F-DPU100 通信管理机使用说明书

此说明书适用于下列型号产品：

型号	产品类别

厦门四信通信科技有限公司

Add：厦门集美区软件园三期诚毅大街 370 号
A06 栋 11 层
客户热线：400-8838-199
电话：+86-592-6300320
传真：+86-592-591273
网址：www.four-faith.com

文档修订记录

日期	版本	说明	作者
2015-5-21	V1.00	初始版本	ZBQ/WT
2016-1-20	V1.01	修改参数与安装图片	Harven
2017-9-12	V1.2.0	修改参数与更新地址	Harven

著作权声明

本文档所载的所有材料或内容受版权法的保护，所有版权由厦门四信通信科技有限公司拥有，但注明引用其他方的内容除外。未经四信公司书面许可，任何人不得将本文档上的任何内容以任何方式进行复制、经销、翻印、连接、传送等任何商业目的的使用，但对于非商业目的的、个人使用的下载或打印（条件是不得修改，且须保留该材料中的版权说明或其他所有权的说明）除外。

商标声明

Four-Faith、四信、

、

、均系厦门四信通信科技有限公司注册商标，未经事先书面许可，任何人不得以任何方式使用四信名称及四信的商标、标记。


F-DPU100
Distributed Processing Unit
通信管理机
F-DPU100
LAN-2
LAN-4
LAN-1
LAN-3
USB
WAN

目录

第一章 产品简介.....7
1.1 产品概述.....7
1.2 产品特点.....8
1.3 工作原理框图.....9
1.4 产品规格.....9
第二章 安装.....12
2.1 概述.....12
2.2 装箱清单.....12
2.3 安装与电缆连接.....12
2.4 电源说明.....16
2.5 指示灯说明.....16
2.6 复位按钮说明.....17
第三章 参数配置.....17
3.1 配置连接图.....17
3.2 登录到配置页面.....18
3.2.1 PC 机 IP 地址设置（两种方式）.....18
3.2.2 登入到配置页面.....19
3.3 管理和配置.....21
3.3.1 设置.....21
3.3.1.1 基本设置.....21
3.3.1.2 动态 DNS(DDNS).....26
3.3.1.3 MAC 地址克隆.....27
3.3.1.4 高级路由.....27
3.3.1.5 VLANs.....29
3.3.1.6 网络.....29
3.3.2 无线.....32
3.3.2.1 基本配置.....32
3.3.2.2 无线安全.....34
3.3.3 服务.....36
3.3.3.1 服务.....36
3.3.4 VPN.....39
3.3.4.1 PPTP.....39
3.3.4.2 L2TP.....40
3.3.4.3 OPENVPN.....41
3.3.4.4 IPSEC.....45
3.3.4.5 GRE.....48
3.3.5 安全.....49
3.3.5.1 防火墙.....49
3.3.6 访问限制.....51
3.3.6.1 WAN 访问.....51
3.3.6.2 URL 过滤.....54

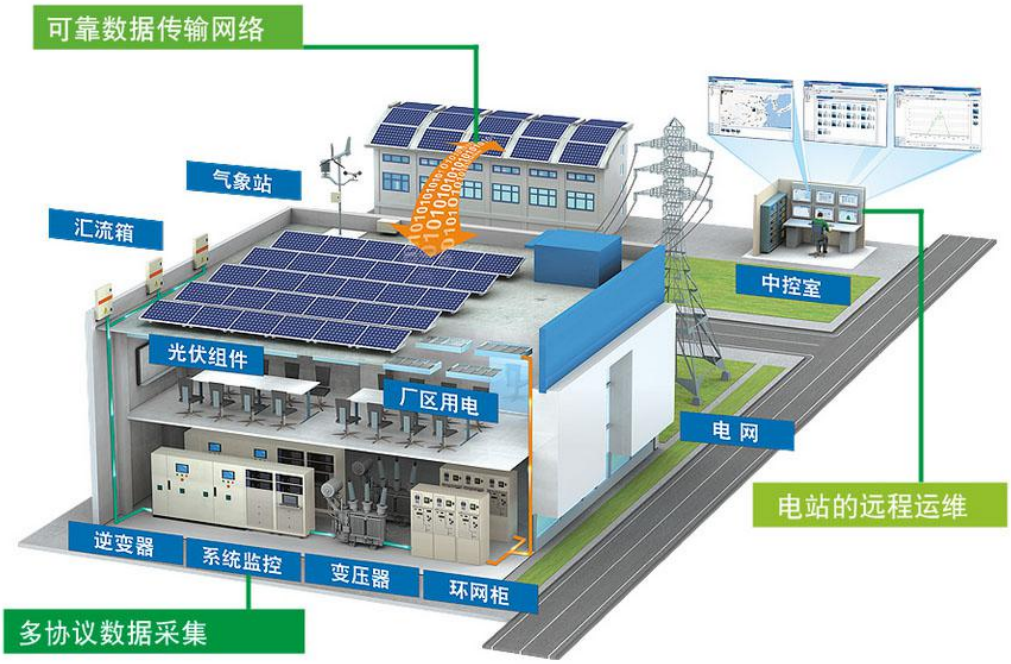
3.3.6.3 数据流过滤.....54
3.3.7 NAT.....55
3.3.7.1 端口转发.....55
3.3.7.2 端口范围转发.....56
3.3.7.3 DMZ.....57
3.3.8 QoS 设置.....57
3.3.8.1 基本.....57
3.3.8.2 分类.....57
3.3.9 应用.....58
3.3.9.1 串口应用.....58
3.3.9.2 通信网关应用.....60
3.3.10 管理.....65
3.3.10.1 管理.....65
3.3.10.2 保持活动.....67
3.3.10.3 命令.....68
3.3.10.4 出厂默认.....69
3.3.10.5 固件升级.....69
3.3.10.6 备份.....69
3.3.11 状态.....70
3.3.11.1 通信管理机.....70
3.3.11.2 WAN.....72
3.3.11.3 LAN.....74
3.3.11.4 无线.....77
3.3.11.5 宽带.....79
3.3.11.6 系统信息.....80
附录.....83

第一章 产品简介

1.1 产品概述

F-DPU100 是一种物联网无线通信管理机，利用公用无线网络为用户提供协议集成和无线长距离数据传输功能。

该产品采用高性能的工业级 32 位通信处理器和工业级无线模块，以嵌入式实时操作系统为软件支撑平台，同时提供 1 个 RS232、5 个 RS485、4 个以太网 LAN，1 个以太网 WAN 以及 1 个 WIFI 接口，可同时连接串口设备、以太网设备和 WIFI 设备，实现多协议采集、数据透明传输和路由功能。



该产品已广泛应用于物联网产业链中的 M2M 行业，如光伏发电、变电所等电力行业、城市楼宇能源管理、能耗企业能源管理等。

1.2 产品特点

工业级应用设计

- 采用高性能工业级无线模块
- 采用高性能工业级 32 位通信处理器
- 支持低功耗模式，包括休眠模式、定时上下线模式
- 采用金属外壳，保护等级 IP30。金属外壳和系统安全隔离，特别适合于工控现场的应用
- 宽电源输入（DC 5~36V）

稳定可靠

- WDT 看门狗设计，保证系统稳定
- 采用完备的防掉线机制，保证数据终端永远在线
- 以太网接口内置 1.5KV 电磁隔离保护
- RS232/RS485/RS422 接口内置 15KV ESD 保护
- SIM/UIM 卡接口内置 15KV ESD 保护
- 电源接口内置反相保护和过压保护
- 天线接口防雷保护（可选）

标准易用

- 提供标准 RS232、RS485、以太网和 WIFI 接口，可直接连接串口设备、以太网设备和 WIFI 设备
- 提供标准有线 WAN 口（支持标准 PPPOE 协议），可直接连接 ADSL 设备
- 智能型数据终端，上电即可进入数据传输状态
- 提供功能强大的中心管理软件，方便设备管理（可选）
- 使用方便，灵活，多种工作模式选择
- 方便的系统配置和维护接口（包括本地和远端 WEB 和 CLI 方式）

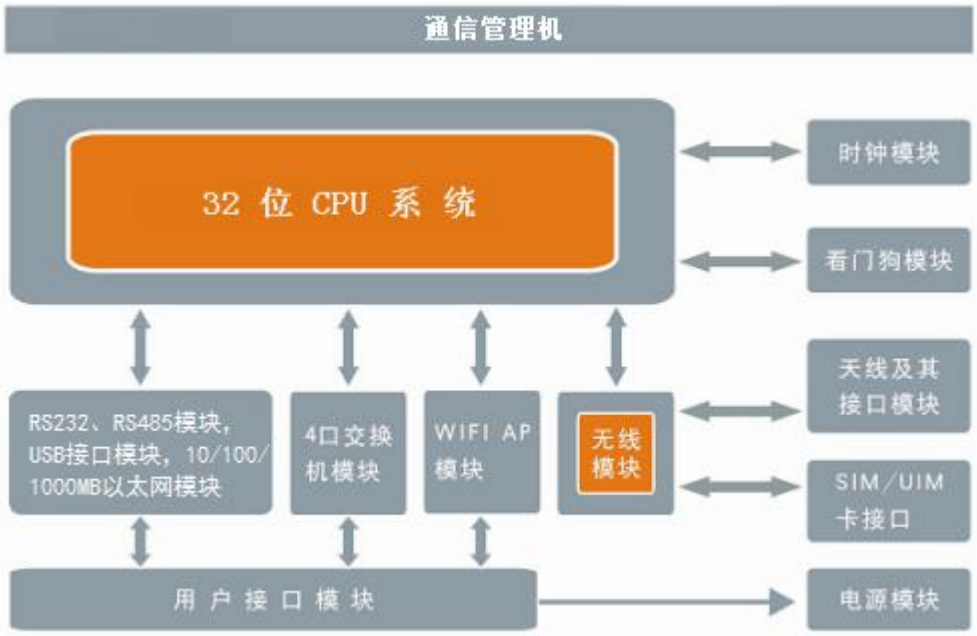
功能强大

- 支持各种行业化协议集成，提供编译器供客户对应用层自定义开发
- 支持多种 WAN 连接方式，包括静态 IP，DHCP，L2TP，PPTP，PPPOE，2.5G/3G/4G
- 支持无线蜂窝和有线 WAN 双链路智能切换备份功能（可选）
- 支持 VPN client（PPTP，L2TP，OPENVPN，IPSEC 和 GRE）（注：仅 VPN 版支持）
- 支持 VPN sever（PPTP，L2TP，OPENVPN，IPSEC 和 GRE）（注：仅 VPN 版支持）
- 支持远程管理，SYSLOG、SNMP、TELNET、SSHD，HTTPS 等功能
- 支持本地和远程在线升级，导入导出配置文件
- 支持 NTP，内置 RTC
- 支持国内外多种 DDNS
- 支持 VLAN，MAC 地址克隆，PPPoE 服务器
- WIFI 支持 802.11b/g/n/ac，双频 2.4G 和 5.8G，支持 WIFI AP、AP Client、中继器、中继桥接和 WDS 等多种工作模式（可选）
- WIFI 支持 WEP、WPA、WPA2 等多种加密方式，支持 RADIUS 认证，MAC 地址过滤等功能。

- 支持多种上下线触发模式，包括短信、电话振铃、串口数据、网络数据触发上下线模式
- 支持 APN/VPDN
- 支持多路 DHCP server 及 DHCP client，DHCP 捆绑 MAC 地址，DDNS，防火墙，NAT，DMZ 主机，QoS，流量统计，实时显示数据传输速率等功能
- 支持 TCP/IP、UDP、FTP（可选）、HTTP 等多种网络协议
- 支持 SPI 防火墙，VPN 穿越，访问控制，URL 过滤，等功能
- 定时上下线功能

1.3 工作原理框图

通信管理机原理框图如下：



1.4 产品规格

无线参数

项　目	内　容
无线模块	工业级无线模块（可选单模块、双模块或无模块）
标准	可支持 TDD-LTE/FDD-LTE/EVDO/WCDMA/TD-SCDMA/CDMA1X /GPRS/EDGE 可选单模、多模或全网通讯
理论带宽	FDD LTE(下行速率 100Mbps，上行速率 50Mbps) TDD LTE(下行速率 68Mbps，上行速率 17Mbps) CDMA2000 1X EVDO Rev A (下行速率 3.1Mbps，上行速率 1.8Mbps) WCDMA(下行速率 42Mbps，上行速率 5.76Mbps) TD-SCDMA(下行速率 4.2Mbps，上行速率 2.2Mbps)
发射功率	<24dBm
接收灵敏度	<-109dBm

WIFI 无线参数

项　目	内　容
标准及频段	支持 IEEE802.11b/g/n，2.4G, 2*2 MIMO，支持 AP 模式，Station 模式（可选） 支持 IEEE802.11ac，5.8G, 2*2 MIMO，支持 AP 模式，Station 模式（可选）
理论带宽	IEEE802.11b/g：最高速率达 108Mbps IEEE802.11n：最高速率达 300Mbps IEEE802.11ac：最高速达 780Mbps
安全加密	支持 WEP、WPA、WPA2 等多种加密方式
发射功率	26dBm（11b），21.5dBm（11g），20dBm（11n），16dBm（11ac）
接收灵敏度	<-72dBm@54Mpbs

硬件系统

项　目	内　容
CPU	工业级 32 位通信处理器
FLASH	512MB
DDR3	512MB

接口类型

项　目	内　容
WAN 接口	1 个 10/100/1000M 以太网口（RJ45 插座），自适应 MDI/MDIX，内置 1.5KV 电磁隔离保护
LAN 接口	4 个 10/100/1000M 以太网口（RJ45 插座），自适应 MDI/MDIX，内置 1.5KV 电磁隔离保护
串口	1 个 RS232 串口，5 个 RS485 串口，内置 15KV ESD 保护，串口参数如下： 数据位：5、6、7、8 位 停止位：1、1.5（可选）、2 位 校验：无校验、偶校验、奇校验、SPACE（可选）及 MARK（可选）校验 串口速率：2400~115200bits/s

指示灯	具有“Power”、“System”、“Online”、“SIM”、“WAN”、“LAN”、“WIFI”、“信号强度指示灯”等指示灯
天线接口	蜂窝：2 个标准 SMA 阴头天线接口，特性阻抗 50 欧 WIFI：2 个标准 SMA 阳头天线接口，特性阻抗 50 欧
SIM/UIM 卡接口	标准的抽屉式用户卡接口，支持 1.8V/3V SIM/UIM 卡，内置 15KV ESD 保护
电源接口	2 芯端子电源插座，内置电源反相保护
Reset 复位按钮	长按此按钮 15 秒，可将通信管理机的参数配置恢复为出厂值





供电

项　目	内　容
标准电源	DC 12V/1.5A
供电范围	DC 5~36V
工作电流	3G：<640mA (12V)　　4G：<720mA (12V)
待机电流	3G：<530mA (12V)　　4G：<600mA (12V)

物理特性

项　目	内　容
外壳	金属外壳，保护等级 IP30
外形尺寸	172x122x38 mm（不包括天线和安装件）
重量	700g

其它参数

项　目	内　容
工作温度	-35～+75℃（-31～+167℉）
储存温度	-40～+85℃（-40～+185℉）

相对湿度	95%（无凝结）

第二章 安装

2.1 概述

通信管理机必须正确安装方可达到设计的功能，通常设备的安装必须在本公司认可合格的工程师指导下进行。

➢ *注意事项：*
请不要带电安装通信管理机。

2.2 装箱清单

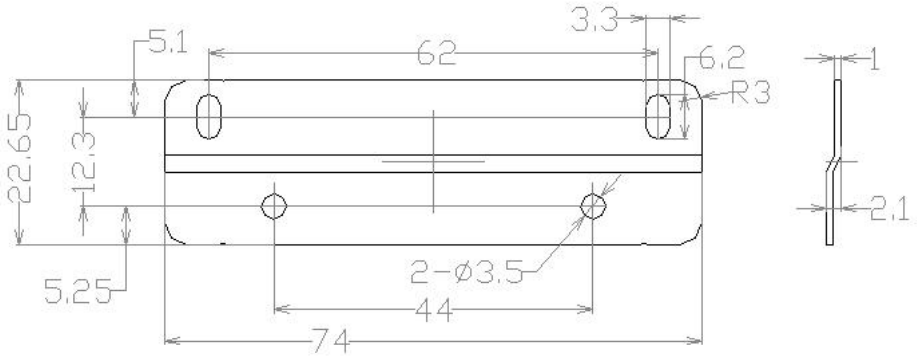
当您开箱时请保管好包装材料，以便日后需要转运时使用。清单如下：

✧ 通信管理机主机 1 台
✧ 无线蜂窝天线（SMA 阳头）2 根
✧ WIFI 天线（SMA 阴头）1 根
✧ 配套电源 1 个
✧ 以太网直连线 1 条
✧ 使用说明书光盘 1 张
✧ 产品合格证
✧ 产品保修卡

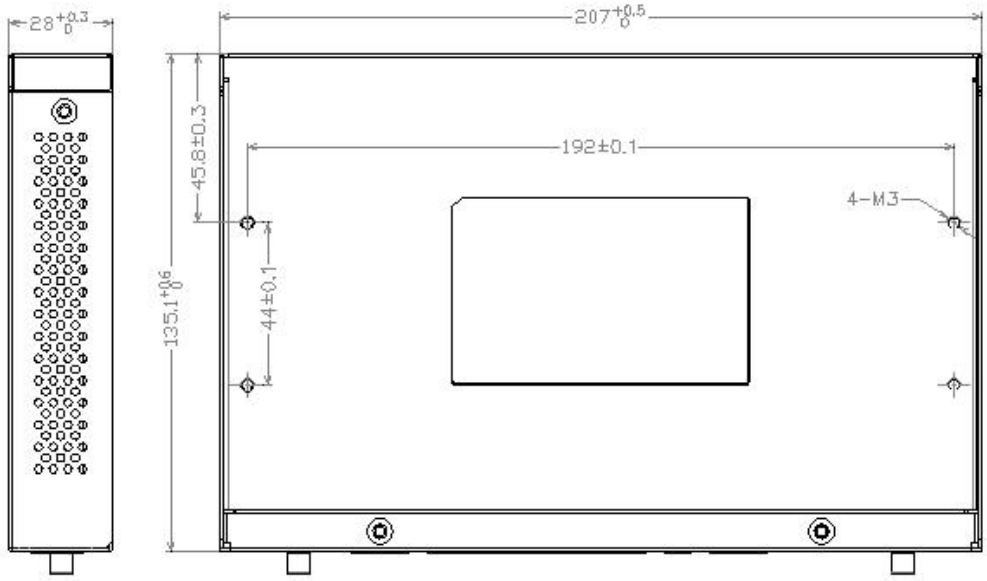
2.3 安装与电缆连接

外形尺寸：

外形尺寸如下图。（单位:mm）



固定片尺寸



通信管理机尺寸

注：使用固定片安装通信管理机螺钉为 M3，螺钉锁进通信管理机的深度为 3～4mm。

天线安装：

无线广域网天线接口为 SMA 阴头插座（标识为“ANT-1”和“ANT-2”），将配套的无线蜂窝天线的 SMA 阳头旋到该天线接口上，并确保旋紧，以免影响信号质量。

无线局域网天线接口为 SMA 阳头插座（标识为“WIFI”），将配套 WIFI 天线的 SMA 阴头旋到该天线接口上，并确保旋紧，以免影响信号质量。

注意：无线蜂窝天线和 WIFI 天线不能接反，否则设备无法工作。

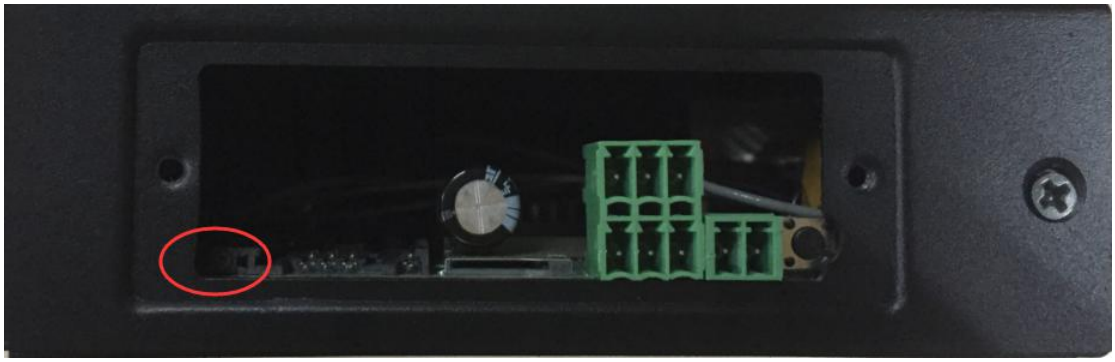
SIM/UIM 卡安装：

安装或取出 SIM/UIM 卡时，先用尖状物轻轻顶住退卡钮（SIM/UIM 左侧的圆形小圆点），SIM/UIM 卡套即可弹出。安装 SIM/UIM 卡时，先将 SIM/UIM 卡放入卡套，并确保 SIM/UIM 卡的金属接触面朝外，再将 SIM/UIM 卡套插入抽屉中，并确保插到位。

（下图以单卡为例）



步骤 1



步骤 2



步骤 3



步骤 4

连接网线：

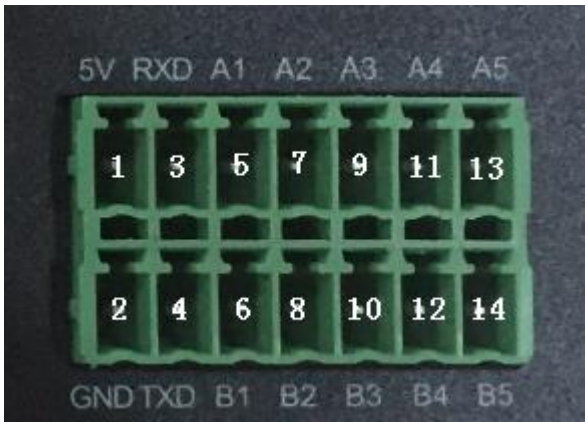
将网络直连线的一端插到通信管理机的 LAN1~LAN4 的任意一个口上，另一端插到用户设备的以太网接口上。网络直连线信号连接如下：

RJ45-1	RJ45-2	线颜色
1	1	白/橙
2	2	橙
3	3	白/绿
4	4	蓝
5	5	白/蓝
6	6	绿
7	7	白/棕
8	8	棕



连接 RS232/RS485 线：

将 RS232 和 RS485 线端插到通信管理机的 14PIN 接口上，引出来的 RS232/RS485 线到用户设备的 RS232/RS485 串行接口上,接口信号连接如下：



14PIN	信号定义	信号描述	相对于通信管理机方向
1	5V	5V 电源（1W）	输出
2	GND	电源地	输出
3	RXD	接收数据	输入
4	TXD	发送数据	输出
5	A1	485A1	输入/输出
6	B1	485B1	输入/输出

7	A2	485A2	输入/输出
8	B2	485B2	输入/输出
9	A3	485A3	输入/输出
10	B3	485B3	输入/输出
11	A4	485A4	输入/输出
12	B4	485B4	输入/输出
13	A5	485A5	输入/输出
14	B5	485B5	输入/输出



2.4 电源说明

通信管理机 通常应用于复杂的外部环境。为了适应复杂的应用环境，提高系统的工作稳定性，通信管理机采用了先进的电源技术。用户可采用标准配置的 12VDC/1.5A 电源适配器给通信管理机供电，也可以直接用直流 5~36V 电源给通信管理机供电。当用户采用外加电源给通信管理机供电时，必须保证电源的稳定性（纹波小于 300mV，并确保瞬间电压不超过 36V），并保证电源功率大于 8W 以上。

推荐使用标配的 12VDC/1.5A 电源。

2.5 指示灯说明

通信管理机提供以下指示灯：“Power”、“System”、“Online”、“SIM”、“LAN1~LAN4”、“WAN”、“WIFI”、“信号强度指示灯”。各指示灯状态说明如下表：

指示灯	状 态	说 明
Power	亮	设备电源正常
	灭	设备未上电
System	闪烁	系统正常运行
	灭	系统不正常
Online	亮	设备已登录网络
	灭	设备未登录网络
SIM	亮	识别到 SIM/UIM 卡
	灭	未识别到 SIM/UIM 卡
LAN1~LAN4	灭	相应网络接口未连接
	亮/闪烁	相应网络接口已连接/正在数据通信
WAN	灭	WAN 接口未连接
	亮/闪烁	WAN 接口已连接/正在数据通信
WIFI	灭	WIFI 未启动
	亮	WIFI 已启动
信号强度指示灯	亮一个灯	信号强度较弱(小于-90dbm)
	亮两个灯	信号强度中等(-70dbm~-90dbm)
	亮三个灯	信号强度极好(大于-70dbm)

2.6 复位按钮说明

通信管理机设有一个复位按钮，标识为“Reset”。该按钮的作用是将通信管理机的参数配置恢复为出厂值。方法如下：用尖状物插入“Reset”孔位，并轻轻按住复位按钮约 15 秒钟后放开，此时，通信管理机会自动把参数配置恢复为出厂值，并在约 10 秒钟之后，通信管理机自动重启（自动重启现象如下：“System”指示灯熄灭 10 秒钟左右，然后又正常工作）。

第三章 参数配置

3.1 配置连接图

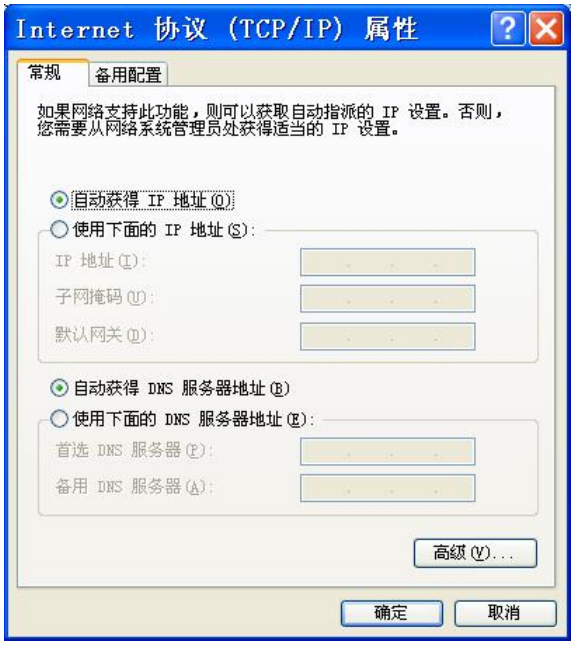
在对通信管理机进行配置前，需要将通信管理机和用于配置的 PC 通过出厂配置的网络线或 WIFI 连接起来。用网络线连接时，网络线的一端连接通信管理机“Local Network”（以下简称 LAN 口）的任意一个以太网接口，另外一端连接到 PC 的以太网口。用 WIFI 连接时，通信管理机出厂默认的 SSID 为“FOUR-FAITH”，无须密码验证。



3.2 登录到配置页面

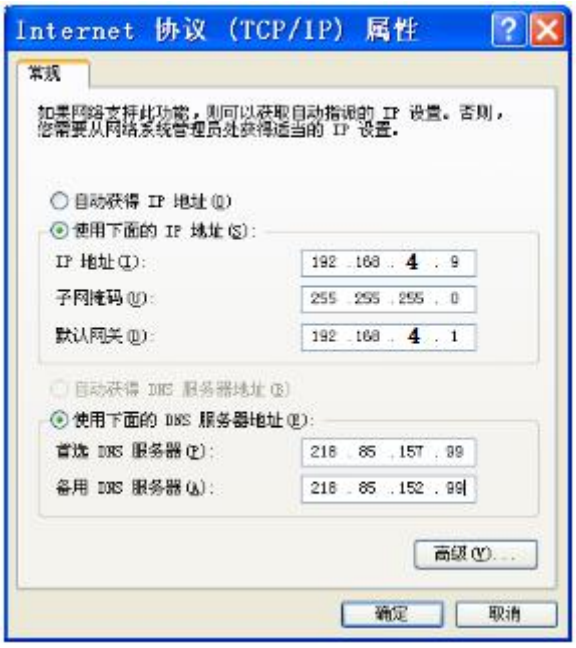
3.2.1 PC 机 IP 地址设置（两种方式）

第一种方式：自动获得 IP 地址



第二种方式：指定 IP 地址

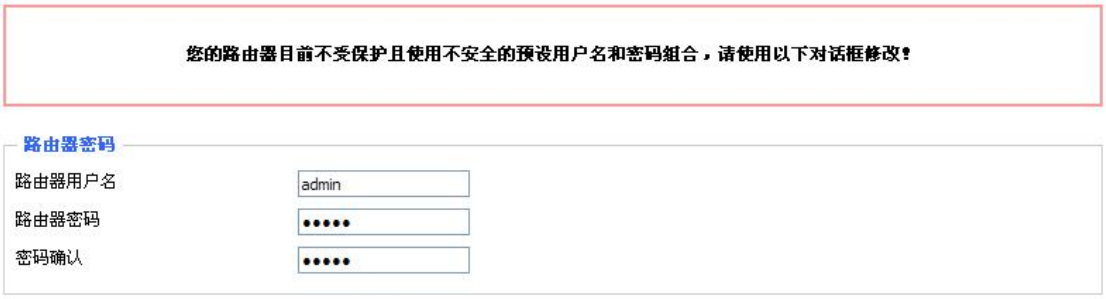
设置 PC 的 IP 地址为 192.168.4.9(或者其他 192.168.1 网段的 IP 地址)，子网掩码设为：255.255.255.0，默认网关设为：192.168.4.1。DNS 设为当地可用的 DNS 服务器。



3.2.2 登入到配置页面

本章对每个页面的主要功能进行了描述。可以使用连接到通信管理机上的计算机通过网页浏览器来对网页工具进行访问。一共有十一个主页面，即：设置、无线、服务、VPN、安全、访问限制、NAT、QoS 设置、应用、管理以及状态。单击其中一个主页面，则会出现更多的从页面。

为了访问通信管理机基于网页的 Web 管理工具，启动 IE 或其他浏览器，并在“地址”栏输入通信管理机的默认 IP 地址 192.168.4.1。按回车键。若是首次登入到 Web 页面，可以看到如下所示的页面，提示用户是否修改通信管理机的默认用户名和密码，若需要输入用户自行定义的用户名的密码，单击“Change Password”按键予以生效



之后就可以进入信息主页面



若是第一次单击主菜单则需要输入相应的用户名和密码



输入正确的用户和密码既可以访问相应的菜单页面默认用户名 admin，默认密码 admin。(可以在管理页面更改用户名和密码)。然后点击“确定”

3.3 管理和配置

3.3.1 设置

点击“设置”打开的第一个页面是基本设置。通过此页面，您可以按照提示来对基本设置进行更改，单击“保存设置”按钮来更改但不生效，单击“应用”按钮来使更改生效，或是单击“取消改动”按钮来取消更改。

3.3.1.1 基本设置

“WAN 连接类型”设置部分描述如何配置将通信管理机连接到互联网。可以从您的 ISP 处取得这方面的详细信息。

WAN 连接类型

从下拉菜单中选择您的 ISP 为您提供的 Internet 连接类型，WAN 连接类型包括 7 种方式：禁用，静态 IP，自动配置-DHCP，PPPOE，3G/UMTS/4G/LTE，DHCP-4G。

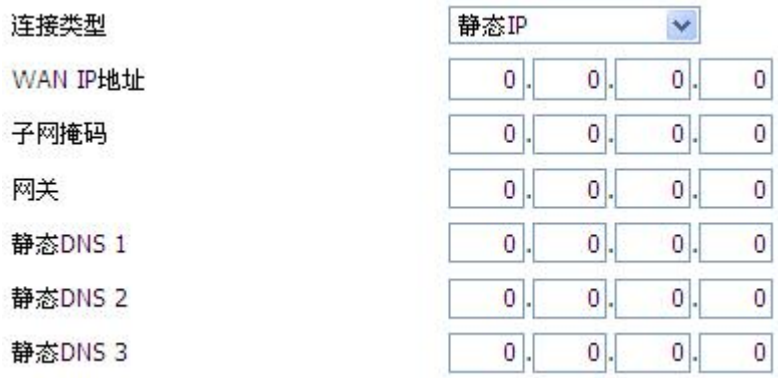
方式一：禁用



禁止 WAN 口的连接类型设置

方式二：静态 IP

商务光纤等专线接入通常会采用这种连接类型。宽带服务商会向您提供 IP 地址，子网掩码，网关和 DNS 等详细参数，您需要将这些参数设置在通信管理机上。



WAN IP 地址： 用户根据自己或者 ISP 分配而设置的 IP 地址
子网掩码： 用户根据自己或者 ISP 分配而设置的子网掩码
网关： 用户根据自己或者 ISP 分配而设置的网关
静态 DNS（1-3）： 用户根据自己或者 ISP 分配而设置的静态 DNS

方式三：自动配置-DHCP

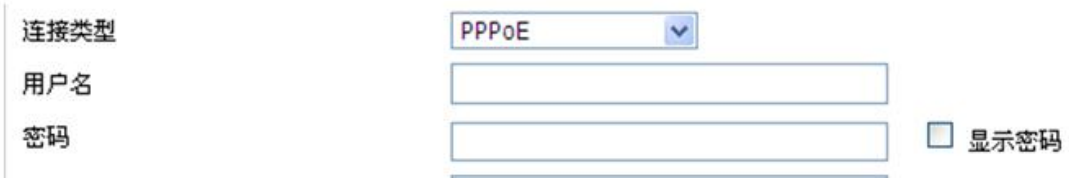
通信管理机默认的 WAN 连接类型。有线电视（Cable）和部分小区宽带采用这种连接方式。如深圳天威视讯，上海有线通等。



WAN 口的 IP 地址有 DHCP 的方式获取

方式四：PPPOE

中国电信和中国网通 ADSL 宽带服务通常会采用这种连接类型，其他一些宽带服务商也会采用这种方式。PPPoE 连接类型需要 ISP 向您提供用户名，密码和服务名称，这些信息需要设置到通信管理机上。



用户名： 用于登录到 Internet 的用户名。
密码： 用于登录到 Internet 的密码。

方式五：3G/UMTS/4G/LTE



用户名： 用于登录到 Internet 的用户名。
密码： 用于登录到 Internet 的密码。
呼叫中心号码： 呼叫到运营商的呼叫号码。
APN ： 接入点名称。
PIN： SIM 卡提供的 PIN 码

网络类型



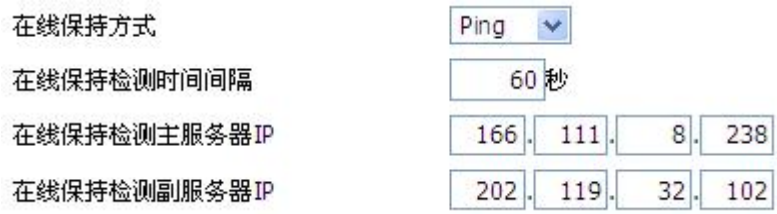
网络的选择：包括自动方式，强制到 3g，强制到 2g，3g 优先，2g 优先等多种方式，若使用 4G 模块，则相应的会增加 4G 的网络选项，根据用户需要和不同的模块类型进行选择

方式六：DHCP-4G



WAN 口的 IP 地址由 DHCP-4G 的方式获取

在线保持



在线保持功能用于检测 Internet 链路是否处于有效状态。如果设置了此项，通信管理机将自动检测 Internet 链路，一旦检测到链路断开或者无效，系统将自动重联，重新建立有效链路。如果网络环境比较差，或者在专网的情况下，建议用通信管理机模式。

在线保持方式：

None: 不使用在线保持功能。

Ping: 发送 ping 包检测链路。如果设置成此方式，还必须正确配置 “在线保持检测时间间隔”，“在线保持检测主服务器 IP ”和“在线保持检测副服务器 IP ”配置项。

Route: 使用 route 方式检测链路，如果设置成此方式，还必须正确配置“在线保持检测时间间隔”，“在线保持检测主服务器 IP ”和“在线保持检测副服务器 IP ”配置项。

PPP: 使用 PPP 方式检测链路，如果设置成此方式，还必须正确配置“在线保持检测时间间隔”配置项。

在线保持检测时间间隔：

两次在线保持检测之间的时间间隔，单位为秒。

在线保持检测主服务器 IP ：

响应通信管理机在线检测数据包的主服务器的 IP 地址。只有当“在线保持方式”设置成“Ping”或者“Route”时，此配置项才有效。

在线保持检测副服务器 IP ：

响应通信管理机在线检测数据包的副服务器的 IP 地址。只有当“在线保持方式”设置成“Ping”或者“Route”时，此配置项才有效。



强制重新连接：该功能可以指定通信管理机在指定的时间重新连接 Internet。

时间：输入正确的重连时间

STP



STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

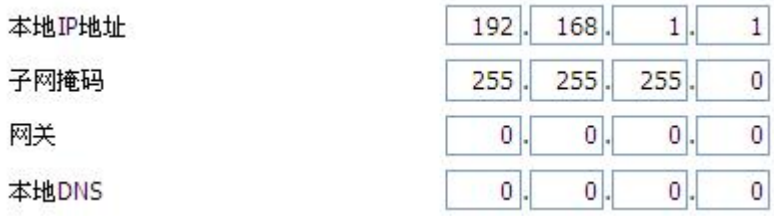
可选配置



通信管理机名称：在这个字段中，您可以输入代表通信管理机的长达 39 个字符的名称。
主机名与域名：可以利用这些选项来提供主机名与域名。一些 ISP（通常是固定网络 ISP）要求提供这些名称作为身份识别。您要与 ISP 确认您的宽带互联网服务中是否配置了主机名与域名。在大多数情况下，保持这些信息空白就可以了。
MTU：MTU 指的是最大传输单元。最大传输单元设置规定了互联网传输中所允许的最大包值。默认状态为“自动”，可以手动输入将要进行传输的最大包值。建议此值的范围为 1200 到 1500。对于大多数 DSL 用户而言，建议使用 1492。您应当使这一数值处于 1200 到 1500 范围内。如果希望通信管理机能够为您的互联网选择最佳的 MTU，则选择“自动”选项。

网络设置

网络设置部分可以对连接到通信管理机以太网端口上的网络设置进行修改。



本地 IP 地址：表示可以由您的局域网看到的通信管理机 IP 地址
子网掩码：表示可以由您的局域网看到的通信管理机 IP 地址子网掩码。
网关：设置通信管理机内部的网关，若默认设置，则内部网关为通信管理机本身的地址
本地 DNS：DNS 服务器由运营商接入服务器自动分配，如果你有自己的 DNS 服务器或者其他稳定可靠的 DNS 服务器，可以选择使用这些可靠的 DNS 服务器。否则，默认设置

网络地址服务器设置 (DHCP)

这些设置用于对通信管理机的动态主机配置协议（DHCP）服务器功能进行配置。通信管理机可以作为网络的一个 DHCP 服务器。DHCP 服务器自动为网络中的每一台计算机分配一个 IP 地址。如果选择启用通信管理机的 DHCP 服务器选项，则您可以将局域网上所有电脑设置成自动获取 IP 地址和 DNS，并确保在网络中没有其它的 DHCP 服务器。



DHCP 类型：包括 DHCP 服务器和 DHCP 转发器两种
若设置成 DHCP 转发器则输入 DHCP 的服务器地址，如下



DHCP 服务器：DHCP 在出厂的时候默认启用。如果网络中已经有 DHCP 服务器，或者您不希望有 DHCP 服务器，则单击“禁用”。若你选择 DHCP 转发器则填入相应的 DHCP 服务器 IP。

起始 IP 地址：输入范围 1-254 输入一个数值，用于 DHCP 服务器分配 IP 地址时的起始值。因为本通信管理机的默认 IP 地址为 192.168.1.1，所以，起始 IP 地址必须为 192.168.1.2 或更大但又比 192.168.1.254 小的数值。默认的起始 IP 地址为 192.168.1.100 。

最大 DHCP 用户数：输入您希望 DHCP 服务器分配 IP 地址的最大电脑数量。这个数量不能超过 253，且 IP 起始地址加上用户数不能大于 255，默认数值为 50。

客户端租约时间：指动态 IP 地址的网络用户占用 IP 地址的租约周期。输入以分钟为单位的时间，这样，该用户“租用”了这个动态 IP 地址。动态 IP 地址到期后，会自动分配给用户一个新的动态 IP 地址。默认设置为 1440 分钟，代表 1 天。可设置范围 0-99999

静态 DNS（1-3）：域名解析系统（DNS）用于互联网将域名或是网页名翻译成为互联网地址或 URL（通用资源定位器）。您的 ISP 至少会提供给您一个 DNS 服务器的 IP 地址。可以输入多达三个 DNS 服务器 IP 地址。通过使用这些地址，可以达到对正在工作的 DNS 服务器的快速访问。

WINS：视窗系统因特网命名服务（WINS）管理与互联网进行互动的每一台电脑。如果使用 WINS 服务器，则要在这里输入该服务器的 IP 地址。否则，不填写任何地址。

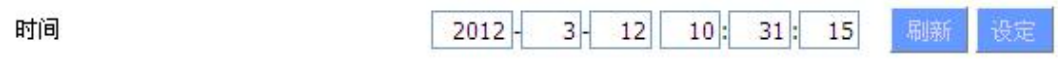
DNSMasq：您的域名加入本地搜索领域，增加扩展主机选项，采用 DNSMasq 可以为子网分配 IP 地址和 DNS，若不选择 DNSMasq，则采用 dhcpd 服务为子网提供 IP 地址和 DNS

时间设置



NTP 客户端：开启和禁用为系统内部提供一个对时功能，即设置系统时间
时区：西 12 区到东 12 区，通过自己的位置设定
夏令时：根据自己的位置设定
服务器 IP/主机名称：你 NTP 服务器的 IP 地址，最长 32 个字符，若无则系统会默认去找服务器

校准时间



为系统校准时间，刷新则获取网页当时的时间，设置，则修改系统的时间。为系统校时的功能，特别是在无法获取到 NTP 服务的时候，可以手动为系统校时

完成修改后，单击“**保存设置**”按钮来更改但不生效，单击“**应用**”按钮来使更改生效，或是单击“**取消改动**”按钮来取消更改。帮助信息位于屏幕的右侧。

3.3.1.2 动态 DNS(DDNS)

如果通信管理机 Internet 接入获得的 IP 地址由运营商动态分配，通信管理机每次获得的 IP 地址都可能不一样。在这种情况下可以采用动态域名服务，域名提供商允许你注册一个域名，该域名始终对应通信管理机当前的动态 IP 地址。这样，通过访问域名就可以访问到通信管理机最新的 Internet IP 地址

DDNS 服务：此路由支持多种的 DDNS 服务器，如：DynDNS，freedns，Zoneedit，NO-IP，3322，easyDNS，TZO，DynSIP。还可以自行定义



用户名：用户在 DDNS 服务器注册的用户名，最大长度 64 个字符

密码：用户在 DDNS 服务器注册用户名时输入的密码，最大长度 32 个字符
主机名：用户在 DDNS 服务器申请的主机名，目前的输入长度还没有限制
类型：不同的服务器不一样
通配符：是否支持通配符，缺省为 OFF。ON 意为着 *.host.3322.org 等同于 host.3322.org
不使用外部 IP 检测:开启或禁用不使用外部 IP 检测



强制更新间隔：单位天，在设置的天数里面强制去更新动态 DNS 到服务器中

状态



状态显示目前连接的状态，已经在连接过程中的信息

完成修改后，单击“**保存设置**”按钮来更改但不生效，单击“**应用**”按钮来使更改生效，或是单击“**取消改动**”按钮来取消更改。帮助信息位于屏幕的右侧。

3.3.1.3 MAC 地址克隆

某些 ISP 可能要求您注册您的 MAC 地址。如果您不想重新注册您的 MAC 地址，您可以将通信管理机的 MAC 地址克隆为您在 ISP 注册的 MAC 地址。



Mac 地址克隆可以克隆 3 个部分，一个是 LAN 口的克隆，一个是 WAN 口的克隆，另一个是无线 MAC 地址克隆，需要注意的有两点，第一、MAC 地址为 48 位，不能设置成多播的地址，即第一个字节应该为偶数。第二、由于无线和 LAN 口有网桥 br0 连接在一起，所以网桥 br0 的 MAC 地址由 LAN 的 MAC 地址与无线 MAC 地址的较小值决定。

3.3.1.4 高级路由

在高级路由页面上，可以设置运行模式和静态路由。对于大多数用户，建议使用网关模式。



工作模式：选择正确的运行模式。如果通信管理机共享 Internet 宽带连接，则保持默认设置网关（对于大多数用户，建议使用网关模式）。如果要在网络上只使用通信管理机的路由功能，则选择通信管理机。

动态路由



该功能在网关模式下不可用。动态路由功能使通信管理机能够针对网络布局中的物理更改进行自动调整，并与其他通信管理机交换路由表。通信管理机根据源和目标之间的最小跳数确定网络包的路由。

要对 WAN 端启用动态路由功能，请选择 WAN 。要对 LAN 和无线端启用该功能，请选择 LAN&WLAN。要对 WAN 和 LAN 同时启用该功能，请选择两者。要对所有数据传输禁止动态路由功能，请保持默认设置禁用。

静态路由

要在通信管理机和另一个网络之间设置静态路由，请从静态路由下拉列表中选择一个编号进行设置。（静态路由是网络信息必须传输到特定主机或网络而预先确定的路径。）



选择设置标号：1-50 个静态路由

路由名称：用户定义的路由名称，最长可以输入 25 字符

跳点数：源地址到目标地址之间路由的度量单位。范围 0-9999

目的 LAN IP：目标 IP 地址是静态路由的目的网络或主机的地址。

子网掩码：子网掩码确定目的 IP 地址的哪个部分是网络部分，哪个部分是主机部分。

网关：这是允许通信管理机和目的网络或主机之间进行联系的网关设备的 IP 地址。

接口：根据目标 IP 地址所在的位置，可选择 LAN 和无线或 WAN（Internet）等若干的端

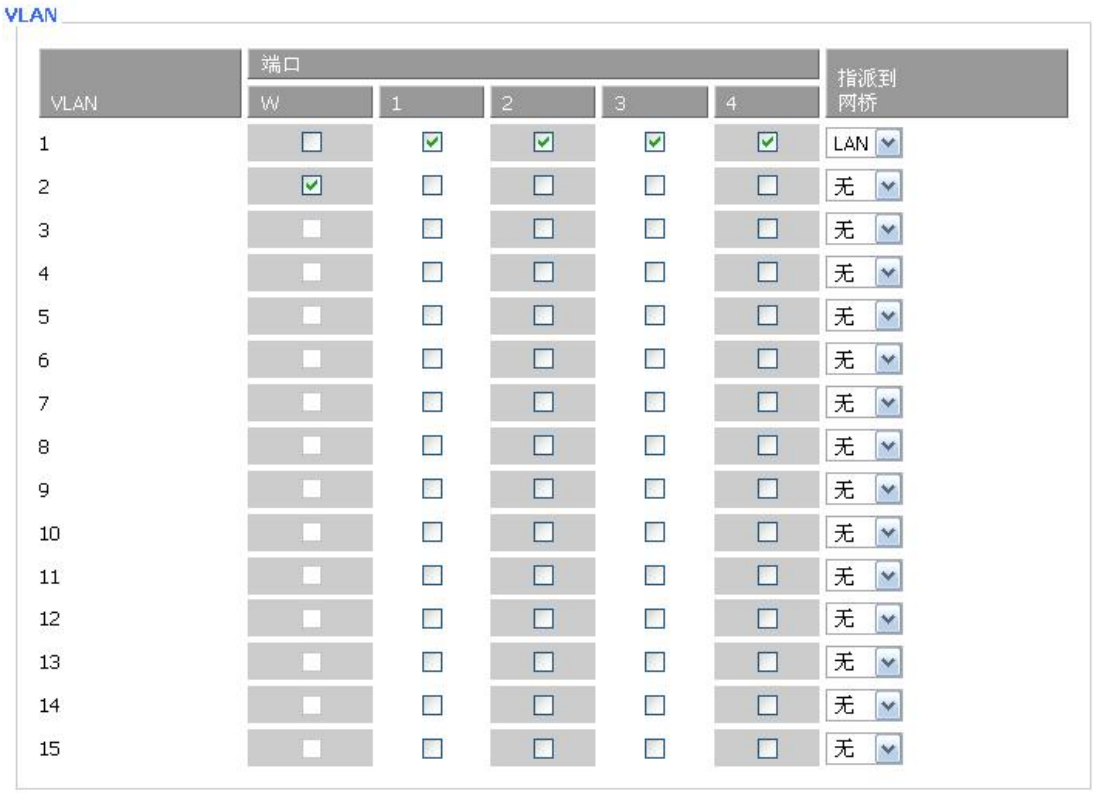
口

要先删除已经设置好的静态路由，请选择对应的路由表编号，点击“**删除**”按钮。要查看当前通信管理机的详细路由信息，点击“**显示路由表**”按钮。



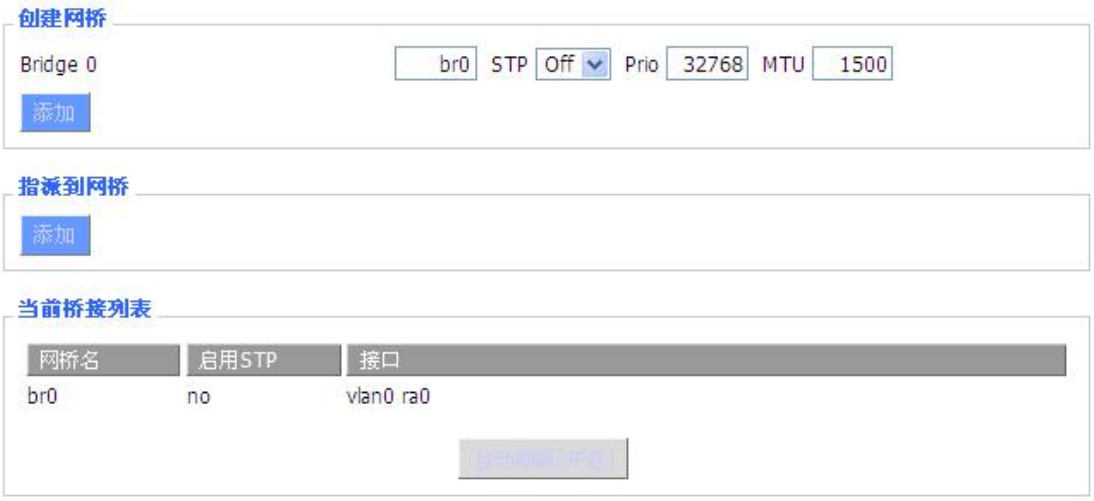
完成修改后，单击“**保存设置**”按钮来更改但不生效，单击“**应用**”按钮来使更改生效，或是单击“**取消改动**”按钮来取消更改。帮助信息位于屏幕的右侧。

3.3.1.5 VLANs



VLANs 功能是可以根据用户自己的意愿来划分不同的 VALN 口，系统中支持 VLAN1-VLAN15 这个 15 个 VLAN 口，但是时间的端口只有 5 个，其中 WAN 口一个，LAN 口 4 个，根据自己的需要划分，同时 LAN 口和 WAN 口不能划分为同一个 VLAN 口

3.3.1.6 网络



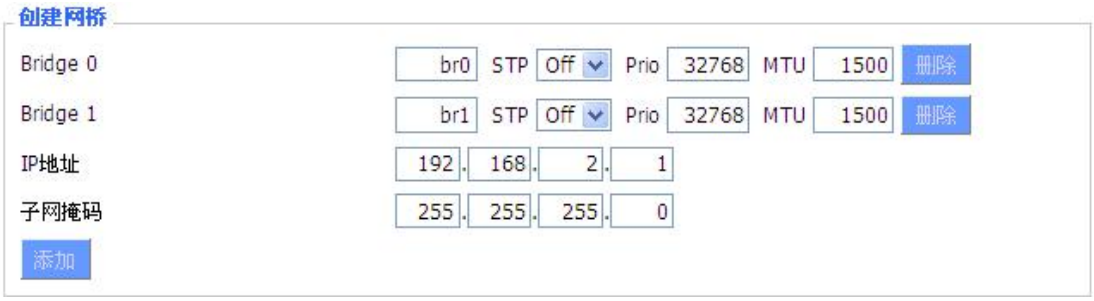
桥接中-创建网桥：创建一个新的网桥，供使用。 STP 是指生成树协议的缩写，你可以设置桥的优先顺序。最低的数字，具有最高的优先权。
桥接中-指派到网桥：允许您指定任何有效的接口到已经建立好的网桥中。
当前桥接列表：显示当前桥接列表

创建的步骤如下：

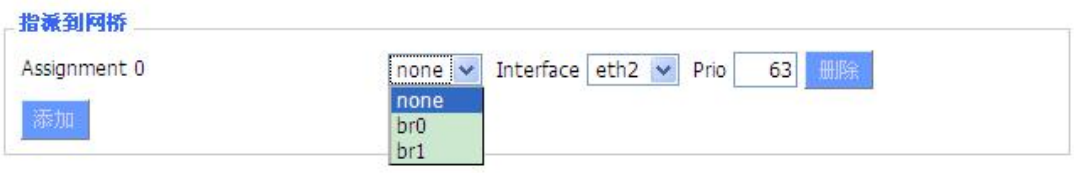
在创建网桥中先点击**添加**按钮，然后出现如下的配置



此项是创建网桥的选项，第一个 br0 代表网桥的名称，STP 代表是否开启生成树协议，Prio 代表生成树协议的优先等级，数字越小代表等级越高，MTU 代表最大传输单元。默认 1500，若不需要，则删除，然后点击保存或者应用，则出现如下所示的网桥属性配置：



输入相应的网桥的 IP 地址和子网掩码后，点击应用按钮，生成网桥。
注意：只有生成网桥后才可以应用网桥



此项是指派到网桥，可以把不同的接口指派到已经创建好的网桥中，如在 br1 的网桥中指派接口为 ra0 的接口（即无线接口），如下所示



其中 Prio 代表优先等级，若有多个接口绑定在同一个网桥中时就有用，值越小代表等级越高。点击应用使其生效。

注意：对应接口中出现的一些 WAN 口的接口，应该不予以绑定，此网桥功能基本是用于 LAN 口侧，不应与 WAN 口绑定。

若绑定成功，则在当前网桥列表中出现网桥的绑定列表，如下：



若要时 br1 的网桥也具有 DHCP 分配地址的功能，则需要设置多路 DHCP 功能，详见多路 DHCPD 的介绍：



端口配置：配置各个端口的属性，以下以一个 ra0 端口做说明



选择未桥接就可以设置端口自己的属性，详细的属性如下：

MTU：最大传输单元

组播转发：是否启用组播转发功能

Masquerade/NAT：是否启用 Masquerade/NAT

IP 地址：设置 ra0 的 IP 地址，不要与其他的端口或者网桥冲突

子网掩码：配置端口的子网掩码



多路 DHCPD：使用多路 DHCP 服务。在多路 DHCP 服务器中点击添加，即可出现相印的配置，其中第一个代表接口或者网桥的名称（不要配置成 eth0），第二个代表是否开启 DHCP 功能，Start 代表开始的地址是多少，Max 代表最多分配的 DHCP 客户端数，Leasetime 代表客户端租约时间，单位为分钟，设置好后点击保存或者应用按键使其生效，

注意：只能一个配置完后在点击保存，然后才可以配置下一个，而不能一次性多个 DHCP 同时设置

3.3.2 无线

3.3.2.1 基本配置



启用：开启 WIFI。

禁用：关闭 WIFI。

无线模式：AP、客户端、Ad-hoc、中继、中继桥接四种模式可选。

无线网络模式：

混合：同时支持 802.11b、802.11g、802.11n 标准的无线设备。

BG-混合：同时支持 802.11b、802.11g 标准的无线设备 。

仅 B：只支持 802.11b 标准的无线设备。

仅 G：只支持 802.11g 标准的无线设备。

NG-混合：同时支持 802.11g、802.11n 标准的无线设备。

仅 N：只支持 802.11n 标准的无线设备。

8021.11n 传输模式：在无线网络模式为”仅 N”时，选择传其传输模式:

绿地：当您确定，周围环境中，没有其它 802.11a/b/g 设备使用相同的频道，使用此模式或提高吞吐量。如果环境中有其它 802.11a/b/g 设备使用相同的频道，您发送的信息可能产生错误、重发等。

混合：此模式与绿地模式相反，但会减少吞吐量。

无线网络名(SSID):无线网络中所有设备共享的网络名称，所有设备的 SSID 是一致的。SSID 由数字和字母组成，区分大小写，不得超过 32 个字符。

无线频道：共有 1-13 频道可选择，在多个无线设备环境下，请尽量避免与其它设备使用相同的频道。

频道宽度：20MHZ 与 40MHZ 可供选择。

宽频：频道为 40MHZ 时，可选择 upper 或 lower.

无线 SSID 广播：

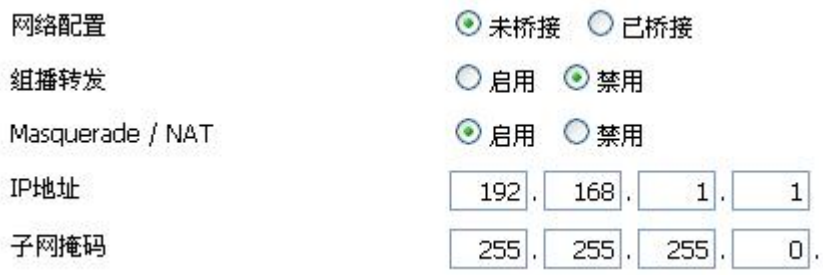
启用：广播 SSID。

禁用：隐藏 SSID。

网络配置：

已桥接：桥接到通信管理机上，一般情况下，请选择已桥接。

未桥接：没有桥接到通信管理机上，IP 地址需要手动配置。



虚拟接口：点击添加可添加一个虚拟接口。添加成功后，点击移除，可移除虚拟接口。



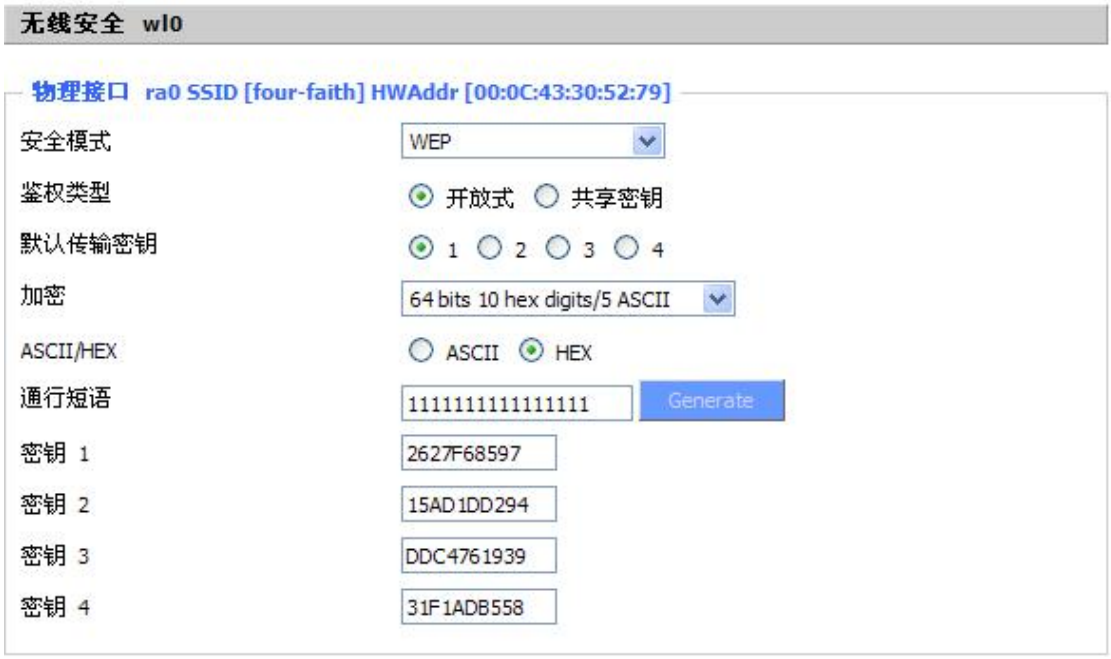
AP 独立：将所有的无线客户端设备完全隔离，使之只能访问 AP 连接的固定网络。

注意：保存设置：保存更改，在更改“无线模式”、“无线网络模式”、“无线宽度”、“宽频”选项后，请先点击此按键，再配置其它选项。

3.3.2.2 无线安全

无线安全选项用于对您的无线网络的安全性进行配置。本路由共有 7 种无线安全模式。默认禁用，不启用安全模式。如改变安全模式，请点击应用立即生效。





WEP：是一种基本的加密算法，安全性不如 WPA。

鉴权类型：可以选择开放式或共享密钥。

默认传输密钥：选择使用密钥 1-密钥 4 中的某一个为传输加密使用的密钥。

加密：有”64 bit 10 hex digits/5 ASCII”,”128 bit 26 hex digits/13 ASCII”。可利用通行短语生成或手动输入。

64 bit 10 hex digits/5 ASCII:每一个密钥为 10 位 16 进制的字符或者 5 位 ASCII 码字符。

128 bit 26 hex digits/13 ASCII: 每一个密钥为 26 位 10 进制的字符或者 13 位 ASCII 码字符。

ASCII/HEX: ASCII,选择密钥为 ASCII 码。

HEX，选择密钥为 16 进制数。

通行短语：用来生成密钥的字母和数字组合。

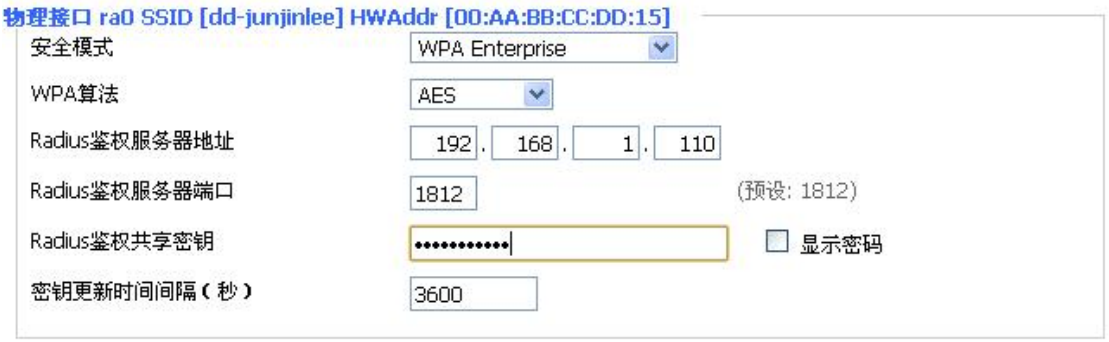
密钥 1-密钥 4：可以手动填写也可由通信管理机根据输入的通行短语生成。



WPA Personal/WPA2 Personal/WPA2 Person Mixed:提供三种 WPA 算法，TKIP 和 AES，TKIP+AES，采用动态加密密钥。TKIP+AES，自适用 TKIP 或 AES。WPA Person Mixed,允许 WPA Personal 和 WPA2 Personal 客户端混合。

WPA 共享密钥： 8-63 位字符，由字母和数字组成。

密钥更新时间间隔（秒）：1-99999。



WPA Enterprise/WPA2 Enterprise/WPA2 Enterprise Mixed：企业 WPA/WPA2 加密，通信管理机需连接 Radius 验证服务器。

WPA 算法:AES/TKIP/TPIP+AES。

Radius 鉴权服务器地址：连接到通信管理机的 Radius 服务器 IP。

Radius 鉴权服务器端口：Radius 服务器上，radius 服务使用的端口。

Radius 鉴权共享密钥：Radius 服务器和通信管理机之间的共享密钥。

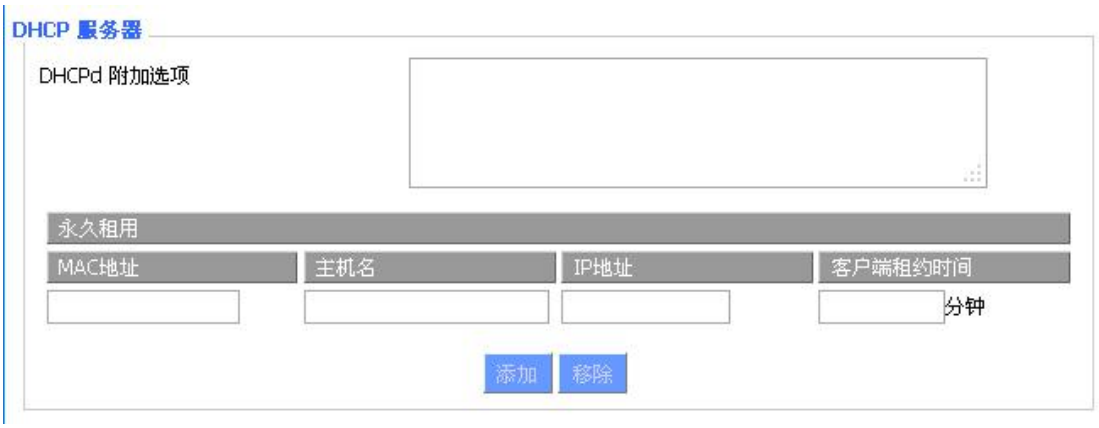
密钥更新时间间隔(秒): 1-99999。

3.3.3 服务

3.3.3.1 服务

DHCP 服务器

DHCP 服务是为你的本地设备分配 IP 地址的，你可以进入主菜单，然后到设置页面上配置你自己需要的一下 DHCP 的特殊功能



DNSMasq

DNSMasq 是本地 DNS 服务器。这将解决所有已知的主机从 DHCP（动态和静态）的通信管

理机以及远程 DNS 服务器的转发和缓存的 DNS 条目的名称。本地的 DNS 使局域网上的 DHCP 客户端解决静态和动态 DHCP 主机名



本地 DNS：采用本地的 DNS，在设置页面中可以设置 DNS 服务器
No DNS Rebind: 启用时它可以防止让外部攻击者访问通信管理机内部 Web 的接口，是一种安全措施
DNSMasq 附加选项：可以设置有一些额外的选项，输入你自己的相应配置。
例如：

静态分配地址 ：dhcp-host=AB:CD:EF:11:22:33,192.168.0.10,myhost,myhost.domain,12h
最大的租约数量 ：dhcp-lease-max=2
DHCP 服务器的 IP 范围 ：dhcp-range=192.168.0.110,192.168.0.111,12h

SNMP

SNMP（简单网络管理协议）。这是一种应用广泛的网络管理协议。数据经由 SNMP 代理进行传递。SNMP 代理指的是硬件与/或软件进程，向工作站报告每一种网络设备（比如集线器、通信管理机以及桥接器等）的活动，从而达到对网络的监控目的。代理会返回 MIB（管理信息库）中所包含的信息。MIB 是一种数据结构，用于定义可以从设备得到的以及可以控制的（比如打开或关闭）选项。



位置：设备所在的位置标识，由客户自定义
联系：用户定义，应与客户端一致
名称：用户定义，应与客户端一致
只读团体字：用户定义，应与客户端一致，只有读权限
读写团体字：用户定义，应与客户端一致，具有读写权限

SSHD

启用 SSHD 服务后就允许通过 SSH 客户端通过远程访问你的通信管理机的操作系统



SSH TCP 转发: 是否支持 TCP 转发功能
密码登录: 是否需要密码登录
端口：设置 SSHD 的端口，默认系统设置成 22 端口
授权密钥：根据需要设定，默认使用系统的登录密码和用户名

系统日志



输出模式：网络与串口，网络方式时需要设置远程服务器 IP 地址
远程服务器：接受系统日志的远程服务器 IP 地址

Telnet

这是一种终端模拟协议，通常用于 Internet 以及基于 TCP/IP 的网络。它可以允许终端用户或计算机登录到远程设备并进行程序运行。



Telnet：启用或禁用 Telnet 功能

WAN 流量计数器



Ttraff 守护进程：启用或者禁用流量统计功能

3.3.4 VPN

3.3.4.1 PPTP

PPTP 服务器



广播支持：开启或禁用 PPTP 服务器支持广播功能
强制 MPPE 加密：是否要强制 PPTP 数据 MPPE 加密
DNS1，DNS2，WINS1，WINS2：设置你的第一 DNS，第二 DNS，第一 WINS，第二 WINS
服务器 IP：输入通信管理机作为 PPTP 服务器的 IP 地址，应与 LAN 地址不一样。
客户端 IP：分配给客户端的 IP 地址，格式为 **xxx.xxx.xxx.xxx-xxx**
CHAP Secrets：客户端使用 PPTP 服务时的用户名和密码
注意：客户端 IP 不能和通信管理机 DHCP 分配的 IP 重复，只要是这个范围以外的都可以。
CHAP Secrets 格式为 user 空格*空格 password 空格*

PPTP 客户端



服务器 IP 或 DNS 名称：PPTP 服务器的 IP 地址或者对应的 DNS 名称
远程子网：远程 PPTP 服务器的内网
远程子网掩码：远程 PPTP 服务器的子网掩码
MPPE 加密：是否支持 MPPE 加密。
MTU：最大传输单元 0-1500
MRU：最大接收单元 0-1500
NAT：启用或者禁用 NAT 穿越
用户名：PPTP 服务器所允许的用户名
密码：PPTP 服务器所允许的用户名对应的密码

3.3.4.2 L2TP

L2TP 服务器



强制 MPPE 加密：是否要强制 L2TP 数据 MPPE 加密
服务器 IP：输入通信管理机作为 L2TP 服务器的 IP 地址，应与 LAN 地址不一样。
客户端 IP：分配给客户端的 IP 地址，格式为 **xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx**
CHAP Secrets：客户端使用 L2TP 服务时的用户名和密码
注意：客户端 IP 不能和通信管理机 DHCP 分配的 IP 重复，只要是这个范围以外的都可以。
CHAP Secrets 格式为 user 空格*空格 password 空格*

L2TP 客户端



L2TP 服务器：L2TP 服务器的 IP 地址或对应的 DNS 名称
远程子网：L2TP 服务器内网所属的网络
远程子网掩码：L2TP 服务器内网所属的网络掩码
MPPE 加密：是否支持 MPPE 加密。
MTU：最大传输单元 0-1500
MRU：最大接收单元 0-1500
NAT：启用或者禁用 NAT 穿越
用户名：L2TP 服务器所允许的用户名
密码：L2TP 服务器所允许的用户名对应的密码
允许 CHAP 认证协议：是否支持 chap 认证
拒绝 PAP 认证协议：是否拒绝支持 pap 认证
允许认证协议：是否支持认证协议

3.3.4.3 OPENVPN

OPENVPN 服务端



启动类型：WAN Up---上线后启用，System---开机启用



配置途径：GUI---界面配置，Config File---配置文件配置
服务器模式：通信管理机---路由模式，Bridge---网桥模式

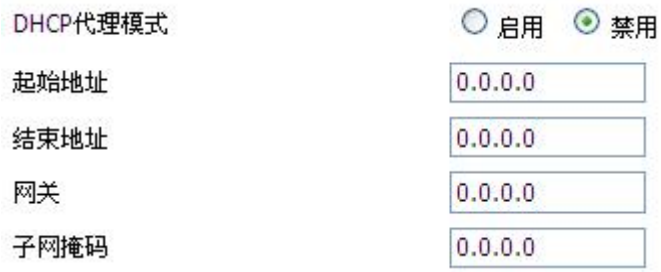
Route 方式：



网络地址：OPENVPN 服务端允许的网络地址

子网掩码：OPENVPN 服务端允许的子网掩码

网桥模式：



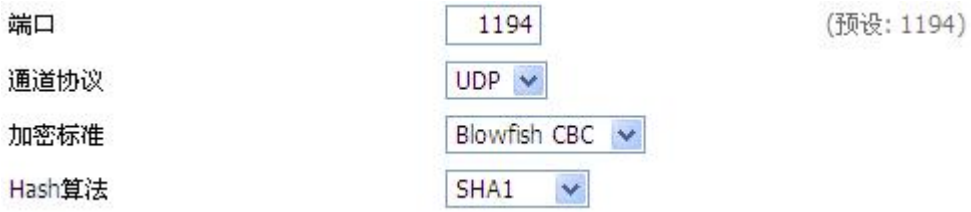
DHCP 代理模式：启用或禁用 DHCP 代理模式

起始地址：OPENVPN 服务端允许客户端的起始地址

结束地址：OPENVPN 服务端允许客户端的结束地址

网关：OPENVPN 服务端允许客户端的网关

子网掩码：OPENVPN 服务端的允许客户端子网掩码



端口：OPENVPN 服务器的监听端口

通道协议：OPENVPN 的通道协议 UDP 或 TCP

加密标准：通道的加密标准包括：Blowfish CBC，AES-128 CBC，AES-192 CBC，AES-256 CBC，AES-512 CBC 五种加密

Hash 算法：Hash 算法提供了一种快速存取数据的方法，包括 SHA1，SHA256，SHA512，MD5 四种算法

高级选项



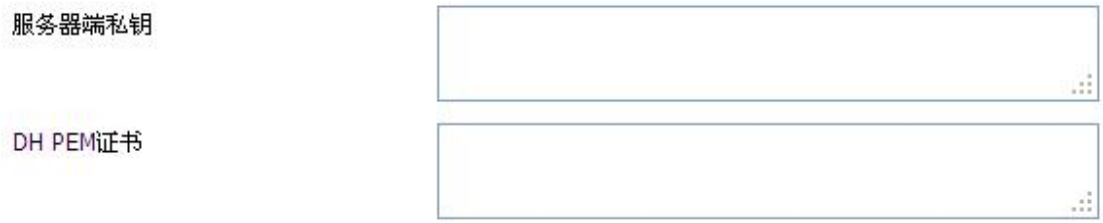
使用 LZO 压缩：启用或禁用传输数据使用 LZO 压缩
重定位默认网关：启用或禁用重定位网关
允许客户端到客户端：启用或禁用允许客户端到客户端
允许重复 CN：启用或禁用允许重复 CN
TUN MTU 设置：设置通道的 MTU 值
TCP MSS：TCP 数据的最大分段大小
TLS 加密标准：TLS（安全传输层协议）加密标准支持 AES-128 SHA 和 AES-256 SHA
客户端连接脚本：自行定义的一些客户端脚本



公共服 CA 证书：服务器和客户端公共的 CA 证书



公共的服务器端证书：服务器端的证书

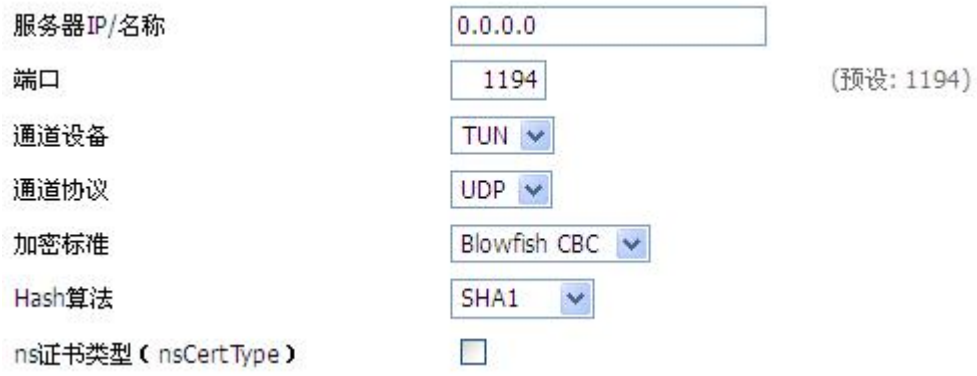


服务器端私钥：服务器端设置的密钥
DH PEM 证书：服务端的 PEM 证书



额外的配置：服务器其他额外配置
CCD 路径默认文件：其他的文件途径
TLS 认证密钥：安全传输层的认证密钥
证书撤销列表：配置一些撤销的证书列表

OPENVPN 客户端



服务器 IP / 名称：OPENVPN 服务器的 IP 地址或域名
端口：OPENVPN 客户端的监听端口
通道设备：TUN---路由模，式 TAP---网桥模式
通道协议：UDP 和 TCP 协议
加密标准：通道的加密标准包括：Blowfish CBC，AES-128 CBC，AES-192 CBC，AES-256 CBC，AES-512 CBC 五种加密
Hash 算法：Hash 算法提供了一种快速存取数据的方法，包括 SHA1，SHA256，SHA512，MD5 四种算法
ns 证书类型：是否支持 ns 证书类型



使用 LZO 压缩：启用或禁用传输数据使用 LZO 压缩
NAT：启用或禁用 NAT 穿越功能
TAP 绑定到 br0 网桥上：启用或禁用 TAP 绑定到 br0 网桥上
本地 IP 地址：设置本地 OPENVN 客户端的 IP 地址
TUN MTU 设置：设置通道的 MTU 值
TCP MSS：TCP 数据的最大分段大小
TLS 加密标准：TLS（安全传输层协议）加密标准支持 AES-128 SHA 和 AES-256 SHA
TLS 认证密钥：安全传输层的认证密钥
额外的配置：OPENVPN 服务器其他额外配置
基于路由策略：输入自定义的一些路由策略



公共服 CA 证书：服务器和客户端公共的 CA 证书
公共客户端证书：客户端证书
客户端私钥：客户端的密钥

3.3.4.4 IPSEC

连接状态及操作

在 IPSEC 页面，会显示当前设备具有的 IPSEC 连接及其状态。



名称：IPSEC 连接的名称；
类型：当前 IPSEC 连接的类型及功能；
通用名称：当前连接的本端子网、本端地址、对端地址及对端子网；
状态：连接所处的状态，总共三种，分别为关闭、协商中及建立；
关闭：该条连接未向对端发起连接请求；
协商中：该条连接已向对端发起请求，并处在协商过程中，连接仍未建立；
建立：连接已经建立，已能使用该通道。
操作：可以对该连接进行的操作，目前有四种，分别为删除、编辑、重连接及使能。
删除：该操作将删除连接，如果 IPSEC 通道已建立，亦将被拆除；
编辑：修改该条连接的配置信息，修改之后，如果要使配置生效，需重新加载该连接；
重连接：该操作将拆除当前通道，重新发起通道建立请求；
使能：当连接处于使能状态时，系统重启或进行重连接操作时，该连接将发起通道建立请求；而相反的，将不会发起请求。
添加：该功能用于新添一条 IPSEC 连接。

添加 IPSEC 连接或编辑 IPSEC 连接

类型：在该栏目对 IPSEC 模式及对应的功能进行选择，目前支持隧道模式的客户端功能、隧道模式的服务器功能及传输模式。



连接配置：该栏目包含了通道的基本地址信息。



名称：用以标示该连接的名称，须唯一；
启用：选择启用，则该条连接在系统起机或者进行重连接操作的时候，将发起通道连接请求；否则不会；
本机的 WAN 接口：通道的本端地址；
远程主机地址：对端的 IP/域名。如果采用了隧道模式的服务端功能，则该选项不可填；

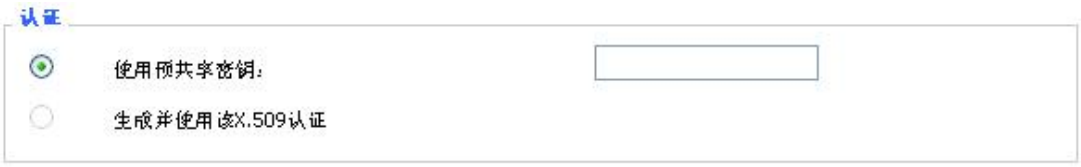
本地子网：IPSec 本地保护子网及子网掩码，例如：192.168.1.0/24；如果采用传输模式，则该选项不可填写；
远程子网：IPSec 对端保护子网及子网掩码，例如：192.168.7.0/24；如果采用传输模式，则该选项不可填写；
本地主机标识符：通道本端标识，可以为 IP 及域名；
远程主机标识符：通道对端标识，可以为 IP 及域名。
检测：该栏目包含了连接检测（DPD）的配置信息。



启用 DPD 检测：是否启用该功能，打钩表示启用；
时间间隔：设置连接检测（DPD）的时间间隔；
超时时间：设置连接检测（DPD）超时时间；
操作：设置连接检测的操作。
高级配置：该栏目包含了 IKE、ESP 以及协商模式等相关配置。



启用高级配置：启用，则可以配置第一阶段及第二阶段的信息，否则，将根据对端自动协商；
IKE 加密：IKE 阶段的加密方式；
IKE 完整性：IKE 阶段的完整性方案；
IKE DH 小组：DH 交换算法；
IKE 生命周期：设置 IKE 的生命周期，目前以小时为单位，默认为 0；
ESP 加密：ESP 的加密方式；
ESP 完整性：ESP 完整性方案；
ESP 生命周期：设置 ESP 的生命周期，目前以小时为单位，默认为 0；
采用野蛮模式：如果打钩，则协商模式将采用野蛮模式，否则为主模式；
会话密钥向前加密：如果打钩，则启用 PFS，否则不启用；
认证方式：可以根据需要选择共享密钥或者证书认证，目前仅能选择共享密钥方式。



3.3.4.5 GRE

GRE（Generic Routing Encapsulation，通用路由封装）协议是对某些网络层协议（如 IP 和 IPX）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议（如 IP）中传输。GRE 采用了 Tunnel（隧道）技术，是 VPN（Virtual Private Network）的第三层隧道协议。



GRE 隧道：启用或者禁用 GRE 功能



通道：可设置的通道，目前最多可以设置 12 条 GRE 隧道
状态：启用代表启用当前配置的 GRE 隧道，否则代表关闭当前 GRE 隧道
名称：隧道的名称最长 30 个字符
通过：GRE 收发接口，目前有 LAN 口，和 PPP 拨号口
对端 WAN IP：输入对端 GRE 的 WAN 口 IP 地址
对端子网：GRE 对端的子网 IP，如：192.168.1.0/24
对端隧道 IP：对端的 GRE 隧道 IP
本段隧道 IP：本地 GRE 隧道 IP 地址
本端子网掩码：本地子网掩码



保活：开启/关闭 GRE 保活
重拨次数：GRE 保活失败最大次数
重拨间隔：GRE 保活包发送间隔
失败策略：保活失败策略

点击“查看 GRE 隧道”按键可以查看 GRE 的信息



3.3.5 安全

3.3.5.1 防火墙

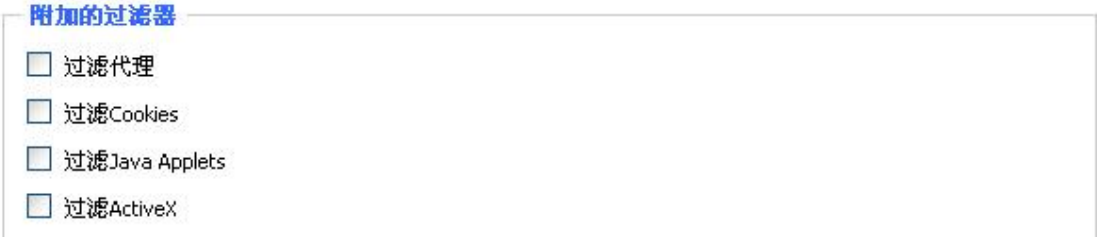
您可以启用或禁用防火墙，选择过滤特定的 Internet 数据类型，以及阻止匿名 Internet 请求，通过这些增强网络的安全性。

防火墙保护



防火墙增强网络安全性并使用状态监测（SPI）对进入网络的数据包进行检查，要使用防火墙保护，选择启用，否则禁用。只有启用了 SPI 防火墙，才能使用其他的防火墙功能：过滤代理、阻止 WAN 请求等。

其他过滤器



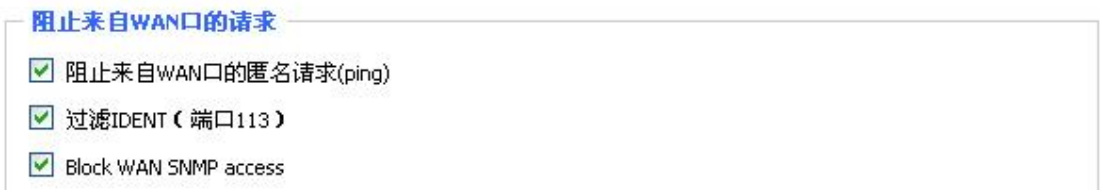
过滤代理：使用 wan 代理服务器可能降低网关的安全性，过滤 Proxy 将拒绝任意对任意 wan 代理服务器的访问，单击该复选框启用 Proxy 过滤或反选以禁用该功能。

过滤 Cookies：Cookies 是 Web 网站保存在您电脑上的数据，当您和 Internet 站点交互的时候就会使用到 Cookie。单击该复选框启用 cookies 过滤或反选以禁用该功能。

过滤 Java Applets：如果拒绝 Java，则可能无法打开使用 Java 工具编程的网页，单击该复选框启用 Java 小程序过滤或反选以禁用该功能。

过滤 ActiveX：如果拒绝 ActiveX，则可能无法打开使用 ActiveX 工具编程的网页，单击该复选框启用 ActiveX 过滤或反选以禁用该功能。

阻止 WAN 请求



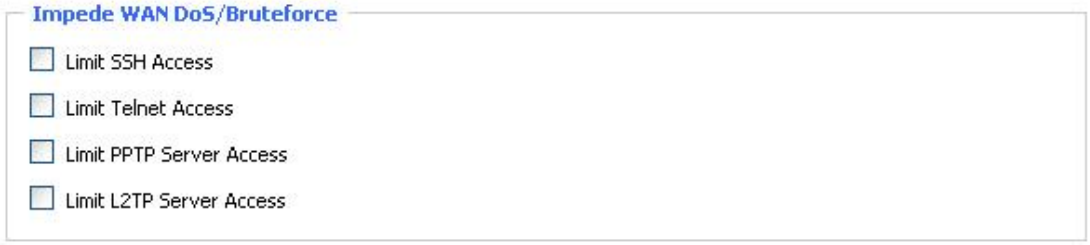
阻止来自 WAN 口的匿名请求（ping）：通过选中“阻止匿名 Internet”请求旁的选项框，启用该功能，从而防止您的网络遭受其他 Internet 用户的 Ping 或者探测，使外部用户更加难以侵入您的网络，这一功能的默认状态为启用，选择禁用可以允许匿名 Internet 请求。

过滤 IDENT(端口 113)：这一功能可以使 113 端口免于被您的本地网络之外的设备进行扫描。选择启用来对 113 端口进行过滤，或是反选禁用这一功能。

阻止 SNMP 访问：这一功能阻止来自广域网的 SNMP 连接请求。

完成修改后，单击“**保存设置**”，保存所作更改，或是“**取消改动**”，取消所作更改。

Impede WAN DoS/Bruteforce



Limit SSH Access：该功能限制了来自广域网的 SSH 访问请求，对同一个 IP 每分钟最多接受 2 个 SSH 连接请求。

Limit Telnet Access：该功能限制了来自广域网的 Telnet 访问请求，对同一个 IP,每分钟最多接受 2 个 Telnet 连接请求。

Limit PPTP Server Access：当设备建立了 PPTP 服务器，该功能限制了来自广域网的 PPTP 访问请求，对同一个 IP,每分钟最多接受 2 个 PPTP 连接请求。

Limit L2TP Server Access：当设备建立了 L2TP 服务器，该功能限制了来自广域网的 L2TP 访问请求，对同一个 IP,每分钟最多接受 2 个 L2TP 连接请求。

日志管理

通信管理机可以保存您的所有 Internet 连接的日志，包括连入和连出。

日志



为了保持日志活动，选择“启用”，要停止记录，选择“禁用”。 当选择启用的时候，将会出现下面的选择页面。

日志等级：设置“日志级别”，更高的级别会记录更多的日志。

选项



当以上 3 项各自选择启用的时候，对应的连接会被记录在日志里，禁用则不记录。

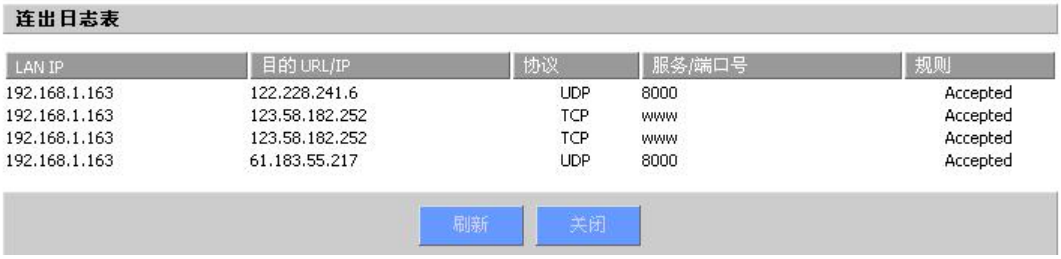
连入日志

要看到通信管理机的最近期的传入的临时日志，单击“连入日志”按钮。



连出日志

要看到通信管理机的最近期的传入的临时日志，单击“连出日志”按钮。



3.3.6 访问限制

3.3.6.1 WAN 访问

使用 Internet 访问页面可以阻止或允许特定类型的 Internet 应用，您可以设置特定 PC 的 Internet 访问策略。



默认策略规则中有“过滤”和“拒绝”两种选项，如果选择“拒绝”，将拒绝特定的电脑在特定时间段访问任何互联网服务；如果选择“过滤”，将阻止特定电脑在特定时间段对特定的网站的访问；您可以设置 10 条 Internet 访问策略过滤特定的 PC 在特定时间段访问的 Internet 服务。

策略：您最多可以定义 10 条访问策略。点击“删除”钮删除一条策略，或者点击摘要按钮察看策略综述。

状态：启用或禁用一条策略。

策略名称：您应该为您的策略指定一个名称。

PCs：该栏目用于编辑客户端列表，策略只对处在该列表中的 PC 有效。



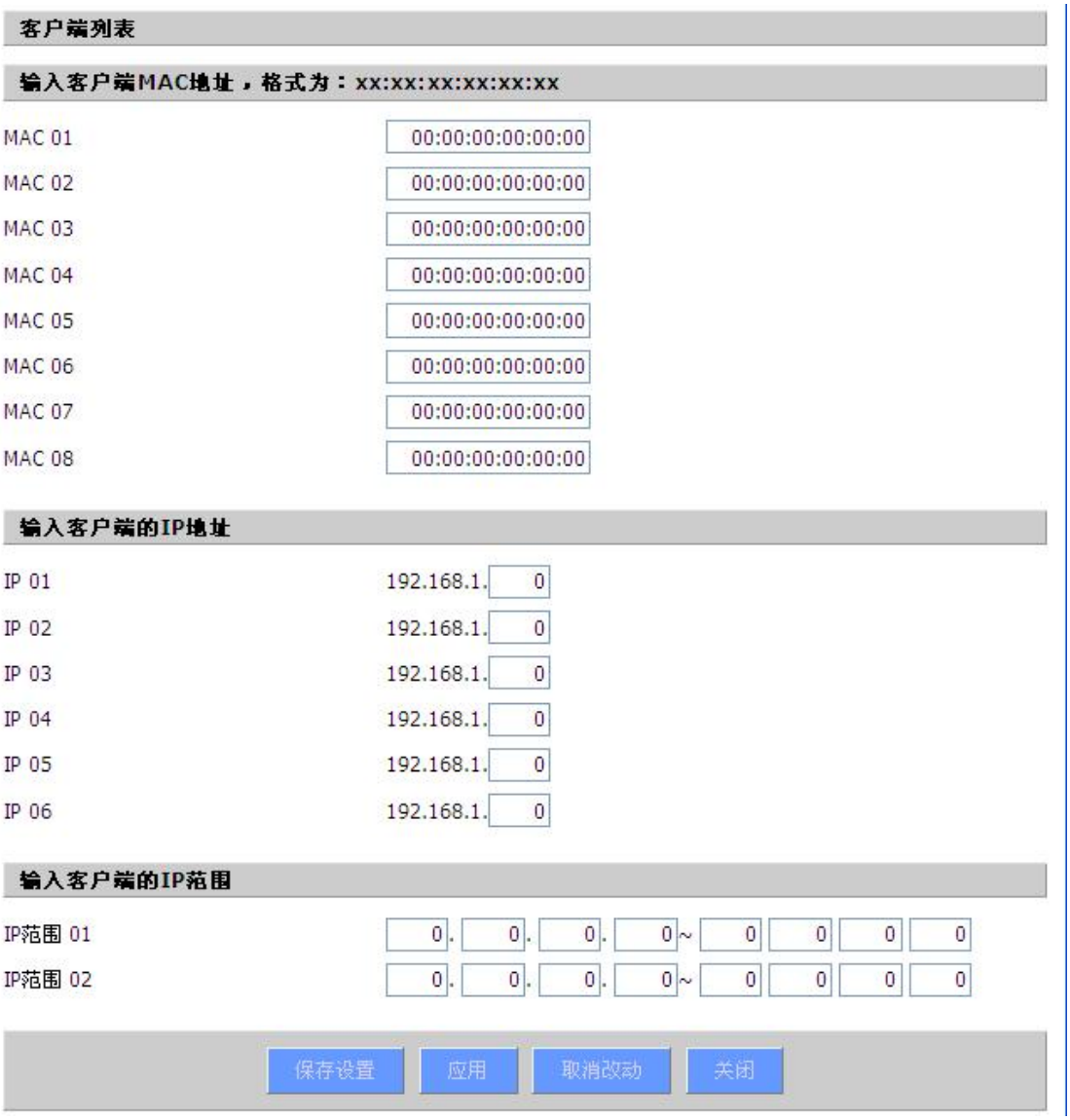
天：请选择您希望您的策略被应用的日期。

时间 ：输入您希望您的策略被应用的时间。



通过 URL 地址封锁 Web 站点：您可以通过输入的 URL 来封锁对部分网站的访问。

通过关键字封锁 Web 站点：您可以通过包含在 Web 页面中的关键字来封锁对其的访问。



创建 Internet 访问策略

1. 从“Internet 访问策略”下拉菜单中选择一条。
2. 如欲启用这一策略，单击“启用“旁边的单选按钮。
3. 在所提供的字段中输入策略名称。
4. 单击“编辑 PC 列表”按钮，出现“PC 列表”页面，输入应用该策略的 PC，可以使用 MAC 地址或者 PC 地址来指定 PC。如果您希望这一策略应用到一组 PC，则可以输入一组 IP 地址范围，完成页面修改后，单击“保存设置”，保存所作的修改，或是单击“取消改动”修改，完成修改后关闭这一窗口。
5. 确定这条策略生效的时间。选择这一策略生效的具体日期或是选择“每天”，之后输入这一策略生效的具体时段范围，或选择“24 小时”。
6. 如果拒绝或只允许访问特定 URL 地址的网站，则在“网站 URL 地址”旁边的单独字段内输入每一个 URL 地址。
7. 如果欲拒绝或只允许访问带特定关键字的网站，则在“网站关键字“旁白的单独字段内输入每一个关键字。

8. 单击“保存设置”按钮来保存对策略的社会子，如欲取消对策略的设置，则单击“取消改动”按钮。

注意

1. 默认策略规则出厂值为“过滤”，如果用户选择默认策略规则为“拒绝”，编辑相关策略保存或者直接保存设置。如果您编辑的策略是第一条，保存后会自动变成第二条，如果不是第一条，则按原编号保存。
2. 通信管理机本身没有电池保持时钟运行，关闭通信管理机电源或通信管理机重启会导致通信管理机时钟暂时失效，通信管理机失效后，如不能自动同步 NTP 时间服务器，则需要重新校正时间以确保相关“按时段控制”功能正确执行。

3.3.6.2 URL 过滤

如果想阻止某些客户端访问特定的外网域名，例如 www.sina.com。可以通过 URL 过滤功能实现。

URL 过滤功能



只接受符合以下规则的网址：只允许访问匹配的 URL 地址。

丢弃符合以下规则的网址：只接收符合自定义规则的网络地址，丢弃所有其他的 URL 地址。

3.3.6.3 数据流过滤

如果想阻止某些数据包通过通信管理机进入 Internet，或者阻止来自 Internet 的某些数据包，可以通过过滤器实现。

数据包过滤



启用包过滤：是否开启包过滤功能。

策略

丢弃符合以下规则的数据包：丢弃匹配自定义规则的数据包，接收所有其他的数据包。

只接收符合以下规则的数据包：只接收符合自定义规则的数据包，丢弃所有其他的数据包。

删除	源地址	源端口	目的地址	目的端口	协议	方向
☐	0.0.0.0/0	1-- 65535	0.0.0.0/0	1-- 65535	tcp	output

自定义包过滤规则列表会列出已经设定的包过滤规则。如果要删除其中某一项，选中对应项，并勾选“删除”按钮，然后在点击“保存”按钮。



添加过滤规则

添加自定义的包过滤规则。"源端口"， " 目的端口"， " 源地址"， " 目的地址" 必须至少填写一项。

方向

Input：数据包从 WAN 口到 LAN 口 。

Outpu：数据包从 LAN 口到 WAN 口 。

协议：数据包的协议类型。

源端口：数据包的源端口。

目的端口：数据包的目的端口。

源地址：数据包的源 IP 地址。

目的地址：数据包的目的 IP 地址。

3.3.7 NAT

3.3.7.1 端口转发

端口转发用于设置网络上的公共服务，如 web 服务器、ftp 服务器或其他专用的 internet 应用（专用的 Internet 应用程序指使用 internet 访问来使用功能的任何应用程序）。



应用程序：在应用程序提供的字段内输入应用程序的名字。
协议：为每一种应用选择 UDP 或者 TCP 协议 ，两者为同时时选择两种协议。
允许的源 IP 范围：在该栏填入 Internet 用户的 IP 地址。
来源端口：在该栏填入由服务所使用的外部端口编号。
IP 地址：输入您想让 internet 用户访问的服务器的内网 IP 地址。
目的端口：在该栏输入服务所使用的内部端口编号。
启用：选择“启用”框，启用您所定义的多端口转发服务。缺省配置为禁用（未选择）。

完成页面修改后，单击“**保存设置**”按钮，保存所作的修改，或是单击“**取消改动**”键来取消修改，帮助信息位于右侧，详细信息，点击“**更多**”。

3.3.7.2 端口范围转发

某些应用程序可能要求转发特定的端口范围才能正常运行，当从 Internet 发出对某个端口范围的请求时，通信管理机会将这些数据发送到指定的计算机。出于安全考虑，可能要将端口转发仅限制在正在使用的那些端口上，如果不再使用该端口转发，建议取消“启用”复选框暂时禁用该端口转发。



应用程序：在应用程序提供的字段内输入应用程序的名字；
开始：输入端口转发范围的开始端口号；
结束：输入端口转发范围的结束端口号；
协议：为每一种应用选择 UDP 或者 TCP 协议 ，两者为同时时选择两种协议；
IP 地址：输入您想让 Internet 用户访问的服务器的内网 IP 地址。
启用：选择“启用”框，启用您所定义的多端口转发服务。缺省配置为禁用（未选择）。

完成页面修改后，单击“**保存设置**”按钮，保存所作的修改，或是单击“**取消改动**”键来取消修改，帮助信息位于右侧，详细信息，点击“**更多**”。

3.3.7.3 DMZ

DMZ 功能允许一个网络用户暴露于 Internet，从而使用特定服务。DMZ 主机同时向一台电脑转发所有的端口，因为只有您想要的端口被打开，所以端口转发更为安全，而 DMZ 主机则打开所有的端口，使计算机暴露于 Internet。



要想启用 DMZ 功能，选择启用，之后在“DMZ 主机 IP 地址”字段输入计算机的 IP 地址。

完成页面修改后，单击“**保存设置**”按钮，保存所作的修改，或是单击“**取消改动**”键来取消修改，帮助信息位于右侧，详细信息，点击“**更多**”。

3.3.8 QoS 设置

3.3.8.1 基本

使用 QOS 功能可以分别限制上传和下载的流量，并且可以为特定的 iP 或者 MAC 分配优先级。



上传（kbps）：该栏目填入你分配给上传的带宽，在实际使用中，一般为你所拥有的最大带宽的 80%到 90%。

下载（kbps）：该栏目填入你分配给下载的带宽，在实际使用中，一般为您所拥有的最大带宽的 80%到 90%。

3.3.8.2 分类

Netmask 优先顺序



您可以为一个给定的 IP 地址或者 IP 范围的所有流量指定优先顺序。

优先级说明：本系统提供了五种优先级，其中“不受限”优先级独立于其他四种优先级之外，其他四种优先级分别为：高优先级（Premium）、优先（Express）、标准（Standard）、低（Bulk）。

不受限：处在不受限（Exempt）级别的数据流，其带宽只受限于硬件，不受限的带宽和其他四种优先级的关系如下所述：

设上传总带宽为Max_Up，下载总带宽为Max_Down，“QOS 设置”中的上传限制为Uplink，下载限制为 Downlink,不受限的数据流的流量速率为 Exempt_Rate_Up 和 Exempt_Rate_Do。

则其他优先级总上传带宽为：mini(Max _Up– Exempt_Rate_Up，Uplink)；

其他优先级总下载带宽为：mini(Max _Downlink– Exempt_Rate_Do，Downlink)。

其余四种优先级

在不受限的数据流发送完成之后，系统剩余的带宽由其余四种优先级的数据流根据一定的比例分配，假设剩余的上传带宽为 1000kbps，下载 1000kbps，此时有四条数据流，其优先级分别为高优先级、优先、标准、低，那么各数据流的上传和下载带宽如下：

高优先级:（75/100） * Uplink ； （75/100） * Downlink

优先：（15/100）*Uplink ；（15/100） * Downlink

标准：（10/100）*Uplink ；（10/100） * Downlink

低：1000bit（几乎为 0）；1000bit（几乎为 0）；

对于低优先级，其上传下载速率均为 1000bit,当其他优先级的数据流发送完成了，才轮到它；当只有一种级别的数据流的时候，该数据流的带宽只受限于“QOS 设置”中的上传和下载限制；

注意：当某条连接同时符合 MAC 优先级和 netmask 优先级中的控制条件时，则以最先添加的那条规则为准。

3.3.9 应用

3.3.9.1 串口应用

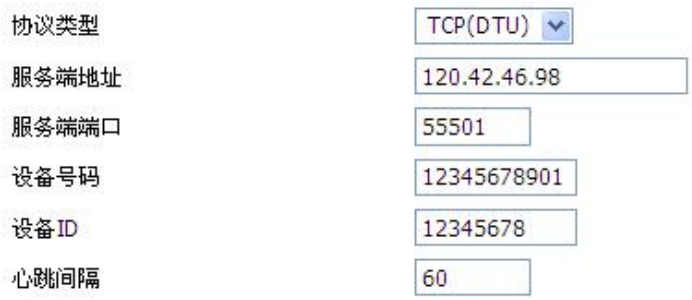
通常情况下通信管理机的 Console 口做控制台用。这个 Console 口也可以配置成普通串口使

用，通信管理机 内置了串口转 TCP/IP 程序。通过配置，通信管理机的 Console 口作为一个串口协

议转换设备，或者完全等同于一台四信 DTU 设备。



串口通信时的串口参数设置。



波特率：表示设备每秒传送的字节数，常用的波特率有 115200,57600,38400,19200 等。
数据位：数据位的个数可以是 4、5、6、7、8 等，构成一个字符。通常采用 ASCII 码。从最低位开始传送，靠时钟定位。
停止位：它是一个字符数据的结束标志。可以是 1 位、1.5 位、2 位的高电平。
检验：表示一组数据所采用的数据差错校验方式。有奇偶校验两种方式。
流控：包括硬件部分和软件部分两种方式。

协议类型
UDP(DTU)：串口转 UDP 连接，含自定义应用层协议，完全等同于一台四信 IP MODEM 的功能。
纯 UDP：标准的串口转 UDP 连接.
TCP(DTU)：串口转 TCP 连接，含自定义应用层协议，完全等同于一台四信 IP MODEM 的功能。
纯 TCP ：标准的串口转 TCP 连接.
TCP 服务器：标准的 TCP 服务器连接
TCST：自定义的 TCP 连接

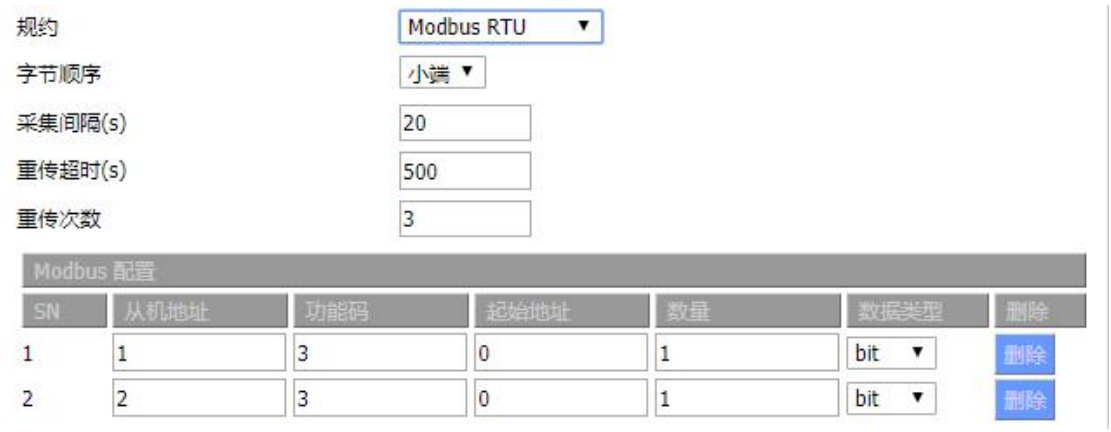
服务器地址：与通信管理机串口转 TCP 程序进行通信的数据服务中心的 IP 地址或者域名。
服务器端口：数据服务中心程序监听的端口。
设备号码： 设备的 ID 号，11 字节的数据字符串。只有当协议类型设置成“UDP(DTU)”或者“TCP(DTU)”的时候这个配置项才有效。
设备 ID： 8 个字节的数据字符串，只有当协议类型设置成“UDP(DTU)”或者“TCP(DTU)”的时候这个配置项才有效。
心跳时间间隔：心跳包的时间间隔，只有当协议类型设置成“UDP(DTU)” “TCP(DTU)”的时候这个配置项才有效。
自定义心跳包：心跳包

自定义注册包：注册包

3.3.9.2 通信网关应用



通道选择:选择需要使用的通道，每个通道可作为采集服务或者数据服务模式。
采集服务:从接入的设备采集信息。
数据服务:设备作为从机或者服务端提供被采集的信息。
规约：设备之间通讯所用到的协议。支持的协议有：modbus RTU,modbus ASCII，Modbus TCP,bacnet mstp,bacnet BIP,IEC101,IEC104.
端口：设备之间用到的通讯方式。目前支持的有串口，tcp/udp 协议。



Modbus 协议部分说明

从机地址：需要访问的设备地址。（0~255）

数据名称: 创建数据点，用于不同协议之间的相互转换。

读线圈(功能码为 1):根据数据域的每个比特将响应报文中的线圈分成为一个线圈。指示状态为 1= ON 和 0= OFF。第一个数据字节的 LSB（最低有效位）包括在询问中寻址的输出。其它线圈依次类推，一直到这个字节的高位端为止，并在后续字节中从低位到高位的顺序。如果返回的输出数量不是八的倍数，将用零填充最后数据字节中的剩余比特（一直到字节的高位端）。字节数量域说明了数据的完整字节数。

读离散量(功能码为 2):根据数据域的每个比特将响应报文中的离散量输入分成为一个输入。指示状态为 1= ON 和 0= OFF。第一个数据字节的 LSB（最低有效位）包括在询问中寻址的输入。其它输入依次类推，一直到这个字节的高位端为止，并在后续字节中从低位到高位的顺序。如果返回的输入数量不是八的倍数，将用零填充最后数据字节中的剩余比特（一直到字节的高位端）。字节数量域说明了数据的完整字节数。

读保持寄存器(功能码为 3:在一个远程设备中，使用该功能码读取保持寄存器连续块的内容。

读输入寄存器(功能码为 4):在一个远程设备中，使用该功能码读取输入寄存器连续块的内容。



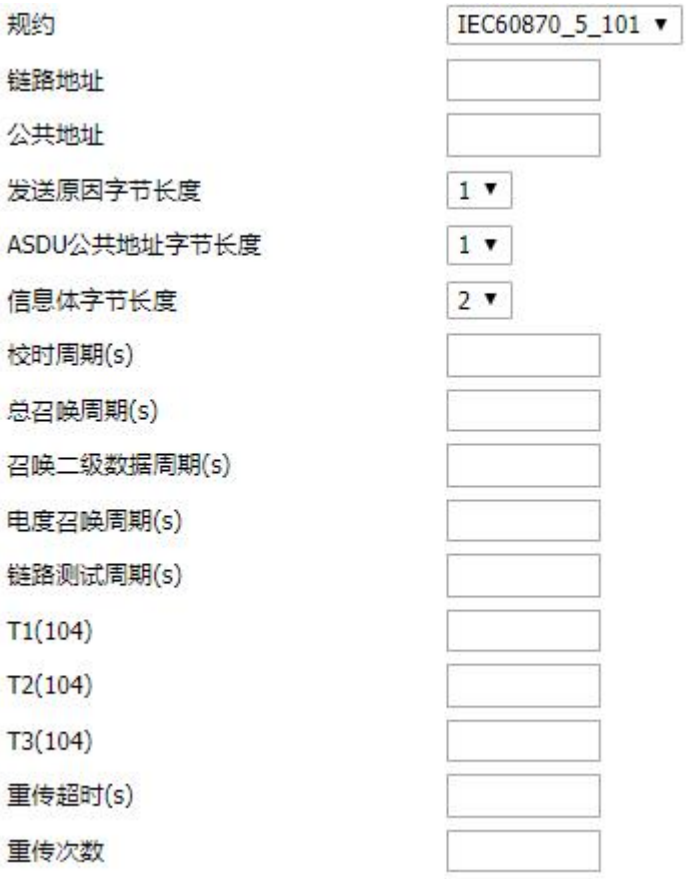
BACNET 协议部分说明

MSTP MAC:用于 bacnet 寻址的 MAC 地址。

设备地址：表示设备的编号。



IEC 电力协议部分说明



链路地址：用于设备寻址。
公共地址：与链路地址相同，为终端地址。
发送原因字节长度:101 协议一般为 1 个字节，104 协议一般为 2 个字节。
ASDU 公共地址字节长度:101 协议一般为 1 个字节，104 协议一般为 2 个字节。
信息体字节长度:101 协议一般为 2 个字节，104 协议一般为 3 个字节。
校时周期:主站与子站之间进行时钟同步的周期。
总召唤周期:召唤控制站在初始化完后,控制站必须获得现场设备的所有状态信号和所有的模拟量数据。
召唤二级数据周期:一般为循环发送的遥信遥测等.
电度召唤周期：定期获取数据累计量。
链路测试周期:链路没有数据交互时，需要定时发送链路测试报文用了检测链路是否断开。
T1:控制报文确认超时,发送测试帧。
T2:监控报文响应超时，发送 S 确认帧。
T3:长期空闲超时，发送测试帧。
重传超时:重复发送报文的超时时间。
重传次数：重新发送报文的次数。



设备管理:添加终端设备的配置项，可以配置以及查询，这些参数包括设备编号，设备地址，设备类型，遥信个数，遥控个数，要测个数，脉冲个数，遥信标志位，遥测标志位，脉冲标志位。

采集内容:创建数据点，并且与设备相关联。



端口部分说明

是否启用:控制串口是否启用。

使用串口：总共有四个串口可供使用。

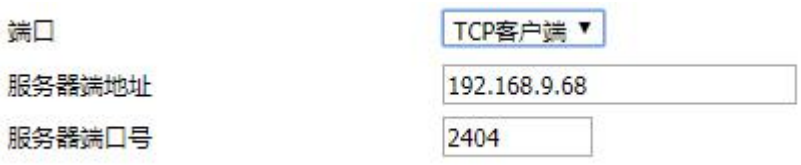
波特率：表示设备每秒传送的字节数，常用的波特率有 115200,57600,38400,19200 等。

数据位：数据位的个数可以是 4、5、6、7、8 等，构成一个字符。通常采用 ASCII 码。从最低位开始传送，靠时钟定位。

停止位：它是一个字符数据的结束标志。可以是 1 位、1.5 位、2 位的高电平。

检验:表示一组数据所采用的数据差错校验方式。有奇偶校验两种方式。

流控：包括硬件部分和软件部分两种方式。

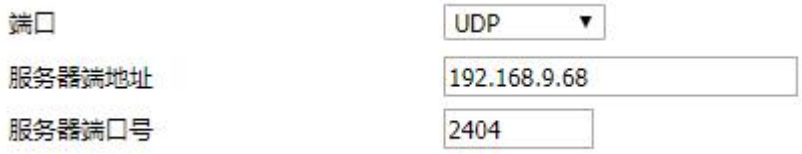


服务器端地址：与通信管理机串口转 TCP 程序进行通信的数据服务中心的 IP 地址或者域名。

服务器端口号：数据服务中心程序监听的端口。



监听端口：设备作为数据服务中心程序监听的端口。



UDP：标准的串口转 UDP 连接.

数据服务部分



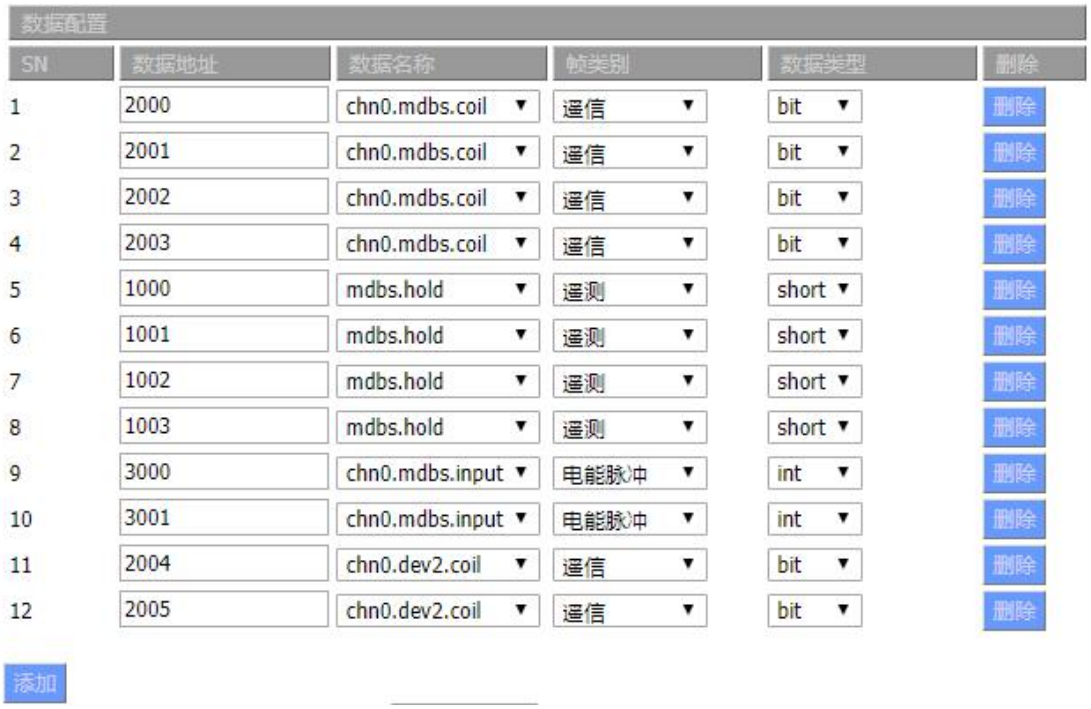
数据服务部分的配置项大致与采集部分相同，主要提供转发数据服务。

规约：设备之间通讯所用到的协议。支持的协议有：modbus RTU,modbus ASCII，Modbus TCP,bacnet mstp,bacnet BIP,IEC101,IEC104.

Modbus 协议部分

数据配置项：主要就是根据 Modbus 协议不同的功能码与数据点相关联。主要的配置项有数据地址(Modbus 起始地址)，数据名称（就是提供采集的点），功能码，数据类型。

IEC 协议部分



链路地址：用于设备寻址。
公共地址：与链路地址相同，为终端地址。
发送原因字节长度:101 协议一般为 1 个字节，104 协议一般为 2 个字节。
ASDU 公共地址字节长度:101 协议一般为 1 个字节，104 协议一般为 2 个字节。
信息体字节长度:101 协议一般为 2 个字节，104 协议一般为 3 个字节。
链路测试周期:链路没有数据交互时，需要定时发送链路测试报文用了检测链路是否断开。
T1:控制报文确认超时,发送测试帧。
T2:监控报文响应超时，发送 S 确认帧。
T3:长期空闲超时，发送测试帧。
数据配置:用于创建点表，配置信息体地址，关联转发数据以及配置帧类别，数据类型。

3.3.10 管理

3.3.10.1 管理

这一页面可以允许网络管理员管理特定的通信管理机功能，从而保证访问与安全。



新密码长度不得超过 32 个字符，不得包含任何空格。确认密码应该和你设置的新密码一致，

否则会设置不成功。

警告：

默认的用户名是：admin。

我们强烈建议您修改出厂的默认密码 admin，这样所有的用户试图访问和修改通信管理机都应该基于输入正确的通信管理机密码，才可以访问和使用。

Web 访问

此功能允许您使用 HTTP 协议或 HTTPS 协议来管理通信管理机。如果您选择禁用此功能，将需要手动重新启动。您还可以激活或禁用通信管理机的信息网页。那样就可以用密码保护此页（输入正确的用户名和密码）。



协议：web 页面支持的协议包括 HTTP 和 HTTPS

自动刷新（秒）：调整 Web 界面自动刷新时间间隔。0 表示关闭这个特性。

登入前显示系统信息网页：是否启用登入前显示系统信息网页

系统信息网页密码保护：是否启用系统信息网页密码保护功能



Web 界面管理：此功能允许您通过互联网从远程位置管理通信管理机。要禁用此功能，保持默认设置，就是禁用。要启用此功能，请选择启用，并使用电脑上的指定端口（默认是 8080），远程管理通信管理机。如果你还没有设置密码，您还必须为您自己的通信管理机设置的默认密码。

要远程管理通信管理机，进入 http://xxx.xxx.xxx.xxx:8080（x 代表的通信管理机的 Internet IP 地址，8080 代表指定的端口），在您的网页浏览器地址栏。你会被要求输入通信管理机的密码。

如果您使用 HTTPS，您需要指定 URL 为 https://xxx.xxx.xxx.xxx:8080（并非所有的固件都支持 SSL 的重建）

SSH 管理：您可以启用 SSH 来远程安全的访问通信管理机。请注意，想了解 SSH 守护进程的设置，可以在服务页面访问到更多内容。

警告：

如果远程通信管理机的访问功能被启用，任何人知道通信管理机的 Internet IP 地址和密码，将可以改变通信管理机的设置。

Telnet 管理：启用或禁用远程 Telnet 功能



Cron：cron 的子系统，是你计划要执行的 Linux 命令。你在实际使用中需要使用命令行或启动脚本。



语言：设置通信管理机页面显示的语言类型，包括简体中文和英文。



设备管理: 通过自定义开发的远程管理服务器对本台通信管理机进行监控管理、参数配置、WIFI 广告更新等。

3.3.10.2 保持活动

定时开关机



用户可以设置开机或者关机的时间:

设置 8:07 关机，9:07 开机，设置如下图所示。



定时重启



你可以设置定时重启路由：

定时 xxx 秒之后重启

在某一特定日期时间，星期或每天重启。

警告：

选择何时重新启动通信管理机。在管理标签中，Cron 选项必须被开启。

3.3.10.3 命令

指令：您可以通过 Web 界面运行命令行。将您的命令填入文本区域并且点击运行命令按钮提交



运行命令：您可以通过 Web 界面运行命令行。将您的命令填入文本区域并且点击运行命令按钮提交。

保存为启动指令：您可以保存启动通信管理机时在执行的某些命令行。输入命令（只有一个命令行）到文本区域，然后点击保存为启动指令。

保存为关机指令：您可以保存关闭通信管理机时在执行的某些命令行。输入命令（只有一个命令行）到文本区域，然后点击保存为关机指令。

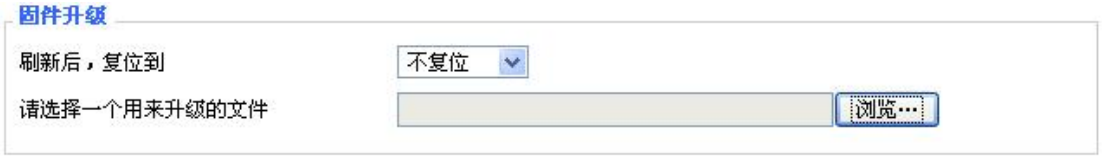
保存为防火墙指令：每次启动防火墙，它可以运行一些自定义的 iptables 指令。输入防火墙的命令（只有一个命令行）到文本区域，并点击保存为防火墙指令。
保存为自定义指令：自定义指令存储在/tmp/custom.sh 文件。您可以收到运行或使用 cron 来调用它。输入脚本的命令（只有一个命令行）到文本区域，并点击保存为自定义指令。

3.3.10.4 出厂默认



恢复出厂默认值 单击“**是**”按钮并保存设置，将所有配置清空恢复到出厂值。在恢复到默认设置时，您所做的所有设置都会丢失。这一功能的默认配置为“**否**”。 详细信息，请点击“**更多**”

3.3.10.5 固件升级



固件升级：可将新的固件加载到通信管理机上。新的固件版本将在 www.four- faith.com 上发布，并可免费进行下载。如果通信管理机没有出现问题，则无需下载更新的固件版本，除非新版本中包含您要使用的新增功能。
注意：在升级通信管理机的固件时，可能会丢失其配置设置，因此，请确保在升级固件之前，先备份好通信管理机的设置信息。
刷新后，复位到：如果你想在升级后重置通信管理机的固件版本默认设置，请按一下预设设置选项。
单击浏览，选择要升级的固件文件，再点击升级按钮开始固件升级。升级固件需要花费几分钟的时间，请不要关闭电源或按重置按钮。

3.3.10.6 备份

本页面用于对通信管理机的配置文件进行备份或恢复。



如欲对通信管理机的配置文件进行备份，请单击“**备份**”按钮。之后，请按照屏幕上的说明进行操作。

如欲恢复通信管理机的配置文件，单击“**浏览**”按钮，找到备份文件之后，请按照屏幕上的说明进行操作。选择好备份文件，单击“**恢复**”按钮。

3.3.11 状态

3.3.11.1 通信管理机



通信管理机名称：即此通信管理机的名称，可以在设置→基本设置中修改

通信管理机型号：即此通信管理机的型号，由系统固定生产，不可修改

固件版本： 软件的固件版本号，由系统固定产生，不可修改
MAC 地址： 反应了 WAN 的 MAC 地址，可以在设置→MAC 地址克隆中修改
主机名： 通信管理机的主机名，可以在设置→基本设置中修改
WAN 域名： WAN 口的域名，可以在设置→基本设置中修改
LAN 域名： LAN 口的域名，由系统固定产生，不可修改
当前时间： 系统的本地时间
运行时间： 系统上电开启的时间



所有可用： 所有可用 RAM 大小 （即物理内存减去一些预留位和内核的二进制代码大小）
空闲： 被系统留着未使用的内存，若内存小于 500kB 则会重启，
已使用： 已经使用的内存，所有的可用内存减去空闲内存
缓冲区： 即缓冲区使用的内存，总内存减去已经分配的内存即为缓冲区内存。
已缓存： 被高速缓冲存储器（cache memory）用的内存的大小
使用中： 活跃使用中的缓冲或高速缓冲存储器页面文件的大小
非使用中： 不经常使用中的缓冲或高速缓冲存储器页面文件的大小



IP 过滤器最大端口数： 预设 4096，可以在管理
活动的 IP 连接： 实时检测系统活动的 IP 连接数，若点击可以看到如下所示

活动的IP连接 91

序号	协议	超时(秒)	来源地址	远程地址	服务名称	状态
1	UDP	30	192.168.8.81	255.255.255.255	2654	UNREPLIED
2	UDP	42	192.168.8.81	255.255.255.255	2654	UNREPLIED
3	UDP	21	192.168.8.72	255.255.255.255	2654	UNREPLIED
4	UDP	15	192.168.8.81	255.255.255.255	2654	UNREPLIED
5	UDP	12	192.168.8.81	255.255.255.255	2654	UNREPLIED
6	UDP	27	192.168.8.72	255.255.255.255	2654	UNREPLIED
7	UDP	30	192.168.8.81	255.255.255.255	2654	UNREPLIED
8	TCP	8	192.168.1.120	192.168.1.1	80	CLOSE
9	UDP	3	192.168.8.81	255.255.255.255	2654	UNREPLIED
10	UDP	30	192.168.8.72	255.255.255.255	2654	UNREPLIED
11	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
12	UDP	24	192.168.8.81	255.255.255.255	2654	UNREPLIED
13	UDP	48	192.168.8.72	255.255.255.255	2654	UNREPLIED
14	UDP	15	192.168.8.81	255.255.255.255	2654	UNREPLIED
15	UDP	3	192.168.8.72	255.255.255.255	2654	UNREPLIED
16	UDP	6	192.168.8.72	255.255.255.255	2654	UNREPLIED
17	UDP	21	192.168.8.81	255.255.255.255	2654	UNREPLIED
18	UDP	51	192.168.8.81	255.255.255.255	2654	UNREPLIED
19	UDP	15	192.168.8.72	255.255.255.255	2654	UNREPLIED
20	UDP	45	192.168.8.81	255.255.255.255	2654	UNREPLIED
21	UDP	45	192.168.8.72	255.255.255.255	2654	UNREPLIED
22	UDP	42	192.168.8.81	255.255.255.255	2654	UNREPLIED
23	UDP	18	192.168.8.81	255.255.255.255	2654	UNREPLIED
24	UDP	9	192.168.8.72	255.255.255.255	2654	UNREPLIED
25	UDP	57	192.168.8.72	255.255.255.255	2654	UNREPLIED
26	UDP	27	192.168.8.81	255.255.255.255	2654	UNREPLIED
27	UDP	51	192.168.8.72	255.255.255.255	2654	UNREPLIED
28	UDP	18	192.168.8.81	255.255.255.255	2654	UNREPLIED

活动的 IP 连接：总的活动 IP 连接
协议：连接的协议
超时：连接的超时秒
来源地址：来源的 IP 地址
远程地址：远程的 IP 地址
服务名称：连接的服务端口号
状态：显示活动 IP 的详细状态

3.3.11.2 WAN

连接类型	自动配置 - DHCP
已连接时间	不可用

连接类型：包括 7 种方式：禁用，静态 IP，自动配置-DHCP，PPPOE，PPTP，L2TP，3G/UMTS。
已连接时间：已经连接上的时间，若没有连接上则问“不可用”

IP地址	0.0.0.0
子网掩码	0.0.0.0
网关	0.0.0.0
DNS 1	
DNS 2	
DNS 3	

IP 地址：通信管理机 WAN 口获取到的 IP 地址
子网掩码：通信管理机 WAN 口获取到的子网掩码
网关：通信管理机 WAN 口获取到的网关
DNS1，DNS2，DNS3：通信管理机 WAN 口获取到的第一 DNS，第二 DNS，第三 DNS



租约剩余时间：DHCP 方式下占用获取到 IP 地址的剩余时间
DHCP 释放：释放 DHCP 地址
DHCP 续期：续期 DHCP 方式获取到的 IP 地址，默认续期为 1 天



登录状态：WAN 口的连接状态
断开连接：断开已经连接的状态
连接：连接已经断开的状态



模块类型：3G/UMTS 方式时的模块类型
信号强度：3G/UMTS 方式时的模块模块信号强度
网络类型：3G/UMTS 方式时的模块的网络类型

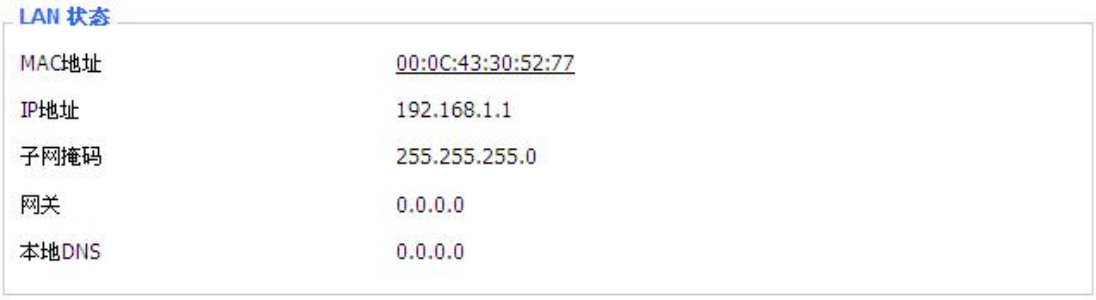


总流量：统计上一次断电到现在使用的流量分为下载和上传两个方向
月流量：一个月统计的流量单位的 MB
上月：查看上个月流量
下月：查看下个月流量



备份：备份数据流量统计
恢复：恢复数据流量统计
删除：删除数据流量统计

3.3.11.3 LAN



MAC 地址：LAN 口的 MAC 地址
IP 地址：LAN 口的 IP 地址
子网掩码：LAN 口的子网掩码
网关：LAN 口的网关
本地 DNS：LAN 口的 DNS



主机名：LAN 口客户端的主机名称
IP 地址：客户端的 IP 地址
MAC 地址：客户端的 MAC 地址
连接数：客户端产生的连接数
比例：占 4096 个连接中的百分比



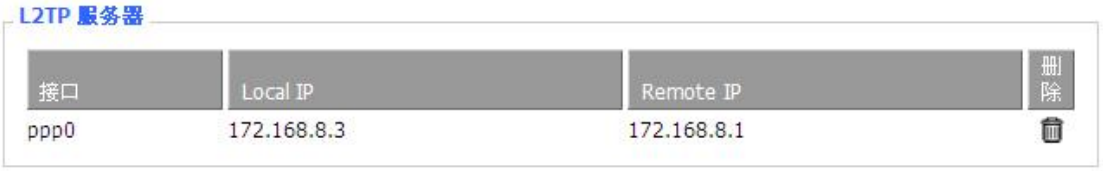
DNCP 服务器：是否启用 DHCP 服务器
DHCP 守护进程：DHCP 采用的那个协议分配主要包括 DNSMasq 和 DHCPd
起始 IP 地址：DHCP 客户端的起始 IP 地址
结束 IP 地址：DHCP 客户端的结束 IP 地址
客户端租约时间：DHCP 客户端的租约时间



主机名：LAN 口客户端的主机名称
IP 地址：客户端的 IP 地址
MAC 地址：客户端的 MAC 地址
客户端租约时间：客户端租约这个 IP 地址的时间
删除：点击可以删除 DHCP 客户端



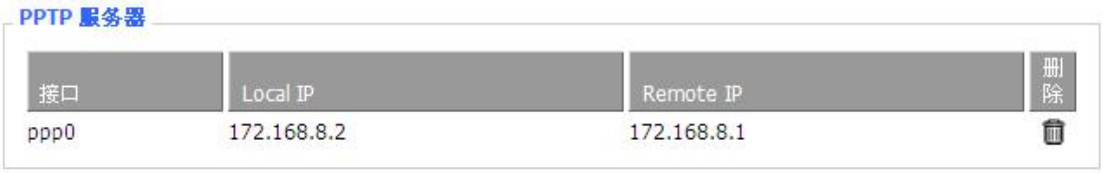
接口：系统拨号分配的接口
用户名：PPPoE 客户端的用户名
Local IP：PPPoE 客户端分配的 IP 地址
删除：点击可以删除 PPPoE 客户端



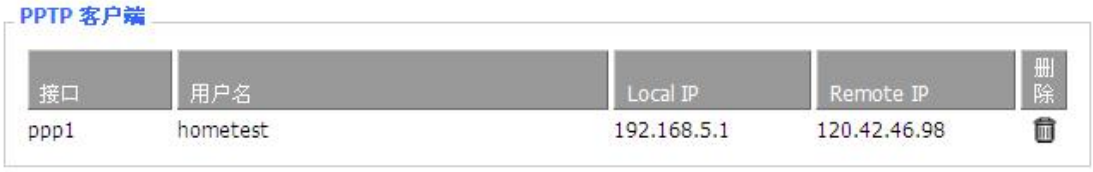
接口：系统拨号分配的接口
Local IP：本地 L2TP 隧道 IP 地址
Remote IP：服务器 L2TP 隧道 IP 地址
删除：点击可以断开 L2TP 连接



接口：系统拨号分配的接口
用户名：客户端的用户名
Local IP：L2TP 客户端隧道 IP 地址
Remote IP：L2TP 客户端 IP 地址
删除：点击可以删除 L2TP 客户端



接口：系统拨号分配的接口
Local IP：本地 PPTP 隧道 IP 地址
Remote IP：服务器 PPTP 隧道 IP 地址
删除：点击可以断开 PPTP 连接



接口：系统拨号分配的接口
用户名：客户端的用户名
Local IP：PPTP 客户端隧道 IP 地址
Remote IP：PPTP 客户端 IP 地址
删除：点击可以删除 PPTP 客户端

3.3.11.4 无线



MAC 地址：无线的 MAC 地址
无线网络：显示是否开启无线网络
模式：无线的模式
网络：无线网络的模式
SSID：无线网络的名称

频道：无线网络的频道
传送功率：无线网络的反射功率
速率：无线网络的反射速率
加密-接口 wl0：是否加密 wl0 接口



已接收的（RX）：已经接收到的数据包
已传送的（TX）：已经发送的数据包



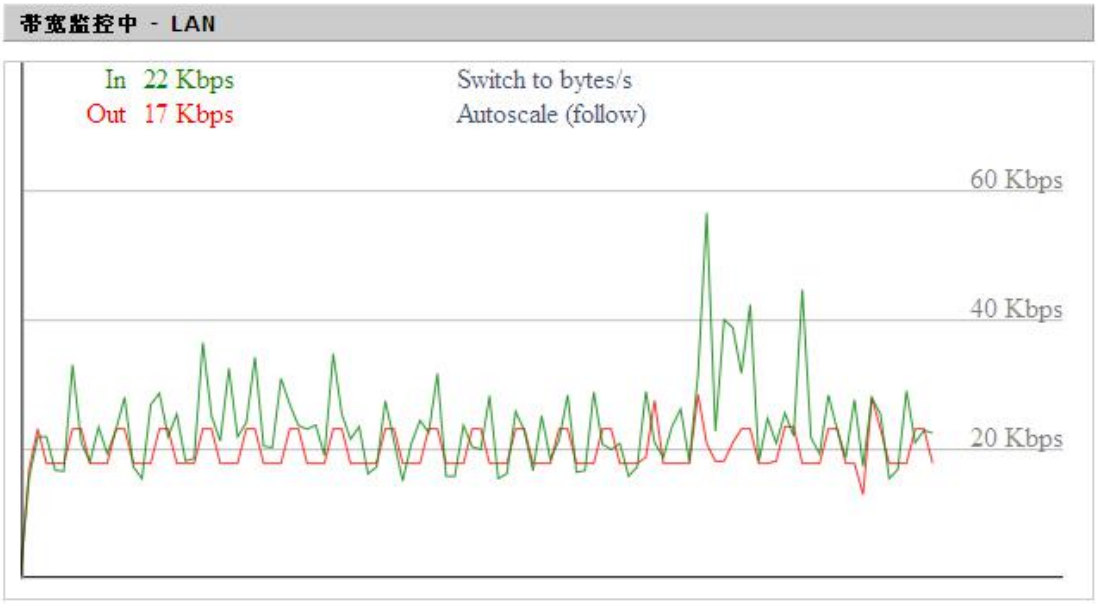
MAC 地址：无线客户端的 MAC 地址
接口：无线客户端的接口
运行时间：无线客户端的接入时间
传输速率：无线客户端的传输速率
接收速率：无线客户端的接收速率
信号：无线客户端的信号
噪声：无线客户端的噪声
SNR：无线客户端的信噪比
信号质量：无线客户端的信号质量



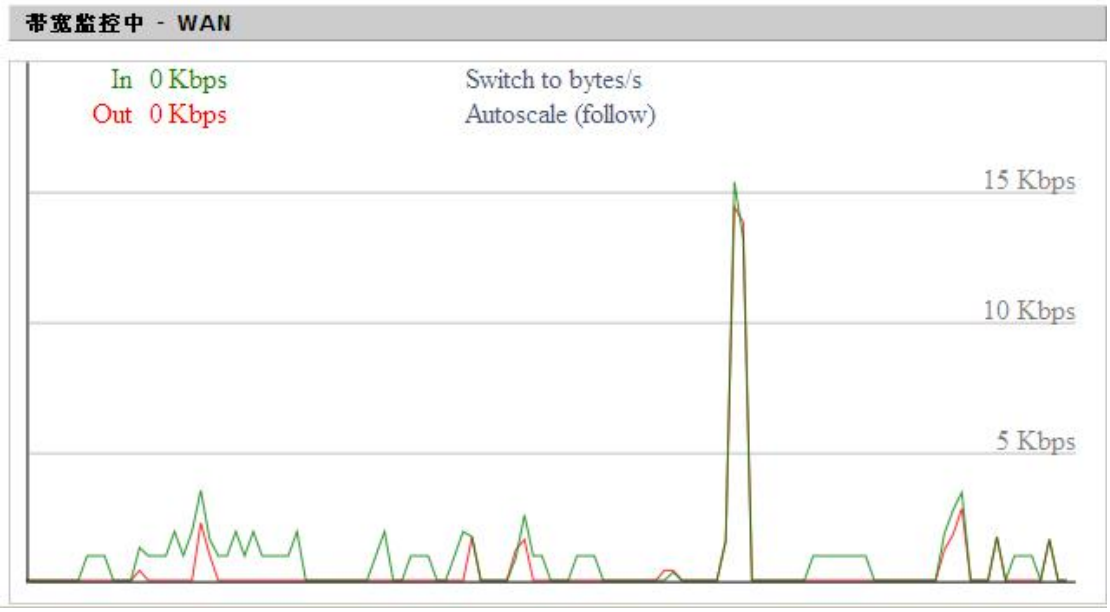
邻近的无线网络：显示邻近的其他网络
SSID：邻近无线网络的名称
Mode：邻近无线工作模式
MAC 地址：邻近无线的 MAC 地址
频道：邻近无线频道
Rssi： 邻近无线信号强度
噪声：邻近无线噪声

信标：邻近无线信号标记
打开：邻近无线是否打开
Dtim：邻近无线的投递传输指示信息
速率：邻近无线的速率
加入基站：点击则加入到邻近无线网络中

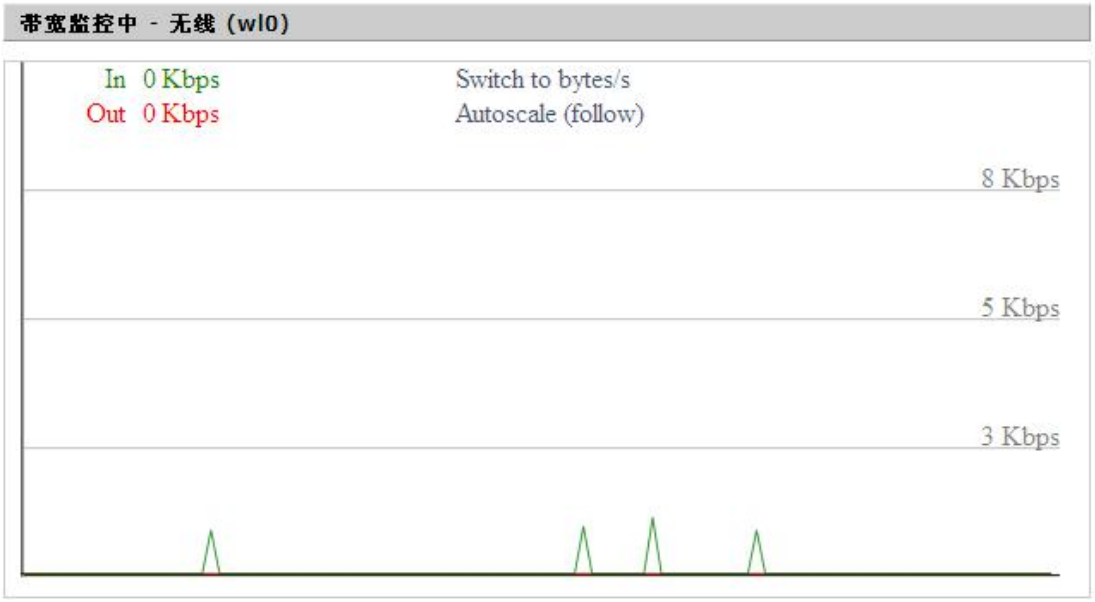
3.3.11.5 宽带



LAN 口的时时检测状态图横坐标代表时间纵坐标代码速率



WAN 口的时时检测状态图横坐标代表时间纵坐标代码速率



无线网络的时时检测状态图横坐标代表时间纵坐标代码速率

Switch to：点击标签选择单位（字节/秒 或 位/秒）。

Autoscale：点击标签选择图形自动调整类型。

3.3.11.6 系统信息



通信管理机名称：本机通信管理机的名称

通信管理机型号：本机通信管理机的型号

LAN MAC：LAN 口的 MAC 地址

WAN MAC：WAN 口的 MAC 地址

Wireless MAC：无线的 MAC 地址

WAN IP：WAN 口的 IP 地址

LAN IP：LAN 口的 IP 地址



无线网络：显示是否开启无线网络
模式：无线的模式
网络：无线网络的模式
SSID：无线网络的名称
频道：无线网络的频道
传送功率：无线网络的反射功率
速率：无线网络的反射速率



已接收的（RX）：已经接收到的数据包
已传送的（TX）：已经发送的数据包



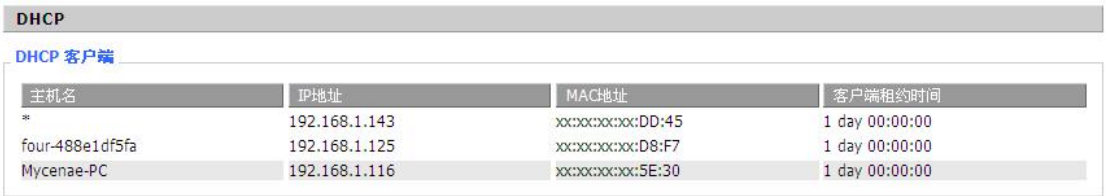
MAC 地址：无线客户端的 MAC 地址
接口：无线客户端的接口
运行时间：无线客户端的接入时间
传输速率：无线客户端的传输速率
接收速率：无线客户端的接收速率
信号：无线客户端的信号
噪声：无线客户端的噪声
SNR：无线客户端的信噪比
信号质量：无线客户端的信号质量



DHCP 服务器：是否启用 DHCP 服务器
ff-radauth：是否启用 radauth 服务
USB 支持：是否启用 USB 支持



所有可用： 所有可用 RAM 大小 （即物理内存减去一些预留位和内核的二进制代码大小）
空闲： 被系统留着未使用的内存，若内存小于 500kB 则会重启，
已使用： 已经使用的内存，所有的可用内存减去空闲内存
缓冲区： 即缓冲区使用的内存，总内存减去已经分配的内存即为缓冲区内存。
已缓存： 被高速缓冲存储器（cache memory）用的内存的大小
使用中： 活跃使用中的缓冲或高速缓冲存储器页面文件的大小
非使用中： 不经常使用中的缓冲或高速缓冲存储器页面文件的大小



主机名：LAN 口客户端的主机名称
IP 地址：客户端的 IP 地址
MAC 地址：客户端的 MAC 地址
客户端租约时间：客户端租约这个 IP 地址的时间

附录

通过 Console 的方式捕捉调试信息时，超级终端的运行步骤和配置方法(WINDOWS XP)

1. 点击 “开始”→“程序”→“附件”→“通讯”→“超级终端”（或者如下图，直接点击“开始”→“运行”输入“hypertrm”启动超级终端）。



超级终端运行后的界面如下：



2. 输入连接名，选择 ”确定”

3. 选择连接到通信管理机 Console 口所采用的 PC 实际物理串口，选择”确定”

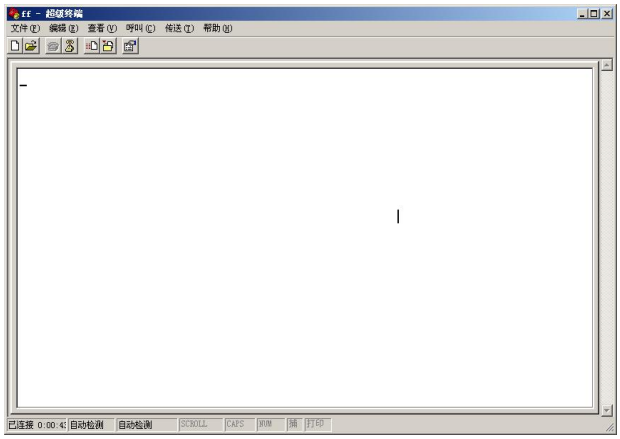


4. 如下图配置超级终端，并选择 ”确定”。

通信速率：115200
数据位：8
奇偶校验：无
停止位：1
数据流控: 无



至此，超级终端正常运行起来了。



如果用户使用的是 win7 系统，可以在网上下载一个 win7 超级终端。或者其它通用的串行交互软件，使用方式类似。