

*Tenda*



**企业级路由器**

**使用说明书**

## 声明

版权所有©2018 深圳市吉祥腾达科技有限公司。保留一切权利。

未经本公司书面许可，任何单位或个人不得擅自复制、摘抄及翻译本文档部分或全部内容，且不得以任何形式传播。

**Tenda** 是深圳市吉祥腾达科技有限公司在中国和（或）其它国家与地区的注册商标。文中提及的其它品牌和产品名称均为其相应持有人的商标或注册商标。

由于产品版本升级或其它原因，本文档内容会不定期更新。除非另有约定，本文档仅作为产品使用指导，文中的所有陈述、信息和建议均不构成任何形式的担保。

本文档对设备的使用步骤和功能设置步骤提供详细描述，对于页面直接提示信息和简单的信息查看不作详述。

# 前言

感谢选择腾达产品。开始使用本产品前，请先阅读本说明书。

## 约定

本说明书适用于以下型号的 Tenda 路由器，具体产品图和软件截图以实物为准。文中如无特别说明，均以 G0-PoE 为例。

型号	描述
G0-PoE	企业级 PoE 路由器
G0	企业级路由器

本文可能用到的格式说明如下。

项目	格式	举例
菜单项	「」	选择「状态」菜单。
按钮	边框+底纹	点击 <span style="border: 1px solid black; padding: 2px;">确定</span> 。
窗口	【】	在【新增】窗口。

本文可能用到的标识说明如下。

标识	含义
 注意	表示重要信息或需要特别关注的信息。若忽略此等信息，可能导致配置失效、数据丢失或设备故障。
 提示	表示有助于节省时间或资源的方法。

## 缩略语

缩略语	全称
AP	接入点 (Access Point)
ARP	地址解析协议 (Address Resolution Protocol)
AES	高级加密标准 (Advanced Encryption Standard)
DHCP	动态主机配置协议 (Dynamic Host Configuration Protocol)
DNS	域名系统 (Domain Name System)
DDNS	动态域名服务 (Dynamic Domain Name Server)
DDoS	分布式拒绝服务 (Distributed Denial of Service)
GMT	格林威治时间 (Greenwich Mean Time)
IP	网际协议 (Internet Protocol)
ICMP	网际控制报文协议 (Internet Control Message Protocol)
ISP	因特网服务提供者 (Internet Service Provider)
TKIP	临时密钥完整性协议 (Temporal Key Integrity Protocol)
LAN	局域网 (Local Area Network)
MAC	媒体接入控制 (Medium Access Control)
NAT	网络地址转换 (Network Address Translation)
PoE	以太网供电 (Power Over Ethernet)
PVID	端口的虚拟局域网 ID 号 (Port-based Vlan ID)
SSID	服务集标识符 (Service Set Identifier)
TCP	传输控制协议 (Transmission Control Protocol)
UDP	用户数据报协议 (User Datagram Protocol)
URL	统一资源定位符 (Uniform Resource Locator)

缩略语	全称
UPnP	通用即插即用 (Universal Plug and Play)
VLAN	虚拟局域网 (Virtual Local Area Network)
WAN	广域网 (Wide Area Network)
WLAN	无线局域网 (Wireless Local Area Networks)
WEP	有线等效保密字段 (Wired Equivalent Privacy)
WPA-PSK	WPA 预共享密钥 (WPA-Preshared Key)
WMM	无线多媒体 (Wi-Fi multi-media)

## 相关资料获取方式

访问 Tenda 官方网站 <http://www.tenda.com.cn>，在右上角搜索栏搜索对应产品型号，可获取最新的产品资料。

## 技术支持

如需了解更多信息，请通过以下方式与我们联系。

腾达官网：<http://www.tenda.com.cn>



热线：400-6622-666



邮箱：tenda@tenda.com.cn



腾达微信公众号



腾达官方微博

# 目录

1	产品介绍.....	1
1.1	简介.....	1
1.2	外观.....	1
1.2.1	指示灯.....	1
1.2.2	按钮&接口.....	2
1.2.3	贴纸.....	2
2	快速上网.....	3
3	设备登录.....	6
3.1	登录路由器的管理页面.....	6
3.2	退出登录.....	8
3.3	页面布局.....	9
3.4	常用按钮.....	10
4	系统状态.....	11
4.1	查看连线状态及系统状态.....	11
4.2	查看流量统计.....	15
4.3	管理在线用户.....	16
4.4	添加/移出黑名单.....	17
4.5	管理在线 AP.....	18
5	联网设置.....	20
5.1	概述.....	20
5.2	设置联网.....	22
5.2.1	宽带拨号.....	22
5.2.2	动态 IP.....	24
5.2.3	静态 IP.....	25

6	网速控制.....	27
6.1	概述.....	27
6.2	自定义限速.....	29
6.3	全部限速.....	30
6.4	自动分配网速.....	31
6.5	分组限速.....	32
6.6	分组限速配置举例.....	34
7	认证管理.....	37
7.1	PPPoE 认证.....	37
7.1.1	概述.....	37
7.1.2	配置 PPPoE 认证.....	39
7.2	认证用户管理.....	41
7.2.1	概述.....	41
7.2.2	新增认证账号.....	43
7.3	PPPoE 认证配置举例.....	45
8	AP 管理.....	51
8.1	基本设置.....	52
8.1.1	概述.....	52
8.1.2	下发无线策略到 AP.....	54
8.2	AP 维护.....	55
8.2.1	概述.....	55
8.2.2	升级.....	55
8.2.3	恢复出厂设置.....	56
8.2.4	重启.....	56
8.2.5	删除.....	57
8.2.6	刷新.....	58
8.2.7	导出.....	58
8.2.8	修改.....	58

8.3	高级设置	60
8.3.1	概述	60
8.3.2	下发 2.4GHz/5GHz 网络配置到 AP	65
8.3.3	下发 VLAN 等其他配置到 AP	66
9	行为管理	68
9.1	IP 组与时间组	68
9.1.1	概述	68
9.1.2	新增时间组	69
9.1.3	新增 IP 组	70
9.2	MAC 地址过滤	72
9.2.1	概述	72
9.2.2	新增 MAC 地址过滤规则	73
9.2.3	MAC 地址过滤配置举例	74
9.3	IP 地址过滤	78
9.3.1	概述	78
9.3.2	新增 IP 地址过滤规则	79
9.3.3	IP 地址过滤配置举例	80
9.4	端口过滤	84
9.4.1	概述	84
9.4.2	新增端口过滤规则	85
9.4.3	端口过滤配置举例	86
9.5	应用过滤	90
9.5.1	概述	90
9.5.2	新增应用过滤规则	91
9.5.3	新增例外 QQ 号	93
9.5.4	应用过滤+QQ 过滤配置举例	94
9.6	网站过滤	98
9.6.1	概述	98

9.6.2	新增网站过滤规则.....	99
9.6.3	自定义网址组.....	100
9.6.4	网站过滤配置举例.....	102
9.7	多 WAN 策略.....	107
9.7.1	概述.....	107
9.7.2	自定义多 WAN 策略.....	108
9.7.3	自定义多 WAN 策略配置举例 .....	109
10	VPN .....	113
10.1	概述 .....	113
10.2	配置 PPTP/L2TP 客户端.....	115
10.3	PPTP/L2TP 客户端配置举例 .....	116
11	更多设置.....	120
11.1	局域网设置.....	120
11.1.1	LAN 口设置.....	120
11.1.2	DHCP 服务器 .....	121
11.1.3	静态地址分配.....	123
11.2	WAN 口参数 .....	129
11.2.1	WAN 口速率 .....	129
11.2.2	MTU .....	130
11.2.3	MAC 地址 .....	130
11.2.4	快速转发.....	132
11.3	静态路由 .....	133
11.3.1	概述 .....	133
11.3.2	新增静态路由.....	134
11.3.3	静态路由配置举例.....	136
11.4	端口镜像 .....	140
11.4.1	概述 .....	140
11.4.2	配置端口镜像.....	140
11.4.3	端口镜像配置举例.....	141

11.5	远程 WEB 管理 .....	143
11.5.1	概述 .....	143
11.5.2	配置远程 WEB 管理 .....	144
11.5.3	远程 WEB 管理配置举例 .....	144
11.6	DDNS .....	147
11.6.1	概述 .....	147
11.6.2	配置 DDNS .....	148
11.6.3	DDNS 配置举例 .....	149
11.7	端口映射 .....	152
11.7.1	概述 .....	152
11.7.2	配置端口映射 .....	153
11.7.3	端口映射配置举例 .....	153
11.8	DMZ 主机 .....	156
11.8.1	概述 .....	156
11.8.2	配置 DMZ 主机 .....	156
11.8.3	DMZ 主机配置举例 .....	157
11.9	UPnP .....	159
11.9.1	概述 .....	159
11.9.2	开启 UPnP .....	159
11.10	DNS 劫持 .....	160
11.10.1	概述 .....	160
11.10.2	配置 DNS 劫持 .....	160
11.11	DNS 缓存 .....	162
11.12	攻击防御 .....	163
12	系统维护 .....	165
12.1	重启 .....	165
12.2	升级 .....	166
12.2.1	概述 .....	166
12.2.2	软件本地升级 .....	167

12.2.3 特征库本地升级 .....	168
12.3 恢复出厂设置 .....	169
12.3.1 概述 .....	169
12.3.2 软件恢复出厂设置 .....	169
12.3.3 硬件恢复出厂设置 .....	170
12.4 登录密码 .....	171
12.4.1 概述 .....	171
12.4.2 修改登录密码 .....	171
12.5 定时重启 .....	172
12.5.1 概述 .....	172
12.5.2 定时重启路由器 .....	172
12.6 备份与恢复 .....	174
12.6.1 概述 .....	174
12.6.2 配置备份 .....	174
12.6.3 配置恢复 .....	174
12.7 系统时间 .....	175
12.7.1 网络校时 .....	175
12.7.2 手动设置 .....	176
12.8 系统日志 .....	177
12.9 诊断工具 .....	178
12.9.1 概述 .....	178
12.9.2 执行 Ping .....	178
12.9.3 执行 Traceroute .....	180
附录 .....	183
A 常见问题解答 .....	183
B 规格参数 .....	184

# 1

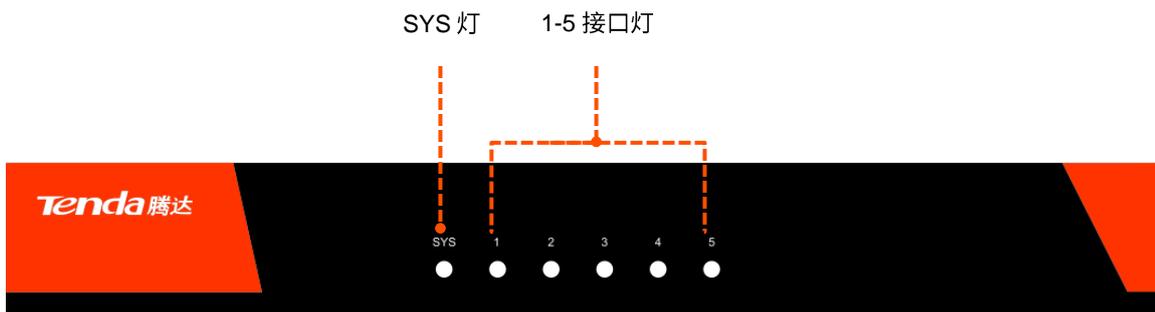
# 产品介绍

## 1.1 简介

Tenda 企业级路由器，它采用企业级系统固件，内置智能带宽管理技术，会基于实际带宽使用情况自动分配带宽，保障多用户上网体验；集成 AP 管理功能，可自动管理与维护网络中所有 Tenda AP。

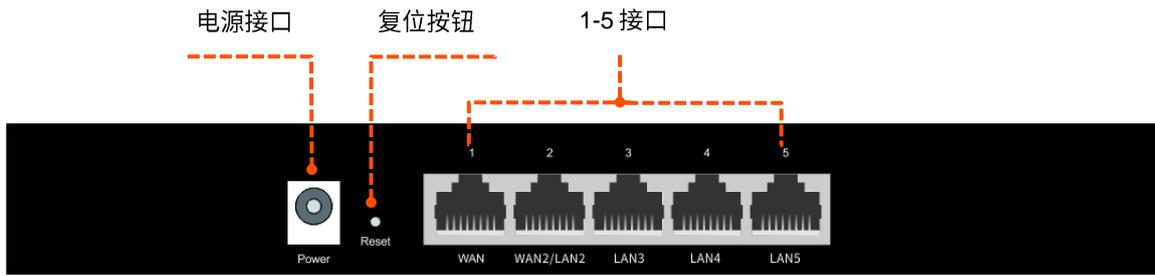
## 1.2 外观

### 1.2.1 指示灯



标题项	状态	说明
SYS	长亮	系统正在启动或者出现故障（使用过程中）。
	闪烁	系统工作正常。
	熄灭	路由器未通电。
1/2/3/4/5	长亮	对应接口没有数据传输。
	闪烁	对应接口正在传输数据。
	熄灭	对应接口没有设备连接或连接异常。

## 1.2.2 按钮&接口



接口/按钮	说明
Power	电源接口。 请使用包装盒内的电源适配器给路由器通电。
Reset	复位按钮。 SYS 灯闪烁状态下，用尖状物按下此按钮 8 秒后松开，路由器将会恢复到出厂状态。
1	外网接口。 连接外网线，外网线可能是从光猫、ADSL 猫、有线电视猫接出来的网线，或互联网服务提供商直接提供的宽带网线。
2	内网接口、外网接口复用，默认为内网接口。 可以登录路由器管理页面修改接口属性。
3/4/5	内网接口。 <ul style="list-style-type: none"><li>- G0: 内网接口。连接电脑、AP、交换机等。</li><li>- G0-PoE: 内网接口，支持 PoE 供电功能。可以给符合 IEEE 802.3af 标准的受电设备供电，如 AP、网络摄像机等。</li></ul>

## 1.2.3 贴纸

贴纸位于路由器的底面。您可以在贴纸上找到路由器的默认登录 IP 地址等信息。

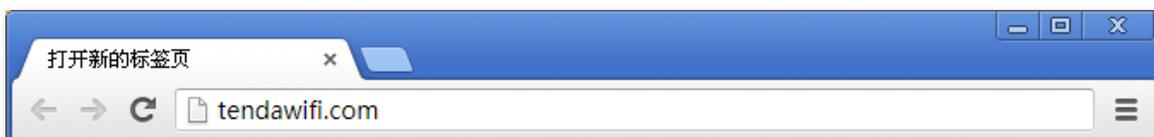


# 2

# 快速上网

首次使用路由器时，可以通过快速设置向导设置上网。具体步骤如下：

- 步骤 1** 用网线将管理电脑接到路由器的任一内网接口；
- 步骤 2** 设置电脑的本地连接为“自动获得 IP 地址，自动获得 DNS 服务器地址”；
- 步骤 3** 打开电脑上的浏览器（如 IE），访问路由器的管理地址（tendawifi.com 或 192.168.0.252），进入路由器的登录页面；



- 步骤 4** 点击 **开始体验** ；



若未出现上述页面，请查看常见问题解答的[问1](#)。

**步骤 5** 系统自动检测联网方式，请根据页面提示设置相关上网信息，点击 **下一步**；(此处以宽带拨号为例)



**Tenda** 联网设置

检测成功，系统推荐联网方式为：宽带拨号

联网方式： 宽带拨号

宽带账号：

宽带密码：

下一步

跳过

**步骤 6** 设置无线名称和无线密码，如“zhangsan”；



此处设置的无线名称和无线密码将会在 AP 连接到路由器后生效。

**步骤 7** 是否将无线密码设置为登录密码，如果不，请取消勾选“将无线密码设置为路由器登录密码”，然后自定义登录密码；

**步骤 8** 点击 **下一步**。



**Tenda** AP无线配置

请设置无线名称和无线密码

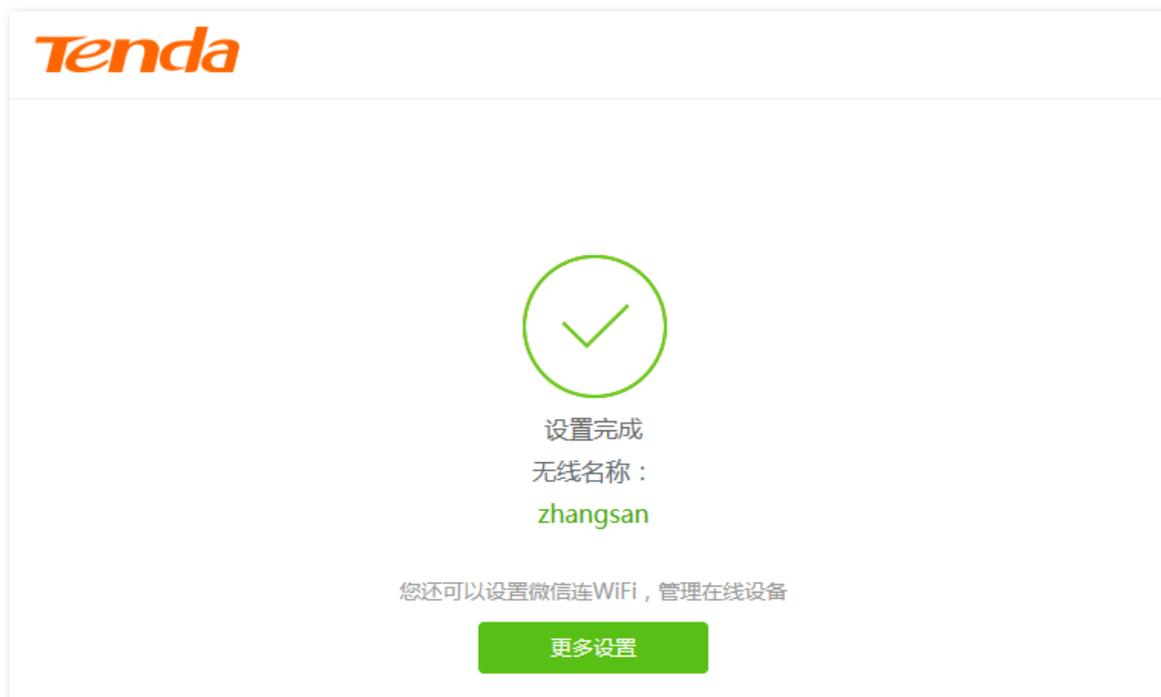
无线名称： zhangsan

无线密码： ●●●●●● 不设密码

将无线密码设置为路由器登录密码

上一步 下一步

稍等片刻，联网成功。此时，连接页面显示的无线网络的无线设备（路由器下接 Tenda AP 有效），以及连接到路由器内网接口的有线设备，都可以上网了。



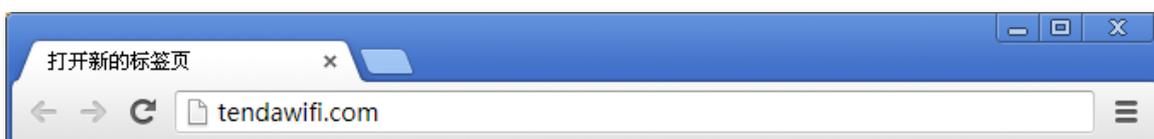
# 3

## 设备登录

### 3.1 登录路由器的管理页面

如果是初次使用本路由器，请参考 [2 快速上网](#)；完成快速设置后，需要登录路由器时，请参考下文。

**步骤 1** 打开电脑上的浏览器（如 IE），访问路由器的管理地址（tendawifi.com 或 192.168.0.252），进入路由器的登录页面；



**步骤 2** 输入登录密码，点击 **登录**。



----完成



若未出现上述页面，请查看常见问题解答的[问1](#)。

成功登录路由器管理页面。

The screenshot displays the Tenda router's management interface. At the top left is the Tenda logo, and at the top right is a '退出登录' (Logout) link. A left sidebar contains navigation options: '系统状态' (System Status), '联网设置' (Network Settings), '网速控制' (Speed Control), '认证管理' (Authentication Management), 'AP管理' (AP Management), '行为管理' (Behavior Management), 'VPN', '更多设置' (More Settings), and '系统维护' (System Maintenance). The main content area is titled '系统状态' (System Status) and shows a '网络状态' (Network Status) diagram. The diagram illustrates the connection between '互联网' (Internet) and the '路由器' (Router), with WAN1 showing 0.00KB/s upload and download speeds. To the right, it indicates '终端: 1台' (1 Terminal) and 'AP: 1台' (1 AP). Below the diagram, there is a section for '网速最高的5台设备' (Top 5 devices by speed) with a link to '更多统计' (More statistics). A table lists the top device with columns for '主机名称' (Host Name), '上传速率' (Upload Rate), '下载速率' (Download Rate), '最大上传速率' (Max Upload Rate), '最大下载速率' (Max Download Rate), and '禁止上网' (Block Internet). The device listed is '未知' (Unknown) with IP '192.168.0.23/C8:3A:35:12:12:14', showing 0 KB/s for both upload and download rates. Action buttons for '自动分配网速' (Auto Assign Speed) and '禁止上网' (Block Internet) are provided for this device.

系统状态 运行时间：0小时19分

网络状态

互联网 WAN1 ↑0.00KB/s ↓0.00KB/s 路由器

终端：1台  
AP：1台

网速最高的5台设备 | [更多统计](#)

主机名称	上传速率	下载速率	最大上传速率	最大下载速率	禁止上网
未知 192.168.0.23/C8:3A:35:12:12:14	0 KB/s	0 KB/s	自动分配网速	自动分配网速	禁止上网

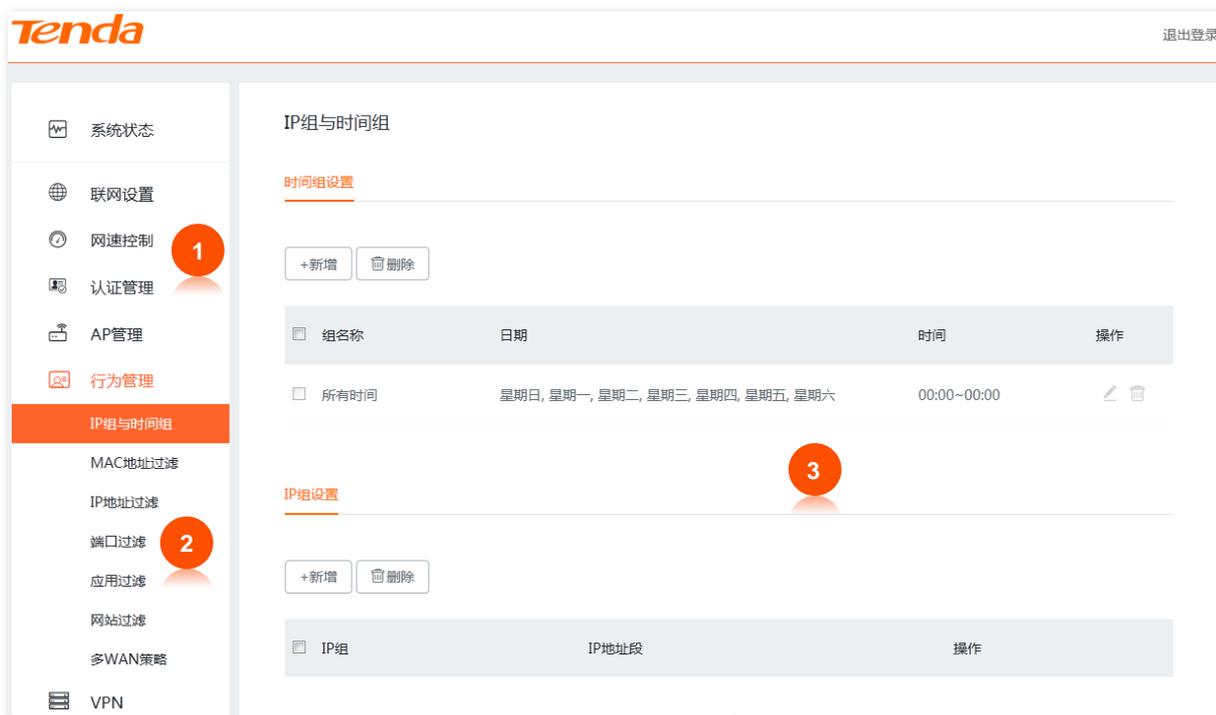
## 3.2 退出登录

您登录到路由器的管理页面后，如果在 20 分钟内没有任何操作，系统将自动退出登录。此外，在管理页面上，单击右上角的“退出登录”，也可以安全地退出管理页面。



## 3.3 页面布局

路由器的管理页面共分为：一级导航栏、二级导航栏和配置区三部分。如下图所示。



序号	名称	说明
1	一级导航栏	以导航树的形式组织路由器的功能菜单。用户在导航栏中可以方便地选择功能菜单，选择结果显示在配置区。
2	二级导航栏	
3	配置区	用户进行配置或查看配置的区域。

## 3.4 常用按钮

路由器管理页面中常用按钮的功能介绍如下表。

常用按钮	说明
	用于保存当前页面配置，并使配置生效。
	用于取消当前页面未保存的配置，并恢复到修改前的配置。

# 4 系统状态

在路由器的「系统状态」模块，您可以：

- 查看连线状态及系统状态。
- 查看 WAN 口的上/下行流量动态图。
- 管理在线用户，添加/移出黑名单。
- 管理在线 AP。

## 4.1 查看连线状态及系统状态

进入页面：点击「系统状态」。

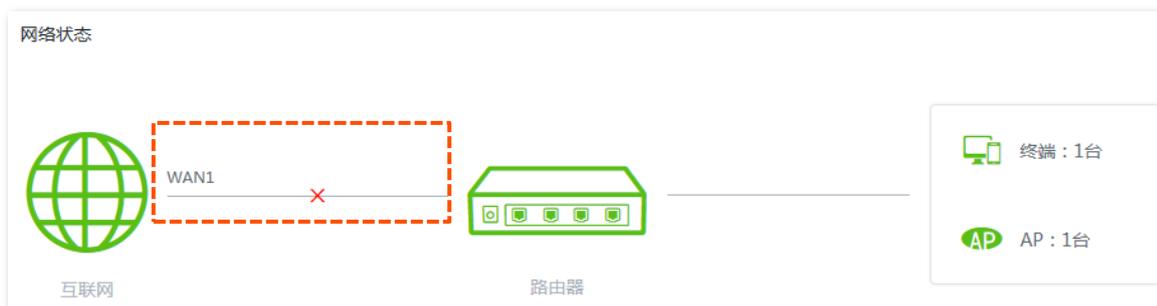
在这里，您可以查看路由器的物理连线是否正常，也可以查看路由器系统状态。

### ■ 查看连线状态

当“互联网”与“路由器”之间的连线正常，则表示对应 WAN 口网线连接正常。如下图示：



当“互联网”与“路由器”之间的连线打叉，则表示对应 WAN 口网线连接异常，请检查并接好该 WAN 口网线。如下图示：



## ■ 查看系统状态

点击“系统状态”页面的路由器图标即可查看系统状态。

在“基本信息”模块，可以查看路由器的系统时间、运行时间、软件版本等信息。

基本信息	系统时间：	2018-04-09 09:39:25
	运行时间：	18小时10分7秒
	软件版本：	V15.11.0.2(2245_4877_1009)
	设备名称：	企业级路由器
	CPU使用率：	27%
	内存使用率：	78%

## 参数说明

标题项	说明
系统时间	路由器当前的系统时间。
运行时间	路由器最近一次启动后连续运行的时长。
软件版本	路由器系统软件的版本号。
设备名称	路由器的名称。
CPU 使用率	路由器当前的 CPU 使用率。
内存使用率	路由器当前的内存使用率。

在“LAN口状态”模块，可以查看路由器的LAN口IP地址和MAC地址。

LAN口状态	IP地址：	192.168.0.252
	MAC地址：	50:2B:73:FE:DA:A0

在“WAN”模块，可以查看路由器当前所有的WAN口信息，包括：联网方式、接口连接状态、IP地址信息以及上传/下载速率等。

WAN1	联网方式：	宽带拨号
	联网状态：	已插网线
	IP地址：	172.20.20.2
	子网掩码：	255.255.255.255
	默认网关：	172.20.20.1
	首选DNS服务器：	192.168.1.60
	备用DNS服务器：	8.8.8.8
	上传速率：	0.00KB/s
	下载速率：	0.00KB/s

### 参数说明

标题项	说明
联网方式	对应WAN口的联网方式。
联网状态	对应WAN口的网线连接状态。
IP地址	对应WAN口的IP地址。
子网掩码	对应WAN口的子网掩码。

标题项	说明
默认网关	对应 WAN 口的网关地址。客户端访问外网时，数据包必须通过网关进行转发。
首选 DNS 服务器	对应 WAN 口的首选/备用 DNS 服务器地址。
备用 DNS 服务器	
上传速率	对应 WAN 口的上传/下载速率。
下载速率	

## 4.2 查看流量统计

进入页面：点击「系统状态」，然后点击“[更多统计](#)”。

在这里，您可以查看路由器 WAN 口的上传和下载流量动态图，也可以了解局域网某个用户基本信息，如上传/下载速率，在线时长等。



### 参数说明

标题项	说明
主机名称	用户设备的名称。
并发连接数	用户的并发连接数。
上传速率	用户当前的上传/下载速率。
下载速率	
下载总流量	用户下载数据的总量。
在线时长	用户的在线时长。

## 4.3 管理在线用户

进入页面：点击「系统状态」。

可以在系统状态页面直接管理局域网内网速最高的 5 台客户端，也可以点击“终端”进行全局管理。



网络状态

互联网 WAN1 ↑0.00KB/s ↓0.00KB/s

路由器

终端：2台

AP：1台

网速最高的5台设备 | [更多统计](#)

主机名称	上传速率	下载速率	最大上传速率	最大下载速率	禁止上网
未知 192.168.0.23/C8:3A:35:12:12:14	0 KB/s	0 KB/s	自动分配网速	自动分配网速	禁止上网
HUAWEI_P10 192.168.0.182/14:5F:94:BC:FC:83	0 KB/s	0 KB/s	自动分配网速	自动分配网速	禁止上网

点击“终端”后，可以对局域网的终端进行管理，包括修改主机名称、设置最大上传/下载速率、禁止用户上网等。



设备管理

在线设备 黑名单

全部限速 刷新 主机名称/IP/MAC 搜索

主机名称	上传速率	下载速率	最大上传速率	最大下载速率	禁止上网
HUAWEI_P10 192.168.0.182/14:5F:94:BC:FC:83	0 KB/s	0 KB/s	自动分配网速	自动分配网速	禁止上网
未知 192.168.0.23/C8:3A:35:12:12:14	0 KB/s	0 KB/s	自动分配网速	自动分配网速	禁止上网

## 4.4 添加/移出黑名单

进入页面：点击「系统状态」。

在这里，您可以添加/移出黑名单。

### ■ 添加黑名单

可以在系统状态页面添加黑名单，也可以点击终端，进入“设备管理”页面进行添加。

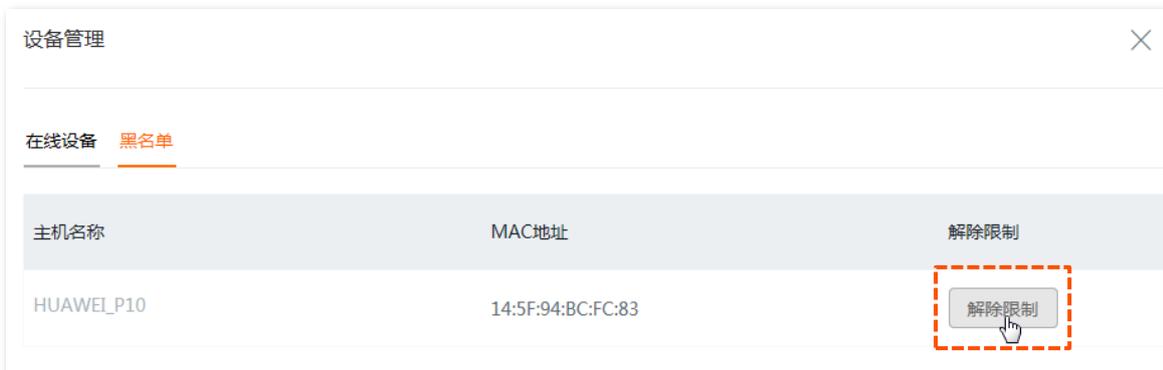
如果“在线设备”列表中出现陌生的设备，可以点击 **禁止上网**，将其加入黑名单。加入黑名单的设备，不可以连接路由器上网。



### ■ 移出黑名单

添加黑名单后，如果需要将该设备移出黑名单，可在“黑名单”页面设置，步骤如下：

1. 在“系统状态”页面点击终端进入“设备管理”弹窗；
2. 点击黑名单，进入“黑名单”列表；
3. 找到对应设备，点击 **解除限制**。



## 4.5 管理在线 AP

进入页面：点击「系统状态」。

在「系统状态」页面点击 **AP**，可以管理网络中的在线 AP。

AP管理 ×

在线AP数：1台 跳转到AP管理

AP型号	备注	无线名称	在线设备	IP/MAC地址	设置
i21V1.0	i21V1.0	2.4G: zhangsan 5G: zhangsan	0台 1台	192.168.0.153 50:2B:73:09:94:50	

- **跳转到 AP 管理**：点击可转到路由器的“AP 管理”页面，对 AP 进行管理，详情请参考 [AP 管理](#)。

**基本设置**

AP管理：

无线网络	启用状态	无线名称	频段	加密方式	无线密码	更多设置
1	<input checked="" type="checkbox"/>	zhangsan	2.4G&5G	WPA2-PSK	zhangsan	⋮
2	<input type="checkbox"/>	Tenda_AP_1	2.4G&5G	不加密		⋮
3	<input type="checkbox"/>	Tenda_AP_2	2.4G&5G	不加密		⋮
4	<input type="checkbox"/>	Tenda_AP_3	2.4G&5G	不加密		⋮
5	<input type="checkbox"/>	Tenda_AP_4	2.4G	不加密		⋮
6	<input type="checkbox"/>	Tenda_AP_5	2.4G	不加密		⋮
7	<input type="checkbox"/>	Tenda_AP_6	2.4G	不加密		⋮
8	<input type="checkbox"/>	Tenda_AP_7	2.4G	不加密		⋮

- : 点击可跳转到 AP 的管理页面。例如 AP 的型号为 i21, 点击 , 即可跳转到 i21 的管理页面, 如下:



# 5 联网设置

## 5.1 概述

通过联网设置，可以实现局域网内的多台设备共享您办理的宽带服务上网。点击「联网设置」进入页面。

### 联网设置

#### WAN口个数

WAN口个数：

				
WAN	WAN/LAN	LAN	LAN	LAN

接口类型：WAN1 LAN2 LAN3 LAN4 LAN5

#### WAN1口

联网方式：

宽带账号：

宽带密码：

联网状态：认证成功

## 参数说明

标题项	说明
WAN 口个数	<p>路由器 WAN 口的个数，默认的 WAN 口个数为 1。可以根据需要修改 WAN 口个数为 2 个。</p> <p>：表示接口连接正常。：表示接口未连接设备或连接异常。</p>
接口类型	路由器接口的类型。
联网方式	<p>路由器的联网方式，支持宽带拨号、动态 IP、静态 IP。</p> <ul style="list-style-type: none"><li>- 宽带拨号：ISP（互联网服务提供商）提供了宽带账号和密码。用户不使用路由器时，需要在电脑上拨号上网。</li><li>- 动态 IP：ISP 没有提供任何上网信息。用户不使用路由器时，电脑只需要接上宽带网线即可上网。</li><li>- 静态 IP：ISP 提供了固定的 IP 地址信息。用户不使用路由器时，需要在电脑上设置静态 IP 地址上网。</li></ul>
宽带账号	联网方式为“宽带拨号”时才需设置。可以在办理宽带的业务单据上查到，如果没有，请咨询您的 ISP。
宽带密码	
IP 地址	
子网掩码	联网方式为“静态 IP”时才需设置。可以在办理宽带的业务单据上查到，如果没有，请咨询您的 ISP。
默认网关	 <b>提示</b>
首选 DNS 服务器	如果 ISP 没有提供两个 DNS 地址，“备用 DNS 服务器”可以不填。
备用 DNS 服务器	
联网状态	<p>显示路由器 WAN 口的连接状态。</p> <ul style="list-style-type: none"><li>- 已连接：路由器 WAN 口已插网线，并已经获得 IP 地址信息。</li><li>- 认证成功：路由器拨号成功，并已经获得 IP 地址信息。</li><li>- 连接中...：路由器正在连接到上级网络设备。</li><li>- 未连接：未连接或连接失败，请检查网线连接状态、联网信息设置或咨询相应的 ISP。</li></ul> <p>如果显示其他状态信息，请根据联网状态提示信息采取相应措施。</p>

## 5.2 设置联网

首次使用路由器时，需要在设置向导完成联网设置。之后，如果需要修改联网参数，可在“联网设置”模块设置，点击「联网设置」进入设置页面。

可以先根据下表说明或咨询您的 ISP，确定路由器的联网方式，再进行联网设置。

联网方式	特征
<a href="#">宽带拨号</a>	ISP 提供了宽带账号和宽带密码。
<a href="#">动态 IP</a>	ISP 未提供任何上网信息，或说明了联网方式为“动态 IP”。
<a href="#">静态 IP</a>	ISP 提供了一组固定 IP 地址信息，如 IP 地址，子网掩码、默认网关、DNS 等。



- 路由器默认提供 1 个 WAN 口，下文以 WAN1 设置为例，其他 WAN 口的设置与 WAN1 方法类似。
- 各上网设置参数均由 ISP（互联网服务提供商）提供，如不清楚，请咨询您的 ISP。

### 5.2.1 宽带拨号

**步骤 1** 点击「联网设置」进入设置页面；

**步骤 2** 联网方式：选择“宽带拨号”；

**步骤 3** 宽带账号：输入 ISP 提供的宽带账号；

**步骤 4** 宽带密码：输入 ISP 提供的宽带密码；

**步骤 5** 点击页面底端的 **保存**。

### 联网设置

#### WAN口个数

WAN口个数：

接口类型：

				
WAN	WAN/LAN	LAN	LAN	LAN

接口类型：WAN1LAN2LAN3LAN4LAN5

---

#### WAN1口

联网方式：

宽带账号：

宽带密码：

----完成

稍等片刻，当联网状态显示“认证成功”时，您可以尝试上网了。如果您仍然不能上网，可以进入「更多设置」>「WAN口参数」页面，尝试修改 [WAN口参数](#) 解决问题。

#### WAN1口

联网方式：

宽带账号：

宽带密码：

联网状态：认证成功

## 5.2.2 动态 IP

**步骤 1** 点击「联网设置」进入设置页面；

**步骤 2** 联网方式：选择“动态 IP”；

**步骤 3** 点击页面底端的 **保存**。

**联网设置**

**WAN口个数**

WAN口个数：

接口类型：  
WAN1    LAN2    LAN3    LAN4    LAN5

**WAN1口**

联网方式：

---完成

稍等片刻，当联网状态显示“已连接”时，您可以尝试上网了。如果您仍然不能上网，可以进入「更多设置」>「WAN 口参数」页面，尝试修改 [WAN 口参数](#) 解决问题。

**WAN1口**

联网方式：

联网状态：

## 5.2.3 静态 IP

**步骤 1** 点击「联网设置」进入设置页面；

**步骤 2** 联网方式：选择“静态 IP”；

**步骤 3** IP 地址、子网掩码、默认网关、首选/备用 DNS 服务器：输入 ISP 提供的相关信息；

**步骤 4** 点击页面底端的 **保存**。

The screenshot displays a network configuration interface. At the top, under the heading "WAN口个数", there is a dropdown menu for "WAN口个数" set to "1". Below this, five port icons are shown: WAN, WAN/LAN, LAN, LAN, and LAN. The WAN and the final LAN port are highlighted with green borders. Below the icons, the labels "WAN1", "LAN2", "LAN3", "LAN4", and "LAN5" are aligned under the "接口类型" label. The second section, "WAN1口", contains several input fields: "联网方式" is set to "静态IP"; "IP地址" is "192.168.1.55"; "子网掩码" is "255.255.255.0"; "默认网关" is "192.168.1.60"; "首选DNS服务器" is "192.168.1.60"; and "备用DNS服务器" is empty with "(可选)" next to it.

----完成

稍等片刻，当联网状态显示“已连接”时，您可以尝试上网了。如果您仍然不能上网，可以进入「更多设置」>「WAN 口参数」页面，尝试修改 [WAN 口参数](#) 解决问题。

## WAN1口

联网方式：

IP地址：

子网掩码：

默认网关：

首选DNS服务器：

备用DNS服务器： (可选)

联网状态：已连接

# 6

# 网速控制

## 6.1 概述

通过网速控制功能，网络管理员可以对用户的网速进行限制，使有限的带宽资源得到合理分配。

进入页面：点击「网速控制」。

### 网速控制

#### WAN口宽带

请填写宽带运营商提供的带宽大小以获取更好的上网体验

WAN1:            上传速率：  Mbps            下载速率：  Mbps

#### 限速模式

限速模式：

### 参数说明

标题项	说明
WAN 口带宽	上传速率 设置所办理的宽带的带宽值。不清楚时，可以咨询您的 ISP。 下载速率
限速模式	不限速 不对局域网用户的上传/下载速率进行限制。 <a href="#">自定义限速</a> 网络管理员根据实际环境需要，为每个连接到路由器的用户设置最大上传/下载速率。相较于分组限速来说，设置更加灵活。 <a href="#">自动分配网速</a> 路由器根据「网速控制」页面设置的 WAN 口上传/下载速率，智能地给局域网用户分配带宽。

标题项	说明
<a href="#">分组限速</a>	<p>网络管理员根据实际环境需要，手动设置网速控制规则。</p> <p>控制指定 IP 组内的用户在指定时间组内共享或独享所设置的上传/下载速率,并设置单台并发连接数等。</p>

---

## 6.2 自定义限速

为连接到路由器的用户单独设置最大上传/下载速率。

设置步骤：

**步骤 1** 点击「网速控制」；

**步骤 2** 限速模式：选择“自定义限速”；

**步骤 3** 在线设备/离线设备：请根据需要选择；

**步骤 4** 最大上传/下载速率：指定对应主机的最大上传/下载速率；

**步骤 5** 点击页面底端的 **保存**。



---完成

### 参数说明

标题项	说明
主机名称	用户设备名称，可根据需要修改。
下载总流量	该用户下载数据的总量。
上传速率	该用户当前的上传/下载速率。
下载速率	
最大上传速率	该用户限定的最大上传/下载速率。
最大下载速率	

## 6.3 全部限速

为局域网所有在线用户或离线用户设置最大上传/下载速率。

设置步骤：

**步骤 1** 点击「网速控制」；

**步骤 2** 限速模式：选择“自定义限速”；

**步骤 3** 在线设备/离线设备：请根据需要选择；

**步骤 4** 点击 **全部限速** ；



**步骤 5** 为局域网所有的在线用户或离线用户设置最大上传/下载速率；

**步骤 6** 点击 **保存**。



---完成

## 6.4 自动分配网速

为连接到路由器的在线用户平均分配网速。

设置步骤：

**步骤 1** 点击「网速控制」；

**步骤 2** WAN：根据 ISP 提供的带宽，设置上传/下载速率；

**步骤 3** 限速模式：选择“自动分配网速”；

**步骤 4** 点击页面底端的 **保存**。



The screenshot shows a configuration page for WAN settings. It is divided into two sections: "WAN口宽带" (WAN Port Bandwidth) and "限速模式" (Speed Limit Mode). In the "WAN口宽带" section, there is a prompt to enter the bandwidth provided by the ISP. Below this, the "WAN1" section shows "上传速率" (Upload Rate) and "下载速率" (Download Rate) both set to 100 Mbps. In the "限速模式" section, the "限速模式" (Speed Limit Mode) is set to "自动分配网速" (Automatic Bandwidth Allocation).

---完成

## 6.5 分组限速

通过分组限速功能，使 IP 组内的用户在一段时间内共享或独享所设置的上传/下载速率。

**步骤 1** 点击「网速控制」；

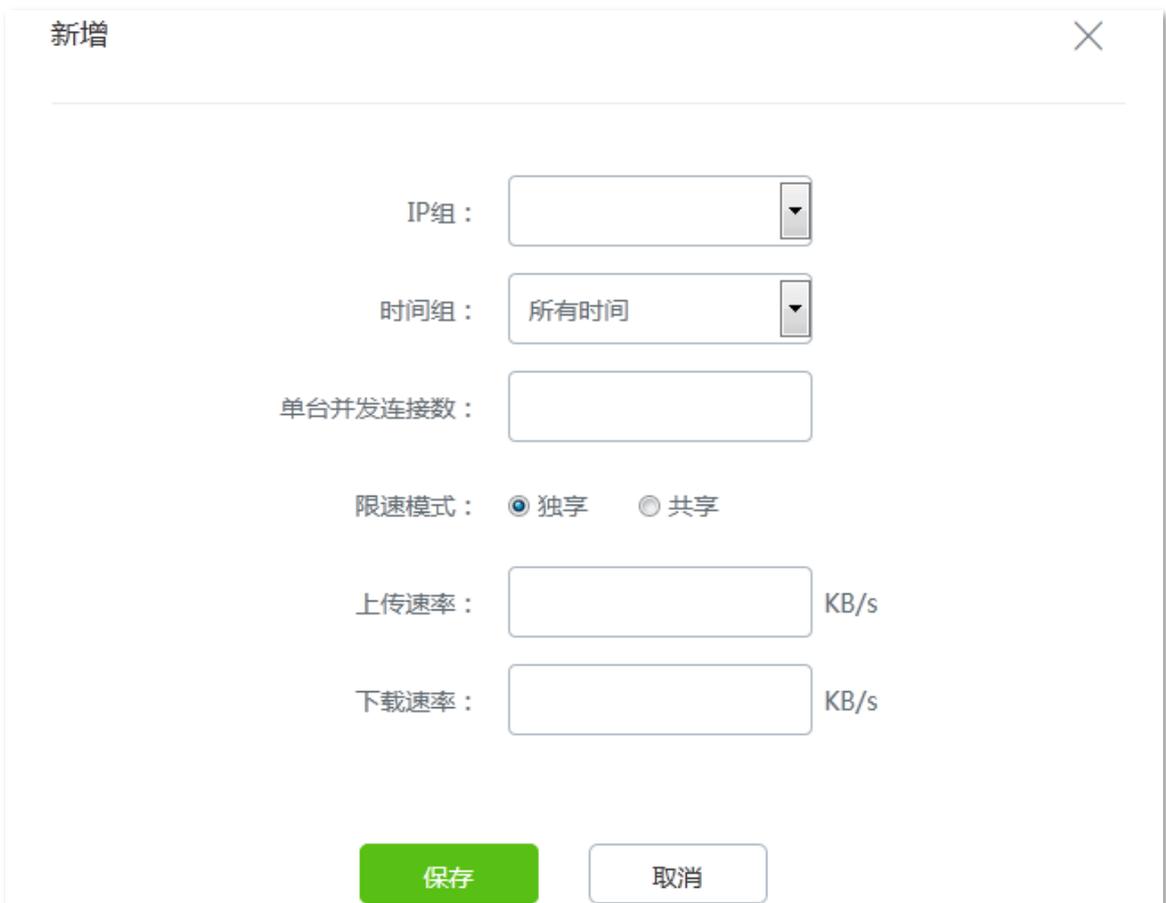
**步骤 2** 限速模式：选择“分组限速”；

**步骤 3** 点击 **+新增** ；



**步骤 4** 在【新增】窗口配置各项参数；

**步骤 5** 点击 **保存**。



----完成

成功添加“分组限速”规则后，可以在「网速控制」页面查看到已添加的规则。如下图示例。



## 参数说明

标题项	说明
IP 组	选择引用的 IP 组，以指定规则对应的用户。IP 组应事先已在「行为管理」>「IP 组与时间组」页面配置好。
时间组	选择引用的时间组，以指定规则对应的生效时间。时间组应事先已在「行为管理」>「IP 组与时间组」页面配置好。
单台并发连接数	受控 IP 地址范围中，每台用户设备所能使用的最大连接数。若无特殊需求，建议设置为 300。
限速模式	设置网速控制的模式。 <ul style="list-style-type: none"><li>- 独享：受控 IP 地址范围内的每个用户独享所设置的上传/下载速率。此模式下，每个受控用户所获得的带宽都是一样的。</li><li>- 共享：受控 IP 地址范围内的所有用户共享所设置的上传/下载速率。此模式下，每个受控用户所获得的带宽可能不一样。</li></ul>
上传速率	限制的上传/下载速率。
下载速率	限制的上传/下载速率。
启用状态	规则当前的状态，可根据需要启用或禁用。
操作	可对规则进行如下操作： <ul style="list-style-type: none"><li>- 点击  可以修改规则。</li><li>- 点击  可以删除规则。</li></ul>

## 6.6 分组限速配置举例

### 组网需求

某企业使用路由器进行网络搭建，要求：局域网中采购部（IP 地址为 192.168.0.2~192.168.0.100）的每个员工在星期一到星期五的上班时间（8:00~18:00）都能使用 1Mbps 的固定上下行带宽。对于局域网其他设备，不限制使用带宽。

可以使用路由器的“分组限速”功能实现上述需求。假设每台用户设备的并发连接数为 300。

### 配置步骤

#### 步骤 1 配置时间组；

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。



#### 步骤 2 配置 IP 组；

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。



**步骤 3** 启用“分组限速”功能；

进入「网速控制」页面，在“限速”模块选择“分组限速”，然后点击 **保存**。



**步骤 4** 设置“分组限速”规则。

1. 进入“网速控制”页面，点击 **+新增**；
2. 在【新增】窗口配置各项参数；
  - (1) IP 组：点击下拉框，选择规则应用的 IP 组，本例为“采购部”。
  - (2) 时间组：点击下拉框，选择规则应用的时间组，本例为“上班时间”。
  - (3) 单台并发连接数：设置单个客户端并发连接数，本例为“300”。
  - (4) 限速模式：选择“独享”。
  - (5) 上传/下载速率：设置客户端的最大上传/下载速率，本例为“128KB/s”。
3. 点击 **保存**。

新增 ×

---

IP组：

时间组：

单台并发连接数：

限速模式： 独享  共享

上传速率： KB/s

下载速率： KB/s

## 验证配置

IP 地址在 192.168.0.2~192.168.0.100 范围内的用户，在星期一到星期五的 8:00~18:00 的最大上传速率为 128KB/s，最大下载速率为 128KB/s。

# 7 认证管理

## 7.1 PPPoE 认证

### 7.1.1 概述

默认情况下，路由器接入互联网后，连接到路由器局域网的客户端就可以访问互联网了。开启 PPPoE 认证功能后，路由器下的用户访问网络前，需要先进行宽带拨号，连接成功后才能上网。

路由器还支持账号到期提醒功能。网络管理员可以设置路由器，使用户在用户账号到期前 7 天之内接收到通知信息，从而简化网络管理工作，并提高网管工作效率。

进入页面：点击「认证管理」>「PPPoE 认证」。

默认情况下，路由器关闭了 PPPoE 认证功能，开启后，页面显示如下：

## PPPoE认证

PPPoE认证：



服务器IP地址：

PPPoE用户起始IP地址：

用户结束IP地址：

首选DNS服务器：

备选DNS服务器：

### 账号到期提醒

---

到期前多久开始提醒：



到期提醒页面：

## 参数说明

标题项	说明
PPPoE 认证	PPPoE 认证功能开关。  表示关闭，  表示开启。
服务器 IP 地址	设置 PPPoE 服务器的 IP 地址。建议保持默认设置，如必须修改时，通常建议也将此 IP 地址设在私网 IP 地址段。私网 IP 地址如下。 <ul style="list-style-type: none"><li>- A 类：10.0.0.1~10.255.255.254</li><li>- B 类：172.16.0.1~172.31.255.254</li><li>- C 类：192.168.0.1~192.168.255.254</li></ul>
PPPoE 认证	
PPPoE 用户起始 IP 地址	设置用户宽带拨号成功后，PPPoE 服务器可以分配给用户的 IP 地址的范围。PPPoE 用户起始/结束 IP 地址必须与服务器 IP 地址在同一个网段。
用户结束 IP 地址	
首选 DNS 服务器	路由器分配给 PPPoE 用户的域名服务器地址，一般与路由器 WAN 口的首选/备用 DNS 地址相同。
备选 DNS 服务器	
到期前多久开始提醒	设置账号到期前多少天进行提醒。默认为账号到期前 7 天提醒。
账号到期提醒	
到期前提醒页面	设置账号到期前提醒的页面信息。点击 <a href="#">配置</a> 可以修改页面提醒信息。

## 7.1.2 配置 PPPoE 认证

**步骤 1** 点击「认证管理」>「PPPoE 认证」；

**步骤 2** PPPoE 认证：点击滑块至 ；

**步骤 3** 根据需要设置 PPPoE 服务器信息、账号到期前提醒信息；

**步骤 4** 点击页面底端的 [保存](#)。

## PPPoE认证

PPPoE认证：

服务器IP地址：

PPPoE用户起始IP地址：

用户结束IP地址：

首选DNS服务器：

备选DNS服务器：

### 账号到期提醒

到期前多久开始提醒：

到期前提醒页面： [预览](#)

---完成

## 7.2 认证用户管理

### 7.2.1 概述

在这里，可以设置用户进行 PPPoE 认证上网时使用的用户名和密码，设置不需要进行认证上网的主机，以及导出或导入认证账号信息。

进入页面：点击「认证管理」>「认证用户管理」。

#### 认证用户管理

##### 免认证主机

+新增

免认证方式	主机名称/IP/MAC	备注	操作
暂无数据			

##### 认证用户管理

+新增

用户名/备注  搜索

用户名	密码	备注	状态	有效期/上网时长	启用状态	操作
-----	----	----	----	----------	------	----

#### 参数说明

标题项	说明
免认证方式	以何种形式指定免认证主机，本路由器支持 IP 地址、MAC 地址、主机名称。
免认证主机	不需要进行认证上网的主机信息。 <ul style="list-style-type: none"><li>- 当“免认证方式”选择为“IP 地址”时，输入不需要进行认证上网的设备的 IP 地址。</li><li>- 当“免认证方式”选择为“MAC 地址”时，输入不需要进行认证上网的设备的 MAC 地址。</li></ul>

标题项	说明
	- 当“免认证方式”选择为“主机名称”时，输入不需要进行认证上网的设备的名称。
备注	不需要进行认证上网的设备的描述。
操作	<p>可对规则进行如下操作：</p> <ul style="list-style-type: none"> <li>- 点击  可以修改规则。</li> <li>- 点击  可以删除规则。</li> </ul>
用户名	用户认证上网使用的用户名、密码。
密码	启用 PPPoE 认证功能后，用户上网前，需要先使用此用户名/密码在用户设备上 PPPoE 认证（宽带拨号）。
备注	账号的描述信息。可不填。
状态	账号的使用状态。
有效期/上网时长	该账号的有效使用时间。过了有效期后，用户不能使用该账号认证上网。
认证用户管理	
启用状态	规则的使用状态，可根据需要启用或禁用。
操作	<p>可对规则进行如下操作：</p> <ul style="list-style-type: none"> <li>- 点击  可以修改规则。</li> <li>- 点击  可以删除规则。</li> </ul>
导出用户账户	将已配置好的认证用户账号数据导出到本地电脑保存。
导入用户账户	导入之前导出的认证用户账号数据到路由器。

## 7.2.2 新增认证账号

**步骤 1** 点击「认证管理」>「认证用户管理」；

**步骤 2** 在“认证用户管理”模块点击 **+新增** ；



**步骤 3** 在【新增】窗口配置各项参数；

**步骤 4** 点击 **保存**。

----完成

## 部分参数说明

标题项	说明
共享账号用户数	允许同时使用该账号认证上网的用户数量。
并发连接数	单台设备的最大并发连接数。
上传速率	账号的最大上传/下载速率。
下载速率	

## 7.3 PPPoE 认证配置举例

### 组网需求

某企业使用路由器进行网络搭建。要求：

- 员工访问互联网时需要进行 PPPoE 认证（宽带拨号）。
- 网络管理员访问互联网时不需要认证。

### 方案设计

可以通过路由器的 PPPoE 认证功能实现上述需求。假设网络管理员电脑的物理地址为 44:37:E6:12:34:56。

### 配置步骤

**步骤 1** 设置 PPPoE 认证；

1. 点击「认证管理」>「PPPoE 认证」；
2. PPPoE 认证：点击滑块至 ；
3. 根据需要设置 PPPoE 服务器信息、账号到期前提醒信息；
4. 点击页面底端的 **保存**。

### PPPoE认证

PPPoE认证：

服务器IP地址：

PPPoE用户起始IP地址：

用户结束IP地址：

首选DNS服务器：

备选DNS服务器：

#### 账号到期提醒

到期前多久开始提醒：

到期前提醒页面：

## 步骤 2 添加认证账号；

1. 点击「认证管理」>「认证用户管理」；
2. 在“认证用户管理”模块点击  ；

### 认证用户管理

用户名	密码	备注	状态	有效期/上网时长	启用状态	操作
-----	----	----	----	----------	------	----

3. 在【新增】窗口配置各项参数。
  - (1) 用户名：设置 PPPoE 认证的用户名，如“zhangsan”。
  - (2) 密码：设置 PPPoE 认证的密码，如“zhangsan”。
  - (3) 备注：输入该用户的描述，如“员工”。
  - (4) 有效期：设置账号有效期，如“永不过期”。
  - (5) 共享账号用户数：设置允许同时使用该账号认证上网的用户数量，如“10”。

(6) 并发连接数：设置使用该账号上网的设备的并发连接数。可保持默认设置。

4. 点击 **保存**。

### 新增

用户名：

密码：

备注：

有效期：

共享账号用户数：

并发连接数：

上传速率： KB/s

下载速率： KB/s

**保存**

**步骤 3** 新增不需要认证上网的主机。

1. 点击「认证管理」>「认证用户管理」；
2. 在“免认证主机”模块点击 **+新增**；

#### 免认证主机

免认证方式	主机名称/IP/MAC	备注	操作
-------	-------------	----	----

3. 在【新增】窗口配置各项参数；

- (1) 免认证方式：选择以何种形式指定免认证主机，本例为“MAC地址”。
- (2) MAC地址：输入该客户端的MAC地址，本例为“44:37:E6:12:34:56”。
- (3) 备注：输入该用户的备注，本例为“网络管理员”。

4. 点击 **保存**。



新增

免认证方式： MAC地址

MAC地址： 44:37:E6:12:34:56

备注： 网络管理员

保存 取消

----完成

添加成功，如下图示：



认证用户管理

免认证主机

+新增

免认证方式	主机名称/IP/MAC	备注	操作
MAC地址	44:37:E6:12:34:56	网络管理员	✎ 删除

认证用户管理

+新增

用户名/备注 搜索

用户名	密码	备注	状态	有效期/上网时长	启用状态	操作
zhangsan	zhangsan	员工	离线	永不过期	开启	✎ 删除

## 验证配置

管理员访问互联网时无需认证。

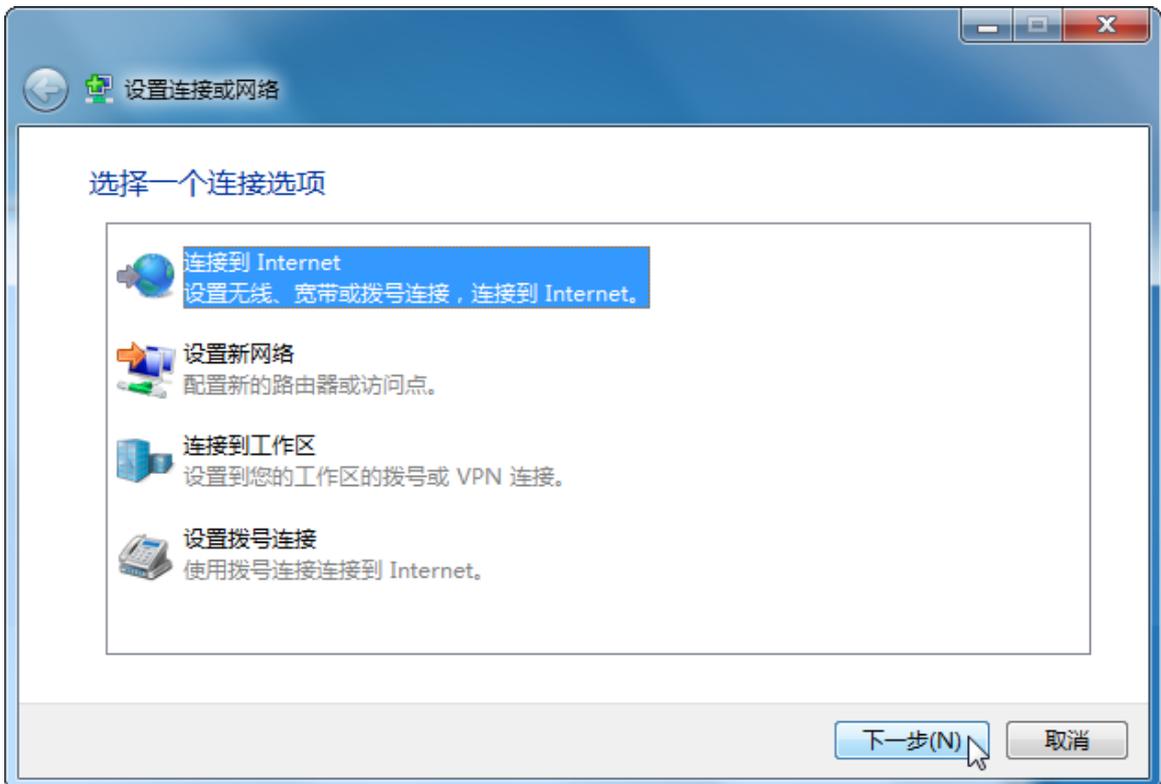
员工访问互联网时，需要先在电脑上进行宽带拨号，步骤如下（以 Window 7 为例）。

**步骤 1** 点击桌面左下角的开始图标；

**步骤 2** 点击控制面板>网络和 Internet>网络和共享中心>设置新的连接或网络；



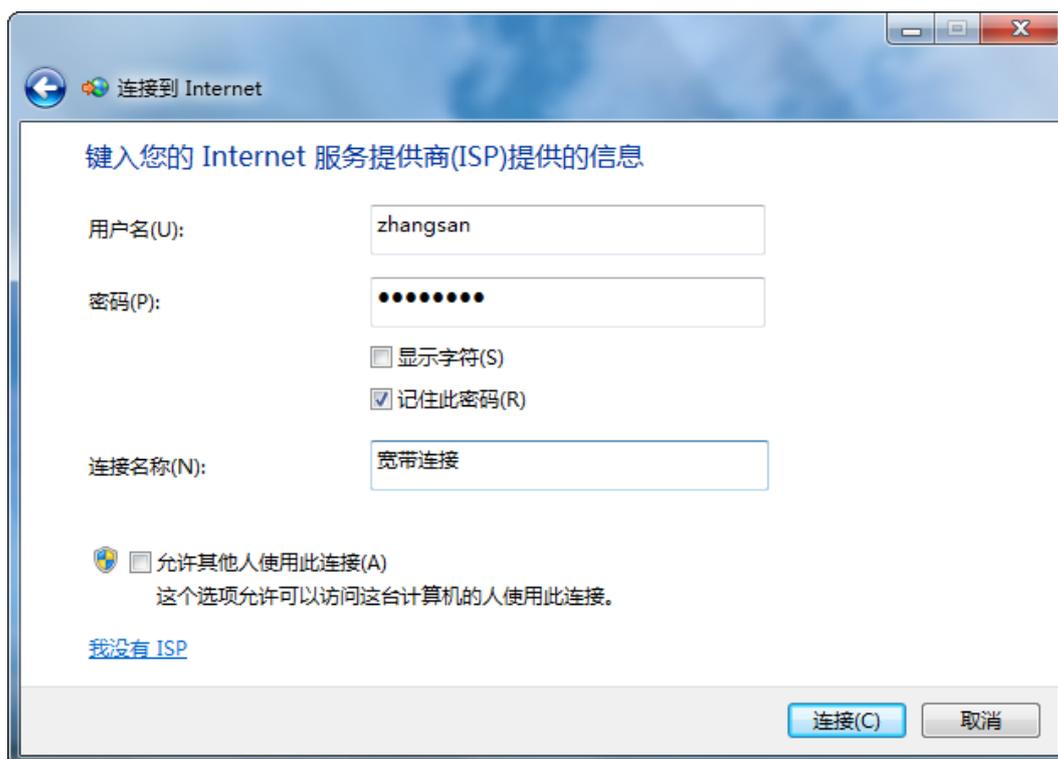
**步骤 3** 选择连接到 Internet，然后点击  ；



**步骤 4** 点击宽带 (PPPoE) (R);



**步骤 5** 填写 PPPoE 认证用户名和密码，本例中用户名为“zhangsan”，密码为“zhangsan”，勾选记住此密码 (R)，点击 **连接**。



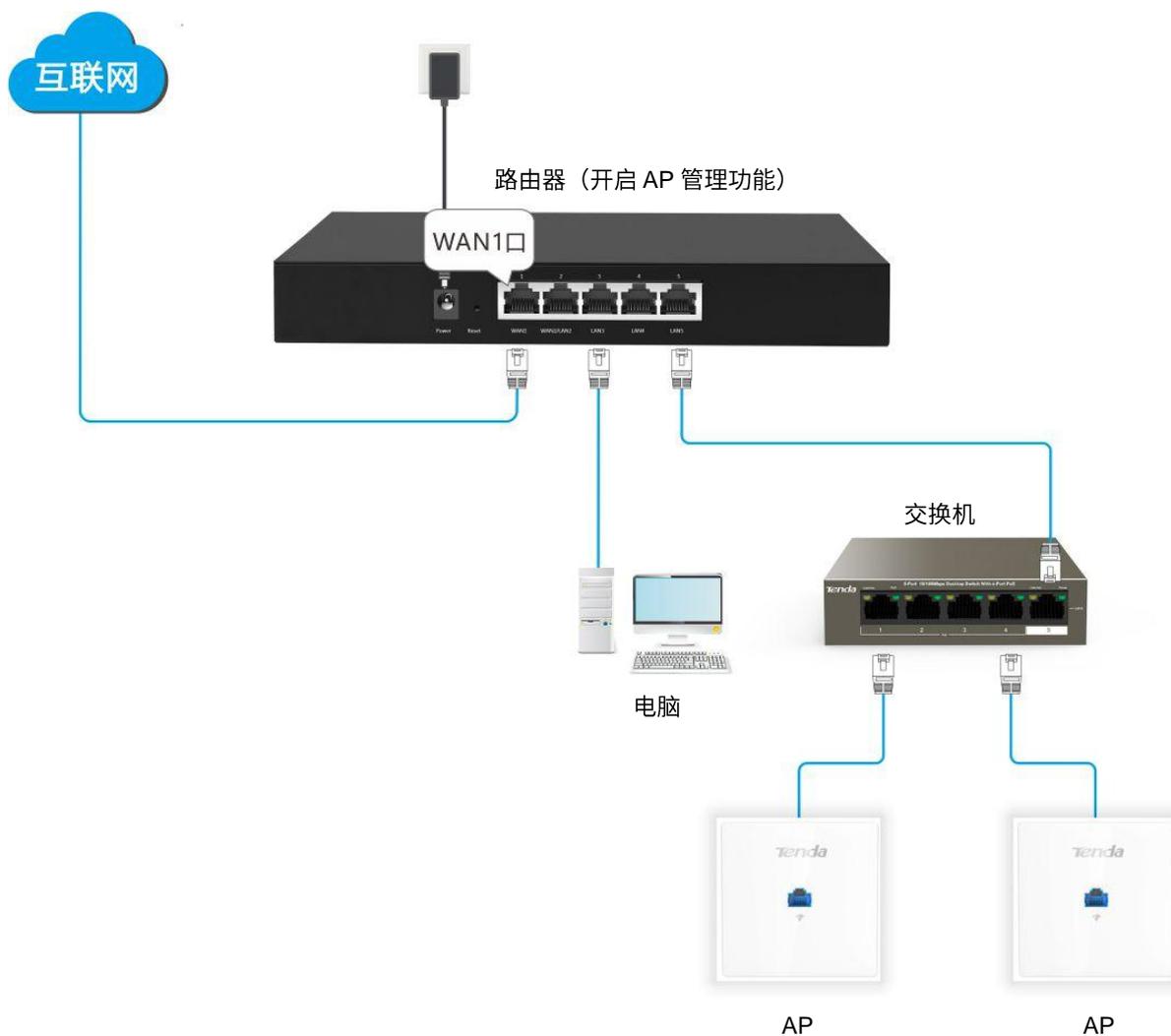
稍等片刻，拨号成功，可以上网了。

以后每次开机后，点击电脑桌面右下角的网络图标，然后点击宽带连接，拨号成功后即可正常上网。

# 8 AP 管理

路由器的「AP 管理」模块包括：[基本设置](#)、[AP 维护](#)、[高级设置](#)。

路由器集成了无线控制器的功能，可以管理 Tenda 公司 AP。网络应用拓扑图如下：



## 8.1 基本设置

### 8.1.1 概述

进入页面：点击「AP 管理」>「基本设置」。

在这里，可以集中配置局域网中 AP 的无线网络相关参数，如无线名称、启用状态、频段、无线密码等。这些配置在 Tenda AP 连接到路由器时自动生效。

初次使用本路由器或将路由器恢复出厂设置后，在“设置向导”进行的 AP 无线配置为此处的第一条无线策略。

#### 基本设置

AP管理：

无线网络	启用状态	无线名称	频段	加密方式	无线密码	更多设置
1	<input checked="" type="checkbox"/>	Tenda_1	2.4G&5G	WPA2-PSK	12345678	⋮
2	<input type="checkbox"/>	Tenda_AP_1	2.4G&5G	不加密		⋮
3	<input type="checkbox"/>	Tenda_AP_2	2.4G&5G	不加密		⋮
4	<input type="checkbox"/>	Tenda_AP_3	2.4G&5G	不加密		⋮
5	<input type="checkbox"/>	Tenda_AP_4	2.4G	不加密		⋮
6	<input type="checkbox"/>	Tenda_AP_5	2.4G	不加密		⋮
7	<input type="checkbox"/>	Tenda_AP_6	2.4G	不加密		⋮
8	<input type="checkbox"/>	Tenda_AP_7	2.4G	不加密		⋮

#### 参数说明

标题项	说明
	无线策略的序号。
无线网络	- 1~4：用于修改 AP 2.4GHz 或 5GHz 频段的第 1~4 个 SSID 的相关参数。 - 5~8：用于修改 AP 2.4GHz 频段的第 5~8 个 SSID 的相关参数。

标题项	说明
启用状态	<p>无线策略的状态，也是 AP 对应 SSID 的启用/禁用状态。默认启用第一条无线策略，禁用其他无线策略。</p> <p> 注意</p> <p>关闭第 1 条无线策略会导致 AP 的无线功能关闭，因此，不建议关闭。AP 的无线功能关闭后，如果要启用，可以启用第 1 条无线策略，也可以到「AP 管理」&gt;「高级设置」页面点击 <b>保存</b> 开启。</p>
无线名称	<p>点击可修改无线网络名称。</p>
频段	<p>选择无线策略的使用频段，即，选择要将无线策略下发到 AP 的哪个频段。</p> <ul style="list-style-type: none"> <li>- 2.4G：无线策略下发到 AP 的 2.4GHz 频段。</li> <li>- 5G：无线策略下发到 AP 的 5GHz 频段。</li> <li>- 2.4G&amp;5G：无线策略同时下发到 AP 的 2.4GHz 频段和 5GHz 频段。</li> </ul> <p> 注意</p> <ul style="list-style-type: none"> <li>- 若第 1 条无线策略的频段为单频，如 2.4G（或 5G），则点击 <b>保存</b> 后，AP 将关闭另一频段如 5G（或 2.4G）的无线功能。</li> <li>- 关闭 AP 某频段的无线功能后，可到「AP 管理」&gt;「高级设置」页面点击 <b>保存</b> 重新开启。</li> </ul>
加密方式	<p>无线网络的加密方式。</p> <ul style="list-style-type: none"> <li>- 不加密：不加密无线网络，用户连接无线网络时，无需输入密码即可接入。为保障网络安全，不建议选择此项。</li> <li>- WPA-PSK：无线网络采用 WPA-PSK 认证方式（AES 加密规则）。</li> <li>- WPA2-PSK：无线网络采用 WPA2-PSK 认证方式（AES 加密规则）。</li> </ul>
无线密码	<p>WPA-PSK 或 WPA2-PSK 的预共享密码，也是用户连接无线网络时需要输入的无线密码。</p>
更多设置	<p>点击  可进行高级参数设置，包括：客户端隔离、隐藏无线网络、最大用户数、VLAN ID。</p> <ul style="list-style-type: none"> <li>- 客户端隔离：启用后，连接到该无线网络下的设备之间不能互相通信，可增强无线网络的安全性。</li> <li>- 隐藏无线网络：启用后，周边的其他无线设备不能扫描到该 SSID。</li> <li>- 最大用户数：无线网络最多允许接入的无线设备数量。默认为 48。</li> <li>- VLAN ID：无线网络所属的 VLAN（IEEE 802.1Q）。默认为 1000。</li> </ul>

## 8.1.2 下发无线策略到 AP



下发无线策略时，如果部分功能 AP 不支持，那么配置可以下发成功，但不会生效。例如：通过 AP 管理功能下发 5G 的配置，若网络中有 AP 不支持 5G，虽然配置可以下发成功，但该 AP 不会生效。

**步骤 1** 点击「AP 管理」>「基本设置」；

**步骤 2** 修改无线网络参数；

**步骤 3** 点击 **保存**。

**基本设置**

AP管理：

无线网络	启用状态	无线名称	频段	加密方式	无线密码	更多设置
1	<input checked="" type="checkbox"/>	Tenda_1	2.4G&5G	WPA2-PSK	12345678	⋮
2	<input checked="" type="checkbox"/>	Tenda_2	2.4G&5G	WPA-PSK	123456789	⋮
3	<input type="checkbox"/>	Tenda_AP_2	2.4G&5G	不加密		⋮
4	<input type="checkbox"/>	Tenda_AP_3	2.4G&5G	不加密		⋮
5	<input type="checkbox"/>	Tenda_AP_4	2.4G	不加密		⋮
6	<input type="checkbox"/>	Tenda_AP_5	2.4G	不加密		⋮
7	<input type="checkbox"/>	Tenda_AP_6	2.4G	不加密		⋮
8	<input type="checkbox"/>	Tenda_AP_7	2.4G	不加密		⋮

---完成

稍等片刻，局域网中 AP 的相关无线设置会变为与无线策略一致。

## 8.2 AP 维护

### 8.2.1 概述

进入页面：点击「AP 管理」>「AP 维护」。

在这里,可以批量升级/恢复出厂设置/重启在线 AP,批量删除离线 AP 信息,单独修改某一 AP 的配置信息、查看/导出“管理 AP”信息等。

#### AP维护

在线AP数量: 2 台

AP型号/备注/IP/MAC

<input type="checkbox"/>	AP型号	备注	IP/MAC地址	频段	发射功率	信道	在线设备/限制数	状态	更多设置
<input type="checkbox"/>	W9V1.0	<input type="text" value="W9V1.0"/>	192.168.0.254 50:2B:73:F4:EA:60	2.4G 5G	22dBm 20dBm	自动 自动	0/96 0/96	在线	⋮
<input type="checkbox"/>	i21V1.0	<input type="text" value="i21V1.0"/>	192.168.0.24 50:2B:73:09:94:50	2.4G 5G	22dBm 20dBm	自动 自动	0/96 0/96	在线	⋮

### 8.2.2 升级

使用升级功能,可以同时升级多个 AP 的软件版本。



AP 升级过程中,为了避免损坏 AP 导致其无法使用,请切勿关闭路由器和 AP 的电源。

升级 AP 前,需要先登陆 Tenda 官网 <http://www.tenda.com.cn>, 下载对应型号的 AP 软件到本地电脑。然后,再按以下步骤进行操作:

**步骤 1** 点击「AP 管理」>「AP 维护」;

**步骤 2** 选择需要进行软件升级的 AP;

**步骤 3** 点击  ,之后按页面提示操作。



----完成

## 8.2.3 恢复出厂设置

使用恢复出厂设置功能，可以同时多个 AP 恢复出厂设置。

设置步骤：

- 步骤 1** 点击「AP 管理」>「AP 维护」；
- 步骤 2** 选择需要恢复出厂设置的 AP；
- 步骤 3** 点击 **恢复出厂设置**，之后按页面提示操作。



----完成

## 8.2.4 重启

使用重启功能，可以同时多个 AP 重新启动。

设置步骤：

- 步骤 1** 点击「AP 管理」>「AP 维护」；
- 步骤 2** 选择需要重新启动的 AP；

**步骤 3** 点击 **重启**，之后按页面提示操作。



---完成

重启时，AP 将离线一段时间，重启完成后，AP 将自动上线。AP 从离线到重新上线的过程可能需要 1~2 分钟，请耐心等待。您可以点击 **刷新** 查看。

## 8.2.5 删除

使用删除功能，可以同时删除多个处于离线状态的 AP。



提示

在线 AP 不能删除。

设置步骤：

**步骤 1** 点击「AP 管理」>「AP 维护」；

**步骤 2** 选择需要删除的离线 AP；

**步骤 3** 点击 **删除**，之后按页面提示操作。



---完成

## 8.2.6 刷新

如果要更新页面显示的 AP 信息，请点击 **刷新**。



----完成

## 8.2.7 导出

使用导出功能，可以将 AP 列表信息以 Excel 的格式导出并保存到本地电脑。

设置步骤：

**步骤 1** 点击「AP 管理」>「AP 维护」；

**步骤 2** 点击 **导出**，之后按页面提示操作。



----完成

## 8.2.8 修改

使用修改功能，可以单独修改某一 AP 的配置信息，如无线开关、国家或地区、信道、发射功率等参数。

设置步骤：

**步骤 1** 点击「AP 管理」>「AP 维护」；

**步骤 2** 找到需要修改配置的 AP，然后点击对应操作栏的 ；

**AP维护**

升级 恢复出厂设置 重启 删除 刷新 导出 在线AP数量：2 台

AP型号/备注/IP/MAC 搜索

AP型号	备注	IP/MAC地址	频段	发射功率	信道	在线设备/限制数	状态	更多设置
W9V1.0	W9V1.0	192.168.0.97 50:2B:73:F4:EA:60	2.4G 5G	18dBm 17dBm	9 153	0/96 2/96	在线	
i21V1.0	i21V1.0	192.168.0.24 50:2B:73:09:94:50	2.4G 5G	20dBm 18dBm	7 153	0/96 0/96	在线	

**步骤 3** 根据需要修改 AP 的配置；

**步骤 4** 点击页面底端的 **保存**。

---完成

## 8.3 高级设置

### 8.3.1 概述

进入页面：点击「AP 管理」>「高级设置」。

在这里，可以集中配置局域网中 AP 的高级参数。

### 2.4GHz/5GHz 网络设置

在“2.4GHz/5GHz 网络设置”模块，可以集中配置局域网中 AP 的网络模式、信道、发射功率等射频参数。

#### 高级设置

##### 2.4GHz网络设置

国家或地区：

网络模式：

信道带宽： 20MHz  40MHz  自动

信道：

发射功率：

接入信号强度限制： dBm (范围：-90 - -60)

空口调度： 启用  禁用

[更多设置...](#)

## 参数说明 1

标题项	说明
国家或地区	选择 AP 当前所在的国家或地区。
网络模式	<p>选择 AP 的无线网络模式。2.4GHz 包括 11b、11g、11b/g、11b/g/n；5GHz 包括 11a、11ac、11a/n。</p> <ul style="list-style-type: none"><li>- 11b：此模式下，仅允许 802.11b 无线设备接入 AP 的 2.4GHz 无线网络。</li><li>- 11g：此模式下，仅允许 802.11g 无线设备接入 AP 的 2.4GHz 无线网络。</li><li>- 11b/g：此模式下，允许 802.11b、802.11g 无线设备接入 AP 的 2.4GHz 无线网络。</li><li>- 11b/g/n：此模式下，允许 802.11b、802.11g 以及工作在 2.4 GHz 的 802.11n 无线设备接入 AP 的 2.4GHz 无线网络。</li><li>- 11a：此模式下，仅允许 802.11a 无线设备接入 AP 的 5GHz 无线网络。</li><li>- 11ac：此模式下，允许 802.11ac 无线设备接入 AP 的 5GHz 无线网络。</li><li>- 11a/n：此模式下，允许工作在 5GHz 的 802.11a 和 802.11n 无线设备接入 AP 的 5GHz 无线网络。</li></ul>
信道带宽	<p>选择 AP 的无线信道带宽。</p> <ul style="list-style-type: none"><li>- 20MHz：AP 只能使用 20MHz 的信道带宽。</li><li>- 40MHz：AP 只能使用 40MHz 的信道带宽。</li><li>- 80MHz：仅适用 5GHz，AP 根据周围环境，自动调整信道带宽为 20MHz、40MHz 或 80MHz。</li><li>- 自动：仅适用于 2.4GHz，AP 根据周围环境，自动调整信道带宽为 20MHz 或 40MHz。</li></ul>
信道	<p>选择 AP 的无线工作信道。</p> <p>信道的可选择范围由当前选择的“国家或地区”和“频段”（2.4GHz 或 5GHz）决定。</p>
发射功率	<p>设置 AP 的发射功率。</p> <p>若 AP 不支持设置的功率，则配置下发后，以 AP 支持的最大范围为准生效。即，当功率超过 AP 的上限功率时，只使用 AP 的最大功率；当功率小于 AP 的下限功率时，只使用 AP 的最小功率。</p>
接入信号强度限制	<p>设置 AP 相关射频可接受的无线客户端信号强度。如果无线客户端信号强度比此阈值小，AP 将主动断开无线客户端。</p>
5GHz 优先	<p>仅“5GHz 网络设置”支持。启用后，当 2.4GHz 和 5GHz 的无线名称（SSID）和无线密码都相同，且无线客户端支持双频 WiFi 时，客户端将会优先选择 5GHz 频段的 SSID 进行连接。</p> <p>生效前提：无线网络加密方式为 WPA/WPA2-PSK，并且 SSID 不能包含中文字符。</p>

标题项	说明
空口调度	启用/禁用空口调度功能。 空口调度可以保证每个客户端的数据传输时间相等，如果低速率终端在单位时间内没有传输完数据，也要等到下次继续传输。解决了某些低速率客户端占用无线空口太多资源问题，提升 AP 的整体效率，有效保障了带机量和吞吐量。
更多设置...	配置更多高级参数，详细可参考下文 <a href="#">参数说明 2</a> 。

在“高级设置”模块，点击[更多设置...](#)，将展开更多高级参数。



## 参数说明 2

标题项	说明
无线网络隔离	AP 的 SSID 隔离功能开关。 表示关闭， 表示开启。 开启后，连接到 AP 对应频段不同 SSID 的无线客户端之间不能互相通信。
WMM	WMM，即“无线多媒体”。 表示关闭， 表示开启。 开启 WMM 后，音视频数据优先转发。如果要提高 AP 对于无线多媒体数据（如观看在线视频）的传输性能，建议开启。

标题项	说明
APSD	APSD, 即“自动省电模式”, 是 WiFi 联盟的 WMM 省电认证协议。  表示关闭,  表示开启。开启“APSD”能降低 AP 的电能消耗。默认关闭。
部署模式	<p>请根据实际应用场景, 选择“部署模式”特性。</p> <ul style="list-style-type: none"> <li>- 强覆盖: 常用于 AP 部署密度较低的场景, 此模式可以尽可能地确保客户端成功接入 AP。</li> <li>- 高密度: 常用于 AP 部署密度较高的场景, 此模式可以确保客户端连接到信号好的 AP。</li> <li>- 默认: 介于“强覆盖”和“高密度”之间。</li> </ul>
客户端老化时间	客户端连接到 AP 的 WiFi 后, 如果在该时间段内与 AP 没有数据通信, AP 将主动断开该客户端; 如果在该时间段内与 AP 有数据通信, 则停止老化计时。

## 其他设置

在“其他设置”模块, 可以集中配置局域网 AP 的端口驱动模式、指示灯状态、定时重启、VLAN 相关参数。



### 参数说明 1

标题项	说明
端口驱动模式	<p>AP 的以太网口驱动距离。</p> <ul style="list-style-type: none"> <li>- 标准: 速率高, 驱动距离较短。一般情况下, 建议选择此模式。</li> <li>- 增强: 驱动距离远, 但速率较低, 一般协商为 10Mbps。</li> </ul> <p>连接 AP 以太网口与对端设备的网线超过 100 米时, 才建议尝试改为“增强”来提高网线驱动距离。此时, 必须确保对端端口工作模式为自协商, 否则可能导致 AP 以太网口无法正常收发数据。</p>

标题项	说明
指示灯	<p>启用/禁用 AP 的指示灯显示功能。</p> <ul style="list-style-type: none"> <li>- 启用：开启 AP 的所有指示灯，可根据指示灯判断 AP 的工作状态。默认为“启用”。</li> <li>- 禁用：关闭 AP 的所有指示灯。</li> </ul>
定时重启	<p>启用/禁用 AP 的“定时重启”功能。启用后，可以预防长时间地运行 AP 导致 WLAN 出现性能降低、不稳定等现象。但重启过程中，会断开所有连接，因此建议将“维护时间”设置在无线业务相对空闲的时间。</p> <ul style="list-style-type: none"> <li>- 禁用：关闭定时重启功能。</li> <li>- 定时维护：AP 在指定日期的指定时间点自动重启一次。</li> <li>- 按间隔时间段重启：AP 每隔一个“间隔时间”就会自动重启一次。</li> </ul>
维护时间	指定“定时维护”的维护时间。
间隔时间	指定“按间隔时间段重启”的间隔时间。
更多设置...	配置更多参数，详细可参考下文 <a href="#">参数说明 2</a> 。

在“其他设置”模块，点击[更多设置...](#)，将展开更多参数。

其他设置
✕

---

VLAN :

管理VLAN :

PVID :  (范围 : 1-4094)

Trunk口 :  LAN0  LAN1

保存

取消

## 参数说明 2

标题项	说明
VLAN	<p>AP 的 QVLAN 功能开关。 表示关闭， 表示开启。</p> <p>开启后，本页配置的“管理 VLAN”等参数和「AP 管理」&gt;「基本设置」页面配置的“VLAN ID”将生效。默认为“关闭”。</p>
管理 VLAN	<p>AP 的管理 VLAN ID，默认为“1”。</p> <p>更改管理 VLAN ID 并成功下发到 AP 后，路由器或管理电脑需要连接到新的管理 VLAN，才能管理 AP。</p>
PVID	<p>AP Trunk 口默认所属的 VLAN ID。</p>
Trunk 口	<p>选择作为 AP Trunk 口的有线 LAN 口。Trunk 口允许所有 VLAN 通过。</p> <p> <b>注意</b></p> <p>启用 802.1Q VLAN 功能时，至少要选择一个 LAN 口作为 Trunk 口。如果网络中有的 AP 只有一个 LAN 口，请选择 LAN 0 为 Trunk 口，否则可能会导致配置失败。</p>

### 8.3.2 下发 2.4GHz/5GHz 网络配置到 AP

**步骤 1** 点击「AP 管理」>「高级设置」；

**步骤 2** 在“网络设置”模块修改相关参数；

**步骤 3** 点击页面底端的 **保存**。

## 高级设置

### 2.4GHz网络设置

国家或地区：

网络模式：

信道带宽： 20MHz  40MHz  自动

信道：

发射功率：

接入信号强度限制： dBm（范围：-90 - -60）

空口调度： 启用  禁用

[更多设置...](#)

---完成

稍等片刻，局域网中 AP 的相关网络配置会变为与此处下发的策略一致。

### 8.3.3 下发 VLAN 等其他配置到 AP

**步骤 1** 点击「AP 管理」>「高级设置」；

**步骤 2** 在“其他设置”模块修改相关参数；

**步骤 3** 点击页面底端的 **保存**。

## 其他设置

- 端口驱动模式： 标准  增强
- 指示灯： 启用  禁用
- 定时重启： 禁用  定时维护  按间隔时间段重启

[更多设置...](#)

----完成

稍等片刻，局域网中 AP 的相关配置会变为与此处下发的策略一致。

# 9 行为管理

路由器的「行为管理」模块包括：[IP 组与时间组](#)、[MAC 地址过滤](#)、[IP 地址过滤](#)、[端口过滤](#)、[应用过滤](#)、[网站过滤](#)、[多 WAN 策略](#)。

## 9.1 IP 组与时间组

### 9.1.1 概述

进入页面：点击「行为管理」>「IP 组与时间组」。

在使用路由器的 MAC 地址过滤、IP 地址过滤、端口过滤、应用过滤、网站过滤、分组限速、自定义多 WAN 策略等功能时，会引用时间组、IP 组配置。

默认存在一条时间组，包含了所有时间。默认的时间组规则不能删除。

#### IP组与时间组

##### 时间组设置

<input type="checkbox"/> 组名称	日期	时间	操作
<input type="checkbox"/> 所有时间	星期日, 星期一, 星期二, 星期三, 星期四, 星期五, 星期六	00:00~00:00	<input type="button" value="编辑"/> <input type="button" value="删除"/>

##### IP组设置

<input type="checkbox"/> IP组	IP地址段	操作
------------------------------	-------	----

## 参数说明

标题项	说明	
时间组设置	组名称	时间组的名称，注意不能和已有的时间组名称重复。
	日期	时间段所包含的日期。
	时间	时间段的开始~结束时间。00:00~00:00，表示全天。
操作	可对规则进行如下操作：	
	- 点击  可以修改规则。 - 点击  可以删除规则。	
IP 组设置	IP 组	IP 组的名称，注意不能和已有的 IP 组名称重复。
	IP 地址段	IP 段的开始~结束 IP 地址。
	可对规则进行如下操作：	
操作	- 点击  可以修改规则。 - 点击  可以删除规则。	

## 9.1.2 新增时间组

**步骤 1** 点击「行为管理」>「IP 组与时间组」；

**步骤 2** 在“时间组设置”模块，点击 **+新增** ；



**步骤 3** 在【新增】窗口配置各项参数；

**步骤 4** 点击 **保存**。

新增

组名称：

时间： :  ~  :

日期： 每天     星期日     星期一  
 星期二     星期三     星期四  
 星期五     星期六

----完成

### 9.1.3 新增 IP 组

**步骤 1** 点击「行为管理」>「IP 组与时间组」;

**步骤 2** 在“IP 组设置”模块，点击  ；

IP组设置

<input type="checkbox"/>	IP组	IP地址段	操作
暂无数据			

**步骤 3** 在【新增】窗口配置各项参数；

**步骤 4** 点击  。

新增 ×

---

组名称：

IP地址段： ~

---完成

## 9.2 MAC 地址过滤

### 9.2.1 概述

进入页面：点击「行为管理」>「MAC 地址过滤」。

通过 MAC 地址黑白名单，限制可以通过路由器上网的用户。

- 白名单：对应过滤规则“允许访问互联网”。
- 黑名单：对应过滤规则“禁止访问互联网”。

MAC 地址过滤功能默认关闭，开启后，页面显示如下：



#### 参数说明

标题项	说明
MAC 地址过滤	MAC 地址过滤功能开关。  表示关闭，  表示开启。
过滤方式	MAC 地址过滤的过滤规则。 <ul style="list-style-type: none"><li>- 白名单：即，允许访问互联网。使用此规则时，指定 MAC 地址的用户在对应时间段内可以访问互联网，在其他时间段内不可以访问互联网。</li><li>- 黑名单：即，禁止访问互联网。使用此规则时，指定 MAC 地址的用户在对应时间段内禁止访问互联网，在其他时间段内可以访问互联网。</li></ul>
MAC 地址	规则对应的用户设备的 MAC 地址。

标题项	说明
时间组	选择引用的时间组，以指定规则对应的生效时间。 时间组应事先已在「行为管理」>「IP 组与时间组」页面配置好。
备注	规则的备注信息。
生效开关	规则的状态，可根据需要启用或禁用。
操作	可对规则进行如下操作： - 点击  可以修改规则。 - 点击  可以删除规则。
允许未启用规则和列表外的主机访问互联网	- 勾选时：列表中“未启用”规则的设备 and 列表外的设备均可以访问互联网。 - 未勾选时：只有列表中的规则生效，列表中“未启用”规则的设备 and 列表外的设备均不能访问互联网。

## 9.2.2 新增 MAC 地址过滤规则

**步骤 1** 开启 MAC 地址过滤功能；

1. 点击「行为管理」>「MAC 地址过滤」；
2. MAC 地址过滤：点击滑块至 ；
3. 点击页面底端的 **保存**。



**步骤 2** 添加 MAC 地址过滤规则。

1. 点击 **+新增**；



2. 在【新增】窗口配置各项参数；
3. 点击 **保存**。



----完成

## 9.2.3 MAC 地址过滤配置举例

### 组网需求

某企业使用路由器进行网络搭建。要求：上班时间（周一到周五的 8:00~18:00），仅允许某一采购人员访问互联网，其他员工禁止访问互联网。

### 方案设计

可以使用路由器的 MAC 地址过滤功能实现上述需求。假设该采购人员电脑的物理地址为 CC:3A:61:71:1B:6E。

## 配置步骤

### 步骤 1 配置时间组；

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。

新增

组名称： 上班时间

时间： 8 : 00 ~ 18 : 00

日期：  
 每天     星期日     星期一  
 星期二     星期三     星期四  
 星期五     星期六

保存 取消

### 步骤 2 开启 MAC 地址过滤功能；

1. 点击「行为管理」>「MAC 地址过滤」；
2. MAC 地址过滤：点击滑块至 ；
3. 点击页面底端的 **保存**。

MAC地址过滤

MAC地址过滤：

+新增 删除

过滤方式	MAC地址	时间组	备注	生效开关	操作
------	-------	-----	----	------	----

### 步骤 3 添加 MAC 地址过滤规则。

1. 点击 **+新增**；



2. 在【新增】窗口配置各项参数；

- (1) 过滤模式：选择“白名单（允许访问互联网）”。
- (2) 时间组：选择规则生效的时间组，本例为“上班时间”。
- (3) MAC 地址：输入采购人员电脑的物理地址，本例为“CC:3A:61:71:1B:6E”。
- (4) 备注：设置本规则的备注，如“允许上网”。

3. 点击 **保存**；



4. 禁止未启用规则和列表外的主机访问互联网。

- (1) 禁用“允许未启用规则和列表外的主机访问互联网”；
- (2) 点击页面底端的 **保存**。



---完成

## 验证配置

在星期一~星期五的 8:00~18:00，局域网中，只有使用 MAC 地址为 CC:3A:61:71:1B:6E 的电脑的采购人员才能访问互联网，使用其他员工的电脑不能访问互联网。

## 9.3 IP 地址过滤

### 9.3.1 概述

进入页面：点击「行为管理」>「IP 地址过滤」。通过 IP 地址黑白名单，限制可以通过路由器上网的用户。

- 白名单：对应过滤规则“允许访问互联网”。
- 黑名单：对应过滤规则“禁止访问互联网”。

IP 地址过滤功能默认关闭，开启后，页面显示如下：



#### 参数说明

标题项	说明
IP 地址过滤	IP 地址过滤功能开关。  表示关闭，  表示开启。
过滤方式	IP 地址过滤的过滤规则。 <ul style="list-style-type: none"><li>- 白名单：即，允许访问互联网。使用此规则时，指定 IP 地址的用户在对应时间段内可以访问互联网，在其他时间段内不可以访问互联网。</li><li>- 黑名单：即，禁止访问互联网。使用此规则时，指定 IP 地址的用户在对应时间段内禁止访问互联网，在其他时间段内可以访问互联网。</li></ul>
IP 组	选择引用的 IP 组，以指定规则对应的用户。 IP 组应事先已在「行为管理」>「IP 组与时间组」页面配置好。

标题项	说明
时间组	选择引用的时间组，以指定规则对应的生效时间。 时间组应事先已在「行为管理」>「IP 组与时间组」页面配置好。
备注	规则的备注信息。
生效开关	规则的状态，可根据需要启用或禁用。
操作	可对规则进行如下操作： - 点击  可以修改规则。 - 点击  可以删除规则。
允许未启用规则和列表外的主机访问互联网	- 勾选时：列表中“未启用”规则的设备 and 列表外的设备均可以访问互联网。 - 未勾选时：只有列表中的规则生效，列表中“未启用”规则的设备 and 列表外的设备均不能访问互联网。

## 9.3.2 新增 IP 地址过滤规则

**步骤 1** 开启 IP 地址过滤功能；

1. 点击「行为管理」>「IP 地址过滤」；
2. IP 地址过滤：点击滑块至 ；
3. 点击页面底端的 **保存**。



**步骤 2** 添加 IP 地址过滤规则。

1. 点击 **+新增**；



2. 在【新增】窗口配置各项参数；
3. 点击 **保存**。



----完成

### 9.3.3 IP 地址过滤配置举例

#### 组网需求

某企业使用路由器进行网络搭建。要求：上班时间（周一到周五的 8:00~18:00），仅允许采购部门人员访问互联网，其他员工禁止访问互联网。

#### 方案设计

可以使用路由器的 IP 地址过滤功能实现上述需求。假设采购部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.250。

## 配置步骤

### 步骤 1 配置时间组；

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。

新增

组名称： 上班时间

时间： 8 : 00 ~ 18 : 00

日期：  
 每天     星期日     星期一  
 星期二     星期三     星期四  
 星期五     星期六

保存 取消

### 步骤 2 配置 IP 组；

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

新增

组名称： 采购部

IP地址段： 192.168.0.2 ~ 192.168.0.250

保存 取消

### 步骤 3 开启 IP 地址过滤功能；

1. 点击「行为管理」>「IP 地址过滤」；
2. IP 地址过滤：点击滑块至 ；
3. 点击页面底端的 **保存**。



**步骤 4** 添加 IP 地址过滤规则。

1. 点击 **+新增** ；



2. 在【新增】窗口配置各项参数；
  - (1) 过滤模式：选择“白名单（允许访问互联网）”。
  - (2) 时间组：选择规则生效的时间组，本例为“上班时间”。
  - (3) IP 组：选择规则生效的 IP 组，本例为“采购部”。
  - (4) 备注：设置本规则的备注，如“允许上网”。
3. 点击 **保存** ；

新增
✕

---

过滤模式：

白名单（允许访问互联网）

黑名单（禁止访问互联网）

时间组：

上班时间

IP组：

采购部

备注：

允许上网

保存

取消

4. 禁止未启用规则和列表外的主机访问互联网。

- (1) 禁用“允许未启用规则和列表外的主机访问互联网”。
- (2) 点击页面底端的 保存。

### IP地址过滤

IP地址过滤：

+新增
删除

<input type="checkbox"/>	过滤方式	IP组	时间组	备注	生效开关	操作
<input type="checkbox"/>	白名单	采购部	上班时间	允许上网	<input checked="" type="checkbox"/>	<span>✎</span> <span>🗑</span>

允许未启用规则中的主机和列表外的主机访问互联网

----完成

## 验证配置

在星期一~星期五的 8:00~18:00，局域网中，只有使用采购部门人员的电脑（IP 地址在 192.168.0.2~192.168.0.250 范围内）才能访问互联网，使用其他员工的电脑不能访问互联网。

## 9.4 端口过滤

### 9.4.1 概述

进入页面：点击「行为管理」>「端口过滤」。

互联网上众多服务所涉及的应用协议都有特定的端口号，从 0 到 1023 是常用服务的端口号，这些端口号一般固定分配给特定的服务。

端口过滤通过禁止用户对互联网上指定端口的访问，以此来控制用户访问的互联网服务类型。

端口过滤功能默认关闭，开启后，页面显示如下：



#### 参数说明

标题项	说明
端口过滤	端口过滤功能开关。  表示关闭，  表示开启。
IP 组	选择引用的 IP 组，以指定规则对应的用户。 IP 组应事先已在「行为管理」>「IP 组与时间组」页面配置好。
时间组	选择引用的时间组，以指定规则对应的生效时间。 时间组应事先已在「行为管理」>「IP 组与时间组」页面配置好。
端口	禁止访问的服务使用的 TCP 或 UDP 端口号。

标题项	说明
协议	禁止访问的服务使用的协议。“全部”表示 TCP 和 UDP。
生效开关	规则的状态，可根据需要启用或禁用。
操作	<p>可对规则进行如下操作：</p> <ul style="list-style-type: none"> <li>- 点击  可以修改规则。</li> <li>- 点击  可以删除规则。</li> </ul>

## 9.4.2 新增端口过滤规则

**步骤 1** 开启端口过滤功能；

1. 点击「行为管理」>「端口过滤」；
2. 端口过滤：点击滑块至 ；
3. 点击页面底端的 **保存**。



**步骤 2** 添加端口过滤规则。

1. 点击 **+新增**；



2. 在【新增】窗口配置各项参数；
3. 点击 **保存**。

新增

IP组/用户组：

时间组：所有时间

端口：

协议：全部

保存 取消

---完成

### 9.4.3 端口过滤配置举例

#### 组网需求

某企业使用路由器进行网络搭建。要求：上班时间（周一到周五的 8:00~18:00），禁止采购部门员工浏览网页（浏览网页服务默认的端口号是 80）。

#### 方案设计

可以使用路由器的端口过滤功能实现上述需求。假设采购部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.250。

#### 配置步骤

**步骤 1** 配置时间组；

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。

新增

组名称：

时间： :  ~  :

日期： 每天     星期日     星期一  
 星期二     星期三     星期四  
 星期五     星期六

**步骤 2** 配置 IP 组；

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

新增

组名称：

IP地址段： ~

**步骤 3** 开启端口过滤功能；

1. 点击「行为管理」>「端口过滤」；
2. 端口过滤：点击滑块至 ；
3. 点击页面底端的 。



#### 步骤 4 添加端口过滤规则。

1. 点击 **+新增** ；



2. 在【新增】窗口配置各项参数；
  - (1) IP 组/用户组：选择规则生效的 IP 组，本例为“采购部”。
  - (2) 时间组：选择规则生效的时间组，本例为“上班时间”。
  - (3) 端口：输入浏览网页服务使用的端口号“80”。
  - (4) 协议：保持默认“全部”。

3. 点击 **保存** 。



----完成

添加成功，如下图示：



## 验证配置

在星期一~星期五的 8:00~18:00，局域网中，IP 地址在 192.168.0.2~192.168.0.250 范围内的电脑不能浏览网页。

## 9.5 应用过滤

### 9.5.1 概述

进入页面：点击「行为管理」>「应用过滤」。

使用应用过滤功能，可以禁止局域网的用户使用指定的应用，如聊天应用、视频影音、音乐盒子等，有效提升员工的工作效率。

应用过滤功能默认关闭，开启后，页面显示如下：



#### 参数说明

标题项	说明
IP 组	选择引用的 IP 组，以指定规则对应的用户。 IP 组应事先已在「行为管理」>「IP 组与时间组」页面配置好。
应用过滤	选择引用的时间组，以指定规则对应的生效时间。 时间组应事先已在「行为管理」>「IP 组与时间组」页面配置好。
过滤应用	规则对应的应用的类别。

标题项	说明
生效开关	规则的状态，可根据需要启用或禁用。
操作	可对规则进行如下操作： <ul style="list-style-type: none"> <li>- 点击  可以修改规则。</li> <li>- 点击  可以删除规则。</li> </ul>
例外 QQ 号	允许进行正常通讯的 QQ 号码。
备注	该例外 QQ 号的描述，如“zhangsan”。可不填。
例外 QQ 号	可对规则进行如下操作： <ul style="list-style-type: none"> <li>- 点击  可以修改规则。</li> <li>- 点击  可以删除规则。</li> </ul>

## 9.5.2 新增应用过滤规则

**步骤 1** 开启应用过滤功能；

1. 点击「行为管理」>「应用过滤」；
2. 应用过滤：点击滑块至 ；
3. 点击页面底端的 **保存**。



**步骤 2** 添加应用过滤规则。

1. 点击 **+新增**；



2. 在【新增过滤规则】窗口配置各项参数；
3. 点击 **保存**。



---完成

## 9.5.3 新增例外 QQ 号

**步骤 1** 开启应用过滤功能；

1. 点击「行为管理」>「应用过滤」；
2. 应用过滤：点击滑块至 ；
3. 点击页面底端的 **保存**。



**步骤 2** 添加例外 QQ 号。

1. 点击 **+新增例外 QQ 号**；



2. 在【新增例外 QQ 号】窗口配置各项参数；
3. 点击 **保存**。



----完成

## 9.5.4 应用过滤+QQ 过滤配置举例

### 组网需求

某企业使用路由器进行网络搭建。要求：上班时间（周一到周五的 8:00~18:00），采购部门员工不能：

- 使用这些应用：聊天、视频、音乐、金融、购物、社交、婚恋、手机游戏、网络游戏、对战平台。
- 使用 QQ，但允许技术支持人员使用 QQ 与客户沟通。假设该员工的 QQ 号为 12345678。

### 方案设计

可以使用路由器的应用过滤功能实现上述需求。假设采购部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.250。

### 配置步骤

#### 步骤 1 配置时间组；

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。



新增

组名称： 上班时间

时间： 8 : 00 ~ 18 : 00

日期：  
 每天     星期日     星期一  
 星期二     星期三     星期四  
 星期五     星期六

保存 取消

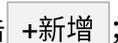
#### 步骤 2 配置 IP 组；

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

**步骤 3** 开启应用过滤功能；

1. 点击「行为管理」>「应用过滤」；
2. 应用过滤：点击滑块至 ；
3. 点击页面底端的 。

**步骤 4** 添加应用过滤规则；

1. 点击 ；

2. 在【新增过滤规则】窗口配置各项参数；

- (1) IP 组/用户组：选择需要限制网络应用的 IP 组，本例为“采购部”。
- (2) 时间组：选择规则生效的时间组，本例为“上班时间”。
- (3) 备注：设置规则备注信息，可不填。

- (4) 过滤应用：在“应用类别”栏选择聊天、视频、音乐、金融、购物、社交、婚恋、手机游戏、网络游戏、对战平台。

3. 点击 **保存**。



新增过滤规则

IP组/用户组： 采购部

时间组： 上班时间

备注： 可不填

过滤应用：

应用类别	请选择
<input checked="" type="checkbox"/> 音乐	<input checked="" type="checkbox"/> 浩方对战平台 <input checked="" type="checkbox"/> QQ游戏
<input checked="" type="checkbox"/> 金融	<input checked="" type="checkbox"/> 联众世界 <input checked="" type="checkbox"/> 中国游戏中心
<input checked="" type="checkbox"/> 购物	<input checked="" type="checkbox"/> 11对战平台 <input checked="" type="checkbox"/> 波克城市
<input type="checkbox"/> 新闻	<input checked="" type="checkbox"/> VS对战平台
<input checked="" type="checkbox"/> 社交	
<input checked="" type="checkbox"/> 婚恋	
<input checked="" type="checkbox"/> 手机游戏	
<input checked="" type="checkbox"/> 网络游戏	
<input checked="" type="checkbox"/> 对战平台	
<input type="checkbox"/> 下载	

**保存** **取消**

**步骤 5** 添加例外 QQ 号。

1. 点击 **+新增例外 QQ 号**；



+新增例外QQ号 删除

例外QQ号	备注	操作
-------	----	----

2. 在【新增例外 QQ 号】窗口配置各项参数；

- (1) QQ 号码：输入可以正常使用的 QQ 号码，本例为“12345678”。
- (2) 备注：输入 QQ 号码的备注信息，如“技术支持”。

3. 点击 **保存**。

新增例外QQ号
✕

---

QQ号码	备注	操作
12345678	技术支持	<input type="button" value="+"/> <input type="button" value="-"/>

----完成

添加成功，如下图示：

### 应用过滤

应用过滤：

<input type="checkbox"/>	IP组	时间组	过滤应用	生效开关	操作
<input type="checkbox"/>	采购部	上班时间	腾讯QQ, 腾讯TM, QT语音, 飞信, 阿里旺旺	<input checked="" type="checkbox"/>	✎ 删除

注意：如果规则有重复或有交集，则先配置的规则生效，后配置的规则无效。

<input type="checkbox"/>	例外QQ号	备注	操作
<input type="checkbox"/>	12345678	技术支持	删除

## 验证配置

局域网中 IP 地址在 192.168.0.2~192.168.0.250 范围内的电脑在星期一到星期五的 8:00-18:00 不能使用聊天、视频、音乐、金融、购物、社交、婚恋、手机游戏、网络游戏、对战平台等应用，不能使用 QQ。只有 12345678 的 QQ 号可以正常使用。

## 9.6 网站过滤

### 9.6.1 概述

进入页面：点击「行为管理」>「网站过滤」。

使用网站过滤，禁止局域网用户访问指定类别网址，可以规范局域网用户上网行为，提升员工工作效率。路由器的特征库默认添加了多个类别的网站，如果需要，用户可以自定义新增分类。

网站过滤功能默认关闭，开启后，页面显示如下：



#### 参数说明

标题项	说明
网站过滤	网站过滤功能开关。  表示关闭，  表示开启。
过滤方式	网站过滤规则的类型。 <ul style="list-style-type: none"><li>- 白名单：即，允许访问互联网。允许 IP 组内的用户在对应时间段内访问指定的网站，不能访问其他网站；在其他时间段内可以访问所有网站。</li><li>- 黑名单：即，禁止访问互联网。禁止 IP 组内的用户在对应时间段内访问指定的网站，可以访问其他网站；在其他时间段内可以访问所有网站。</li></ul>
IP 组	选择引用的 IP 组，以指定规则对应的用户。 IP 组应事先已在「行为管理」>「IP 组与时间组」页面配置好。

标题项	说明
时间组	选择引用的时间组，以指定规则对应的生效时间。 时间组应事先已在「行为管理」>「IP 组与时间组」页面配置好。
过滤网站类型	规则对应的网址分类。
生效开关	规则的状态，可根据需要启用或禁用。
操作	可对规则进行如下操作： - 点击  可以修改规则。 - 点击  可以删除规则。

## 9.6.2 新增网站过滤规则

**步骤 1** 开启网站过滤功能；

1. 点击「行为管理」>「网站过滤」；
2. 网站过滤：点击滑块至 ；
3. 点击页面底端的 **保存**。



**步骤 2** 添加网站过滤规则。

1. 点击 **+新增**；



2. 在【新增】窗口配置各项参数；
3. 点击 **保存**。

新增 ×

---

过滤模式：  
 白名单（允许访问互联网）  
 黑名单（禁止访问互联网）

IP组/用户组：

时间组：

备注：

网址：

网址类别	请选择	全选 反选
<input type="checkbox"/> 休闲娱乐	<input type="checkbox"/> 音乐网站	<input type="checkbox"/> 娱乐时尚
<input type="checkbox"/> 购物网站	<input type="checkbox"/> 游戏网站1	<input type="checkbox"/> 游戏网站2
<input type="checkbox"/> 政府组织	<input type="checkbox"/> 游戏网站3	<input type="checkbox"/> 图片摄影
<input type="checkbox"/> 综合其他	<input type="checkbox"/> 星座运势	<input type="checkbox"/> 视频电影1
<input type="checkbox"/> 教育文化	<input type="checkbox"/> 视频电影2	<input type="checkbox"/> 小说网站1
<input type="checkbox"/> 行业企业	<input type="checkbox"/> 小说网站2	<input type="checkbox"/> 幽默笑话
<input type="checkbox"/> 生活服务	<input type="checkbox"/> 收藏爱好	<input type="checkbox"/> 动漫网站
<input type="checkbox"/> 网络科技	<input type="checkbox"/> 明星粉丝	
<input type="checkbox"/> 体育健身		

**保存**

----完成

### 9.6.3 自定义网址组

**步骤 1** 开启网站过滤功能；

1. 点击「行为管理」>「网站过滤」；
2. 网站过滤：点击滑块至 ；
3. 点击页面底端的 **保存**。



**步骤 2** 添加网址组。

1. 点击 **网址管理** ；



2. 点击 **新增** ；



3. 在【新增】窗口配置各项参数；
4. 点击 **保存** 。

新增 ×

---

组名称：

网址：

备注：

---完成

## 9.6.4 网站过滤配置举例

### 组网需求

某企业使用路由器进行网络搭建。要求：上班时间（周一到周五的 8:00~18:00），采购部门人员只能访问网络科技网站，不能访问其他类型网站。

### 方案设计

可以使用路由器的网站过滤功能实现上述需求。假设采购部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.250。

### 配置步骤

**步骤 1** 配置时间组；

进入「行为管理」>「IP 组与时间组」页面，配置如下时间组。

新增

组名称：

时间： :  ~  :

日期： 每天  星期日  星期一  
 星期二  星期三  星期四  
 星期五  星期六

**步骤 2** 配置 IP 组；

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

新增

组名称：

IP地址段： ~

**步骤 3** 开启网站过滤功能；

1. 点击「行为管理」>「网站过滤」；
2. 网站过滤：点击滑块至 ；
3. 点击页面底端的 。



#### 步骤 4 添加网站过滤规则。

1. 点击 **+新增** ；



2. 在【新增】窗口配置各项参数；
  - (1) 过滤模式：选择“白名单（允许访问互联网）”。
  - (2) IP 组/用户组：选择需要限制网络应用的 IP 组，本例为“采购部”。
  - (3) 时间组：选择规则生效的时间组，本例为“上班时间”。
  - (4) 备注：设置规则备注信息，可不填。
  - (5) 过滤应用：选择要过滤的网址类型，本例为“网络科技”。
3. 点击 **保存**。

新增
✕

---

过滤模式：  
 白名单（允许访问互联网）  
 黑名单（禁止访问互联网）

IP组/用户组：

时间组：

备注：

网址：

网址类别	请选择 <span style="float: right;">全选 反选</span>
<input type="checkbox"/> 休闲娱乐	<input checked="" type="checkbox"/> 应用工具
<input type="checkbox"/> 购物网站	<input checked="" type="checkbox"/> 软件下载
<input type="checkbox"/> 政府组织	<input checked="" type="checkbox"/> 设计素材
<input type="checkbox"/> 综合其他	<input checked="" type="checkbox"/> 网络安全
<input type="checkbox"/> 教育文化	<input checked="" type="checkbox"/> 邮件通信
<input type="checkbox"/> 行业企业	<input checked="" type="checkbox"/> 手机数码
<input type="checkbox"/> 生活服务	<input checked="" type="checkbox"/> 广告联盟
<input checked="" type="checkbox"/> 网络科技	<input checked="" type="checkbox"/> 电商服务
<input type="checkbox"/> 体育健身	<input checked="" type="checkbox"/> 电脑硬件
<input type="checkbox"/> 医疗健康	<input checked="" type="checkbox"/> 技术编程
	<input checked="" type="checkbox"/> 域名主机
	<input checked="" type="checkbox"/> 网络硬盘
	<input checked="" type="checkbox"/> 站长资源
	<input checked="" type="checkbox"/> 电子支付
	<input checked="" type="checkbox"/> 数据分析
	<input checked="" type="checkbox"/> 创业投资

保存
取消

----完成

添加成功，如下图示：

**网站过滤**

网站过滤：

+新增
🗑️删除

过滤方式	IP组	时间组	过滤网站类型	生效开关	操作
<input checked="" type="checkbox"/> 白名单	采购部	上班时间	应用工具, 电脑硬件, 软件下载, 技术编程,...	<input checked="" type="checkbox"/>	<span>✎</span> <span>🗑️</span>

## 验证配置

局域网中 IP 地址在 192.168.0.2~192.168.0.250 范围内的电脑在星期一到星期五的 8:00-18:00 只能访问路

由器中“网络科技”包含的网站，不能访问其他网站。

## 9.7 多 WAN 策略

### 9.7.1 概述

路由器默认启用 1 个 WAN 口，最多支持 2 个 WAN 口。当 2 个 WAN 口同时工作时，合理的设置多 WAN 策略可以大幅提升路由器的带宽利用率。路由器支持两种多 WAN 策略，用户可以根据需要自行选择。

进入页面：点击「行为管理」>「多 WAN 策略」。

### 多WAN策略

多WAN策略：  
 智能负载均衡  
 自定义

---

#### 广域网线路检测

广域网线路检测：  
 启用  禁用

检测地址：

检测间隔：  
 分（范围：1-200）

#### 参数说明

标题项	说明
多 WAN 策略	<p>路由器多 WAN 口同时工作时采用的数据转发策略。</p> <ul style="list-style-type: none"><li>- 智能负载均衡：系统自动寻找流量最小的 WAN 口通信，完全不用人工干预，自动分配流量。</li><li>- 自定义：用户根据实际需要，将特定源 IP 地址的流量指定由特定 WAN 口进行转发。</li></ul>
广域网线路检测	<p>启用后，路由器会定期检测 WAN 口与“检测地址”的连通情况。</p> <ul style="list-style-type: none"><li>- 检测地址：需检测的目标主机的 IP 地址或域名。</li><li>- 检测间隔：执行广域网线路检测的时间间隔，默认为 5 分钟检测一次。</li></ul>

## 9.7.2 自定义多 WAN 策略

**步骤 1** 开启自定义多 WAN 策略功能；

1. 点击「行为管理」>「多 WAN 策略」；
2. 选择“自定义”；
3. 点击页面底端的 **保存**。



**步骤 2** 自定义多 WAN 策略规则。

1. 点击 **+新增**；



2. 在【新增】窗口配置各项参数；
3. 点击 **保存**。

新增

生效开关：

IP组：

WAN口： WAN1  WAN2

保存 取消

---完成

#### 参数说明

标题项	说明
生效开关	是否启用该规则。
IP 组	选择引用的 IP 组，以指定规则对应的用户。IP 组应事先在「行为管理」>「IP 组与时间组」页面配置。
WAN 口	对应 IP 组数据流量使用的 WAN 口。

### 9.7.3 自定义多 WAN 策略配置举例

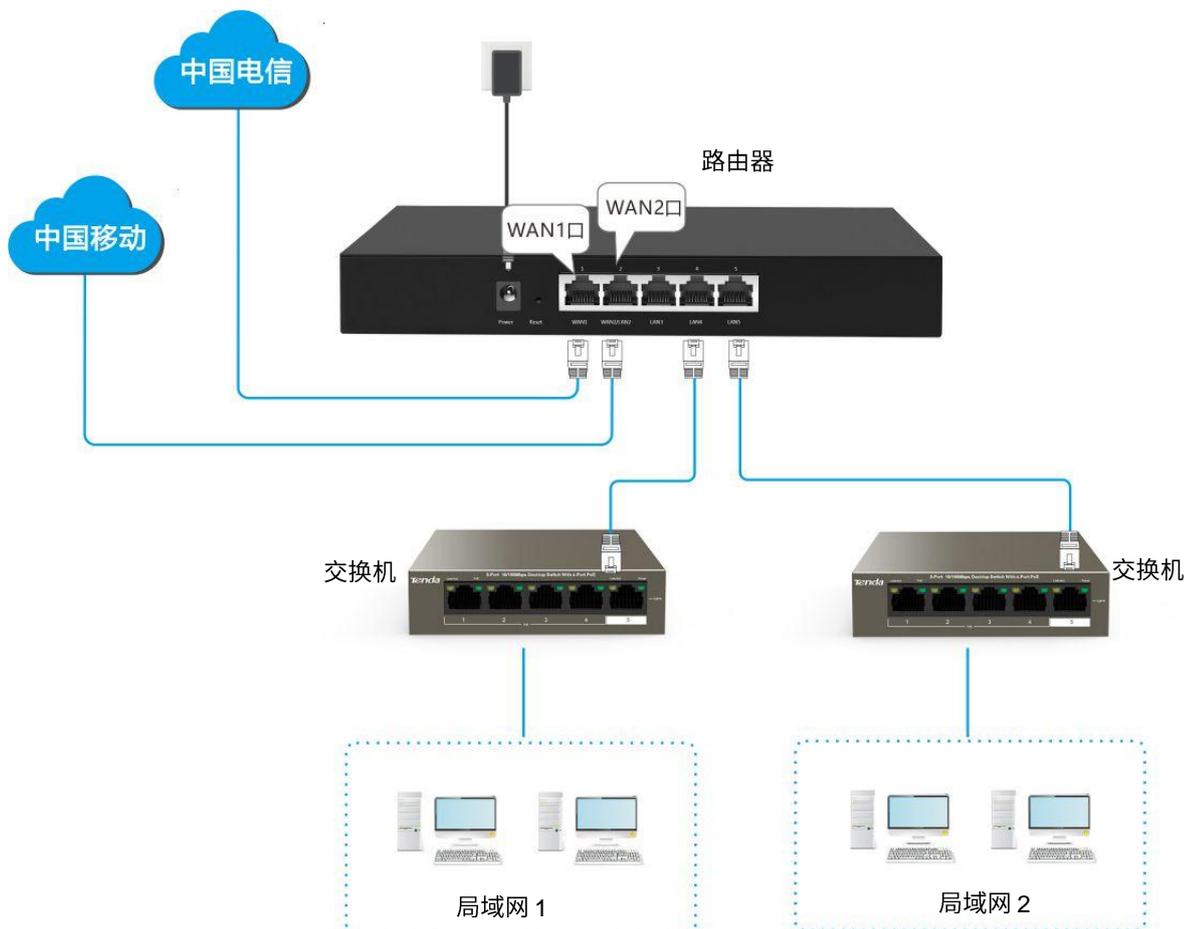
#### 组网需求

某企业使用路由器进行网络搭建，为了满足企业网络需求，办理了两条宽带线路（中国电信和中国移动），并且已经成功访问互联网。为了实现负载均衡，现要求局域网中：

- 局域网 1：IP 地址为 192.168.0.2~192.168.0.100 的设备通过电信宽带访问互联网。
- 局域网 2：IP 地址为 192.168.0.101~192.168.0.250 的设备通过移动宽带访问互联网。

#### 方案设计

可以使用路由器的多 WAN 策略功能实现上述需求。



## 配置步骤

### 步骤 1 配置 IP 组；

进入「行为管理」>「IP 组与时间组」页面，配置如下 IP 组。

IP组设置		
<input type="button" value="+新增"/> <input type="button" value="删除"/>		
IP组	IP地址段	操作
<input type="checkbox"/> IP组1	192.168.0.2~192.168.0.100	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> IP组2	192.168.0.101~192.168.0.250	<input type="button" value="编辑"/> <input type="button" value="删除"/>

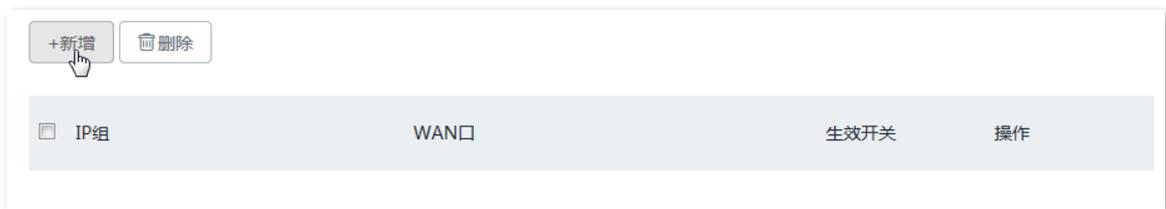
### 步骤 2 开启自定义多 WAN 策略功能；

1. 点击「行为管理」>「多 WAN 策略」；
2. 选择“自定义”；
3. 点击页面底端的 **保存**。



### 步骤 3 自定义多 WAN 策略规则。

1. 点击 **+新增** ；



2. 在【新增】窗口配置各项参数；
  - (1) IP 组：选择规则生效的 IP 组，本例为“IP 组 1”。
  - (2) WAN 口：选择该 IP 组数据流量使用的 WAN 口，本例为“WAN1”。
3. 点击 **保存**。



4. 重复步骤 1~2，添加 IP 组 2 的 WAN 口策略。

---完成

添加成功，如下图示：



## 验证配置

局域网中 IP 地址在 192.168.0.2~192.168.0.100 范围内的设备访问外网时，数据流量由 WAN1 口转发；局域网中 IP 地址在 192.168.0.101~192.168.0.250 范围内的设备访问外网时，数据流量由 WAN2 口转发。

# 10 VPN

## 10.1 概述

VPN (Virtual Private Network, 虚拟专用网), 是一个建立在公用网 (通常是互联网) 上的专用网络, 这个专用网络只在逻辑上存在, 并没有实际物理线路。使用 VPN 技术, 可以让企业的分公司员工在方便共享对方或公司总部局域网资源的同时, 保证这些资源不会暴露给互联网上的其他用户。

本系列路由器支持两种 VPN: PPTP、L2TP, 可以作为 PPTP/L2TP 客户端连接到 PPTP/L2TP 服务器端。

进入页面: 点击「VPN」>「PPTP/L2TP 客户端」。PPTP/L2TP 客户端默认禁用, 启用后, 页面显示如下:

### PPTP/L2TP客户端

PPTP/L2TP客户端:

客户端类型:  PPTP  L2TP

WAN口:  WAN1  WAN2

服务器IP地址/域名:

用户名:

密码:

加密:  启用  禁用

VPN代理上网:  启用  禁用

服务器内网网段:

服务器内网子网掩码:

状态: 未连接

## 参数说明

标题项	说明
PPTP/L2TP 客户端	<p>PPTP/L2TP 客户端功能开关。 表示关闭， 表示开启。</p> <p>开启后，路由器作为 PPTP/L2TP VPN 客户端。</p> <p>PPTP (Point to Point Tunneling Protocol, 点到点隧道协议) 和 L2TP (Layer 2 Tunneling Protocol, 第二层隧道协议) 都是二层 VPN 隧道协议, 使用 PPP (Point to Point Protocol, 点到点协议) 进行数据封装, 并都为数据增添额外首部。</p>
客户端类型	<p>路由器充当的客户端类型, PPTP 或 L2TP。</p> <ul style="list-style-type: none"><li>- PPTP: 要连接的 VPN 服务器是 PPTP 服务器时, 选择此项。</li><li>- L2TP: 要连接的 VPN 服务器是 L2TP 服务器时, 选择此项。</li></ul>
WAN 口	选择路由器进行 VPN 拨号时使用的 WAN 口。
服务器 IP 地址/域名	要拨入的 VPN 服务器的 IP 地址或域名, 一般是对端 VPN 路由器上开启了“PPTP/L2TP 服务器”功能的 WAN 口的 IP 地址或域名。
用户名	输入 PPTP/L2TP 用户账号, 即, VPN 服务器分配的用户名和密码。
密码	
加密	根据 VPN 服务器配置选择是否启用数据加密。请和服务器配置保持一致, 否则不能正常通信。只有 PPTP VPN 才支持此选项, L2TP VPN 不支持。
VPN 代理上网	启用后, 局域网内的用户通过 PPTP/L2TP 服务器端路由器上网。
服务器内网网段	PPTP/L2TP 服务器端局域网的网段。
服务器内网子网掩码	PPTP/L2TP 服务器端局域网的子网掩码。
状态	显示当前 VPN 的连接状态。

## 10.2 配置 PPTP/L2TP 客户端

**步骤 1** 点击「VPN」>「PPTP/L2TP 客户端」；

**步骤 2** PPTP/L2TP 客户端：点击滑块至 ；

**步骤 3** 配置各项参数；

**步骤 4** 点击 **保存**。

### PPTP/L2TP客户端

PPTP/L2TP客户端：

客户端类型： PPTP  L2TP

WAN口： WAN1  WAN2

服务器IP地址/域名：

用户名：

密码：

加密： 启用  禁用

VPN代理上网： 启用  禁用

服务器内网网段：

服务器内网子网掩码：

状态：未连接

----完成

## 10.3 PPTP/L2TP 客户端配置举例

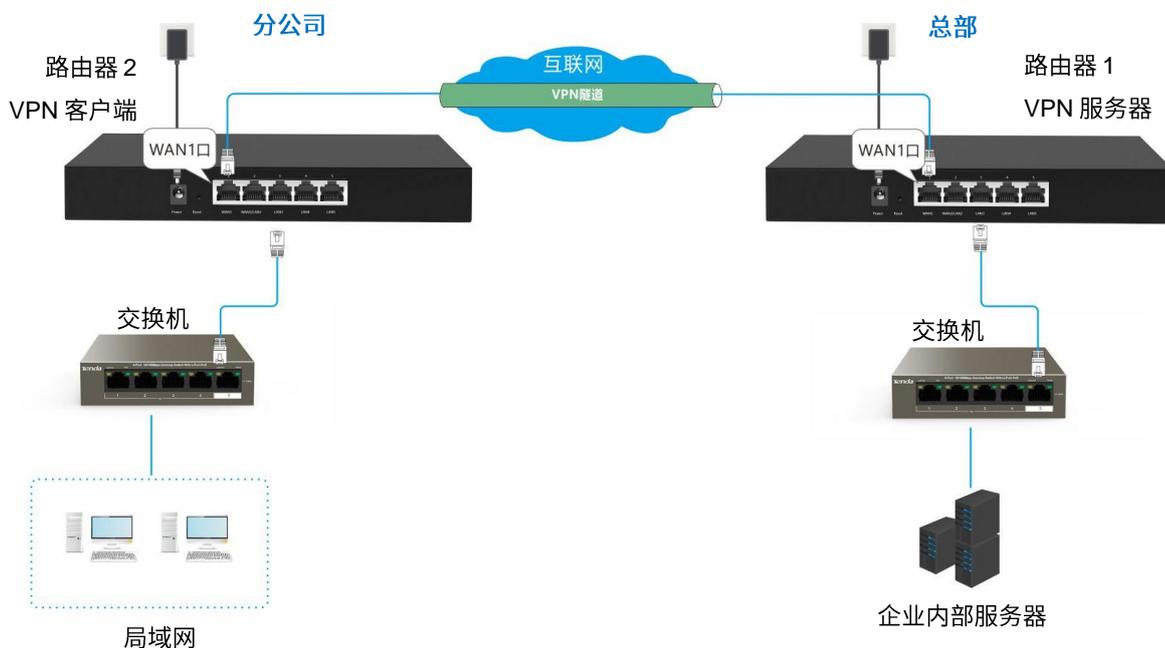
### 组网需求

某企业使用路由器进行网络搭建，并成功接入互联网。各地分公司员工需要访问公司内部局域网资源，如，内部资料、办公 OA 等。

### 方案设计

可在路由器上设置 VPN 服务，实现远端用户经互联网安全访问企业内部局域网的需求。本例以 PPTP VPN 为例说明，L2TP VPN 的设置方法类似。假设基本信息如下：

- VPN 服务器分配的用户名、密码均为 fengongsi1。
- VPN 服务器 IP 地址为 202.105.11.22。
- VPN 服务器对数据启用加密。
- VPN 服务器内网为 192.168.1.0/24。
- VPN 服务器内网子网掩码为 255.255.255.0。
- 本路由器与 VPN 服务器建立隧道的接口为 WAN1。



### 配置步骤

**步骤 1** 点击「VPN」>「PPTP/L2TP 客户端」；

**步骤 2** PPTP/L2TP 客户端：点击滑块至 ；

### 步骤 3 配置各项参数；

- (1) 客户端类型：和 VPN 服务器侧保持一致，本例为“PPTP”。
- (2) WAN 口：指定 VPN 客户端与服务器建立隧道的出口，本例为“WAN1”。
- (3) 服务器 IP 地址/域名：输入 VPN 服务器侧作为隧道出口的 WAN 口的 IP 地址，本例为“202.105.11.22”。
- (4) 用户名/密码：输入 VPN 服务器分配的用户名和密码，本例中均为“fengongsi1”。
- (5) 加密：选择“启用”，和 VPN 服务器侧配置保持一致。
- (6) VPN 代理上网：选择“禁用”。
- (7) 服务器内网网段：输入 VPN 服务器内网的网段，本例为“192.168.1.0”。
- (8) 内网子网掩码：输入 VPN 服务器内网的子网掩码，本例为“255.255.255.0”。

### 步骤 4 点击 **保存**。

#### PPTP/L2TP客户端

PPTP/L2TP客户端：

客户端类型： PPTP  L2TP

WAN口： WAN1  WAN2

服务器IP地址/域名：

用户名：

密码：

加密： 启用  禁用

VPN代理上网： 启用  禁用

服务器内网网段：

服务器内网子网掩码：

状态：未连接

----完成

## 验证配置

当页面的状态显示为“已连接”且已经获取 IP 地址时，VPN 连接成功。如下图示。



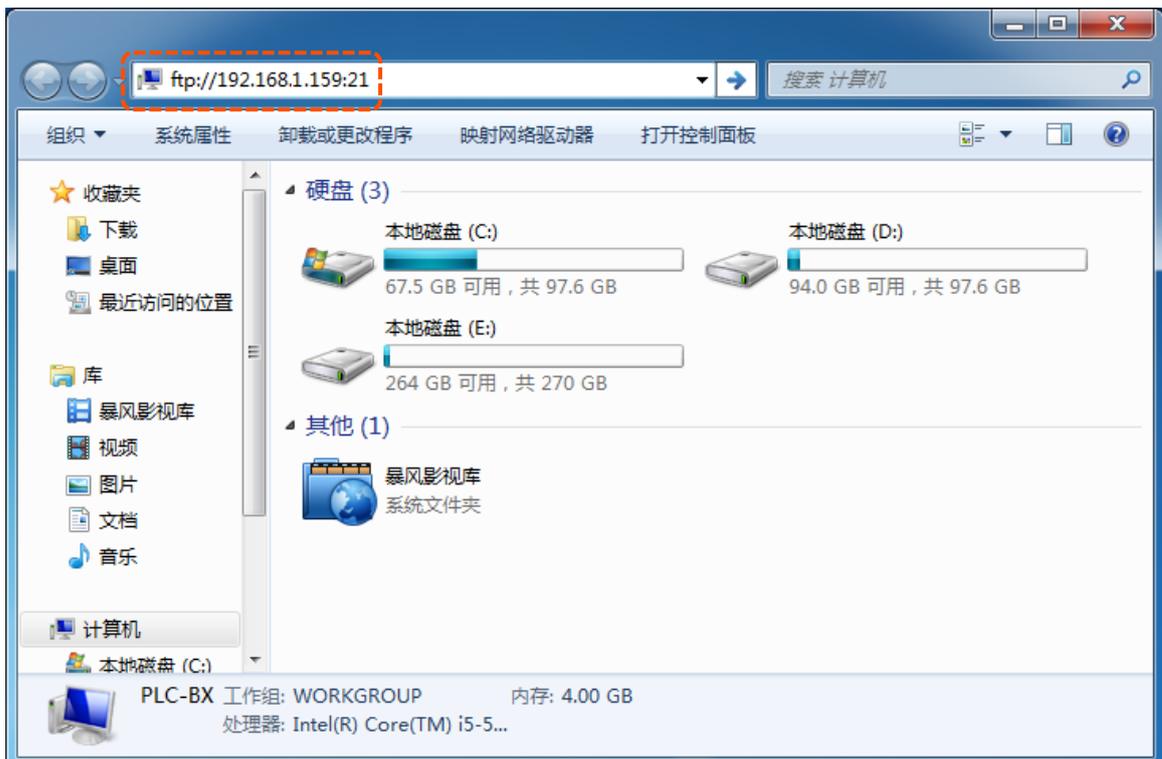
之后，分公司和总部的员工就可以通过互联网安全访问对方的局域网资源了。

下文以分公司访问总部 FTP 服务器为例。公司总部的项目资料放在 FTP 服务器中，假设服务器信息如下：

- FTP 服务器 IP 地址：192.168.1.159
- 服务器端口：21
- 登录用户名/密码：admin/admin

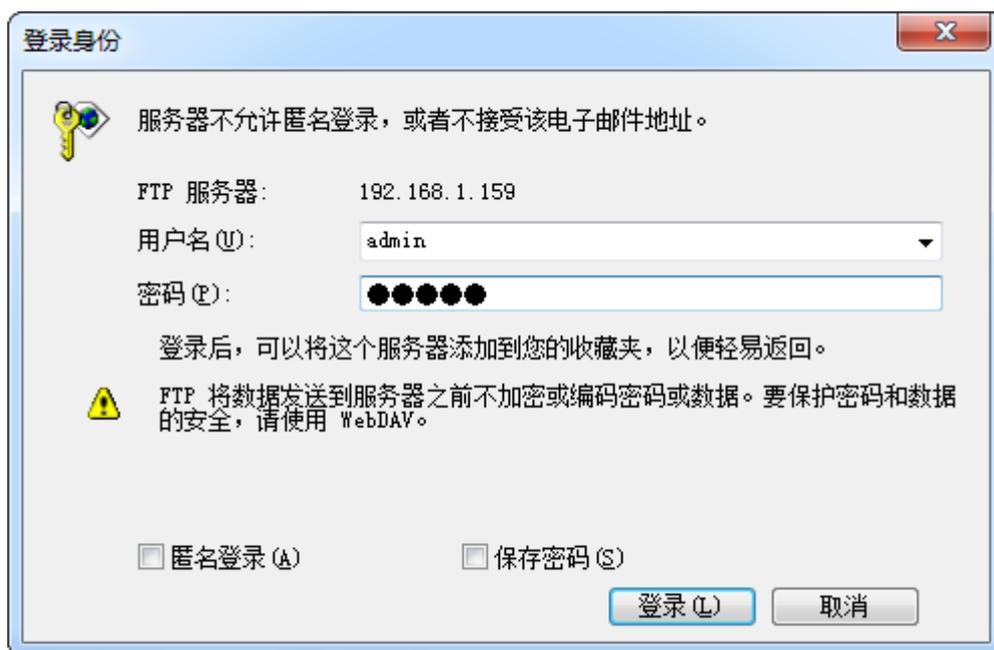
当分公司员工访问总部项目资料时，步骤如下：

**步骤 1** 在电脑上访问“ftp://服务器 IP 地址:服务端口号”，本例为 <ftp://192.168.1.159:21>；

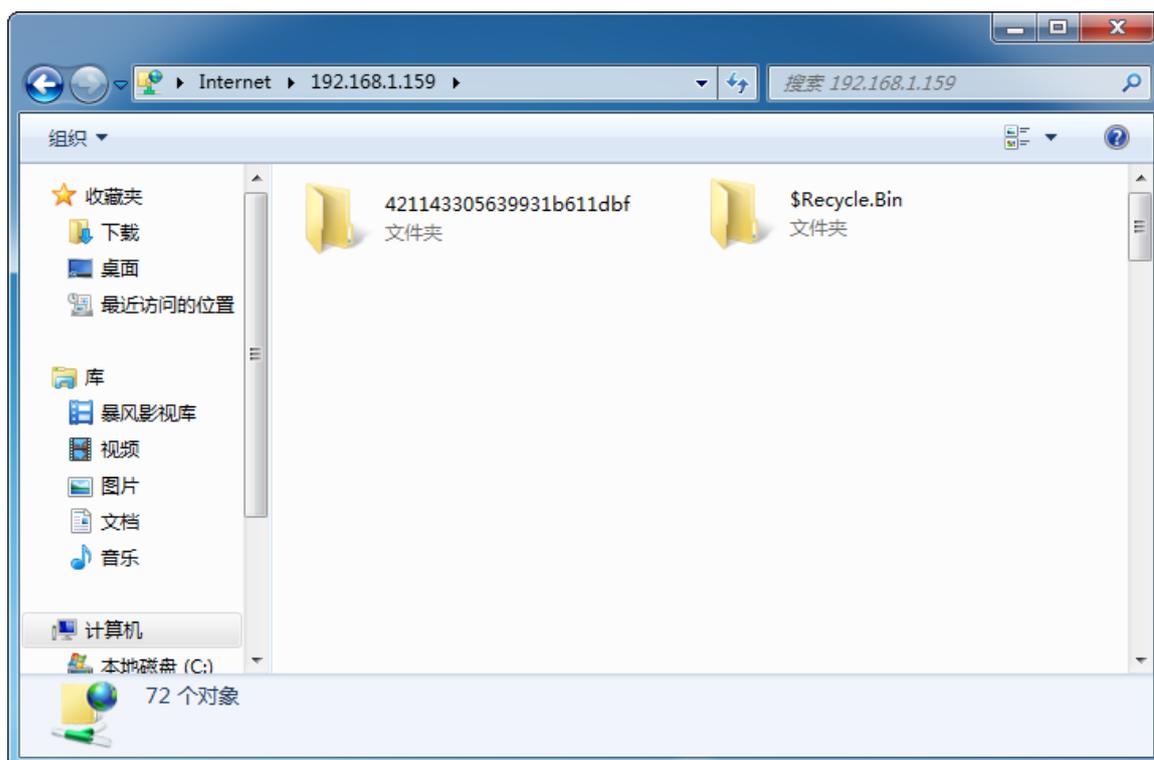


**步骤 2** 在弹出的窗口输入登录用户名和密码，本例均为“admin”；

**步骤 3** 点击 **登录**。



访问成功。



# 11 更多设置

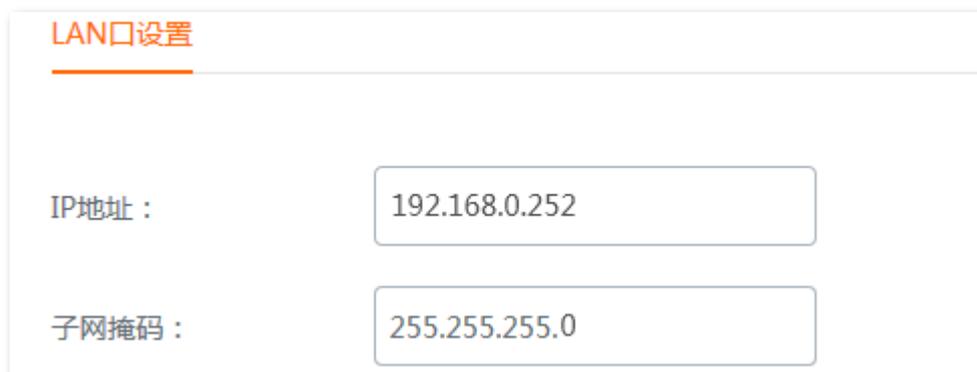
路由器的「更多设置」模块包括：[局域网设置](#)、[WAN 口参数](#)、[静态路由](#)、[端口镜像](#)、[远程 WEB 管理](#)、[DDNS](#)、[端口映射](#)、[DMZ 主机](#)、[UPnP](#)、[DNS 劫持](#)、[DNS 缓存](#)、[攻击防御](#)。

## 11.1 局域网设置

进入页面：点击「网络设置」>「局域网设置」。在这里，您可以设置路由器的 LAN 口 IP 地址、DHCP 服务器和静态地址分配等参数。

### 11.1.1 LAN 口设置

LAN 口 IP 地址是路由器对局域网的 IP 地址，也是路由器的管理 IP 地址。路由器默认的 LAN 口 IP 为 192.168.0.252，子网掩码为 255.255.255.0。



LAN口设置

IP地址： 192.168.0.252

子网掩码： 255.255.255.0

一般情况下，您无需修改 LAN 口设置，除非遇到 IP 地址冲突，如：路由器获得的 WAN 口 IP 和其 LAN 口 IP 处于同一网段；局域网内，有其它设备的 IP 地址也为 192.168.0.252。

修改 LAN 口 IP 后，系统出现如下提示。



提示

正在修改LAN口IP地址，修改成功后，将自动跳转到登录页面 6.67%

进度条走完后，系统将自动重新登录。如果没有，请确保电脑的本地连接 IP 地址设置为“自动获得”，之后使用新的 LAN 口 IP 地址重新尝试。



如果新的 LAN 口 IP 与原 LAN 口 IP 不在同一网段，系统将自动匹配修改 DHCP 地址池，使其和新的 LAN 口 IP 在同一网段。

## 11.1.2 DHCP 服务器

### 概述

DHCP 服务器能自动给局域网用户分配 IP 地址、子网掩码、网关地址、DNS 等上网信息。如果关闭该功能，需要在局域网设备上手动配置 IP 地址信息才能实现上网。如无特殊情况，请保持 DHCP 服务器为开启状态。

### DHCP服务器

DHCP服务器：

起始IP地址：192.168.  .

结束IP地址：192.168.  .

租约时间：

首选DNS服务器：

备用DNS服务器： (可选)

### 参数说明

标题项	说明
DHCP 服务器	DHCP 服务器功能开关。 <input type="checkbox"/> 表示关闭， <input checked="" type="checkbox"/> 表示开启。

标题项	说明
起始 IP 地址	DHCP 服务器可分配的 IP 地址范围，起始 IP 地址默认为 192.168.0.100，结束 IP 地址默认为 192.168.0.200。
结束 IP 地址	
租约时间	<p>DHCP 服务器所分配给局域网设备的 IP 地址的有效时间。当地址到期后：</p> <ul style="list-style-type: none"> <li>- 如果设备仍连接在路由器上，设备将自动续约，继续占用该 IP 地址。</li> <li>- 如果设备未连接（关机、网线已拔掉、无线已断开等）到路由器，路由器将释放该 IP。以后若有其它设备请求 IP 地址信息，路由器可将该 IP 分配给其它设备。</li> </ul> <p>如无特殊需要，建议保持默认设置。</p>
首选 DNS 服务器	<p>DHCP 服务器分配给局域网设备的首选 DNS 服务器 IP 地址。路由器支持 DNS 代理功能，故首选 DNS 默认为路由器的 LAN 口 IP 地址。</p> <p> <b>提示</b></p> <p>一般情况下，建议保持默认设置。如需修改，为了使局域网设备能够正常上网，请务必确保修改的首选 DNS 是正确的 DNS 服务器或 DNS 代理的 IP 地址。</p>
备用 DNS 服务器	DHCP 服务器分配给局域网设备的备用 DNS 服务器 IP 地址。不填表示 DHCP 服务器不分配此项。

## 修改 DHCP 服务器

**步骤 1** 点击「更多设置」>「局域网设置」，转到“DHCP 服务器”模块；

**步骤 2** DHCP 服务器：点击滑块至 ；

**步骤 3** 起始/结束 IP 地址：设置 DHCP 服务器可分配给客户端的 IP 地址范围；

**步骤 4** 首选 DNS 服务器：可设置为路由器的 LAN 口 IP 地址或正确的 DNS 服务器地址；

**步骤 5** 点击页面底端的 **保存**。

### DHCP服务器

DHCP服务器：

起始IP地址：192.168.  .

结束IP地址：192.168.  .

租约时间：

首选DNS服务器：

备用DNS服务器： (可选)

----完成

## 11.1.3 静态地址分配

### 概述

通过静态地址分配，您可以让同一客户端始终获得固定的 IP 地址，避免路由器的“行为管理”、“网速控制”、“虚拟服务器”等功能因客户端 IP 地址变化而失效。本功能仅在路由器“DHCP 服务器”功能启用时生效。

- 在“静态地址分配-快速”模块，可以查看从路由器 DHCP 服务器自动获取 IP 地址的客户端信息，并一键绑定客户端，使 DHCP 服务器始终给同一客户端分配固定的 IP 地址。
- 在“静态地址分配-手动”模块可以手动绑定客户端，使 DHCP 服务器始终给同一客户端分配固定的 IP 地址。

### 情景 1：客户端当前已连接到路由器

客户端当前已连接到路由器时，推荐在“静态地址分配-快速”模块进行设置。

点击「更多设置」>「局域网设置」，转到“静态地址分配-快速”模块。

## 静态地址分配-快速

绑定已选

注意：静态地址分配规则将在终端设备下次连接路由器时生效。

<input type="checkbox"/>	IP地址	MAC地址	主机名称	IP-MAC绑定
<input type="checkbox"/>	192.168.0.133	1C:5C:F2:B4:40:08	Du	绑定
<input type="checkbox"/>	192.168.0.182	14:5F:94:BC:FC:83	HUAWEI_P10	绑定

## 参数说明

标题项	说明
<input type="checkbox"/>	将选中的客户端都进行 IP 地址、MAC 地址绑定。
IP 地址	客户端的 IP 地址。
MAC 地址	客户端的 MAC 地址。
主机名	客户端的名称。
IP-MAC 绑定	点击 <a href="#">绑定</a> 即可一键绑定客户端 IP 地址、MAC 地址，使客户端始终获取同一 IP 地址。绑定成功后将显示“已绑定”。

## 绑定单个客户端的 IP 地址

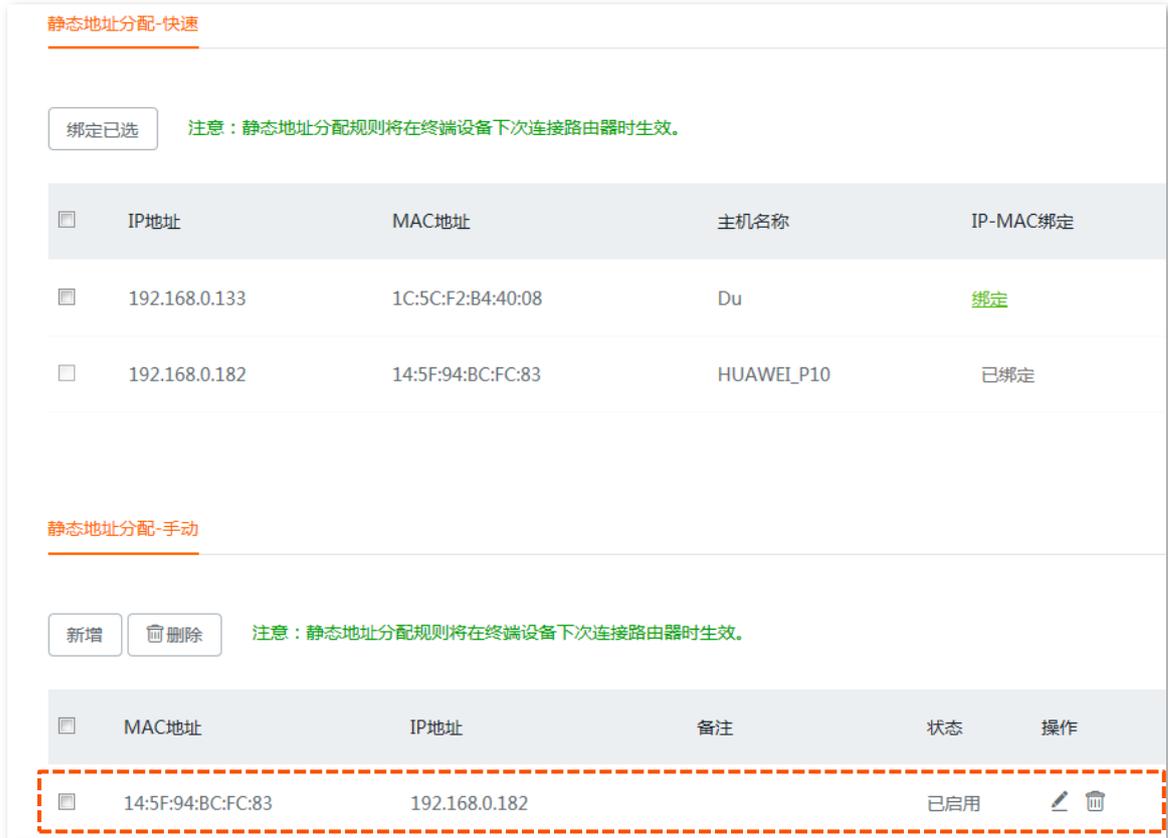
**步骤 1** 点击「更多设置」>「局域网设置」，转到“静态地址分配-快速”模块；

**步骤 2** 在“静态地址分配-快速”列表，找到要分配固定 IP 地址的客户端，点击[绑定](#)。



---完成

绑定成功后，您可以在「更多设置」>「局域网设置」的“静态地址分配-手动”页面查看到已添加的规则。如下图示例。



### 同时绑定多个客户端的 IP 地址

- 步骤 1** 点击「更多设置」>「局域网设置」，转到“静态地址分配-快速”模块；
- 步骤 2** 在“静态地址分配-快速”列表，选择多个要分配固定 IP 地址的客户端；
- 步骤 3** 然后点击 **绑定已选**。



---完成

绑定成功后，您可以在「更多设置」>「局域网设置」的“静态地址分配-手动”页面查看到已添加的规则。如下图示例。



## 情景 2：客户端未连接到路由器

客户端未连接到路由器时，请在“静态地址分配-手动”模块进行设置。

点击「更多设置」>「局域网设置」，转到“静态地址分配-手动”模块。



### 新增 IP 地址绑定规则

**步骤 1** 点击「更多设置」>「局域网设置」，转到“静态地址分配-手动”模块；

**步骤 2** 点击 **新增** ；



**步骤 3** 在【静态地址分配-手动】窗口配置各项参数；

**步骤 4** 点击 **保存**。



----完成

规则添加成功后，您可以在「更多配置」>「局域网设置」的“静态地址分配-手动”页面查看到已添加的规则。如下图示例。

如果需要添加多个客户端，重复**步骤 1~步骤 4**即可。



## 参数说明

标题项	说明
MAC 地址	客户端的 MAC 地址。
IP 地址	为对应 MAC 地址的客户端预留的 IP 地址。
备注	DHCP 固定 IP 地址分配规则的备注信息。
状态	DHCP 固定 IP 地址分配规则的启用状态。
操作	<p>可对规则进行如下操作：</p> <ul style="list-style-type: none"> <li>- 点击  可以修改规则。</li> <li>- 点击  可以删除规则。</li> </ul>

## 11.2 WAN 口参数

如果您已经正确完成[联网设置](#)，但接在路由器下的用户还是不能上网，或者上网出现问题，可以尝试修改 WAN 口参数解决。

进入页面：点击「更多设置」>「WAN 口参数」。

[← 返回](#) **WAN口参数**

---

**WAN1参数**

---

WAN口速率：

MTU：

MAC地址： 默认MAC：50:2B:73:FE:DA:B9

---

**快速转发**

---

快速转发： 启用  禁用

### 11.2.1 WAN 口速率

如果路由器 WAN 口已正确连接网线，且网线工作正常，但对应 WAN 口灯不亮；或者插上网线后 WAN 口灯要等待一会儿（5 秒以上）才亮。此时，可以将路由器的 WAN 口速率调为 10Mbps 半双工或 10Mbps 全双工尝试解决问题。

否则，建议 WAN 口速率保持默认设置“自动协商”。



## 11.2.2 MTU

MTU，即“最大传输单元”，是网络设备传输的最大数据包。联网方式为“宽带拨号”时，默认 MTU 值为 1492。联网方式为“动态 IP”或“静态 IP”时，默认 MTU 值为 1500。一般情况下，建议保持 MTU 值为默认设置，除非您遇到以下情况：

- 无法访问某些网站、或打不开安全网站（如网银、支付宝登录页面）。
- 无法收发邮件、无法访问 FTP 和 POP 等服务器等。

此时，可以尝试从最大值 1500 逐渐减少 MTU 值（建议修改范围 1400~1500），直到问题消失。

MTU 值	应用
1500	非宽带拨号、非 VPN 拨号环境下最常用的设置。
1492	用于宽带拨号拨号环境。
1472	使用 ping 的最大值（大于此值的包会被分解）。
1468	用于一些 DHCP（动态 IP）环境。
1436	用于 VPN 或 PPTP 环境。

## 11.2.3 MAC 地址

当联网设置完毕后，如果路由器还是无法联网，有可能是 ISP 将上网账号信息与某一 MAC 地址（物理地址）绑定了。此时，您可以尝试通过 MAC 地址克隆（方法 1 或方法 2）解决该问题。



请克隆之前能正常上网的电脑 MAC 地址或能正常上网的路由器 WAN 口 MAC 地址。

## 方法 1:

**步骤 1** 使用之前能正常上网的电脑连接路由器;

**步骤 2** 登录路由器管理页面, 点击「更多设置」>「WAN 口参数」进入设置页面, 在对应 WAN 口的 MAC 地址选项框选择“克隆本地 MAC”;

**步骤 3** 点击页面底端的 **保存**。



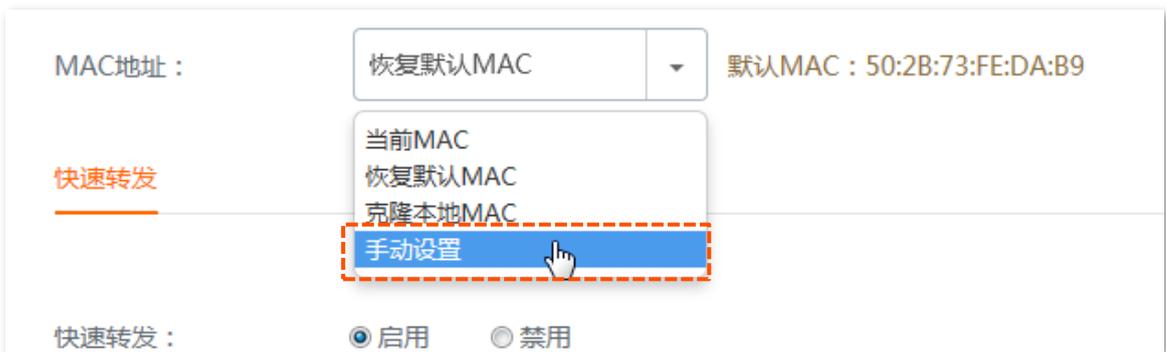
----完成

## 方法 2:

**步骤 1** 记录正确的 MAC 地址;

**步骤 2** 登录路由器管理页面, 点击「更多设置」>「WAN 口参数」页面, 在对应 WAN 口的 MAC 地址选项框选择“手动设置”, 然后填入正确的 MAC 地址 (可能是“直连宽带网线时能成功联网的电脑的 MAC 地址”或“之前能正常上网的路由器的 WAN 口 MAC 地址”);

**步骤 3** 点击页面底端的 **保存**。



----完成



提示

如果需要将 MAC 地址恢复为出厂 MAC, 请点击「更多设置」>「WAN 口参数」, 在对应 WAN 口的 MAC 地址选项框选择“恢复默认 MAC”, 点击 **保存**。

## 11.2.4 快速转发

路由器支持“快速转发”功能，启用后，可以提高路由器的 NAT（网络地址转换）转发性能。



## 11.3 静态路由

### 11.3.1 概述

路由，是选择一条最佳路径把数据从源地址传送到目的地址的行为。静态路由则是手动配置的一种特殊路由，具有简单、高效、可靠等优点。合适的静态路由可以减少路由选择问题和路由选择数据流的过载，提高数据包的转发速度。

通过设置目标网络、子网掩码、默认网关和接口来确定一条静态路由，其中，目标网络和子网掩码用来确定一个目标网络或主机。静态路由设置完成后，所有目的地址为静态路由目的地址的数据均直接通过该静态路由接口转发至网关地址。



注意

在大型复杂网络中完全使用静态路由时，如果网络发生故障或者拓扑发生变化，可能会出现路由不可达，并导致网络中断，此时必须由网络管理员手工修改静态路由的配置。

进入页面：点击「更多设置」>「静态路由」。

← 返回 **静态路由**

**静态路由**

+新增

目标网络	子网掩码	默认网关	接口	操作
暂无数据				

**路由表**

目标网络	子网掩码	默认网关	接口
0.0.0.0	0.0.0.0	172.16.200.1	WAN
172.16.200.1	255.255.255.255	0.0.0.0	WAN
192.168.0.0	255.255.255.0	0.0.0.0	LAN

## 参数说明

标题项	说明
目标网络	目的网络的 IP 地址。
子网掩码	目的网络 IP 地址的子网掩码。
默认网关	数据包从路由器的接口出去后，下一跳路由的入口 IP 地址。
接口	数据从路由器出去的接口。请根据需要选择相应接口。
操作	点击  可以删除规则。

## 11.3.2 新增静态路由

**步骤 1** 点击「更多设置」>「静态路由」；

**步骤 2** 点击  ；



**步骤 3** 在【新增】窗口配置各项参数；

**步骤 4** 点击  。

新增
✕

---

目标网络：

子网掩码：

默认网关：

接口： WAN1  LAN口

保存
取消

---完成

静态路由添加成功后，可以在「更多设置」>「静态路由」页面查看已添加的静态路由规则。配置好的静态路由也将显示在下方的路由表中，如下图示例。

静态路由
?

静态路由
+添加静态路由

目标网络	子网掩码	网关	接口	操作
172.16.100.0	255.255.255.0	192.168.98.1	WAN1	✎ 🗑

路由表

目标网络	子网掩码	网关	接口
0.0.0.0	0.0.0.0	172.16.200.1	WAN0
172.16.200.1	255.255.255.255	0.0.0.0	WAN0
192.168.0.0	255.255.255.0	0.0.0.0	LAN
192.168.98.0	255.255.255.0	0.0.0.0	WAN1
172.16.100.0	255.255.255.0	192.168.98.1	WAN1

路由表中，目标网络/子网掩码都为“0.0.0.0”的路由为路由器的默认路由，当在路由表中找不到与数据包的目的地址精确匹配的路由时，路由器会选择默认路由来转发该数据包；网关为“0.0.0.0”的路由为直连路由，表示该目标网络是路由器该接口直连的网络。



注意  
当静态路由规则和自定义的多WAN策略冲突时，静态路由优先生效。

## 11.3.3 静态路由配置举例

### 组网需求

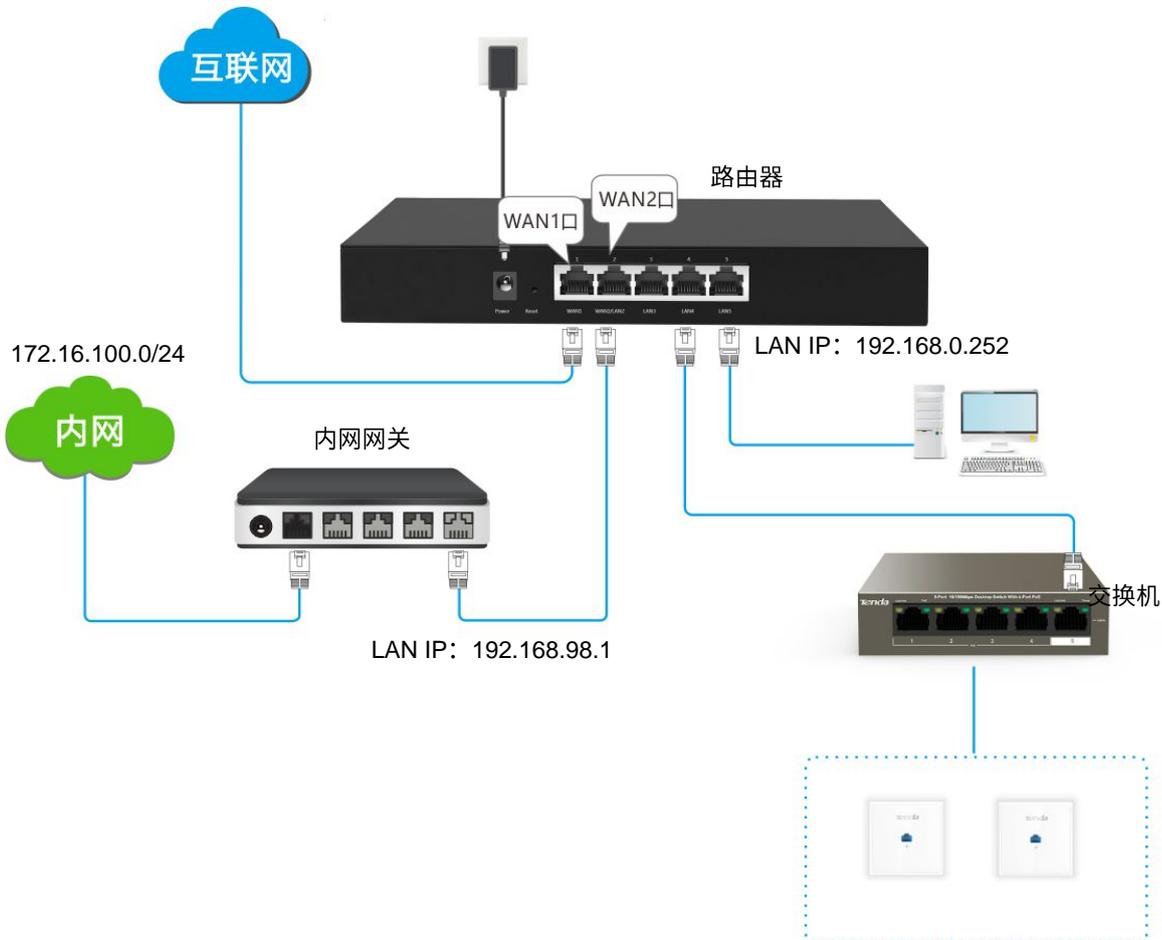
某企业使用路由器进行网络搭建。互联网、公司内网在不同的网络，其中，WAN1 口通过宽带拨号接入互联网，WAN2 口通过动态 IP 接入公司内网。现要求：局域网的用户能同时访问互联网和公司内网。

假设宽带账号信息如下：

- 宽带账号：zhangsan
- 宽带密码：zhangsan

### 方案设计

使用路由器的静态路由功能实现上述需求。

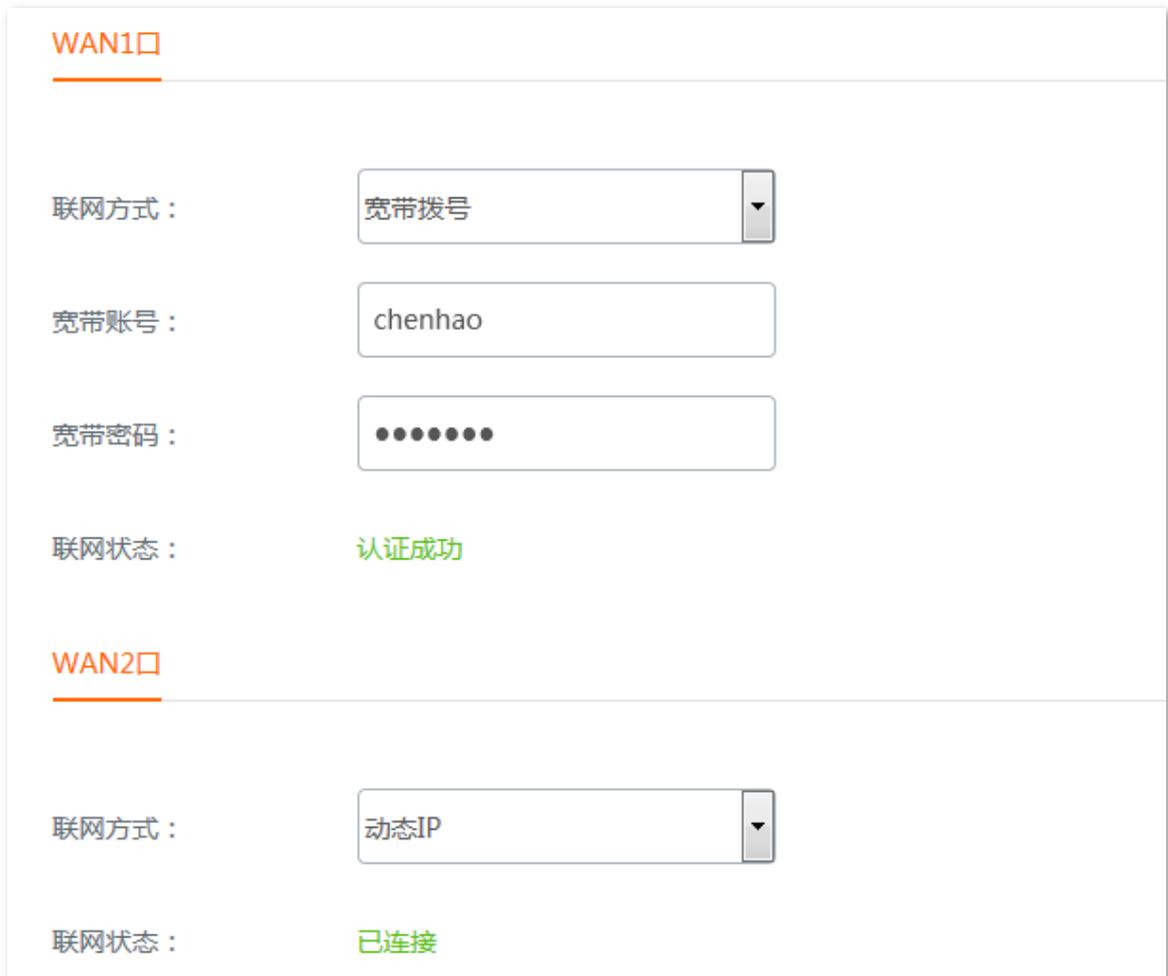


### 配置步骤

**步骤 1** 启用 2 个 WAN 口，并进行上网设置；

1. 点击「联网设置」；

2. WAN 口个数：点击下拉框，选择 2；
3. 在 WAN1 处设置“宽带拨号”上网；
4. 在 WAN2 处设置“动态 IP”上网；
5. 点击页面底端的 **保存**，之后按页面提示进行操作。



**WAN1口**

联网方式：

宽带账号：

宽带密码：

联网状态：认证成功

---

**WAN2口**

联网方式：

联网状态：已连接

## 步骤 2 配置静态路由。

1. 点击「系统状态」，查看 WAN2 获取的 IP 地址信息，假设如下：
  - IP 地址：192.168.98.190
  - 子网掩码：255.255.255.0
  - 默认网关：192.168.98.1
  - 首选 DNS 服务器：192.168.98.1
2. 添加静态路由规则。
  - (1) 点击「更多设置」>「静态路由」。
  - (2) 点击 **+新增**。



(3) 在【新增】窗口配置各项参数；

- 目标网络：输入目的网络的 IP 地址，本例为“172.16.100.0”。
- 子网掩码：输入目的网络 IP 地址的子网掩码，本例为“255.255.255.0”。
- 默认网关：输入下一跳路由的入口 IP 地址，本例为“192.168.98.1”。
- 接口：选择目标网络接在路由器的接口，本例为“WAN2”。

(4) 点击 **保存**。

新增

目标网络： 172.16.100.0

子网掩码： 255.255.255.0

默认网关： 192.168.98.1

接口：  WAN1  WAN2  LAN口

**保存** 取消

----完成

添加成功。

静态路由

+新增

目标网络	子网掩码	默认网关	接口	操作
172.16.100.0	255.255.255.0	192.168.98.1	WAN2	

配置好的静态路由将显示在路由表中，如下图所示。

路由表

目标网络	子网掩码	默认网关	接口
0.0.0.0	0.0.0.0	172.16.200.1	WAN1
172.16.200.1	255.255.255.255	0.0.0.0	WAN1
192.168.0.0	255.255.255.0	0.0.0.0	LAN
192.168.98.0	255.255.255.0	0.0.0.0	WAN2
172.16.100.0	255.255.255.0	192.168.98.1	WAN2

## 验证配置

局域网中的电脑可以同时访问互联网和公司内网。



如果公司内网和互联网没有完全隔离，则路由器可能会将默认路由指向内网网关，导致路由出错。此时，请转到「网速控制」页面，修改 WAN2 口的速率，使其远小于 WAN1 的值。

若发生上述情况，建议使用路由器的[自定义多 WAN 策略](#)，将局域网中所有用户指定到 WAN1 口。否则可能导致网络异常。

## 11.4 端口镜像

### 11.4.1 概述

路由器提供了端口镜像功能，可将路由器一个或多个端口（被镜像端口）的数据复制到指定的端口（镜像端口），在镜像端口一般接有数据监测设备，以便网络管理员实时进行流量监控、性能分析和故障诊断。

进入页面：点击「更多设置」>「端口镜像」。端口镜像默认禁用，开启后，页面显示如下：



#### 参数说明

标题项	说明
端口镜像	端口镜像功能开关。  表示关闭，  表示开启。
镜像端口	即监控端口，该端口下的设备要安装监控软件。镜像端口默认为 LAN4，暂不支持修改。
被镜像端口	选择被监控端口。开启端口镜像功能后，被镜像端口的报文会被复制到镜像端口。

### 11.4.2 配置端口镜像

**步骤 1** 点击「更多设置」>「端口镜像」；

**步骤 2** 端口镜像：点击滑块至 ；

**步骤 3** 被镜像端口：选择“被镜像端口”；

**步骤 4** 点击页面底端的 。



----完成

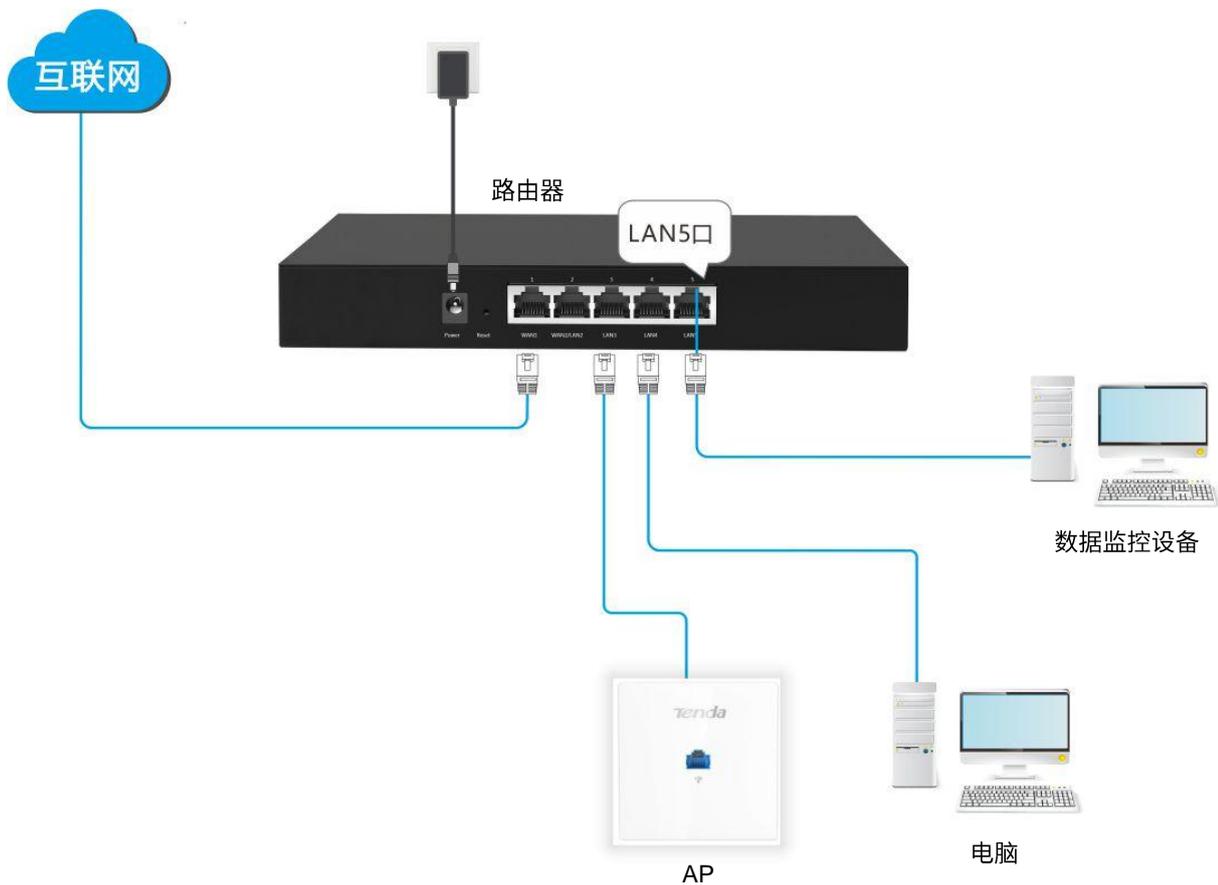
### 11.4.3 端口镜像配置举例

#### 组网需求

某企业使用路由器进行网络搭建,最近公司网络异常,经常上不了网,网络管理员需要捕获路由器 WAN 口、LAN 口的数据进行分析。

#### 方案设计

使用路由器的端口镜像功能实现上述需求。



## 配置步骤

**步骤 1** 点击「更多设置」>「端口镜像」；

**步骤 2** 端口镜像：点击滑块至 ；

**步骤 3** 被镜像端口：勾选“WAN1、LAN2、LAN3、LAN5”复选框；

**步骤 4** 点击页面底端的 **保存**。



---完成

## 验证配置

在监控电脑上运行监控软件，如 Wireshark，可以抓取到被镜像端口的数据包。

## 11.5 远程 WEB 管理

### 11.5.1 概述

一般情况下，只有接到路由器 LAN 口下的设备才能登录路由器的管理页面。

通过远程 WEB 管理功能，使您在有特殊需要时（如远程技术支持），也可以远程通过 WAN 口访问路由器的管理页面。

进入页面：点击「更多设置」>「远程 WEB 管理」。远程 WEB 管理默认禁用，开启后，页面显示如下：



返回 远程WEB管理

远程WEB管理：

WAN口： WAN1

远程主机的IP地址：

远程管理地址：

#### 参数说明

标题项	说明
远程 WEB 管理	远程 WEB 管理功能开关。 <input type="checkbox"/> 表示关闭， <input checked="" type="checkbox"/> 表示开启。
WAN 口	选择路由器的 WAN 口，即远程访问路由器时所使用的 WAN 口。
远程主机的 IP 地址	可以远程访问路由器的电脑的 IP 地址。 <ul style="list-style-type: none"><li>- 任意 IP 地址：互联网上所有电脑都能访问路由器的管理页面。为了网络安全，不建议选择此项。</li><li>- 特定 IP 地址：只有指定 IP 地址的电脑能远程访问路由器的管理页面。如果该管理电脑在局域网，则应填入电脑的网关的 IP 地址（公网 IP）。</li></ul>
远程管理地址	远程管理路由器时使用的域名。启用“远程 WEB 管理”功能后，互联网用户可以使用此域名登录到路由器管理页面。

## 11.5.2 配置远程 WEB 管理

**步骤 1** 点击「更多设置」>「远程 WEB 管理」；

**步骤 2** 远程 WEB 管理：点击滑块至  ；

**步骤 3** WAN 口：选择远程访问路由器时所使用的 WAN 口；

**步骤 4** 远程主机的 IP 地址：指定可以远程访问路由器的电脑的 IP 地址；

**步骤 5** 点击页面底端的 **保存**。



---完成

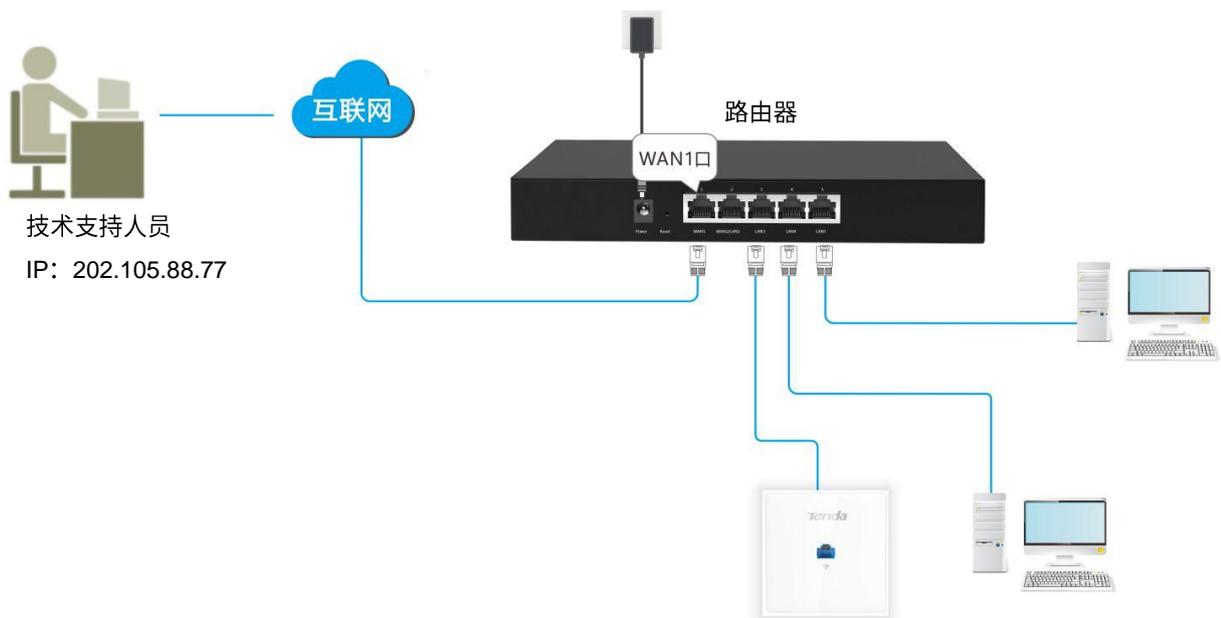
## 11.5.3 远程 WEB 管理配置举例

### 组网需求

某企业使用路由器进行网络搭建，网络管理员在设置网络时遇到问题，需要 Tenda 技术支持远程登录到路由器分析并解决。

### 方案设计

可以采用路由器的远程 WEB 管理功能实现上述需求。



## 配置步骤

- 步骤 1** 网络管理员登录路由器管理页面；
- 步骤 2** 点击「更多管理」>「远程 WEB 管理」；
- 步骤 3** 远程 WEB 管理：点击滑块至  ；
- 步骤 4** WAN 口：选择远程访问路由器时所使用的 WAN 口，本例为“WAN1”；
- 步骤 5** 远程主机的 IP 地址：选择“特定 IP 地址”，然后输入 Tenda 技术支持的电脑的 IP 地址，本例为“202.105.88.77”；
- 步骤 6** 点击页面底端的 **保存**。

← 返回

### 远程WEB管理

远程WEB管理：

WAN口： WAN1

远程主机的IP地址：特定IP地址 202.105.88.77

远程管理地址：http://1i7fiak8.cloud.tendacn.net:8080

----完成

## 验证配置

Tenda 技术支持在其电脑 (IP 地址为 202.105.88.77) 的浏览器访问“<http://1i7fiak8.cloud.tendacn.net:8080>”，即可登录路由器并对其进行管理。

# 11.6 DDNS

## 11.6.1 概述

DDNS, 动态域名服务。当服务运行时, 路由器上的 DDNS 客户端将其当前的 WAN 口 IP 地址传送给 DDNS 服务器, 服务器再更新数据库中域名与 IP 地址的映射关系, 实现动态域名解析。

使用 DDNS 功能, 可以让路由器动态变化的 WAN 口 IP 地址 (公网 IP) 始终被映射到一个固定的域名上。DDNS 功能一般与其他功能如端口映射、DMZ 主机、远程 WEB 管理等结合使用, 这样, 用户在进行诸如远程访问局域网服务器、远程访问路由器管理页面等应用时, 无需再关注路由器的 WAN 口 IP 变化, 直接使用对应的域名即可, 更加方便易用。

进入页面: 点击「更多设置」>「DDNS」。DDNS 默认禁用, 启用后, 页面显示如下:

### 参数说明

标题项	说明
DDNS 服务	启用/禁用 DDNS 功能。

标题项	说明
服务提供商	DDNS 的服务提供商。路由器支持的 DDNS 服务提供商有：3322、88ip、oray（花生壳）、gnway（金万维）。
服务类型	该 DDNS 账号的类型。仅在服务提供商为 oray 时显示此参数。
用户名	登录 DDNS 服务的用户名，即在 DDNS “服务提供商”网站上注册的登录用户名。
密码	登录 DDNS 服务的密码，即在 DDNS “服务提供商”网站上注册的登录用户名对应的登录密码。
域名	从 DDNS 服务器获取的域名信息。除了 oray 外，设置其他 DDNS 提供商时，需要手动输入在其网站上申请的域名。
联网状态	显示 DDNS 服务的运行状态。

## 11.6.2 配置 DDNS

**步骤 1** 点击「更多设置」>「DDNS」，转到对应 WAN 口模块；

**步骤 2** DDNS 服务：选择“启用”；

**步骤 3** 设置各 DDNS 参数；

**步骤 4** 点击页面底端的 **保存**。

← 返回 **DDNS**

---

**WAN1口**

DDNS服务： 启用  禁用

服务提供商： [去注册](#)

用户名：

密码：

域名：

联网状态：未连接

----完成

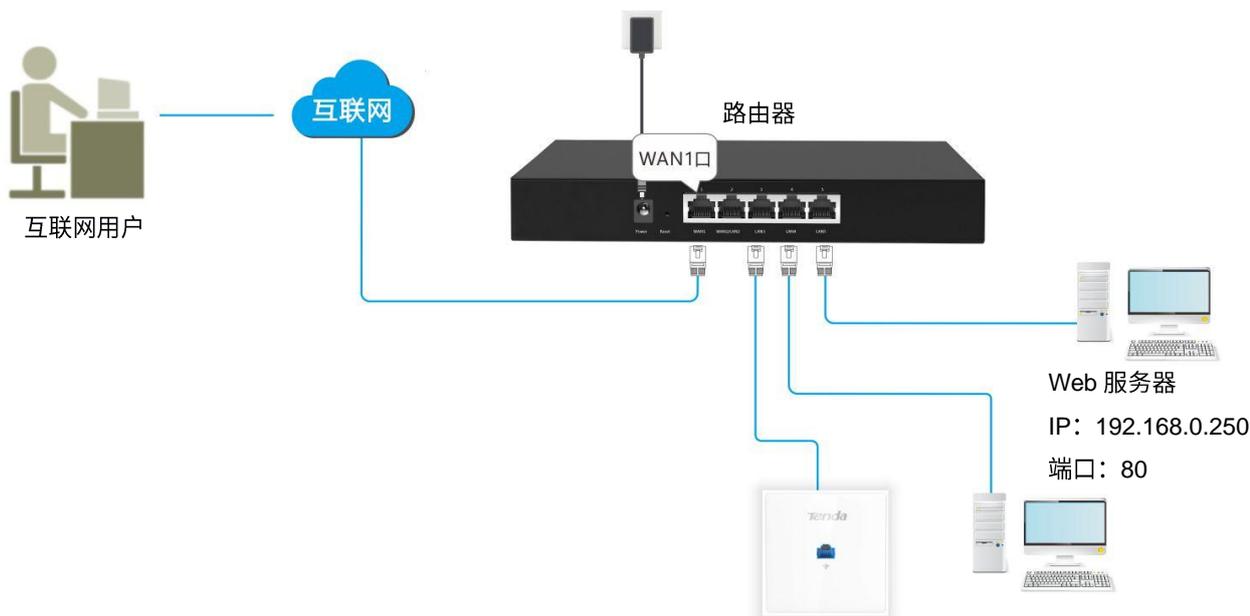
### 11.6.3 DDNS 配置举例

#### 组网需求

某企业使用路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。该企业内部有一个 Web 服务器，需要开放给广域网用户，好让企业员工即使不在公司，也能访问企业内部网络。

#### 方案设计

网络管理员使用路由器的端口映射功能实现上述需求（假设路由器开放给广域网用户访问的端口为 80）。另外，为避免路由器 WAN 口 IP 动态变化导致广域网用户不能正常访问，管理员还开启了路由器的 DDNS 功能，使广域网用户可以每次都能使用同一域名访问。



## 配置步骤

### 步骤 1 配置端口映射；

在「更多设置」>「端口映射」页面，配置如下规则。若有需要，可参考[配置端口映射](#)。

<input type="checkbox"/>	内网服务器IP地址	内网端口	外网端口	协议	接口	状态	操作
<input type="checkbox"/>	192.168.0.250	80-80	80-80	TCP	WAN1	<input checked="" type="checkbox"/>	<a href="#">编辑</a> <a href="#">删除</a>

### 步骤 2 配置 DDNS。

#### 1. 注册域名；

登陆到 DDNS 服务提供商网站进行注册。假设您到 3322 网站注册的用户名为 zhangsan，密码为 123456，申请到的域名为 zhangsan.3322.org。

#### 2. 设置 DDNS。

登录到路由器的管理页面，设置对应 WAN 口。本例为“WAN1”。

- (1) DDNS 服务：选择“启用”。
- (2) 服务提供商：选择您申请域名的 DDNS 提供商，本例为“3322”。
- (3) 用户名：输入您在 DDNS 服务提供商网站注册的用户名，本例为“zhangsan”。
- (4) 密码：输入您在 DDNS 服务提供商网站注册的用户名对应的密码，本例为“123456”。
- (5) 域名：输入您从 DDNS 服务提供商网站申请的域名，本例为“zhangsan.3322.org”。



如果您使用的 DDNS 服务提供商为“oray”，即“花生壳”，则无需输入域名信息。

(6) 点击页面底端的 **保存**。

### WAN1口

DDNS服务： 启用  禁用

服务提供商： [去注册](#)

用户名：

密码：

域名：

联网状态：未连接

----完成

完成设置后，刷新一下页面，稍等片刻。当 WAN1 口“联网状态”显示为“已连接”时，连接成功。

## 验证配置

广域网用户使用“内网服务应用层协议名称://对应 WAN 口域名:外网端口”可以成功访问企业内部 Web 服务器。在本例中，访问地址为“http://zhangsan.3322.org:80”。



配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，请依次尝试以下方法解决。

- 确保路由器 WAN 口获取的是公网 IP 地址，您填写的内网端口段是正确的相应服务端口。
- 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。
- 手动配置局域网服务器 IP，避免因为 IP 的自动变化而导致服务中断。

# 11.7 端口映射

## 11.7.1 概述

默认情况下，广域网中的用户不能主动访问局域网内的设备。端口映射开放了一个服务端口，并以 IP 地址和内网端口来指定其对应的局域网服务器，之后，路由器将广域网中对此服务端口的请求定位到该局域网服务器上，这样，广域网中的用户就能够访问局域网设备，局域网也能避免受到侵袭。

进入页面：点击「更多设置」>「端口映射」。



### 参数说明

标题项	说明
内网服务器 IP 地址	内网服务器的 IP 地址。
内网端口	内网服务器的服务端口。
外网端口	路由器开放给广域网用户访问的端口。
协议	服务的协议类型。设置时，如果不确定服务的协议类型，可以选择“全部”，表示同时选择 TCP 和 UDP 协议。
接口	内网服务映射的 WAN 口，即广域网用户访问局域网服务器时使用的 WAN 口。
状态	规则的状态，可根据需要启用或禁用。
操作	可对规则进行如下操作： <ul style="list-style-type: none"><li>- 点击  可以修改规则。</li><li>- 点击  可以删除规则。</li></ul>

## 11.7.2 配置端口映射

**步骤 1** 点击「更多设置」>「端口映射」;

**步骤 2** 点击 **+新增** ;

**步骤 3** 在【新增】窗口配置各项参数;

**步骤 4** 点击 **保存**。

新增

内网服务器IP地址：

内网端口： ~

外网端口： ~

协议： 全部  TCP  UDP

接口： WAN1

**保存**

---完成

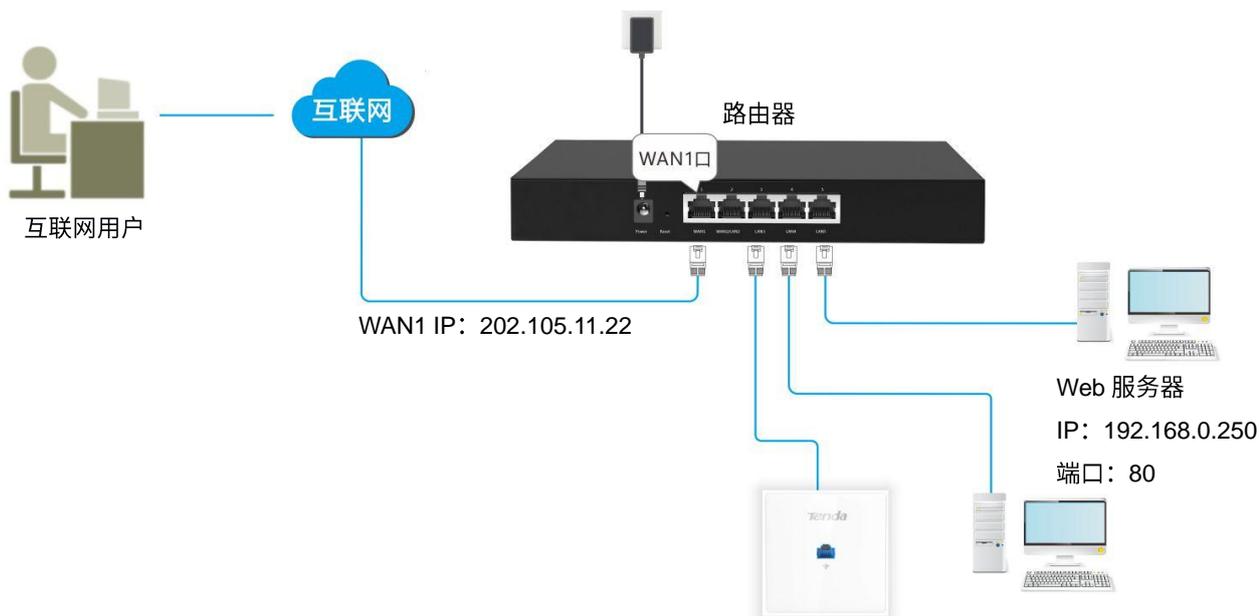
## 11.7.3 端口映射配置举例

### 组网需求

某企业使用路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。该企业内部有一个 Web 服务器，需要开放给广域网用户，好让企业员工即使不在公司，也能访问企业内部网络。

### 方案设计

可以使用路由器的端口映射功能实现上述需求。假设路由器开放给广域网用户访问的端口为 80。



## 配置步骤

**步骤 1** 点击「更多设置」>「端口映射」;

**步骤 2** 点击  ;

**步骤 3** 配置端口映射规则。

1. 内网服务器 IP 地址: 输入 Web 服务器的 IP 地址, 本例为 “192.168.0.250” ;
2. 内网端口: 输入 Web 服务器使用的端口, 本例为 “80~80” ;
3. 外网端口: 输入路由器开放给广域网用户访问的端口, 本例为 “80~80” ;
4. 协议: Web 服务器使用的协议为 “TCP” , 如果您不清楚, 可以选择 “全部” ;
5. 点击  。

新增
✕

---

内网服务器IP地址：

内网端口： ~

外网端口： ~

协议： 全部  TCP  UDP

接口： WAN1

保存
取消

----完成

添加完成，如下图示。

☐	内网服务器IP地址	内网端口	外网端口	协议	接口	状态	操作
☐	192.168.0.250	80-80	80-80	TCP	WAN1	<span style="color: green;">🟢</span>	<span>✎</span> <span>🗑️</span>

## 验证配置

互联网用户使用“内网服务应用层协议名称://对应 WAN 口 IP:外网端口”可以成功访问企业内部 Web 服务器。在本例中，访问地址为“http://202.105.11.22:80”。

如果对应 WAN 口开启了 [DDNS](#)，还可使用“内网服务应用层协议名称://对应 WAN 口域名:外网端口”访问。



配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，请依次尝试以下方法解决。

- 确保路由器 WAN 口获取的是公网 IP 地址，您填写的内网端口段是正确的相应服务端口。
- 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。
- 手动配置局域网服务器 IP，避免因 IP 的自动变化而导致服务中断。

## 11.8 DMZ 主机

### 11.8.1 概述

将局域网中某台电脑设置为 DMZ 主机后，该电脑与互联网通信时将不受限制。例如：某台电脑正在进行视频会议或在线游戏，可将该电脑设置为 DMZ 主机使视频会议和在线游戏更加顺畅。

进入页面：点击「更多设置」>「DMZ 主机」。DMZ 主机默认禁用，启用后，页面显示如下：



- 当把电脑设置成 DMZ 主机后，该电脑相当于完全暴露于外网，路由器的防火墙对该电脑不再起作用。
- 黑客可能会利用 DMZ 主机对本地网络进行攻击，请不要轻易使用 DMZ 主机功能。

← 返回 **DMZ主机**

WAN0口

DMZ主机：  启用  禁用

DMZ主机IP地址：

### 11.8.2 配置 DMZ 主机

**步骤 1** 点击「更多设置」>「DMZ 主机」，转到对应 WAN 口模块；

**步骤 2** DMZ 主机：选择“启用”；

**步骤 3** DMZ 主机 IP 地址：输入局域网内需要设置为 DMZ 主机的设备的 IP 地址；

**步骤 4** 点击页面底端的 **保存**。



---完成

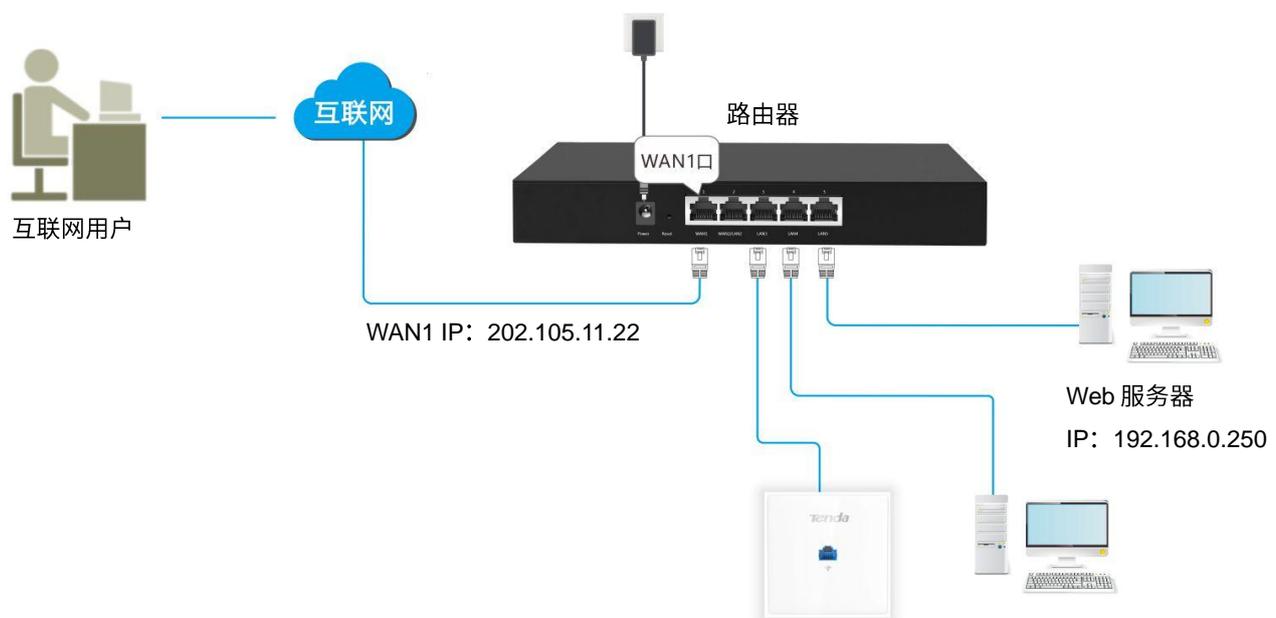
### 11.8.3 DMZ 主机配置举例

#### 组网需求

某企业使用路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。该企业内部有一个 Web 服务器，需要开放给广域网用户，好让企业员工即使不在公司，也能访问企业内部网络。

#### 方案设计

可以使用路由器的 DMZ 功能实现上述需求。



## 配置步骤

**步骤 1** 点击「更多设置」>「DMZ 主机」，转到对应 WAN 口模块；

**步骤 2** DMZ 主机：选择“启用”；

**步骤 3** DMZ 主机 IP 地址：输入局域网内要设置为 DMZ 主机的设备的 IP 地址，本例为“192.168.0.250”；

**步骤 4** 点击页面底端的 **保存**。



The screenshot shows the configuration interface for the WAN0 port. At the top, it is labeled "WAN0口". Below this, there are two main settings:

- DMZ主机 :** This setting has two radio buttons: "启用" (Enabled) and "禁用" (Disabled). The "启用" button is selected.
- DMZ主机IP地址 :** This is a text input field containing the IP address "192.168.0.250".

---完成

## 验证配置

互联网用户使用“内网服务应用层协议名称://对应 WAN 口 IP”可以成功访问企业内部 Web 服务器。在本例中，访问地址为“http://202.105.11.22”。

如果对应 WAN 口开启了 [DDNS](#)，还可使用“内网服务应用层协议名称://对应 WAN 口域名”访问。



配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，请依次尝试以下方法解决。

- 确保路由器 WAN 口获取的是公网 IP 地址，您填写的内网端口段是正确的相应服务端口。
- 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。
- 手动配置局域网服务器 IP，避免因为 IP 的自动变化而导致服务中断。

# 11.9 UPnP

## 11.9.1 概述

UPnP，通用即插即用。启用 UPnP 功能后，路由器可以为内网中支持 UPnP 的程序（如迅雷、BitComet、AnyChat 等）自动打开端口，使应用更加顺畅。

## 11.9.2 开启 UPnP

**步骤 1** 点击「更多设置」>「UPnP」；

**步骤 2** UPnP：点击滑块至 。



----完成

开启 UPnP 功能后，当局域网中运行支持 UPnP 的程序（如迅雷等）时，就可以在 UPnP 页面看到的应用程序发出请求时提供的端口转换信息。如下图示例。



## 11.10 DNS 劫持

### 11.10.1 概述

启用 DNS 劫持后，可以设置域名与 IP 地址的对应规则。这样，当局域网用户访问规则中的域名时，直接解析为访问对应的 IP 地址。

进入页面：点击「更多设置」>「DNS 劫持」。



#### 参数说明

标题项	说明
域名	要解析为固定 IP 地址的域名。
IP 地址	域名解析的 IP 地址，即用户访问指定域名时，都会解析到该 IP 地址。
状态	规则的状态，可根据需要启用或禁用。
操作	可对规则进行如下操作： <ul style="list-style-type: none"><li>- 点击  可以修改规则。</li><li>- 点击  可以删除规则。</li></ul>

### 11.10.2 配置 DNS 劫持

**步骤 1** 点击「更多设置」>「DNS 劫持」；

**步骤 2** 点击 **+新增** ；

**步骤 3** 在【新增】窗口配置各项参数；

步骤 4 点击 **保存**。

新增 ×

---

域名	IP地址	操作
<input type="text"/>	<input type="text"/>	<input type="button" value="+"/> <input type="button" value="-"/>

---完成

## 11.11 DNS 缓存

通过 DNS 缓存功能，使路由器可以记录用户访问网站的 DNS 解析信息。这样，当用户访问已存在于路由器 DNS 缓存列表中的网站时，将直接使用缓存的 DNS 解析信息，不再询问 DNS 服务器，提高了访问速率。

DNS 缓存功能默认开启，缓存容量默认为 1000 条，可根据需要修改。

进入页面：点击「更多设置」>「DNS 缓存」。



返回 DNS缓存

DNS缓存：

缓存容量： 条

## 11.12 攻击防御

路由器支持的攻击防御类型有：ARP 攻击防御、DDoS 防御、IP 攻击防御、防 WAN 口 Ping。

- ARP 攻击防御：路由器可以抵御局域网的 ARP 欺骗、ARP 广播等攻击。
- DDoS 防御：DDoS 攻击，即分布式拒绝服务（Distributed Denial of Service）攻击。利用 DDoS 攻击，攻击者可以消耗目标系统资源，使该目标系统无法提供正常服务。路由器可以防止的 DDoS 攻击类型包括：ICMP Flood、UDP Flood、SYN Flood 攻击。
- IP 攻击防御：路由器可以按照要求拦截具有特殊 IP 选项的数据包，这些 IP 选项包括：IP Timestamp Option、IP Security Option、IP Stream Option、IP Record Route Option、IP Loose Source Route Option 及非法 IP 选项等。
- 防 WAN 口 Ping：广域网主机 Ping 路由器 WAN 口 IP 时，路由器可以自动忽略该 Ping 请求，防止暴露自己，同时防范外部的 Ping 攻击。

进入页面：点击「更多设置」>「攻击防御」。

[← 返回](#) **攻击防御**

---

**ARP攻击防御**

启用ARP防御（防ARP攻击、ARP欺骗、ARP广播）

ARP广播间隔： s（默认1秒）

---

**DDoS防御**

ICMP Flood阈值： pps

UDP Flood阈值： pps

SYN Flood阈值： pps

---

**IP攻击防御**

IP Timestamp Option

## 参数说明

标题项	说明
ARP 攻击防御	启用 ARP 防御 启用/禁用 ARP 防御（包括防 ARP 攻击、防 ARP 欺骗、防 ARP 广播等）功能。
	ARP 广播间隔 设置路由器发送 ARP 广播报文的间隔。
DDoS 防御	ICMP Flood 阈值 一秒钟内，如果路由器收到超过此阈值的 ICMP 请求包，则认为路由器正受到 ICMP Flood 攻击。
	UDP Flood 阈值 一秒钟内，如果路由器某一端口收到超过此阈值的 UDP 包，则认为路由器该端口正受到 UDP Flood 攻击。
	SYN Flood 阈值 一秒钟内，如果路由器某一端口收到超过此阈值的 TCP SYN 包，则认为路由器该端口正受到 SYN Flood 攻击。
IP 攻击防御	IP Timestamp Option 启用后，路由器将拦截带有 Internet Timestamp 选项的 IP 包。
	IP Security Option 启用后，路由器将拦截带有 Security 选项的 IP 包。
	IP Stream Option 启用后，路由器将拦截带有 Stream ID 选项的 IP 包。
	IP Record Route Option 启用后，路由器将拦截带有 Record Route 选项的 IP 包。
	IP Loose Source Route Option 启用后，路由器将拦截带有 Loose Source Route 选项的 IP 包。
	非法 IP 选项 启用后，路由器将检查 IP 包的完整性、正确性，如果不符合，则拦截。
防 WAN 口 Ping	启用/禁用路由器的防 WAN 口 Ping 功能。默认“禁用”。 启用防 WAN 口 Ping 功能后，路由器自动忽略广域网主机对其 WAN 口 IP 地址的 Ping，以防止暴露自己，同时防范外部的 Ping 攻击。

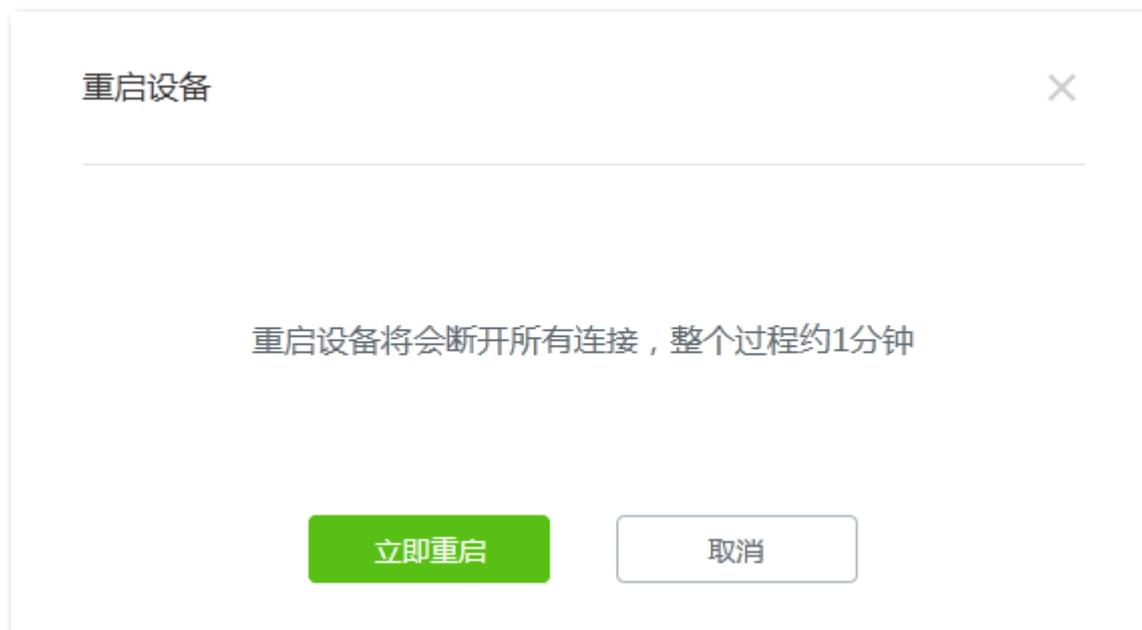
# 12 系统维护

路由器的「系统维护」模块包括：[重启](#)、[升级](#)、[恢复出厂设置](#)、[登录密码](#)、[定时重启](#)、[备份与恢复](#)、[系统时间](#)、[系统日志](#)、[诊断工具](#)。

## 12.1 重启

当您设置的某项参数不能正常生效时，可以尝试手动重启路由器解决。

进入页面：点击「系统维护」>「重启」。



## 12.2 升级

### 12.2.1 概述

您可对路由器进行软件升级和特征库升级。

- 软件升级：可以使路由器获得更多新增功能或更稳定的性能。路由器支持“本地升级”和“在线升级”两种升级方式。默认为“在线升级”。
- 特征库升级：可以更新路由器行为管理模块的应用特征库和 URL 特征库，而不对路由器系统软件进行更新。路由器支持“本地升级”和“在线升级”两种升级方式。默认为“在线升级”。

进入页面：点击「系统维护」>「升级」。

[← 返回](#) **升级**

---

**软件升级**

当前软件版本： V15.11.0.5(5876)

升级方式：  本地升级  在线升级

正在检测新版本，请稍候...

---

**特征库升级**

当前策略版本： 5.0.2.13

升级方式：  本地升级  在线升级

正在检测新版本，请稍候...

## 参数说明

标题项	说明
本地升级	先访问 Tenda 官方网站 <a href="http://www.tenda.com.cn">www.tenda.com.cn</a> 下载对应型号的路由器的升级文件到本地电脑，然后再进行升级。
在线升级	联网后，路由器系统自动检测是否有新的升级文件，并将检测到升级文件的相关信息显示在管理页面，您可以根据该信息决策是否进行升级。需要升级时，点击 <b>升级</b> ，系统将自动下载升级文件，并将路由器系统软件/特征库升级。

## 12.2.2 软件本地升级



为了确保升级正确，避免路由器损坏，请在升级之前，务必确认软件的正确性；升级过程中，请勿断开路由器电源。

- 步骤 1** 访问 Tenda 官网 [www.tenda.com.cn](http://www.tenda.com.cn)，下载对应型号的路由器最新的升级软件并存放本地电脑；
- 步骤 2** 进入路由器的「系统维护」>「升级」页面，转到“软件升级”模块；
- 步骤 3** 升级方式：选择“本地升级”；
- 步骤 4** 点击 **浏览...**，找到并载入相应目录下的升级软件；
- 步骤 5** 点击 **升级**。

### 软件升级

当前软件版本： V15.11.0.5(5876)

升级方式：  
 本地升级  在线升级

选择升级文件：  
 **浏览...** **升级**

将出现进度条，等待进度条走完即可。进度条走完后，您可重新登录路由器，进入「系统维护」>「升级」页面，在“软件升级”模块查看路由器当前的软件版本号。



为了更好的体验高版本软件的稳定性及增值功能，路由器升级完成后，建议将路由器恢复出厂设置，然后重新配置路由器。

## 12.2.3 特征库本地升级



为了确保升级正确，避免路由器损坏，请在升级之前，务必确认升级文件的正确性；升级过程中，请勿断开路由器电源。

- 步骤 1** 访问 Tenda 网站 [www.tenda.com.cn](http://www.tenda.com.cn)，下载对应型号的路由器最新的特征库文件并存放本地电脑；
- 步骤 2** 进入路由器的「系统维护」>「升级」页面，转到“特征库升级”模块；
- 步骤 3** 升级方式：选择“本地升级”；
- 步骤 4** 点击 **浏览...**，找到并载入相应目录下的特征库文件；
- 步骤 5** 点击 **升级**。

### 特征库升级

当前策略版本： 5.0.2.13

升级方式：  
 本地升级  在线升级

选择升级文件：

将出现进度条，等待进度条走完即可。进度条走完后，您可重新登录路由器，进入「系统维护」>「升级」页面，在“特征库升级”模块查看路由器当前的策略版本号。

## 12.3 恢复出厂设置

### 12.3.1 概述

当局域网用户不能访问互联网，但又找不到问题所在时；或您需要登录路由器的管理页面，但是却忘记登录密码时，可以将路由器恢复出厂设置后重新设置。路由器支持“软件恢复出厂设置”和“硬件恢复出厂设置”两种恢复出厂设置方式。

恢复出厂设置后，路由器的登录 IP 地址为 192.168.0.252。



- 恢复出厂设置意味着路由器的所有设置将会丢失，您需要重新设置路由器才能上网。若不是万不得已，不建议将路由器恢复出厂设置。
- 为避免损坏路由器，恢复出厂设置过程中，请确保路由器供电正常。

### 12.3.2 软件恢复出厂设置

**步骤 1** 点击「系统维护」>「恢复出厂设置」；

**步骤 2** 点击 **恢复出厂设置**。



----完成

### 12.3.3 硬件恢复出厂设置

使用此方式时，您无需进入路由器管理页面就可以将路由器恢复出厂设置。

**步骤 1** 路由器 SYS 灯闪烁状态下，用尖状物按住机身前面板上的复位按钮（RESET 或 Reset）8 秒后放开；

**步骤 2** 等待约 1 分钟。

---完成

## 12.4 登录密码

### 12.4.1 概述

在“登录密码”页面，您可以修改路由器的登录密码。首次使用路由器时，需要设置登录密码。

进入页面：点击「系统维护」>「登录密码」。



账号类型	密码	权限
管理员	<input type="text" value="admin"/>	拥有对路由器的所有操作权限
认证管理	<input type="text" value="rzadmin"/>	只能查看系统状态、配置认证账号

### 12.4.2 修改登录密码

**步骤 1** 点击「系统维护」>「登录密码」；

**步骤 2** 在对应账号类型的输入框中修改登录密码；

**步骤 3** 点击页面底端的 **保存**。

---完成

页面将会跳转到登录页面，此时输入刚才设置的密码，然后点击 **登录** 即可登录到路由器的管理页面。

## 12.5 定时重启

### 12.5.1 概述

在“定时重启”页面，您可以设置周期性定时地自动重启路由器，预防路由器长时间运行导致其出现性能下降、不稳定等现象。

进入页面：点击「系统维护」>「定时重启」。定时重启默认禁用，启用后如下。

定时重启： 启用  禁用

重启时间： 时  分

重复： 每天  指定日期

星期日  星期一  星期二  星期三  星期四  星期五  星期六

### 12.5.2 定时重启路由器

**步骤 1** 点击「系统维护」>「定时重启」；

**步骤 2** 定时重启：选择“启用”；

**步骤 3** 重启时间：选择路由器自动重启的时间点，如凌晨 3 点；

**步骤 4** 重复：设置路由器自动重启的日期，如指定“星期四”；

**步骤 5** 点击页面底端的 **保存**。

← 返回 **定时重启**

定时重启： 启用  禁用

重启时间： 时  分

重复： 每天  指定日期

星期日  星期一  星期二  星期三  星期四  星期五  星期六

---完成

之后，每个星期四的凌晨 3 点，路由器将自动重启。



定时重启时间以路由器的系统时间为准，为避免重启时间出错，请确保您已正确设置了路由器的[系统时间](#)。

## 12.6 备份与恢复

### 12.6.1 概述

使用备份功能，可以将路由器当前的配置信息保存到本地电脑；使用恢复功能，可以将路由器配置还原到之前备份的配置。

如，当您对路由器进行了大量的配置，使其在运行时拥有较好的状态/性能，或更符合对应环境的需求，此时建议对该配置进行备份；当您对路由器进行了升级操作、恢复出厂设置等操作后，可以恢复路由器原有的配置文件。

进入页面：点击「系统维护」>「备份与恢复」。



### 12.6.2 配置备份

**步骤 1** 点击「系统维护」>「备份与恢复」；

**步骤 2** 点击 **备份**，之后按页面提示选择备份文件的存储路径。

---完成

### 12.6.3 配置恢复

**步骤 1** 点击「系统维护」>「备份与恢复」；

**步骤 2** 点击 **浏览...**，选择并加载之前备份的配置文件；

**步骤 3** 点击 **恢复配置**。

---完成

将出现重启进度提示，请耐心等待。路由器重启后配置恢复完成。

## 12.7 系统时间

在“系统时间”页面，您可以设置路由器的系统时间。

为了保证路由器上行为管理等涉及时间的功能正常生效，需要确保路由器的系统时间准确。路由器支持“网络校时”和“手动设置”两种时间设置方式，默认为“网络校时”。

进入页面：点击「系统维护」>「系统时间」。

← 返回 **系统时间**

系统时间： 网络校时  手动设置

校时周期：

时区：

### 12.7.1 网络校时

系统时间自动同步互联网上的时间服务器。使用此方式时，只要路由器成功连接至互联网就能自动校准其系统时间，即使路由器经历重启，也能自行校准，无需网络管理员重新设置。

系统时间： 网络校时  手动设置

校时周期：

时区：

#### 参数说明

标题项	说明
校时周期	路由器向互联网上的时间服务器校对系统时间的时间间隔。
时区	选择路由器当前所在地区的标准时区。

设置完成后，您可以进入「系统状态」页面，查看路由器的系统时间是否校对正确。

## 12.7.2 手动设置

网络管理员手动设置路由器的系统时间。如果使用此方式，则路由器每次重启后，您都需要重新设置路由器的系统时间。选择“手动设置”时，页面展开的相关参数如下图所示。

系统时间： 网络校时  手动设置

日期： 年  月  日

时间： 时  分  秒

[复制管理主机时间](#)

### 参数说明

标题项	说明
日期	可以直接在此处输入正确的时间。
时间	
与电脑同步	可以点击 <a href="#">复制管理主机时间</a> ，可将正在管理路由器的电脑的时间同步到路由器。

设置完成后，您可以进入「系统状态」页面，查看路由器的系统时间是否校对正确。

## 12.8 系统日志

路由器的系统日志记录了系统的启动、PPPoE 拨号、时间同步、设备登录、WAN 口连接等情况，如遇网络故障，可以利用路由器的系统日志信息进行问题排查。

进入页面：点击「系统维护」>「系统日志」。



序号	时间	类型	日志内容
1	2018-08-15 11:26:13	系统日志	[system] Sync time success!
2	2018-05-01 00:10:24	系统日志	[system] wan1 up
3	2018-05-01 00:10:22	系统日志	[wan1] Get ip success
4	2018-05-01 00:10:21	系统日志	[wan1] PPPoE Recv PADS
5	2018-05-01 00:10:21	系统日志	[wan1] PPPoE Wait for PADS
6	2018-05-01 00:10:21	系统日志	[wan1] PPPoE Send PADR

日志记录时间以路由器的系统时间为准，如果要让日志记录时间准确，请先确保路由器的系统时间准确。可以到「系统维护」>「系统时间」页面校准路由器的系统时间。



- 路由器重启后，之前的日志信息将丢失。
- 断电后重新通电、软件升级、备份/恢复设置、恢复出厂设置等操作都会导致路由器重启。

## 12.9 诊断工具

### 12.9.1 概述

在“诊断工具”页面，您可以进行 Ping/Traceroute 检测。

- Ping：用于检测网络的连通性和连通质量。
- Traceroute：用于检测数据包从路由器到目标主机所经过的路由。

进入页面：点击「系统维护」>「诊断工具」。

返回 诊断工具

诊断工具： Ping

IP地址或域名：

Ping包个数： 4

数据包大小： 32 单位: 字节

Ping结果将显示在这里

开始

### 12.9.2 执行 Ping

假设要检测路由器到百度服务器的链路是否畅通。

**步骤 1** 点击「系统维护」>「诊断工具」；

**步骤 2** 诊断工具：选择“Ping”；

**步骤 3** IP 地址或域名：输入目的 IP 地址或域名，本例为 “www.baidu.com”；

**步骤 4** Ping 包个数：设置 ping 发送的数据包的个数，建议保持默认设置；

**步骤 5** 数据包大小：设置 ping 发送的数据包的大小，建议保持默认设置；

**步骤 6** 点击 **开始**。

返回 诊断工具

诊断工具： Ping

IP地址或域名： www.baidu.com

Ping包个数： 4

数据包大小： 32 单位: 字节

Ping结果将显示在这里

开始

----完成

稍后，诊断结果将显示在页面下方。如下图示。

← 返回 **诊断工具**

诊断工具：

IP地址或域名：

Ping包个数：

数据包大小： 单位: 字节

```
32 bytes from www.baidu.com: ttl=54 time=10.000
32 bytes from www.baidu.com: ttl=54 time=10.000
32 bytes from www.baidu.com: ttl=54 time=10.000
32 bytes from www.baidu.com: ttl=54 time=0.000
---www.baidu.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0/7.500/10ms
```

### 12.9.3 执行 Traceroute

假设要检测路由器到百度服务器所经过的路由。

**步骤 1** 点击「系统维护」>「诊断工具」；

**步骤 2** 诊断工具：选择“Traceroute”；

**步骤 3** IP 地址或域名：输入目的 IP 地址或域名，本例为“www.baidu.com”；

**步骤 4** 点击 。

← 返回 **诊断工具**

诊断工具：

IP地址或域名：

Traceroute结果将显示在这里

----完成

稍后，诊断结果将显示在页面下方。如下图示例。

← 返回

## 诊断工具

诊断工具：

Traceroute

IP地址或域名：

www.baidu.com

traceroute to www.baidu.com (14.215.177.38), 30 hops  
max, 38 byte packets

1 172.16.200.1 (172.16.200.1) 0.000 ms 0.000 ms  
0.000 ms

2 192.168.20.1 (192.168.20.1) 0.000 ms 10.000 ms  
0.000 ms

3 192.168.21.254 (192.168.21.254) 0.000 ms 0.000 ms

停止

# 附录

## A 常见问题解答

**问 1:** 输入 `tendawifi.com` 或 `192.168.0.252` 登录不了路由器的管理页面，怎么办？

**答:** 请分别从以下几个方面检查：

- 请确保网线连接正确，且网线无松动现象。
- 在浏览器地址栏（非搜索栏）输入 `tendawifi.com` 或 `192.168.0.252`。
- 确认电脑 IP 地址已设为自动获取。
- 清空浏览器的缓存或更换别的浏览器进行尝试。
- 关闭电脑的防火墙或更换别的电脑进行尝试。
- 确认局域网内没有其他 DHCP 服务器或其他 DHCP 服务器已关闭。
- 若经过上述操作仍无法登录，请将路由器恢复出厂设置再重新登录。

**问 2:** 不能登录路由器管理页面的情况下，怎么将路由器恢复出厂设置？

**答:** 路由器 SYS 灯闪烁状态下，使用尖状物按住路由器复位按钮（RESET 或 Reset）8 秒后放开，等待约 1 分钟即可。路由器恢复出厂设置后，需要重新配置参数。

**问 3:** 连接路由器后，电脑出现“IP 地址与网络上的其他系统有冲突”提示信息，怎么办？

**答:** 请参考以下方法解决：

- 确保局域网没有其他 DHCP 服务器或其他 DHCP 服务器已关闭。
- 确保局域网内的电脑没有占用路由器的 LAN 口 IP 地址，路由器出厂默认的 LAN 口 IP 是 `192.168.0.252`。
- 请确保局域网内为电脑静态设置的 IP 没有其它电脑使用。

## B 规格参数

产品型号	G0	G0-PoE
带机量	30 台终端	30 台终端
CPU	400MHz	400MHz
内存	64MB	64MB
FLASH	16MB	16MB
网络接口	5 个 10/100Mbps 自适应 RJ45 端口	5 个 10/100Mbps 自适应 RJ45 端口
PoE 供电	/	2-5 口支持 IEEE 802.3af 标准 PoE 供电
PoE 最大功率	/	单端口最大 15.4W，整机 35W
指示灯	1 个 SYS 灯，5 个 RJ45 端口灯	1 个 SYS 灯，5 个 RJ45 端口灯
按钮	1 个 Reset 按钮	1 个 Reset 按钮
工作环境	工作温度：0°C ~ 40°C 工作湿度：（10 ~ 90）%RH，无凝结	工作温度：0°C ~ 40°C 工作湿度：（10 ~ 90）%RH，无凝结
存储环境	存储温度：-40°C ~ 70°C 存储湿度：（5 ~ 90）%RH，无凝结	存储温度：-40°C ~ 70°C 存储湿度：（5 ~ 90）%RH，无凝结
电源	9V $\overline{=}$ 600mA	48V $\overline{=}$ 800mA
外形尺寸 (长×宽×高)	177.5mm×104mm×26mm	177.5mm×104mm×26mm