显示黑名单；选择白名单添加时，默认显示白名单
源 MAC	匹配报文源 MAC 设置，匹配上了源 MAC，规则生效	手动输入 如：00:1A:4D:34:B1:8E



说明

- 白名单下面必须配置一条规则，因为白名单最后有一条 deny any 的规则，否则会影响正常的业务运行

2.5.2.3. 域名过滤

可以基于源域名地址进行转发过滤，这里只要域名地址匹配上了，TCP 和 UDP 协议都会生效。
域名过滤规则配置步骤如下：

步骤 1 单击“安全设置>黑白名单>域名过滤”。选择+添加黑白名单规则；

图2-71 域名过滤规则添加

步骤 2 单击保存，规则添加成功

表2-40 域名过滤规则参数说明：

参数名称	含义	如何配置
规则名称	IP 过滤规则名称	手动输入 最大支持 64 个字符
过滤模式	IP 过滤规则模式设置	下拉框选项 ☒ 黑名单 ☐ 白名单 选择黑名单，添加的时候默认显示黑名单；选择白名单添加时，默认显示白名单
关键字	域名关键字设置，域名里面匹配到了关键字则规则生效，关键字可以是域名的一部分如 baidu	手动输入 如：baidu



说明

- 白名单下面必须配置一条规则，因为白名单最后有一条 deny any 的规则，否则会影响正常的业务运行

2.5.3. NAT 设置

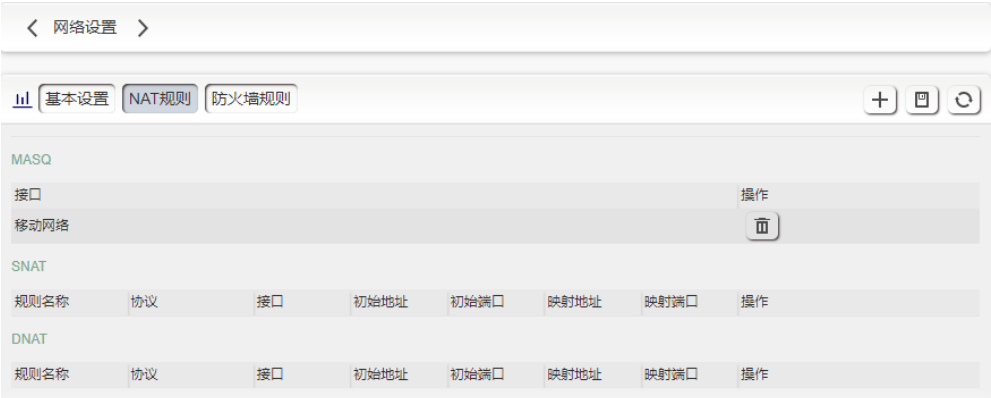
NAT（Netword Address Translation），网络地址转换，一般用于将私网（局域网）IP 地址替换成公网 IP 地址。

2.5.3.1. DNAT 规则配置

DNAT 是目的地址替换，用于将外网访问 H61XX 工业智能网关内部的目的地址替换成用户设置的地址。

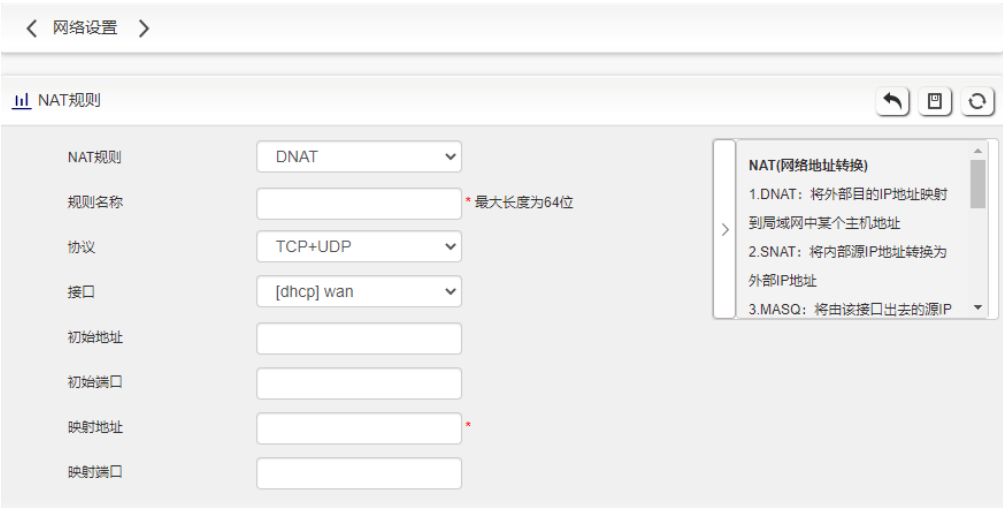
步骤 1 单击“网络设置>安全设置>NAT 规则”。

图2-72 NAT 页签



步骤 2 单击“NAT 规则”右上角“添加”按钮，选择“NAT 规则”为“DNAT”。

图2-73 DNAT 配置页签



步骤 3 配置 DNAT 规则参数。

DNAT 的参数说明。

表2-41 DNAT 参数说明

参数名称	含义	如何配置
NAT 规则	NAT 规则的转换类型。	下拉框选项 ☒ DNAT ☒ SNAT ☒ MASQ
规则名称	NAT 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 64 字节，输入规范请参见“5. 参数规范表”。

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。	下拉框选项 ☒ TCP ☒ UDP ☒ TCP+UDP ☒ ICMP ☒ ALL
接口	选择 IP 数据包的目的地址为 H61XX 工业智能网关的某个接口。	下拉框选项 ☒ [bridge]lan ☒ [dhcp]wan ☒ [modem]移动网络 ☒ [modem]移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） ☒ wlan2g/5g (WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)
初始地址	表示进入 H61XX 工业智能网关的 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“5. 参数规范表”
初始端口	IP 数据包中目的地址使用的端口。	手动输入 取值范围：1~65535
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“5. 参数规范表”
映射端口	初始端口替换后的端口。	手动输入 取值范围：1~65535

步骤 4 点击“保存”，完成该条 DNAT 规则配置。



说明

当 DNAT 规则中协议选择“ALL”表示选择“TCP”、“UDP”、“ICMP”三种协议。

2.5.3.2. SNAT 规则配置

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

步骤 1 单击“网络设置>安全设置>NAT 规则”。

打开“NAT 规则”页签。

步骤 2 单击“NAT 规则”右上角“添加”按钮，选择“NAT 规则”为“SNAT”。

图2-74 NAT 配置页签

< 网络设置 >

NAT规则

NAT规则

SNAT

规则名称

* 最大长度为64位

协议

TCP+UDP

接口

[dhcp] wan

初始地址

*

初始端口

映射地址

映射端口

NAT(网络地址转换)

1.DNAT: 将外部目的IP地址映射到局域网中某个主机地址

2.SNAT: 将内部源IP地址转换为外部IP地址

3.MASQ: 将由该接口出去的源IP

步骤 3 配置 SNAT 规则参数。

表2-42 SNAT 参数说明

参数名称	含义	如何配置
NAT 规则	NAT 规则的转换类型。	下拉框选项 ☒ DNAT ☒ SNAT ☒ MASQ
规则名称	NAT 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 64 字节，输入规范请参见“5. 参数规范表”。
协议	针对哪种协议数据包做目的地址转换。	下拉框选项 ☒ TCP ☒ UDP ☒ TCP+UDP ☒ ICMP ☒ ALL
接口	选择 IP 数据包的目的地址为 H61XX 工业智能网关的某个接口。	下拉框选项 ☒ [brideg] lan ☒ [dhcp] wan ☒ [modem] 移动网络 ☒ [modem] 移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） ☒ wlan2g/5g (WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)

参数名称	含义	如何配置
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“5. 参 数规范表”。
初始端口	需要替换的源地址端口	手动输入 取值范围：1～65535
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“5. 参数规 范表”
映射端口	替换之后的源地址端口。	手动输入 取值范围：1～65535

步骤 4 点击“保存”，完成该条路由模式规则配置。



说明

当 DNAT 规则中协议选择“ALL”表示选择“TCP”、“UDP”、“ICMP”三种协议。

2.5.3.3. MASQ 规则配置

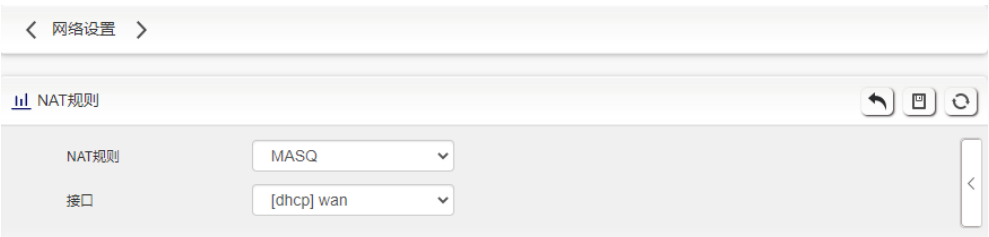
MASQ 也就是 MASQUIREADE，地址伪装，将所有经过 H61XX 工业智能网关转发的数据包源 IP 地址转换成用户设置的 IP 地址。H61XX 工业智能网关支持将数据包的源 IP 地址转换成 H61XX 工业智能网关的某个接口地址。

步骤 1 单击“网络设置>安全设置> NAT 规则”。

打开“NAT 规则”页签。

步骤 2 单击“NAT 规则”右上角“添加”按钮，选择“NAT 规则”为“MASQ”后。

图2-75 MASQ 配置页签



MASQ 的参数说明。

表2-43 MASQ 参数说明

参数名称	含义	如何配置
接口	选择某个接口作为 H61XX 工业智能网关及局域网与外部的通信地址	下拉框选项 ☒ [bridge]lan ☒ [dhcp]wan ☒ [modem] 移动网络 ☒ [modem] 移动网络 2（双模时支持） ☒ VPN 接口（配置 VPN 时支持） ☒ wlan2g/5g (WiFi 版本时，wlan 未与 bridge0 桥接且作 Station 时支持)

步骤 3 点击“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 H61XX 工业智能网关指定接口的 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 H61XX 工业智能网关页面将 MASQ 规则删除，则 H61XX 工业智能网关 LAN 侧的 PC 不能与外部进行通信。

2.5.4. 端口禁用

外网接口部分 TCP 和 UDP 端口是不能对外开放的，防止外部用户非法登录设备后台和网页，做出一些破坏性的操作，另外一些端口暴露在外面，也可能遭到一些非法用户的攻击，严重情况可能导致设备瘫痪。端口禁用，允许用户针对设备接口，选择性的过滤部分端口，确保设备在网络环境下的安全性。

IP 过滤规则配置步骤如下：

步骤 1 单击“安全设置>黑白名单>端口禁用”。部分接口添加了默认配置：

图2-76 端口禁用界面



默认情况，modem 和 wan 口添加了部分网络上容易被攻击的端口，用户也可以对这些端口做出调整

步骤 2 选择+添加黑白名单规则；

图2-77 端口禁用参数设置页面

步骤 3 配置完成，点击保存按钮

表2-44 端口禁用参数说明

参数名称	含义	如何配置
规则名称	端口禁用规则名称	手动输入 最大支持 64 个字符
接口	禁用端口设置	下拉框选项 下拉列表会显示当前设备上所有的接口，用户根据自身需求选择
协议	端口禁用生效协议设置	下拉框选项 ☒ TCP+UDP ☒ TCP ☒ UDP 默认选择 TCP+UDP
端口（80）	禁用 80 端口，80 端口为 web 登录端口，默认禁用	复选框 默认勾选，表示禁用
端口（22）	禁用 22 端口，22 端口为 SSH 登录端口，默认禁用	复选框 默认勾选，表示禁用

参数名称	含义	如何配置
端口（23）	禁用 23 端口，22 端口为 Telnet 登录端口，默认禁用	复选框 默认勾选，表示禁用
自定义禁用端口	自定义禁用的端口	手动输入 支持单个端口输入，如 100；也支持多个端口输入，如 1000-2000，或者 1000,2000

2.5.5. DDOS 防御

DDoS（分布式拒绝服务攻击）旨在通过大量恶意流量淹没目标系统，导致服务不可用。针对常见的 DDOS 攻击的类型，该功能可以开启对应的 DDoS 的防御。

步骤 1 单击“安全设置>黑白名单>DDOS 防御”。具体配置页面信息如下图所示；

图2-78 DDOS 防御配置页面



步骤 2 开启对应的防护功能后，点击保存

表2-45 DDOS 防御参数说明

参数名称	含义	如何配置
禁止 ping	开启后，外部设备不能对设备进行 ping 操作	复选框 默认不开启

参数名称	含义	如何配置
Fraggle	Fraggle 防御设置； Fraggle 攻击是一种 DDoS 攻击的变种，属于反射放大攻击类型，与 Smurf 攻击类似，但使用 UDP 协议（而非 ICMP）。攻击者伪造目标 IP 向网络广播地址发送 UDP 数据包（通常使用端口 7（echo），导致大量主机向目标返回响应流量，形成流量洪泛	复选框 默认不开启
Ip Land	Ip Land 防御设置； IP Land 攻击（Land Attack）是一种古老的拒绝服务（DoS）攻击，攻击者发送伪造的 TCP SYN 包，其中源 IP 和目的 IP 相同，导致目标系统陷入循环处理自己的请求，最终耗尽资源（如 CPU、内存）而崩溃或重启	复选框 默认开启
Echo Chargen	Echo Chargen 防御设置 Echo-Chargen 攻击是一种利用 UDP 协议的反射放大攻击，通过滥用两种古老的网络服务实现流量放大（通常使用 19（chargen）	复选框 默认不开启
端口防扫描	端口放扫描设置 端口扫描是网络侦察的基础手段，攻击者通过系统化探测目标开放端口，绘制网络服务地图，为后续攻击做准备	复选框 默认不开启
SYN 洪泛	SYN 洪泛防御设置 SYN 洪泛是典型的 DoS/DDoS 攻击，利用 TCP 协议三次握手缺陷消耗目标资源	手动设置 通过配置的值限制每秒建立连接的数量来进行防御 设置范围 0-5000



说明

- 默认不是所有的防御都打开的，防御都打开虽然确保了安全的时候，但也会产品的一些性能有一定的影响，所以需要结合自身实际的情况来进行设置

2.6. 应用中心

H61XX 工业智能网关支持二次开发，部分定制业务功能可以插件的形式安装到该设备，如 DTU、GPS 功能；部分定制功能可以容器的形式安装到该设备，如 AI 识别、工业协议功能。

2.6.1. 插件

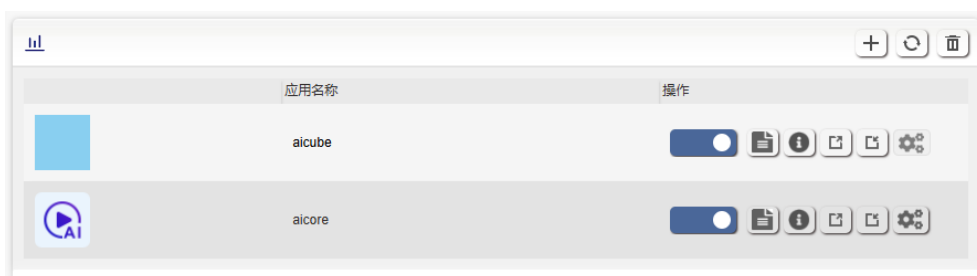
步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“应用中心”。

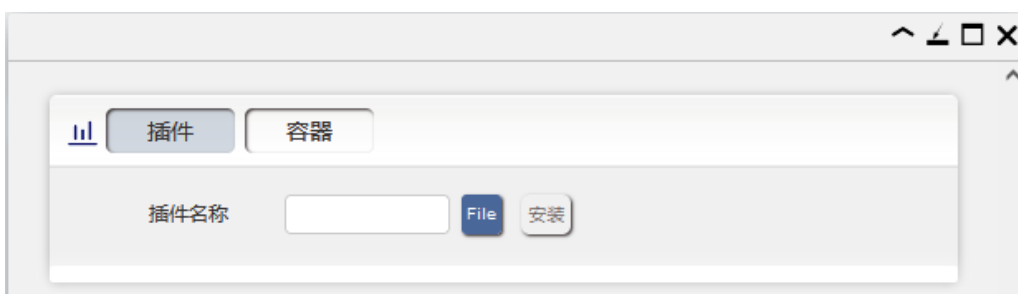
打开“应用中心”页签，如下图所示，插件安装后会显示在应用中心列表中。

图2-79 应用中心页签



步骤 3 若需添加新的插件，请单击右上角“添加”，进入插件安装界面。

图2-80 插件安装页签



2.6.2. 容器

容器安装

步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“应用中心”。

打开“应用中心”页签，容器安装后会显示在应用中心列表中。

步骤 3 若需添加新的容器，请单击右上角“添加”，默认进入本地容器安装页签，点击“仓库”，进入仓库容器安装页签。

图2-81 本地容器安装页签



图2-82 仓库容器安装页签



步骤 4 配置容器参数。

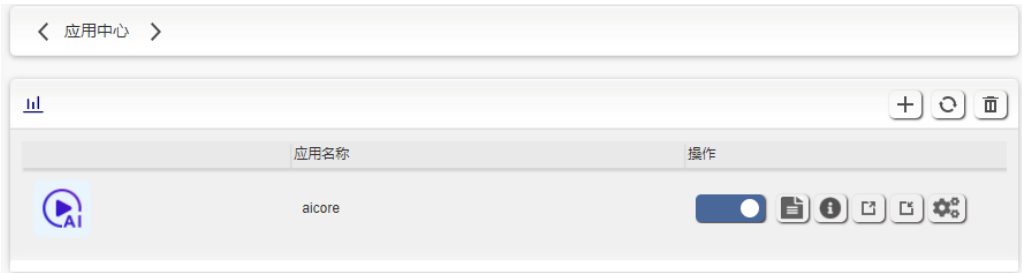
参数说明。

表2-46 添加容器参数说明

参数名称	含义	如何配置
本地基本设置		
初始配置	在已安装容器基础上更新时将容器配置初始化	勾选即初始化配置
镜像类型	全量包：包含容器所有文件。安装时在设备内有同名容器运行的情况下，会替换掉同名容器。 差分包：包含需要更新的文件。基线容器在设备内运行的情况下，对基线容器进行部分文件替换或者新增文件。 预装：包含容器所有文件。安装时在设备内有同名容器运行的情况下，会替换掉同名容器，并且将容器包备份记录。当设备恢复出厂时，预装包能自动恢复安装。	下拉选择不同镜像类型
镜像名称	实现需要功能对应的镜像文件。	选择本地对应的文件
映射端口	宿主机和容器之间的端口映射	左侧输入宿主机端口，右侧输入容器端口
映射目录	宿主机和容器之间的目录映射	左侧输入宿主机目录，右侧输入容器目录
容器名称	容器自定义名称，仅用于区分不同的容器。	最大长度为 64 位，输入规范请参见“规范参数表”。
仓库基本设置		
镜像名称	远程容器仓库的镜像名称。	<REPOSITORY:TAG>形式
高级选项	控制仓库配置的展示	点击按钮打开
仓库配置	配置远程容器仓库的路径、账号密码	——

步骤 5 点击“安装”，完成容器安装后退出，显示页签。

图2-83 容器安装页签



步骤 6 在“应用中心”对安装的插件或者容器，进行开关控制、查看日志、查看基本信息、打开设置、删除操作。

参数说明。

表2-47 容器操作参数说明

参数名称	含义	如何配置
开关	控制插件、容器功能的使能	单选择按钮。 ☒ 开 ☒ 关
日志	查看插件、容器的日志信息	进入日志页面，查看日志，下载和删除；可以分等级查看日志，分“ALL、ERR、WARN、INFO、DEBUG”。
基本信息	查看插件和容器的基本信息	查看应用名称、版本号、状态信息、应用大小、适应平台、安装时间、API、网络适配、用户权限、镜像名称、映射端口、映射目录、仓库配置、用户名、CPU 占用、内存占用基本信息。
设置	设置插件或者容器的相关应用	进入设置里添加插件、容器的配置，进行应用。

2.6.3. DTU

DTU 功能支持设备与单、多透明中心进行数据传输，支持带 DDP 封装的单、多中心传输方式进行数据传输。

2.6.3.1. TCP 或 UDP 透明传输

步骤 1 单击“应用中心>DTU”。

图2-84 DTU 配置页签

DTU

基本设置

身份识别码

13912345678

最大长度为11位

RTU的最大数据包

1024

* 30-1460

数据包间隔时间

300

* 10-2000毫秒

串口缓存

ON

详细报文开关

OFF

工作模式

多通道模式

串口选择

COM1

SM加密

开启

关闭

数据中心设置

通道1

通道2

通道3

通道4

连接状态

断开

通道连接方式1

UDP+DDP

IP地址1

0.0.0.0

如：192.168.8.1

域名1

最大长度为32位

端口1

5002

* 1-65535

本地端口1

1-65535

自定义注册包1

最大长度为128位

最大注册次数1

5

* 1-255

自定义心跳包1

最大长度为128位

心跳包发送时间间隔1

30

* 0或5-65535

表2-48 DTU 配置参数说明

基本设置		
身份识别码	终端标识身份识别码，用于区分DTU 客户端。	手动输入，最大长度不超过 11 位。 一般设置为 WORD 型字符串，输入规范请参见“参数规范表”。
RTU 最大数据包	DTU 串口接收来自数据中心数据时的最大包长度	手动输入。 取值范围：30~1460
数据包间隔时间	DTU 串口接收来自数据中心数据时的等待超时时间。 在不超过接收包的最大包长范围内，在这个时间内读取数据，若有数据，则一直读取，且一次性显示这个时间内读取的数据；若没有数	手动输入。 取值范围：10~2000 单位：毫秒

	据，大于超时时间后，则认为读取数据完毕，显示到 DTU 端串口工具。	
串口缓存	通道断开后是否进行数据缓存，开启缓存则在通道重连成功后发送缓存数据；最大缓存 8 帧*1460 字节数据。	下拉框选择 • ON • OFF
详细报文开关	日志是否打印报文详细内容	下拉框选择 • ON • OFF
工作模式	选择对应支持的通道模式： 多通道模式：支持 1-4 路数据中心同时进行数据收发； 主备模式：其中 1、2 为主通道，3、4 为备通道，主通道断连会切到备通道，并一直重连主通道，主通道连接成功立刻断开备通道； 轮询模式：默认连接通道 1，若通道 1 重连则切到通道 2，通道 2 重连则切到通道 3，以此类推； 互备模式：其中 1、2 为主通道，3、4 为备通道，主通道断连会切到备通道，只有备通道断连才切主通道；	下拉框选择 • 多通道模式 • 主备模式 • 轮询模式 • 互备模式
串口选择	可选择任意串口传输数据。	下拉框选择 • COM1 • COM2
数据中心设置		
通道连接方式	DSC 和 DTU 的通讯方式	下拉框选择。 • TCP • UDP • TCP+DDP • UDP+DDP • TCP_SER
IP 地址	DSC 的固定 IP 地址方式	A.B.C.D 接口型或一般 WORD 型，输入规范请参见“参数规范表”。
域名	DSC 的域名	WORD 类型，输入规范请参见“参数规范表”。
端口	进行测试/调试的 IP 地址对应的端口号。	手动输入。 取值范围：1~65535
本地端口	DTU 绑定的本地端口	手动输入。 取值范围：1~65535
自定义注册包	支持自定义注册包内容，配置为十六进制时需要以"0x"或"0X"开头为标志位。	手动输入。 最大输入长度：128 位

最大注册次数	客户端 DTU 与服务器端在注册失败后尝试注册的最大次数设置。	手动输入。 取值范围：1~255
自定义心跳包	支持自定义心跳包内容，配置为十六进制时需要以"0x"或"0X"开头为标志位。	手动输入。 最大输入长度：128 位
心跳包发送时间间隔	设置心跳发送间隔时间（无数据发送时，每隔这个时间，发出心跳内容一次）配置 0 则不发心跳。	手动输入。 取值范围：0 或 5~65535 单位：秒

图2-85 DTU 高级设置页签

高级设置 隐藏

RDP协议开关

OFF

DTU下行协议

NONE

通道重连间隔

60

重试次数

5

通道数据检测

0

ICMP检测地址

TCP链接维护

启用

禁用

TCP心跳检测时间

30

TCP心跳检测间隔

10

TCP心跳检测次数

3

协议缓存超时

2

最大长度为32位

表2-49 DTU 高级设置配置说明

高级设置		
RDP 协议关 关	通过 RDP 协议设置参数和查询参 数	下拉框选择。 • OFF（默认） • ON
DTU 下行协 议	配置 GPRS 则下行数据遵循 RDP 协议组包	下拉框选择。 • NONE（默认） • GPRS ON
通道重连间 隔	客户端 DTU 与服务器端在连接失 败后重新建立连接的时间间隔。	手动输入。 取值范围：1~65535 单位：秒
重连次数	客户端 DTU 与服务器端在连接失 败后尝试连接的最大次数设置。	手动输入。 取值范围：1~65535 单位：次
通道数据检 测	0 表示通道一直无数据不会重拨 号； 配置数值则表示固定数值时间内通 道无数据则会重拨号；	手动输入。 取值范围：0~65535 单位：分
ICMP 检测地 址	UDP 通道 ICMP 检测的地址	手动输入。 最大输入长度：32 位
TCP 链接维 护	TCP Keepalive 开关。	下拉框选择。 • 启用（默认） • 禁用

TCP 心跳检测时间	TCP Keepalive 正常有回应情况下的心跳间隔时间	手动输入。 取值范围：1~13767 单位：秒
TCP 心跳检测间隔	TCP Keepalive 无回应包情况下的心跳间隔时间	手动输入。 取值范围：1~13767 单位：秒
TCP 心跳检测次数	TCP Keepalive 无回应包情况下达到检测次数则断开连接	手动输入。 取值范围：1~127 单位：秒
协议缓存超时	RDP 和 DDP 的缓存时间，默认 2s	手动输入。 取值范围：1~65535 单位：秒

步骤 2 进行透明 TCP 或 UDP 传输时，通道需要配置通道连接方式、IP 地址和端口，其它参数在非必要情况下可保持默认值，配置完成后，点击保存并启用功能个输入。

图2-86 单中心透明方式参数配置

数据中心设置

通道1

通道2

通道3

通道4

连接状态

断开

通道连接方式1

TCP

IP地址1

183.238.239.220

如：192.168.8.1

域名1

最大长度为32位

端口1

51590

* 1-65535

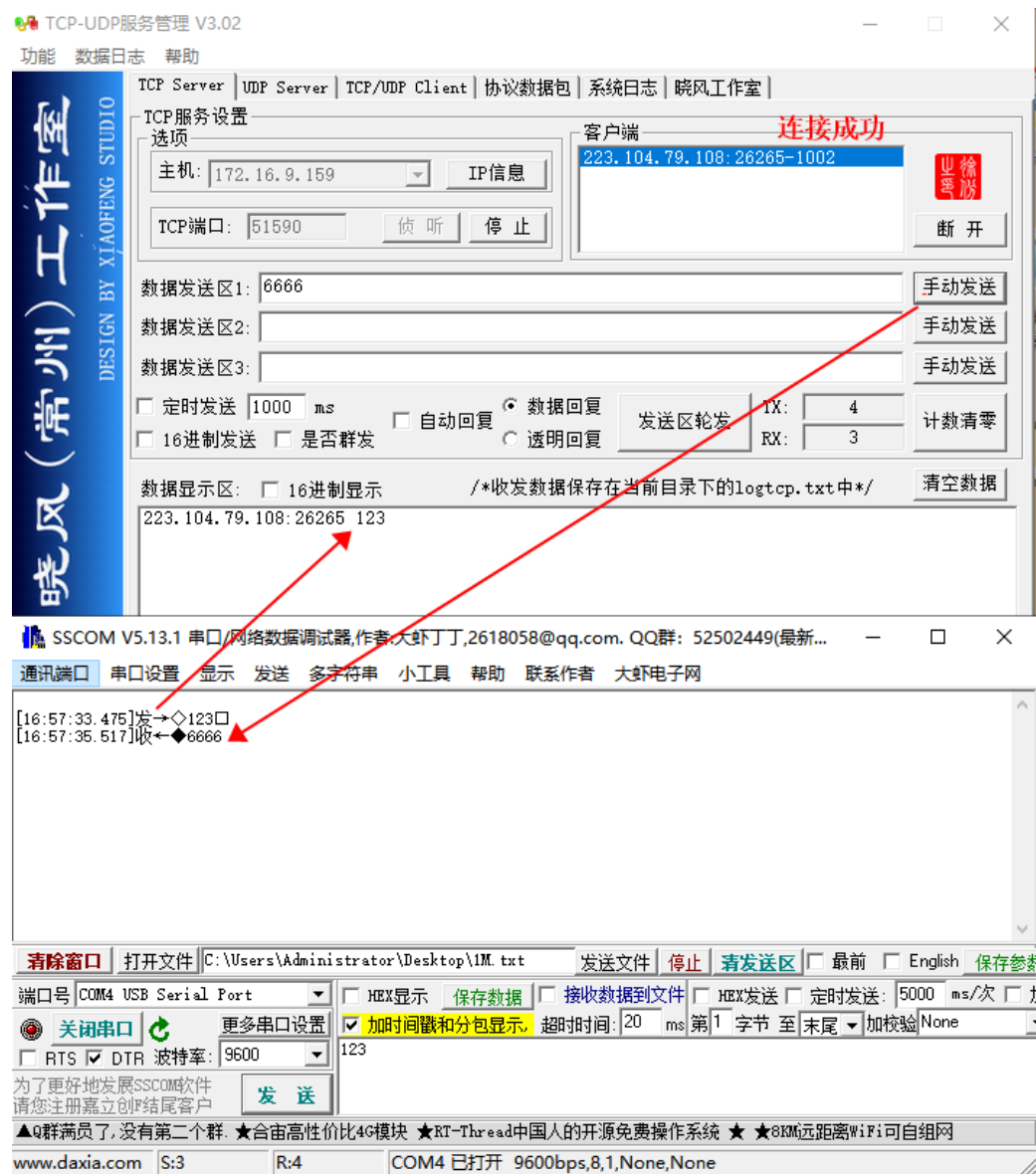
步骤 3 启动“TCP-UDP 服务管理 3.2.exe”，选择“TCP Server”页签，配置对应的地址和端口，点击侦听。

表2-50 服务端参数说明

参数名称	配置说明
主机	您进行测试/调试的 PC 对应的公网 IP 地址。
端口	您进行测试/调试的 PC 的 IP 地址对应的端口号。 如果该 IP 地址为非公网 IP，则需要贵司 IT 部门协助做 NAT 端口映射，或者联系我司技术人员。

步骤 4 待 DTU 与“TCP-UDP 服务管理 3.2.exe”连接成功，在“客户端”显示设备连接信息，此时使用串口 SSCOM 工具进行发送数据，数据中心可收到数据；数据中心发送数据，串口工具可收到数据。

图2-87 TCP 通道数据收发



2.6.3.2. DDP 封装传输

步骤 1 UDP+DDP/TCP+DDP 是较透传更安全的传输方式，数据在透明传输的基础上封装了我司定义的 DDP 协议。通道参数的配置方法同其它传输方式（如 TCP 传输方式），以配置 UDP+DDP 为例，配置完成后，点击保存并启用功能。

步骤 2 启动无线数据中心演示 Demo，选择“设置>服务设置”，打开服务设置窗口

图2-88 DDP 服务端参数配置

设置

×

服务设置

文件设置

串口设置

颜色设置

蜂鸣设置

服务类型

☒ UDP ☐ TCP

终端注册时间间隔

3 (分钟)

☒ 指定IP

172.16.9.159

服务端口

取值范围: 1-65535 51590

启动类型

☐ 手工启动 ☒ 自动启动

等待时间

600

链接名称

确定(C)

取消(C)

步骤 3 在界面右下角单击“确定”，退回到无线数据中心演示系统 Demo 主界面，单击左上角启动按钮“”，待无线数据中心演示系统 Demo 和工具箱调试窗口分别显示如下图所示信息表示 DTU 已经成功注册到中心，即可以通过串口工具进行数据收发。

图2-89 DDP 封装通道数据收发



2.6.4. 国密 SSL

国密 SSL 功能仅支持结合 DTU 功能使用，加密方式支持 SM2 和 SM4。

2.6.4.1. SM2

步骤 1 单击“应用中心>国密 SSL”

图2-90 SM2 配置页签

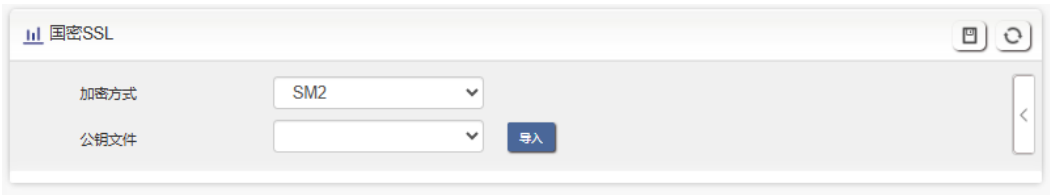


图2-90展示了“国密SSL”配置页签的界面。该界面包含两个配置项：

- 加密方式**：下拉菜单，当前选择为“SM2”。
- 公钥文件**：下拉菜单，右侧有一个“导入”按钮。

 界面顶部有“国密SSL”标题和刷新、保存图标。右侧有一个垂直滚动条。

表2-51 SM2 配置参数说明

基本设置		
加密方式	数据采用的加密方式	可选择 SM2、SM4
公钥文件	加密使用的公钥，需与解密对端设备的密钥匹配	

步骤 2 在“应用中心>DTU”配置中，需要启用“SM 加密”

图2-91 DTU 中启用 SM 加密



图2-91展示了“DTU”配置页签的“基本设置”部分。配置项如下：

- 身份识别码**：输入框，值为“13912345678”，右侧提示“最大长度为11位”。
- RTU的最大数据包**：输入框，值为“1024”，右侧提示“* 30-1460”。
- 数据包间隔时间**：输入框，值为“300”，右侧提示“* 10-2000毫秒”。
- 串口缓存**：下拉菜单，选择“ON”。
- 详细报文开关**：下拉菜单，选择“OFF”。
- 工作模式**：下拉菜单，选择“多通道模式”。
- 串口选择**：下拉菜单，选择“COM1”。
- SM加密**：位于底部，被红色框选中。包含两个单选按钮：“开启”（当前选中）和“关闭”。

 界面顶部有“DTU”标题、开关图标、刷新、保存图标。右侧有一个垂直滚动条。

注意：SM2 只加密小于等于 255 字节长度的数据，发送数据长度大于 255 字节时，以明文发送

2.6.4.2. SM4

步骤 1 单击“应用中心>国密 SSL”，SM4 配置。

图2-92 SM4 配置页签

国密SSL

加密方式

SM4

运算模式

CBC

填充方式

PKCS7

偏移

* 32位的16进制字符串

密钥

* 32位的16进制字符串

表2-52 SM2 配置参数说明

基本设置		
运算模式	SM4 加密的工作模式	仅支持 CBC（密码块链接）
填充方式	SM4 使用 CBC 加密时，对明文进行填充的方式	仅支持 PKCS7，填充后其长度为 16 的倍数
偏移	SM4 第一个数据块用来异或（其他的数据块都是和上一个数据块异或）	32 位 16 进制字符
密钥	SM4 加密密钥，需与解密对端设备的密钥匹配	32 位 16 进制字符

步骤 2 在“应用中心>DTU”配置中，需要启用“SM 加密”

2.6.5. LBS

LBS 是利用定位技术提供位置相关服务的技术，支持北斗、GPS 或北斗&GPS（视定位芯片能力而定）

步骤 1 单击“应用中心>LBS”。

图2-93 LBS 配置页签

LBS

传输协议

TCP

UDP

工作模式

北斗

本地端口

1-65535

服务地址

最大长度为64位

服务端口

1-65535

发送包头

最大长度为64位

发送包尾

最大长度为64位

上报间隔

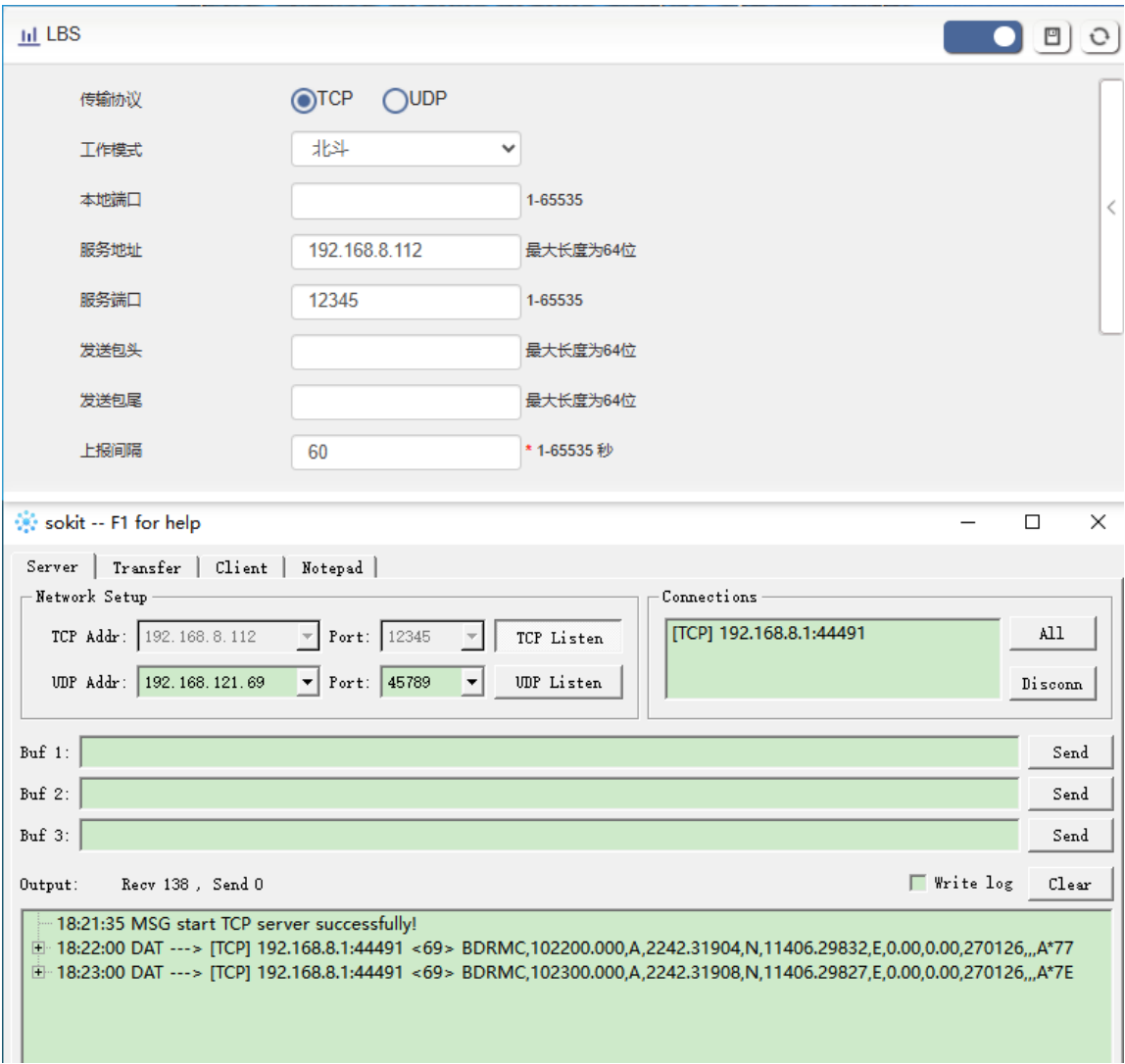
60

* 1-65535 秒

表2-53 LBS 配置参数说明

参数名称	含义	如何配置
传输协议	数据传输使用的协议	可选 TCP 或 UDP
工作模式	定位采用的模式	可选择北斗、GPS 或北斗 &GPS
本地端口	用于上报 LBS 数据的本地端口	取值范围：1～65535
服务地址	LBS 服务器的 IP 地址或域名	一般 WORD 类型/CODE 类型，最大 64 个字节，输入规范请参见“5. 参数规范表”。
服务端口	LBS 服务器使用的端口，与服务器匹配即可	取值范围：1～65535
发送包头	定位数据报文头部设置的内容	一般 WORD 类型/CODE 类型，最大 64 个字节，输入规范请参见“5. 参数规范表”。
发送包尾	定位数据报文尾部设置的内容	一般 WORD 类型/CODE 类型，最大 64 个字节，输入规范请参见“5. 参数规范表”。
上报间隔	LBS 数据报文上报的间隔	取值范围：1～65535 秒

- 步骤 2 进行 TCP 或 UDP 传输时，需要配置服务地址和服务端口，其它参数可保持默认，配置完成后保存并启用 LBS 功能。
- 步骤 3 启动 sokit 工具，选择“TCP Server”页签，配置对应的地址和端口，点击侦听。



2.6.6.Dedgebus 配置

Dedgebus 配置仅支持结合工业协议功能使用，主要用途为：使用网关配置工具实现远程管理设备。

步骤 1 单击“应用中心>Dedgebus 配置”，配置如图 1-13 所示，参数说明如表 1-13 所示。

图2-94 Dedgebus 配置页签

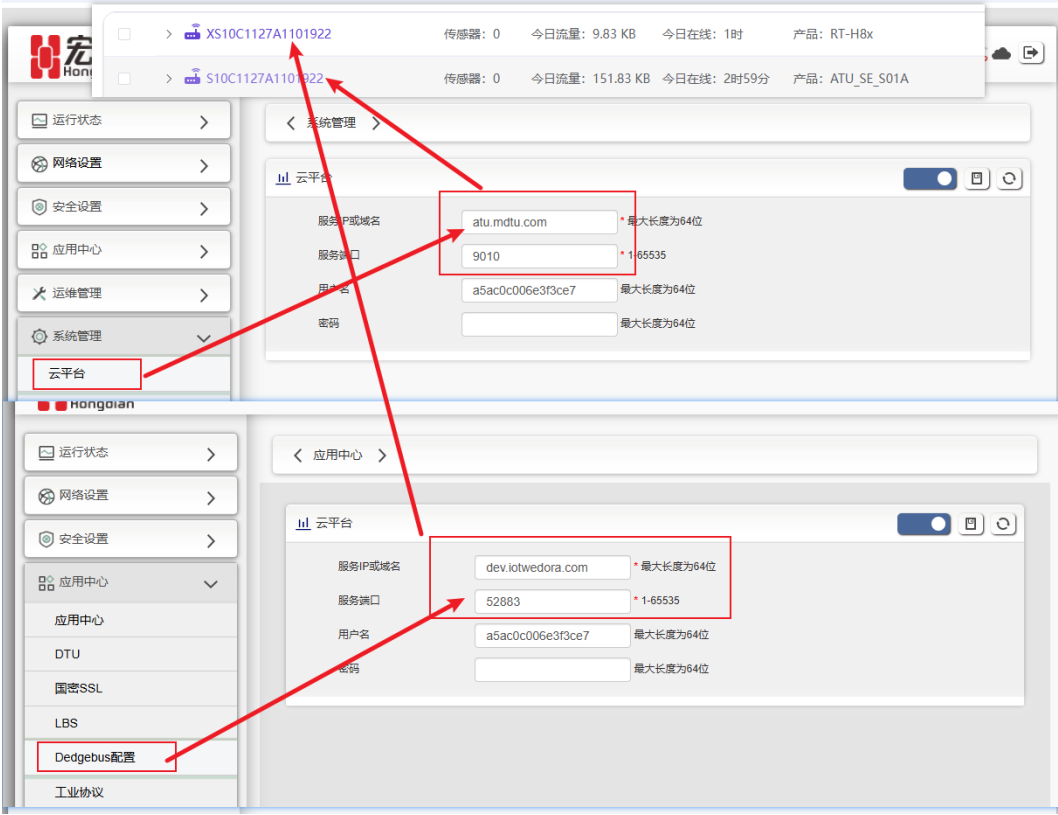


表2-54 Dedgebus 配置参数说明

参数名称	含义	如何配置
启用/禁用	使能云平台服务，云平台功能需要配合我司网关配置工具使用。	单选按钮 ☒ 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 MQTT 服务所使用的端口号，与服务器匹配即可。	取值范围：1~65535
用户名/密码	设备与云平台服务器建立连接所需的用户名/密码，适用于需要鉴权认证的 MQTT 协议连接。	一般 WORD 类型/CODE 类型，最大 64 个字节，输入规范请参见“参数规范表”。

步骤 2 使用默认配置连接平台，通过在 SN 前增加 X 实现平台兼容，平台增加设备时，需在 SN 号前加 X，并选择产品为 RT-H8x。

图2-95 Dedgebus 配置与云平台配置



2.6.7.工业协议

工业协议功能目前支持 43 个协议库，支持历史数据库导出、工业协议配置导入导出、协议库更新等。

步骤 1 单击“应用中心>工业协议>基础云配置”，配置如图 1-13 所示，参数说明如表 1-14 所示。

图2-96 工业协议业务配置页签

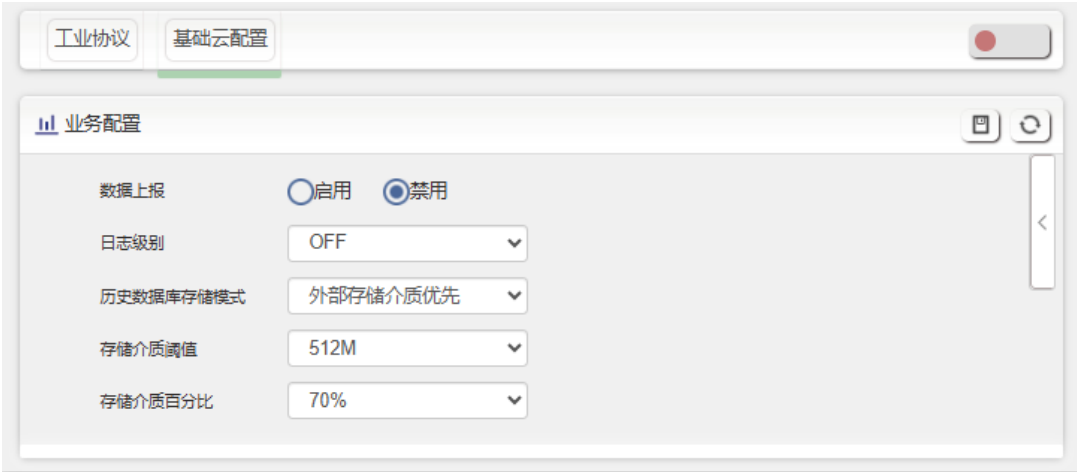


表2-55 工业协议业务配置配置参数说明

参数名称	含义	如何配置
启用/禁用	使能工业协议服务。	单选按钮 ☒ 启用 ☒ 禁用
业务设置		
数据上报	使能数据上报功能（启用后可通过网关配置工具实现远程管理设备）	单选按钮 ☒ 启用 ☒ 禁用
上报策略	上报数据的策略（配合数据上报使用）	支持最新值上报、变化上报、原始值上报
上报间隔	上报数据的间隔（配合数据上报使用）	取值范围：1～65535
组包大小	数据上报组包的条数（配合数据上报使用）	取值范围：1～200 条
日志级别	工业协议日志的级别选择，默认关闭	可选 OFF/DEBUG/ERROR/INFO
历史数据库存储模式	存储历史数据的介质选择	可选外部存储介质优先/内部存储介质优先/仅适

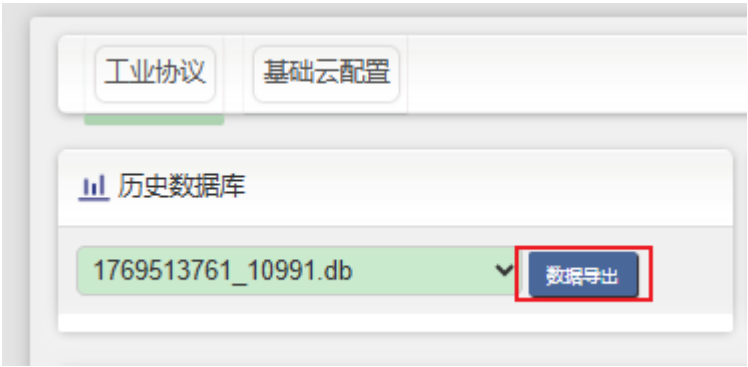
参数名称	含义	如何配置
		用内部存储介质
存储介质阈值	只针对外部存储生效，当外部存储空间大于该阈值优先保存到外部存储，小于该阈值则保存到内部存储	可选 128M/256M/512M/1G
存储介质百分比	前提：历史数据保存在外部存储；当历史数据文件占外部存储的总空间为该百分比时，开启覆盖存储	可选 10%-90%

历史数据存储备注：

- (1) 先判断是否有外部存储（U 盘、TF 卡），如果有，优先存到外部存储
- (2) 若无外部存储，会继续判断 data 目录是否有大于 1M 的空间，若有，则存到 data 目录下 (/data/history
- (3) 若 data 空间小于 1M，则会存储到/tmp/industry/history 目录下
- (4) /tmp 下为历史数据划分 5M 的空间，若总的历史数据大于 5M 则覆盖，且每个 db 文件大小不超过 1M

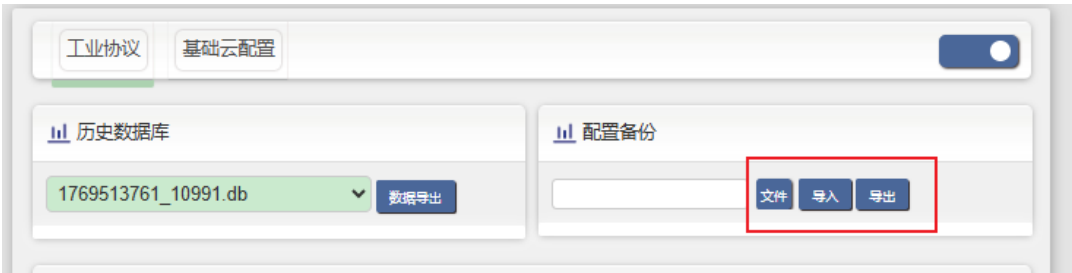
步骤 2 单击“应用中心>工业协议”，可通过图 1-15 所示点击“数据导出”则可导出历史数据库

图2-97 历史数据导出



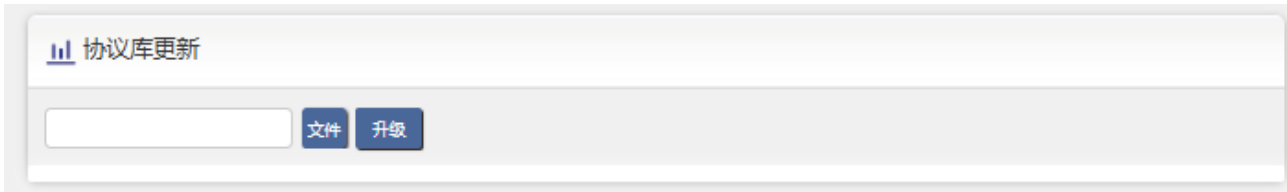
步骤 3 单击“应用中心>工业协议”，可通过图 1-16 所示选择工业协议配置文件，点击导入即可；点击导出可导出当前设备的工业协议配置文件

图2-98 配置文件导入导出



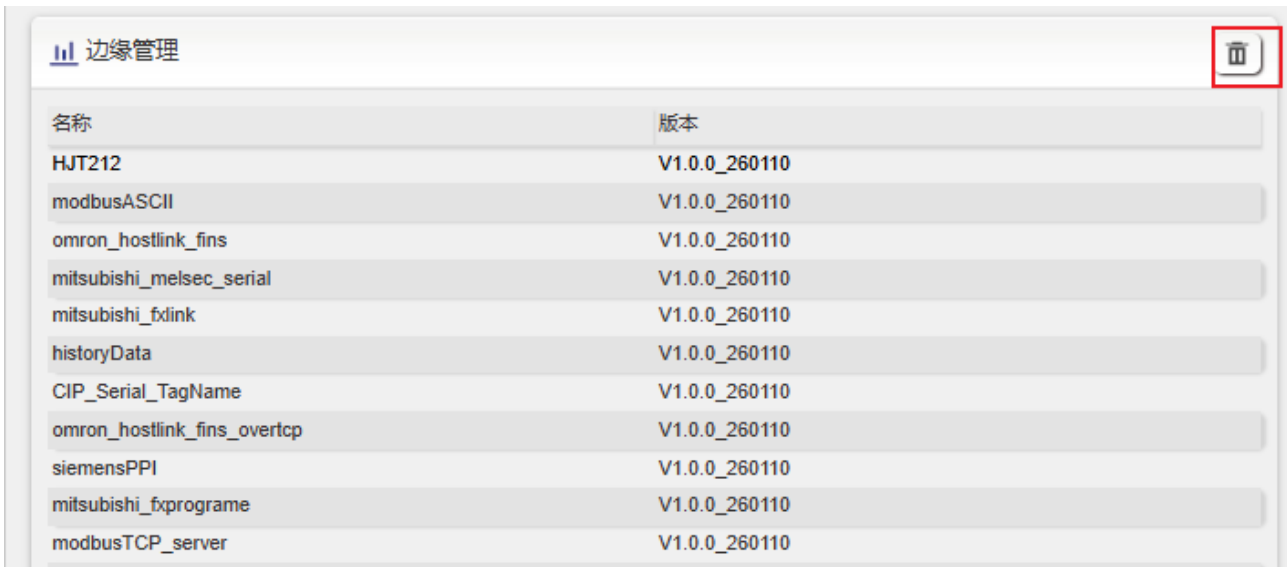
步骤 4 单击“应用中心>工业协议”，可通过图 1-17 所示选择工业协议补丁包文件，点击升级即可更新协议库

图2-99 协议库更新



步骤 5 单击“应用中心>工业协议”，可通过图 1-18 所示，点击“删除”图标，可删除当前协议库

图2-100 协议库删除



名称	版本
HJT212	V1.0.0_260110
modbusASCII	V1.0.0_260110
omron_hostlink_fins	V1.0.0_260110
mitsubishi_melsec_serial	V1.0.0_260110
mitsubishi_fxlink	V1.0.0_260110
historyData	V1.0.0_260110
CIP_Serial_TagName	V1.0.0_260110
omron_hostlink_fins_overtcp	V1.0.0_260110
siemensPPI	V1.0.0_260110
mitsubishi_fxprograme	V1.0.0_260110
modbusTCP_server	V1.0.0_260110

2.7. 运维管理

H61XX 工业智能网关运维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。

2.7.1. 网络诊断

网络诊断，包括常用的网络检测功能和网络追踪功能，具体使用步骤如下：

- 步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。
登录方法请参见“2.2 登录 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。

图2-101 网络诊断配置页签

< 运维管理 >

PING功能

目的地址

Ping

TRACERT功能

目的地址

Tracert

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 H61XX 工业智能网关与目的地址的连通性，几秒钟后界面弹出检测结果。

参数和按钮说明。

表2-56 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 H61XX 工业智能网关到达目的地址的跳数。	单击该按钮即可使用 Tracert 命令。

说明

Tracert：即 traceroute，通过 Traceroute 我们可以知道信息从的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。

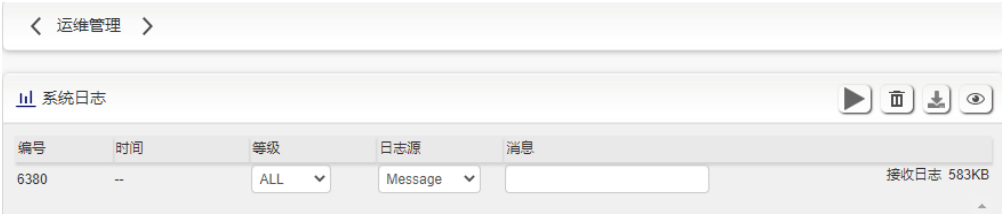
---结束

2.7.2. 本地日志

本地日志是指通过在 H61XX 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 H61XX 工业智能网关 WEB 配置界面。
- 登录方法请参见“2.2 登录 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。

图2-102 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，单击右上角“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 H61XX 工业智能网关运行日志，用户一般只适用系统日志。
- Preinstal：插件安装日志，记录 H61XX 工业智能网关安装插件的状态信息
- Api：应用程序日志，记录 H61XX 工业智能网关进程的开启或关闭等信息。
- Sm_trace：系统监控日志，打印系统监控信息，查看 CPU 状态信息，一般由研发人员查看参考。

---结束

2.7.3. 远程日志

“远程日志”主要用于连接远程日志服务器，H61XX 工业智能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：

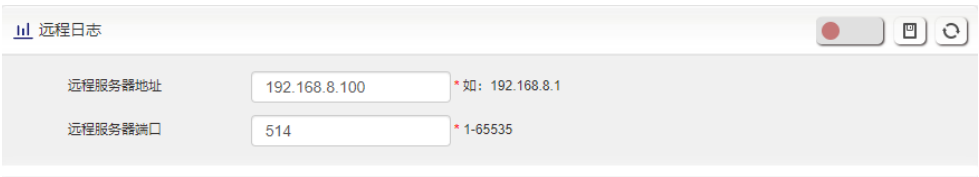
步骤 4 登录 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 5 单击“运维管理>远程日志”。

打开“远程日志”页签。

图2-103 远程日志页签



步骤 6 配置系统日志参数。

参数说明。

表2-57 系统日志参数说明

参数名称	含义	如何配置
启用/禁用	启用/禁用远程日志。	单击“启用”即可启用系统日志功能。

参数名称	含义	如何配置
远程服务器地址	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 7 点击“保存”，完成系统日志参数配置。



说明

在 H61XX 工业智能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 H61XX 工业智能网关、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

2.8. 系统管理

2.8.1. 云平台

H61XX 工业智能网关通过 MQTT 协议（Message Queuing Telemetry Transport）实现与宏电云服务平台的通信功能，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，如设备状态监控、流量监控、软件升级、参数配置、设备定位等，同时支持 DFS 云穿透、VPN 组网、支持远程下位机管理。宏电云服务默认为启用状态，具体设置说明如下。

步骤 8 登录 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 9 单击“系统管理>云平台”。

打开“云平台”页签。

图2-104 云平台配置页签

< 系统管理 >

云平台

服务IP或域名: wh.mapali.cn * 最大长度为64位

服务端口: 51553 * 1-65535

用户名: hd 最大长度为64位

密码: ●● 最大长度为64位

心跳间隔: 60 1-65535

步骤 10 配置云平台参数。

参数说明。

表2-58 云平台参数说明

参数名称	含义	如何配置
启用/禁用	使能云平台服务，云平台功能需要配合我司下位机管理工具使用。	单选按钮 ☒ 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“5. 参数规范表”。
服务端口	设备云平台服务器 MQTT 服务所使用的端口号，与服务器匹配即可。	取值范围：1~65535
用户名/密码	设备与云平台服务器建立连接所需的用户名/密码，适用于需要鉴权认证的 MQTT 协议连接。	一般 WORD 类型/CODE 类型，最大 64 个字节，输入规范请参见“5. 参数规范表”。
心跳间隔	设备与云平台维持链路稳定的心跳包发送时间间隔。	手动输入 取值范围：1~65535 单位：秒 默认值：60

步骤 11 点击“保存”，完成云平台配置。

---结束

2.8.2. TR069

TR069 是一种远程管理协议，也称为 CPE WAN 管理协议（CWMP），它允许互联网服务提供商（ISP）通过自动配置服务器（ACS）对客户端设备（CPE）进行远程管理和配置。这些设备包括家庭网关、路由器、调制解调器等

步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 2 单击“系统管理>RT069 配置”，进行 TR069 参数配置。

图2-105 TR069 配置页签

系统管理

TR069

数据模型

TR-098

TR-181

ACS用户名

最大长度为64位

ACS密码

最大长度为64位

ACS地址

* 最大长度为64位

定期上报周期

300

0-65535

CPE用户名

最大长度为64位

CPE密码

最大长度为64位

CPE接口

认证方式

基本认证

摘要认证

XMPP

禁用

启用

表2-59 TR069 配置参数说明

参数名称	含义	如何配置
数据模型	TR-098 主要用于互联网网关设备，如家庭路由器； TR-181 适用于启用 TR-069 的终端设备，例如调制解调器、机顶盒等	下拉框选项 ☒ TR-098 ☒ TR-181
ACS 用户名	管理服务器用户名	手动输入，最大长度为64 位
ACS 密码	管理服务器密码	手动输入，最大长度为64 位
ACS 地址	管理服务器地址	格式：A.B.C.D 接口型，输入规范请参见“参数规范表”。
定期上报周期	数据上报周期	取值范围：0~65535 缺省：300
CPE 用户名	终端连接用户名	手动输入，最大长度为64 位
CPE 密码	终端连接密码	手动输入，最大长度为64 位
CPE 接口	连接服务器所用的外网接口	下拉框选择 ☒ Lan ☐ Wan ☐ Wlan ☐ Modem
认证方式	基本认证：用户名和密码以 Base64 编码的形式在网络中传输 摘要认证：此方法通过使用 MD5 等	手动选择 基本认证 摘要认证（默认）

参数名称	含义	如何配置
	哈希算法对密码进行加密，不会在网络上传输明文密码 摘要认证相比基本认证具有更高的安全性	
XMPP	XMPP 技术在 TR069 中的应用主要体现在协助通信方面，通过使用 XMPP，可以更好地实现 TR069 的私网穿越功能，从而提高设备管理的效率和可靠性	下拉框选择 ☒ 禁用（默认） ☒ 启用

2.8.3.SNMP

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 3 登录 H61XX 工业智能网关 WEB 配置界面。
登录方法请参见“2.2 登录 WEB 配置界面”。
- 步骤 4 单击“系统管理>SNMP 配置”，进行 SNMP 参数配置。

图2-106 SNMP 配置页签

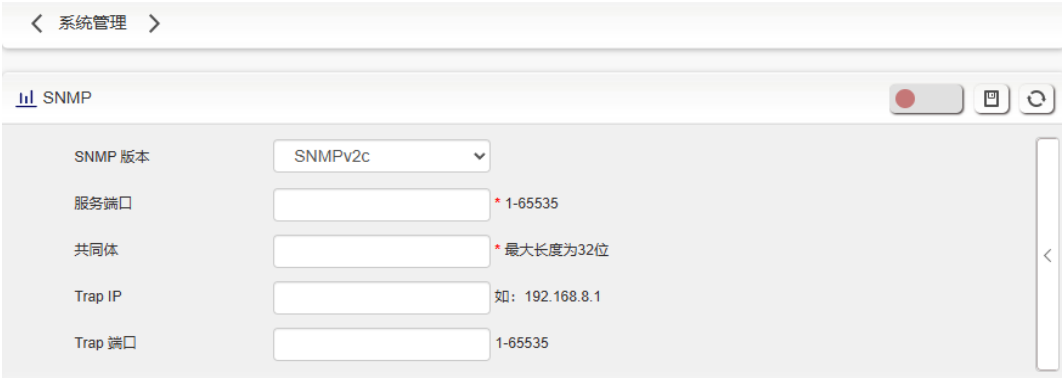


表2-60 SNMP 配置参数说明

参数名称	含义	如何配置
SNMP 版本	SNMP 的不同版本。	下拉框选项 ☒ SNMPv1 ☒ SNMPv2c ☒ SNMPv3
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 客户端连接设备 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	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	链路状态上报的服务器端口。	取值范围：1~65535 缺省：162

--结束

2.8.4.硬件配置

H61XX 工业智能网关支持 2 个串口，硬件配置可对两个串口的波特率、校验位、数据位和停止位进行配置管理。

- 步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。
- 登录方法请参见“2.2 登录 WEB 配置界面”。
- 步骤 2 单击“系统管理>硬件配置”。
- 打开“硬件配置”页签。

图2-107 硬件配置页签



- 步骤 3 单击 COM 口右侧“编辑”按钮，配置串口参数。

图2-108 串口参数配置页签

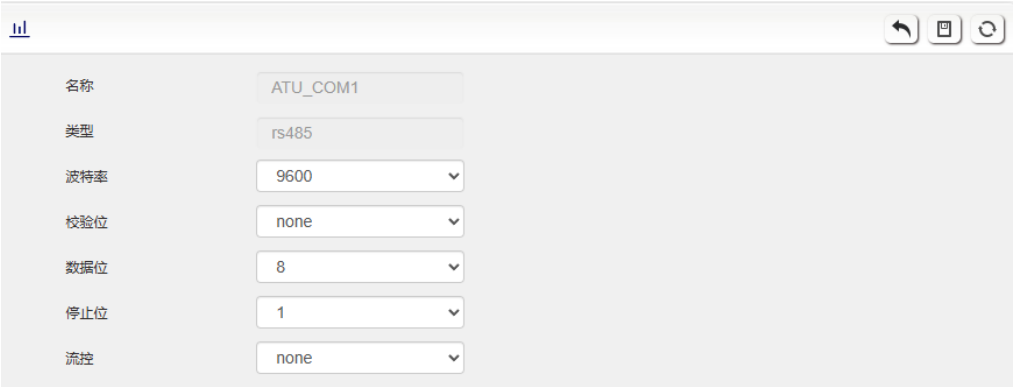


表2-61 硬件配置参数说明

参数名称	含义	如何配置
名称	串口的名称标识，用于区分设备串口。	H61XX 工业智能网关支持 2 个串口，名称分别为 ATU_COM1、ATU_COM2，不可配置。
波特率	串口数据传输速率。	下拉列表选择。 根据 DTU 的实际串口要求设置。 取值范围：300～115200 默认值：9600 单位：bps
校验位	数据校验方式。	下拉框选项 ☒ none ☒ even ☒ odd 根据 DTU 的实际串口要求设置。 默认值：None (无校验)
数据位	数据传输位。	下拉框选项 ☒ 5 ☒ 6 ☒ 7 ☒ 8 根据 DTU 的实际串口要求设置。 默认值：8
停止位	数据停止位。	下拉框选项 ☒ 1 ☒ 2 根据 DTU 的实际串口要求设置。 默认值：1

步骤 4 点击“保存”，完成硬件配置参数配置。

若硬件支持接入拓展板，则支持动态识别串口，拓展板的串口默认流控配置为 hardware，主板的串口默认流控为 none。

图2-109 动态识别串口显示

硬件配置							
串口							
名称	类型	波特率	校验位	数据位	停止位	流控	操作
ATU_COM1	rs485	9600	none	8	1	none	
ATU_COM2	rs232	9600	none	8	1	none	
EXT1_COM1	rs485	9600	none	8	1	hardware	
EXT1_COM2	rs485	9600	none	8	1	hardware	

2.8.5.计划管理

H61XX 工业智能网关计划管理能够为用户提供 H61XX 工业智能网关在线时长、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 H61XX 工业智能网关 WEB 配置界面。
- 登录方法请参见“2.2 登录 WEB 配置界面”。
- 步骤 2 单击“系统管理>计划管理”。
- 打开“计划管理”页签。

图2-110 计划管理配置页签

计划管理

任务名称

* 最大长度为12位

任务类型

移动网络 上线

设置时间

时间类型

range

时钟

:

-

:

* 如: 00:00-23:59

天数

-

如: 01-31

星期

-

如: 1-7

- 步骤 3 配置计划管理规则参数。

表2-62 任务管理规则参数说明

参数名称	含义	如何配置
启用/禁用	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。	单选框选择。 ☒ 启用 ☒ 禁用

参数名称	含义	如何配置
	间任务控制。	
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。	WORD 类型，最大长度为 12 位，输入规范请参见“5. 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移动网络处于上线状态（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 ☒ 移动网络 上线 ☒ 移动网络 2 上线（双模时支持） ☒ 重启 ☒ 自定义 选择“自定义”，则显示“命令”参数，需要用户输入命令（可以是 dial up 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“5. 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
当“时间类型”选择“interval”时		

参数名称	含义	如何配置
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 4 点击“保存”，完成计划管理服务配置。



说明

当计划管理的时间类型为“range”时，则必须先开启“系统时间”，即 NTP 服务（计划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“”。

因考虑到移动网络的稳定性，H61XX 工业智能网关有多个对移动网络操作的功能，如计划管理、链路备份、链路检测等，其中计划管理是改变保持移动网络状态，而其它功能则是改变移动网络状态但并不保持，故在使用计划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

2.8.6. 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 H61XX 工业智能网关的 WEB 访问端口，屏蔽其他用户访问路由。

- 步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。
- 登录方法请参见“2.2 登录 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。

图2-111 用户管理页签



- 步骤 3 点击“用户名”右侧的“编辑”按钮，可对用户名/密码进行配置操作，用户管理配置页签。

图2-112 用户管理配置页签

用户管理

用户等级

超级用户

新用户名

* 最大长度为64位

新密码

* 最大长度为64位

确认新密码

* 最大长度为64位

步骤 4 配置用户管理参数。

参数说明。

表2-63 用户管理参数说明

参数名称	含义	如何配置
用户级别	登录 H61XX 工业智能网关的用户级别。分为“超级用户”和“游客用户”，不可配。	
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“5. 参数规范表”。
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“5. 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“5. 参数规范表”。
端口	用户登录 H61XX 工业智能网关页面端口。	手动输入 取值范围 1~65535 默认值：80

步骤 5 修改完毕后点击“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。

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 H61XX 工业智能网关的 IP 地址就可以登录 H61XX 工业智能网关页面；若端口修改为其他数字且修改成功，则需要输入 H61XX 工业智能网关的“IP：端口”才能登录 H61XX 工业智能网关页面。

admin 用户只能修改 admin 本身的密码，但不能修改 guest 的密码和参数；guest 本身没有用户管理功能。

---结束

2.8.7.系统时间

H61XX 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 H61XX 工业智能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 5 登录 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 WEB 配置界面”。

步骤 6 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，展示的页签不同。

图2-113 网络时间同步方式

< 系统管理 >

系统时间

主机名

Router

* 最大长度为32位

时间同步类型

网络时间

主服务器地址

clock.fmt.he.net

* 最大长度为64位

备用服务器地址

最大长度为64位

时区

Asia/Shanghai

图2-114 手动方式同步时间

< 系统管理 >

系统时间

主机名

Router

* 最大长度为32位

时间同步类型

手动

日期

-

-

如：1970-01-01

时钟

-

-

如：12:01:01

时区

Asia/Shanghai

步骤 7 配置系统时间参数。

参数说明。

表2-64 系统时间参数说明

参数名称	含义	如何配置
启用/禁用	“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。

参数名称	含义	如何配置
时间同步类型	进行系统时间校验的时间同步类型。	下拉框选项 ☒ 网络时间 ☒ 手动
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。WORD 类型，最大 64 个字节，输入规范请参见“5. 参数规范表”。
时区	地理时区。	从下拉列表中选择 H61XX 工业智能网关所在的时区。
当“时间同步类型”选择“手动”时（本页只显示配置的时间，系统实时时间在 WEB 页面右上角）		
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 8 点击“保存”，完成系统时间参数配置。

---结束

2.8.8.证书管理

提供证书导入的功能，可对需要导入设备的证书进行统一管理，可以导入 VPN 证书等。具体使用步骤如下：

步骤 1 登录 H61XX 工业智能网关 WEB 配置界面。

登录方法请参见“2.2 登录 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。

图2-115 证书管理页签



步骤 3 点击“文件”选择本地证书，点击“导入”上传证书。可对证书进行保存、删除、导入、导出操作。

---结束

2.8.9.系统升级

升级设置

H61XX 工业智能网关支持本地网络方式升级系统文件，在升级之前请确定用户已获得系统更新的目标文件，并将更新文件已经存放至局域网的计算机中。

步骤 1 单击“系统管理>系统升级”，显示“系统升级”界面。

图2-116 文件升级页签



步骤 2 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，H61XX 工业智能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，H61XX 工业智能网关的参数配置将会保持。若升级补丁，则升级完成后系统补丁列表会显示补丁标识信息。

查看补丁信息

H61XX 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。

图2-117 补丁文件操作页签



- 删除：删除所有补丁文件。

——结束

2.8.10. 配置管理

H61XX 工业智能网关支持配置文件的备份和恢复。

- 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 H61XX 工业智能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。其中不勾选差分配置则导出的是全功能配置。
- 勾选差分配置，点击导出，导出的是当前修改功能的配置和应用程序自启动生成的配置文件。

图2-118 备份设置页签



导入备份文件后，系统自动重启，在重启系统之后才能生效。

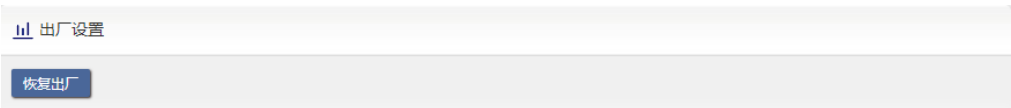
——结束

2.8.11. 复位重启

出厂设置

H61XX 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。单击“恢复出厂”按钮，可以恢复出厂配置。

图2-119 出厂设置页签



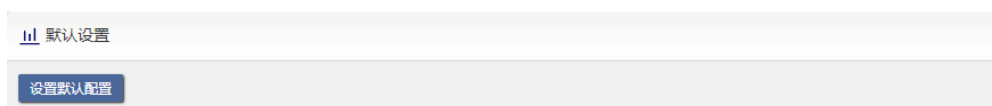
- 设置默认：将当前配置保存为默认出厂配置。
- 恢复出厂：恢复出厂配置。

——结束

默认设置

H61XX 工业智能网关也可以将现有的配置设为默认配置，并在 H61XX 工业智能网关中生成一个默认配置文件，用户可以单击“恢复出厂”随时将配置恢复到这个默认配置。若该默认配置文件被删除，则 H61XX 工业智能网关会恢复至最初的出厂设置。

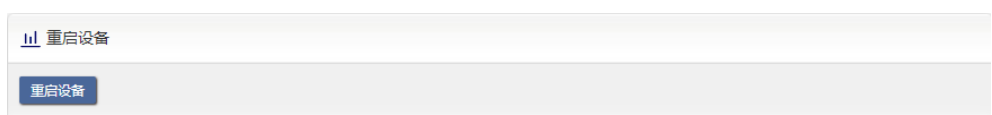
图2-120 默认设置页签



重启

单击“重启设备”按钮可以重新启动系统。

图2-121 重启设备页签



2.9. 按键重启

H61XX 工业智能网关按键重启功能定义如下：

按住 RST 键 1-5 秒，重启设备；

按住 RST 键 5-20 秒，恢复用户配置，如果没有设置用户配置，则恢复出厂配置；

按住 RST 键 20 秒以上，恢复出厂配置。

——结束

3. 业务场景

关于本章

章节	内容简介
3.1 SDN	本节介绍 SDN（软件定义网络）的功能定义、组成架构，以及 M2M 组网应用和平台实际配置（TUN/TAP 组网）。
3.2 VXLAN	本节介绍 VXLAN（虚拟扩展局域网）的功能简介、基本原理、典型组网应用，以及设备上的配置方法和连通性检测。
3.3 双发选收	本节介绍双发选收技术的使用场景（如金融交易、视频会议、物联网等）及典型应用组网。
3.4 负载均衡	本节介绍负载均衡的场景（如按需选择 WAN 接口）、参数配置方法（接口、成员、策略、规则）及应用结果。
3.5 链路参数备份	本节介绍链路参数备份的多种场景（如物理链路虚拟链路组合切换），并提供对应的参数配置和应用结果说明。

3.1.SDN

3.1.1. SDN 功能简介

3.1.1.1. SDN 功能定义

SDN 从业务场景层面可以划分为 SDLAN 与 SDWAN，SDLAN 主要用于解决终端下挂设备的访问管理或相互访问的问题；SDWAN 则着重于数据转发、流量识别与选路、链路聚合加速等；

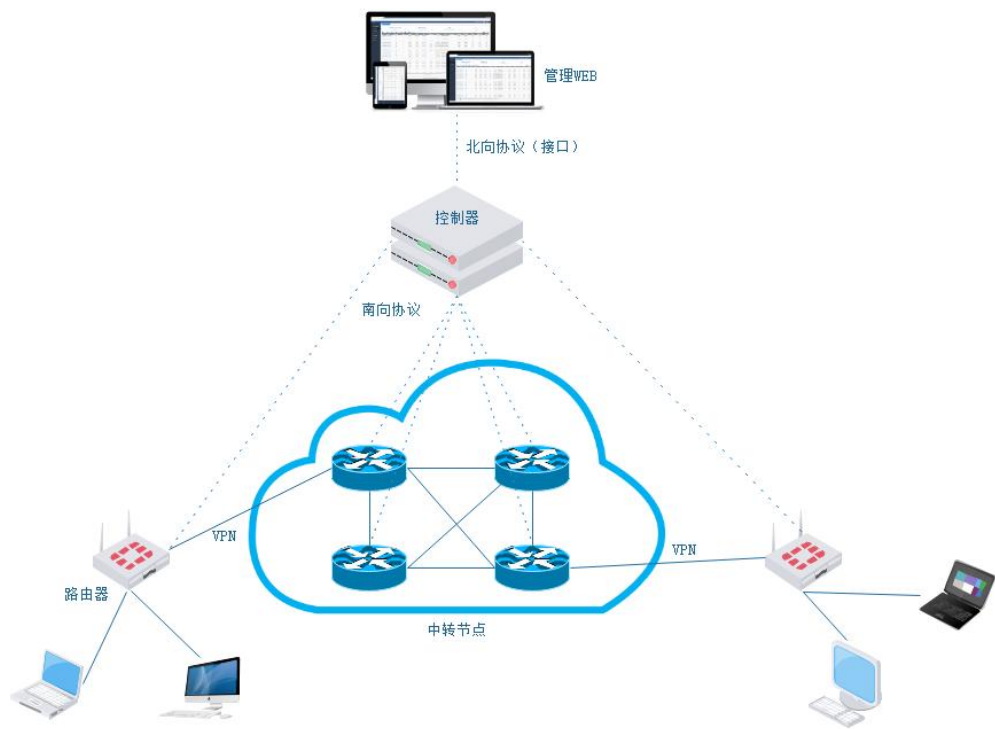
SDN 的核心是控制平面和数据转发平面的分离，这种分离使得网络的控制逻辑（控制平面）可以从数据的转发逻辑（数据平面）中独立出来，通常由一个中心化的控制器来实现网络的控制功能。

SDN 是公司一体化规划中不可缺少的一部分，同时也是生态建设中关键的一环；通过 SDN（Software-Defined Networking），可以实现网络的集中化控制、自动化管理、灵活的流量调度、快速的业务部署和创新，同时提高网络的可编程性和安全性，降低运营成本。

缩写/术语	解释
SDN	Software Defined Network，软件定义网络
ODL	OpenDayLight 控制器的缩写

XML	Extensible Markup Language，可扩展标记语言
YANG	Yet Another Next Generation
RPC	Remote Procedure Call，远程过程调用

3.1.1.2. 组成架构



控制器：作为 SDN 网络的“大脑”，负责管理和控制整个网络的行为，功能上包括网络拓扑发现、流表管理、故障检测与恢复、网络安全策略实施、负载均衡、北向和南向接口管理等一系列网络监控与控制动作

南向协议：实现数据平面与控制平面的信息交互，这包括向上收集数据平面信息以及向下下发控制策略，指导转发行为

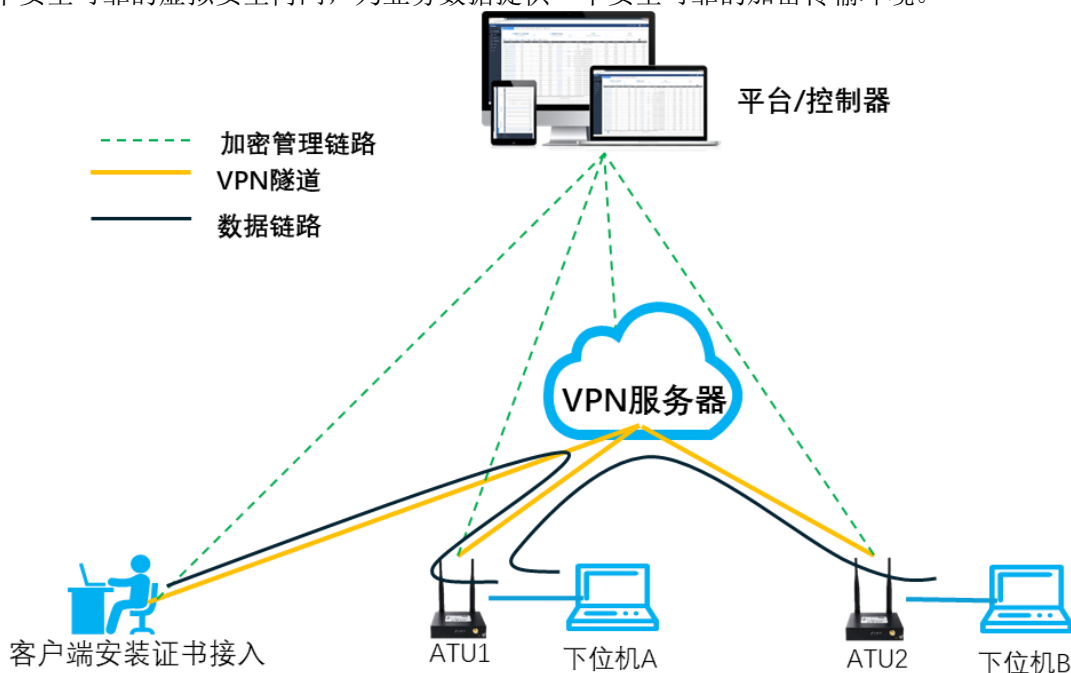
北向协议：作为管理 WEB 关键的后端服务支撑体，实现控制器与管理 WEB 的信息交互，提供数据与接口供管理 WEB 进行显示与调用

用户管理 UI：将 SDN 直观呈现给用户的一种最直接的方法，用户通过浏览器登录账户后，即可对自己的网络拓扑进行有效的监控与管理

中转节点：边缘联网的真实载体，提供转发上网的能力，同时在控制器的干预下实现链路的选择与切换；中转节点可被控制器要求做一些流量识别或策略选路的动作

3.1.2. M2M 组网应用

M2M(Machine to Machine) VPN 为用户的物联网应用的提供了批量接入和数据转发服务，适合用于当有大量的 IoT 设备需要接入同一个网络并进行数据互通的场景用户通过对 M2M 服务器和 ATU 进行图形化配置操作，SDN 控制器会自动生成该网络的 VPN 配置和安全证书，并为用户在公网之上快速组建一个安全可靠的虚拟安全内网，为业务数据提供一个安全可靠的加密传输环境。



3.1.2.1. M2M 组网特性

- 提供一个安全可靠的虚拟内网，让 ATU 之间可以相互通信
- 利用穿透的方式，实现下位机之间的三层通信
- 利用大二层的方式，实现下位机之间的二层通信
- 生成证书配置，支持多平台如 PC、手机等接入并访问
- 对网络内每个账号实现精准的流量统计

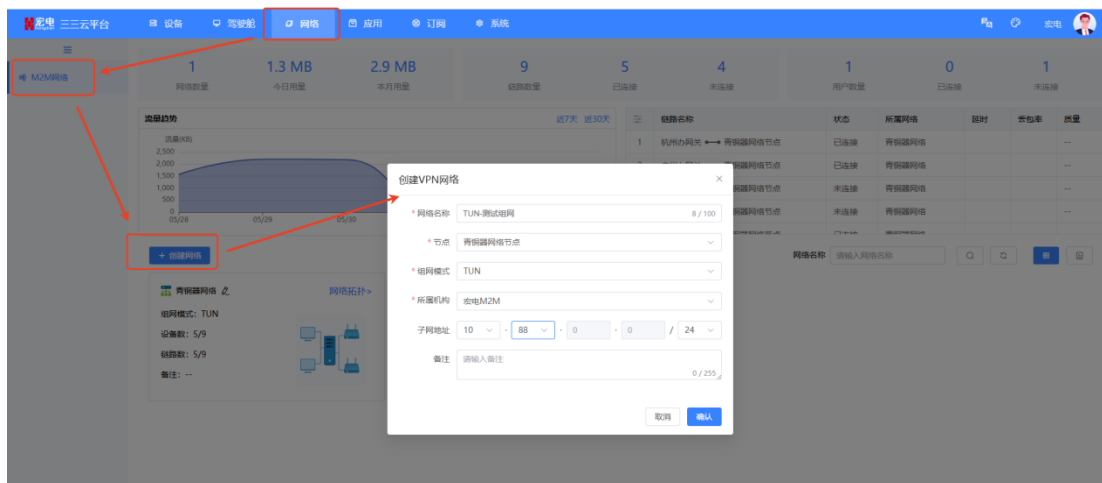
3.1.2.2. 实现功能点

- 通道管理：控制器集中管理每个 ATU 的通道接入与断开
- 账号管理：每个 ATU 或第三方设备，拥有专属的账号，利用账号实现虚拟 IP 地址的绑定与管理
- 穿透管理：控制器集中管理每个 ATU 的映射规则，实现三层的穿透通信
- 大二层管理：通过 tap 与桥接技术的结合，实现大二层的广播通信

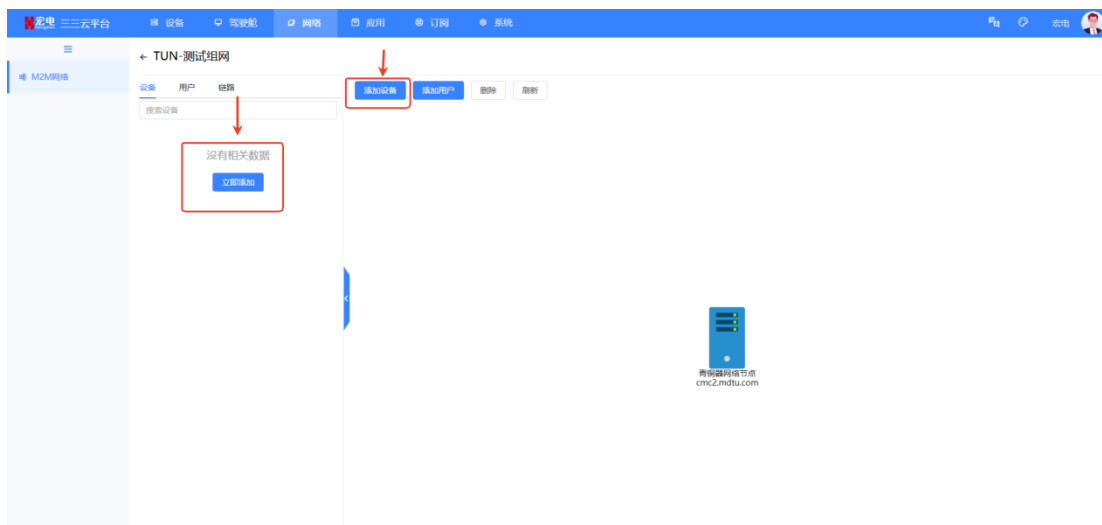
3.1.3. 平台实际配置

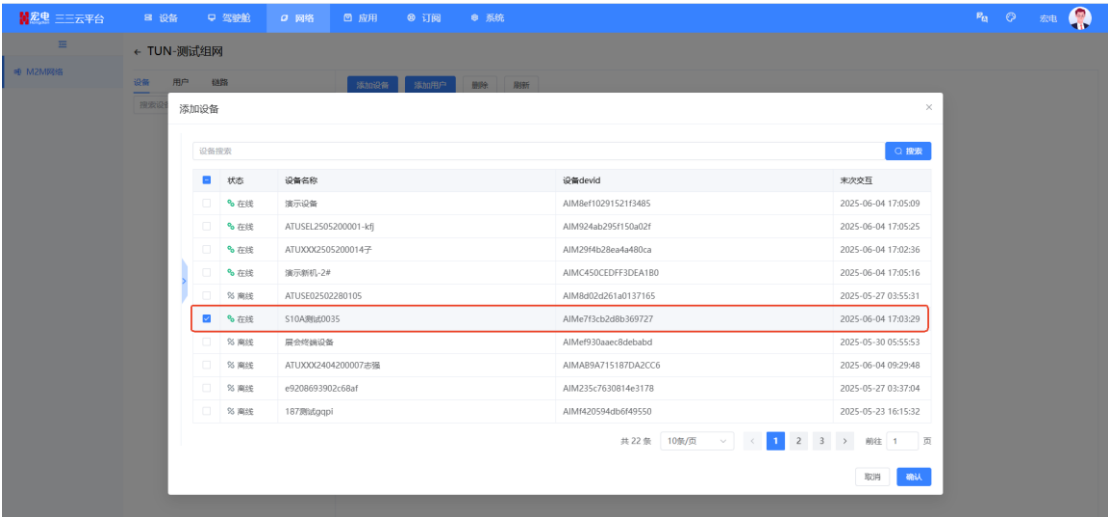
3.1.3.1. TUN 组网配置

(1) 平台端创建组网，在“网络”中选择“M2M 网络”后，点击“创建网络”，配置组网名称、节点服务器、组网模式、分组、网络子网后，点击确认，即可创建网络



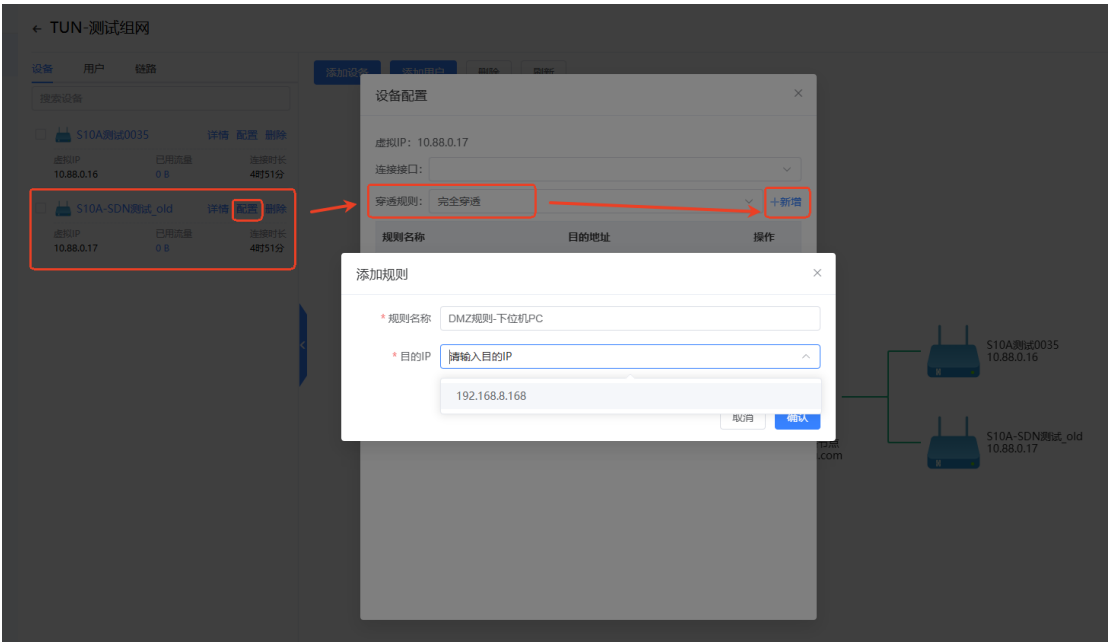
(2) 点击“网络拓扑”按钮可进入网络拓扑页面，点击“添加设备”按钮，可选择需要组网的设备，点击确认，自动下发组网配置





(3) 通过组网，远程访问设备下位机 PC 或摄像头等，可通过添加设备的 DNAT 规则实现

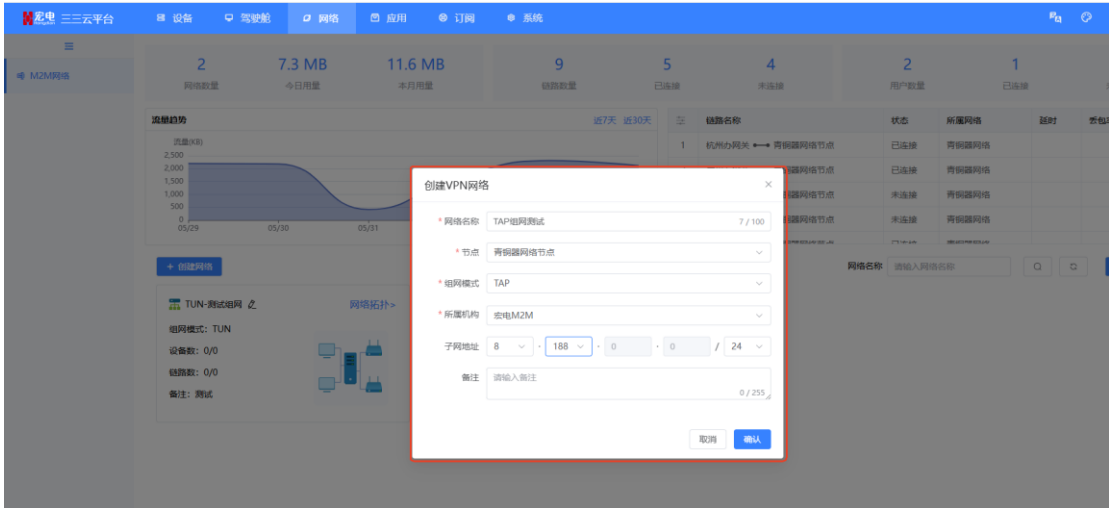
配置“完全穿透”规则，即配置 DNAT 规则，将 tun 接口的所有数据，映射到下位机，点击设备的“配置”按钮--->穿透规则选择“完全穿透”后，点击“新增”按钮，弹框配置规则名称、“目的 IP”下拉框选择下位机 IP 地址，即可确认保存成功



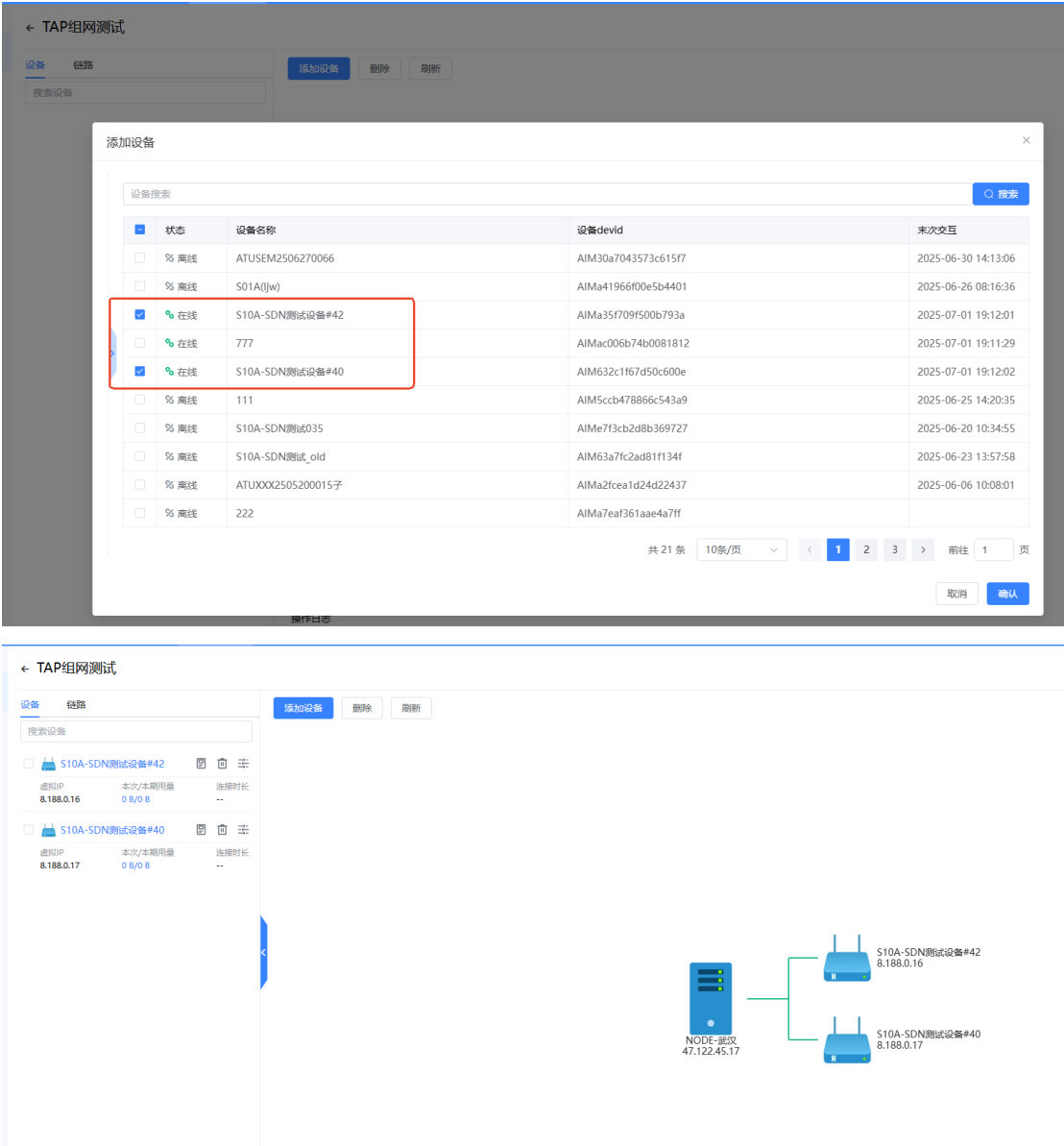


3.1.3.2. TAP 组网配置

(1) 平台端创建组网，在“网络”中选择“M2M 网络”后，点击“创建网络”，配置组网名称、节点服务器、组网模式、分组、网络子网后，点击确认，即可创建网络



(2) 进入组网拓扑，选择要组网的设备，添加进网络



- (3) 若要实现组网内的所有下位机互通，则将 tap 接口桥接至 LAN 口的桥下，使得设备下位机可通过 LAN 口子网地址实现互通。
- 组网拓扑中选测试设备，点击“配置”按钮，打开配置下发页面，“桥接”配置处，勾选开启



3.2. VXLAN

3.2.1. VXLAN 功能简介

3.2.1.1. 简介

VXLAN（虚拟扩展局域网）是一种网络虚拟化技术，通过将二层以太网帧封装在 UDP 报文中，实现跨三层网络扩展，解决传统 VLAN（虚拟局域网）在大型网络中的扩展性和隔离性问题。

核心功能

跨三层网络扩展

通过将二层以太帧封装成 UDP 报文，在 IP 网络中传输，实现二层网络跨物理网络段扩展。支持 1600 万个虚拟网络（VNI 标识），远超 VLAN 的 4094 个限制。

动态虚拟网络迁移

支持虚拟机在数据中心内的动态迁移，无需修改物理网络配置即可实现跨节点通信。

多租户隔离与互通

可划分多个独立虚拟网络（VNI），实现多租户隔离；同时支持不同租户间通过隧道互通。

简化运维管理

通过 VXLAN 隧道终结点（VTEP）自动封装/解封装报文，降低对物理网络设备的依赖。

3.2.1.2. 基本原理

VXLAN（Virtual eXtensible Local Area Network）是一种隧道技术，能在三层网络的基础上建立二层以太网网络隧道，从而实现跨地域的二层互连。

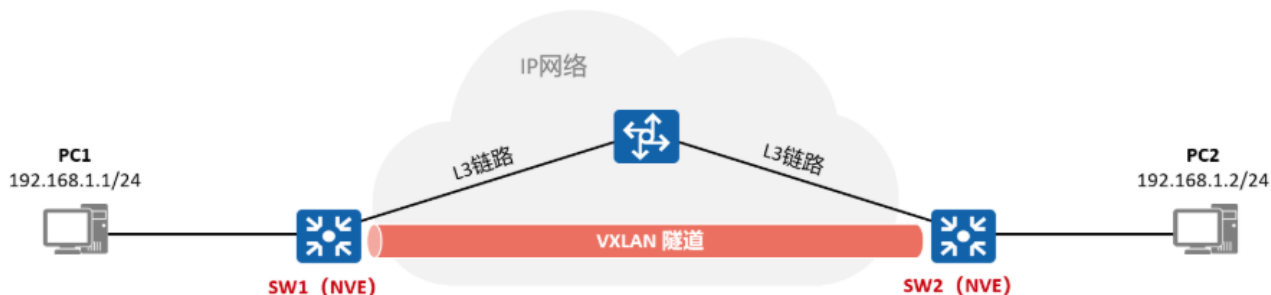
VXLAN 采取了将原始以太网报文封装在 UDP 数据包里的封装格式。将原来的二层数据帧加上 VXLAN 头部一起封装在一个 UDP 数据包里。

VXLAN 头部包含有一个 VXLAN 标识（即 VNI，VXLAN Network Identifier），只有在同一个 VXLAN 上的虚拟机之间才能相互通信。VNI 在数据包之中占 24 比特，故可支持 1600 万个 VXLAN 的同时存在，远多于 VLAN 的 4094 个，因此可适应大规模租户的部署。

VXLAN 一般通过安装在服务器上的软件实现报文的封装与解封装，网络只要 IP 路由可达即可。VXLAN 实现了应用与物理网络的解耦，但网络与虚拟机还是相互独立的。业界一般通过网络控制器（如 SDN，Software Defined Network）实现 VXLAN 网络与云业务的联动。当虚拟机发生迁移后，虚机/存储控制器会把虚拟机迁移信息通知给网络控制器，网络控制器根据虚拟机迁移的新位置，重新调整网络配置，从而实现网络与云业务的联动。也就是说，物理网络可以是传统的三层 IP 网络，路由可达即可。虚拟机可跨三层 IP 网络远距离迁移，不再受限于二层技术。物理网络也无需允许所有 VLAN 通过。接入交换机需要学习的 MAC 地址的数量也大大减少，削弱了网络设备 MAC 地址表项规格对虚拟机规模的约束。

3.2.2.VXLAN 组网应用

当前我们的设备主要是使用 VXLAN 通过三层网络，搭建一个虚拟的二层虚拟局域网，组网图如下所示：



3.2.3.VXLAN 配置说明

3.2.3.1. 设备上配置 VXLAN

- ◆ 这个里面需要配置的内容 VXLAN ID（VNI），这个类似 VLAN 中的 VLAN ID，只有在相同的 VNI 中才能相互进行通信。
- ◆ 端口号指导是外层 UDP 封装时带的端口，NVE 之间的端口号必须是一致的。
- ◆ 远端 IP 指的是建立隧道的对端 IP 地址。
- ◆ 网络接口指的是建立隧道时报文的出接口
- ◆ VXLAN 接口 MTU，这个指的是 VXLAN 接口的 MTU，这个地方需要慎用，需要结合实际的组网场景进行配置，VXLAN 报文头会占用 50 字节的长度，需要计算好，免得网络出现丢包和分包现象。
- ◆ UDP 校验和指的是数据的合法性校验

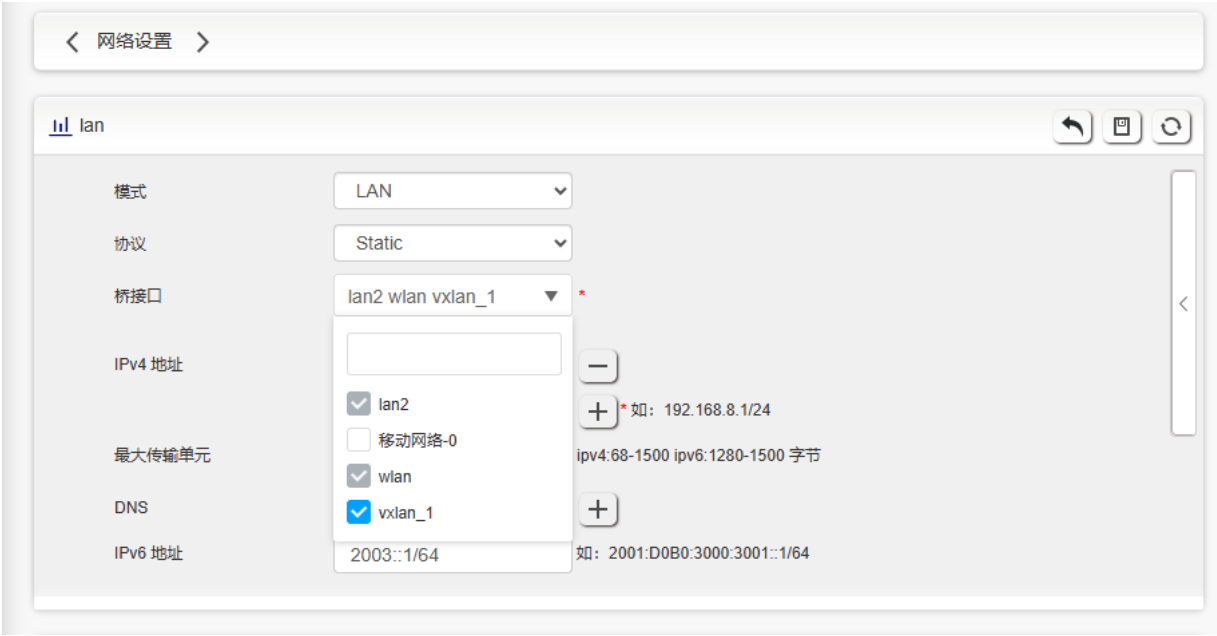
The screenshot shows the 'VXLAN' configuration page in a network management system. The page has a tabbed interface with 'VXLAN' selected. The configuration fields are as follows:

Field	Value	Hint/Range
VXLAN ID	1	* 范围:1~16777214
端口号	3000	* 如:4789
远端IP	200.1.1.2	* 如:192.168.8.1
网络接口	[dhcpv6] wan	
VXLAN接口MTU		128-15360
UDP校验和	☒ 启用 ☐ 禁用	

NVE 上的配置参照上述的描述进行配置，必须保持参数的一致性

3.2.3.2. 配置桥接

VXLAN 配置完成之后，还需要将 VXLAN 接口桥接到默认的桥上，这样才能确保下位机的数据包能正确按照 VXLAN 的方式进行转发。



3.2.3.3. 检测 VXLAN 配置是否生效

在 PC1 上 ping PC2 的地址，如果能通则说明 VXLAN 功能生效；如果不通，检测当前配置的 VNI，端口等信息是否正确，远端 IP 是否可以 ping 通等。

3.3. 双发选收

3.3.1. 使用场景

- 金融交易系统

在金融领域，对数据传输的准确性、完整性和及时性要求极高。双发选收技术可以确保即使在网络出现故障的情况下，交易指令也能准确无误地到达目的地。

- 视频会议/直播

视频会议或直播服务需要稳定的网络连接以提供流畅的观看体验。双发选收技术可以帮助减少由于网络抖动、延迟或丢包造成的画面卡顿或音质下降的问题。

- 云计算与数据中心互连

对于需要高可用性的云服务提供商来说，双发选收可以用来在多个数据中心之间复制关键业务数据，确保即使在一个数据中心发生故障时，另一个中心的数据也是最新且可用的。

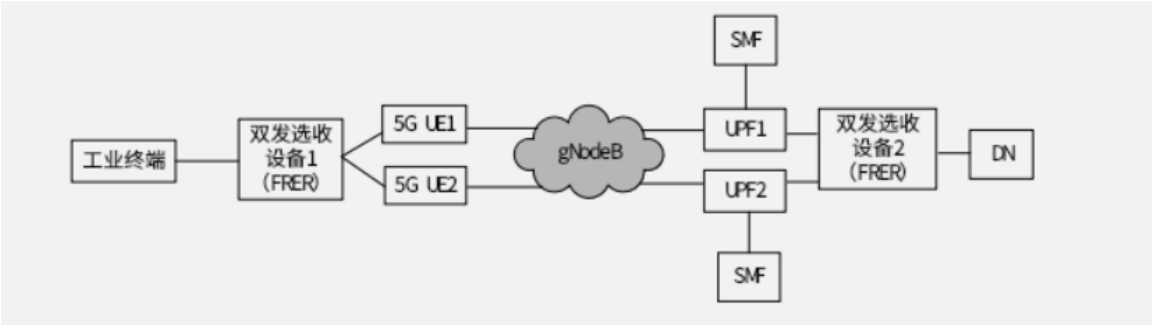
- 物联网(IoT)

在物联网应用中，传感器采集的数据至关重要。采用双发选收技术可以在各种可能的网络干扰下保证重要信息能够被准确接收。

- 远程医疗

远程医疗服务依赖于稳定可靠的通信链路来传输高清影像资料和实时健康监测数据。双发选收有助于保障这些敏感信息的安全传输。

3.3.2.应用组网



3.4. 负载均衡

场景介绍

通过智能地选择最经济的 WAN 接口处理特定类型的流量，可以帮助企业降低网络费用。如所有下位机访问指定服务器 1.1.1.1 的请求连接数较大、且要求稳定，优先配置有线 wan 口；以防有线网络故障，移动网络作为备用方案，但需要减少无线网络费用。

参数配置

该场景下，需要依次配置接口、成员、策略、规则，如下图所示，接口保证可访问外网，或者说服务器；成员分配连接数的权重。

图3-1 接口-wan 口配置

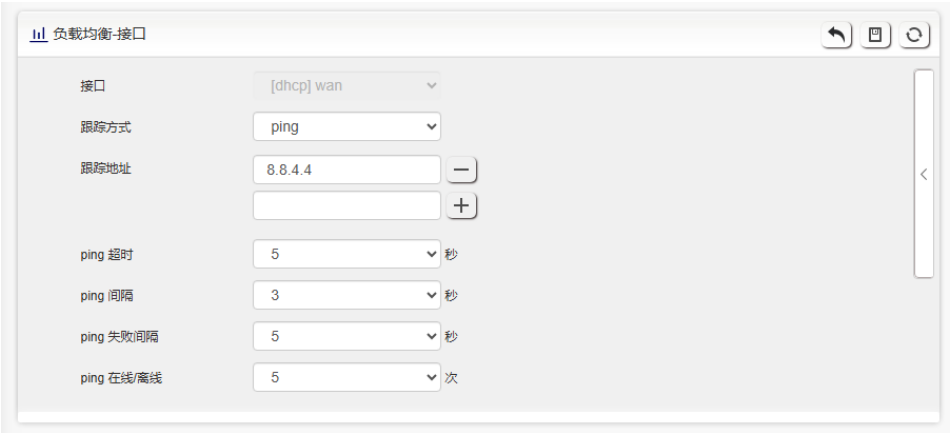


图3-2 接口-移动网络配置

负载均衡-接口

接口

[modem] 移动网络-0

跟踪方式

ping

跟踪地址

8.8.8.8

-

+

ping 超时

5

秒

ping 间隔

3

秒

ping 失败间隔

5

秒

ping 在线/离线

5

次

图3-3 成员配置

接口成员策略规则

成员

接口

跃点数

权重

操作

wan_m1_w9

wan

1

9

modem_m1_w1

移动网络-0

1

1

图3-4 策略配置

接口成员策略规则

策略

分配成员

备用成员

操作

wan9_modem1

wan_m1_w9,modem_m1_w1

默认（使用主路由表）

图3-5 规则配置

接口成员策略规则

规则

分配的策略

协议

源地址

源端口

目的地址

目的端口

操作

rule1

wan9_modem1

all

1.1.1.1

图3-6 默认路由为 wan

静态路由策略路由

名称

网络地址

子网掩码

网关

度量

路由表ID

操作

wan

0.0.0.0

0.0.0.0

IPv6设置

名称

网络地址

网关

度量

MTU

路由类型

路由表ID

操作

wan

:::0

应用结果

配置好之后，访问服务器 1.1.1.1 的连接数约 90%通过 wan 口访问，约 10%的通过移动网络访问。如果移动网络无法访问 1.1.1.1，则全部访问服务器 1.1.1.1 的连接均通过 wan 口访问。如果 wan 口无法访问 1.1.1.1，则全部访问服务器 1.1.1.1 的连接数均通过移动网络访问，访问其他地址的连接则失败。

图3-7 后台 mwan3 status 查看负载均衡状态

```
root@S01A:~#  
root@S01A:~# mwan3 status  
Interface status:  
  interface 4g is online 00h:13m:47s, uptime 02h:52m:43s and tracking is active  
  interface wan is offline and tracking is paused  
  
Current ipv4 policies:  
wan9_modem1:  
  4g (100%)  
  
Directly connected ipv4 networks:  
  
Active ipv4 user rules:  
  0      0 - wan9_modem1  all  --  *      *      0.0.0.0/0      1.1.1.1
```

3.5. 链路参数备份

场景介绍 1

H61XX 工业智能网关支持物理链路、虚拟链路、物理链路+虚拟链路的组合切换，当工作链路不通后，可以快速的切换至其他的链路，并在切换后的链路上继续工作。

例如，门站数据上报需要稳定的网络做保证，若门站平常使用的有线网络出现故障，则可以快速的切换至无线网络，保证门站数据上报业务的正常进行。

参数配置 1

该场景下，需要进行“链路备份”的配置。如下图所示。

图3-8 主链路-wan

智能链路

规则名称

0

* 最大长度为12位

优先级

0

* 0-9

链路运行方式

main

备份模式

hot

检测间隔

10

1-65535 秒

失败间隔

5

1-65535 秒

重传次数

3

1-65535

接口名字

[dhcp] wan

检测方法

icmp

检测地址

8.8.8.8

接入规则

+

图3-9 备份链路-移动网络

智能链路

规则名称

1

* 最大长度为12位

优先级

1

* 0-9

链路运行方式

backup

备份模式

hot

检测间隔

30

1-65535 秒

失败间隔

3

1-65535 秒

重传次数

5

1-65535

接口名字

[modem] 4g

检测方法

http

检测地址

www.baidu.com

接入规则

+

图3-10 链路状态

规则管理

主链路稳定时间

60

1-65535 秒

备份链路最短工作时间

30

1-65535 秒

规则名称	优先级	链路运行方式	备份模式	接口规则项	当前规则	操作
0	0	main	hot	wan	yes	
1	1	backup	hot	4g		

应用结果 1

配置完所有参数后，默认路由走的是主链路 wan 接口，此时产品若一直能够 ping 通 8.8.8.8 地址，则产品就会一直工作在主链路上；而备份链路移动网络则一直处于启用状态。若 wan 口因为故

障而无法 ping 通 8.8.8.8，则在多次检测失败后，产品会将链路切换至移动网络，使下位机的各种业务能够正常进行。

场景介绍 2

H61XX 工业智能网关支持物理链路、虚拟链路、物理链路+虚拟链路的组合切换，当工作链路不通后，可以快速的切换至其他的链路，并在切换后的链路上继续工作。

例如，门站数据上报优先 L2TP 加密，否则 PPTP 加密，注意 L2TP 服务器和 PPTP 服务器地址不一样。

参数配置 2

该场景下，需要进行“链路备份”的配置。如下图所示。

图3-11 主链路-L2TP

智能链路

规则名称

0

* 最大长度为12位

优先级

0

* 0-9

链路运行方式

main

备份模式

hot

检测间隔

1-65535 秒

失败间隔

1-65535 秒

重传次数

1-65535

接口名字

[l2tp] l2tp

检测方法

icmp

检测地址

192.168.120.1

接入规则

+

图3-12 备份链路-移动网络

智能链路

规则名称

2

* 最大长度为12位

优先级

2

* 0-9

链路运行方式

backup

备份模式

cold

检测间隔

1-65535 秒

失败间隔

1-65535 秒

重传次数

1-65535

接口名字

[pptp] pptp

检测方法

icmp

检测地址

192.168.180.1

接入规则

+

图3-13 链路状态

规则管理

主链路稳定时间

60

1-65535 秒

备份链路最短工作时间

30

1-65535 秒

规则名称	优先级	链路运行方式	备份模式	接口规则项	当前规则	操作
0	0	main	hot	l2tp	yes	
2	2	backup	cold	pptp		

应用结果 2

配置完所有参数后，默认路由不变，一直为路由设置里的默认路由。此时产品若一直能够 ping 通 L2TP 对端虚拟地址 192.168.120.1，则产品就会一直工作在主链路上；而备份链路 PPTP 为冷备，则为禁用状态。若 L2TP 故障无法 ping 通对端虚拟地址 192.168.120.1，则在多次检测失败后，产品会将启用 PPTP 并切换链路；此时，L2TP 为主链路 模式，仍保持启用状态。

场景介绍 3

H61XX 工业智能网关支持物理链路、虚拟链路、物理链路+虚拟链路的组合切换，当工作链路不通后，可以快速的切换至其他的链路，并在切换后的链路上继续工作。

例如，门站数据上报优先移动网络+L2TP 加密，否则 wan+PPTP 加密，注意 L2TP 服务器和 PPTP 服务器地址不一样。

参数配置 3

该场景下，需要进行“链路备份”的配置。如下图所示。

图3-14 主链路-移动网络+L2TP

智能链路

规则名称

0

* 最大长度为12位

优先级

0

* 0-9

链路运行方式

backup

备份模式

hot

检测间隔

1-65535 秒

失败间隔

1-65535 秒

重传次数

1-65535

接口名字

[modem] 4g

检测方法

icmp

检测地址

8.8.8.8

接入规则

[l2tp] l2tp

icmp

192.168.120.1

图3-15 备份链路-wan+PPTP

智能链路

规则名称

1

* 最大长度为12位

优先级

1

* 0-9

链路运行方式

backup

备份模式

cold

检测间隔

1-65535 秒

失败间隔

1-65535 秒

重传次数

1-65535

接口名字

[dhcp] wan

检测方法

icmp

检测地址

8.8.4.4

接入规则

[pptp] pptp

icmp

192.168.180.1

图3-16 链路状态

规则管理

主链路稳定时间

60

1-65535 秒

备份链路最短工作时间

30

1-65535 秒

规则名称	优先级	链路运行方式	备份模式	接口规则项	当前规则	操作
0	0	backup	hot	4g l2tp	yes	
1	1	backup	cold	wan pptp		

应用结果 3

配置完所有参数后，默认路由不变，一直为路由设置里的默认路由。此时产品若移动网络一直能够 ping 通 8.8.8.8，且 L2TP 服务可 ping 通对端虚拟地址 192.168.120.1，则产品就会一直工作在主链路上；而备份链路 wan+PPTP 为冷备，则为 wan 接口、PPTP 服务均为禁用状态。若 L2TP 故障无法 ping 通对端虚拟地址 192.168.120.1，或者 modem 无法 ping 通 8.8.8.8，则在多次检测失败后，产品会将启用 wan 接口和 PPTP 服务，并切换链路至备份链路；此时，移动网络+L2TP 为主链路模式，仍保持启用状态。

4. FAQ/异常处理

关于本章

章节	内容简介
4.1 硬件类问题	本节简要介绍 H61XX 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。
4.2 拨号类问题	本节简要介绍 H61XX 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。
4.3VPN 连接类问题	本节简要介绍 H61XX 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。
4.4WEB 配置操作类问题	本节简要介绍 H61XX 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。

4.1. 硬件类问题

4.1.1.所有指示灯均不亮

问题现象

H61XX 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 H61XX 工业智能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，请确保电源适配符合设备供电要求 DC 9-36V。
- 如果是 H61XX 工业智能网关电源口与供电电源未连接上，请将电源线插入电源口。

4.1.2.SIM 卡座连接问题

问题现象

SIM 卡座无法正常插入 SIM 卡。

原因分析

- SIM 卡座已经损坏
- SIM 卡的插入方向错了

解决方法

- 如果是 SIM 卡座损坏，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。

4.1.3.网口连接问题

问题现象

LAN 口指示灯不亮，且无法访问 H61XX 工业智能网关页面。

原因分析

可能原因如下：

- 网线故障
- 网线插错
- PC 端网卡 IP 地址与设备的 lan 口 IP 地址不在同一个子网

解决方法

- 更换一根网线再次连接后，PC 端 ping 一下设备检查网络连通性。
- 确保网线是插在 lan 口上，不要插在 wan 口。
- 确保 PC 端网卡的 IP 地址与设备 lan 口在同一网段。

4.1.4.天线连接问题

问题现象

天线无法正常安装。

原因分析

- 天线不符合配件要求。
- 天线连接不正确。

解决方法

- 如果是天线不符合要求，请更换符合要求的天线。
- 如果是天线连接不正确，请重新连接天线。

4.2. 拨号类问题

4.2.1. 拨号中断

问题现象

H61XX 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
- 移动网络拨号配置不正确

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。
- 如果是移动网络拨号配置有误，请参见“ ”进行正确的配置。

4.2.2. 无信号显示

问题现象

H61XX 工业智能网关移动网络状态页面无信号显示。

原因分析

- 天线连接不正常
- 移动网络没有拨上号
- 移动网络掉线

解决方法

- 如果是天线连接不正常，请参见“ ”。
- 如果是移动网络没有拨上号，请参见“ ”。

- 如果移动网络掉线，请确认 H61XX 工业智能网关的应用程序中是否有进程导致 H61XX 工业智能网关下线。

4.2.3.无法找到 SIM 卡

问题现象

H61XX 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

可能原因如下：

- 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。

4.2.4.通信信号薄弱

问题现象

H61XX 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

可能原因如下：

- 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。

4.3.VPN 连接类问题

4.3.1.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。如果是移动网络接口工作不正常，请参见“ ”。
- 如果是 VPDN 接口工作不正常，请参见“ ”。
- 如果是 VPDN 配置参数不正确，请参见“ ”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。

4.3.2.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。

4.3.3.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 H61XX 工业智能网关没有做 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 H61XX 工业智能网关没有做 MASQ，请手动添加 VPN 接口的 MASQ，具体操作方法请参见“ ”。
- 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“ ”。

4.4.WEB 配置操作类问题

4.4.1.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

可能原因如下：

- 升级时 H61XX 工业智能网关受其他功能影响而重启（如移动网络拨不上号自动重启）
- 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 H61XX 工业智能网关断电

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 H61XX 工业智能网关相匹配的升级固件。
- 如果是升级过程中 H61XX 工业智能网关断电，请确保在升级过程中 H61XX 工业智能网关供电在正常。

4.4.2.恢复参数失败

问题现象

H61XX 工业智能网关恢复参数失败。

原因分析

可能原因如下：

- 参数文件格式不正确
- 恢复参数后未重启 H61XX 工业智能网关

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 H61XX 工业智能网关，恢复参数才能生效。

4.4.3.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。

4.4.4.忘记登录密码

问题现象

登录 H61XX 工业智能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 H61XX 工业智能网关启动的情况下，需要通过按 RST 键 20 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 H61XX 工业智能网关启动的情况下，若按住 RST 键 1s 左右后松手，H61XX 工业智能网关将会重启，且不会更改任何配置。

5. 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，如移动网络接口名称
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

6. 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。

路由器 为信息流或数据分组选择路由的设备。

M

移动网络 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 终端与设备云平台之间、M2M 终端之间、设备云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。

7. 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	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	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

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

