

H8951S、H8951、H7920 Router 使用说明书



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

深圳市宏电技术股份有限公司

地址： 深圳市龙岗区布澜路中海信科技园总部中心14-16层

网址： <http://www.hongdian.com>

技术专线： 400-00-64288拨2

投诉热线： 400-00-64288拨3

传真： 0755-83644677

邮政编码： 518112

版权所有 ©2019 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

 宏电[®]、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

概述

H8951 系列路由器是宏电自主研发的移动通信网络数据通信终端接入产品。该系列产品基于 4G 无线通信技术，采用高性能 32 位嵌入式操作系统，全工业级设计。通过内嵌 4G 模块接入全球 4G 网络，提供高性能 4G 通信速度，广泛应用于智能物流柜、充电桩、自主终端机、电信、金融、信息传媒、电力、交通、车载和环保等行业。

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。

本文档适用于 H8951 系列路由器，分别为 H8951S、H8951、H7920 工业路由器。

产品版本

与本文档相对应的产品版本如下所示。

产品名称	产品版本
H8951S 4G Router	2xLAN，其中一个 LAN 可定制为 WAN，有串口、WIFI 功能
H8951 4G Router	2xLAN，其中一个 LAN 可定制为 WAN，有 WIFI 功能
H7920 4G Router	1xLAN，有串口

读者对象

本文档适用于以下人员：

- 研发工程师
- 技术支持工程师
- 客户

如果是初次接触和使用宏电 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。

目录

1 产品介绍	6
1.1 概述.....	6
1.2 产品定位.....	6
1.3 功能与特点.....	7
H8951、H8951S、H7920 主要功能差异点见表 1-1.	7
2 产品结构	9
2.1 设备的配件以及型号说明.....	9
2.2 功能结构.....	10
3 安装 Router	12
3.1 开箱.....	12
3.2 安装与接线.....	12
3.2.1 SIM 卡的安装.....	12
3.2.2 以太网线连接.....	13
3.2.3 以太网线的连接.....	14
3.3 供电电源.....	14
3.4 安装检查.....	14
4 配置前准备	15
4.1 本地连接配置.....	15
5 路由器配置	25
5.1 概述.....	25
5.2 基本配置.....	25
5.2.1 登录 WEB 配置界面.....	25
5.2.2 网络设置.....	26
5.3 应用程序配置.....	47
5.3.1 ICMP 检测.....	47
5.3.2 DDNS 设置.....	50
5.3.3 DTU 配置（H8951S 和 H7920 支持）.....	51
5.3.4 SNMP 配置.....	57
5.3.5 M2M 配置.....	59
5.3.6 任务管理设置.....	60
5.4 安全配置.....	62
5.4.1 概述.....	62
5.4.2 IP 过滤.....	62
5.4.3 域名过滤.....	65
5.4.4 MAC 过滤.....	67
5.5 转发配置.....	68

5.5.1 概述.....	68
5.5.2 NAT.....	69
5.5.3 路由配置.....	73
5.5.4 QoS.....	76
5.5.5 动态路由配置(可选).....	78
5.6 VPN 功能配置.....	83
5.6.1 概述.....	83
5.6.2 VPDN 配置.....	83
5.6.3 Tunnel 配置.....	85
5.6.4 IPSec 设置.....	86
5.6.5 Open VPN 设置.....	93
5.7 系统管理配置.....	96
5.7.1 概述.....	96
5.7.2 本地日志.....	96
5.7.3 远程日志.....	97
5.7.4 系统时间.....	98
5.7.5 用户管理.....	99
5.7.6 网络测试.....	101
5.7.7 文件升级.....	102
5.8 状态.....	105
5.8.1 概述.....	105
5.8.2 基本信息.....	105
5.8.3 LAN 状态.....	106
5.8.4 WAN 状态（可选）.....	107
5.8.5 移动网络状态.....	108
5.8.6 WLAN 状态.....	110
5.8.7 路由表.....	113
5.9 RESET 键功能.....	114
6 典型应用.....	115
6.1 概述.....	115
6.2 ICMP 检测功能应用.....	115
6.3 链路备份功能应用.....	116
6.4 参数切换功能应用.....	118
6.5 VPN 功能应用.....	121
6.6 任务管理应用.....	124
7 FAQ/异常处理.....	126
7.1 硬件类问题.....	126
7.1.1 所有指示灯均不亮.....	126
7.1.2 SIM 卡座连接问题.....	126

7.1.3 网口连接问题.....	127
7.2 拨号类问题.....	127
7.2.1 拨号中断.....	127
7.2.2 无信号显示.....	127
7.2.3 无法找到 SIM/UIM 卡.....	128
7.2.4 通信信号薄弱.....	128
7.3 VPN 连接类问题.....	129
7.3.1 VPDN 无法连接.....	129
7.3.2 VPN 无法通信.....	129
7.3.3 路由可通信但子网不可通信.....	129
7.4 WEB 配置操作类问题.....	130
7.4.1 升级固件失败.....	130
7.4.2 恢复参数失败.....	130
7.4.3 升级补丁失败.....	131
7.4.4 CFE 升级失败.....	131
7.4.5 页面升级失败.....	131
7.4.6 忘记路由器登录密码.....	132
参数规范表.....	133
缩略语构.....	134

1 产品介绍

1.1 概述

H8951 系列路由器是基于 4G 技术研究的无线路由网关设备，除了具备传统路由器的 VPN、防火墙、NAT、PPPoE、DHCP 等功能之外，还能支持 4G 无线拨号，提供最高可达 150Mbps 的无线高速带宽。H8951 系列路由器支持两个以太网接口，可更好的满足自助终端机、广告机等多 LAN 需求的应用。H8951 系列路由器内置防火墙，支持 IP、域名、MAC 白黑名单过滤，支持访问控制列表，有效控制内外部用户非法访问。

H8951 系列路由器支持 802.11b/g/n，速率最高可达 300Mbps，轻松构建无线局域网；支持 WEP/WPA/WPA2 等加密，保障无线局域网安全。

H8951 系列路由器支持宏电自主研发 M2M 管理平台。M2M 平台能实现对设备现场 4G 无线网络信息及状态的统计及设备的远程升级和配置管理。

1.2 产品定位

H8951 系列路由器广泛应用于：智能物流柜、充电桩、自主终端机、电信、金融、信息传媒、电力、交通、车载和环保等行业。

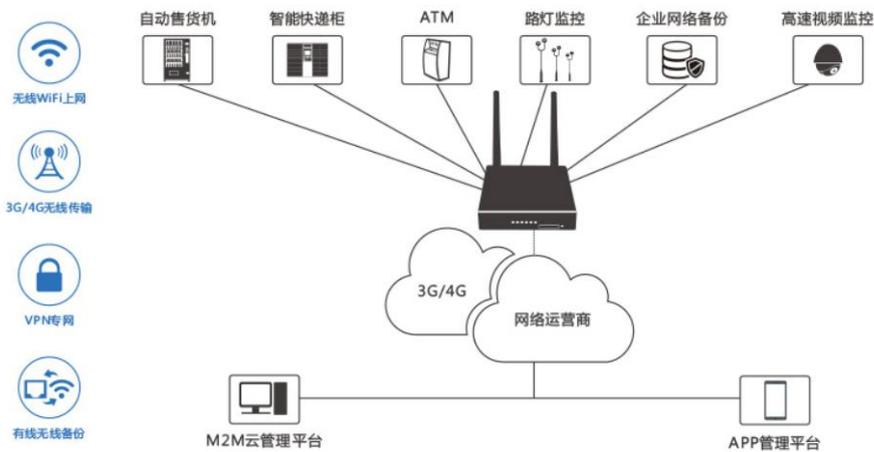


图 1-1

1.3 功能与特点

H8951、H8951S、H7920 主要功能差异点见表 1-1.

	WAN	串口 (DTU)	WIFI
H8951	可选。默认出厂 LAN	不支持	支持
H8951S	可选。默认出厂 LAN	支持	支持
H7920	不支持	支持	不支持

表 1-1

基本功能

- 支持 LTE、HSPA+、CDMA 2000 EV-DO Rev.A、WCDMA (HSDPA, HSUPA)、TD-SCDMA 等网络，同时向下兼容 GPRS/EDGE/GSM 或 CDMA 1X 网络
- 支持 WAN、WLAN、4G 等多网同时在线、多网备份切换
- 支持 WLAN AP/station 客户端功能，支持 802.11b/g/n，当有 WIFI 功能时
- 支持 LAN 口百兆网速交换
- 支持 WAN 口 PPPoE 拨号 (可选)
- 支持 VPDN、APN 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
- 可选支持 OpenVPN
- 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
- 支持串口 DTU 功能
- 支持本地、远程、平台固件升级
- 支持本地、远程、平台补丁升级
- 支持 CFE 升级固件（升级等业务过程中设备断电等异常引起文件系统崩溃后的升级方法，升级效率更高）
- 支持 WEB、CLI、SSH、平台多种参数管理方式
- 支持 M2M 平台管理，可实时统计设备流量、监控设备网络状态
- 支持参数备份及导入，支持使用私钥导入导出参数配置
- 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
- 可选支持 QoS（Quality of Service），可针对业务、协议、IP 网段进行多种方式的 QoS 带宽智能管理
- 支持静态路由、支持 RIPv2（路由信息协议，Routing Information Protocol）和 OSPF（开放式最短路径优先，Open Shortest Path First）动态路由、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 网络类型和信号强度等状态）
- 支持本地和远程系统日志功能，实现设备运行的实时监控

2 产品结构

2.1 设备的配件以及型号说明

配件说明

H8951 系列路由器包含如表 2-1 所示配件。

配件名称	数量	备注
根据不同需求，可选配件有		
H8951 系列路由器	1 个	据用户订货情况包装，有 H8951、H8951S、H7920
4G 天线	1 根	
WLAN 天线	1 根	H8951、H8951S 可配。H7920 不支持。
RJ45 网线	1 根	无
安装固定件	1 份	无
合格证和保修卡	1 份	无
+12V 电源适配器	1 个	无

表 2-1



说明

根据客户实际需求，可配备高增益天线，详询技术支持。

型号说明

H8951 系列路由器是基于 4G 无线通信技术研究的无线路由传输产品（同时支持有线传输），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。

接口说明

详见各型号产品的技术规格书。

2.2 功能结构

H8951 系列路由器功能结构如图 2-1 所示。

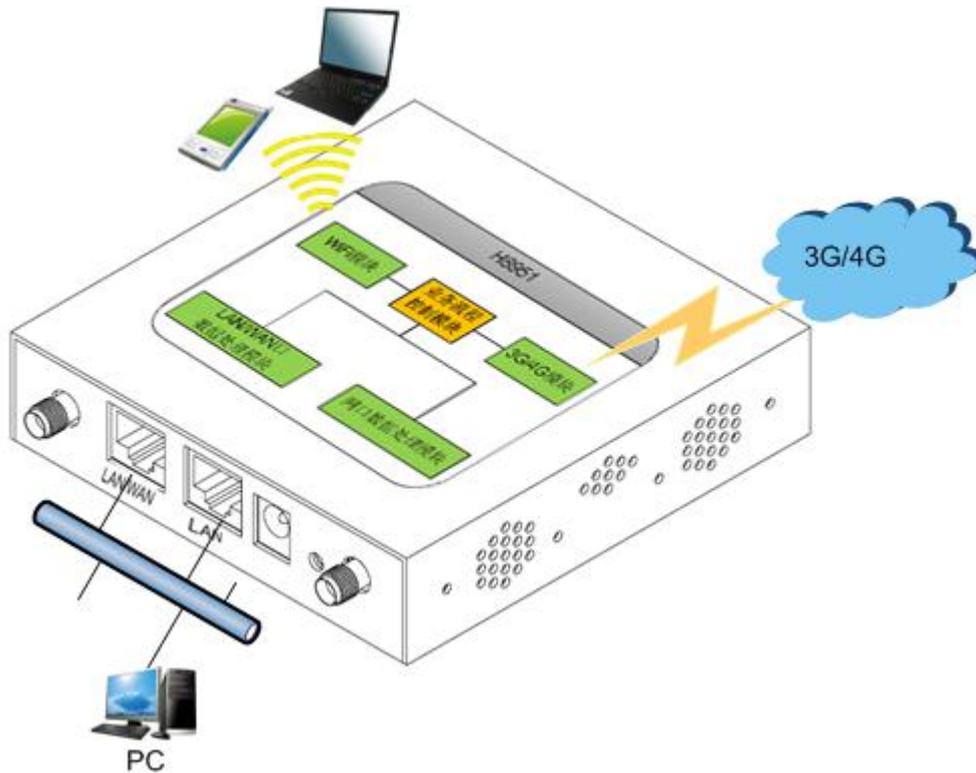


图 2-1

业务流程控制模块

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

串口（H8951S 和 H7920 支持）

6pin 端子，主要用于对路由器进行调试、参数配置、路由器出现的问题诊断等，支持 DTU 功能。

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。

WAN（H8951 和 H8951S 可选支持）

该模块主要用于使路由器能够通过有线方式连接到 Internet。

WLAN（H8951 和 H8951S 支持）

该模块主要用于 WLAN 终端连接 Wi-Fi 热点，便于 WLAN 终端连接外网。它还支持桥接和客户端两种功能模式，通过该模式可以实现与其他 AP 连接而实现 Internet 上网功能。

3 安装 Router

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 2-1 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



在进行 SIM 卡安装时，请确保路由器处于断电状态

步骤 1 用尖锐物体轻按下 SIM 卡座上的按钮使卡座弹出，如图 3-1 所示。



图 3-1

步骤 2 将 SIM 卡金属面朝上，插入到卡座，缺角端朝外侧。然后将卡座按推入卡槽。如图 3-2 所示。

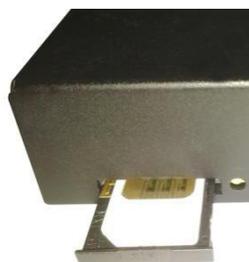


图 3-2

3.2.2 以太网线连接

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。以太网连接可以分为单设备直连方式和多设备局域网连接方式。

单设备直连方式

使用RJ-45类型接头的以太网线将配置电脑与产品的LAN口直接连接(H8922和H8922S有4个LAN口，取其中的任何一个连接都可以)，如图3-3所示。

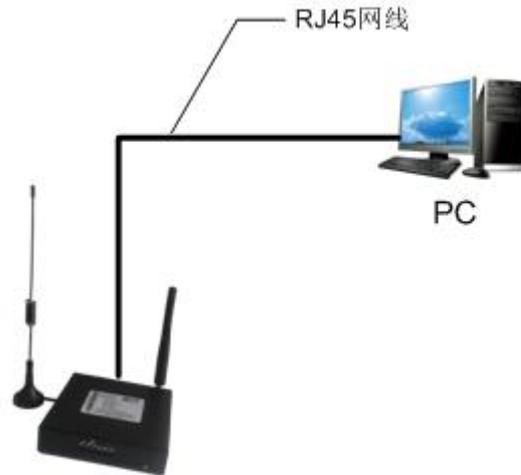


图 3-3

多设备局域网连接方式

H8951 LAN口可以连接一个交换机，实现同时接入多台设备连接组成本地局域网网络（多台设备可以在同一网段），如图3-4所示。

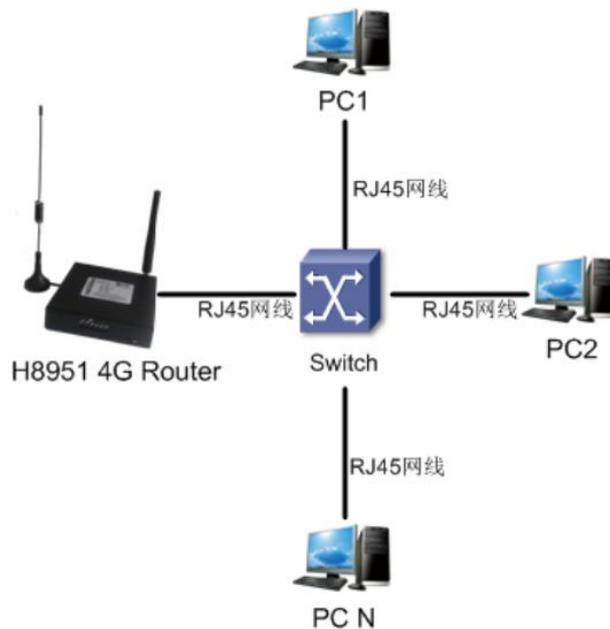


图 3-4

3.2.3 以太网线的连接

H8951 系列路由器产品支持 LAN 口和 WAN 口的局域网/广域网的连接，可以使用 RJ45 网线将网线的一端插入路由器的 LAN/WAN 接口，另一端连接其他设备即可。

3.3 供电电源

H8951 系列路由器产品使用+5V~+36V 直流供电，建议使用 12V/1.5A 的电源。

H8951 型号路由器产品使用+12V 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 向路由器供电，下面仅以左侧的 SIM 卡来说明路由器的拨号情况，右侧的 SIM 相同。

- 供电后如果路由器上接有下位机的 LAN 口灯亮，表示 Router 供电正常。
- 供电一段时间后，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，NET 指示灯亮并快闪，表示路由器已找到模块并开始拨号。
- 路由器在拨号过程中，RF 灯会亮，表示路由器已获得 SIM 卡信号强度，根据 RF 灯的闪动情况可以判断网络信号强度。详情请参见“路由器技术规格书”。
- 路由器拨号结束后，若 4G 灯常亮，则表示拨上的网络是 4G。若慢闪，表示拨上的网络为 2G/2.5G/2.75G。



对于不同的模块以及不同网络环境，路由器找到模块以及拨号的时间可能不一致，但路由器拨号流程则严格按照上面所述。

4 配置前准备

4.1 本地连接配置

前提条件

- 已经为路由器通电。
- 已经通过以太网网线连接路由器网口。

以太网连接具体操作请参见“3.2.2 以太网线连接”。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“网络和共享中心”，如图 4-1 所示。



图 4-1

步骤 2 双击“本地连接”，打开“本地连接状态”窗口，如图 4-2 所示。



图 4-2

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

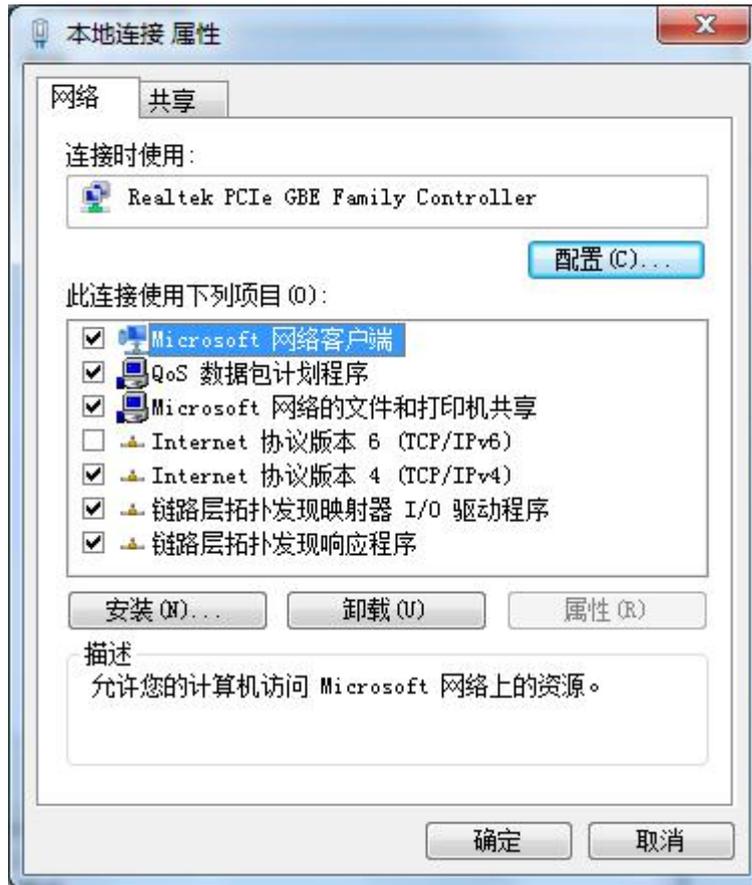


图 4-3

后面的配置存在两种配置方法，即常规方法配置和高级配置。

- 常规方法配置
 1. 在“本地连接属性”窗口中双击“Internet 协议版本 4 (TCP/IPv4)”，打开 Internet 协议版本 4 (TCP/IPv4) 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。



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

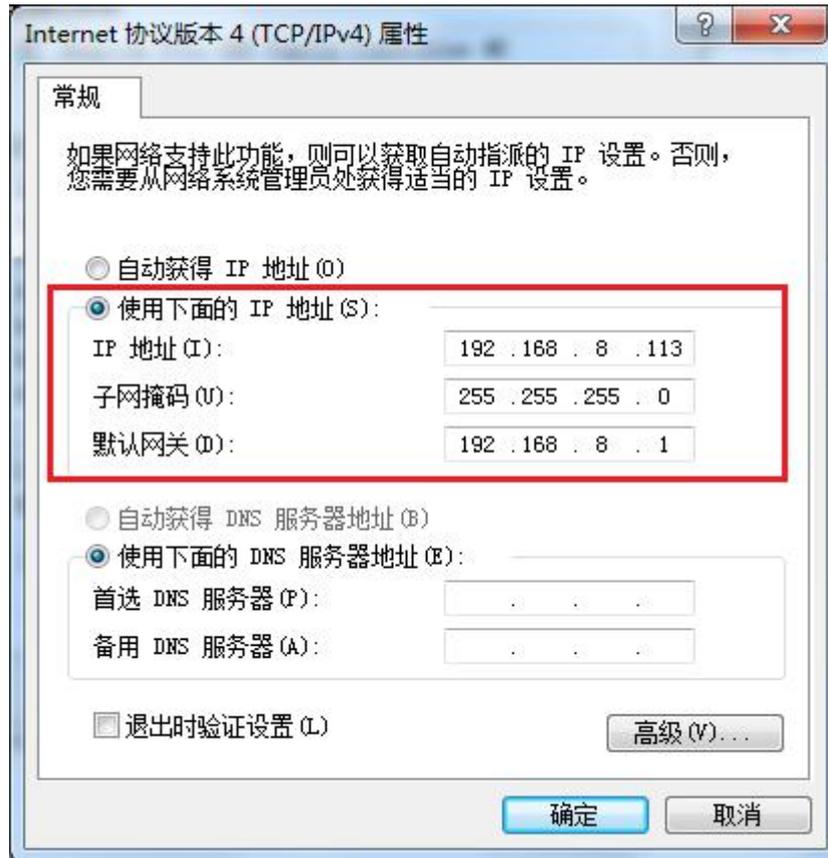


图 4-4

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。

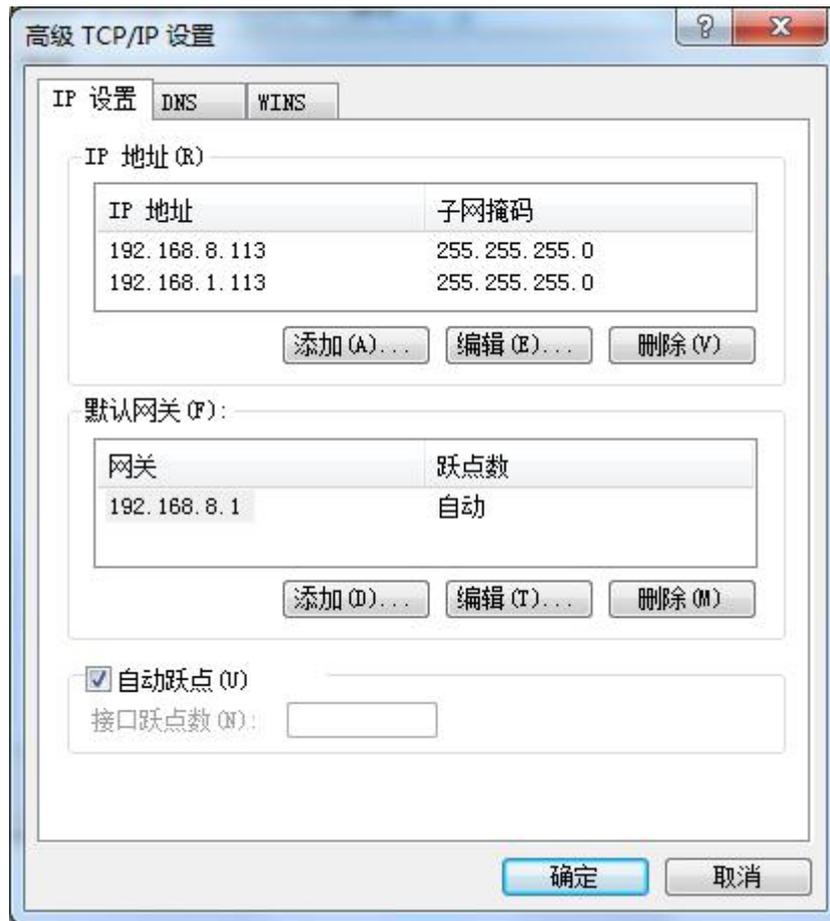


图 4-5

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

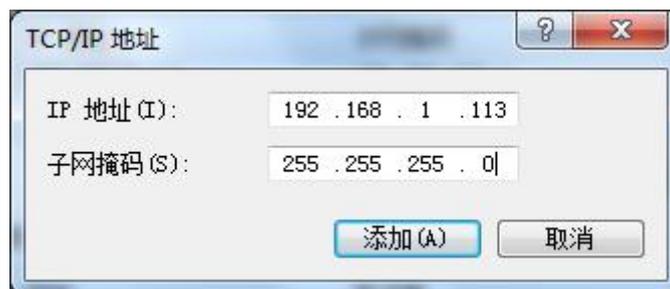


图 4-6

- 单击“添加”，完成配置。

DHCP 自动获取 IP 方式

H8951 系列路由器内置 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

H8951 系列路由器内置的 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

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

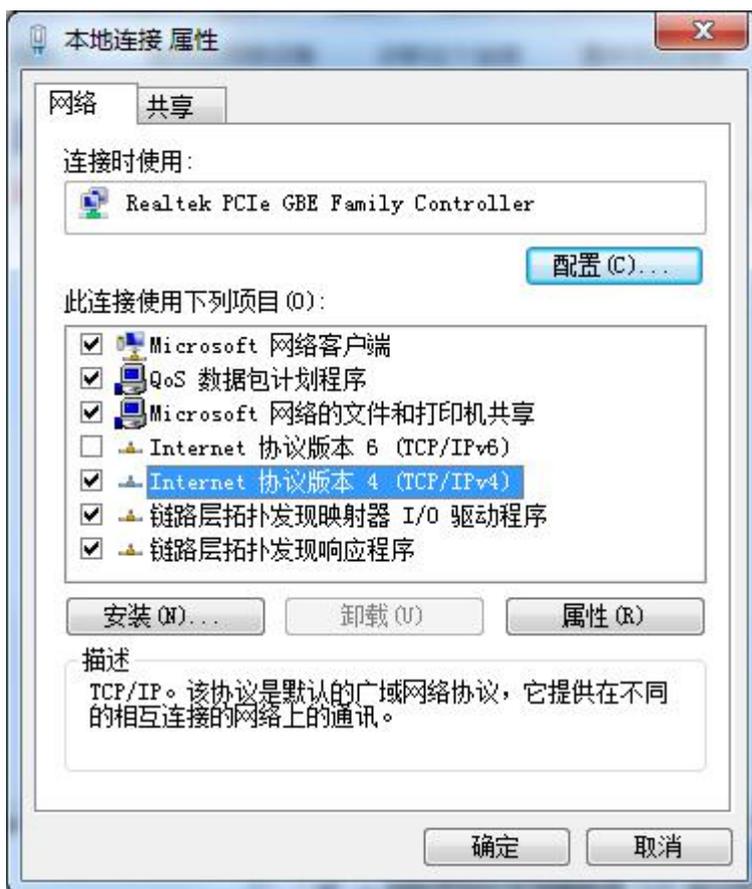


图 4-8

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

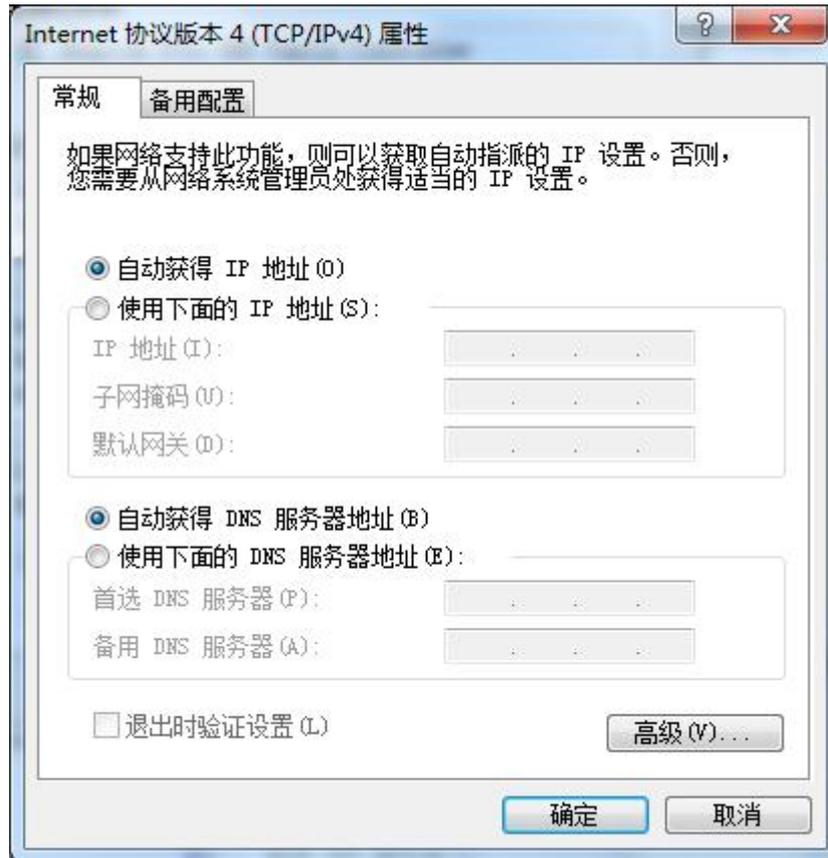


图 4-9

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。

配置检查

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



图 4-10

步骤 7 在命令行窗口中输入命令“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。

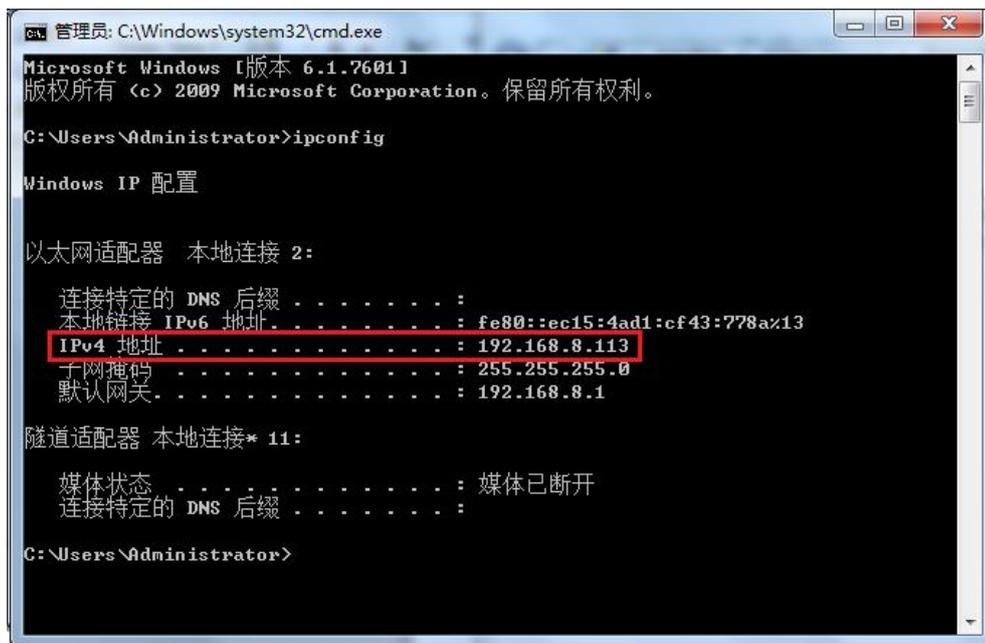


图 4-11

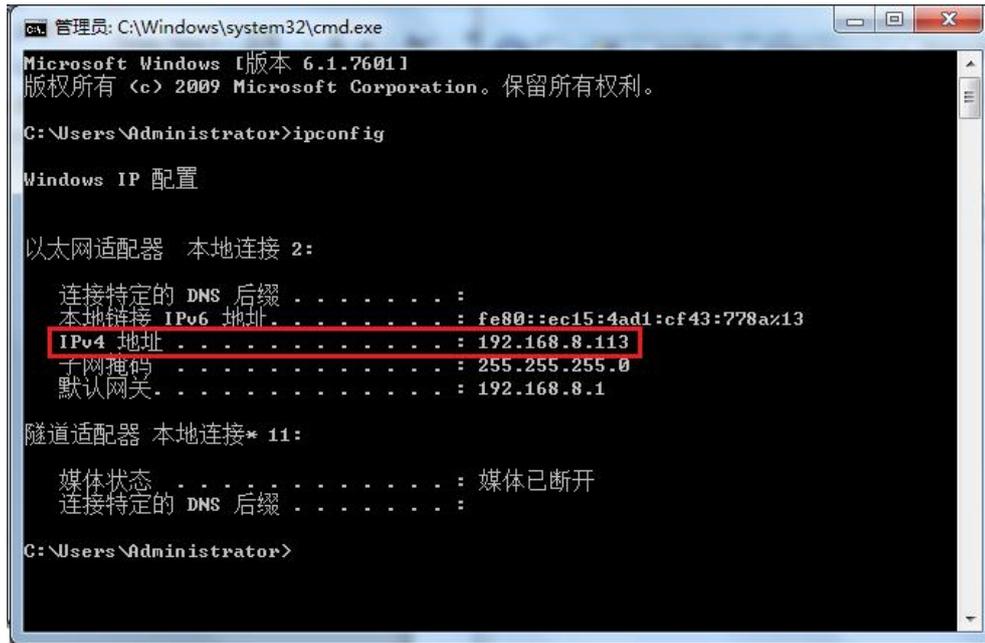


图 4-12

步骤 8 在命令行窗口中输入“ping 192.168.8.1”命令确认连通性是否正常。

如果出现如图 4-13 所示界面，表示本地计算机与路由器连通性正常。



图 4-13

5 路由器配置

5.1 概述

H8951 系列路由器可采用 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，登录到路由器进行配置操作。

5.2 基本配置

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。

5.2.1 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/”。进入用户登录身份认证界面，如图 5-1 所示。



图 5-1

步骤 2 输入“用户名”、“密码”，单击“确定”。即可登录到路由器的 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”。

5.2.2 网络设置

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

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 H8951 系列路由器的 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。

图 5-2

步骤 3 配置 LAN 口连接参数，参数说明如表 5-1 所示。

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

参数名称	含义	如何配置
		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 接口关闭而消失。	手动输入。 格式：A.B.C.D/M 接口型，输入规范请参见“参数规范表”。

表 5-1

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。

WAN（可选）

WAN 主要用于通过以太网连接 Internet，连接方式有静态 IP、DHCP、PPPoE 三种方式。（出厂默认 WAN 口是 LAN 功能）

步骤 1 单击“网络设置>WAN”。

打开“WAN”页签，如图 5-3 所示。

图 5-3

步骤 2 配置 WAN 口连接类型。

WAN 口参数说明如表 5-2 所示。

参数名称	含义	如何配置
连接类型	广域网的连接类型。	下拉框选择，包含： <ul style="list-style-type: none"> • 静态 IP：手动配置接口 IP，若需要通过 WAN 上网则需要在网络连接类型中补充网关、DNS、默认路由等配置。 • DHCP：DHCP 客户端自动获取 IP 方式，若需要通过 WAN 上网，则需在网络连接类型中补充默认路由配置。

参数名称	含义	如何配置
		<ul style="list-style-type: none"> • PPPoE: PPPoE 拨号获取 IP 方式（通常是外接 ADSL 猫进行 ADSL 拨号上网），若需要通过 WAN 上网，则需要在网络类型类型中补充默认路由配置。
IP: “连接类型”选择“静态 IP”时显示		
IP	当“连接类型”选择“静态 IP”时需配置。	接口型 A.B.C.D/M， 输入规范请参见“参数规范表” 例如：10.0.0.1/24
基本设置: “连接类型”选择“PPPoE”时显示		
接口名称	接口的唯一标识名，用于其他功能调用或者关联本接口时使用，如配置该接口的路由、控制该规则接口的禁用、启用。	PPPoE 不可配置项。 网页配置的 PPPoE 接口名由系统指定，其接口名是：pppoe
服务名称	配置 PPPoE 服务名，通常是用于客户端与服务端之间的身份识别与判断，通常由服务端提供，ADSL 拨号时由 ISP 提供。	一般 WORD 类型，最大 64 字节，不能为空，输入规范请参见“参数规范表”。
用户名/密码	PPPoE 拨号所用用户名/密码，通常由服务器端提供，ADSL 拨号时由 ISP 提供。	一般 WORD 类型/CODE 类型，各最大长度 64 字节，均非空，输入规范请参见“参数规范表”。
高级设置	高级参数在特殊情况下使用，通常不建议配置，“高级设置”的参数说明，请参见“移动网络”中的相关参数。	单击“显示”即可显示高级设置参数。

表 5-2

步骤 3 单击“保存”，完成 WAN 口连接类型配置。

WLAN

H8951 系列路由器可提供 2.4G WLAN。H8951 系列支持 ap、station 客户端两种工作模式。

步骤 1 单击“网络设置>WLAN”。

打开“WLAN 配置”页签，选择不同工作模式时，显示页面分别如图 5-4、图 5-5 所示。当工作模式为 Station 时，需要扫描周围 AP，以选择一个 AP 接入，如图 5-7 所示。



图 5-4



图 5-5



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。

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 WAN WLAN 移动网络 参数切换 网络连接 链路备份 DHCP服务

无线访问点

ID	BSSID	SSID	工作通道	信号强度	认证	加密	操作
0	5C:0E:8B:89:35:D0	CMCC-WEB	1	-86	open	none	连接
1	5C:0E:8B:8D:CD:E0	and-Business	1	-68	open	none	连接
2	D4:CA:6D:A4:18:0D	HDWIFI	1	-72	wpa2	aes	连接
3	5C:0E:8B:92:18:80	and-Business	1	-86	open	none	连接
4	5C:0E:8B:8D:CD:E1	CMCC-FREE	1	-74	open	none	连接
5	5C:0E:8B:8D:CD:E2	CMCC	1	-68	wpa2	tkip	连接
6	5C:0E:8B:92:14:D1	CMCC-FREE	1	-68	open	none	连接
7	D4:CA:6D:A4:CF:9D	HDWIFI	3	-72	wpa2	aes	连接
8	D6:CA:6D:A4:CF:9D	HD-Guest	3	-64	wpa2	aes	连接
9	BC:30:0A:C8:D8:00	VIFI-ybli	5	-74	open	none	连接
10	04:F0:1A:E9:1A:00	hp8899	5	-70	open	none	连接
11	48:A9:D2:44:37:29	AndroidAP	6	-66	wpa2	tkip	连接
12	60:BB:0C:1F:0E:80	ChinaNet-YP3i	8	-70	wpa	aes	连接
13	BC:D1:77:76:C1:7A	iscan-mobile3	11	-88	wpa2	tkip	连接
14	F0:B4:29:21:D7:CD	Xiaomi_D7CC	11	-72	wpa	tkip	连接

返回 刷新

图 5-7

步骤 2 配置“WLAN”相关参数。

WLAN 的参数说明如表 5-3 所示。

参数名称	含义	如何配置
基本信息		
SSID	WLAN 服务端身份标识。	一般 WORD 类型，最大 32 字节，输入规范请参见“参数规范表”。
工作模式	WLAN 工作模式，支持 ap/station 模式。	下拉框选项 <ul style="list-style-type: none"> • ap • station
网络模式	WLAN 网络模式，不同网络模式传输速率有较大差异，默认 n 模式。当工作模式选择 AP 时，需	下拉框选项 <ul style="list-style-type: none"> • bgn 表示 WLAN 速率可支持 11Mbps、54Mbps、150Mbps、

参数名称	含义	如何配置
	要手动设置 AP 的网络模式；当工作模式选择 station 时，网络模式为选择的 AP 的网络模式，不可手动修改。	300Mbps
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。 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。	下拉框选项 • auto • 1~13
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
AP 隔离	将接入 AP 的 WLAN 客户端进行隔离，使各客户端之间相互不能访问。	单选按钮选择 • 启用 • 禁用
广播状态	用于配置 WLANSSID 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 SSID。	单选框选择 • 启用 • 禁用
IP 分配（当工作模式选择 station 时需要配置）	路由器当做 station 连接到 AP 时与 AP 通信的地址。	下拉框选项 • dhcp: 通过 AP 的 DHCP 功能获得 IP 地址 • static: 手动设置 IP 地址
IP（当工作模式选择 station 时需要配置）	当“IP 分配”选择 static 时需要配置，与 AP 建立通信的地址。	格式：A.B.C.D 型，输入规范请参见“参数规范表”
WLAN 加密		
加密方式	配置 WLAN 的加密方式，当不需要加密验证时可以 disable。加密可使用 WPA 或者 WPA2 加密方式。	下拉框选项 • wpa • wpa2
wpa/wpa2（WiFi Protected Access，WiFi 网络安全存取）		
算法	加密采用算法 • tkip • aes	下拉框选项选择。

参数名称	含义	如何配置
WPA 共享密钥	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“参数规范表”。
WPA 更新时间间隔	AP 验证 WLAN 客户端密钥时间间隔;如果验证通过则继续保持 WLAN 连接,如果验证不通过,则断开 WLAN 连接。	取值范围: 120~86400 单位: 秒

表 5-3



说明

802.11n 的速率为 150Mbps,是物理层通信速率;终端业务下载速率是 100Mbps。

移动网络

移动网络是 H8951 系列路由器最核心功能之一, H8951 系列路由器支持单模单卡拨号、单模双卡备份拨号两种移动网络拨号方式,为用户提供高速无线宽带上网功能。LTE 可高达近 100Mbps 的上网速率。

步骤 1 单击“网络设置>移动网络”。

单模单卡/单模双卡规则如图 5-9 所示:



图 5-9

步骤 2 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 5-10 所示。

图 5-10

2. 对“移动网络”参数进行添加操作。“移动网络”参数说明如表 5-4 所示。

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。 <ul style="list-style-type: none"> • 启用 • 禁用
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”。
服务代码	网络的一种代码标识，通常一种制式的网络有固定的服务代码，如 G 网：*99***1#，C 网：#777。	CODE 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	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
	商也开始使用。	
PIN	Personal Identification Number, SIM 卡的识别密码, 用户可以使用 PIN 码对 SIM 卡进行解锁和加锁, 防止非法用户使用。	字母数字 WORD 型, 输入规范请参见“参数规范表”。
SIM 卡 (单模双卡)	单模双卡模式下配置选项, 用于指定拨号时选择 SIM 卡。	单选框选择 <ul style="list-style-type: none"> • SIM1 • SIM2
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 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 <ul style="list-style-type: none"> • auto • wcdma • edge • evdo • cdma • td-scdma • lte AUTO 表示 2.5G/4G 自适应。
高级设置	用于配置 PPP 拨号的高级参数, 通常情况下不建议配, 通常在专网业务服务端有对应匹配要求情况下使用, 本产品 VPDN、PPPoE 的拨号高级选项与 modem 高级选项一致, 如图 5-13 所示。	单击即可显示高级设置。
认证&加密 (配置时需要与服务端匹配, 默认全部为协商)		
CHAP	挑战握手协议 (Challenge-Handshake Authentication Protocol), 是一种加密验证方式, 能够避免建立连接时传送用户的真实密码。主要针对 PPP 的, 认证时密钥信息不需要在通信信道中发送, 而且每次认证所交换信息都不一样, 可以很有效地避免监听攻击, 安全性较高。	单选框选择 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 禁用 • 协商
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 <ul style="list-style-type: none"> • 禁用 • 协商
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 <ul style="list-style-type: none"> • 禁用

参数名称	含义	如何配置
		<ul style="list-style-type: none"> • 协商
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 认证方法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 <ul style="list-style-type: none"> • 禁用 • 协商
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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 接受 • 禁用
协议域压缩	是否启用协议域压缩。	单选框选择 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 接受 • 禁用
其它		
调试	使能 PPP 拨号时链路交互的调试日志, 主要用于分析 PPP 拨号协商过程, 默认打开, 当设备可以正常运行又不希望看到过多调试信息可以关闭, 默认为打开, 不建议禁用。	单选框选择 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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	取值范围: 1~512 单位: 秒

参数名称	含义	如何配置
	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。	缺省值：30/5
最大传输单元	PPP 接口发送单个数据报的报文最大长度，通常拨号过程中与运营商协商得到。下位机有报文大小传输要求时配置，通常金融数据交互有此要求的较多。	取值范围：128~16364 单位：byte
最大接收单元	PPP 接口接收单个数据报的报文最大长度，通常拨号过程中与运营商协商得到，通常金融数据交互有此要求的较多。	取值范围：128~16364 单位：byte
本地 IP	PPP 拨号时指定本地 IP，以便使得本地获得的 IP 地址一直是固定的，通常在专网业务有此配置，需要运营商提供该服务才能配置。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：10.10.10.1
远端 IP	PPP 拨号协商 IP 地址时对端的身份识别，现大多数网络已经不使用该参数，通常指定本地 IP 即可，需要运营商提供该服务才能配置。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：10.10.10.254
专家选项	<ul style="list-style-type: none"> • 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。 <p>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。</p>	<p>LINE 类型，输入规范请参见“参数规范表”。</p> <p>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。</p>

表 5-4



图 5-11



图 5-12

3. 单击“保存”，完成对“移动网络”的参数配置。

- 编辑

如图 5-9 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 5-4 所示。

- 删除

如图 5-9 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 5-9 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 5-9 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。

认证 & 加密

CHAP	<input checked="" type="radio"/> 协商 <input type="radio"/> 禁用
PAP	<input checked="" type="radio"/> 协商 <input type="radio"/> 禁用
MS-CHAP	<input checked="" type="radio"/> 协商 <input type="radio"/> 禁用
MS2-CHAP	<input checked="" type="radio"/> 协商 <input type="radio"/> 禁用
EAP	<input checked="" type="radio"/> 协商 <input type="radio"/> 禁用

压缩 & 控制协议

压缩控制协议	<input type="radio"/> 接受 <input checked="" type="radio"/> 禁用
地址/控制压缩	<input type="radio"/> 接受 <input checked="" type="radio"/> 禁用
协议域压缩	<input type="radio"/> 接受 <input checked="" type="radio"/> 禁用
VJ TCP/IP 头部压缩	<input type="radio"/> 接受 <input checked="" type="radio"/> 禁用
连接ID压缩	<input type="radio"/> 接受 <input checked="" type="radio"/> 禁用

其它

调试	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
对端DNS	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
LCP间隔时间	<input type="text" value="30"/> 1-512 秒
LCP重试次数	<input type="text" value="5"/> 1-512 次
最大传输单元	<input type="text"/> 128-16384 字节
最大接收单元	<input type="text"/> 128-16384 字节
本地IP	<input type="text"/> 如：192.168.8.1
远端IP	<input type="text"/> 如：192.168.8.254

专家选项

nompe: 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。

图 5-13

参数切换

H8951 系列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。其主要应用场景为：多服务端互备份，多运营商备份（一张 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），功能参数需要捆绑组合等相互冲突的组网但又需要相互间备份切换的应用场景。

步骤 1 单击“网络设置>参数切换”。

打开“参数切换”页签，如图 5-14 所示。



图 5-14

步骤 2 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 5-15 所示。



图 5-15

2. 添加一条“参数切换”规则。

参数切换参数说明如表 5-5 所示。

参数名称	含义	如何配置
基本信息		
规则名称	参数切换规则名称标识，用于区分不同的规则。	取值范围：[0,9]
间隔时间/重试次数	检测的时间间隔和最大失败次数。若失败次数达到配置的次数则切换到下一条规则进行工作。	取值范围：1~512 单位：秒/次数 默认值：60/3
超时时间	用于限定当前规则最大工作时间，rule0 中该参数无效，其他规则中配置该参数并且到达最大工作时间后切换到 rule0，不配置则按 rule 的顺序切换。通常没有严格主备要求时不建议配置。	取值范围：1~65535 单位：秒
添加接口检测规则		
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

表 5-5

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



说明

为保证用户对路由器上线和下线的控制，H8951 系列路由器提供了多个对 modem 起作用的功能，如参数切换、链路备份、ICMP 检测、任务管理等。其中任务管理是对 modem 执行动作并保持该动作执行后的状态，而参数切换、链路备份、ICMP 检测都是对 modem 执行动作但并不保持状态。故参数切换和 ICMP 检测、任务管理等功能只对 modem 执行动作而不会有冲突，可配合使用。

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

网络连接

网络连接功能是为用户提供默认路由配置。

步骤 1 单击“网络设置>网络连接”。

打开“网络连接”页签，如图 5-16 所示。



图 5-16

步骤 2 配置“网络连接”相关参数。

网络连接的参数说明如表 5-6 所示。

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。
网关	默认路由选择 eth0 口并且 WAN 口为静态 IP 时，需要配置 WAN 口地址的下一跳网关地址，如果需要访问域名则还需要自定义配置 DNS。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.10.254
DNS 类型	配置路由器的 DNS 类型，选择接口时则使用接口拨号等方式自动的获取 DNS，若为 WAN 静态 IP 时必须手动定义设置 DNS。	下拉框选项 • interface • custom
DNS1/DNS2	DNS 类型选择 custom 时配置，手动配置 DNS 地址，最多可配置两个。	接口型 A.B.C.D 例如：8.8.8.8

参数名称	含义	如何配置
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 <ul style="list-style-type: none"> • modem • eth0 • eth1 eth0 表示关联 WAN 口 PPPoE 拨号或者 DHCP 获取的 DNS，特别注意 WAN 静态 IP 时选择 eth0 无效，PPP 拨号配置禁用对端 DNS 时选择 modem 无效，eth1 表示 WLAN 获得的 DNS。

表 5-6

步骤 3 单击“保存”，完成网络连接的配置。



说明

当“默认路由”选择“eth0”接口，且 WAN 口形式从 DHCP 或静态 IP 切换至 PPPoE 时，路由器默认路由需要点击“网络连接”页面的“保存”才会显示并生效。

当“默认路由”选择“eth0”接口，且 WAN 口形式从 DHCP 切换至静态 IP 时，路由器默认路由需要先到“转发设置->路由”先删除默认路由，然后点击“网络连接”页面的“保存”才会显示并生效。

链路备份

H8951 系列路由器能实现无线与无线、无线与有线链路之间的互备切换，能在某一链路故障时能快速切换到备份链路，保障下位机通讯链路的联通性和稳定性，从而保障用户数据业务不受影响。路由器支持冷、热两种主备份模式。

步骤 1 单击“网络设置>链路备份”。

打开“链路备份”页签，如图 5-17 所示。



图 5-17

步骤 2 单击“添加”，打开添加“链路备份”规则页面，如图 5-18 所示。

图 5-18

步骤 3 配置“链路备份”相关参数。

链路备份的参数说明如表 5-7 所示。

参数名称	含义	如何配置
状态	使能链路备份功能。	按钮 <ul style="list-style-type: none"> • 启用 • 禁用
规则名称	链路备份规则名称标识 说明 0 可以为主链路，也可以为备份链路； 1~9 只能为备份链路； 备份链路 1~9 之间根据数字大小决定优先级，数字越小，优先级越高。	取值范围：0~9
链路运行方式	备份方式，包含： <ul style="list-style-type: none"> • main: 链路模式为主链路。 • backup: 链路模式为备份链路。 	下拉框选择。
备份模式	备份模式，有冷备份和热备份。热备份是指对应的链路处于启用状态，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。	下拉框选项 <ul style="list-style-type: none"> • cold • hot

参数名称	含义	如何配置
超时时间	<ul style="list-style-type: none"> • 如果当前链路为主链路，表示主链路稳定时间。 • 如果当前链路为备份链路，表示该链路最短工作时间。 说明 超时时间仅适用于主备切换。	取值范围：1~65535 单位：秒
接口名称	用于链路切换的接口。	有如下可选项： <ul style="list-style-type: none"> • modem 0 • eth1 • eth0
检测 IP 或域名	通过 ping 包方式检测 IP 地址或域名，ping 不通则判定检测失败。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。
检测间隔/重传次数	链路正常检测时间间隔和最大失败次数。最大失败次数到达则切换链路。	取值范围：1~65535 单位：秒/次数

表 5-7

步骤 4 单击“保存”，完成链路备份配置。



说明

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

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 单击“网络设置>DHCP 服务”。

打开“DHCP 服务”页签，如图 5-19 所示。

图 5-19

步骤 2 配置“DHCP 服务器设置”。

DHCP 服务器设置参数如表 5-8 所示。

参数名称	含义	如何配置
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。	下拉框选项 • br0 • custom
起始 IP	地址池选择 custom 时配置，配置 DHCP 地址池的起始 IP 地址。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.8.2
结束 IP	地址池选择 custom 时配置，配置 DHCP 地址池的结束 IP 地址。	接口型 A.B.C.D，输入规范请参见“参数规范表”。 例如：192.168.8.254
网关类型	DHCP 客户端获取的网关 IP 来源，分为 default、br0、eth0、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	接口型 A.B.C.D，输入规范请

参数名称	含义	如何配置
	要指定下位机网关 IP 时使用。	参见“参数规范表”。 例如：192.168.8.1
DNS 类型	DHCP 客户端获取的 DNS 的 IP 地址的来源，有 default、modem、eth0、br0、custom 等方式，通常不建议修改该配置。	下拉框选项 <ul style="list-style-type: none"> • default • modem • mdoem2 • eth0 • 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“参数规范表”。 例如：192.168.8.2
MAC	配置需要指定 DHCP 获取 IP 的 DHCP 客户端的 MAC 地址。	WORD 类型 MAC 格式 例如：00:1A:4D:34:B1:8E

表 5-8

5.3 应用程序配置

H8951 系列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。

5.3.1 ICMP 检测

无线网络存在假链接（拨号可获得 IP，但是链路不通）等异常现象，通常通过 LCP 等方式进行维护，H8951 系列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是否异常，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（推荐配置此功能，避免网络假连接）。ICMP

链路检测在设计之初主要用于检测无线链路，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 单击“应用程序设置>ICMP 检测”。

打开“ICMP 检测”页签，如图 5-20 所示。



图 5-20

步骤 2 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 5-21 所示。



图 5-21

2. 配置 ICMP 检测服务参数。

ICMP 检测服务的参数说明如表 5-9 所示。

参数名称	含义	如何配置
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”

参数名称	含义	如何配置
		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”。
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 • custom: 自定义动作
执行命令	超时动作选择 custom 时配置，命令为后台操作命令，通常不建议使用。如有配置需要请联系我司技术人员。	WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。

表 5-9

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 5-20 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。
- 删除
如图 5-20 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 5-20 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 5-20 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。

5.3.2 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 单击“应用程序设置>DDNS 设置”。

打开“DDNS 设置”页签，如图 5-22 所示。

图 5-22

步骤 2 配置 DDNS 服务参数。

DDNS 服务的参数说明如表 5-10 所示。

参数名称	含义	如何配置
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 <ul style="list-style-type: none"> • 3322 • 88ip • Dnsexit • Dyndns • Zoneedit • changeip • custom
服务地址	服务提供商选择 custom 时配置，当自建 DDNS 服务器时配置，自定义默认为标准 DDNS 协议，如有配置需要可联系我司技术人员定制协议。	一般 WORD 类型，最大 64 字节，输入规范请参见“参数规范表”。

参数名称	含义	如何配置
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

表 5-10

步骤 3 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。

5.3.3 DTU 配置（H8951S 和 H7920 支持）

H8951 系列路由器系统内置与注册中心和数据中心通信功能，可提供类似 DTU 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 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 5-23、图 5-24、图 5-25 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 5-24。

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 5-25。

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	GPS设置	SNMP 设置	M2M设置	任务管理

DTU 服务 启用 禁用

基本设置

工作模式

本地端口 * 1-65535

传输协议 TCP UDP

接收报文超时 * 1-65535 毫秒

最后包空闲时间 * 1-65535 毫秒

串口参数设置

速率

校验位

数据位

停止位

图 5-23

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	GPS设置	SNMP 设置	M2M设置	任务管理
DTU 服务 <input type="button" value="启用"/> <input type="button" value="禁用"/>						
基本设置						
工作模式	客户端 <input type="button" value="v"/>					
本地端口	<input type="text" value=""/> 1-65535					
传输协议	<input checked="" type="radio"/> TCP <input type="radio"/> UDP					
通信类型	<input checked="" type="radio"/> 三中心 <input type="radio"/> 主备					
接收报文超时	<input type="text" value=""/> * 1-65535 毫秒					
最后包空闲时间	<input type="text" value=""/> * 1-65535 毫秒					
数据中心设置						
服务地址	<input type="text" value=""/>	最大长度为64位				
服务端口	<input type="text" value=""/>	1-65535				
服务地址2	<input type="text" value=""/>	最大长度为64位				
服务端口2	<input type="text" value=""/>	1-65535				
服务地址3	<input type="text" value=""/>	最大长度为64位				
服务端口3	<input type="text" value=""/>	1-65535				
重连间隔	<input type="text" value=""/>	1-65535 秒				
重连次数	<input type="text" value=""/>	1-65535				
心跳设置						
心跳内容	<input type="text" value=""/>	最大长度为64位				
心跳间隔	<input type="text" value=""/>	1-65535 秒				
串口参数设置						
速率	115200 <input type="button" value="v"/>					
校验位	none <input type="button" value="v"/>					
数据位	8 <input type="button" value="v"/>					
停止位	1 <input type="button" value="v"/>					
<input type="button" value="保存"/> <input type="button" value="刷新"/>						

图 2-24

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	GPS设置	SNMP设置	M2M设置	任务管理
DTU 服务 <input type="button" value="启用"/> <input type="button" value="禁用"/>						
基本设置						
工作模式	DDP客户端 ▾					
本地端口	<input type="text"/>	1-65535				
身份识别码	<input type="text"/>	* 最大长度为11位				
传输协议	<input checked="" type="radio"/> TCP <input type="radio"/> UDP					
通信类型	<input checked="" type="radio"/> 三中心 <input type="radio"/> 主备					
接收报文超时	<input type="text"/>	* 1-65535 毫秒				
响应包空闲时间	<input type="text"/>	* 1-65535 毫秒				
数据中心设置						
服务器址	<input type="text"/>	最大长度为64位				
服务器端口	<input type="text"/>	1-65535				
服务器址2	<input type="text"/>	最大长度为64位				
服务器端口2	<input type="text"/>	1-65535				
服务器址3	<input type="text"/>	最大长度为64位				
服务器端口3	<input type="text"/>	1-65535				
通信间隔	<input type="text"/>	1-65535 秒				
重试次数	<input type="text"/>	1-65535				
心跳设置						
心跳间隔	<input type="text"/>	1-65535 秒				
串口参数设置						
速率	115200 ▾					
校验位	none ▾					
数据位	8 ▾					
停止位	1 ▾					
<input type="button" value="保存"/> <input type="button" value="刷新"/>						

图 5-25

步骤 2 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 5-23 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 5-24 和图 5-25 所示。参数说明如表 5-11 所示。

参数名称	含义	如何配置
基本设置		
工作模式	DTU 工作模式，可设置为： <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • TCP • UDP 	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 <ul style="list-style-type: none"> • 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。 • 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。 	单选按钮选择。 根据自身需求可以选择。
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	手动输入。 取值范围：1~65535 缺省值：500 单位：毫秒

参数名称	含义	如何配置
	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。	
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”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 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

参数名称	含义	如何配置
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
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

表 5-11

步骤 3 单击“保存”，完成 DTU 服务器/客户端/DDP 客户端配置。

5.3.4 SNMP 配置

SNMP（Sample 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 单击“应用程序设置>SNMP 配置”。

打开“SNMP 配置”页签，如图 5-26 所示。

图 5-26

步骤 2 配置 SNMP 参数。

SNMP 的参数说明如表 5-12 所示。

参数名称	含义	如何配置
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 <ul style="list-style-type: none"> • 启用 • 禁用

表 5-12

步骤 3 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。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。

5.3.5 M2M 配置

H8951 系列路由器通过 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 单击“应用程序设置>M2M 配置”。

打开“M2M 配置”页签，如图 5-27 所示。

图 5-27

步骤 2 配置 M2M 参数。

M2M 参数说明如表 5-13 所示。

参数名称	含义	如何配置
服务 IP 或域名	M2M 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	M2M 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
登录次数	路由器登录 M2M 平台最大重试次数，	取值范围：1~5

参数名称	含义	如何配置
	若到达最大次数则重启 M2M 功能重新初始化并再次登录。	单位：次
心跳间隔	路由器与 M2M 平台用来维持连接的心跳包的发送间隔时间，除此之外，心跳包还包含了路由器的网络状态数据，实现 M2M 平台实时网络状态数据的更新。	取值范围：1~65535 单位：秒
重发次数	路由器与 M2M 平台的所有数据包交互均有重传机制，重传次数到达之后则判断本次交互失败，一般数据交互失败后无具体操作。	取值范围：1~5 单位：次
超时时间	路由器与 M2M 平台所有数据包交互的重传判断时间，超过超时时间无应答则判断数据交互超时并进行数据重传。	取值范围：1~65535 单位：秒

表 5-13

步骤 3 单击“保存”，完成 M2M 配置。

5.3.6 任务管理设置

H8951 系列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（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 单击“应用程序设置>任务管理”。

打开“任务管理”页签，图 5-28 所示。



图 5-28

步骤 2 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 5-29 所示。



图 5-29

步骤 3 配置任务管理规则参数。

任务管理参数说明如表 5-14 所示。

参数名称	含义	如何配置
基本设置		
任务名称	任务管理规则名称标识，仅用于区分不同的规则。	最大长度为 12 位，输入规范请参见“参数规范表”。
任务类型	任务主要有动作类任务和状态类任务，动作类任务配置为时间点或者时间间隔，状态类任务则配置为时间段，状态类任务只有在线，它表示所配置时间区域 modem 处于上线状态（掉线自动重拨号），其他时间区域时保持下线（不拨号）。	下拉框选项 <ul style="list-style-type: none"> • modem-online • reboot • custom 选择“custom”，需要用户输入命令（如：reboot 等命令）。 最大长度为 64 位字符串，输入规范请参见“参数规范表”。
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	下拉框选项 <ul style="list-style-type: none"> • range • interval

参数名称	含义	如何配置
	务。	
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。	取值范围：[01,31] 格式：XX-XX
星期	任务执行的星期设置，代表一个星期中某天。	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

表 5-14

步骤 4 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”。“系统时间”设置，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。

5.4 安全配置

5.4.1 概述

安全设置是指路由器的防火墙功能。H8951 系列路由器支持 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。

5.4.2 IP 过滤

IP 过滤是指路由器通过 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 单击“安全设置>IP 过滤”。

打开“IP 过滤”页签，如图 5-30 所示。



图 5-30

输入/转发过滤规则中

- 黑名单：默认允许数据包转发，符合名单中“丢弃”规则的数据包不能经过路由器转发。
- 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 2 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 5-31 和图 5-32 所示。



图 5-31

图 5-32

IP 过滤的参数说明如表 5-15 所示。

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”。 <ul style="list-style-type: none"> • 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”。 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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

参数名称	含义	如何配置
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 • eth0 • eth1
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		
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。

表 5-15

步骤 3 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。

5.4.3 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 单击“安全设置>域名过滤”。

打开“域名过滤”页签，如图 5-33 所示。



图 5-33

- 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 2 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 5-34 所示。



图 5-34

域名过滤的参数说明如表 5-16 所示。

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。 <ul style="list-style-type: none"> • 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

表 5-16

步骤 3 单击“保存”，完成该条域名过滤规则配置。

5.4.4 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。H8922S 4G Router 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 单击“安全设置>MAC 过滤”。

打开“MAC 过滤”页签，如图 5-35 所示。



图 5-35

MAC 过滤的参数说明如表 5-17 所示。

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。 <ul style="list-style-type: none"> • 黑名单 • 白名单 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。 <ul style="list-style-type: none"> • 黑名单 • 白名单 同一时间，黑名单、白名单只有一个名单生效。

表 5-17

步骤 2 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 5-36 所示。

图 5-36

MAC 过滤的参数说明如表 5-18 所示。

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”。 <ul style="list-style-type: none"> 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”。 <ul style="list-style-type: none"> 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”。

表 5-18

步骤 3 单击“保存”，完成该条 MAC 过滤规则配置。

5.5 转发配置

5.5.1 概述

H8951 系列路由器转发功能包括 NAT、静态路由、动态路由（RIP、OSPF）（可选）和 QoS。

5.5.2 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 单击“转发设置>NAT”。

打开“NAT”页签，如图 5-37 所示。

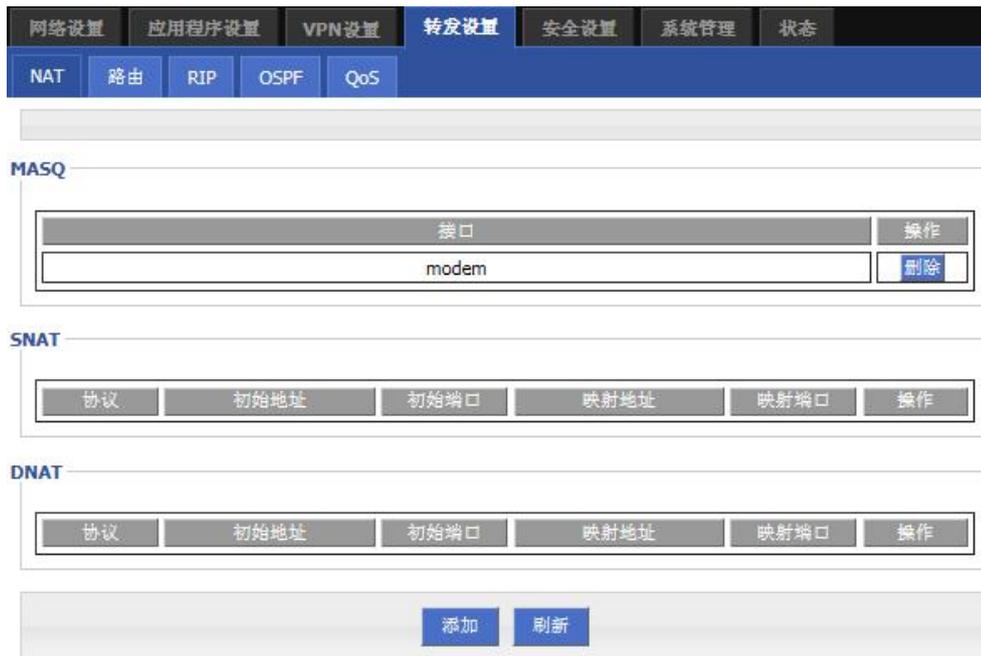


图 5-37

步骤 2 单击“添加”按钮，选择转换类型为“DNAT”新建一条 DNAT 规则，如图 5-38 所示。

图 5-38

步骤 3 配置 DNAT 规则参数。

DNAT 的参数说明如表 5-19 所示。

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： <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • br0 • modem • eth0 • eth1
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”
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”

参数名称	含义	如何配置
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。

表 5-19

步骤 4 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。

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 5 单击“转发设置>NAT”。

打开“NAT”页签，如图 5-37 所示。

步骤 6 选择“转换类型”为“SNAT”后，配置界面如图 5-39 所示。

The screenshot shows the NAT configuration page with the following settings:

- Network Settings: NAT, Routing, RIP, OSPF, QoS
- Security Settings: Security, System Management, Status
- Basic Settings:
 - Conversion Type: DNAT SNAT MASQ
 - Protocol: all
 - Initial Address: * 192.168.8.1 或 192.168.8.0/24
 - Initial Port: 1-65535或[1-65535]
 - Mapping Address Type: interface
 - Interface: br0
 - Mapping Port: 1-65535或[1-65535]
- Buttons: 保存 (Save), 返回 (Return)

图 5-39

步骤 7 配置 SNAT 规则参数。

SNAT 的参数说明如表 5-20 所示。

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： <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • br0 • modem • eth0 • eth1
映射地址	源地址替换后的新源地址	A.B.C.D 接口型，输入规范请参见“参数规范表”
映射端口	替换之后的源地址端口	取值范围：1~65535 或[1~65535]；可以是范围，也可以是单个端口。

表 5-20

步骤 8 单击“保存”，完成该条路由模式规则配置。



说明

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

MASQ 规则配置

MASQ 也就是 MASQUERADE，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。H8951 系列路由器支持将数据包的源 IP 地址转换成路由器的某个接口地址。

步骤 1 单击“转发设置>NAT”。

打开“NAT”页签，选择“转换类型”为“MASQ”，如图 5-40 所示。



图 5-40

步骤 2 配置 MASQ 规则参数。

MASQ 的参数说明如表 5-21 所示。

参数名称	含义	如何配置
接口	选择某个接口笛之爱作为路由器及局域网与外部的通信地址	下拉列表选择： <ul style="list-style-type: none"> • br0 • modem • eth0 • eth1

表 5-21

步骤 3 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。

5.5.3 路由配置

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。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），且策略路由由优先级，以 3~252 数字来区分，数字越小，优先级越高。而静态路由和策略路由之间也有优先级：策略路由的优先级高于静态路由。

步骤 1 单击“转发设置>路由”。

打开“路由”页签，如图 5-41 所示。



图 5-41

单击“添加”按钮，新建一条路由规则。配置界面如图 5-42 和图 5-43 所示。



图 5-42



图 5-43

路由的参数说明如表 5-22 所示。

参数名称	含义	如何配置
基本设置		
路由类型	选择是“静态路由”还是“策略路由”。	下拉框选项
当“路由类型”选择“静态路由”时		
网络地址	设置静态路由的目标地址和子网掩码位数。	填入目的地址和子网掩码位数即可。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。
网关类型	指定静态路由所作用的网关类型。包含： • 接口 • 静态 IP	下拉列表选择。 可以从下拉列表选择需要的接口标识，分别是静态 IP 和接口。
网关	设置静态路由的下一跳 IP 地址，即相邻路由器的端口地址。	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。	下拉框选项。 • 静态 IP • 接口
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。	下拉框选项。 • 静态 IP • 接口
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	取值范围：[3,252]

参数名称	含义	如何配置
	数字越小，则优先级越高。	

表 5-22

步骤 2 单击“保存”，完成该条静态路由配置。



说明

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/目的地地址为 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。

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。

5.5.4 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，我司 H8951 系列路由器支持定制 QoS 业务。

步骤 1 单击“转发设置> QoS”。

步骤 2 打开“QoS”页签，如图 5-44 所示。



图 5-44

步骤 3 单击“添加”，新建一条 QoS 规则。配置界面如图 5-45 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 RIP OSPF QoS

状态

基本设置

规则名称 * 最大长度为12位

流控接口

网络地址 * 如: 192.168.8.1/24

端口 1-65535

速率 * 1-65535 Kbps

冗余带宽 1-65535 Kbps

优先级 1-30

图 5-45

步骤 4 配置 QoS 参数。

QoS 的参数说明如表 5-23 所示。

参数名称	含义	如何配置
规则名称	QoS 的规则名称。	最大允许输入 12 个字符。 只能在添加新规则的时候设定，后续不能修改。 规则名称不能重复，否则后添加的规则将覆盖前面添加的规则。
流控接口	进行流量控制的接口类型，包含： <ul style="list-style-type: none"> • br0：流控的接口为 LAN 口 • modem：流控的接口为 modem 	下拉框选项
网络地址	进出流控接口的网络地址，限速的对象。	填入目的地址和子网掩码位数即可。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。
端口	需要进行流控的网络端口。	取值范围：1~65535 该端口可以不配置，若不配置则代表所有端口。
速率	对网络地址设置的传输速率。	取值范围：1~65535 单位：Kbps

参数名称	含义	如何配置
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
优先级	设置该规则的优先级。	取值范围：[1,30]

表 5-23

步骤 5 单击“保存”完成参数配置。



说明

QoS 主要用于路由器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。如路由器下接有两个子网：192.168.8.1/24 和 192.168.9.1/24，则路由器可以通过 QoS 来控制这两个子网的速率；若路由器的带宽比较宽裕，则路由器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。

5.5.5 动态路由配置(可选)

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，H8951 系列路由器支持 RIP v2 协议。对于更复杂的环境，一般不使用 RIP 协议。RIP 业务可在路由器出厂时根据用户是否需要配置。

步骤 1 单击“转发设置>RIP”。

步骤 2 打开“RIP”页签，如图 5-46 所示。



图 5-46

RIP 的参数说明如表 5-24 所示。

参数名称	含义	如何配置
RIP 服务	是否启用相关功能	单选按钮选择。
发布连接路由		• 启用
发布静态路由		• 禁用
发布内核路由		

表 5-24

步骤 3 单击“添加”按钮，新建一条 RIP 规则。配置界面如图 5-47 所示。



图 5-47

步骤 4 配置 RIP 规则参数。

RIP 规则的参数说明如表 5-25 所示。

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。 <ul style="list-style-type: none"> 当选择为“网络”时，需要配置目的网络地址（一般为路由器直连的网络）。 当选择为“邻居”时，需要配置邻居的 IP 地址（与路由器相连的路由器的 IP 地址）。
网络（与路由器直接相连的网络才能添加）	添加 RIP 路由的目的网络。	填入需要添加 RIP 路由的目的网络地址。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。
邻居（与路由器直接相连的路由器）	添加 RIP 路由的邻居的 IP 地址。	填入需要添加 RIP 路由的邻居的 IP 地址即可。 格式：A.B.C.D/M，输入规范请参见“参数规范表”。

表 5-25

步骤 5 单击“保存”，完成该条 RIP 规则配置。



说明

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

仅和相邻的路由器交换信息。如果两个路由器之间的通信不经过另外一个路由器，那么这两个路由器是相邻的。RIP 协议规定，不相邻的路由器之间不交换信息。

路由器交换的信息是当前本路由器所知道的全部信息。即自己的路由表。

按固定时间交换路由信息（如每隔 30 秒），然后路由器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)，因为每经过一个路由器，跳数就加 1。RIP 认为好的路由就是它通过的路由器的数目少，即“距离短”。RIP 允许一条路径最多只能包含 15 个路由器。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。

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 业务可在路由器出厂时根据用户是否需要配置

步骤 1 单击“转发设置>OSPF”。

步骤 2 打开“OSPF”页签，如图 5-48 所示。



图 5-48

OSPF 的参数说明如表 5-26 所示。

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

表 5-26

步骤 3 单击“添加”，新建一条 OSPF 规则。配置界面如图 5-49 所示。

步骤 4 配置路由模式规则参数。

OSPF 的参数说明如表 5-27 所示。

参数名称	含义	如何配置
当“通告类型”选择“网络”时		
网络	设置某个网段作为路由器 OSPF 发送地址。	格式：A.B.C.D/M 接口型，输入规范请参见“参数规范表”。
域地址	用于标识网络（只有域地址相同的路由器之间才会使用 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	路由器可以一跳到达的设备地址。	手动输入，格式：A.B.C.D/M 接口型，输入规范请参见“参数规范表”。
当“通告类型”选择“接口”时		
接口名称	路由器的某个接口	下拉列表选择： <ul style="list-style-type: none"> • br0 • modem • eth1 • eth0
接口属性	配置路由器接口的属性，包括开销和网络两种属性	单击按钮选择 <ul style="list-style-type: none"> • 开销 • 网络
开销	配置路由器接口的开销，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）	配置路由器接口的网络类型。	下拉列表选择： <ul style="list-style-type: none"> • broadcast • non-broadc • point-to-multipoint • point-to-point

表 5-27

步骤 5 单击“保存”，完成该条 OSPF 规则配置。



说明

OSPF 路由协议是一种典型的链路状态（Link-state）的路由协议，一般用于同一个路由域内。在这里，路由域是指一个自治系统，它是指一组通过统一的路由政策或路由协议互相交换路由信息的网络。在这个 AS 中，所有的 OSPF 路由器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 路由器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路由器，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路由器。

5.6 VPN 功能配置

5.6.1 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 H8951 系列路由器不仅支持 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。

5.6.2 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。

步骤 1 单击“VPN 设置>VPDN 配置”。

步骤 2 打开“VPDN 配置”页签，如图 5-50 所示。

接口名称	协议	服务地址	用户名	操作

图 5-50

步骤 3 单击“添加”，添加一条新 VPDN 规则。如图 5-51 所示。

图 5-51

步骤 4 配置 VPDN 规则参数，参数说明如表 5-28 所示。

参数名称	含义	如何配置
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、特定事件等。保存后不允许修改。
协议	VPDN 采用的协议，包括： <ul style="list-style-type: none"> • 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。
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。
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。
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。

表 5-28

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 5-52 所示。



图 5-52

5.6.3 Tunnel 配置

隧道技术是一种通过互连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上传递时所经过的逻辑路径称为隧道。

Tunnel 配置支持 GRE 和 IPsec 两种模式。

步骤 1 单击“VPN 设置>Tunnel 配置”，打开“Tunnel 配置”页签。

步骤 2 单击“添加”，添加一条新 Tunnel 规则，如图 5-53 所示。



图 5-53

配置 Tunnel 规则参数，参数说明如表 5-29 所示。

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： <ul style="list-style-type: none"> • 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”。

表 5-29

步骤 3 单击“保存”，完成该条 Tunnel 规则配置。

5.6.4 IPSec 设置

IPSec（IP_SECURITY）是一种建立在 Internet 协议(IP)层之上的协议，能够让两个或更多主机以安全的方式来通讯，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。H8951 系列路由器中的 IPSec 采用公用的 phase1，

可以与大部分 IPSec 服务器进行连接协商，同时 H8922S 4G Router 也支持通过其他接口拉起 IPSec（如通过 modem 拉起），省去用户手动操作。IPSec 有两种模式：隧道模式和传输模式。

步骤 1 单击“VPN 设置>IPSec 配置”，打开“IPSec 配置”页签，如图 5-54 所示。



图 5-54

步骤 2 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，如图 5-55 所示。

图 5-55

IPSec 规则第一阶段参数说明如表 5-30 所示。

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。 这里添加的是第一阶段的规则，所以选择“Phase 1”。
策略名称	该阶段的名称，主要用于第三阶段的匹配。	填入该阶段的名称。保存后不能修改。
协商模式	IPSec 第一阶段的协商模式，包括“main”（主模式）和“aggr”（野蛮模式）。	下拉列表选择。 从下拉列表中选择要设置的启动模式，一般两端有经过 NAT 且使用 USERID 的方式建议“野蛮模式”。
加密方式	支持 des、3des 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式。

参数名称	含义	如何配置
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。
认证方式	支持预共享密钥方式认证。	下拉列表选择。 <ul style="list-style-type: none"> • psk • rsaRF
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。
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

参数名称	含义	如何配置
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

表 5-30

单击“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，如图 5-56 所示。

图 5-56

IPSec 规则第二阶段参数说明如表 5-31 所示。

参数名称	含义	如何配置
基本设置		

参数名称	含义	如何配置
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、ah、ah+esp 三种认证加密协议。	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”。

参数名称	含义	如何配置
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”。

表 5-31

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

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

3. IPsec 阶段参数配置，如图 5-57 所示。

图 5-57



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

IPsec 规则匹配阶段参数说明如表 5-32 所示。

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

表 5-32

配置 IPSec 规则匹配阶段参数，配置完后单击“保存”。

5.6.5 Open VPN 设置

Open VPN 是一个基于 OpenSSL 库的应用层 VPN 实现。和传统 VPN 相比，它的优点是简单易用。Open VPN 所有的通信都是基于一个单一的 IP 端口，默认且推荐使用 UDP 协议通信，同时也支持 TCP。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 AsRfined Numbers Authority）指定给 Open VPN 的官方端口为 1194。

步骤 1 单击“VPN 设置>OpenVPN 配置”。

打开“OpenVPN 配置”页签，如图 5-58 所示。



图 5-58

步骤 2 配置 Open VPN 参数

参数如图表 5-33 所示。

参数名称	含义	如何配置
工作模式	支持 client 和 multi 两种工作模式 <ul style="list-style-type: none"> Client 模式为客户端类型模式 Multi 模式为一对一工作模式(对端为非服务端) 	下拉列表选择。 从下拉列表选择需要的工作模式。
Dev	Dev 表示网络接口类型。支持 tun 和 tap 两种类型 <ul style="list-style-type: none"> 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。

参数名称	含义	如何配置
协议	数据传输协议类型设置。 <ul style="list-style-type: none"> • TCP • UDP 	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 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 启用 • 禁用
证书	配置 VPN 数据传输的方式 <ul style="list-style-type: none"> • 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 	下拉列表选择。 从下拉列表选择需要的数据传输方式
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”。

参数名称	含义	如何配置
Cipher	SSL 的加密算法系统	下拉框选项 <ul style="list-style-type: none"> • NONE • BF-CBC • DES-CBC • DES-EDE-CBC • DES-EDE3-CBC • DESX-CBC • RC2-40-CBC • CAST5-CBC • RC2-64-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • SEED-CBC

表 5-33

步骤 3 点击“保存”，完成 Open VPN 配置。

5.7 系统管理配置

5.7.1 概述

H8951 系列路由器的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、系统时间的设置、用户账户信息的管理、网络测试以及系统文件升级等。

5.7.2 本地日志

本地日志是指通过在 H8951 系列路由器的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 单击“系统管理>本地日志”。

打开“本地日志”页签，如图 5-59 所示。



图 5-59

步骤 2 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。

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。

5.7.3 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 1 单击“系统管理>远程日志”。

打开“远程日志”页签，如图 5-60 所示。



图 5-60

步骤 2 配置系统日志参数。

参数说明如表 5-34 所示。

参数名称	含义	如何配置
远程日志服务器地址	远端日志服务器的 IP 地址（既可以是 LAN 侧 PC 的 IP 地址，又可以是公网地址）。	填入接收日志信息的 PC 机的 IP 地址即可。
远程日志服务器端口号	远端日志服务器的端口号。	填入远端日志服务器的端口号，默认为 514。

表 5-34

步骤 3 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。

5.7.4 系统时间

H8951 系列路由器支持 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 1 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 5-61 和图 5-62 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
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 <input type="checkbox"/> 启用 <input type="checkbox"/> 禁用						
时间同步类型 <input type="text" value="网络时间"/>						
主服务器地址 <input type="text" value="ntp.sjtu.edu.cn"/> * 最大长度为64位						
备用服务器地址 <input type="text"/> 最大长度为64位						
同步间隔 <input type="text"/> * 1-65535 秒						
时区 <input type="text" value="abu-dhabi/muscat"/>						
<input type="button" value="保存"/> <input type="button" value="刷新"/>						

图 5-61

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
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 <input type="checkbox"/> 启用 <input type="checkbox"/> 禁用						
时间同步类型 <input type="text" value="手动"/>						
日期 <input type="text" value="1970-01-01"/> 如: 1970-01-01						
时钟 <input type="text" value="07:01:01"/> 如: 07:01:01						
<input type="button" value="保存"/> <input type="button" value="刷新"/>						

图 5-62

步骤 2 配置系统时间参数。

参数说明如表 5-35 所示。

参数名称	含义	如何配置
状态	“启用”或“禁用”系统时间同步。	<ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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 如 1970-01-01
时钟	校验的标准时间。	格式为 HH:MM:mm 如 07:01:01

表 5-35

步骤 3 单击“保存”，完成系统日志参数配置。

5.7.5 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 1 单击“系统管理>用户管理”。

打开“用户管理”页签，如图 5-63 所示。

图 5-63

步骤 2 配置用户管理参数。

参数说明如表 5-36 所示。

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。 <ul style="list-style-type: none"> • 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，还能导出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

表 5-36



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 3 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。

5.7.6 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 单击“系统管理>网络测试”。

打开“网络测试”页签，如图 5-64 所示。



图 5-64

步骤 2 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 5-37 所示。

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。

表 5-37

5.7.7 文件升级

升级设置

H8951 系列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 单击“系统管理>文件升级”。

显示“文件升级”界面，如图 5-65 所示。



图 5-65

步骤 2 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。

CFE 模式升级

当对路由器进行程序升级时（一般来说，对程序升级即对程序进行全面的替换升级），如果文件大小超过 6MB 或通过 WEB 配置页面升级失败，则可选择采用 CFE 模式进行升级。其具体升级操作方式如下。

步骤 1 在升级 PC 机器上增加一个 192.168.1.X 网段的 IP 地址，如图 5-66 所示。

具体添加方法请参见“4.1 本地连接配置”。

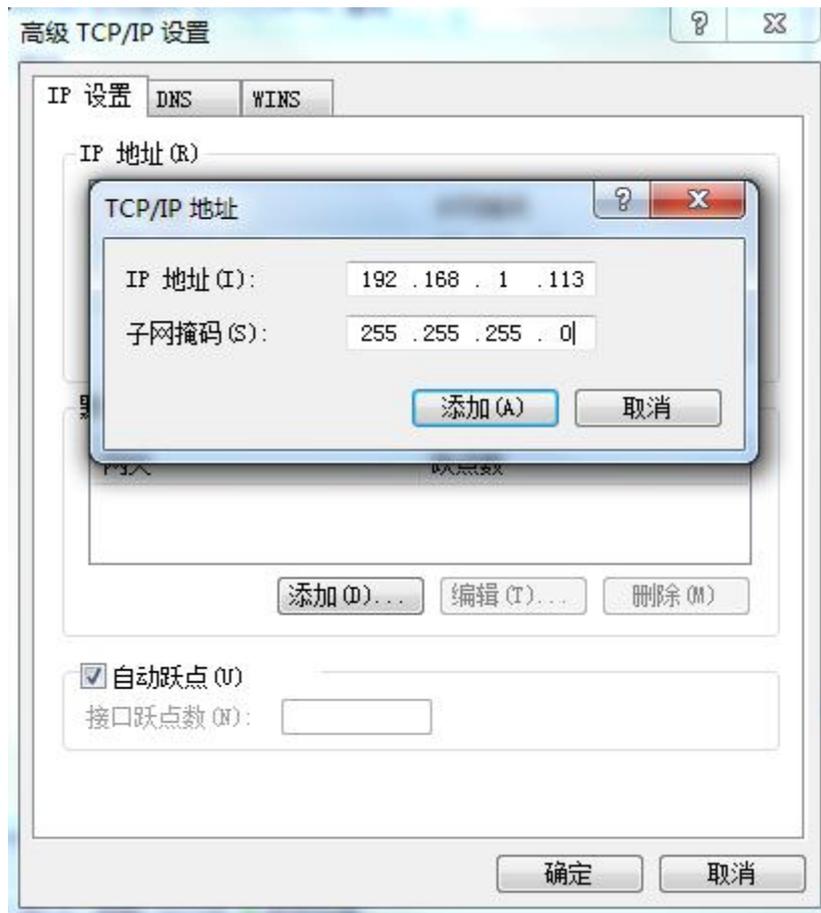


图 5-66

步骤 2 轻压设备后面板的“RESET”键，同时为设备上电（上电后维持轻压“RESET”键 2~5 秒以上秒后松开“RESET”键）。

步骤 3 在 PC 机端浏览器中输入 <http://192.168.1.1> 升级页面，如图 5-67 所示。

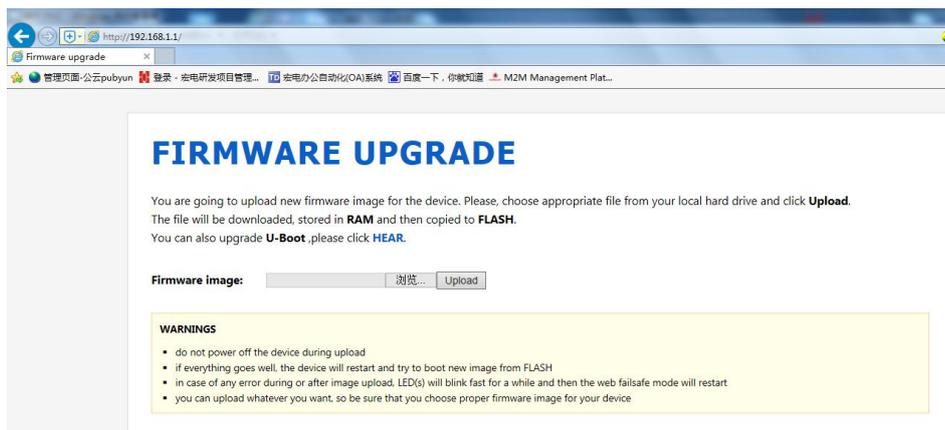


图 5-67

步骤 4 单击“浏览”，在本地 PC 上浏览并选择升级文件，然后单击“Upload”开始升级，界面如图 5-68 所示。



图 5-68

升级过程大约会持续 3~6 分钟，请耐心等待，同时观察设备的 SYS 指示灯。如果 SYS 指示灯亮，则表示程序升级成功。

🔑 窍门

也可以同时在 PC 上 ping 路由器的 br0 地址（例如：`ping 192.168.8.1 -t`），如果可 ping 通，则说明升级成功。

备份设置

H8951 系列路由器支持配置文件的备份和恢复，如图 5-69 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 5-69

📖 说明

导入备份文件后，系统自动重启，在重启系统之后才能生效。

密钥：当导出一份文件时添加密钥，那在导入该份文件时需要输入该密钥，否则会导致路由器乱码；该密钥可以不填写。若在导入时，密钥输入错误，则会导致无法进入路由器页面。

密钥的最大长度为 8 位。

出厂设置

H8951 系列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 5-70

- 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

H8951 系列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 5-71

- 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 5-72

5.8 状态

5.8.1 概述

H8951 系列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。

5.8.2 基本信息

通过对查看路由器的基本信息，可以了解路由器系统的基本信息。具体操作方法如下。

步骤 1 单击“状态>基本信息”，打开“基本信息”页签，如图 5-73 所示，参数说明如表 5-38 所示。



图 5-73

基本信息的参数配置如表 5-38 所示。

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
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

表 5-38



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。

5.8.3 LAN 状态

通过对查看 H8951 系列路由器的“LAN 状态”信息，可以了解路由器系统“LAN 状态”的基本信息。具体操作方法如下。

步骤 1 单击“状态>LAN 状态”，打开“LAN 状态”页签，如图 5-74 所示。参数说明如表 5-39 所示。



图 5-74

LAN 状态的参数说明如表 5-39 所示。

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

表 5-39



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。

5.8.4 WAN 状态（可选）

通过对查看 H8951 系列路由器的“WAN 状态”信息，可以了解路由器的系统“WAN 状态”的基本信息。具体操作方法如下。

步骤 1 单击“状态> WAN 状态”。

打开“WAN 状态”页签，因为 WAN 口有静态 IP/DHCP/PPPOE 三种形式，故当 WAN 口处于这三种形式中的任一种时，WAN 状态就显示该形式的 WAN 信息各种形式的 WAN 口状态如图 5-75、图 5-76、图 5-77 所示，参数说明如表 5-40 所示。



图 5-75



图 5-76



图 5-77

WAN 状态参数说明如表 5-40 所示。

参数名称	含义	如何配置
WAN 状态	显示当前 WAN 接口功能的状态是启用还是禁止状态。	不可配
WAN 口类型	显示当前 WAN 接口的类型。	不可配
本地 IP	显示 WAN 口配置的本地 IP 地址。	不可配
掩码	显示配置的 WAN 接口所在的网络地址号。	不可配
物理地址	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
WAN 口采用 PPPoE 方式时状态显示		
状态	显示 WAN 口 PPPoE 的连接状况	不可配
本地 IP	显示 PPPoE 服务器给路由器分配的 IP 地址	不可配
远端 IP	显示 PPPoE 服务器的 IP 地址	不可配

5.8.5 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 1 单击“状态>移动网络状态”，打开“移动网络状态”页签，如图 5-78 所示，参数说明如表 5-41 所示。



图 5-78

移动网络状态页面参数说明如表 5-41 所示。

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	路由器与无线网络的连接状态。包含 connected 和 disconncted 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	路由器拨号时获取的外网 IP 地址。	不可配
域名服务器	路由器拨号时获取的首选 DNS 地址。	不可配
SIM 卡状态	路由器当前使用的卡槽对应的 SIM 的工作状态。	不可配
SIM 卡 ICCID	SIM 卡卡号，相当于手机号码的身份证	不可配

参数名称	含义	如何配置
SIM 卡 IMSI	国际移动用户识别码，区别移动用户的标志	不可配
基站 LAC	基站位置区码	不可配
小区 ID	小区识别码	不可配
RSRP	路由器 SIM 卡的参考信号接收功率	不可配
SINR	SIM 卡接收到的有用信号的强度与接收到的干扰信号（噪声和干扰）的强度的比值	不可配

表 5-41

5.8.6 WLAN 状态

通过对查看 H8951 系列路由器的“WLAN 状态”信息，可以了解路由器 WLAN 的基本信息。具体操作方法如下。

步骤 1 单击“状态> WLAN 状态” H8951 系列路由器的 WLAN 有 ap、station 两种模式，各模式下的基本信息如图 5-79、图 5-80、图 5-81 所示，参数说明如表 5-42、表 5-43、表 5-44 所示。



图 5-79



图 5-80



图 5-81

AP 模式状态参数说明如表 5-42 所示。

参数名称	含义	如何配置
基本信息		
工作模式	WLAN 的工作模式。	不可配
SSID	ap 的表示。	不可配
AP 隔离	WLAN 客户端设备的隔离状态。	不可配
工作通道	ap 的工作信道。	不可配
网络模式	当前 ap 所使用的网络模式。	不可配
物理地址	设备的物理地址。	不可配
客户端信息		
IP 地址	WLAN 客户端的 IP 地址。	不可配
物理地址	WLAN 客户端的物理地址。	不可配
WDS 连接信息		
WDS 对端 MAC	与 ap 进行桥接的设备的物理地址	不可配

表 5-42

Station 模式状态参数说明如表 5-43 所示。

参数名称	含义	如何配置
基本信息		
状态	WLAN 做 station 时的连接其他 AP 的状态	不可配
工作模式	station 模式	不可配
SSID	路由器连接的 AP 标识	不可配
工作通道	路由器连接的 AP 的工作通道	不可配
网络模式	路由器连接的 AP 的网络模式	不可配
IP 地址	路由器连接的 AP 给路由器分配的 IP 地址	不可配
子网掩码	路由器连接的 AP 给路由器分配的子网掩码	不可配
默认网关	路由器连接的 AP 给路由器分配的默认网关	不可配
首选 DNS 服务器	路由器连接的 AP 给路由器分配的首选 DNS 地址	不可配
备用 DNS 服务	路由器连接的 AP 给路由器分配的备份 DNS 地址	不可配

参数名称	含义	如何配置
器		
物理地址	路由器连接的 AP 的物理地址	不可配

表 5-43

5.8.7 路由表

通过查询路由表的状态，可以了解到 H8922S 4G Router 的路由信息。

步骤 1 单击“状态>路由表”，打开“路由表”页签，如图 5-82 所示。参数说明如表 5-45 所示。

图 5-82

路由表参数说明如表 5-45 所示。

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

表 5-45

5.9 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功能：

- 轻压“RESET”键 0~5 秒左右放手，则重启系统。
- 轻压“RESET”键 5 秒以上后放手，则重启系统，同时系统配置将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，保持按“RESET”键 2 秒以上，路由器就会进入 CFE 模式，可以进行程序升级，参照“CFE 模式升级”。

6 典型应用

6.1 概述

H8951 系列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 ICMP 检测功能应用

场景介绍

H8951 系列路由器提供 ICMP 检测功能，从技术上来说，ICMP 是一个“错误侦测与回报机制”，可用来检测网络链路是否处于假连接状态，主机是否可达，路由是否可用等。比如：正在工作的 modem 拨号链路因为某些原因出现 IP 可获得，但实际链路连接不通的假连接异常现象，这时可通过 ICMP 检测来检测网路链路，当检测到异常时可执行用户设置的动作，从而实现链路和系统的快速恢复，保证网路链路的准确性和可靠性。

参数配置

该场景下，需要进行“ICMP 检测”配置，配置步骤请参见“5.3.1 ICMP 检测”，配置如图 6-1 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

基本设置

规则名称	<input type="text" value="icmp1"/>	* 最大长度为12位
目的地址	<input type="text" value="114.114.114.114"/>	* 最大长度为64位
备份地址	<input type="text" value="www.baidu.com"/>	最大长度为64位
检测间隔	<input type="text" value="60"/>	* 1-65535 秒
重传次数	<input type="text" value="6"/>	* 1-65535
源接口	<input type="text" value="modem"/>	
超时动作	<input type="text" value="modem-reset"/>	

图 6-1

应用结果

当路由器拨号成功，且能通过路由器连接网络，ICMP 检测目的地址或备份地址成功如图 6-2 所示。当路由器拨号成功，但出现假连接状态不能连接网络时，ICMP 检测失败，且达到检测次数后执行配置的动作如 modem-reset，如图 6-3 所示。

```
Jun 24 13:25:50 router daemon.info icmpcheck[2881]: [icmp1]-----begin-----{icmpcheck.c->813}
Jun 24 13:25:50 router daemon.info icmpcheck[2881]: [icmp1]          >>>> link check destination[114.114.114.114]>>>>{icmpcheck.c->848}
Jun 24 13:25:50 router daemon.alert icmpcheck[2881]: output dstip[114.114.114.114] output if[fail]
Jun 24 13:25:50 router daemon.info icmpcheck[2881]: **** ICMP send icmp packet successful ****{icmp.c->218}
Jun 24 13:25:50 router daemon.info icmpcheck[2881]: [icmp1]          <<<< link recieve icmp successfully[idle 60s] <<<<{icmpcheck.c->1015}
Jun 24 13:25:50 router daemon.info icmpcheck[2881]: [icmp1]-----end-----{icmpcheck.c->1023}
```

图 6-2

```
Jun 24 13:37:00 router daemon.info icmpcheck[21870]: [icmp1]-----begin-----{icmpcheck.c->813}
Jun 24 13:37:00 router daemon.info icmpcheck[21870]: [icmp1]          >>>> link check destination[114.114.114.114]>>>>{icmpcheck.c->848}
Jun 24 13:37:00 router daemon.alert icmpcheck[21870]: output dstip[114.114.114.114] output if[fail]
Jun 24 13:37:00 router daemon.err icmpcheck[21870]: sendto icmp packet error:Network is unreachable^M {icmp.c->211}
Jun 24 13:37:00 router daemon.info icmpcheck[21870]: [icmp1]          >>>> link check destination[www.baidu.com]>>>>{icmpcheck.c->848}
Jun 24 13:37:00 router daemon.info icmpcheck[21870]: [icmp1]          ==== destination unreachable[1][6][idle 60s]{icmpcheck.c->995}
Jun 24 13:37:00 router daemon.info icmpcheck[21870]: [icmp1]-----end-----{icmpcheck.c->1023}
.....
Jun 24 13:42:00 router daemon.info icmpcheck[21870]: [icmp1]-----begin-----{icmpcheck.c->813}
Jun 24 13:42:00 router daemon.info icmpcheck[21870]: [icmp1]          >>>> link check destination[114.114.114.114]>>>>{icmpcheck.c->848}
Jun 24 13:42:00 router daemon.alert icmpcheck[21870]: output dstip[114.114.114.114] output if[fail]
Jun 24 13:42:00 router daemon.err icmpcheck[21870]: sendto icmp packet error:Network is unreachable^M {icmp.c->211}
Jun 24 13:42:00 router daemon.info icmpcheck[21870]: [icmp1]          >>>> link check destination[www.baidu.com]>>>>{icmpcheck.c->848}
Jun 24 13:42:00 router daemon.info icmpcheck[21870]: [icmp1]          ==== destination unreachable[8][6][idle 60s]{icmpcheck.c->995}
Jun 24 13:42:00 router daemon.info icmpcheck[21870]: [icmp1]          ==== excuting command[modem-reset][idle 360s]{icmpcheck.c->852}
Jun 24 13:42:00 router daemon.info icmpcheck[21870]: [icmp1]-----end-----{icmpcheck.c->1023}
```

图 6-3

6.3 链路备份功能应用

场景介绍

H8951 系列路由器支持无线与无线、无线与有线之间的链路切换，当路由器的工作链路不通后，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，商场 POS 刷卡需要稳定的网络做保证，若 POS 平常使用的有线网络出现故障，则路由器可以快速的切换至无线网络，保证 POS 机刷卡业务的正常进行。

参数配置

该场景下，需要进行“链路备份”的配置。配置请参见“5.2.2 网络设置”下的“链路备份”。

配置情况如图 6-4、图 6-5 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	WAN	WLAN	移动网络	参数切换	网络连接	链路备份	DHCP服务
状态		<input type="button" value="启用"/> <input type="button" value="禁用"/>					
规则名称	<input type="text" value="0"/> * 0-9						
链路运行方式	main <input type="button" value="v"/>						
备份模式	hot <input type="button" value="v"/>						
超时时间	<input type="text"/> 1-65535 秒						
接口名称	eth0 <input type="button" value="v"/>						
检测IP或域名	<input type="text" value="202.170.138.60"/> 最大长度为64位						
检测间隔	<input type="text" value="10"/> 1-65535 秒						
重试次数	<input type="text" value="5"/> 1-65535						
		<input type="button" value="保存"/> <input type="button" value="返回"/>					

图 6-4

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	WAN	WLAN	移动网络	参数切换	网络连接	链路备份	DHCP服务
状态		<input type="button" value="启用"/> <input type="button" value="禁用"/>					
规则名称	<input type="text" value="1"/> * 0-9						
链路运行方式	backup <input type="button" value="v"/>						
备份模式	hot <input type="button" value="v"/>						
超时时间	<input type="text"/> 1-65535 秒						
接口名称	modem 0 <input type="button" value="v"/>						
检测IP或域名	<input type="text" value="202.170.138.60"/> 最大长度为64位						
检测间隔	<input type="text" value="10"/> 1-65535 秒						
重试次数	<input type="text" value="5"/> 1-65535						
		<input type="button" value="保存"/> <input type="button" value="返回"/>					

图 6-5

应用结果

配置完所有参数后，路由器的默认路由走的是主链路 eth0（WAN）接口，此时路由器若一直能够 ping 通 202.170.138.60 的 IP 地址，则路由器就会一直工作在主链路上，如图 6-6 所示；而备份链路 modem 则一直处于在线状态。若有线网络（WAN 口）因为故障而无法 ping 通 202.170.138.60，则在多次检测失败后，路由器会将链路切换至 modem，使下位机的各种业务能够正常进行，如图 6-7 所示。

```
##### rule[0], main link[vpdnppoe], icmp check begin #####[linkbackup.c->739]
**** ICMP send icmp packet successful ****[icmp.c->219]
>>>> ICMP rcv one packet success!>>>>[icmp.c->304]
##### rule[0], main link[vpdnppoe], icmp check end #####[linkbackup.c->741]
now checking rule[0], check main link[vpdnppoe] ret[0] (0:success, <0:failed)[linkbackup.c->744]
```

静态路由

网络地址	子网掩码	网关	接口	度量
192.168.8.0	255.255.255.0	0.0.0.0	br0	0
0.0.0.0	0.0.0.0	0.0.0.0	vpdnppoe	0

图 6-6

```
**** ICMP send icmp packet successful ****[icmp.c->219]
rcv_icmp_pack:select time out[icmp.c->98]
**** ICMP Recv icmp packet timeout ****[icmp.c->299]
**** ICMP send icmp packet successful ****[icmp.c->219]
rcv_icmp_pack:select time out[icmp.c->98]
**** ICMP Recv icmp packet timeout ****[icmp.c->299]
##### rule[0], main link[vpdnppoe], icmp check end #####[linkbackup.c->741]
now checking rule[0], check main link[vpdnppoe] ret[-2] (0:success, <0:failed)[linkbackup.c->744]
switch from [rule:0] main [link:vpdnppoe] to [rule:1] backup [link:modem][linkbackup.c->475]
```

静态路由

网络地址	子网掩码	网关	接口	度量
192.168.8.0	255.255.255.0	0.0.0.0	br0	0
0.0.0.0	0.0.0.0	0.0.0.0	modem	0

图 6-7

6.4 参数切换功能应用

场景介绍

H8951 系列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。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“5.2.2 网络设置”下的“参数切换”。

配置情况如图 6-8、图 6-9、图 6-10 所示。



图 6-8



图 6-9

The screenshot displays the configuration page for interface detection rules. At the top, there is a navigation bar with tabs for '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', and '状态'. Below this, there is a secondary set of tabs for 'LAN', 'WAN', 'WLAN', '移动网络', '参数切换', '网络连接', '链路备份', and 'DHCP服务'. The main configuration area includes a table with columns for '规则名称', '接口名称', '检测方法', and '操作'. Below the table, there is a '状态' section with '启用' and '禁用' buttons. The '基本信息' section contains four input fields: '规则名称' (value: 2), '间隔时间' (value: 60), '重试次数' (value: 3), and '超时时间' (empty). The '添加接口检测规则' section has three fields: '接口名称' (dropdown: vpdn2), '检测方法' (dropdown: icmp), and '目的IP' (value: 192.168.110.1). At the bottom, there are '刷新' and '返回' buttons.

图 6-10

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 ping 192.168.100.1 失败后，切换到 L2TP 链路，并维持与服务器的连接，如图 6-11 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 6-11

6.5 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 H8922S 4G Router 支持 L2TP/PPTP/GRE/IPIP/IPSec/OpenVPN 多种协议 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。

此处以 H8922S 为例说明，H8922S 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 6-12 所示。

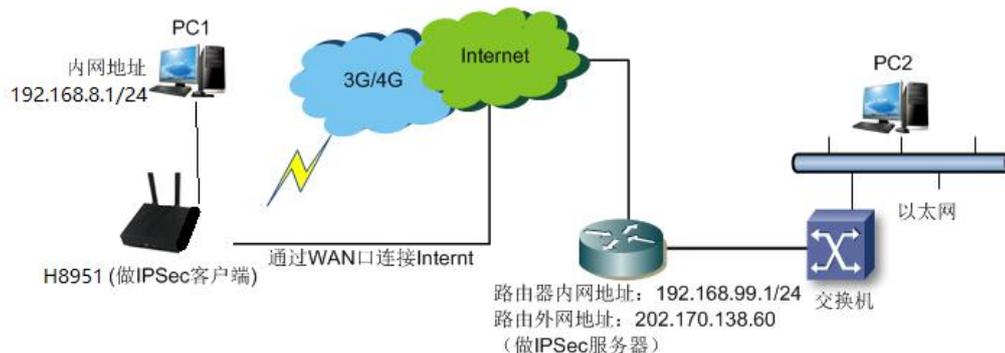


图 6-12

PC1 通过 H8922S 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。H8922 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 6-113、图 6-114、图 6-15 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			

基本设置	
选择	<input checked="" type="radio"/> Phase1 <input type="radio"/> Phase2 <input type="radio"/> IPSec
策略名称	<input type="text" value="1"/> * 最大长度为12位
协商模式	<input type="text" value="main"/>
加密方式	<input type="text" value="3des"/>
哈希算法	<input type="text" value="md5"/>
认证方式	<input type="text" value="psk"/>
预共享密钥	<input type="text" value="****"/> * 最大长度为64位
本端标识	<input type="text" value="xxx@xxx"/> 最大长度为64位
对端标识	<input type="text" value="yyy@yyy"/> 最大长度为64位
IKE生存时间	<input type="text" value="28800"/> * 120-86400 秒
DH组	<input type="text" value="group1024"/>
DPD检测	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
检测间隔	<input type="text" value="30"/> 1-512 秒
重试次数	<input type="text" value="4"/> 1-512 次

<input type="button" value="保存"/>	<input type="button" value="返回"/>
-----------------------------------	-----------------------------------

图 6-13

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			

基本设置

选择 Phase1 Phase2 IPSec

策略名称 * 最大长度为12位

传输协议

加密方式

哈希算法

完美向前加密

DH组

密钥存活时间 * 120-86400 秒

本地协议端口 : 如: 47:0

远端协议端口 : 如: 47:0

传输方式

本地子网 * 如: 192.168.8.0/24

远端子网 * 如: 192.168.88.0/24

图 6-14

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			

基本设置

选择 Phase1 Phase2 IPSec

接口名称 * 最大长度为12位

匹配 Phase1

匹配 Phase2

服务地址 * 最大长度为64位

加密接口

图 6-15

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 H8922S 的配置相反。

应用结果

在配置 H8922S 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 6-16 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 6-16

```

~ # 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

```

6.6 任务管理应用

场景介绍

H8951 系列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

该场景下参数配置请参见“5.3.7 任务管理设置”，配置如图 6-17 所示。

任务名称	定时	任务类型	操作			
1	date:1005-1008 day:01-10	modem-online	编辑	删除	启用	禁用
2	interval:1400	reboot	编辑	删除	启用	禁用

图 6-17

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 6-18、图 6-19 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 6-20 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 6-18

```

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/pppdown-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 6-19

```

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

```

图 6-20

7

FAQ/异常处理

7.1 硬件类问题

7.1.1 所有指示灯均不亮

问题现象

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与卡槽切角对应后插入卡座。

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。

7.2 拨号类问题

7.2.1 拨号中断

问题现象

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
- Modem 压缩协议配置与服务器对端不匹配。

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“5.2.2 网络配置”下的“移动网络”进行正确的配置。
- 请修改 Modem 压缩协议配置，具体操作方法请参见“5.2.2 网络配置”下的“移动网络”。

7.2.2 无信号显示

问题现象

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

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

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 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 CFE 升级失败

问题现象

CFE 升级后发现固件升级失败。

原因分析

可能原因如下：

- 电源供电不符合要求
- 升级固件型号、格式不正确
- 升级未完成（web 页面显示以发送升级包到路由器，但是路由器还在升级）就断电导致

解决方法

- 如果是供电电源不符合要求，请更换符合要求的供电电源后重新升级 CFE。
- 如果是升级固件型号、格式不正确，请更换格式正确、与路由器相匹配的升级固件后重新升级 CFE。
- 如果是升级未完成时为设备断电导致 CFE 升级失败，则请参见“CFE 模式升级”重新升级。

7.4.5 页面升级失败

问题现象

用页面升级时，显示升级失败，且串口改为 DTU 通信，断电重启后，无法进入页面。

原因分析

升级的程序太大，导致升级失败。

解决办法

直接采用 CFE 模式升级，CFE 模式升级的具体操作请参见“CFE 模式升级”。五分钟后，可以进入路由器页面，此时的页面恢复了出厂设置。若通过该方法无法进入路由器页面，请联系我司工作人员。

7.4.6 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 10~11 秒后松开，将系统配置恢复到出厂状态（用户名：admin，密码：admin）；“设为默认”的配置将会被清除，恢复到最初的默认配置，但补丁将会被保留。



在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。

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

缩略语

A

ATM Auto Table Machine 自动柜员机

C

CDMA Code Division Multiple Access 码分多址

D

DDNS Dynamic Domain Name Server 动态域名服务

DHCP Dynamic Host Configuration Protocol 动态主机配置协议

DMZ Demilitarized Zone 隔离区

DNS Domain Name System 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 通用分组无线服务技术

GRE Generic Routing Encapsulation 通用路由封装协议

GSM Global System 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 介质访问控制

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	用户数据报协议
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



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

地址：深圳市龙岗区布澜路中海信科技园总部中心 14-16 楼

技术支持：400-00-64288 拨 2 投诉热线：400-00-64288 拨 3

传真：0755-83644677

网址：<http://www.hongdian.com>