WR301D 4G 无线
工业路由器产品手册

前言

感谢您使用深圳市讯记科技有限公司的 WR301D 4G 无线工业路由器，阅读本产品说明书能让您快速掌握本产品的功能和使用方法。

版权声明

免责声明

由于运营商升级网络造成设备无法继续使用的，本公司不能提供免费的升级服务。由于特殊原因造成运营商网络服务中断时，本机将无法正常工作，本公司不承担由此带来的后果。

本产品主要用于基于 GSM/短信/GPRS/3G/4G/网络的数据传输应用，请按照说明书提供的参数和技术规格使用，同时请注意无线电产品特别是 GSM/3G/4G 产品使用时应该关注的注意事项，本公司不承担由于不正常使用或不恰当使用本产品造成的财产或人身伤害。

修订记录

更新日期	文档版本	说明	作者
2020 年 09 月 20 日	V1.0		YRY

目录

1 产品简介

1.1 概述

近年来，WiFi 的发展是大家有目共睹的，时至今日，WiFi 已经遍及全球的各个角落，从办公室到家庭，从酒店到咖啡厅，从火车站到机场，只要你打开笔记本就可以搜索到 WiFi 信号，人们可以随时随地可以无线上网冲浪、收发 email 和观看视频。这都归功于 WiFi 路由器的大量普及。

科技的发展，技术的演绎，每一天都在催生新事物的诞生，而无线技术的日新月异，更为新事物带来了无限的发展契机。

4G 时代的到来，无线蜂窝网络内高速数据传输的实现，使得 WiFi 路由器也具备了无线接入到 Internet 的可能。

本路由器是一款工业物联网高速路由器，全线兼容 4G/3.5G/3G/2.5G 网路，旗舰级配置、VPN 链接、工业级防护、宽温、宽电压设计，可轻松组建高速、稳定的无线传输网络，利用公用 LTE 网络为用户提供无线长距离数据传输功能。

4G 路由器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 RS485/RS232、以太网 LAN，以太网 WAN 以及 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。

目前工业级产品拥有维护系统稳定的专利技术，确保设备永远在线；产品整机采用金属外壳，抗干扰防辐射，硬件上采用工业级设计；系统带有看门狗保护，另外加载了系统监测保护；经过严格的设计、测试和实际应用，产品性能稳定可靠。

1.2 典型应用

- 基站收发，ATM 监控，发电站监控，泵站监控等远程数据采集监控领域；
- 无人值守机房监控、动力机房监控、机房动环监控；
- 太阳能发电站、智能充电桩远程数据采集监控；
- 电柜的电流、电压、功率等参数采集；
- 水位、水压、流量、流速等参数采集；
- 气象台的风速、风力、雨量、温度等参数采集；

- 油位、油温、油压等数据采集；
- 智能化农业温湿度数据采集以及监控；
- 智能化养殖温湿度数据采集以及监控；
- ATM、POS、电表、PLC、DAQ 等设备的数据传输；
- 智能电网数据传输；
- 智能交通数据传输；
- 工业自动化数据传输；
- 环境保护数据传输；
- 气象台信息的数据采集以及监控；
- 农业、水务、煤矿等场合的数据传输；
- 智慧农业、智慧消防、智慧城市、智慧楼宇控制等场所；

1.3 安全说明

安全须知

请不要在禁止使用手机的场所使用本产品！

无线干扰

本产品使用 GSM/GPRS/3G/4G 无线网络，请注意无线干扰！

1.4 功能特点

- 支持数百种 3G/4G 无线模组，基本做到即插即用；
- 智能防掉线，支持在线检测，在线维持，掉线自动重拨，确保设备永远在线；
- 云端远程后台管理，广告推送，远程升级和远程配置；
- 本地网络 PHP 浏览，并可远程同步本地存储内容；
- 支持串口数据串口 TCP/UDP 透明数据传输或者 AT 指令传输；
- 短信控制路由上线下线，短线通知路由状态；
- 支持 VPN 安全隧道功能,包括 PPTP、L2TP；
- 完整强健的路由器功能，支持多种上网方式：自动分配，指定 IP， PPPoE；

- 支持 IPTABLES 防火墙，各种网络协议；
- 支持串口本地 TFTP、web 软件升级；
- 支持动态 DDNS ：支持花生壳、88IP 和 dyndns 域名服务商；

1.5 技术参数

分类	参数	描述
电源	输入电压	7～35V DC
	输入电流	正常：50mA@12V，最大：150mA@12V
	电源防护	防反接保护
以太网	接口数量	1 x WAN 接口/LAN 接口 1 x LAN 接口
	接口规格	RJ45，10/100Mbps，自适应 MDI/MDIX
	接口保护	ESD 接触：8KV ，浪涌：4KV（10/1000us）
串口	串口数量	1 通道
	串口类型	RS485（默认）/RS232
	串口波特率	110bps-128000bps
	数据位	7、8
	校验位	None，Even，Odd
	停止位	1,2
	工作模式	AT 指令模式、透传模式
	串口保护	ESD 接触：8KV 浪涌：4KV（8/20us）
WIFI	天线接口数量	2
	天线接口类型	SMA 孔式
	协议	802.11a/b/g/n （mixed）
	模式	AP 模式 、客户端模式
	频段	2.4G
	信道	Channel 1 - 13
	安全性	Open 、WPA、WPA2
	加密	AES、TKIP、TKIPAES
	连接数	32（Max）
	速率	300Mbps（Max）
	传输距离	室外无阻拦/空旷，覆盖范围可达 100 米
	SSID 广播开关	支持
蜂窝网	天线接口数量	1
	天线接口类型	SMA 孔式
	SIM/UIM 卡接口	自弹式接口，支持 1.8V/3V SIM/UIM 卡，内置 15KV ESD 保护
	4G（E 版本）	GSM/EDGE：900,1800MHz WCDMA：B1,B5,B8 FDD：B1,B3,B5,B7,B8,B20

		TDD：B38,B40,B41
	4G（AU 版本）	GSM/EDGE：850,900,1800MHz WCDMA：B1,B2,B5,B8 FDD：B1,B2,B3,B4,B5,B7,B8,B28 TDD：B40
	4G（A 版本）	WCDMA：B2,B4,B5 FDD：B2,B4,B12
	4G（V 版本）	FDD：B4,B13
	4G（J 版本）	WCDMA：B1,B3,B8,B18,B19，B26 FDD：B2,B4,B12 TDD：B41
	4G（CE 版本）	GSM/EDGE：900,1800MHz WCDMA：B1,B8 TD-SCDMA：B34,B39 FDD：B1,B3,B8 TDD：B38,B39,B40,B41
系统	CPU	MIPS CPU，主频 580Mhz
	存储	64Mbits SPI Flash
	内存	1024Mbits DDR2
软件参数	网络协议	IPV4、TCP/IP、PPPOE、DHCP、DNS、DDNS、NAT、HTTPS、ARP、FTP、telnet、SSH
	防火墙	支持 IPTABLES 、DMZ、DoS 防御
	VPN	PPTP、L2TP
	远程管理	支持 web 远程配置
	端口映射	支持
	短信指令	支持
	系统日志	支持
	固件升级	支持串口本地 TFTP、web 软件升级
认证	MTBF	≥10 万小时
	EMC	EN 55022: 2006/A1: 2007 (CE &RE) Class B
		IEC 61000-4-2 (ESD) Level 4
		IEC 61000-4-3 (RS) Level 4
		IEC 61000-4-4 (EFT) Level 4
		IEC 61000-4-5 (Surge)Level 3
		IEC 61000-4-6 (CS)Level 4
		IEC 61000-4-8 (M/S) Level 4
	其他	CE、FCC、ROHS、3C
环境	工作温度、湿度	-40～85℃，5～95%RH
	存储温度、湿度	-40～105℃，5～95%RH
其他	外壳	金属材质
	尺寸	86x71x28mm
	防护等级	IP30
	净重	280g

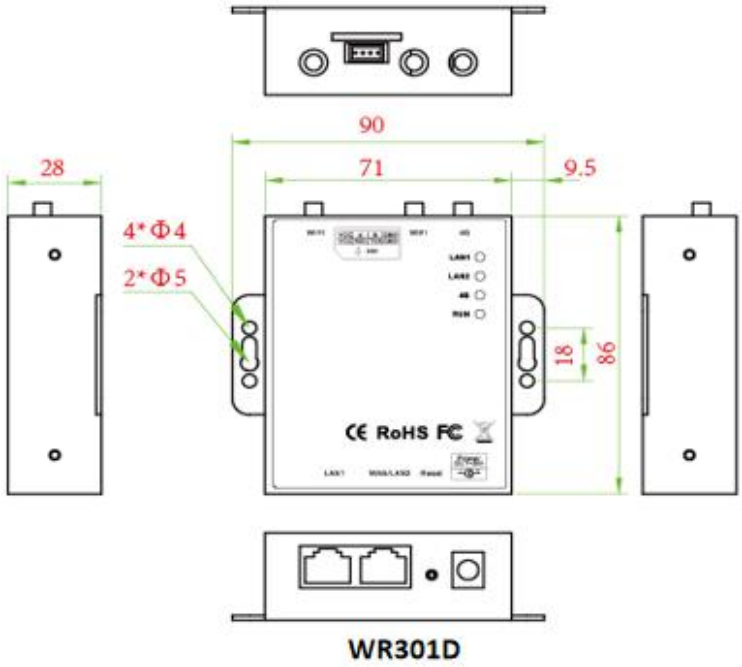
	安装方式	壁挂式、导轨式

1.6 设备选型

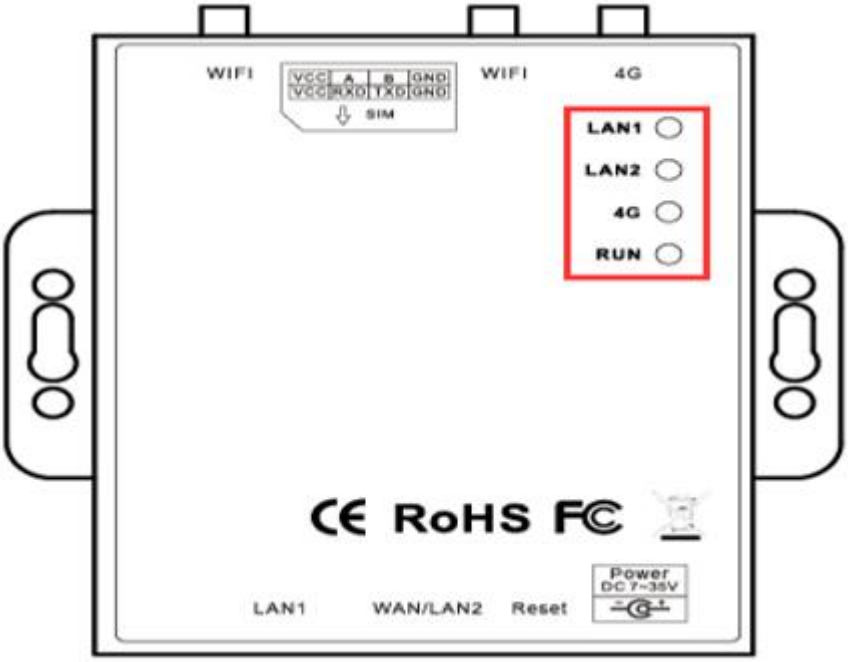
型号	串口	WAN	LAN	WIFI	GPS
WR301D	1	1	1	支持	不支持

2 硬件说明

2.1 外形尺寸



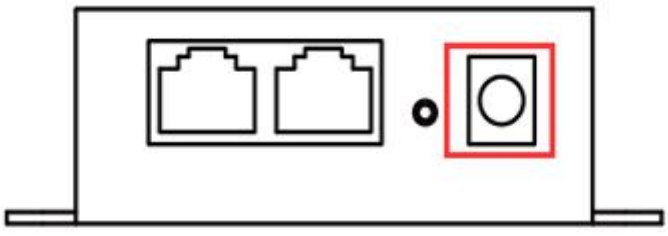
2.2 LED 指示灯



LED 指示灯			
型号	**名称**	**状态**	**描述**
WR301D	RUN	闪烁	系统正在运行
		灭	系统已停止运行
	4G	常亮	Internet 网连接正常
		灭	Internet 网未连接
	LAN1	常亮	LAN1 接口已连接设备
		灭	LAN1 接口未连接设备
	LAN2	常亮	LAN2 接口已连接设备
		灭	LAN2 接口未连接设备

2.3 电源输入

WR301D 支持 DC2.0 端子插入方式；

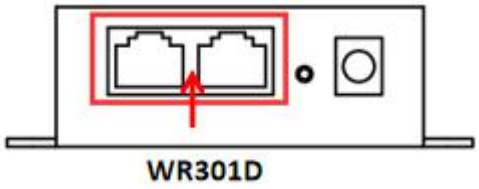


WR301D

2.4 以太网口

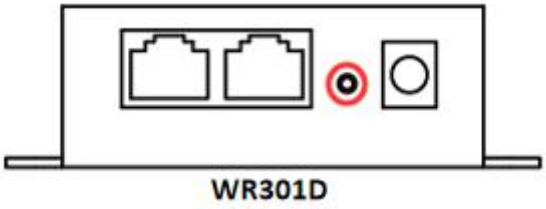
WR301D 有 2 个以太网口，1 个 WAN/LAN 口和 1 个 LAN 口；WAN/LAN 接口只有在“标准路由模式”下为 WAN 功能，其他模式下为 LAN 功能。

注：路由器出厂默认为“3G/4G 无线路由模式”，WAN/LAN 口默认为 LAN 功能。



2.5 重置按钮

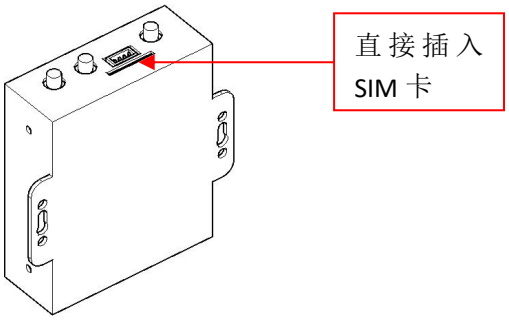
路由器正常运行后，用一根尖状棒持续按住重置键 5 秒，直到 RUN 指示灯出现快速闪烁，此时路由器已恢复出厂默认设置。



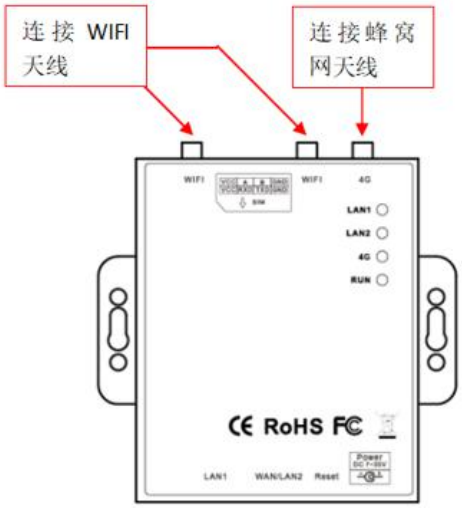
2.6 SIM 卡

插入/移除 SIM 卡时，先确保设备已关机。

WR301D 支持自弹式卡槽接口

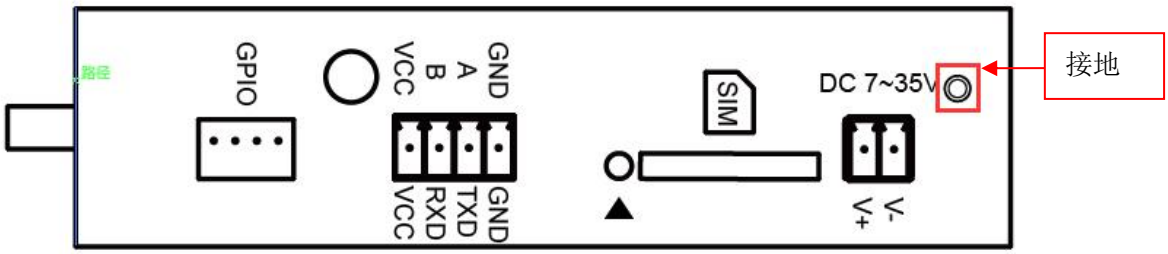


2.7 连接外部天线



2.8 路由器接地

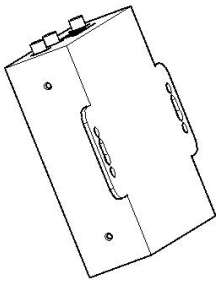
路由器接地线有助于防止电磁干扰带来的影响。在连接设备之前，先通过接地螺丝接线让设备接地。注：该产品宜安装在接地良好的器件表面，如金属板。



3 产品安装

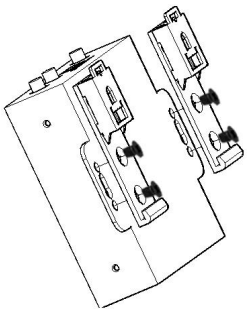
本设备支持水平桌面放置、壁挂式和导轨安装

3.1 壁挂式

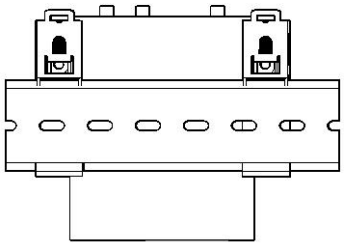


壁挂式

3.2 导轨式安装



卡扣安装



导轨安装

4 参数配置

4.1 配置前准备

路由器支持网页配置，支持使用的浏览器有 IE6.0 或以上版本、谷歌和火狐等，而支持使用的操作系统有 Linux 2.6 及以上，Mac OS 10.3.7 及以上，Windows XP/ Vista/7/8 /10 等。

连接路由器的方式有 2 种，一种是通过有线连接，通过外部中继器/集线器连接，或直接连接到电脑；另一种是通过 WIFI 连接到路由器。路由器直接连接到电脑的以太网口时，如果路由器作为 DHCP 服务器，那么电脑可以直接从路由器获取 IP；电脑也可以设置和路

由器同在一网段的静态 IP，这样电脑与路由器就构成了一个小型的局域网。电脑与路由器已成功建立连接后，在电脑浏览器上输入设备的默认登录地址，即可进入路由器的 WEB 登录界面。

4.1.1 通过有线连接

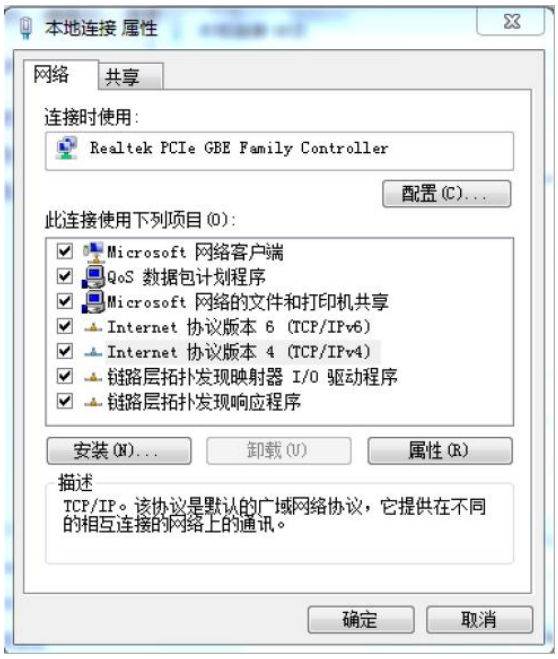
在 PC 这端，有两种方法配置其 IP 地址：一是在 PC 的本地连接上开启自动获取 IP 地址，二是在 PC 的本地连接上配置一个跟路由器在同一个子网的静态 IP 地址。

下面以配置 Windows 7 系统为例。Windows 系统的配置均相似。

1. 单击“开始 > 控制面板 > 网络和共享中心”，在打开的窗口中双击“本地连接”。

2. 在“本地连接 状态”窗口中，单击“属性”。

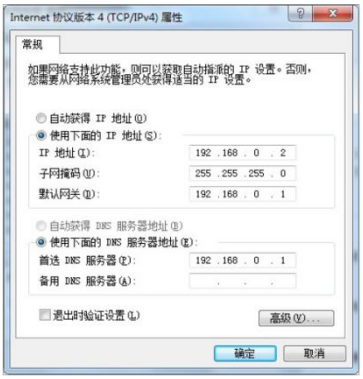
3. 选择“Internet 协议版本 4（TCP/IPv4）”，并单击“属性”。



4. 两种方法配置 PC 的 IP 地址：

自动从 DHCP 服务器获取 IP 地址，单击“自动获得 IP 地址”；

手动给 PC 配置一个跟路由器地址在同一个子网的静态 IP 地址，单击并配置“使用下面的 IP 地址”。

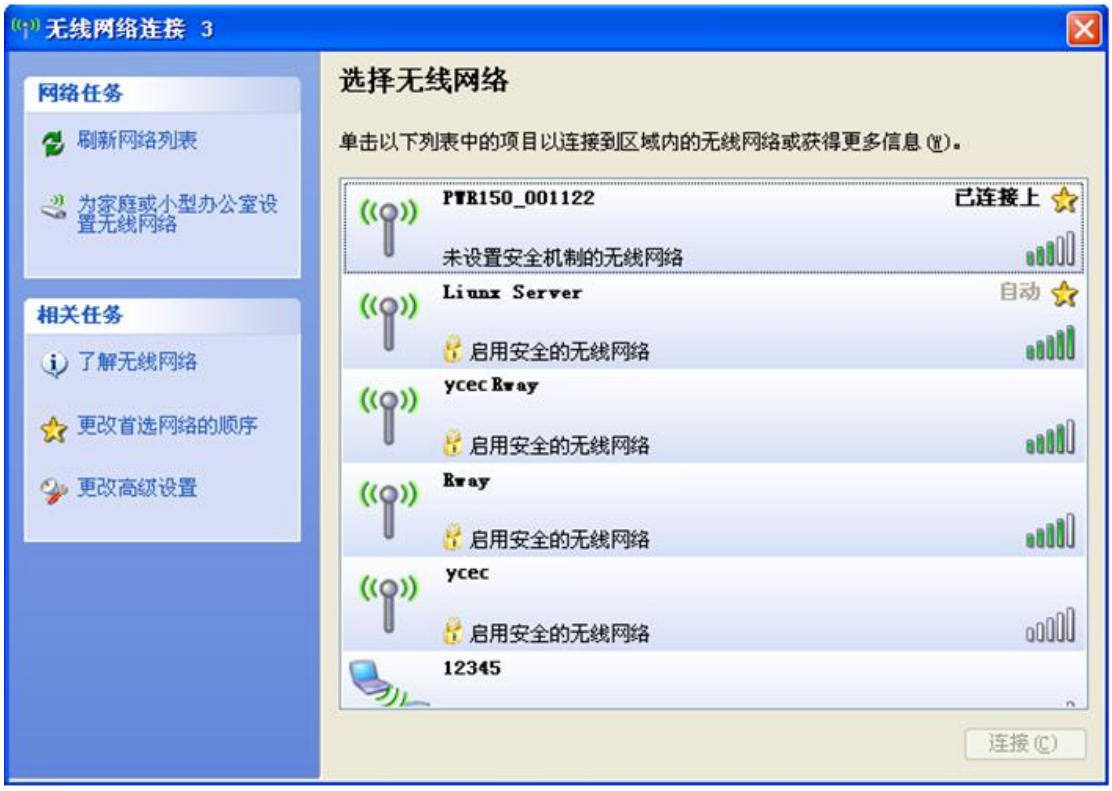


5. 单击“确定”以完成配置。

4.1.2 通过 WIFI 连接

1. 检测无线路由器的无线网络连接

2. 后点击“连接”建立连接。



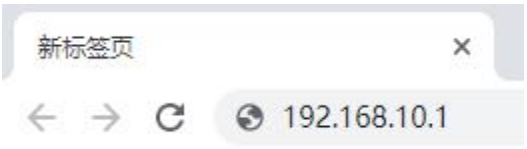
4.1.3 出厂默认设置

登录配置页面前，您有必要了解以下的默认设置。

项目	描述
用户名	admin
密码	admin
DHCP 服务器	开启
WIFI	AP 模式 SSID：Wifi-xxxx-xxxx KEY ： 12345678

4.1.4 登录 web 配置页面

1. 在 PC 上，打开浏览器，如 IE、谷歌等；
2. 在浏览器的地址栏上输入路由器的 IP 地址 http://192.168.10.1/以进入用户登录身份认证界面；



3. 在登录页面输入“用户名”、“密码”，再单击“确定”按钮。

成功登录路由器后，页面显示如下图所示：

5 路由器配置

5.1 当前状态

在当前状态中，提供了系统状态、系统信息、流量统计、用户统计、连接统计、NAT 统计和接口统计等。

5.1.1 系统状态

显示当前系统的运行状态

系统状态		
项目	说明	默认
WAN 状态	当前的连接方式和状态，以及获取到的 IP 地址、网关地址和 DNS 服务器地址等。可以根据这些来判断路由器是否正常工作。	--
LAN 状态	LAN 的 IP 地址，DHCP 服务器是否启动以及可以分配的 IP 地址范围等。	--
3G/4G 状态	是否连接了 3G/4G 设备以及设备名称、制造商、类型和 ID 等。	--
因特网时间	系统的因特网时间。	--

5.1.2 系统信息

在系统信息页中，将显示系统的一些基本信息和目前系统资源的使用情况。

系统信息		
项目	说明	默认
CPU 类型	设备使用的 CPU 具体型号	--
序列号	设备序列号	--
运行时间	路由器上电运行到现在的时间	--
内存使用	当前内存使用率。	--
内存大小	64M	--
软件版本	设备当前的系统版本	--
CPU 负荷	当前 CPU 使用率	--
连接数使用率	当前建立的 NAT 会话数占系统能处理的最大 NAT 会话数的百分比	--
系统历史记录	记录系统的一些重要信息，可以帮助您快速定位设备故障或了解网络情况，如系统在运行过程中的设置状态变化、网络攻击等信息。	--

注①：路由器重启后，所有记录的日志都会丢失。

5.1.3 文件共享

路由器保留功能，暂未开放。

5.1.4 视频监控

路由器保留功能，暂未开放。

5.2 工作模式

WR301D 支持以下 4 中工作模式：

工作模式		
项目	说明	默认
3G/4G 无线路由模式	路由器的“3G/4G 设置”界面即为 WAN 设置界面，其“上网方式”只有 4G 拨号；	勾选
标准无线路由模式	路由器的上网方式是可选择的，有静态地址、动态地址和 PPPoE；	未选
无线 AP+无线客户端桥模式	无线和有线网络作为局域网接入点,无线以桥接连接远程 AP；	未选
无线 AP+客户端模式	即中继模式或 WISP，无线接口同时作为客户端连接其他的 AP。请结合 ISP 提供的信息选择合适的上网方式。	未选

选择<工作模式>后，您可以在〈3G/4G 设置〉或〈WAN 设置〉中设置：

- 连接方式
- 断线检测
- MAC 克隆(非 3G/4G 模式)
- 动态域名设置
- AT 指令 (3G/4G 模式)

5.3 3G/4G 设置（WAN 设置）

5.3.1 连接方式

5.3.1.1 3G/4G 无线路由模式

- 自动适配运营商:对于普通手机 SIM 卡或物联网 SIM 卡，不需要设置，系统自动查询合适的 ISP 拨号上网。
- VPDN 拨号:对于专网资费卡，需要设置特定的 APN，用户名和密码,实现 VPDN 接入。VPDN 英文为 Virtual Private Dial－up Networks，又称为虚拟专用拨号网，是 VPN 业务的一种，是基于拨号用户的虚拟专用拨号网业务。即以拨号接入方式上网，是利用 IP 网络的承载功能结合相应的认证和授权机制建立起来的安全的虚拟专用网，是近年来随着 Internet 的发展而迅速发展起来的一种技术,可用于跨地域集团企业内部网、专业信息服务提供商专用网、金融大众业务网、银行存取业务网等业务。VPDN 采用专用的网络安全和通信协议，可以使企业在公共网络上建立相对安全的虚拟专网。VPN 用户可以经过公共网络，通过虚拟的安全通道和用户内部的用户网络进行连接,而公共网络上的用户则无法穿过虚拟通道访问用户网络内部的资源。

3G/4G 无线路由模式@连接方式		
项目	说明	默认
拨号设备选择	选择下拉框中的静态地址。	3G/4G
自动选择 3G/4G 服务商	勾选，将会自动选择网络运营商	勾选
3G/4G 服务商	一般为 中国移动，中国联通，中国电信	--
APN	一般由 ISP 提供。专网卡须填入。	--
Pin code	SIM卡 pin code	--
拨号号码	一般由 ISP 提供。	--
用户名	一般由 ISP 提供。专网卡须填入。	--
密码	一般由 ISP 提供。专网卡须填入。	--
认证方式	分为CHAP 和PAP。 chap是三次握手，双方只传用户名，不传密码，密码是事先在路由器上配好了的，只需要比较就可以了。而pap是二次握手，不仅传用户名还传密码，且密码是明文传输，不安全。	自动

断线自动重连	可选项，建议打开。	勾选
重拨 N 次后重启	默认 3 次。如果没插 SIM 卡测试，建议取消，防止测试中自动重启。	3
特殊初始化 AT 指令	手动添加 AT 拨号时自动执行的项目。	空

5.3.1.2 标准无线路由模式

动态上网方式

动态地址@WAN 设置		
项目	说明	默认
上网方式	包括：动态地址、静态地址、PPPOE	动态地址
MTU	最大传输单元（Maximum Transmission Unit），是在一定的物理网络中能够传送的最大数据单元。参数取值范围为 576～1500，单位为字节，默认值为 1500，建议保持默认值。	1500
主 DNS 服务器	可选项，一般情况下当地 ISP 运营商 提供，也可以自行设置。	空
辅 DNS 服务器	可选项，一般情况下当地 ISP 运营商 提供，也可以自行设置。	空
主机名	可选项，网络中其他设备看到的 PWR 系列的设备名称，默认为空。	空

当上网方式选择为“静态地址”时，界面如下：

静态地址@WAN 设置		
项目	说明	默认
上网方式	静态地址。	动态
IP 地址	一般由 ISP 提供。局域网自定义。	0.0.0.0
子网掩码	一般由 ISP 提供。局域网自定义。	0.0.0.0
缺省网关	一般由 ISP 提供。局域网自定义。	0.0.0.0
MTU	最大传输单元（Maximum Transmission Unit），是在一定的物理网络中能够传送的最大数据单元。参数取值范围为576～1500，单位为字节，默认值为1500，建议保持默认值。	1500
主 DNS 服务器	可选项，一般情况下当地 ISP 运营商 提供，也可以自行设置，至少要输入一个。	空
辅 DNS 服务器	可选项，一般情况下当地 ISP 运营商 提供，也可以自行设置。	空

当上网方式选择为“PPPOE”时，界面如下：

PPPOE@WAN 设置		
项目	说明	默认
上网方式	PPPoE	动态
PPPoE 用户名	由当地 ISP 运营商 提供。	空
PPPoE 密码	由当地 ISP 运营商 提供。	空
MTU	最大传输单元（Maximum Transmission Unit），是在一定的物理网络中能够传送的最大数据单元。参数取值范围为546～1492，单位为字节，默认值为1492，建议保持默认值。	1492
主 DNS 服务器	可选项，一般情况下当地 ISP运营商 提供，也可以自行设置。	空
辅 DNS 服务器	可选项，一般情况下当地 ISP 运营商 提供，也可以自行设置。	空
主机名	可选项，输入 ISP 提供的 PPPoE 的服务器的名称，一般 ISP 不要求填写。	空
服务名称	可选项，输入 ISP 提供的 PPPoE 的服务器的名称，一般 ISP 不要求填写。	空

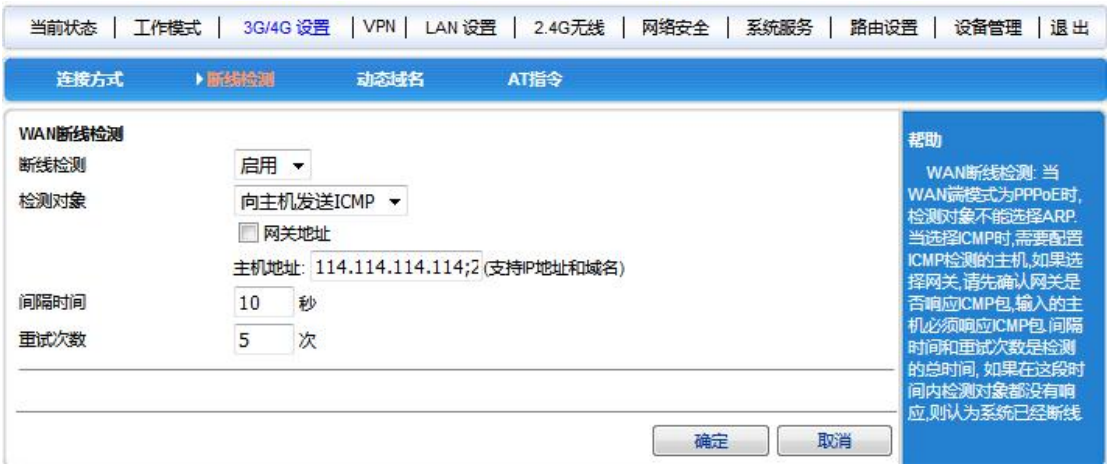
5.3.1.3 无线 AP+客户端桥模式

我们可以将路由器作为一个桥接 AP 使用，用于桥接前一级无线路由器。通过网线连接 LAN 接口，进入路由器<工作模式>，选择无线 AP+客户端桥模式。

5.3.1.4 无线 AP+客户端模式

5.3.2 断线检测

WAN 口断线检测：每隔多少时间检测 WAN 口网络情况，以及检测失败后允许重试的次数。



5.3.3 WAN 口 MAC 地址克隆

路由器出厂时，各个接口（LAN、WAN 口）都有一个缺省的 MAC 地址，一般情况下，无需改变。有些 ISP 要求只有注册的那个 MAC 地址才能上网，这种情况下，应选择“使用下面手工输入的 MAC 地址”，将 MAC 地址改为 ISP 指定注册的 MAC 地址。设置界面如下图所示。

5.3.4 动态域名

由于通过 PPPoE 地址上网时，获取到的 IP 地址不固定，这给想访问本局域网服务器的因特网用户带来很大的不便。

DDNS（Dynamic Domain NameService，动态域名服务）可以解决这个问题。路由器在 DDNS 服务器上会建立一个 IP 与域名（需要预先注册）的关系表，当 WAN 口 IP 地址变化时，路由器会自动向指定的 DDNS 服务器发起更新请求，DDNS 服务器上更新域名与 IP 地址的对应关系，无论路由器 WAN 口IP 地址如何改变，因特网上的用户仍可以通过域名对其进行访问。

【举例】

如果您已经在www.3322.org上注册了域名gg.3322.org，建立该域名与路由器的 WAN 口IP地址之间动态对应关系的方法如下图：

状态显示是否连接成功，只有状态栏显示为“已连接”，DDNS 功能才正常启动。

5.4 VPN 设置

在〈VPN 设置〉中您可以设置：

- PPTP 设置
- L2TP 设置

5.4.1 PPTP

PPTP@VPN 设置		
项目	说明	默认
启用 PPTP	PPTP启用开关	未选
PPTP 自动连接	当WAN口连接成功后自动拨VPN	未选
只用 PPTP 连接外网	全局流量走 VPN 网关,配合"VPN NAT"可使用端口转发\DMZ	未选
PPTP 服务器	必填	空
PPTP 用户名	必填	空
PPTP 密码	必填	空
MTU,MRU	默认 1450,如无必要,不建议改动	1450
对方网段	访问VPN子网使用	1450
断线检测	ping检测VPN服务器,如果服务器禁止ping,禁用此项	启用
VPN NAT	配合"只用 PPTP 连接外网" 使用端口转发\DMZ	勾选
VPN DNS	PPTP 使用 VPN 服务器的 DNS	勾选

5.4.2 L2TP

L2TP@VPN 设置		
项目	说明	默认
启用 L2TP	L2TP启用开关	未选
L2TP 自动连接	当WAN口连接成功后自动拨VPN	未选
只用 L2TP 连接外网	全局流量走 VPN 网关,配合"VPN NAT"可使用端口转发\DMZ	未选
L2TP 服务器	必填	空
L2TP 用户名	必填	空
L2TP 密码	必填	空
MTU,MRU	默认 1450,如无必要,不建议改动	1450
对方网段	访问VPN子网使用	1450
断线检测	ping检测VPN服务器,如果服务器禁止ping,禁用此项	启用
VPN NAT	配合"只用 L2TP 连接外网" 使用端口转发\DMZ	勾选
VPN DNS	L2TP 使用 VPN 服务器的 DNS	勾选

5.5 LAN 设置

在〈LAN 设置〉中您可以设置：

- LAN 口的基本设置
- IP&MAC 地址绑定
- DHCP 分配状态表

5.5.1 基本设置

5.5.1.1 LAN 设置

局域网内计算机可以通过 LAN 口 IP 地址来管理路由器。如下图：

注：修改 LAN 口的 IP 地址后需重新登陆到新的设备地址才能继续访问路由器 Web 界面。

LAN 设置@基本设置		
项目	说明	默认
IP 地址	LAN 口 IP 地址。您可以通过该 IP 地址访问路由器 Web 界面。	192.168.10.1
子网掩码	LAN 口的 IP 地址对应的子网掩码	255.255.255.0。
同步地址池	默认 IP 为 192.168.10.1，如果修改为 192.168.12.1，点击同步地址池，可分配的地址自动变为 192.168.12.2-192.168.12.254	--

5.5.1.2 DHCP 服务器设置

路由器可以作为 DHCP 服务器，给局域网内计算机分配 IP 地址。

路由器的 DHCP 服务器 IP 地址分配机制：

- 路由器接收到 DHCP 客户端获取 IP 地址的请求时，首先查找IP/MAC绑定关系表（设置路径：**LAN设置→IP/MAC 绑定**，具体请参见“**6.2 IP/MAC 地址绑定**”），如果这台计算机在 IP/MAC 绑定表中，则把对应的的 IP 地址分配给该计算机。
- 如果请求获取 IP 地址的计算机不在 IP/MAC 绑定表中，路由器会从地址池中选择一个在局域网中未被使用的 IP 地址分配给该计算机。
- 如果计算机离线（如关机），路由器不会马上把之前分给它的 IP 地址分配出去，只有在地址池中没有其它可分配的 IP 地址，且该离线计算机 IP 地址的租约过期时，才会分配出去。
- 如果地址池中没有任何可分配的 IP 地址，则计算机获取不到 IP 地址。

【例 6.1】：
比如，假设地址池范围为 192.168.10.190～192.168.10.200，计算机 A 设置 IP/MAC 地址绑定，绑定的 IP 地址为 192.168.10.210；计算机 B 未设置 IP/MAC 地址绑定关系。这种情况下，计算机 A 分配到 IP 地址 192.168.10.210。计算机 B 分配到地址池范围内的一个 IP 地址，如 192.168.10.2。

DHCP@基本设置		
项目	说明	默认
启用 DHCP 服务器功能	选中此项，启用 PWR 的 DHCP 服务器功能，否则禁用。	启用
可分配的起始地址	DHCP 服务器地址池的起始地址，必须与 LAN 口设置在同一子网内。	192.168.10.2
结束地址	DHCP 服务器地址池的的结束地址，必须与 LAN 口设置在同一子网内。地址池结束地址要大于地址池起始地址。	192.168.10.254
租约时间	输入给计算机分配 IP 地址的租约时间，当租约时间到后，计算机必须重新向 PWR 申请一次（一般计算机会自动申请）。单位为分钟。	1440

注：若所设置的路由器 LAN 口 IP 地址包含于 DHCP 可分配的 IP 起始地址和结束地址之间，路由器会自动将 DHCP 可分配的 IP 起始地址设置为路由器 LAN 口 IP 地址最后一位加一所得的地址，以避免路由器地址和局域网中 PC 机分配到的 IP 地址间的冲突。

5.5.2 IP&MAC 地址绑定

〈IP&MAC 绑定〉启用有 3 个功能：
- DHCP 服务器根据添加的 IP&MAC 来分配 IP 地址。

- 在路由器的 ARP 表中设置静态 ARP 缓存,防止 ARP 病毒修改 ARP 表。
- 可严格控制用户修改 IP 或者 MAC 地址,控制用户的上网行为,同时也可以防止一些 DDoS 攻击。

说明：

- 最多支持 254 个 IP/MAC 绑定表项,各型号支持的数量不一样。
- 缺省情况下，未进行 IP/MAC 地址绑定。

IP/MAC 绑定功能可以通过三种方式实现：

- 手工逐条配置，点击下图中的<添加到列表>按钮，将设置添加到 IP/MAC 绑定表中。
- 支持一键绑定功能，在网络稳定并且所有计算机都在线的情况下，单击<查看新 IP>按钮，自动绑定没有添加的 IP&MAC，导入 IP/MAC 绑定表中.
- 先写好“.cfg” 格式的文件，然后单击<批量导入>按钮导入。

注： .cfg 文件的格式是“MAC 地址 - IP 地址 - 用户名”

【举例】

00:00:e8:f5:6e:3a -192.168.10.22- host

00:00:00:00:11:11- 192.168.10.111- host 1

IP&MAC 绑定		
项目	说明	默认
IP&MAC 地址绑定	点击〈启用〉才能设置后面相关项，点击〈禁用〉则路由器 IP&MAC 地址绑定功能全部失效。	启用
已绑定 IP&MAC 地址	如启用〈禁止修改 IP 地址〉，已绑定的 MAC 地址对应的 IP 地址不能修改，如更改，则不能通过路由器 。	允许修改 IP 地址

未绑定 IP&MAC 地址	启用〈允许通过〉，未绑定的 MAC 地址可以通过 LAN 口网段的 IP 地址通过路由器，反之，起用〈禁止通过〉则未帮定的 IP&MAC 地址是不能通过路由器 的。	允许通过
静态 IP 地址	输入该计算机的 IP 地址。IP 地址可以不在路由器 DHCP 服务器分配的地址池内，但要与 LAN 口 IP 地址在同一子网内。	空
MAC 地址	输入该计算机的 MAC 地址。	空
用户名	输入进行 IP 和 MAC 地址绑定的计算机名称。	空
查看新 IP	单击该键，路由器会自动扫描整个该局域网内的所有 IP，将未绑定的 MAC 地址，进行 IP&MAC 地址。 说明：这种方法比较适合网络稳定、所有计算机在线的情况下使用，可轻松获得局域网内计算机 IP/MAC 绑定表项。但使用这种方式，可能由于 ARP 表项老化等情况，ARP 缓存表中缺少一些计算机的信息，即这些 IP/MAC 地址未绑定。建议通过此方法设置完后，检查希望绑定的计算机是否在绑定列表中，如果没有，再手工添加。	--
批量导入	单击改键，选择需要绑定的 ARP 表项，单击<确定>，即可导入页面下方的 IP/MAC 绑定表。	--

【例6.2】：

某网吧由于局域网内计算机有病毒或其它原因，ARP 攻击报文不停攻击路由器，导致局域网内计算机上网不正常。希望实现以下需求：

- 局域网内计算机通过 DHCP 动态获取到 IP 地址；
- 计算机 IP 地址与设置的绑定关系表不一致时，该计算机就不能上网，从而避免上网用户随意修改计算机的 IP 地址；
- 外来计算机(如上网用户自带的笔记本计算机)接入不能访问因特网；
- 局域网的 ARP 攻击不影响局域网内计算机访问因特网。

设置步骤：

(1) 启用路由器的 DHCP 服务器功能(**LAN 设置→基本设置→DHCP 服务器设置**)，设置 IP 地址池范围，如192.168.10.2～192.168.10.254，使局域网内计算机动态获取 IP 地址。(计算机必须设置为自动获取 IP 地址）。

(2) 设置 IP/MAC 绑定关系表，把局域网内所有计算机的 IP 地址与 MAC 地址对应关系设置到列表中。（也可参照上表中**〈查看新 IP〉**的方式，对局域网内所有计算机的 IP 地址与之相对应的 MAC 地址进行帮定）

(3) 选中**〈已绑定 IP/MAC 地址〉→〈禁止修改 IP 地址〉**。

(4) 选中**〈未绑定 IP/MAC 地址〉→〈禁止通过〉**。

(5) 单击**<确定>**按钮，配置完成。

5.5.3 分配状态表

通过该表您可以看到 DHCP 服务器已分配的所有 IP 地址列表。

5.6 媒体设置

路由器保留功能，暂未开放。

5.7 2.4G 无线

在<无线设置>中，您可以进行以下设置：

- 无线设置
- 无线安全
- 无线高级设置
- 无线用户列表
- 无线 MAC 过滤

5.7.1 无线设置

设置无线连接基础信息。在此页面中，您可以设置开启和关闭无线功能、广播和禁止广播 SSID、设置 SSID 名称等。

5.7.2 无线安全

无线安全模式有以下几种类型，可以按需要选择不同的安全模式。

- 停用
- Open System
- WPA-PSK
- WPA2-PSK
- WPAPSK/WPA2PSK(即 WPA-PSK 和 WPA2-PSK 混合模式)

5.7.2.1 Open System

在此安全模式下，加密类型有：None 和 WEP。

Open System @无线安全		
项目	说明	默认
加密类型	有两种加密类型可供选择：None 和 WEP。选择 None 则为不加密。	None
WEP 加密长度	有两种加密长度可供选择：64bit 和 128bit。	64bit
默认密钥 ID	可以同时设置 4 个密钥,但只可选择 1 个密钥在当下使用。此项为选择当前要使用的密钥。	密钥 1
WEP 密钥	可以选择设置的密钥类型并设置密钥。有两种密钥类型可供选择:十六进制型和字符型。根据不同的加密长度和密钥类型，设置不同的密钥。	--

密钥设置：
64bit 加密： 10 位十六进制型 或 5 位字符型。
128bit 加密：26 位十六进制型 或 13 位字符型。

5.7.2.2 WPA-PSK

此安全模式即为 WPA-PSK 加密模式。

WAP-PSK @无线安全		
项目	说明	默认
安全模式	选择 WPA-PSK。	--
加密类型	有两种可供选择：TKIP 和 AES。	--
WPA-PSK 密钥	设置密钥，合法的密钥长度为：8-63 个 ASCII 字符或 64 个十六进制数(0~9、a~f 或 A~F)。	--
密钥更新间隔	设置密钥更新时间间隔，以秒为单位。	3600

5.7.2.3 WPA2-PSK

WAP2-PSK @无线安全		
项目	说明	默认
安全模式	选择 WPA2-PSK。	--
加密类型	有两种可供选择：TKIP 和 AES。	--
WPA-PSK 密钥	设置密钥，合法的密钥长度为：8-63 个 ASCII 字符或 64 个十六进制数(0~9、a~f 或 A~F)。	--
密钥更新间隔	设置密钥更新时间间隔，以秒为单位。	3600

5.7.2.4 WPAPSK/WPA2PSK

WAP-PSK/WAP2-PSK @无线安全		
项目	说明	默认
安全模式	选择 WPA-PSK/WPA2-PSK。	--
加密类型	有两种可供选择：TKIP 和 AES。	--
WPA-PSK 密钥	设置密钥，合法的密钥长度为：8-63 个 ASCII 字符或 64 个十六进制数(0~9、a~f 或 A~F)。	--
密钥更新间隔	设置密钥更新时间间隔，以秒为单位。	3600

5.7.3 高级设置

设置无线连接的一些高级信息。

高级设置		
项目	说明	默认
分片阈值	分片阈值就是报文的长度大于设定的值时进行分片发送，就是一个报文被拆成几个依次发送	2346
RTS 阈值	RTS 阈值是指当报文长度超过设定的阈值时，AP 会先发送 RTS 报文用来清空信道，防止干扰	2347
Beacon 间隔	是用来设定多长时间发送一次 beacon 报文	100
数信比例	1	1
发射功率	百分之 1-100%	100
信号连接限制	0-（-100）	-90

5.7.4 无线用户列表

可以查看当前无线连接的用户信息。

5.7.5 无线 MAC 过滤

无线 MAC 过滤可以实现路由器的无线白名单和黑名单。如果设置为 “允许接入”，只有列表中 MAC 能连接到无线，其他不能接入。如果设置为“禁止接入”，列表中的 MAC 不能连接到无线，其他的都可以。

无线 MAC 过滤		
项目	说明	默认
停用	关闭过滤	勾选
允许接入	只有列表中 MAC 能连接到无线，其他不能接入	未选
禁止接入	列表中的 MAC 不能连接到无线，其他的都可以	未选

5.8 网络安全

网络安全设置包括：防火墙设置、站点控制、MAC 地址过滤、访问控制、端口阻挡、防止 DOS 攻击。

5.8.1 防火墙设置

启用防火墙功能后，可防止因特网对路由器或局域网内计算机的恶意攻击，保证路由器和局域网计算机的安全运行。特别是一些对外开放的服务器（如虚拟服务器、DMZ 主机等），启用路由器防火墙功能可以阻断恶意攻击源，防止 DoS 攻击。

在防火墙设置中（并发连接数，若非 0）可控制每个 IP 地址的 TCP 连接数，防止 WAN 端来的 PING 行为，若禁用防火墙功能则所有有关防火墙的设置将失效，路由器将存在危险。

通过设置，可控制 PPTP、L2TP、IPSEC 数据包是否通过路由器，WAN 口 ping 防止。

5.8.2 访问控制

在**〈访问控制〉**中您可根据源 IP 地址、目的 IP 地址、协议类型、目的端口范围、时间段和星期等来控制局域网内的计算机访问因特网，您也可以通过特殊应用，对您局域网内的用户分时间段控制 QQ，MSN 等上网行为。

可以方便灵活的添加规则，来达到您自己想要的控制目的。

添加规则的原则是：**最先添加的规则，优先权最高**。优先权最高的，通过路由器的数据最先与这条规则比较，若符合就不再跟以后的规则比较了，由这条规则决定该数据是通过还是阻挡。

访问控制		
项目	说明	默认
启用	选中后站点控制才开始生效	未选
源 IP 地址	输入需要控制的局域网内计算机的 IP 地址。源地址必须填写。	空
目的 IP 地址	输入需要控制的目的 IP 地址。如果无需控制目的地址，此项设置不填即可，表示所有 IP 地址。	空
协议	选择需要控制的协议类型。有 TCP、UDP 、TCP/UDP、ICMP 和 ALL 五个选项，其中 ALL 包括 TCP、UDP 、TCP/UDP 和 ICMP。缺省是 TCP。	TCP
目的端口	输入需要控制的目的端口号。如果无需控制目的端口，此项请选〈所有端口 1~65535〉，起始端口号应不能大于终止端口号。	空
天	选择一周内每天或工作日（星期一到星期五），规则生效	每天
时间	选择规则每天生效的时间段，时间使用 24 小时制。起始时间应早于终止时间，00：00～23：55 表示该规则在一天内任何时间都生效。	--
阻挡或通过	选择允许匹配的报文（通过）还是（阻挡）。	阻挡

【举例】

我们按上面原则来配置一个应用案例,仅仅允许用户能收发邮件，和使用 MSN 和 QQ。

分析： 收邮件用到的端口号为 TCP 的 110， 发送邮件为 TCP 的 25， 由于邮件服务器都是以域名的方式，所以还有域名解析（DNS）的 UDP 端口 53， 由于 QQ, MSN 用到的端口号不是固定的， 所以不能用端口来控制， 应选择特殊应用， 要实现本案例的目的， 需要允许该主机能访问端口 110，25，53 和特殊应用 QQ,MSN， 其他的都不能访问。按照上面定义的规则， 所以应该添加规则如下：（本例以 192.168.10.100 这台主机为例）

1 允许主机 192.168.10.100 能访问协议为 TCP 的 110 端口， 该条规则的操作为通过
2 允许主机 192.168.10.100 能访问协议为 TCP 的 25 端口， 该条规则的操作为通过
3 允许主机 192.168.10.100 能访问协议为 UDP 的 53 端口， 该条规则的操作为通过
4 允许主机 192.168.10.100 能访问协议为 TCP/UDP 的特殊应用 QQ 和 MSN， 该条规则的操作为通过
5 禁止主机 192.168.10.100 不能访问协议为 ALL 或者 TCP/UDP，端口号为 1－65535，该条规则的操作为阻挡。

1－4 的规则应先添加，是允许通过的数据， 5 最后添加， 是阻止主机 192.168.10.100 的所有数据通过。

根据上面规则的意义，通过路由器的数据与最先添加的规则比较，当主机 192.168.10.100 在发送邮件时， 路由器将会寻找是否有与该数据匹配的规则，发送邮件是 25 端口， 所以第一条规则不符合， 路由器会继续往下找。

第二条符合， 由这条规则决定数据是通过还是阻挡， 由于设定的操作是通过， 所以这个数据可以通过路由器，就能发送邮件了。

假如这条主机想浏览网页， 即需要允许协议为 TCP， 端口为 80 的数据通过， 当它的数据到达路由器时， 路由器寻找规则并与之比较， 结果发现 1－4 都不匹配， 所以继续往下找。

第 5 条规则匹配， 并且该规则的操作是阻挡， 所以该主机不能浏览网页。

上面这个案例是没有时间控制的， 若你需要按时间段来控制， 只需要把时间范围按你的需要设置即可以了。

【举例】
某企业需要禁止局域网内192.168.16.2~192.168.16.254所有的计算机，在上班时间不能上网（上班时间为9：00～17：00，周一～周五），其他时间允许。
设置如下：

设置所选项后，单击**〈确定〉**，设置完成。

【举例】

网络管理员希望仅允许 IP 地址为192.168.10.2～192.168.10.50 的计算机使用 Web 业务（端口为80），其它计算机都不允许上网。

注：计算机所有的IP 地址为192.168.10.2～192.168.10.254

设置如下：

(1) 添加一条访问控制归档，允许 IP 地址为192.168.10.2～192.168.10.50 的计算机访问因特网：

(2) 按**〈填加到列表〉**，增加这条规则。

(3) 禁止其他计算机上网

(4) 按**〈填加到列表〉**，增加这条规则。

(5) 单击**〈确定〉**按钮，设置完成。

此时，只有 IP 地址为192.168.10.2～192.168.10.50 的计算机能使用 Web 业务，其它的计算机都不能上网。

5.8.3 端口阻挡

在**〈端口阻挡〉**中，通过对端口范围的控制，您可以阻挡某些端口通过路由器，有效的阻挡某些病毒通过某个端口不停发起连接并占有大量 SESSION。注，该处的端口包括源端口和目的端口，所以不管数据包的源端口或者目的端口在该范围内， 该数据包都将被路由器丢弃。

5.8.4 防止 DOS 攻击

选中后，单击**〈确认〉**按钮，设置完成。

防止 DOS 攻击		
项目	说明	默认
禁用/启用	选用该项，将禁止或启动无线路由器的防止 DOS 攻击功能。	启用
防止 SYN flood 攻击	启用该项，无线路由器可以防止 Syn Flood 攻击。可以根据服务器正常情况下的访问量来设定最大 Syn 包速率值，一般保持临界值 150 包/秒即可。	启用
防止 UDP flood 攻击	启用该项，无线路由器其可以防止 UDP Flood 攻击。可以根据服务器正常情况下的访问量来设定最大 UDP 包速率值，一般保持临界值 150 包/秒即可。	启用
防止 ICMP flood 攻击	启用该项，无线路由器可以防止 ICMP Flood 攻击。可以根据服务器正常情况下的访问量来设定最大 ICMP 包速率值，一般保持临界值 150 包/秒即可。	启用
阻挡 IP 选项	启用该项，无线路由器可以防止 IP 选项攻击。	启用
防止 Land 攻击	启用该项，无线路由器可以防止 Land 攻击。	启用
防止 Tear Drop 攻击	启用该项，无线路由器可以防止 Tear Drop 攻击。	启用
防止 Smuef 攻击	启用该项，无线路由器可以防止 Smuef 攻击。	启用
防止 Ping of Death 攻击	启用该项，无线路由器可以防止 Ping of Death 攻击。	启用
阻挡 ICMP 碎片	启用该项，无线路由器可以阻挡 ICMP 碎片攻击。	启用
阻挡未知协议	启用该项，无线路由器可以阻挡未知协议的攻击。	启用
阻挡 Fraggle Attack	启用该项，无线路由器可以阻挡 Fraggle Attack 的攻击。	启用
阻挡源 IP 欺骗攻击	启用该项，无线路由器可以阻挡 IP 欺骗攻击。	启用
防止 ARP 欺骗	启用该项，无线路由器 则启动防 ARP 欺骗功能，间隔选用的时间越短，防 ARP 欺骗病毒的效果越好，但是对系统的影响也相对比较大，请根据需要选择。	启用

5.9 系统服务

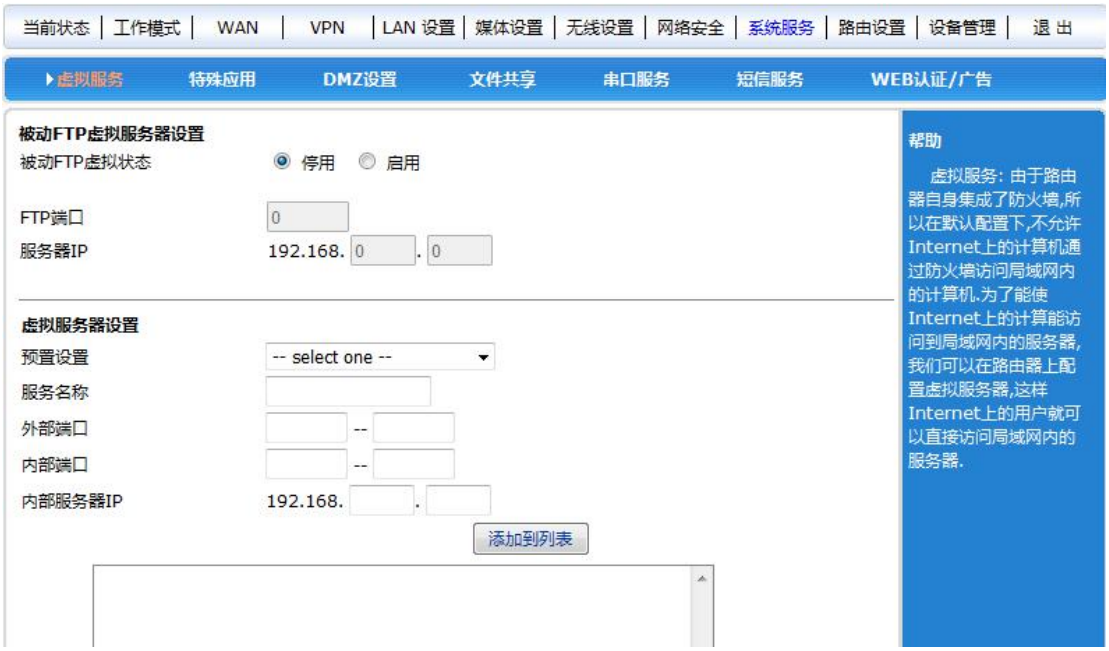
在系统服务中，您可以设置：

- 虚拟服务器，设置内部服务器提供给因特网用户访问。
- DMZ（Demilitarized zone，非管制区），DMZ 的主机，实际就是缺省的虚拟服务器，当需要设置的虚拟服务器的开放端口不确定时，可以把它设置成 DMZ 主机。
- 端口触发，可以实现无线路由器根据局域网访问因特网的端口来自动开放向内的服务端口。

5.9.1 虚拟服务器

虚拟服务器也可称为端口映射。您可以通过设置虚拟服务器，实现让因特网用户访问局域网内部服务器提供的服务，比如 Web 服务、Email 以及 FTP 等。缺省情况下，为保证局域网的安全，无线路由器会阻断从因特网主动发起的连接请求，因此，如果要使因特网用户能够访问局域网内的服务器，需要设置虚拟服务器。

虚拟服务器可以将 WAN 口 IP 地址、外部端口号和局域网内服务器 IP 地址、内部端口号建立映射关系，所有对该 WAN 口某服务端口的访问将会被重定向到指定的局域网内服务器的相应内部端口。



虚拟服务器		
项目	说明	默认
FTP 端口	被动 FTP 虚拟服务器的端口	空
服务器 IP	被动 FTP 虚拟服务器的 IP 地址	空
预设设置	系统提供常用的服务选项，如 FTP、Web 等服务。在下拉列表框中选择一项服务，服务名称、外部端口、内部端口	空

	项都将自动完成设置。 说明： • 如果无线路由器提供的预设服务没有您需要的，您可以自行设置下面的服务信息。 • 预设服务的端口号是常用端口号，如果需要，您可以自行修改。	
服务名称	该条虚拟服务器设置项的名称。	空
外部端口	客户端访问虚拟服务器所使用的端口。取值范围：1～65535，端口范围必须从小到大。如果只有一个端口，则两处填写同一端口号。 说明：各设置项的外部端口不能重复，且内部端口和外部端口的设定个数必须一样，即内部端口和外部端口一一对应。例如，设置一条虚拟服务器，外部端口为100-102，内部端口为10-12，如果无线路由器收到外部101 端口的访问请求，则无线路由器 把数据报文转发到内部服务器的11 端口。	空
内部端口	虚拟服务器上真实开放的服务端口。取值范围：1～65535，端口范围必须从小到大。如果只有一个端口，则两处填写同一端口号。 说明：各设置项的内部端口允许重复，且内部端口和外部端口的设定个数必须一样，即内部端口和外部端口一一对应。	空
内部服务器 IP	虚拟服务器的 IP 地址	空

【举例】
某公司的内部局域网，通过无线路由器连接因特网，局域网内有一台 Web 服务器（IP 地址为 192.168.10.100，服务端口为 80），客户端（因特网上用户或本公司局域网用户）需要通过 8080 端口访问这台服务器的 Web 服务。
设置如下：

设置完成后，只需在客户端浏览器中输入 http://xxx.xxx.xxx.xxx:8080，就可以访问 Web 服务器（xxx.xxx.xxx.xxx 为无线路由器当前的 WAN 口地址）了。

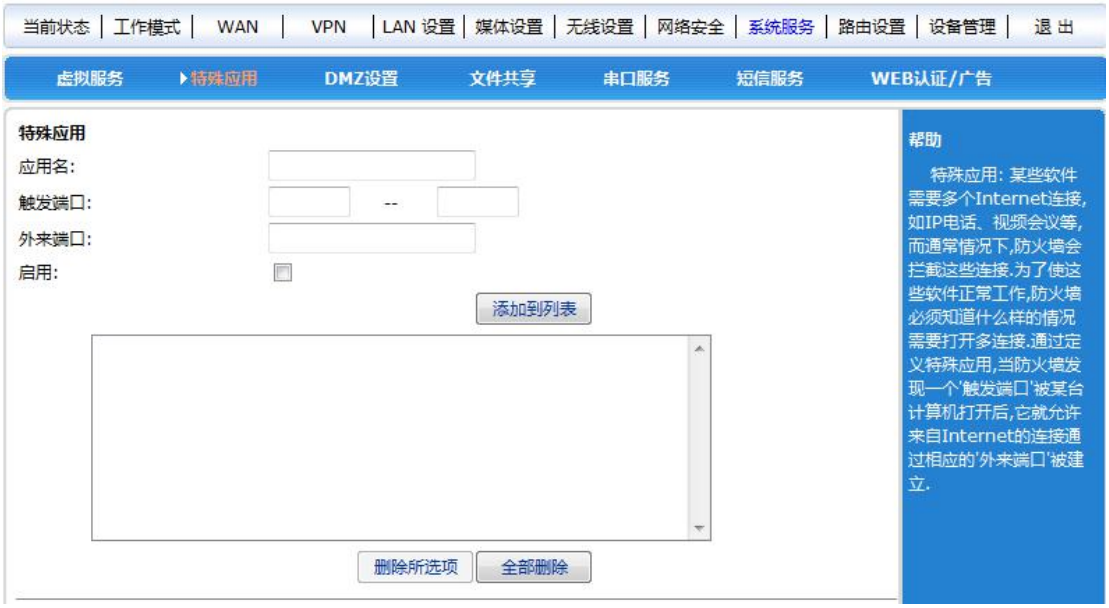
5.9.2 特殊应用

局域网客户端访问因特网上服务器，对于某些应用，客户端向服务器主动发起连接的同时，也需要服务器向客户端主动发起连接请求，而默认情况下无线路由器收到 WAN 侧主动

连接的请求都会拒绝，这样就会中断通信。通过定义端口触发规则，当客户端访问服务器触发此规则后，无线路由器自动开放服务器需要向客户端请求的端口，这样可以保证通信正常。客户端和无线路由器没有数据交互一段时间后，无线路由器自动关闭之前对外开放的端口，既保证应用的正常使用，又能最大限度地保证局域网的安全。

说明：

- 端口触发最多支持 50 条设置项。
- 各设置项中，触发端口、外来端口允许有重叠。
- 当局域网内计算机通过触发端口与外部网络建立连接，其相应的外来端口也将被打开，这时外部网络的计算机可以通过这些端口来访问局域网。
- 每个定义的端口触发只能同时被一台计算机所使用。如果有多台机器同时打开同一个“触发端口”，那么“外来端口”的连接只会被重定向到最后一次打开“触发端口”的那台计算机。



特殊应用		
项目	说明	默认
应用名	该条端口触发设置项的名称。	空
触发端口	局域网客户端向服务器发起请求的端口。取值范围：1～65535，端口范围必须从小到大。如果只有一个端口，则两处填写同一端口号。	空
外来端口	服务器需要主动向局域网内客户端请求的端口。取值范围：1～65535，可设置单一端口、端口范围或两者的组合，端口间用英文逗号“,”隔开。例如：100,200-300,400。	空

5.9.3 DMZ 设置

DMZ 主机实际上就是一个缺省的虚拟服务器，优先级低于虚拟服务器。如果无线路由器收到一个来自外部网络的连接请求时，它将首先根据外部请求的服务端口号，查找虚拟服务

列表，检查是否有匹配的映射表项：

- 如果有匹配的表项，就把请求消息发送到该表项对应的虚拟服务器上去；
- 如果没有查到匹配的表项，检查是否有匹配的 DMZ 主机，如果 DMZ 主机存在，就把请求消息全都转发到 DMZ 主机上去，否则丢弃。

说明：

- 启用 DMZ 功能之后，DMZ 主机就等于暴露在了因特网中，安全性降低。
- 访问 DMZ 主机的端口号应与 DMZ 实际开启的服务端口号一样。

DMZ 设置		
项目	说明	默认
丢弃	选中该项，当外来报文没有匹配到任何虚拟服务器表项时，路由器将丢弃该报文。	勾选
重定向 DMZ 主机	选中该项，当外来报文没有匹配到任何虚拟服务器表项时，路由器会把报文全都转发到 DMZ 主机上。选中该项后，还需要设置“DMZ 主机 IP 地址”。如果设置的 DMZ 主机 IP 地址不存在，则路由器丢弃该报文。	未选
DMZ 主机地址	设置 DMZ 主机的 IP 地址。 说明：局域网内只能设置一个DMZ 主机	空

5.9.4 串口服务

路由器硬件上 UART2 接口 即为串口通讯服务的物理接口。

串口服务		
项目	说明	默认
COM 服务模式	选择透传模式或指令模式。 也可以命令切换：在透传模式下 ，输入+++进入指令模式。在指令模式下，输入ato进入透传模式	透传模式
心跳	可以设置nvram中变量作为心跳发送的内存	空
心跳时间	设置心跳时间，0为不启用。	空
客户端模式	客户端模式下，路由器串口服务做客户端，LAN连接的设备做串口服务器。	ON
服务器模式	客户端模式下，路由器串口服务做串口服务器，LAN连接的设备做客户端	OFF

5.9.5 Web 认证/广告

Web 认证/广告		
项目	说明	默认
工作模式	简单模式：本地的认证服务器 远程模式：远程wifidog服务器	--
网关 ID	本机的MAC地址	--
本地信任	选择后,本地有线网络不需要认证	--
无需认证的 MAC 列表	设置本地不需要认证的无线MAC	--
信任的 IP 列表	设置在访问某域名或IP地址的时候不需要认证	--
服务器主机 SSL	需要服务器支持SSL，默认不能勾选,否则无法开启认证	

5.10 路由设置

在路由设置中，您可以设置静态路由。

5.10.1 当前路由表

5.10.2 静态路由

静态路由通过手工设定目的地址、子网掩码、下一跳地址和出接口等来使到指定目的地址的报文走指定的路径。静态路由不会根据网络结构的变化而变化，当到目的网络路径变化或网络故障时，只能通过手工修改对应的静态路由表重新指定报文到目的网络的路径。

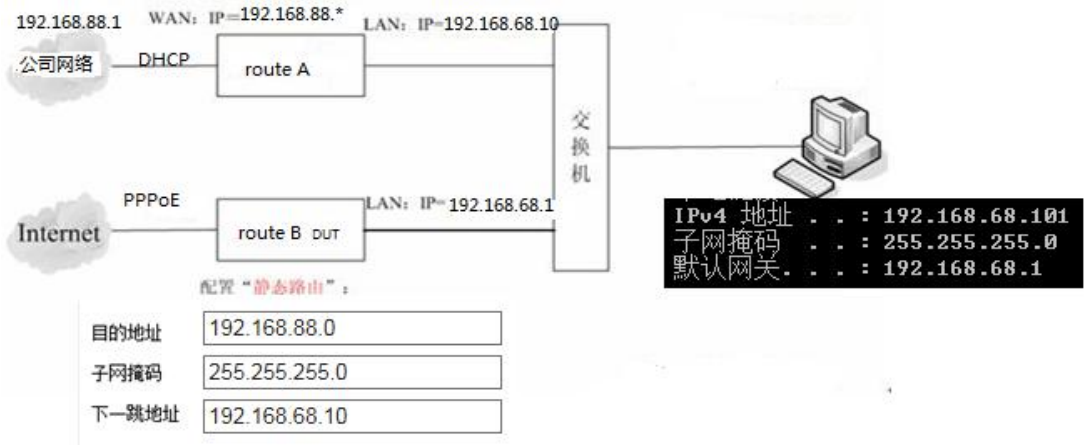
静态路由添加完毕后，单击<当前路由表>按钮查看所添加的静态路由是否生效。如果添加了错误的路由，则只在下图中的路由表中显示，却并不生效，路由信息表中没有该路由。

静态路由		
项目	说明	默认
选择	路由器共有 20 条静态路由可选择，点击下拉框选择	1
注释	可以对所设的静态路由进行注释说明	空
目的地址	需要到达的目的IP 地址。	0.0.0.0
子网掩码	需要到达的目的地址子网掩码。	0.0.0.0
下一跳地址	数据在到达目的地址前，需要经过的下一个路由器的IP地址	0.0.0.0

说明：设置完成后，单击<当前路由表>按钮查看所添加的静态路由是否生效。如果添加了错误的路由，则只在下图中的路由表中显示，却并不生效，路由信息表中没有该路由。

【举例】

在一个公司网络中，不仅可以通过无线路由器 B 连接外网，还可以通过无线路由器 A 来连接公司内网服务器。在不修改本地连接的 IP 地址及网关情况下，公司电脑需要能够同时访问外网和内网服务器。配置实例如下图：



PC 默认将数据发送给网关 192.168.68.1，即 router B。router B 接收到数据后，检查数据包的目的地址。如果发现目的地址 IP 为 192.168.88.0 的数据包，则路由器添加一个静态路由表，把 PC 后续发往 192.168.88.0 网段的数据包，都发送给 router A 网关即可。这样 PC 就可以直接访问公司内网服务器了。

5.11 设备管理

本章将介绍如何通过 Web 页面对无线路由器进行操作。您可以进行如下操作：

- 区域设置，用于设置当地所在时区，获取真实的网络时间。
- NTP 服务器设置，用于设置指定的 NTP 服务器的地址，为路由器、交换机和工作站之间提供时间同步。
- 备份系统设置信息，用于备份系统设置信息，防止信息意外丢失。
- 从文件中恢复设置信息，用于将当前设置恢复到以前备份过的设置。
- 恢复到出厂设置，用于将无线路由器恢复到出厂的初始状态。
- 软件升级，用于通过 Web 页面升级无线路由器的软件。
- 远程管理，用于允许/禁止用户通过 WAN 口远程登录无线路由器的设置页面对无线路由器进行管理。
- 重启动，用于通过 Web 页面重新启动无线路由器。
- 修改密码，用于防止非授权人员随意登录 Web 设置页面。

5.11.1 设备管理

5.11.1.1 设备功能

UPnP 协议是由Windows ME, 2000,XP 等系统使用。如果启用此功能，将使这些操作系统通过该协议自动找到路由器.

UPnP（Universal Plug and Play，通用即插即用）主要用于实现设备的智能互联互通，无需用户参与和使用主服务器，能自动发现和控制来自各家厂商的各种网络设备。

启用 UPnP 功能，路由器可以实现 NAT 穿越：当局域网内的计算机通过无线路由器与因特网通信时，无线路由器可以根据需要自动增加、删除 NAT 映射表，从而解决一些传统业务（比如 MSN 语音，视频）不能穿越 NAT 的问题。

单选框打勾，按〈**确定**〉按钮，设置完成。

5.11.1.2 远程管理

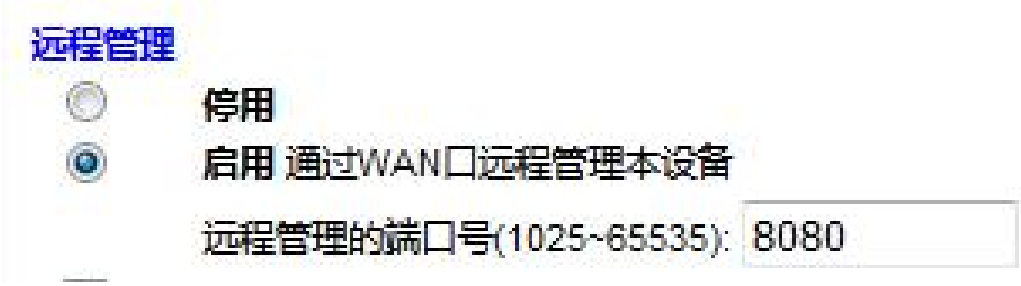
您可以采用远程管理的方式设置与管理无线路由器。

远程管理@设备管理		
项目	说明	默认
停用	选中该项表示禁止对无线路由器进行远程管理	勾选
启用通过WAN口远程管理本设备	选中该项表明可以对无线路由器进行远程管理。输入远程管理端口号，外部用户通过此端口登录无线路由器的设置页面对路由器进行管理。缺省为8080。	未选
启用telnet远程管理	选中该项表示可以对无线路由器通过 telnet 进行远程管理	未选
启用SSHD	选中该项表示可以对无线路由器通过 SSHD 进行远程管理	勾选

【举例】

允许因特网上的一台计算机通过8080 端口管理无线路由器。

设置如下图：

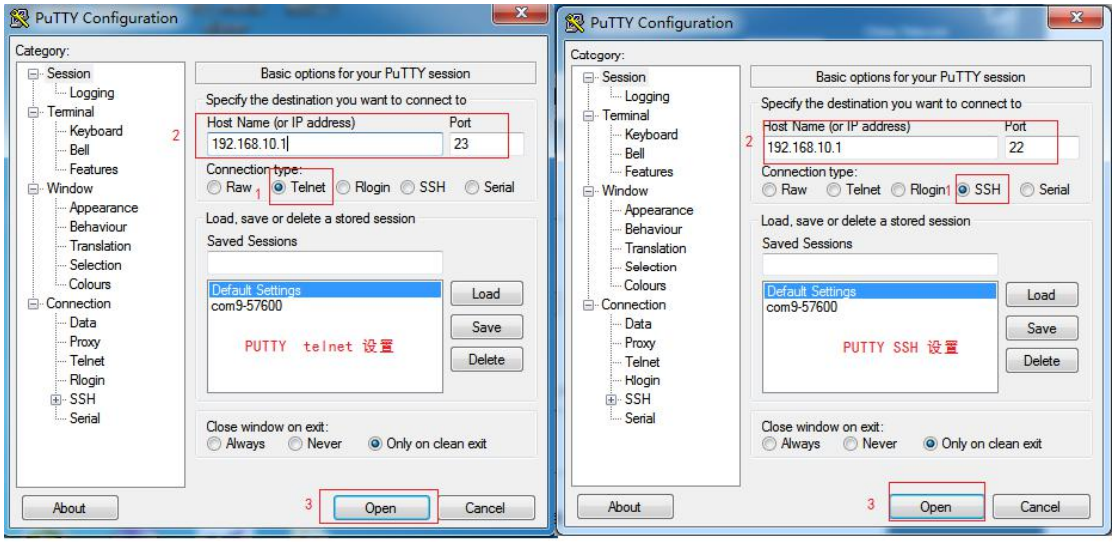


以后只要在这台计算机的浏览器地址栏输入“http://XX.XX.XX.XX:8080”即可登录无线路由器，（其中“XX.XX.XX.XX”为无线路由器的WAN口IP地址）进行配置管理。

SSH默认开启， telnet管理默认关闭,需要手动打开。

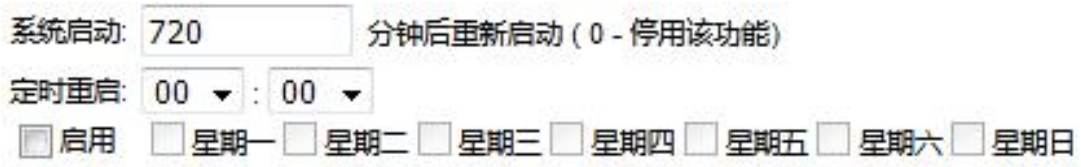
使用方法:

以PUTTY为例， 如下图， 可以选择使用ssh或telnet其中一个:



5.11.1.3 系统重启

系统重启分为计时重启(系统启动x分钟后重启)和定时重启(系统在某天的某个时间点重启)



5.11.2 时区管理

远程管理@设备管理		
项目	说明	默认
时区	选择自己所在的时区，无线路由器将自动从网络中获取时间	Beijing
使用本设备的缺省NTP服务器	选中该项，无线路由器从缺省的 NTP 服务器更新时间。缺省情况下，使用无线路由器的缺省 NTP 服务器。	勾选
使用下面手工输入的NTP服务器	若您需要设置其他的 NTP 服务器，请选中该项，并在文本框中输入该 NTP 服务器的地址（IP 地址形式或域名形式），无线路由器向指定的 NTP 服务器更新时间。	未选

5.11.3 设置信息

5.11.3.1 备份系统设置信息

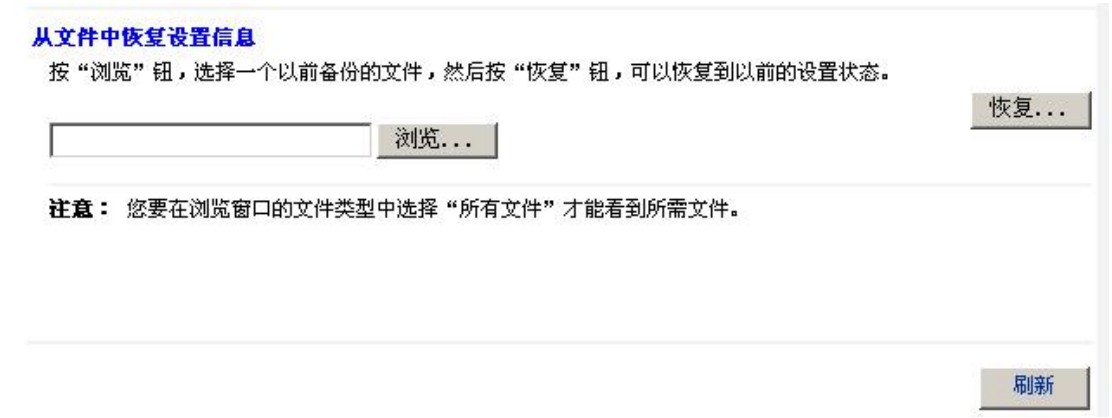
如果您之前备份过系统设置信息，当发生误操作或其他情况导致无线路由器的系统设置信息丢失时，您可将当前设置恢复到之前备份的设置，保证无线路由器的正常运行，并减少信息丢失带来的损失。备份系统设置信息还有助于进行故障分析。

单击<备份>按钮，选择设置信息备份路径后，单击<确定>按钮，将无线路由器当前的设置信息保存到计算机上，方便以后通过该文件（后缀名为.cfg）恢复设置。

5.11.3.2 在文件中恢复设置信息

您可以使用此功能将当前设置恢复到以前备份过的设置。

说明：恢复设置后，当前的设置将会丢失。如果您不希望丢失当前设置信息，请注意进行备份。备份方法请参见“5.11.3.1 **备份系统设置信息**”。



单击**<浏览>**按钮，在计算机上选择一个以前备份的文件（*.cfg），然后单击**<恢复>**按钮，即可将设置恢复到备份文件的状态。

恢复设置过程中，无线路由器将会重新启动。

5.11.4 软件升级

通过软件升级，您可以加载最新版本的软件到路由器，以获得更多的功能和更为稳定的性能。

软件升级步骤如下：
(1) 单击<浏览>按钮，选择需要升级的软件。
(2) 单击<升级>按钮，开始升级。
(3) 如果需要升级后恢复出厂，单击<恢复出厂设置>按钮。

说明：升级恢复出厂设置有两个条件同时满足：
1. 版本号发生变化；
2. 升级时点击<恢复出厂设置>按钮。

5.11.5 重启设备

注：重启动期间，请勿断电。
重启动期间，网络通信将暂时中断。

单击<**重启动**>按钮，无线路由器重新启动。

5.11.6 恢复出厂值

说明：

- 恢复设置后，当前的设置将会丢失。如果您不希望丢失当前设置信息，请注意进行备份。备份方法请参见“5.11.3.1 **备份系统设置信息**”。
- 恢复设置过程中，无线路由器将会重新启动。

恢复到出厂设置将清除无线路由器的所有设置信息，恢复到初始状态。该功能一般用于设备从一个网络环境换到另一个不同的网络环境的情况，将设备恢复到出厂设置，然后再进行重新设置，以更适合当前的组网。

单击<**恢复出厂值**>按钮，确认后，恢复出厂设置。

5.11.7 密码管理

无线路由器缺省的用户名/密码为***admin***，用户名不可修改，密码可修改，最大支持16位。为了安全起见，建议修改此密码，并保管好密码信息。

设置步骤如下：

(1) 在〈**原密码**〉文本框中输入原来的密码；在〈**新密码**〉文本框中输入新的密码，在〈**确认密码**〉文本框中重新输入新密码以确认。

(2) 单击<**确定**>按钮，完成密码修改。

6 保修条款

1）此设备从购买之日算起，为期一年内有任何材料或质量问题，免费维修。
2）此一年保修不包括任何人为损坏、操作不当等造成的产品故障问题。

7 技术支持

深圳市讯记科技有限公司
地址：广东省深圳市宝安区西乡街道固戍社区西井路 21 号塘西智谷 G 栋 4 楼
电话：0755-26055466
免费服务热线：400-863-2699
网址：http://www.comark.cn/