

F3X28-D 系列使用说明书	文档版本	密级
	V1.0.3	
	产品名称: F3X28-D	共 28 页

F3X28-D 系列使用说明书

此说明书适用于下列型号产品:

型号	产品类别
F3828-D	4G 模块
F3828-DS	4G 模块+国网加密
F3828-DG	4G 模块+GPS/北斗
F3828-DGS	4G 模块+GPS/北斗+国网加密
F3Z28-D	公专一体模块
F3Z28-DS	公专一体模块+国网加密
F3Z28-DG	公专一体模块+GPS/北斗
F3Z28-DGS	公专一体模块+GPS/北斗+国网加密
F3928-D	5G 模块
F3928-DS	5G 模块+国网加密
F3928-DG	5G 模块+GPS/北斗
F3928-DGS	5G 模块+GPS/北斗+国网加密



客户热线: 400-8838-199

电话: 0592-5936326

传真: 0592-5912735

网址: www.four-faith.net

地址: 厦门集美软件园三期 A06 栋 11 层

文档修订记录

日期	版本	说明	作者
2021.02.05	V1.0.0	初始版本	HCW
2021.04.12	V1.0.1	图片更新, 供电范围更新	HCW
2021.4.30	V1.0.2	更新版本	WWW
2022.10.10	V1.0.3	新增各串口复用说明	WWW

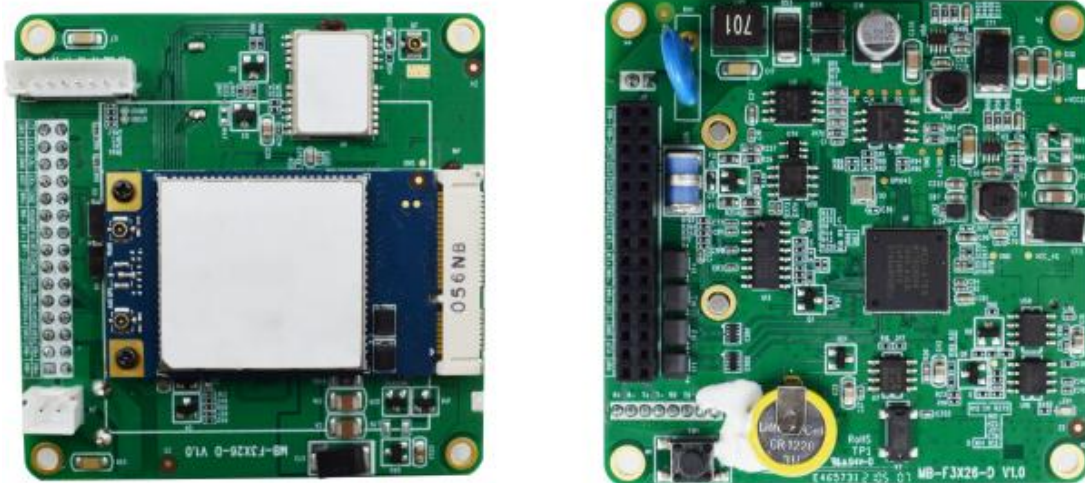
著作权声明

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、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。

产品外形图



注：不同型号配件和接口可能存在差异，具体以实物为准。

目录

第一章 产品简介	5
1.1 产品 F3X28-D 概述	5
1.2 产品特点	5
1.3 工作原理框图	7
1.4 产品规格	7
第二章 安装	12
2.1 概述	12
2.2 装箱清单	12
2.3 安装尺寸	13
2.4 电源说明	13
2.5 指示灯说明	14
2.6 复位按钮说明	14
第三章 参数配置	15
3.1 配置连接图	15
3.2 登录到配置页面	15
3.2.1 PC 机 IP 地址设置（两种方式）	15
3.2.2 登入到配置页面	16
3.3 管理和配置	18
3.3.1 设置	18
3.3.2 服务	28
3.3.3 VPN	31
3.3.4 安全	37
3.3.5 访问限制	40
3.3.6 NAT	43
3.3.7 QoS 设置	45
3.3.8 应用	46
3.3.9 管理	48
3.3.10 状态	52
附录	62

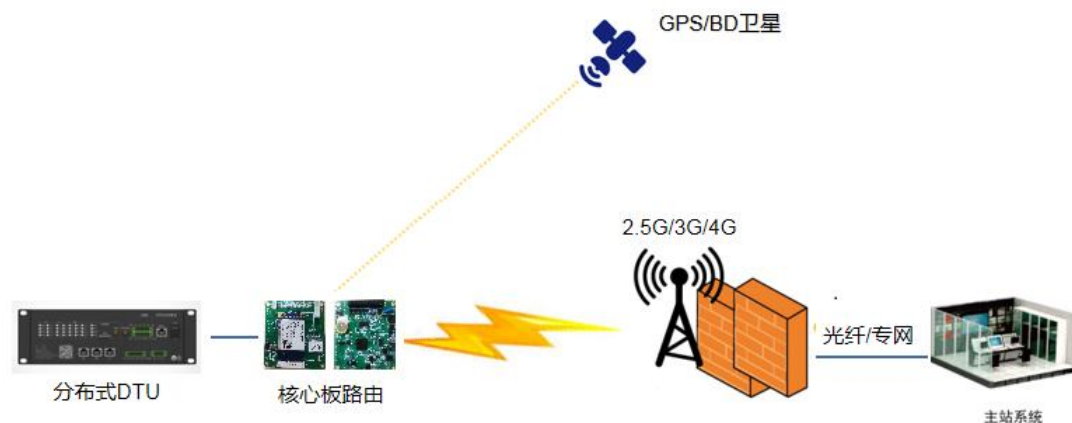
第一章 产品简介

1.1 产品 F3X28-D 概述

F3X28-D 系列 ROUTER 是一种物联网无线通信路由器，利用公用 2.5G/3G/4G/5G 或者专用 1.8GHz 专用蜂窝网络为用户提供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/RS485、1 个 RS232、1 个以太网 LAN，1 个以太网 WAN、1 路 UART 口、1 个 SIM 卡接口、5 个 LED，可连接串口设备或者以太网设备，实现数据透明传输和路由功能。可选配 GPS、北斗对时功能和国网加密功能，保证传输数据安全。

该产品已广泛应用于物联网产业链中的 M2M 行业，如自助终端、智能电网、智能交通、智能家居、金融、移动 POS 终端、供应链自动化、工业自动化、智能建筑、消防、公共安全、环境保护、气象、数字化医疗、遥感勘测、军事、空间探索、农业、林业、水务、煤矿、石化等领域。



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
- ◆ 宽电源输入 DC4.0~5.5V (DC9.0~36V 可选)

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 接口内置 15KV ESD 保护
- ◆ 电源接口内置反相保护和过压保护

标准易用

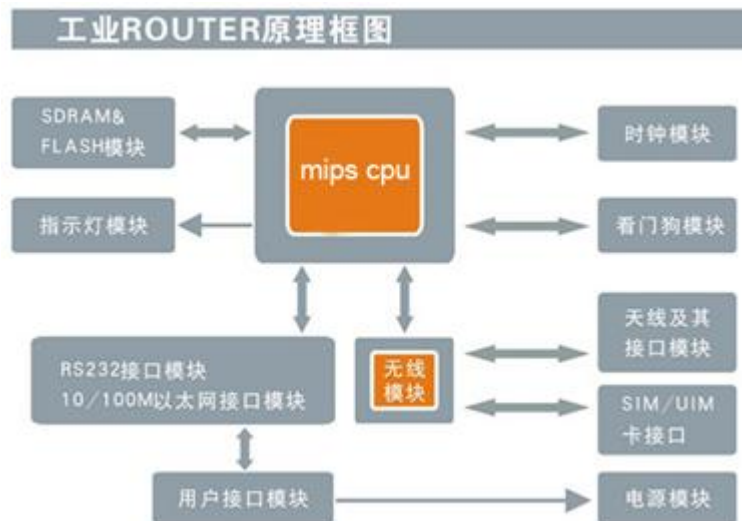
- ◆ 提供标准 RS232 (RS485)、以太网接口, 可直接连接串口设备、以太网设备
- ◆ 智能型数据终端, 上电即可进入数据传输状态
- ◆ 提供功能强大的中心管理软件, 方便设备管理 (可选)
- ◆ 使用方便, 灵活, 多种工作模式选择
- ◆ 方便的系统配置和维护接口 (包括本地和远端 WEB 和 CLI 方式)

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 (PPTP, L2TP, GRE 和 IPSEC) (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 MAC 地址克隆, PPPoE 服务器
- ◆ 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、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
- ◆ 支持 1.8G 专网频段 (选配)
- ◆ 支持国网加密功能 (选配)
- ◆ 支持 GPS、北斗对时功能 (选配)

1.3 工作原理框图

Router 原理框图如下：



1.4 产品规格

无线参数

项目	内容
标准及频段	支持 LTE FDD 2600/2100/1800/900/800MHz, 可选 700/1700/2100MHz 支持 DC-HSPA+/HSPA+/HSDPA/HSUPA/UMTS 850/900/2100MHz 三频,可选 800/850/1900/2100MHz 四频 支持 EDGE/GPRS/GSM 850/900/1800/1900MHz 四频 支持 GPRS CLASS 10 支持 EDGE CLASS 12
理论带宽	LTE FDD: 下行速率 100Mbps, 上行速率 50Mbps DC-HSPA+: 下行速率 42Mbps, 上行速率 5.76 Mbps HSPA+: 下行速率 21Mbps, 上行速率 5.76 Mbps HSDPA: 下行速率 7.2Mbps, HSUPA: 上行速率 5.76Mbps UMTS: 384Kbps
发射功率	<23dBm
接收灵敏度	>-97dBm

专网参数 (选配)

项 目	内 容
标准及频段	1.8G LTE 无线专网网络环境
理论带宽	LTE FDD: 下行速率 100Mbps, 上行速率 50Mbps DC-HSPA+: 下行速率 42Mbps, 上行速率 5.76 Mbps HSPA+: 下行速率 21Mbps, 上行速率 5.76 Mbps HSDPA: 下行速率 7.2Mbps, HSUPA: 上行速率 5.76Mbps UMTS: 384Kbps
发射功率	<23dBm
接收灵敏度	>-97dBm

GPS/BDS 参数 (选配)

项 目	内 容
接收机类型	32 通道 GPS/BDS L1, 1575.42MHz; B1, 1561.098MHz
数据更新速率	1Hz
精确度	GPS&BDS<2.5m CPE50% (开阔地) GPS ONLY 3m CPE50% (开阔地) BDS ONLY 5m CPE50% (开阔地)
捕获	冷启动: 32S 热启动: 1S 重启: 1S
灵敏度	跟踪: -160dBm 冷启动: -148dBm
授时精度	20ns

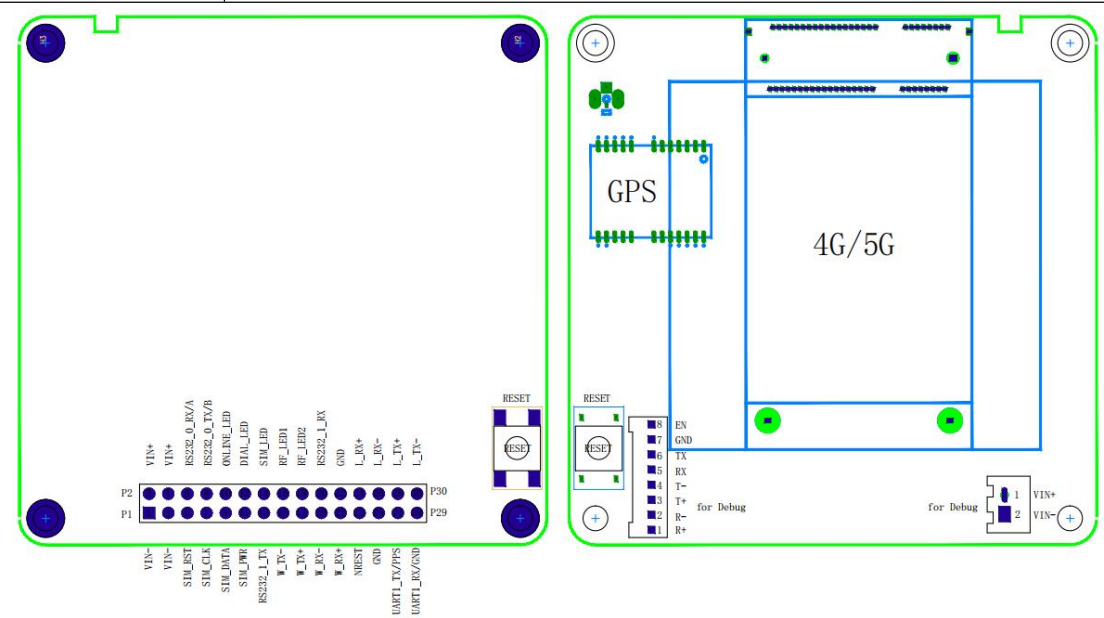
硬件系统

项 目	内 容
CPU	工业级 32 位通信处理器
FLASH	16MB (可扩展至 64MB)
DDR2	64MB

接口类型

项 目	内 容
调试电源接口	采用 2.54mm 间距的 XH-2 接口, 支持 DC4.0~5.5V (DC9.0~36V 可选) 电压输入, 内置电源反相保护和过压保护
调试通信接口	采用 2.0mm 间距的 PH-8 接口, 1 路 232/485 (默认 232) 和 1 路网口
主接口	采用 30 pin 的 2.54mm 间距双排插座 电源供电: DC4.0~5.5V (DC9.0~36V 可选)

	UART 接口 (PPS 口复用, 默认 UART): 1 个 1 路 RS232_0、1 路 RS232_1/RS485 (默认 RS232) 以太网端子接口: 1 路 LAN 口, 1 路 LAN/WAN 复用口 (默认 LAN 口) SIM 卡接口 NRESET 信号 网络指示信号: Online、DIAL、SIM、RF1、RF2 等 5 个指示网络状态
复位按键	长按可将 Router 的参数配置恢复为出厂值 (与 30pin 中的 RST#信号复用)


调试电源接口接口引脚定义及接线要求

引脚号	标记	I/O	标记说明	备注
1	VIN+	P	电源正极	DC4.0~5.5V (DC9.0~36V 可选) 电源要求大于 15W
2	VIN-	P	电源负极	

调试通信接口接口引脚定义及接线要求

引脚号	标记	I/O	标记说明	备注
1	L_RX+	I	LAN 口收据接收正	符合 10/100M 以太网通讯规范, 不用悬空
2	L_RX-	I	LAN 口收据接收负	
3	L_TX+	O	LAN 口收据发送正	
4	L_TX-	O	LAN 口收据发送负	
5	RXD	I	RS232_0 数据接收	可定制 RS485, 不用悬空
6	TXD	O	RS232_0 数据发送	
7	GND	P	系统地	
8	NC	I/O	预留 IO	

主接口引脚定义及接线要求
电源

引脚号	标记	I/O	标记说明	备注
-----	----	-----	------	----

1	VIN-	P	电源负极	DC4.0~5.5V (DC9.0~36V 可选) 电源要求大于 15W
2	VIN+	P	电源正极	
3	VIN-	P	电源负极	
4	VIN+	P	电源正极	
GND 引脚				
引脚号	标记	I/O	标记说明	备注
22	GND	P	系统地	
25	GND	P	系统地	
串口信号				
引脚号	标记	I/O	标记说明	备注
6	RS232_0_RX/A	I	RS232_0 数据接收	可定制 RS485
8	RS232_0_TX/B	O	RS232_0 数据发送	不用悬空
13	RS232_1_TX	O	RS232_1 数据发送	不用悬空
20	RS232_1_RX	I	RS232_1 数据接收	
UART 信号/PPS				
引脚号	标记	I/O	标记说明	备注
27	UART1_TX/PPS	O	UART1 数据发送/PPS	默认 UART1
29	UART1_RX/GND	I	UART1 数据接收/GND	可定制 PPS (GPS 版本)
SIM 卡信号				
引脚号	标记	I/O	标记说明	备注
5	SIM_RST	O	SIM 卡复位信号	
7	SIM_CLK	O	SIM 卡时钟信号	
9	SIM_DATA	IO	SIM 卡数据信号	
11	SIM_PWR	P	SIM 卡供电电源	设备自动识别 1.8V 或 3.0V SIM 卡
以太网 WAN 口 (可配置为 LAN 口)				
引脚号	标记	I/O	标记说明	备注
21	W_RX+	I	WAN 口数据接收正	符合 10/100M 以太网通信规范 不用悬空
19	W_RX-	I	WAN 口数据接收负	
17	W_TX+	O	WAN 口数据发送正	
15	W_TX-	O	WAN 口数据发送负	
以太网 LAN 口				
引脚号	标记	I/O	标记说明	备注
24	L_RX+	I	LAN 口数据接收正	符合 10/100M 以太网通信规范 不用悬空
26	L_RX-	I	LAN 口数据接收负	
28	L_TX+	O	LAN 口数据发送正	
30	L_TX-	O	LAN 口数据发送负	
网络指示				
引脚号	标记	I/O	标记说明	备注
10	ONLINE_LED	O	指示通信状态	高电平: 数据通信正常
12	DIAL_LED	O	指示拨号状态	高电平: 拨号成功

				1Hz 方波: 拨号过程中
14	SIM_LED	O	指示 SIM 卡是否插入	高电平: 读到 SIM 卡 低电平: 读不到 SIM 卡
16	RF_LED1	O	指示信号强度	信号强度弱: RF_LED1 高电平, RF_LED2 低电平 信号强度一般: RF_LED1 高电平, RF_LED2 高电平
18	RF_LED2	O	指示信号强度	信号强度高: RF_LED1 低电平, RF_LED2 高电平
复位信号				
引脚号	标记	I/O	标记说明	备注
23	NREST	I	复位信号	内部上拉到 3.3V 不用悬空
注: 1) I/O 参数定义: P: 电源 I: 数字输入 O: 数字输出 IO: 双向 2) 硬件上 RS232-1、UART1、GPS 为同一串口, 带 GPS 的版本 RS232-1、UART1 皆不可用;				

供电

项 目	内 容
标准电源	DC 5V/3A (DC12V/1.5A 可选)
供电范围	DC4.0~5.5V (DC9.0~36V 可选)

功耗

工作状态	功 耗
待机	150~350mA@5VDC (90~150mA@12VDC)
通信	250~550mA@5VDC (160~250mA@12VDC)

物理特性

项 目	内 容
外形尺寸	70x70x25 mm (不包括天线和安装件)
重量	45g

其它参数

项 目	内 容
工作温度	-35~+75°C (-31~+167°F)
储存温度	-40~+85°C (-40~+185°F)
相对湿度	95% (无凝结)

第二章 安装

2.1 概述

Router 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 Router。

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：

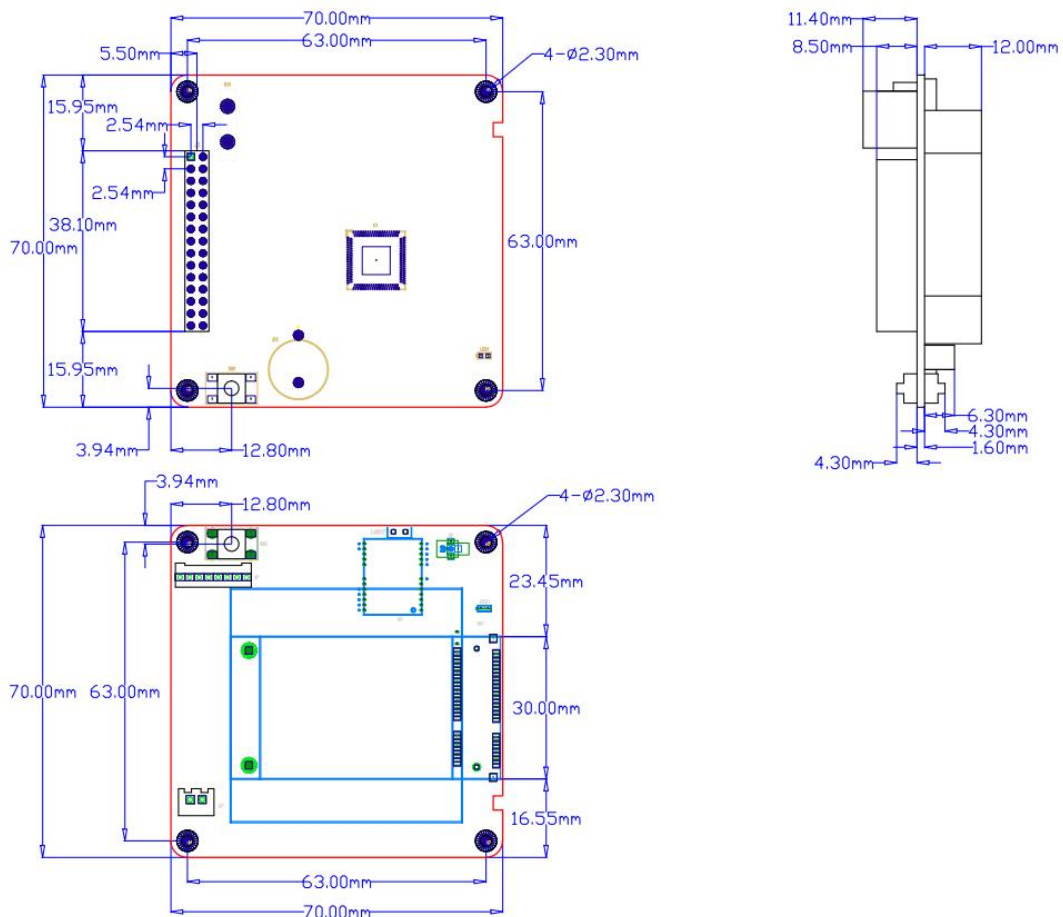
- ◇ Router 主板 1 台
- ◇ 产品合格证
- ◇ 产品保修卡

2.3 安装尺寸

外形尺寸:

主板上 4 个直径 2.3mm 的安装孔, 便于固定到用户设备中。

产品尺寸图 (单位: mm)



Router 尺寸

注: 安装 Router 螺钉为 M2, 螺钉锁进 Router 的深度为 3~4mm。

2.4 电源说明

Router 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, Router 采用了先进的电源技术。用户可采用标准配置的 5V/3A (12V/1.5A 可选) 电源适配器给 Router 供电, 也可以直接用直流 DC4.0~5.5V (DC9.0~36V 可选) 电源给 Router 供电。当用户采用外加电源给 Router 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 Router 的最高电压范围 5.5V (或 36V 可选)), 并保证电源功率大

于 15W 以上。

2.5 指示灯说明

Router 提供以下指示灯：“DIAL”、“SIM”、“Online”、“RF1”、“RF2”。各指示灯状态说明如下表：

网络指示				
引脚号	标记	I/O	标记说明	备注
10	ONLINE_LED	O	指示通信状态	高电平：数据通信正常
12	DIAL_LED	O	指示拨号状态	高电平：拨号成功 1Hz 方波：拨号过程中
14	SIM_LED	O	指示 SIM 卡是否插入	高电平：读到 SIM 卡 低电平：读不到 SIM 卡
16	RF_LED1	O	指示信号强度	信号强度弱：RF_LED1 高电平， RF_LED2 低电平
18	RF_LED2	O	指示信号强度	信号强度一般：RF_LED1 高电平， RF_LED2 高电平 信号强度强：RF_LED1 低电平， RF_LED2 高电平

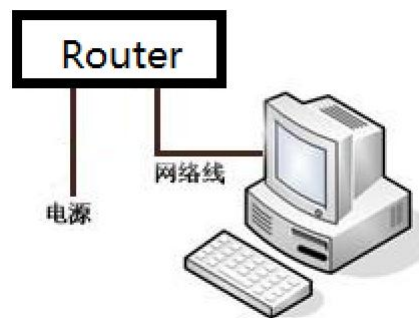
2.6 复位按钮说明

Router 设有一个复位按钮。该按钮的作用是将 Router 的参数配置恢复为出厂值。方法如下：按住复位按钮，约 15 秒钟后放开，此时，Router 会自动把参数配置恢复为出厂值，并在约 5 秒钟之后，Router 自动重启（自动重启现象如下：“SYS”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

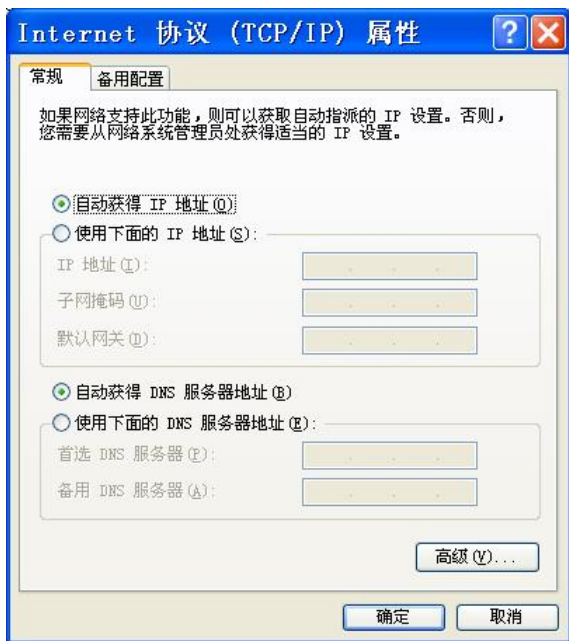
在对路由器进行配置前，需要将路由器和用于配置的 PC 通过出厂配置的网络线连接起来。用网络线连接时，网络线的一端连接路由器以太网接口，另外一端连接到 PC 的以太网口。



3.2 登录到配置页面

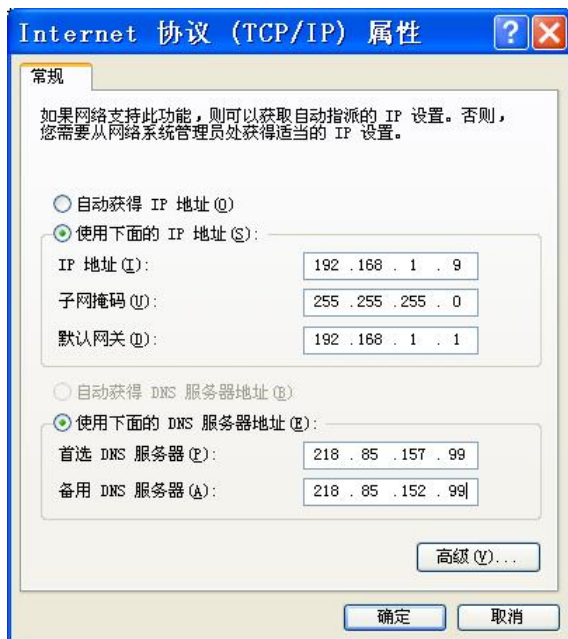
3.2.1 PC 机 IP 地址设置（两种方式）

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 192.168.1.9(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: 192.168.1.1。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。可以使用连接到路由器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。

为了访问路由器基于网页的 Web 管理工具，启动 IE 或其他浏览器，并在“地址”栏输入路由器的默认 IP 地址 192.168.1.1。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，提示用户是否修改路由器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

您的路由器目前不受保护且使用不安全的预设用户名和密码组合，请使用以下对话框修改！

路由器密码

路由器用户名	<input type="text" value="admin"/>
路由器密码	<input type="password" value="••••"/>
密码确认	<input type="password" value="••••"/>

之后就可以进入信息主页面



The screenshot shows the 'Wireless Mobile Router' web interface. The top navigation bar includes the Four-Faith logo, the product name 'Wireless Mobile Router', and various network standards supported (GPRS/CDMA/EDGE/WCDMA/HDR/HSDPA/HSUPA/TD-SCDMA/HSPA+/LTE). A status bar at the top right shows the firmware version (F3x27 v1.0), date (Oct 16 2014 18:28:31), and system time (00:15:33 up 15 min).

The main content area is divided into three sections:

- 菜单 (Menu):** A sidebar with options like 设置 (Settings), 服务 (Services), VPN, 安全 (Security), 访问限制 (Access Control), NAT, QoS设置 (QoS Settings), 应用 (Applications), 管理 (Management), and 状态 (Status).
- WAN 设置 (WAN Settings):** The primary configuration area. It includes:
 - WAN 连接类型 (WAN Connection Type):** Set to 3G/UMTS/4G/LTE.
 - 用户名 (Username):** card
 - 密码 (Password):** masked with dots, with a '显示密码' (Show Password) checkbox.
 - 呼叫中心号码 (Call Center Number):** #777 (CDMA/EVDO)
 - PIN:** empty, with a '显示密码' checkbox.
 - 允许的认证协议 (Allowed Authentication Protocols):** PAP, CHAP, MS-CHAP, and MS-CHAPv2 are all checked.
 - 在线保持方式 (Online Maintenance Method):** Ping
 - 在线保持检测时间间隔 (Online Maintenance Detection Interval):** 60 秒
 - 在线保持检测主服务器IP (Online Maintenance Detection Primary Server IP):** 208.67.222.222
 - 在线保持检测副服务器IP (Online Maintenance Detection Secondary Server IP):** 208.67.220.220
 - 是否启用手动设置WAN IP (Enable Manual WAN IP Settings):** 禁用 (Disabled)
 - 是否启用手动设置WAN网关 (Enable Manual WAN Gateway Settings):** 禁用 (Disabled)
 - 是否启用拨号失败重启机制 (Enable Restart Mechanism on Dialing Failure):** 启用 (Enabled)
 - 强制重新连接 (Force Reconnect):** 禁用 (Disabled)
 - Wan Nat:** 启用 (Enabled)
 - STP:** 启用 (Enabled)
- 可选设置 (Optional Settings):**
 - 路由器名称 (Router Name):** Router
 - 主机名 (Hostname):** empty
 - 域名 (Domain):** empty
 - MTU:** Auto (dropdown), 1500 (input)
- 帮助 (Help):** A sidebar on the right with sections for 主机名 (Hostname), 域名 (Domain), 本地IP地址 (Local IP Address), 子网掩码 (Subnet Mask), DHCP 服务器 (DHCP Server), 起始IP地址 (Starting IP Address), 最大DHCP用户数 (Maximum DHCP Users), and 时间设置 (Time Settings).

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路由器连接到互联网。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 2 种方式：禁用，3G/UMTS/4G/LTE。

方式一：禁用

连接类型

禁止 WAN 口的连接类型设置

方式二：dhcp-4G/5G

该方式是 4G/5G 无线网络模块高速率通讯网络连接方式，标配 4G/5G 模块建议用户选择该设置方式

连接类型	dhcp-4G/5G	
用户名	root	
密码	••••	<input type="checkbox"/> 显示密码
APN	3gnet	
网络类型选择	Auto	

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。

网络类型

网络类型选择	Auto
--------	------

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

在线保持

在线保持方式	Ping
在线保持检测时间间隔	60 秒
在线保持检测主服务器 IP	166 . 111 . 8 . 238
在线保持检测副服务器 IP	202 . 119 . 32 . 102

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，路由器将自动检测 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 Router 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 :

响应路由器在线检测数据包的主服务器的 IP 地址。注意：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 :

响应路由器在线检测数据包的副服务器的 IP 地址。注意：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 启用 禁用

时间 :

强制重新连接：该功能可以指定路由器在指定的时间重新连接 Internet。

时间：输入正确的重连时间。注意这个时间是具体的时间点，不是时间间隔。00:00 时，也就是 24:00。

STP

STP 启用 禁用

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

路由器名称

主机名

域名

MTU

路由器名称：在这个字段中，您可以输入代表路由器的长达 39 个字符的英文字符名称。

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。如果希望路由器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，可以修改连接到路由器以太网口上的网络参数。

本地IP地址	192	.	168	.	1	.	1
子网掩码	255	.	255	.	255	.	0
网关	0	.	0	.	0	.	0
本地DNS	0	.	0	.	0	.	0

本地 IP 地址：表示在您的局域网中，可以通过设置的这个 ip 地址访问到路由器

子网掩码：表示用于分隔不同网段互联的一个参数。请用户不要随便改动。

网关：设置路由器内部的网关，若默认设置，则内部网关为路由器本身的地址，此项可以不填。

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)

这些设置用于对路由器的动态主机配置协议 (DHCP) 服务器功能进行配置。路由器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。如果选择启用路由器的 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	DHCP 服务器
DHCP 服务器	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
起始IP地址	192.168.1. 100
最大DHCP用户数	50
客户端租约时间	1440 分钟
静态DNS 1	0 . 0 . 0 . 0
静态DNS 2	0 . 0 . 0 . 0
静态DNS 3	0 . 0 . 0 . 0
WINS	0 . 0 . 0 . 0
为DHCP使用DNSMasq	<input checked="" type="checkbox"/>
为DNS使用DNSMasq	<input checked="" type="checkbox"/>
以DHCP为准	<input checked="" type="checkbox"/>

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 类型	DHCP 转发器
DHCP 服务器	0 . 0 . 0 . 0

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。因为本路由器的默认 IP 地址为 192.168.1.1，所以，起始 IP 地址必须为 192.168.1.3 或更大但又比 192.168.1.154 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，则要在这一页输入该服务器的 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 启用 禁用

时区

夏令时 (DST)

服务器IP/主机名

NTP 客户端: 开启或者禁用为系统内部提供一个对时，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

Adjust Time

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)

如果路由器 Internet 接入获得的 IP 地址由运营商动态分配，路由器每次获得的 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，该域名始终对应路由器当前的动态 IP 地址。这样，通过访问域名就可以访问到路由器最新的 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

DDNS 服务	<input type="text" value="3322.org"/>	
用户名	<input type="text"/>	
密码	<input type="password"/>	<input type="checkbox"/> 显示密码
主机名	<input type="text"/>	
类型	<input type="text" value="动态"/>	
通配符	<input type="checkbox"/>	
不使用外部 IP 检测	<input checked="" type="radio"/> 是 <input type="radio"/> 否	

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 (预设: 10 天, 范围: 1 - 60)

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

DDNS 状态

```

Fri Nov 25 13:58:32 2011: INADYN: Started 'INADYN Advanced version 1.96-ADV' - dynamic DNS updater.
Fri Nov 25 13:58:32 2011: INADYN: IP read from cache file is '192.168.8.222'. No update required.
Fri Nov 25 13:58:32 2011: I:INADYN: IP address for alias 'testsixin.3322.org' needs update to '192.168.8.38'
Fri Nov 25 13:58:33 2011: I:INADYN: Alias 'testsixin.3322.org' to IP '192.168.8.38' updated successfully.
                    
```

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，您可以将路由器的 MAC 地址克隆为您在 ISP 注册的 MAC 地址。

启用 禁用

克隆 LAN 口 MAC

00 : AA : BB : CC : DD : 44

克隆 WAN 口 MAC

00 : AA : BB : CC : DD : 45

获取当前 PC 的 MAC 地址

克隆无线 MAC

00 : AA : BB : CC : DD : 46

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

工作模式

网关

工作模式：选择正确的运行模式。如果路由器共享 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路由器的路由功能，则选择路由器。

动态路由

动态路由

接口

禁用

该功能在网关模式下不可用。动态路由功能使路由器能够针对网络布局中的物理更改进行自动调整，并与其他路由器交换路由表。路由器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

要在路由器和另一个网络之间设置静态路由，请从静态路由下拉列表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。）

静态路由

选择设置编号:

路由名称:

跃点数:

目的LAN IP: ...

子网掩码: ...

网关: ...

接口:

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：这是允许路由器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。要查看当前路由器的详细路由信息，点击“显示路由表”按钮。

路由表条目列表			
目的LAN IP	子网掩码	网关	接口
192.168.8.1	255.255.255.255	0.0.0.0	WAN
192.168.1.0	255.255.255.0	0.0.0.0	LAN & WLAN
192.168.8.0	255.255.255.0	0.0.0.0	WAN
169.254.0.0	255.255.0.0	0.0.0.0	WAN
0.0.0.0	0.0.0.0	192.168.8.1	WAN

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 网络

桥接中

创建网桥

Bridge 0 STP Prio MTU

指派到网桥

当前桥接列表

网桥名	启用STP	接口
br0	no	vlan1

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

创建网桥

Bridge 0 STP Prio MTU

Bridge 1 STP Prio MTU

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：

创建网桥

Bridge 0 STP Prio MTU

Bridge 1 STP Prio MTU

IP地址

子网掩码

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

指派到网桥

Assignment 0 none Interface eth2 Prio 63 删除

添加

none
 none
 br0
 br1

端口配置

端口配置

网络配置 eth2	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 默认
网络配置 vlan1	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 默认
网络配置 br0	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 默认

端口配置：配置各个端口的属性，以下以一个 ra0 端口做说明

网络配置 ra0 未桥接 预设

MTU 1500

组播转发 启用 禁用

Masquerade / NAT 启用 禁用

IP地址 0 . 0 . 0 . 0

子网掩码 0 . 0 . 0 . 0

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

DHCPD

多路DHCP服务器

DHCP 0 vlan1 On Start 100 Max 50 Leasetime 3600

删除

添加

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 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

DHCP 服务器

使用JFFS2存储客户端租约数据 (未连接)

使用NVRAM存储客户端租约数据

已使用的域 WAN ▼

LAN域

DHCPd 附加选项

永久租用			
MAC地址	主机名	IP地址	客户端租约时间
<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/> 分钟

使用 NVRAM 储存客户端租约数据： 启用则可以把数据储存到系统的 NVRAM 区域

已使用的域： 你可以在这里选择哪个域的 DHCP 客户端应该得到他们的本地域名。这可以设置局域网域，也可以设置局域网和广域网域

LAN 域： 你可以在这里定义你的本地局域网域。如果配置，则使用本地域名的 dnsmasq 和 DHCP 服务

永久租用： 在这里你可以定义一些如果你想指定某些主机特定的地址。这也是一种方式来增加一个固定地址的主机到路由器本地 DNS 服务（dnsmasq）中，“添加”按键可以添加指定 MAC 地址、IP 地址和租约时间的客户端

DHCPd 附加选项： 输入你自己的相应配置

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）的路由器以及远程 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

DNSMasq

DNSMasq 启用 禁用

本地DNS 启用 禁用

No DNS Rebind 启用 禁用

DNSMasq 附加选项

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路由器内部 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、路由器以及桥接器等）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。

SNMP

SNMP 启用 禁用

位置

联系

名称

只读团体字

读写团体字

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路由器的操作系统

Secure Shell

SSHD	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
SSH TCP转发	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
密码登录	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
端口	<input type="text" value="22"/>	(预设: 22)
授权密钥	<input type="text"/>	

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

系统日志

系统日志	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
输出模式	<input checked="" type="radio"/> 网络	<input type="radio"/> 串口
远程服务器	<input type="text"/>	

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

Telnet	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
--------	-------------------------------------	--------------------------

Telnet: 启用或禁用 Telnet 功能

WAN 流量计数器

WAN流量计数器

ttraff守护进程	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
------------	-------------------------------------	--------------------------

Ttraff 守护进程: 启用或者禁用流量统计功能

3.3.3 VPN

3.3.4.1 PPTP

PPTP 服务器

PPTP服务器

PPTP服务器 启用 禁用

广播支持 启用 禁用

强制MPPE加密 启用 禁用

DNS1

DNS2

WINS1

WINS2

服务器IP

客户端IP

本地用户管理(CHAP Secrets)

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: 输入路由器作为 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 不能和路由器 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

PPTP客户端

PPTP客户端选项 启用 禁用

服务器IP或DNS名称

远程子网 . . .

远程子网掩码 . . .

MPPE加密

MTU (预设: 1450)

MRU (预设: 1450)

NAT 启用 禁用

用户名

密码 显示密码

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

L2TP服务器

L2TP服务器选项 启用 禁用

强制MPPE加密 启用 禁用

服务器IP

客户端IP

本地用户管理(CHAP Secrets)

强制 MPPE 加密: 是否要强制 L2TP 数据 MPPE 加密

服务器 IP: 输入路由器作为 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 不能和路由器 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客户端

L2TP客户端选项 启用 禁用

用户名

密码 显示密码

L2TP服务器

远程子网

远程子网掩码

MPPE加密

MTU (预设: 1450)

MRU (预设: 1450)

NAT 启用 禁用

允许CHAP认证协议 是 否

拒绝PAP认证协议 是 否

允许认证协议 是 否

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 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。

连接状态及操作

名称	类型	通用名称	状态	操作
<input type="button" value="添加"/>				

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。

类型

类型 Net-to-Net虚拟专用网 ▼

IPSEC功能 客户端 服务端

连接配置：该栏目包含了通道的基本地址信息。

连接配置

名称	<input type="text"/>	启用	<input checked="" type="checkbox"/>
本机的WAN接口	WAN ▼	远程主机地址	<input type="text"/>
本地子网	<input type="text"/>	远程子网	<input type="text"/>
本地主机标志符	<input type="text"/>	远程主机标志符	<input type="text"/>

名称：用以标示该连接的名称，须唯一；

启用：选择启用，则该条连接在系统开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器端功能，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。

检测

启用DPD检测

时间间隔 (秒) 超时时间 (秒) 操作

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。

高级配置

启用高级配置

IKE 加密 IKE 完整性 IKE DH 小组

IKE 生命周期 小时

ESP 加密 ESP 完整性

ESP 生命周期 小时

IKE+ESP: Use only proposed settings.

采用野蛮模式

会话密钥向前加密(PFS)

Negotiate payload compression

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。

认证

使用预共享密钥:

生成并使用该X.509认证

3.3.4.4 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

GRE隧道 启用 禁用

GRE 隧道: 启用或者禁用 GRE 功能

通道	1 (fff) <input type="button" value="删除"/>
状态	启用 <input type="button" value="v"/>
名称	fff <input type="text"/>
通过	PPP <input type="button" value="v"/>
对端WAN IP	120.42.46.98 <input type="text"/>
对端子网	192.168.5.0/24 <input type="text"/> (eg: 192.168.1.0/24)
对端隧道IP	200.200.200.1 <input type="text"/>
本端隧道IP	200.200.200.5 <input type="text"/>
本端子网掩码	255.255.255.0 <input type="text"/>

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 WAN 口, 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

本端隧道 IP: 本地 GRE 隧道 IP 地址

本端子网掩码：本地子网掩码

保活 启用 禁用
 重拨次数
 重拨间隔
 失败策略 保持 ▾

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”按钮可以查看 GRE 的信息

GRE 隧道列表

隧道	名称	启用	通过	对端WAN IP	对端子网	对端隧道IP	本端隧道IP	本端子网掩码	保活	重拨次数	重拨间隔	失败策略
1	fff	是	PPP	120.42.46.98	192.168.5.0/24	200.200.200.1	200.200.200.5	255.255.255.0	否	0	0	保持

3.3.4 安全

3.3.4.1 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

防火墙保护
 SPI防火墙 启用 禁用

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

附加的过滤器
 过滤代理
 过滤Cookies
 过滤Java Applets
 过滤ActiveX

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

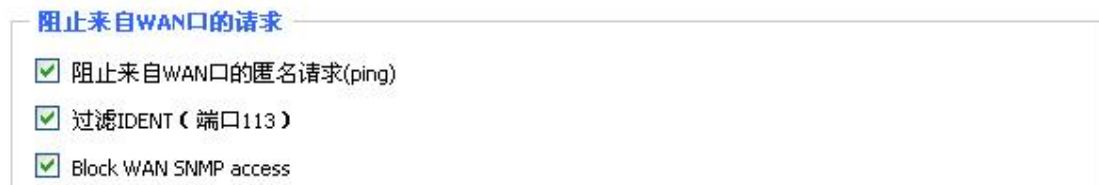
代理服务器的访问，单击该复选框启用 Proxy 过滤或反选以禁用该功能。

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



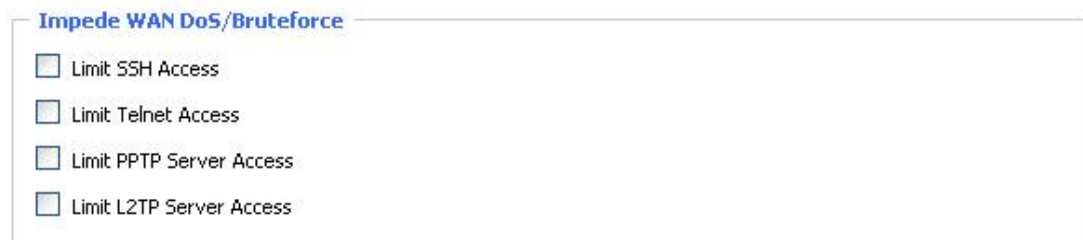
阻止来自 WAN 口的匿名请求 (ping): 通过选中“阻止匿名 Internet”请求旁的选项框，启用该功能，从而防止您的网络遭受其他 Internet 用户的 Ping 或者探测，使外部用户更加难以侵入您的网络，这一功能的默认状态为启用，选择禁用可以允许匿名 Internet 请求。

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

路由器可以保存您的所有 Internet 连接的日志，包括连入和连出。

日志

日志

日志 启用 禁用

日志等级 低

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
选项

丢弃的 禁用

拒绝的 启用

已接受的 启用

当选择启用的时候，对应的连接会被记录在日志里，禁用则不记录。

连入日志

要看到路由器的最近期的传入的临时日志，单击“连入日志”按钮。

连入日志表

来源IP	协议	目的端口号	规则
183.60.49.59	UDP	4000	Accepted
183.60.49.59	UDP	4000	Accepted
123.58.182.252	TCP	3884	Accepted
123.58.182.252	TCP	3884	Accepted
123.58.182.252	TCP	3884	Accepted
123.58.182.252	TCP	3884	Accepted
123.58.182.252	TCP	3884	Accepted
123.58.182.252	TCP	3884	Accepted
123.58.182.252	TCP	3884	Accepted
123.58.182.252	TCP	3884	Accepted
123.58.182.252	TCP	3884	Accepted
183.60.49.59	UDP	4000	Accepted
183.60.49.59	UDP	4000	Accepted

刷新

关闭

连出日志

要看到路由器的最近期的传入的临时日志，单击“连出日志”按钮。

连出日志表

LAN IP	目的 URL/IP	协议	服务/端口号	规则
192.168.1.163	122.228.241.6	UDP	8000	Accepted
192.168.1.163	123.58.182.252	TCP	www	Accepted
192.168.1.163	123.58.182.252	TCP	www	Accepted
192.168.1.163	61.183.55.217	UDP	8000	Accepted

刷新

关闭

3.3.5 访问限制

3.3.5.1 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。

访问策略

策略

状态 启用 禁用

策略名称

PCs

拒绝 过滤

在选定的日期和时间允许Internet访问。

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”按钮删除一条策略，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

每天	周日	周一	周二	周三	周四	周五	周六
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

时间

24小时

起始于 0 : 00 终止于 0 : 00

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

<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

通过关键字封锁Web站点

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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。

客户端列表

输入客户端MAC地址，格式为：xx:xx:xx:xx:xx:xx

MAC 01	<input type="text" value="00:00:00:00:00:00"/>
MAC 02	<input type="text" value="00:00:00:00:00:00"/>
MAC 03	<input type="text" value="00:00:00:00:00:00"/>
MAC 04	<input type="text" value="00:00:00:00:00:00"/>
MAC 05	<input type="text" value="00:00:00:00:00:00"/>
MAC 06	<input type="text" value="00:00:00:00:00:00"/>
MAC 07	<input type="text" value="00:00:00:00:00:00"/>
MAC 08	<input type="text" value="00:00:00:00:00:00"/>

输入客户端的IP地址

IP 01	192.168.1.	<input type="text" value="0"/>
IP 02	192.168.1.	<input type="text" value="0"/>
IP 03	192.168.1.	<input type="text" value="0"/>
IP 04	192.168.1.	<input type="text" value="0"/>
IP 05	192.168.1.	<input type="text" value="0"/>
IP 06	192.168.1.	<input type="text" value="0"/>

输入客户端的IP范围

IP范围 01	<input type="text" value="0"/> .	<input type="text" value="0"/> .	<input type="text" value="0"/> .	<input type="text" value="0"/> ~	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
IP范围 02	<input type="text" value="0"/> .	<input type="text" value="0"/> .	<input type="text" value="0"/> .	<input type="text" value="0"/> ~	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

保存设置

应用

取消改动

关闭

已阻止的服务：您可以选择封禁某些服务。点击添加/编辑服务按钮更改这些设置。

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”旁边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设置，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. 路由器本身没有电池保持时钟运行，关闭路由器电源或路由器重启会导致路由器时钟暂时失效，路由器失效后，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。

3.3.5.2 数据流过滤

如果想阻止某些数据包通过路由器进入 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

启用数据包过滤

启用 禁用

策略

丢弃符合以下规则的数据包

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
<input type="checkbox"/>	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

方向

协议

源端口 -

目的端口 -

源地址 . . . /

目的地址 . . . /

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。

Output: 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。

3.3.6 NAT

3.3.6.1 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）。

端口转发

映射

应用程序	协议	允许的源IP范围	来源端口	IP地址	目的端口	启用
web	TCP	192.168.8.11	8000	192.168.1.12	80	<input checked="" type="checkbox"/>
ftp	两者	192.168.8.12	24	192.168.1.12	21	<input checked="" type="checkbox"/>

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，若是一个网段的 IP 地址可以以如下的形式表示如 172.168.2.0/24，其中 172.168.2.0 表示网段地址，24 表示子网掩码位数。

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**”。

3.3.6.2 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，路由器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。

端口范围转发

转发

应用程序	开始	结束	协议	IP地址	启用
web-tftp	800	8100	两者	192.168.1.16	<input checked="" type="checkbox"/>
	0	0	两者	0.0.0.0	<input type="checkbox"/>

添加 移除

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**”。

3.3.6.3 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。

非军事区 (DMZ)

DMZ

使用DMZ 启用 禁用

DMZ主机IP地址 192.168.1.

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”。

3.3.7 QoS 设置

3.3.7.1 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。

QoS设置

开启QoS 启用 禁用

端口

数据包调度器

上传 (kbps)

下载 (kbps)

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%。

3.3.7.2 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。

3.3.8 应用

3.3.8.1 串口应用

通常情况下路由器的 Console 口做控制台用。这个 Console 口也可以配置成普通串口使

用，Router 内置了串口转 TCP/IP 程序。通过配置，路由器的 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。

串口应用	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
波特率	115200 ▼
数据位	8 ▼
停止位	1 ▼
检验	无 ▼
流控	无 ▼

串口通信时的串口参数设置。

协议类型	TCP(DTU) ▼
服务端地址	120.42.46.98
服务端端口	55501
设备号码	12345678901
设备ID	12345678
心跳间隔	60

协议类型

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。

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：与路由器串口转 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：由 8 位的数字组成(只能是数字)，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，注意：这个是在 TCST 模式下才有用的

3.3.9 管理

3.3.9.1 管理

这一页面可以允许网络管理员管理特定的路由器功能，从而保证访问与安全。

路由器密码

路由器用户名	<input type="password"/>
路由器密码	<input type="password"/>
密码确认	<input type="password"/>

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路由器都应该基于输入正确的路由器密码，才可以访问和使用。

Web 访问

此功能允许您使用 HTTP 协议或 HTTPS 协议来管理路由器。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路由器的信息网页。那样就可以用密码保护此页（输入正确的用户名和密码）。

Web访问

协议	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
自动刷新（秒）	<input type="text"/>
登陆前显示系统信息网页	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
系统信息网页密码保护	<input type="checkbox"/> 已启用

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

远程管理

Web界面管理	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
使用HTTPS	<input type="checkbox"/>	
Web界面端口	<input type="text" value="8088"/>	(默认: 8088, 范围: 1 - 65535)
本地Web界面端口	<input type="text" value="90"/>	(默认: 80, 范围: 1 - 65535)
SSH管理	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
SSH远程端口	<input type="text" value="22"/>	(默认: 22, 范围: 1 - 65535)
Telnet管理	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	

Web 界面管理：此功能允许您通过互联网从远程位置管理路由器。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），远程管理路由器。如果你还没有设置密码，您还必须为您自己的路由器设置的默认密码。要远程管理路由器，进入 `http://xxx.xxx.xxx.xxx:8080`（x 代表的路由器的 Internet IP 地址，8080 代表指定的端口），在您的网页浏览器地址栏。你会被要求输入路由器的密码。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 来远程安全的访问路由器。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：

如果远程路由器的访问功能被启用，任何人知道路由器的 Internet IP 地址和密码，将可以改变路由器的设置。

Telnet 管理：启用或禁用远程 Telnet 功能

Cron	
Cron	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
Cron 附加任务	<input type="text"/>

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。

路由

路由	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
----	--

路由：如果你有设置 OSPF 或 RIP 路由，则选择启用就代表启用路由 OSPF 和 RIP 的路由守护进程。

语言选择

语言	<input type="text" value="简体中文 (Simplified Chinese)"/>
----	--

语言：设置路由器页面显示的语言类型，包括简体中文和英文。

3.3.9.2 保持活动

定时开关机

定时开关机

定时开关机	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
匹配	<input checked="" type="radio"/> 月天 <input type="radio"/> 周天 <input type="radio"/> 月时段 <input type="radio"/> 周时段
关机时间	00 : 00
关机日期	* - 01 - 星期天 - 星期天
开机时间	00 : 00
开机日期	* - 01 - 星期天 - 星期天

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。

定时开关机

定时开关机	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
匹配	<input type="radio"/> 月天 <input type="radio"/> 周天 <input checked="" type="radio"/> 月时段 <input type="radio"/> 周时段
关机时间	08 : 07
关机日期	* - 01 - 星期天 - 星期天
开机时间	09 : 07
开机日期	* - 01 - 星期天 - 星期天

定时重启

定时重启

定时重启	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
间隔 (秒)	<input checked="" type="radio"/> 3600
在设定的时间	<input type="radio"/> 00 : 00 - 星期天

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:

选择何时重新启动路由器。在管理标签中, **Cron** 选项必须被开启。

3.3.9.3 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

指令解释器

指令

运行命令
保存为启动指令
保存为关机指令
保存为防火墙指令

保存为自定义指令

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：您可以保存启动路由器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：您可以保存关闭路由器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。

3.3.9.4 出厂默认

复位路由器设置

恢复出厂默认 是 否

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”

3.3.9.5 固件升级

固件升级

刷新后，复位到 不复位

请选择一个用来升级的文件 浏览...

固件升级：可将新的固件加载到路由器上。新的固件版本将在 www.four-faith.com 上发布，并可免费进行下载。如果路由器没有出现问题，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：在升级路由器的固件时，可能会丢失其配置设置，因此，请确保在升级固件之前，先备份好路由器的设置信息。

刷新后，复位到：如果你想在升级后重置路由器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。

3.3.9.6 备份

本页面用于对路由器的配置文件进行备份或恢复。

备份配置

备份设置

点击“备份”按钮将配置备份文件下载到您的电脑。

恢复配置

恢复设置

请选择一个用来恢复的文件

【警】【告】

只能上传使用此固件并且相同型号路由器的备份文件。

请勿上传任何不是通过本界面创建的文件！

如欲对路由器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。

如欲恢复路由器的配置文件，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。

3.3.10 状态

3.3.10.1 路由器

系统

路由器名称	Four-Faith
路由器型号	Four-Faith Router
固件版本	FXXXX v1.0 (01/10/12) std - build 93
MAC地址	<u>00:AA:BB:CC:DD:45</u>
主机名	
WAN 域名	
LAN 域名	
当前时间	Sat, 01 Jan 2000 03:31:43
运行时间	3:31,

路由器名称: 即此路由器的名称, 可以在设置→基本设置中修改

路由器型号: 即此路由器的型号, 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: 路由器的主机名, 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

内存

所有可用	125240 kB / 131072 kB	 96%
空闲	97560 kB / 125240 kB	 78%
已使用	27680 kB / 125240 kB	 22%
缓冲区	2976 kB / 27680 kB	 11%
已缓存	10144 kB / 27680 kB	 37%
使用中	5232 kB / 27680 kB	 19%
非使用中	9912 kB / 27680 kB	 36%

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

网络

IP过滤器最大连接数	4096	
活动的IP连接	69	<div style="width: 2%; background-color: #4f81bd; height: 10px;"></div> 2%

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

3.3.10.2 WAN

连接类型 3G/UMTS

连接类型：包括 2 种方式：禁用，3G/UMTS。

已连接时间 0:20:28

已连接时间：已经连接上的时间，若没有连接上则问“不可用”

已连接时间	0:21:11
IP地址	192.168.13.92
子网掩码	255.255.255.255
网关	10.64.64.64
DNS 1	218.104.128.106
DNS 2	10.11.12.14
DNS 3	

IP 地址：路由器 WAN 口获取到的 IP 地址

子网掩码：路由器 WAN 口获取到的子网掩码

网关：路由器 WAN 口获取到的网关

DNS1, DNS2, DNS3：路由器 WAN 口获取到的第一 DNS, 第二 DNS, 第三 DNS

登录状态 已连接 断开连接

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	ZTE-EVDO MODULE
信号强度	 -79 dBm
网络类型	CDMA/HDR

模块类型：3G/UMTS 方式时的模块类型

信号强度：3G/UMTS 方式时的模块信号强度

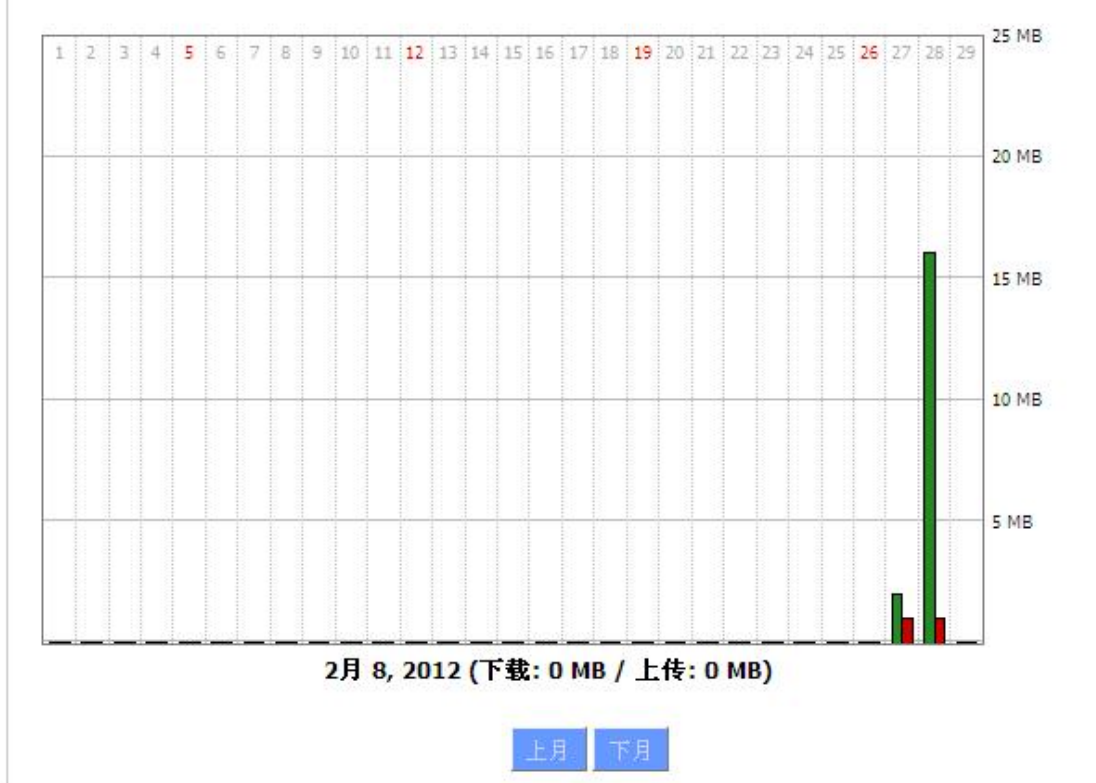
网络类型：3G/UMTS 方式时的模块的网络类型

流量

总流量

下载 (MBytes)	0
上传 (MBytes)	0

月流量



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

数据管理

- 备份
- 恢复
- 删除

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

3.3.10.3 LAN

LAN 状态

MAC地址	<u>00:0C:43:30:52:77</u>
IP地址	192.168.1.1
子网掩码	255.255.255.0
网关	0.0.0.0
本地DNS	0.0.0.0

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

活动的客户端

主机名	IP地址	MAC地址	连接数	比例 [4096]
*	192.168.1.120	<u>10:78:D2:98:C9:46</u>	40	1%

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

DHCP 状态

DHCP 服务器	已启用
DHCP 守护进程	DNSMasq
起始IP地址	192.168.1.100
结束IP地址	192.168.1.149
客户端租约时间	1440 分钟

DHCP 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

DHCP 客户端

主机名	IP地址	MAC地址	客户端租约时间	删除
Mycenae-PC	192.168.1.116	<u>00:25:56:68:5E:30</u>	1 day 00:00:00	
four-488e1df5fa	192.168.1.125	<u>44:37:E6:09:D8:F7</u>	1 day 00:00:00	


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

PPPOE 客户端

接口	用户名	Local IP	删除
ppp1	hometest	192.168.10.10	

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

L2TP 服务器

接口	Local IP	Remote IP	删除
ppp0	172.168.8.3	172.168.8.1	

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

L2TP 客户端

接口	用户名	Local IP	Remote IP	删除
ppp1	hometest	192.168.50.2	120.42.46.98	

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

PPTP 服务器

接口	Local IP	Remote IP	删除
ppp0	172.168.8.2	172.168.8.1	

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

PPTP 客户端

接口	用户名	Local IP	Remote IP	删除
ppp1	hometest	192.168.5.1	120.42.46.98	

接口: 系统拨号分配的接口

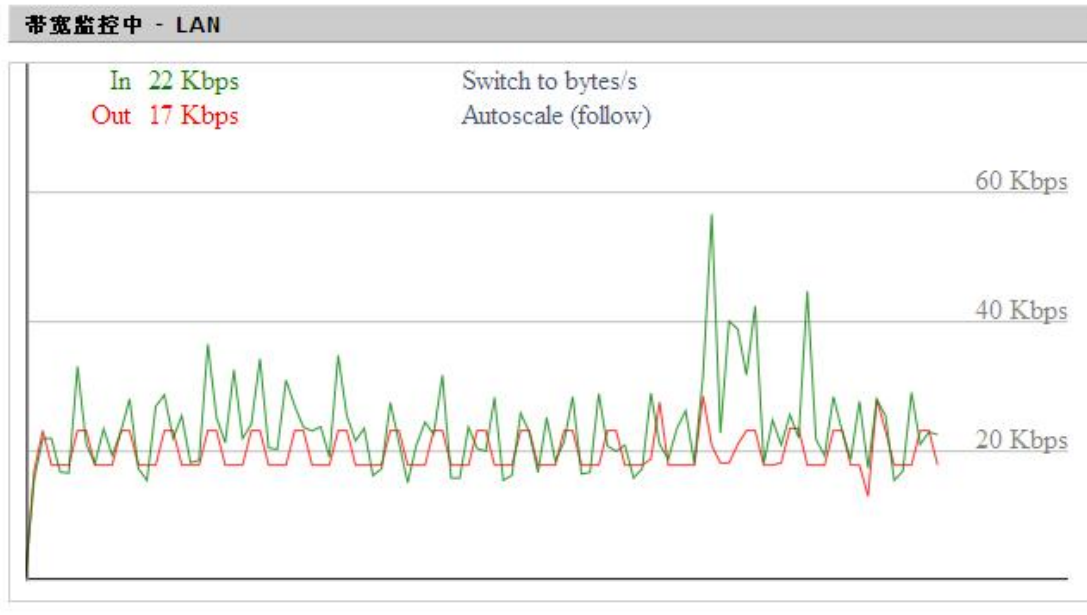
用户名: 客户端的用户名

Local IP: PPTP 客户端隧道 IP 地址

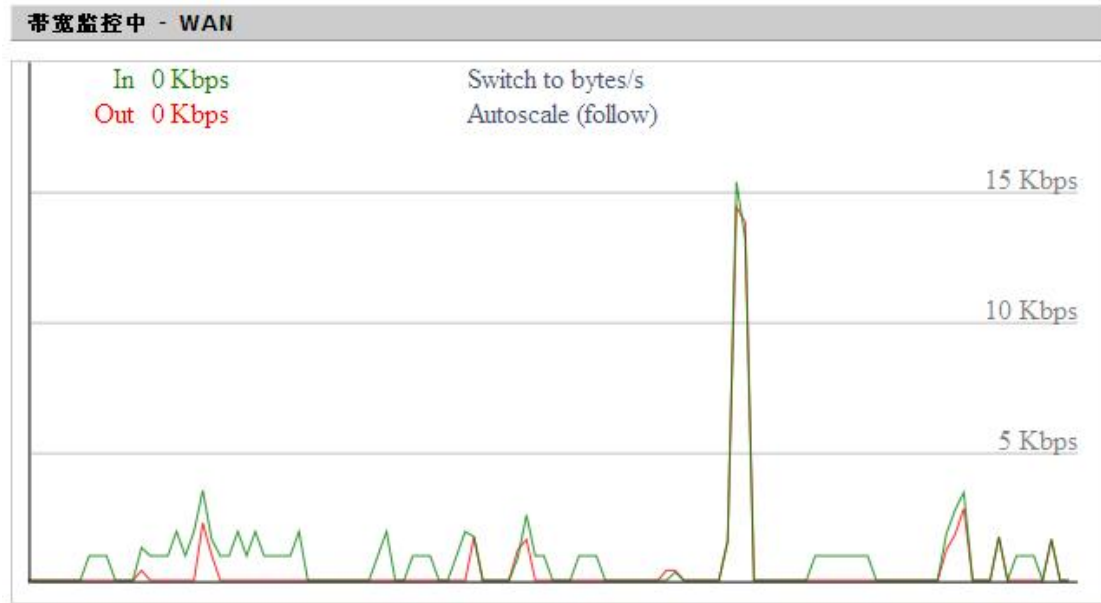
Remote IP: PPTP 客户端 IP 地址

删除: 点击可以删除 PPTP 客户端

3.3.10.4 宽带



LAN 口的时时检测状态图横坐标代表时间纵坐标代表速率



WAN 口的时时检测状态图横坐标代表时间纵坐标代表速率

3.3.10.5 系统信息

路由器	
路由器名称	Router
路由器型号	Four-Faith Router
LAN MAC	<u>00:0C:43:3F:05:0B</u>
WAN MAC	<u>00:0C:43:3F:05:0B</u>
WAN IP	0.0.0.0
LAN IP	192.168.1.1

路由器名称: 本机路由器的名称

路由器型号: 本机路由器的型号

LAN MAC: LAN 口的 MAC 地址

WAN MAC: WAN 口的 MAC 地址

WAN IP: WAN 口的 IP 地址

LAN IP: LAN 口的 IP 地址

服务

DHCP 服务器	已启用
ff-radauth	已禁用
USB支持	已禁用

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

内存

所有可用	122.3 MB / 128.0 MB
空闲	95.3 MB / 122.3 MB
已使用	27.0 MB / 122.3 MB
缓冲区	2.9 MB / 27.0 MB
已缓存	9.9 MB / 27.0 MB
使用中	5.1 MB / 27.0 MB
非使用中	9.7 MB / 27.0 MB

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

DHCP
DHCP 客户端

主机名	IP地址	MAC地址	客户端租约时间
*	192.168.1.143	xx:xx:xx:xx:DD:45	1 day 00:00:00
four-488e1df5fa	192.168.1.125	xx:xx:xx:xx:D8:F7	1 day 00:00:00
Mycenae-PC	192.168.1.116	xx:xx:xx:xx:5E:30	1 day 00:00:00

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

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. 选择连接到路由器 Console 口所采用的 PC 实际物理串口，选择“确定”

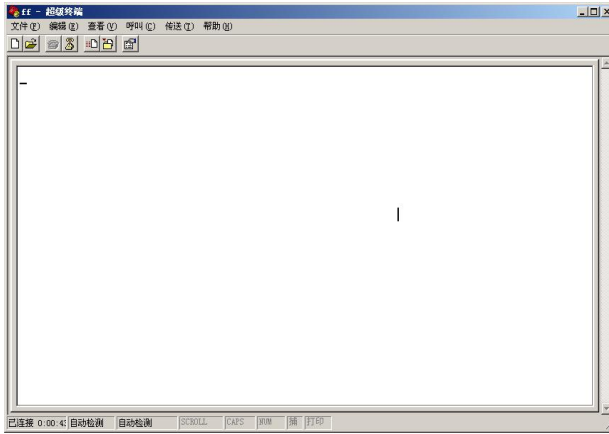


4. 如下图配置超级终端，并选择“确定”。

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。