企业级路由器

使用说明书

版权声明

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

本说明书适用 Tenda 企业级路由器型号：G1、G3，正文如无特殊说明均以 G3 为例。

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
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 产品简介

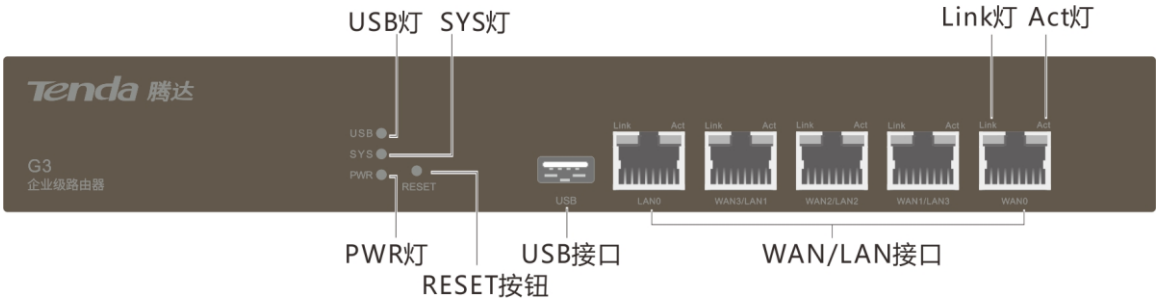
G1/G3 是 Tenda 专为中小型企业、连锁酒店设计的多 WAN 路由器。采用高性能处理器，最大支持 4 个 WAN 口，将负载均衡、流量控制、用户认证功能集中到一体。支持 IPSec/PPTP/L2TP VPN。除此之外，还具备 AC 管理功能，可以管理 Tenda 所有型号的 AP。满足企业、酒店组建高效、安全、易管理网络的需求。

1.2 主要特性

- 默认 2 个广域网 WAN 口，3 个局域网 LAN 口。
- 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 AC 管理，可以管理网络中的 AP。
- 支持 PPPoE 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 USB 文件共享，可以简单设置企业文件服务器。
- 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
USB	USB 接口灯	长亮	有 USB 设备连接，没有数据传输。
		闪烁	正在进行读写操作，有数据传输。
		熄灭	没有 USB 设备连接或连接异常。
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。
PWR	电源灯	长亮	通电正常。
		熄灭	通电异常，请检查电源线是否松动。
Link	/	长亮	接口有设备连接成功。
		熄灭	接口没有设备连接或连接异常。
Act	/	长亮	接口没有数据传输。
		闪烁	接口有数据传输。
		熄灭	接口没有设备连接或连接异常。

接口、按钮说明如下：

接口&按钮	说明
RESET	在路由器启动完成的状态下，用尖状物持续按下 8 秒后松开，设备将会恢复到出厂状态。
USB	USB 接口。可以连接 U 盘、移动硬盘等 USB 设备。
LAN0	内网接口，可连接交换机、电脑等设备。

接口&按钮	说明
WAN3/LAN1、WAN2/LAN2、WAN1/LAN3	内网接口、外网接口复用。 WAN3/LAN1、WAN2/LAN2 默认为 LAN 口，WAN1/LAN3 默认为 WAN 口。 若要修改 WAN 口个数，可在 WEB 页面中设置，详情可参考 WAN 口个数设置。
WAN0	外网接口，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，或网络服务提供商直接提供的宽带网线。

1.3.2 后面板

- 电源接口：用于连接电源线。请使用产品包装盒内的配套电源线进行连接。
- 电源开关：设备连接好电源线后，按下此按钮给设备供电。

1.3.3 贴纸

路由器底部贴纸上有路由器登录地址，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。

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

本路由器支持桌面安装和 19 寸机架安装，请根据您的安装环境，选择最适合的安装方式。

2.2.1 桌面安装

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。安装完成效果图如下。

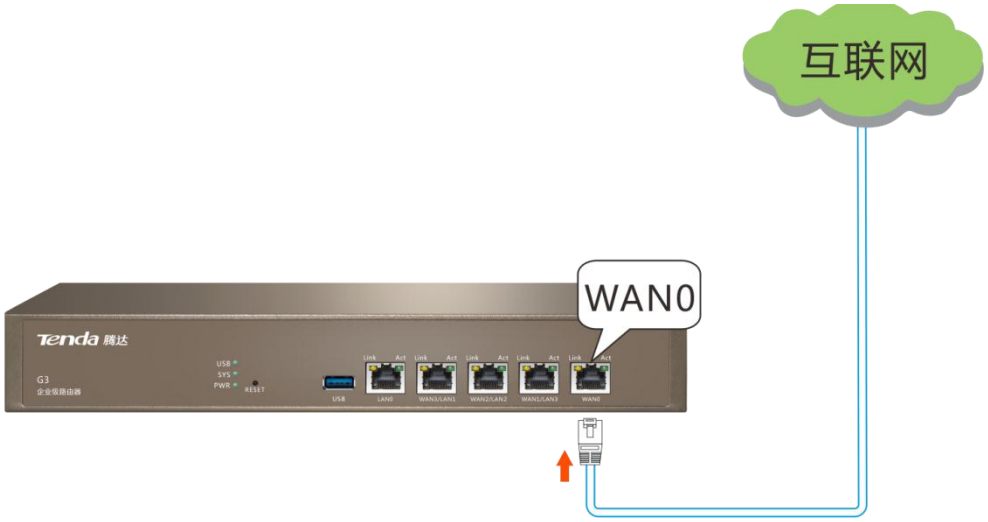
2.2.2 机架安装

1. 确保机架平稳且已接地。
2. 使用包装盒内提供的螺钉将两个 L 型支架分别固定在路由器两侧。

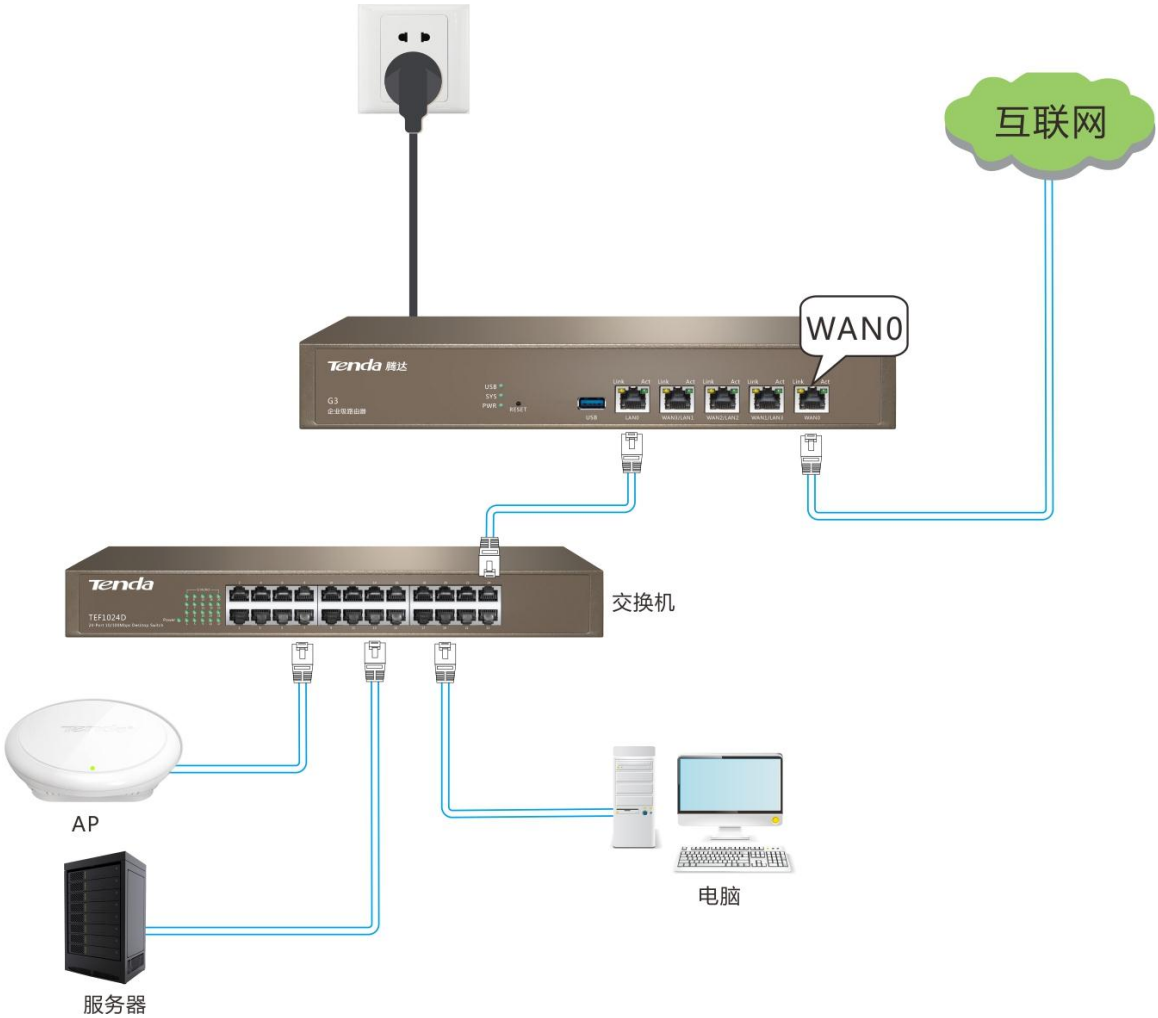
3. 使用螺钉（用户自备）将路由器固定在机架上。

2.3 连接路由器

1. 将外网线接在路由器的 WAN 口。



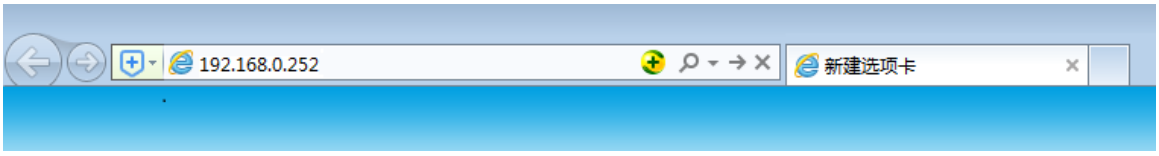
2. 用网线连接路由器和其它网络设备（服务器、电脑等）。检查无误后，使用产品包装盒内的电源适配器连接路由器和电源插座，按下电源开关给路由器上电。



3 设置上网

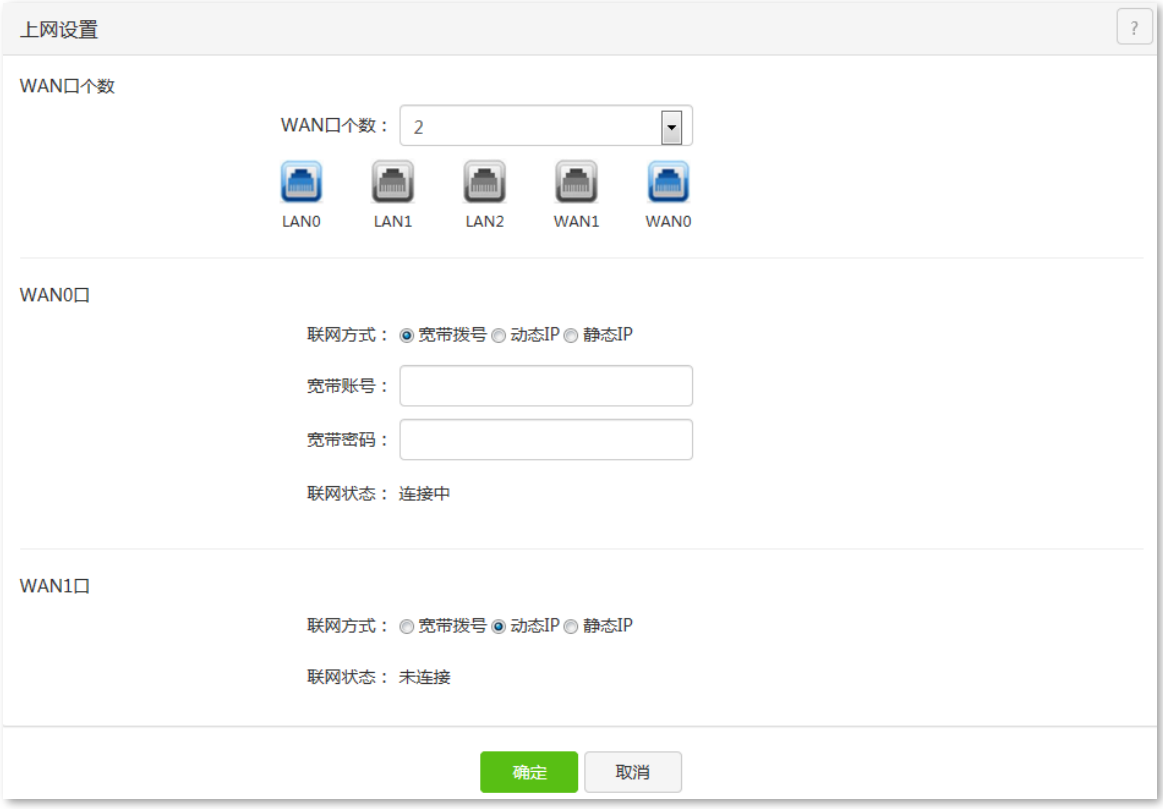
步骤 1 登录路由器管理页面。

1. 在已连接到路由器的电脑上打开浏览器，在地址栏输入 **192.168.0.252**，回车。



2. 在出现的页面设置登录密码，如“admin”，点击 确定 。

成功进入路由器管理页面。



提示

若不能登录路由器的管理页面，请参考**常见问题解答**问题 1。

步骤 2 **设置上网参数。**

请根据实际情况在情景一、情景二、情景三中选择一种进行设置。设置完成后，即可尝试上网。

点击『网络设置』，进入上网设置页面。

提示

- 本路由器默认提供 2 个 WAN 口，下文以 WAN0 设置为例，WAN1 口的设置与 WAN0 一致。
- 路由器 WAN0 默认的联网方式为宽带拨号，WAN1 默认的联网方式为动态 IP。
- 上网设置参数均由宽带运营商提供，如不清楚，请咨询宽带运营商。
- 设置过程中如果有弹出提示框，请根据提示框的内容采取相应措施。

情景一：网络服务提供商提供了宽带账号和密码，联网方式为宽带拨号。

设置步骤：

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. 点击页面底端的 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。

情景二：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，上网方式为动态 IP。

设置步骤：

1. 点击『网络设置』。
2. 联网方式：点击选择“动态 IP”。
3. 点击页面底端的 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。

情景三：网络服务提供商提供固定 IP 地址信息，上网方式为静态 IP。

设置步骤：

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. 点击页面底端的 确定 。

—完成

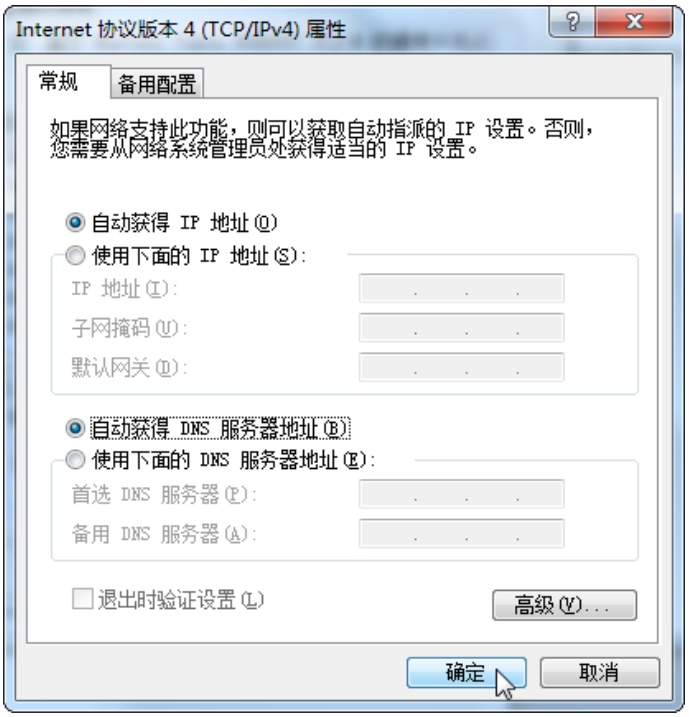
稍等片刻，当联网状态显示“已连接”时，可以尝试上网了。

4 页面简介

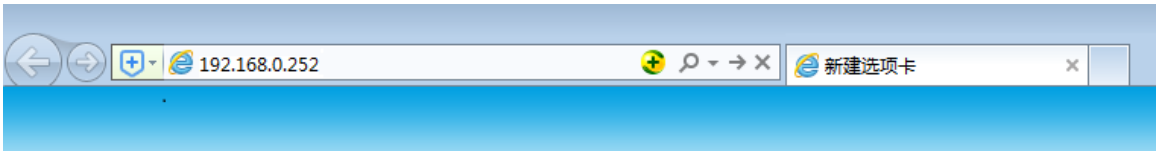
4.1 登录路由器管理页面

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。



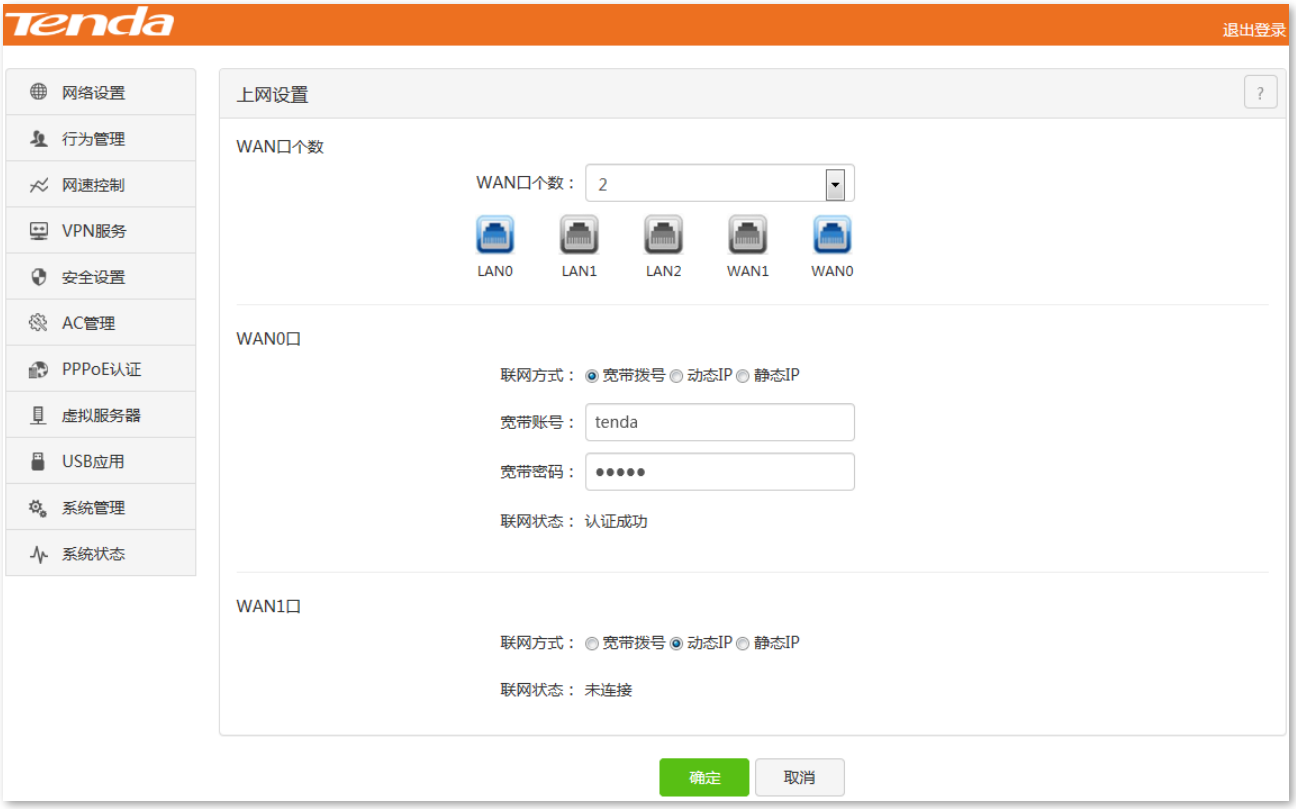
2. 已连接到路由器的电脑上打开浏览器，在地址栏输入 **192.168.0.252**，回车。



3. 输入登录密码，点击 登录 。

—完成

成功登录路由器管理页面。

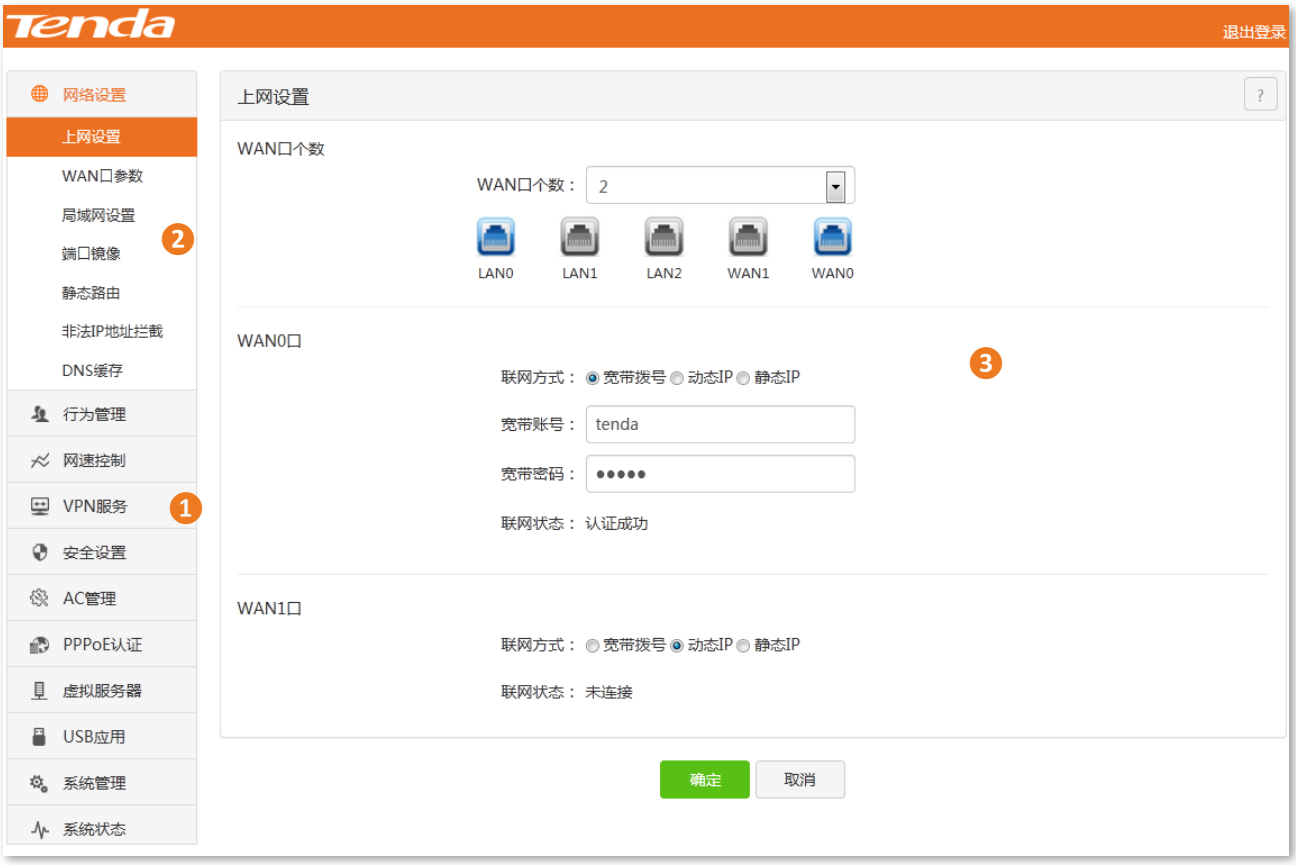


4.2 退出路由器管理页面

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

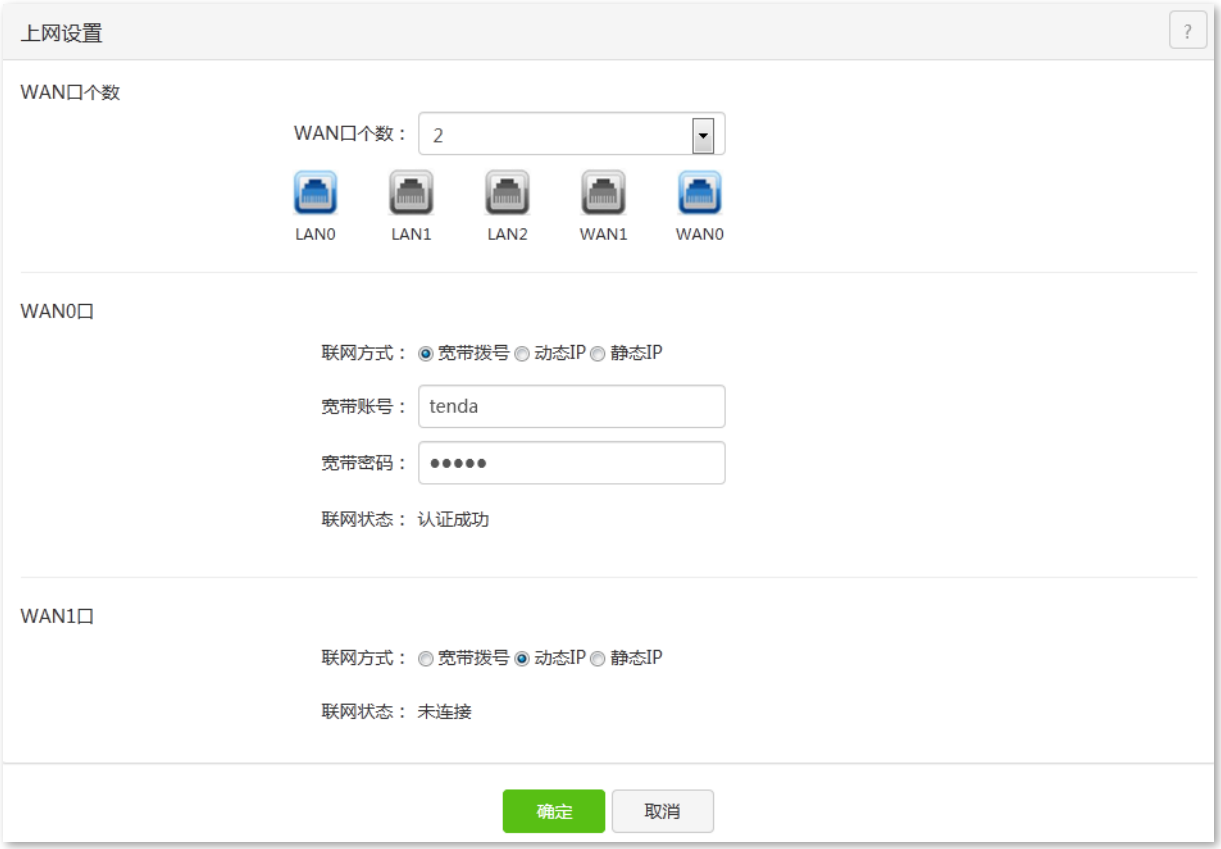
网络设置章节包括：

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。

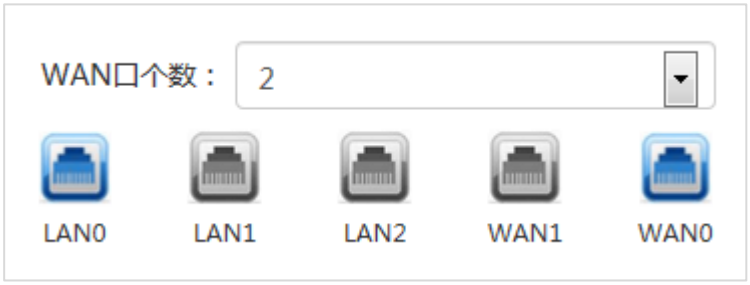
5.1 上网设置

在“上网设置”页面，您可以修改 WAN 口个数，设置上网参数。设置上网详细步骤请参考 3 设置上网。

点击『网络设置』进入设置页面。



参数说明

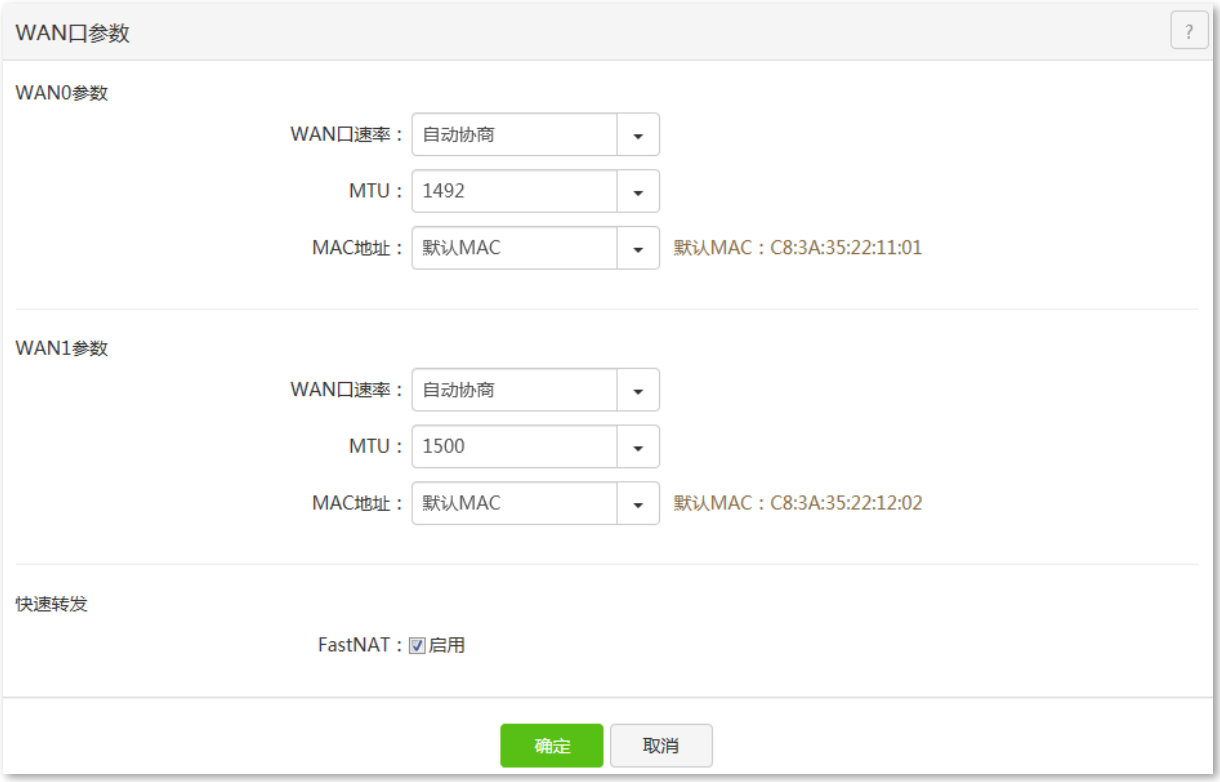
参数	说明
WAN 口个数	设置 WAN 口个数、查看 RJ45 口状态(连接状态、充当角色是 WAN 或 LAN)。默认启用 1 个 WAN 口。 修改 WAN 口个数后，RJ45 口状态图也会改动，如下：   表示接口连接正常。  表示接口未连接设备或连接异常。
联网方式	路由器的联网方式，说明如下： • 宽带拨号：网络服务提供商提供了宽带账号和密码。 • 动态 IP：网络服务提供商没有提供宽带账号和密码，也没有提供 IP 地址信息。 • 静态 IP：网络服务提供商提供固定 IP 地址信息。
宽带账号、宽带密码	联网方式为宽带拨号时有效，可以在办理宽带的业务单据上查到，如果没有，请咨询您的网络服务提供商。
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。

5.2 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。
快速转发	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. 点击页面底端的 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。

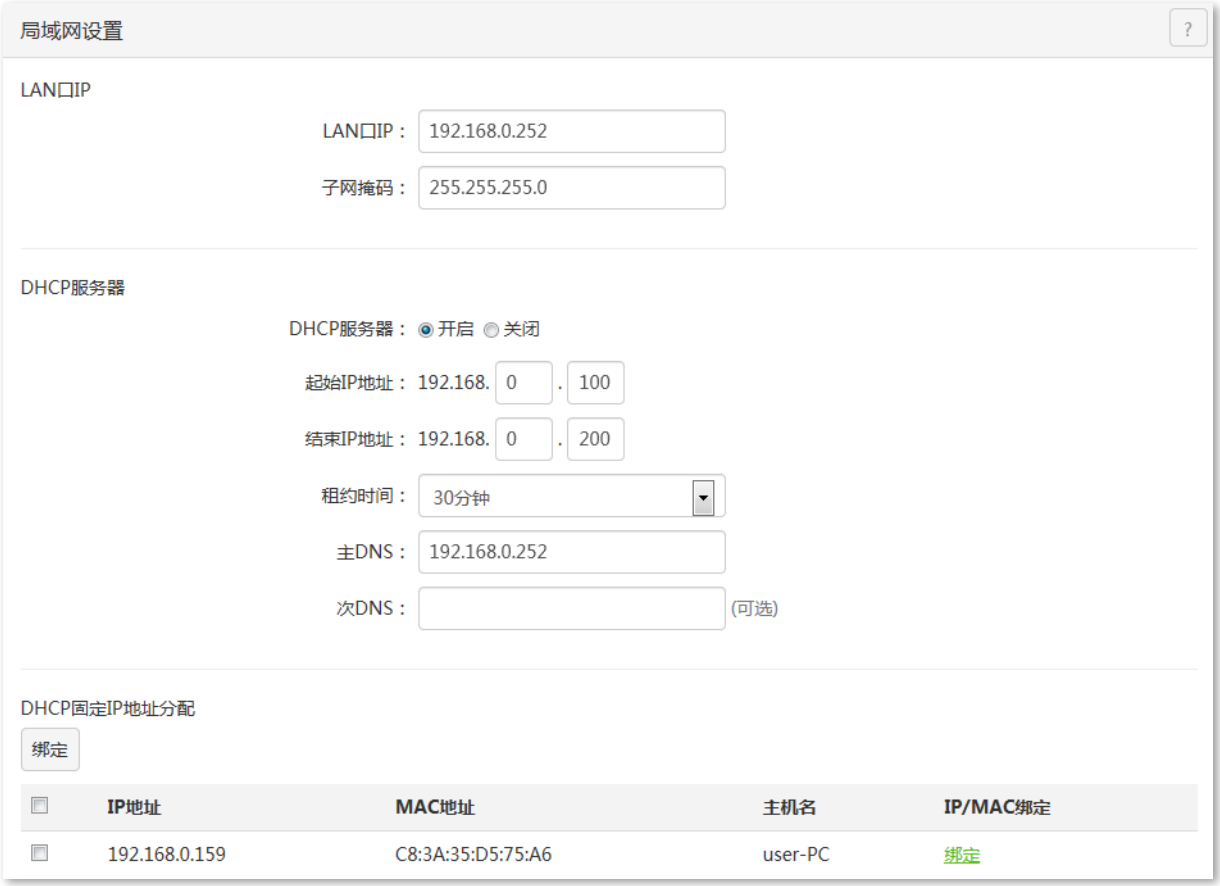
5.3 局域网设置

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 192.168.0.252，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 192.168.0.252）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

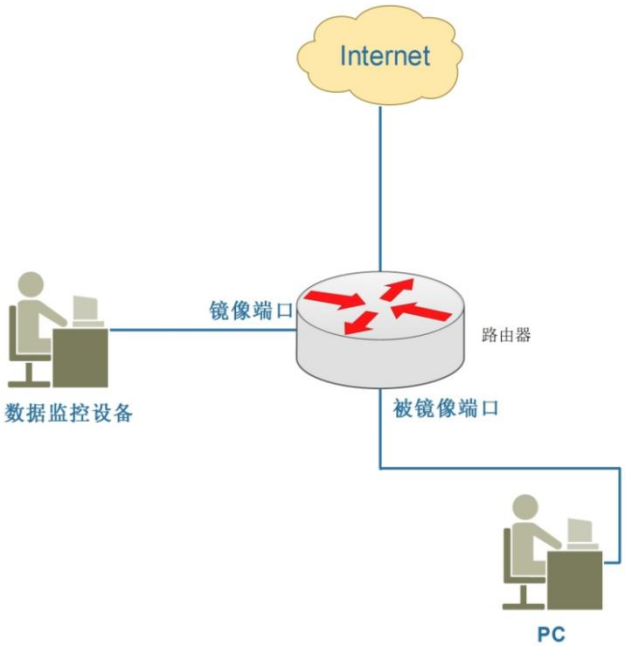
参数	说明
+新增分配	点击此按钮，手动为客户端绑定固定的 IP 地址。首先要知道客户端的 MAC 地址信息。
删除	删除已选中的 IP 地址、MAC 地址绑定规则。
MAC 地址	客户端的 MAC 地址。
IP 地址	对应 MAC 地址的客户端绑定的 IP 地址。
备注	客户端 IP 地址、MAC 地址绑定规则的备注信息，动态绑定或手动添加时没有设置，均不显示。
状态	IP 地址、MAC 地址绑定规则的状态，包括已启用和未启用。
操作	可对 IP 地址、MAC 地址绑定规则进行如下操作： • 点击可以禁用该规则。 • 点击可以启用该规则。 • 点击可以编辑规则信息，包括修改 MAC 地址、IP 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 LAN0 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 LAN0，且不可更改。
被镜像端口	被监控端口，启用端口镜像功能后，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

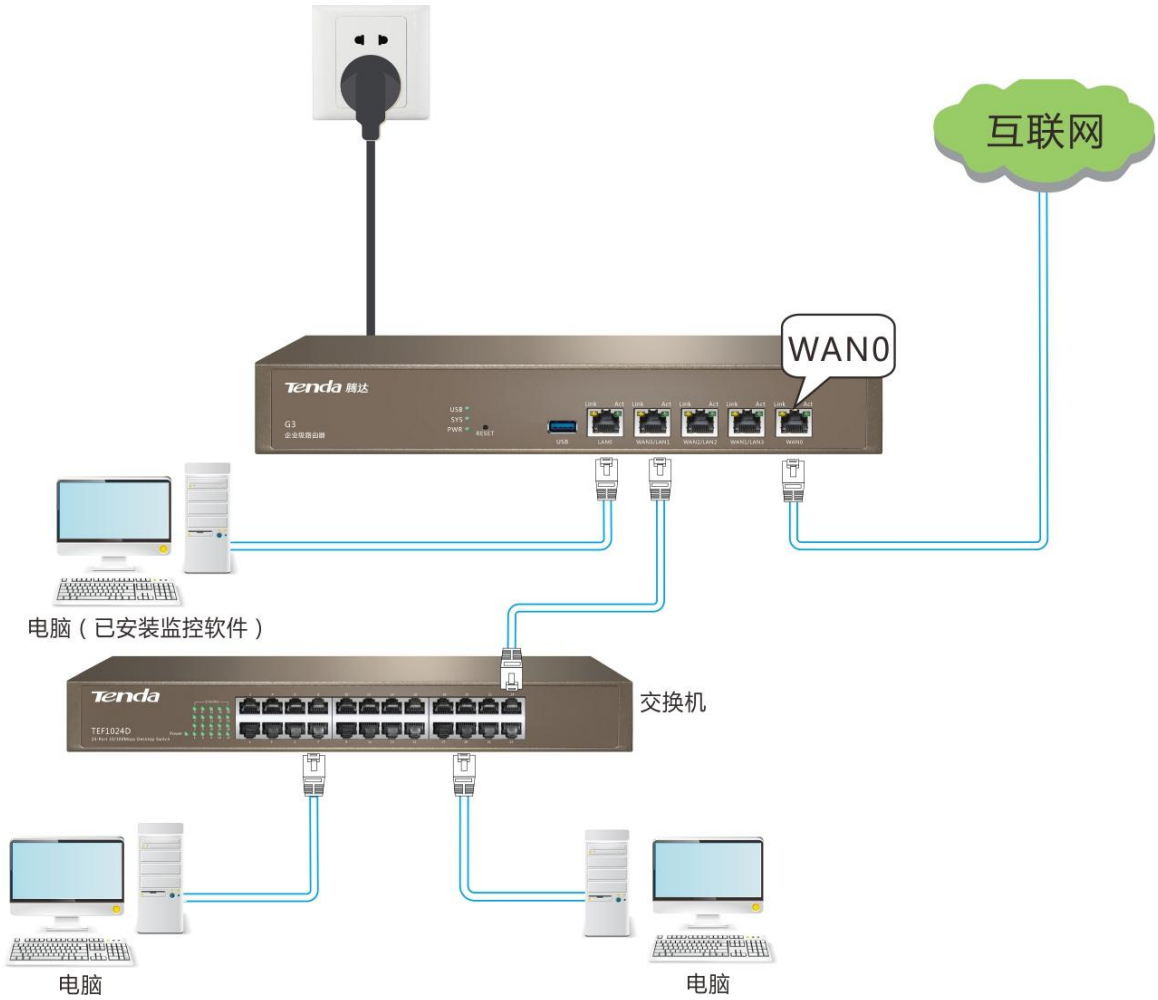
组网需求

某企业使用 G3 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 LAN0 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 LAN1、LAN2、WAN1、WAN0。
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 LAN0 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。
端口号	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G3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WAN0口接入互联网，通过WAN1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

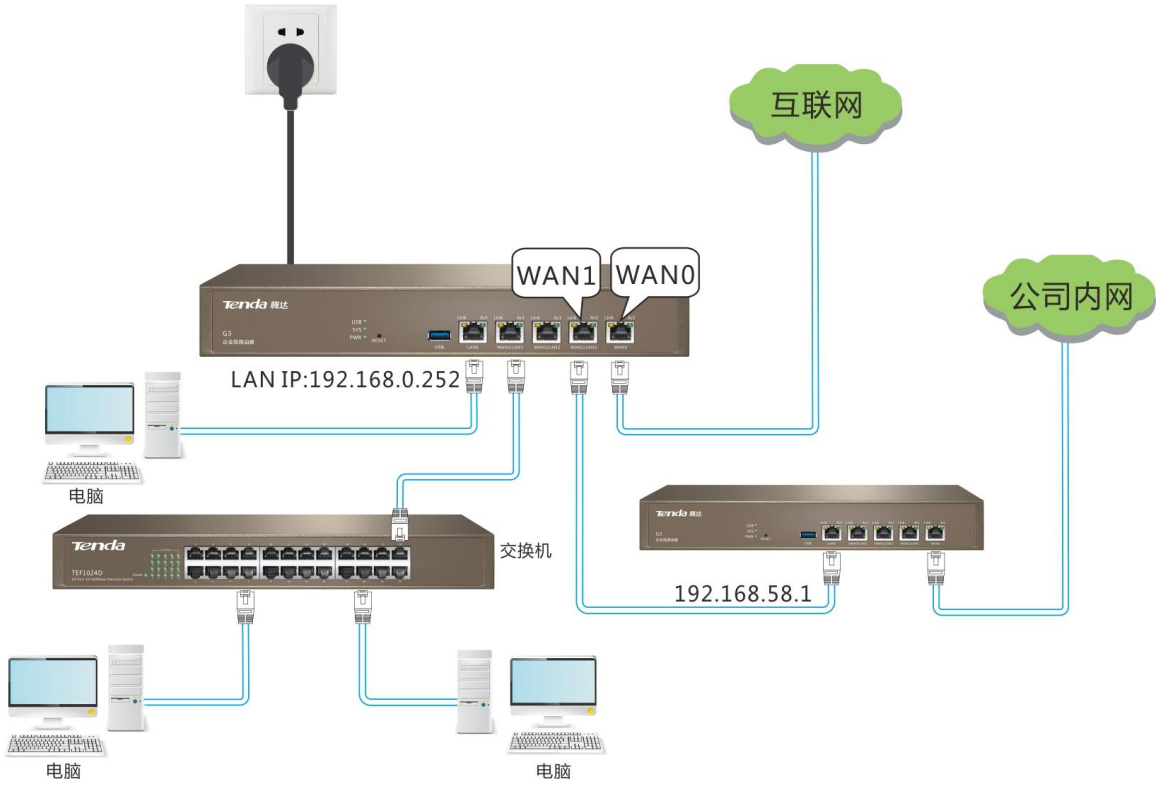
公司分配的访问互联网信息：

- 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 WAN0 口，内网接在 WAN1 口）。设置 WAN 口相关参数。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：输入路由器 WAN1 口的网关地址，本例为“192.168.58.1”。

(4) 端口号：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，本功能默认启用，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 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。

6.1 IP 组和时间组

6.1.1 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。

6.1.2 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。

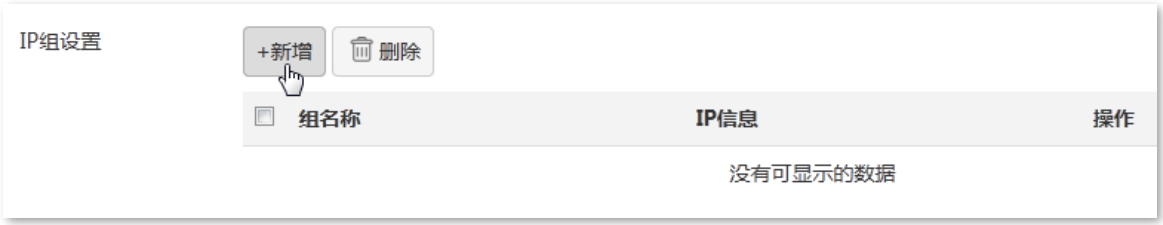
(2) 时间、星期：设置本时间组的具体时间。

(3) 点击 确定 。

—完成

6.1.3 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

6.2 IP 地址过滤

6.2.1 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 地址过滤默认禁用，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。

6.2.2 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

6.2.3 IP 地址过滤示例

组网需求

某企业使用 G3 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 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 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。

6.3 MAC 地址过滤

6.3.1 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。

6.3.2 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

6.3.3 MAC 地址过滤示例

组网需求

某企业使用 G3 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。

6.4 端口过滤

6.4.1 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。

6.4.2 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

6.4.3 端口过滤示例

组网需求

某企业使用 G3 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。

6.5 网络应用过滤

6.5.1 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。

6.5.2 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

6.5.3 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

6.5.4 网络应用过滤示例

组网需求

某企业使用 G3 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。

6.6 网址分类过滤

6.6.1 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。

6.6.2 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

6.6.3 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

6.6.4 网址分类过滤示例

组网需求

某企业使用 G3 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 。

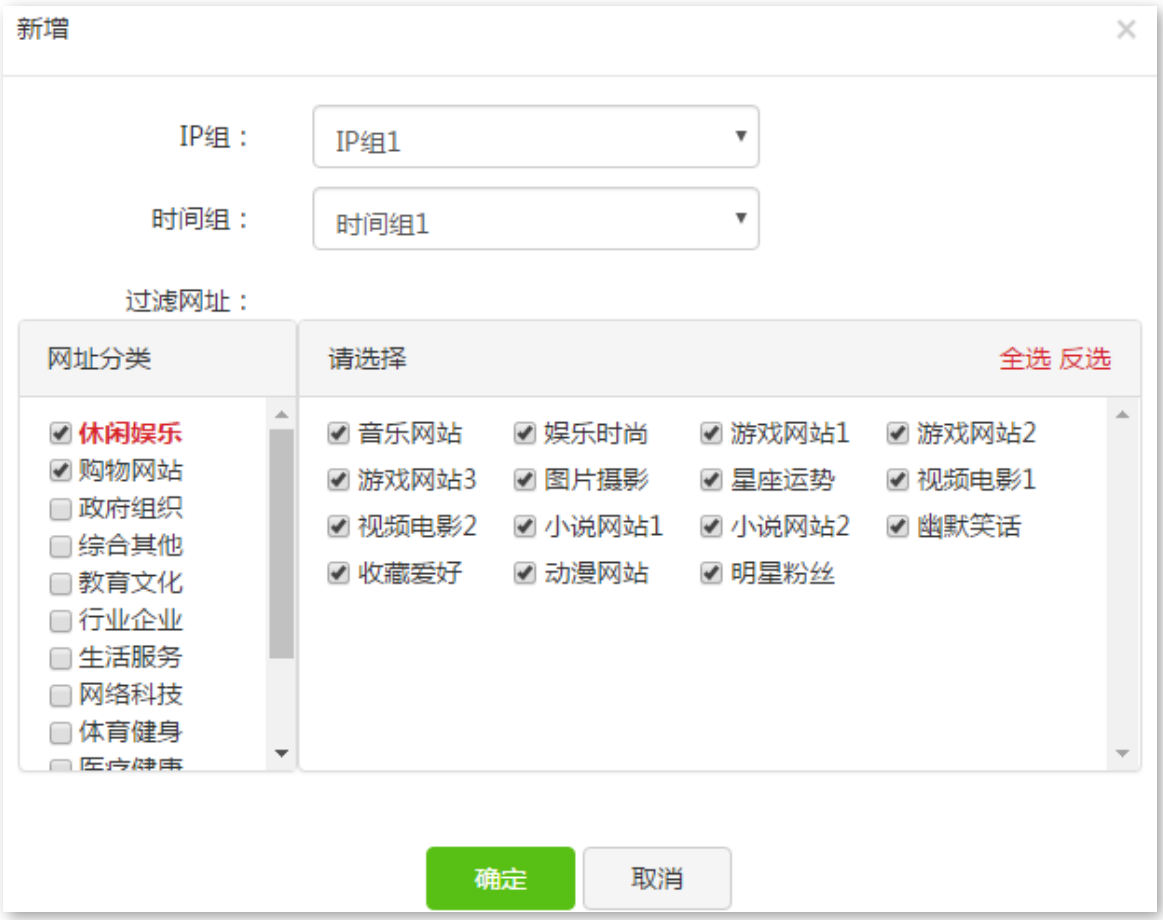
(1) IP 组：点击下拉框，选择规则运用的 IP 组，如“IP 组 1”。

(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。

6.7 多 WAN 策略

6.7.1 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。

6.7.2 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。

6.7.3 用户自定义策略示例

组网需求

某企业使用 G3 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“WAN0”。
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 WAN0 口。

7 网速控制

7.1 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。

7.2 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。

7.3 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。
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。

参数	说明
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。

7.4 单独限速示例

组网需求

某企业使用 G3 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。

8 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。

8.1 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。

8.2 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。

8.3 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。

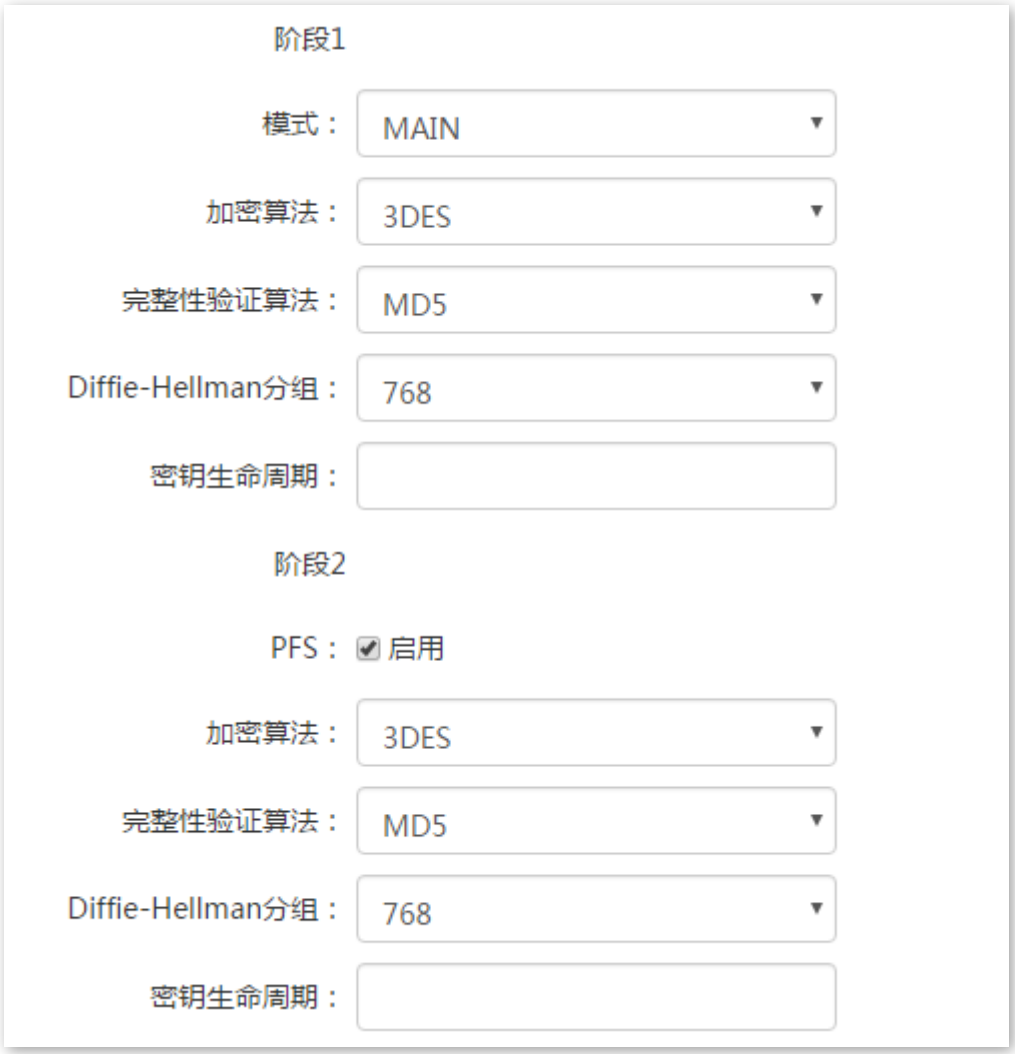
  阶段 1，通信双方将协商交换验证算法、加密算法等安全提议，并建立一个 ISAKMP SA，用于在阶段 2 中安全交换更多信息。

  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。

8.4 PPTP/L2TP 配置示例

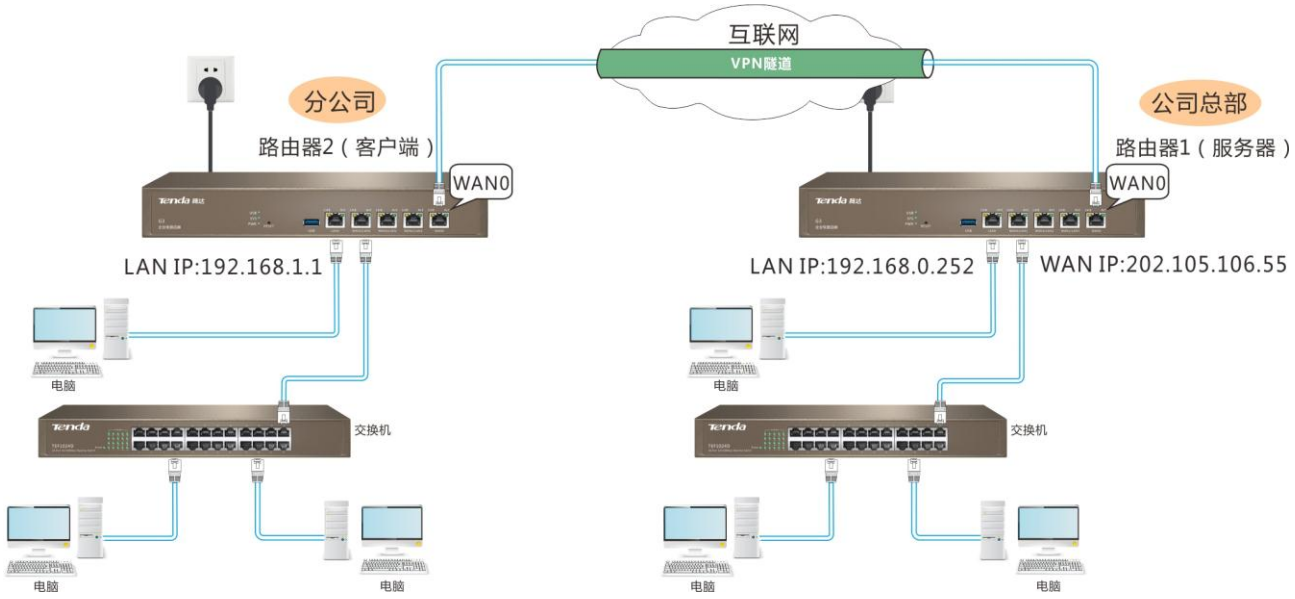
组网需求

某企业总部和分公司使用 G3 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“WAN0”。
   (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”。

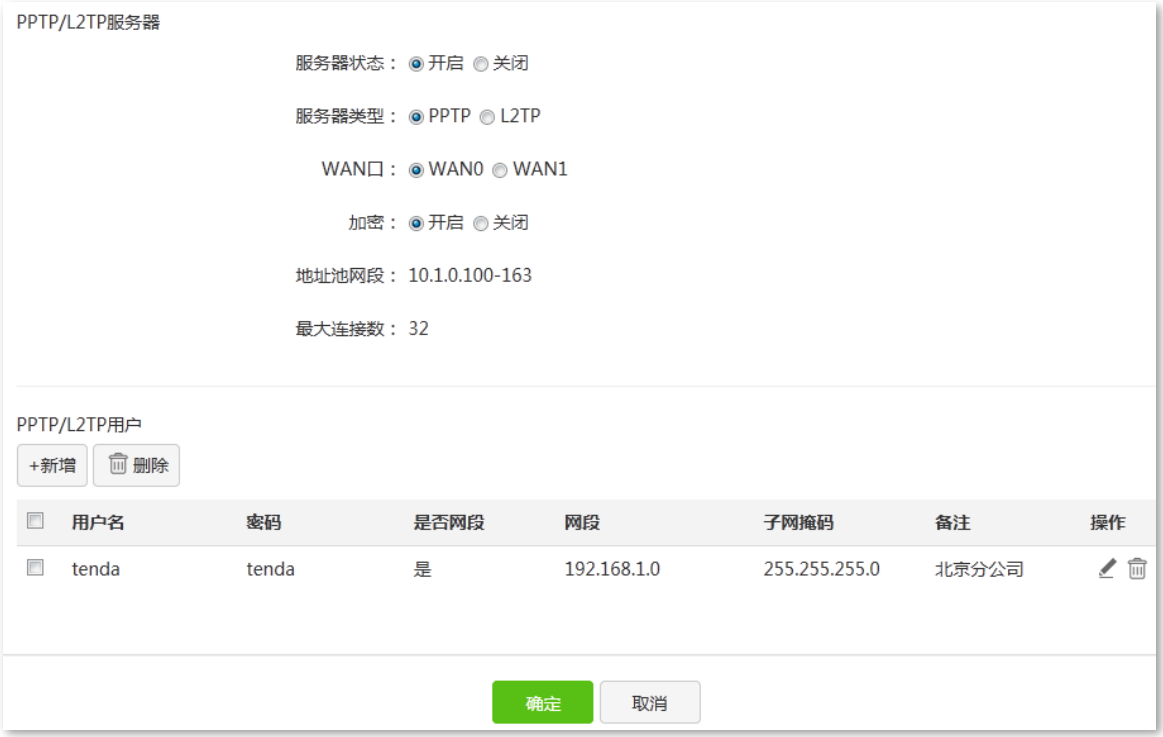
(4) 网段、子网掩码：VPN 客户端为网段时，输入客户端局域网的网段及子网掩码，本例为“192.168.1.0、255.255.255.0”。

(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
服务器状态：
开启
关闭
服务器类型：
PPTP
L2TP
WAN口：
WAN0
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“WAN0”。
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。

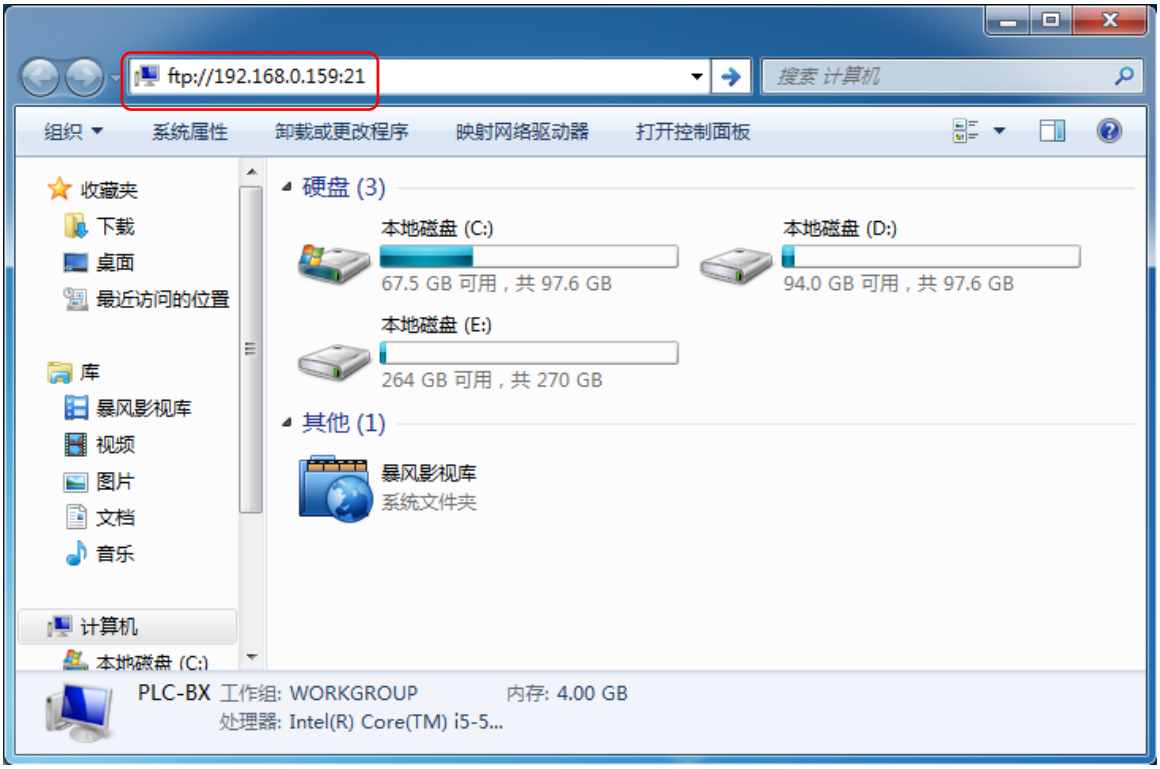
VPN 连接成功后，分公司员工可以访问总部的资源了。下文以分公司访问总部 FTP 服务器内容为例。

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

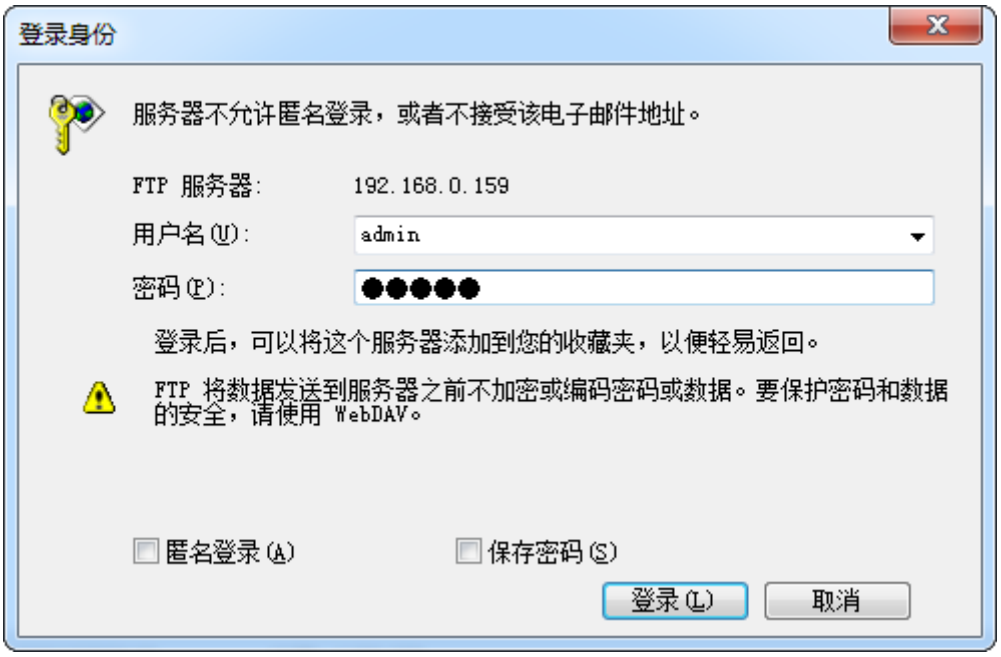
当分公司员工访问总部项目资料时，步骤如下：

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”。

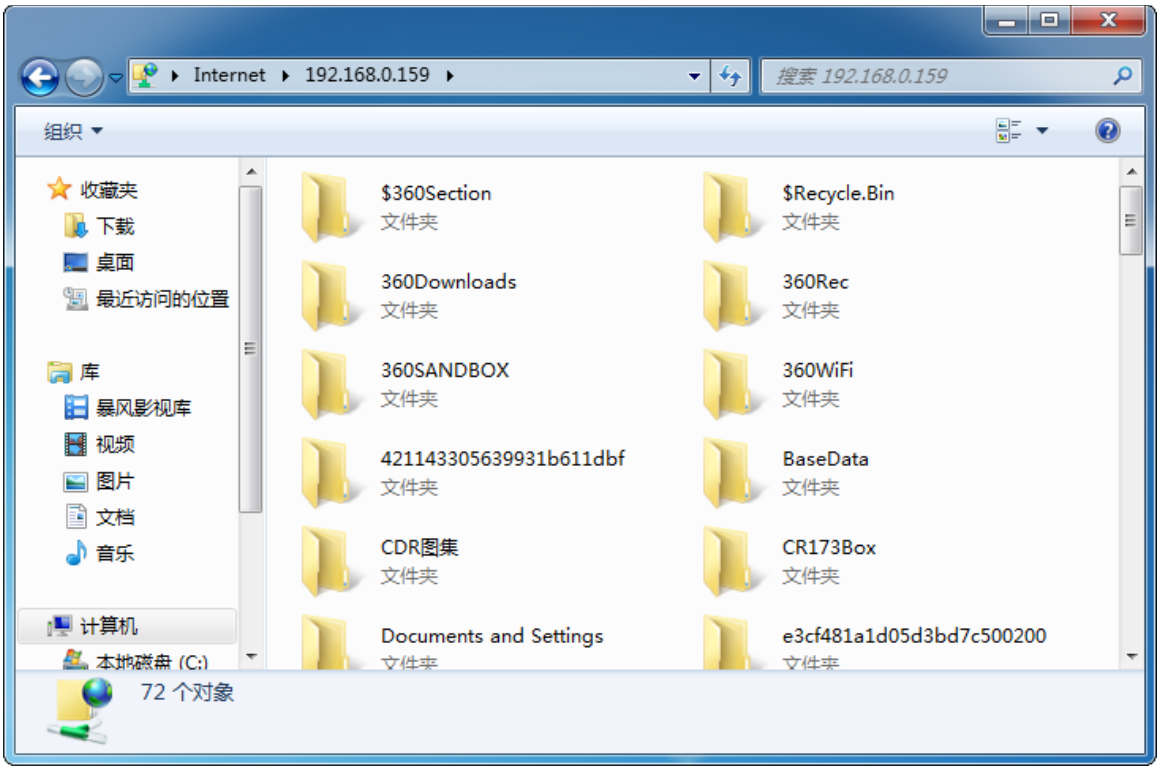


2. 在弹出的窗口输入登录用户名和密码，本例均为 admin。

3. 点击 登录 。



访问成功。



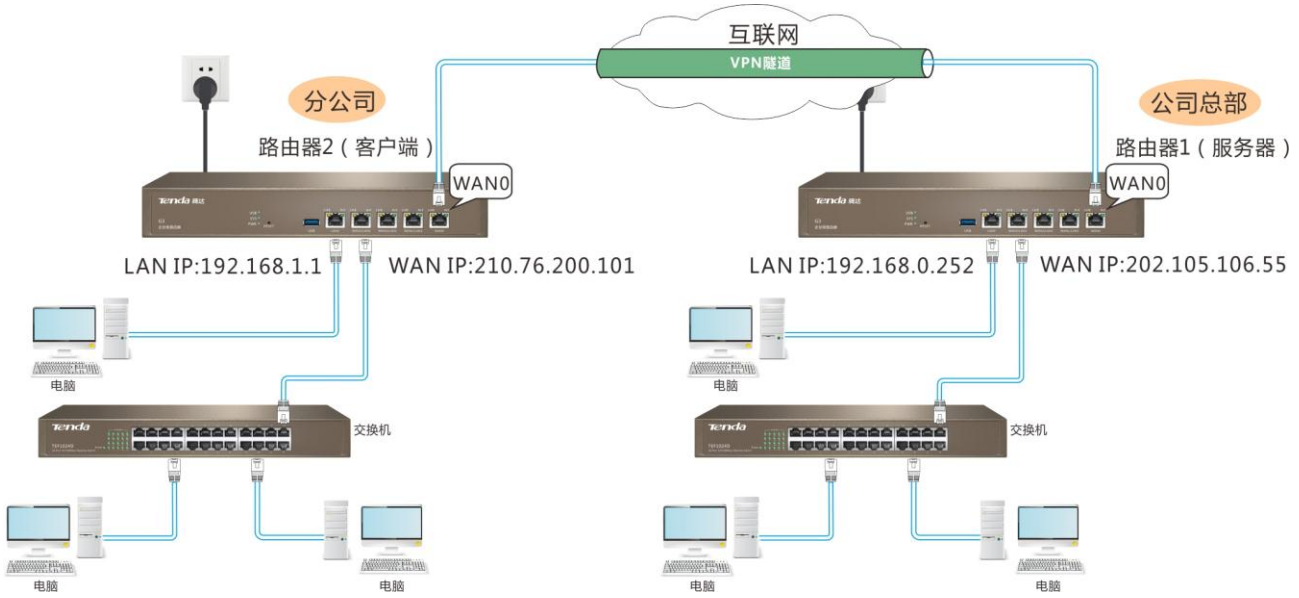
8.5 IPSec 配置示例

组网需求

某企业总部和分公司使用 G3 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“WAN0”。

(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“WAN0”。

(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。

9 安全设置

安全设置章节包括：

IP-MAC 访问控制、攻击防御。

9.1 IP-MAC 访问控制

9.1.1 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”。

9.1.2 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

9.1.3 IP-MAC 绑定示例

组网需求

某企业使用 G3 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：

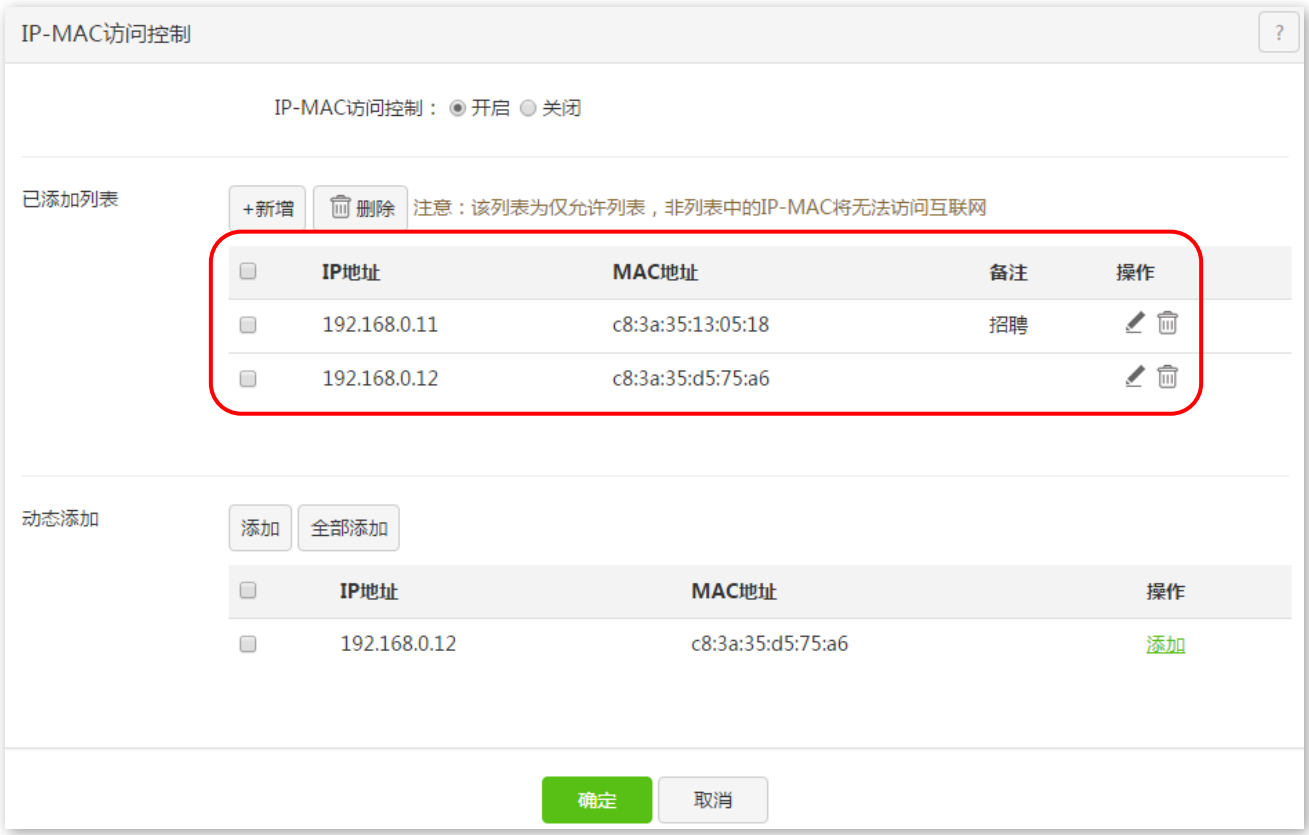
(1) 点击 +新增 。

(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。

9.2 攻击防御

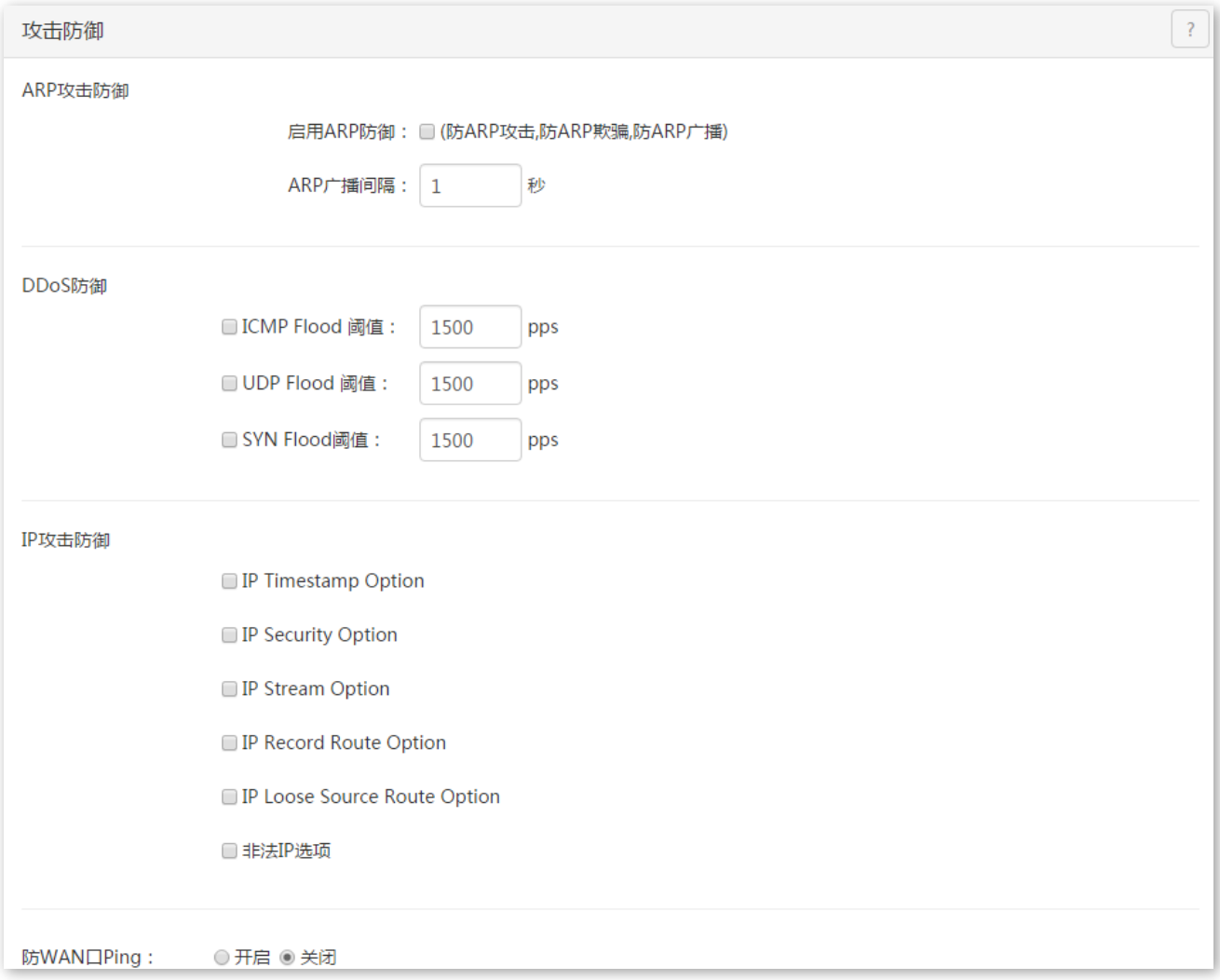
在“攻击防御”页面，您可以设置路由器攻击防御功能。

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。

10 AC 管理

AC 管理章节包括：

无线配置、高级配置、AP 管理、用户状态。

10.1 无线配置

10.1.1 概述

在无线配置页面，您可以添加无线策略，并下发到网络中的 AP。点击『AC 管理』，进入设置页面。

AC 管理功能默认关闭。点击“开启”即可启用 AC 管理功能，如下所示：

参数说明：

参数	说明
状态	无线策略的状态。默认启用一个无线策略，可根据需要启用其他无线策略，并设置相关参数。点击**确定**后，已启用的策略将会下发到网络中的 AP。
SSID	无线策略的 SSID，可根据需要设置。
隐藏 SSID	是否隐藏该策略的 SSID。启用后，不广播该 SSID，该 SSID 不会显示在客户端的可用网络列表中。
频段	无线策略工作的频段，前 4 条策略支持 2.4G、5G 和 2.4G&5G，默认为 2.4G&5G。后 4 条策略仅支持 2.4G。
最大用户数	该 SSID 最多允许接入的无线客户端个数。
VLAN ID	无线网络所属的 VLAN，默认为 1000。需要在『AC 管理』→『高级配置』的“全局配置”模块中启用 VLAN，VLAN 配置才生效。
认证类型	该无线策略中 SSID 的无线网络认证方式。 • 不加密：不加密无线网络，允许任意客户端接入。为保障网络安全，不建议选择此项。 • WPA-PSK：无线网络使用 WPA-PSK 认证方式。 • WPA2-PSK：无线网络使用 WPA2-PSK 认证方式。
密码	无线密码，作为无线客户端访问无线网络时所需要输入的无线密码。
高级	客户端隔离：开启/关闭 SSID 的“客户端隔离”功能： • 开启：连接到本 SSID 的无线设备之间不能相互通信。 • 关闭：连接到本 SSID 的无线设备之间能相互通信。

10.1.2 下发无线策略

1. 状态：点击下拉菜单，选择“开启”。
2. SSID：设置 SSID 内容。
3. 频段 :点击下拉菜单 ,选择下发给 AP 的频段 ,若只选择单频下发 ,则另一频段的无线将会被禁用。
4. 认证类型：选择无线加密方式，如“WPA-PSK”。
5. 密码：设置无线密码
6. 点击 确定 ，已启用的策略将会下发到 AP 中。如果需要设置客户端隔离，可点击 进行设置。

—完成

10.2 高级配置

10.2.1 概述

在高级配置页面，您可以设置射频策略信息、VLAN 信息等，并下发到网络中的 AP。

点击『AC 管理』→『高级配置』进入设置页面。

参数说明：

参数		说明
射频配置	频段	选择要设置的频段，2.4G 频段或 5G 频段。
	国家	选择当前所在的国家。
	无线开关	关闭/开启相应频段的无线功能。
	网络模式	选择无线网络模式。2.4G 包括 11b、11g、11b/g、11b/g/n ；5G 包括 11a、11ac、11a/n。 • 11b：仅允许 802.11b 客户端连接到 AP。 • 11g：仅允许 802.11g 客户端连接到 AP。 • 11b/g：允许 802.11b、802.11g 客户端连接到 AP。 • 11b/g/n：工作在 2.4G 频段的 802.11b、802.11g、802.11n 客户端均可连接到 AP。 • 11a：仅允许 802.11a 客户端连接到 AP。 • 11ac：允许 802.11ac 客户端连接到 AP。 • 11a/n：工作在 5G 频段的 802.11a 和 802.11n 客户端均可连接至 AP。
	带宽	选择无线带宽。 • 20：AP 使用 20MHz 的信道带宽。 • 40：AP 使用 40MHz 的信道带宽。 • 80：仅适用 5G，AP 使用 80MHz 的信道带宽。 • 自动：仅适用 2.4G，AP 根据周围环境，自动调整信道带宽为 20MHz 或 40MHz。
	信道	选择无线工作信道，可选择范围由当前选择的“国家”和“频段”决定。
	功率	射频策略的无线功率，当 AP 支持的发射功率小于下发的发射功率时，以 AP 的最大发射功率为准。
	SSID 隔离	开启/关闭 SSID 隔离功能。开启后，连接到 AP 不同 SSID 的无线客户端之间不能互相通信。
	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 AP 的整体效率，有效保障了带机量和吞吐量。
	更多配置...	射频配置高级参数，详细参数说明可参考射频配置高级参数说明。

参数		说明
全局配置	VLAN	开启/关闭 AP 的 VLAN 功能，默认为关闭。
	管理 VLAN ID	AP 的管理 VLAN ID，默认为 1。更改管理 VLAN，并成功下发到 AP 后，客户端（如管理电脑）需要重新连接到新的管理 VLAN，才能进入 AP 的 Web 管理页面。
	LED 状态	AP 的 LED 灯的开启/关闭状态。
	端口驱动能力	AP LAN 口驱动能力，默认为“标准”模式，支持最长 100 米网线（超 5 类或 6 类）供电。 如果 AP 与 LAN 口对端设备链路协商失败，可尝试更改端口驱动能力为“增强”模式，支持最长 150-200 米网线（超 5 类或 6 类）供电。注意，此模式下会影响端口的协商速率，网口吞吐量性能可能下降。
	更多配置...	全局配置高级参数，详细参数说明可参考全局配置高级参数说明。

射频配置高级参数：

在射频配置模块点击更多配置...，进入设置页面。

射频配置高级参数说明：

参数	说明
RSSI 阀值	AP 可接受的无线客户端信号强度，信号强度低于此值的客户端将无法接入该 AP。正确设置 RSSI 可以确保客户端主动连接到信号比较强的 AP。
穿墙能力	仅 2.4G 有效，通过调节 AP 的发射功率，满足用户需求。 • 强覆盖：适用于无线信号穿墙的场景，常用于 AP 部署密度较低的情况。 • 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、AP 部署密度较高的情况，此模式不需要考虑 AP 覆盖范围问题。
部署模式	仅 2.4G 有效，通过调节 AP 可接受的客户端信号强度范围，满足用户需求。 • 强覆盖 :适用于用户分散、干扰较少的环境。常用于 AP 部署密度较低的情况，需要确保确保客户端尽可能地成功接入 AP。 • 高密度：适用于环境空旷、用户密度大、干扰多的场景。常用于 AP 部署密度较高的情况，需要保证客户端能尽可能地连接到信号更好的 AP。
WMM	即“无线多媒体”。在 WiFi 网络中，根据增强型分布式信道存取(EDCA)方法，提供区分优先级的媒体存取。开启“WMM”功能，它定义 4 种优先级，即话音、视频、尽力而为和低优先级数据，以管理不同应用的业务量。默认开启。
APSD	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 AP 的电能消耗。默认关闭。
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。

全局配置高级参数：

在全局配置模块点击更多配置...，进入设置页面。

全局配置参数说明：

参数	说明
PVID	AP Trunk 口的 VLAN ID，默认为 1。
Trunk 口	设置 AP 的 Trunk 口。
自动维护设置	开启/关闭 AP 自动维护功能。
维护类型	设置 AP 的维护类型。 • 定时维护：AP 在选定的日期的时间点重启。 • 循环维护：AP 在设定的时间间隔后重启。
维护时间设置	“定时维护”有效，设置 AP 重启的时间点。
每天、星期一、星期二、星期三、星期四、星期五、星期六、星期日	“定时维护”有效，设定 AP 进行定时重启的日期。
间隔时间	“循环维护”有效，设置 AP 的重启时间间隔。

10.2.2 下发射频策略、VLAN 策略

1. 频段：选择 2.4G 频段进行设置。
2. 信道：点击下拉菜单，选择 2.4G 工作信道。
3. 功率：设置无线发射功率。
4. 在频段选项选择“5G”，并进行相关设置。
5. VLAN：点击“开启”。
6. 点击 确定 ，策略将会下发到 AP 中。如果需要设置其他参数，可点击更多配置...进行设置。

—完成

10.3 AP 管理

10.3.1 概述

在“AP 管理”页面，您可以管理网络中的 AP。可以对 AP 进行重启、升级、复位等操作。点击『AC 管理』→『AP 管理』，进入设置页面。

参数说明：

参数	说明
导出	点击此按钮可以导出当前列表所有的 AP 信息。
重启	重新启动已选中的 AP。
升级	为选中的 AP 升级软件。
复位	把被选中的 AP 恢复出厂设置。
删除	把被选中的处于离线状态下的 AP 信息删除。
刷新	刷新当前 AP 列表。
AP 型号	AP 的型号。
备注	AP 的描述信息，点击可以修改信息。
IP/MAC 地址	AP 的 IP 地址和 MAC 地址。
频段	AP 的无线频段。
终端/限制数	• 终端：当前接入 AP SSID 的无线客户端数量。 • 限制数：能接入 AP 主 SSID 的无线客户端的最大数量。
功率	AP 的发射功率。
信道	AP 的无线信道。
状态	AP 当前与本路由器的连接状态，有“在线”和“离线”两种。路由器只能对处于“在线”的 AP 进行配置。
操作	点击 可修改 AP 的相关信息。

10.3.2 修改单个 AP 射频信息

1. 点击相应 AP 的图标。

2. 在出现的页面修改相应信息。

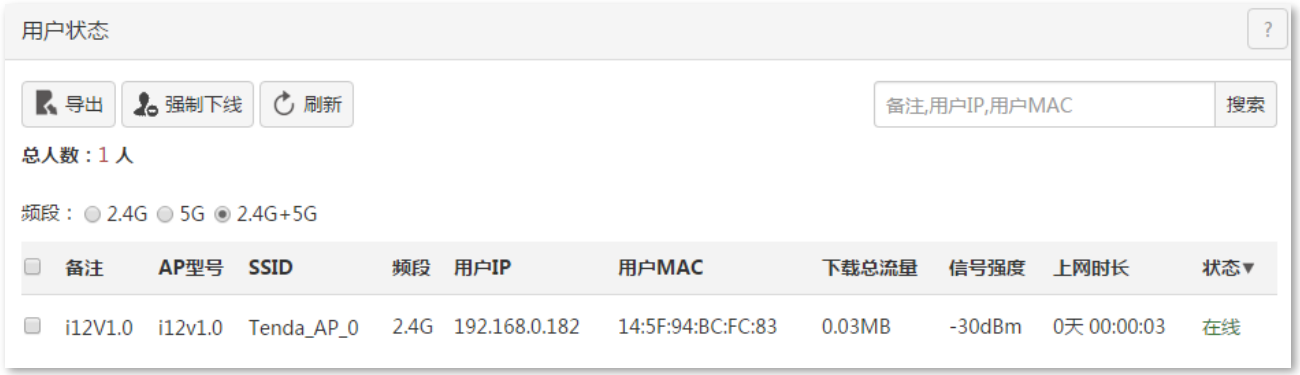
3. 点击 确定 ，修改成功。

—完成

10.4 用户状态

10.4.1 概述

在用户状态页面，您可以查看/导出连接 AP WiFi 的用户信息。点击『AC 管理』→『用户状态』进入页面。可以查看/导出连接到网络中的无线客户端的信息。



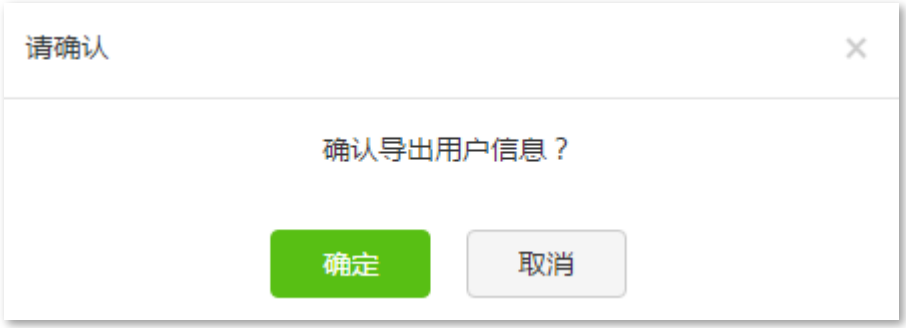
参数说明：

参数	说明
导出	点击此按钮可以导出当前列表所有的客户端信息。
强制下线	点击此按钮可以将选中的用户强制下线。
刷新	点击此按钮可以刷新当前客户端列表。
备注	AP 备注信息。
AP 型号	AP 型号。
SSID	客户端连接的 SSID 信息。
频段	SSID 工作的频段。
用户 IP	连接该 AP 无线信号的客户端获取到的 IP 地址。
用户 MAC	连接该 AP 无线信号的客户端的 MAC 地址。
下载总流量	客户端下载的总流量。
信号强度	接收的信号强度（RSSI），即 AP 接收到的用户终端的无线信号强度。
上网时长	客户端接入网络的时长。
状态	客户端当前接入 AP 的状态。

10.4.2 导出用户操作步骤

1. 点击 导出 。

2. 在弹出的对话框中，点击 确定 。



—完成

11 PPPoE 认证

PPPoE 认证章节包括：

基本设置、账号管理。

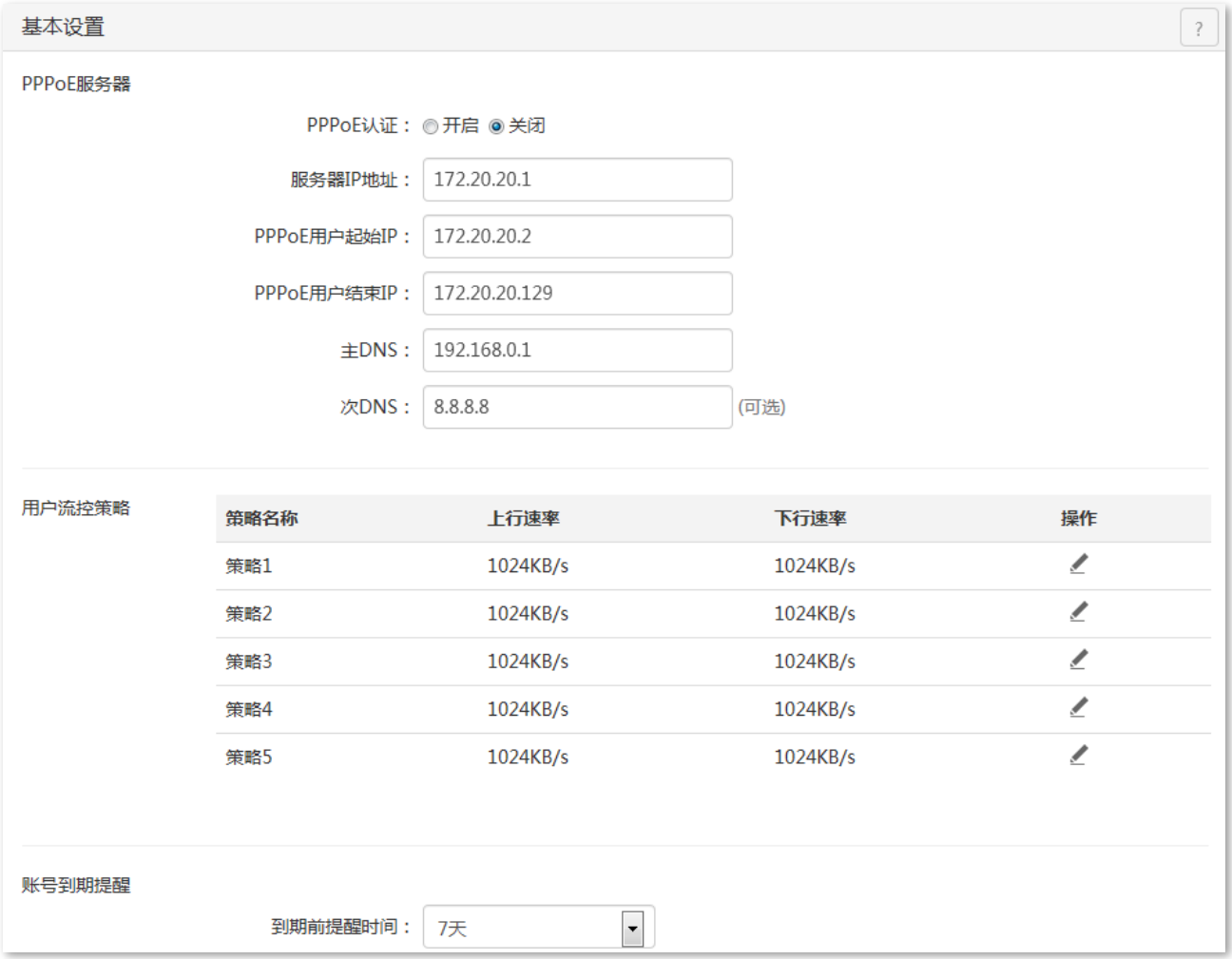
11.1 基本设置

11.1.1 概述

在“基本设置”页面，您可以设置 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。

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  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  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		点击此按钮可增加无需认证即可上网的客户端。
		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。

11.1.2 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

11.2 账号管理

11.2.1 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。

11.2.2 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

11.3 PPPoE 认证示例

组网需求

某小区使用 G3 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。

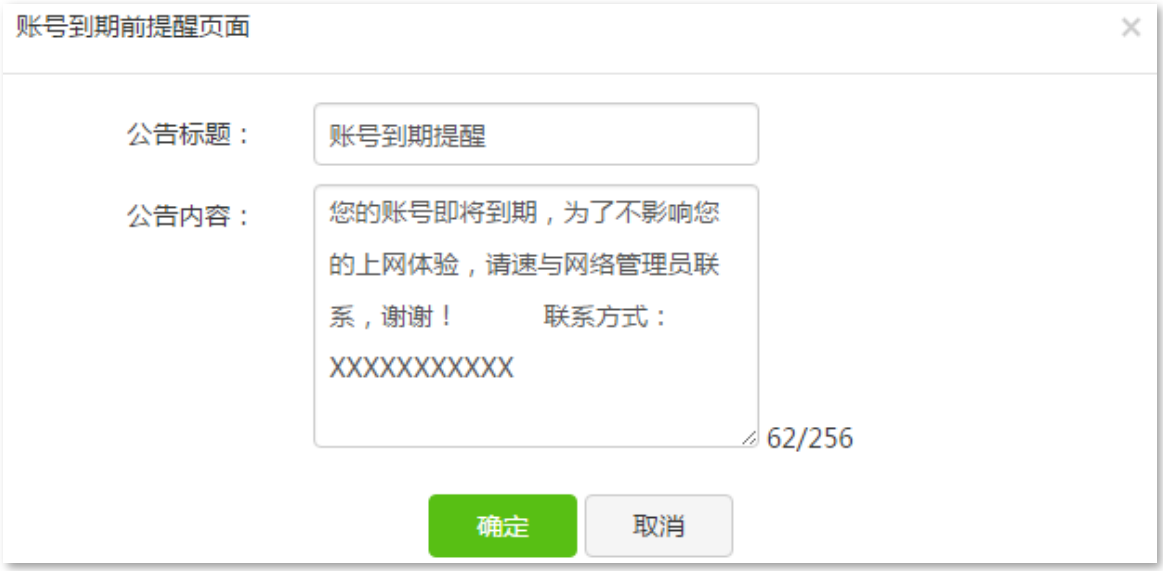
1. 进入『PPPoE 认证』→『基本设置』页面。
2. 在“PPPoE 认证”选项选择“开启”，点击页面底端的 确定 ，启用该功能。

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。

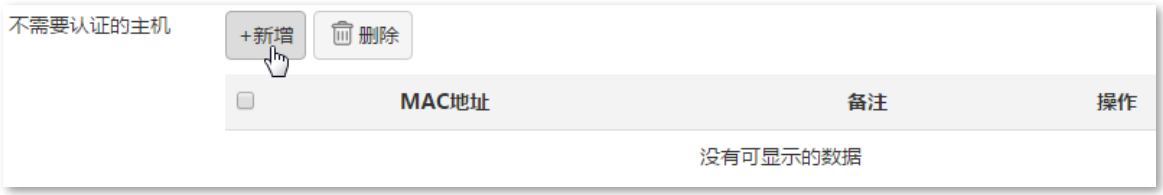
- 公告标题：修改账号到期提醒页面的标题内容。
- 公告内容：修改账号到期提醒页面的公告内容。
- 点击 确定 。



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

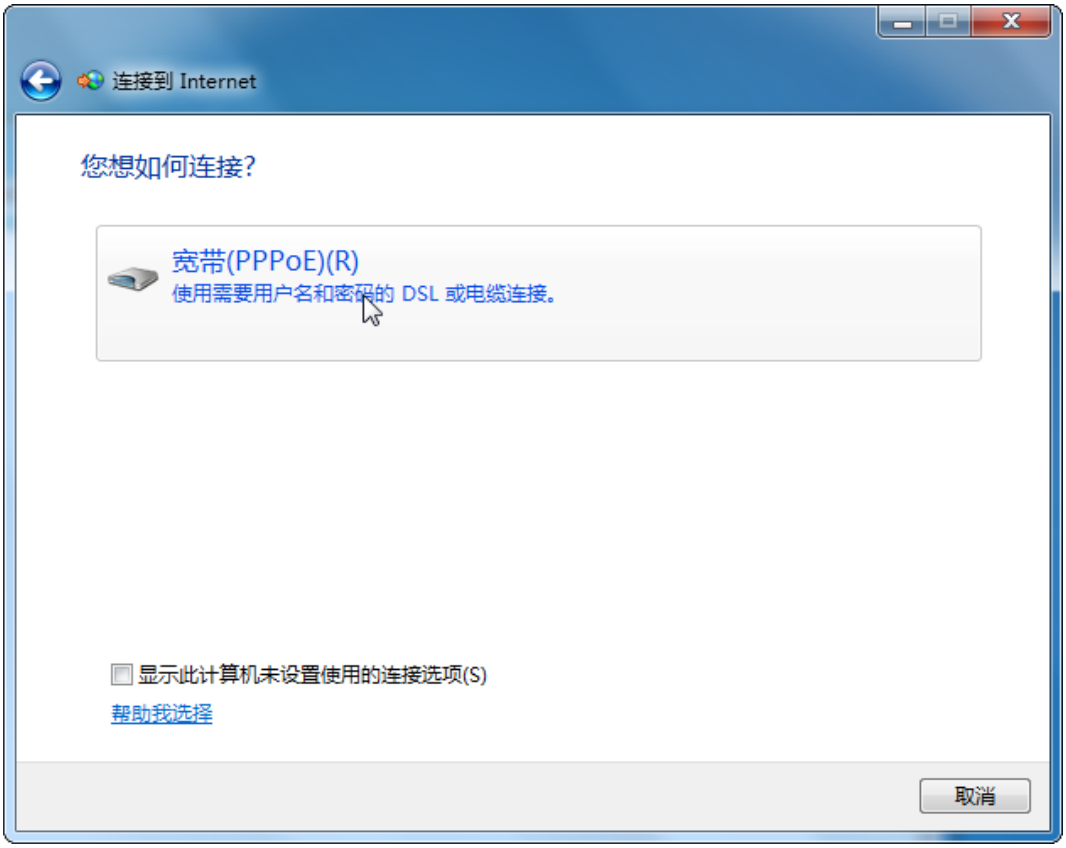
配置验证

客户端拨号上网（以 Windows 7 为例）。

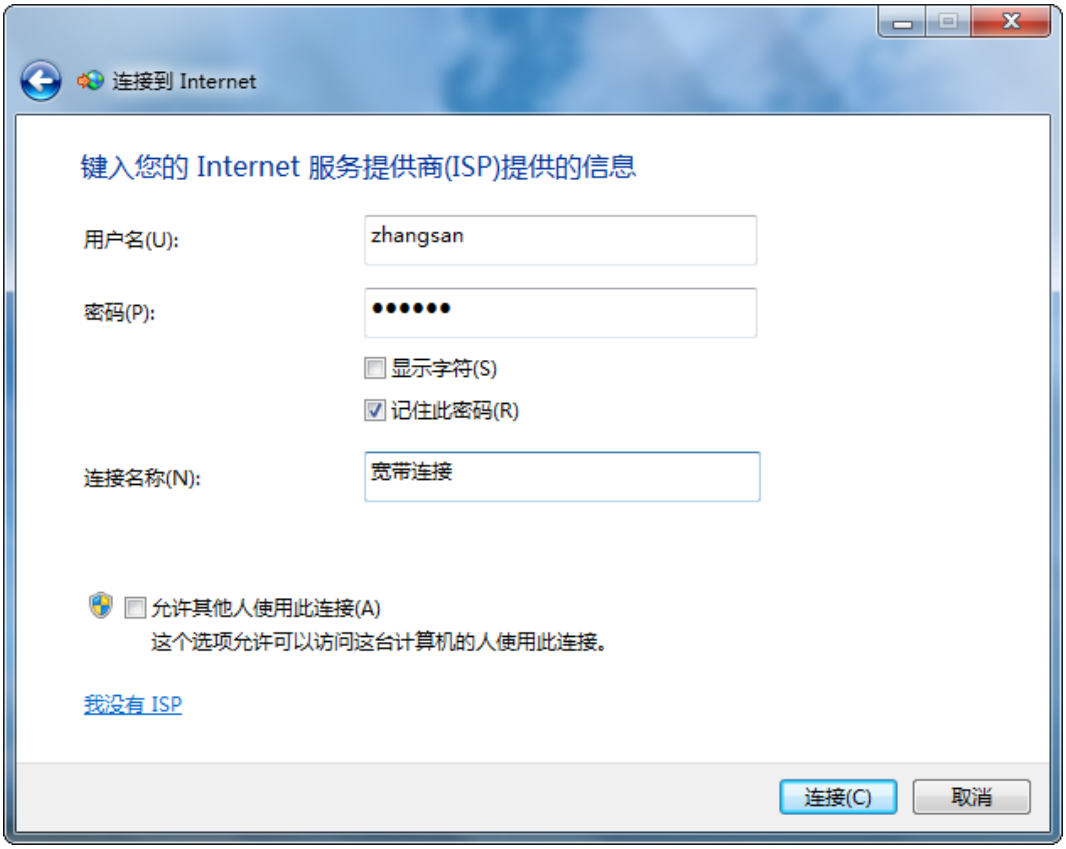
1. 点击桌面左下角的开始图标 。
2. 点击“控制面板”→“网络和 Internet”→“网络和共享中心”→“设置新的连接或网络”。

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。

12 虚拟服务器

虚拟服务器章节包括：

端口映射、UPnP、DMZ 主机、DDNS。

12.1 端口映射

12.1.1 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。

12.1.2 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。
内部端口段	局域网服务器的服务端口。
外部端口段	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”。
映射线路	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。

12.1.3 端口映射示例

组网需求

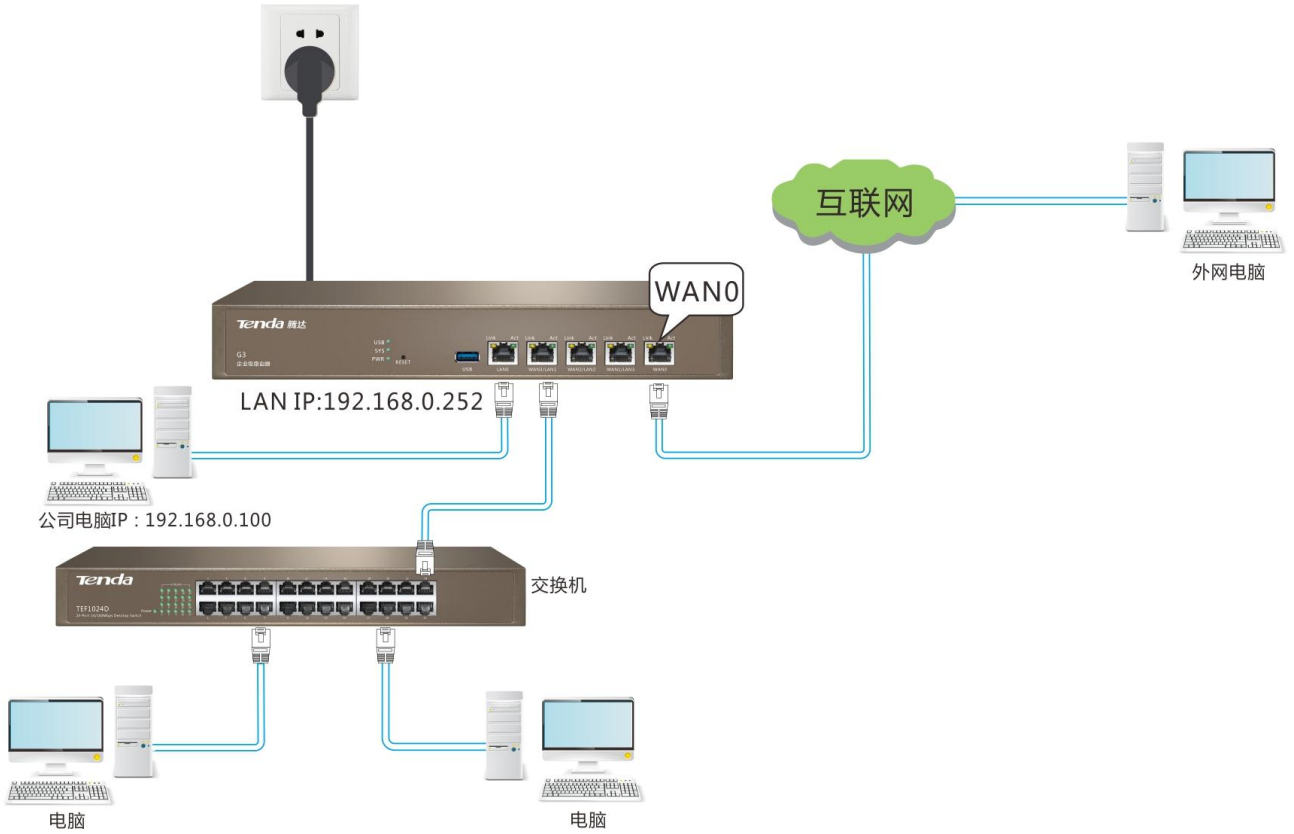
某企业使用 G3 进行网络搭建。假设路由器 WAN 口获取的 IP 地址为 202.105.106.55。外出出差人员需要访问自己在公司电脑上的资源。

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. 内网端口段：输入服务器使用的端口，如“21~21”。
5. 外网端口段：输入路由器开放给外网的端口，如“21~21”。
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“WAN0”。
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。

12.2 UPnP

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。

12.3 DMZ 主机

12.3.1 概述

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。
- 须为作为 DMZ 主机的内网电脑设置静态 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。

12.3.2 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。

12.4 DDNS

12.4.1 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。

12.4.2 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

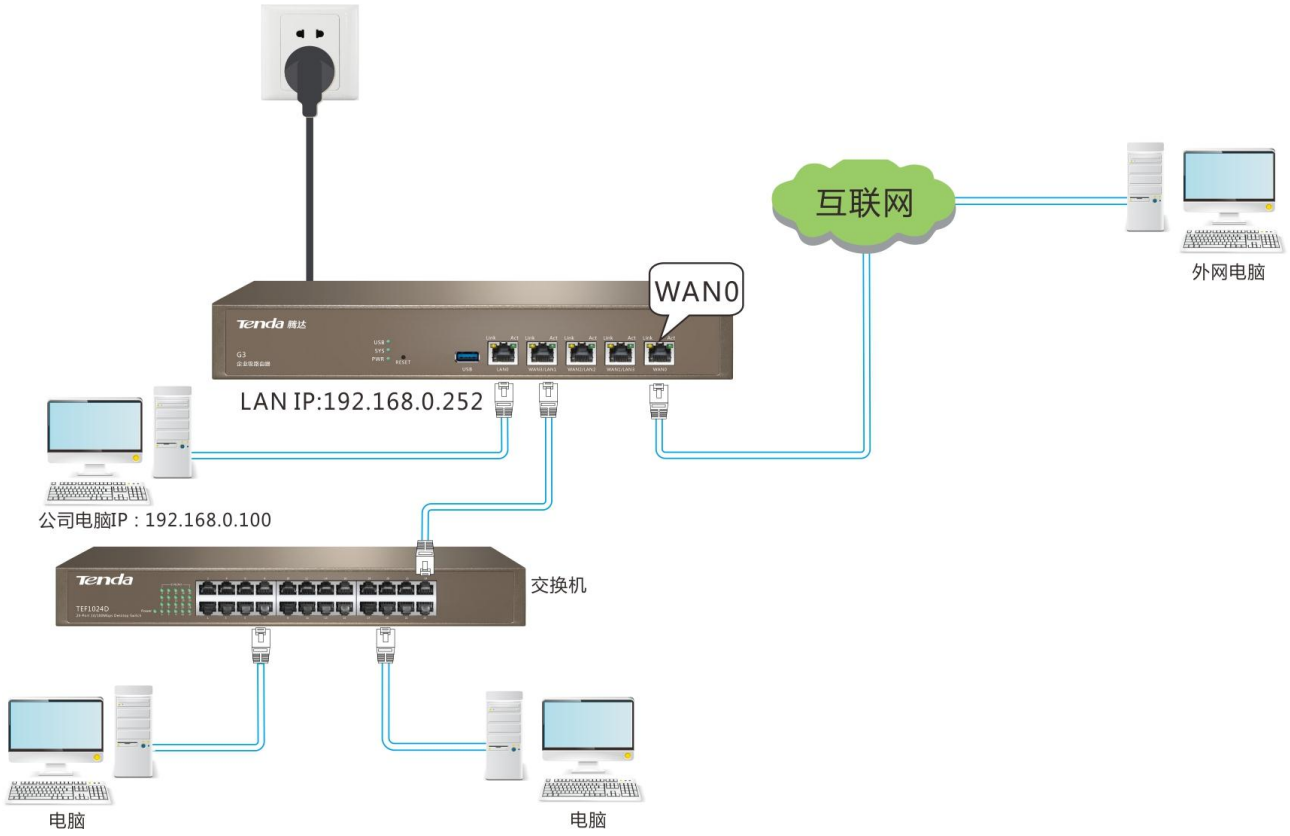
12.4.3 DDNS 示例

组网需求

某企业使用 G3 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 进入路由器 DDNS 设置页面，设置 DDNS 规则。

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. 点击页面底端的 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。

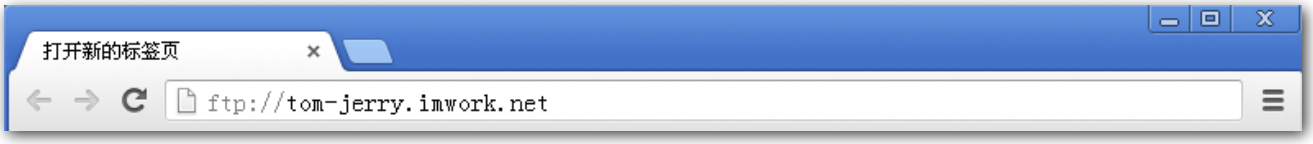
该账号在 DDNS 供应商网站关联了几个域名，本页的“域名信息”就会显示几个域名，这些域名都映射路由器的 WAN 口 IP 地址。

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。



13 USB 应用

USB 应用章节包括：USB 文件共享。

13.1 USB 文件共享

13.1.1 概述

在“USB 文件共享”页面，您可以查看 USB 存储设备信息，查看/修改访问 USB 设备的账号信息。

本路由器能自动识别插上其 USB 接口的 USB 存储设备，并在设置页面显示该 USB 存储设备使用率。局域网用户可以直接访问 USB 存储设备的信息。

点击『USB 文件共享』，进入设置页面。

路由器上插入 U 盘时，可以自动识别 U 盘信息，如下图示。

参数说明：

参数		说明
基本设置	Sda1	显示路由器上 USB 存储设备的使用率。
	安全弹出	为了避免 USB 存储设备的数据丢失，需要拔出 USB 设备时，请先点击此按钮后，再将该设备拔下。
	本地访问	路由器下的客户端访问 USB 存储设备资源的地址。默认参数如下： • ftp://192.168.0.252:21：直接点击此链接即可访问。 • \\192.168.0.252：需要将此网址复制到电脑的“开始”→“运行”菜单中，才能访问。
	允许互联网访问	禁止/允许互联网用户访问 USB 存储设备资源，默认禁用。
	互联网访问	启用“允许互联网访问”时，互联网用户可以通过此地址访问 USB 存储设备资源。
账号访问管理	用户名、密码	用户访问 USB 存储设备时需要输入的用户名、密码。用户名、密码可以根据实际情况进行修改。
	用户权限	账号的权限。 • 读写：用户可以对 USB 存储设备的资源进行访问和修改。 • 只读：用户只能访问 USB 存储设备的资源。

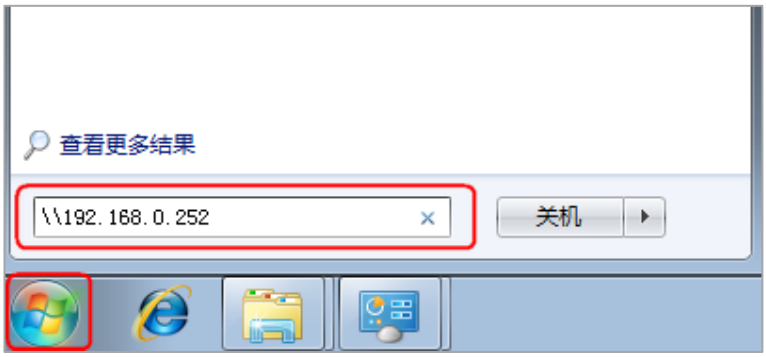
13.1.2 内网访问路由器 USB 设备资源

示例：某企业使用 G3 进行网络搭建，在路由器的 USB 接口接了一个移动存储设备作为服务器。公司员工查找资料时可以登录到该服务器上下载。假设网络管理员告知公司员工访问服务器的信息如下：

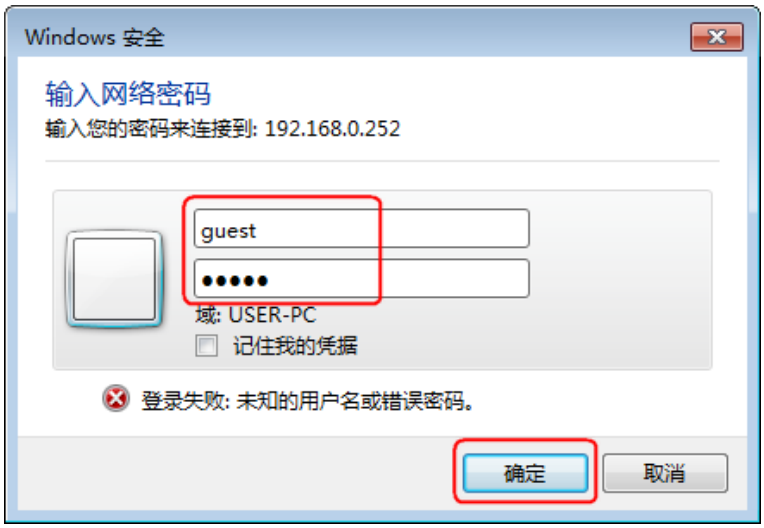
- 公司内部员工访问服务器地址：\\192.168.0.252。
- 用户名、密码均为 guest。

用户访问步骤（以 Windows 7 为例）：

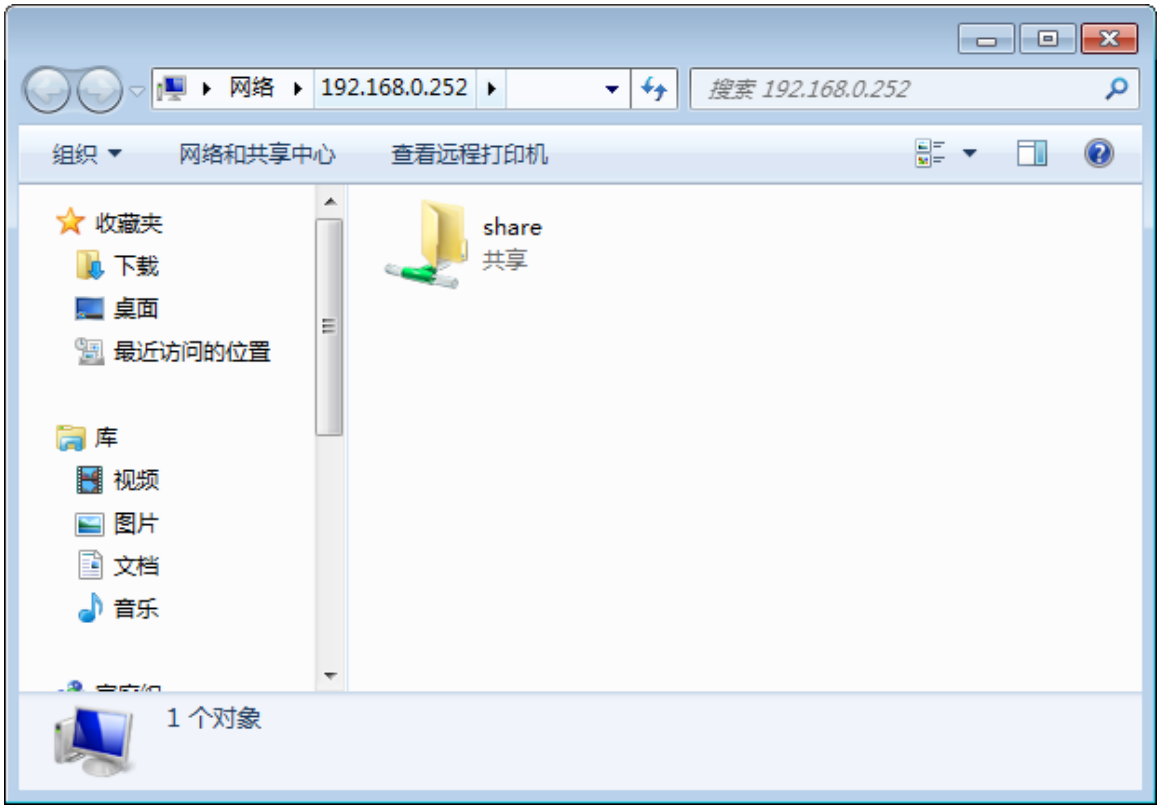
1. 在电脑上点击开始图标，然后输入“\\192.168.0.252”。
2. 回车（按键盘上的 Enter 键）。



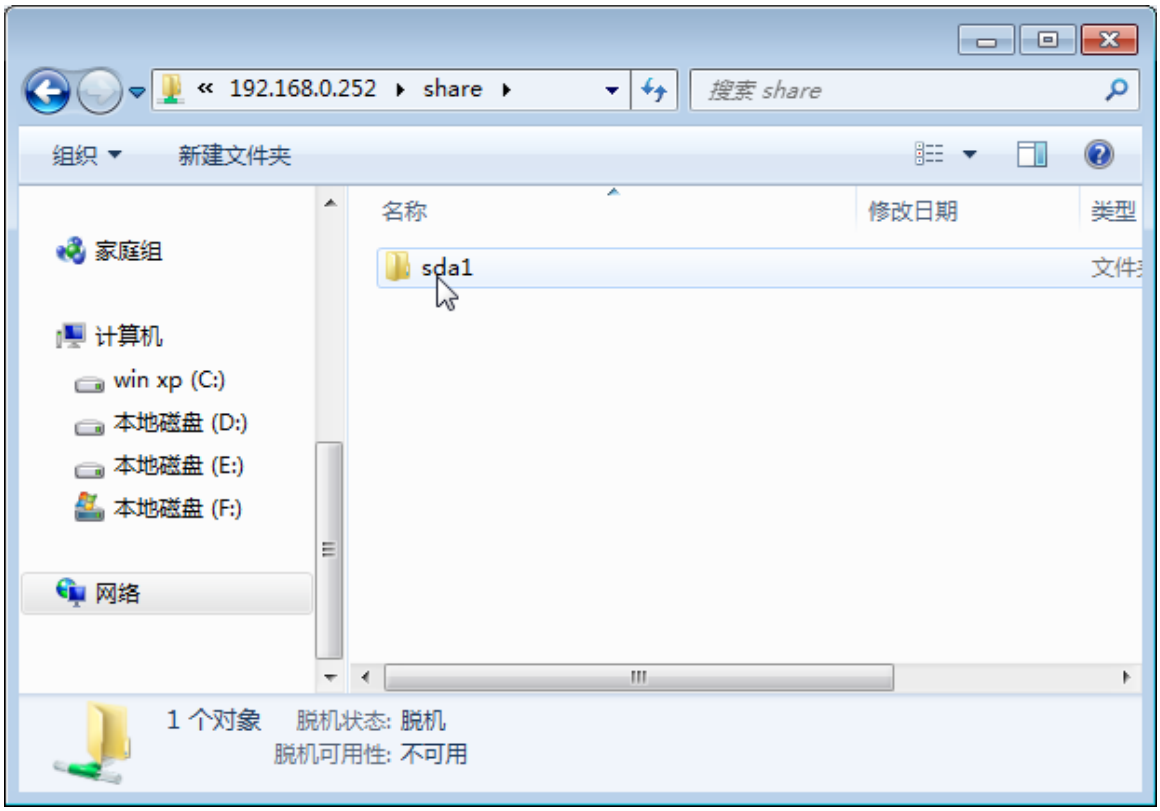
3. 在弹出的对话框输入用户名、密码，本例中均为 guest，然后点击 确定 。



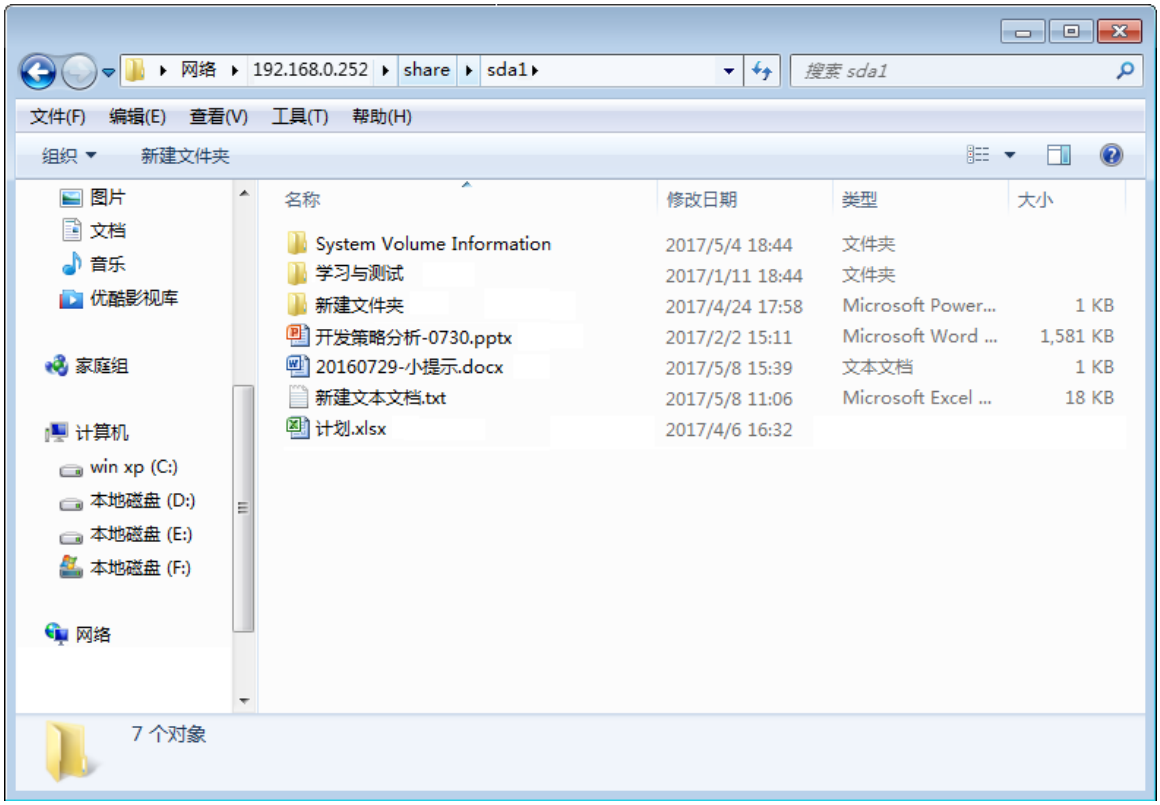
4. 在弹出的对话框双击“share”文件夹。



5. 在弹出的对话框双击“sda1”文件夹。



访问成功，将会弹出路由器上 USB 存储设备内的资源。



13.1.3 互联网访问路由器 USB 设备资源示例

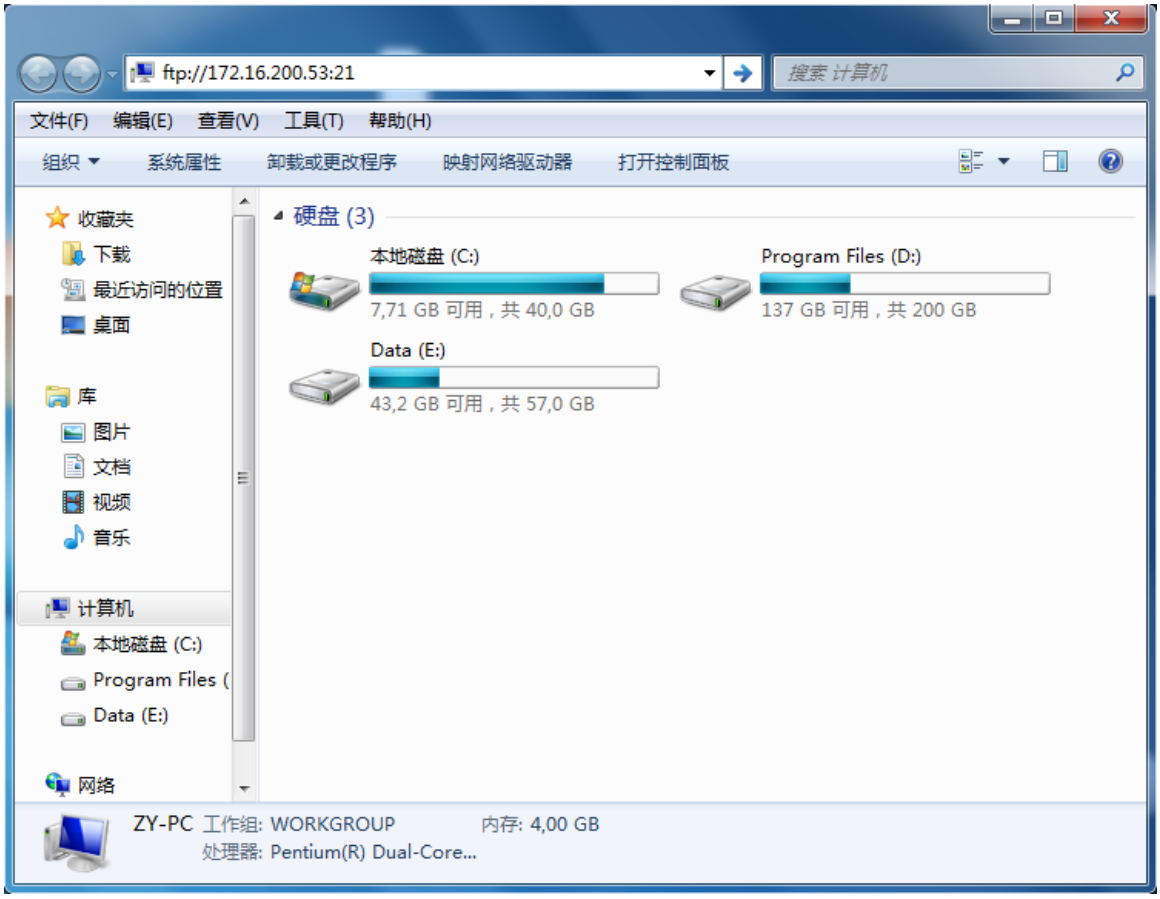
示例：某企业使用 G3 进行网络搭建，在路由器的 USB 接口接了一个移动存储设备作为服务器。公司员工出差需要登录该服务器查找资料。可以通过启用 USB 文件共享的“互联网访问功能”实现。假设网络管理员告知出差员工访问服务器的信息如下：

- 出差员工通过互联网访问服务器地址：ftp://172.16.200.53:21
- 用户名、密码均为 guest。

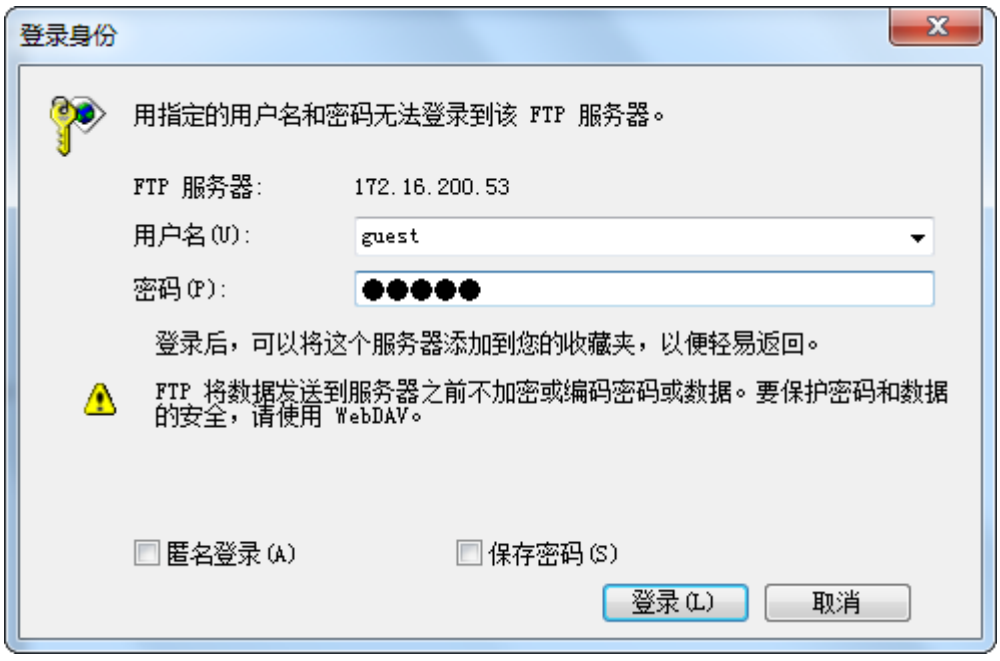
用户访问步骤（以 Windows 7 为例）：

1. 双击打开桌面“计算机”。

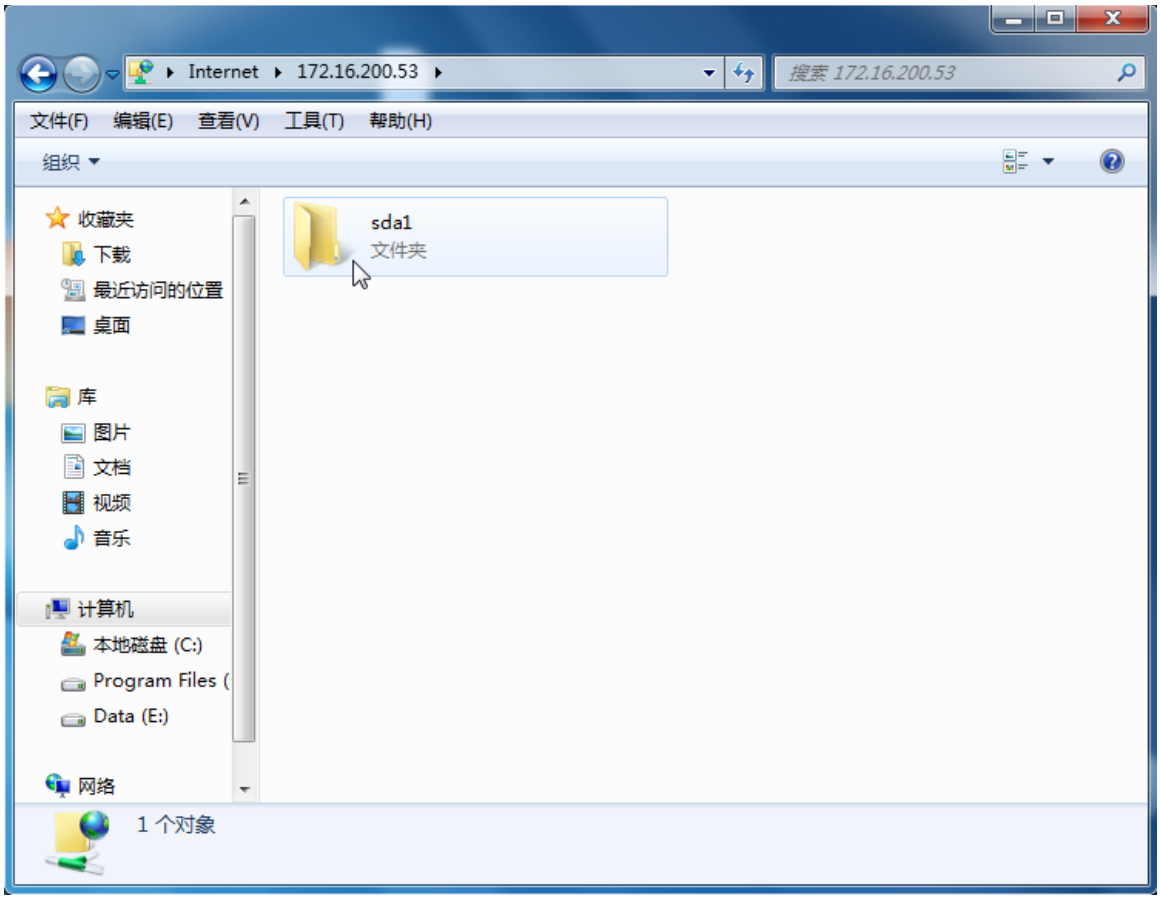
2. 在打开的窗口地址栏中输入远程访问公司服务器地址，本例为“ftp://172.16.200.53:21”，回车。



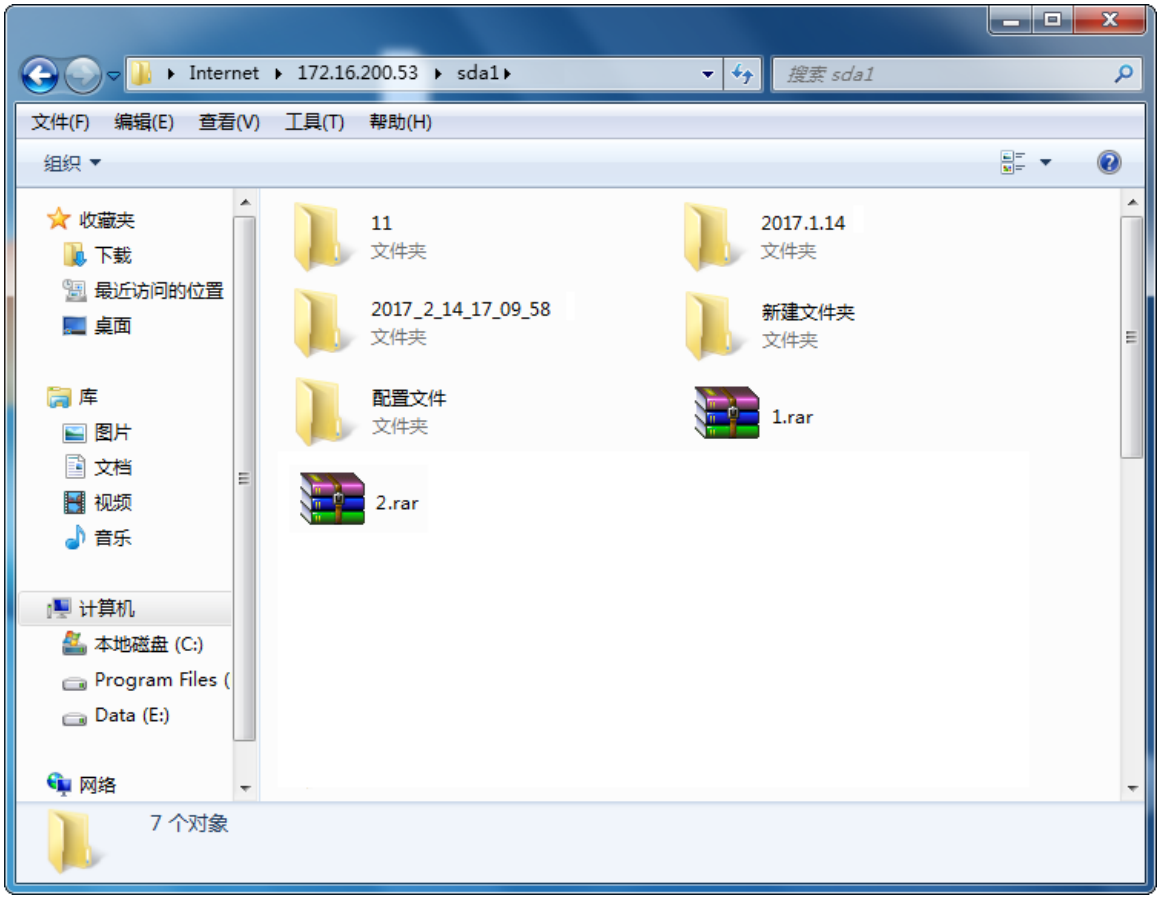
3. 在弹出的对话框输入用户名、密码，本例中均为 guest，然后点击 登录 。



4. 在弹出的对话框双击“sda1”文件夹。



访问成功，将会弹出路由器上 USB 存储设备内的资源。



—完成

14 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。

14.1 登录密码

14.1.1 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。

14.1.2 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。

14.2 重启

14.2.1 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。

14.2.2 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

14.2.3 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。

14.3 配置备份/恢复

14.3.1 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。

14.3.2 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

14.3.3 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

14.4 软件升级

14.4.1 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。

14.4.2 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。

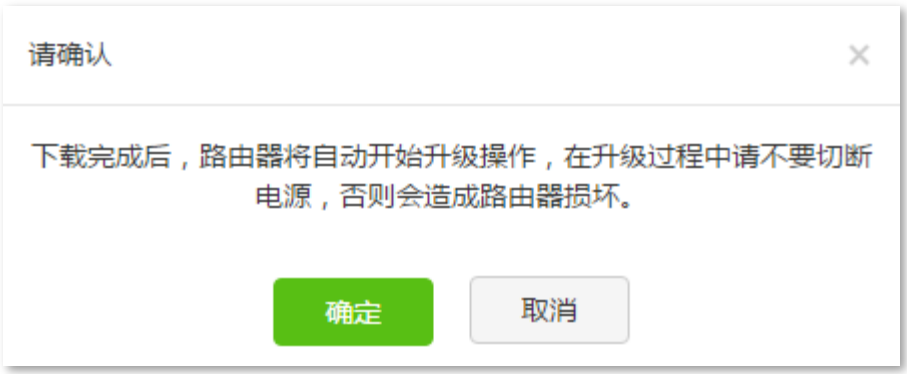
进度条走完后，将会自动跳转到登录页面。此时进入系统管理页面将路由器恢复出厂设置，然后重新设置上网。

14.4.3 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。

14.5 策略升级

14.5.1 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。

14.5.2 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。

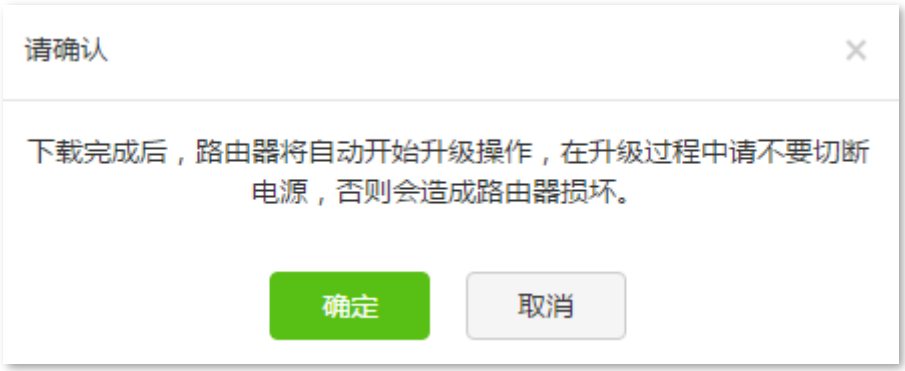
—完成

14.5.3 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。

14.6 恢复出厂设置

14.6.1 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。

14.6.2 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。

14.6.3 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。

14.7 系统时间

14.7.1 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。

14.7.2 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

14.8 远端 WEB 管理

14.8.1 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。

14.8.2 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

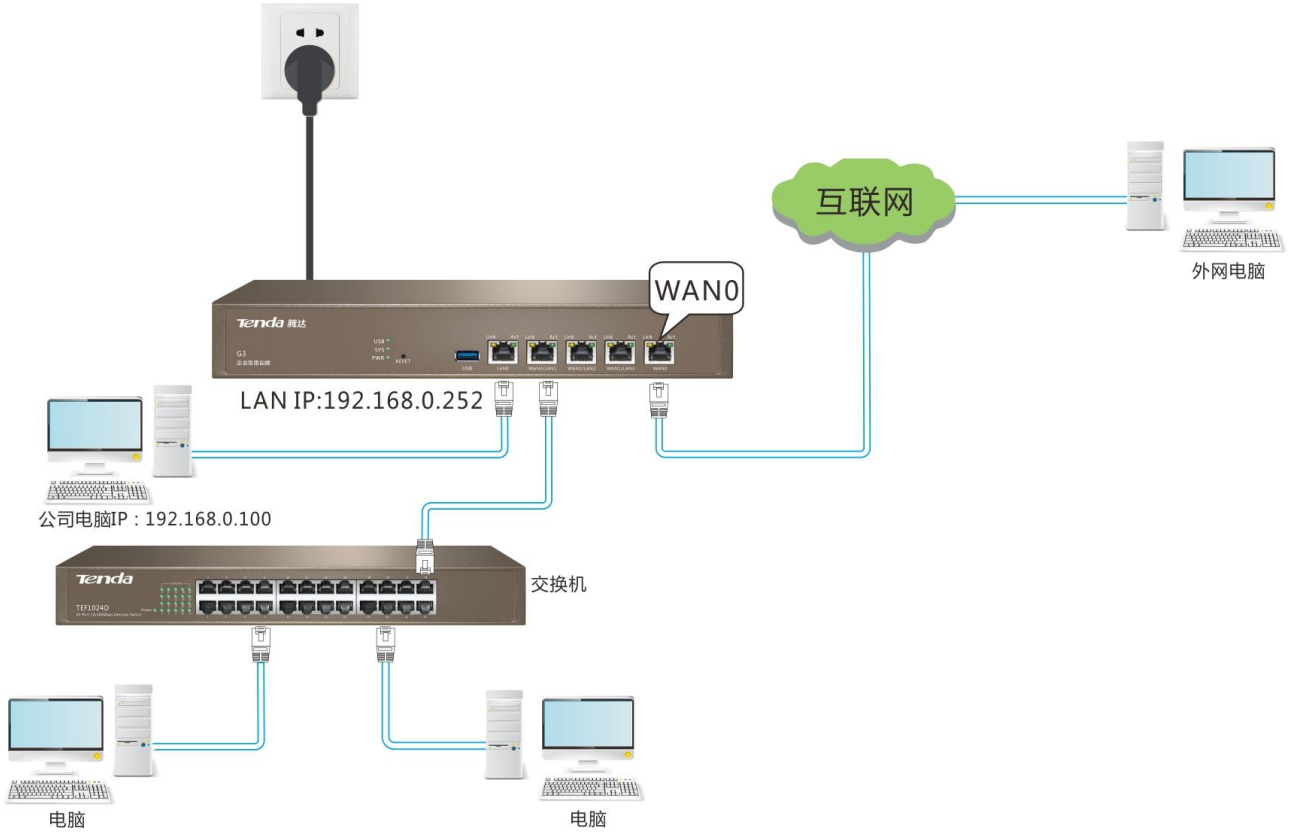
14.8.3 远端 WEB 管理示例

组网需求

某企业使用 G3 进行网络搭建，路由器 WAN0 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“WAN0”。
4. 点击 确定 。

—完成

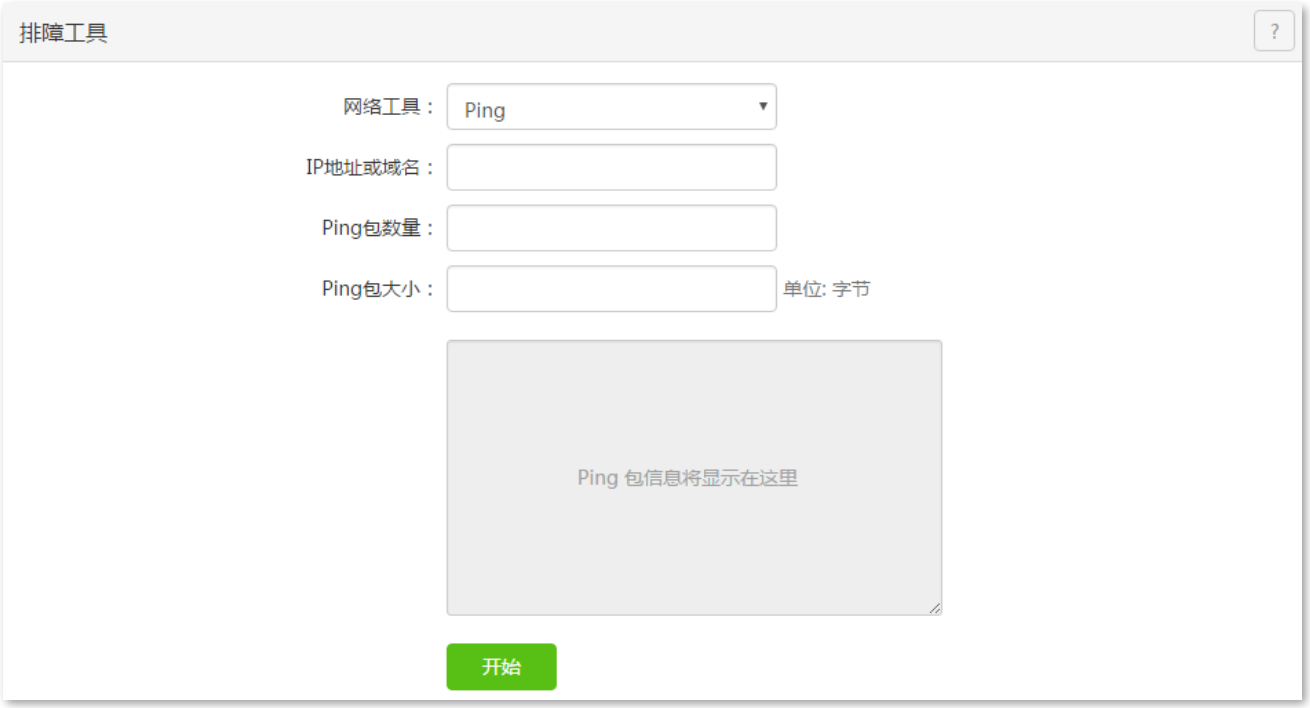
配置验证

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。

14.9 排障工具

14.9.1 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。

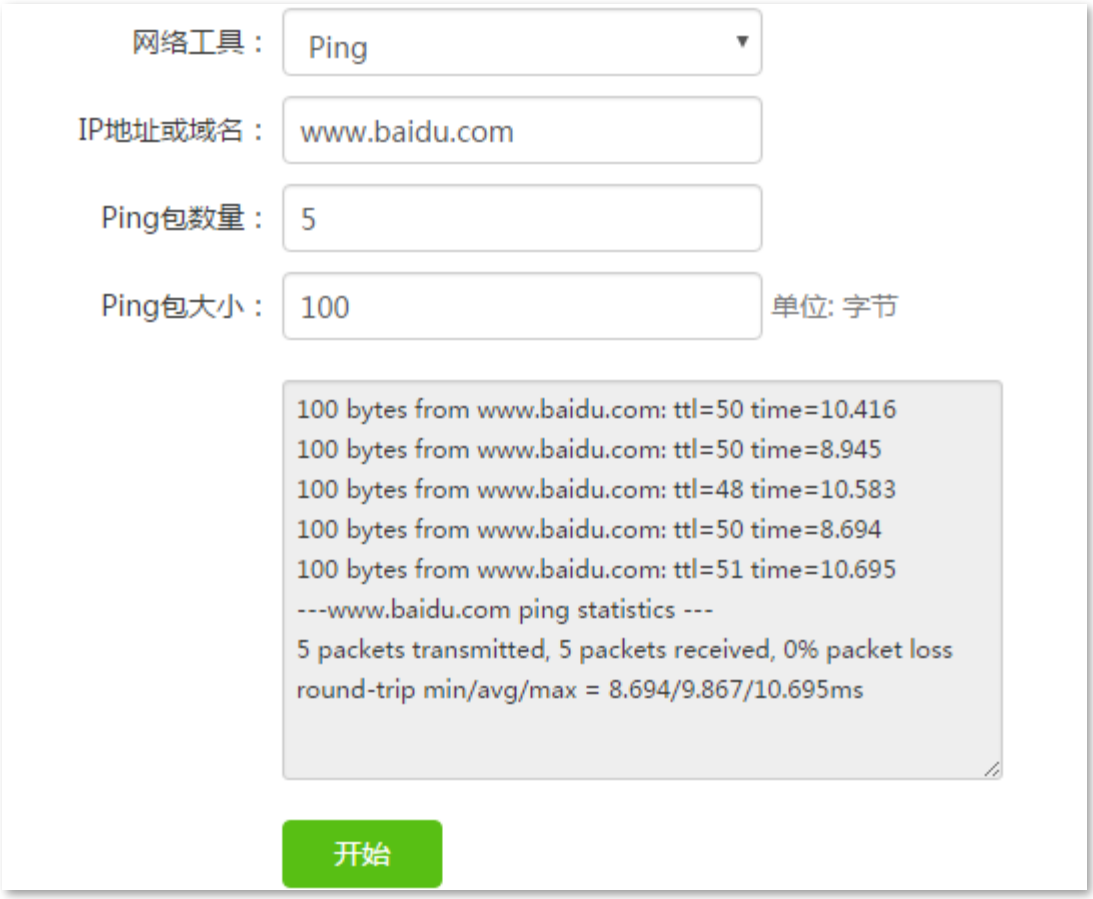
14.9.2 Ping 检测步骤

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 。

—完成

稍等片刻，结果将会显示在页面下方。



14.9.3 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。

15 系统状态

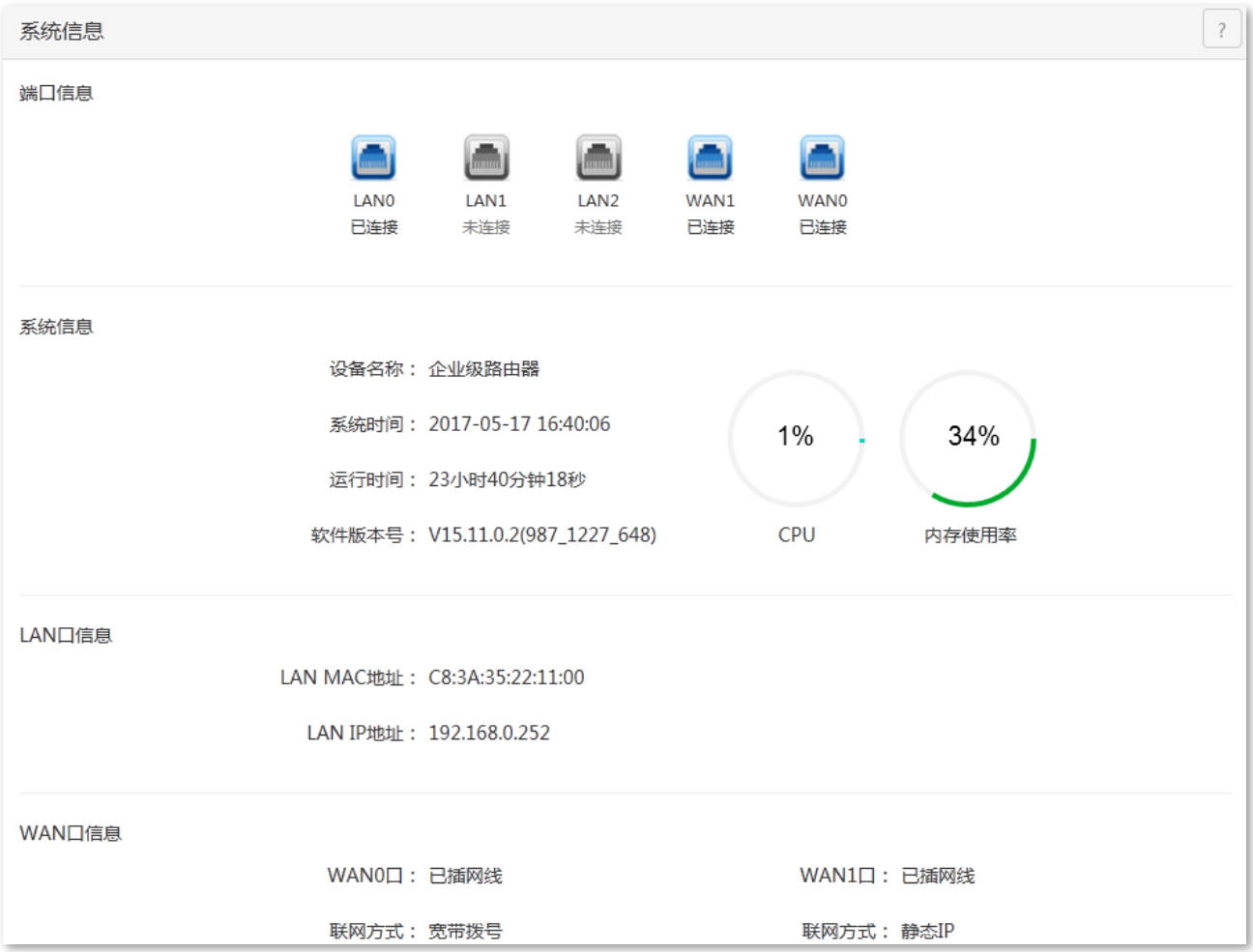
系统状态章节包括：

系统信息、用户列表、流量统计、防攻击日志、系统日志。

15.1 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。

15.2 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、VPN 用户、PPPoE 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。

15.2.1 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。

15.2.2 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。

15.2.3 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。

15.2.4 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。

15.3 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。

流量统计

序号	IP地址	在线时长	连接数	上行速率	下行速率	下载总流量
1	192.168.0.11	0天2小时1分钟8秒	8	0KB/s	0KB/s	0KB

15.4 防攻击日志

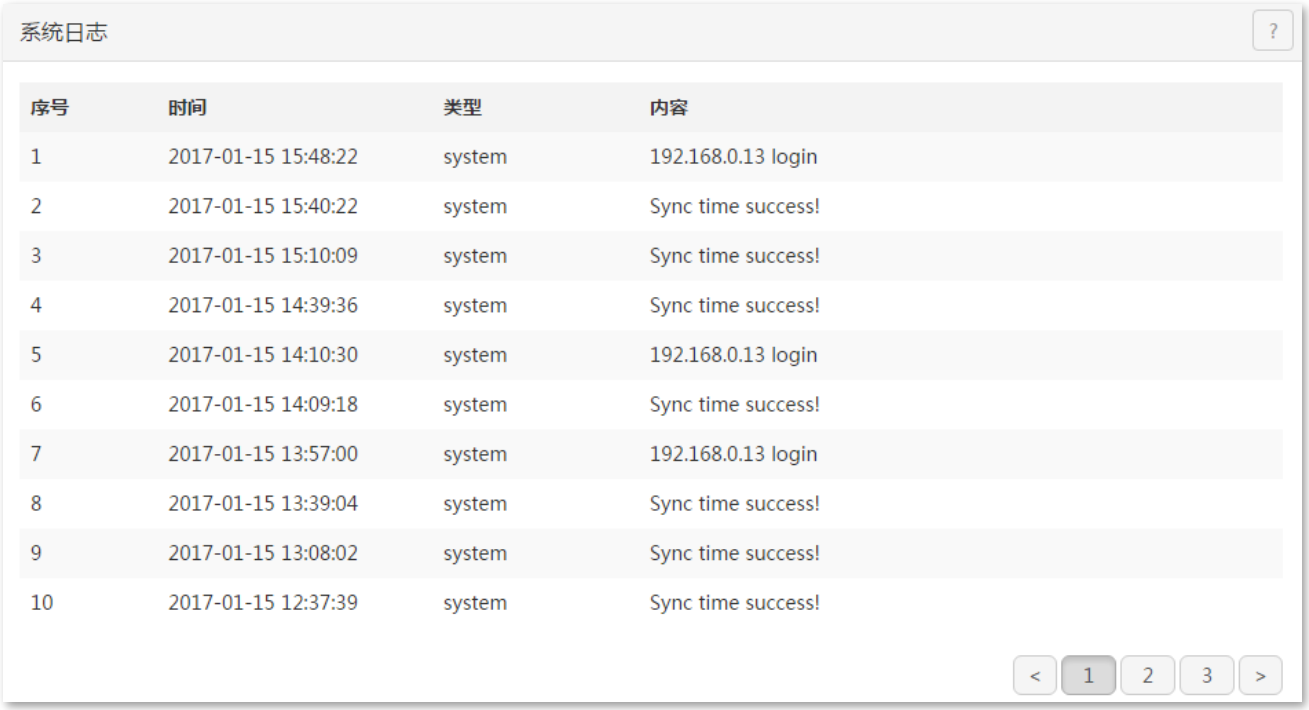
路由器开启“攻击防御”中的功能后，如果发生攻击，路由器会将攻击情况显示在防攻击日志里。根据防攻击日志，网络管理员可以快速地定位攻击者，采取针对措施并解决问题。

点击『系统状态』→『防攻击日志』，进入页面。

15.5 系统日志

在“系统日志”页面，您可以查看路由器的日志信息。如路由器故障时，可以查看日志信息进行问题排查。日志记录时间以路由器的系统时间为准，请确保路由器的系统时间准确。可以到『系统管理』→『系统时间』页面校准路由器的系统时间。

点击『系统状态』→『系统日志』，进入页面。



注意

- 路由器重启后，之前的日志信息将丢失。
- 断电后重新上电、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。

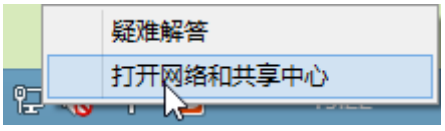
附录

A.1 设置电脑 IP 地址

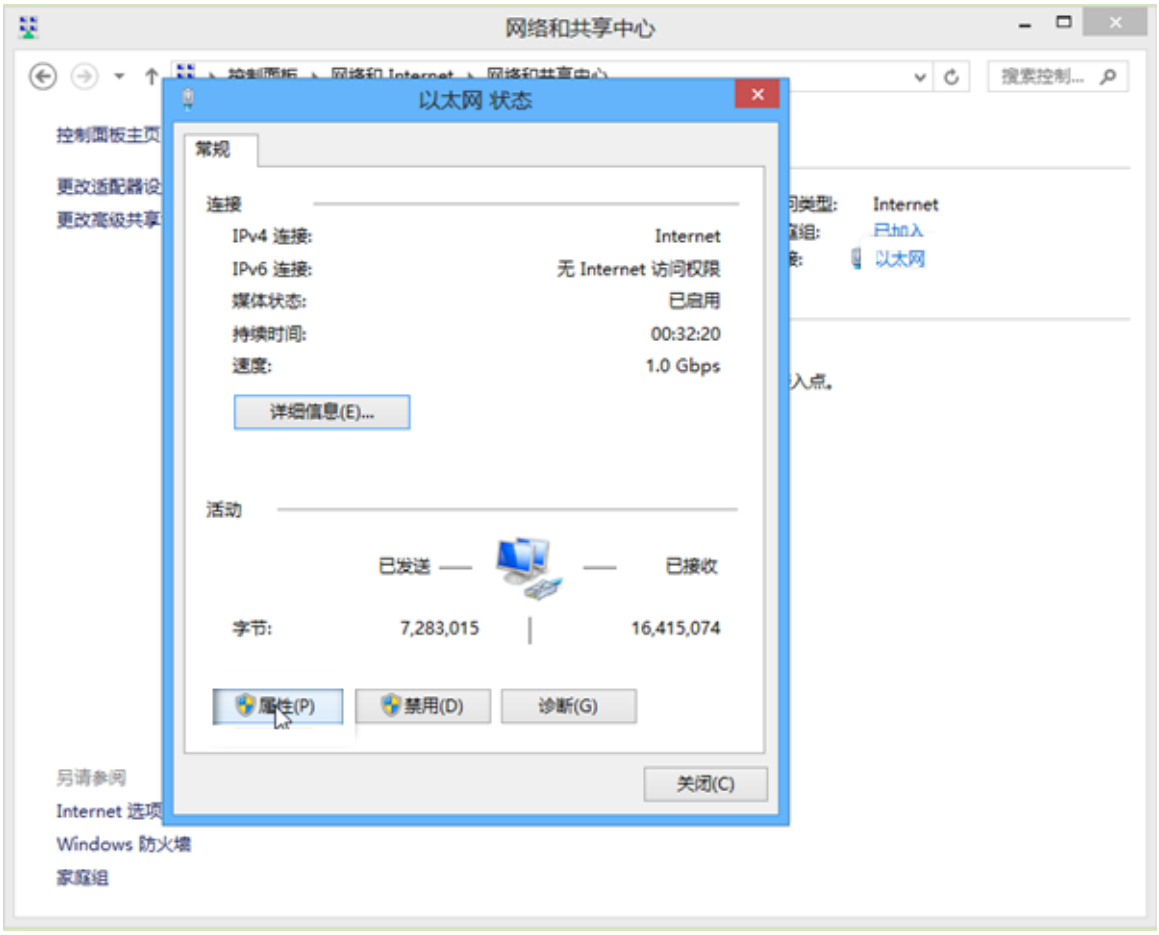
请根据电脑的操作系统，参考对应的设置步骤：Windows 8，Windows 7。

A.1.1 Windows 8

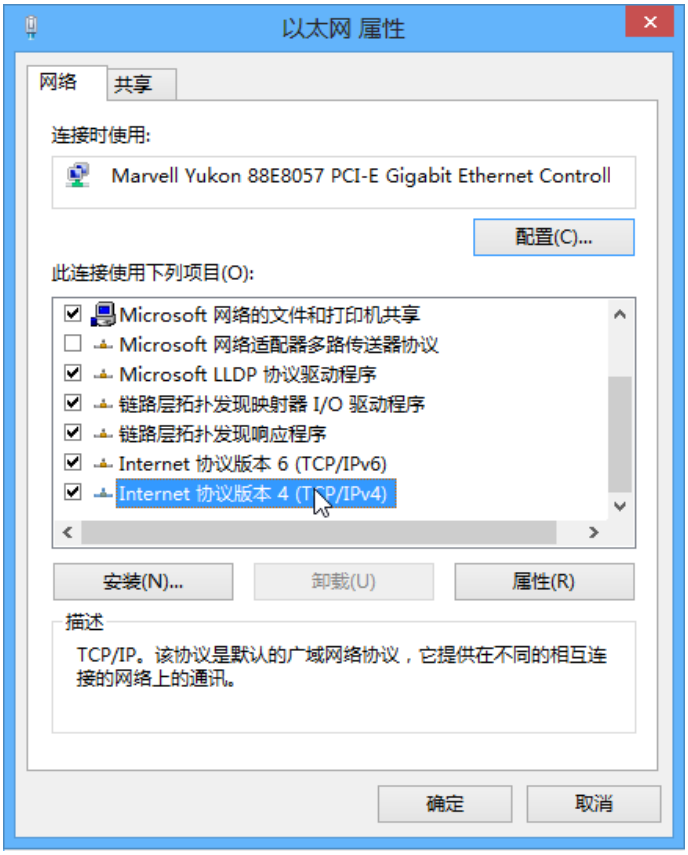
1. 右键点击桌面右下角的网络图标，点击**打开网络和共享中心。**



2. 点击以太网，点击 属性 。



3. 找到并双击 Internet 协议版本 4（TCP/IPv4）。

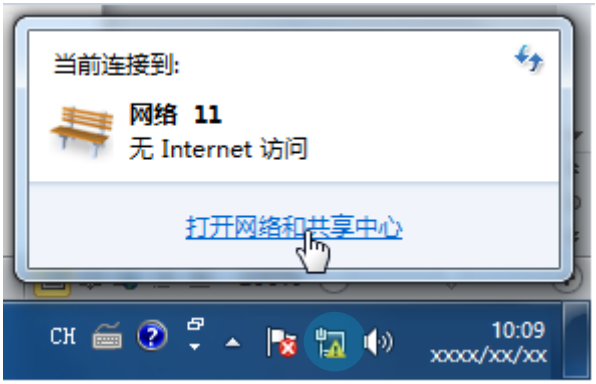


4. 选择自动获得 IP 地址，自动获得 DNS 服务器地址，点击 确定 。

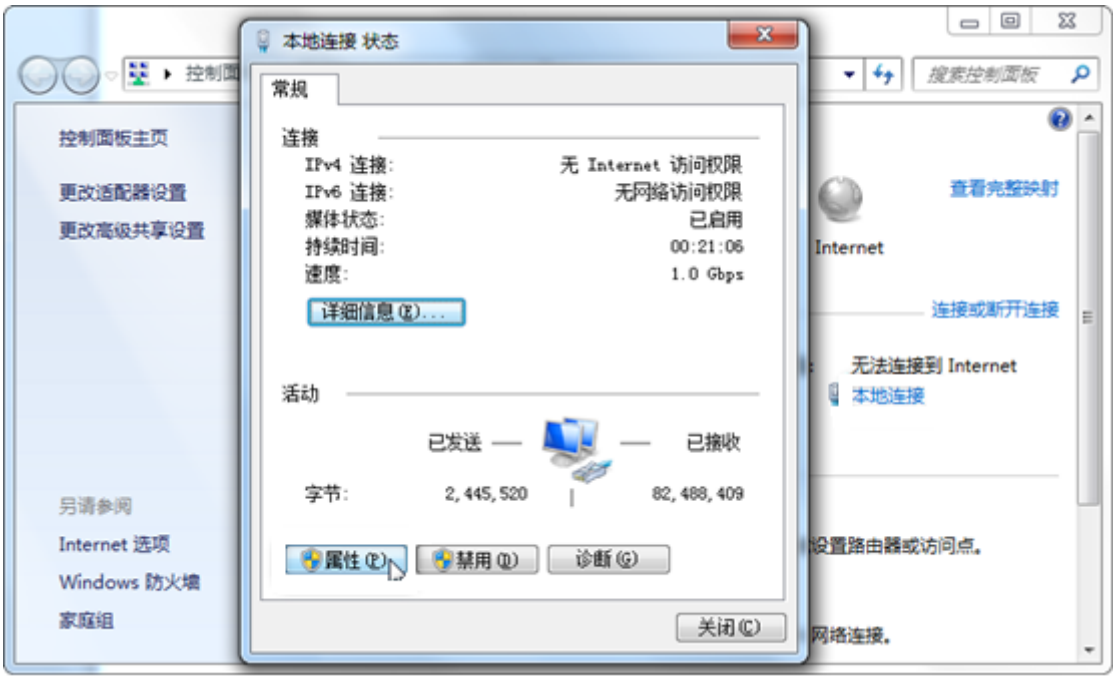
5. 页面自动返回**以太网 属性**对话框后，再点击 确定 。

A.1.2 Windows 7

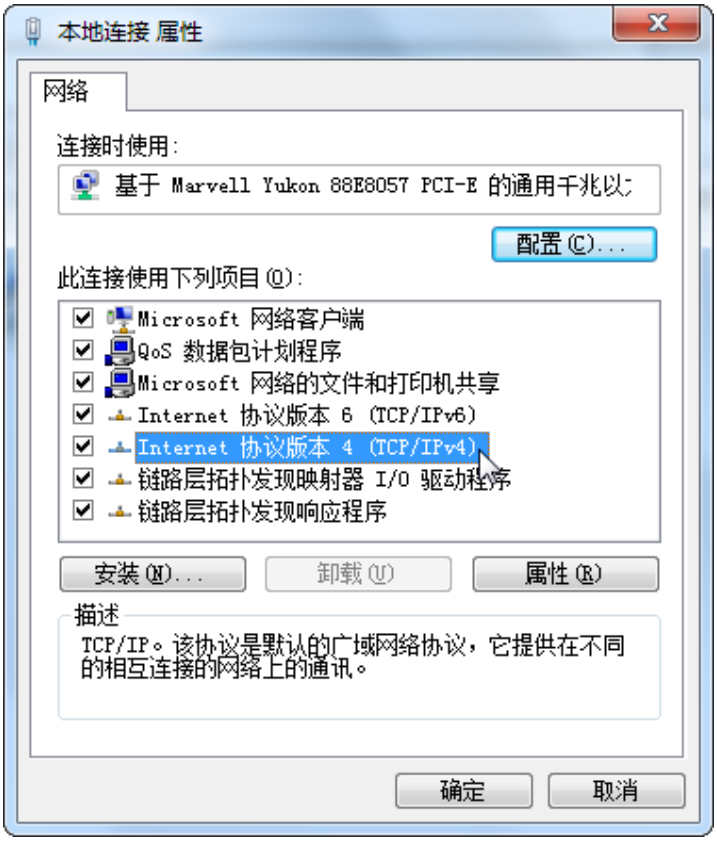
1. 点击桌面右下角的网络图标，如  ，点击**打开网络和共享中心**。



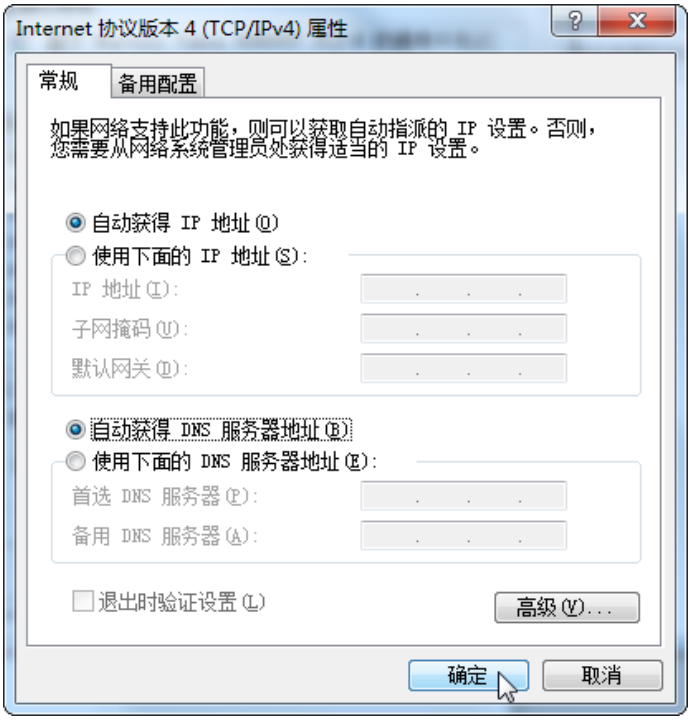
2. 点击本地连接，点击 属性 。



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

产品型号	G1	G3
带机量	100 台终端	200 台终端
可管理 AP 数	100 台	100 台
CPU	RAM 800MHz	RAM 800MHz
内存	256MB	512MB
FLASH	128MB	
网络接口	5 个 10/100/1000Mbps 自适应 RJ45 端口	
其它接口	1 个 USB 接口	
指示灯	1 个 PWR 灯，1 个 SYS 灯，1 个 USB 灯，每个 RJ45 端口带有 1 个 Link 灯、1 个 Act 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）	294mm*178.8mm*44mm	

A.3 常见问题解答

问1. 输入 tendawifi.com 或 192.168.0.252 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。
- 确认电脑 IP 地址为 192.168.0.X（X 为 2~254，除开 252）。
- 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 192.168.0.252 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。
- 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，重新设置上网。
- 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 192.168.0.252。

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 192.168.0.252。
- 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。