

F5934 WIFI ROUTER 使用说明书	文档编号	产品版本	密级
		V1.0	
	产品名称： 路由器		共 82 页

# F5934 WIFI ROUTER 使用说明书

此说明书适用于下列型号产品：

型号	产品类别
F5934	WIFI ROUTER



## 厦门四信通信科技有限公司

Add: 中国厦门市软件园观日路 44 号 3 楼

客户热线: 400-8838 -199

电话: +86-592-6300320

传真: +86-592-5912735

网址 <http://www.four-faith.com>

## 文档修订记录

日期	版本	说明	作者
2012-5-16	V1.00	初始版本	ZYL

## 著作权声明

本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。



# 目录

第一章 产品简介.....	7
1.1 产品概述.....	7
1.2 产品特点.....	7
1.3 工作原理框图.....	8
1.4 产品规格.....	9
第二章 安装.....	11
2.1 概述.....	11
2.2 装箱清单.....	11
2.3 安装与电缆连接.....	11
2.4 电源说明.....	13
2.5 指示灯说明.....	13
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
3.3.1.1 基本设置.....	18
3.3.1.2 动态 DNS(DDNS).....	24
3.3.1.3 MAC 地址克隆.....	25
3.3.1.4 高级路由.....	25
3.3.1.5 VLANs.....	27
3.3.1.6 网络.....	27
3.3.2 无线.....	30
3.3.2.1 基本配置.....	30
3.3.2.2 无线安全.....	32
3.3.2.3 无线 MAC 过滤.....	35
3.3.2.4 高级设置.....	35
3.3.2.5 WDS.....	39
3.3.3 服务.....	40
3.3.3.1 服务.....	40
3.3.3.2 PPPoE 服务器.....	43
3.3.4 VPN.....	45
3.3.4.1 PPTP.....	45
3.3.4.2 L2TP.....	46
3.3.4.3 OPENVPN.....	47
3.3.4.4 IPSEC.....	51
3.3.5 安全.....	54
3.3.5.1 防火墙.....	54

3.3.5.2	VPN 穿越.....	57
3.3.6	访问限制.....	58
3.3.6.1	WAN 访问.....	58
3.3.7	NAT/QoS.....	60
3.3.7.1	端口转发.....	60
3.3.7.2	端口范围转发.....	61
3.3.7.3	端口触发.....	61
3.3.7.4	DMZ.....	62
3.3.7.5	QOS.....	62
3.3.8	管理.....	64
3.3.8.1	管理.....	64
3.3.8.2	保持活动.....	66
3.3.8.3	命令.....	66
3.3.8.4	出厂默认.....	67
3.3.8.5	固件升级.....	67
3.3.8.6	备份.....	67
3.3.9	状态.....	68
3.3.9.1	路由器.....	68
3.3.9.2	WAN.....	70
3.3.9.3	LAN.....	72
3.3.9.4	无线.....	75
3.3.9.5	宽带.....	77
3.3.9.6	系统信息.....	78
附录	.....	81

# 第一章 产品简介

## 1.1 产品概述

F5934 WIFI ROUTER 是一种物联网路由器,利用公用网络为用户提供数据传输功能。

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 (或 RS485/RS422)、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、定时上下线模式和定时开关机模式(仅特殊版本支持)
- ◆ 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 5~35V)

### 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
- ◆ 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

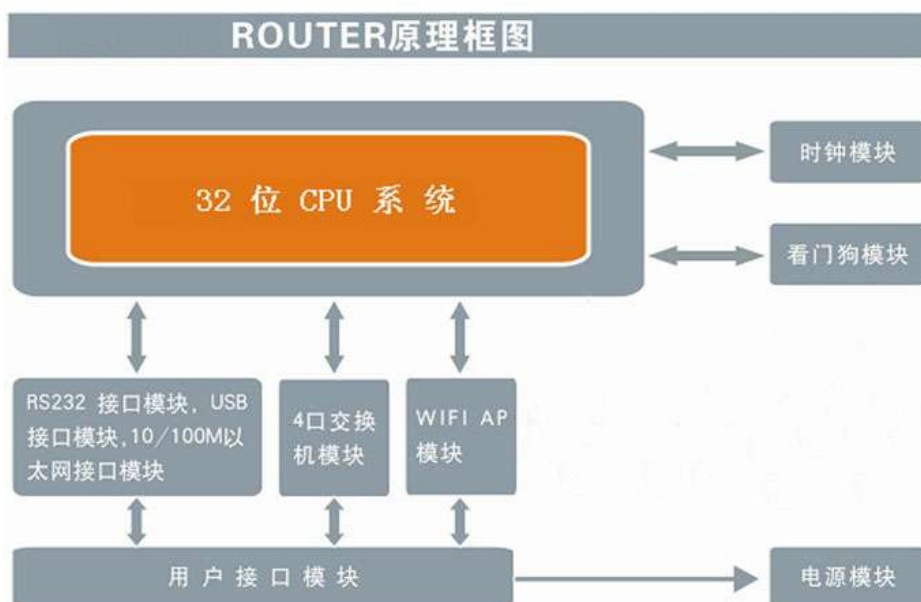
- ◆ 提供标准 RS232 (或 RS485/RS422)、以太网和 WIFI 接口,可直接连接串口设备、以太网设备和 WIFI 设备
- ◆ 提供标准有线 WAN 口(支持标准 PPPOE 协议),可直接连接 ADSL 设备
- ◆ 智能型数据终端,上电即可进入数据传输状态
- ◆ 提供功能强大的中心管理软件,方便设备管理(可选)
- ◆ 使用方便,灵活,多种工作模式选择
- ◆ 方便的系统配置和维护接口(包括本地和远端 WEB 和 CLI 方式)

### 功能强大

- ◆ 支持多种 WAN 连接方式，包括静态 IP, DHCP, L2TP, PPTP, PPPOE。
- ◆ 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, 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、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。
- ◆ 定时重启, 定时上下线功能。

## 1.3 工作原理框图

ROUTER 原理框图如下:





## 1.4 产品规格

### WIFI 无线参数

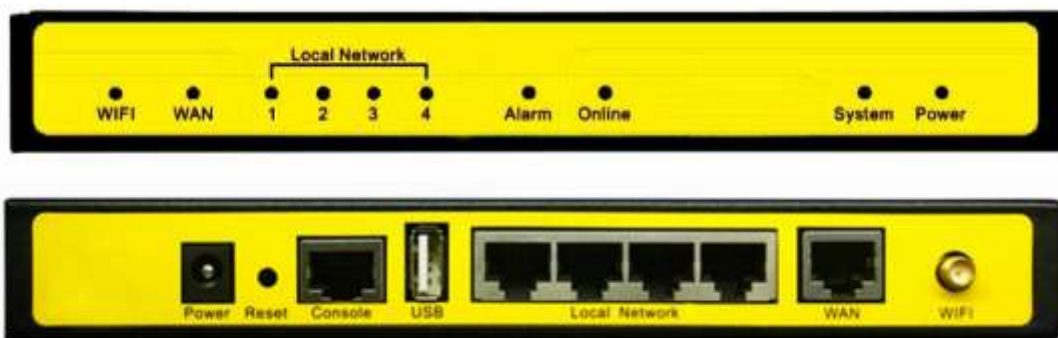
项 目	内 容
标准及频段	支持 IEEE802.11b/g/n 标准
理论带宽	IEEE802.11b/g: 最高速率达 54Mbps IEEE802.11n: 最高速率达 300Mbps
安全加密	支持 WEP、WPA、WPA2 等多种加密方式, 可选 WPS 功能
发射功率	21.5dBm (11g), 26dBm (11b)
接收灵敏度	<-72dBm@54Mbps

### 硬件系统

项 目	内 容
CPU	工业级 32 位通信处理器
FLASH	8MB (可扩展至 16MB)
RAM	64MB

### 接口类型

项 目	内 容
WAN 接口	1 个 10/100M 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 10/100M 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 (或 RS422/RS485), 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、2 位 校验: 无校验、偶校验、奇校验、SPACE 及 MARK 校验 串口速率: 110~230400bits/s
指示灯	具有“Power”、“System”、“Online”、“Alarm”、“Local Network”、“WAN”、“WLAN”、“信号强度指示灯”等指示灯
天线接口	WIFI: 标准 SMA 阳头天线接口, 特性阻抗 50 欧
电源接口	标准的 3 芯火车头电源插座, 内置电源反相保护和过压保护
Reset 复位按钮	通过此按钮, 可将 ROUTER 的参数配置恢复为出厂值
USB 接口	标准 A 型 USB host 接口 (预留)



**供电**

项 目	内 容
标准电源	DC 12V/1.5A
供电范围	DC 5~35V
通信电流	<450mA (12V)

**物理特性**

项 目	内 容
外壳	金属外壳，保护等级 IP30。外壳和系统安全隔离，特别适合工控现场应用
外形尺寸	206x135x28 mm (不包括天线和安装件)
重量	790g

**其它参数**

项 目	内 容
工作温度	-25~+70°C (-13~+158°F)
扩展工作温度	-30~+75°C (-22~+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：

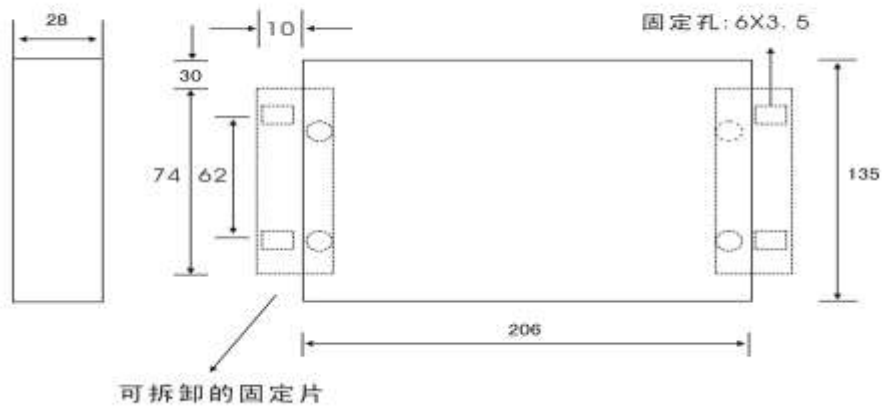
- ◇ ROUTER 主机 1 台
- ◇ WIFI 天线（SMA 阴头）1 根
- ◇ 配套电源 1 个
- ◇ 以太网直连线 1 条
- ◇ 使用说明书光盘 1 张
- ◇ RS232 控制台线 1 条（选配）
- ◇ 产品合格证
- ◇ 产品保修卡

### 2.3 安装与电缆连接

外形尺寸：

外形尺寸如下图。（单位:mm）

## 安装指示图



### 天线安装:

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。

### 安装电缆:

将网络直连线的一端插到 ROUTER 的交换机接口上（标识为“Local Network”），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
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

将 RS232 控制台线的 RJ45 端插到 ROUTER 的 RS232 接口上（标识为“Console”），另一端插到用户设备的 RS232 串行接口上。RS232 控制台线的信号连接如下：

RJ45	DB9F
1	8
2	6
3	2
4	1
5	5
6	3
7	4
8	7

DB9F 串行通信接口信号定义如下表：

引脚	RS232 信	描述	相 对 于
----	---------	----	-------

**厦门四信通信科技有限公司**

Page 12 of 82

Add: 中国厦门市软件园二期观日路 44 号 3 层

http: //www.four-faith.com

客服热线: 400-8838-199

Tel: 0592-6300320

Fax: 0592-5912735

	号名称		ROUTER 的方向
1	DCD	载波信号检测	输出
2	RXD	接收数据	输出
3	TXD	发送数据	输入
4	DTR	数据终端准备好	输入
5	GND	电源参考地	
6	DSR	数据设备准备好	输出
7	RTS	请求发送	输入
8	CTS	数据设备准备好接收数据	输出

## 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 12VDC/1.5A 电源适配器给 ROUTER 供电，也可以直接用直流 5~35V 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 35V），并保证电源功率大于 7W 以上。

推荐使用标配的 12VDC/1.5A 电源。

## 2.5 指示灯说明

ROUTER 提供以下指示灯：“Power”、“System”、“Online”、“Alarm”、“Local Network”、“WAN”、“WLAN”、“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
Alarm	亮	正在存参数或者升级
	灭	设备无报警
Local Network	灭	相应交换机接口未连接
	亮/闪烁	相应交换机接口已连接/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
WLAN	灭	WLAN 未启动
	亮	WLAN 已启动

## 2.6 复位按钮说明

ROUTER 设有一个复位按钮，标识为“Reset”。该按钮的作用是将 ROUTER 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，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：“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

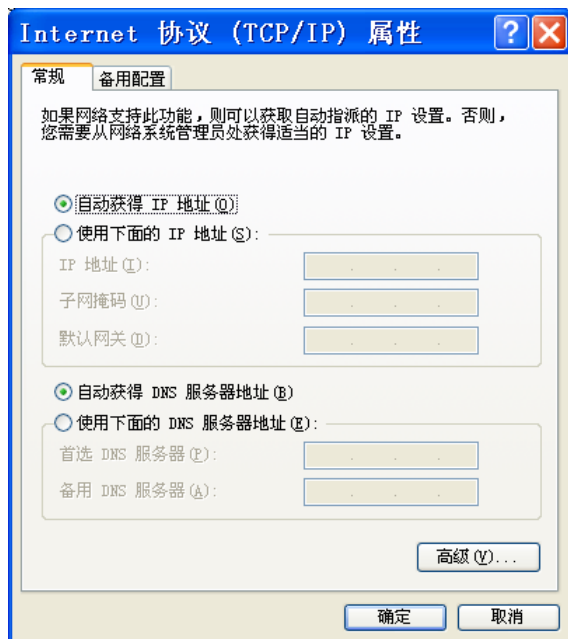
在对路由器进行配置前，需要将路由器和用于配置的 PC 通过出厂配置的网络线或 WIFI 连接起来。用网络线连接时，网络线的一端连接路由器“Local Network”（以下简称 LAN 口）的任意一个以太网接口，另外一端连接到 PC 的以太网口。用 WIFI 连接时，路由器出厂默认的 SSID 为“FOUR-FAITH”，无须密码验证。



### 3.2 登录到配置页面

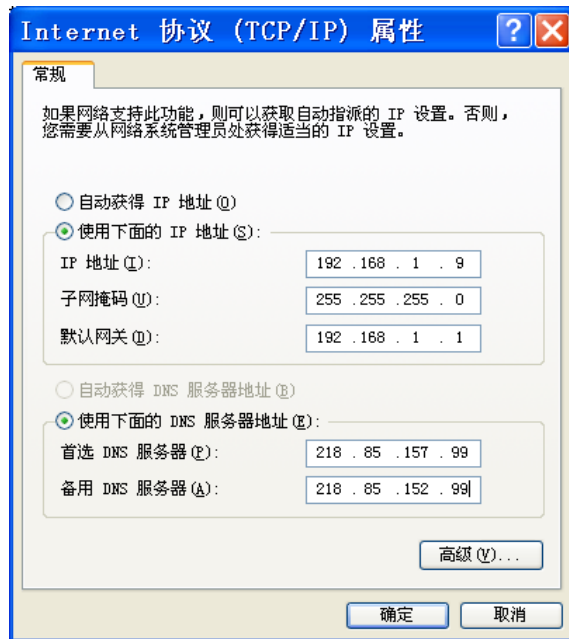
#### 3.2.1 PC 机 IP 地址设置（两种方式）

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 192.168.1.9(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。一共有九个主页面，即：设置、无线、服务、VPN、安全、访问限制、NAT/QoS、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”按钮予以生效

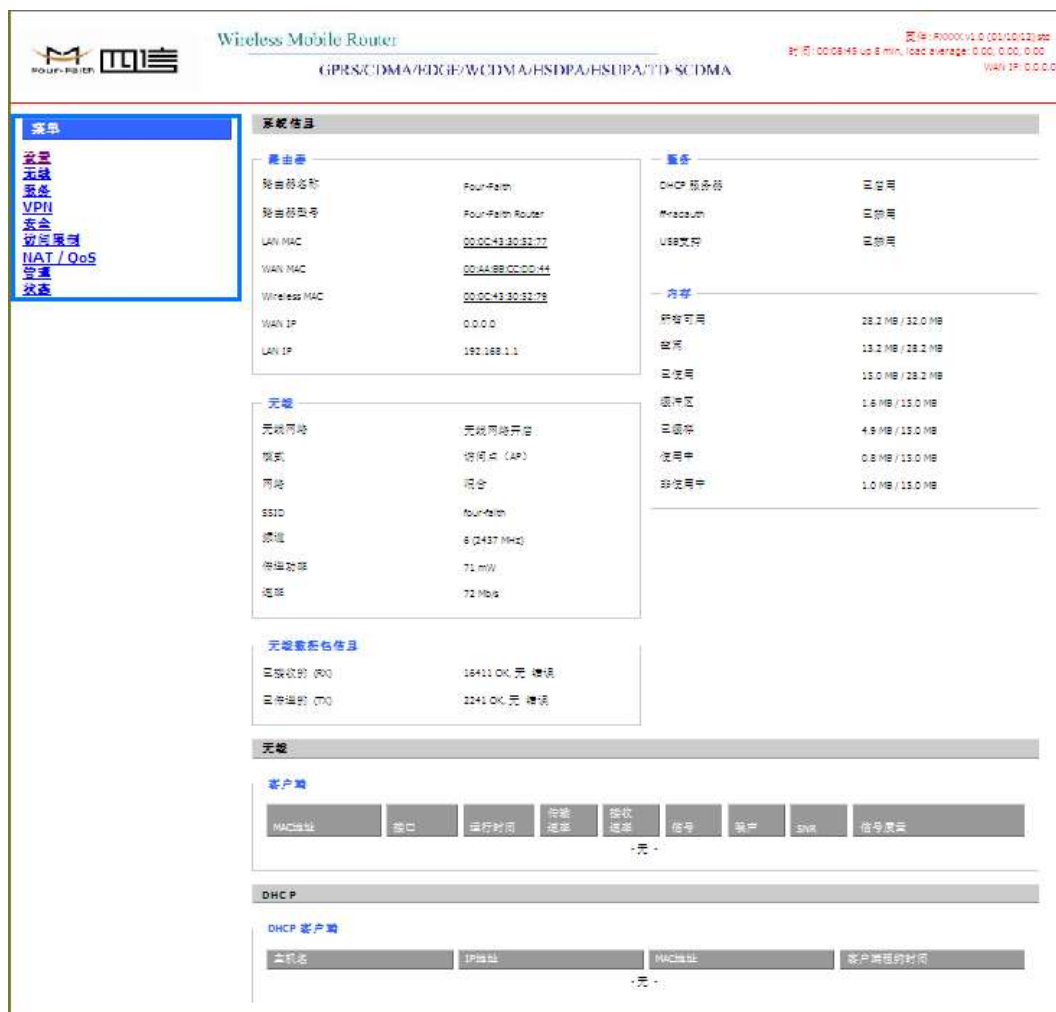
**您的路由器目前不受保护且使用不安全的预设用户名和密码组合，请使用以下对话框修改！**

**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

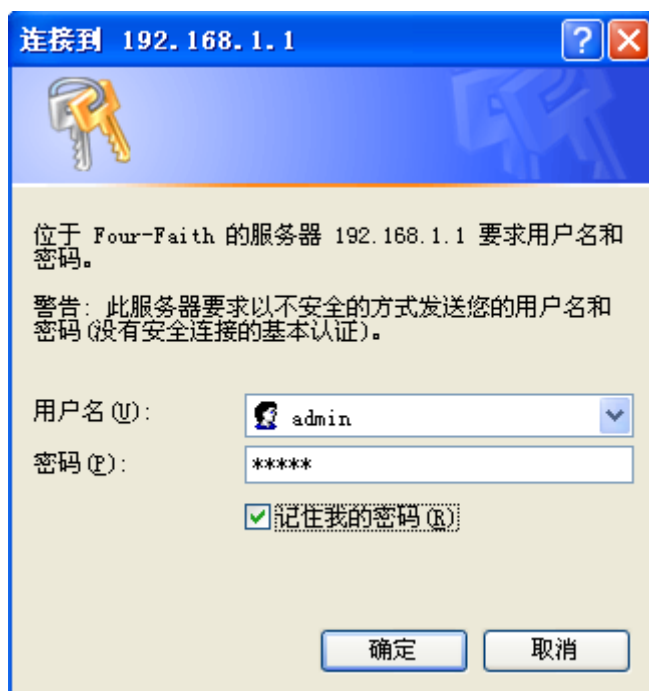




The screenshot shows the configuration page for a Four-Faith Wireless Mobile Router. The interface includes a sidebar menu with options like '首页', '无线', '安全', 'VPN', 'NAT/QoS', '管理', and '状态'. The main content area is divided into several sections:

- 系统信息 (System Information):** Displays router details such as name (Four-Faith), model (Four-Faith Router), LAN MAC, WAN MAC, Wireless MAC, WAN IP (0.0.0.0), and LAN IP (192.168.1.1).
- 无线 (Wireless):** Shows wireless settings including mode (无线局域网), SSID (four-faith), channel (9), and power (71 mW).
- 无线兼容信息 (Wireless Compatibility Information):** Lists supported standards like 802.11n and 802.11g.
- 客户端 (Clients):** A table showing connected devices with columns for MAC address, interface, connection time, connection type, signal strength, and client name.
- DHCP 客户端 (DHCP Clients):** A table showing DHCP-assigned clients with columns for client name, IP address, MAC address, and connection time.

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 6 种方式：禁用，静态 IP，自动配置-DHCP，PPPOE，PPTP，L2TP。

##### 方式一：禁用

连接类型

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路由器上。

连接类型	<input type="text" value="静态IP"/>
WAN IP地址	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
子网掩码	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
网关	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
静态DNS 1	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
静态DNS 2	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
静态DNS 3	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

**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

**子网掩码：** 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

路由器默认的 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

[厦门四信通信科技有限公司](http://www.four-faith.com)

Page 18 of 82

Add: 中国厦门市软件园二期观日路 44 号 3 层

http: //www.four-faith.com

客服热线: 400-8838-199

Tel: 0592-6300320

Fax: 0592-5912735

深圳天威视讯，上海有线通等。

连接类型 自动配置 - DHCP

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路由器上。

连接类型	<span style="border: 1px solid black; padding: 2px;">PPPoE</span>	
用户名	<input type="text"/>	
密码	<input type="password"/>	<input type="checkbox"/> 显示密码
服务名称	<input type="text"/>	
PPP压缩	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	
兼容VDSL前置解调器	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	
MPPE加密	<input type="text"/>	
单链路多连接	<input type="checkbox"/>	

**用户名：** 用于登录到 Internet 的用户名。

**密码：** 用于登录到 Internet 的密码。

**服务器名称：** ISP 提供的服务器名称，若无，则为空

**PPP 压缩：** PPP 压缩提供了一种方法来协商和使用压缩在 PPP 封装链路协议

**兼容 VDSL 前置解调器：** 若启用支持前端的调制解调器是 vdsl

**MPPE 加密：** MPPE 代表微软点至点的加密。它是用于点至点链接传输的加密数据报的协议

**单链路多连接：** 为单链路连接启用或禁用多重链接

#### 方式五：PPTP

连接类型	<input type="text" value="PPTP"/>
使用DHCP	<input type="radio"/> 是 <input checked="" type="radio"/> 否
WAN IP地址	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
子网掩码	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
网关	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
网关 (PPTP服务)	<input type="text"/>
用户名	<input type="text"/>
密码	<input type="text"/> <input type="checkbox"/> 显示密码
PPTP加密	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
是否禁用数据包重新排列	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
额外的PPTP选项	<input type="text"/>

**使用 DHCP:** 使用 DHCP 的方式来获取 IP 地址, 然后在采用 PPTP 方式连接到服务器

**网关 (PPTP 服务):** 用户根据自己或者 ISP 分配而设置的网关 (PPTP 服务)

**用户名:** 用于登录到 Internet 的用户名。

**密码:** 用于登录到 Internet 的密码。

**PPTP 加密:** 为 PPTP 数据加密

**是否禁用数据包重新排列:** 启用或者禁用数据包重新排列功能

**额外的 PPTP 选项:** 为 PPTP 客户端增加额外的 PPTP 功能选项, 根据需要设置

#### 方式六: L2TP

连接类型	<input type="text" value="L2TP"/>
用户名	<input type="text"/>
密码	<input type="text"/> <input type="checkbox"/> 显示密码
L2TP服务器	<input type="text"/>
允许CHAP认证协议	<input checked="" type="radio"/> 是 <input type="radio"/> 否
拒绝PAP认证协议	<input checked="" type="radio"/> 是 <input type="radio"/> 否
允许认证协议	<input checked="" type="radio"/> 是 <input type="radio"/> 否

**用户名:** 用于登录到 Internet 的用户名。

**密码:** 用于登录到 Internet 的密码。

**L2TP 服务器:** 用户根据自己或者 ISP 分配而设置的 L2TP 服务器

**允许 CHAP 认证协议:** 开启或禁用允许 CHAP 认证协议

**允许 PAP 认证协议:** 开启或禁用拒绝 PAP 认证协议

**允许认证协议:** 开启或禁用允许认证协议

## 在线保持

在线保持方式

在线保持检测时间间隔  秒

在线保持检测主服务器IP  .  .  .

在线保持检测副服务器IP  .  .  .

这个功能用于检测 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。

### 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。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。只有当“在线保持方式”设置成“Ping”或者“Route”时，此配置项才有效。

## 连接策略

连接策略

按需连接：最大空闲时间  分

保持活动：重拨周期  秒

**按需连接：**选择手动按需连接，如果在指定的最大空闲时间没有网络访问流量通过路由器，连接会自动断开，最大空闲时间可以手动设置，默认 5 分钟。您也可以在状态→WAN 页面点击“断开连接”按钮手动断开连接。连接断开后不会自动重连，除非您再次点击状态→WAN 页面“连接”按钮手动重连。

**保持活动：重新拨号周期。**该选项可以确保您持续连接到 Internet，即使连接站点处于空闲状态也保持连接状态。要使用该选项，请单击保持活动旁边的单选按钮。默认重新拨号周期为 30 秒（换句话说，路由器将每周期检查一次 Internet 连接）。

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

## 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	<input type="text" value="Four-Faith"/>
主机名	<input type="text"/>
域名	<input type="text"/>
MTU	<input type="text" value="Auto"/> <input type="text" value="1500"/>

**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

网络设置部分可以对连接到路由器以太网端口上的网络设置进行修改。

本地 IP 地址	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
子网掩码	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
网关	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
本地 DNS	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

**本地 IP 地址：**表示可以由您的局域网看到的路由器 IP 地址

**子网掩码：**表示可以由您的局域网看到的路由器 IP 地址子网掩码。

**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

**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	<input type="button" value="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. <input type="text" value="100"/>
最大DHCP用户数	<input type="text" value="50"/>
客户端租约时间	<input type="text" value="1440"/> 分钟
静态DNS 1	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
静态DNS 2	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
静态DNS 3	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
WINS	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="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	<input type="button" value="DHCP 转发器"/>
DHCP 服务器	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="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 192.168.1.2 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，则要在这一输入该服务器的 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

### 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

用户名

密码   显示密码

主机名

类型

通配符

不使用外部IP检测  是  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

---

克隆 WAN 口 MAC

---

克隆无线 MAC

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	1 ( )	删除
路由名称	<input type="text"/>	
跃点数	<input type="text" value="0"/>	
目的LAN IP	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	
子网掩码	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	
网关	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	
接口	LAN & WLAN	
显示路由表		

**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 VLANs

VLAN	端口					指派到网桥
	W	1	2	3	4	
0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN <input type="button" value="v"/>
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	无 <input type="button" value="v"/>

VLANs 功能是可以根据用户自己的意愿来划分不同的 VLAN 口，系统中支持 VLAN0-VLAN15 这个 16 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

[厦门四信通信科技有限公司](http://www.four-faith.com)

Page 27 of 82

Add: 中国厦门市软件园二期观日路 44 号 3 层

http: //www.four-faith.com

客服热线: 400-8838-199

Tel: 0592-6300320

Fax: 0592-5912735

**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	vlan0 ra0

**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  Interface  Prio

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

**指派到网桥**

Assignment 0 br1  Interface ra0  Prio 63

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：

**当前桥接列表**

网桥名	启用STP	接口
br0	no	vlan0
br1	no	ra0

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**

网络配置 eth2	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 预设
网络配置 vlan0	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 预设
网络配置 ra0	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 预设
网络配置 apcli0	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 预设
网络配置 wds0	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 预设
网络配置 wds1	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 预设
网络配置 wds2	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 预设
网络配置 wds3	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 预设
网络配置 br0	<input type="radio"/> 未桥接	<input checked="" type="radio"/> 预设

**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	<input checked="" type="radio"/> 未桥接 <input type="radio"/> 预设
MTU	<input type="text" value="1500"/>
组播转发	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
Masquerade / NAT	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
IP地址	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
子网掩码	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="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

**多路DHCP服务器**

DHCP 0	<input type="text" value="ra0"/> ▼	<input type="text" value="On"/> ▼	Start	<input type="text" value="100"/>	Max	<input type="text" value="50"/>	Leasetime	<input type="text" value="3600"/>
<input type="button" value="删除"/>								
<input type="button" value="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：**只能一个配置玩后在点击保存，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

**无线物理接口 w10 [2.4 GHz]**

无线网络  启用  禁用

**物理接口 ra0 - SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]**

无线模式 访问点 (AP) ▼

无线网络模式 仅N ▼

802.11n 传输模式 混合 ▼

无线网络名 (SSID) dd-junjinlee

无线频道 11 - 2.462 GHz ▼

频道宽度 40 MHz ▼

宽频 upper ▼

无线SSID广播  启用  禁用

网络配置  未桥接  已桥接

**虚拟接口**

添加

保存设置
应用
取消改动

**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。

**802.11n 传输模式：** 在无线网络模式为”仅 N”时，选择其传输模式：

**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：桥接到路由器上，一般情况下，请选择已桥接。

未桥接：没有桥接到路由器上，IP 地址需要手动配置。

网络配置	<input checked="" type="radio"/> 未桥接 <input type="radio"/> 已桥接
组播转发	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
Masquerade / NAT	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
IP地址	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
子网掩码	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>

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。

**虚拟接口**

虚拟接口 ra1 SSID [dd-wrt\_vap] HWAddr [00:AA:BB:CC:DD:16]

无线网络名 (SSID)	<input type="text" value="dd-wrt_vap"/>
无线SSID广播	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
AP 独立	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
网络配置	<input type="radio"/> 未桥接 <input checked="" type="radio"/> 已桥接

**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。

**无线安全 w10**

物理接口 ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

安全模式	<input type="text" value="已禁用"/>
------	----------------------------------



## 无线安全 w10

物理接口 ra0 SSID [four-faith] HWAddr [00:0C:43:30:52:79]

安全模式	WEW
鉴权类型	<input checked="" type="radio"/> 开放式 <input type="radio"/> 共享密钥
默认传输密钥	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4
加密	64 bits 10 hex digits/5 ASCII
ASCII/HEX	<input type="radio"/> ASCII <input checked="" type="radio"/> HEX
通行短语	1111111111111111 <input type="button" value="Generate"/>
密钥 1	2627F68597
密钥 2	15AD1DD294
密钥 3	DDC4761939
密钥 4	31F1ADB558

**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路由器根据输入的通行短语生成。

## 无线安全 w10

物理接口 ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

安全模式	WPA Personal
WPA算法	AES
WPA共享密钥	..... <input type="checkbox"/> 显示密码
密钥更新时间间隔 (秒)	3600 (预设: 3600, 范围: 1 - 99999)



**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。

物理接口 ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

安全模式	WPA Enterprise
WPA算法	AES
Radius鉴权服务器地址	192 . 168 . 1 . 110
Radius鉴权服务器端口	1812 (预设: 1812)
Radius鉴权共享密钥	..... <input type="checkbox"/> 显示密码
密钥更新时间间隔(秒)	3600

**WPA Enterprise/WPA2 Enterprise/WPA2 Enterprise Mixed:** 企业 WPA/WPA2 加密，路由器需连接 Radius 验证服务器。

**WPA 算法:** AES/TKIP/TPIP+AES。

**Radius 鉴权服务器地址:** 连接到路由器的 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 服务器和路由器之间的共享密钥。

**密钥更新时间间隔(秒):** 1-99999。

#### 无线安全 w10

物理接口 ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

安全模式	802.1x
XSupplicant类型	<input type="radio"/> Peap <input checked="" type="radio"/> TTLS
用户	<input type="text"/>
匿名验证	<input type="text"/>
密码	<input type="text"/>
第二认证	<input type="text"/>
公共服务器端认证	<input type="text"/>
其它网络配置	<input type="text"/>

**802.1x :** 802.1x 协议是基于 Client/Server 的访问控制和认证协议。它可以限制未经授权的用户/设备通过接入端口(access port)访问 LAN/WLAN。

**Peap:** PEAP (受保护的可扩展验证协议) 是一种用于在无线网络和点至点连接，认证协议 EAP 的版本。PEAP 是 802.11 的 WLAN (无线局域网) 支持 802.1X 端口访问控制，以提供更安全的身份验证。这里用的是 PEAP-EAP-MS-CHAPv2 的。

1. 输入用户名。
2. 输入密码。

**TTLS:** TTLS 使用 TLS 通道交换“属性 - 值对”(的 AVP)，很像的 RADIUS。(事实上，

AVP 的编码格式是非常类似的半径。)的信息的一般编码允许一个 TTLS 服务器验证的 AVP 对任何类型的身份验证机制。目前的 TTLS 实现支持的 EAP，以及一些老方法（CHAP，PAP 的，MS-CHAP 和 MS-CHAPv2 的）中定义的所有方法。TTLS 的，可以很容易地扩展新的协议通过定义新的属性，以支持新的协议。

1. 输入用户名。
2. 输入密码。
3. 输入公共服务器证书内容。

### 3.3.2.3 无线 MAC 过滤

无线 Mac 过滤可通过编辑 mac 地址，允许或禁止无线设备与路由器无线通信。

**无线MAC过滤**

ra0 - MAC过滤

开启过滤  启用  禁用

过滤模式

阻止所列客户端访问无线网络

只允许所列客户端访问无线网络

[编辑MAC过滤列表](#)

保存设置
应用
取消改动

**开启过滤：**默认禁用。选择启用，开启无线 MAC 过滤。

**过滤模式：**

**阻止所列客户端访问无线网络：**MAC 过滤列表中的无线设备不能与路由器无线通信。

**只允许所列客户端访问无线网络：**禁 MAC 地址列表外的无线设备与路由器无线通信。

点出“编辑 MAC 过滤列表”，编辑 MAC 地址列表，在弹出的页面，填入允许/禁止与路由器无线通信的设备的 MAC 地址。编辑完后，请点击“保存”按钮。然后点出此页面，“保存设置”，“应用”按钮。取消改动，点击“取消改动”按钮。

### 3.3.2.4 高级设置

本页面用路由器无线高级功能的设置。这些配置，请谨慎配置，不正确的配置会降低无线的性能。

## 高级无线设置

高级设置		
基本速率	<input type="button" value="预设"/>	(预设: 预设)
MIMO - 固定传输速率	<input type="button" value="自动"/>	(预设: 自动)
固定传输速率	<input type="button" value="自动"/>	(预设: 自动)
CTS 保护模式	<input checked="" type="radio"/> 自动 <input type="radio"/> 禁用	(预设: 自动)
帧突发	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
发射站间隔	<input type="text" value="100"/>	(预设: 100ms, 范围: 10 - 65535)
DTIM 间隔	<input type="text" value="1"/>	(预设: 1, 范围: 1 - 255)
分片阈值	<input type="text" value="2346"/>	(预设: 2346, 范围: 256 - 2346)
RTS 阈值	<input type="text" value="2347"/>	(预设: 2347, 范围: 0 - 2347)
最大关联客户端数	<input type="text" value="128"/>	(预设: 128, 范围: 1 - 256)
AP 独立	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	(预设: 禁用)
传送天线	<input type="button" value="自动"/>	(预设: 自动)
接收天线	<input type="button" value="自动"/>	(预设: 自动)
前导码	<input type="button" value="长"/>	(预设: 长)
Shortslot Override	<input type="button" value="自动"/>	(预设: 自动)
传送功率	<input type="text" value="71"/>	(预设: 71, 范围: 1 - 251mW)
界面无线访问	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	(预设: 启用)

**基本速率:** 默认值是设置为预设。根据您所选择的无线模式，设置默认支持的数据传输速率。默认设置将确保所有设备的最大兼容性。您也可以选择所有的数据传输速率，这时应选择所有。若是较老的 Wireless-B 设备的兼容性，选择 1-2Mbps。

**MIMO-固定传输速率:** 默认设置是自动。范围是从 13.5 到 270Mbps。设置应取决于您的无线网络的高速数据传输速率。您可以选择一个传输速度的范围内，或保留默认设置，“自动”，路由器会自动使用尽可能快的数据传输速率和启用自动回归的特点。自动回归谈判最好的路由器和无线客户端之间的连接速度。

**固定传输速率:** 默认设置是自动。范围是从 1 到 54Mbps。设置应取决于您的无线网络的高速数据传输速率。您可以选择一个传输速度的范围内，或保留默认设置，“自动”，路由器会自动使用尽可能快的数据传输速率和启用自动回归的特点。自动回归谈判最好的路由器和无线客户默认值是禁用。当设置为自动，保障机制，将确保您的无线-B 设备连接到无线-G 路由器，当存在很多的无线-G 设备时。这时您的无线-G 设备的性能可能会下降。端之间的连接速度。

**CTS 保护模式:** 默认值是禁用。当设置为自动，保障机制，将确保您的无线-B 设备连接到无线-G 路由器，当存在很多的无线-G 设备时。这时您的无线-G 设备的性能可能会下降。

**帧突发:** 默认值是禁用。帧突发允许包损坏, 这会增加整个网络的速度虽然这只是建议约 1-3 无线客户端, 也可以形成是消极的结果和吞吐量会受到影响。

**发射站间隔:** 默认值是 100。输入值 1 到 65535 之间, 单位毫秒。发射站间隔值表示的发射站的频率间隔。一个发射站间隔是由路由器的数据包广播同步无线网络。 在接收欠佳下, 建议设置 50。

**DTIM 间隔:** 默认值是 1。此值在 1 和 255 之间, 表明传输指示消息 (DTIM) 的间隔。一个 DTIM 字段是倒计的, 当路由器有广播或组播消息缓冲去关联的客户端, 他通知一个客户在下一个窗口中收听广播和多播消息, 它将发送未来的 DTIM 与 DTIM 间隔值。客户端听到发射站的唤醒而后接收广播和多播消息。

**分片阈值:** 此值应保持在 2346 的默认设置。范围为 256-2346 字节。它指定一个数据包的最大尺寸数据在没有被分割成多个数据包之前。如果您遇到高封包错误率, 你可能会稍微增加的分段阈值。设置分段阈值太低, 可能会导致网络性能不佳。这个值建议不要修改。

**RTS 阈值:** 此值应保持在其 2347 的默认设置。范围是 0-2347 字节。如果您遇到不一致的数据流, 只建议稍微改动。如果一个网络数据包是比预设的 RTS 阈值小, 则不会启用 RTS/CTS 机制。路由器发送请求发送 (RTS) 帧到一个特定的接收站和协商发送一个数据帧。收到 RTS 后, 无线设备有了明确的响应发送 (CTS) 帧承, 则开始传输。

**最大关联客户端:** 可连接最多客户端数, 1-128。

**AP 独立:** 默认值是关闭。此设置隔离无线客户端, 所以与其它无线客户端的访问都停止了。

**传送天线/接收天线:** 值有自动, 左, 右, 默认值是自动。这是用来与外部天线一起给他们最佳的性能。左边和右边的天线, 在某些型号的路由器可能要根据你自己的需求来调整。

**前导码:** 值是长, 短, 自动, 默认值是长。如果您的无线设备支持前导码, 当它与其他 802.11b 设备进行通信遇到的困难, 则应确保它是使用长的类型。

**界面无线访问:**默认值是启用。设置允许从无线客户端 (GUI) 访问的路由器的设置,。如果你想阻止所有的无线客户端访问设置页面, 请禁用。



**无线网络时间限制:** 从无线网络时间限制的设置可以构成一个无线网络时间。默认情况下, 时间限制是不活跃, WLAN 是永久的。启用时间限制, 如果你想一天工作几个小时后的关闭 WLAN。时段内的 WLAN 是被标记为绿色, 而红色表示关闭。点击各自小时的开和关之间切换。

**无线网络时间限制**

 无线网络调度  启用  禁用 (预设: 禁用)

**无线多媒体支持设置**

 无线多媒体支持  启用  禁用 (预设: 启用)

 无ACK  启用  禁用 (预设: 禁用)

**EDCA AP参数 (AP到客户端)**

	CWmin	CWmax	AIFSN	TXOP(b)	TXOP(a/g)	管理员强制
后台	15	1023	7	0	0	<input type="checkbox"/>
尽力达到	15	63	3	0	0	<input type="checkbox"/>
视频	7	15	1	6016	3008	<input type="checkbox"/>
语音	3	7	1	3264	1504	<input type="checkbox"/>

**EDCA STA参数 (客户端到AP)**

	CWmin	CWmax	AIFSN	TXOP(b)	TXOP(a/g)	管理员强制
后台	15	1023	7	0	0	<input type="checkbox"/>
尽力达到	15	1023	3	0	0	<input type="checkbox"/>
视频	7	15	2	6016	3008	<input type="checkbox"/>
语音	3	7	2	3264	1504	<input type="checkbox"/>

**WMM传送Retry限制, fallback限制和最大速率参数。**

	S. Retry	S. Fallbk	L. Retry	L. Fallbk	最大数率
后台	7	3	4	2	0
尽力达到	7	3	4	2	0
视频	7	3	4	2	0
语音	7	3	4	2	0

**无线多媒体支持:** 启用 Wi - Fi 多媒体功能。配置 QoS 功能, 包括设置在不同类型的无线通信的现有队列的参数。传输的数据包被要求送到媒体, 基于每个队列可以配置不同的最低和最高的等待时间。队列自动提供语音, 视频, 多媒体, 和任务关键应用程序的最小传输延迟, 并尽力依靠传统的 IP 数据参数。

**无 ACK:** 这是指在 MAC 层使用的无校验。启用无 ACK, 可能会导致效率更高的吞吐量, 但错误率较高, 特别在在嘈杂的射频 (RF) 的环境。

**EDCA AP 参数 (AP 到客户端):** 这会影响到接入点到用户端站的流量。

**EDCA STA 参数 (客户端到 AP):** 这会影响到流量数据从客户端站的接入点。

**后台:** 优先级为“低”高吞吐量。需要最大的吞吐量和时间敏感的批量数据发送到该队列 (例如: FTP 数据)。

**尽力达到:** 优先级为“中等”中等吞吐量和延迟。大多数传统 IP 数据发送到该队列。

**视频:** 级为“高”最小延迟。时间敏感的视频数据自动发送到该队列。

**语音:** 优先级为“高”如 VoIP 和流媒体的时间敏感的数据自动发送到该队列。

**CWmin:** 小竞争窗口。此参数是输入的算法, 它决定传输重试初始随机退避等待时间 (“窗口”)。最小竞争窗口中指定的值是一个确定的范围从最初的随机退避等待时间 (毫秒) 的上限。第一个随机数生成的是一个介于 0 和这里指定的号码。如果第一个随机退

避等待时间到期前的数据帧被发送，一个重试计数器是递增和随机退避值（窗口）的一倍。随机退避值的大小，直到达到最大竞争窗口中定义的数量翻番将继续。“cwmin”有效的值是 1, 3, 7, 15, 31, 63, 127, 255, 511 或 1024。“cwmin”的值必须低于“CWmax”的值。

**Cmax:** 大竞争窗口。这里指定的最大竞争窗口的值是随机退避值增加一倍（以毫秒为单位）的上限。这增加一倍，继续，直到该数据帧发送或到达的最大竞争窗口大小。一旦达到的最大竞争窗口大小，重试将继续，直到达到允许的最大重试。“cwmax”有效的值是 1, 3, 7, 15, 31, 63, 127, 255, 511 或 1024。“cwmax”的值必须高于“CWmin”的值。

**AIFSN:** IFSN 指定一个数据帧的等待时间（以毫秒为单位）。

**TXOP(b)/ TXOP(a/g):** 表示的是传输模式为“a”“b”和“g”时，当 WME AP 启动连接到无线传输介质（WM）的时间间隔。此值指定（以毫秒为单位）为 AP 的传输机会（TXOP），即间隔时的 WMM AP 在无线网络上传输有权启动。

### 3.3.2.5 WDS

WDS(无线分布式系统)就是可以让无线 AP 或者无线路由器之间通过无线进行桥接(中继)，而在中继的过程中并不影响其无线设备覆盖效果的功能。这样我们就可以用两个无线设备，让其之间建立 WDS 信任和通讯关系，从而将无线网络覆盖范围扩展到原来的一倍以上，大大方便了我们无线上网。目前该固件支持 WDS 的一种类型，局域网。

#### 无线分布式系统

**WDS设置**

无线MAC 00:AA:BB:CC:DD:15

局域网(LAN) ▼	00	AA	BB	CC	DD	20	NAME
禁用 ▼	00	00	00	00	00	00	
禁用 ▼	00	00	00	00	00	00	
禁用 ▼	00	00	00	00	00	00	
禁用 ▼	00	00	00	00	00	00	
禁用 ▼	00	00	00	00	00	00	
禁用 ▼	00	00	00	00	00	00	
禁用 ▼	00	00	00	00	00	00	
禁用 ▼	00	00	00	00	00	00	
禁用 ▼	00	00	00	00	00	00	

**其它选项**

Lazy WDS  启用  禁用 (预设: 禁用)

保存设置
应用
取消改动

### LAN-type WDS

这是最简单，目前最常见的，用于连接局域网 WDS 的类型。这是非常简单的设置和要求没有额外的路由协议或网络知识。简而言之，它是纯粹的衔接。一个简单的例子，将扩大现有 AP 的范围内设立一个第二 AP 和它连接到第一次使用 WDS LAN 型。

1. 确保您使用的两个路由器上，使用的是相同的无线设置，没有设置任何类型的安全。
2. 找到禁用的下拉菜单，选择局域网（LAN），其他的路由也做相同的操作。
3. 在第一个路由器上，记录下 MAC 地址输入到第二个路由的相同的位置，同时设置为“局域网”。
4. 从第二个路由器记录下无线 MAC 地址，并输到的第一个路由器上。
5. 检测确认无误后，然后点击保存设置。
6. 进入到无线状态页，您应该看到 WDS 的链接和其他路由器的无线 MAC 地址列表以及可读的信号值。如果信号是“0dBm 的”，那么有可能发生了错误。请检查天线的连接和配置设置，然后再试一次。
7. 一旦你有一个很好的信号（-70dBm 到-30dBm 的，-70dBm 最低），您可以在第二个路由中更改 Internet 连接类型在基本设置页，然后选择停用，同时在第一个路由器的 LAN IP 地址设置中选择 *网关*。现在，您可以运行正常的测试以检查是否连接（如 ping 方式）。

**Lzay WDS:** 预设禁用。

**注意:** WDS 只有在 AP 模式下有效，同时当无线加密模式为 WPA 和无线网络模式为仅 B 时是不支持 WDS 的。

## 3.3.3 服务

### 3.3.3.1 服务

#### DHCP 客户端

**DHCP 客户端**

设置供应商类	<input type="text"/>
Request IP	<input type="text"/>

**设置供应商类:** DHCP 服务器可以自动识别运行某些操作系统的计算机所发送的特定的标识符，例如 DHCP 服务器可以识别 DHCP 客户端运行的操作系统是否是 Windows2000 或 Windows98 等。通过对标识符的识别，可以将 DHCP 选项分配给基于特定操作系统的 DHCP 客户端。

**Request IP:** 请求的 IP 地址

#### 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些 DHCP 的特殊功能

[厦门四信通信科技有限公司](#)

Page 40 of 82

Add: 中国厦门市软件园二期观日路 44 号 3 层

http: //www.four-faith.com

客服热线: 400-8838-199

Tel: 0592-6300320

Fax: 0592-5912735



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

添加
移除

**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**

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**

启用
  禁用

启用
  禁用

启用
  禁用

端口:  (预设: 22)

授权密钥:

**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  启用  禁用

输出模式  网络  串口

远程服务器

**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  启用  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  启用  禁用

**Ttraff 守护进程:** 启用或者禁用流量统计功能

### 3.3.3.2 PPPoE 服务器

#### PPPoE 服务器

**PPPoE 服务器**

RP-PPPoE服务端守护进程  启用  禁用

**RP-PPPoE 服务端守护进程:** 启用或禁用 PPPoE 服务器功能

#### RP-PPPoE 服务器选项

**RP-PPPoE服务器选项**

PPPOE服务器对外接口	<input type="text" value="LAN"/>	
客户端IP	<input type="text" value="192.168.1.10-100"/>	
Deflate 压缩	<input type="checkbox"/>	
BSD 压缩	<input type="checkbox"/>	
LZS Stac 压缩	<input type="checkbox"/>	
MPPC 压缩	<input type="checkbox"/>	
MPPE PPPoE 加密	<input type="checkbox"/>	
每个MAC地址限制PPPOE客户端数	<input type="text" value="10"/>	(预设: 10)
LCP回应间隔	<input type="text" value="5"/>	(预设: 5)
LCP回应失败	<input type="text" value="12"/>	(预设: 12)
空闲时间	<input type="text" value="0"/>	(预设: 0 = Deactivate)
鉴权	<input type="radio"/> Radius <input checked="" type="radio"/> 本地用户管理 (CHAP Secrets)	

**PPPOE 服务器对外接口：**PPPoE 对外的接口，只支持 LAN 口

**客户端 IP：**分配给 PPPoE 客户端的 IP 范围，格式为：**xxx.xxx.xxx.xxx-xxx**

**Deflate 压缩：**启用或禁用 Deflate 压缩

**BSD 压缩：**启用或禁用 BSD 压缩

**LZS Stac 压缩：**启用或禁用 LZS Stac 压缩

**MPPC 压缩：**启用或禁用 MPPC 压缩

**MPPE PPPoE 加密：**启用或禁用 MPPE PPPoE 加密

**每个 MAC 地址限制 PPPoE 客户端数：**默认值为 10

**LCP 回应间隔：**设置 LCP 校验阶段回应的时间间隔

**LCP 回应失败：**超过次数则释放 PPPoE，客户端则要重新连接

**空闲时间：**若有设置空闲时间，则在相应时间内空闲时则释放 PPPoE

**鉴权：**包括本地和 Radius（远程用户拨号认证）

**本地用户管理（CHAP Secrets）**
**本地用户管理（CHAP Secrets）**

用户	密码	IP地址	启用
<input type="text"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>

**用户：**设置 PPPOE 客户端的用户名

**密码：**设置 PPPOE 客户端的密码

**IP 地址：**设置 PPPOE 客户端的 IP 地址

**启用：**使用此设置

**Radius**
**厦门四信通信科技有限公司**

Add: 中国厦门市软件园二期观日路 44 号 3 层

http: //www.four-faith.com

客服热线: 400-8838-199

Tel: 0592-6300320

Fax: 0592-5912735

### Radius 鉴权

Radius服务器IP	<input type="text" value="192.168.1.1"/>	
Radius鉴权端口	<input type="text" value="1812"/>	(预设: 1812)
Radius计费端口	<input type="text" value="1813"/>	(预设: 1813)
Radius共享密钥	<input type="password" value="....."/>	

**Radius 服务器 IP:** 设置远程用户拨号认证服务器 IP 地址

**Radius 鉴权端口:** 设置远程用户拨号认证鉴权端口号

**Radius 计费端口:** 设置远程用户拨号认证计费端口号

**Radius 共享密钥:** 设置远程用户拨号认证共享密钥

## 3.3.4 VPN

### 3.3.4.1 PPTP

#### PPTP 服务器

<b>PPTP服务器</b>	
PPTP服务器	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
广播支持	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
强制MPPE加密	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
DNS1	<input type="text"/>
DNS2	<input type="text"/>
WINS1	<input type="text"/>
WINS2	<input type="text"/>
服务器IP	<input type="text"/>
客户端IP	<input type="text"/>
本地用户管理(CHAP Secrets)	<div style="border: 1px solid black; height: 50px; width: 100%;"></div>

**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\*

[厦门四信通信科技有限公司](#)

Page 45 of 82

Add: 中国厦门市软件园二期观日路 44 号 3 层

http: //www.four-faith.com

客服热线: 400-8838-199

Tel: 0592-6300320

Fax: 0592-5912735

## 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 OPENVPN

#### OPENVPN 服务端

启动类型  WAN Up  System

启动类型：WAN Up---上线后启用，System---开机启用

配置途径  GUI  Config File

服务器模式  Router (TUN)  Bridge (TAP)

配置途径: GUI---界面配置, Config File---配置文件配置

服务器模式: Router---路由模式, Bridge---网桥模式

Route 方式:

网络地址	<input type="text" value="0.0.0.0"/>
子网掩码	<input type="text" value="0.0.0.0"/>

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	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
起始地址	<input type="text" value="0.0.0.0"/>
结束地址	<input type="text" value="0.0.0.0"/>
网关	<input type="text" value="0.0.0.0"/>
子网掩码	<input type="text" value="0.0.0.0"/>

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	<input type="text" value="1194"/>	(预设: 1194)
通道协议	<input type="text" value="UDP"/>	
加密标准	<input type="text" value="Blowfish CBC"/>	
Hash算法	<input type="text" value="SHA1"/>	

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



高级选项	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
使用 LZO 压缩	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
重定向默认网关	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
允许客户端到客户端	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
允许重复 CN	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
TUN MTU 设置	<input type="text" value="1500"/>	(预设: 1500)
TCP MSS	<input type="text"/>	(预设: Disable)
TLS 加密标准	<input type="text" value="Disable"/>	
客户端连接脚本	<input type="text"/>	

**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

**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

**公共的服务器端证书:** 服务器端的证书

服务器端私钥

DH PEM 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

额外配置

CCD路径的默认文件

TLS认证密钥

证书撤销列表

**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

端口

(预设: 1194)

通道设备

通道协议

加密标准

Hash算法

ns证书类型 ( nsCertType )

**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

高级选项	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
使用LZO压缩	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
NAT	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
TAP绑定到br0网桥上	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
本地IP地址	<input type="text"/>	
TUN MTU设置	<input type="text" value="1500"/>	(预设: 1500)
TCP MSS	<input type="text"/>	(预设: Disable)
TLS加密标准	<input type="text" value="Disable"/> ▼	
TLS认证密钥	<input type="text"/>	
额外配置	<input type="text"/>	
基于路由策略	<input type="text"/>	

**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 OPENVPN 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	<input type="text"/>
公共客户端证书	<input type="text"/>
客户端私钥	<input type="text"/>

**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

[厦门四信通信科技有限公司](#)

## 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
<a href="#">添加</a>				

**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	vlan1 ▼	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。

**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

### 3.3.5 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口的请求**

阻止来自WAN口的匿名请求(ping)  
 过滤IDENT (端口113)  
 Block WAN SNMP access

**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

**Impede WAN DoS/Bruteforce**

Limit SSH Access

Limit Telnet Access

Limit PPTP Server Access

Limit L2TP Server Access

**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

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

拒绝的

已接受的

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
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

### 3.3.5.2 VPN 穿越

虚拟专用网（VPN）通常用于与工作相关的网络。对于 VPN 隧道，路由器目前支持 IPSec，PPTP 和 L2TP 的穿越。

**虚拟专用网 (VPN)**

**VPN 穿透**

IPSec 穿透  启用  禁用

PPTP 穿透  启用  禁用

L2TP 穿透  启用  禁用

**IPSec 穿透：**Internet 协议安全（IPSec）是一套协议，用于实现在 IP 层的报文的安全交换。要允许 IPsec 隧道通过路由器，则启用 IPSec 穿越功能。要禁用的 IPSec 穿越功能，选择禁用。

**PPTP 穿透：**点对点隧道协议（PPTP）是用于启用 VPN 会话的 Windows NT 4.0 或 2000 服务器的方法。要允许 PPTP 隧道通过路由器，启用 PPTP 穿越功能。要禁用 PPTP 穿越功能，选择禁用。

**L2TP 穿透：**第二层隧道协议（L2TP），是虚拟专用网（VPN）的 PPP 协议的扩展。L2TP 合并其他两个隧道协议的特点：从微软和思科系统公司的 L2F PPTP。要允许 L2TP 隧道通过路

由器，则启用 L2TP 穿越功能。要禁用的 L2TP 穿越功能，选择禁用。

点击“**保存设置**”按钮保存更改。点击“**取消改动**”按钮取消未保存的更改。

### 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。

**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”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。

## 3.3.7 NAT/QoS

### 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）。

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"/>
		<input type="button" value="添加"/> <input type="button" value="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。

**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。

**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。

[厦门四信通信科技有限公司](#)

Page 60 of 82

Add: 中国厦门市软件园二期观日路 44 号 3 层

http: //www.four-faith.com

客服热线: 400-8838-199

Tel: 0592-6300320

Fax: 0592-5912735

**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，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
<input type="text" value="web-tftp"/>	<input type="text" value="800"/>	<input type="text" value="8100"/>	<input type="text" value="两者"/>	<input type="text" value="192.168.1.16"/>	<input checked="" type="checkbox"/>
<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="两者"/>	<input type="text" value="0.0.0.0"/>	<input 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；

**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**”。

### 3.3.7.3 端口触发

端口触发页面可以设置使路由器侦测特定触发端口号的出局数据，自动转发特定的端口范围，这样当所请求的数据通过路由器返回的时候，则会通过 IP 地址与端口映射规则回到相应的计算机。

**端口触发**

**转发**

	已触发端口范围		转发端口范围			
应用程序	开始	结束	协议	开始	结束	启用
<input type="text" value="web-tftp"/>	<input type="text" value="80"/>	<input type="text" value="880"/>	<input type="text" value="两者"/>	<input type="text" value="21"/>	<input type="text" value="63"/>	<input checked="" type="checkbox"/>

**应用程序：**输入端口触发的应用名称；

**触发端口范围：**为每一个应用列出触发端口号的范围。

**开始端口：**输入触发范围的开始端口号。

**结束端口：**输入触发范围的结束端口号。

**转发端口范围：**对每一种应用列出转发端口范围。

**开始端口：**输入转发范围的开始端口号。

**结束端口：**输入转发范围的结束端口号。

**启用：**选择“启用”框，启用您所定义的端口触发服务，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**”。

### 3.3.7.4 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**”。

### 3.3.7.5 QOS

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%。

### Netmask 优先顺序

**Netmask 优先顺序**

删除	IP/Mask	优先级
<input type="checkbox"/>	192.168.1.1/24	Exempt (不受限)
<input type="checkbox"/>	192.168.2.3/24	Standard (标准)
<input type="checkbox"/>	192.168.3.4/32	Express (优先)
<input type="checkbox"/>	192.168.4.5/32	Bulk (低)

.
 .
 .
  /

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。

### MAC 优先顺序

**MAC 优先顺序**

删除	MAC地址	优先级
<input type="checkbox"/>	00:AA:BB:0C:DD:EE	Standard (标准)
<input type="checkbox"/>	CC:AA:BB:DD:FF:AA	Premium (高优先)

:
 :
 :
 :
 :

您可以为来自一个给定的 MAC 地址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:  $\text{mini}(\text{Max\_Up} - \text{Exempt\_Rate\_Up}, \text{Uplink})$ ;

其他优先级总下载带宽为:  $\text{mini}(\text{Max\_Down} - \text{Exempt\_Rate\_Do}, \text{Downlink})$ 。

### 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:  $(75/100) * \text{Uplink}$  ;  $(75/100) * \text{Downlink}$

优先:  $(15/100) * \text{Uplink}$  ;  $(15/100) * \text{Downlink}$

标准:  $(10/100) * \text{Uplink}$  ;  $(10/100) * \text{Downlink}$

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;

## 3.3.8 管理

### 3.3.8.1 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。

**登陆前显示系统信息网页：** 是否启用登陆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="8080"/> (预设: 8080, 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"/> (预设: 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  启用  禁用

Cron 附加任务

**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。

**802.1x**

802.1x  启用  禁用

**802.1x：**有限的 802.1x 的服务器需要履行 WPA 握手的要求，使 Windows XP 客户端的工作在 WPA 状态。

**路由**

路由  启用  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

**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。

**IP过滤设置 (为P2P调整这些设置)**

TCP Congestion Control

最大端口数  (预设: 4096, 范围: 256 - 4096)

TCP超时 (秒)  (预设: 3600, 范围: 1 - 86400)

UDP超时 (秒)  (预设: 120, 范围: 1 - 86400)

**IP 过滤设置 (为 P2P 调整这些设置)：**如果您有 (P2P) 的应用程序在网络上运行，为了保持链路的稳定性，请增加最大的端口数和降低的 TCP/UDP 超时。因为 P2P 应用程序会打开

多个连接而且不会正确的关闭这些连接。

最大的端口数为：4096

TCP 超时（秒）：预设 3600 秒

UDP 超时（秒）：预设 120 秒

### 3.3.8.2 保持活动

定时重启

**定时重启**

定时重启  启用  禁用

间隔（秒）

在设定的时间   :

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。

### 3.3.8.3 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：**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。

### 3.3.8.4 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”

### 3.3.8.5 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

**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](http://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。

### 3.3.8.6 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。

## 3.3.9 状态

### 3.3.9.1 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

[厦门四信通信科技有限公司](#)

Page 68 of 82

Add: 中国厦门市软件园二期观日路 44 号 3 层

http: //www.four-faith.com

客服热线: 400-8838-199

Tel: 0592-6300320

Fax: 0592-5912735

- 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	28880 kB / 32768 kB	88%
空闲	12604 kB / 28880 kB	44%
已使用	16276 kB / 28880 kB	56%
缓冲区	1656 kB / 16276 kB	10%
已缓存	5656 kB / 16276 kB	35%
使用中	1347 kB / 16276 kB	8%
非使用中	730 kB / 16276 kB	4%

- 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过滤器最大端口数	4096	
活动的IP连接	128	3%

- 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

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

### 3.3.9.2 WAN

**连接类型** 自动配置 - DHCP

**已连接时间** 不可用

**连接类型：**包括 6 种方式：禁用，静态 IP，自动配置-DHCP，PPPOE，PPTP，L2TP。

**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**

[厦门四信通信科技有限公司](http://www.four-faith.com)

Page 70 of 82

Add: 中国厦门市软件园二期观日路 44 号 3 层

http: //www.four-faith.com

客服热线: 400-8838-199

Tel: 0592-6300320

Fax: 0592-5912735

**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

租约剩余时间

0 days 23:59:06

DHCP 释放

DHCP 续期

**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

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

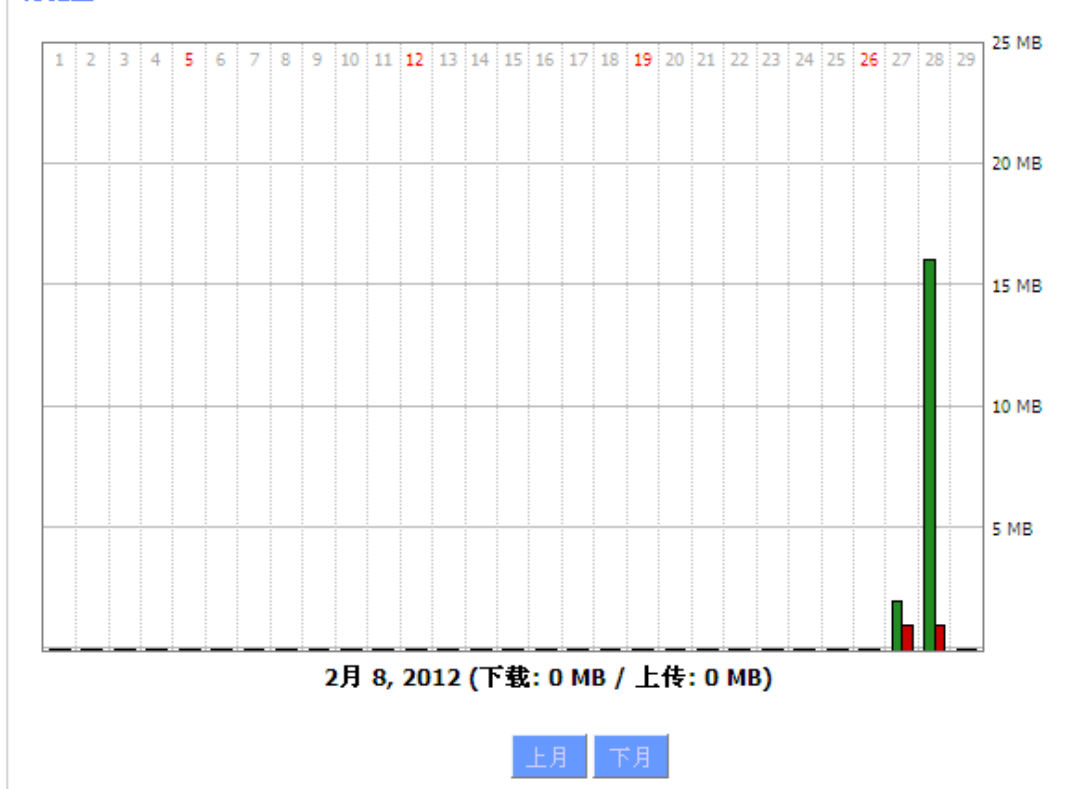
**连接:** 连接已经断开的状态

**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:** 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

**3.3.9.3 LAN**



**LAN 状态**

MAC地址	00:0C:43:30:52:77
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	10:78:D2:98:C9:46	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

**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

**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	<a href="#">00:25:56:68:5E:30</a>	1 day 00:00:00	
four-488e1df5fa	192.168.1.125	<a href="#">44:37:E6:09:D8:F7</a>	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

### 3.3.9.4 无线

**无线状态**

MAC地址	<u>00:0C:43:30:52:79</u>
无线网络	无线网络开启
模式	访问点 (AP)
网络	混合
SSID	xcy-ra
频道	11 (2462 MHz)
传送功率	71 mW
速率	72 Mb/s
加密 - 接口 w10	已禁用
PPTP状态	已断开连接

**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

**厦门四信通信科技有限公司**

Page 75 of 82

Add: 中国厦门市软件园二期观日路 44 号 3 层

http: //www.four-faith.com

客服热线: 400-8838-199

Tel: 0592-6300320

Fax: 0592-5912735

**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 w10:** 是否加密 w10 接口

无线数据包信息		
已接收的 (RX)	44 OK, 无 错误	100%
已传送的 (TX)	23 OK, 无 错误	100%

**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

客户端								
MAC地址	接口	运行时间	传输速率	接收速率	信号	噪声	SNR	信号质量
- 无 -								

**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										
SSID	Mode	MAC地址	频道	Rssi	噪声	信标	打开	dtim	速率	加入基站
ff	未知	00:aa:bb:cc:dd:9a	6	-20	-95	0	查	0	300(b/g/n)	加入
ff-old	AP	00:13:10:09:56:92	6	-44	-95	0	查	0	54(b/g)	加入

**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

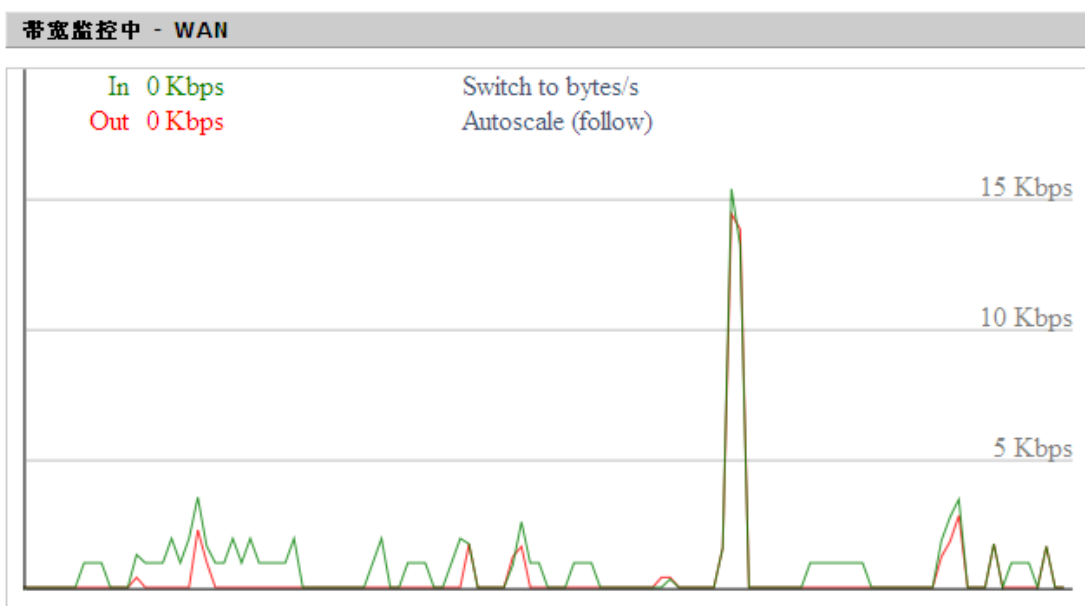
**噪声:** 邻近无线噪声

- 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

### 3.3.9.5 宽带

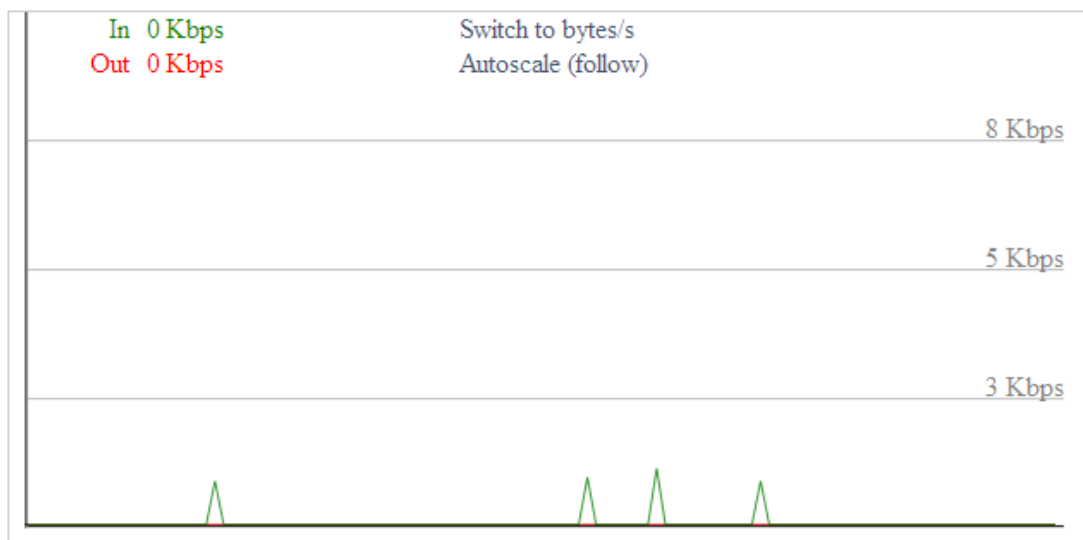


LAN 口的时时检测状态图横坐标代表时间纵坐标代码速率



WAN 口的时时检测状态图横坐标代表时间纵坐标代码速率

## 带宽监控中 - 无线 (wl0)



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。

### 3.3.9.6 系统信息

#### 路由器

路由器名称	Four-Faith
路由器型号	Four-Faith Router
LAN MAC	<u>00:0C:43:30:52:77</u>
WAN MAC	<u>00:0C:43:30:52:78</u>
Wireless MAC	<u>00:0C:43:30:52:79</u>
WAN IP	10.34.107.156
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

**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**

无线网络	无线网络开启
模式	访问点 (AP)
网络	混合
SSID	xcy-ra
频道	11 (2462 MHz)
传送功率	71 mW
速率	72 Mb/s

**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

**无线数据包信息**

已接收的 (RX)	18047 OK, 无 错误
已传送的 (TX)	74340 OK, 无 错误

**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

无线								
客户端								
MAC地址	接口	运行时间	传输速率	接收速率	信号	噪声	SNR	信号质量
- 无 -								

**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

**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	28.2 MB / 32.0 MB
空闲	10.3 MB / 28.2 MB
已使用	17.9 MB / 28.2 MB
缓冲区	1.8 MB / 17.9 MB
已缓存	6.3 MB / 17.9 MB
使用中	1.3 MB / 17.9 MB
非使用中	1.1 MB / 17.9 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

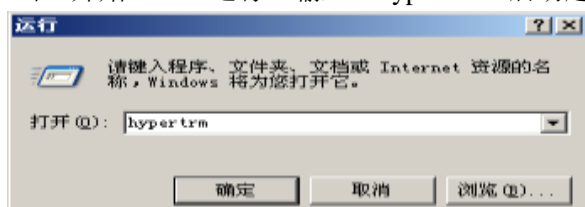
**客户端租约时间:** 客户端租约这个 IP 地址的时间



## 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

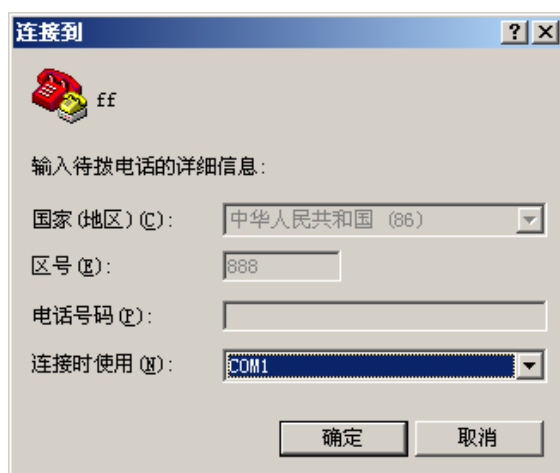
1. 点击“开始”→“程序”→“附件”→“通讯”→“超级终端”（或者如下图，直接点击“开始”→“运行”输入“hypertrm”启动超级终端）。



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。

