

## S-IR311 工业路由器使用手册

此说明书适用于下列型号产品：

型号	产品类别
S-IR311-G	GPRS WIFI ROUTER
S-IR311-C	CDMA WIFI ROUTER
S-IR311-W	WCDMA WIFI ROUTER
S-IR311-T	TD-SCDMA WIFI ROUTER
S-IR311-E	EVDO WIFI ROUTER
S-IR311-LT	LTE/TD-SCDMA ROUTER
S-IR311-LF	LTE/WCDMA ROUTER
S-IR311-A	TDD/FDD ROUTER



厦门欣仰邦科技有限公司

地址：厦门市集美区软件园三期B区04栋708室

网址：[www.xmsiyb.com](http://www.xmsiyb.com)

电话：0592-3564822

邮箱：[Support@xmsiyb.com](mailto:Support@xmsiyb.com)



## 文档修订记录


日期	版本	说明	作者
2014.6.23	V1.0	第一次发布手册	HJC
2014.8.18	V1.1	增加 OPENVPN 功能和串口应用	HJC
2014.10.19	V1.2	增加定时开关机功能	HJC
2015.8.6	V1.3	修改文档格式、删减冗余功能	HJC



## 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，所有版权由厦门欣仰邦科技有限公司拥有，但注明引用其他方的内容除外。未经欣仰邦公司书面许可，任何人不得将本文档上的任何内容以任何方式进行复制、经销、翻印、连接、传送等任何商业目的的使用，但对于非商业目的的、个人使用的下载或打印（条件是不得修改，且须保留该材料中的版权说明或其他所有权的说明）除外。

## 商标声明

欣仰邦、siyb、均系厦门欣仰邦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欣仰邦名称及欣仰邦的商标、名称、标记。





注：不同型号配件、接口、批次可能存在差异，具体以实物为准。



# 目录

一、 术语与定义.....	7
二、 产品介绍.....	7
2.1 产品简介.....	7
2.2 应用介绍.....	8
2.3 产品尺寸图.....	8
三、 产品安装.....	9
3.2 装箱清单.....	9
3.2 安装与电缆连接.....	10
321 SIM/UIM 卡安装.....	10
322 线缆安装 .....	10
323 电源 .....	11
324 天线安装 .....	11
3.3 指示灯说明.....	11
3.4 复位按钮说明.....	12
四、 参数配置.....	12
4.1 配置连接.....	12
4.2 登录 .....	12
4.3 管理和配置.....	14
4.3.1 设置 .....	14
MAC 地址克隆 .....	19
4.3.2 无线 .....	20
4.3.2.1 基本配置 .....	20
4.3.2.2 无线安全 .....	21
4.3.2.3 无线MAC 过滤 .....	23
4.3.2.5 WDS .....	23
4.3.3 VPN.....	25
4.3.3.2 L2TP VPN.....	27
4.3.3.3 OPEN VPN.....	29
4.3.3.4 IPSEC VPN.....	34



添加 IPSEC 连接或编辑 IPSEC 连接.....	35
4.3.3.5 GRE VPN .....	36
4.3.4.3 VPN 穿透.....	39
4.3.4.4 访问限制.....	41
1. 端口转发.....	42
2. 端口范围转发.....	43
3. 端口触发.....	44
4. DMZ .....	44
4.3.4.6 QoS 设置.....	46
1. 基本 .....	46
2. 分类 .....	46
4.3.5 应用 .....	48
4.3.6 管理 .....	49
2. 保持活动.....	51
4. 出厂默认.....	52
5. 固件升级.....	52
6. 备份 .....	52
4.3.7 状态 .....	53
2. WAN.....	54
3. LAN .....	56
4. 无线 .....	58
5. PPTP/L2TP .....	59
五、订购信息 .....	61



## 一、术语与定义

4G: LTE-TDD、LTE-FDD 等 4G 网络制式的统称

3G: 中国移动 3G(TD-SCDMA), 中国联通 3G(WCDMA) 和电信 3G(EVDO)

EMC: 设备或系统在其电磁环境中能正常工作且不对该环境中任何事物构成不能承受电磁骚扰的能力

S-IR311: 是欣仰邦物联研发的一款无线路由器

## 二、产品介绍

### 2.1 产品简介

S-IR311 系列 ROUTER 是一款工业级无线路由器, 设计完全满足工业级标准和工业用户的需求, 采用高性能的工业级 32 位通信处理器, 软件和硬件多级检测多重保护机制来提高设备稳定性。支持中国电信 4G/3G, 中国联通 4G/3G、中国移动 4G/3G 并往下兼容 EDGE、CDMA

1X 及 GPRS 网络, 同时支持多种 VPN 协议来保证数据传输的安全性。支持 RS232 (或 RS485/RS422) 和以太网接口, 和 WIFI 功能。

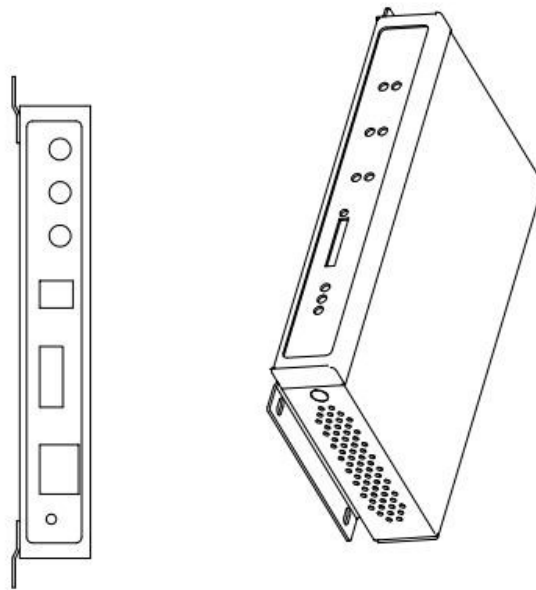
该系列产品可帮助用户快速接入互联网, 实现安全可靠的数据传输, 广泛应用于交通、电力、金融、水利、气象、环保、工业自动化、能源矿产、医疗、农业、林业、石油、建筑、智能家居、智能交通、智能家居等物联网应用。



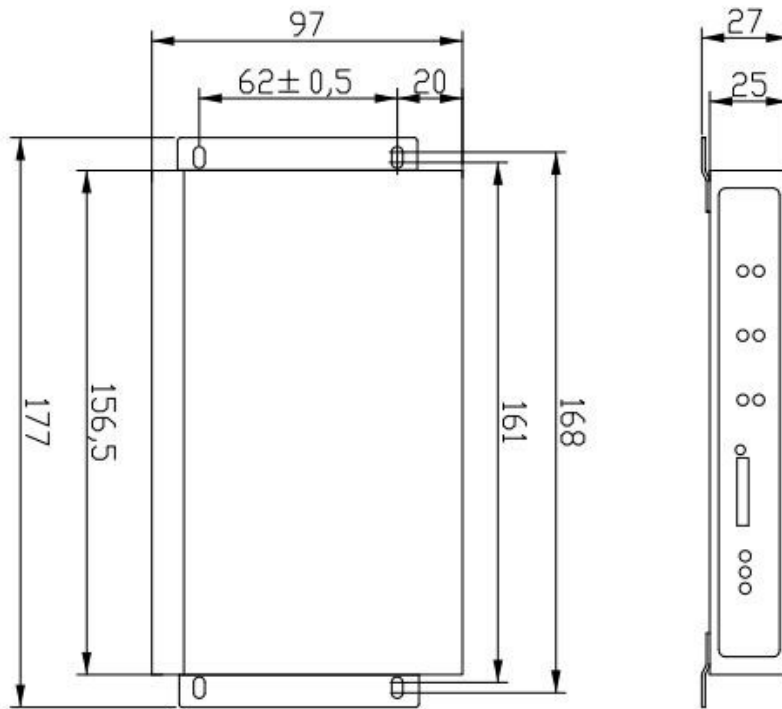
## 2.2 应用介绍

S-IR311 产品系列借助无线网络实现远程无线网络连接，在工业领域上实现远程监测和视频监控。

## 2.3 产品尺寸图







## 三、产品安装

### 3.1 概述

注意：请不要在带电情况下安装本公司产品。

ROUTER 必须正确安装方可达到设计的功能。

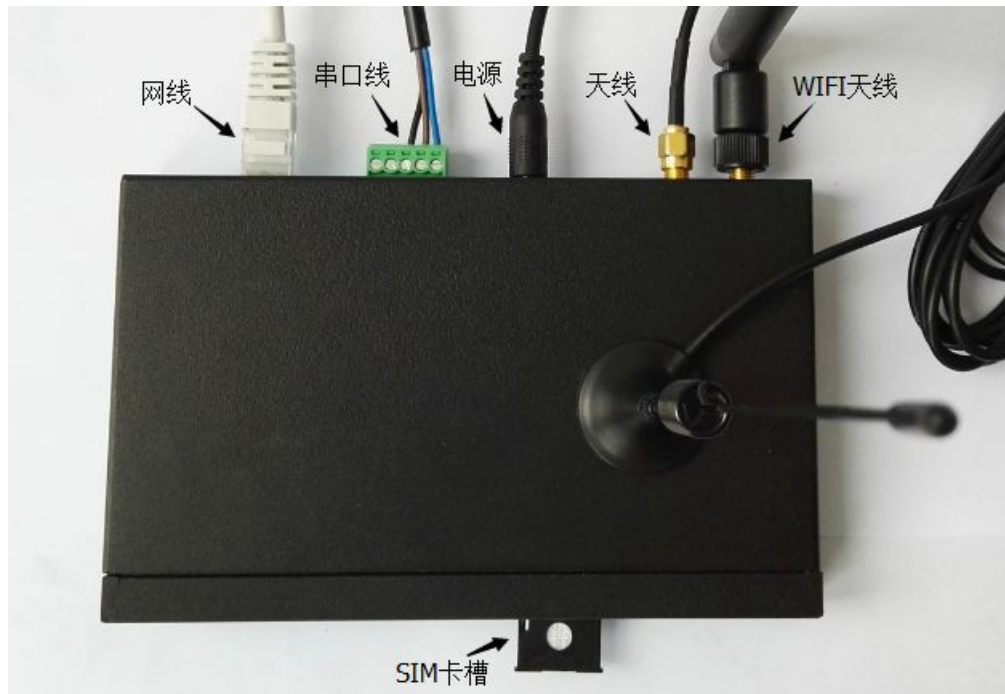
### 3.2 装箱清单

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：

- ◇ S-IR311 路由器主机 1 台
- ◇ 车载天线（SMA 阳头）1 根
- ◇ WIFI 天线（SMA 阴头）1 根
- ◇ 1.5A/12VDC 电源 1 个
- ◇ 网线 1 条
- ◇ RS232 串口直连线 1 条
- ◇ 5PIN 接线端子 1 个
- ◇ 产品合格证
- ◇ 产品保修卡



### 3.2 安装与电缆连接



#### 321 SIM/UIM 卡安装

SIM/UIM 卡是无线路由器拨号上网的必要辅件，所以 SIM/UIM 卡必须被正确安装才能达到无线路由器稳定快速上网的效果。

现今运营商办理在 SIM/UIM 卡有多种标准，本路由器使用的是大卡，若办理的是小卡，则需要带着相应卡套方能在本路由器上使用。

安装时先用尖状物插入 SIM/UIM 卡座旁边小黄点，卡槽弹出。SIM/UIM 金属芯片朝外放置于 SIM/UIM 卡槽中，插入抽屉，并确保插到位。

#### 322 线缆安装

本路由器自带一个 RS232 和一个 S485 串口，此串口可用于路由器固件升级、系统日志查看、串口 DTU 功能等应用。

S-IR311 串口采用工业级端子接口，标配串口线为一端剥线，一端 DB9 母头，其线序定义定义如下：

RS232线（一端为DB9母头）

RS232线（一端为DB9母头）

线材颜色	对应 DB9 母头管脚	对应路由器（1：靠近电源，5：靠近网线）
蓝色	2 (RX)	1
棕色	3 (TX)	2
黑色	5 (GND)	3

RS485 线：

线材颜色	对应路由器
红	4 (A)
黑	5 (B)



### 323 电源

可使用标配 1.5A/12VDC 电源，也可以直接采用 5-35VDC 电源给设备供电，当用户采用外加电源给设备供电时，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4W以上。

### 324 天线安装

天线为路由器增强信号的必要配件，必须正确安装方能达到最优的上网体验。

S-IR311 天线接口为 SMA 阴头插座。将配套天线的 SMA 阳头旋到 ANT 天线接口上，并确保旋紧，以免影响信号质量。

## 3.3 指示灯说明

指示灯是路由器运行状态的最直观显示，从指示灯的状态可以方便、快速、较准确地判断路由器的运行状态。

S-IR311 系统路由器共有 7 种状态指示灯，其状态说明如下：

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
WIFI	灭	WIFI 未启动
	亮	WIFI 已启动
LAN	闪烁	LAN 口连接正常
	灭	LAN 口未连接
Online	亮	设备已登录网络
	灭	设备未登录网络
Alarm	亮	SIM/UIM 卡未插到位或损坏。天线信号弱
	灭	设备无报警
信号强度指示灯	亮一个灯	信号强度较弱
	亮两个灯	信号强度中等
	亮三个灯	信号强度极好



### 3.4 复位按钮说明

Reset 按钮是路由器的复位按钮，其作用是不进入路由器配置页面的条件下直接将路由器的参数配置恢复到出厂默认值。

复位按钮可以直接、有效地解决由于参数配置不当，造成的路由器无法上网、无法登录、无法管理等问题。

S-IR311 系统无线路由器设有一个 Reset 按钮，位于 LAN 口附近。在需要将路由器恢复出厂设置时，用尖锐硬物插入“Reset”孔位，并轻轻按住，直到所有的指示灯全部熄灭后放开，ROUTER 的配置即已恢复为出厂值。

## 四、 参数配置

### 4.1 配置连接

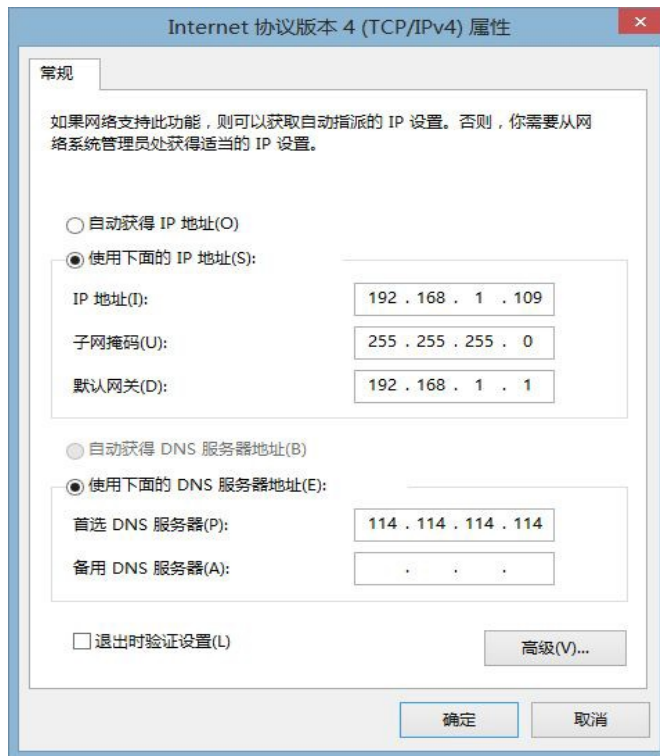
在对路由器进行配置前，需要将路由器和用于配置的 PC 通过出厂配置的网络线或 WIFI 连接起来。用网络线连接时，网络线的一端连接路由器 LAN 口，另外一端连接到 PC 的以太网口。用 WIFI 连接时，路由器出厂默认的 SSID 为“top-iot”，无须密码验证。

### 4.2 登录

Router 默认 IP 地址为 192.168.1.1。可将用于参数配置的 PC 地址设置成自动获取或手动设置。其中子网掩码设为：255.255.255.0，默认网关设为：192.168.1.1

如下图所示举例：





启动 IE 或其他浏览器，访问路由器的默认 IP 地址 192.168.1.1。

首次登入到 Web 页面时，会提示用户选择显示语言和是否修改路由器的默认用户名和密码。

若需要修改密码，则输入用户自行定义的用户名的密码，显示中文界面则在 Language 选项中选中“Chinese simplified”，显示英文界面则选中“English”，并单击“Change Password”按键予以生效。



## 4.3 管理和配置

点击“Change Password”后将进入路由器的管理页面。通过此管理页面，用户可以按照提示来对路由器的设置进行更改。

在每个设置页面底部都有三个按钮，分别是“保存设置”、“应用”、“取消”。

“保存设置”按钮将保存已配置参数，这些参数不会立即生效，而是在路由器重启后生效，“应用”按钮使更改的参数立即生效，“取消”按钮取消更改，关闭当前配置页面或消除已配置参数。

通常情况下，路由器可以根据自身所支持的网络类型及 SIM 卡类型进行自动识别，无需手动设置，即插好 SIM 卡，插上电源，即可上网。

用户在使用专用网络等非常用卡，或某些特定场合需指定特定网络类型时需做如下设置。

### 4.3.1 设置

#### WAN 连接类型

WAN 连接类型包括：禁用、LTE、3G 三种

Router 通常可以根据支持的网络类型及 SIM 卡类型进行自动识别，无需手动设置。

##### ➤ 方式一：禁用

禁止 WAN 口的连接类型设置

##### ➤ 方式二：LTE



LTE 方式是 4G 网络拨号类型，当需要连接 4G 网络时选择此连接类型。  
LTE 连接类型只有在 Router 和 SIM 卡同时支持 4G 网络的情况下可用。

**WAN连接类型**

连接类型: LTE

用户名:

密码:   显示密码

APN:

### 方式三: 3G

3G 方式是 3G 网络拨号类型，当需要连接 3G 网络时选择此拨号类型。

**WAN连接类型**

连接类型: 3G

用户名:

密码:   显示密码

拨号号码: \*99\*\*\*1# (UMTS/3G/3.5G)

APN:

用户名: 用于登录到Internet 的用户名。密码:

通常情况下用户名、密码、APN 等参数无需手动设置，用户在使用专用网络时，需要按照运营商提供的用户名、密码、APN 等信息进行相应的设置。

用于登录

## 在线探测

在线探测主要是用于维持数据链路处于在线状态，以 Ping、Route 等方式定时向指定的服务器发送探测数据包。

在线探测方式: Ping

在线探测时间间隔: 120 秒

主探测主服务器: 208 . 67 . 222 . 222

若启用了此功能，路由器将自动检测数据链路，一旦检测到链路断开或者无效，系统将自动重连，重新建立有效链路。

### 在线保持检测时间间隔:

两次在线探测之间的时间间隔，单位为秒。





## 网络设置

此项设置可以对路由器的 LAN 地址进行修改。





## 网络设置

### 路由器IP

本地IP地址	<input type="text" value="192"/>	.	<input type="text" value="168"/>	.	<input type="text" value="10"/>	.	<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"/>

**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

### 网络地址服务器设置 (DHCP)

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	<input type="text" value="192.168.10."/> <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

取 IP 地址和 DNS，并确保在网络中没有其它的 DHCP 服务器。

**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”。若您选择 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

## 时间设置

### 时间设置

NTP客户端	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
时区	<input type="button" value="UTC+08:00"/>
夏令时 (DST)	<input type="button" value="无"/>
服务器IP/主机名	<input type="text"/>



---

NTP 客户端：开启和禁用为系统内部提供一个对时功能，即设置系统时间



时区：西12 区到东12 区，通过自己的位置设定夏令

时：根据自己的位置设定

服务器 IP/主机名称：你NTP 服务器的 IP 地址，最长 32 个字符，若无则系统会默认去找服务器

## 校准时间:

时间调整

自动  2015 - 08 - 02 17 : 40 : 34

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

## MAC 地址克隆

克隆LAN口VLAN MAC 00 : 0C : 43 : E1 : C2 : BB

---

克隆WAN口MAC 00 : 0C : 43 : E1 : C2 : BC

---

克隆LAN口无线MAC 00 : 0C : 43 : E1 : C2 : BD

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。

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。

### 4.3.2 无线

此页面主要用于 WIFI 相关参数的配置。

无线网络  启用  禁用

物理接口 ra0 - SSID [SSID] HWAddr [00:0C:43:E1:C2:BD]

无线模式

无线网络模式

无线网络名 (SSID)

无线频道

频道宽度

无线SSID广播  启用  禁用

网络配置  未桥接  已桥接

#### 4.3.2.1 基本配置



**启用:** 开启 WIFI。**禁用:** 关闭 WIFI。

**无线模式:** AP、客户端、Ad-hoc、中继、中继桥接四种模式可选。 **无线网络模式:**

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

**BG-混合:** 同时支持 802.11b、802.11g 标准的无线设备。**仅B:** 只支持 802.11b 标准的无线设备。

**仅 G:** 只支持 802.11g 标准的无线设备。

**NG-混合:** 同时支持 802.11g、802.11n 标准的无线设备。**仅 N:** 只支持 802.11n 标准的无线设备。

**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。

## 4.3.2.2 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。

物理接口 ra0 SSID [SSID] HWAddr [00:0C:43:E1:C2:BD]

安全模式

物理接口 ra0 SSID [SSID] HWAddr [00:0C:43:E1:C2:BD]

安全模式

鉴权类型  开放式  共享密钥

默认传输密钥  1  2  3  4

加密

ASCII/HEX  ASCII  HEX

密钥 1

密钥 2

密钥 3

密钥 4



**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 16 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。

物理接口 ra0 SSID [SSID] HWAddr [00:0C:43:E1:C2:BD]

安全模式 WPA Personal

WPA算法 TKIP

WPA共享密钥   显示密码

密钥更新时间间隔 (秒) 3600 (默认: 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 [SSID] HWAddr [00:0C:43:E1:C2:BD]

安全模式 WPA Enterprise

WPA算法 TKIP

Radius鉴权服务器地址 0 . 0 . 0 . 0

Radius鉴权服务器端口 1812 (默认: 1812)

Radius鉴权共享密钥   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。





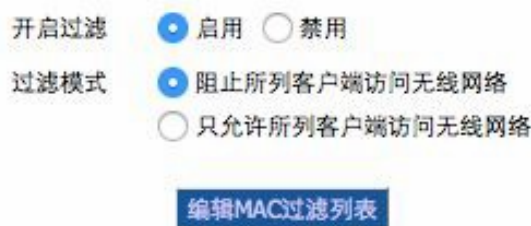
### 4.3.2.3 无线 MAC 过滤

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。**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。

点击“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。



### 4.3.2.4 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。



### 4.3.2.5 DS

W



WDS设置

无线MAC 00:0C:43:E1:C2:BD

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	
禁用	00	00	00	00	00	00	





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,大大方便了我们的无线上网。目前该固件支持 WDS 的一种类型,局域网。

### 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 /~~禁用~~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。

## 4.3.3 VPN

### 4.3.3.1 PPTP VPN

#### PPTP 服务器

**广播支持:** 开启或禁用 PPTP 服务器支持广播功能**强制MPPE 加密:** 是否要强制

PPTP 数据MPPE 加密

**DNS1, DNS2, WINS1, WINS2:** 设置你的第一 DNS, 第二 DNS, 第一 WINS, 第二 WINS **服务器 IP:** 输入路由器作为 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。



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)

test \* test \*

CHAP Secrets 格式为 user 空格\*空格 password 空格\*

PPTP 客户端

**服务器 IP 或DNS 名称:** PPTP 服务器的 IP 地址或者对应的 DNS 名称  
远程子网 : 远程PPTP 服务器的内网

**远程子网掩码:** 远程 PPTP 服务器的子网掩码

**MPPE 加密:** 是否支持 MPPE 加密。

**MTU:** 最大传输单元 0-1500

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  (默认: 1450)

MRU  (默认: 1450)

NAT  启用  禁用

启用手动设置隧道IP  启用  禁用

用户名

密码   显示密码

保存设置 应用 取消



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

### 4.3.3.2 L2TP VPN

## L2TP 服务器



The screenshot shows the 'L2TP 服务器' (L2TP Server) configuration page. It includes the following fields and options:

- L2TP服务器选项:** Radio buttons for '启用' (Enabled) and '禁用' (Disabled). '启用' is selected.
- 强制MPPE加密:** Radio buttons for '启用' (Enabled) and '禁用' (Disabled). '启用' is selected.
- 服务器IP:** Text input field containing '10.100.100.100'.
- 客户端IP:** Text input field containing '10.100.100.101-10.100.100.200'.
- 隧道验证密码(可选):** Text input field, currently empty. A '显示密码' (Show Password) checkbox is to its right.
- 本地用户管理(CHAP Secrets):** A text area containing 'test \* test \*'.

**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

隧道名称

用户名

密码   显示密码

隧道验证密码(可选)   显示密码

L2TP服务器

远程子网  .  .  .

远程子网掩码  .  .  .

MPPE加密

MTU  (默认: 1450)

MRU  (默认: 1450)

NAT  启用  禁用

启用手动设置隧道IP  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  
**认证协议:** 是否支持认证协议

### 4.3.3.3 OPEN VPN

#### OPENVPN 服务端

**启动类型:** WAN Up---上线后启用, System---开机启用  
**配置途径:** GUI---界面配置, Config File---配置文件配置



开启OPENVPN服务器选项  启用  禁用

启动类型  WAN Up  System

配置途径  GUI  Config File

服务器模式  Router (TUN)  Bridge (TAP)

网络地址

子网掩码

端口  (默认: 1194)

通道协议

加密标准

Hash算法

高级选项  启用  禁用

公共的服务器端证书

公共CA证书

服务器端私钥

DH 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



服务器模式: Router---路由模式, Bridge---网桥模式

### Route 方式:

网络地址: OPENVPN 服务端允许的网络地址子网掩码: OPENVPN 服务端允许的子网掩码

### 网桥模式:

DHCP 代理模式: 启用或禁用 DHCP 代理模式  
起始地址: OPENVPN 服务端允许客户端的起始地址结束地址: OPENVPN 服务端允许客户端的结束地址网关: OPENVPN 服务端允许客户端的网关子网掩码: OPENVPN 服务端的允许客户端子网掩码

端口: OPENVPN 服务器的监听端口

通道协议: OPENVPN 的通道协议 UDP 或 TCP

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

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

使用 LZO 压缩: 启用或禁用传输数据使用 LZO 压缩重定位默认网关: 启用或禁用重定位网关

允许客户端到客户端: 启用或禁用允许客户端到客户端 允许重复 CN: 启用或禁用允许重复 CN

TUN MTU 设置: 设置通道的 MTU 值

TCP MSS: TCP 数据的最大分段大小

TLS 加密标准: TLS (安全传输层协议) 加密标准支持 AES-128 SHA 和 AES-256 SHA

客户端连接脚本: 自行定义的一些客户端脚本 公共 CA 证书: 服务器和

客户端公共的 CA 证书公共的服务器端证书: 服务器端的证书

服务器端私钥: 服务器端设置的密钥DH

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

PEM证书

### OPENVPN 客户端





开启OpenVPN客户端选项  启用  禁用

服务器IP/名称

端口  (默认: 1194)

通道设备

通道协议

加密标准

Hash算法

ns证书类型 (nsCertType)

高级选项  启用  禁用

使用LZO压缩  启用  禁用

NAT  启用  禁用

TAP绑定到br0网桥上  启用  禁用

本地IP地址

TUN MTU设置  (默认: 1500)

TCP MSS  (默认: Disable)

TLS加密标准

TLS认证密钥

额外配置

基于路由策略

公共CA证书

公共客户端证书

客户端私钥

**服务器 IP / 名称:** OPENVPN 服务器的 IP 地址或域名  
**端口:** OPENVPN 客户端的监听端口

**通道设备:** TUN---路由模式 TAP---网桥模式  
**通道协议:** UDP 和 TCP 协议

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

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

**ns 证书类型:** 是否支持 ns 证书类型

**使用 LZO 压缩:** 启用或禁用传输数据使用 LZO 压缩

**NAT:** 启用或禁用 NAT 穿越功能

**TAP 绑定到 br0 网桥上:** 启用或禁用 TAP 绑定到 br0 网桥上  
**本地 IP 地址:** 设置本地 OPENVN 客户端的 IP 地址

**TUN MTU 设置:** 设置通道的 MTU 值

**TCP MSS:** TCP 数据的最大分段大小

**TLS 加密标准:** TLS (安全传输层协议) 加密标准支持 AES-128 SHA 和 AES-256 SHA

**TLS 认证密钥:** 安全传输层的认证密钥





---

额外的配置：OPENVPN 服务器其他额外配置



**基于路由策略：**输入自定义的一些路由策略

**公共服 CA 证书：**服务器和客户端公共的 CA 证书

**公共客户端证书：**客户端证书

#### 4.3.3.4 IPSEC VPN

##### 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。

**类型**

类型 Net-to-Net虚拟专用网

功能  客户端  服务端

---

**连接配置**

连接配置

名称	<input type="text"/>	启用	<input checked="" type="checkbox"/>
本端WAN接口	<span style="border: 1px solid #ccc; padding: 2px;">WAN</span>	对端地址	<input type="text"/>
本端子网	<input type="text"/>	对端子网	<input type="text"/>
本端标志符	<input type="text"/>	对端标志符	<input type="text"/>

---

**检测**

检测

启用DPD检测

时间间隔  (秒) 超时时间  (秒) 操作 restart

---

**高级配置**

高级配置

启用高级配置

**第一阶段**

IKE加密 3DES IKE完整性 MD5 IKE DH小组 组2(1024)

IKE生命周期  小时

**第二阶段**

ESP加密 3DES ESP完整性 MD5-96

ESP生命周期  小时

采用野蛮模式

会话密钥向前加密(PFS)

**名称：**IPSEC 连接的名称；

**类型：**当前 IPSEC 连接的类型及功能；

**通用名称：**当前连接的本端子网、本端地址、对端地址及对端子网； **状态：**连接所处的状态，总共三种，分别为关闭、协商中及建立； **关闭：**该条连接未向对端发起连接请求；



**协商中:** 该条连接已向对端发起请求, 并处在协商过程中, 连接仍未建立; **建立:** 连接已经建立, 已能使用该通道。

**操作:** 可以对该连接进行的操作, 目前有四种, 分别为删除、编辑、重连接及使能。 **删除:** 该操作将删除连接, 如果 IPSEC 通道已建立, 亦将被拆除;

**编辑:** 修改该条连接的配置信息, 修改之后, 如果要使配置生效, 需重新加载该连接; **重连接:** 该操作将拆除当前通道, 重新发起通道建立请求;

**使能:** 当连接处于使能状态时, 系统重启或进行重连接操作时, 该连接将发起通道建立请求; 而相反的, 将不会发起请求。

**添加:** 该功能用于新添一条 IPSEC 连接。

## 添加 IPSEC 连接或编辑 IPSEC 连接

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

**连接配置:** 该栏目包含了通道的基本地址信息。 **名称:** 用以标示该连接的名称, 须唯一;

**启用:** 选择启用, 则该条连接在系统起机或者进行重连接操作的时候, 将发起通道连接请求; 否则不会;

**本机的 WAN 接口:** 通道的本端地址;

**远程主机地址:** 对端的 IP/域名。如果采用了隧道模式的服务器端功能, 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。

**启用 DPD 检测:** 是否启用该功能, 打钩表示启用; **时间间隔:** 设置连接检测 (DPD) 的时间间隔;

**超时时间:** 设置连接检测 (DPD) 超时时间; **操作:** 设置连接检测的操作。

**高级配置:** 该栏目包含了 IKE、ESP 以及协商模式等相关配置。

**启用高级配置:** 启用, 则可以配置第一阶段及第二阶段的信息, 否则, 将根据对端自动协商;

**IKE 加密:** IKE 阶段的加密方式;

**IKE 完整性:** IKE 阶段的完整性方案;

**IKE DH 小组:** DH 交换算法;

**IKE 生命周期:** 设置 IKE 的生命周期, 目前以小时为单位, 默认为 0;

**ESP 加密:** ESP 的加密方式;

**ESP 完整性:** ESP 完整性方案;

**ESP 生命周期:** 设置 ESP 的生命周期, 目前以小时为单位, 默认为 0; **采用野蛮模式:** 如果打钩, 则协商模式将采用野蛮模式, 否则为主模式; **会话密钥向前加密:** 如果打钩, 则启用 PFS, 否则不启用;

**认证方式:** 可以根据需要选择共享密钥或者证书认证, 目前仅能选择共享密钥方式。



#### 4.3.3.5 GRE VPN



GRE隧道

GRE隧道  启用  禁用

通道

状态

名称

通过

对端WAN IP

对端子网  (eg:192.168.1.0/24)

对端隧道IP

本端隧道IP

本端子网掩码

保活  启用  禁用

重拔次数

重拔间隔

失败策略

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

**GRE 隧道:** 启用或者禁用 GRE 功能

**通道:** 可设置的通道, 目前最多可以设置 12 条 GRE 隧道

**状态:** 启用代表启用当前配置的 GRE 隧道, 否则代表关闭当前 GRE 隧道  
**名称:** 隧道的名称最长 30 个字符

**通过:** GRE 收发接口, 目前有 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:** 开启/关闭 GRE 保活

**重拔次数:** GRE 保活失败最大次数 **重拔间隔:** 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



## 4.3.4 安全

### 4.3.4.1

#### 防火墙

防

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

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

SPI防火墙  启用  禁用

#### 附加的过滤器

- 过滤代理
- 过滤Cookies
- 过滤Java Applets
- 过滤ActiveX

#### 其他过滤器

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

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

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

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

### 4.3.4.2 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)
- 阻止WAN口SNMP访问

**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。

厦门欣仰邦科技有限公司

Xiamen Siyb Technology Co.,Ltd.

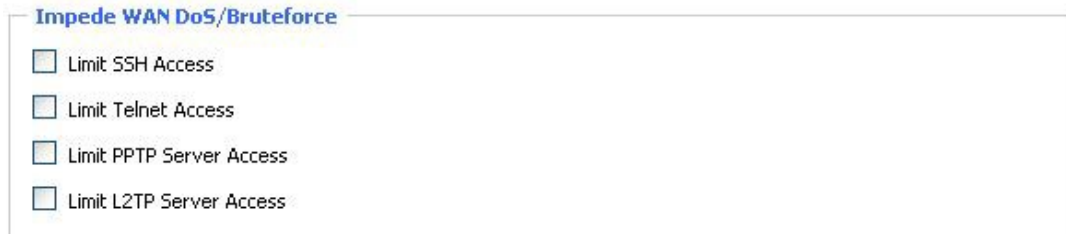
地址：厦门市集美区软件园三期B区  
04栋708室

网址：www.xmsiyb.com 邮箱：Support@xmsiyb.com  
电话：0592-3564822



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。

### 4.3.4.3

#### PN 穿透

V

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。

#### VPN穿透



**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。





#### 4.3.4.4

### 访问限制

#### 1. 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

删除	编号	源地址	源端口	目的地址	目的端口	协议	接口	方向
<input type="checkbox"/>	1	0.0.0.0/0	1-- 65535	0.0.0.0/0	1-- 65535	both	主链路	output

添加过滤规则

方向

接口

协议

源端口  -

目的端口  -

源地址     /

目的地址     /

**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。

**数据包包：**只接收符合自定义规则的数据包，丢弃所有其他的数据包。



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

### 添加过滤规则

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

#### 方向

**Input:** 数据包从 WAN 口到LAN 口。

**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。

## 4.3.4.5

## NAT

### 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）

映射

删除	编号	应用程序	协议	源IP范围	来源端口	IP地址	目的端口	启用
<input type="checkbox"/>	1		两者		0	0.0.0.0	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。

**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

**允许的源 IP 范围:** 在该栏填入 Internet 用户的 IP 地址。

**来源端口:** 在该栏填入由服务所使用的外部端口编号。

**IP 地址:** 输入您想让 internet 用户访问的服务器的内网 IP 地址。目

**的端口:** 在该栏输入服务所使用的内部端口编号。

**启用:** 选择“启用”框，启用您所定义的多端口转发服务。缺省配置为禁用（未选择）

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



## 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

删除	编号	应用程序	开始	结束	协议	IP地址	启用
<input type="checkbox"/>	1		0	0	两者	0.0.0.0	<input type="checkbox"/>



时禁用该端口转发。

**应用程序：**在应用程序提供的字段内输入应用程序的名字； **开始：**输入端口转发范围的开始端口号；

**结束：**输入端口转发范围的结束端口号；

**协议：**为每一种应用选择 UDP 或者 TCP 协议，两者为同时选择两种协议；

**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.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。

删除	编号	应用程序	已触发端口范围		转发端口范围		启用	
			开始	结束	协议	开始		结束
<input type="checkbox"/>	1	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	TCP	<input type="text" value="0"/>	<input type="text" value="0"/>	<input 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**”。

### 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。



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。

DMZ

使用DMZ  启用  禁用

DMZ主机IP地址 192.168.10.



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**”。

## 4.3.4.6 QoS 设置

### 1.基本

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



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%。

### 2.分类

#### Netmask 优先顺序



Netmask优先顺序

删除	Net	协议	源端口范围	目的端口范围	优先级
<input type="checkbox"/>	0.0.0.0/0	both	1-- 65535	1-- 65535	标准
<input type="button" value="添加"/>	<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"/>	TCP/UDP	<input type="text" value="1"/> -- <input type="text" value="65535"/>	<input type="text" value="1"/> -- <input type="text" value="65535"/>	

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:  $\min(\text{Max\_Up} - \text{Exempt\_Rate\_Up}, \text{Uplink})$ ;

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

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。

### 4.3.5

## 应用

### 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 DTU 设备。

串口通信时的串口参数设置。

### 协议类型

**UDP(DTU):** 串口转 UDP 连接, 添加自定义应用层协议, 完全等同于一台 DTU 的功能。**纯UDP:** 标准的串口转 UDP 连接。

**TCP(DTU):** 串口转 TCP 连接, 添加自定义应用层协议, 完全等同于一台 DTU 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

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
协议类型	纯UDP





**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：**8 字节的数据字符串，只有当协议类型设置成“UDP(DTU)”或者“TCP(DTU)”的时候这个配置项才有效。

**心跳时间间隔：**心跳包的时间间隔，只有当协议类型设置成“UDP(DTU)”“TCP(DTU)”的时候这个配置项才有效。

**自定义心跳包：**用户自定义的心跳包自

**定义注册包：**用户自定义的注册包

## 4.3.6 管理

### 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。 **路由器密码修改：**

#### 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" value="3"/>
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  启用  禁用

使用HTTPS

Web界面端口  (默认: 8088, 范围: 1 - 65535)

本地Web界面端口  (默认: 80, 范围: 1 - 65535)

SSH管理  启用  禁用

Telnet管理  启用  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

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。

## 2.保持活动

定时重启

你可以设置定时重启路由：定时 xxx 秒之后重启  
在某一特定日期时间，星期或每天重启。

定时重启

定时重启  启用  禁用

间隔（秒）

在设定的时间   :



## 4. 出厂默认

恢复出厂默认值 单击“是”按钮并保存设置，将所有配置清空恢复到出厂值。在恢复到默认设

### 复位路由器设置

恢复出厂默认  是  否

应用

取消

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”

## 5. 固件升级

### 固件升级

请选择一个用来升级的文件

选取文件

未选择文件

升级

**固件升级：**可将新的固件加载到路由器上。新的固件版本需要与我与欣仰邦物联网技术工程师联系。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。

## 6. 备份

本页面用于对路由器的配置文件进行备份或恢复。

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。



备份设置

点击 "备份" 按钮将配置备份文件下载到您的电脑。 [备份](#)

恢复配置

恢复设置

请选择一个用来恢复的文件 [选取文件](#) [未选择文件](#) [恢复](#)

## 4.3.7 状态

### 1. 路由器系统截图



## 2. 各参数说明

**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  
**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  
**WAN 域名:** WAN 口的域名, 可以在设置→基本设置中修改 **系统的本**  
**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  
**运行时间:** 系统上电开启的时间  
**所有可用:** 所有可用RAM 大小 (即物理内存减去一些预留位和内核的二进制代码大小) **空闲:** 被系统留着未使用的内存, 若内存小于500kB 则会重启,  
**已使用:** 已经使用的内存, 所有的可用内存减去空闲内存  
**缓冲区:** 即缓冲区使用的内存, 总内存减去已经分配的内存即为缓冲区内内存。 **已缓存:** 被高速连  
**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

**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:** 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

## 2. WAN

连接类型	自动配置 - DHCP
已连接时间	不可用

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

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



**IP 地址:** 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

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



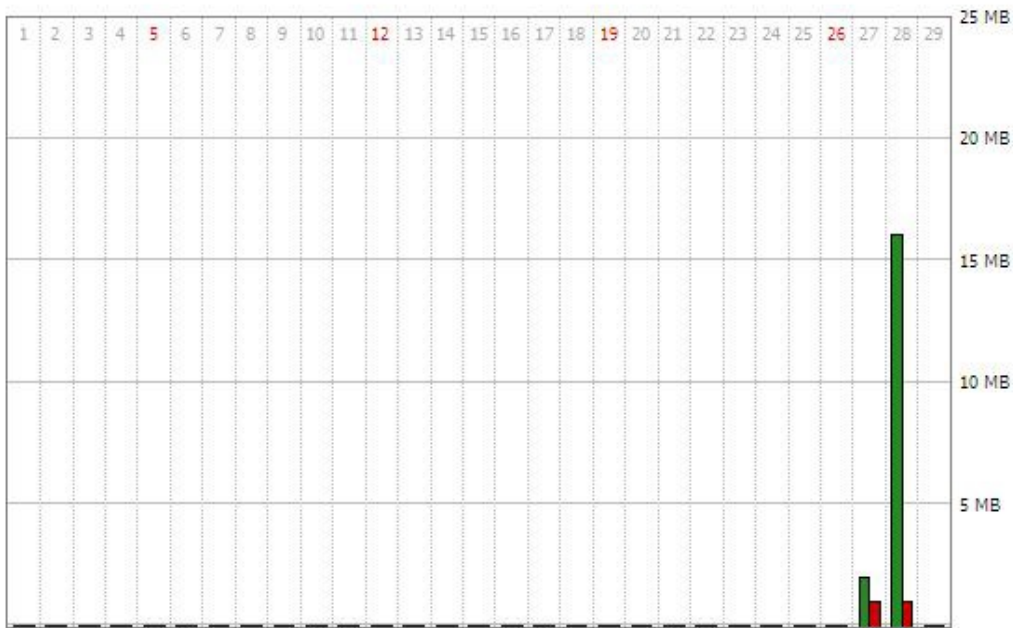


流量

总流量

下载 (MBytes)	0
上传 (MBytes)	0

月流量



2月 8, 2012 (下载: 0 MB / 上传: 0 MB)

上月 下月

**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. 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

**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	00:25:56:68:5E:30	1 day 00:00:00	
four-488e1df5fa	192.168.1.125	44:37:E6:09:D8:F7	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**删除：**点击可以删除  
DHCP 客户端

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

## 4.无线

无线状态	
MAC地址	00:0C:43:30:52:79
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**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	否	0	300(b/g/n)	加入
ff-old	AP	00:13:10:09:56:92	6	-44	-95	0	否	0	54(b/g)	加入

刷新

关闭

**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

## 5.PPTP/L2TP



**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



## 五、订购信息

您可以联系我司的销售人员来购买模块和开发套件。购买时请具体标明需要的产品型号。

联系方式如下：

厦门欣仰邦科技有限公司

地址：厦门市集美区软件园三期B区04栋708室

网址：[www.xmsiyb.com](http://www.xmsiyb.com)

电话：0592-3564822

邮箱：[Sales@xmsiyb.com](mailto:Sales@xmsiyb.com)

声明：本说明书所有权归我司所有，本公司保留未经通知随时更新本产品使用手册的最终解释权和修改权！

