

使用说明书

H8820 专用型工业路由器



前言

文档说明

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

读者对象

本文档适用于以下读者：

- 研发工程师
- 技术支持工程师
- 终端用户

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

如果已经了解或使用过宏电 Router 产品或其他公司生产的类似产品，建议可通过文档结构导航选择性阅读想了解的章节内容。

产品名称

本说明文档适用以下产品：

产品型号	产品类别
H8820	专用型工业路由器

修订记录

文档版本	修订时间	修订说明	修订人
V1.0.0.1	2019.11.15-18	统一模板，首次发布	MJ

内容简介

本文档对 H8820 专用型工业路由器产品的使用进行了以下描述。

章节	内容
1 产品介绍	本章介绍 H8820 专用型工业路由器以及其功能特点、产品定位。
2 产品结构	本章介绍 H8820 专用型工业路由器软件、硬件结构。
3 安装 H8820 专用型工业路由器	本章介绍如何安装 H8820 专用型工业路由器。
4 配置前准备	本章介绍 H8820 专用型工业路由器配置前准备工作。
5 路由器配置	本章介绍 H8820 专用型工业路由器功能配置操作。
6 典型应用	本章介绍 H8820 专用型工业路由器几种典型应用方式。
7 FAQ/异常处理	本章介绍 H8820 专用型工业路由器使用过程中常见故障原因及处理方法。
A 参数规范表	介绍本文档中各类参数输入规范。
B 术语	介绍本文档中出现的术语。
C 缩略语	介绍本文档中出现的缩略语。

约定

符号约定

文中出现的下列标志所代表含义如下。

符号	说明
 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。
“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。

目录

1 产品介绍.....	8
1.1 概述.....	8
1.2 产品定位.....	8
1.3 功能与特点.....	9
1.4 技术指标及规范.....	10
2 产品结构.....	11
2.1 硬件结构.....	11
2.1.1 设备外观与尺寸.....	11
2.1.2 设备的配置以及配件.....	13
2.2 功能结构.....	14
3 安装 H8820 专用型工业路由器.....	15
3.1 开箱.....	15
3.2 安装与接线.....	15
3.2.1 SIM 卡的安装.....	15
3.2.2 以太网线连接.....	16
3.2.3 以太网线的连接.....	16
3.3 供电电源.....	16
3.4 安装检查.....	16
4 配置前准备.....	18
4.1 终端面板指示灯状态.....	18
4.2 本地连接配置.....	19
5 路由器配置.....	29
5.1 概述.....	30
5.2 登录 WEB 配置界面.....	30
5.3 网络设置.....	31
5.3.1 LAN.....	32
5.3.2 移动网络.....	33
5.3.3 参数切换.....	36
5.3.4 网络连接.....	38
5.3.5 DHCP 服务.....	39
5.4 应用程序配置.....	42
5.4.1 ICMP 检测.....	42

5.4.2 DDNS 设置.....	45
5.4.3 DTU 设置.....	47
5.4.4 SNMP 配置.....	53
5.4.5 M2M 配置.....	55
5.4.6 任务管理设置.....	56
5.5 安全配置.....	59
5.5.1 概述.....	59
5.5.2 IP 过滤.....	59
5.5.3 域名过滤.....	63
5.5.4 MAC 过滤.....	64
5.6 转发配置.....	67
5.6.1 概述.....	67
5.6.2 NAT.....	67
5.6.3 静态路由配置.....	72
5.7 VPN 功能配置.....	75
5.7.1 概述.....	75
5.7.2 VPDN 配置.....	75
5.7.3 Tunnel 配置.....	78
5.7.4 IPSec 设置.....	80
5.7.5 OPENvpn 设置.....	87
5.8 系统管理配置.....	91
5.8.1 概述.....	91
5.8.2 本地日志.....	91
5.8.3 远程日志.....	92
5.8.4 系统时间.....	93
5.8.5 用户管理.....	95
5.8.6 网络测试.....	97
5.8.7 文件升级.....	98
5.9 状态.....	100
5.9.1 概述.....	100
5.9.2 基本信息.....	101
5.9.3 LAN 状态.....	101
5.9.4 移动网络状态.....	103
5.9.5 路由表.....	104

5.10 RESET 键功能.....	106
6 典型应用.....	107
6.1 概述.....	107
6.2 参数切换功能应用.....	107
6.3 VPN 功能应用.....	110
6.4 任务管理应用.....	113
7 FAQ/异常处理.....	115
7.1 硬件类问题.....	115
7.1.1 所有指示灯均不亮.....	115
7.1.2 SIM 卡座连接问题.....	116
7.1.3 网口连接问题.....	116
7.1.4 天线连接问题.....	116
7.2 拨号类问题.....	117
7.2.1 拨号中断.....	117
7.2.2 无信号显示.....	117
7.2.3 无法找到 SIM/UIM 卡.....	117
7.2.4 通信信号薄弱.....	118
7.3 VPN 连接类问题.....	118
7.3.1 VPDN 无法连接.....	118
7.3.2 VPN 无法通信.....	119
7.3.3 路由可通信但子网不可通信.....	119
7.4 WEB 配置操作类问题.....	120
7.4.1 升级固件失败.....	120
7.4.2 恢复参数失败.....	120
7.4.3 升级补丁失败.....	120
7.4.4 忘记路由器登录密码.....	121

1 产品介绍

关于本章

章节	内容简介
1.1 概述	本节简要介绍 H8820 专用型工业路由器产品概述。
1.2 产品定位	本节简要介绍 H8820 专用型工业路由器产品定位。
1.3 功能与特点	本节简要介绍 H8820 专用型工业路由器产品功能与特点。
1.4 技术指标及规范	本节简要介绍 H8820 专用型工业路由器产品所采用技术指标及相关规范。

1.1 概述

H8820 专用型工业路由器是基于模块 OPEN 方案研发的无线路由网关设备，除了具备传统路由器的 VPN、防火墙、NAT、DHCP 等功能之外，还能支持全网通无线拨号，提供最高可达 100Mbps 的无线高速带宽。H8820 专用型工业路由器支持单模单卡，支持宏电自主研发的宏电设备云平台。该平台能实现对 H8820 专用型工业路由器现场无线网络信息及状态的统计及 H8820 专用型工业路由器的远程升级和配置管理。

1.2 产品定位

H8820 专用型工业路由器广泛应用于商业、电力、能源、农业、数控、信息传媒、金融、自助终端、智能物流、智慧油田、智慧城市、环保减灾等场景，产品尺寸短小，性能稳定，便于布置安装。

商业联网应用

H8820 专用型工业路由器基于互联网+4G 无线联网，可广泛用于商业联网。其典型组网如图 1-1 所示。

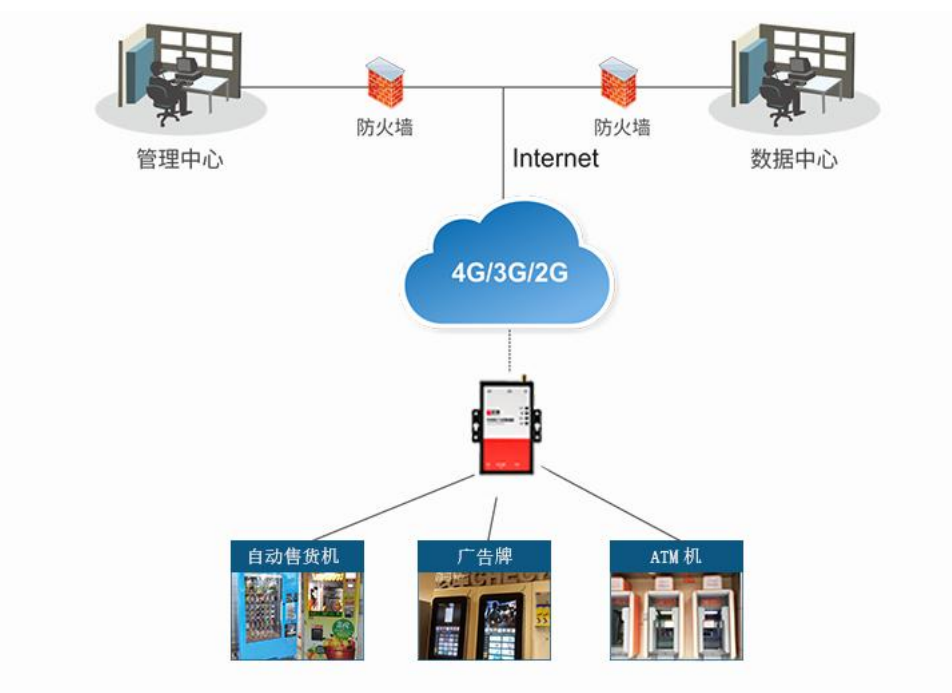


图 1-1 应用示意图

1.3 功能与特点

基本功能

- 支持模块 open 方案
- 支持全网通
- 支持 1 个 LAN 口高速交换
- 支持 VPN 专网接入
- 支持 IPSec、GRE（Generic Routing Encapsulation）、IPIP、PPTP（Point to Point Tunneling Protocol）、L2TP（Layer 2 Tunneling Protocol），IPSec 支持 CA 数字证书
- 支持 GRE over IPSec，IPSec over PPTP/L2TP/GRE/IPIP
- 支持宏电自主研发多参数多功能组合切换功能,实现多服务器的灵活快速通信切换和单卡多运营商切换
- 支持 DHCP Server
- 支持本地、远程、平台固件/补丁升级
- 支持 WEB、CLI、SSH、平台多种参数管理方式
- 支持设备云平台管理，可实时统计设备流量、监控设备网络状态

- 支持参数备份及导入
- 支持设备内部存储
- 支持 DNS 代理，支持 DDNS
- 支持 NTP 网络对时
- 支持 SNMP 网络管理
- 提供系统本地日志和远程日志发送，实现网络实时监控
- 支持静态路由、支持源地址策略路由
- 支持定时管理，有效控制上网流量和时长
- 支持 LCP（Link Control Protocol）检测、ICMP（Internet Control Message Protocol）检测、心跳包检测等链路检测功能，保障无线网络稳定可靠
- LED 状态监测（显示电源、系统、4G 网络类型等状态）
- 支持 RUNlog 本地及远程系统日志功能，实现设备运行的实时监控

1.4 技术指标及规范

接口

- 天线接口：SMA-K 母头，暂不支持 4G2-A 天线
- 以太网接口：1 个百兆 LAN 口，10M/100MBase-T 自适应
- RESET 按键：一键恢复出厂按键
- DC 电源插座：提供电压
- 1 个接地螺柱：可接地线

供电

- 电压：+5V ~+36VDC
- 空闲平均功耗：50mA@12V DC
- 工作平均功耗：200mA@12V DC

其他参数

- 重量：270g
- 工作环境温度：-30~+75° C
- 储存温度：-40~+85° C
- 相对湿度：≤95%（无凝结）

2 产品结构

关于本章

章节	内容简介
2.1 硬件结构	本节简要介绍 H8820 专用型工业路由器硬件结构。
2.2 功能结构	本节简要介绍 H8820 专用型工业路由器产品功能结构。

2.1 硬件结构

2.1.1 设备外观与尺寸

外观图

宏电 H8820 专用型工业路由器外观实物图如图 2-1 所示。



图 2-1 H8820 专用型工业路由器外观实物图

尺寸

表 2-1 H8820 专用型工业路由器设备尺寸规格说明

设备名称	长×宽×高(mm)	插口描述
H8820 专用型工业路由器	127×83×24	1 个百兆 RJ45 网口：用于连接下位机

H8820 专用型工业路由器外观结构尺寸图如图 2-2 所示。



说明

下面几个图中，对应设备实物的尺寸的单位是毫米，下文不再赘述。

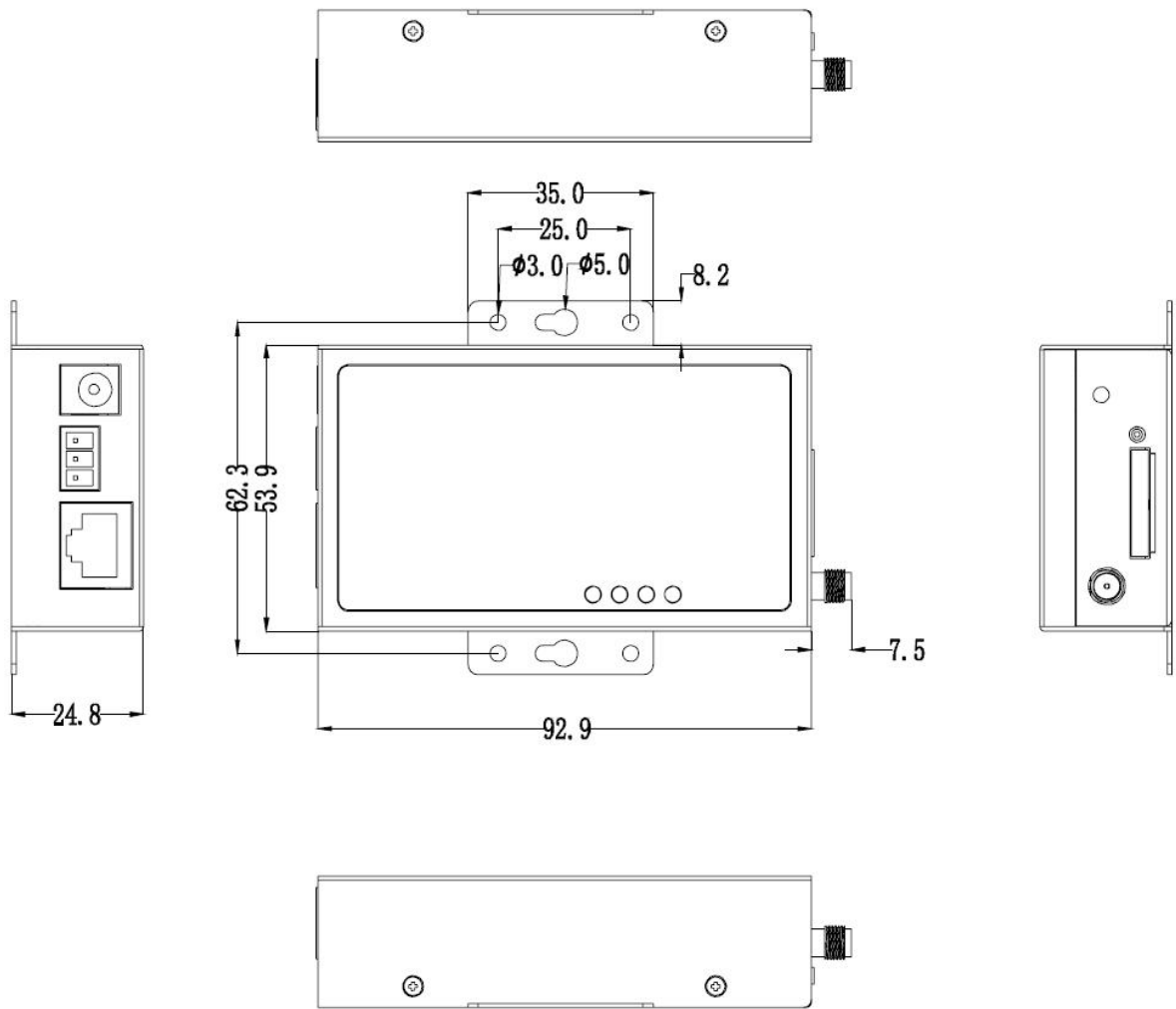


图 2-2 H8820 专用型工业路由器总体外观图

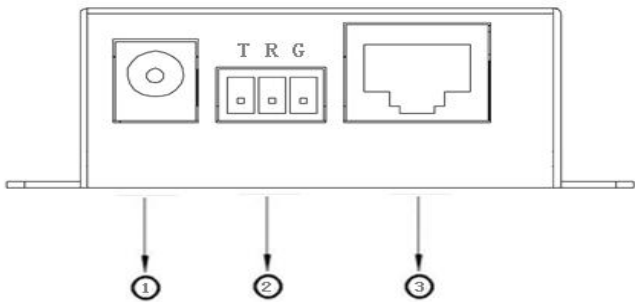


图 2-3 H8820 底面板接口图

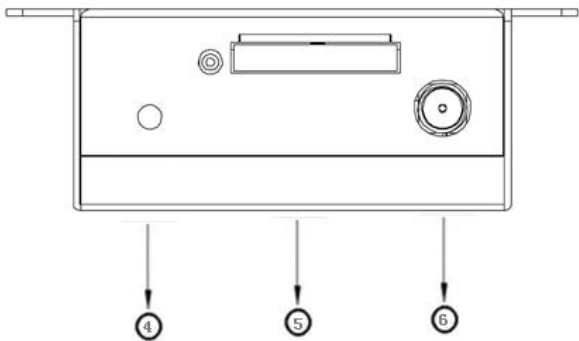


图 2-4 H8820 顶面板接口图

表 2-2 接口定义说明表

序号	说明	序号	说明
①	2PIN 电源端子	④	RST 按键
②	3PIN RS232/485 接线端子	⑤	SIM 卡槽
③	百兆 RJ45 网口	⑥	4G 线接口

2.1.2 设备的配置以及配件

配件说明

H8820 专用型工业路由器包含如表 2-3 所示配件。

表 2-3 H8820 专用型工业路由器配件清单

配件名称	数量	备注
标配		
H8820 专用型工业路由器主机	1 个	据用户订货情况包装
4G 天线	1 根	根据网络配对应的天线
RJ45 网线	1 根	无

配件名称	数量	备注
安装固定件	1 对	无
合格证和保修卡	1 份	无
+12V 电源适配器	1 个	无

型号说明

H8820 专用型工业路由器是基于 4G 无线通信技术研发的无线路由传输产品，采用全工业级设计、电磁兼容性设计、模块化设计，适用于不同行业应用需求和运营商的网络环境。

2.2 功能结构

主控制器模块

该模块主要负责以下几个功能：

- 控制 4G 模块拨号上网和下线
- 控制路由器与 Internet 的有线连接
- 对 IP 数据包进行转发
- 运行路由协议、防火墙协议、VPN 协议等高级功能
- 维护设备的正常运行

LAN

路由器的网口数据处理模块通过 RJ45 网线与下位机进行通讯，为下位机提供 IP 数据包转发功能。

4G 模块

该模块主要实现 4G 上网功能，从而实现终端产品对 IP 数据的转发。

3

安装 H8820 专用型工业路由器

关于本章

章节	内容简介
3.1 开箱	本节简要介绍 H8820 专用型工业路由器产品安装时开箱操作及需要检查的设备清单。
3.2 安装与接线	本节简要介绍 H8820 专用型工业路由器产品 SIM 卡的安装和以太网连接、串口线连接等。
3.3 供电电源	本节简要介绍 H8820 专用型工业路由器的供电要求及供电方法。
3.4 安装检查	本节简要介绍 H8820 专用型工业路由器安装后检查操作。

3.1 开箱

设备到达现场后，需要开箱并检验配件是否齐全。正常情况下，整套设备应包含的配件如表 2-3 所示。开箱后保管好包装材料，以备二次转运过程中需要使用。

3.2 安装与接线

3.2.1 SIM 卡的安装

H8820 专用型工业路由器支持单 SIM 卡，在正常安装使用过程中需要在 SIM 卡槽安装 SIM 卡。



在进行 SIM 卡安装时，请确保路由器处于断电状态。

步骤 1 将 SIM 卡金属面朝上，缺角一端朝内，将卡推入卡槽。

3.2.2 以太网线连接

H8820 专用型工业路由器配置使用简单，通过以太网网线连接即可进行正常的配置管理和数据通信。以太网连接主要为单设备直连方式。

单设备直连方式

使用 RJ-45 类型接头的以太网线将配置电脑与 H8820 专用型工业路由器的交换口直接连接，如图 3-1 所示。

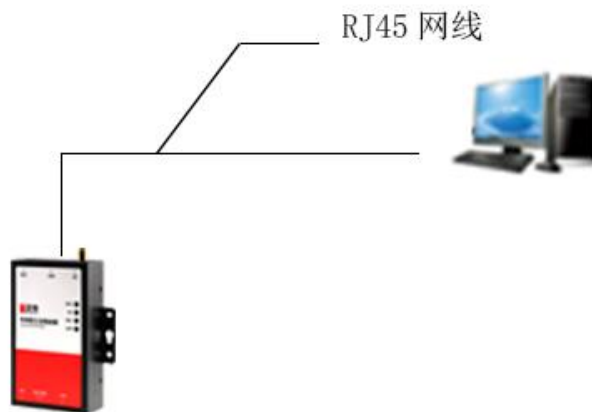


图 3-1 单设备直连方式

3.2.3 以太网线的连接

H8820 专用型工业路由器支持 1 个 LAN 口的局域网的连接，可以使用 RJ45 网线将网线的一端插入路由器的 LAN 接口，另一端连接其他设备即可。

3.3 供电电源

H8820 专用型工业路由器产品使用+9V~+36V 直流供电。

3.4 安装检查

安装并准备上电前，试按一下 SIM 卡，检查卡有没有插紧。插上电后检查路由器工作状态指示灯，在插上电的一瞬间接有下位机的 LAN 口会亮，再过一段时间，SYS 灯会亮，表示系统已经启动并开始正常工作。



上电前务必连接天线，以免射频部分阻抗失配，导致信号差而无法拨号上线。

操作步骤

步骤 1 检查天线连接是否正确。

步骤 2 检查 SIM 卡是否安装无误，并确认 SIM 卡是否有效。

步骤 3 向 H8820 专用型工业路由器供电，下面仅以一个 SIM 卡来说明路由器的拨号情况。

- 供电后如果 H8820 专用型工业路由器上接有下位机的 LAN 口灯亮，表示 Router 供电正常。
- 上电后路由器 SYS 指示灯亮，表示路由器系统已启动。
- 在 SYS 指示灯亮一段时间后，4G 指示灯闪，表示路由器已找到模块并开始拨号。
- 路由器在拨号成功后，4G 灯会亮，表示路由器已获得 SIM 卡信号。详情请参见“4.1 终端面板指示灯状态”。



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

---结束

4 配置前准备

关于本章

章节	内容简介
4.1 终端面板指示灯状态	本节简要介绍 H8820 专用型工业路由器终端面板指示灯状态。
4.2 本地连接配置	本节简要介绍 H8820 专用型工业路由器安装后本地连接配置过程。

4.1 终端面板指示灯状态

H8820 专用型工业路由器面板上有 4 个 LED 指示灯，指示 H8820 专用型工业路由器的工作状态和网络状态。指示灯状态说明如表 4-1 所示。

表 4-1 指示灯说明表

指示灯	显示说明	描述
SYS	灭	系统供电异常
	常亮	系统供电正常
4G	常亮	移动网络上线
	闪烁	移动网络拨号中
	灭	移动数据离线
SIG	常亮	信号强度大于等于 15
	闪烁	信号强度大于 0 小于 15
	灭	信号强度为 0
LAN	常亮	网口连接正常

	闪烁	网口有数据传输
	灭	网口连接异常

4.2 本地连接配置

前提条件

- 已经为 H8820 专用型工业路由器供电。
- 已经通过以太网网线连接 H8820 专用型工业路由器网口。

以太网连接具体操作请参见“3.2.2 以太网线连接”。H8820 专用型工业路由器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”，如图 4-1 所示。



图 4-1 网络连接窗口

步骤 2 双击“以太网”，打开“以太网状态”窗口，如图 4-2 所示。



图 4-2 以太网状态

步骤 3 在“以太网状态”窗口中单击“属性”，打开“以太网属性”窗口。



图 4-3 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
 1. 在“以太网属性”窗口中双击“Internet 协议（TCP/IP）”，打开 Internet 协议（TCP/IP）属性窗口。在“常规”选项卡中修改常规网络配置。如图 4-4 所示。



注意

由于 H8820 专用型工业路由器出厂默认参数中

- 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 H8820 专用型工业路由器出厂默认值。



图 4-4 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）。

2. 单击“确定”，完成配置。
- 高级配置
该方法即在原有网络环境配置（步骤 1～步骤 3）下不希望中断本地 PC 机继续局域网通信，又能对 H8820 专用型工业路由器进行配置时，可考虑添加高级配置。

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

高级 TCP/IP 设置

IP 设置

DNS

WINS

IP 地址(R)

IP 地址

192.168.8.111

子网掩码

255.255.255.0

添加(A)...

编辑(E)...

删除(V)

默认网关(F):

网关

192.168.8.1

跃点数

自动

添加(D)...

编辑(T)...

删除(M)

☒ 自动跃点(U)

接口跃点数(N):

确定

取消

图 4-5 高级 TCP/IP 设置

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

TCP/IP 地址

IP 地址(I):

192 . 168 . 8 . 111

子网掩码(S):

255 . 255 . 255 . 0

添加(A)

取消

图 4-6 TCP/IP 地址

3. 单击“添加”，完成配置。

---结束

DHCP 自动获取 IP 方式

H8820 专用型工业路由器内置 DHCP（Dynamic Host Configuration Protocol）服务器，自动按照预先设定的参数对连接在其上的终端(或 PC 等)分配 IP（Internet Protocol）地址。



说明

H8820 专用型工业路由器内置的 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”，如图 4-7 所示。



图 4-7 网络连接窗口

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

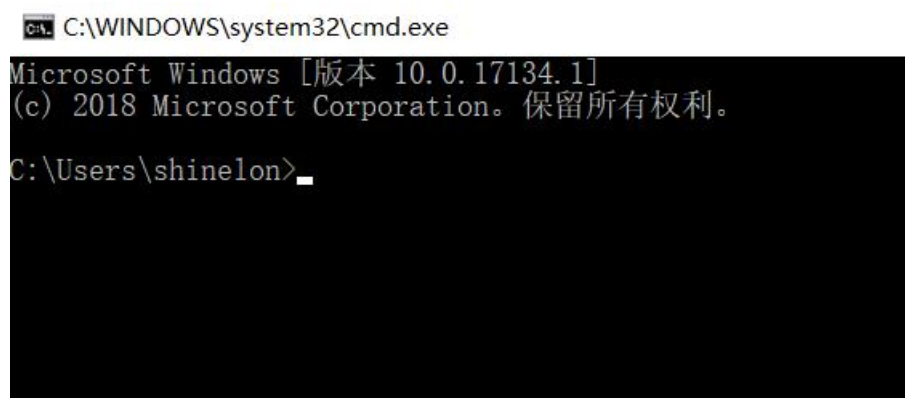


图 4-8 本地连接 2 属性

- 步骤 3 在“此连接使用下列项目(O):”中，选择“Internet 协议 (TCP/IP)”并双击进入“Internet (TCP/IP) 属性”窗口，如图 4-9 所示。
- 步骤 4 如果 Internet 协议 (TCP/IP) 属性如图 4-9 所示，则无需改动；如果 Internet 协议 (TCP/IP) 属性不是图 4-9 所示，则在“常规”中选择“自动获得 IP 地址”。
- 步骤 5 单击“确定”完成配置。

图 4-9 Internet (TCP/IP) 属性

---结束



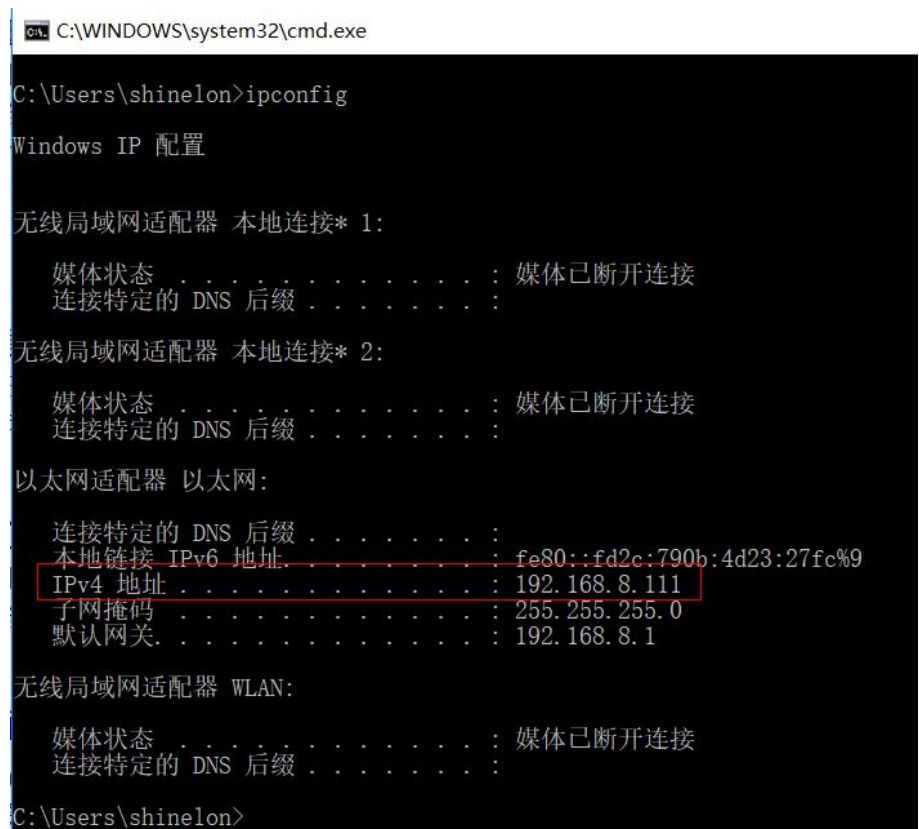
配置检查

- 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，如图 4-10 所示。

图 4-10 “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 显示的是输入的图 4-4 中的 IP 地址，如图 4-11 所示；以路由器 DHCP 自动获取 IP 的配置方法中 IP Address 显示的“2~254”的随机数字，如图 4-12 所示。窗口显示如图 4-12 所示信息表示 IP 配置正常。

图 4-11 指定 IP 方式的 “ipconfig” 执行结果



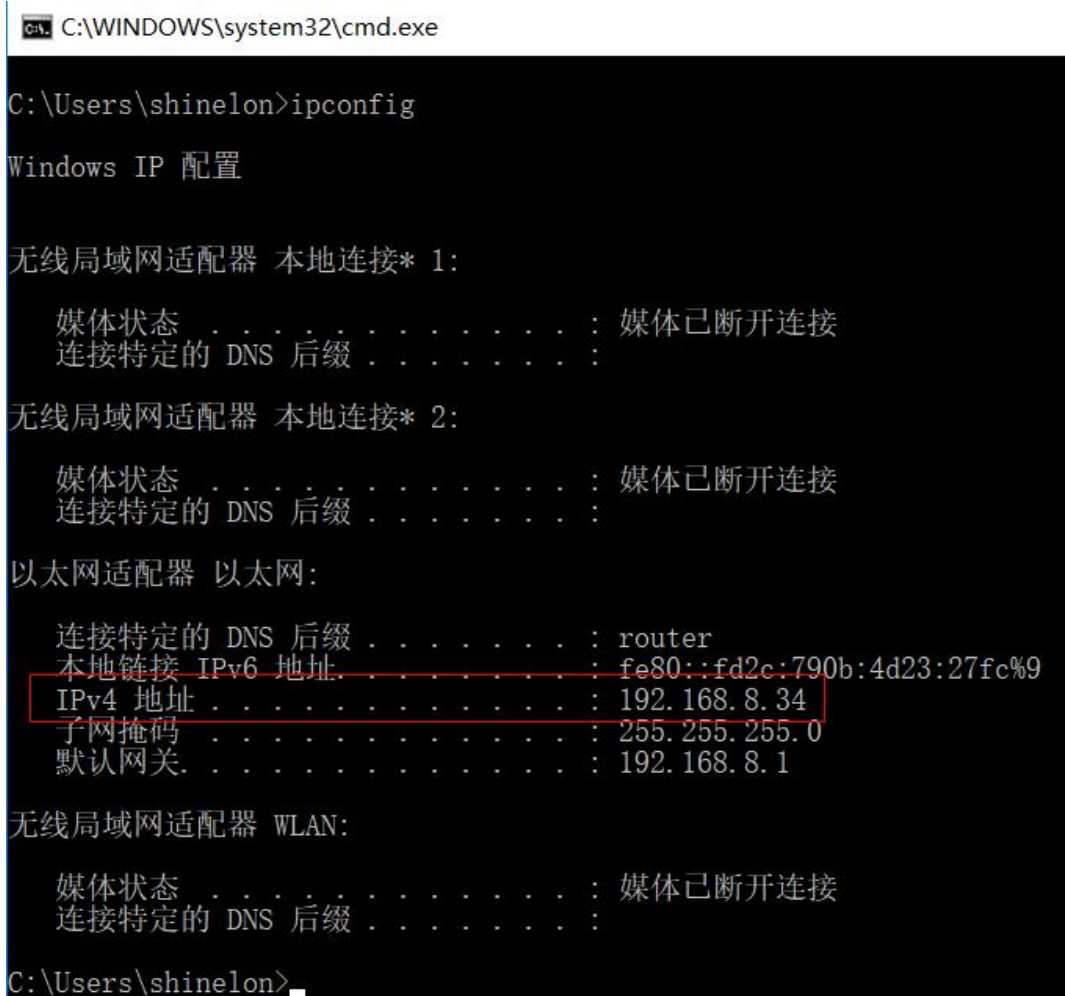


图 4-12 DHCP 自动获取 IP 方式“ipconfig”执行结果

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
```

如果出现如图 4-13 所示界面，表示本地计算机与 H8820 专用型工业路由器连通性正常。

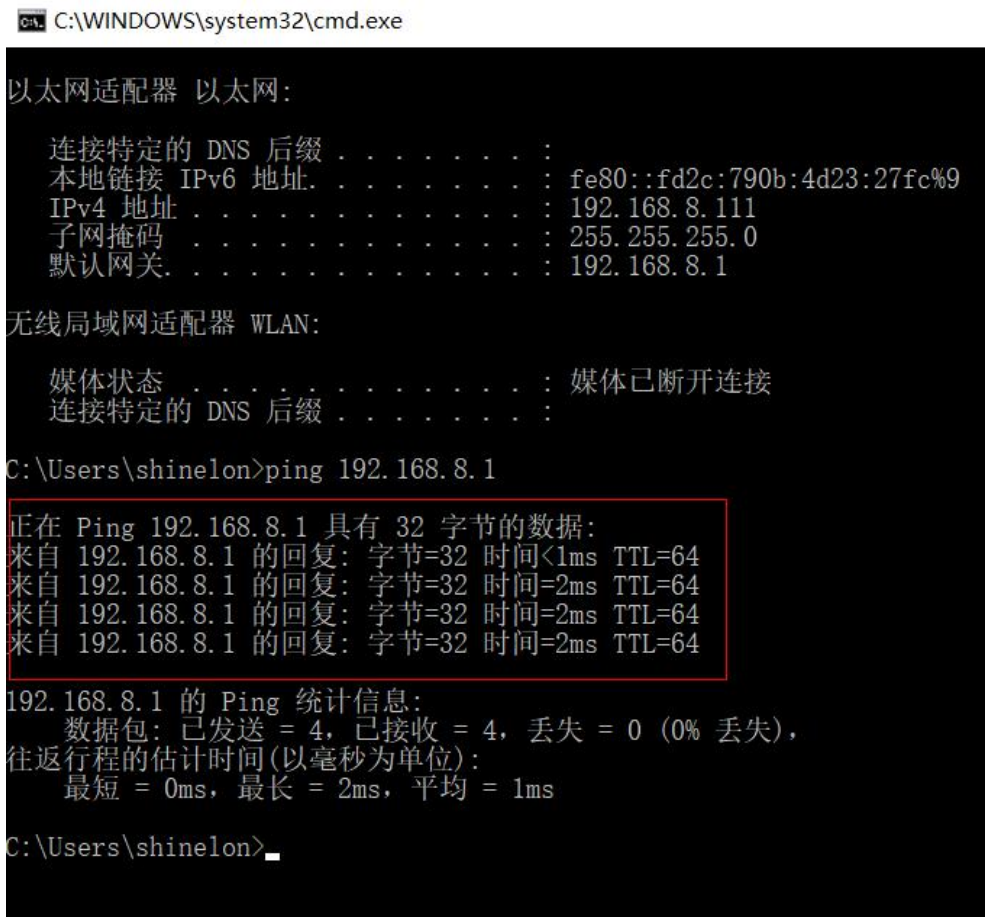


图 4-13 连通性验证结果

---结束

5 路由器配置

关于本章

章节	内容简介
5.1 概述	本节简要介绍 H8820 专用型工业路由器采用 WEB 方式进行配置操作。
5.2 基本配置	本节简要介绍 H8820 专用型工业路由器在进行高级配置前需要完成基本配置操作包含哪些内容。
5.3 应用程序配置	本节简要介绍 H8820 专用型工业路由器应用程序配置包含哪些，以及具体配置操作方法。
5.4 安全配置	本节简要介绍 H8820 专用型工业路由器安全配置包含哪些，以及具体配置操作方法。
5.5 转发配置	本节简要介绍 H8820 专用型工业路由器转发配置包含哪些，以及具体配置操作方法。
5.6 VPN 功能配置	本节简要介绍 H8820 专用型工业路由器 VPN 功能包含哪些，以及具体配置操作方法。
5.7 系统管理配置	本节简要介绍 H8820 专用型工业路由器系统管理配置包含哪些，以及具体的配置操作方法。
5.8 状态	本节简要介绍 H8820 专用型工业路由器状态查询包含哪些，以及状态查询方法。

5.1 概述

H8820 专用型工业路由器可采用 WEB 方式进行配置操作，该方式具有操作简便、直观等特点。按照“本地连接配置”完成 PC 机和 H8820 专用型工业路由器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 H8820 专用型工业路由器进行配置操作。

5.2 登录 WEB 配置界面

通过“5.2.2 网络设置”，可以实现拨号上网和访问公网基本功能。

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/”。进入用户登录身份认证界面，如图 5-1 所示。

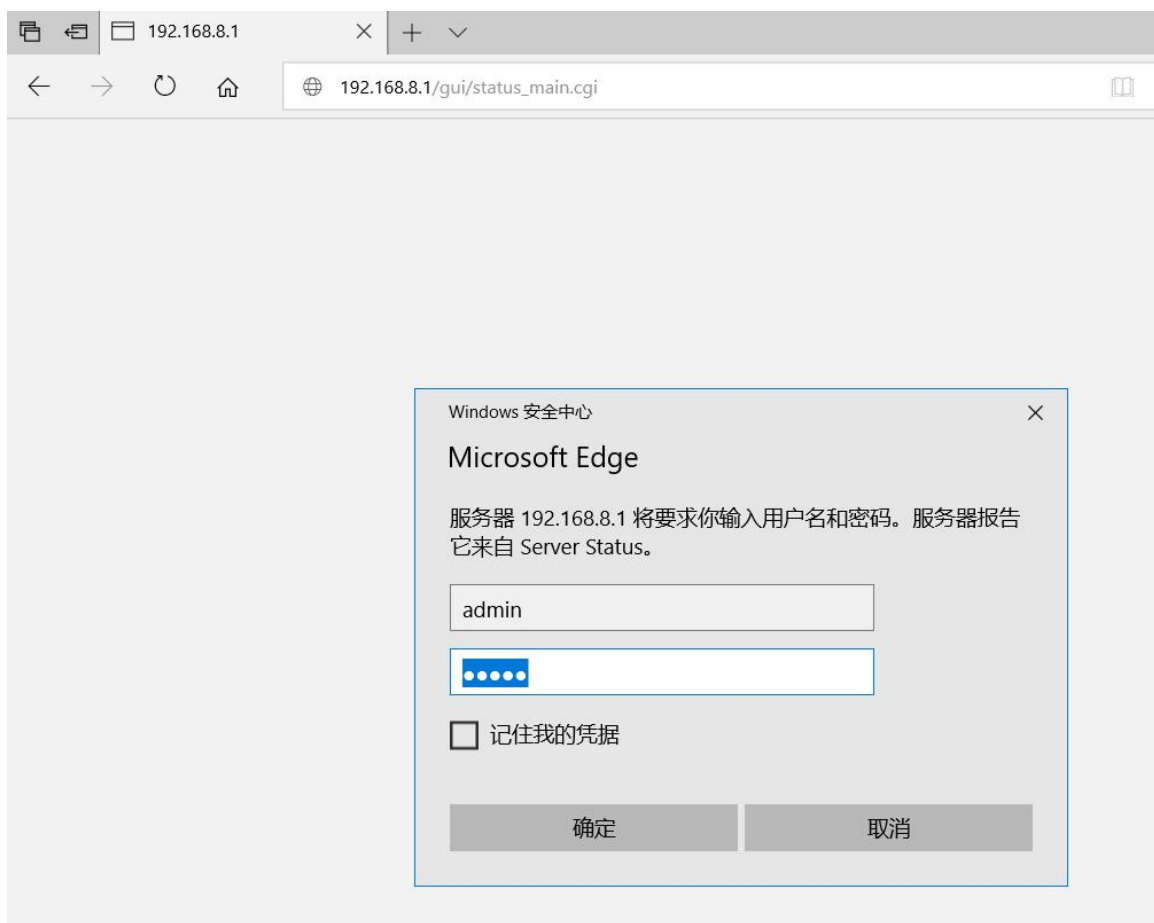


图 5-1 用户登录身份认证界面

步骤 2 输入“用户名”、“密码”，单击“确定”。即可登录到 H8820 专用型工业路由器的 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“5.7.5 用户管理”。

---结束

5.3 网络设置

步骤 1 网络设置主要完成 LAN、移动网络、参数切换以及网络连接、DHCP 服务器等配置。配置完成后可满足基本网络通信需要。

5.3.1 LAN

LAN 口配置主要用于路由器与下位机连接，使下位机可以通过路由器访问外网，同时保证连接在路由器上的各个网段之间能够正常通信。

步骤 1 登录 H8820 专用型工业路由器的 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“网络设置> LAN”。

打开“LAN”页签，如图 5-2 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

LAN

移动网络

参数切换

网络连接

DHCP服务

主机名

router

* 最大长度为32位

IP1

192.168.8.1/24

* 如：192.168.8.1/24

IP2

IP3

IP4

回环地址

如：10.1.1.1/24

保存

刷新

图 5-2 LAN 页签

步骤 3 配置 LAN 口连接参数，参数说明如表 5-1 所示。

表 5-1 LAN 口连接类型参数说明

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

参数名称	含义	如何配置
	消失。	请参见“参数规范表”。

步骤 4 单击“保存”，完成 LAN 口连接类型的配置。



说明

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

---结束

5.3.2 移动网络

移动网络是 H8820 专用型工业路由器最核心功能之一，H8820 专用型工业路由器支持单模单卡拨号，为用户提供高速无线宽带上网功能。

步骤 1 登录 H8820 专用型工业路由器的 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“网络设置>移动网络”。

打开“移动网络”页签，如图 5-3 所示。



图 5-3 移动网络页签

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

- 添加

1. 单击“添加”，显示“移动网络配置”添加界面，如图 5-4 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

LAN

移动网络

参数切换

网络连接

DHCP服务

帮助

自动拨号

启用

禁用

提示与建议:

如果新添加的规则名称已存在, 则原配置参数将被覆盖。

基本设置

接口名称

2

* 最大长度为12位

网络接入点

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

chap+pap

网络类型

auto

保存

返回

图 5-4 移动网络配置页面

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

表 5-2 “移动网络”参数说明

参数名称	含义	如何配置
自动拨号	使能当前 modem 参数用于 modem 拨号，所有使能的 modem 参数同时只有一个在运行（随机或者其他功能进行控制），当多套 modem 参数都禁用时则禁用 modem 拨号。	按钮选择。 • 启用 • 禁用 单击按钮后变成灰色表示当前状态生效，如“启用”显示为灰色时，表示功能或参数被启用。
接口名称	接口的唯一标识名，用于其他功能调用或者关联本接口时使用，如配置该接口的路由、控制该规则接口的禁用、启用。	字母数字型 WORD 类型，最大 12 字节，非空，输入规范请参见“参数规范表”。
网络接入点	接入运营商网络的一个标识信息，通常用于表示接入到运营商网络的类型，专网业务情况通常按照专网的业务类型来命名，由运营商或 ISP 提供。通常情况下 G 网运营商才有接入点配置。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。
用户名/密码	接入运营商网络身份标识，专网业务情况下用于接入到不同的专网业务中来隔离不同的专用网络。通常情况下 C 网运营商才有用户名密码，现在很多 G 网运营商也开始使用。	WORD 类型 /CODE 类型，各最大长度 64 字节，同时存在或同时为空。

参数名称	含义	如何配置
鉴权类型	pap:用于用户向 PPP 服务器证明自己的身份 chap:用于用户与 PPP 服务器之间的认证	单选框选择 • chap+pap • chap • pap • none
网络类型	通过该选项将所需接入网络类型强制为 2.5G 或者 3G/4G。通常某一网络不稳定或者只希望工作在某一网络情况下使用。	下拉框选项选项 AUTO/2G/3G/4G。 AUTO 表示 2.5G/3G/4G 自适应。

3. 单击“保存”，完成对“移动网络”的参数配置。

- 编辑
如图 5-4 中确定某一条参数配置记录，单击“编辑”，即可对该条参数记录进行编辑操作。参数说明如表 5-3 所示。
- 删除
如图 5-4 中确定某一条参数配置记录，单击“删除”，即可删除该条参数记录。
- 启用
如图 5-4 中确定某一条参数配置记录，单击“启用”，即可启用该条参数配置。
- 禁用
如图 5-4 中确定某一条参数配置记录，单击“禁用”，即可禁用该条参数配置生效。
- 刷新
单击“刷新”，刷新当前页面。



说明

当按钮为灰色时，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启用状态。

---结束

5.3.3 参数切换

H8820 专用型工业路由器参数切换功能是我司自主研发的备份切换功能，具备多功能组合的备份与切换。其主要应用场景是：多服务端互备份，多运营商备份（很多国家一个 SIM 卡支持多个运营商，某一运营商网络异常则切换到另外一个运营商）。

步骤 1 登录 H8820 专用型工业路由器的 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“网络设置>参数切换”。

打开“参数切换”页签，如图 5-5 所示。



图 5-5 参数切换页签

步骤 3 配置“参数切换”相关参数。

可以“添加”、“编辑”、“删除”、“启用”、“删除”对应的“参数规则”。

- 添加

1. 单击“添加”，显示“参数切换配置”页面，如图 5-14 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

LAN

移动网络

参数切换

网络连接

DHCP服务

规则名称	接口名称	检测方法	操作
------	------	------	----

状态

启用禁用

基本信息

规则名称* 0-9

间隔时间

60

* 1-512 秒

重试次数

3

* 1-512

超时时间1-65535 秒

保存

添加接口检测规则

接口名称

modem 111

检测方法

state

添加

刷新

返回

图 5-6 参数切换配置页面

2. 添加一条“参数备份”规则。
参数说明如表 5-3 所示。

表 5-3 参数切换参数说明

参数名称	含义	如何配置
状态	使能当前规则。所有使能规则同时只有一个规则在运行，所有禁用规则中关联接口都为禁用状态。如：rule0 中选择 modem0、ipsec1、vpdn2，若 rule0 禁用则 modem0、ipsec1、vpdn2 则都被禁用。	按钮选择 - 启用 - 禁用
基本信息		
规则名称	参数切换规则名称标识，用于区分不同的规则。	取值范围：[0,9]
间隔时间/重试次数	检测的时间间隔和最大失败次数。若失败次数达到配置的次数则切换到下一	取值范围：1~512 单位：秒/次数

文档版本 V1.0.0.1(2019-11-15)

参数名称	含义	如何配置
	条规则进行工作。	默认值：60/3
超时时间	用于限定当前规则最大工作时间，rule0 中该参数无效，其他规则中配置该参数并且到达最大工作时间后切换到 rule0，不配置则按 rule 的顺序切换。通常没有严格主备要求时不建议配置。	取值范围：1~65535 单位：秒
添加接口检测规则		
接口名称	规则关联参数接口名称，如 modem 接口名称：modem0。	下拉框选项，取决于当前系统配置接口名称个数，自动生产。
检测方法	检测方法分为接口状态检测和 ICMP 检测，通过检查状态或者链路来判定是否需要切换到下一条规则（达到最大失败次数后切换）。	下拉框选项 • state • icmp
目的 IP	选择 icmp 检测方法时才需要配置，用于配置 icmp 检测目的地址。	接口型 A.B.C.D，输入规范 请参见“参数规范表”。 例如：192.168.8.2

3. 单击“添加”完成规则添加。
- 删除
单击“删除”，删除选中的“参数切换规则”。
 - 启用
单击“启用”，启动并应用该“参数切换规则”。
 - 禁用
单击“禁用”，禁用该“参数切换规则”。
 - 刷新
单击“刷新”，刷新当前页面。

---结束

5.3.4 网络连接

为用户提供默认路由配置页面。

步骤 1 登录 H8820 专用型工业路由器的 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“网络设置>网络连接”。

打开“网络连接”页签，如图 5-7 所示。



图 5-7 网络连接页签

步骤 3 配置“网络连接”相关参数。
参数说明如表 5-4 所示。

表 5-4 网络连接参数说明

参数名称	含义	如何配置
默认路由	路由器数据包默认的转发路径。根据具体需要配置默认路由，当需要多网切换可以参见链路备份功能。	下拉框选项 根据需要进行配置。
DNS 类型	配置路由器的 DNS 类型，选择接口时则使用接口拨号等方式自动的获取 DNS。	下拉框选项 • interface • custom
DNS1/DNS2	DNS 类型选择 custom 时配置，手动配置 DNS 地址，最多可配置两个。	接口型 A.B.C.D 例如：8.8.8.8
接口名称	DNS 类型选择 interface 时配置，配置后路由器使用 DNS 关联接口获得的 DNS，所以需要特别注意该接口是否能获取 DNS。	下拉框选项 • modem

步骤 4 单击“保存”，完成网络连接的配置。
---结束

5.3.5 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 H8820 专用型工业路由器 WEB 配置界面。
登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“网络设置>DHCP 服务”。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

LAN

移动网络

参数切换

网络连接

DHCP服务

DHCP 服务

启用

禁用

基本设置

标识名

最大长度为32位

地址池

br0

网关类型

default

DNS 类型

default

租约时间

3600

* 120-86400 秒

IP

* 如: 192.168.8.1

MAC

* 如: 00:1A:4D:34:B1:8E

添加

IP

MAC

操作

保存

刷新

打开“DHCP 服务”页签，如图 5-8 所示。

图 5-8 DHCP 服务页签

步骤 3 配置“DHCP 服务器设置”。

DHCP 服务器设置参数如表 5-5 所示。

表 5-5 DHCP 服务器设置参数说明

参数名称	含义	如何配置
DHCP 服务	DHCP 服务使能按钮，用于启用/禁用 DHCP 服务。	按钮选择设置。 • 启用 • 禁用
基本设置（DHCP 在无特殊组网要求的情况下不建议配置）		
地址池	DHCP 客户端获取 IP 地址的范围。选择接口时则表示关联接口的网段。该选项通常需要在指定下位机可分配的地	下拉框选项 • br0 • custom

参数名称	含义	如何配置
	址范围时配置，例如：只希望最多四台机器能自动获取 IP。	
起始 IP	地址池选择 custom 时配置，配置 DHCP 地址池的起始 IP 地址。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.8.2
结束 IP	地址池选择 custom 时配置，配置 DHCP 地址池的结束 IP 地址。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.8.254
网关类型	DHCP 客户端获取的网关 IP 来源，分为 default、br0、custom 四类，关联接口时则将接口的 IP 分配给 DHCP 客户端作为网关。	下拉框选项 默认值：default
网关	网关类型选择 custom 时配置，通常需要指定下位机网关 IP 时使用。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.8.1
DNS 类型	DHCP 客户端获取的 DNS IP 的来源，有 default、modem、br0、custom 等方式，通常不建议修改该配置，特别是双模应用场景下不建议配置。	下拉框选项 • default • modem • mdoem2 • br0 • custom 配置为 default 则根据路由器本身的 DNS 地址来分配。
DNS1/DNS2	DNS 类型选择 custom 时配置，配置 DHCP 客户端获取 DNS 的 IP 地址。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：8.8.8.8
租约时间	DHCP 客户端获取 IP 后对 IP 租用时间，客户端通常在租约时间过半的时候重新协商获取 IP 地址。租约时间主要是用于释放空闲的 IP，避免 DHCP 客户端关机之后还占用 IP 地址资源。	取值范围：120~86400 单位：秒 默认值为 3600
IP、MAC 绑定，用于为指定范围内的机器分配的固定的 IP 地址		
IP	与指定的 MAC 配对，当被绑定 MAC 的 DHCP 客户端发起 DHCP 请求时则会与该 MAC 地址绑定的 IP 地址分配给它。该 IP 地址即使没有被占用也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“参数规范表”。 例如：192.168.8.2
MAC	配置需要指定 DHCP 获取 IP 的 DHCP	WORD 类型 MAC 格式

参数名称	含义	如何配置
	客户端的 MAC 地址。	例如：00:1A:4D:34:B1:8E

---结束

5.4 应用程序配置

H8820 专用型工业路由器根据多年用户应用场景，除了常用的 SNMP、DDNS 等功能之外还自主研发了很多适用于无线网络产品的功能，主要有 ICMP 链路检测、M2M 终端管理、任务管理功能等。

5.4.1 ICMP 检测

无线网络存在假链接（拨号获得 IP 在，但是链路不通）等异常现象，通常通过 LCP 等方式进行维护，H8820 专用型工业路由器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，H8820 专用型工业路由器支持对 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 H8820 专用型工业路由器 WEB 配置界面。
登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“应用程序设置>ICMP 检测”。
打开“ICMP 检测”页签，如图 5-9 所示。



图 5-9 ICMP 检测页面

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

- 添加

1. 单击“添加”，显示“ICMP 检测”的添加界面，如图 5-10 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

ICMP 检测

DDNS设置

SNMP 设置

M2M设置

任务管理

检测服务

启用

禁用

基本设置

规则名称

* 最大长度为12位

检测类型

icmp

目的地址

114.114.114.114

* 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

br0

超时动作

modem-reset

保存

返回

图 5-10 ICMP 添加页面

2. 配置 ICMP 检测服务参数。

参数说明如表 5-6 所示。

表 5-6 ICMP 检测规则参数说明

参数名称	含义	如何配置
检测服务	使能 ICMP 检测规则。多条规则可同时运行，也可禁用某一条规则。	按钮 • 启用 • 禁用
基本设置		
规则名称	ICMP 检测规则名称标识，没有特定意义，仅用于区分不同规则。	WORD 类型，最大 12 字节，输入规范请参见“参数规范表”。
目的地址	ICMP 检测目的地址，可以是 IP 也可以是域名，设置为域名时需要确保路由器配置正确的 DNS。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。
备份地址	ICMP 检测备份目的地址，主地址检测不通时检测备份地址，若备份地址检测不通则判定检测失败。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。

参数名称	含义	如何配置
检测间隔/重传次数	链路正常时检测时间间隔和最大失败次数。最大失败次数到达则执行 ICMP 规则对应的动作任务，例如：modem 重新拨号等。	取值范围：1~65535 单位：秒/次
源接口	路由器发送 ICMP 检测包的源地址	下拉框选项 • br0 • modem
超时动作	当检测失败达到最大失败次数时执行的动作，主要有重拨号、自定义动作。	下拉框选项。 • modem-reset: modem 重拨号
执行命令	超时动作选择 custom 时配置，命令为后台操作命令，通常不建议使用。如有配置需要请联系我司技术人员。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。

3. 单击“保存”，完成一条 ICMP 检测规则的添加。



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，则路由器执行“超时动作”。

- 编辑
- 如图 5-11 中确定某一条参数配置记录，单击“编辑”，即可对该条参数记录进行编辑操作。参数说明如表 5-6 所示。



图 5-11 ICMP 编辑页面

- 删除
- 如图 5-11 中确定某一条参数配置记录，单击“删除”，即可删除该条参数记录。
- 启用

- 如图 5-11 中确定某一条参数配置记录，单击“启用”，即可启用该条参数配置。
 - 禁用
 - 如图 5-11 中确定某一条参数配置记录，单击“禁用”，即可禁用该条参数配置生效。
 - 刷新
 - 单击“刷新”，刷新当前页面。
- 结束

5.4.2 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 机通过域名访问路由器的页面。当然，路由器使用的 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路由器。

- 步骤 1 登录 H8820 专用型工业路由器 WEB 配置界面。
登录方法请参见“5.2.1 登录 WEB 配置界面”。
- 步骤 2 单击“应用程序设置>DDNS 设置”。
- 打开“DDNS 设置”页签，如图 5-12 所示。



图 5-12 DDNS 设置页签

- 步骤 3 配置 DDNS 服务参数。
- 参数说明如表 5-7 所示。

表 5-7 DDNS 服务参数说明

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

步骤 4 单击“保存”，完成 DDNS 服务配置。



说明

- 国内的 DDNS 服务商：88IP（www.88ip.net）、3322（www.3322.org）
- 国外的 DDNS 服务商：DNSEXIT(www.dnsexit.com)、ZONEEDIT(www.zoneedit.com)、CHANGEIP(www.changeip.com)、DYNDNS(www.members.dyndns.org)
- 每次路由器重启时，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路由器时使用的是申请到的 DDNS 域名，那么不管路由器 modemIP 地址怎么改变，用户都可以登录到路由器页面。

---结束

5.4.3 DTU 设置

H8820 4G Router 系统内置与注册中心和数据中心通信功能，可提供类似 DTU(Data Transfer Unit，数据传输单元的传输，是专门用于将串口数据转换为 IP 数据或将 IP 数据转换为串口数据通过无线通信网络进行传送的无线终端设备，具有透明数据传输功能)功能，同时也提供缓存功能，避免数据中心发生切换后而导致的丢包。

步骤 1 登录 H8820 4G Router WEB 配置界面。

登录方法请参见“5.2 登录 WEB 配置界面”。

步骤 2 单击“应用程序设置>DTU 配置”。

打开“DTU 配置”页签，选择不同工作模式，如图 5-13、图 5-14、图 5-15 所示。



注意

- 当“工作模式”选择“客户端”时，将显示“数据中心设置”页签和“心跳设置”页签，对应图 5-22。
- 当“工作模式”选择“DDP 客户端”时，将显示“数据中心设置”页签和“心跳设置”页签，并且在“基本设置”中显示参数“身份识别码”，对应图 5-14。
- DDP 客户端模式可支持 TCP、UDP 协议。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

ICMP 检测

DDNS设置

DTU设置

SNMP 设置

M2M设置

任务管理

帮助

DTU 服务

启用 禁用

基本设置

工作模式

客户端

本地端口

1-65535

传输协议

TCP

UDP

通信类型

三中心

主备

接收报文超时

1-65535 毫秒

最后包空闲时间

1-65535 毫秒

数据中心设置

服务地址

最大长度为64位

服务端口

1-65535

服务地址2

最大长度为64位

服务端口2

1-65535

服务地址3

最大长度为64位

服务端口3

1-65535

重连间隔

1-65535 秒

重连次数

1-65535

注册包配置

注册包内容

最大长度为64位

心跳设置

心跳内容

最大长度为64位

心跳间隔

1-65535 秒

串口参数设置

速率

115200

校验位

none

数据位

8

停止位

1

保存

刷新

工作模式:

当工作模式为服务器模式时, 端口号为必填项。如果是客户端模式, 本地端口为空, 服务将随即获取端口。

数据中心:

当工作模式为"服务器"时, 您无须设置数据中心; 若为"客户端"模式, 请设置数据中心。

注册包配置:

当注册包配置为十六进制时, 配置内容需要以"0x"或"0X"开头为标志位, 比如"0x123abc", "0X123abc"

心跳设置:

当心跳包配置为十六进制时, 配置内容需要以"0x"或"0X"开头为标志位, 比如"0x123abc", "0X123abc"

图 5-13 DTU 服务器配置界面

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

ICMP 检测

DDNS设置

DTU设置

SNMP 设置

M2M设置

任务管理

帮助

DTU 服务

启用禁用

基本设置

工作模式

本地端口

传输协议

接收报文超时

最后包空闲时间

串口参数设置

速率

校验位

数据位

停止位

保存

刷新

工作模式:

数据中心:

注册包配置:

心跳设置:

图 5-14 DTU 客户端配置页面

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

ICMP 检测

DDNS设置

DTU设置

SNMP 设置

M2M设置

任务管理

帮助

DTU 服务

启用禁用

基本设置

工作模式

本地端口

身份识别码

传输协议

通信类型

接收报文超时

最后包空闲时间

数据中心设置

服务地址

服务端口

服务地址2

服务端口2

服务地址3

服务端口3

重连间隔

重连次数

心跳设置

心跳间隔

串口参数设置

速率

校验位

数据位

停止位

保存

刷新

工作模式:

数据中心:

注册包配置:

心跳设置:

图 5-15 DDP 客户端配置页面

步骤 3 如果 DTU 在服务器工作模式下工作，需配置 DTU 为服务器工作模式下的参数，如图 5-13 所示。

如果 DTU 在客户端/DDP 客户端工作模式下工作，需设置“工作模式”为“DTU 客户端”或“DDP 客户端”，并配置相应参数。如图 5-14 和图 5-15 所示。参数说明如表 5-8 所示。

表 5-8 DTU 参数说明

参数名称	含义	如何配置
DTU 服务	启用/禁用 DTU 服务。	单击“启用”按钮即启用。
基本设置		
工作模式	DTU 工作模式，可设置为： • 服务器：路由器作为 DTU 服务器使用。 • 客户端：路由器作为 DTU 客户端使用。 • DDP 客户端：路由器作为 DDP 客户端使用（DDP 协议为我司专有协议）。	下拉列表选择。
本地端口	DTU 服务端口。	手动输入。
身份识别码 (当工作模式 选择为 DDP 客户端时需 要配置的属 性)	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”。
传输协议	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，适用于对效率要求相对高、对可靠性要求相对低的场景。	单选按钮选择。 根据自身需求可以选择。
通道类型	数据传输通道类型设置 • 三中心：三中心通道指的是可以设置三个主通道，可同时在线；三个通道是相互独立，若通道 1 发生故障的时候不会影响其他两个通道的通信。	单选按钮选择。 根据自身需求可以选择。

参数名称	含义	如何配置
	主备：主备通道指的是 DTU 可以设置一个主通道，一个备通道，当主通道发生故障的时候 DTU 会自动转换到备用通道运行，当备通道没有数据发送时重新尝试连接主通道。	
UDP 接收报文最大长度	当工作模式选择“DDP 客户端”时需配置，表示 UDP+DDP 协议通讯时可接收的报文的最大长度。若发送报文超过最大长度，则 DDP 客户端丢弃超出的部分报文。	手动输入。 取值范围：1~65535 单位：字节 请根据实际情况配置最大报文长度。
接收报文超时	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。	手动输入。 取值范围：1~65535 缺省值：500 单位：毫秒
最后包空闲时间	DTU 串口向数据中心端发送数据的等待时间。 如果在该时间内，发送的数据已经超过 UDP/TCP 接收报文最大报文长度，则立即发送；若没有超过 UDP/TCP 接收报文最大报文长度，则等待数据，直到到达最后包空闲时间，然后一起发送。	手动输入。 取值范围：1~65535 缺省值：500 单位：毫秒
数据中心设置 【参数仅在“客户端”、“DDP 客户端”工作模式下需配置】 注：当工作模式为“客户端”且“传输协议”为“TCP”，工作模式为“DDP 客户端”时候需配置“服务地址 2”和“服务端口 2”。		
服务地址	DTU 数据中心服务器（DSC）的 IP 地址或域名。	A.B.C.D 接口型或一般 WORD 型，输入规范请参见“参数规范表”。
服务端口	DTU 数据中心的端口号（必须与服务器设置的服务端口一致）。	手动输入。 取值范围：1~65535
服务地址 2	DTU 数据中心服务器（DSC）的 IP 地址或域名，用于和“服务地址”	A.B.C.D 接口型或一般 WORD 型，输入规范请参见“参数规范

参数名称	含义	如何配置
	互相备用。	表”。
服务端口 2	DSC 数据中心的端口号（必须与服务器设置的服务端口一致）。	手动输入。 取值范围：1～65535
服务地址 3	DTU 数据中心服务器（DSC）的 IP 地址或域名，用于和“服务地址”互相备用。	A.B.C.D 接口型或一般 WORD 型，输入规范请参见“参数规范表”。
服务端口 3	DSC 数据中心的端口号（必须与服务器设置的服务端口一致）。	手动输入。 取值范围：1～65535
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
心跳设置		
心跳内容	设置心跳发送内容（无数据发送时，每隔心跳时间，路由器就发出该内容一次）	手动输入。 最大输入长度：64 位
心跳间隔	设置心跳发送间隔时间（无数据发送时，每隔这个时间，路由器就发出心跳内容一次）。	手动输入。 取值范围：1～65535 单位：秒
串口参数设置（主要用于和 DTU 端口相连的设备之间的正确连接）		
速率	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。 缺省：115200
校验位	数据校验方式。	下拉列表选择。 根据 DTU 的实际串口要求设置。 取值范围：None、Odd、Even 缺省：None(无校验)
数据位	数据传输位。	下拉列表选择。 根据 DTU 的实际串口要求设置。 取值范围：5、6、7、8 缺省：8

参数名称	含义	如何配置
停止位	数据停止位。	下拉列表选择。 根据 DTU 的实际串口要求设置。 取值范围：1、2 缺省：1

步骤 4 单击“保存”，完成 DTU 服务器/客户端/DDP 客户端配置。

---结束

5.4.4 SNMP 配置

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

步骤 1 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“应用程序设置>SNMP 配置”。

打开“SNMP 配置”页签，如图 5-16 所示。



该截图展示了 H8820 专用型工业路由器的 SNMP 配置界面。顶部有多个配置标签，包括“网络设置”、“应用程序设置”（当前选中）、“VPN 设置”、“转发设置”、“安全设置”、“系统管理”和“状态”。在“应用程序设置”下，有“ICMP 检测”、“DDNS 设置”、“SNMP 设置”（当前选中）、“M2M 设置”和“任务管理”子标签。主配置区域包含“SNMP 服务”开关，目前处于“启用”状态。下方是“基本设置”区域，包含以下配置项：

- 服务端口：输入框，右侧标注“* 1-65535”
- 共同体：输入框，右侧标注“* 最大长度为32位”
- Trap IP：输入框，右侧标注“如：192.168.8.1”
- Trap 端口：输入框，右侧标注“1-65535”
- 回环标识状态：包含两个单选按钮，“启用”和“禁用”，其中“禁用”按钮被选中。

底部有“保存”和“刷新”两个操作按钮。

图 5-16 SNMP 配置页签

步骤 3 配置 SNMP 参数。

参数说明如表 5-9 所示。

表 5-9 SNMP 参数说明

参数名称	含义	如何配置
SNMP 服务	使能 SNMP 服务。	单选按钮选择。 • 启用 • 禁用
基本设置		
服务端口	SNMP 服务侦听端口，建议配置为其默认端口 161。	取值范围：1~65535 缺省：161
共同体	SNMP 客户端连接路由器 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	路由器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	路由器链路状态上报的服务器端口。	取值范围：1~65535 缺省：162
回环标识状态	与“LAN”页面中的回环地址对应：在“回环标识状态”为“启用”，如果回环地址配置成功，则路由器 Trap 上报的 IP 包源地址就是回环地址；若“回环标识状态”为“禁用”，则路由器 Trap 上报的 IP 包源地址为 LAN 口地址。	单选按钮选择 • 启用 • 禁用

步骤 4 单击“保存”，完成 SNMP 配置。



说明

Trap：SNMP 协议 5 个数据类型中的一个，指被管理设备上报的陷阱报文，表明设备发生故障或变更的通知。H8820 专用型工业路由器上报 Trap 的类型和内容包括：modem 的连接状况及哪个接口、哪张 SIM 卡拨号，VPDN/TUNNEL/IPSec 接口的连接和断开等。

与 SNMP 对应的 MIB 库可以在我司公网上下载，如有需要，请联系我司技术人员。

---结束

5.4.5 M2M 配置

H8820 专用型工业路由器通过 WMMP 协议（Wireless Machine-to-Machine Protocol）实现与 M2M（Machine-to-Machine）平台通信功能，可通过平台实现对设备的远程维护管理和现场网络状态的监控管理，如查看设备信息、升级补丁、升级固件、配置参数等，查看设备网络信号强度、时延、流量等。具体设置说明如下。

步骤 1 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“应用程序设置>M2M 配置”。

打开“M2M 配置”页签，如图 5-17 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

ICMP 检测

DDNS 设置

SNMP 设置

M2M设置

任务管理

M2M 服务

启用禁用

基本设置

服务IP或域名

www.iotvip.site

* 最大长度为64位

服务端口

5002

* 1-65535

状态

disconnected

保存

刷新

图 5-17 M2M 配置页签

步骤 3 配置 M2M 参数。

参数说明如表 5-10 所示。

表 5-10 M2M 参数说明

参数名称	含义	如何配置
M2M 服务	使能 M2M 服务，该功能需要配合我司 M2M 终端管理平台使用。	按钮 - 启用 - 禁用
基本设置		
服务 IP 或域名	设备云平台服务器的 IP 地址或域名。	WORD 类型，最大 64 个字节，输入规范请参见“参数规范表”。

参数名称	含义	如何配置
服务端口	设备云平台服务器 WMMP 服务所使用的端口号，与服务器匹配即可。	取值范围：1～65535
状态		• Disconnected • connected

---结束

5.4.6 任务管理设置

H8820 专用型工业路由器任务管理能够为用户提供路由器在线时长、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。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

打开“任务管理”页签，图 5-18 所示。

网络设置	应用程序设置	VPN设置	转发设置	安全设置	系统管理	状态
ICMP 检测	DDNS设置	DTU设置	SNMP 设置	M2M设置	任务管理	

帮助

任务名称	定时	任务类型	操作
------	----	------	----

添加

刷新

提示与建议:

为使定时管理生效, 请您设定正确的系统时间。

命令条数限制:

您最多能设定10条规则!

命令格式:

命令不能包含这些字符: '<'、'>'。

时间格式:

时间模式支持三种: 时间间隔, 时间范围, 时间点。其中时间点设定方式为将前后时钟设置为相同值时, 即为时间点。
online动作只支持时间范围模式, reboot及custom动作不支持时间范围模式。

图 5-18 任务管理设置页签

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

ICMP 检测

DDNS设置

DTU设置

SNMP 设置

M2M设置

任务管理

帮助

状态

启用禁用

提示与建议:

为使定时管理生效, 请您设定正确的系统时间。

基本设置

任务名称

* 最大长度为12位

任务类型

modem-online

reboot

时间格式:

时间模式支持三种: 时间间隔, 时间范围, 时间点。其中时间点设定方式为将前后时钟设置为相同值时, 即为时间点。online动作只支持时间范围模式, reboot及custom动作不支持时间范围模式。

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

保存

返回

图 5-19 任务管理配置界面

- 步骤 3 若需添加新的任务管理规则，请单击“添加”，进入任务管理规则设置界面，如图 5-19 所示。
- 步骤 4 配置任务管理规则参数。
- 参数说明如表 5-11 所示。

表 5-11 任务管理规则参数说明

参数名称	含义	如何配置
状态	使能定时规则。多条规则可同时运行，也可禁用某一条规则。本功能除了时间间隔类型动作任务外，其他任务需要配合 NTP 服务一起使用，否则很难达到合理的时间任务控制。	单选框选择。 - 启用 - 禁用
基本设置		
任务名称	任务管理规则名称标识，仅用于区分不同的规则。	最大长度为 12 位，输入规范请参见“参数规范表”。
任务类型	任务主要有动作类任务和状态类任务，动作类任务配置为时间点或者时间间隔，状态类任务则配置为时间段，状态类任务只有在线，它表示所配置时间区域 modem 处	下拉框选项 - modem-online - reboot

参数名称	含义	如何配置
	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）。	
命令	命令为后台操作命令，通常不建议使用，如有配置需要请联系我司技术人员。	WORD 类型，最大 64 个字节，输入规范请参见“参数规范表”。
设置时间		
时间类型	分为时间范围和时间间隔，分别对应状态任务和动作任务。	下拉框选项 • range • interval
当“时间类型”选择“range”时		
时钟	配置小时、分钟，，当时间间隔前后一致则表示时间点，适用于动作类任务。	取值范围：[00:00,23:59] 格式：HH:mm-HH:mm
天数	任务执行的天数，表示一个月中的某天的某个时间段或时间点执行任务。	取值范围：[01,31] 格式：XX-XX
星期	动作执行的星期设置。 代表一个星期中某天的某个时间段或时间点执行任务。 当天数和星期都配置时表示两个时间条件同时满足时执行任务。	取值范围：[1,7] 格式：X-X 1 表示星期一
当“时间类型”选择“interval”时		
时间间隔	动作类任务除了可以配置时间点执行外，还可以配置为每隔一段时间执行一次。	取值范围：1~65535 单位：分钟

步骤 5 单击“保存”，完成任务管理服务配置。

当任务管理的时间类型为“range”时，则必须先开启“系统时间”，即 NTP 服务（任务管理暂时不支持手动对时）；若时间类型为“interval”，则不需要开启“系统时间”。要使用“系统时间”，请参见“5.7.4 系统时间”。

因考虑到 modem 的稳定性，路由器有多个对 modem 操作的功能，如任务管理、参数切换、链路备份、ICMP 检测、触发设置等，其中任务管理是改变保持 modem 状态，而其它功能则

是改变 modem 状态但并不保持，故在使用任务管理时请兼顾其它功能，如有需要，可联系我司技术人员。

---结束

5.5 安全配置

5.5.1 概述

安全设置是指路由器的防火墙功能。H8820 专用型工业路由器支持 IP 过滤、域名过滤和 MAC 地址过滤等三种安全设置。用户通过分析进入路由器数据包的 IP 地址/端口、MAC 地址、域名，与用户添加的防火墙规则进行对比，并对与防火墙规则匹配的数据包执行接收或丢弃动作来达到如允许/禁止某些网段访问外网、允许/禁止其他用户访问路由器等目的。

5.5.2 IP 过滤

IP 过滤是指路由器通过过滤 ip 地址规则来判定是否允许外部设备访问路由器以及是否允许数据包经过路由器转发，IP 过滤通常用来实现只允许某一部分主机访问外网或禁止某一部分主机访问特定网络。

步骤 1 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“安全设置>IP 过滤”。

打开“IP 过滤”页签，如图图 5-19 所示。



图 5-20 IP 过滤页签

转发过滤规则中，

- 黑名单：默认允许数据包转发，符合名单中“丢弃”规则的数据包不能经过路由器转发。
- 白名单：默认拒绝数据包转发，符合名单中“接受”规则的数据包可以经过路由器转发出去。

步骤 3 单击“添加”，添加一条新的 IP 过滤规则，配置 IP 过滤参数。IP 过滤有两种过滤类型：“输入”和“转发”，规则配置页面如图 5-21 和图 5-22 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

IP 过滤

域名过滤

MAC过滤

基本设置

过滤类型

☐ 输入

☒ 转发

过滤动作

☒ 接受

☐ 丢弃

镜像规则

☐ 启用

☒ 禁用

协议

all

▼

源地址

* 192.168.8.1 或 192.168.8.0/24

源端口

1-65535或[1-65535]

目的地址

* 192.168.0.1,192.168.0.1/24

目的端口

1-65535或[1-65535]

保存

返回

图 5-21 输入过滤规则页面

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

IP 过滤

域名过滤

MAC过滤

基本设置

过滤类型

☒ 输入

☐ 转发

过滤动作

☒ 接受

☐ 丢弃

协议

all

▼

源地址

* 192.168.8.1 或 192.168.8.0/24

源端口

1-65535或[1-65535]

目的地址类型

interface

▼

接口

br0

▼

目的端口

1-65535或[1-65535]

保存

返回

图 5-22 转发过滤规则页面

参数说明如表 5-12 所示。

表 5-12 IP 过滤参数说明

参数名称	含义	如何配置
过滤类型	选择一种过滤类型，可以根据自身需求选择“输入”或者“转发”。 • 输入：是否允许访问路由器。 • 转发：是否允许经过路由器转发。	单选按钮选择。
过滤动作	该条规则的默认动作。可以选择“接受”或“丢弃”。 • 接受：防火墙接受这个包，即可以通过。 • 丢弃：防火墙对这个包直接做丢弃处理。	单选按钮选择。 根据自身需求选择“接受”或“丢弃”即可。
镜像规则	当过滤类型选择“转发”时需要配置 • 启用：在所配置规则基础上额外添加一条源地址/端口与目的地址/端口反向的规则； • 禁用：不做任何处理。	单选按钮选择。
协议	IP 数据包使用的协议	下拉列表选择。 • all • tcp • udp • icmp
源地址	IP 数据包的源地址。	格式：A.B.C.D 型，输入规范请参见“参数规范表”。 例如：192.168.8.1 或 192.168.8.1/24
源端口	IP 数据包的源端口，当协议选择“icmp”时，不需要配置。	取值范围：1~65535 或 [1-65535]；可以是范围，也可以是单个端口。
当过滤类型选择“输入”时		
目的地址类型	指定 IP 数据包访问的路由器接口。	下拉列表选择。 • interface • any
接口	目的地址类型选择“interface”时需要配置，表示 IP 数据包访问的路由器端口（若目的地址类型选择的是“any”，则表示路由器的所有接口）。	下拉列表选择。 • br0 • modem
目的端口	IP 数据包访问的路由器端口（当协议选择“icmp”时，不需要配置）	取值范围：1~65535 或 [1-65535]；可以是范围，也可以是单个端口。
当过滤类型选择“转发”时		

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

步骤 4 单击“保存”，完成该条 IP 过滤规则配置。



说明

IP 输入规则表示是否允许其他设备访问路由器，该规则中的目的地址只能选择路由器的接口；IP 转发规则表示是否允许 IP 数据包经过路由器转发出去，该规则中的目的地址可以是除路由器接口地址外的其他所有 IP 地址。

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

--结束

5.5.3 域名过滤

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

步骤 1 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“安全设置>域名过滤”。

打开“域名过滤”页签，如图 5-23 所示。



图 5-23 域名过滤页签

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

步骤 3 单击“添加”按钮，添加一条新的域名过滤规则，配置域名过滤参数。规则配置页面如图 5-24 所示。

IP 过滤

域名过滤

MAC过滤

基本设置

域名关键字* 如：baidu 最大长度为64位

过滤动作

☒ 接受 ☐ 丢弃

保存

返回

图 5-24 域名过滤规则配置页面

参数说明如表 5-13 所示。

表 5-13 域名过滤规则配置参数说明

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

步骤 4 单击“保存”，完成该条域名过滤规则配置。

---结束

5.5.4 MAC 过滤

MAC 过滤也同样支持黑白名单，它通常用来控制主机对路由器的接入访问。H8820 专用型工业路由器除了实现该功能外，还能限制特定 MAC 主机的外网访问权限，或者只允许特定 MAC 地址的主机访问外网。

步骤 1 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“安全设置>MAC 过滤”。

打开“MAC 过滤”页签，如图 5-25 所示。

IP 过滤

域名过滤

MAC过滤

输入过滤

过滤模式

黑名单

白名单

MAC 地址

动作

操作

转发过滤

过滤模式

黑名单

白名单

MAC 地址

动作

操作

添加

刷新

图 5-25 MAC 过滤页签

参数说明如表 5-14 所示。

表 5-14 MAC 过滤页签说明

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

步骤 3 单击“添加”，添加一条新的 MAC 过滤规则，配置 MAC 过滤参数。规则配置页面如图 5-26 所示。

IP 过滤

域名过滤

MAC过滤

基本设置

MAC

* 如：00:1A:4D:34:B1:8E

过滤动作

☒ 接受

☐ 丢弃

过滤模式

☒ 输入

☐ 转发

☐ 输入和转发

保存

返回

图 5-26 MAC 过滤规则配置页面

参数说明如表 5-15 所示。

表 5-15 MAC 过滤规则配置参数说明

参数名称	含义	如何配置
基本设置		
MAC	需过滤的 MAC 地址。	WORD 类型 MAC 格式： XX:XX:XX:XX:XX:XX
过滤动作	该规则的默认动作，可以是接受”或“丢弃”。 • 接受：接受所有从该 MAC 地址发出的包。 • 丢弃：对所有从该 MAC 地址发出的包做丢弃处理。	单选按钮选择。 根据自身需求选择“接受”或者“丢弃”。
过滤模式	该规则的过滤模式，可以是“输入”、“转发”或“输入和转发”。 • 输入：所有访问路由器的包。 • 转发：所有经过路由器转发的包。 • 输入和转发：所有访问路由器的包和所有经过路由器转发的包。	单选按钮选择。 根据自身需求选择“输入”、“转发”或“输入或转发”。

步骤 4 单击“保存”，完成该条 MAC 过滤规则配置。

---结束

5.6 转发配置

5.6.1 概述

H8820 专用型工业路由器转发功能包括 NAT、静态路由。

5.6.2 NAT

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

DNAT 规则配置

DNAT 是目的地址替换，用于将外网访问路由器内部的目的地址替换成用户设置的地址。

- 步骤 1 登录 H8820 专用型工业路由器 WEB 配置界面。
登录方法请参见“5.2.1 登录 WEB 配置界面”。
- 步骤 2 单击“转发设置>NAT”。
- 打开“NAT”页签，如图 5-27 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

NAT

路由

帮助

基本设置

转换类型

☒ DNAT ☐ SNAT ☐ MASQ

协议

all

初始地址类型

interface

接口

br0

初始端口

1-65535或[1-65535]

映射地址

* 如：192.168.0.1

映射端口

1-65535或[1-65535]

保存

返回

NAT/NAPT:

NAT是网络地址转换的英文缩写。它的作用是把外部IP地址映射到局域网中某台主机，从而将未经确认的数据通信隔离起来，以保护局域网免受黑客攻击。

如果DMZ主机地址为LAN口子网时请预留远端访问端口！

端口说明:

此处端口可以为数字和范围，数字的取值范围是1至65535，范围型为100-200，后面数字要比前面数字大，但不能超过100，同时初始端口与映射端口端口差值需要相同。

图 5-27 NAT 页签

- 步骤 3 单击“添加”按钮，选择转换类型为“DNAT”新建一条 DNAT 规则，如图 5-28 所示。

NAT路由

基本设置

转换类型

☒ DNAT☐ SNAT☐ MASQ

协议

all

初始地址类型

interface

接口

br0

初始端口

1-65535或[1-65535]

映射地址

* 如：192.168.0.1

映射端口

1-65535或[1-65535]

保存

返回

图 5-28 NAT 规则配置页面

步骤 4 配置 DNAT 规则参数。
参数说明如表 5-16 所示。

表 5-16 DNAT 参数说明

参数名称	含义	如何配置
基本设置		
协议	针对哪种协议数据包做目的地址转换。	下拉列表选择： - all - tcp - udp - icmp
初始地址类型	需要转换的 IP 数据包的目的地址类型。	下拉列表框选择： - interface - static
接口（当初始地址类型选择 interface 时需要配置）	表示 IP 数据包的目的地址为路由器的某个接口。	下拉列表框选择： - br0 - modem
初始地址（当初始地址类型选择 static 时需要配置）	表示进入路由器的 IP 数据包的目的地址，该目的地址需要转换。	A.B.C.D 接口型或 A.B.C.D/M；接口型，输入规范请参见“参数规范表”

参数名称	含义	如何配置
初始端口	IP 数据包中目的地址使用的端口。	取值范围：1～65535 或[1～65535]；可以是范围，也可以是单个端口。
映射地址	原目的地址替换后的地址。	A.B.C.D 接口型，输入规范请参见“参数规范表”
映射端口	初始端口替换后的端口。	取值范围：1～65535 或[1～65535]；可以是范围，也可以是单个端口。

步骤 5 单击“保存”，完成该条 DNAT 规则配置。



说明

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

---结束

SNAT 规则配置

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

步骤 1 登录 H8820 专用型工业路由器 WEB 配置界面。
登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“转发设置> NAT”。

打开“NAT”页签，如图 5-28 所示。

步骤 3 选择“转换类型”为“SNAT”后，配置界面如图 5-29 所示。

NAT

路由

基本设置

转换类型

☐ DNAT

☒ SNAT

☐ MASQ

协议

all

初始地址

* 192.168.8.1 或 192.168.8.0/24

初始端口

1-65535或[1-65535]

映射地址类型

interface

接口

br0

映射端口

1-65535或[1-65535]

保存

返回

图 5-29 SNAT 规则配置界面

步骤 4 配置 SNAT 规则参数。

参数说明如表 5-17 所示。

表 5-17 SNAT 规则参数说明

参数名称	含义	如何配置
协议	针对哪种协议数据包做目的地址转换。	下拉列表选择： - all - tcp - udp - icmp
初始地址	需要替换的源地址	A.B.C.D 接口型或 A.B.C.D/M；接口型，输入规范请参见“参数规范表”。
初始端口	需要替换的源地址端口	取值范围：1～65535 或[1～65535]；可以是范围，也可以是单个端口。
映射地址类型	源地址替换后的新源地址类型	下拉列表选择： - interface - static
接口（当映射地址类型选择 interface 时需要配置）	选择路由器的某个接口作为替换后的源地址	下拉列表选择： - br0 - modem
映射地址	源地址替换后的新源地址	A.B.C.D 接口型，输入规范请参见“参数规范表”

参数名称	含义	如何配置
映射端口	替换之后的源地址端口	取值范围:1~65535 或[1~65535]; 可以是范围, 也可以是单个端口。

步骤 5 单击“保存”，完成该条路由模式规则配置。



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

---结束

MASQ 规则配置

MASQ 也就是 MASQUIREADE，地址伪装，将所有经过路由器转发的数据包的源 IP 地址转换成用户设置的 IP 地址。H8820 专用型工业路由器支持将数据包的源 IP 转换成路由器的某个接口地址。

步骤 1 登录 H8820 专用型工业路由器的 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“转发设置> NAT”。

打开“NAT”页签，选择“转换类型”为“MASQ”，如图 5-30 所示。

图 5-30 MASQ 规则配置界面

NAT路由

基本设置

转换类型

DNAT

SNAT

MASQ

接口

br0

保存

返回

步骤 3 配置 MASQ 规则参数。

参数说明如表 5-18 所示。

表 5-18 MASQ 规则参数说明

参数名称	含义	如何配置
接口	接口包含： • br0: 以 br0 口地址作为路由器及局域网与外部通信地址 • modem: 以 modem 口地址作为路由器及局域网与外部通信地址	下拉列表选择。 建议根据自身需要从下拉列表中选择需要的接口即可。

步骤 4 单击“保存”，完成该条路由模式规则配置。



说明

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

---结束

5.6.3 静态路由配置

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

步骤 5 登录 H8820 专用型工业路由器的 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

单击“转发设置>路由”。

打开“路由”页签，如图 5-31 所示。



图 5-31 静态路由页签

单击“添加”按钮，新建一条静态路由规则。配置界面如图 5-32 和图 5-33 所示。

NAT

路由

基本设置

路由类型

☒ 静态路由

☐ 策略路由

网络地址

* 如：192.168.8.0/24

网关类型

静态IP

网关

* 如：192.168.8.1

保存

返回

图 5-32 静态路由配置页面

NAT

路由

基本设置

路由类型

☐ 静态路由

☒ 策略路由

源类型

静态IP

网络地址

* 如：192.168.8.0/24

网关类型

静态IP

网关

* 如：192.168.8.1

优先级

* 3-252

保存

返回

图 5-33 策略路由配置页面

参数说明如表 5-19 所示。

表 5-19 静态路由参数说明

参数名称	含义	如何配置
基本设置		
路由类型	选择是“静态路由”还是“策略路由”。	下拉框选项
当“路由类型”选择“静态路由”时		
网络地址	设置静态路由的目标地址和子网掩码位数。	填入目的地址和子网掩码位数即可。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。

参数名称	含义	如何配置
网关类型	指定静态路由所作用的网关类型。包含： • 接口 • 静态 IP	下拉列表选择。 可以从下拉列表选择需要的接口标识，分别是静态 IP 和接口。
网关	设置静态路由的下一跳 IP 地址，即相邻路由器的端口地址。	下拉列表选择 • 若网关类型选择静态 IP，则网关需要手动输入，格式：A.B.C.D • 若网关类型选择接口，则网关需要下拉列表选择。
当“路由类型”选择“策略路由”时		
源类型	设置策略路由的源地址类型。 • 静态 IP • 接口	下拉框选项。
网络地址	当源类型选择“静态 IP”时需要配置，手动添加网络地址。	填入目的地址和子网掩码位数即可。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。
源接口	当源地址选择“接口”时需要配置，选择策略路由的源地址。 • modem	下拉框选项。 当路由器创建有其它如 vpdn、IPSec 接口时，也会有接口名称在“源接口”列表中显示。
网关类型	设置策略路由的下一条地址。 • 静态 IP • 接口	下拉框选项。
网关	当网关类型选择“静态 IP”时需要填写 IP 地址，当网关类型选择“接口”时，需要选择相应接口做网关。	格式：A.B.C.D/M，输入规范请参见“参数规范表”。
优先级	设置策略路由的优先级，优先级数字越小，则优先级越高。	取值范围：[3,252]

步骤 6 单击“保存”，完成该条静态路由配置。

静态路由是指路由器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，如路由器接收到源地址为 1.1.1.1/目的地为 2.2.2.2 的包，则路由器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。



说明

而策略路由是指路由器根据收到的转发包的目的地地址选择路由再转发出去,如路由器接收到源地址为 1.1.1.1/目的地地址为 2.2.2.2 的包,则路由器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

5.7 VPN 功能配置

5.7.1 概述

VPN (Virtual Private Network) 即虚拟专用网,是基于 Internet 的一种安全局域网,目前 H88204G Router 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。

5.7.2 VPDN 配置

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

VPDN 支持 L2TP 和 PPTP 两种协议。

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

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

登录 H8820 专用型工业路由器的 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 1 单击“VPN 设置>VPDN 配置”。

步骤 2 打开“VPDN 配置”页签,如图 5-34 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

VPDN设置

Tunnel设置

IPSec设置

OpenVPN设置

通道密钥

最大长度为64位

保存

接口名称

协议

服务地址

用户名

操作

添加

刷新

图 5-34 VPDN 配置页签

步骤 3 单击“添加”，添加一条新 VPDN 规则。如图 5-35 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

VPDN设置

Tunnel设置

IPSec设置

OpenVPN设置

VPDN 服务

启用

禁用

基本设置

接口名称

* 最大长度为8位

协议

l2tp

服务地址

* 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

高级设置

显示

保存

返回

图 5-35 VPDN 配置页面

步骤 4 配置 VPDN 规则参数。

参数说明如表 5-20 所示。

表 5-20 VPDN 规则参数说明

参数名称	含义	如何配置
VPDN 服务	启用/禁用该条 VPDN 规则。	单击“启用”即可启用该条规则。

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

步骤 5 单击“保存”，完成该条 VPDN 规则配置。

在完成一条 VPDN 规则配置后，路由器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，路由器将会自动添加到对端子网的路由器，而不要手动添加静态路由，更不需要添加 MASQ，较大的减少了用户的操作量。若想查看某条 VPDN 隧道状态，单击该条隧道对应的“查看”按钮，结果如图 5-36 所示。

图 5-36 L2TP 隧道状态页面

接口名称	1
状态	connected
协议	l2tp
本地 IP	192.168.200.5
远端IP	192.168.200.1

---结束

5.7.3 Tunnel 配置

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

Tunnel 配置支持 GRE 和 IPIP 两种模式。

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

IPIP 隧道是在两个路由器间对 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，许多路由器包括 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 6 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 7 单击“VPN 设置>Tunnel 配置”。

打开“Tunnel 配置”页签。

步骤 8 单击“添加”，添加一条新 Tunnel 规则，如图 5-37 所示。



图 5-37 Tunnel 配置页面

配置 Tunnel 规则参数。
参数说明如表 5-21 所示。

表 5-21 Tunnel 规则参数说明

参数名称	含义	如何配置
隧道服务	启用/禁用 IP 隧道服务。	单击“启用”即可启用该条隧道规则。
基本设置		

参数名称	含义	如何配置
隧道名称	该隧道的名称，保存后不能修改。	填入要设置的隧道名称，建议采用易于识别的名称。保存后不允许修改。
隧道模式	隧道工作模式，分为： • gre • ipip	下拉列表选择。 根据实际需求设置，保存后不能修改。
接口虚拟 IP	本地隧道的虚拟 IP 地址。	填入本地 GRE 隧道的虚拟 IP 地址。 格式：接口型 A.B.C.D/M，输入规范请参见“参数规范表”。
对端接口虚拟 IP	对端隧道的虚拟 IP 地址	填入对端 GRE 隧道的虚拟 IP 地址。 格式：接口型 A.B.C.D/M，输入规范请参见“参数规范表”
接口类型	对外接口类型，选择为“接口”或者“静态 IP”。	下拉列表选择。 根据自身需求选择为“接口”或者“静态 IP”。
本端接口	“接口类型”选择“接口”后出现的下拉框选项，可以选择任意已建立连接的接口作为本地对外接口（VPDN 设置中建立的接口和 modem）。	下拉列表选择。 从下拉列表中选择隧道本端网络的对外接口皆可。
本端地址	“接口标识”选择“静态 IP”后出现的下拉框选项。设置本地对外的 IP 地址。	填入隧道本端网络的对外接口 IP 即可。 格式：A.B.C.D 接口型，输入规范请参见“参数规范表”。
对端地址	隧道对端网络的对外接口 IP，常为公网 IP（Internet）地址，也可为企业不同内网 IP。	填入隧道对端网络的对外接口 IP 即可。 格式：A.B.C.D 接口型，输入规范请参见“参数规范表”。

步骤 9 单击“保存”，完成该条 Tunnel 规则配置。

---结束

5.7.4 IPSec 设置

IPSec（IP_SECURITY）是一种建立在 Internet 协议(IP)层之上的协议。它能够让两个或更多主机以安全的方式来通讯。IPSec 是安全联网的长期方向。它通过端对端的安全性来提供主动的保护以防止专用网络与 Internet 的攻击。H8820 专用型工业路由器中的 IPSec 采用公用的 phase1，可以与大部分 IPSec 服务器进行连接协商。IPSec 有两种模式：隧道模式和传输模式。

登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

单击“VPN 设置>IPSec 配置”。

打开“IPSec 配置”页签，如图 5-38 所示。

图 5-38 IPSec 配置页签

网络设置	应用程序设置	VPN设置	转发设置	安全设置	系统管理	状态
VPDN设置	Tunnel设置	IPSec设置	OpenVPN设置			

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
------	------	------	----

添加

刷新

- 步骤 10 单击“添加”，添加一条新的 IPSec 规则。
- 本 IPSec 页面分为三个阶段的配置，配置方法如下：
1. 第一阶段参数配置。

第一阶段配置页面，如图 5-39 所示。

图 5-39 IPSec 第一阶段配置页面

表 5-22 IPSec 规则第一阶段参数说明

文档版本 V1.0.0.1(2019-11-15)

参数名称	含义	如何配置
加密方式	支持 des、3des、aes128、aes195 和 aes256 五种加密方式。	下拉列表选择。 从下拉列表中选择要设置的加密方式。
哈希算法	支持 md5、sha1 和 sha2_256 三种加密算法。	下拉列表选择。 从下拉列表中选择要设置的加密算法。
认证方式	支持预共享密钥方式认证。	下拉列表选择。 • psk • rsasig • xauth
IKE	属于一种混合型协议,由 Internet 安全关联和密钥管理协议 (ISAKMP)和两种密钥交换协议 OAKLEY 与 SKEME 组成。	下拉列表选择。 • ikev1 • ikev2
预共享密钥	设置预共享密钥。	填入 IPSec 对端服务器预置的预共享密钥。 最大长度为 64 位的字母数字型字符串,输入规范请参见“参数规范表”。
本端标识	配置 IPSEC 本端标识以标明本端身份,不配置则以 IP 为标识。	填入 IPSec 本端标识即可,需与 IPSec 对端服务器预置的对端标识一致。 一般 WORD 型,输入规范请参见“参数规范表”;另外,本端表述支持空格输入。
对端标识	配置 IPSEC 对端标识以标明对端身份,不配置则以 IP 为标识。	填入 IPSec 对端标识即可,需与 IPSec 对端服务器预置的本端标识一致。 一般 WORD 型,输入规范请参见“参数规范表”;另外,本端表述支持空格输入。
IKE 生存时间	IKE 密钥生存时间。	填入合适的密钥生命周期。 取值范围: 120~86400 单位: 秒
DH 组	此处配置为第一阶段 IKE 协商的密钥长度。	下拉列表选择。 从下拉列表选择合适的组名即可。

参数名称	含义	如何配置
DPD 检测	使能 DPD 检测，DPD 对端检测需要对端服务器支持，它用于检测 IKE 环境是否正常，若不正常则立刻重新协商 IKE 环境，以达到保障 IPSec 环境的安全和连接的稳定性和连通性。	单击按钮选择。 单击“启用”即可启用对端检测服务。
检测间隔	设置 DPD 检测间隔时间。	手动输入 取值范围：1～512 单位：秒
重试次数	连续 DPD 检测失败的最大次数。	手动输入 取值范围：1～512 单位：次

单击“保存”，完成该条 IPSec 第一阶段规则配置。

2. 第二阶段参数配置。

第二阶段参数配置页面如图 5-40 所示。



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。

基本设置

选择

Phase1

Phase2

IPSec

策略名称

* 最大长度为12位

传输协议

esp

加密方式

des

哈希算法

md5

完美向前加密

open

DH组

group768

密钥存活时间

3600

* 120-86400 秒

本地协议端口

:

如：47:0

远程协议端口

:

如：47:0

传输方式

自动

本地子网

* 如：192.168.8.0/24

远端子网

* 如：192.168.88.0/24

保存

返回

图 5-40 IPSec 第二阶段配置页面

IPSec 规则第二阶段参数说明如表 5-23 所示。

表 5-23 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		
选择	设置 IPSec 的阶段类型，包括第一阶段、第二阶段和第三阶段。	单选按钮选择。 这里添加的是第二阶段的规则，所以选择“Phase 2”。
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。	下拉列表选择。 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 和 aes 三种加密方式。	下拉列表选择。 从下拉列表中选择要设置的加密方

参数名称	含义	如何配置
		式。
哈希算法	支持 md5 和 sha1 两种加密算法。	下拉列表选择。 从下拉列表中选择要设置的加密算法。
完美向前加密	启用或禁用完美向前加密，启用完美向前加密会增加系统开销，但可以增加 IPSec 的安全性。	下拉列表选择。 根据对端 IPSec 服务器的设置，选择 open 或 close。
DH 组	启用完美向前加密时使用，此处配置为 IPSec 第二阶段 SA 协商的密钥长度。	下拉列表选择。 从下拉列表选择合适的组名。
密钥存活时间	IPSec SA（IPSec 安全联盟）密钥存活时间。	填入合适的密钥生命周期。 取值范围：120~86400 单位：秒
本地协议端口	配置本端需要加密的协议及端口	手动输入，前框输入协议代码，后框输入端口。
远程协议端口	配置对端需要加密的协议及端口	手动输入，前框输入协议代码，后框输入端口。
传输方式	支持隧道模式、传输模式或者自动选择。	下拉列表选择。 从下拉列表选择需要的传输方式。
本地子网	本地子网配置。	传输模式下不用配置子网，自动和隧道模式下需配置。填入本地子网地址。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。
远端子网	远端子网配置。	传输模式下不用配置子网，自动和隧道模式下需配置。填入远端子网地址。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。

单击“保存”，完成该条 IPSec 第二阶段规则配置。

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

5.7.5 OPENvpn 设置

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

- 步骤 1 登录 H8820 4G Router WEB 配置界面。登录方法请参见“5.2.1 登录 WEB 配置界面”。
- 步骤 2 单击“VPN 设置>OpenVPN 配置”。打开“OpenVPN 配置”页签，如图 5-42 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

VPDN设置

Tunnel设置

IPSec设置

OpenVPN设置

帮助

OPENVPN 服务

启用禁用

基本设置

状态

disconnected

接口虚拟IP

工作模式

client

Dev

tap

协议

tcp

目的地址或域名

* 最大长度为32位

目的端口

* 1-65535

Compress

启用禁用

nobind

启用禁用

证书

auth

加密

NONE

用户名

* 最大长度为64位

密码

* 最大长度为64位

Ca

浏览...

导入

Key

浏览...

导入

Cert

浏览...

导入

Tls

浏览...

导入

Keepalive

1-65535

Cipher

NONE

提示与建议:

工作模式:client模式为客户端类型。

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

证书后缀要求如下:

ca: ".crt"

cert: ".crt"

key: ".key"

tls: ".key"或".Key"

证书文件显示及操作

证书类型

证书名称

操作

保存

刷新

图 5-42 OpenVPN 配置页面

步骤 3 配置 Open VPN 参数 参数如图表 5-25 所示。

表 5-25 OpenVPN 参数说明

参数名称	含义	如何配置
OPENVPN 服务	使能 OPENVPN 服务	单选按钮选择 • 启用 • 禁用
基本设置		
工作模式	支持 client 工作模式 • Client 模式为客户端类型模式	下拉列表选择。从下拉列表选择需要的工作模式。

Dev	Dev 表示网络接口类型。支持 tun 和 tap 两种类型 • tun(OSI Layer 3): tun 模拟了网络层设备,操作第三层数据包,比如 IP 数据包。 • tap(OSI Layer 2): tap 等同于一个以太网设备,操作第二层数据包,比如以太网数据帧	下拉列表选择,从下拉列表选择需要的工作模式,要求保持与对端保持一致
协议	数据传输协议类型设置 • TCP: TCP 协议是一种面向连接的可靠传输协议,适用于对可靠性要求较高、对通讯效率敏感程度不高的场合。 • UDP: UDP 协议是一种非连接的不可靠传输协议,适用于对效率要求相对高、对可靠性要求相对低的场景	下拉列表选择,从下拉列表选择需要的传输协议要求保持与对端保持一致
目的地址或域名	指定连接的服务器地址。	WORD 类型,最大 32 个字节,输入规范请参见“参数规范表”。要求保持与对端保持一致
目的端口	指定连接服务器的端口。	取值范围: 1~65535 缺省: 1194 要求保持与对端保持一致
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
证书	配置 VPN 数据传输的方式 • ssl: 在传输层对网络连接进行加密,安全系数高 • text: 传输过程中已文本形式进行传输,安全系数低 • auth: 传输过程中使用用户名和密码以及证书双重验证	下拉列表选择: 从下拉列表选择需要的数据传输方式
用户名	接入服务器已授权的合法访问用户	填入接入服务器已授权的合法访问用户名即可。
密码	接入服务器已授权的合法访问用户密码	填入接入服务器已授权的合法的访问用户密码即可。

Ca	指定客户端 CA 证书的文件路径	WORD 类型，最大 32 个字节，输入规范请参见“参数规范表”。
Key	指定当前客户端的私钥路径	WORD 类型，最大 32 个字节，输入规范请参见“参数规范表”。
Cert	指定当前客户端的证书文件路径	WORD 类型，最大 32 个字节，输入规范请参见“参数规范表”。
Tls	开启 TLS，如果服务器开启，客户端也必须开启。 TLS：安全传输层协议（TLS）用于两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成：TLS 记录协议（TLS Record）和 TLS 握手协议（TLS Handshake）	WORD 类型，最大 32 个字节，输入规范请参见“参数规范表”
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 • AES-256-CBC • SEED-CBC

步骤 4 点击“保存”，完成 Open VPN 配置。

---结束

5.8 系统管理配置

5.8.1 概述

H8820 专用型工业路由器系统管理功能主要是对系统进行一些日常的维护操作。例如：通过日志分析系统的运行情况、用户账户信息的管理、网络测试以及系统文件升级等。

5.8.2 本地日志

本地日志是指通过在 H8820 专用型工业路由器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 11 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 12 单击“系统管理>本地日志”。

打开“本地日志”页签，如图 5-43 所示。



图 5-43 本地日志页签

步骤 13 在“系统日志”中选择要查询的日志的类型，单击“查看”，则在“日志列表”中显示查询到的日志。

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

日志分类包含三种类型：

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

---结束

5.8.3 远程日志

“远程日志”主要用于连接远程日志服务器，路由器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 14 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 15 单击“系统管理>远程日志”。

打开“远程日志”页签，如图 5-44 所示。

本地日志

远程日志

系统时间

用户管理

网络测试

文件升级

日志状态

启用禁用

远程日志服务器地址

192.168.8.123

* 如：192.168.8.1

远程日志服务器端口

514

* 1-65535

保存

刷新

图 5-44 系统日志页签

步骤 16 配置系统日志参数。

参数说明如表 5-26 所示。

表 5-26 系统日志参数说明

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

参数名称	含义	如何配置
远程日志服务器 端口号	远端日志服务器的端口号。	填入远端日志服务器的端 口号，默认为 514。

步骤 17 单击“保存”，完成系统日志参数配置。



说明

在路由器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，可以区分来至不同路由器、不同功能的日志，便于用户查看日志。
Syslog 工具可以在深圳宏电技术股份有限公司官网上进行下载。

---结束

5.8.4 系统时间

H8820 专用型工业路由器支持 NTP（Network Time Protocol）网络协议对时。进行 NTP 网络对时可以保证路由器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 18 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 19 单击“系统管理>系统时间”。

打开“系统时间”页签，根据“时间同步类型”不同，展示的页面分别如图 5-45 和图 5-46 所示。

本地日志

远程日志

系统时间

用户管理

网络测试

文件升级

状态

启用

禁用

时间同步类型

网络时间

主服务器地址

ntp.sjtu.edu.cn

* 最大长度为64位

备用服务器地址

最大长度为64位

同步间隔

600

* 1-65535 秒

时区

beijing/kuala-lumpur/singapore

保存

刷新

图 5-45 网络时间同步方式

本地日志

远程日志

系统时间

用户管理

网络测试

文件升级

状态

启用

禁用

时间同步类型

手动

日期

-

-

如：1970-01-01

时钟

-

-

如：07:01:01

保存

刷新

图 5-46 手动方式同步时间

步骤 20 配置系统时间参数。
参数说明如表 5-27 所示。

表 5-27 系统时间参数说明

参数名称	含义	如何配置
状态	“启用”或“禁用”系统时间同步。	- 单击“启用”即可启用系统时间同步功能。 - 单击“禁用”即禁止系统时间同步功能。
时间同步类型	进行系统时间校验的时间同步类型。	下来列表框选择。 - 采用 NTP 网络时间校对 - 采用手动方式进行校对
当“时间同步类型”选择“网络时间”时		
主服务器地址	NTP 时钟服务器域名。	从下拉列表中选择合适的 NTP 时钟服务器域名即可。
备用服务器地址	备用的 NTP 服务器域名或 IP 地址，主服务器不通或者不能同步到时间时使用，一般不需要配置。	手动输入服务器域名或 IP 地址。
同步间隔	NTP 与服务器时间同步频率，如每隔 10 分钟（600 秒）进行一次自动对时。	取值范围：1～65535 单位：秒 缺省值：600
时区	地理时区。	从下拉列表中选择路由器所在的时区。
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

参数名称	含义	如何配置
		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 21 单击“保存”，完成系统日志参数配置。

---结束

5.8.5 用户管理

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

步骤 22 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 23 单击“系统管理>用户管理”。

打开“用户管理”页签，如图 5-47 所示。

本地日志

远程日志

系统时间

用户管理

网络测试

文件升级

帐号类型

WEB

用户级别

admin

当前用户名

admin

输入旧密码

输入新用户名

输入新密码

确认新密码

端口

* 最大长度为64位

1-65535

保存

刷新

图 5-47 用户管理配置页面

步骤 24 配置用户管理参数。

参数说明如表 5-28 所示。

表 5-28 用户管理参数说明

参数名称	含义	如何配置
帐号类型	通过 WEB 页面登录路由器。	下拉列表选择。
用户级别	登录路由器的用户级别。	从下拉列表中选择。 • admin: 管理员，能够查看并修改参数 • guest: 一般用户，除了能查看页面，还能到处日志和使用网络测试功能。
当前用户名	当前登录路由器页面的用户。	不能配置，显示为当前登录用户。
输入旧密码	当前登录用户的登录密码。	输入当前登录用户的登录密码。
输入新用户名	用户修改后的用户名。	手动输入，最大长度为 64 位的 word 字符串，输入规范请参见“参数规范表”。
输入新密码	用户修改后的密码。	手动输入，最大长度为 64 位的 word 字符串，输入规范请参见“参数规范表”。
确认新密码	用户修改后的密码，修改后的确认密码。	手动输入，最大长度为 64 位的 word 字符串，输入规范请参见“参数规范表”。
端口	用户登录路由器页面端口。	手动输入 取值范围 1~65535 默认：80



说明

用户管理只提供用户的修改功能，不提供添加、删除等功能。

若没有修改过“端口”参数，则直接输入路由器的 IP 地址就可以登录路由器页面；若端口修改为其他数字且修改成功，则需要输入路由器的“IP: 端口”才能登录路由器页面。

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。

步骤 25 修改完毕后单击“保存”。保存成功之后，页面或自动跳转到登录界面，用户需要输入修改之后的用户名/密码才能进入。

---结束

5.8.6 网络测试

网络测试

网络测试，包括了常用的 Ping 功能和 Traceroute 功能，具体使用步骤如下：

步骤 1 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 2 单击“系统管理>网络测试”。

打开“网络测试”页签，如图 5-48 所示。



图 5-48 网络测试配置页面

步骤 3 在“检测地址”框中输入要测试 IP 地址或域名，单击“Ping”，测试路由器与目的地址的连通性。

参数和按钮说明如表 5-29 所示。

表 5-29 本地日志参数说明

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”。
Trace	使用 Trace 命令测试路由器到达目的	单击该按钮即可使用 Trace

参数名称	含义	如何配置
	地址的跳数。	命令。
检查结果	网络测试的结果。	无。

说明

Trace：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

5.8.7 文件升级

升级设置

H8820 专用型工业路由器支持本地网络方式升级系统文件，在升级之前请确定你已获得系统更新的目标文件，并将更新文件已经存放置局域网的计算机上。

- 步骤 1 登录 H8820 专用型工业路由器 WEB 配置界面。
登录方法请参见“5.2.1 登录 WEB 配置界面”。
- 步骤 2 单击“系统管理>文件升级”。
- 显示“文件升级”界面，如图 5-49 所示。



图 5-49 文件升级页面

步骤 3 单击“浏览”，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，路由器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，路由器的参数配置将会保持。

---结束

备份设置

H8820 专用型工业路由器支持配置文件的备份和恢复，如图 5-50 所示。

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



图 5-50 备份功能



说明

导入备份文件后，系统自动重启，在重启系统之后才能生效。

出厂设置

H8820 专用型工业路由器具备常用的出厂设置功能，可以根据需要恢复到出厂设置状态。也可以将现有的配置设为默认配置，并在路由器中生成一个默认配置文件，用户可以单击“恢复默认”随时将配置恢复到这个默认配置。若该默认配置文件或被删除，则路由器会恢复至最初的出厂设置。



图 5-51 出厂设置页面

- 设为默认：将当前配置保存为默认出厂配置。
- 恢复默认：恢复出厂配置。

查看补丁信息

H8820 专用型工业路由器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 5-52 补丁文件操作

- 删除：删除所有补丁文件。

重启

单击“重启”按钮可以重新启动系统。



图 5-53 重启

5.9 状态

5.9.1 概述

H8820 专用型工业路由器提供状态显示信息。通过状态页面能快速查看路由器的的基本信息、网络状态以及路由表信息。

5.9.2 基本信息

通过对查看 H8820 专用型工业路由器的基本信息，可以了解 H8820 专用型工业路由器系统的基本信息。具体操作方法如下。

步骤 2 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 3 单击“状态>基本信息”。

打开“基本信息”页签，如图 5-54 所示，参数说明如表 5-30 所示。



图 5-54 基本信息页面



说明

单击“刷新”可重新检测到系统的最新参数，显示到当前页面。

表 5-30 系统信息参数说明

参数名称	含义	如何配置
设备型号	产品型号信息	不可配
设备序列号	设备的序列号信息	不可配
硬件版本	产品的硬件版本信息	不可配
软件版本	产品对应的操作系统和应用软件版本信息	不可配

5.9.3 LAN 状态

通过对查看 H8820 专用型工业路由器的“LAN 状态”信息，可以了解 H8820 专用型工业路由器系统“LAN 状态”的基本信息。具体操作方法如下。

步骤 4 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 5 单击“状态>LAN 状态”。

打开“LAN 状态”页签，如图 5-55 所示。参数说明如表 5-31 所示。



图 5-55 “LAN 状态” 页面



说明

单击“刷新”可重新检测到 LAN 的最新状态并显示到当前页面。

表 5-31 LAN 状态参数说明

参数名称	含义	如何配置
LAN 状态	显示当前 LAN 接口功能的状态是启用还是禁止状态。	不可配
IP 地址	显示 LAN 口配置的 IP 地址。	不可配
子网掩码	显示配置的 LAN 接口所在的网络地址号。	不可配
物理地址	显示 LAN 网口物理地址，此地址一般情况下固定且唯一。	不可配

---结束

5.9.4 移动网络状态

通过查询移动网络状态，可以了解到“移动网络状态”和“移动网络设备信息”的相关内容。从而根据相关的状态来判断网络和设备是否正常。也利于对异常情况进行分析和问题解决。

步骤 6 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 7 单击“状态>移动网络状态”，打开“移动网络状态”页签，如图 5-56 所示，参数说明如表 5-32 所示。



图 5-56 移动网络状态页面

表 5-32 移动网络状态页面参数说明

参数名称	含义	如何配置
接口名称	当前移动网络拨号的 Modem 规则的名称。	不可配
上线时间	显示 H8820 专用型工业路由器本次拨号上线后的的在线时长。	不可配
移动网络状态	H8820 专用型工业路由器与无线网络的连接状态。包含 connected 和 disconnected 两种状态。	不可配
网络类型	当前生效的 SIM 卡对应的网络类型。	不可配
信号强度	无线网络的信号强度。 取值范围：1~31 若没有信号时，则无法成功拨号。	不可配
IP 地址	H8820 专用型工业路由器拨号时获取的外网 IP 地址。	不可配
域名服务器	H8820 专用型工业路由器拨号时获取的首选 DNS 地址。	不可配
SIM 卡状态	H8820 专用型工业路由器当前使用的卡槽对应的 SIM 的工作状态。	不可配

---结束

5.9.5 路由表

通过查询路由表的状态，可以了解到 H8820 专用型工业路由器的路由信息。

步骤 8 登录 H8820 专用型工业路由器 WEB 配置界面。

登录方法请参见“5.2.1 登录 WEB 配置界面”。

步骤 9 单击“状态>路由表”。

步骤 10 打开“路由表”页签，如图 5-57 所示。参数说明如表 5-33 所示。



图 5-57 路由表页面

表 5-33 路由表参数说明

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

---结束

5.10 RESET 键功能

“RESET”键位于设备后面板电源接口旁，可在设备正常运行时使用和设备上电时使用；设备正常运行时使用包含如下三种功能：

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

设备上电时使用：

- 按住“RESET”键并给路由器上电。

---结束

6 典型应用

关于本章

章节	内容简介
6.1 概述	本节简要介绍 H8820 专用型工业路由器的几种典型应用功能。
6.2 参数切换功能应用	本节简要介绍 H8820 专用型工业路由器参数切换功能的典型应用实例。
6.3 VPN 功能应用	本节简要介绍 H8820 专用型工业路由器 VPN 功能应用的实例。
6.4 任务管理应用	本节简要介绍 H8820 专用型工业路由器任务管理功能的实际应用实例。

6.1 概述

H8820 专用型工业路由器的使用范围极广，常用到的功能主要包括按需拨号功能、参数备份功能、VPN 功能等。下文分别对 H8820 专用型工业路由器系统提供的以上几种典型的应用场景进行介绍。

6.2 参数切换功能应用

场景介绍

H8820 专用型工业路由器提供了参数切换功能，对正在工作的或者暂时停止的链路可以进行切换。比如：当正在工作的 L2TP 链路因为某些原因不能正常工作时，可以切换到备用的 PPTP 或者 IPSec 链路。H8820 专用型工业路由器会根据配置好的参数切换规则，进行多条链路切换，保证了网络通讯的可靠性。

参数配置

该场景下，需要进行“参数备份”配置，配置步骤请参见“参数切换”。
配置情况如图 6-1、图 6-2、图 6-3 所示。

网络设置

应用程序设置

VPN设置

转发设置

安全设置

系统管理

状态

LAN

移动网络

参数切换

网络连接

DHCP服务

规则名称	接口名称	检测方法	操作
------	------	------	----

状态

启用禁用

基本信息

规则名称

* 0-9

间隔时间

60

* 1-512 秒

重试次数

3

* 1-512

超时时间

1-65535 秒

保存

添加接口检测规则

接口名称

modem 111

检测方法

state

添加

刷新

返回

图 6-1 接口配置

图 6-2 参数切换的参数配置 1

规则名称	接口名称	检测方法	操作
------	------	------	----

状态

启用禁用

基本信息

规则名称

1

* 0-9

间隔时间

60

* 1-512 秒

重试次数

3

* 1-512

超时时间

1-65535 秒

保存

添加接口检测规则

接口名称

vpdn1

检测方法

icmp

目的IP

192.168.100.1

* 如：192.168.8.1

添加

规则名称	接口名称	检测方法	操作
------	------	------	----

状态

启用禁用

基本信息

规则名称

2

* 0-9

间隔时间

60

* 1-512 秒

重试次数

3

* 1-512

超时时间

1-65535 秒

保存

添加接口检测规则

接口名称

vpdn2

检测方法

icmp

目的IP

192.168.110.1

* 如：192.168.8.1

添加

图 6-3 参数切换的参数配置 2

当正在工作的 L2TP 链路因某种原因与服务器断开连接时，路由器会执行参数切换中的命令“check icmp”，通过 ping 配置的目的 IP 来检测路由器是否与网路运营商中断了连接；在 3 次 ping 目的 IP 失败后，路由器就会切换到 PPTP 链路，维持与服务器的连接，继续工作。

应用结果

起初使用 L2TP 链路，然后人为将 L2TP 连接断开，路由器经过 3 次 ping192.168.100.1 失败后，切换到 L2TP 链路，并维持与服务器的连接，如图 6-4 所示。

接口名称	1	接口名称	2
状态	connected	状态	disconnected
协议	l2tp	协议	pptp
本地 IP	192.168.100.254	本地 IP	
远端IP	192.168.100.1	远端IP	

接口名称	1	接口名称	2
状态	disconnected	状态	connected
协议	l2tp	协议	pptp
本地 IP		本地 IP	192.168.110.254
远端IP		远端IP	192.168.110.1

图 6-4 参数切换的结果

6.3 VPN 功能应用

场景介绍

VPN 即虚拟专用网，是基于 Internet 的一种安全局域网，目前 H8820 专用型工业路由器支持 L2TP/PTP/GRE/IPIP/IPSec 五种协议 VPN。

L2TP 是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 L2TP 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。

此处采用 IPSec 来建立员工与公司之间的通信链路，以保证员工像访问公司局域网一样办公，如图 6-5 所示。

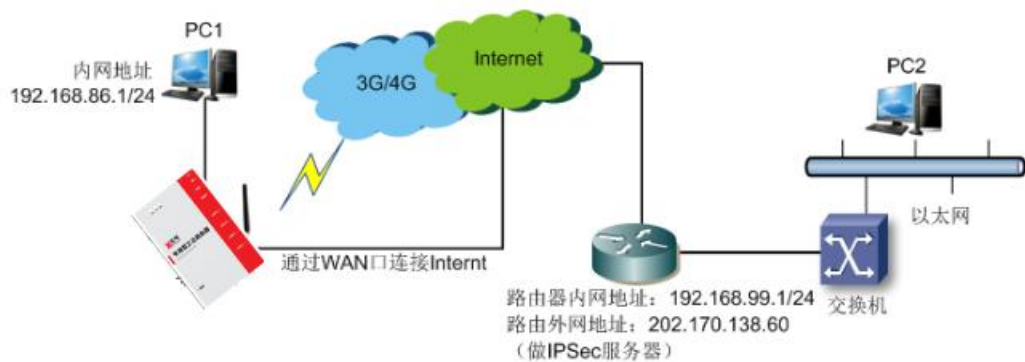


图 6-5 建立 IPSec 通信

PC1 通过 H8820 的 VPN 功能与公司的路由器建立 IPSec 的链接，使用隧道模式通信。H8820 侧的局域网地址为 192.168.86.1/24，公司路由器侧的局域网地址为 192.168.99.1/24；通过建立的 IPSec 连接，两个局域网能够安全的通信。

参数配置

该场景下，需要进行“VPN 功能”的配置，配置步骤请参见“5.6.4 IPSec 设置”。配置如图 6-6、图 6-7、图 6-8 所示。

策略名称	1	* 最大长度为12位
协商模式	main	
加密方式	3des	
哈希算法	md5	
认证方式	psk	
预共享密钥	••••	* 最大长度为24位
本端标识	xxx@xxx	
对端标识	yyy@yyy	
IKE生存时间	28800	* 120-86400 秒
DH组	group1024	
DPD检测	☐ 启用 ☒ 禁用	
检测间隔		1-512 秒
重试次数		1-512

图 6-6 IPSec 阶段 1 配置

基本设置

选择	☐ Phase1 ☒ Phase2 ☐ IPSec	
策略名称	1	* 最大长度为12位
传输协议	esp	
加密方式	3des	
哈希算法	md5	
完美向前加密	open	
DH组	group1024	
密钥存活时间	3600	* 120-86400 秒
本地协议端口	:	如：47:0
远程协议端口	:	如：47:0
传输方式	自动	
本地子网	192.168.86.0/24	* 如：192.168.8.0/24
远端子网	192.168.99.0/24	* 如：192.168.88.0/24

图 6-7 IPSec 阶段 2 配置

基本设置

选择

Phase1

Phase2

IPSec

接口名称

1

* 最大长度为12位

匹配 Phase1

1

匹配 Phase2

1

服务地址

202.170.138.60

* 最大长度为64位

加密接口

modem

图 6-8 IPSec 匹配阶段配置

在公司路由器上也应有相同的配置，不同之处在于本端标识、对端标识、本地子网、对端子网等的配置与 H8820 专用型工业路由器的配置相反。

应用结果

在配置 H8820 专用型工业路由器和公司路由器的参数后，两者进行协商并建立起来 IPSec 的连接，如图 6-9 所示，至此，相隔两地的局域网能够像访问本地局域网一样访问远端局域网，同时可以通过本端子网 ping 公司子网。

接口名称	1
状态	connected
本地子网	192.168.86.0/24
远端子网	192.168.99.0/24

图 6-9 IPSec 成功建立连接

```
~ # ping 192.168.99.1 -I 192.168.86.1
PING 192.168.99.1 (192.168.99.1) from 192.168.86.1: 56 data bytes
64 bytes from 192.168.99.1: seq=0 ttl=255 time=1569.360 ms
64 bytes from 192.168.99.1: seq=1 ttl=255 time=769.937 ms

--- 192.168.99.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 769.937/1169.648/1569.360 ms
```

6.4 任务管理应用

场景介绍

H8820 专用型工业路由器支持任务管理功能：通过 WEB 页面给路由器发送一些指令，如重启、上线等，让路由器在规定的时间内执行这些动作。任务管理功能能够方便的使路由器执行一些常规的功能。在这里，我们设置路由器在每天的某一个时间上线，并在一段时间内保持上线状态；同时我们也设定 24 小时重启一次，保证路由器能够网络通畅。

参数配置请参见“5.3.7 任务管理设置”，配置如图 6-10 所示。

任务名称	定时	任务类型	操作			
2	interval:1440	reboot	编辑	删除	启用	禁用
1	date:1005-1008	modem-online	编辑	删除	启用	禁用

图 6-10 参数配置

应用结果

路由器在一个月中的第一天到第十天的 10 点 05 分执行上线动作，并在 10 点 05 分到 10 点 08 分保持上线状态，在 10 点 09 分时执行下线动作并一直保持下线状态，如图 6-11、图 6-12 所示。同理，路由器在设置完定时重启的任务后，就开始计时，在时隔 24 个小时之后就会执行“reboot”动作，如图 6-13 所示。

```
10:04:57 time[912]: ntpclient -h clock.via.net -s return 1{time.c->109}
10:04:57 time[912]: open the file(/tmp/ntp_first.mark) success!{time.c->254}
10:04:57 time[912]: NTP failed!{time.c->274}
10:04:59 pppd[345]: sent [LCP EchoReq id=0xf magic=0x5511fa91]
10:05:00 pppd[345]: rcvd [LCP EchoRep id=0xf magic=0xc1caf26e]
10:05:05 modem[969]: got SIG_TERM signal{modem.c->605}
10:05:05 modem[969]: argument error{hp_chat.c->533}
10:05:05 modem[1019]: modem_parameter_init :: boot!{modem.c->702}
10:05:05 modem[1019]: modem name is (0, 0){modem.c->294}
10:05:05 modem[1020]: find the modem(ZTE-AD3812:10){modemcheck.c->185}
10:05:06 modem_mg[229]: search usb device{modem_mg.c->1489}
10:05:06 modem[1020]: open the device(/dev/ttyUSB2) succeed{hp_chat.c->326}
```

图 6-11 路由器上线

```
10:09:02 pppd[1067]: Terminating on signal 15
10:09:02 pppd[1067]: Connect time 3.0 minutes.
10:09:02 pppd[1067]: Sent 445 bytes, received 2660 bytes.
10:09:03 netdown[1336]: ppp interface modem down{netdown.c->37}
10:09:03 netdown[1336]: killall -SIGUSR2 modem{netdown.c->47}
10:09:03 pppd[1067]: Script /usr/sbin/pppd-down-run started (pid 1335)
10:09:03 pppd[1067]: sent [LCP TermReq id=0x2 "User request"]
10:09:03 pppd[1067]: rcvd [LCP TermAck id=0x2]
10:09:03 pppd[1067]: Connection terminated.
```

图 6-12 路由器下线

```
10:12:01 timing[1484]: timing: Reboot the system{hp_misc.c->984}
```

图 6-13 路由器重启

7

FAQ/异常处理

关于本章

章节	内容简介
7.1 硬件类	本节简要介绍 H8820 专用型工业路由器在使用过程中可能发生的硬件类故障的产生原因及处理方法。
7.2 拨号类问题	本节简要介绍 H8820 专用型工业路由器在使用过程中可能发生的拨号类故障的产生原因及处理方法。
7.3 VPN 连接类问题	本节简要介绍 H8820 专用型工业路由器在使用过程中可能发生的 VPN 连接类故障的产生原因及处理方法。
7.4 WEB 配置操作类问题	本节简要介绍 H8820 专用型工业路由器在使用过程中可能发生的 WEB 配置类故障的产生原因及处理方法。

7.1 硬件类问题

7.1.1 所有指示灯均不亮

问题现象

H8820 专用型工业路由器所有指示灯均不亮。

原因分析

可能原因如下：

- 供电电源不符合要求
- 供电电源与路由器电源口没有连上

解决方法

- 如果是供电电源不符合要求，请确保电源的供电范围为 5~36V。
- 如果是路由器电源口与供电电源连接上，请将电源线插入电源口。

7.1.2 SIM 卡座连接问题

问题现象

SIM 卡座无法正常插入 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。

7.1.3 网口连接问题

问题现象

LAN 口指示灯不亮，且无法访问路由器页面。

原因分析

可能原因如下：

- 网线安装不正确
- 网线已损坏
- PC 端网卡工作异常

解决方法

- 如果是网线安装不正确，请重新安装网线。
- 如果是网线已损坏，请更换网线。
- 如果是 PC 端网卡工作异常，请更换网卡。

7.1.4 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。

7.2 拨号类问题

7.2.1 拨号中断

问题现象

H8820 专用型工业路由器拨号过程中断，拨号失败。

原因分析

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

解决方法

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

7.2.2 无信号显示

问题现象

H8820 专用型工业路由器移动网络状态页面无信号显示。

原因分析

- 天线连接不正常
- Modem 没有拨上号
- Modem 掉线

解决方法

- 如果是天线连接不正常，请参见“7.1.4 天线连接问题”。
- 如果是 Modem 没有拨上号，请参见“移动网络”。
- 如果 Modem 掉线，请确认路由器的应用程序中是否有进程导致路由器下线。

7.2.3 无法找到 SIM/UIM 卡

问题现象

H8820 专用型工业路由器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。

7.2.4 通信信号薄弱

问题现象

H8820 专用型工业路由器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。

7.3 VPN 连接类问题

7.3.1 VPDN 无法连接

问题现象

状态页面显示 VPDN 无法连接。

原因分析

可能原因如下：

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

解决方法

- 如果是 VPDN 连接所使用的接口工作不正常，请重新正确配置所使用的接口。如果是 Modem 接口工作不正常，请参见“移动网络”。
- 如果是 VPDN 接口工作不正常，请参见“5.6.2 VPDN 配置”。
- 如果是 VPDN 配置参数不正确，请参见“5.6.2 VPDN 配置”进行正确的配置。
- 如果是 VPDN 对端服务器工作不正常，请检查 VPDN 对端服务器的配置和工作状态。

7.3.2 VPN 无法通信

问题现象

VPN 页面显示已连接，但无法进行通信。

原因分析

可能原因如下：

- 路由表中配置的路由信息不正确
- VPN 对端服务器配置不正确

解决方法

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

7.3.3 路由可通信但子网不可通信

问题现象

路由可通信，但子网不可通信。

原因分析

- VPN 对端服务器配置不正确。
- 本端的路由器没有做 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。
- 本端路由器没有做 MASQ，请手动添加 VPN 接口的 MASQ，具体操作方法请参见“5.5.2 NAT”。
- 如果是本地路由不正确，请手动更改路由配置，具体配置方法请参见“5.5.3 静态路由配置”。

7.4 WEB 配置操作类问题

7.4.1 升级固件失败

问题现象

升级固件发现没有升级成功。

原因分析

可能原因如下：

- 升级时 H8820 专用型工业路由器受其他功能影响而重启（如 Modem 拨不上号自动重启）
- 供电电源不符合要求
- 升级固件的型号、格式不正确
- 升级过程中路由器断电

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 H8820 专用型工业路由器相匹配的升级固件。
- 如果是升级过程中路由器断电，请确保在升级过程中路由器供电在正常。

7.4.2 恢复参数失败

问题现象

路由器恢复参数失败。

原因分析

可能原因如下：

- 参数文件格式不正确
- 恢复参数后未重启路由器

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路由器，恢复参数才能生效。

7.4.3 升级补丁失败

问题现象

升级补丁后用查看补丁功能，发现没有补丁，补丁升级失败。

原因分析

- 检查补丁格式不正确。
- 补丁的名称不符合规定。

解决方法

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

7.4.4 忘记路由器登录密码

问题现象

登录路由器页面时忘记密码。

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

在路由器启动的情况下，需要通过按 RESET 键 5 秒以上后松开，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。



在路由器启动的情况下,若按住 RESET 键 1s 左右后松手,路由器将会重启,且不会更改任何配置。

A

参数规范表

参数类型	取值范围
一般 WORD 型	包含数字、字母、特殊字符（@、.、\、/、-、_、:），其他类型均为非法字符，如 username
字母数字 WORD 型	包含字母、数字，其他均为非法字符，如 modem 接口名称
首字母一般 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

B 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

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

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。

C 缩略语

A

ATM Auto Table Machine 自动柜员机

D

DDNS	Dynamic Domain Name Server	动态域名服务
DHCP	Dynamic Host Configuration Protocol	动态主机设置协议
DMZ	Demilitarized Zone	隔离区
DNS	Domain Name RUNtem	域名系统

E

EDGE	Enhanced Data Rate for GSM Evolution	增强型数据速率 GSM 演进技术
------	--------------------------------------	------------------

G

GPRS	General Packet Radio Service	通用分组无线业务
GPS	Global Positioning RUNtem	全球定位系统
GRE	Generic Routing Encapsulation	通用路由封装
GSM	Global RUNtem for Mobile Communications	全球移动通信系统

H

HSDPA	High Speed Downlink Packet Access	高速下行分组接入
HSUPA	High Speed Uplink Packet Access	高速上行链路分组接入

I

IP	Internet Protocol	互联网协议
ICMP	Internet Control Message Protocol	Internet 控制报文协议

L

LAN	Local Area Network	局域网
LCP	Link Control Protocol	链路控制协议

M

MAC	Media Access Control	媒体存取控制
-----	----------------------	--------

N

NAT	Network Address Translation	网络地址转换
-----	-----------------------------	--------

P

PPTP	Point to Point Tunneling Protocol	点对点隧道协议
------	-----------------------------------	---------

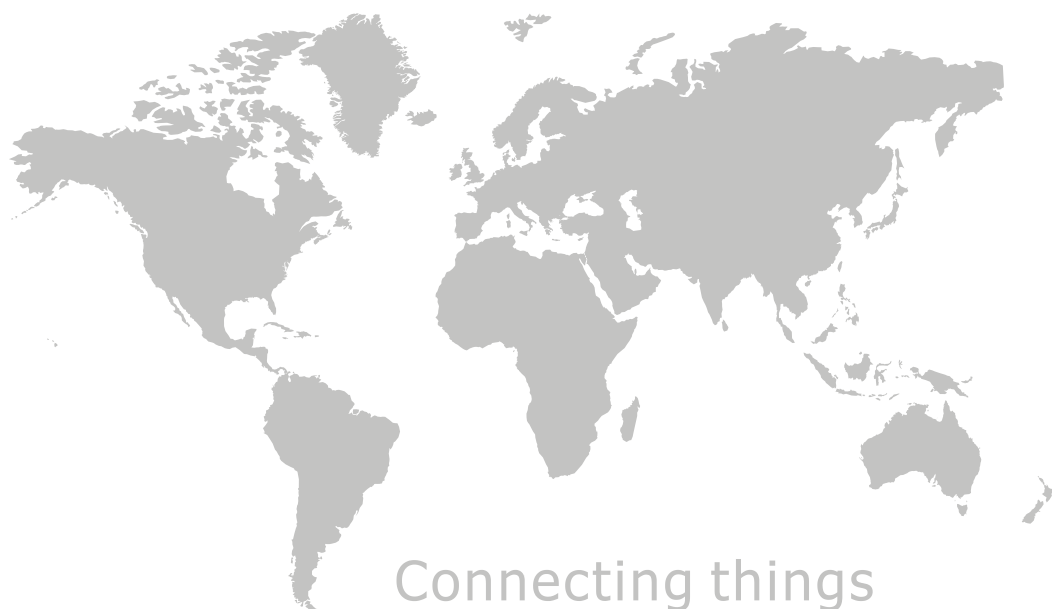
S

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
-----	-------------------------------	--------

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		
WWW	World Wide Web	环球信息网,万维网



 **宏电®** 深圳市宏电技术股份有限公司
Hongdian Shenzhen Hongdian Technologies Corporation

地址：深圳市吉华街道中海信科技园 14A14-16 层

电话：400-00-64288

传真：0755-83404677

网址：www.hongdian.com

E-mail: market@hongdian.com