1200M 11AC 双频企业级无线路由器 • W15E

使用说明书

版权声明

版权所有©2017 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。

本文档对路由器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

说明书中使用的图片、IP 地址等数据信息均为举例说明，具体请以实际信息为准。

本文可能用到的格式说明如下。

项目	格式	举例
菜单项	『』	选择『开始』菜单。
按钮	边框+底纹	点击 确定 。
连续菜单选择	>	进入『系统管理』→『时间设置』页面。
窗口	【】	设置【SSID 策略】里面的参数。

本文可能用到的标识说明如下。

标识	含义
	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。
	表示有助于节省时间或资源的方法。

缩略语

缩略语	全称
ISP	Internet Service Provider
DNS	Domain Name System
SSID	Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
VPN	Virtual Private Network
L2TP	Layer 2 Tunneling Protocol
MPPE	Microsoft Point-to-Point Encryption

缩略语	全称
PPP	Point To Point Protocol
PPTP	Point to Point Tunneling Protocol
URL	Uniform Resource Locator
DDNS	Dynamic Domain Name System
DMZ	Demilitarized Zone

更多信息

如需获取更多信息，请访问腾达官方网站：http://www.tenda.com.cn。

技术支持

如需技术支持，请通过以下方式与我们联系。

热线	400-6622-666	电子邮件	tenda@tenda.com.cn	网站	http://www.tenda.com.cn
官方微信	Tenda_1999	官方微博	Tenda 腾达		

目录

1 产品介绍 - 1 -

1.1 产品简介 - 1 -

1.2 主要特性 - 1 -

1.3 产品外观 - 2 -

2 安装路由器 - 5 -

2.1 安装注意事项 - 5 -

2.2 安装路由器 - 6 -

2.3 连接路由器 - 6 -

3 设置上网 - 8 -

4 页面简介 - 11 -

4.1 登录路由器管理页面 - 11 -

4.2 退出路由器管理页面 - 12 -

4.3 页面布局 - 13 -

5 网络设置 - 14 -

5.1 上网设置 - 14 -

5.2 WAN 口参数 - 17 -

5.3 局域网设置 - 18 -

5.4 端口镜像 - 25 -

5.5 静态路由 - 27 -

5.6 非法 IP 地址拦截 - 31 -

5.7 DNS 缓存 - 32 -

6 无线设置 33

6.1 无线基本设置 33

6.2 无线高级设置 35

6.3 WMM 设置 38
6.4 射频优化 40
6.5 访客网络 42
6.6 无线中继 44
6.7 无线访问过滤 48
7 行为管理 51
7.1 IP 组和时间组 51
7.2 IP 地址过滤 53
7.3 MAC 地址过滤 58
7.4 端口过滤 63
7.5 网络应用过滤 68
7.6 网址分类过滤 76
7.7 多 WAN 策略 83
8 网速控制 87
8.1 概述 87
8.2 设置智能限速 87
8.3 设置单独限速 88
8.4 单独限速示例 89
9 VPN 服务 92
9.1 PPTP/L2TP 客户端 92
9.2 PPTP/L2TP 服务器 94
9.3 IPSEC 96
9.4 PPTP/L2TP 配置示例 101
9.5 IPSEC 配置示例 107
10 安全设置 111
10.1 IP-MAC 访问控制 111
10.2 攻击防御 116
11 WEB 认证 118
11.1 基本设置 118

11.2 用户管理 120
11.3 WEB 认证示例 123
12 PPPOE 认证 127
12.1 基本设置 127
12.2 账号管理 129
12.3 PPPoE 认证示例 132
13 微信连 WIFI 137
13.1 微信连 WiFi 137
13.2 微信认证示例 142
14 虚拟服务器 147
14.1 端口映射 147
14.2 UPnP 151
14.3 DMZ 主机 151
14.4 DDNS 153
15 系统管理 159
15.1 登录密码 159
15.2 重启 160
15.3 配置备份/恢复 162
15.4 软件升级 163
15.5 策略升级 165
15.6 恢复出厂设置 167
15.7 系统时间 167
15.8 远端 WEB 管理 169
15.9 排障工具 172
16 系统状态 175
16.1 系统信息 175
16.2 用户列表 177
16.3 流量统计 181
16.4 防攻击日志 181

16.5 系统日志 182

附录 183

A.1 设置电脑 IP 地址 183

A.2 产品规格 187

A.3 常见问题解答 187

A.4 有毒有害物质申明 189

1 产品介绍

1.1 产品简介

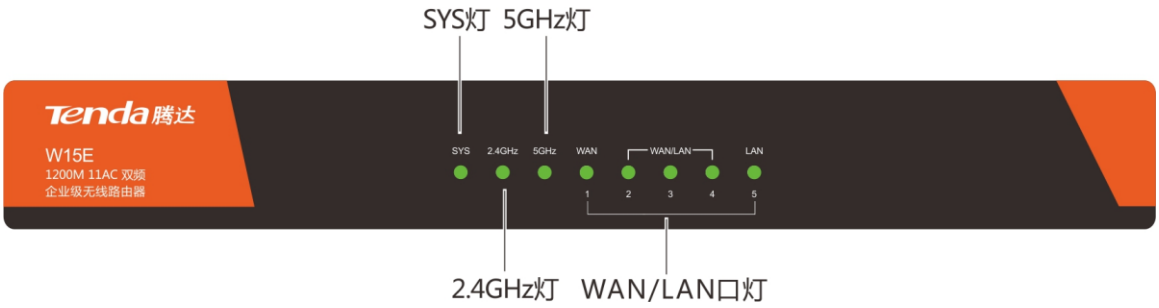
W15E 是 Tenda 专为中小型企业、连锁酒店设计的 1200M 11AC 双频无线路由器。采用高性能处理器，主频高达 900MHz，最大支持 4 个 WAN 口，将微信认证、Web 认证、多 WAN 负载均衡、智能限速等功能集中到一体。采用 Beamforming+智能无线技术，有效提高无线稳定性，可提供总带机 50 人，无线带机 30 人。支持 IPSec/PPTP/L2TP VPN。

1.2 主要特性

- 默认 1 个广域网 WAN 口，4 个局域网 LAN 口。
- 外置 2 根 2.4G、2 根 5G 全向型天线 ,内置独立功放与低噪声放大器 ,可实现 300 平方米稳定覆盖。
- 支持多 WAN 策略，有效防止网络拥塞。
- 支持智能带宽管理，保证网络资源合理利用。
- 支持 PPTP/L2TP 服务器模式和客户端模式，服务器模式主要部署在企业总部，客户端模式主要部署在企业分支机构。
- 支持 IPSec VPN 服务，保证数据完整性校验、防数据包重放、数据加密等。
- 支持 WEB 认证、PPPoE 认证、微信认证功能，只允许合法用户享有上网权限。
- 丰富的网址分类库和 APP 应用库，对员工上网行为进行有效管控。
- 支持软件在线升级。

1.3 产品外观

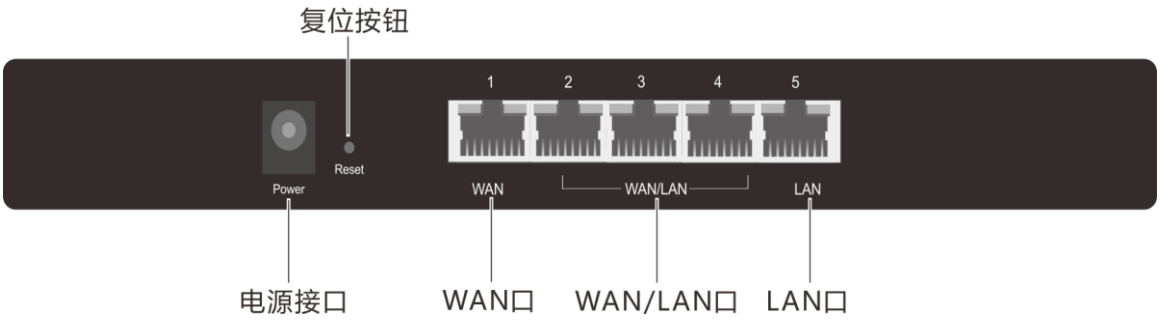
1.3.1 前面板



设备通电后，指示灯状态说明如下：

指示灯丝印	指示灯名称	状态	说明
SYS	系统灯	长亮	系统上电，系统启动完成后，长亮表示系统故障。
		闪烁	系统工作正常。
		熄灭	系统不通电。
2.4GHz	2.4G 无线信号灯	长亮	2.4G 无线功能已开启，没有数据传输。
		闪烁	2.4G 有数据正在传输。
		熄灭	未开启 2.4G 无线功能。
5GHz	5G 无线信号灯	长亮	5G 无线功能已开启，没有数据传输。
		闪烁	5G 有数据正在传输。
		熄灭	未开启 5G 无线功能。
1	1 接口（WAN 口）指示灯	长亮	1 接口没有数据传输。
		闪烁	1 接口有数据传输。
		熄灭	1 接口没有设备连接或连接异常。
2/3/4	2/3/4 接口指示灯	长亮	对应接口没有数据传输。
		闪烁	对应接口有数据传输。
		熄灭	对应接口没有设备连接或连接异常。
5	5 接口（LAN 口）指示灯	长亮	5 接口没有数据传输。
		闪烁	5 接口有数据传输。
		熄灭	5 接口没有设备连接或连接异常。

1.3.2 后面板



接口、按钮说明如下：

接口&按钮	说明
Power	电源接口，请使用产品包装盒内的配套电源适配器进行连接
Reset	复位按钮，通电状态下，用尖状物持续按下 8 秒后松开，路由器将会恢复到出厂状态。
1	WAN 口，连接外网线。外网线可能是从 ADSL 猫、光猫、有线电视猫接出来的网线，或宽带运营商直接提供的宽带网线。
2/3/4	WAN/LAN 口，默认为 LAN 口（内网接口）。可登录路由器管理页面进行修改。
5	LAN 口，可连接交换机、电脑等设备。

1.3.3 贴纸

路由器底部贴纸上有路由器登录地址，WiFi 名称，有需要时，请查阅。

（1）路由器的登录地址。可以使用此地址进入路由器的 Web 管理界面。

（2）路由器的序列号，如果路由器出现故障，客户送修时需填写此序列号。

（3）路由器默认无线网络。

- 首次使用路由器时，手机等无线设备可以搜索并连接该无线网络，进入路由器的管理页面设置上网。
- 路由器连接互联网后，如果没有更改该无线名称，手机等无线设备可以搜索并连接该无线网络访问互联网。

2 安装路由器

2.1 安装注意事项

为避免使用不当造成设备损坏或人身伤害，请遵从以下注意事项。

2.1.1 安全措施

- 使用产品包装盒内的电源给设备供电。
- 确保输入电压范围与设备上标明的输入电压范围相符。
- 确保设备的安装位置通风良好。
- 不要拆卸设备机壳。
- 清洁设备时，请切断电源。请勿使用任何液体擦洗设备。
- 设备需远离电力线、电灯、电网。

2.1.2 环境要求

- 温度、湿度要求

环境描述	温度	湿度
工作环境	0℃ ~ 40℃	10% ~ 90% RH 无凝结
存储环境	-40℃ ~ 70℃	5% ~ 90% RH 无凝结

- 洁净度要求

  为避免静电影响设备正常工作，请保持室内空气清洁，定期给设备除尘；确保设备接地良好，使静电顺利转移。

- 防雷要求

  为避免雷电产生的强大瞬间电流破坏设备，请采取以下防雷措施：

  - 确认电源插座、工作台均接地良好。
  - 合理布线，避免内部感应雷；需要室外布线时，建议使用信号防雷器。

- 工作台要求

  - 确认工作台够平稳、牢固。
  - 保持良好的通风，设备四周留出 10 厘米的散热空间。
  - 不要在设备上放置重物。

2.2 安装路由器

1. 将路由器底部朝上放置于桌面，把 4 个脚垫分别粘贴在机壳底部的凹槽中。
2. 翻转路由器，让其正面朝上放置于桌面，然后摆放好天线位置。安装完成效果图如下。

2.3 连接路由器

1. 将外网线接在路由器的 WAN 口。

2. 用网线连接路由器和其它网络设备（服务器、电脑等）。检查无误后，使用产品包装盒内的电源适配器连接路由器和电源插座。

3 设置上网

1. 在已连接到路由器的电脑上打开浏览器，在地址栏输入 **tendawifi.com** 或 **192.168.0.1**，回车。

2. 在出现的页面点击**开始体验**。

3. 系统会自动检测联网方式，请根据页面提示输入相关上网信息，点击**下一步**。

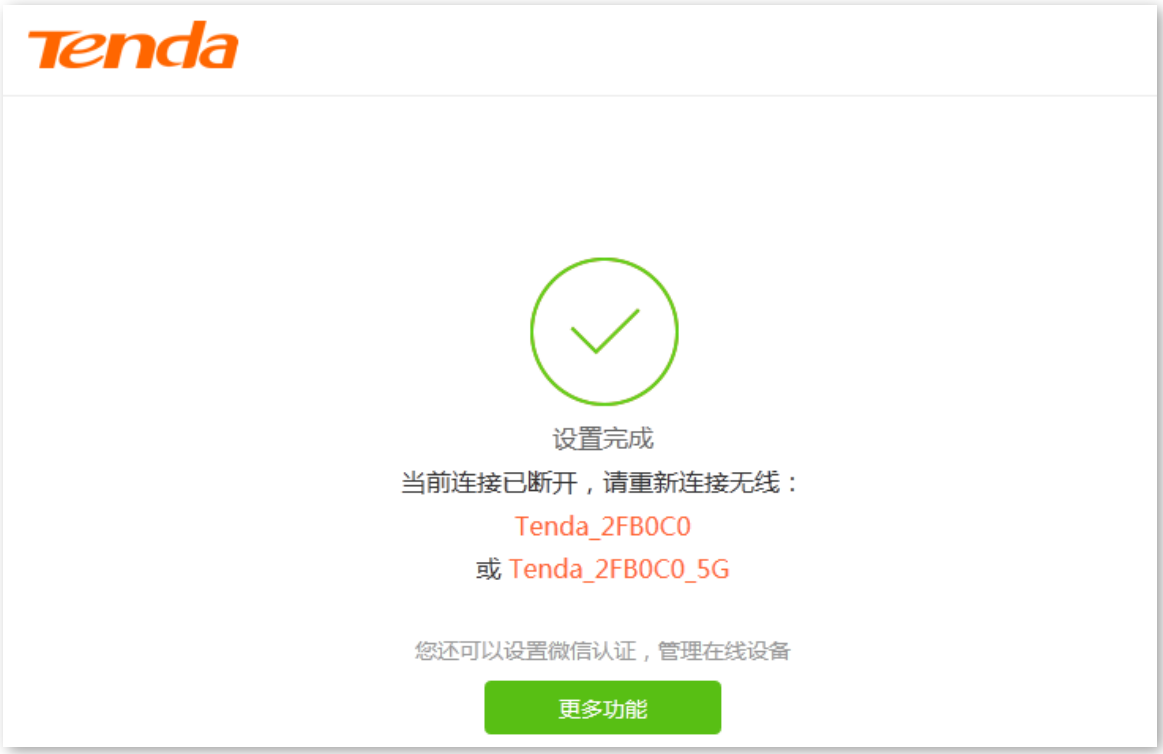
4. 设置无线名称和无线密码，点击**下一步**。

—完成

提示

系统默认将无线密码同步设置为登录密码，如果要将登录密码设置为其他字符，请取消勾选“将无线密码同时设置为登录密码”，然后自定义登录密码。

稍等片刻，联网成功。如果需要设置更多功能，请前往 http://www.tenda.com.cn 下载本路由器的使用说明书。



提示

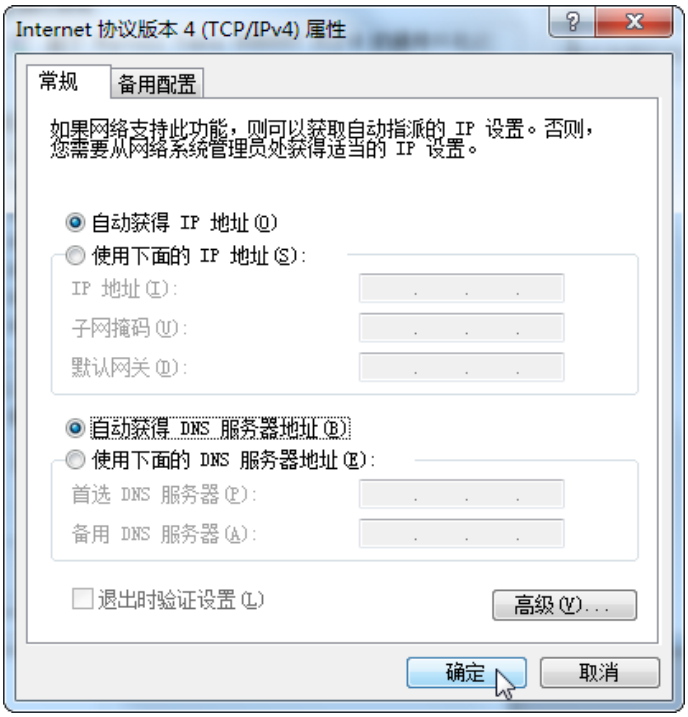
- 路由器的无线信号初始没有密码，更改无线名称、无线密码后需要重新连接 WiFi。
- 路由器默认 2.4G 无线名称为 Tenda_XXXXXX，具体信息请查看路由器底部贴纸；默认 5G 无线名称为 Tenda_XXXXXX_5G。
- 如果台式电脑没有无线网卡，需成功安装无线网卡后才能连接 WiFi。

4 页面简介

4.1 登录路由器管理页面

如果是首次使用路由器，请参考 3 设置上网；完成快速设置后，需要登录路由器时，请参考下文。

1. 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”，详细设置步骤可参考附录 A.1 设置电脑 IP 地址。

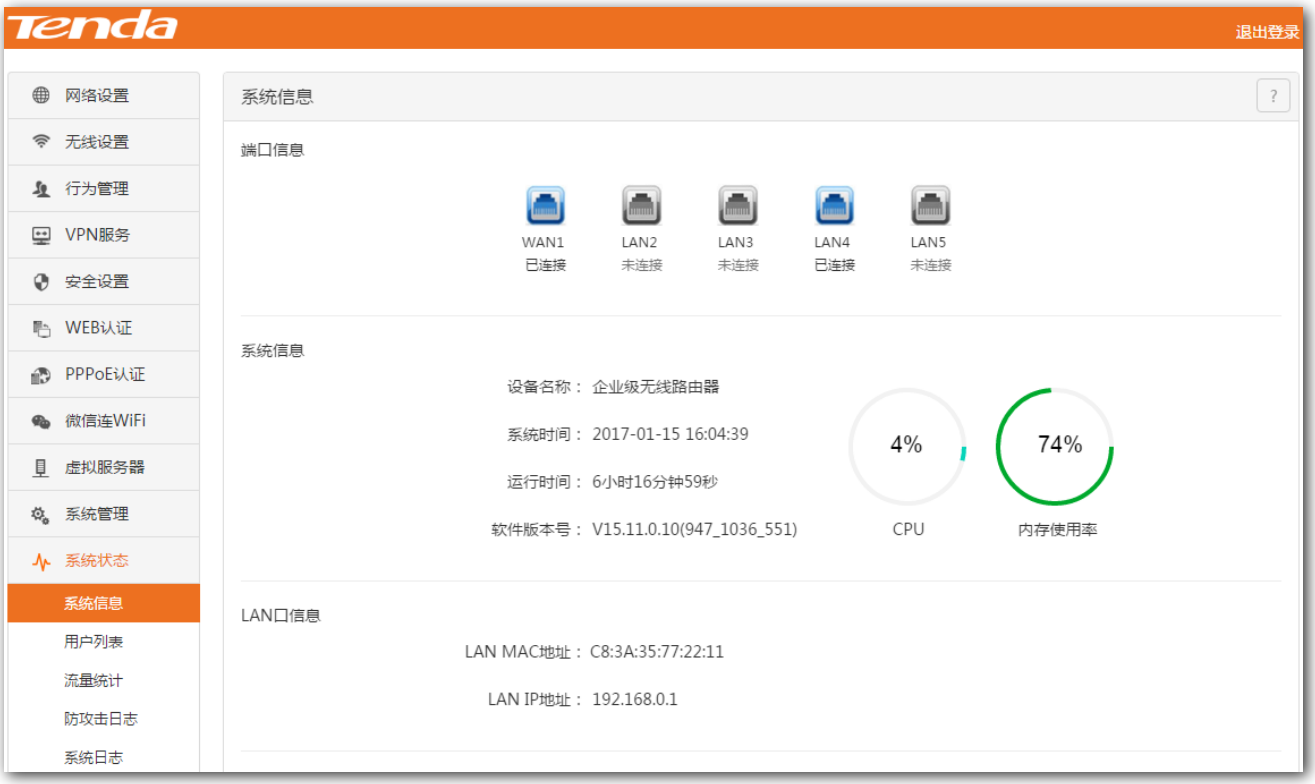


2. 已连接到路由器的电脑上打开浏览器，在地址栏输入 **tendawifi.com** 或 **192.168.0.1**，回车。

3. 输入登录密码，点击 登录 。

—完成

成功登录路由器管理页面。

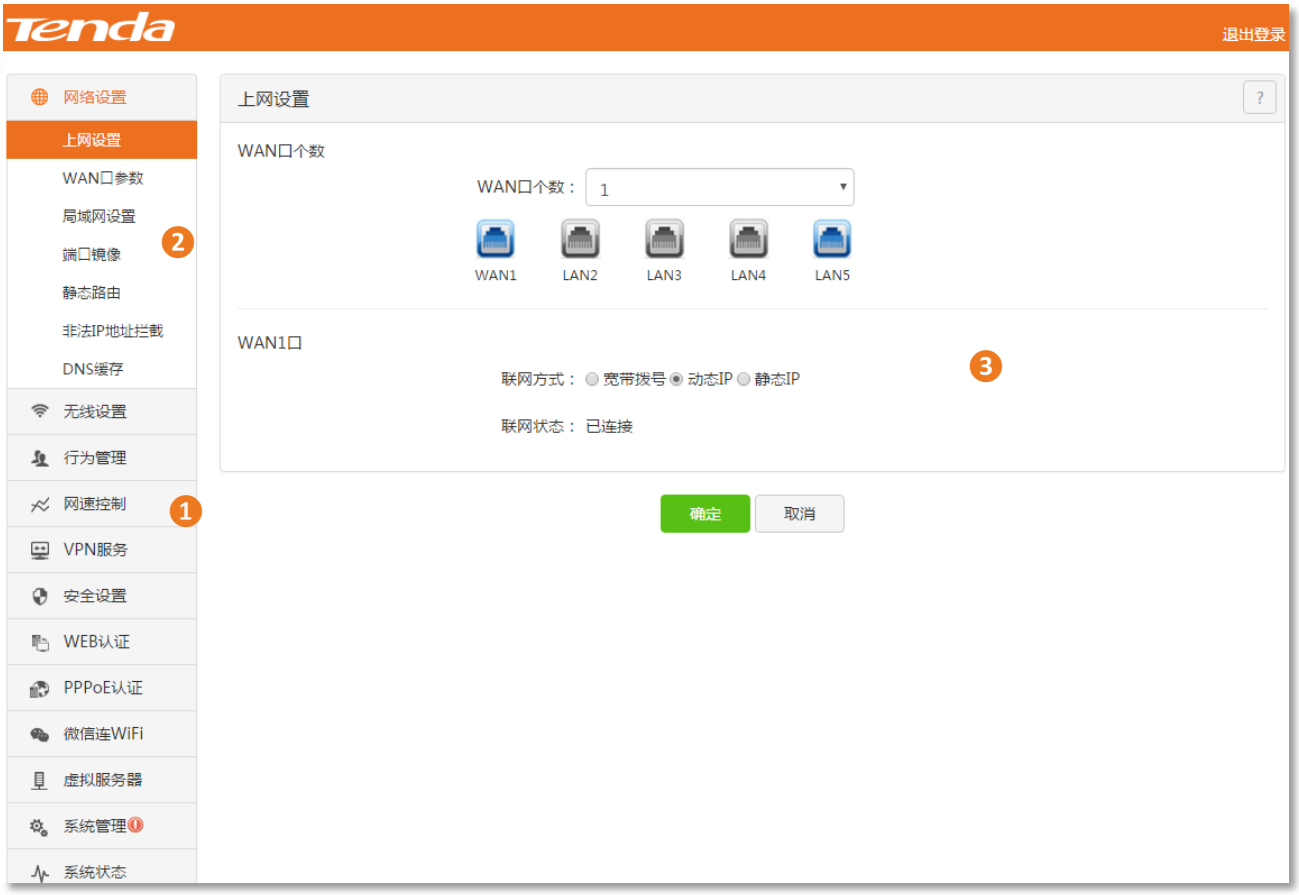


4.2 退出路由器管理页面

登录到路由器的管理页面后，如果在 5 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。

4.3 页面布局

路由器的 Web 管理页面分为：一级导航栏、二级导航栏和配置区三部分，如下图所示。



菜单说明：

序号	参数	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，选择后将会在下方显示二级导航栏。
2	二级导航栏	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，选择二级导航栏后，结果显示在配置区。
3	配置区	用户进行配置和查看的区域。

常用按钮和链接：

参数	说明
确定	用于保存当前页面配置，使配置生效。
取消	用于取消当前页面未保存的配置。
退出登录	点击此链接可返回到路由器的登录页面。

5 网络设置

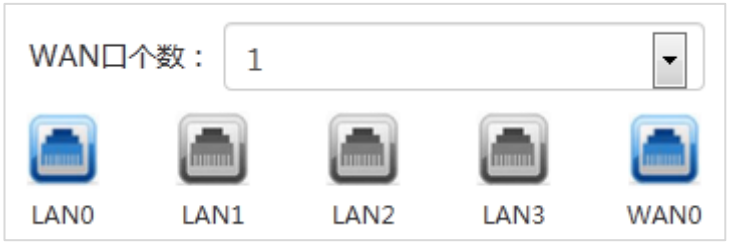
网络设置章节包括：

上网设置、WAN 口参数、局域网设置、端口镜像、静态路由、非法 IP 地址拦截、DNS 缓存。

5.1 上网设置

在“上网设置”页面，您可以修改 WAN 口个数，设置上网参数。在”设置向导“中完成上网设置后，如果需要修改上网参数，可在此处修改。点击『网络设置』进入设置页面。

参数说明

参数	说明
WAN 口个数	设置 WAN 口个数、查看 RJ45 口状态（连接状态、充当角色是 WAN 或 LAN）。默认启用 1 个 WAN 口。 修改 WAN 口个数后，RJ45 口状态图也会改动，如下：  表示接口连接正常。 表示接口未连接设备或连接异常。

参数	说明
联网方式	路由器的联网方式，说明如下： • 宽带拨号：网络服务提供商提供了宽带账号和密码。 • 动态 IP :网络服务提供商没有提供宽带账号和密码 ,也没有提供 IP 地址信息。 • 静态 IP：网络服务提供商提供固定 IP 地址信息。
宽带账号、宽带密码	联网方式为宽带拨号时有效，可以在办理宽带的业务单据上查到，如果没有，请咨询您的网络服务提供商。
IP 地址、子网掩码、网关地址、主/次 DNS	联网方式为静态 IP 时有效，可以在办理宽带的业务单据上查到，如果没有，请咨询您的网络服务提供商。
联网状态	显示 WAN 口的联网状态。主要有以下几种情况： • 已连接或认证成功：路由器已成功连接互联网。 • 连接中...：路由器正在连接到互联网。 • 未连接：未连接或连接失败，请检查上网信息是否输入正确或咨询相应的网络服务提供商。 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。

5.1.1 设置宽带拨号上网

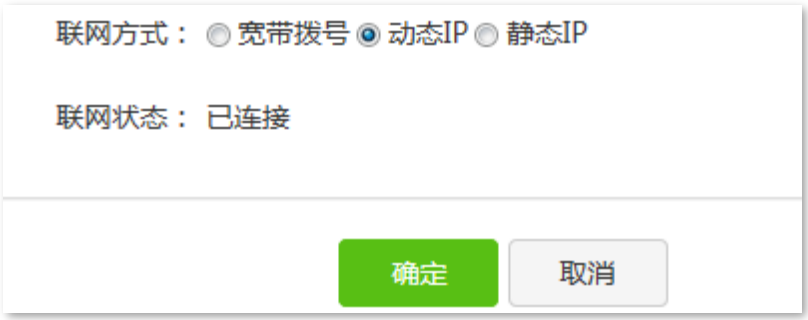
1. 点击『网络设置』。
2. 联网方式：点击选择“宽带拨号”。
3. 宽带账号：输入电信、联通等网络服务提供商提供的宽带账号信息。
4. 宽带密码：输入电信、联通等网络服务提供商提供的宽带密码信息。
5. 点击 确定 。

—完成

稍等片刻，当联网状态显示“认证成功”时，可以尝试上网了。

5.1.2 设置动态 IP 上网

1. 点击『网络设置』。
2. 联网方式：点击选择“动态 IP”。
3. 点击 确定 。



—完成

稍等片刻，当联网状态显示“已连接”时，可以尝试上网了。

5.1.3 设置静态 IP 上网

1. 点击『网络设置』。
2. 联网方式：点击选择“静态 IP”。
3. IP 地址、子网掩码、网关地址、主/次 DNS：输入网络服务提供商提供的固定 IP 地址相关信息。
4. 点击 确定 。

—完成

稍等片刻，当联网状态显示“已连接”时，可以尝试上网了。

5.2 WAN 口参数

5.2.1 概述

在“WAN 口参数”页面，您可以修改 WAN 口速率、MTU 值、WAN 口 MAC 地址，启用/禁用快速转发功能。如果进行上网设置后，还不能访问互联网，可以尝试修改 WAN 口参数来解决。

点击『网络设置』→『WAN 口参数』，进入设置页面。

参数说明

参数	说明
WAN 口速率	路由器 WAN 口的速率，默认为自动协商，如非必要，请勿更改。
MTU	最大传输单元，是网络设备传输的最大数据包，建议保持默认设置。
MAC 地址	克隆 WAN 口 MAC 地址。若进行“上网设置”后，路由器还是无法联网，可能是网络服务提供商将上网信息与某一 MAC 地址绑定，此时请进行 MAC 地址克隆，然后尝试上网。 • 当前 MAC：路由器 WAN 口当前的 MAC 地址。 • 默认 MAC：设置路由器 WAN 口 MAC 地址为出厂默认值。 • 克隆本机 MAC：设置路由器 WAN 口 MAC 地址为当前登录到路由器管理页面的电脑的 MAC 地址。 • 手动输入：手动修改路由器 WAN 口的 MAC 地址。
FastNAT	快速转发功能，开启之后 NAT 转发性能会提高。

5.2.2 修改 WAN 口 MAC 地址

1. 点击『网络设置』→『WAN 口参数』。
2. MAC 地址：点击下拉框，选择“克隆本机 MAC”或“手动输入”。选择手动输入时，在 MAC 输入框输入要克隆的 MAC 地址。
3. 点击 确定 。

—完成

注意

请使用正确的 MAC 地址进行克隆操作！正确的 MAC 地址是安装宽带时，技术人员进行调试上网的电脑的 MAC 地址，或者是之前能正常上网的路由器的 WAN 口 MAC 地址。

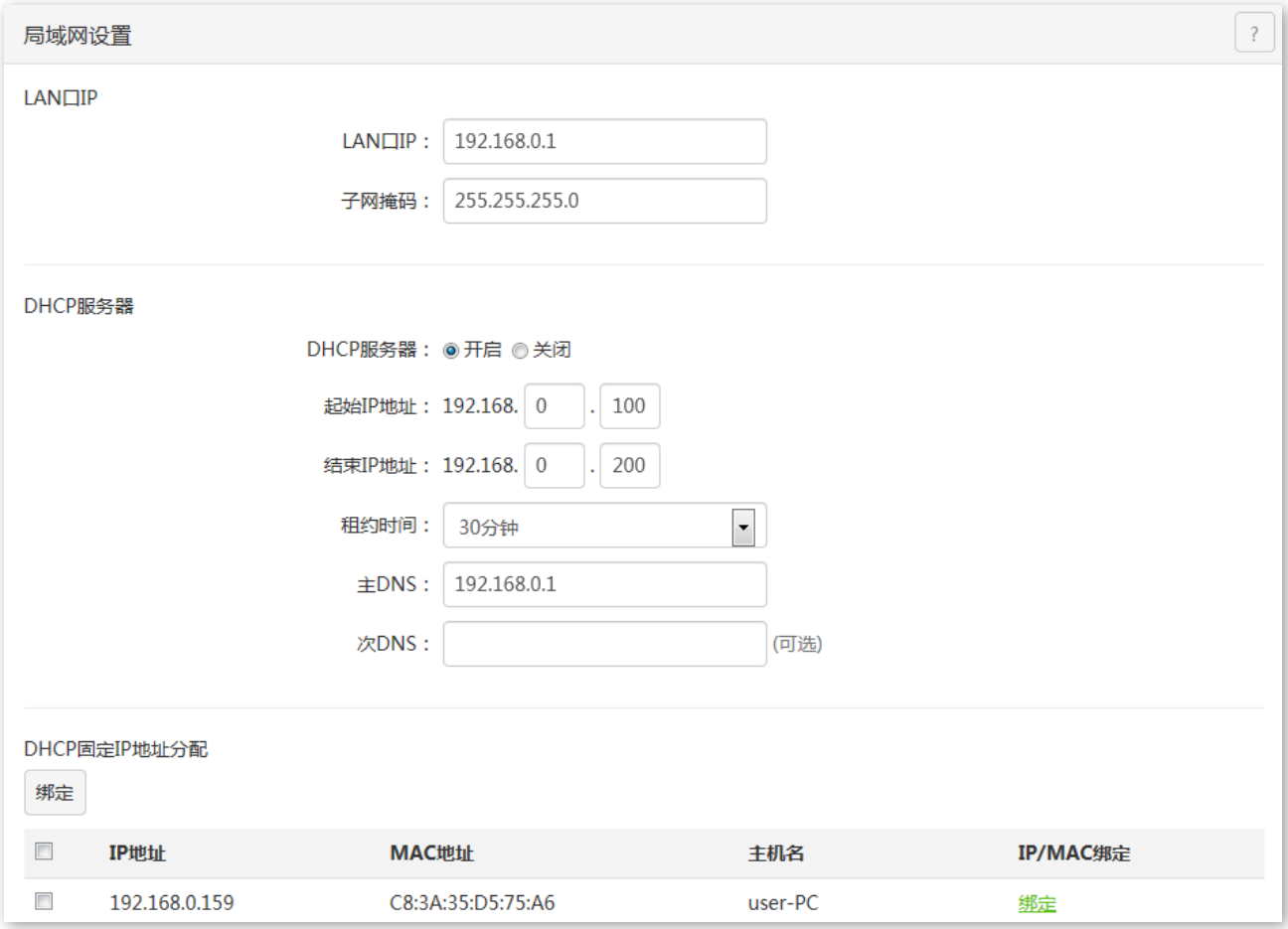
5.3 局域网设置

5.3.1 概述

在”局域网设置“页面，您可以进行以下操作：

- 修改路由器 LAN 口 IP 地址。
- 修改 DHCP 服务器参数。
- 为局域网客户端绑定固定 IP 地址。

点击『网络设置』→『局域网设置』进入设置页面。



LAN 口 IP 地址

LAN 口 IP 地址是路由器的管理 IP 地址，默认为 192.168.0.1，可根据需要修改。

参数说明

参数	说明
LAN 口 IP	路由器的 LAN 口 IP 地址，即登录路由器管理页面的 IP 地址。 本路由器支持 IP 地址（默认为 192.168.0.1）登录和域名地址（tendawifi.com）登录。
子网掩码	IP 地址的子网掩码。

DHCP 服务器

DHCP 服务器能自动给连接上路由器的客户端分配 IP 地址、子网掩码、网关、DNS 等上网信息。如果关闭该功能，需要在客户端上手动配置 IP 地址信息才能实现上网。

如无特殊情况，请保持 DHCP 服务器开启。

参数说明

参数	说明
DHCP 服务器	开启/关闭路由器的 DHCP 服务器功能，默认开启。
起始 IP 地址	DHCP 地址池(DHCP 服务器可分配的 IP 地址范围)的开始 IP 地址 ,默认为 192.168.0.100。
结束 IP 地址	DHCP 地址池的结束 IP 地址，默认为 192.168.0.200。起始 IP 和结束 IP 必须与路由器 LAN 口 IP 地址在同一网段。
租约时间	DHCP 服务器分配给客户端的 IP 地址的有效时间。当地址到期后： • 如果客户端仍连接在路由器上，客户端将自动续约，继续占用该 IP 地址。 • 如果客户端未连接（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。以后若有其它客户端请求 IP 地址信息，路由器可将该 IP 分配给其它客户端。 如无特殊需要，建议保持默认设置。
主 DNS	DHCP 服务器分配给局域网客户端的首选 DNS 服务器 IP 地址。路由器支持 DNS 代理功能，故主 DNS 默认为路由器的 LAN 口 IP 地址。 提示 一般情况下，建议保持默认设置。如需修改，为了使局域网客户端能够正常上网，请务必确保修改的主 DNS 是正确的 DNS 服务器或 DNS 代理的 IP 地址。
次 DNS	DHCP 服务器分配给客户端的备用 DNS 服务器 IP 地址。不填表示 DHCP 服务器不分配此项。

DHCP 固定 IP 地址分配

客户端始终获取同一 IP 地址，从而使路由器的“行为管理”、“网速控制”、“端口映射”等功能正常生效。

在“DHCP 固定 IP 地址分配”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，可以一键绑定客户端 IP 地址、MAC 地址，使本 DHCP 服务器始终给同一客户端分配固定的 IP 地址。

绑定成功后，可以在“DHCP 固定 IP 地址手动分配”模块查看已添加的 IP 地址、MAC 地址绑定规则。

参数说明

参数	说明
绑定	将选中的客户端都进行 IP 地址、MAC 地址绑定。
IP 地址	客户端自动获取路由器 DHCP 服务器分配的 IP 地址。
MAC 地址	客户端的 MAC 地址。
主机名	客户端名称，如 iPhone。
IP/MAC 绑定	点击绑定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”。

DHCP 固定 IP 地址手动分配

客户端始终获取同一 IP 地址，使路由器的“行为管理”、“网速控制”、“端口映射”等功能正常生效。在“DHCP 固定 IP 地址手动分配”模块可以手动绑定客户的 IP 地址、MAC 地址。

5.3.2 修改 LAN 口 IP 地址

1. 点击『网络设置』→『局域网设置』，找到“LAN 口 IP”模块。
2. LAN 口 IP：修改 IP 地址，如 192.168.10.1。
3. 点击页面底端的 确定 。

—完成

稍等片刻，等待进度条走完后，修改完成。如果没有成功登录路由器管理页面，请确保电脑的 IP 地址获取方式为“自动获取”，同时请修复一下电脑的 IP 地址，然后使用新的 IP 地址重新尝试。

5.3.3 设置 DHCP 服务器参数

1. 点击『网络设置』→『局域网设置』，找到“DHCP 服务器”模块。
2. DHCP 服务器：点击“开启”。
3. 起始/结束 IP 地址：设置 DHCP 服务器自动分配给客户端的起始、结束 IP 地址的最后一位。
4. 点击页面底端的 确定 。

—完成

提示

- 路由器默认开启 DHCP 服务器功能，禁用后需要为连接在路由器下的每台客户端手动设置 IP 地址信息。
- 为了不影响正常上网，如果没有专业人士指导，请保持 DHCP 服务器默认设置。

5.3.4 快速为客户端分配固定 IP 地址

1. 点击『网络设置』→『局域网设置』，找到“DHCP 固定 IP 地址分配”模块。
2. 在“DHCP 固定 IP 地址分配”列表，找到要分配固定 IP 地址的客户端，点击绑定；或选择相应的客户端，然后点击 绑定 。

—完成

绑定成功，如下。

5.3.5 手动为客户端分配固定 IP 地址

1. 点击『网络设置』→『局域网设置』，找到“DHCP 固定 IP 地址手动分配”模块。
2. 点击 新增分配 。

3. MAC 地址：输入要获取固定 IP 地址的客户端 MAC 地址，如“C8:3A:35:13:05:18”。
4. IP 地址：设置该 MAC 地址客户端固定获取的 IP 地址，如“192.168.0.20”。
5. （可不填）备注：设置本条规则的备注信息。
6. 点击 确定 。

—完成

规则添加成功，如下。

参数说明

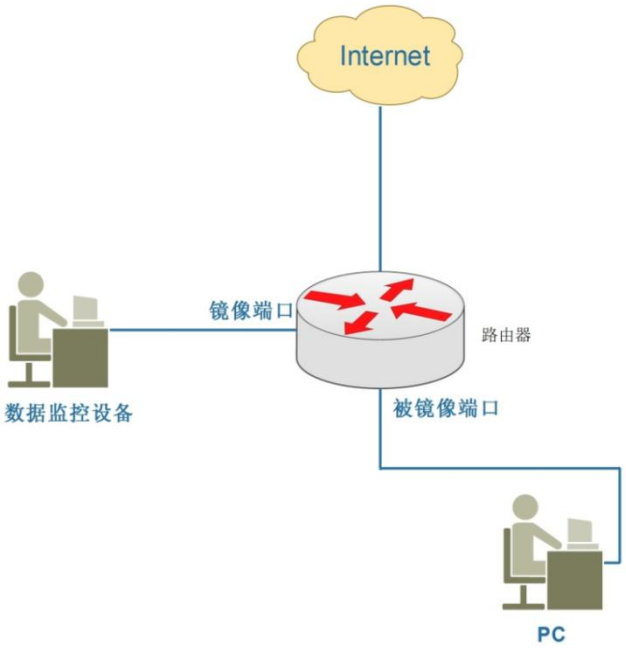
参数	说明
+新增分配	点击此按钮，手动为客户端绑定固定的 IP 地址。首先要知道客户端的 MAC 地址信息。
删除	删除已选中的 IP 地址、MAC 地址绑定规则。
MAC 地址	客户端的 MAC 地址。
IP 地址	对应 MAC 地址的客户端绑定的 IP 地址。
备注	客户端 IP 地址、MAC 地址绑定规则的备注信息，动态绑定或手动添加时没有设置，均不显示。
状态	IP 地址、MAC 地址绑定规则的状态，包括已启用和未启用。
操作	可对 IP 地址、MAC 地址绑定规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改 MAC 地址、IP 地址，备注，启用/禁用规则。 • 点击可以解除绑定，之后，该 MAC 地址对应的客户端可以获得其他 IP 地址。

5.4 端口镜像

5.4.1 概述

在“端口镜像”页面，您可以设置端口镜像功能。

端口镜像是将设备的一个或多个端口的数据报文复制到设备的一个监视端口，网络管理员可以利用这些监测到的数据进行网络监控和故障排查。端口镜像拓扑图如下：



本路由器支持通过 LAN5 口（镜像端口）监控其他接口（被镜像端口）的通信情况。

点击『网络设置』→『端口镜像』，进入设置页面。端口镜像功能默认关闭，开启后，显示如下：

参数说明

参数	说明
端口镜像	开启/关闭端口镜像功能，默认关闭。
镜像端口	监控端口，该端口下的客户端要安装监控软件，默认为 LAN5，且不可更改。
被镜像端口	被监控端口，开启端口镜像功能后，被镜像端口的报文会被自动复制到镜像端口。

5.4.2 端口镜像示例

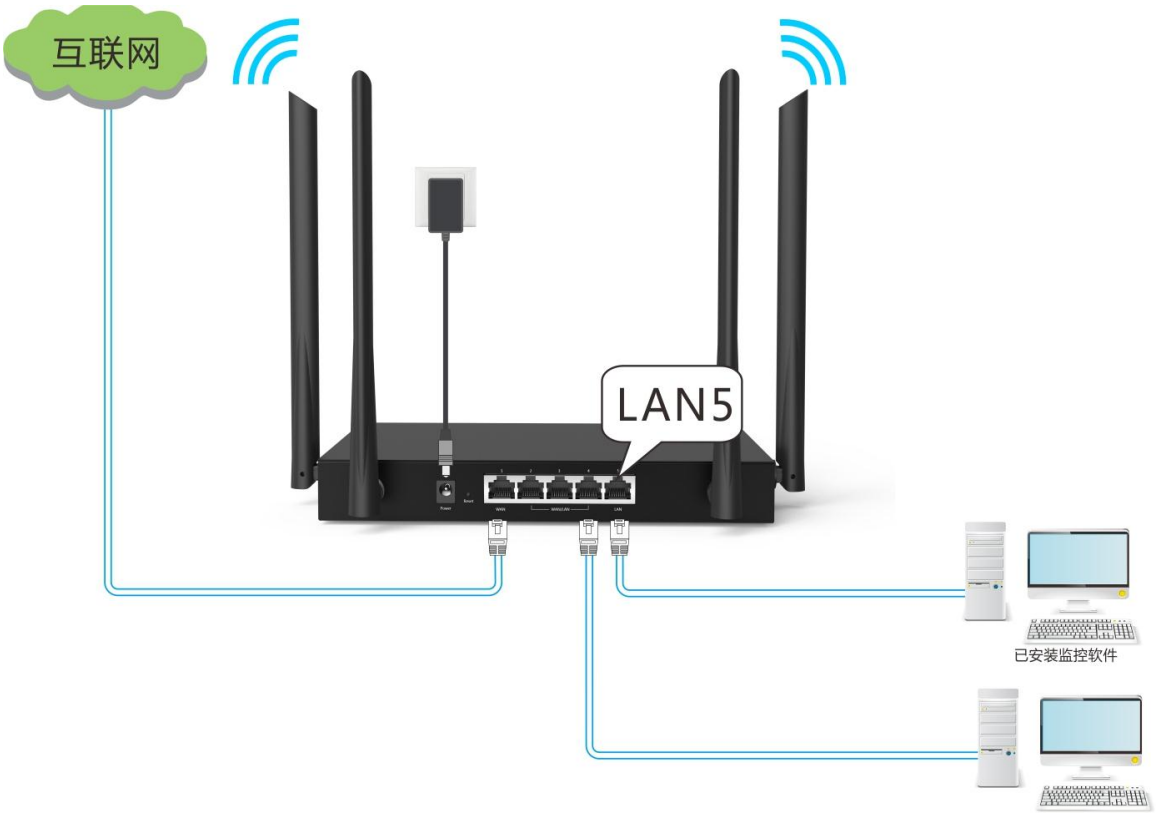
组网需求

某企业使用 W15E 进行网络搭建，最近公司内网络异常，经常上不了网。现在需要找出问题所在。

方案设计

可以利用端口镜像功能捕获 WAN 口、LAN 口的数据进行分析，在 LAN5 下的电脑安装监控软件，其他接口设置为被镜像端口。

参考应用场景如下：



配置步骤

1. 点击『网络设置』→『端口镜像』。
2. 端口镜像：点击“开启”。
3. 被镜像端口：点击选择被监控端口，如 WAN1、LAN2、LAN3、LAN4。
4. 点击 确定 。

—完成

验证配置

设置完成后，安装有监控软件的电脑（接在路由器的 LAN5 端口上）可以监视其他端口的数据包情况了。

5.5 静态路由

5.5.1 概述

在“静态路由”页面，可以添加静态路由规则。

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。

点击『网络设置』→『静态路由』进入设置页面。

参数说明：

参数	说明
静态路由	点击 +新增 ，手动添加静态路由。
路由表	路由器当前的路由表信息，包括默认路由和添加的静态路由。
目标网络	目的网络地址，即数据包到达的 IP 地址。
子网掩码	目的网络地址的子网掩码。
网关地址	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，设置时，请根据需要，选择相应 WAN 口。

5.5.2 静态路由示例

组网需求

某企业使用W15E进行网络搭建。公司内网和互联网在不同的网络，要求接在路由器下的客户端既能访问互联网又能访问公司内网。

方案设计

设置路由器通过WAN1口接入互联网，通过WAN2口连接公司内网。并在路由器上设置静态路由，实现局域网客户端同时访问两个网络。假设基本信息如下：

公司分配的内网信息：

- IP 地址：192.168.58.190
- 子网掩码：255.255.255.0
- 网关/主 DNS：192.168.58.1

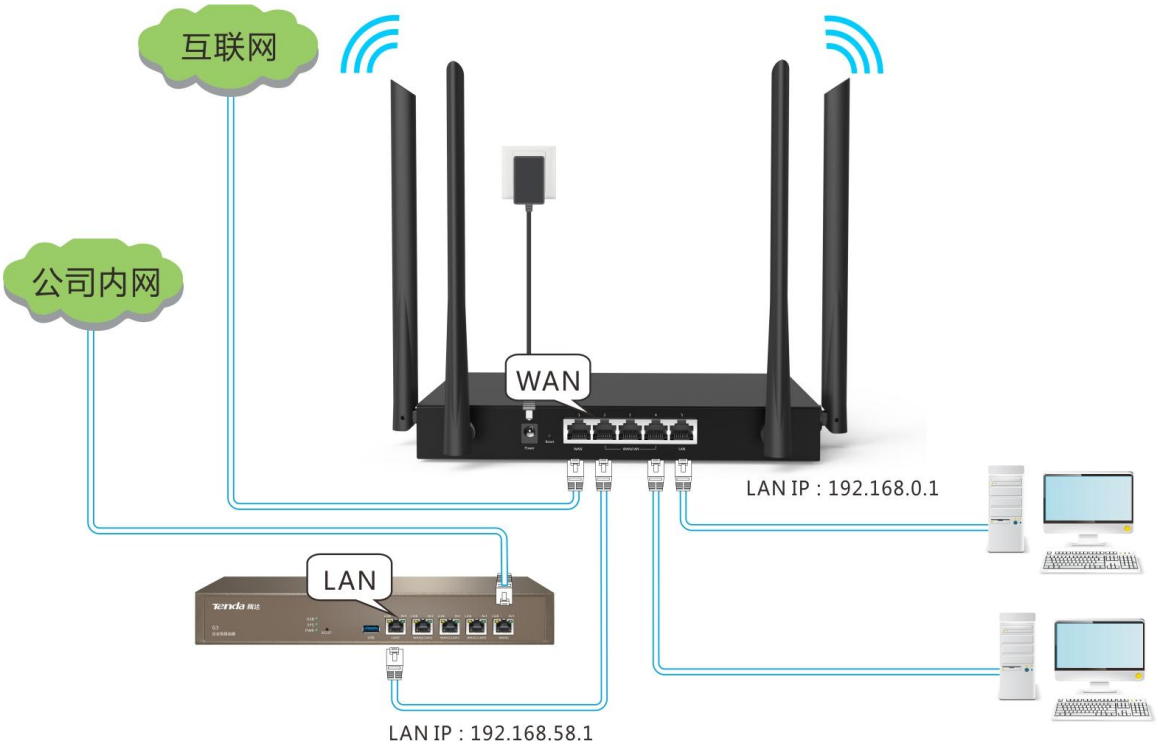
公司分配的访问互联网信息：

- 账号/密码：tenda

公司内网服务器信息：

- IP 地址：172.16.0.0
- 子网掩码：255.255.0.0

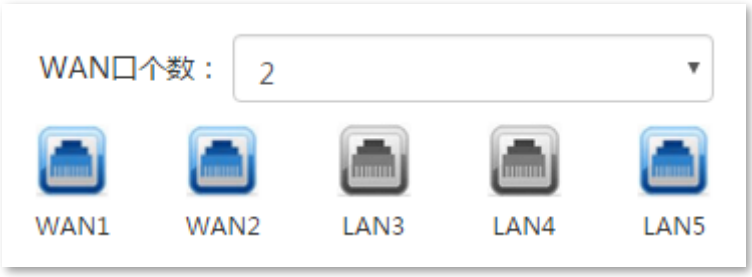
参考拓扑图如下：



配置步骤

步骤 1 根据公司分配的信息设置 WAN 口（互联网接在 WAN1 口，内网接在 WAN2 口）。

启用 2 个 WAN 口，并设置相关信息。如下图所示，详细设置步骤可参考 5.1 上网设置。



步骤 2 设置静态路由器规则。

1. 点击 +新增 。

2. 在弹出的窗口设置静态路由器规则。

(1) 目标网段：输入目的网络地址，本例为“172.16.0.0”。

(2) 子网掩码：输入目 IP 地址的子网掩码，本例为“255.255.0.0”。

(3) 网关地址：输入路由器 WAN1 口的网关地址，本例为“192.168.58.1”。

(4) 接口：选择目的网络接在路由器的接口，本例为“WAN1”。

(5) 点击 确定 。

—完成

完成设置后，新添加的静态路由器规则会显示在路由表中。

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。

5.6 非法 IP 地址拦截

在“非法 IP 地址拦截”页面，可以开启/关闭非法 IP 地址拦截功能。

非法 IP 地址拦截即路由器禁止不正确的 IP 地址上网，本功能默认开启，接在路由器下的客户端可以通过自动获取 IP 地址上网，也可以手动配置正确的 IP 地址、网关、DNS 信息上网。

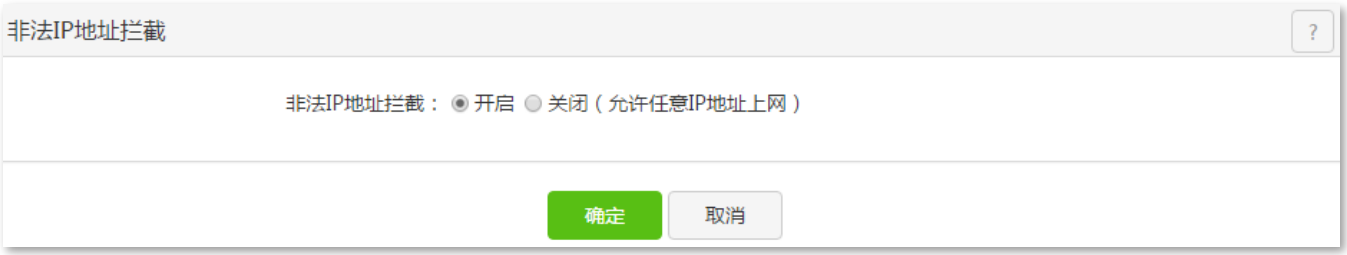
关闭“非法 IP 地址拦截”功能后，路由器下的客户端配置任意 IP 地址信息均可以上网，用户无需修改客户端设备原有网络设置即可上网。

提示

关闭“非法 IP 地址拦截”功能后，不影响客户端自动获取 IP 地址上网，且局域网内的客户端配置任意 **IP 地址**、**网关**、**DNS** 都可以上网。

点击『网络设置』→『非法 IP 地址拦截』，进入设置页面。

本功能默认开启，可根据实际需要点击开启或关闭，然后点击 确定 即可。



5.7 DNS 缓存

在“DNS 缓存”页面，您可以开启/关闭 DNS 缓存功能，设置缓存容量条数。

DNS 缓存功能，即，系统可以记录用户访问网站的 DNS 解析信息。当用户访问的网站存在于缓存中时，系统直接从路由器的 DNS 缓存列表中调用缓存的信息，不必再去询问 DNS 服务器，提高了访问速率。

点击『网络设置』→『DNS 缓存』，进入设置页面。

缓存容量默认为 1000 条，可根据需要修改，最多可设置 10000 条。输入缓存容量值，然后点击 确定 即可。

6 无线设置

无线设置章节包括：

无线基本设置、无线高级设置、WMM 设置、射频优化、访客网络、无线中继、无线访问过滤。

6.1 无线基本设置

6.1.1 概述

在“无线基本设置”页面，您可以开启/关闭相应 WiFi、修改 SSID（无线信号名称）、设置无线密码等。点击『无线设置』进入无线基本设置页面。

提示

- 路由器默认的 2.4G SSID（无线信号名称）为 Tenda_XXXXXX，请查看机壳底部贴纸或无线基本设置页面。
- 如果没有专业人士指导，建议只修改无线名称、无线密码，其它选项保持默认设置。
- WPA-PSK 认证类型的兼容性比较好，WPA2-PSK 认证方式的安全性比较强，请用户根据需要设置。

参数说明：

参数	说明
2.4G/5G 网络总开关	开启/关闭 2.4G 或 5G 无线功能。
无线开关	开启/关闭对应无线网络（主网络、次网络 1、次网络 2）的无线功能。
SSID 广播	SSID（无线名称）的广播状态。 • 开启：路由器广播本 SSID，客户端可以扫描到该 SSID。 • 关闭：路由器不广播本 SSID，SSID 不会显示在客户端的可用网络列表中。客户端连接本无线网络时，需要正确输入本 SSID 名称。
无线名称	显示路由器当前无线网络（主网络、次网络 1、次网络 2）的名称。 路由器连接互联网后，客户端连接该无线网络即可上网。可以根据需要修改路由器的无线名称，即 WiFi 名称。
无线名称编码	选择当前无线名称（SSID）中的中文字符采用的编码格式，默认为 UTF-8。 如果路由器同时启用 2 个或以上 SSID，建议一些 SSID 选择 UTF-8，另一些选择 GB2312，以支持任意无线客户端识别并连接。
安全选项	无线名称的加密方式。 • 不加密：不启用无线加密。 • WPA-PSK：是一种基于标准的可互操作的 WLAN 安全性增强解决方案，采用比 WEP 更强的加密算法。 • WPA2-PSK：能提供比 WEP 或 WPA 更佳的安全性。 • WPA-PSK&WPA2-PSK：同时支持 WPA-PSK 和 WPA2-PSK。
无线密码	无线信号的密码，用于客户端连接相应 WiFi 时输入。为了无线网络安全，强烈建议设置无线密码。
密钥更新周期	无线数据加密密钥自动更新周期，自动更新密钥来增加数据安全性。
最多可接入设备数	设置当前无线名称（SSID）最大允许连接的无线客户端数量。连上该 SSID 的无线客户端数达到此值后，该 SSID 不再接受无线连接请求。
次网络 1/2	本路由器支持两个次无线网络，默认禁用。次网络的设置方法与主网络一致。

6.1.2 修改无线名称、密码

1. 点击『无线设置』。
2. 无线名称：修改无线名称，即 WiFi 名称。
3. 安全选项：选择安全选项，如“WPA-PSK&WPA2-PSK”，在“无线密码”选框设置无线密码。
4. 点击页面底端的 确定 。

—完成

6.2 无线高级设置

6.2.1 概述

在“无线高级设置”页面，您可以修改无线高级参数，调节路由器的无线性能。

如果没有专业人士的指导，建议只修改无线信道，其他选项保持默认设置即可。点击『无线设置』→『无线高级设置』，进入设置页面。

参数说明：

参数	说明
国家	选择国家，以遵从不同国家对信道的支持和管制。
无线功率	路由器对应射频的无线发射功率，单位：dBm。 发射功率越大，无线覆盖范围越广。但适当的减少发射功率更有助于提高无线网络的性能和安全性。
网络模式	显示路由器对应射频的无线网络模式。 2.4G 包括 11b 模式、11g 模式、11b/g 混合模式、11b/g/n 混合模式，默认工作在 11b/g/n 混合模式。 • 11b 模式：仅允许 11b 客户端连接到本路由器，无线速率最大可达 11Mbps； • 11g 模式：仅允许 11g 客户端连接到本路由器，无线速率最大可达 54Mbps； • 11b/g 混合模式：11b、11g 的客户端可以连接到本路由器，无线速率最大可达 54Mbps; • 11b/g/n 混合模式：工作在 11b、11g、11n 模式的客户端均可连接到本路由器，无线速率最大可达 300Mbps（W60E 为 600Mbps）。 5G 包括 11a 模式、11ac 模式、11a/n 混合模式，默认工作在 11ac 模式。 • 11a 模式：仅允许 802.11a 客户端连接到本路由器，无线速率最大可达 54Mbps； • 11ac 模式：允许 802.11ac 客户端连接到本路由器，无线速率最大可达 867Mbps（W60E 为 1300Mbps）； • 11a/n 混合模式：工作在 5G 频段的 802.11a 和 802.11n 客户端均可连接到本路由器，无线速率最大可达 300Mbps（W60E 为 600Mbps）。

参数	说明
SSID 隔离	设置连接路由器同一频段，不同 SSID 的无线客户端的隔离状态。 • 开启：连接不同 SSID 下的无线客户端之间不能互相通信，可增强无线网络的安全性。 • 关闭：连接不同 SSID 下的无线客户端之间能互相通信。
无线频宽	路由器无线信道的频带宽度，单位 MHz。 • 20 MHz：路由器使用 20MHz 的信道带宽。 • 40 MHz：路由器使用 40MHz 的信道带宽。 • 自动：仅适用于 2.4G，路由器根据周围环境，自动调整信道带宽为 20MHz 或 40MHz。 • 80 MHz：仅适用于 5G，路由器使用 80MHz 的信道带宽
无线信道	路由器无线数据传输的通道，建议选择 1，6 或者 11。
扩展信道	40MHz 带宽时，用于确定路由器无线工作的频率段。

6.2.2 修改无线高级参数

1. 点击『无线设置』→『无线高级设置』。
2. 根据需要修改相关参数，如“无线信道”。
3. 点击 确定 。

—完成

6.3 WMM 设置

在“WMM 设置”页面，您可以设置路由器的使用场景。

WMM 是一种无线 QoS 协议，用于保证高优先级的报文有优先的发送权利，从而保证语音、视频等应用在无线网络中有更好的质量。

点击『无线设置』→『WMM 设置』进入页面。

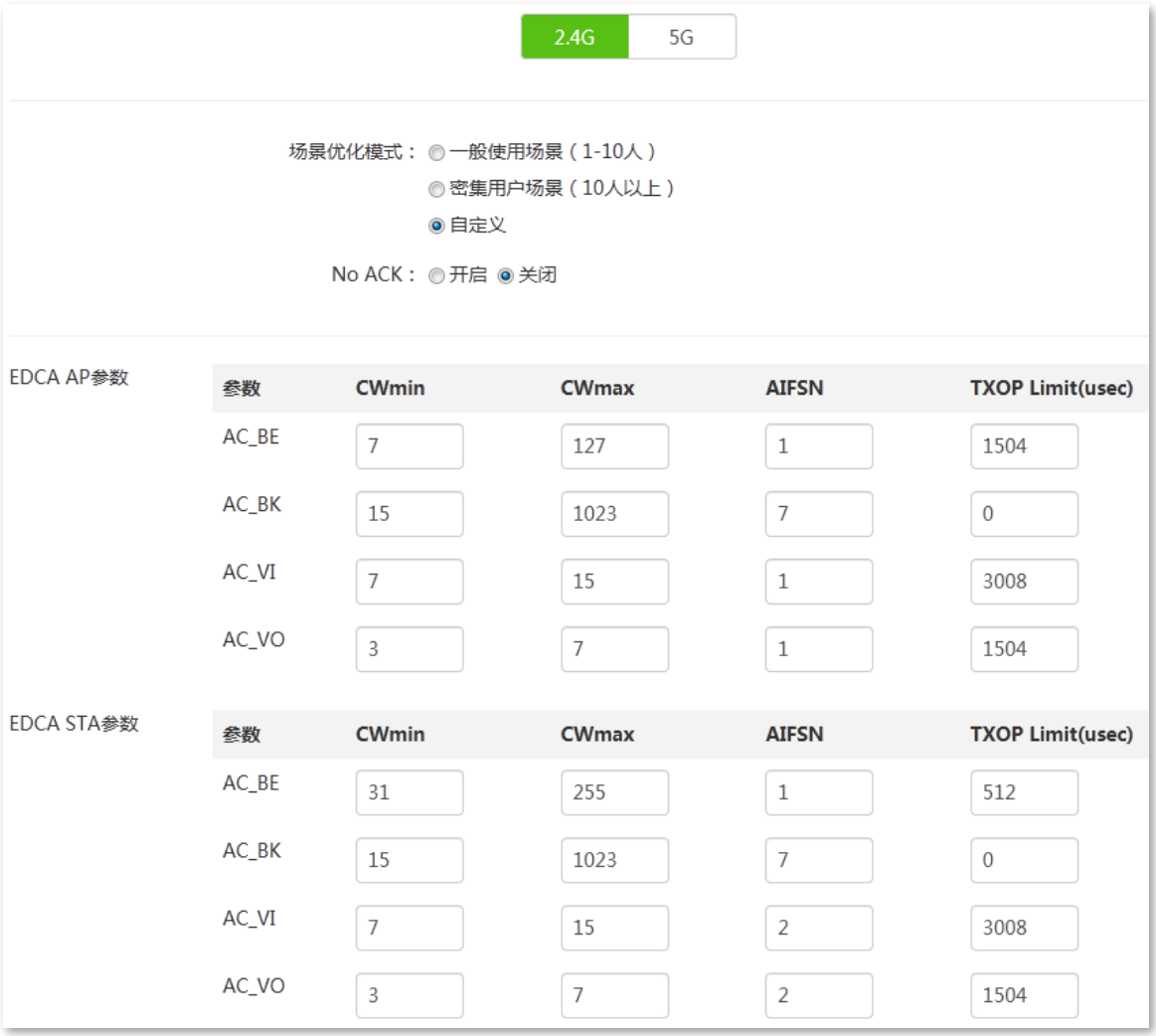
WMM 功能默认启用，并支持 3 种场景优化模式，用户可根据实际环境中路由器的使用场景来选择对应的模式，如下：

- 一般使用场景（1-10 人）：连接路由器 WiFi 用户少于 10 人可选择此项，从而获得较高的吞吐量。
- 密集用户场景（10 人以上）：连接路由器 WiFi 用户 10 人以上可选择此项，保障更高的用户容量。
- 自定义：用户可以自定义 WMM EDCA 参数，进行精细优化，详细内容见下文说明。

自定义 WMM EDCA 参数说明。

场景优化模式选择“自定义”，将会弹出以下页面。

通过优化 AC_BE、AC_BK、AC_VI、AC_VO 的 CWmin、CWmax、AIFSN、TXOP Limit(usec)值可以细化窗口值，从而保障无线业务的稳定性。但是如果没有特殊需要或专业人士指导，请保持默认值。



参数说明：

参数	说明
No ACK	No ACK 是针对通信质量较好，干扰较小的情况下，在无线报文交互过程中，不使用 ACK 报文进行接收确认的一种策略。 No ACK 策略能有效提高传输效率，但在不使用 ACK 确认的情况下，如果通信质量较差，即使接收端没有收到发送包，发送端也不会重发，会造成丢包率增大的问题。
EDCA	EDCA（Enhanced Distributed Channel Access，增强的分布式信道访问）是 WMM 定义的一套信道竞争机制，有利于高优先级的报文享有优先发送的权利和更多的带宽。
EDCA AP 参数	路由器使用的 EDCA 参数。
EDCA STA 参数	客户端的 EDCA 参数。
EDCA 参数	• CWmin：（Exponent form of CWmin）最小竞争窗口指数形式。 • CWmax :(Exponent form of CWmax)最大竞争窗口指数形式。CW ,竞争窗口。CWmin 和 CWmax 决定了平均退避时间值，这两个数值越大，用户的平均退避时间越长。

参数	说明
	• AIFSN：（Arbitration Inter Frame Spacing Number，仲裁帧间隔隙数），802.11 协议中 ,空闲等待时长(DIFS)为固定值 ,WMM 针对不同 AC(AC_BE/AC_BK/AC_VI/AC_VO) 可以配置不同的空闲等待时长，AIFSN 数值越大，用户的空闲等待时间越长。 • TXOP Limit（usec）：Transmission Opportunity Limit，传输机会限制），用户一次竞争成功后，可占用信道的最大时长。这个数值越大，用户一次能占用信道的时长越大，如果是 0，则每次占用信道后只能发送一个报文。
AC_BE、AC_BK、AC_VI、AC_VO	AC（Access Category，接入类），WMM 按照优先级从高到低的顺序分为 AC-VO（语音流）、AC-VI（视频流）、AC-BE（尽力而为流）、AC-BK（背景流）四个优先级队列，越高优先级队列中的报文，抢占信道的能力越高。

6.4 射频优化

在”射频优化”页面，您可以修改射频参数，调试路由器的无线性能，打造优质的无线网络。如果没有专业人士指导，建议不要进行此页面的相关设置，以免降低无线性能。

点击『无线设置』→『射频优化』进入页面。

参数说明：

参数	说明
Short GI	GI（Guard Interval）即保护间隔，射频芯片在使用 OFDM 调制方式发送数据时，被划分成不同的数据块进行发送，为了数据传输的可靠性，数据块之间会有 GI，保证接收侧正确的解析出各个数据块。无线信号在空间传输会因多径等因素在接收侧形成时延，如果后续数据块发送过快，会和前一个数据块形成干扰，而 GI 就是用来规避这个干扰的。 选择自动时，会根据环境自动选择 Short GI 开启或禁用。
接入信号强度限制	设置路由器相关射频可接受的无线客户端信号强度，默认-90dBm。如果无线客户端信号强度比此阈值小，路由器将主动断开无线客户端。
5GHz 优先	仅 5G 射频优化页面有效。 启用后，当 2.4GHz 和 5GHz 两个频段的 SSID 和密码都相同，且无线客户端支持双频 WiFi 时，客户端将会优先选择 5G 频段的 SSID 进行连接。 注意，这种情况下加密方式仅支持 WPA/WPA2-PSK 加密，并且不支持中文 SSID。
部署模式	仅 2.4G 有效，通过调节路由器可接受的客户端信号强度范围，满足用户需求。 • 强覆盖：适用于大面积、多墙体穿透、用户分散、周围无线信号小于 10 个的环境。 • 高密度：高密度用户带机模式，适用于用大面积空旷、用户集中、周围无线信号大于 25 个的环境。 • 中密度：路由器标准工作模式，适用于用大面积空旷、用户集中、周围无线信号小于 25 个的环境。 • 低密度：适用于大面积、多墙体穿透、用户分散、周围无线信号小于 20 个的环境。
穿墙能力	仅 2.4G 有效，通过调节路由器的发射功率，满足用户需求。 • 强覆盖：适用于多墙体穿透的场景。 • 高密度：适用于环境空旷，无需考虑穿墙的场景。常用于用户密度大的情况。
空口调度	开启/关闭空口调度功能。 空口调度可以保证每个客户端的数据传输时长相等，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，提升路由器的整体效率，有效保障了吞吐量。
探测广播报文回复抑制	开启/关闭探测广播报文回复抑制功能。 无线终端默认都在不停的做广播探测扫描，利用 Probe Request（探测请求）帧扫描目前所在区域的无线网络，Probe Request 帧包含 SSID 字段。路由器接收到该报文后会根据此来判断对方能否加入网络，并回应 Probe Response 报文（包含 Beacon 帧所有参数），消耗大量的无线资源。 开启本功能后，路由器针对 SSID 为空的探测请求不进行回复，节省无线资源。

参数	说明
APSD	仅 5G 有效, APSD（Automatic Power Save Delivery），即“自动省电模式”，是 WiFi 联盟的 WMM 省电认证协议。开启“APSD”能降低路由器的电能消耗。默认关闭。
抗干扰模式	仅 2.4G 有效，路由器的干扰抑制模式。 • 关闭：禁用所有干扰抑制。 • 自动：开启硬件和周围环境检测自动抗干扰。
客户端老化时间	客户端连接到路由器的 WiFi 后，如果在该时间段内与路由器没有数据通信，将主动断开该客户端；如果在该时间段内与路由器有数据通信，则停止老化计时。
强制速率、支持速率	通过调整“强制速率”和“支持速率”，可以限制低速率客户端接入，从而提升客户端的使用体验。 强制速率：路由器正常工作所必须的速率集，客户端必须满足路由器所配置的强制速率才能够与路由器进行连接。 支持速率：在路由器的“强制速率集”基础上路由器所能够支持的其他速率集合，支持让客户端在满足强制速率的前提下选择更高的速率与路由器进行连接。

6.5 访客网络

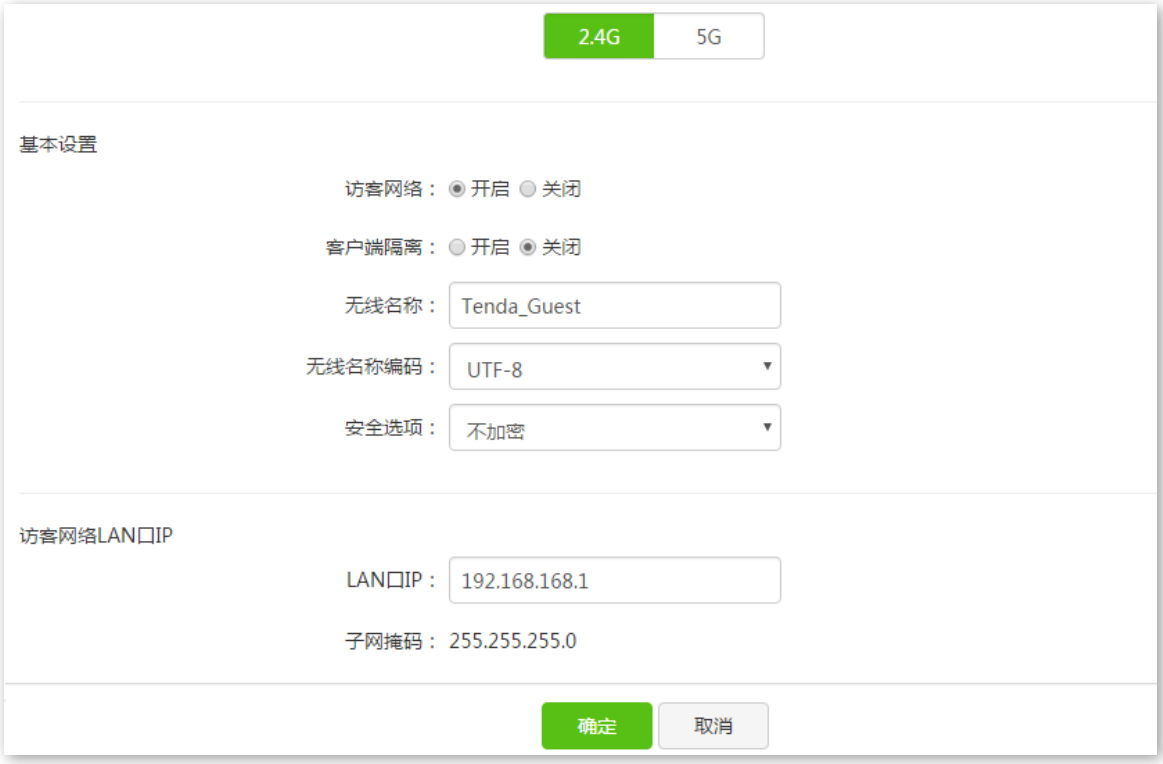
6.5.1 概述

在“访客网络”页面，您可以开启/关闭访客网络功能，修改访客网络 WiFi 名称、无线密码等。

接入访客网络的客户端只能访问互联网或该访客网络下的其他无线客户端，不能访问路由器管理页面或其他局域网，在满足客人上网需求的同时确保主网络安全。

点击『无线设置』→『访客网络』，进入设置页面。访客网络默认关闭。

开启访客网络，页面如下：



参数说明：

参数		说明
基本设置	访客网络	开启/关闭访客网络，默认关闭。
	客户端隔离	连接到访客网络的无线用户的隔离状态。 • 开启 连接该访客网络的设备之间不能互相通信 ,可增强无线网络的安全性。 • 关闭：连接该访客网络的设备之间能互相通信。
	无线名称	路由器访客网络的 WiFi 名称，2.4G 默认为 Tenda_Guest，5G 默认为 Tenda_Guest_5G。 可根据需要修改。为了区别路由器本身的网络名称，建议不要将访客网络的无线名称与路由器本身的无线名称设置成一样。
	无线名称编码	访客网络 WiFi 名称的中文字符采用的编码格式，默认为 UTF-8。 如果修改无线名称为中文后，智能手机等无线客户端搜索不到该无线信号，且可用的无线列表中有显示乱码的无线信号。此时可以将“无线名称编码”改为 GB2312。
	安全选项	访客网络的加密方式。 • 不加密：不启用无线加密。 • WPA-PSK：是一种基于标准的可互操作的 WLAN 安全性增强解决方案，采用比 WEP 更强的加密算法。

参数		说明
		• WPA2-PSK：能提供比 WEP 或 WPA 更佳的安全性。 • WPA-PSK&WPA2-PSK：同时支持 WPA-PSK 和 WPA2-PSK。
	无线密码	访客网络的无线密码，请根据需要设置。
访客网络 LAN 口 IP	LAN 口 IP	访客网络 LAN 口 IP 地址。默认为 192.168.168.1，无线客户端连接访客网络后，会获取到 192.168.168.X 的 IP 地址。如无特殊需要请保持默认设置。
	子网掩码	显示访客网络 LAN 口 IP 地址的子网掩码。

6.5.2 修改访客网络参数

1. 点击『无线设置』→『访客网络』。
2. 根据需要修改相关参数，如修改无线名称为“访客网络”。
3. 点击页面底端的 确定 。

—完成

6.6 无线中继

6.6.1 概述

在“无线中继”页面，您可以桥接上级无线网络，扩展无线覆盖范围。

如果无线客户端距离路由器较远而接收不到路由器的无线信号，可以增加一台支持无线中继功能的路由器，通过无线中继功能来实现扩大无线网络覆盖范围。

点击『无线设置』→『无线中继』，进入设置页面，无线中继功能默认关闭。

开启无线中继功能，页面如下：

进行无线中继设置时，为了方便管理路由器，建议将两台路由器的 LAN 口 IP 地址改为同一网段。

6.6.2 无线中继配置示例

组网需求

某企业使用 W15E 进行网络覆盖，且已经接入互联网。由于企业的面积太大，一台无线网关不能满足无线覆盖需求，现在需要扩大无线覆盖范围。

方案设计

可以增加一台无线路由器，将其放在原路由器的无线网络覆盖范围内，通过设置新增路由器的无线中继功能，使两台路由器建立无线连接，扩大无线网络覆盖范围。

本例以两台 W15E 进行说明。如果使用我司其他型号的路由器或其他厂商的路由器进行无线中继，具体设置方法请参考相关型号的说明书。

参考拓扑图如下：

配置步骤

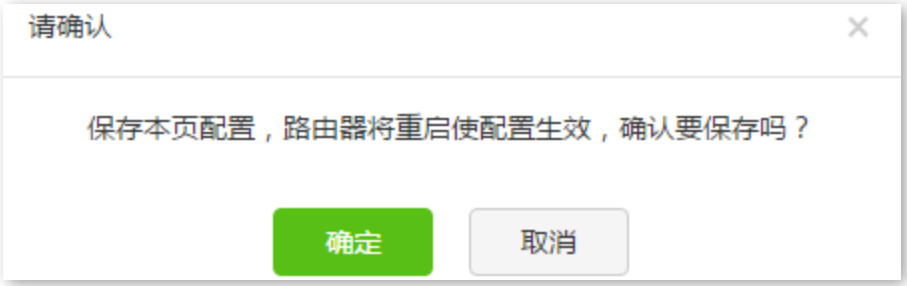
登录路由器 2 进行无线中继设置。

1. 进入『无线设置』→『无线中继』页面。
2. 无线中继：点击“开启”。
3. 点击扫描按钮。

4. 点击下拉框，选择要桥接的无线信号，如“Tenda_888885_5G”。

5. 输入该无线信号的无线密码，如“12345678”。
6. 点击 确定 。

7. 在弹出的对话框点击 确定 。



—完成

配置验证

路由器重启后生效，重新进入无线中继页面，当“联网状态”显示**已连接**时，桥接成功。此时连接路由器 2 的无线名称即可上网，无线名称请进入无线基本设置页面查看。

如果路由器重启后使用原来的 IP 地址不能登录路由器的管理页面，请尝试以下操作：

- 使用域名 www.tendawifi.com 登录。
- 登录上级路由器（本例为路由器 1）查看分配给本路由器（本例为路由器 2）的 IP 地址，然后使用该 IP 地址登录。

6.7 无线访问过滤

6.7.1 概述

在“无线访问过滤”页面，您可以添加允许或禁止连接路由器相应 WiFi 信号的客户端。

笔记本、平板电脑、智能手机等都有各自的 MAC 地址。本路由器支持基于 MAC 地址过滤，即根据无线客户端的 MAC 地址来控制其是否可以连接上 WiFi。

点击『无线设置』→『无线访问过滤』进入页面。无线访问过滤功能默认禁用。如果还要限制上网时间或限制有线客户端上网，可参考 7.3 MAC 地址过滤。

启用无线访问过滤功能后，如下所示：

参数说明：

参数	说明
启用无线访问过滤	启用/禁用无线访问过滤功能，默认禁用。
仅允许	仅允许列表中的无线客户端连上该 SSID。
仅禁止	仅禁止列表中的无线客户端连上该 SSID，其他无线客户端可以连上该 SSID。

参数	说明
+新增	点击此按钮可手动添加要过滤的无线客户端的 MAC 地址。
删除	点击此按钮可以删除选中的规则。
MAC 地址	过滤规则的地址信息。
状态	规则的当前状态，包括启用和禁用。
操作	可对无线访问过滤规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改 MAC 地址、备注。 • 点击可以删除规则。

6.7.2 无线访问过滤配置示例

组网需求

某企业使用 W15E 进行网络覆盖。一般情况下，禁止连接路由器 WiFi 的无线客户端上网。现在招聘人员需要连接 WiFi 信号 Tenda_2FB0C0 访问互联网。

方案设计

可以通过无线客户端过滤功能实现，仅允许招聘人员连接 WiFi 信号 Tenda_2FB0C0 上网。假设招聘人员的笔记本 MAC 地址为 CC:3A:61:71:1B:6E。

配置步骤

1. 点击『无线设置』→『无线访问过滤』。
2. 找到相应无线信号，本例为“Tenda_2FB0C0”，勾选“启用无线访问过滤”选框，点击“仅允许”。
3. 点击 +新增 。

4. 输入允许上网的 MAC 地址，本例为“CC:3A:61:71:1B:6E”。
5. （可选）备注：输入本条规则的备注，如“招聘”。
6. 点击 确定 。

7. 返回“无线访问过滤”规则设置页面，点击 确定 。

—完成

配置验证

只有 MAC 地址为 CC:3A:61:71:1B:6E 的设备才能连接 WiFi 信号 Tenda_2FB0C0 上网。

7 行为管理

行为管理章节包括：

IP 组和时间组、IP 地址过滤、MAC 地址过滤、端口过滤、网络应用过滤、网址分类过滤、多 WAN 策略。

7.1 IP 组和时间组

7.1.1 概述

在“IP 组和时间组”页面，您可以添加 IP 组、时间组。本路由器大部分行为管理功能都是基于 IP 组与时间组进行设置。

点击『行为管理』，进入 IP 组和时间组设置页面。

7.1.2 添加时间组

1. 点击 +新增 。

2. 在弹出的窗口设置时间组规则内容。

(1) 组名称：设置本条规则的名称。

(2) 时间、星期：设置本时间组的具体时间。

(3) 点击 确定 。

—完成

7.1.3 添加 IP 组

1. 点击 +新增 。

2. 在弹出的窗口设置 IP 组规则内容。

(1) 组名称：设置本条规则的名称。

(2) IP 组或 IP 段：设置本 IP 组包含的具体 IP 地址或 IP 地址段。

(3) 点击 确定 。

—完成

7.2 IP 地址过滤

7.2.1 概述

在“IP 地址过滤”页面，您可以添加 IP 地址过滤规则，设置指定 IP 地址访问互联网的权限，包括“允许访问互联网”、“禁止访问互联网”。

点击『行为管理』→『IP 地址过滤』进入设置页面。IP 地址过滤默认关闭，自动获取路由器 IP 地址或手动配置正确 IP 地址信息，都可以访问互联网。

启用规则，页面如下。

参数说明：

参数	说明
IP 地址过滤	开启/关闭 IP 地址过滤功能，默认关闭。
+新增	点击此按钮可以添加 IP 地址过滤规则。
删除	点击此按钮可以删除已选中的规则。
模式	访问互联网的权限。 • 白名单：允许列表中的 IP 地址访问互联网。 • 黑名单：禁止列表中的 IP 地址访问互联网。

参数	说明
IP 地址	禁止/允许访问互联网的 IP 地址。
时间组	IP 地址过滤规则生效的时间。
状态	规则当前的状态，包括已启用和未启用。
操作	可对 IP 地址过滤规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改过滤规则模式、IP 组，时间组、备注。 • 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	规则列表外的主机访问互联网的权限。 • 启用时，未启用的规则中的 IP 以及所有规则以外的 IP 均可以访问互联网。 • 禁用时，只有已启用的白名单规则中的 IP 可以访问互联网。

7.2.2 添加 IP 地址过滤规则

1. 点击『行为管理』→『IP 地址过滤』。
2. 在 IP 地址过滤选项点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 +新增 。

4. 在弹出的窗口设置过滤规则信息，包括过滤模式、IP 组、时间组等。

—完成

7.2.3 IP 地址过滤示例

组网需求

某企业使用 W15E 进行网络搭建。公司规定，上班时间（8:00~18:00）禁止员工上网，局域网 IP 范围是 192.168.0.2~192.168.0.250。

方案设计

可以通过 IP 地址过滤功能实现。

配置步骤

步骤 3 设置时间组（8:00~18:00）如下，详细设置步骤请参考 7.1.2 添加时间组。

步骤 4 设置 IP 组（IP 段为 192.168.0.2~192.168.0.250）如下，详细设置步骤请参考 7.1.3 添加 IP 组。

步骤 5 添加 IP 地址过滤规则。

1. 进入『行为管理』→『IP 地址过滤』页面。
2. 在 IP 地址过滤选项点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 +新增 。

4. 过滤规则：选择相应的规则，本例为“禁止访问互联网”。
5. IP 组：点击下拉框，选择规则生效的 IP 组，如“IP 组 1”。
6. 时间组：点击下拉框，选择规则生效的时间组，如“时间组 1”。
7. （可选）备注：输入本条规则的备注，如“员工”。

8. 点击 确定 。

—完成

规则添加成功，如下：

配置验证

IP 地址为 192.168.0.2~192.168.0.250，在 8:00~18:00 的时间不能访问互联网，其他时间可以访问互联网。

7.3 MAC 地址过滤

7.3.1 概述

在“MAC 地址过滤”页面，您可以添加 MAC 地址过滤规则，设置指定 MAC 地址访问互联网的权限，包括“允许访问互联网”、“禁止访问互联网”。

点击『行为管理』→『MAC 地址过滤』进入设置页面。

启用规则，页面如下。

参数说明：

参数	说明
MAC 地址过滤	开启/关闭 MAC 地址过滤功能，默认关闭。
+新增	点击此按钮可以添加 MAC 地址过滤规则。
删除	点击此按钮可以删除已选中的规则。
模式	访问互联网的权限。 • 白名单：允许使用该 MAC 地址的设备访问互联网。 • 黑名单：禁止使用该 MAC 地址的设备访问互联网。
MAC 地址	客户端设备的 MAC 地址。

参数	说明
时间	禁止/允许列表中对应的设备访问互联网的时间。
状态	规则当前的状态，包括已启用和未启用。
操作	可对 MAC 地址过滤规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改过滤规则模式、时间组、MAC 地址、备注。 • 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	规则列表外的主机访问互联网的权限。 • 启用时，列表中未启用规则的设备和列表外的设备均可以访问互联网。 • 禁用时，只有列表中的规则生效，列表中未启用规则的设备和列表外的设备均不能访问互联网。

7.3.2 添加 MAC 地址过滤规则

1. 进入『行为管理』→『MAC 地址过滤』页面。
2. 在 MAC 地址过滤选项点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 +新增 。

4. 在弹出的窗口设置过滤规则信息，包括过滤规则、时间组、MAC 地址等。

—完成

7.3.3 MAC 地址过滤示例

组网需求

某企业使用 W15E 进行网络搭建。上班时间禁止员工上网，但允许招聘人员上班时间（8:00~18:00）访问互联网。

方案设计

可以通过 MAC 地址过滤功能实现，假设允许上网的 MAC 地址为 CC:3A:61:71:1B:6E。

配置步骤

步骤 1 设置时间组（8:00~18:00）如下，详细设置步骤请参考 7.1.2 添加时间组。

步骤 2 添加 MAC 地址过滤规则。

1. 点击『行为管理』→『MAC 地址过滤』。
2. 在 MAC 地址过滤选项点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 +新增 。

4. 过滤规则：选择相应的规则，本例为“允许访问互联网”。
5. 时间组：点击下拉框，选择规则生效的时间组。
6. MAC 地址：输入相应 MAC 地址信息，本例为“CC:3A:61:71:1B:6E”。
7. （可选）备注：输入本条规则的备注，如“招聘”。
8. 点击 确定 。

9. 返回 MAC 地址过滤页面，禁用“允许未启用规则和列表外的主机访问互联网”，然后点击 确定 。

—完成

规则添加成功，如下：

配置验证

在 8:00~18:00 的时间，只有 MAC 地址为 CC:3A:61:71:1B:6E 可以访问互联网。

7.4 端口过滤

7.4.1 概述

在“端口过滤”页面，您可以添加端口过滤规则，限制局域网客户端访问指定端口。

互联网上众多服务所涉及的网络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。为了方便对局域网中的客户端进行进一步管理，可以通过设置端口过滤功能来控制局域网中客户端对互联网上某些端口的访问。

点击『行为管理』→『端口过滤』进入设置页面。

启用规则，页面如下。

参数说明：

参数	说明
端口过滤	开启/关闭端口过滤功能，默认关闭。
+新增	点击此按钮可以添加端口过滤规则。
删除	点击此按钮可以删除已选中的规则。
IP 组	规则生效的 IP 组。
时间组	规则生效的时间，即禁止规则中 IP 组对应的设备访问指定服务的时间。
端口号	禁止访问的服务的端口号。

参数	说明
协议类型	禁止访问的服务使用的协议，建议保持默认设置。
状态	规则当前的状态，包括已启用和未启用。
操作	可对端口过滤规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改过滤规则模式、IP 组，时间组、备注。 • 点击可以删除规则。

7.4.2 添加端口过滤规则

1. 点击『行为管理』→『端口过滤』。
2. 在端口过滤选项点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 +新增 。

4. 在弹出的窗口设置过滤规则信息，包括过滤模式、IP 组、时间组等。

—完成

7.4.3 端口过滤示例

组网需求

某企业使用 W15E 进行网络搭建。要求局域网中 192.168.0.2~192.168.0.250 的电脑在星期一到星期五的 8:00-18:00（上班时间）不能浏览网页（浏览网页服务默认的端口号是 80）。

方案设计

可以通过端口过滤功能实现。

配置步骤

步骤 1 设置时间组（8:00~18:00）如下，详细设置步骤请参考 7.1.2 添加时间组。

步骤 2 设置 IP 组（IP 段为 192.168.0.2~192.168.0.250）如下，详细设置步骤请参考 7.1.3 添加 IP 组。

步骤 3 添加端口过滤规则。

1. 点击『行为管理』→『端口过滤』。
2. 在端口过滤选项点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 +新增 。

4. IP 组：点击下拉框，选择规则生效的 IP 组，如“IP 组 1”。
5. 时间组：点击下拉框，选择规则生效的时间组，如“时间组 1”。
6. 端口或端口段：设置禁止局域网访问的服务端口，可以是单个端口或端口段，本例为“80”。
7. 协议类型：设置所禁止服务使用的协议，建议保持默认设置。
8. 点击 确定 。

—完成

规则添加成功，如下：

配置验证

IP 地址为 192.168.0.2~192.168.0.250，在 8:00~18:00 的时间不能访问网页，其他时间可以访问。

7.5 网络应用过滤

7.5.1 概述

在“网络应用过滤”设置页面，您可以禁止局域网指定客户端使用指定的应用，如通讯软件、视频软件、音乐软件等。

点击『行为管理』→『网络应用过滤』进入设置页面。

启用规则，页面如下。

参数说明：

参数		说明
网络应用过滤	网络应用过滤	开启/关闭网络应用过滤功能，默认关闭。
	+新增过滤规则	点击此按钮可以添加网络应用过滤规则。
	删除	点击此按钮可以删除已选中的规则。
	IP 组	规则生效的 IP 组。
	时间组	规则生效的时间。
	过滤应用	禁止 IP 组对应的客户端使用的应用。
	状态	规则当前的状态，包括已启用和未启用。
	操作	可对网络应用过滤规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改 IP 组，时间组、过滤应用。 • 点击可以删除规则。
QQ 过滤	QQ 过滤	开启/关闭 QQ 过滤功能，默认关闭。
	+新增例外QQ号	点击此按钮可以添加 QQ 号。
	例外 QQ 号	可以访问互联网的 QQ 号。
	备注	对规则的描述。设置规则时，如果没有设置，则不显示。
	操作	删除对应的规则。

7.5.2 添加网络应用过滤规则

1. 点击『行为管理』→『网络应用过滤』。
2. 在网络应用过滤模块点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 +新增过滤规则 。

4. 在弹出的窗口设置过滤规则信息，包括 IP 组、时间组、应用类别等。

—完成

7.5.3 添加允许上网的 QQ

1. 点击『行为管理』→『网络应用过滤』。
2. 在 QQ 过滤模块点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 +新增例外 QQ 号 。

4. 在弹出的窗口设置规则信息，包括 QQ 号码、备注等。

—完成

7.5.4 网络应用过滤示例

组网需求

某企业使用 W15E 进行网络搭建。要求局域网中 192.168.0.2~192.168.0.250 的电脑在星期一到星期五的 8:00-18:00（上班时间）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，同时不能使用 QQ，但是允许一些技术支持人员使用 QQ 与客户沟通。

方案设计

可以通过网络应用过滤功能实现，添加禁止局域网指定客户端使用的应用；添加允许正常使用的 QQ 号码，假设技术人员的 QQ 号为 987654321。

配置步骤

步骤 1 设置时间组（8:00~18:00）如下，详细设置步骤请参考 7.1.2 添加时间组。

步骤 2 设置 IP 组（IP 段为 192.168.0.2~192.168.0.250）如下，详细设置步骤请参考 7.1.3 添加 IP 组。

步骤 3 设置“网络应用过滤”功能。

1. 在“网络应用过滤”和“QQ 过滤”模块点击“开启”，点击页面底端的 确定 ，启用过滤功能。

2. 设置“网络应用过滤”规则内容。

(1) 点击 +新增过滤规则 。

(2) IP 组：点击下拉框，选择规则运用的 IP 组，如“IP 组 1”。

(3) 时间组：点击下拉框，选择规则运用的时间组，如“时间组 1”。

(4) 应用类别：选择禁止客户端使用的应用类型。

(5) 请选择：选择某一应用中禁止客户端使用的程序。可通过“全选、反选”进行快速选择。

(6) 点击 确定 。

步骤 4 设置“QQ 过滤”。

1. 点击 +新增例外 QQ 号 。

2. QQ 号码：输入允许上网 QQ 号，本例为“987654321”。
3. （可选）备注：输入该 QQ 号的描述，如“技术支持”。
4. 点击 确定 。

—完成

规则添加完成，如下图示：

配置验证

局域网中 192.168.0.2~192.168.0.250 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 987654321 的 QQ 号可以正常使用。

7.6 网址分类过滤

7.6.1 概述

在“网址分类过滤”页面，您可以禁止局域网指定客户端访问指定类别的网站，如购物、团购、视频等。

点击『行为管理』→『网址分类过滤』进入设置页面。

启用规则，页面如下。

参数说明：

参数	说明
网址分类过滤	开启/关闭网址分类过滤功能，默认关闭。
+新增	点击此按钮可以添加网址分类过滤规则。
删除	点击此按钮可以删除已选中的规则。
IP 组	规则生效的 IP 组。
时间	规则生效的时间，即禁止规则中 IP 组对应的客户端访问指定网址的时间。
过滤网址	禁止客户端访问的网址类。

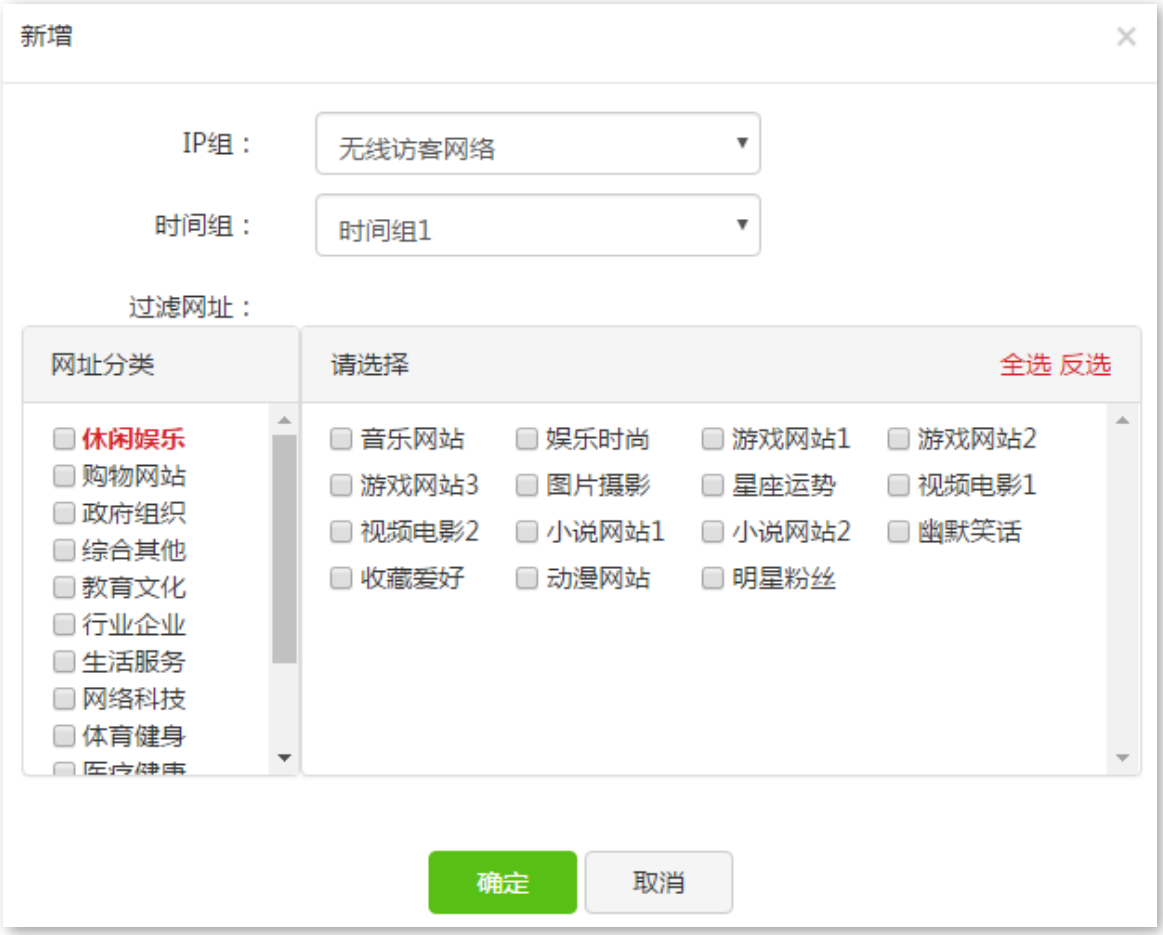
参数	说明
状态	规则当前的状态，包括已启用和未启用。
操作	可对网址分类过滤规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改 IP 组，时间组、过滤网址。 • 点击可以删除规则。
网址分类管理	路由器默认的网址分类，可以点击 网址分类管理 可以查看、增加网址。

7.6.2 新增网址过滤规则

1. 点击『行为管理』→『网址分类过滤』。
2. 在网址分类过滤选项点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 +新增 。

4. 在弹出的窗口设置过滤规则信息，包括包括 IP 组、时间组、过滤网址等。



—完成

7.6.3 新增网址分类

1. 点击『行为管理』→『网址分类过滤』。
2. 在网址分类过滤选项点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 网址分类管理 。

4. 点击 +新增分类 。

5. 在弹出的窗口设置规则信息，包括包括组名称、网址、描述等。

—完成

7.6.4 网址分类过滤示例

组网需求

某企业使用 W15E 进行网络搭建。要求局域网中 192.168.0.2~192.168.0.250 的电脑在星期一到星期五的 8:00-18:00（上班时间）不能浏览休闲娱乐、购物网站的网址。

方案设计

可以通过网址分类过滤功能实现，添加禁止局域网指定客户端访问相关网站。

配置步骤

步骤 1 设置时间组（8:00~18:00）如下，详细设置步骤请参考 7.1.2 添加时间组。

步骤 2 设置 IP 组（IP 段为 192.168.0.2~192.168.0.250）如下，详细设置步骤请参考 7.1.3 添加 IP 组。

步骤 3 设置“网址分类过滤”功能。

1. 点击『行为管理』→『网址分类过滤』。
2. 在网址分类过滤选项点击“开启”，点击页面底端的 确定 ，启用过滤功能。

3. 点击 +新增 。

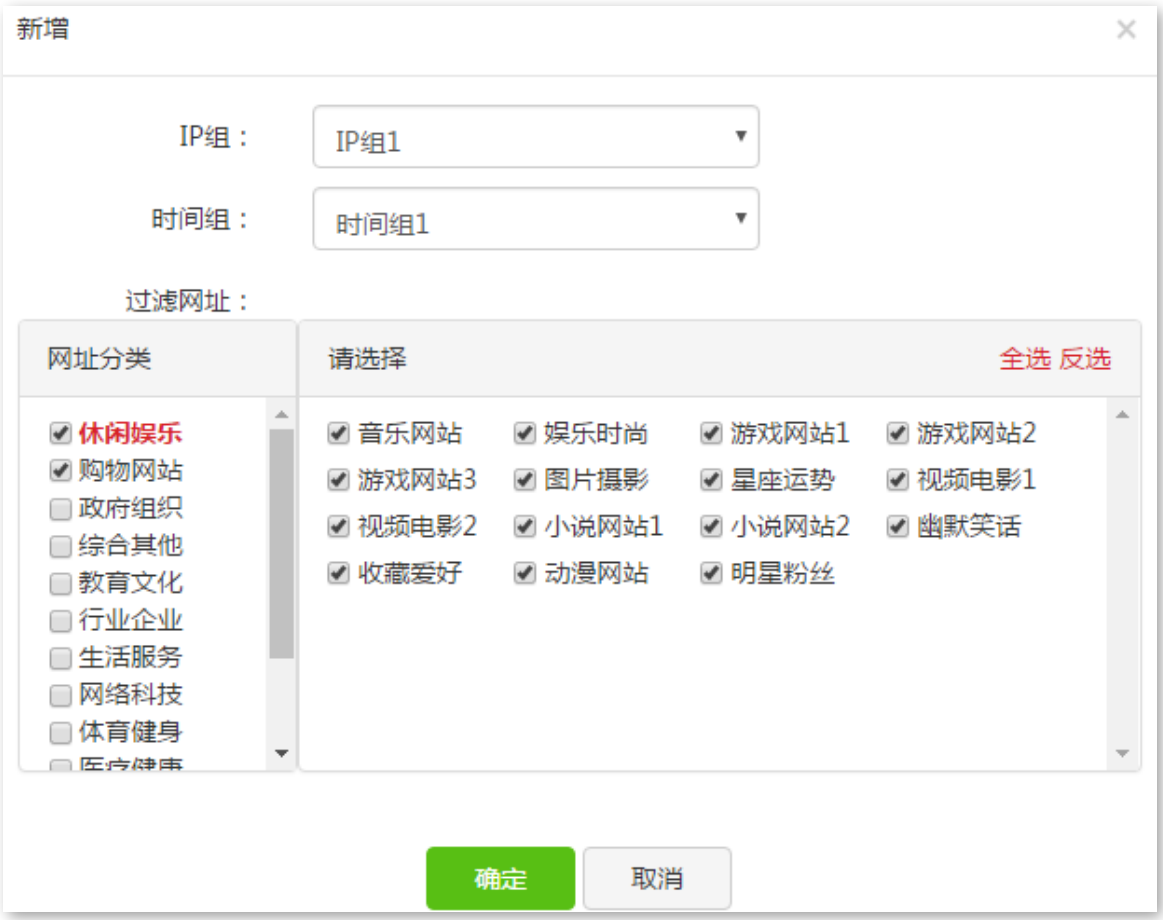
(1) IP 组：点击下拉框，选择规则运用的 IP 组，如“IP 组 1”。

(2) 时间组：点击下拉框，选择规则运用的时间组，如“时间组 1”。

(3) 网址分类：选择禁止客户端访问的网站类型。

(4) 请选择：选择禁止客户端访问的网站。可通过“全选、反选”进行快速选择。

(5) 点击 确定 。



—完成

设置成功，如下所示。

配置验证

局域网中 192.168.0.2~192.168.0.250 的电脑在星期一到星期五 8:00-18:00 不能浏览购物、团购、小说等网站。

7.7 多 WAN 策略

7.7.1 概述

在“多 WAN 策略”页面，您可以设置路由器 WAN 口策略，路由器启用多个 WAN 口时，可以设置本功能。路由器 WAN 口策略支持两种模式：智能负载均衡和自定义策略。

点击『行为管理』→『多 WAN 策略』进入设置页面。

参数说明：

参数	说明
多 WAN 策略	路由器 WAN 口的策略。 • 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。 • 自定义策略：用户根据实际需要，针对特定的源地址指定对应的 WAN 口。
广域网线路侦测	开启后，路由器会定期检测 WAN 口与“侦测地址”的连通情况。 • 侦测地址：需侦测的 IP 或域名。 • 侦测间隔：侦测时间间隔，默认为 5 分钟侦测一次，最大可配置 200 分钟。

7.7.2 自定义策略规则

1. 点击『行为管理』→『多 WAN 策略』。
2. 在“多 WAN 策略”模块点击“自定义策略”，点击页面底端的 确定 ，启用多 WAN 策略功能。
3. 点击 +新增 。

4. 设置多 WAN 策略规则信息，包括包括 IP 组、指定 WAN 口等。

—完成

参数说明：

参数	说明
+新增	点击此按钮可以添加网址分类过滤规则。
删除	点击此按钮可以删除已选中的规则。
IP 组	规则生效的 IP 组。
指定 WAN 口	IP 组数据出入的 WAN 口。
状态	规则当前的状态，包括已启用和未启用。
操作	可对多 WAN 策略规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改 IP 组，指定 WAN 口。 • 点击可以删除规则。

7.7.3 用户自定义策略示例

组网需求

某企业使用 W15E 进行网络搭建。为了满足企业网络需求，办理了中国电信和中国移动两个宽带业务。并且已经成功访问互联网，为了更好的管理网络，可以进行多 WAN 策略设置。

配置步骤

步骤 1 添加应用于本 WAN 口策略的 IP 组，本例为 192.168.0.2~192.168.0.250，详细设置步骤请参考 7.1.3 添加 IP 组。

步骤 2 设置 WAN 口策略规则。

1. 点击『行为管理』→『多 WAN 策略』。
2. 在“多 WAN 策略”模块点击“自定义策略”，点击页面底端的 确定 ，启用多 WAN 策略功能。
3. 点击 +新增 。

4. IP 组：点击下拉框，选择相应的 IP 组，如“IP 组 1”。
5. 指定 WAN 口：选择 IP 组的数据流出入的 WAN 口，如“WAN1”。
6. 点击 确定 。

—完成

设置成功，如下图示：

配置验证

局域网中 192.168.0.2~192.168.0.250 设备的数据将会走 WAN1 口。

8 网速控制

8.1 概述

在“网速控制”页面，您可以设置各 WAN 口的最大上传/下载速度，添加网速控制规则，实现对数据传输的带宽控制，从而使有限的带宽资源得到合理分配，达到有效利用现有带宽的目的。

点击『网速控制』，进入设置页面。

参数说明：

参数	说明
WAN 带宽	设置所办理的宽带的带宽，不清楚时，可以咨询您的 ISP。
网速控制	当前 WAN 口的限速规则。 • 不限速：不启用网速控制功能。 • 智能限速：路由器根据实际情况给客户端智能分配带宽。 • 单独限速：手动给客户端设置带宽。

8.2 设置智能限速

点击『网速控制』。在“网速控制”模块选择“智能限速”，点击 确定 ，即可。

8.3 设置单独限速

1. 点击『网速控制』。
2. 在“网速控制”模块选择“单独限速”。
3. 在出现的页面设置限速规则信息。
4. 点击页面底端的 确定 。

—完成

参数说明：

参数	说明
+新增	点击此按钮可以添加客户端限速规则。
删除	点击此按钮可以删除已选中的规则。
IP 组	网速限速规则生效的 IP 组。
时间组	网速限速规则生效时间。
单台并发连接数	受控 IP 地址范围中，每台电脑的最大连接总数。
模式	网速控制规则的模式。 • 共享 受控地址范围内所有 IP 地址带宽总和为当前规则设置的上传/下载速率。 • 独享：受控地址范围内每一个 IP 地址都应用当前规则设置的上传/下载速率。

参数	说明
上传/下载速率	对应规则下的客户端的最大上传/下载速率。1Mbps=128KB/s=1024kb/s
状态	规则当前的状态，包括已启用和未启用。
操作	可对网速控制规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改 IP 组，时间组、上传/下载速率等。 • 点击可以删除规则。
未受控的主机默认为	• 启用时，列表中未启用规则的设备和列表外的设备的带宽情况为“默认参数”。 • 禁用时，只有列表中的规则生效，列表中未启用规则的设备和列表外的设备的带宽均不受限制。
访客网络流控	访客网络中，单个客户端的最大上传/下载速度。

8.4 单独限速示例

组网需求

某企业使用 W15E 进行网络搭建。路由器的 LAN 口 IP 地址为 192.168.0.1，子网掩码为 255.255.255.0。现要对路由器下的客户端设置带宽控制，每个客户端有固定的带宽。IP 地址为 192.168.0.2~192.168.0.250，带宽限制的时间段为：8:00~18:00。

配置步骤

步骤 1 设置时间组（8:00~18:00）如下，详细设置步骤请参考 7.1.2 添加时间组。

步骤 2 设置 IP 组（IP 段为 192.168.0.2~192.168.0.250）如下，详细设置步骤请参考 7.1.3 添加 IP 组。

步骤 3 添加单独限速规则。

1. 点击『网速控制』。
2. 在“网速控制”模块选择“单独限速”，点击页面底端的 确定 ，启用该功能。

3. 点击 +新增 。

4. IP 组：点击下拉框，选择规则应用的 IP 组，如“IP 组 1”。
5. 时间组：点击下拉框，选择规则应用的时间组，如“时间组 1”。

6. 单台设备并发连接数：如无特殊情况，建议设置为 300。
7. 模式：选择“独享”。
8. 上传/下载速率：设置客户端的最大上传/下载速率。
9. 点击 确定 。

—完成

完成设置，如下所示：

配置验证

IP 地址为 192.168.0.2~192.168.0.250 的用户，在 8:00~18:00 的最大上传速率为 128KB/s，最大下载速率为 512KB/s。

9 VPN 服务

VPN 服务章节包括：

PPTP/L2TP 客户端、PPTP/L2TP 服务器、IPSec。

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，但因为这个专用网络只是逻辑存在并没有实际物理线路，故称为虚拟专用网。VPN 技术可以使分公司的企业员工方便地共享对方的局域网资源或公司总部的局域网资源，且这些资源不会暴露给互联网上的其他用户。

VPN 通过隧道技术在两个站点间建立一条虚拟的专用线路，使用端到端的认证和加密保证数据的安全性。本路由器支持的隧道协议包括二层隧道协议 PPTP、L2TP 以及三层隧道协议 IPSec。

9.1 PPTP/L2TP 客户端

在“PPTP/L2TP 客户端”页面，您可以设置路由器为 PPTP/L2TP 客户端。

启用 PPTP/L2TP 客户端功能后，本路由器可以连接到 VPN 服务端。如：企业分支机构与企业总部之间需要实现简单安全的信息互访，可以在企业总部路由器使用 VPN 服务端功能，分支机构路由器中使用 VPN 客户端功能完成操作。

点击『VPN 服务』，进入 PPTP/L2TP 客户端设置页面。

启用“PPTP/L2TP 客户端”，页面如下。

参数说明：

参数	说明
PPTP/L2TP 客户端	开启/关闭 PPTP/L2TP 客户端功能。启用后，路由器作为 VPN 客户端。
客户端类型	路由器充当的客户端类型，包括 PPTP 和 L2TP。
WAN 口	选择路由器开启 PPTP/L2TP 客户端的 WAN 口。
服务器 IP/域名	输入需要连接到的 VPN 服务器 IP 地址/域名，一般是对端充当 VPN 服务器的路由器开启“PPTP/L2TP 服务器”功能的 WAN 口 IP 地址。
用户名/密码	输入 VPN 服务器分配给 PPTP/L2TP 客户端的用户名/密码。
加密	是否启用数据加密。服务器与客户端要设置一致，仅适用于 PPTP。
VPN 代理上网	VPN 规则建立后，启用本功能时，客户端路由器可以通过服务器端路由器上网。
服务器内网网段	VPN 服务器下局域网的网段。
内网子网掩码	VPN 服务器下局域网的子网掩码。
状态	显示当前 VPN 客户端的连接状态。

9.2 PPTP/L2TP 服务器

在“PPTP/L2TP 服务器”页面，您可以设置路由器为 PPTP/L2TP 服务器。

PPTP/L2TP 服务器允许指定的 VPN 用户拨入服务器。如：企业分支机构与企业总部之间需要实现简单安全的信息互访。可以在企业总部路由器使用 VPN 服务器功能，分支机构路由器中使用 VPN 客户端功能完成操作。

点击『VPN 服务』→『PPTP/L2TP 服务器』，进入设置页面。

启用“PPTP/L2TP 服务器”，页面如下。

参数说明：

参数		说明
PPTP/L2TP 服务器	服务器状态	开启/关闭 PPTP/L2TP 服务器功能。启用后，路由器作为 VPN 服务器。
	服务器类型	路由器充当的服务器类型，包括 PPTP 服务器和 L2TP 服务器。
	WAN 口	路由器开启 PPTP/L2TP 服务器的 WAN 口。在需要连接到本服务器的 VPN 客户端路由器上，将“服务器 IP 地址/域名”填写为此接口的的 IP 地址。
	加密	是否启用数据加密。服务器与客户端要设置一致，仅适用于 PPTP。
	地址池网段	服务器分配给 PPTP/L2TP 客户端的 IP 地址段。
	最大连接数	允许接入的最大 PPTP/L2TP 客户端数量，系统固定为 32 个。
PPTP/L2TP 用户	+新增	点击此按钮可以添加 VPN 用户名和密码。
	删除	点击此按钮可以删除已选中的规则。
	用户名/密码	设置 PPTP/L2TP 客户端连接 PPTP/L2TP 服务器时使用的用户名和密码。
	是否网段	客户端是网络或是主机。PPTP/L2TP 客户端是一个网络时，需要设置 PPTP/L2TP 局域网的网段和掩码。
	网段	当 PPTP/L2TP 客户端是一个网络时，此项需要设置。输入 PPTP/L2TP 客户端的局域网 IP 网段。如 192.168.1.0。
	掩码	当 PPTP/L2TP 客户端是一个网络时，此项需要设置。设置 PPTP/L2TP 客户端的局域网子网掩码。
	备注	该用户的描述。如果在设置规则时，没有设置，则不显示。
	操作	可对用户规则进行如下操作： • 点击 可以编辑规则信息，包括修改用户名，密码、是否为网段、备注。 • 点击 可以删除规则。

9.3 IPSec

在“IPSec”页面，您可以添加 IPSec 隧道。

IPSec（IP Security，IP 安全性）是一系列服务和协议的集合，在 IP 网络中保护端对端通信的安全性、防止网络攻击。可通过网络两端分别建立 IPSec VPN 隧道，实现安全通信。

点击『VPN 服务』→『IPSec』，进入设置页面。

启用 IPSec，如下图示。

参数说明：

参数	说明
IPSec	开启/关闭 IPSec 功能。
WAN 口	路由器开启 IPSec 的 WAN 口。该接口的 IP 是对端路由器的“远端网关地址”信息。
连接名称	为本 IPSec 连接设置一个名称，方便识别。
隧道协议	请根据需要选择 ESP、AH 或者 AH+ESP。 • AH，即 Authentication Header，鉴别首部，AH 协议用于保证数据的完整性，若数据报文在传输过程中被篡改，报文接收方将在完整性验证时丢弃报文。 • ESP，即 Encapsulating Security Payload，封装安全性载荷。ESP 协议用于数据完整性检查以及数据加密，加密后的报文即使被截取，第三方也难以获取真实信息。
远端网关地址	对端路由器启用 IPSec 的 WAN 口的 IP 地址或该 IP 地址绑定的域名。
本地内网网段/掩码	本路由器的内网 IP 网段/子网掩码。
远端内网网段/掩码	对端路由器的内网 IP 网段/子网掩码。
密钥协商方式	默认为自动协商。如果要设置为“手动设置”，具体设置信息请参考密钥协商方式—手动设置。
预共享密钥	双方互相认证的密钥，本路由器和对端路由器的预共享密钥必须相同。

- **密钥协商方式—自动协商**

  密钥协商方式为“自动协商”时，整个协商过程被分为两个阶段。

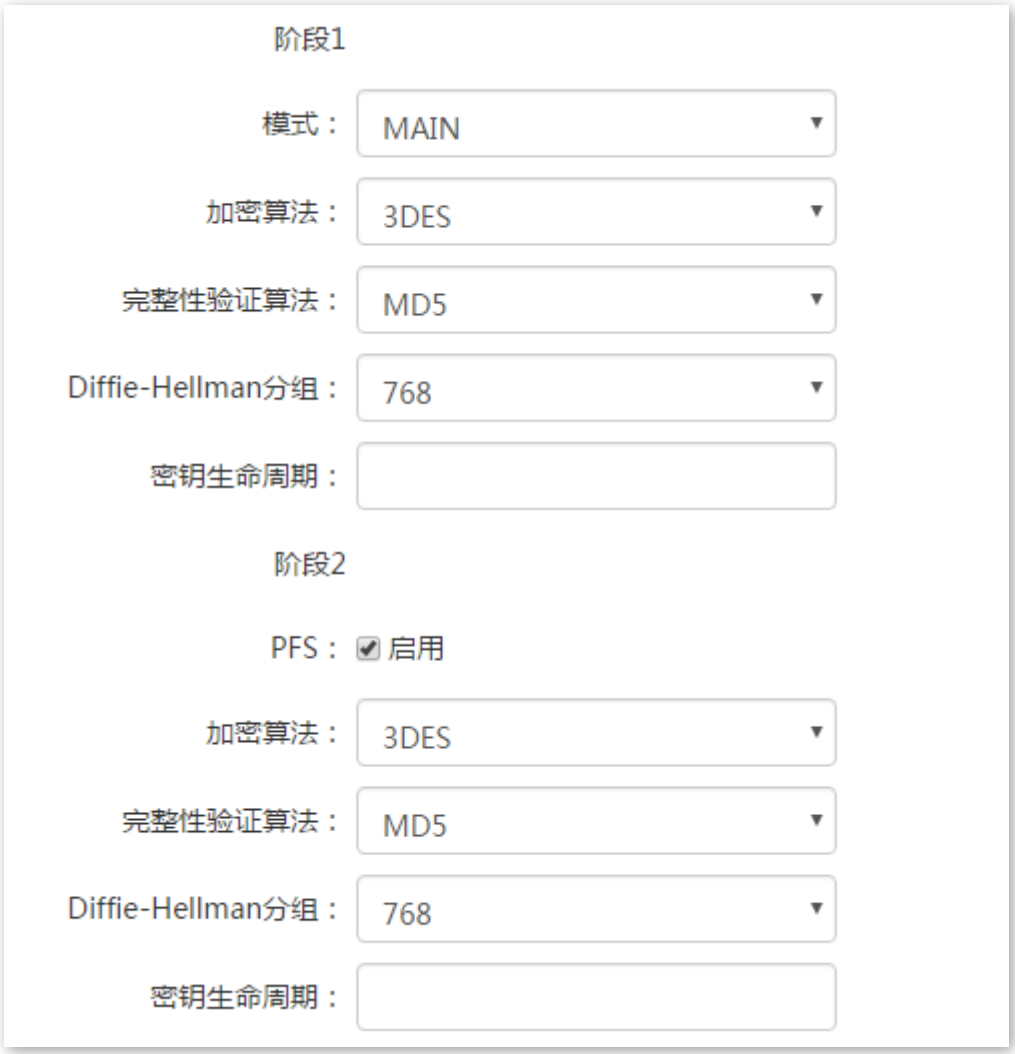
  阶段 1，通信双方将协商交换验证算法、加密算法等安全提议，并建立一个 ISAKMP SA，用于在阶段 2 中安全交换更多信息。

  阶段 2，使用阶段 1 中建立的 ISAKMP SA 为 IPSec 的安全性协议协商参数，创建 IPSec SA，用于对双方的通信数据进行保护。

  提示

  - **ISAKMP**：Internet Security Association and Key Management Protocol，互联网安全性关联和密钥管理协议。
  - **SA**：Security Association，安全联盟。
  - **IKE**：Internet Key Exchange，互联网密钥交换协议。

IPSec 隧道高级参数说明。点击“显示高级设置...”后将会弹出以下页面：



参数说明：

参数	说明
模式	设置阶段 1 协商的交换模式，该交换模式必须与对端相同。交换模式有以下两种： • 主模式（MAIN）：该模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。 • 野蛮模式（AGGRESSIVE）：又称主动模式，该模式不提供身份保护，双方交换报文少，协商速度快，适用于对身份保护要求不高的场合。
加密算法	选择应用于 IKE 会话的加密算法。本路由器支持以下加密算法： • DES（Data Encryption Standard，数据加密标准）：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。 • AES（Advanced Encryption Standard，高级加密标准）：AES128/192/256 表示使用长度为 128/192/256 bit 的密钥进行加密。

参数	说明
完整性验证算法	选择应用于 IKE 会话的验证算法。 本路由器支持以下验证算法： • MD5（Message Digest Algorithm，消息摘要算法）：对一段消息产生 128bit 的消息摘要，防止消息被篡改。 • SHA1（Secure Hash Algorithm， 安全散列算法）：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。
Diffie-Hellman 分组	Diffie-Hellman 算法的组信息，用于产生加密 IKE 隧道的会话密钥。
密钥生命周期	IPSec SA 的生存时间。
PFS	PFS（Perfect Forward Secrecy，完善的前向安全性）特性使得 IKE 阶段 2 协商生成一个新的密钥材料，该密钥材料与阶段 1 协商生成的密钥材料没有任何关联，这样即使 IKE1 阶段 1 的密钥被破解，阶段 2 的密钥仍然安全。 如果没有使用 PFS，阶段 2 的密钥将根据阶段 1 生成的密钥材料来产生，一旦阶段 1 的密钥被破解，用于保护通信数据的阶段 2 密钥也岌岌可危，这将严重威胁到双方的通信安全。

- **密钥协商方式—手动设置**

  密钥协商方式为“手动设置”时，如下图示：

参数说明：

参数	说明
ESP 加密算法	当隧道协议选择“ESP”时可设定 ESP 加密算法。 本路由器支持以下加密算法： • DES（Data Encryption Standard，数据加密标准）：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。 • AES（Advanced Encryption Standard，高级加密标准）：AES128/192/256 表示使用长度为 128/192/256bit 的密钥进行加密。
ESP 加密密钥	设置 ESP 加密密钥。通信双方需保持一致。
ESP/AH 认证算法	当隧道协议选择“ESP”时可设定 ESP 认证算法。当隧道协议选择“AH”时可设定 AH 认证算法。 本路由器支持以下验证算法： • NONE: ESP 认证算法为空，不需要填入认证密钥。 • MD5（Message Digest Algorithm，消息摘要算法）：对一段消息产生 128bit 的消息摘要，防止消息被篡改。 • SHA1（Secure Hash Algorithm，安全散列算法）：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。
AH 认证密钥	设定 AH 认证密钥。通信双方需保持一致。
ESP/AH 外出 SPI	可以设定 SPI 参数。SPI（Security Parameter Index）即安全参数索引。SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPSec 安全联盟，必须与通信对端的“进入 SPI”值相同。
ESP/AH 进入 SPI	可以设定 SPI 参数。SPI（Security Parameter Index）即安全参数索引。SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPSec 安全联盟，必须与通信对端的“外出 SPI”值相同。

9.4 PPTP/L2TP 配置示例

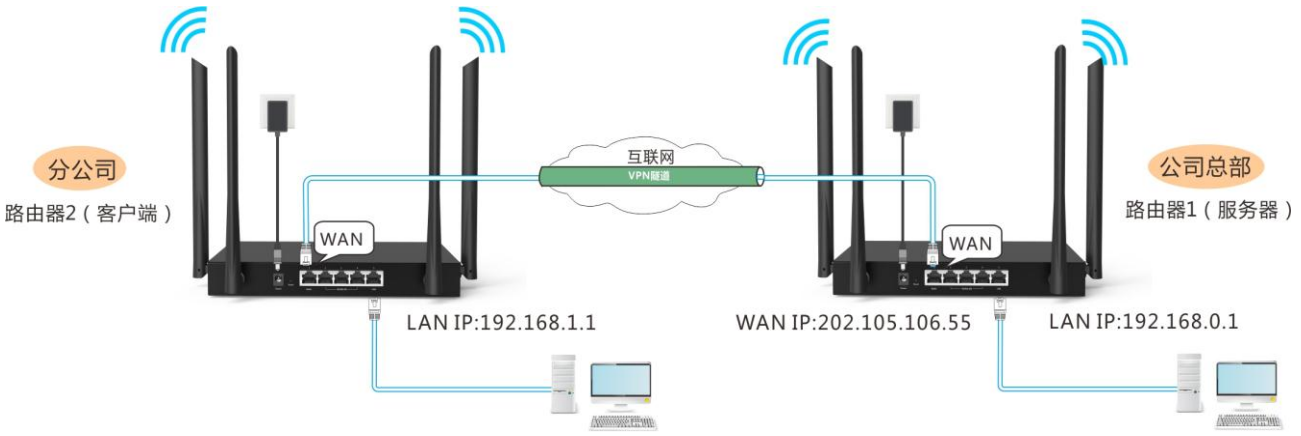
组网需求

某企业总部和分公司使用 W15E 企业级路由器进行网络搭建，并成功接入互联网。分公司员工需要随时经过互联网访问公司总部的资源，这些资源包括：公司的内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

方案设计

可以通过在路由器上设置 VPN 服务，实现远端用户访问企业服务器。本例以 PPTP 为例，L2TP 的设置方法类似。

参考拓扑图如下：



配置步骤

步骤 1 设置充当服务器的路由器 1。

1. 点击『VPN 服务』→『PPTP/L2TP 服务器』。
2. 启用“PPTP/L2TP 服务器”功能。
   (1) 服务器状态：点击“开启”。
   (2) 服务器类型：点击“PPTP”。
   (3) WAN 口：选择路由器 1“VPN 服务器”启用的 WAN 口，本例为“WAN1”。
   (4) 加密：点击“开启”，启用加密。
   (5) 点击 确定 。

3. 添加允许接入的用户名、密码。

(1) 点击 +新增 。

(2) 用户名、密码：设置 VPN 客户端连接 VPN 服务器使用的用户名、密码，如“tenda”。

(3) 是否为网段：选择 VPN 客户端类型，本例为“网络”。

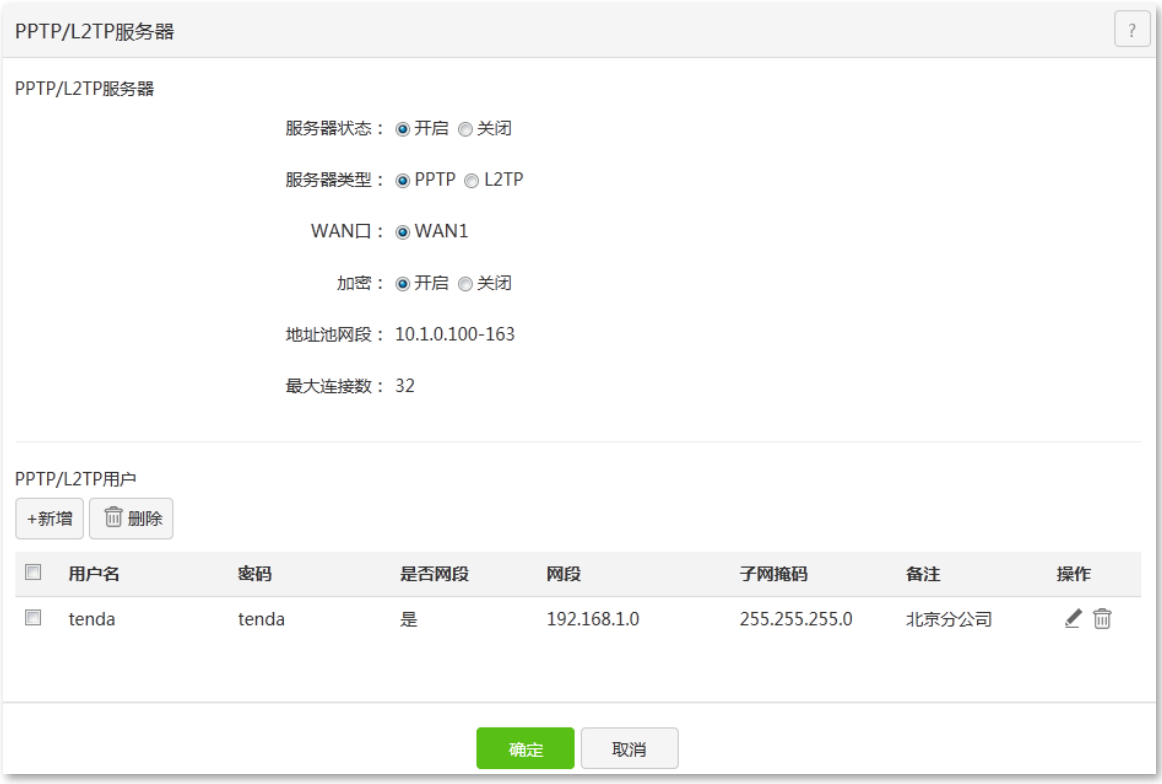
(4) 网段、子网掩码：VPN 客户端为网段时，输入客户端局域网的网段及子网掩码，本例为“192.168.1.0、255.255.255.0”。

(5) （可选）备注：输入对此用户的描述，如“北京分公司”。

(6) 点击 确定 。

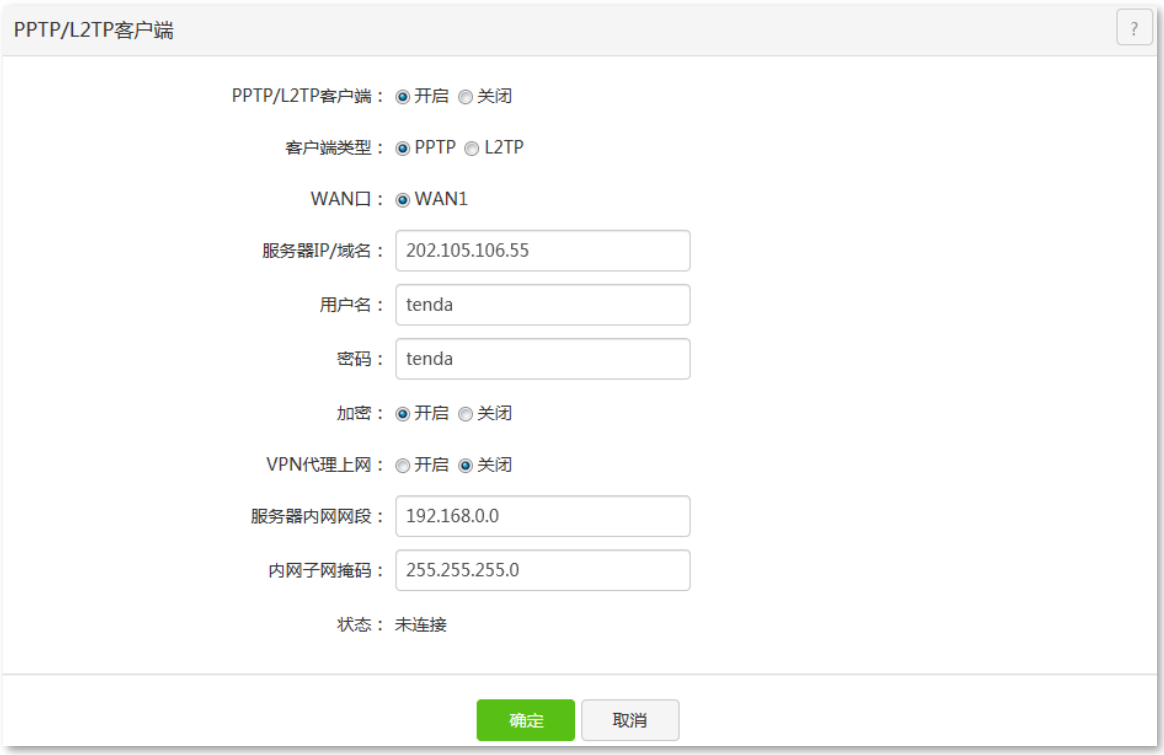
新增
用户名：
tenda
密码：
tenda
是否网段：
是
否
网段：
192.168.1.0
子网掩码：
255.255.255.0
备注：
北京分公司
确定
取消

设置成功后，如下图示。


PPTP/L2TP服务器
PPTP/L2TP服务器
服务器状态：
开启
关闭
服务器类型：
PPTP
L2TP
WAN口：
WAN1
加密：
开启
关闭
地址池网段：
10.1.0.100-163
最大连接数：
32
PPTP/L2TP用户
+新增
删除
用户名
密码
是否网段
网段
子网掩码
备注
操作
tenda
tenda
是
192.168.1.0
255.255.255.0
北京分公司
确定
取消

步骤 2 设置充当客户端的路由器 2。

1. 点击『VPN 服务』→『PPTP/L2TP 客户端』。
2. PPTP/L2TP 客户端：点击“开启”。
3. 客户端类型：点击“PPTP 客户端”。
4. WAN 口：选择路由器 2“VPN 客户端”启用的 WAN 口，本例为“WAN1”。
5. 服务器 IP/域名：输入 VPN 服务器启用的 WAN 口的 IP 地址，本例为“202.105.106.55”。
6. 用户名/密码：输入 VPN 服务器分配给 VPN 客户端的用户名和密码，本例均为“tenda”。
7. 加密：点击“开启”，启用加密。
8. 服务器内网网段：输入服务器局域网的网段，本例为“192.168.0.0”。
9. 内网子网掩码：输入服务器局域网的子网掩码，本例为“255.255.255.0”。
10. 点击 确定 。

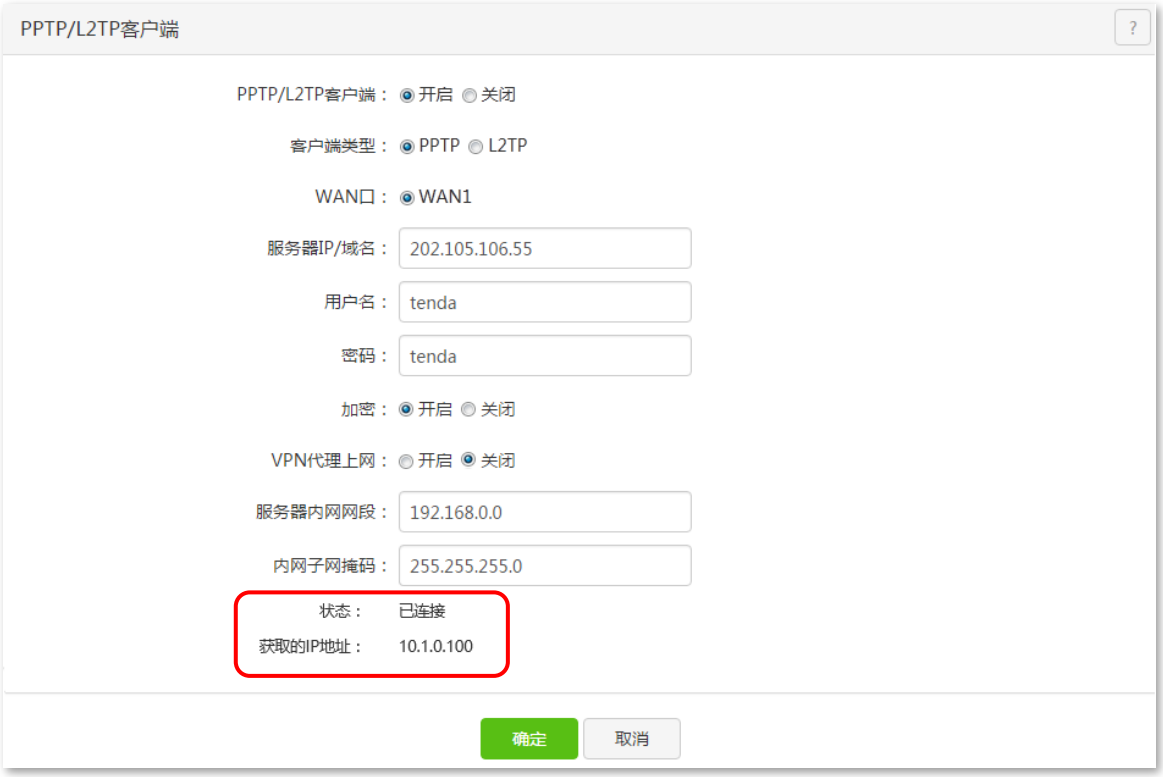


—完成

验证配置

当**路由器 2** 的『VPN 服务』→『PPTP/L2TP 客户端』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。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。

如下图示。



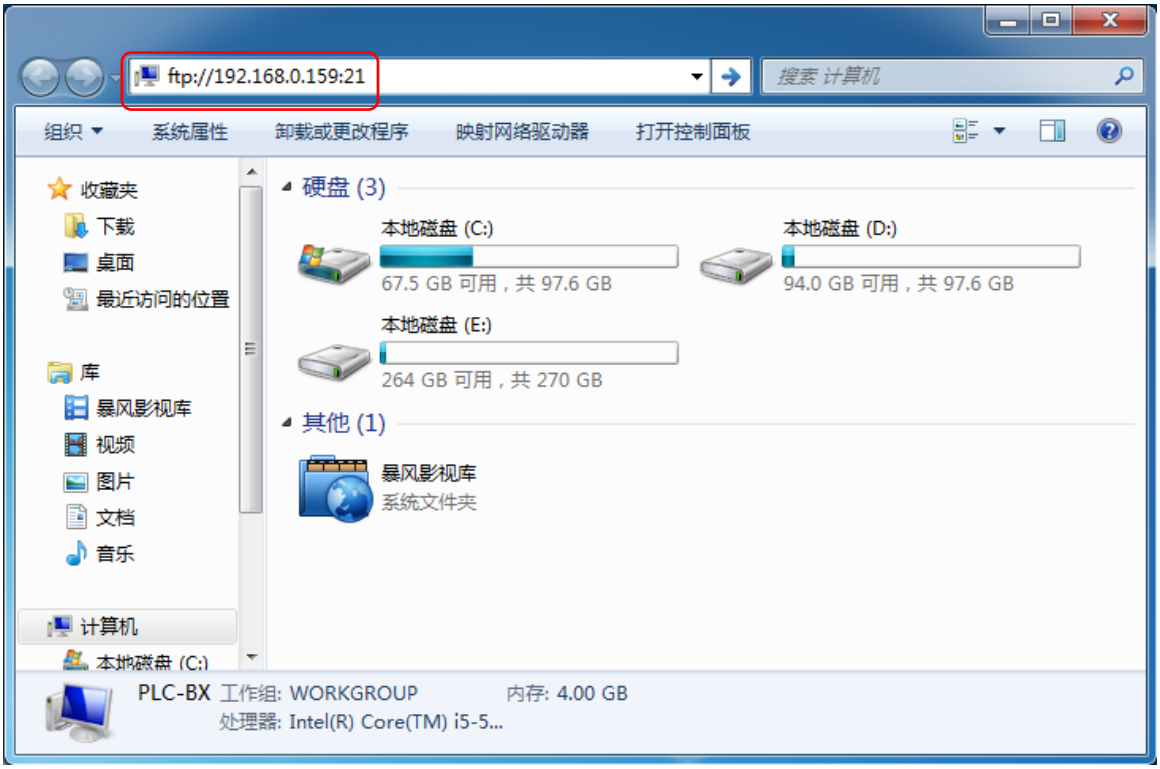
VPN 连接成功后，分公司员工可以访问总部的资源了。下文以分公司访问总部 FTP 服务器内容为例。

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：192.168.0.159
- 服务器端口：21
- 登录用户名：admin
- 登录密码：admin

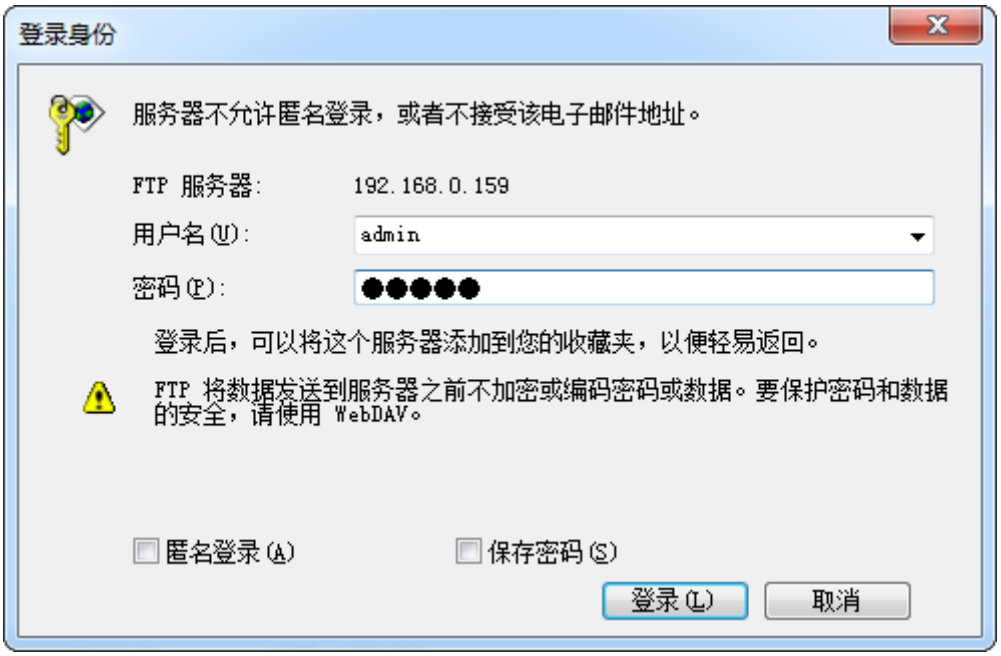
当分公司员工访问总部项目资料时，步骤如下：

1. 在电脑上访问“ftp: //服务器 IP 地址:服务端口号”，本例为“ftp: //192.168.0.159:21”。

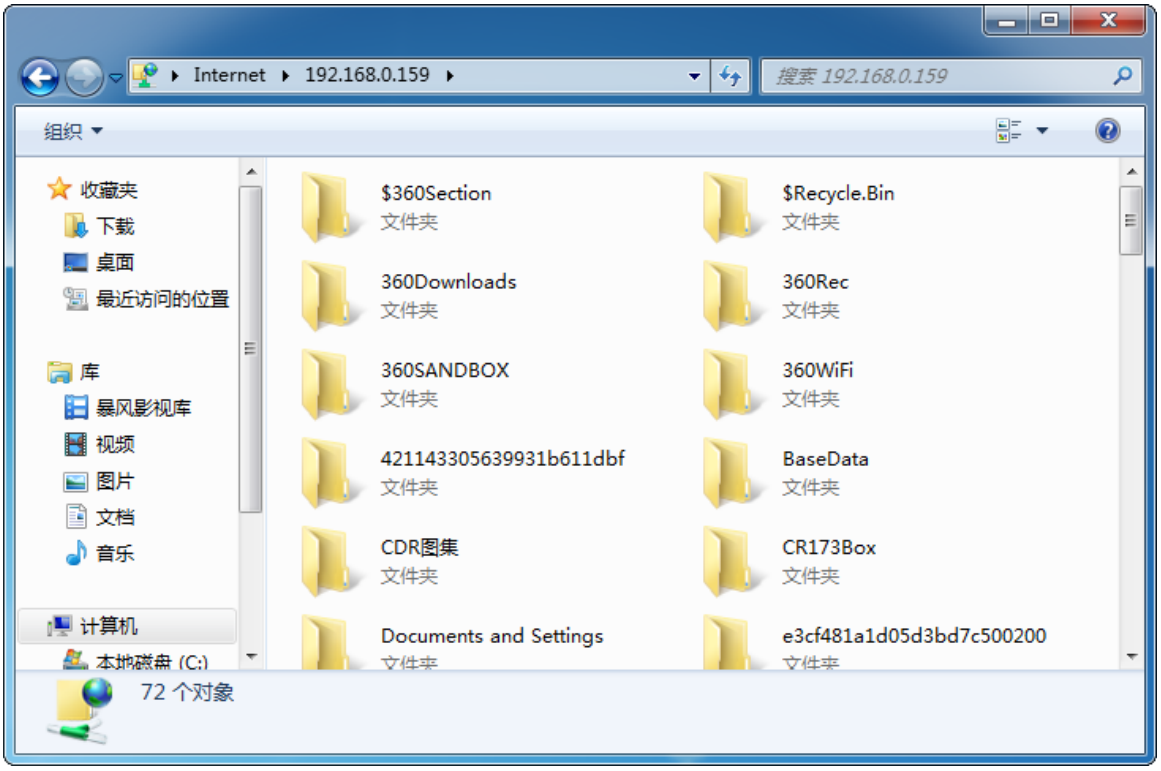


2. 在弹出的窗口输入登录用户名和密码，本例均为 admin。

3. 点击 登录 。



访问成功。



9.5 IPSec 配置示例

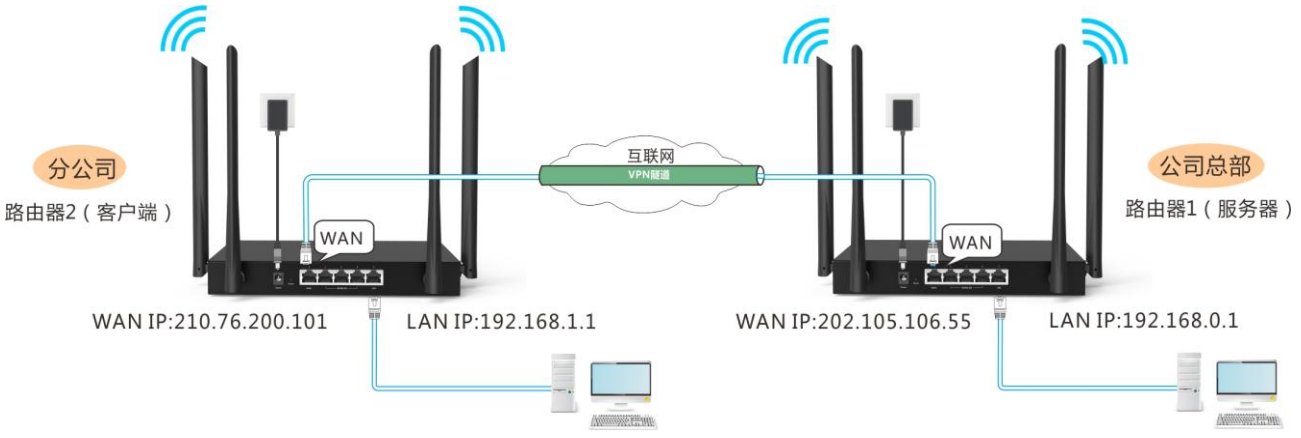
组网需求

某企业总部和分公司使用 W15E 进行网络搭建，并成功接入互联网。分公司员工需要随时经过互联网访问公司的资源，这些资源包括：公司的内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

方案设计

可以通过在路由器上设置 VPN 服务，实现远端用户访问企业服务器。本例以 IPSec 为例。

参考拓扑图如下：



配置步骤

假设两台路由器的 IPSec 隧道基本信息如下：

- 密钥协商方式：自动协商
- 预共享密钥为：12345678

> 提示
>
> - 设置过程中，如果要设置 IPSec 隧道的高级选项，请保持两台路由器的设置参数一致。
> - 密钥协商方式为“手动设置”时，IPSec 两端的加密算法、加密密钥、认证算法一致，设备 1 的外出 SPI 与设备 2 的进入 SPI 一致，设备 1 的进入 SPI 与设备 2 的外出 SPI 一致。

步骤 1 设置路由器 1。

1. 点击『VPN 服务』→『IPSec』。
2. 点击 +新增 。

3. 设置规则内容。

(1) IPSec：点击“开启”。

(2) WAN 口：选择本条隧道启用的 WAN 口，本例为“WAN1”。

(3) 连接名称：设置本条隧道名称，如“IPSec_1”。

(4) 远端网关地址：输入对端路由器 IPSec 隧道的 WAN 口的 IP 地址，本例为“210.76.200.101”。

(5) 本地内网网段/掩码：输入本地局域网的网段/子网掩码，本例为“192.168.0.0/24”。

(6) 远端内网网段/掩码：输入对端路由器局域网的网段/子网掩码，本例为“192.168.1.0/24”。

(7) 预共享密钥：输入预共享密钥，本例为“12345678”。

(8) 点击 确定 。

设置成功后，如下图示。

步骤 2 设置路由器 2。

1. 点击 +新增 。

2. 设置规则内容。

(1) IPSec：点击“开启”。

(2) WAN 口：选择本条隧道启用的 WAN 口，本例为“WAN1”。

(3) 连接名称：置本条隧道名称，如“IPSec_1”。

(4) 远端网关地址：输入对端路由器 IPSec 隧道的 WAN 口的 IP 地址，本例为“202.105.106.55”。

(5) 本地内网网段/掩码：输入本地局域网的网段/子网掩码，本例为“192.168.1.0/24”。

(6) 远端内网网段/掩码：输入对端路由器局域网的网段/子网掩码，本例为“192.168.0.0/24”。

(7) 预共享密钥：输入预共享密钥，本例为“12345678”。

(8) 点击 确定 。

—完成

设置成功后，如下图示。

配置验证

进路由器的管理页面。点击『系统状态』→『用户列表』，进入页面。当“IPSec 安全联盟”显示连接数量时，设置成功。

10 安全设置

安全设置章节包括：

IP-MAC 访问控制、攻击防御。

10.1 IP-MAC 访问控制

10.1.1 概述

在“IP-MAC 访问控制”页面，您可以添加 IP-MAC 访问控制规则，添加成功后，仅允许与“已添加列表”中的 IP 地址和 MAC 地址匹配的用户访问互联网，其他用户禁止访问互联网。

点击『安全设置』，进入设置页面。

启用“IP-MAC 访问控制”，如下图示。

参数说明：

参数		说明
IP-MAC 访问控制		开启/关闭 IP-MAC 访问控制功能。默认关闭。
已添加列表	+新增	点击此按钮可手动添加相应 IP 地址和其对应的 MAC 地址。
	删除	点击此按钮可删除选中的已添加的规则。
	IP 地址	显示已添加的 IP 地址。
	MAC 地址	显示 IP 地址对应的 MAC 地址。
	备注	显示对应规则描述。若动态添加或手动添加时未设置备注信息，将不显示。
	操作	可对已添加的规则进行编辑或删除操作。
动态添加	添加	连接到路由器的客户端信息将会显示在动态列表中。点击此按钮可将已选中的规则添加到“已添加列表”。
	全部添加	点击此按钮可将动态列表中的所有规则添加到“已添加列表”。
	IP 地址	显示连接到路由器的客户端的 IP 地址。
	MAC 地址	显示连接到路由器的客户端的 IP 地址对应的 MAC 地址。
	操作	点击对应规则后的添加，即可将该规则快速添加到“已添加列表”。

10.1.2 添加 IP-MAC 绑定规则

1. 点击『安全设置』→『IP-MAC 访问控制』。
2. 在 IP-MAC 访问控制选项点击“开启”，点击页面底端的 确定 ，启用功能。

3. 点击 +新增 ，设置 IP-MAC 访问控制规则；或在“动态添加”模块添加。

—完成

10.1.3 IP-MAC 绑定示例

组网需求

某企业使用 W15E 进行网络搭建。公司禁止员工访问互联网，只允许招聘组的员工使用固定的电脑和 IP 地址访问互联网。

方案设计

可以通过 IP-MAC 访问控制功能实现。首先需要知道允许上网的招聘人员使用的电脑的 IP 地址和 MAC 地址，假设它们分别为：192.168.0.11、C8:3A:35:13:05:18；192.168.0.12、C8:3A:35:D5:75:A6。

配置步骤

1. 点击『安全设置』→『IP-MAC 访问控制』。
2. 在 IP-MAC 访问控制选项点击“开启”，点击页面底端的 确定 ，启用功能。

3. 添加 IP-MAC 访问控制规则。

- 如果用户没有连接到路由器，请参考如下操作：

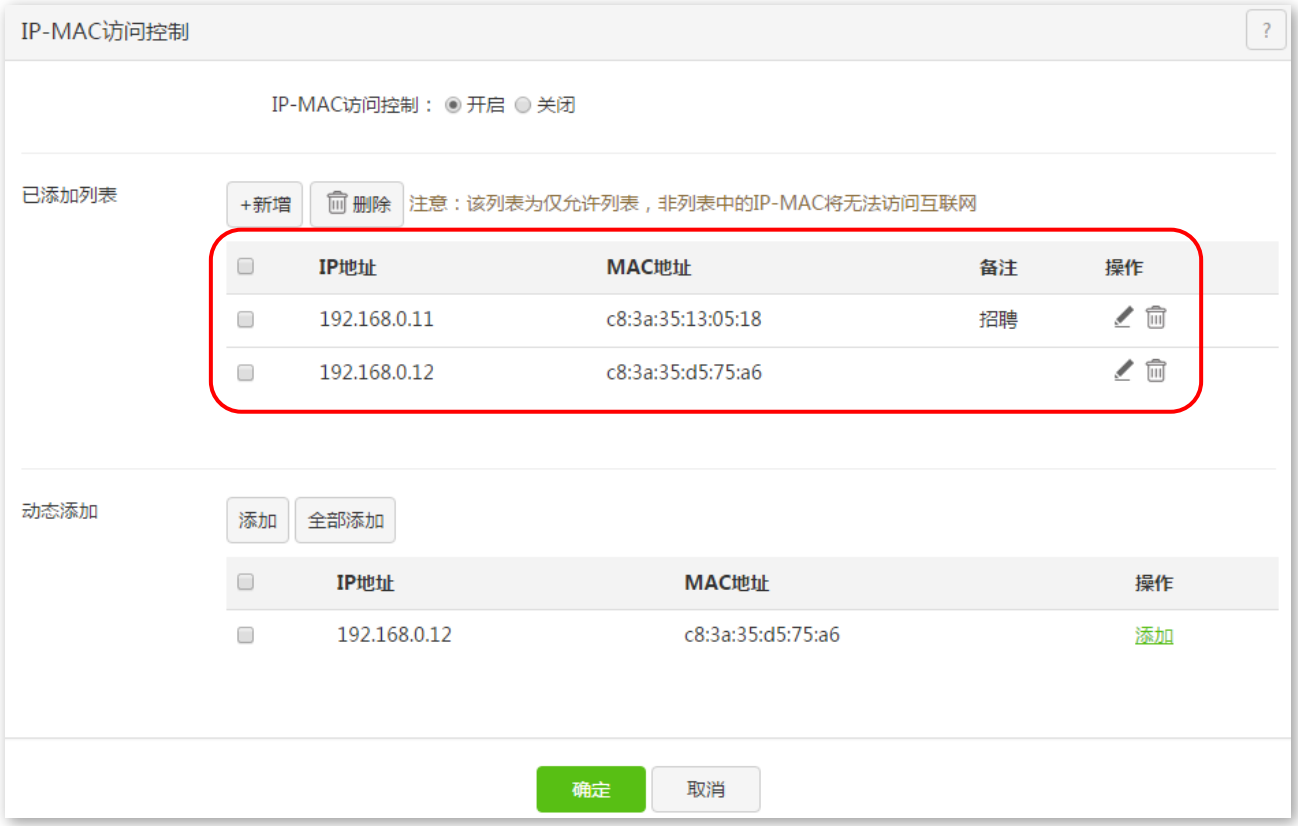
(1) 点击 +新增 。

(2) 在弹出的对话框输入要添加的 IP 地址和 MAC 地址信息，点击 确定 。

- 如果要设置的客户端已经连接路由器，可在“动态添加”列表中找到对应设备并点击添加。

—完成

添加成功后，如下图示。



配置验证

局域网中 MAC 地址为 C8:3A:35:13:05:18 的客户端需要配置 192.168.0.11 的 IP 地址才能访问互联网，MAC 地址为 C8:3A:35:D5:75:A6 的客户端需要配置 192.168.0.12 的 IP 地址才能访问互联网。

10.2 攻击防御

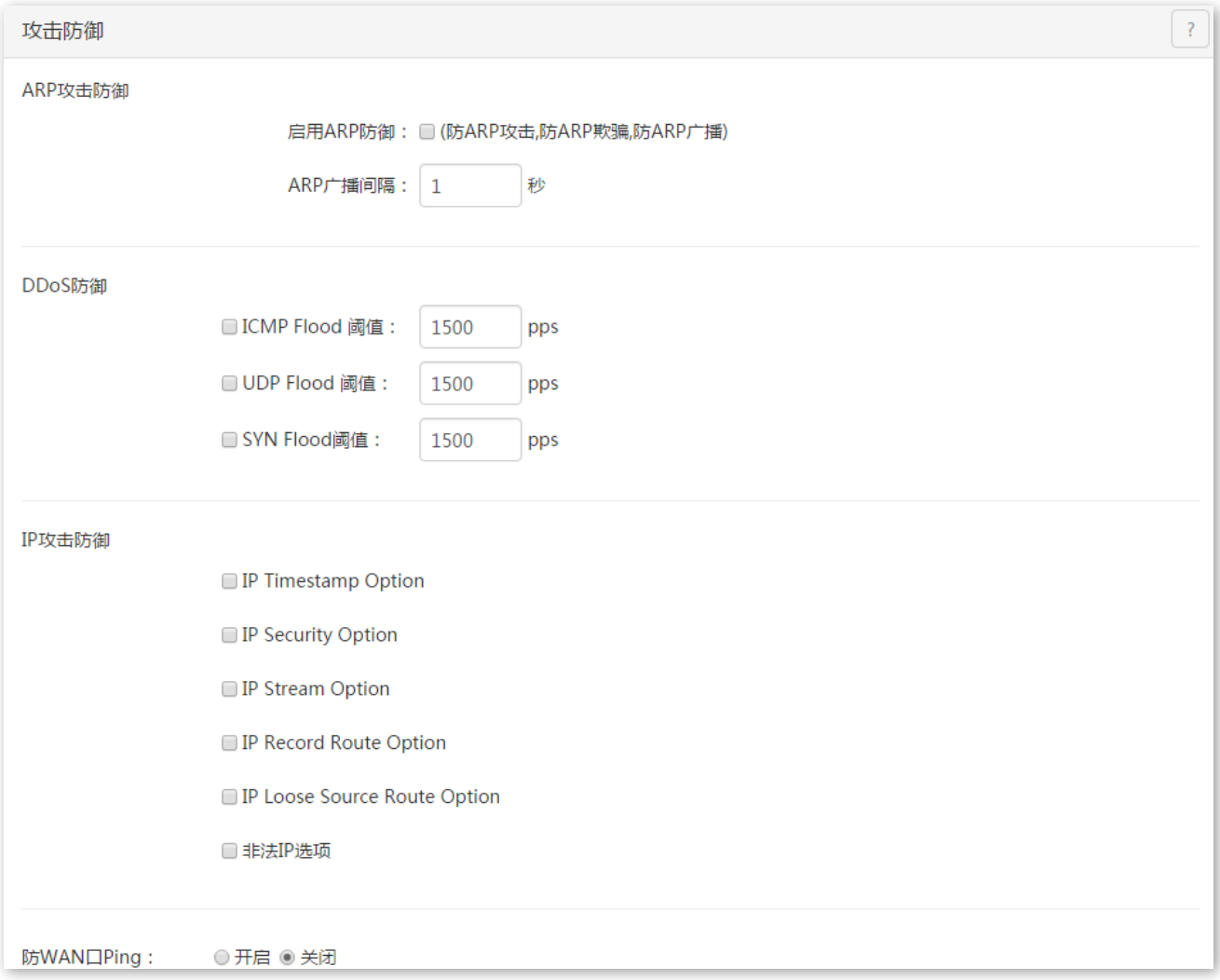
在“攻击防御”页面，您可以设置路由器攻击防御功能。

本路由器支持的攻击防御类型有：ARP 攻击防御、DDOoS 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。本路由器可以防止的 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一些特殊 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。

启用对应的攻击防御后，如果发生攻击，路由器可以将攻击信息如攻击时间、类型、次数，攻击者 IP、MAC 等记录在『系统状态』→『防攻击日志』页面的防攻击日志中。

点击『安全设置』→『攻击防御』，进入设置页面。



参数说明：

参数		说明
ARP 攻击防御	启用 ARP 防御	启用/禁用 ARP 防御功能。
	ARP 广播间隔	路由器发送 ARP 广播的时间间隔。
DDoS 防御	ICMP Flood 阈值	一秒钟内，如果一个目 IP 收到超过规定数量的 ICMP 请求包，则认为此目的 IP 正受到 ICMP Flood 攻击。
	UDP Flood 阈值	一秒钟内，如果一个目 IP 的某一端口收到超过规定数量的 UDP 包，则认为此目的 IP 的此端口正受到 UDP Floo 攻击。
	SYN Flood 阈值	一秒钟内，如果一个目 IP 的某一端口收到超过规定数量的 TCP SYN 包，则认为此目的 IP 的此端口正受到 SYN Flood 攻击。
IP 攻击防御	IP Timestamp Option	是否检查来自指定区域的 IP 包含有 Internet Timestamp 项。
	IP Security Option	是否检查来自指定区域的 IP 包含有 Security 项。
	IP Stream Option	是否检查来自指定区域的 IP 包含有 Stream ID 项。
	IP Record Route Option	是否检查来自指定区域的 IP 包含有 Record Route 项。
	IP Loose Source Route Option	是否检查来自指定区域的 IP 包含有 Loose Source 项。
	非法 IP 选项	是否检查来自指定区域的 IP 包的完整性或正确性。
防 WAN 口 Ping		启用后，互联网中的设备将不能 ping 通路由器 WAN 口。

11 WEB 认证

WEB 认证章节包括：

基本设置、用户管理。

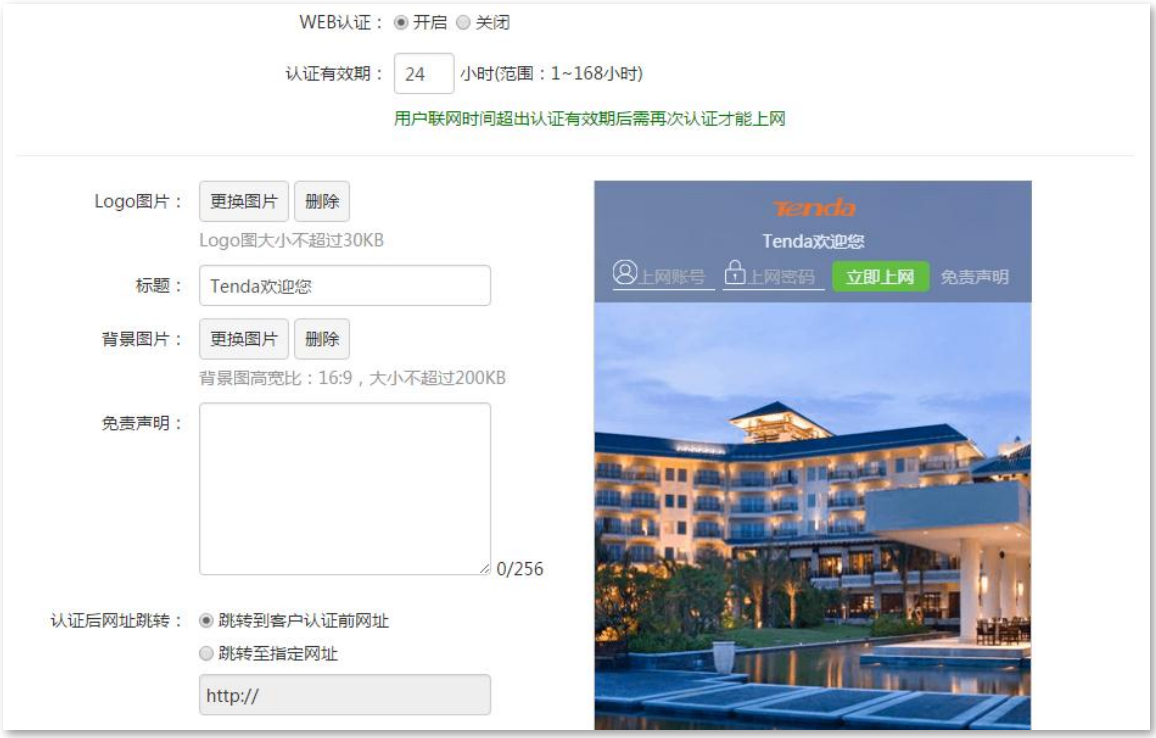
11.1 基本设置

11.1.1 概述

在“基本设置”页面，您可以设置客户端进行 WEB 认证上网时，接受的网页推送信息。

默认情况下，路由器接入互联网后，连接到路由器的客户端即可访问互联网。启用 WEB 认证功能后，路由器下的客户端需要认证后才能访问互联网。点击『WEB 认证』，进入基本设置页面。

启用 WEB 认证，页面如下：



参数说明：

参数	说明
Logo 图片	修改 WEB 推送页面的 Logo 图片。
标题	修改 WEB 推送页面的标题信息，默认为“Tenda 欢迎您”。
背景图片	修改 WEB 推送页面的背景图片。
更换图片	点击可更换推送页面的背景图片。
删除	删除已上传的图片。
免责申明	设置 WEB 推送页面的免责申明信息。
认证后网址跳转	客户端接收 WEB 认证推送完成后，跳转的网址： • 跳转到客户认证前网址：WEB 认证完成后，客户端跳转到认证前访问的网址。如客户端访问百度时，跳转到 WEB 认证页面，认证成功后就会跳转到百度页面。 • 跳转至指定网址：WEB 认证完成后，客户端跳转到此处设置的网址。

11.1.2 启用 WEB 认证

1. 进入『WEB 认证』→『基本设置』页面。
2. 在“WEB 认证”选项选择“开启”。
3. 根据页面提示，设置认证有效期、推送信息。
4. 点击 确定 。

—完成

11.2 用户管理

11.2.1 概述

在“用户管理”页面，您可以添加客户端进行 WEB 认证时，需要输入的用户名和密码，以及不需要进行 WEB 认证的客户端。每个账号（用户名和密码）只能被一个用户使用。

点击『WEB 认证』→『用户管理』，进入设置页面。

参数说明：

参数		说明
+新增		点击此按钮可以增加不需要 WEB 认证的主机或添加 WEB 认证账号。
删除		点击此按钮可以删除已选中的规则。
导出数据		点击此按钮可以导出后缀为 cfg 的 WEB 用户的配置文件。建议添加账号后，导出该数据，WEB 用户数据丢失时，您可以直接将其导入进行数据恢复，而不用重新添加。
浏览..		点击可以载入之前导出的 WEB 用户数据。
导入数据		将已选中的 WEB 用户数据导入路由器中。
不需要认证的主机	主机类型	不需要进行 WEB 认证的主机类型，包括 IP 地址和 MAC 地址。
	主机地址	不需要进行 WEB 认证的主机信息，包括 IP 地址信息和 MAC 地址信息。
	备注	不需要进行 WEB 认证的主机描述，设置时不填则不显示。
	状态	不需要进行 WEB 认证的主机规则的状态，包括已启用和未启用。
	操作	可对规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改主机类型、主机地址、备注。 • 点击可以删除规则。

参数		说明
用户管理	用户名	客户端进行 WEB 认证时需要输入的用户名。
	密码	客户端进行 WEB 认证时需要输入的密码。
	备注	显示对应账号的描述，设置时不填则不显示。
	状态	用户账号的状态，包括已启用和未启用。
	操作	可对 WEB 认证账号进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改用户名、密码、备注、禁用/启用该账号。 • 点击可以删除规则。

11.2.2 添加不需要 WEB 认证的客户端

1. 点击『WEB 认证』→『用户管理』。
2. 在“不需要认证的主机”模块点击 +新增 。

3. 在弹出的窗口设置主机类型、主机地址等参数。
4. 点击 确定 。

—完成

11.2.3 添加 WEB 认证账号

1. 点击『WEB 认证』→『用户管理』。
2. 在“用户管理”模块点击 +新增 。

3. 在弹出的窗口设置用户名、密码等参数。
4. 点击 确定 。

—完成

11.3 WEB 认证示例

组网需求

某企业使用 W15E 进行网络搭建。公司规定员工上班访问互联网或内网时需要认证，认证成功后，跳转到百度。但是允许网络管理人员不需要认证。

方案设计

可以通过 WEB 认证功能实现。假设网络管理人员的电脑 MAC 地址为 CC:3A:61:71:1B:6E。

配置步骤

步骤 1 进行 WEB 认证基本设置。

1. 点击『WEB 认证』→『基本设置』。
2. WEB 认证：选择“开启”。
3. 认证有效期：设置客户端 WEB 认证有效期，如“24 小时”。
4. Logo 图片：点击 更换图片 ，上传企业 Logo 图片。
5. 标题：设置 WEB 推送页面标题，如“XX 企业欢迎您”。
6. 背景图片：点击 更换图片 ，上传 WEB 推送页面的背景图片，如“企业宣传照片”。
7. 免责申明：设置企业的免责申明信息。
8. 认证后网址跳转：选择“跳转到指定网址”，然后输入客户端接收完 WEB 推送页面信息后，跳转到的网址，本例为“www.baidu.com”。
9. 点击 确定 。

步骤 2 添加 WEB 认证账号。

1. 点击『WEB 认证』→『用户管理』。
2. 在“用户管理”模块点击 +新增 。

3. 用户名：设置 WEB 认证的用户名，如“zhangsan”。
4. 密码：设置 WEB 认证的密码，如“zhangsan”。
5. （可选）备注：输入该用户的描述。
6. 点击 确定 。

步骤 3 添加不需要 WEB 认证的客户端。

1. 点击『WEB 认证』→『用户管理』。
2. 在“不需要认证的主机”模块点击 +新增 。

3. 主机类型：选择不需要 WEB 认证的客户端类型，本例为“MAC 地址”。
4. 主机地址：输入该客户端的 MAC 地址信息，本例为“CC:3A:61:71:1B:6E”。
5. （可选）备注：输入该客户端的备注，本例为“管理员”。

6. 点击 确定 。

—完成

验证配置

局域网客户端访问互联网或内网时，将会弹出 WEB 认证页面。此时输入已添加的 WEB 认证用户名和密码，点击**立即上网**，即可上网。

PC 客户端认证页面如下：

移动客户端认证页面如下：

12 PPPoE 认证

PPPoE 认证章节包括：

基本设置、账号管理。

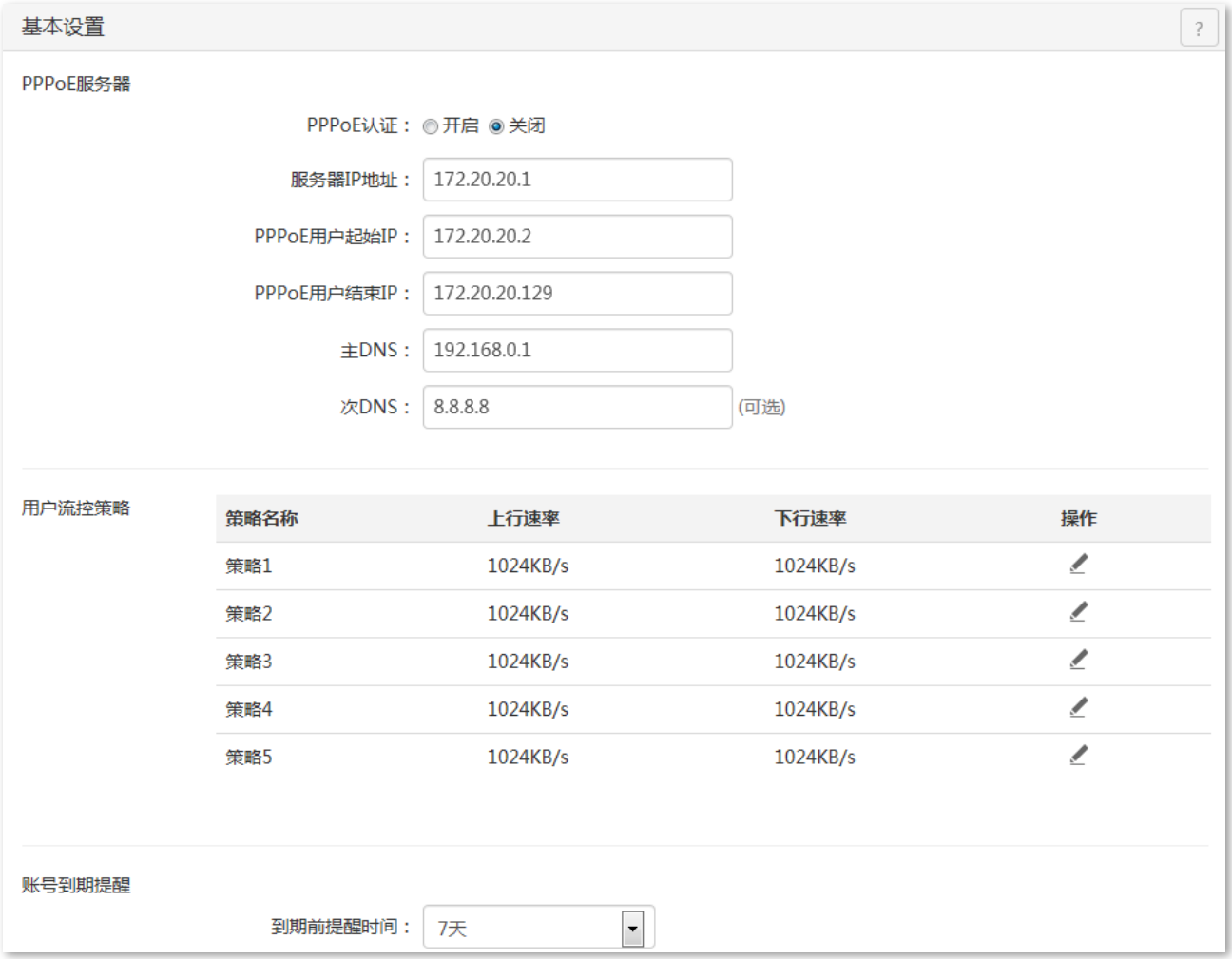
12.1 基本设置

12.1.1 概述

在“基本设置”页面，您可以设置 PPPoE 认证功能。

默认情况下，路由器接入互联网后，连接到路由器的客户端即可访问互联网。启用 PPPoE 认证功能后，路由器下的客户端需要拨号认证后才能访问互联网，且此时 WEB 认证和微信连 WiFi 功能将被禁用。

点击『PPPoE 认证』，进入基本设置页面。



参数说明：

参数		说明
PPPoE 服务器	PPPoE 认证	开启/关闭 PPPoE 认证功能。
	服务器 IP 地址	PPPoE 服务器的 IP 地址。
	PPPoE 用户起始/结束 IP	客户端进行 PPPoE 认证成功后，PPPoE 服务器分配给客户端的 IP 地址范围。
	主/次 DNS 服务器	客户端进行 PPPoE 认证成功后，PPPoE 服务器分配给客户端的主/次 DNS 服务器地址。
用户流控策略	策略名称	流控策略名称，不可修改。启用 PPPoE 认证功能后，路由器原“网速控制”功能将由 PPPoE“用户流控策略”代替。
	上行/下行速率	对应策略的上行/下行速率，这些策略将会关联到 PPPoE 的账号，使用流控策略关联的账号认证上网用户的最大上行/下行速率为此速率。
	操作	点击可修改上行/下行速率，默认为 1024KB/s。 1Mbps=128KB/s=1024kb/s，1B=8b
账号到期提醒	到期前提醒时间	设置账号到期前提醒的时间，默认为账号到期前 7 天提醒。
	账号到期前提醒页面	设置账号到期前提醒的页面信息。 点击 配置页面 可配置提醒页面信息，点击预览页面可查看完成的效果。
	账号已到期提醒页面	设置账号已到期提醒的页面信息。 点击 配置页面 可配置提醒页面信息，点击预览页面可查看完成的效果。
不需要认证主机	+新增	点击此按钮可增加无需认证即可上网的客户端。
	删除	点击此按钮可以删除已选中的不需要认证主机。
	MAC 地址	显示不需要认证上网的客户端的 MAC 地址。
	备注	显示不需要认证上网的客户端的描述，设置时不填则不显示。
	操作	可对不需要认证主机规则进行如下操作： • 点击可以编辑规则信息，包括修改 MAC 地址、备注。 • 点击可以删除规则。

12.1.2 启用 PPPoE 认证

1. 点击『PPPoE 认证』→『基本设置』。
2. PPPoE 认证：选择“开启”。
3. 根据页面提示，设置流控策略、账号到期提醒信息以及不需要认证的客户端。
4. 点击页面底端的 确定 。

—完成

12.2 账号管理

12.2.1 概述

在“账号管理”页面，您可以添加客户端进行 PPPoE 拨号认证时，需要输入的用户名和密码。每个账号（用户名和密码）只能被一个用户使用。

点击『PPPoE 认证』→『账号管理』，进入设置页面。

参数说明：

参数	说明
+新增	点击此按钮可以增加 PPPoE 认证账号。
删除	点击此按钮可以删除已选中的 PPPoE 认证账号。
用户名/密码	客户端进行 PPPoE 认证时需要输入的用户名/密码。
流控策略	该账号对应的流控策略。
备注	显示对应账号的描述，设置时不填则不显示。
到期时间	账号到期时间。
状态	用户当前的状态，包括已启用和未启用。
操作	可对 PPPoE 认证账号进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改用户名、密码、备注、流控策略、到期时间、禁用/启用该账号。 • 点击可以删除规则。
导出数据	点击此按钮可以导出后缀为 cfg 的 PPPoE 用户的配置文件。建议添加账号后，导出该数据，确保当 PPPoE 用户数据丢失时，有数据导入，不用重新添加。
浏览..	点击可载入之前导出的 PPPoE 用户数据。
导入数据	将之前导出的 PPPoE 用户数据导入路由器中。

12.2.2 添加 PPPoE 账号

1. 点击『PPPoE 认证』→『账号管理』。
2. 点击 +新增 。

3. 在弹出的窗口设置用户名、密码等参数。
4. 点击 确定 。

—完成

12.3 PPPoE 认证示例

组网需求

某小区使用 W15E 进行网络搭建，并成功访问互联网。小区管理员不允许租客自己办网络，管理员想给每位租客分配上网账号和密码，且自己不用输入账号和密码，自动获取 IP 地址即可上网。租客网络到期时，需要网页提醒。

方案设计

小区管理员可通过路由器的 PPPoE 认证功能，启用 PPPoE 服务器，并添加账号和密码（分配给租客），然后将自己的电脑设置为“不需要认证的主机”。

配置步骤

步骤 1 设置 PPPoE 认证。

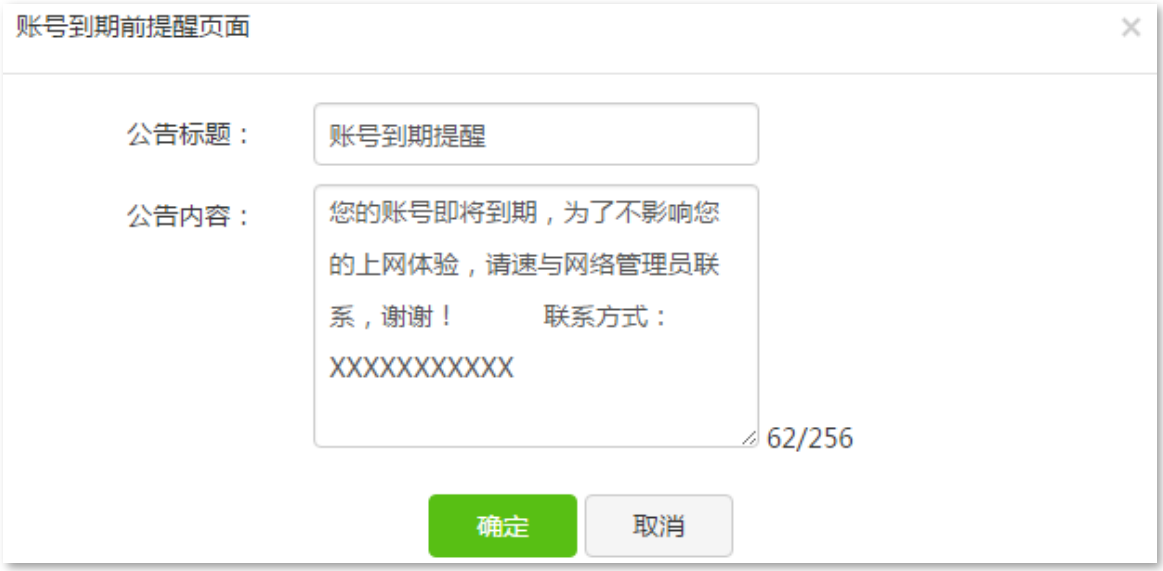
1. 进入『PPPoE 认证』→『基本设置』页面。
2. 在“PPPoE 认证”选项选择“开启”，点击页面底端的 确定 ，启用该功能。

3. 设置客户端将会接收到的账号到期提醒信息。

(1) 点击 配置页面 。

(2) 在弹出的窗口设置页面提醒内容。

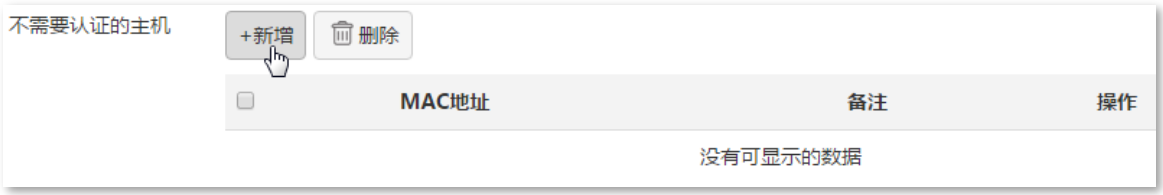
- 公告标题：修改账号到期提醒页面的标题内容。
- 公告内容：修改账号到期提醒页面的公告内容。
- 点击 确定 。



设置完成后，返回基本设置页面，点击预览页面，即可查阅设置效果。

4. 添加不需要认证的主机。本例为“小区管理人员的电脑”，假设其 MAC 地址为 CC:3A:61:71:1B:6E。

(1) 点击 +新增 。



(2) MAC 地址：输入不用 PPPoE 认证就能上网的客户端 MAC 地址。

(3) （可选）备注：输入该客户端的备注，本例为“管理员”。

(4) 点击 确定 。

步骤 2 添加 PPPoE 认证账号。

1. 点击『PPPoE 认证』→『账号管理』。
2. 点击 +新增 。

3. 用户名：设置 PPPoE 认证的用户名，如“zhangsan”。
4. 密码：设置 PPPoE 认证的密码，如“zhangsan”。
5. （可选）备注：设置该账号的描述。
6. 流控策略：选择该账号的流控策略，如“策略 1”。
7. 到期时间：设置该账号的到期时间，如“2017 年 6 月 30 日”。
8. 点击 确定 。

—完成

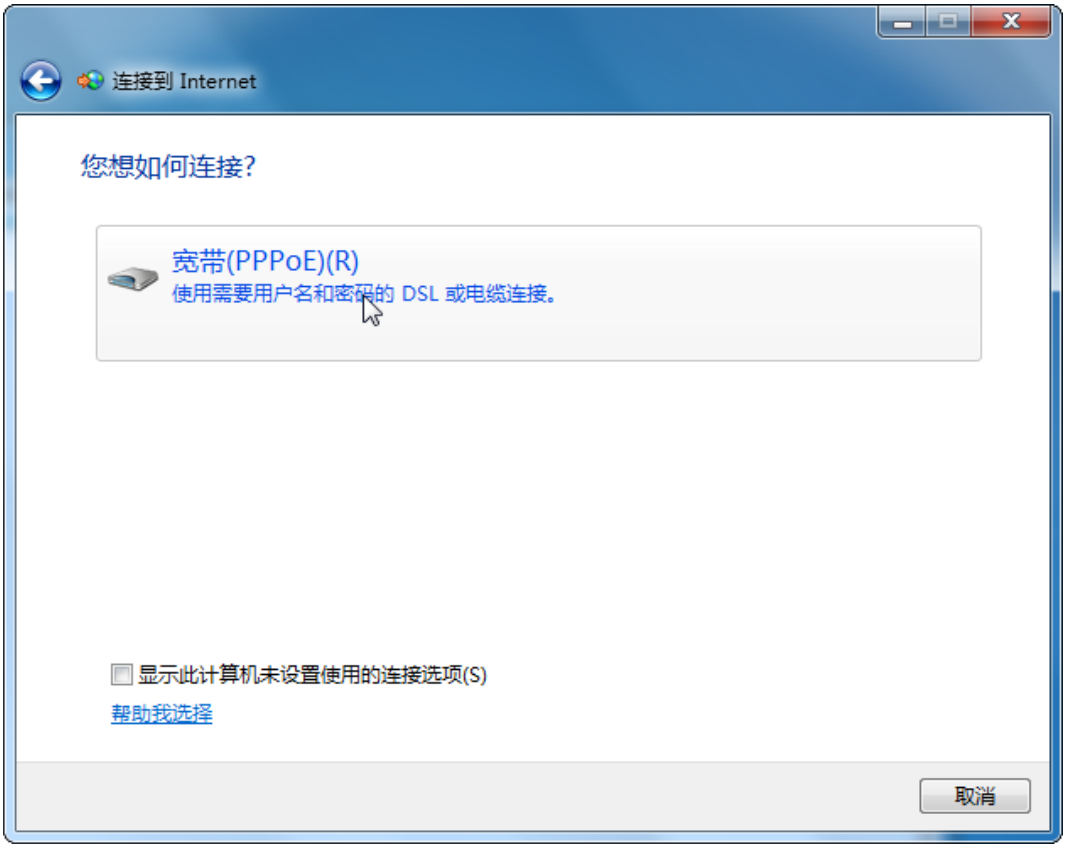
配置验证

客户端拨号上网（以 Windows 7 为例）。

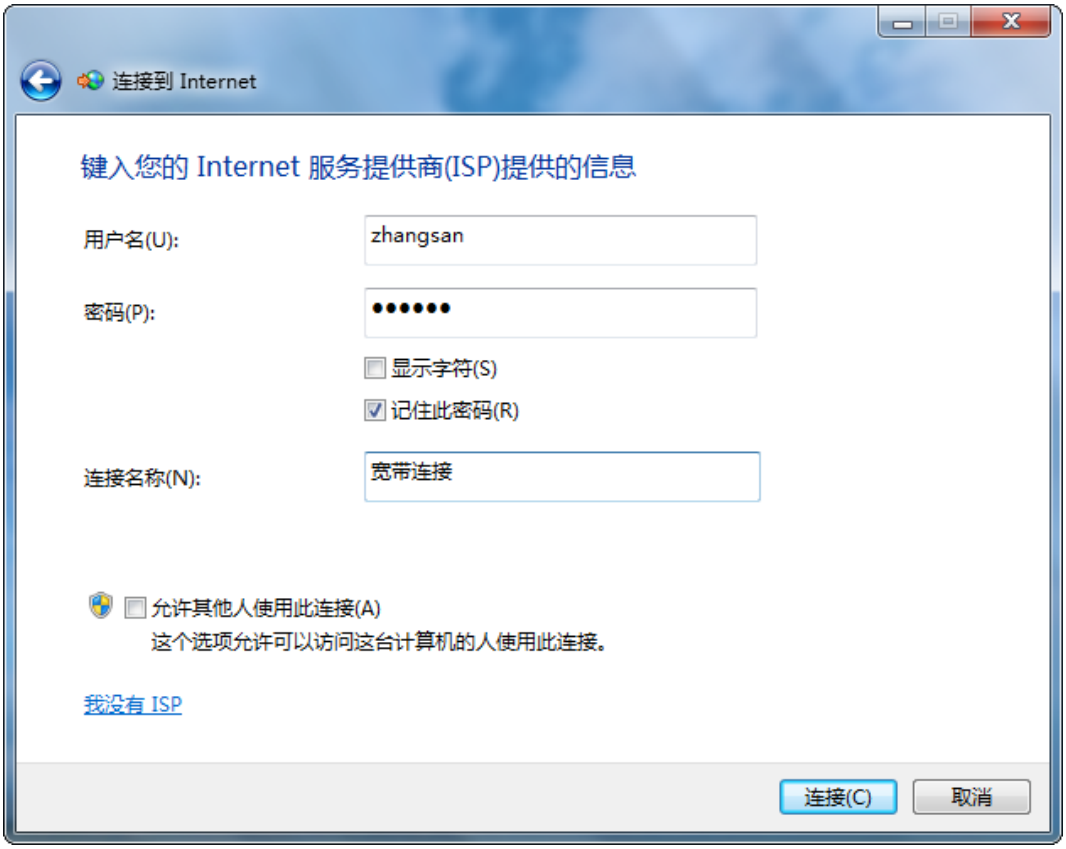
1. 点击桌面左下角的开始图标 。
2. 点击“控制面板”→“网络和 Internet”→“网络和共享中心”→“设置新的连接或网络”。

3. 选中“连接到 Internet”后，点击“下一步”；

4. 点击“宽带（PPPoE）（R）”；



5. 填写 PPPoE 认证用户名和密码，本例均为“zhangsan”，勾选“记住此密码（R）”，点击“连接”。



稍等片刻，拨号成功，可以正常上网。后续如果想进入宽带连接界面，开机后，找到并点击右下角的网络图标，然后点击宽带连接，即可正常上网。

13 微信连 WiFi

13.1 微信连 WiFi

13.1.1 概述

在“微信连 WiFi”页面，您可以设置微信连 WiFi 功能。

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。开启微信连 WiFi 功能后，客户端需要通过微信认证后才能访问互联网，此时需要认证上网的客户端有以下几种情况：

- 连接路由器 2.4G、5G 的主网络无线信号的客户端。
- 有线连接 5 接口（LAN5）的客户端。
- 连接 5 接口（LAN5）下 AP 无线信号的客户端。

点击『微信连 WiFi』，进入设置页面，启用微信连 WiFi，如下图示。

微信公众平台参数设置

使用微信连 WiFi 功能时，需要输入微信公众平台上的相关信息（包括 SSID、shopId、appId、secretKey）。如果没有注册微信公众号，或者该微信公众没有启用微信连 Wi-Fi 功能，请点击路由器管理页面的微信连 WiFi 使用说明链接，参考该帮助文档进行设置。

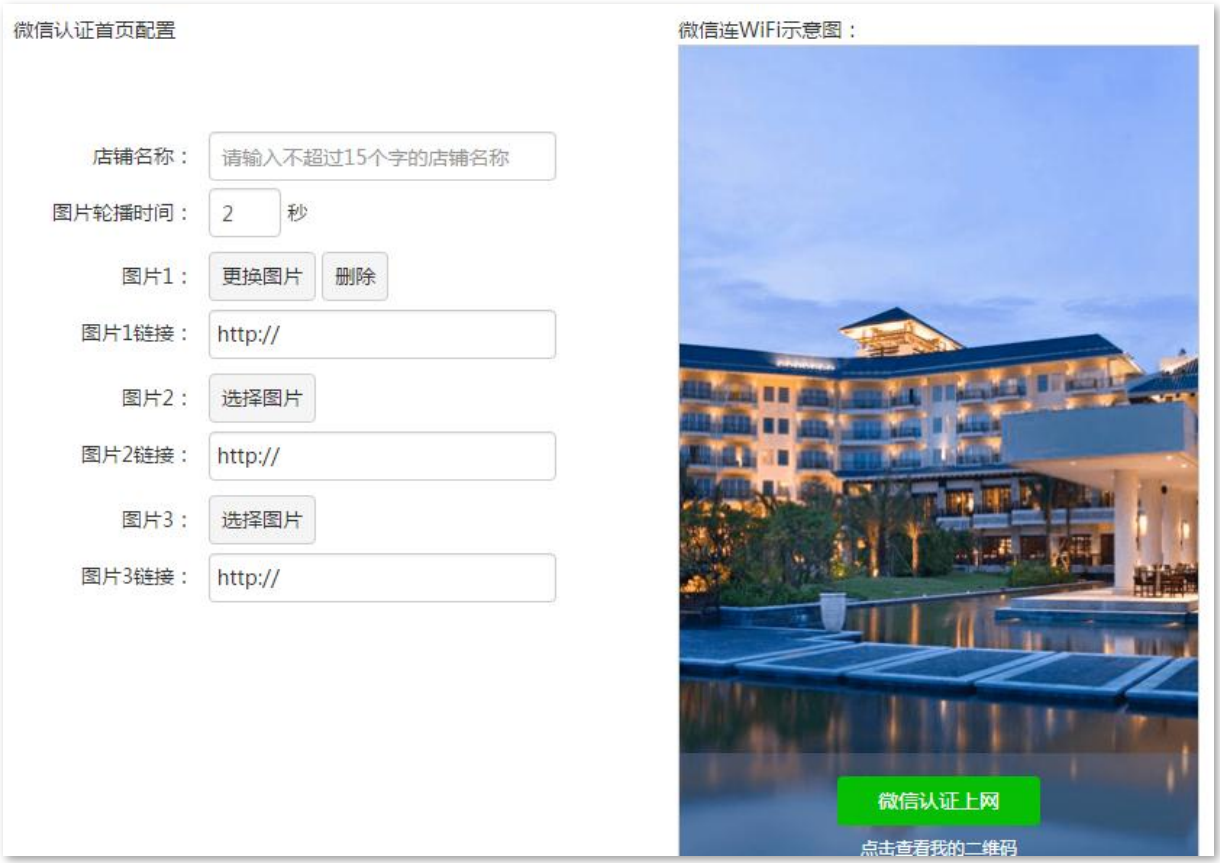
点击『微信连 WiFi』，进入“微信公众平台参数设置”模块页面。

参数说明：

参数	说明
SSID	路由器启用“微信连 WiFi 认证”的无线信号名称，需与微信公众平台中的 SSID 一致。
ShopID	微信公众平台门店的 ID，需登录微信公众平台查看。
AppID	公众号 ID，是微信公众账号身份的唯一标识，需登录微信公众平台查看。
SecretKey	微信公众号支付请求中用于加密的密钥，可验证商户唯一身份，需登录微信公众平台查看。

微信认证首页配置

在“微信认证首页配置”模块，您可以设置客户端进行微信认证时接收的推送页面信息。



参数说明：

参数	说明
店铺名称	设置店铺名称，如“XX 餐厅”。
图片轮播时间	设置图片切换间隔。
图片 1/2/3	进行微信推送的图片，最多支持添加 3 张图片。
图片 1/2/3 链接	图片链接到的网址，可以是 IP 地址或域名，如“www.baidu.com”。
更换图片	更换图片。
删除	删除已上传的图片。
选择图片	上传微信推送图片。

不需要认证的主机

在“不需要认证的主机”模块，您可以添加不需要进行微信认证上网的客户端。

参数说明：

参数	说明
+新增	点击此按钮可以添加不需要进行微信认证上网的客户端。
删除	点击此按钮可以删除已选中的规则。
主机类型	不需要进行微信认证上网的客户端类型，包括 IP 地址和 MAC 地址。
主机地址	不需要进行微信认证上网的客户端信息，包括 IP 地址和 MAC 地址具体信息。
备注	不需要进行微信认证上网的客户端描述，设置时不填则不显示。
状态	规则的状态，包括已启用和未启用。
操作	可对规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改主机类型、主机地址、备注。 • 点击可以删除规则。

13.1.2 启用微信认证

1. 点击『微信连 WiFi』。
2. 微信连 WiFi：选择“开启”。
3. 在“微信公众平台参数设置”模块，输入微信公众平台上的“SSID”、“ShopID”、“AppID”、“SecretKey”参数。
4. 在“微信认证首页配置”模块，设置微信认证的推送页面信息。
5. 在“不需要认证的主机”模块，添加不需要微信认证的客户端信息。
6. 点击 确定 。

—完成

13.2 微信认证示例

组网需求

餐厅使用 W15E 进行网络搭建，要求客人在餐厅连接 WiFi 上网时，需要通过微信认证上网，并且在认证页面可以看到餐厅的宣传推广信息。

方案设计

可以通过微信连 WiFi 功能实现。

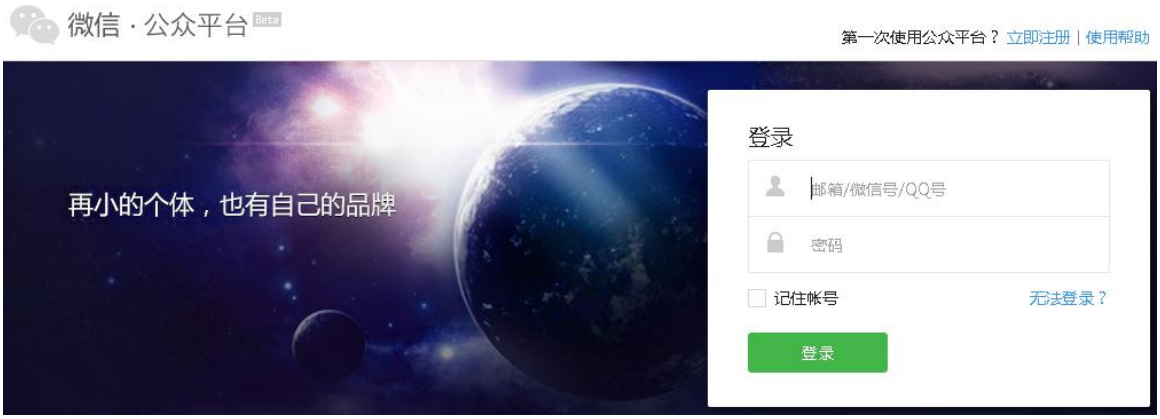
配置步骤

步骤 1 登录微信公众号查阅并记录“SSID”、“ShopId”、“AppId”、“SecretKey”信息。

提示

- 如果是第一次使用微信公众平台，请登录路由器的“微信连 WiFi”页面，点击微信连 WiFi 使用说明，参考该帮助文档进行设置。
- 如果微信公众号没有“微信连 Wi-Fi”功能，请添加，详情可请登录路由器的“微信连 WiFi”页面，点击微信连 WiFi 使用说明，参考该帮助文档进行设置。

1. 使用浏览器访问 https://mp.weixin.qq.com，输入微信公众号账号和密码登录，如果没有请注册。



2. 点击“微信连 Wi-Fi”，再点击“设备管理”，在出现的页面点击“详情”。

3. 在出现的页面点击“详情”。

4. 记录“SSID”、“ShopID”、“Appid”、“SecretKey”参数信息，用于设置路由器微信连 WiFi 功能时输入。

步骤 2 登录路由器设置微信连 WiFi。

1. 点击『微信连 WiFi』。
2. 在“微信连 WiFi”选项选择“开启”。
3. 在“微信公众平台参数设置”模块，输入微信公众平台上的“SSID”、“ShopID”、“AppID”、“SecretKey”参数。

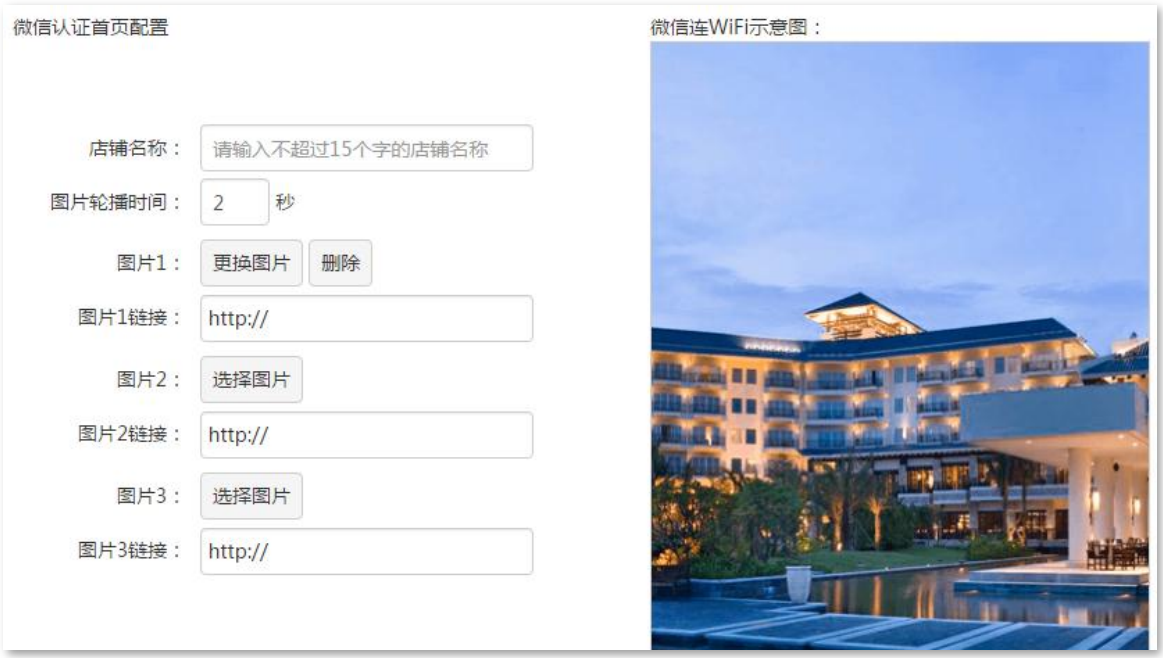
4. 在“微信认证首页配置”模块，设置微信认证的推送页面信息。

(1) 店铺名称：设置广告推送显示的店铺名称，如“XX 餐厅”。

(2) 图片轮播时间：设置图片切换的时间。

(3) 图片 1/2/3：点击 更换图片 ，上传要推送的图片。

(4) 图片 1/2/3 链接：设置点击图片后跳转的网址，如“www.baidu.com”。



5. 在“不需要认证的主机”模块，添加不需要微信认证的客户端信息。

(1) 点击 新增 。

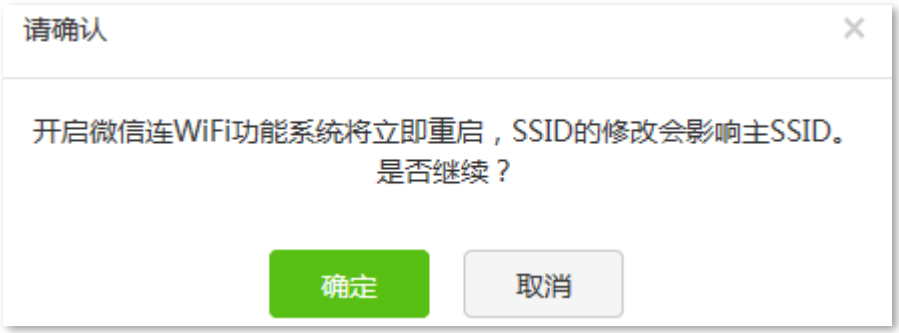
(2) 主机类型：选择不需要微信认证的客户端类型。

(3) 主机地址：输入该客户端的地址信息。

(4) （可选）备注：输入该客户端的备注。

(5) 点击 确定 。

(6) 返回微信连 WiFi 页面，点击 确定 。



—完成

验证配置

无线客户端连接启用“微信认证”的无线信号，在浏览器访问网页时，需要进行微信认证，认证成功后才能上网。

移动设备（如智能手机、平板电脑等）微信连 WiFi 步骤如下：

1. 移动设备连接启用了“微信认证”的 WiFi 信号。
2. 在移动设备上打开浏览器访问网页，出现商家自定义的微信连 WiFi 欢迎页。（有的手机连上该 WiFi 信号后，会自动出现欢迎页）

   提示

   如果没有出现微信连 WiFi 欢迎页，可以访问其他的网址尝试。

3. 用户点击欢迎页面的 微信认证上网 ，并根据页面提示操作，移动设备完成认证就可以上网了。

   另外，在【完成】认证页面，用户还可以点击 关注我们 ，关注商家的微信公众号，以此来增加商家的微信粉丝数并赢得二次营销机会。

PC（笔记本或安装了无线网卡的台式机）微信连 WiFi 步骤如下：

1. PC 连接启用了“微信认证”的 WiFi 信号。
2. 在 PC 上打开浏览器访问网页，出现商家自定义的微信连 WiFi 欢迎页。

   提示

   如果没有出现微信连 WiFi 欢迎页，可以访问其他的网址尝试。

3. 在欢迎页面，点击 一键上网 ，即可访问互联网。

14 虚拟服务器

虚拟服务器章节包括：

端口映射、UPnP、DMZ 主机、DDNS。

14.1 端口映射

14.1.1 概述

在“端口映射”页面，您可以添加端口映射规则。

默认情况下，广域网中的主机不能主动访问本路由器局域网内的主机。端口映射使广域网的用户可以访问局域网主机，同时保护局域网内部不受侵袭。此功能将路由器外网端口映射到局域网服务器，使路由器能够将发送到外网端口的服务请求转发到局域网服务器上。

点击『虚拟服务器』，进入端口映射设置页面。

添加端口映射规则

1. 点击『虚拟服务器』→『端口映射』。
2. 点击 +新增 。

3. 在弹出的窗口设置主机 IP 地址、端口号等参数。
4. 点击 确定 。

—完成

参数说明：

参数	说明
+新增	点击此按钮可以添加端口映射规则。
删除	点击此按钮可以删除已选中的端口映射规则。
内网主机 IP	局域网建立服务器的电脑的 IP 地址。
内部端口	局域网服务器的服务端口。
外部端口	路由器开放给互联网用户访问的端口。
协议	相应服务的协议类型。设置时，如果不确定服务的协议类型，建议选择“全部”。
接口	局域网服务映射的 WAN 口，即外网访问内网服务器时使用的 WAN 口。
状态	该规则的状态，包括已启用和未启用。
操作	可对规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改内网主机 IP 地址、内网端口段、外网端口段、映射线路等。 • 点击可以删除规则。

14.1.2 端口映射示例

组网需求

某企业使用 W15E 进行网络搭建。假设路由器 WAN 口获取的 IP 地址为 202.105.106.55。外出出差人员需要访问自己在公司电脑上的资源。

方案设计

可以通过端口映射功能实现。首先要在公司的电脑上建一个 FTP 服务器，并在服务器上存放要访问的资源，然后在路由器上设置端口映射功能。假设 FTP 服务器的基本信息如下：

- IP 地址：192.168.0.100
- 用户名、密码：admin
- 端口：21

参考拓扑图如下：

提示

- 确保路由器 WAN 口获取公网 IP 地址。
- 须手动配置内网电脑 IP，避免因为 IP 的自动变化而导致服务中断。
- 系统防火墙、某些杀毒软件、安全卫士可能会阻止其它电脑访问内网电脑上的服务器，建议在使用本功能时暂时关闭内网电脑上的这些程序。

配置步骤

1. 点击『虚拟服务器』→『端口映射』。
2. 点击 +新增 。

3. 内网主机：输入内网建立服务的电脑 IP，如“192.168.0.100”。
4. 内网端口：输入服务器使用的端口，如“21”。
5. 外网端口：输入路由器开放给外网的端口，如“21”。
6. 协议：选择服务的协议，建议为“全部”。
7. 映射线路：选择内网服务映射的 WAN 口，本例为“WAN1”。
8. 点击 确定 。

—完成

配置验证

外网用户访问内网资源时，只需在已连接互联网电脑上访问 ftp://202.105.106.55，输入用户名、密码即可。

注意

- 端口映射规则的“外网端口”和远端 WEB 管理的“端口号”不能相同，否则会发生冲突，导致端口映射不能用。
- 设置规则后，互联网上的用户就可以使用“协议名称：//WAN 口当前的 IP 地址：外网端口”的形式访问架设在内网的相应服务器。

14.2 UPnP

在“UPnP”页面，您可以开启或关闭 UPnP 功能。

UPnP（Universal Plug and Play）通用即插即用网络协议。可以实现自动端口映射功能，UPnP 协议可以自动识别用户设备，为某些程序自动打开端口。此功能需要操作系统支持 UPnP 或安装 UPnP 的应用软件。

点击『虚拟服务器』→『UPnP』，进入设置页面。

路由器启用 UPnP 功能后：如果局域网电脑支持 UPnP，可以在“网络”中快速登录路由器管理页面；当局域网中运行支持 UPnP 的程序（如迅雷等）时，就可以看到 UPnP 页面的端口转换信息，端口转换信息由应用程序发出请求时提供。如下图示。

14.3 DMZ 主机

14.3.1 概述

在“DMZ 主机”页面，您可以设置 DMZ 功能。

将局域网中的某台电脑设置为 DMZ 主机后，该电脑与互联网通信时将不受限制。如某些视频会议和在线游戏，可将正在进行这些应用的电脑设置为 DMZ 主机，使视频会议和在线游戏更加顺畅。

点击『虚拟服务器』→『DMZ 主机』进入设置页面。

注意

- 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主机不再起作用。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。
- 须手动设置作为 DMZ 主机的内网电脑的 IP 地址，避免动态获取导致 DMZ 功能失效。
- 安全软件、杀毒软件以及系统自带防火墙，可能会影响 DMZ 主机功能，在使用本功能时，请暂时关闭。不使用 DMZ 主机功能时，建议取消 DMZ 设置，并且打开防火墙、安全卫士和杀毒软件。

14.3.2 启用 DMZ 主机

1. 点击『虚拟服务器』→『DMZ 主机』。
2. DMZ 主机：点击“开启”。
3. 主机 IP 地址：输入要设置 DMZ 主机的电脑 IP 地址。
4. 点击 确定 。

—完成

参数说明：

参数	说明
DMZ 主机	开启/关闭 DMZ 主机功能。
VPN 端口过滤	开启/关闭 VPN 端口过滤功能。 • 开启：启用 DMZ 功能时，启用 VPN 端口过滤。此时由路由器的 VPN 服务响应外网的 VPN 请求。 • 关闭：启用 DMZ 功能时，禁用 VPN 端口过滤。此时路由器的 VPN 功能不可用，由 DMZ 主机响应外网的 VPN 请求。
主机 IP 地址	DMZ 主机 IP 地址。

14.4 DDNS

14.4.1 概述

在“DDNS”页面，您可以设置 DDNS 功能，将 WAN 口 IP 地址绑定固定的域名。

DDNS 即动态域名服务，是将路由器动态变化的 WAN 口 IP 地址（公网 IP）映射到一个固定的域名上。当服务运行时，DDNS 用户端通过信息传递把该主机当前的 WAN 口 IP 地址传送给 DDNS 服务器，服务器会更新数据库中域名与 IP 的映射关系，实现动态域名解析。

提示

DDNS 功能一般与其他功能结合使用，如端口映射、远端 WEB 管理、DMZ 等。

点击『虚拟服务器』→『DDNS』进入设置页面。

启用 DDNS，页面如下。

参数说明：

参数	说明
DDNS 状态	开启/关闭 DDNS 功能。默认关闭。
DDNS 供应商	提供 DDNS 的服务提供商，本路由器支持 3322.org、88ip.cn、oray.com（花生壳）、gnway.com（金万维）。
服务类型	仅对 oray.com 有效，该 DDNS 账号的类型。
用户名	登录 DDNS 服务的用户名，即在“DDNS 供应商”网站上注册的登录用户名。
密码	登录 DDNS 服务的密码，即在“DDNS 供应商”网站上注册的登录密码。
域名信息	从 DDNS 服务器获取的域名信息，除了 oray.com 外，设置其他 DDNS 提供商时，需要手动输入在其网站上注册的域名。
联网状态	DDNS 服务的运行状态。

14.4.2 添加 DDNS 规则

1. 点击『虚拟服务器』→『DDNS』。
2. 在“DDNS 供应商”选项选择相应的 DDNS 服务商，点击注册去。

3. 进入相关 DDNS 服务商网站，注册。
4. 重新进入『虚拟服务器』→『DDNS』页面，设置 DDNS 供应商、用户名、密码、域名等信息。
5. 点击 确定 。

—完成

14.4.3 DDNS 示例

组网需求

某企业使用 W15E 进行网络搭建，且路由器 WAN 口 IP 是动态变化的。外出出差人员需要通过固定域名访问自己在公司电脑上的资源。

方案设计

可以通过 DDNS 功能实现。首先要在公司的电脑上建一个 FTP 服务器，并在服务器上存放要访问的资源，然后在路由器上设置 DDNS 功能、端口映射功能。参考拓扑图如下：

配置步骤

步骤 1 注册域名。

1. 进入 DDNS 设置页面，启用 DDNS，选择“DDNS 供应商”，如“oray.com”，然后点击注册去。

2. 参照网站的提示信息注册域名。

   假设注册的基本信息如下：

   - 提供商：oray.com
   - 用户名：Tom-Jerry
   - 密码：tomjerry123456
   - 域名：tom-jerry.imwork.net

步骤 2 设置 DDNS 规则。

重新进入 DDNS 设置页面，参考下文操作。

1. DDNS 状态：点击“开启”。
2. DDNS 供应商：选择相应的供应商，如本例为 oray.com。
3. 用户名/密码：输入在 DDNS 供应商网站注册的用户名、密码。
4. 点击 确定 。

完成设置后，刷新一下页面，稍等片刻。当“联网状态”显示**已连接**，且“域名信息”已获取到域名地址时，连接成功。

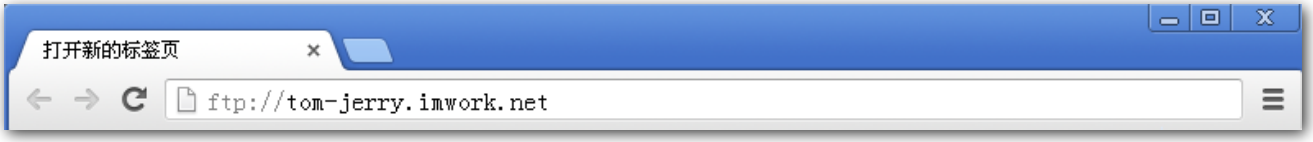
该账号在 DDNS 供应商网站关联了几个域名，本页的“域名信息”就会显示几个域名，这些域名都映射路由器的 WAN 口 IP 地址。

步骤 3 设置端口映射功能，详细设置步骤请参考 14.1 端口映射。

—完成

配置验证

当外网用户访问内网资源时时，只需在已连接互联网电脑上访问 ftp://tom-jerry.imwork.net，根据页面提示操作即可。



15 系统管理

系统管理章节包括：

登录密码、重启、配置备份/恢复、软件升级、策略升级、恢复出厂设置、系统时间、远端 WEB 管理、排障工具。

15.1 登录密码

15.1.1 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。

点击『系统管理』，进入登录密码设置页面。

15.1.2 修改登录密码

1. 点击『系统管理』→『登录密码』。
2. 旧密码：输入当前路由器的登录密码。
3. 新密码：设置新的登录密码。
4. 确认密码：再一次输入新的登录密码。
5. 点击 确定 。

—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。

15.2 重启

15.2.1 概述

在“重启”页面，您可以立即重启路由器或设置路由器定时重启。

当设置的某项参数不能生效或路由器不能正常使用时，可以尝试重启路由器解决。本路由器支持“手动重启”和“定时重启”两种方式。

点击『系统管理』→『重启』，进入设置页面。

15.2.2 手动重启路由器

1. 点击『系统管理』→『重启』。
2. 点击 重启 ，然后根据页面提示操作，等待路由器重启即可。

—完成

15.2.3 定时重启路由器

1. 点击『系统管理』→『重启』。
2. 定时重启：点击“开开”。
3. 重启时间：点击下拉框，选择路由器自动重启的时间，如“23:30”。
4. 重复：设置路由器自动重启的日期，如“每天”。
5. 点击 确定 。

—完成

上述规则设置完成后，路由器每天的 23:30 将会自动重启。

15.3 配置备份/恢复

15.3.1 概述

在“配置备份/恢复”页面，您可以将电脑当前的配置备份到电脑，或将电脑备份的路由器配置文件导入到路由器。

为了防止路由器出现故障后，恢复出厂设置而丢失配置信息，可以对路由器的现有配置信息进行备份。备份后系统会导出一个配置文件，如果将路由器恢复出厂设置，只需导入配置文件即可恢复之前的配置。

点击『系统管理』→『配置备份与恢复』，进入设置页面。

- 备份：对路由器的现有配置信息进行备份。
- 恢复：将路由器的备份文件导入，恢复之前的配置。

15.3.2 备份配置步骤

1. 点击『系统管理』→『重启』。
2. 点击 备份 。
3. 参照电脑的提示选择备份文件的存储路径即可。

—完成

15.3.3 恢复配置设置步骤

1. 点击『系统管理』→『重启』。
2. 点击 浏览 ，选择并加载路由器的备份文件。
3. 点击 恢复 ，等待进度条走完即可。

—完成

15.4 软件升级

15.4.1 概述

在“软件升级”页面，您可以对路由器进行软件升级。

软件升级可以获取更稳定的软件版本或新增功能。本路由器支持软件“本地升级”和“在线升级”，默认为“在线升级”，即系统自动检测是否有新的升级程序，并将检测到升级软件的相关信息显示出来。

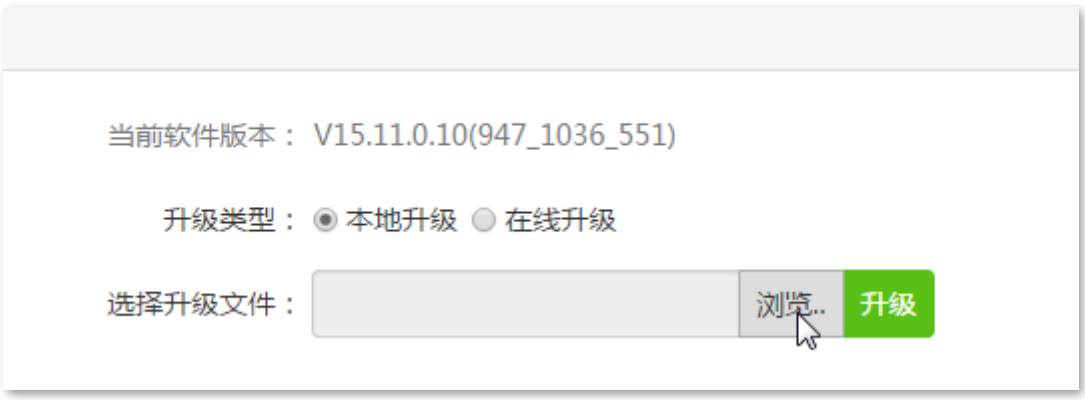
点击『系统管理』→『软件升级』，进入设置页面。

15.4.2 本地升级步骤

注意

- 升级之前，请确认软件的正确性，错误的升级将会损坏路由器。
- 升级过程中，请勿断开路由器电源，否则可能造成路由器损坏！
- 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，请将路由器恢复出厂设置，然后重新配置各上网参数。

1. 登录 Tenda 官网 http://www.tenda.com.cn，下载路由器最新的升级软件并存放到本地电脑的相应目录。
2. 登录路由器管理页面，点击『系统管理』→『软件升级』。
3. 升级类型：点击选择“本地升级”。
4. 点击 浏览 ，找到并载入相应目录下的升级软件。



5. 点击 升级 。

—完成

将会出现进度条，等待进度条走完即可。

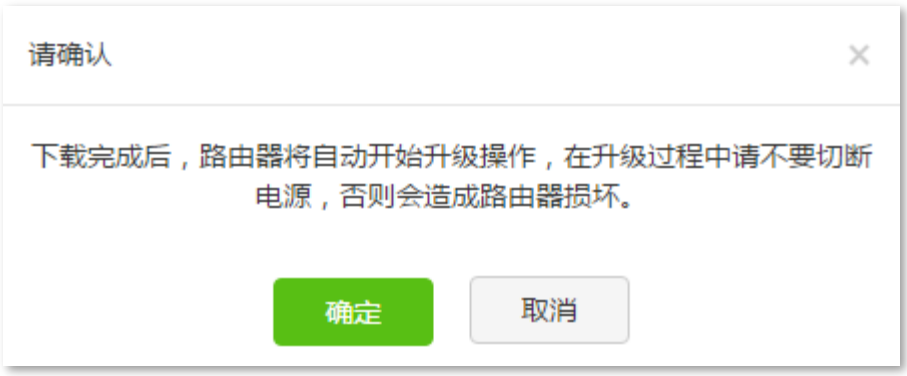
进度条走完后，将会自动跳转到登录页面。此时进入系统管理页面将路由器恢复出厂设置，然后重新设置上网。

15.4.3 在线升级步骤

路由器连接互联网后，会自动检测软件版本。当左侧菜单栏『系统管理』→『软件升级』选项出现时，路由器已经检测到新的软件版本，可以进行在线升级。

1. 进入『系统管理』→『软件升级』页面。
2. 点击 下载并升级 。

3. 在弹出的对话框点击点击 确定 。



—完成

请稍等。升级成功后，会自动跳转到路由器的管理页面。

15.5 策略升级

15.5.1 概述

在“策略升级”页面，您可以对路由器进行策略升级。策略升级不对路由器系统进行更新，只更新行为特征库和 URL 特征库。

点击『系统管理』→『策略升级』，进入设置页面。

15.5.2 本地升级步骤

1. 登录 Tenda 官网 http://www.tenda.com.cn，下载路由器最新策略升级软件并存放到本地电脑相应目录。
2. 登录路由器管理页面，点击『系统管理』→『策略升级』。
3. 点击 浏览 ，找到并载入相应目录下的策略升级软件。
4. 点击 升级 ，出现进度条，等待进度条走完即可。

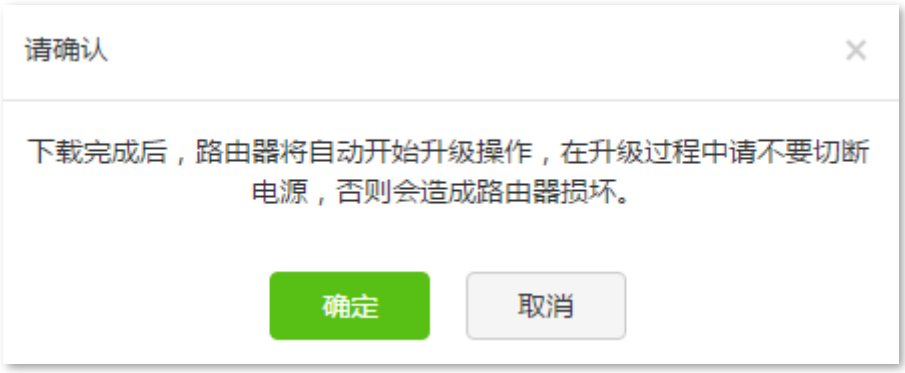
—完成

15.5.3 在线升级步骤

路由器连接互联网后，会自动检测软件版本。当左侧菜单栏『系统管理』→『策略升级』选项出现时，路由器已经检测到新的软件版本，可以进行在线升级。

1. 点击『系统管理』→『策略升级』。
2. 点击 下载并升级 。

3. 在弹出的对话框点击 确定 。



—完成

请稍等。升级成功后，会自动跳转到路由器的管理页面。

15.6 恢复出厂设置

15.6.1 概述

在“恢复出厂设置”页面，您可以将路由器配置恢复到出厂状态。

当不能访问互联网，但又找不到问题所在时，或需要登录路由器的管理页面，但是忘记登录密码时，可以将路由器恢复出厂设置。

路由器支持“软件恢复出厂设置”和“硬件恢复出厂设置”两种方法。路由器默认登录 IP 地址为 192.168.0.1。

注意

- 恢复出厂设置意味着路由器的所有设置将会丢失，需要重新设置路由器才能上网。
- 恢复出厂设置过程中请确保路由器供电正常。

15.6.2 通过 WEB 管理页面恢复出厂设置

点击『系统管理』→『恢复出厂设置』，进入设置页面。点击 恢复出厂设置 。可将路由器恢复到出厂状态。

15.6.3 通过 RESET 按钮恢复出厂设置

在路由器启动完成的状态下，用尖状物按住机身上的 RESET 按钮 8 秒后放开。等待约 1 分钟即可。

15.7 系统时间

15.7.1 概述

在“系统时间”页面，您可以设置路由器的系统时间。路由器的行为管理等功能涉及到时间的设置，因此为了保证规则生效，需要确保路由器的系统时间正确。

点击『系统管理』→『系统时间』，进入设置页面。本路由器支持“与网络时间同步”和“手动设置”两种设置方法。

提示

- 路由器系统时间默认的获取方式是“与网络时间同步”，路由器联网成功后，会自动根据校时周期同步所选择时区的时间。
- 关闭路由器后，时间信息会消失。当下次开启路由器并连上互联网后，路由器会自动获取所选择时区的时间，路由器中所有关于时间设置才能生效。

15.7.2 手动设置系统时间

1. 点击『系统管理』→『系统时间』。
2. 在“系统时间”选项点击“手动设置”。
3. 点击 与电脑同步 。
4. 点击 确定 。

—完成

15.8 远端 WEB 管理

15.8.1 概述

在“远端 WEB 管理”页面，您可以设置远程访问路由器功能。

一般情况下，只有连在路由器局域网的客户端才能登录路由器的 WEB 管理页面。有特殊需要时，可以远程通过 WAN 口访问路由器 WEB 管理页面。

点击『系统管理』→『远端 WEB 管理』，进入设置页面。

启用规则，如下图示。

参数说明：

参数	说明
远端 WEB 管理	开启/关闭远程 WEB 管理功能，默认关闭。
WAN 口	选择远程访问路由器时使用的 WAN 口。
可管理 IP	可以远程访问路由器的 IP 地址。 • 全部 IP 地址：互联网上所有电脑都能登录路由器 WEB 页面，为了网络的安全，不建议选择。 • 特定 IP 地址：只有指定 IP 地址的电脑能远程登录路由器 WEB 页面。
端口号	远程管理路由器时使用的端口号。默认为 8088，可根据需要修改。 提示 1~1024 端口已被熟知服务占用，为避免端口冲突，强烈建议修改该端口为 1025~65535 范围内的端口。

15.8.2 设置远端 WEB 管理

1. 点击『系统管理』→『远端 WEB 管理』。
2. 远端 WEB 管理：点击“开启”。
3. WAN 口：选择相应的 WAN 口。
4. 可管理 IP：设置可以远程访问的主机 IP 地址。
5. 端口号：设置远程访问使用的端口号，如无特殊情况，请保持默认设置。
6. 点击 确定 。

—完成

15.8.3 远端 WEB 管理示例

组网需求

某企业使用 W15E 进行网络搭建，路由器 WAN1 的 IP 地址是 202.105.106.55。网络管理人员外出出差时可能会维护网络，需要远程登录路由器管理页面。

方案设计

可通过远端 WEB 管理功能实现。参考拓扑图如下：

配置步骤

1. 点击『系统管理』→『远端 WEB 管理』。
2. 在“远端 WEB 管理”选项点击“开启”。
3. 在“WAN 口”选项选择远程管理启用的 WAN 口，本例为“WAN1”。
4. 点击 确定 。

—完成

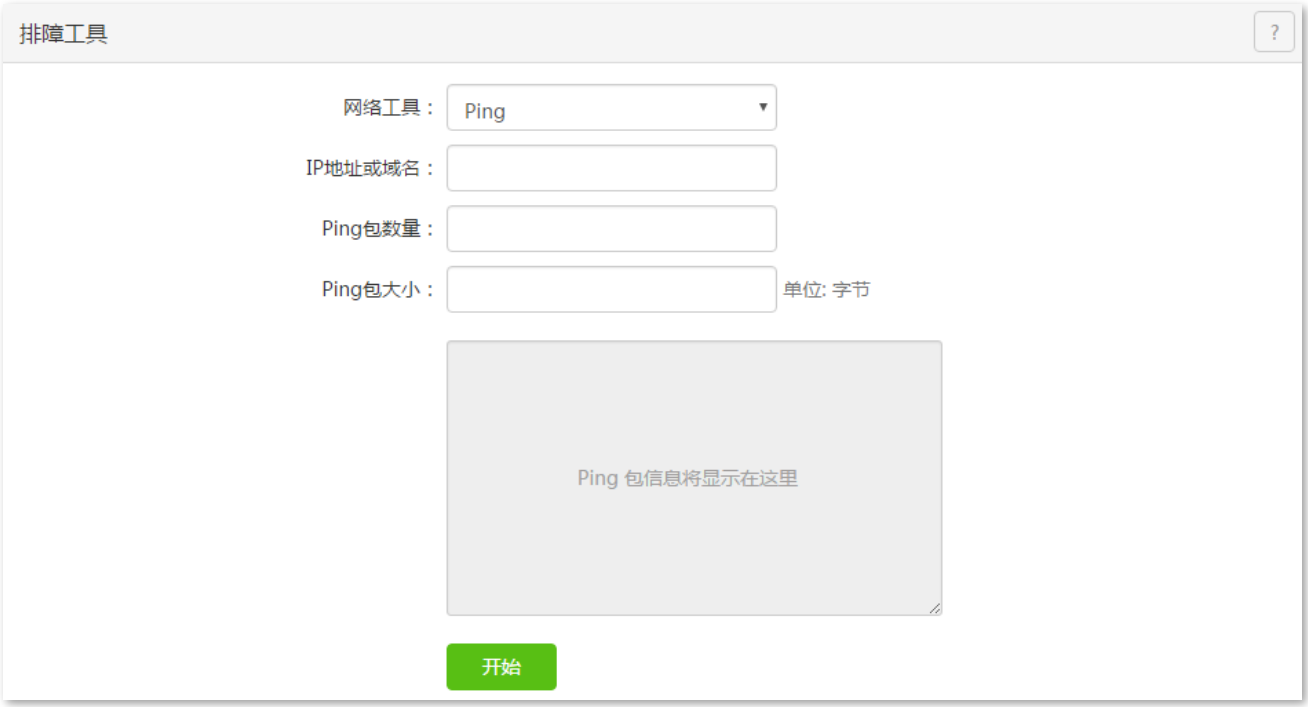
配置验证

在远端电脑（已连接互联网并获取公网 IP 地址）的浏览器访问 http://202.105.106.55:8088，即可登录路由器并对其进行管理。

15.9 排障工具

15.9.1 概述

在“排障工具”页面您可以检测网络通信情况。点击『系统管理』→『排障工具』，进入设置页面。



参数说明：

参数	说明
Ping	常用的故障诊断与排除命令。它由一组 ICMP 回应请求报文组成，如果网络正常运行将返回一组回应应答报文。
Traceroute	路由跟踪实用程序，用于确定 IP 数据访问目标所采取的路径。

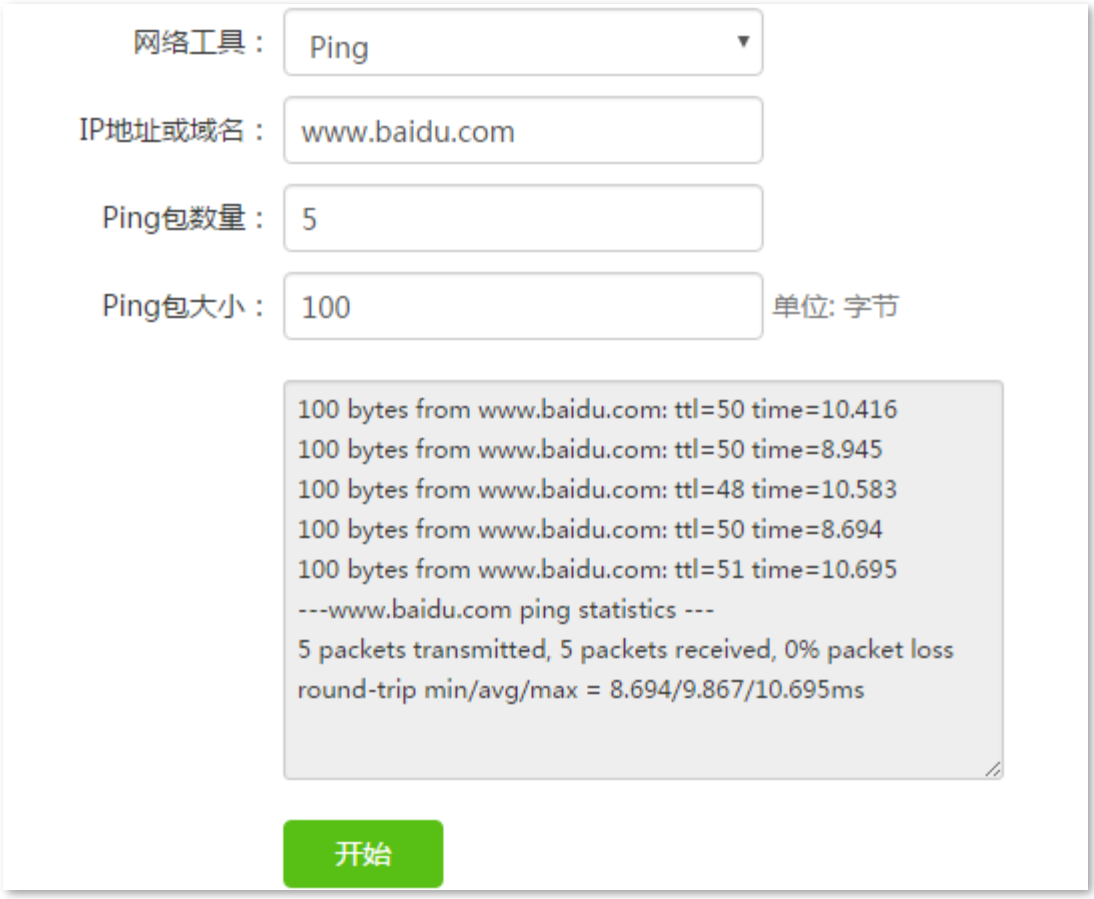
15.9.2 Ping 检测步骤

Ping 功能可以检测网络的连通性。假设要检测路由器与百度的连通性，可参考下文设置。

1. 进入『系统管理』→『排障工具』页面。
2. 点击下拉菜单，选择“Ping”。
3. IP 地址或域名：输入要检测的 IP 地址或域名，本例为“www.baidu.com”。
4. Ping 包个数：设置进行 Ping 包的个数，如“5”。
5. 数据包大小：设置 Ping 包的大小，如“100”。
6. 点击 开始 。

一完成

稍等片刻，结果将会显示在页面下方。



15.9.3 Traceroute 检测步骤

Traceroute 功能用于检测到目的 IP 地址或域名过程中的每一跳地址。假设要检测路由器到百度的路径，可设置如下。

1. 点击『系统管理』→『排障工具』。
2. 点击下拉菜单，选择“Traceroute”。
3. 目标 IP 或域名：输入要检测的 IP 地址或域名，本例为“www.baidu.com”。
4. 点击 开始 。

—完成

稍等片刻，结果将显示在页面下方。路径的记录按序列号从 1 开始，每个纪录是一跳，每跳表示一个网关。

16 系统状态

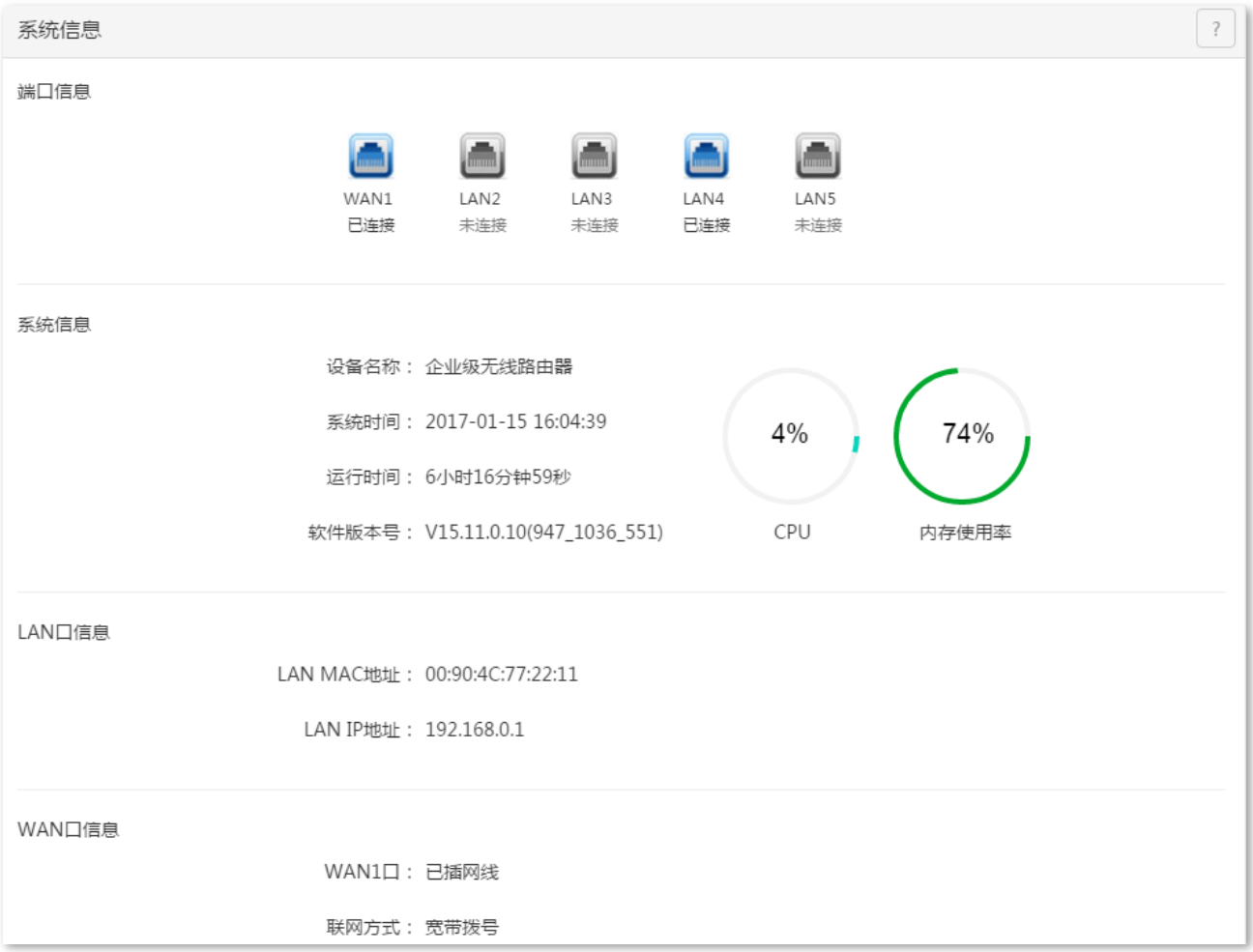
系统状态章节包括：

系统信息、用户列表、流量统计、防攻击日志、系统日志。

16.1 系统信息

在“系统信息”页面，您可以查看可以查看路由器的端口信息，系统信息，LAN 口信息以及 WAN 口信息等。

点击『系统状态』，进入系统信息页面。



参数说明：

参数		说明
端口信息		路由器端口的状态，包括是否有设备连接，充当角色是 WAN 口还是 LAN 口。 表示接口连接正常。 表示接口未连接设备或连接异常。
系统信息	设备名称	本路由器的名称。
	系统时间	本路由器的系统时间。如果显示有误，可以在“系统时间”修改。
	运行时间	路由器本次联网成功的时长。
	软件版本号	路由器的软件版本。 对路由器进行软件升级操作后，可以在此处查看是否已成功升级到目标版本。
LAN 口信息	LAN MAC 地址	路由器 LAN 口 MAC 地址。
	LAN IP 地址	路由器的 LAN 口 IP 地址，即用于登录路由器管理页面的 IP 地址。 本路由器支持 IP 地址（默认为 192.168.0.1）登录和域名地址（tendawifi.com）登录。
WAN 口信息	WAN 口	WAN 口状态，包括“已插网线”和“未插网线”。
	联网方式	对应 WAN 口的上网方式。
	IP 地址	对应 WAN 口的 IP 地址。
	子网掩码	WAN IP 地址的子网掩码。
	主 DNS	对应 WAN 口获取的首选 DNS 服务器 IP 地址。
	次 DNS	对应 WAN 口获取的备用 DNS 服务器 IP 地址。
	上行速率	对应 WAN 口的上行速率。
	下行速率	对应 WAN 口的下行速率。
	联网状态	对应 WAN 口的联网状态。

16.2 用户列表

在“用户列表”页面，您可以查看连接到路由器的 DHCP 用户、无线客户端、VPN 用户、PPPoE 在线用户、WEB 认证在线用户、IPSec 安全联盟的数量。

点击『系统状态』→『用户列表』，进入页面。

16.2.1 DHCP 用户

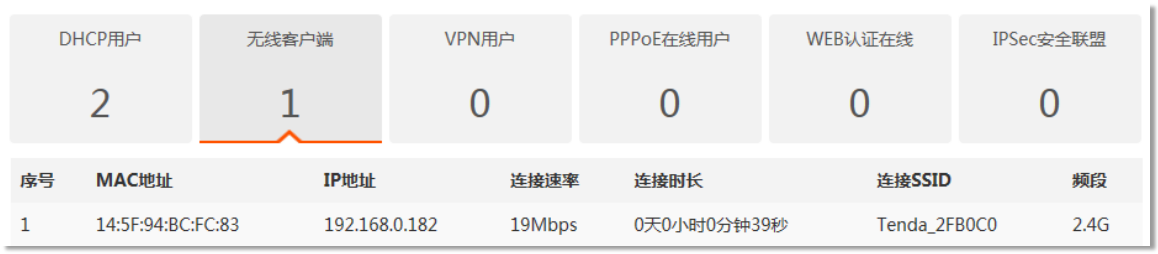
在“DHCP 用户”模块，您可以查看从路由器 DHCP 服务器获取 IP 地址的用户详细信息。

参数说明：

参数	说明
IP 地址	客户端从路由器 DHCP 服务器获取 IP 地址的信息。
MAC 地址	客户端的 MAC 地址信息。
在线时长	客户端的在线时长。
剩余租期	客户端的剩余租期。 客户端 DHCP 获取 IP 地址时，DHCP 服务器分配给客户端的 IP 地址有一定的租约时间。 当租期满后，如果客户端没有续约请求，服务器会收回该 IP 地址；如果客户端希望继续使用，在租期到达一半时间，客户端会向 DHCP 服务器单播发送 DHCP 请求报文，如果续约失败，客户端会在 7/8 时继续单播 DHCP 请求报文进行续约。

16.2.2 无线客户端

在“无线客户端”模块，您可以查看连接路由器 WiFi 信号的无线客户端详细信息。



参数说明：

参数	说明
MAC 地址	客户端的 MAC 地址。
IP 地址	客户端的 IP 地址。
连接速率	客户端当前连接速率。
连接时长	客户端的在线时长。
连接 SSID	客户端连接的无线信号名称。
频段	客户端连接的无线信号所属的频段。

16.2.3 VPN 用户

在“VPN 用户”模块，您可以查看拨入 VPN 服务器的 VPN 客户端详细信息。

参数说明：

参数	说明
用户名	VPN 客户端拨入 VPN 服务器使用的账号信息。
备注	对应账号信息的描述。
拨入 IP	VPN 客户端 IP 地址。如果 VPN 客户端是路由器 ,则会显示路由器启用 VPN 功能的 WAN 口 IP 地址。
分配 IP	VPN 服务器分配给 VPN 客户端的 IP 地址信息。

16.2.4 PPPoE 在线用户

在“PPPoE 在线用户”模块，您可以查看通过拨号上网的客户端详细信息。

参数说明：

参数	说明
账号	客户端进行 PPPoE 认证使用的账号信息。
备注	对应账号信息的描述。
IP 地址	客户端从 PPPoE 服务器获取的 IP 地址信息。
上传/下载速率	客户端的上传/下载速率。

16.2.5 WEB 认证在线

在“WEB 认证在线”模块，您可以查看通过网页认证上网的客户端详细信息。

参数说明：

参数	说明
用户名	客户端进行 WEB 认证使用的账号信息。
备注	对应账号信息的描述。
认证时间	客户端 WEB 认证成功的时间。
IP 地址	客户端获取的 IP 地址信息。

16.2.6 IPSec 安全联盟

在“IPSec 安全联盟”页面，您可以查看路由器的 IPSce 隧道通信信息。

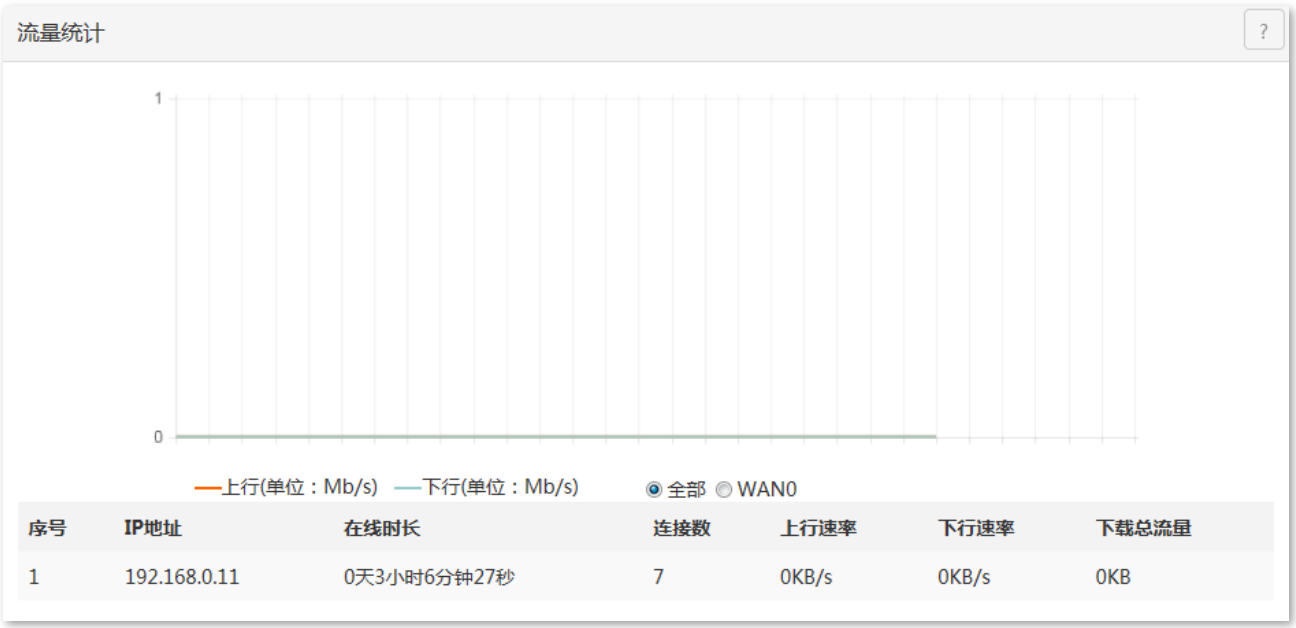
参数说明：

参数	说明
名称	IPSec 隧道名称。
SPI	SPI 参数值。IPSec 隧道的“外出 SPI”值与通信对端的“进入 SPI”值相同。IPSec 隧道的“进入 SPI”值与通信对端的“外出 SPI”值相同。
方向	IPSec 隧道数据的进出方向。
隧道两端	IPSec 隧道数据在互联网的传输方向。
数据流	IPSec 隧道数据在局域网的传输方向。
安全协议	IPSec 隧道使用的安全协议。
AH 验证算法	IPSec 隧道使用的 AH 验证算法。
ESP 验证算法	IPSec 隧道使用的 ESP 验证算法。
ESP 加密算法	IPSec 隧道使用的 ESP 加密算法。

16.3 流量统计

在“流量统计”页面，您可以查看路由器 WAN 口、路由器客户端当前的流量统计信息。动态图表显示路由器当前 WAN 口的上行、下行流量；列表显示单个客户端的具体信息，包括 IP 地址、在线时长、连接数、上行/下行速率、下载总流量。

点击『系统状态』→『流量统计』，进入页面。



16.4 防攻击日志

在“防攻击日志”页面，您可以查看路由器防攻击日志信息。

点击『系统状态』→『防攻击日志』，进入页面。

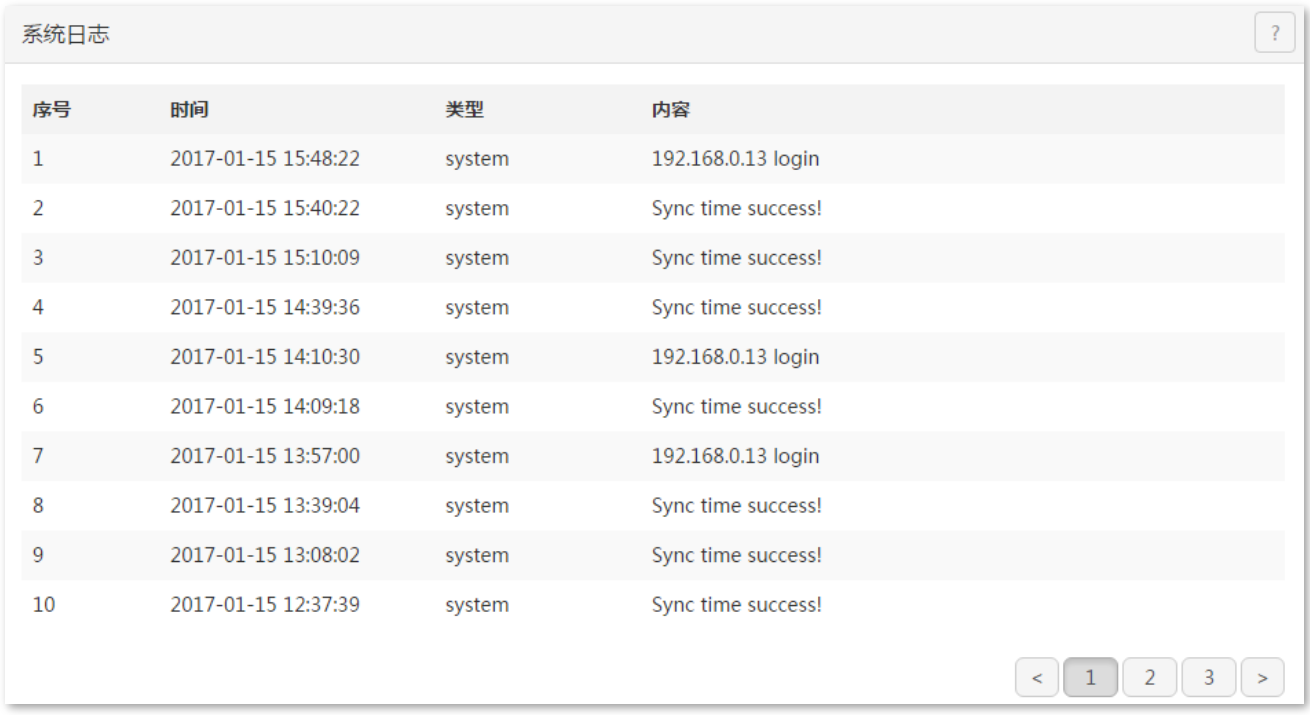
如当路由器受到攻击时，可以查看相关信息。如受到 ARP 攻击时，如下图示：

序号	攻击时间	攻击类型	攻击次数	攻击者IP	攻击者MAC
1	2016-6-9 12:2:53	ARP	340	192.168.0.2	78:E3:B5:9E:60:EF
2	2016-6-9 12:2:53	ARP	214	192.168.0.3	78:E3:B5:9E:60:F0
3	2016-6-9 12:2:53	ARP	153	192.168.0.4	78:E3:B5:9E:5F:F7
4	2016-6-9 12:2:53	ARP	153	192.168.0.5	78:E3:B5:9E:5F:F8
5	2016-6-9 12:2:54	ARP	153	192.168.0.6	78:E3:B5:9E:5F:F9

16.5 系统日志

在“系统日志”页面，您可以查看路由器的日志信息。路由器故障时，可以查看日志信息进行问题排查。

点击『系统状态』→『系统日志』，进入页面。



序号	时间	类型	内容
1	2017-01-15 15:48:22	system	192.168.0.13 login
2	2017-01-15 15:40:22	system	Sync time success!
3	2017-01-15 15:10:09	system	Sync time success!
4	2017-01-15 14:39:36	system	Sync time success!
5	2017-01-15 14:10:30	system	192.168.0.13 login
6	2017-01-15 14:09:18	system	Sync time success!
7	2017-01-15 13:57:00	system	192.168.0.13 login
8	2017-01-15 13:39:04	system	Sync time success!
9	2017-01-15 13:08:02	system	Sync time success!
10	2017-01-15 12:37:39	system	Sync time success!

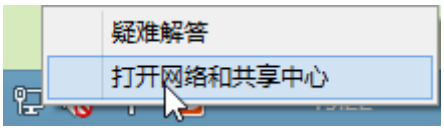
附录

A.1 设置电脑 IP 地址

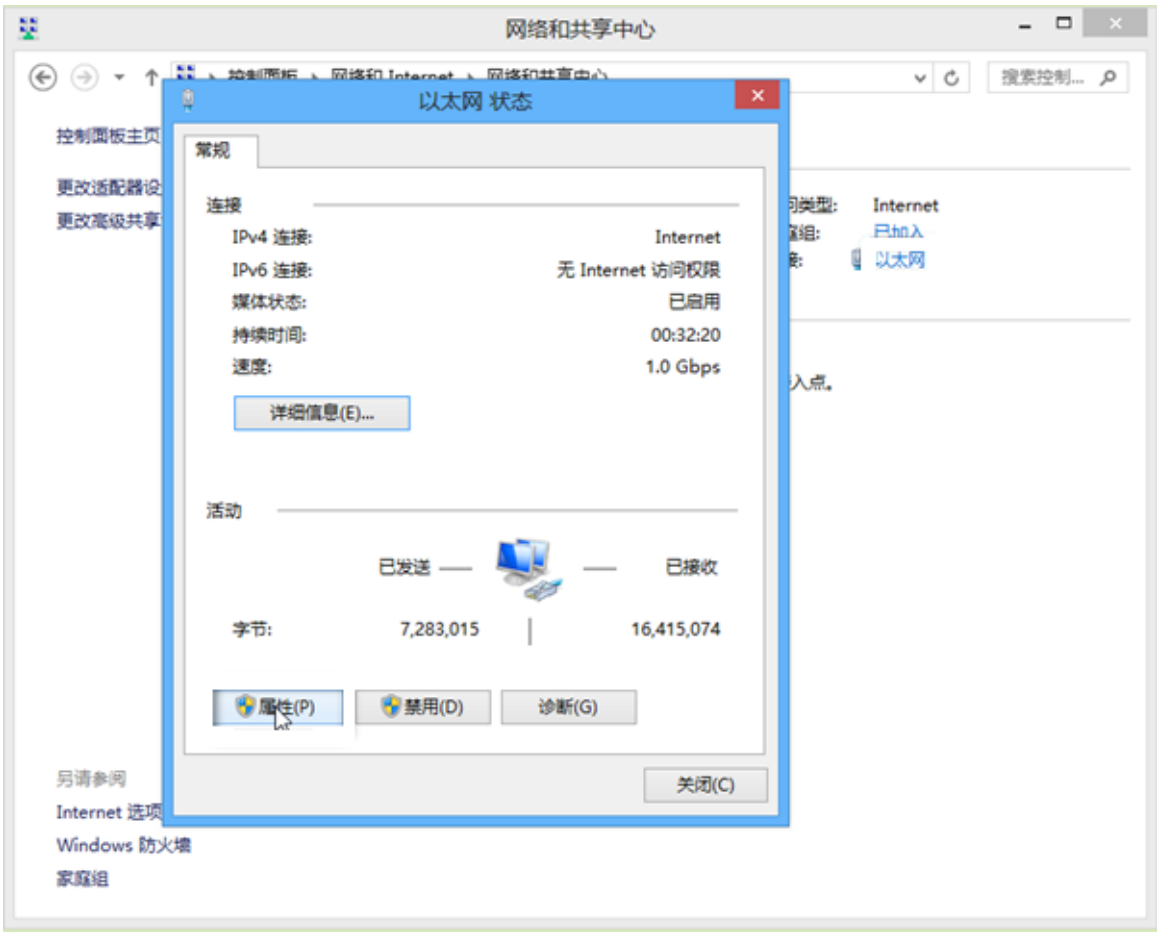
请根据电脑的操作系统，参考对应的设置步骤：Windows 8，Windows 7。此处以有线网卡为例进行设置说明。电脑无线网卡的设置步骤类似。

A.1.1 Windows 8

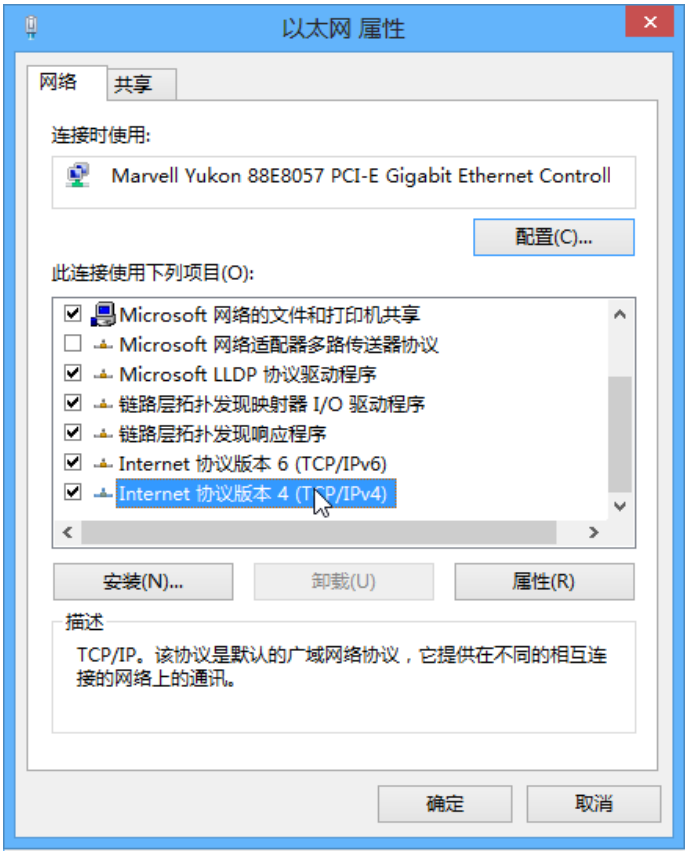
1. 右键点击桌面右下角的网络图标，点击**打开网络和共享中心。**



2. 点击以太网，点击 属性 。



3. 找到并双击 Internet 协议版本 4（TCP/IPv4）。

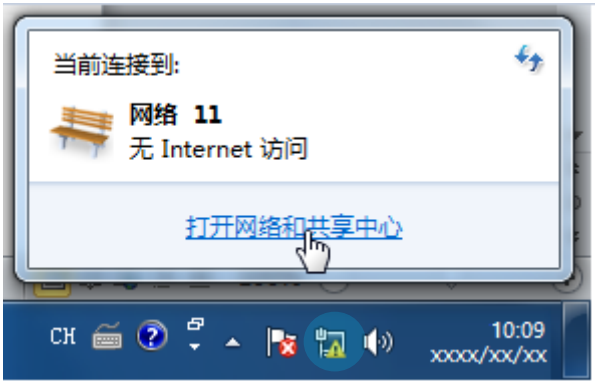


4. 选择自动获得 IP 地址，自动获得 DNS 服务器地址，点击 确定 。

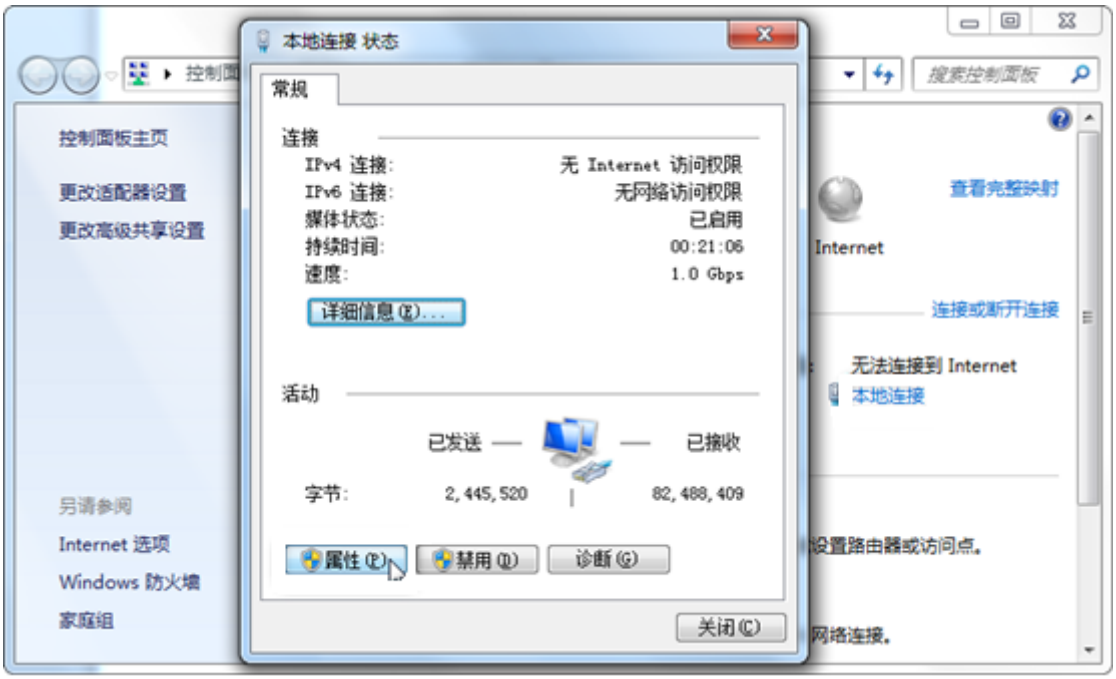
5. 页面自动返回**以太网 属性**对话框后，再点击 确定 。

A.1.2 Windows 7

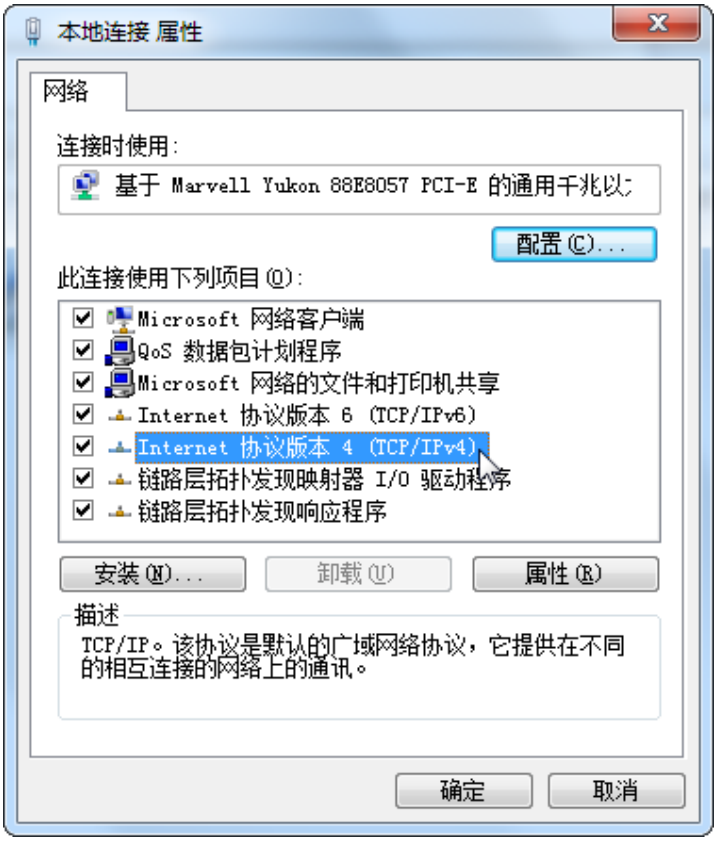
1. 点击桌面右下角的网络图标，如 ，点击**打开网络和共享中心**。



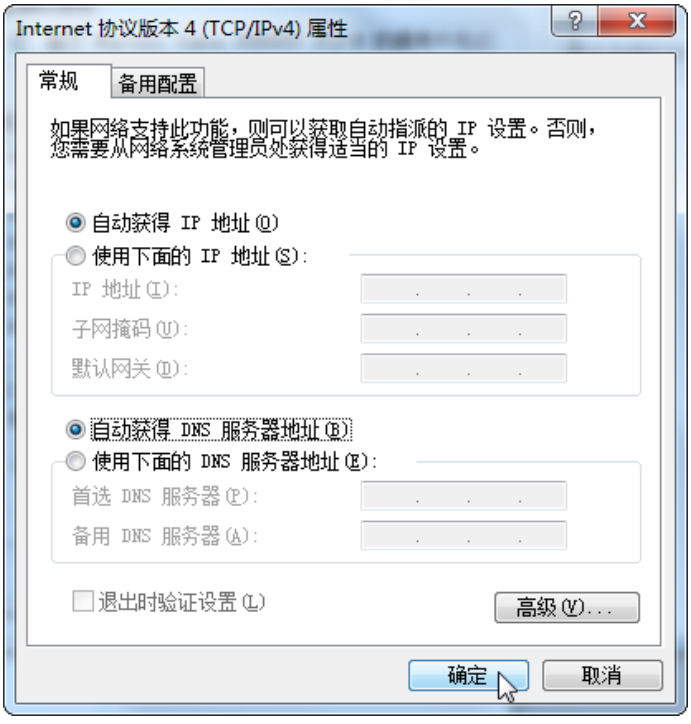
2. 点击本地连接，点击 属性 。



3. 双击 Internet 协议版本 4（TCP/IPv4）。



4. 选择自动获得 IP 地址，自动获得 DNS 服务器地址，点击 确定 。



5. 页面自动返回**本地连接 属性**对话框后，再点击 确定 。

A.2 产品规格

项目	规格
带机量	50 台终端
无线速率	1200Mbps
CPU	单核心 900MHz
内存	128MB
FLASH	16MB
网络接口	5 个 10/100Mbps 自适应 RJ45 端口
指示灯	1 个 SYS 灯，1 个 2.4GHz 灯，1 个 5GHz 灯，1 个 WAN 灯、
按钮	1 个 RESET 按钮
工作环境	工作温度：0℃ ~ 40℃ 工作湿度：（10 ~ 90）%RH，无凝结
存储环境	存储温度：-40℃ ~ 70℃ 存储湿度：（5 ~ 90）%RH，无凝结
电源输入	100-240V AC，50/60Hz
外形尺寸（L*W*H）	225mm*130mm*30 mm

A.3 常见问题解答

问1. 输入 tendawifi.com 或 192.168.0.1 登录不了路由器管理页面，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。
- 无线连接路由器 WiFi 时，请确保已经成功连接 WiFi。
- 确认电脑 IP 地址为 192.168.0.X（X 为 2~254）。
- 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 IP 地址也为 192.168.0.1 的设备。
- 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. 如何选择上网方式？

答：请参考下表描述来选择上网方式，也可以根据系统检测结果来选择或咨询网络供应商。

宽带入户方式	常见上网方式	说明
电话线/网线	宽带拨号	有用户名和密码，需要点击宽带连接（ ）拨号。
有线电视/网线	动态 IP	从上一个路由器接线上网，或者接有线电视上网的用户（珠江宽频、有线通、天威视讯等等）。
网线/光纤	静态 IP	有固定 IP 地址，子网掩码，默认网关，DNS 服务器。

问3. 上网设置完毕，但上不了网，怎么办？

答：请分别从以下几个方面检查：

- 电脑通过网线连接路由器时，请检查线路连接，确保路由器连线正确。
- 手机等无线设备连接路由器 WiFi 设置上网时，设置完成后，请重新连接 WiFi。
- 参考设置电脑 IP 地址将电脑设置为“自动获取” IP 地址。
- 用网线连接电脑和路由器，进入路由器管理页面，修改无线名称和无线密码，然后重连 WiFi。
- 尝试克隆 MAC 地址，重新登录路由器页面，确保路由器联网状态显示“已连接“或“认证成功”。
- 请咨询您的网络供应商。

问4. 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：请用尖状物按住路由器 RESET 按钮 8 秒后放开，等待约 1 分钟即可。路由器恢复设置后，需要重新配置参数。路由器默认登录地址为 192.168.0.1。

问5. 电脑连接路由器后，开机时出现 IP 地址冲突，怎么办？

答：请分别从以下几个方面检查：

- 请确保局域网内没有其他 DHCP 服务器或其它 DHCP 服务器已关闭。
- 请确保局域网内的电脑没有占用路由器的登录 IP 地址，路由器默认登录 IP 地址是 192.168.0.1。
- 请确保局域网内电脑设置的静态 IP 未被其它电脑使用。

问6. 想进入路由器管理页面，但忘记了路由器登录密码，怎么办？

答：请将路由器恢复出厂设置，再重新登录。

恢复出厂设置方法：在路由器启动完成的状态下，持续按住路由器的 RSSET 按钮约 8 秒，指示灯全亮时，路由器将恢复出厂设置。

A.4 有毒有害物质申明

电子信息产品有毒有害物质申明						
部件名称	有毒有害物质或元素					
	铅（pb）	汞（Hg）	镉（Cd）	六价铬（Cr6+）	多溴联苯（PBB）	多溴二苯醚（PBDE）
结构件	×	○	○	○	○	○
单板/电路模块	×	○	○	○	○	○
电源适配器	×	○	○	○	○	○
线缆	×	○	○	○	○	○
连接器	×	○	○	○	○	○
附件	×	○	○	○	○	○

1. “○”表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T11363-2006标准规定的限量要求以下。
2. “X”表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T11363-2006标准规定的限量要求。
3. 由于中国限量标准中没有豁免条例，故标识为“X”并不一定表示为对人体有害。
4. 对生产制造的产品，可能包含这些欧洲豁免的物质。
5. 在所售产品中可能包含所有部件也可能不包含所有部件。

此环保实用期限只适用于产品在用户手册所规定的条件下工作。