

**Tenda**

# User Guide

## Web 配置指南

企业级无线路由器



## 声明

版权所有©2023 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。

# 前言

感谢选择腾达产品。开始使用本产品前，请先认真阅读本指南并妥善保存以备日后参考。

## 约定



本指南介绍 Tenda 企业级无线路由器的 Web 管理界面功能。文中若无特殊说明，Web 管理界面截图均以 W18E 为例，具体请以实际为准。

本指南中，所提到的“路由器”、“无线路由器”“企业级无线路由器”等名称，如无特别说明，均指企业级无线路由器。

本文可能用到的格式说明如下。

项目	格式	举例
菜单项	「」	选择「状态」菜单。
按钮	边框+底纹	点击 <span>取消</span> 。
连续菜单选择	>	进入「更多」>「高级路由」>「WAN 口参数」页面。
窗口	【】	在【新增】窗口。

本文可能用到的标识说明如下。

标识	含义
 注意	表示重要信息或需要特别关注的信息。若忽略此等信息，可能导致配置失效、数据丢失或设备故障。
 提示	表示对配置操作进行补充与说明。

## 相关资料获取方式

访问 Tenda 官方网站 [www.tenda.com.cn](http://www.tenda.com.cn)，搜索对应产品型号，可获取最新的产品资料。

## 技术支持

如需了解更多信息，请通过以下方式与我们联系。

腾达官方网站：[www.tenda.com.cn](http://www.tenda.com.cn)



热线：400-6622-666



邮箱：[tenda@tenda.com.cn](mailto:tenda@tenda.com.cn)



腾达微信公众号



腾达官方微博

## 修订记录

资料版本	修订内容	发布日期
V1.0	首次发行。	2023-08-01



# 目录

1	登录 Web 管理界面 .....	1
1.1	登录 .....	1
1.1.1	使用电脑登录 .....	1
1.1.2	使用手机/平板登录 .....	3
1.2	退出登录 .....	5
2	Web 界面简介 .....	6
2.1	页面布局 .....	6
2.2	常用元素 .....	7
3	系统状态 .....	8
3.1	查看网络状态 .....	8
3.1.1	查看网络连线状态 .....	8
3.1.2	查看路由器（免布线主节点）信息 .....	9
3.1.3	查看扩展子路由（免布线子节点）信息 .....	11
3.2	查看接口信息 .....	13
3.3	查看 WAN 口实时速率 .....	13
3.4	查看连接状态 .....	14
3.5	管理终端用户 .....	15
3.5.1	设置最大上传/下载速率 .....	16
3.5.2	添加/移出黑名单 .....	16
3.6	查看流量统计 .....	17
4	联网设置 .....	18
4.1	联网设置 .....	18
4.1.1	概述 .....	18
4.1.2	设置 WAN 口个数 .....	18

4.1.3 设置联网.....	19
4.2 LAN 口设置 .....	23
4.2.1 查看 LAN 口状态 .....	23
4.2.2 LAN 口 IP 设置 .....	24
4.2.3 DHCP 服务器 .....	24
4.3 DHCP 静态分配 .....	26
5 无线设置 .....	28
5.1 无线网络设置 .....	28
5.2 访客网络 .....	30
5.3 无线访问控制 .....	32
5.3.1 设置无线访问控制规则 .....	32
5.3.2 无线访问控制配置举例 .....	33
5.4 无线高级设置 .....	36
6 网速控制 .....	39
6.1 WAN 口带宽 .....	39
6.2 分组限速 .....	39
6.2.1 设置分组限速 .....	39
6.2.2 分组限速配置举例 .....	41
7 行为管理 .....	44
7.1 分组策略 .....	44
7.1.1 时间组 .....	44
7.1.2 IP 组 .....	45
7.2 上网过滤 .....	47
7.2.1 IP 过滤 .....	47
7.2.2 MAC 过滤 .....	51
7.2.3 端口过滤 .....	55
7.2.4 URL 过滤 .....	59
8 更多设置 .....	63

8.1 高级路由 .....	63
8.1.1 WAN 口参数 .....	63
8.1.2 多 WAN 策略 .....	65
8.1.3 静态路由 .....	69
8.1.4 路由表 .....	74
8.1.5 策略路由 .....	75
8.2 虚拟服务 .....	80
8.2.1 DMZ 主机 .....	80
8.2.2 DDNS .....	84
8.2.3 DNS 劫持 .....	90
8.2.4 IP 劫持 .....	92
8.2.5 UPnP .....	94
8.2.6 端口映射 .....	95
8.3 维护服务 .....	100
8.3.1 远程 WEB 管理 .....	100
8.3.2 安全设置 .....	104
8.4 VPN 服务 .....	105
8.4.1 概述 .....	105
8.4.2 VPN 客户端 .....	105
8.4.3 IPSec .....	111
8.5 IPv6 .....	127
8.5.1 概述 .....	127
8.5.2 外网 .....	128
8.5.3 局域网 .....	131
9 系统工具 .....	134
9.1 系统时间 .....	134
9.1.1 与网络时间同步 .....	134
9.1.2 手动设置系统时间 .....	135
9.2 排障工具 .....	136

9.2.1 Ping.....	136
9.2.2 Tracert.....	137
9.2.3 抓包工具.....	139
9.2.4 系统诊断.....	140
9.2.5 接口信息.....	141
9.3 日志中心.....	143
9.3.1 系统日志.....	143
9.3.2 操作日志.....	143
9.3.3 运行日志.....	144
9.4 系统维护.....	144
9.4.1 设备信息.....	144
9.4.2 配置备份与恢复.....	145
9.4.3 恢复出厂设置.....	147
9.5 升级服务.....	148
9.5.1 概述.....	148
9.5.2 系统软件本地升级.....	148
9.5.3 特征库本地升级.....	150
9.6 重启.....	150
9.6.1 立即重启.....	150
9.6.2 定时重启.....	151
9.7 系统账号.....	152
9.8 诊断.....	152
附录.....	154
缩略语.....	154

# 1 登录 Web 管理界面

## 1.1 登录

如果您是首次使用路由器或已将路由器恢复出厂设置，请参考相应型号路由器的快速安装指南（前往[www.tenda.com.cn](http://www.tenda.com.cn)可下载快速安装指南）。否则，请参考下文。

### 1.1.1 使用电脑登录

**步骤 1** 用网线将管理电脑接到路由器的任一内网接口（LAN 口），或管理电脑连接路由器的无线网络。

**步骤 2** 打开电脑上的浏览器，访问路由器的管理地址“tendawifi.com”，进入路由器的登录页面。



**步骤 3** 输入登录密码，点击 **登录**。



若提示输入密码错误，请尝试使用以下方法解决：

- 您首次设置路由器时，系统默认会将无线网络密码同步设置为登录密码。如果您无法确定是否设置过登录密码，请输入无线网络密码尝试登录。
- 如果还是不行，请将路由器[恢复出厂设置](#)后，重新尝试。注意，恢复出厂设置后需要重新设置路由器联网。



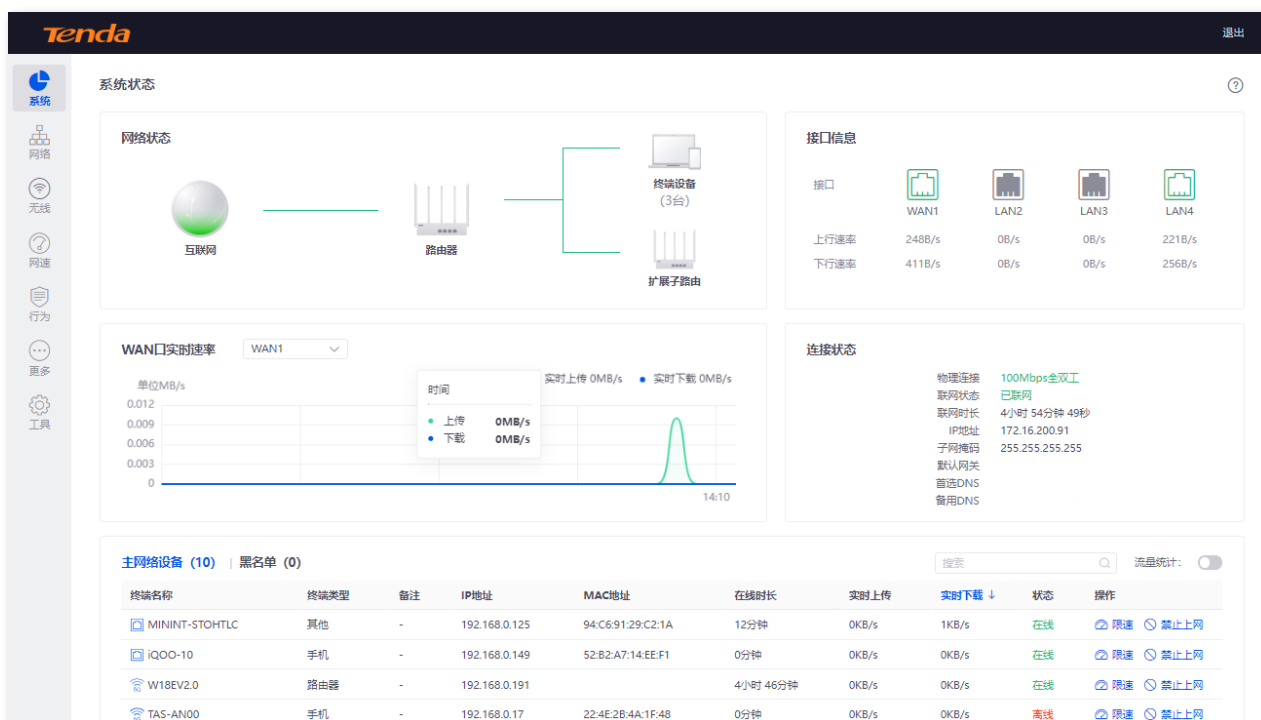
----完成



若未出现上述页面，请尝试使用以下方法解决：

- 确保路由器通电正常。
- 确保电脑连接的是路由器 LAN 口，且网线连接正常，无松动现象。
- 确保电脑已设为“自动获得 IP 地址，自动获得 DNS 服务器地址”。
- 请在浏览器地址栏（非搜索栏）输入 [tendawifi.com](http://tendawifi.com) 或 192.168.0.1。
- 将路由器[恢复出厂设置](#)，然后重新登录。注意，恢复出厂设置后需要重新设置路由器联网。

成功登录路由器管理页面。



## 1.1.2 使用手机/平板登录

此处以手机为例，平板类似。

**步骤 1** 手机连接到路由器的无线网络，此处以“Tenda\_192C60”为例。



**步骤 2** 打开手机上的浏览器，在地址栏（非搜索栏）访问路由器的管理地址“tendawifi.com”，进入路由器管理页面。

**步骤 3** 输入登录密码，点击 **登录**。



提示

若提示输入密码错误，请尝试使用以下方法解决：

- 您首次设置路由器时，系统默认会将无线网络密码同步设置为登录密码。如果您无法确定是否设置过登录密码，请输入无线网络密码尝试登录。
- 如果还是不行，请将路由器[恢复出厂设置](#)后，重新尝试。注意，恢复出厂设置后需要重新设置路由器联网。



----完成



若未出现上述页面，请尝试使用以下方法解决：

- 确保路由器通电正常。
- 请确保已成功连接路由器的无线网络。
- 使用手机登录时，请确保已关闭手机数据流量。
- 将路由器[恢复出厂设置](#)，然后重新登录。

成功登录路由器管理页面。



当前移动端页面暂未做适配，请根据实际情况缩放查看。





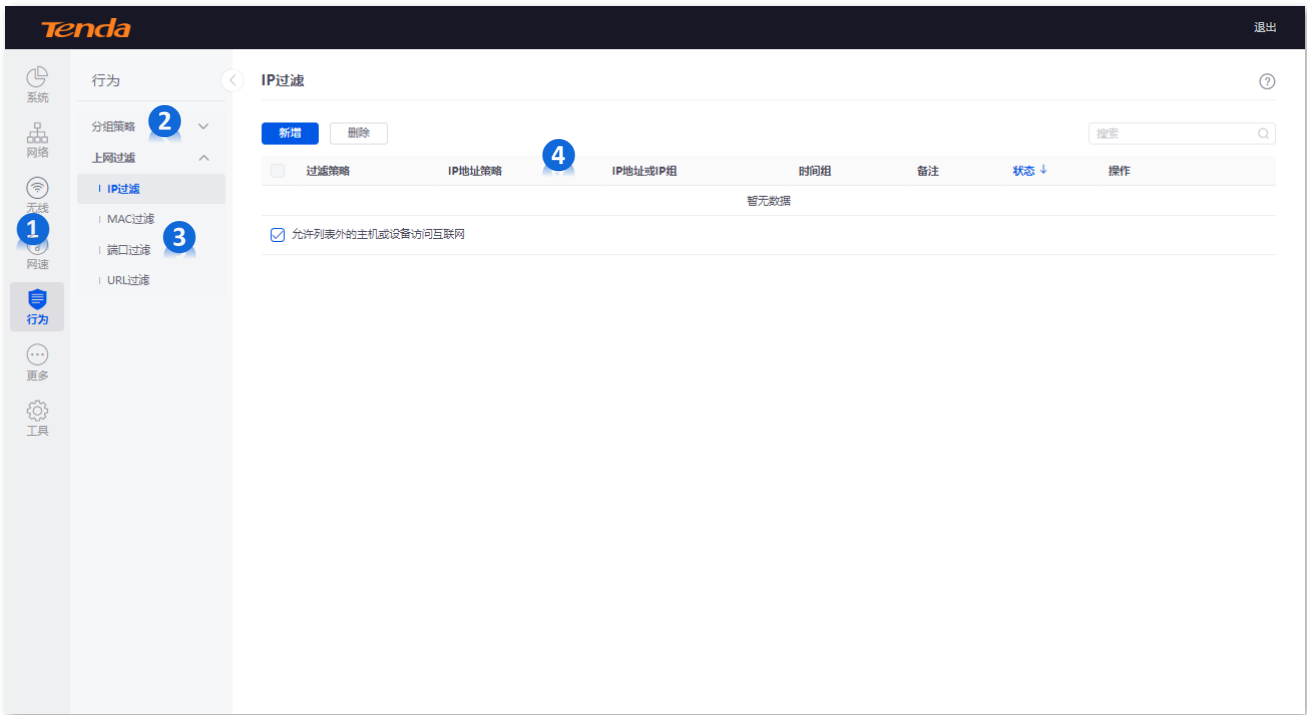
## 1.2 退出登录

您登录到路由器的管理页面后，如果在[闲置超时时间](#)内没有任何操作，系统将自动退出登录。此外，在管理页面上，点击右上角的“退出”，也可以安全地退出管理页面。

# 2 Web 界面简介

## 2.1 页面布局

路由器的管理页面共分为：一级导航栏、二级导航栏、三级导航栏和配置区四部分。如下图所示。



提示

管理页面上显示为灰色的功能或参数，表示路由器不支持或在当前配置下不可修改。

序号	名称	说明
1	一级导航栏	
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，选择结果显示在配置区。
3	三级导航栏	
4	配置区	用户进行配置或查看配置的区域。

## 2.2 常用元素

路由器管理页面中常用元素的功能介绍如下表。

常用元素	说明
新增	用于新增配置。
保存	用于保存当前页面配置，并使配置生效。
取消	用于取消当前页面未保存的配置，并恢复到修改前的配置。
编辑	用于修改配置。
删除	用于删除配置。
?	用于查看当前页面设置的帮助信息。

## 3

# 系统状态

## 3.1 查看网络状态

进入页面：[登录路由器 Web 管理页面](#)，点击「系统」，找到“网络状态”模块。

在这里，您可以查看路由器 WAN 口的网络连接是否正常，也可以查看路由器与扩展子路由的基本信息。

### 3.1.1 查看网络连线状态

当“互联网”与“路由器”之间线路正常，如下图示，则表示对应 WAN 口网络连接正常。



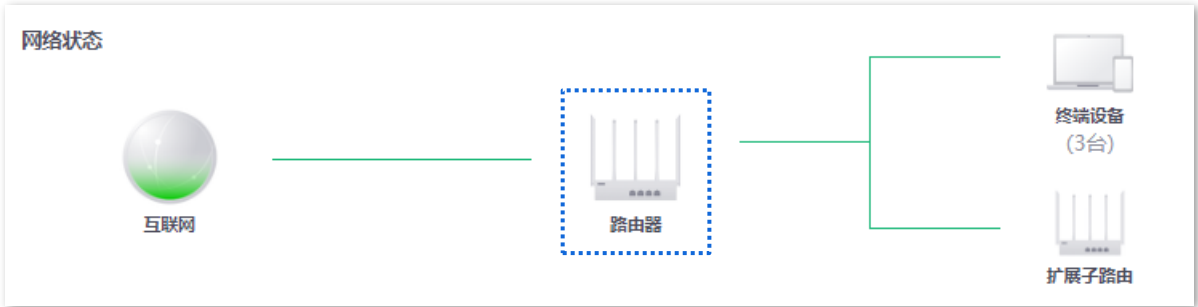
当“互联网”与“路由器”之间线路打叉，如下图示，则表示对应 WAN 口网络连接异常，请检查联网配置与网线连接情况。

点击“互联网”与“路由器”之间线路可跳转至[联网设置](#)页面检查联网配置。



### 3.1.2 查看路由器（免布线主节点）信息

登录路由器 Web 管理页面，在「系统」页面，点击路由器图标，可以查看路由器的[运行状态](#)、[无线状态](#)。



#### 查看运行状态

在“运行状态”模块，您可以查看路由器的名称、工作模式、系统时间、运行时长等信息。

运行状态	
系统时间	2023-07-20 08:59:51
运行时长	23小时 44分钟
工作模式	路由模式
软件版本	V16.01.0.5(1357)
设备名称	1200M 11AC 双频千兆口企业无线路由器
CPU使用率	10%
内存使用率	49%

#### 参数说明

标题项	说明
系统时间	路由器当前的系统时间。
运行时长	路由器最近一次启动后连续运行的时长。
工作模式	<p>路由器当前的工作模式。</p> <ul style="list-style-type: none"><li>- 路由模式：作为免布线网络的主节点，上联到有线网络，是免布线网络中唯一访问外部网络的出口，实现免布线网络和有线网络的数据转换。</li><li>- 信号放大模式：作为免布线网络的子节点，通过免布线自组网，扩展现有免布线网络的覆盖范围。</li></ul>

标题项	说明
软件版本	路由器系统软件的版本号。
设备名称	路由器的名称描述。
CPU 使用率	路由器当前的 CPU 使用率。
内存使用率	路由器当前的内存使用率。

## 查看无线状态

在“无线状态”模块，您可以查看路由器的无线网络状态。

无线状态						
射频	无线名称	无线协议	信道	频宽	加密方式	射频状态
2.4G	zhangsan	WiFi 4 (802.11b/g/n)	7	20MHz	WPA-PSK/WPA2-PSK	已启用
5G	zhangsan	WiFi 5 (802.11a/n/ac)	153	80MHz	WPA-PSK/WPA2-PSK	已启用

## 参数说明

标题项	说明
射频	路由器的工作频段。
无线名称	路由器的无线网络名称。
无线协议	路由器的无线网络协议。
信道	路由器无线数据传输的通道。
频宽	路由器无线信道的频带宽度。
加密方式	无线网络的加密方式。
射频状态	路由器的无线网络的无线功能启用状态。

### 3.1.3 查看扩展子路由（免布线子节点）信息



管理子路由前，请先参考相应型号路由器的快速安装指南（前往 [www.tenda.com.cn](http://www.tenda.com.cn) 可下载快速安装指南），进行免布线组网，将子路由添加到网络中。

登录路由器 Web 管理页面，在「系统」页面，点击扩展子路由图标，可以查看网络中的扩展子路由信息。

网络状态图显示了互联网、路由器和终端设备（3台）的连接。其中，扩展子路由被高亮显示。

设备信息

子节点1

运行状态	
系统时间	2023-07-20 10:38:25
运行时长	16小时 38分钟
工作模式	信号放大模式
软件版本	V16.01.0.5(1357)
设备名称	1200M 11AC 双频千兆口企业无线路由器
LAN状态	
IP地址	<a href="#">192.168.0.194</a>
MAC地址	C8:3A:35:45:87:8E
链路质量	
上级节点MAC地址	C8:3A:35:21:90:80
与上级链接方式/强度	5GHz/ -7dBm
与上级协商速率	390Mbps

取消 确定


在“设备信息”页面，您可以查看扩展子路由的[运行状态](#)、[LAN 口状态](#)和[链路质量](#)。

### 查看 LAN 口状态

在“LAN 口状态”模块，您可以查看扩展子路由的 LAN 口 IP 地址和 MAC 地址。

LAN状态	
IP地址	<a href="#">192.168.0.194</a>
MAC地址	C8:3A:35:45:87:8E

#### 参数说明

标题项	说明
	扩展子路由 LAN 口的 IP 地址。扩展子路由的 IP 地址从主节点的 DHCP 服务器自动获取。
IP 地址	 <b>提示</b> 扩展子路由的 LAN 口 IP 地址，也是管理 IP 地址，局域网用户可访问该 IP 地址登录到扩展子路由的管理页面。扩展子路由管理页面的登录密码与主节点管理页面的登录密码一致。
MAC 地址	扩展子路由 LAN 口的物理地址。

### 查看免布线链路质量

在“链路质量”模块，您可以查看扩展子节点与上级节点的免布线链路信息。

链路质量	
上级节点MAC地址	C8:3A:35:21:90:80
与上级链接方式/强度	5GHz/ -6dBm
与上级协商速率	866Mbps

#### 参数说明





标题项	说明
上级节点 MAC 地址	与该节点免布线组网的上级节点的 MAC 地址。
与上级链接方式/强度	该节点与上级节点的组网方式及上级节点的信号强度。
与上级协商速率	该节点与上级节点的实时协商速率。



## 3.2 查看接口信息

进入页面：[登录路由器 Web 管理页面](#)，点击「系统」，找到“接口信息”模块。

在这里，您可以查看路由器各接口的物理连接状态、当前上下行速率。

接口信息				
接口	 WAN1	 LAN2	 LAN3	 LAN4
上行速率	186B/s	0B/s	0B/s	320B/s
下行速率	207B/s	0B/s	0B/s	108B/s

### 参数说明

标题项	说明
	路由器各接口角色与物理连接状态。
接口	<ul style="list-style-type: none"><li>- 绿色表示接口已连接。</li><li>- 灰色表示接口未连接。</li></ul>
上行速率	接口当前的上/下行速率。
下行速率	

## 3.3 查看 WAN 口实时速率

进入页面：[登录路由器 Web 管理页面](#)，点击「系统」，找到“WAN 口实时速率”模块。

在这里，鼠标悬浮于时间轴上，可查看 WAN 口的实时上传与下载速率。



提示

如果您有设置[多 WAN 口](#)，可以点击“WAN 口实时速率”模块中的下拉框，选择其他 WAN 口，查看对应 WAN 口的实时上传与下载速率。



### 3.4 查看连接状态

进入页面：[登录路由器 Web 管理页面](#)，点击「系统」。找到“连接状态”模块。

在这里，您可以查看对应 WAN 口 IPv4 的网络情况，包括网口连接速率及双工模式、联网状态、联网时长，以及 IP 地址等。



如果您有设置[多 WAN 口](#)，可以点击“WAN 口实时速率”模块中的下拉框，选择其他 WAN 口，查看对应 WAN 口的连接状态。

连接状态

物理连接

100Mbps全双工

联网状态

已联网

联网时长

9分钟 17秒

IP地址

子网掩码

默认网关

首选DNS

备用DNS

#### 参数说明

标题项	说明
物理连接	对应 WAN 口的协商速率和双工模式。 如果显示异常，请根据页面信息及当前环境排障。

标题项	说明
联网状态	显示路由器 WAN 口的连接状态。
	- 已联网/认证成功：路由器 WAN 口已获得 IPv4 地址信息并联网正常。
	- 连接中...：路由器正在连接到上级网络设备。
	- 未联网/联网失败：未连接或连接失败，请检查网线连接状态、联网信息设置或咨询相应宽带服务商。
	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。
联网时长	WAN 口最近一次成功接入 IPv4 网络的时长。
IP 地址	WAN 口的 IPv4 地址。
子网掩码	WAN 口的子网掩码。
默认网关	WAN 口的 IPv4 网关地址。
首选 DNS	WAN 口的首选/备用 IPv4 DNS 服务器地址。
备用 DNS	

### 3.5 管理终端用户

进入页面：[登录路由器 Web 管理页面](#)，点击「系统」。










在这里，您可以查看或管理连接到路由器的用户。

查看或管理用户时，您可以在搜索栏基于终端名称、IP 地址、MAC 地址快速筛选相关用户信息。

主网络设备 (14) | 黑名单 (0)

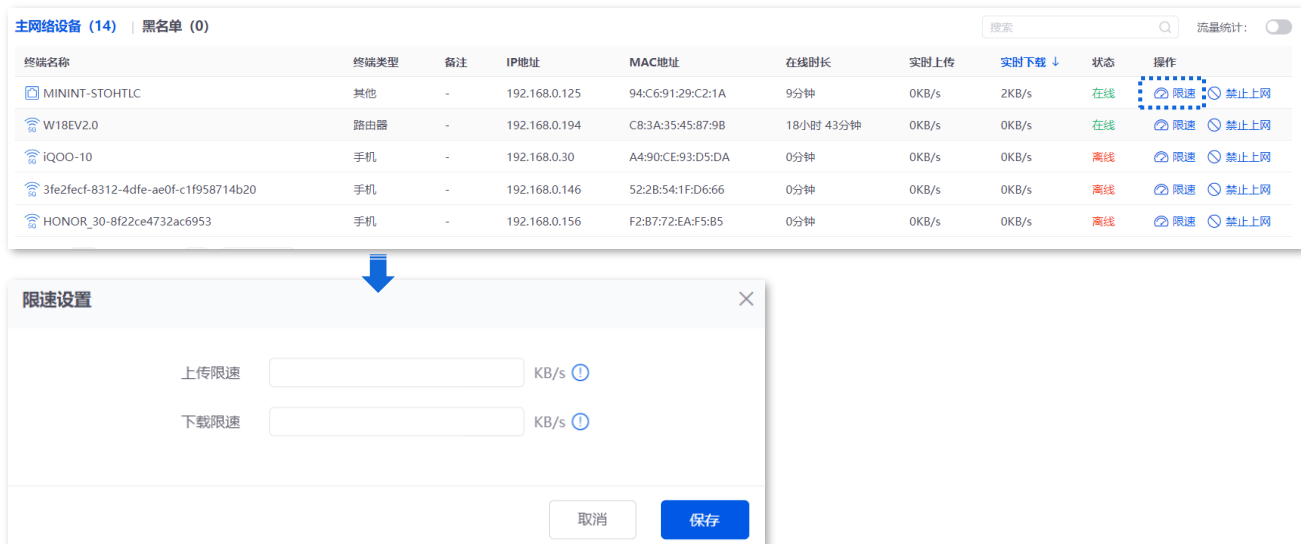
搜索

流量统计: ☐

终端名称	终端类型	备注	IP地址	MAC地址	在线时长	实时上传	实时下载 ↓	状态	操作
 MININT-STOHTLC	其他	-	192.168.0.125	94:C6:91:29:C2:1A	9分钟	0KB/s	2KB/s	在线	 限速  禁止上网
 W18EV2.0	路由器	-	192.168.0.194	C8:3A:35:45:87:9B	18小时 43分钟	0KB/s	0KB/s	在线	 限速  禁止上网
 IQOO-10	手机	-	192.168.0.30	A4:90:CE:93:D5:DA	0分钟	0KB/s	0KB/s	离线	 限速  禁止上网
 3fe2fecf-8312-4dfe-ae0f-c1f958714b20	手机	-	192.168.0.146	52:28:54:1F:D6:66	0分钟	0KB/s	0KB/s	离线	 限速  禁止上网
 HONOR_30-8f22ce4732ac6953	手机	-	192.168.0.156	F2:B7:72:EA:F5:B5	0分钟	0KB/s	0KB/s	离线	 限速  禁止上网

### 3.5.1 设置最大上传/下载速率

登录路由器 [Web 管理页面](#)，在「系统」页面，找到要限制上网速率的设备，点击**限速**，设置最大上传/下载速率。

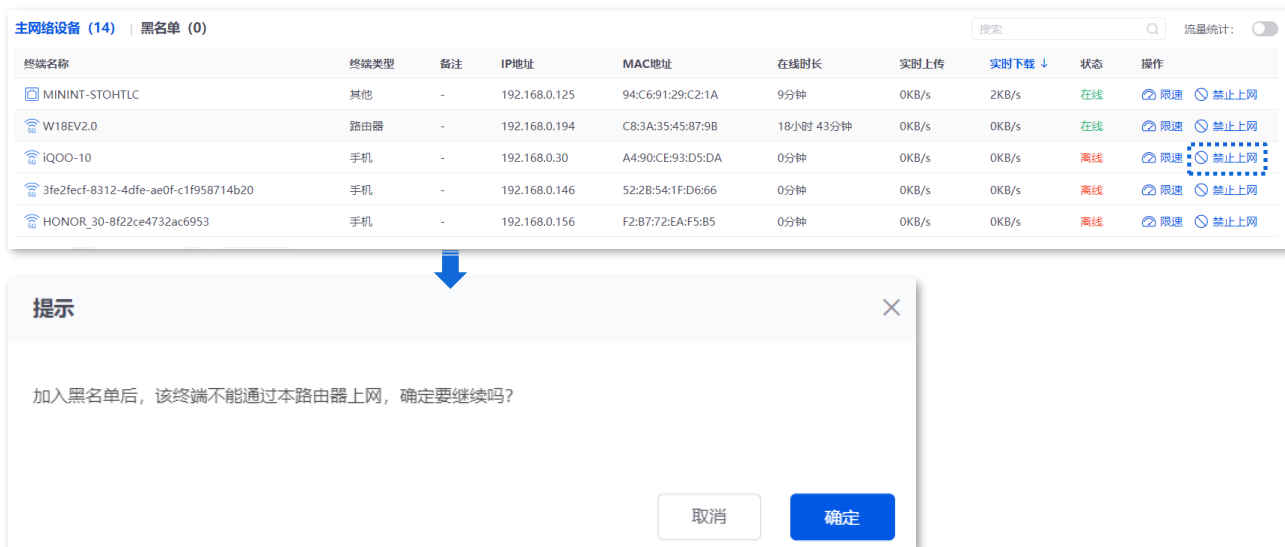


### 3.5.2 添加/移出黑名单

#### 添加黑名单

加入黑名单的设备，不能通过路由器上网。

登录路由器 [Web 管理页面](#)，在「系统」页面，找到要加入黑名单的设备，点击**禁止上网**，确认提示信息后，点击**确定**。



您可以在「系统」页面，点击黑名单，查看已添加到黑名单的设备。

主网络设备 (2)   黑名单 (1)				搜索
终端名称	终端类型	MAC地址	移出黑名单	
iQOO-Neo3	手机	06:1A:39:DF:60:38	移出	

## 移出黑名单

移出黑名单的设备，可重新连接路由器上网。

登录路由器 [Web 管理页面](#)，在「系统」页面，点击黑名单，找到要移出黑名单的设备，点击移出。

主网络设备 (2)   黑名单 (1)				搜索
终端名称	终端类型	MAC地址	移出黑名单	
iQOO-Neo3	手机	06:1A:39:DF:60:38	移出	

## 3.6 查看流量统计



“流量统计”功能默认关闭，开启后可能会影响路由器性能。

进入页面：[登录路由器 Web 管理页面](#)，进入「系统」页面。

在这里，您可以打开“流量统计”开关，然后根据页面提示操作。开启流量统计功能后，您可以查看连接到路由器的用户下载数据的总量。

主网络设备 (14)   黑名单 (0)										搜索	流量统计: <input type="checkbox"/>
终端名称	终端类型	备注	IP地址	MAC地址	在线时长	实时上传	实时下载 ↓	状态	操作		
MININT-STOHTLC	其他	-	192.168.0.125	94:C6:91:29:C2:1A	9分钟	0KB/s	2KB/s	在线	限速 禁止上网		
W18EV2.0	路由器	-	192.168.0.194	C8:3A:35:45:87:9B	18小时 43分钟	0KB/s	0KB/s	在线	限速 禁止上网		
iQOO-10	手机	-	192.168.0.30	A4:90:CE:93:D5:DA	0分钟	0KB/s	0KB/s	离线	限速 禁止上网		
3fe2fecf-8312-4dfe-ae0f-c1f958714b20	手机	-	192.168.0.146	52:2B:54:1F:D6:66	0分钟	0KB/s	0KB/s	离线	限速 禁止上网		
HONOR_30-8f22ce4732ac6953	手机	-	192.168.0.156	F2:B7:72:EA:F5:B5	0分钟	0KB/s	0KB/s	离线	限速 禁止上网		

↓

主网络设备 (14)   黑名单 (0)										搜索	流量统计: <input checked="" type="checkbox"/>
终端名称	终端类型	备注	IP地址	MAC地址	在线时长	实时上传	实时下载 ↓	下载总量	状态	操作	
iQOO-10	手机	-	192.168.0.30	A4:90:CE:93:D5:DA	2分钟	2KB/s	45KB/s	467.98KB	在线	限速 禁止上网	
MININT-STOHTLC	其他	-	192.168.0.125	94:C6:91:29:C2:1A	11分钟	0KB/s	1KB/s	1015.02KB	在线	限速 禁止上网	
W18EV2.0	路由器	-	192.168.0.194	C8:3A:35:45:87:9B	18小时 45分钟	0KB/s	0KB/s	7.95MB	在线	限速 禁止上网	
3fe2fecf-8312-4dfe-ae0f-c1f958714b20	手机	-	192.168.0.146	52:2B:54:1F:D6:66	0分钟	0KB/s	0KB/s	29.88MB	离线	限速 禁止上网	
HONOR_30-8f22ce4732ac6953	手机	-	192.168.0.156	F2:B7:72:EA:F5:B5	0分钟	0KB/s	0KB/s	2.92MB	离线	限速 禁止上网	

# 4 联网设置

## 4.1 联网设置

### 4.1.1 概述

通过联网设置，可以实现局域网多台设备共享您办理的宽带服务上网（IPv4）。

首次使用路由器或将路由器恢复出厂设置后，请根据设置向导完成联网设置。之后，如果要修改或设置更多联网参数，可在本模块设置。

### 4.1.2 设置 WAN 口个数

进入页面：[登录路由器 Web 管理页面](#)，点击「网络」>「联网设置」，找到“WAN 口个数”模块。

在这里，您可以查看 WAN 口的速率类型，设置 WAN 口个数，查看各网口的连接状态及属性。



#### 参数说明

标题项	说明
接口	路由器 WAN 口的速率类型。

标题项	说明
WAN 口个数	路由器 WAN 口的个数。您可以根据需要修改 WAN 口个数。
端口状态	<p>路由器各网口的类型与连接状态。</p> <p>绿色表示接口连接正常。灰色表示接口未连接设备或连接异常。</p>

## 4.1.3 设置联网

### 概述

进入页面：[登录路由器 Web 管理页面](#)，点击「网络」>「联网设置」，找到“连接设置”模块。

在这里，您可以设置 WAN 口的联网参数。路由器的联网方式支持[宽带拨号](#)、[动态 IP](#)、[静态 IP](#)。



- 下文以 WAN1 设置为例，其他 WAN 口的设置与 WAN1 方法类似。
- 各上网参数均由宽带服务商提供，如不清楚，请咨询您的宽带服务商。

### 宽带拨号

路由器使用宽带服务商提供的宽带账号和密码拨号上网。

设置步骤：

**步骤 1** [登录路由器 Web 管理页面](#)，点击「网络」>「联网设置」。

**步骤 2** 在“连接设置”模块，选择“联网方式”为“宽带拨号”。

**步骤 3** 输入宽带服务商提供的“宽带账号”和“宽带密码”。

**步骤 4** 点击 **连接**。

联网方式

宽带拨号

宽带账号

宽带密码

...

服务器名

若没有，可不填

服务名

若没有，可不填

首选DNS

.

.

.

(可选)

备用DNS

.

.

.

(可选)

联网状态

联网中...

连接

断开

---完成

稍等片刻，当联网状态显示“认证成功”时，您可以尝试上网了。

如果您不能上网，可以进入「更多」>「高级路由」>「WAN 口参数」页面，尝试修改 [WAN 口参数](#) 解决问题。

参数说明

标题项	说明
宽带账号	宽带服务商提供的宽带账号/密码。
宽带密码	
服务器名	PPPoE 服务器的名称（Server name），也叫 AC name。用于路由器验证 PPPoE 服务器合法性。 <div><div></div>注意</div> 如果宽带服务商未提供，请勿填写，否则可能会导致拨号失败。



标题项	说明
服务名	<p>PPPoE 服务的名称（Service name）。用于 PPPoE 服务器验证路由器的合法性。</p> <p> 注意</p> <p>如果宽带服务商未提供，请勿填写，否则可能会导致拨号失败。</p>
首选 DNS	设置 WAN 口的首选/备用 DNS 服务器地址。
备用 DNS	当自动获取的 DNS 服务器无法正常解析网址时，您可以在此处手动指定一个正确的首选/备用 DNS 服务器。
联网状态	<p>显示路由器 WAN 口的连接状态。</p> <ul style="list-style-type: none"> <li>- 认证成功：路由器 WAN 口已获得 IPv4 地址信息并联网正常。</li> <li>- 联网中...：路由器正在连接到上级网络设备。</li> <li>- 未联网/联网失败：未连接或连接失败，请检查网线连接状态、联网信息设置或咨询相应宽带服务商。</li> </ul> <p>如果显示其他状态信息，请根据联网状态提示信息采取相应措施。</p>

## 动态 IP

路由器使用宽带服务商动态分配的 IP 地址信息上网。

设置步骤：

**步骤 1** [登录路由器 Web 管理页面](#)，点击「网络」>「联网设置」。

**步骤 2** 在“连接设置”模块，选择“联网方式”为“动态 IP”。

**步骤 3** 点击 **连接**。



该截图展示了路由器的“联网设置”界面。界面包含以下元素：

- 联网方式**：下拉菜单，当前选择“动态IP”，右侧有一个向下的箭头。
- 首选DNS**：输入框，显示三个点“.”，右侧标注“(可选)”。
- 备用DNS**：输入框，显示三个点“.”，右侧标注“(可选)”。
- 联网状态**：显示为“联网中...”。
- 底部有两个按钮：**连接**（蓝色背景，白色文字）和**断开**（白色背景，灰色文字）。

---完成

稍等片刻，当联网状态显示“已联网”时，您可以尝试上网了。

如果您不能上网，可以进入「更多」>「高级路由」>「WAN 口参数」页面，尝试修改 [WAN 口参数](#) 解决问题。

参数说明

标题项	说明
首选 DNS	设置 WAN 口的首选/备用 DNS 服务器地址。
备用 DNS	当自动获取的 DNS 服务器无法正常解析网址时，您可以在此处手动指定一个正确的首选/备用 DNS 服务器。

静态 IP

路由器使用宽带服务商提供的固定 IP 地址、子网掩码、默认网关、DNS 服务器信息上网。

设置步骤：

- 步骤 1** 登录[路由器 Web 管理页面](#)，点击「网络」>「联网设置」。
- 步骤 2** 在“连接设置”模块，选择“联网方式”为“静态 IP”。
- 步骤 3** 输入宽带服务商提供的“IP 地址”、“子网掩码”、“默认网关”和“首选/备用 DNS”。
- 步骤 4** 点击 [连接](#)。

联网方式

静态IP

IP地址

192 . 168 . 96 . 48

子网掩码

255 . 255 . 255 . 0

默认网关

192 . 168 . 96 . 1

首选DNS

192 . 168 . 108 . 110

备用DNS

192 . 168 . 108 . 108

(可选)

联网状态

联网中...

连接


断开

---完成

稍等片刻，当联网状态显示“已联网”时，您可以尝试上网了。

如果您不能上网，可以进入「更多」>「高级路由」>「WAN 口参数」页面，尝试修改 [WAN 口参数](#) 解决问题。

参数说明

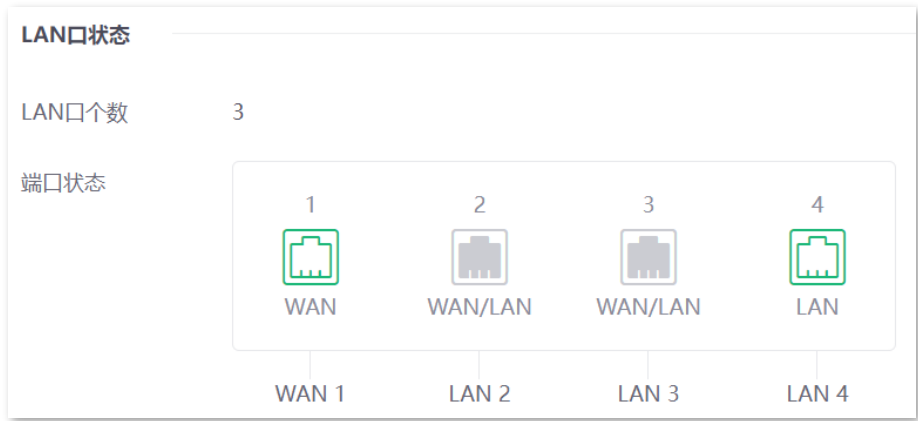
标题项	说明
IP 地址	
子网掩码	宽带服务商提供的“IP 地址”、“子网掩码”、“默认网关”和“首选/备用 DNS”。
默认网关	 提示
首选 DNS	如果宽带服务商只提供一个 DNS 服务器地址，“备用 DNS”可不填。
备用 DNS	

## 4.2 LAN 口设置

### 4.2.1 查看 LAN 口状态

进入页面：[登录路由器 Web 管理页面](#)，点击「网络」>「LAN 口设置」，找到“LAN 口状态”模块。

在这里，您可以查看路由器的 LAN 口个数、各网口的连接状态与属性。



参数说明

标题项	说明
LAN 口个数	路由器 LAN 口的个数。
端口状态	路由器各网口的类型与连接状态。 绿色表示接口连接正常。灰色表示接口未连接设备或连接异常。

## 4.2.2 LAN 口 IP 设置

一般情况下,您无需修改 LAN 口设置。当局域网内有其它网络管理设备的 IP 地址需要设置为 192.168.0.X。您可以修改 LAN 口 IP 地址和 192.168.0.X 不在同一网段。



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

进入页面：[登录路由器 Web 管理页面](#)，点击「网络」>「LAN 口设置」，找到“IP 地址设置”模块。

在这里，您可以设置路由器 LAN 口的 IPv4 地址相关信息。

IP地址设置

IP地址

192 . 168 . 0 . 1

子网掩码

255 . 255 . 255 . 0

MAC地址

00:90:4C:88:88:88

### 参数说明

标题项	说明
IP 地址	<div>路由器 LAN 口的 IPv4 地址，即路由器对局域网的 IPv4 地址，也是路由器的管理 IPv4 地址。连接到路由器 LAN 口的设备可以通过 http 或 https 协议（默认为 http）访问该 IPv4 地址登录路由器的 Web 管理页面。默认为 192.168.0.1。</div> <div><div>提示</div><div>遇到 IP 地址冲突，如：路由器获得的 WAN 口 IP 和其 LAN 口 IP 处于同一网段，LAN 口 IP 网段会自动加 1，变更为 192.168.1.1。</div></div>
子网掩码	路由器 LAN 口的子网掩码，默认为 255.255.255.0。
MAC 地址	路由器 LAN 口的 MAC 地址。

## 4.2.3 DHCP 服务器

DHCP 服务器能自动给局域网用户设备分配 IP 地址、子网掩码、网关地址和 DNS 等上网信息。

如果关闭此功能，需要在局域网用户设备上手动配置 IP 地址信息才能上网。如无特殊情况，请保持 DHCP 服务器为开启状态。

进入页面：[登录路由器 Web 管理页面](#)，点击「网络」>「LAN 口设置」，找到“DHCP 服务器设置”模块。  
在这里，您可以设置路由器 LAN 口的 DHCP 服务器。

DHCP服务器设置

DHCP服务器开关

客户端起始IP地址

192 . 168 . 0 . 2

客户端结束IP地址

192 . 168 . 0 . 254

租约时间

30

分钟

首选DNS

192 . 168 . 0 . 1

备用DNS

. . .

(可选)

参数说明

标题项	说明
DHCP 服务器开关	开启/关闭 DHCP 服务器功能。
客户端起始 IP 地址	DHCP 服务器可分配给局域网用户设备的 IP 地址范围。起始 IP 地址默认为 192.168.0.2，结束 IP 地址默认为 192.168.0.254。
客户端结束 IP 地址	
租约时间	<p>DHCP 服务器分配给局域网用户设备的 IP 地址的有效时间，默认为 30 分钟。</p> <p>当地址到期后：</p> <ul style="list-style-type: none"><li>- 如果设备仍连接在路由器上，设备将自动续约，继续占用该 IP 地址。</li><li>- 如果设备未连接（关机、网线已拔掉、无线已断开等）到路由器，路由器将释放该 IP 地址。以后若有其它设备请求 IP 地址信息，路由器可将该 IP 地址分配给其它设备。</li></ul> <p>如无特殊需要，建议保持默认设置。</p>
首选 DNS	<p>DHCP 服务器分配给局域网用户设备的首选 DNS 服务器 IP 地址。本路由器支持 DNS 代理功能，故首选 DNS 默认为路由器的 LAN 口 IP 地址。</p> <div><div></div><div>提示</div></div> <p>一般情况下，建议保持默认设置。如需修改，为了使局域网设备能够正常上网，请务必确保您设置的首选 DNS 是正确的 DNS 服务器或 DNS 代理的 IP 地址。</p>

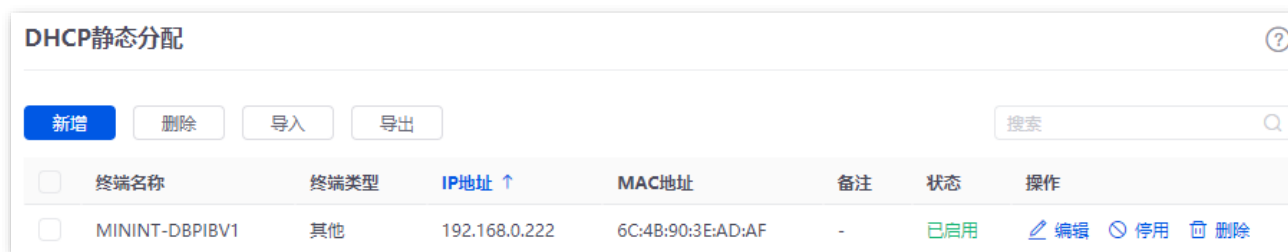
标题项	说明
备用 DNS	DHCP 服务器分配给局域网用户设备的备用 DNS 服务器 IP 地址。不填表示 DHCP 服务器不分配此项。

## 4.3 DHCP 静态分配

通过 DHCP 静态分配功能，您可以让指定局域网用户设备始终获得预设的 IP 地址，避免“行为管理”、“网速控制”、“端口映射”等基于 IP 地址生效的功能因局域网用户设备 IP 地址变化而失效。

进入页面：[登录路由器 Web 管理页面](#)，点击「网络」>「DHCP 静态分配」。

在这里，您可以手动设置局域网用户设备的 IP 地址，使 DHCP 服务器始终给同一局域网用户设备分配固定的 IP 地址。



### 参数&按钮说明

标题项	说明
新增	新增 DHCP 静态分配规则。
删除	删除选中的 DHCP 静态分配规则。
导入	将之前备份的 DHCP 静态分配表文件（.csv 格式文件）导入到路由器。
导出	<p>将 DHCP 静态分配表以.csv 文件格式导出到本地。</p> <p> <b>提示</b></p> <p>如果您要修改导出的文件，需要将该文件以 txt 格式打开。</p>
终端名称	局域网用户设备的名称。
终端类型	局域网用户设备的类型，如果识别不到，则显示“其他”。
IP 地址	为对应 MAC 地址的局域网用户设备固定分配的 IP 地址。

标题项	说明
MAC 地址	局域网用户设备的 MAC 地址。MAC 地址格式示例：00:23:24:E8:14:5A、00-23-24-E8-14-5A 或 002324E8145A。
备注	DHCP 静态分配规则的备注信息。
状态	<ul style="list-style-type: none"><li>- 已启用：该 DHCP 静态分配规则生效。</li><li>- 已停用：该 DHCP 静态分配规则停用。</li><li>- 已失效：该 DHCP 静态分配规则失效。</li></ul>

# 5 无线设置

## 5.1 无线网络设置

进入页面：[登录路由器 Web 管理页面](#)，点击「无线」>「无线网络设置」。

在这里，您可以设置路由器主无线网络个数与无线基本参数，包括修改无线名称、设置无线密码等。

### 无线网络设置

---

#### 无线名称与密码

无线网络个数

1

无线网络1

#### 连接设置

无线名称

Tenda

安全性

WPA-PSK/WPA2-PSK

无线密码

.....

与其它无线网络隔离

☐ 开启 ☒ 关闭

最大接入设备数

40

双频合一

☒



## 参数说明

标题项	说明
无线网络个数	设置开启路由器主无线网络的个数。路由器支持 3 个主无线网络，默认只开启 1 个主无线网络。
无线名称	路由器的主无线网络名称。
安全性	<p>主无线网络的加密方式。</p> <ul style="list-style-type: none"> <li>- 不加密：不加密无线网络，用户连接无线网络时，无需输入密码即可接入。为保障网络安全，不建议选择此项。</li> <li>- WPA-PSK：无线网络采用 WPA-PSK 认证方式（AES 加密规则），此加密方式的兼容性比 WPA2-PSK 好。</li> <li>- WPA2-PSK：无线网络采用 WPA2-PSK 认证方式（AES 加密规则），此加密方式的安全等级比 WPA-PSK 高。</li> <li>- WPA-PSK/WPA2-PSK：同时兼容 WPA-PSK、WPA2-PSK 两种安全模式。</li> </ul>
无线密码	主无线网络密码。为了无线网络安全，强烈建议设置无线密码。
与其它无线网络隔离	开启后，连接到该无线网络的用户与连接到路由器其他无线网络的用户之间不能互相通信，可增强无线网络的安全性。
最大接入设备数	<p>主无线网络最多允许接入的无线设备数量。</p> <p>若接入无线网络的无线设备达到此值，除非某些设备断开连接，否则新的无线设备不能接入该无线网络。</p>
双频合一	<p>开启/关闭双频合一功能。</p> <ul style="list-style-type: none"> <li>- 开启：路由器 2.4GHz 和 5GHz 主无线网络的无线名称与密码相同，只显示 1 个无线名称。用户连接路由器无线网络时，将会自动连接到网络质量最好的无线网络信号。</li> <li>- 关闭：单独设置 2.4GHz 和 5GHz 主无线网络信息。</li> </ul>

## 5.2 访客网络

进入页面：[登录路由器 Web 管理页面](#)，点击「无线」>「访客网络」。

在这里，您可以设置访客网络基本参数，包括开启/关闭访客网络、修改无线名称、设置无线密码等。接入到访客网络的客户端只能访问互联网和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和主网络局域网。可以满足客人上网需求，同时也确保主网络安全。

访客网络默认关闭，开启后，页面显示如下。

访客网络

访客网络状态

☒

开启

☐

关闭

访客网络设置

无线名称

Tenda\_Guest

安全性

不加密

▼

无线密码

.....

👁

双频合一

☒

访客网络LAN口IP

IP地址

192 . 168 . 168 . 1

子网掩码

255 . 255 . 255 . 0

访客网络带宽限制

共享上传速率

不限速

▼

共享下载速率

不限速

▼

最大接入设备数

40

ⓘ

## 参数说明

标题项	说明
访客网络状态	开启/关闭访客网络。
访客网络设置	路由器访客网络的无线名称。  <b>提示</b> 为了区别于路由器主网络的无线名称，建议不要将访客网络的无线名称与路由器主网络的无线名称设置成一样。
	安全性 访客网络的 <a href="#">加密方式</a> 。
	无线密码 访客网络的无线密码。
	双频合一 开启/关闭双频合一功能。 - 开启：路由器 2.4GHz 访客网络和 5GHz 访客网络的无线名称一致，只显示 1 个无线名称。用户连接路由器访客网络时，将会自动连接到网络质量最好的无线网络信号。 - 关闭：单独设置 2.4GHz 访客网络和 5GHz 访客网络信息。
访客网络 LAN 口 IP	IP 地址 访客网络 IP 地址默认为 192.168.168.1，无线设备连接访客网络后，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 访客网络的子网掩码，用于定义访客网络的地址空间。
访客网络带宽限制	共享上传速率 设置访客网络上行/下行速度的上限值。
	共享下载速率
	最大接入设备数 访客网络最多允许接入的无线设备数量。 若接入访客网络的无线设备达到此值，除非某些设备断开连接，否则新的无线设备不能接入该访客网络。

## 5.3 无线访问控制

### 5.3.1 设置无线访问控制规则

进入页面：[登录路由器 Web 管理页面](#)，点击「无线」>「无线访问控制」。

在这里，您可以通过设置无线访问控制规则，允许或禁止指定设备连接到路由器对应的主无线网络。无线访问控制功能默认关闭，开启后，页面显示如下。

无线访问控制

无线访问控制

开启

关闭

MAC地址过滤

无线名称

MAC地址过滤

Tenda

关闭

Tenda

关闭

Tenda

关闭

保存

无线访问控制列表

新增

删除

搜索

MAC地址

备注

生效网络 ↑

状态

操作

#### 参数说明

标题项	说明
无线访问控制	开启/关闭无线访问控制功能。默认关闭。
无线名称	路由器主无线网络的名称。
MAC 地址过滤	MAC 地址过滤规则。 <ul style="list-style-type: none"><li>- 关闭：该无线网络不启用 MAC 地址过滤功能，允许所有无线客户端连接。</li><li>- 仅允许：仅允许无线访问控制列表中指定的无线客户端连接到该无线网络。</li><li>- 仅禁止：仅禁止无线访问控制列表中指定的无线客户端连接到该无线网络，其他无线客户端可以连接到该无线网络。</li></ul>

标题项	说明
<div>新增</div>	新增无线访问控制规则。
<div>删除</div>	删除选中的无线访问控制规则。
MAC 地址	无线客户端的 MAC 地址。
备注	MAC 地址的备注信息。
无线访问控制列表	生效网络
	规则对应的无线网络。
	状态
	规则的状态。
操作	可对规则进行如下操作：
	- 点击 <a href="#">编辑</a> 可以修改规则。
	- 点击 <a href="#">停用/启用</a> 可以停用/启用规则。
	- 点击 <a href="#">删除</a> 可以删除规则。

## 5.3.2 无线访问控制配置举例

### 组网需求

某企业使用企业级无线路由器进行网络搭建。

要求：仅允许某一采购人员连接路由器无线网络（caigou）访问互联网，其他员工禁止连接。

### 方案设计

可以使用路由器的无线访问控制功能实现上述需求。假设该采购人员电脑的物理地址为 CC:3A:61:71:1B:6E。

### 配置步骤

**步骤 1** 进入配置页面。

1. [登录路由器 Web 管理页面](#)。
2. 点击「无线」>「无线访问控制」。

**步骤 2** 开启无线访问控制功能。

1. 选择“无线访问控制”为“开启”。
2. 点击 

保存

。

无线访问控制

无线访问控制

☒ 开启
☐ 关闭

### 步骤 3 设置 MAC 地址过滤模式。

1. 选择无线网络“caigou”的“MAC 地址过滤”模式，本例为“仅允许”。
2. 点击 **保存**。

无线名称	MAC地址过滤
caigou	仅允许
Tenda	关闭
Tenda	关闭

**保存**

### 步骤 4 添加无线访问控制规则。

1. 点击 **新增**。

无线访问控制列表

新增

删除

搜索

☐ MAC地址
备注
生效网络 ↑
状态
操作

2. 在【新增】窗口进行如下配置，然后点击 **保存**。
  - (1) 输入采购人员电脑的 MAC 地址（物理地址），本例为“CC:3A:61:71:1B:6E”。
  - (2) （可选）设置本规则的备注，如“采购”。
  - (3) 选择规则生效的无线网络，本例为“caigou”。

新增

MAC地址

CC:3A:61:71:1B:6E

备注

采购

(可选)

生效网络

caigou

▼

取消

保存

无线访问控制规则添加成功，如下图示。

无线访问控制列表

新增

删除

搜索

<input type="checkbox"/>	MAC地址	备注	生效网络 ↑	状态	操作
<input type="checkbox"/>	CC:3A:61:71:1B:6E	采购	caigou	已启用	<a href="#">编辑</a> <a href="#">停用</a> <a href="#">删除</a>

----完成

## 验证配置

只有 MAC 地址为 CC:3A:61:71:1B:6E 的无线设备可以接入无线网络“caigou”，其他设备无法连接到该网络。

## 5.4 无线高级设置

进入页面：[登录路由器 Web 管理页面](#)，点击「无线」>「无线高级设置」。

在这里，您可以设置无线高级参数，包括发射功率、网络模式、信道、信道带宽等。

无线高级设置

2.4GHz网络

5GHz网络

2.4GHz网络

开启

关闭

国家或地区

中国

网络模式

11b/g/n

发射功率

26 dBm

信道带宽

20MHz

信道

自动

接入信号强度限制

-95 dBm

部署模式

强覆盖

空口调度

开启

关闭

Short GI

开启

关闭

客户端老化时间

10 分钟

强制速率

全选

1M

2M

5.5M

6M

9M

11M

12M

18M

24M

36M

48M

54M

支持速率

全选

1M

2M

5.5M

6M

9M

11M

12M

18M

24M

36M

48M

54M

保存

### 参数说明

标题项	说明
2.4GHz/5GHz 网络	开启/关闭对应无线频段的无线功能。
国家或地区	选择路由器当前所在的国家或地区，以适应不同国家或地区对信道及发射功率的管制要求。



标题项	说明
网络模式	<p>路由器对应频段的无线网络模式。</p> <p>2.4GHz 包括 11b、11g、11b/g、11b/g/n，默认工作在 11b/g/n。</p> <ul style="list-style-type: none"> <li>- 11b：路由器工作在 802.11b 无线网络模式下。</li> <li>- 11g：路由器工作在 802.11g 无线网络模式下。</li> <li>- 11b/g：路由器工作在 802.11b、802.11g 无线网络模式下。</li> <li>- 11b/g/n：路由器工作在 802.11b、802.11g、802.11n 无线网络模式下。</li> </ul> <p>5GHz 包括 11a、11a/n、11a/n/ac，默认工作在 11a/n/ac。</p> <ul style="list-style-type: none"> <li>- 11a：路由器工作在 802.11a 无线网络模式下。</li> <li>- 11a/n：路由器工作在 802.11a、802.11n 无线网络模式下。</li> <li>- 11a/n/ac：路由器工作在 802.11a、802.11n、802.11ac 无线网络模式下。</li> </ul>
发射功率	<p>路由器对应频段的无线发射功率。</p> <p>发射功率越大，无线覆盖范围越广。但适当减少发射功率更有助于提高无线网络的性能和安全性。</p>
信道带宽	<p>路由器无线信道的频带宽度。高信道带宽下，更容易获得较高的传输速率，但穿透性稍差，传输距离近。</p> <ul style="list-style-type: none"> <li>- 20MHz：路由器使用 20MHz 的信道带宽。</li> <li>- 40MHz：路由器使用 40MHz 的信道带宽。</li> <li>- 20MHz/40MHz：仅适用 2.4GHz，路由器根据周围环境，自动调整信道带宽为 20MHz 或 40MHz。</li> <li>- 80MHz：仅适用 5GHz，路由器使用 80MHz 的信道带宽。</li> </ul>
信道	<p>路由器无线数据传输的通道。可选择范围由当前选择的国家或地区、无线工作频段来决定。</p> <p>默认为“自动”，即路由器自动检测各信道利用率，并据此选择合适的工作信道。</p> <p>如果您连接路由器无线网络时，经常出现掉线、卡顿或网速慢的问题，请尝试修改路由器的信道。您可以通过工具软件（如 Wi-Fi 分析仪）检测周边较少用到、干扰较小的信道。</p>
接入信号强度限制	<p>设置路由器对应频段可接受的无线设备信号强度，信号强度低于此值的设备将无法接入路由器。</p>
5GHz 优先	<p>仅“5GHz 网络”支持。</p> <p>开启后，当 2.4GHz 和 5GHz 两个频段的无线名称（不能含中文字符）和密码都相同，且无线客户端支持双频 Wi-Fi 时，客户端优先从 5GHz 频段接入路由器无线网络。</p>
5GHz 优先阈值	<p>开启“5GHz 优先”时，如果路由器在 5GHz 频段接收到的终端信号强度大于此阈值，则让该终端优先连接路由器的 5GHz 信号；如果小于此阈值，则让该终端连接路由器的 2.4GHz 信号。</p>

标题项	说明
部署模式	<p>仅“2.4GHz 网络”支持，根据路由器的实际应用场景，选择部署模式。</p> <ul style="list-style-type: none"> <li>- 强覆盖：适用于大面积、多墙体穿透、用户分散、周围无线信号少于 10 个的环境。</li> <li>- 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、周围无线信号超过 25 个的环境。</li> </ul>
空口调度	<p>开启/关闭空口调度功能。</p> <p>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太多无线空口资源的问题，提升路由器的整体效率，有效保障了吞吐量。</p>
Short GI	<p>短保护间隔。仅“2.4GHz 网络”支持。</p> <p>无线信号在空间传输时会因多径等因素在接收侧形成时延，如果后面的数据块发送过快，会对前一个数据块形成干扰，短保护间隔可以用来规避这个干扰。开启 Short GI 时，可提高无线吞吐量。</p>
APSD	<p>自动省电模式。仅“5GHz 网络”支持。</p> <p>APSD 是 Wi-Fi 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。</p>
客户端老化时间	<p>客户端连接到路由器的无线网络后，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。</p>
强制速率	<p>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，从而提升其他客户端的上网体验。</p> <ul style="list-style-type: none"> <li>- 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。</li> </ul>
支持速率	<ul style="list-style-type: none"> <li>- 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。</li> </ul>

# 6 网速控制

## 6.1 WAN 口带宽

进入页面：[登录路由器 Web 管理页面](#)，点击「网速」>「WAN 口带宽」。

在这里，您可以设置 WAN 口带宽参数，当网络设置为[多 WAN](#)时可以分别对多个 WAN 口设置带宽参数。

正确地配置 WAN 口带宽参数，可以获取更好的上网体验。

WAN口带宽

请填写运营商提供的带宽大小以获取更好的上网体验。

WAN1口

上行速率

1000

Mbps

下行速率

1000

Mbps

保存

### 参数说明

标题项	说明
上行速率	填入所办理的宽带的带宽值。不清楚时，可以咨询您的宽带服务商。
下行速率	

## 6.2 分组限速

### 6.2.1 设置分组限速

外网带宽总是有限的，所以网络管理员需要对用户进行网速控制，使有限的带宽资源得到合理分配，有效利用外网资源。

进入页面：[登录到路由器 Web 管理页面](#)，点击「网速」>「分组限速」。

在这里，您可以点击 **新增** 配置路由器的分组限速策略。通过分组进行网速控制，控制指定 IP 组内的用户在指定时间组内共享或独享所设置的上传/下载速率。

分组限速

新增

策略名称	备注	IP组	时间组	并发连接数 ↑	上传限速	下载限速	操作
------	----	-----	-----	---------	------	------	----

新增分组限速策略

策略名称

备注

(可选)

IP组

请先创建IP组

请跳转到【行为】-【IP组】页面先配置IP组

时间组

请先创建时间组

请跳转到【行为】-【时间组】页面先配置时间组

并发连接数

0

上传限速

0

KB/s

下载限速

0


KB/s

取消

保存

参数说明

标题项	说明
策略名称	分组限速策略的名称。
备注	分组限速策略的备注。
IP 组	分组限速策略生效的 IP 地址范围。需先在 <a href="#">IP 组</a> 页面配置好 IP 组策略。
时间组	分组限速策略生效的时间。需先在 <a href="#">时间组</a> 页面配置好时间组策略。
并发连接数	<div>受控 IP 地址范围中，每台用户设备所能使用的最大连接数。</div> <div> 提示</div> <div>0 表示不限制。</div>
上传限速	受控用户设备的共享最大上传/下载速率，每个受控设备所获得的带宽可能不一样。

标题项	说明
下载限速	 <b>提示</b> 0 表示不限速。
操作	可对规则进行如下操作： <ul style="list-style-type: none"> <li>- 点击<a href="#">编辑</a>可以修改规则。</li> <li>- 点击<a href="#">删除</a>可以删除规则。</li> </ul>

## 6.2.2 分组限速配置举例

### 组网需求

某企业使用企业级无线路由器进行网络搭建。

要求：局域网中采购部（IP 地址范围：192.168.0.2~192.168.0.50）的每位员工在星期一到星期五的上班时间（8:00~18:00）都能使用 10Mbps（1Mbps=128KB/s）的固定上下行带宽上网。对于局域网其他设备，不限制带宽。

### 方案设计

可以使用路由器网速控制功能中的“分组限速”功能实现上述需求。假设每台用户设备的并发连接数为 600。

### 配置步骤



**步骤 1** [登录路由器 Web 管理页面](#)。

**步骤 2** 配置时间组。

进入「行为」>「分组策略」>「时间组」页面，配置如下时间组。

新增时间组

策略名称

上班时间

时间段一

08:00 → 18:00

时间段二

开始时间 → 结束时间

(可选)

时间段三

开始时间 → 结束时间

(可选)

周期

☐ 每天

☒ 星期一

☒ 星期二

☒ 星期三

☒ 星期四

☒ 星期五

☐ 星期六

☐ 星期日

备注

(可选)

取消

保存

步骤 3 配置 IP 组。

点击「行为」>「分组策略」>「IP 组」，配置如下 IP 组。

新增IP组

策略名称

采购部

地址段一

192 . 168 . 0 . 2

~

192 . 168 . 0 . 50

地址段二

.

.

.

~

.

.

.

(可选)

地址段三

.

.

.

~

.

.

.

(可选)

备注

(可选)

取消

保存

步骤 4 添加分组限速规则。

分组限速策略参数示例如下所示。

策略名称：限速

并发连接数：600

IP 组：采购部

上传/下载限速：1280KB/s

时间组：上班时间

- 1. 点击「网速」>「分组限速」。
- 2. 点击 **新增**。
- 3. 配置分组限速策略相关参数，点击 **保存**。

分组限速

新增

策略名称	备注	IP组	时间组	并发连接数	上传限速	下载限速	操作
------	----	-----	-----	-------	------	------	----

新增分组限速策略

策略名称

限速

备注

(可选)

IP组

采购部

时间组

上班时间

并发连接数

600

上传限速

1280

KB/s

下载限速

1280

KB/s

取消

保存

----完成

验证配置

IP 地址在 192.168.0.2~192.168.0.250 范围内的用户，在星期一到星期五的 8:00~18:00 的最大上传速率为 1280KB/s，最大下载速率为 1280KB/s。

# 7 行为管理

## 7.1 分组策略

您在配置 MAC 地址过滤、IP 地址过滤、端口过滤、网站过滤、分组限速和自定义多 WAN 策略等基于 IP 组或时间组生效的功能时，需要先配置好相应的 IP 组和/或时间组。

### 7.1.1 时间组

进入页面：[登录到路由器 Web 管理页面](#)，点击「行为」>「分组策略」>「时间组」。

在这里，您可以点击 **新增** 配置时间组策略。

时间组

新增

策略名称	时间段	周期	备注	操作

新增时间组

策略名称

时间段一

开始时间 → 结束时间

时间段二

开始时间 → 结束时间

(可选)

时间段三

开始时间 → 结束时间

(可选)

周期

☐ 每天
 ☐ 星期一
 ☐ 星期二
 ☐ 星期三
 ☐ 星期四
 ☐ 星期五
 ☐ 星期六
 ☐ 星期日

备注

(可选)

取消

保存



参数说明

标题项	说明
策略名称	时间组策略的名称。
时间段	当前时间组策略包含的时间段。最多包含三个时间段，时间段之间不能重复。
周期	时间组生效的日期。
备注	时间组策略的备注信息。
操作	可对规则进行如下操作： <ul style="list-style-type: none"><li>- 点击<a href="#">编辑</a>可以修改规则。</li><li>- 点击<a href="#">删除</a>可以删除规则。</li></ul>

7.1.2 IP 组

进入页面：[登录到路由器 Web 管理页面](#)，点击「行为」>「分组策略」>「IP 组」。

在这里，您可以点击 [新增](#) 配置 IP 组策略。

IP组

新增

策略名称	IP地址段	备注	操作
------	-------	----	----

新增IP组

策略名称

地址段一

~

地址段二

~

(可选)

地址段三

~

(可选)

备注

(可选)

取消

保存

参数说明

标题项	说明
策略名称	IP 组策略的名称。
IP 地址段	当前 IP 组策略包含的 IP 地址段。最多包含三个 IP 地址段，地址段之间不能重复。
备注	IP 组策略的备注信息。
操作	<p>可对规则进行如下操作：</p> <ul style="list-style-type: none"><li>- 点击<a href="#">编辑</a>可以修改规则。</li><li>- 点击<a href="#">删除</a>可以删除规则。</li></ul>

## 7.2 上网过滤

### 7.2.1 IP 过滤

#### 设置 IP 过滤


进入页面：[登录到路由器 Web 管理页面](#)，点击「行为」>「上网过滤」>「IP 过滤」。

在这里，您可以通过配置 IP 地址过滤策略来允许或禁止局域网主机连接到本路由器上网。



#### 参数说明

标题项	说明
	IP 地址的过滤模式。
过滤策略	<ul style="list-style-type: none"><li>- 黑名单（禁止访问互联网）：指定 IP 地址的用户在对应时间段内禁止访问互联网，在其他时间段内可以访问互联网。</li><li>- 白名单（允许访问互联网）：指定 IP 地址的用户在对应时间段内可以访问互联网，在其他时间段内不可以访问互联网。</li></ul>
IP 地址策略	若需要过滤某一个 IP 地址，“IP 地址策略”选择“IP 地址”并输入 IP 地址；如果需要过滤一个或几个 IP 地址段，“IP 地址策略”选择“IP 地址组”并选择对应的 IP 组策略即可。
IP 地址或 IP 组	IP 地址组策略应事先在 <a href="#">IP 组</a> 页面配置好。
时间组	<p>选择时间组策略，指定 IP 地址过滤策略生效的时间。</p> <p>时间组策略应事先在 <a href="#">时间组</a> 页面配置好。</p>
备注	IP 地址过滤策略的备注信息。
状态	IP 地址过滤策略的状态。

标题项	说明
	可对策略进行如下操作：
操作	<ul style="list-style-type: none"> <li>- 点击<a href="#">编辑</a>可以修改策略。</li> <li>- 点击<a href="#">停用/启用</a>可以停用或启用策略。</li> <li>- 点击<a href="#">删除</a>可以删除策略。</li> </ul>
允许列表外的主机 或设备访问互联网	<ul style="list-style-type: none"> <li>- 勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都可以访问互联网。</li> <li>- 未勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都不能访问互联网。</li> </ul> <div>  <b>注意</b> </div> <p>只有配置了白名单后才能取消勾选。</p>

## IP 过滤配置举例

### 组网需求

某企业使用企业级无线路由器进行网络搭建。

要求：上班时间（星期一到星期五的 8:00~18:00），仅允许采购部门人员访问互联网，其他员工禁止访问互联网。

### 方案设计

可以使用路由器的 IP 过滤功能实现上述需求。假设采购部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.50。

### 配置步骤



**步骤 1** [登录路由器 Web 管理页面](#)。

**步骤 2** 配置时间组。

进入「行为」>「分组策略」>「时间组」页面，配置如下时间组。

新增时间组

策略名称

上班时间

时间段一

08:00 → 18:00

时间段二

开始时间 → 结束时间

(可选)

时间段三

开始时间 → 结束时间

(可选)

周期

每天

☒ 星期一

☒ 星期二

☒ 星期三

☒ 星期四

☒ 星期五

☐ 星期六

☐ 星期日

备注

(可选)

取消

保存

步骤 3 配置 IP 组。

进入「行为」>「分组策略」>「IP 组」页面，配置如下 IP 组。

新增IP组

策略名称

采购部

地址段一

192 . 168 . 0 . 2 ~ 192 . 168 . 0 . 50

地址段二

. . .

~

. . .

(可选)

地址段三

. . .

~

. . .

(可选)

备注

(可选)

取消

保存

步骤 4 添加 IP 过滤策略。

IP 过滤策略参数示例如下所示。

过滤策略：白名单（允许访问互联网）

IP 组：采购部

IP 地址策略：IP 地址组

时间组：上班时间

1.

点击「行为」>「上网过滤」>「IP 过滤」，然后点击 新增。
2.

配置 IP 过滤策略相关参数，点击 保存。

新增IP过滤策略

过滤策略

白名单（允许访问互联网）

IP地址策略

IP地址

IP地址组

IP组

采购部

时间组

上班时间

备注

(可选)

取消

保存

3. 去勾选“允许列表外的主机或设备访问互联网”，确认弹窗提示信息后，点击确定。

IP过滤

新增

删除

搜索

<input type="checkbox"/>	过滤策略	IP地址策略	IP地址或IP组	时间组	备注	状态	操作
<input type="checkbox"/>	白名单（允许访问互联网）	IP地址组	采购部	上班时间	-	已启用	<a href="#">编辑</a> <a href="#">停用</a> <a href="#">删除</a>
<input type="checkbox"/>	允许列表外的主机或设备访问互联网						

---完成

验证配置

星期一到星期五的 8:00~18:00，局域网中，只有使用 IP 地址在 192.168.0.2~192.168.0.50 范围内的电脑才能上网，使用其他电脑不能上网。

## 7.2.2 MAC 过滤

### 设置 MAC 过滤


进入页面：[登录到路由器 Web 管理页面](#)，点击「行为」>「上网过滤」>「MAC 过滤」。

在这里，您可以通过配置 MAC 地址过滤策略来允许和禁止局域网主机连接到本路由器上网。



#### 参数说明

标题项	说明
过滤策略	<p>MAC 地址的过滤模式。</p> <ul style="list-style-type: none"><li>- 黑名单（禁止访问互联网）：指定 MAC 地址的用户在对应时间段内禁止访问互联网，在其他时间段内可以访问互联网。</li><li>- 白名单（允许访问互联网）：指定 MAC 地址的用户在对应时间段内可以访问互联网，在其他时间段内不可以访问互联网。</li></ul>
MAC 地址	需要上网过滤的 MAC 地址。
时间组	<p>选择时间组策略，指定 MAC 地址过滤策略生效的时间。</p> <p>时间组策略应事先在<a href="#">时间组</a>页面配置好。</p>
备注	MAC 地址过滤策略的备注信息。
状态	MAC 地址过滤策略的状态。
操作	<p>可对策略进行如下操作：</p> <ul style="list-style-type: none"><li>- 点击<a href="#">编辑</a>可以修改策略。</li><li>- 点击<a href="#">停用/启用</a>可以停用或启用策略。</li><li>- 点击<a href="#">删除</a>可以删除策略。</li></ul>

标题项	说明
允许列表外的主机或设备访问互联网	<ul style="list-style-type: none"> <li>- 勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都可以访问互联网。</li> <li>- 未勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都不能访问互联网。</li> </ul> <div>  <b>注意</b> </div> <p>只有配置了白名单后才能取消勾选。</p>

## MAC 过滤配置举例

### 组网需求

某企业使用企业级无线路由器进行网络搭建。

要求：上班时间（星期一到星期五的 8:00~18:00），仅允许某一采购人员访问互联网，其他员工禁止访问互联网。

### 方案设计

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

### 配置步骤

配置时间组 > 添加 MAC 过滤策略

**步骤 1** [登录路由器 Web 管理页面](#)。

**步骤 2** 配置时间组。

点击「行为」>「分组策略」>「时间组」，配置如下时间组。



新增时间组

策略名称

上班时间

时间段一

08:00 → 18:00

时间段二

开始时间 → 结束时间

(可选)

时间段三

开始时间 → 结束时间

(可选)

周期

☐ 每天

☒ 星期一

☒ 星期二

☒ 星期三

☒ 星期四

☒ 星期五

☐ 星期六

☐ 星期日

备注

(可选)

取消

保存

步骤 3 添加 MAC 过滤策略。

MAC 地址过滤策略参数示例如下所示。

过滤策略：白名单（允许访问互联网）

MAC 地址：  
CC:3A:61:71:1B:6E

时间组：上班时间

1.

点击「行为」>「上网过滤」>「MAC 过滤」，然后点击 **新增**。
2.

配置 MAC 过滤策略相关参数，点击 **保存**。



如果您需要同时过滤多个 MAC 地址，MAC 地址之间请用“;”隔开。

新增MAC过滤策略

过滤策略

白名单（允许访问互联网）

MAC地址

CC:3A:61:71:1B:6E

时间组

上班时间

备注

(可选)

取消

保存

3.

去勾选“允许列表外的主机或设备访问互联网”，确认弹窗提示信息后，点击 **确定**。



---完成

### 验证配置

星期一到星期五的 8:00~18:00，局域网中，只有使用 MAC 地址为 CC:3A:61:71:1B:6E 的电脑才能上网，使用其他电脑不能上网。

## 7.2.3 端口过滤

### 设置端口过滤

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

进入页面：[登录路由器 Web 管理页面](#)，点击「行为」>「上网过滤」>「端口过滤」。

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



#### 参数说明

标题项	说明
IP 组	选择 IP 组策略，指定端口过滤策略生效的 IP 地址范围。 IP 组策略应事先在 <a href="#">IP 组</a> 页面配置好。
时间组	选择时间组策略，指定 MAC 地址过滤策略生效的时间。 时间组策略应事先在 <a href="#">时间组</a> 页面配置好。
端口	禁止访问的服务的端口。
协议	禁止访问的服务的协议。
备注	端口过滤策略的备注信息。
状态	MAC 地址过滤策略的状态。
操作	可对策略进行如下操作： <ul style="list-style-type: none"><li>- 点击 <a href="#">编辑</a> 可以修改策略。</li><li>- 点击 <a href="#">停用/启用</a> 可以停用或启用策略。</li><li>- 点击 <a href="#">删除</a> 可以删除策略。</li></ul>

## 端口过滤配置举例

### 组网需求

某企业使用企业级无线路由器进行网络搭建。

要求：上班时间（星期一到星期五的 8:00~18:00），禁止财务部门员工浏览网页（浏览网页服务默认的端口号是 80）。

### 方案设计

可以使用路由器的端口过滤功能实现上述需求。假设财务部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.50。

### 配置步骤

设置时间组

设置 IP 组

添加端口过滤策略

**步骤 1** [登录路由器 Web 管理页面](#)。

**步骤 2** 设置时间组。

进入「行为」>「分组策略」>「时间组」页面，配置如下时间组。



新增时间组

策略名称：上班时间

时间段一：08:00 → 18:00

时间段二：开始时间 → 结束时间 (可选)

时间段三：开始时间 → 结束时间 (可选)

周期：☐ 每天

☒ 星期一 ☒ 星期二 ☒ 星期三 ☒ 星期四

☒ 星期五 ☐ 星期六 ☐ 星期日

备注： (可选)

取消 保存

**步骤 3** 配置 IP 组。

进入「行为」>「分组策略」>「IP 组」页面，配置如下 IP 组。

新增IP组

策略名称

采购部

地址段一

192 . 168 . 0 . 2

~

192 . 168 . 0 . 50

地址段二

.

.

.

~

.

.

.

(可选)

地址段三

.

.

.

~

.

.

.

(可选)

备注

(可选)

取消

保存

步骤 4 添加端口过滤策略。

端口过滤策略参数示例如下所示。

IP 组：采购部

时间组：上班时间

端口：80

协议：TCP&UDP

1.

点击「行为」>「上网过滤」>「端口过滤」，然后点击 新增。
2.

配置端口过滤策略相关参数，点击 保存。



- 如果需要同时过滤多个不连续端口，端口号之间请用“;”隔开，如“80;20”。
- 如果需要过滤多个连续端口号，请用“~”表示，如“75~80”。

新增端口过滤策略

IP组

采购部

时间组

上班时间

端口

80

协议

TCP&UDP

备注

(可选)

取消

保存

---完成

验证配置

星期一到星期五的 8:00~18:00，局域网中，IP 地址在 192.168.0.2~192.168.0.50 范围内的电脑不能进行网页浏览服务。

## 7.2.4 URL 过滤

### 设置 URL 过滤


进入页面：[登录路由器 Web 管理页面](#)，点击「行为」>「上网过滤」>「URL 过滤」。

在这里，您可以允许或禁止用户访问指定网址，以规范局域网用户上网行为。



#### 参数说明

标题项	说明
	网址过滤模式。
过滤策略	<ul style="list-style-type: none"><li>- 黑名单（禁止访问互联网）：指定 IP 地址的用户在对应时间段内禁止访问指定网址，可以访问其他网址，在其他时间段内可以访问所有网址。</li><li>- 白名单（允许访问互联网）：指定 IP 地址的用户在对应时间段内可以访问指定网址，不可以访问其他网址，在其他时间段内可以访问所有网址。</li></ul>
IP 地址策略	如果需要过滤某一个 IP 地址，“IP 地址策略”选择“IP 地址”并输入 IP 地址；如果需要过滤一个或几个 IP 地址段，“IP 地址策略”选择“IP 地址组”并选择对应的 IP 组策略即可。
IP 地址或 IP 组	IP 地址组策略应事先在 <a href="#">IP 组</a> 页面配置好。
时间组	<p>选择时间组策略，指定网址过滤策略生效的时间。</p> <p>时间组策略应事先在 <a href="#">时间组</a> 页面配置好。</p>
URL 关键词	禁止/允许访问的网址关键词。
备注	网址过滤策略的备注信息。
状态	网址过滤策略的状态。

标题项	说明
	可对策略进行如下操作：
操作	<ul style="list-style-type: none"> <li>- 点击<a href="#">编辑</a>可以修改策略。</li> <li>- 点击<a href="#">停用/启用</a>可以停用或启用策略。</li> <li>- 点击<a href="#">删除</a>可以删除策略。</li> </ul>
允许列表外的主机 或设备访问互联网	<ul style="list-style-type: none"> <li>- 勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都可以访问指定网址。</li> <li>- 未勾选：列表中“已停用”策略对应的设备，以及不在列表中的设备，都不能访问指定网址。</li> </ul> <div>  <b>注意</b> </div> <p>只有配置了白名单后才能取消勾选。</p>

## URL 过滤配置举例

### 组网需求

某企业使用企业级无线路由器进行网络搭建。

要求：上班时间（星期一到星期五的 8:00~18:00），设计部门人员只能访问一些设计网站，如站酷（zcool.com.cn）、花瓣（huaban.com）、素材中国（sccnn.com）。其他人员不能访问互联网。

### 方案设计

可以使用路由器的 URL 过滤功能实现上述需求。假设设计部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.50。

### 配置步骤



**步骤 1** [登录路由器 Web 管理页面](#)。

**步骤 2** 配置时间组。

进入「行为」>「分组策略」>「时间组」页面，配置如下时间组。



新增时间组

×

策略名称

上班时间

时间段一

08:00 → 18:00

🕒

时间段二

开始时间 → 结束时间

🕒

(可选)

时间段三

开始时间 → 结束时间

🕒

(可选)

周期

☐ 每天
 ☒ 星期一
 ☒ 星期二
 ☒ 星期三
 ☒ 星期四
 ☒ 星期五
 ☐ 星期六
 ☐ 星期日

备注

(可选)

取消

保存

### 步骤 3 配置 IP 组。

进入「行为」>「分组策略」>「IP 组」页面，配置如下 IP 组。

编辑IP组

×

策略名称

设计部

地址段一

192 . 168 . 0 . 2 ~ 192 . 168 . 0 . 50

地址段二

.

.

.

~

.

.

.

(可选)

地址段三

.

.

.

~

.

.

.

(可选)

备注

(可选)

取消

保存

### 步骤 4 添加 URL 过滤策略。

URL 过滤策略参数示例如下所示。

过滤策略：白名单（允许访问互联网）

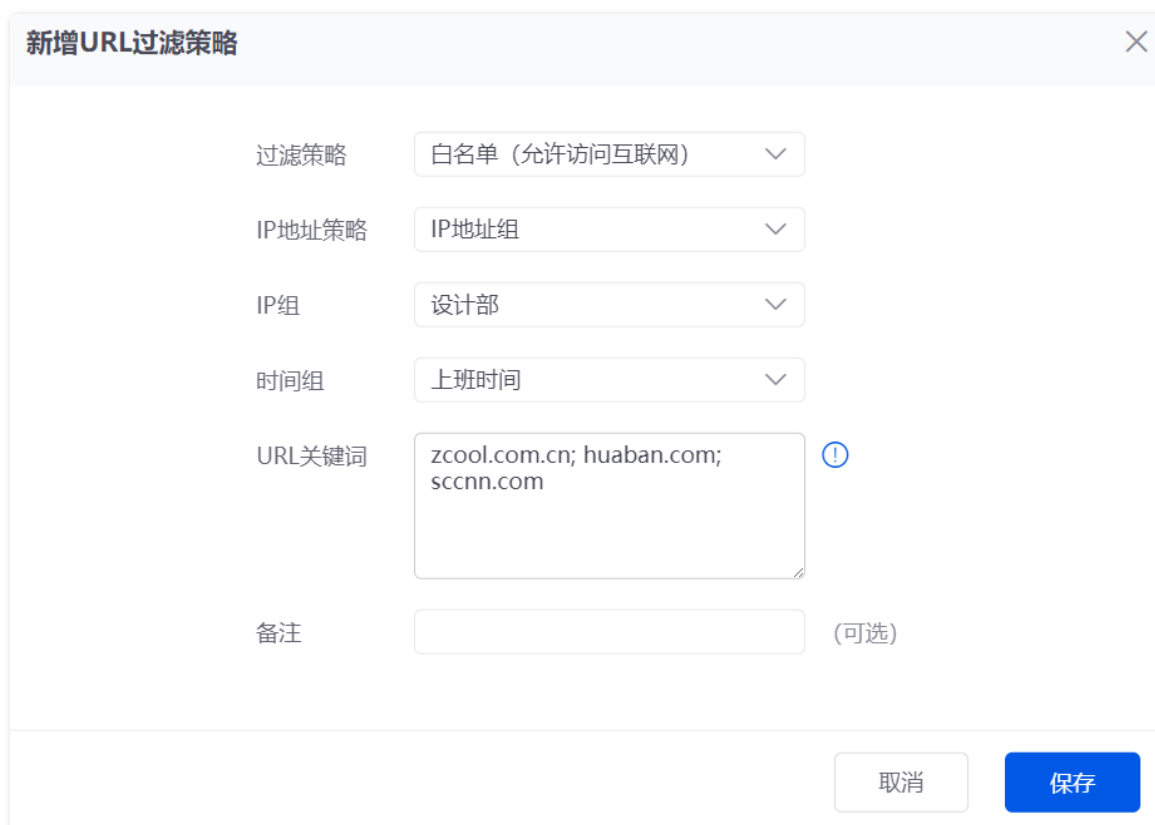
时间组：上班时间

IP 地址策略：IP 地址组

URL 关键词：zcool.com.cn;huaban.com;scnn.com

IP 组：设计部

1. 点击「行为」>「上网过滤」>「URL 过滤」，然后点击 **新增**。
2. 配置 URL 过滤策略相关参数，点击 **保存**。



新增URL过滤策略

过滤策略：白名单（允许访问互联网）

IP地址策略：IP地址组

IP组：设计部

时间组：上班时间

URL关键词：zcool.com.cn; huaban.com; sccnn.com

备注：（可选）

取消 保存

3. 去勾选“允许列表外的主机或设备访问互联网”，确认弹窗提示信息后，点击 **确定**。



URL过滤

新增 删除

搜索

过滤策略	IP地址策略	IP地址或IP组	时间组	URL关键词	备注	状态	操作
<input type="checkbox"/> 白名单（允许访问互联网）	IP地址组	设计部	上班时间	zcool.com.cn; huaban.com; sccnn.com	-	已启用	编辑 停用 删除
<input type="checkbox"/> 允许列表外的主机或设备访问互联网							

---完成

## 验证配置

星期一到星期五的 8:00~18:00，局域网中，IP 地址在 192.168.0.2~192.168.0.50 范围内的电脑只能访问网址 zcool.com.cn、huaban.com 和 sccnn.com。其他电脑不能上网。

# 8 更多设置

## 8.1 高级路由

### 8.1.1 WAN 口参数

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「高级路由」>「WAN 口参数」。

如果您已经正确完成[联网设置](#)，但路由器局域网的用户还是不能上网，或者上网出现问题，可以尝试点击[编辑](#)修改 WAN 口参数解决。

#### WAN口参数

WAN口	速率	MTU	MAC地址	工作模式	操作
WAN1	1000Mbps全双工 (自动协商)	1500	<input type="text" value="(默认MAC地址)"/>	外网	<a href="#">编辑</a>

#### 编辑WAN1口参数

速率

自动协商

MTU

1500

MAC地址

默认MAC地址

工作模式

外网

广域网链路检测

☒ 开启 ☐ 关闭

检测网址

检测间隔

秒

取消

保存

## 参数说明

标题项	说明
WAN 口	当前路由器的 WAN 口。
速率	<p>WAN 口的速率与双工模式，它必须与对端端口的速率与双工模式保持一致。</p> <p>一般情况下，建议保持默认设置“自动协商”。如果路由器 WAN 口连接正常，但对应接口灯不亮；或者插上网线后接口灯要等待一会儿（5 秒以上）才亮。此时，可以将路由器的 WAN 口速率调为 10Mbps 半双工或 10Mbps 全双工尝试解决问题。</p>
MTU	<p>MTU（Maximum Transmission Unit，最大传输单元）是网络设备传输的最大数据包。取值范围与 WAN 口联网方式有关。</p> <p>一般情况下，建议保持默认设置。如果您无法访问某些网站、或打不开安全网站（如网银、支付宝登录页面）、或无法收发邮件、或无法访问 FTP 和 POP 服务器等，可以尝试修改 MTU 值，建议修改范围是 1400~1500，下面是常用的 MTU 值适用的场景：</p> <ul style="list-style-type: none"> <li>- 1500：一般用于非宽带拨号、非 VPN 拨号环境下最常用的设置。</li> <li>- 1492：一般用于宽带拨号环境。</li> <li>- 1480：是使用 ping 的最大值（大于此值的包会被分解）。</li> <li>- 1450：一般用于一些 DHCP（动态 IP）环境。</li> <li>- 1400：一般用于 VPN 或 PPTP 环境。</li> </ul>
MAC 地址	<p>WAN 口的 MAC 地址。</p> <p>正确完成联网设置后，如果路由器还是无法联网，有可能是宽带服务商将上网账号信息与某一 MAC 地址（物理地址）绑定了。此时，您可以尝试通过修改 WAN 口 MAC 地址解决该问题。</p>
工作模式	<p>WAN 口的工作模式。</p> <ul style="list-style-type: none"> <li>- 内网：WAN 口不能访问互联网，一般用于连接企业内网。</li> <li>- 外网：WAN 口可以访问互联网，一般用于连接互联网。</li> </ul>
广域网线路检测	开启后，路由器会周期性地检测 WAN 口与“检测网址”的连通情况，然后根据检测结果选择最佳的 WAN 口链路做为主要出口链路。
检测网址	需要检测的域名。
检查间隔	路由器执行广域网线路检测的时间间隔。

标题项	说明
	可对策略进行如下操作：
操作	<ul style="list-style-type: none"><li>- 点击<a href="#">编辑</a>可以修改策略。</li><li>- 点击<a href="#">删除</a>可以删除策略。</li></ul>

## 8.1.2 多 WAN 策略

### 概述

路由器启用多个 WAN 口后，可允许多条宽带同时接入，实现带宽叠加。当多个 WAN 口同时工作时，合理的设置多 WAN 策略可以大幅提升路由器的带宽利用率。

- 智能负载均衡：自动分配流量，系统自动寻找流量最小的 WAN 口通信。
- 自定义：用户根据实际需要，为某一源 IP 地址的流量指定 WAN 口进行转发。

### 设置多 WAN 策略

进入页面：[登录到路由器 Web 管理页面](#)，点击「更多」>「高级路由」>「多 WAN 策略」。

在这里，您可以设置多 WAN 策略。路由器的多 WAN 策略默认为“智能负载均衡”。选择“自定义”时，页面如下所示。点击 [新增](#) 可以自定义多 WAN 策略。

多WAN策略

多WAN策略 ☐ 智能负载均衡 ☒ 自定义

新增

IP组	WAN口	备注	状态 ↓	操作
-----	------	----	------	----

新增多WAN策略

IP组

设计部

WAN口

WAN1

备注

(可选)

取消

保存

参数说明

标题项	说明
IP 组	自定义多 WAN 策略引用的 IP 组，以指定规则对应的用户。IP 组应事先在 <a href="#">「行为」&gt;「分组策略」&gt;「IP 组」</a> 页面配置好。
WAN 口	选择对应 IP 组数据流量使用的 WAN 接口。
备注	自定义多 WAN 策略的备注信息。
状态	自定义多 WAN 策略的状态。
操作	可对策略进行如下操作： <ul style="list-style-type: none"><li>- 点击<a href="#">编辑</a>可以修改策略。</li><li>- 点击<a href="#">删除</a>可以删除策略。</li></ul>

自定义多 WAN 策略配置举例

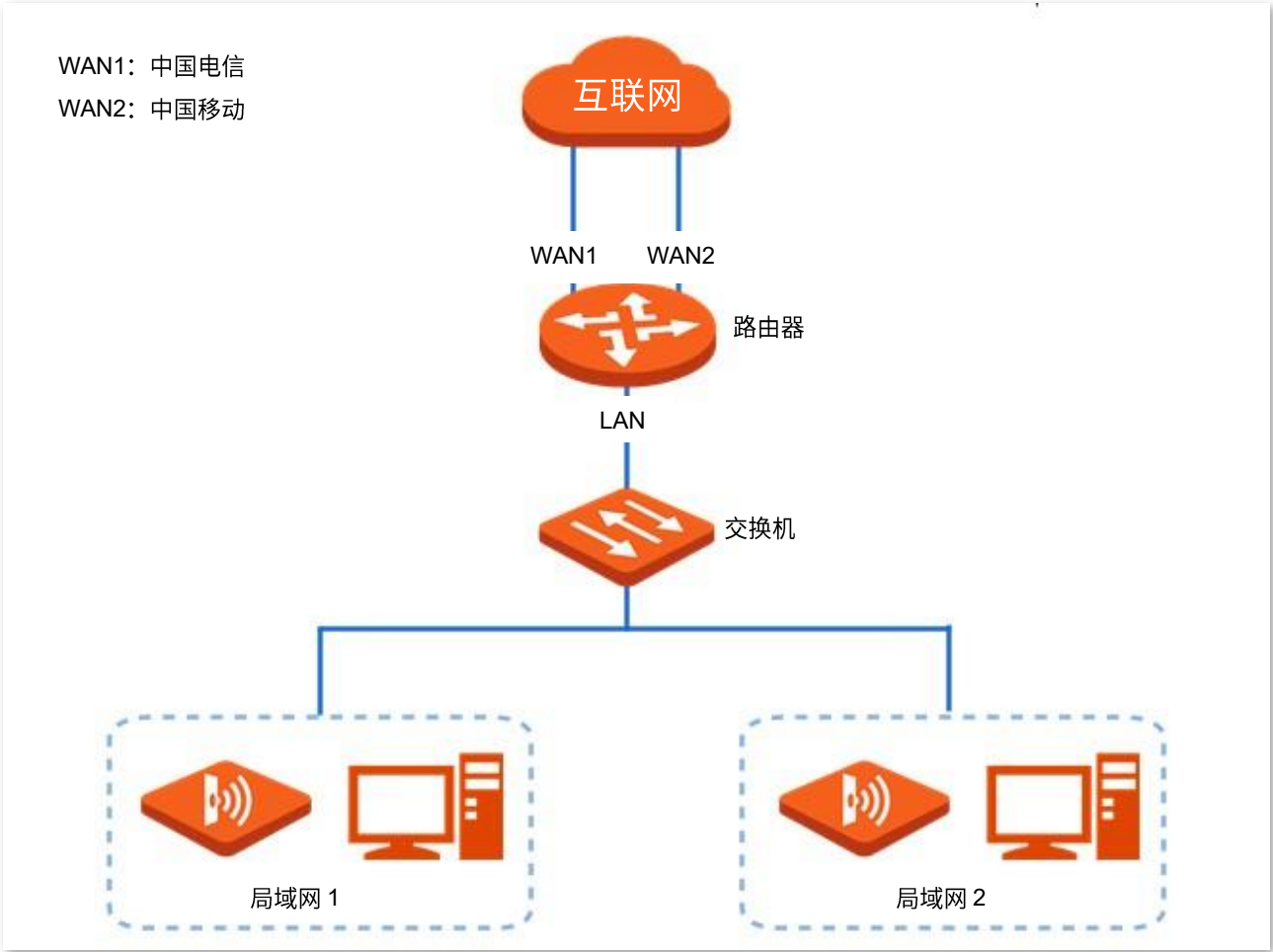
组网需求

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

- IP 地址为 192.168.0.2~192.168.0.100 的终端设备通过电信宽带访问互联网。
- IP 地址为 192.168.0.101~192.168.0.250 的终端设备通过移动宽带访问互联网。

方案设计

可以采用路由器的多 WAN 策略功能实现上述需求。



配置步骤



**步骤 1** [登录到路由器 Web 管理页面。](#)

**步骤 2** 配置 IP 组。

进入「行为」>「分组策略」>「IP 组」页面，点击 **新增**，配置如下 IP 组。

IP组			
<b>新增</b>			
策略名称	IP地址段	备注	操作
IP组1	192.168.0.2~192.168.0.100	-	<a href="#">编辑</a> <a href="#">删除</a>
IP组2	192.168.0.101~192.168.0.250	-	<a href="#">编辑</a> <a href="#">删除</a>

**步骤 3** 开启自定义多 WAN 策略。

1. 点击「更多」>「高级路由」>「多 WAN 策略」。
2. 选择“多 WAN 策略”为“自定义”。
3. 确认提示信息后，点击 **确定**。



**步骤 4** 自定义多 WAN 策略规则。

进入「更多」>「高级路由」>「多 WAN 策略」页面，点击 **新增**，配置如下多 WAN 策略规则。



----完成

**验证配置**

局域网中 IP 组 1（IP 地址在 192.168.0.2~192.168.0.100 范围内）的设备访问外网时，数据流量由 WAN1 口转发；局域网中 IP 组 2（IP 地址在 192.168.0.101~192.168.0.250 范围内）的设备访问外网时，数据流量由 WAN2 口转发。



### 8.1.3 静态路由

#### 概述

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

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

#### 设置静态路由



注意

- 在大型复杂网络中完全使用静态路由时，如果网络发生故障或者拓扑发生变化，可能会出现路由不可达，并导致网络中断，此时必须由网络管理员手工修改静态路由的配置。
- 当静态路由规则和自定义的多 WAN 策略冲突时，静态路由优先生效。

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「高级路由」>「静态路由」。

在这里，您可以根据实际网络情况配置相应的静态路由。点击 **新增** 可以新建静态路由。

静态路由

新增

策略名称	目标网络	子网掩码	默认网关	接口	状态 ↓	操作
------	------	------	------	----	------	----

新增静态路由

策略名称

目标网络

子网掩码

默认网关

接口

VLAN\_Default

取消

保存

## 参数说明

标题项	说明
策略名称	静态路由策略的名称。
目标网络	<p>目的网络的 IP 地址。目标网络和子网掩码均为“0.0.0.0”表示默认路由。</p> <p> <b>提示</b></p> <p>当在路由表中找不到与数据包的目的地址精确匹配的路由时，路由器会选择默认路由来转发该数据包。</p>
子网掩码	目的网络的子网掩码。
默认网关	<p>数据包从路由器的接口出去后，下一跳路由的入口 IP 地址。</p> <p>默认网关为“0.0.0.0”表示直连路由，即该目标网络是路由器接口直连的网络。</p>
接口	数据从路由器出去的接口。请根据需要选择相应接口。
状态	静态路由策略的状态。
操作	<p>可对策略进行如下操作：</p> <ul style="list-style-type: none"> <li>- 点击<a href="#">编辑</a>可以修改策略。</li> <li>- 点击<a href="#">停用/启用</a>可以停用或启用策略。</li> <li>- 点击<a href="#">删除</a>可以删除策略。</li> </ul>

## 静态路由配置举例

### 组网需求

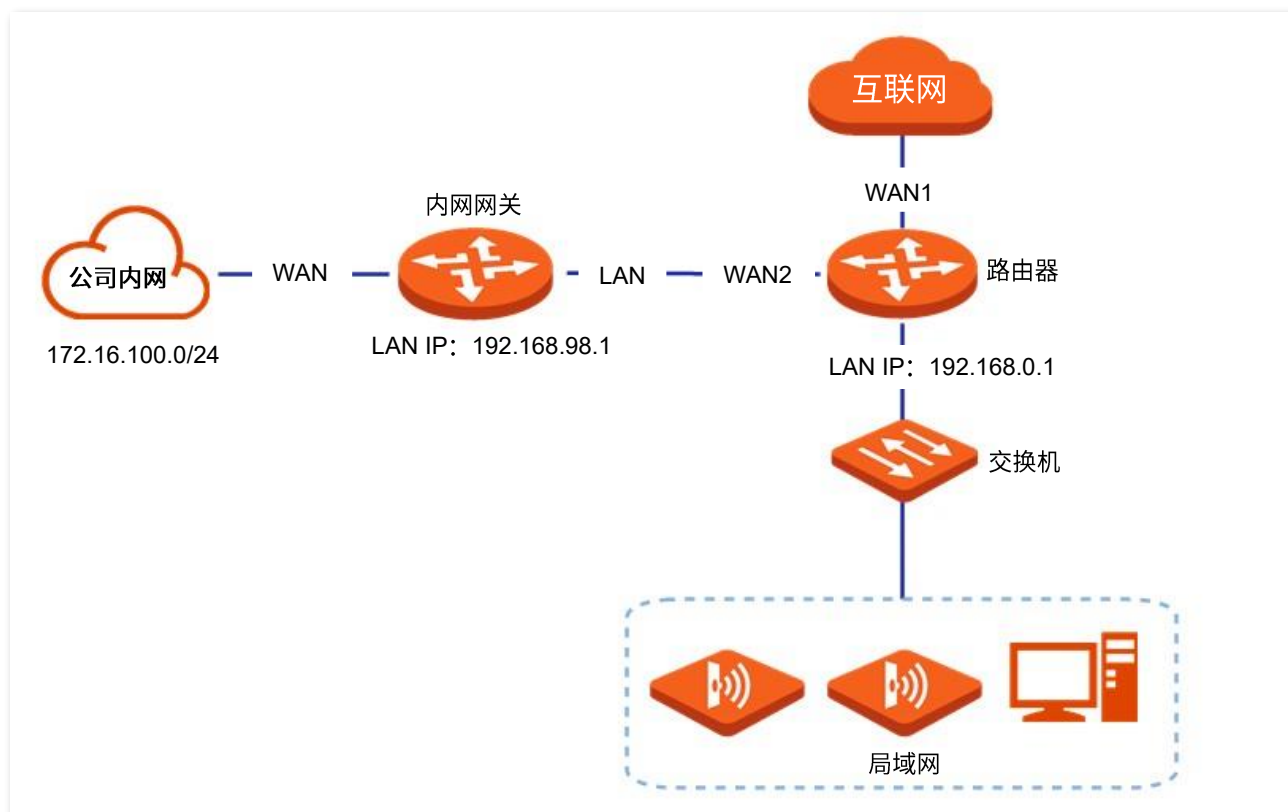
某企业使用企业级无线路由器进行网络搭建。路由器的 WAN1 口已通过宽带拨号接入互联网。现企业内部搭建了一个内网，与互联网在不同的网络。路由器的 WAN2 口通过动态 IP 接入公司内网。

要求：局域网的用户能同时访问互联网和公司内网。

### 方案设计

使用路由器的静态路由功能实现上述需求。

假设宽带账号和宽带密码均为 zhangsan。



## 配置步骤

启用 2 个 WAN 口

配置 WAN2 口联网

配置静态路由

**步骤 1** [登录路由器 Web 管理页面](#)。

**步骤 2** 启用 2 个 WAN 口。

1. 点击「网络」>「联网设置」。
2. 设置“WAN 口个数”为“2”。
3. 确认提示信息后，点击 **确定**。路由器将重启，稍等片刻，路由器重启完成。



**步骤 3** 配置 WAN2 口联网。

- 1. 点击「网络」>「联网设置」。
- 2. 在 WAN2 处选择“联网方式”为“动态 IP”，点击 **连接**。



稍等片刻，当 WAN2 口的联网状态显示“已联网”时，WAN2 口联网成功。

**步骤 4** 配置静态路由。

- 1. 获取 WAN2 口的 IP 地址信息。

进入「系统」页面，在[连接状态](#)模块查看 WAN2 获取的 IP 地址信息，本例中相关信息如下。

WAN2 IP 地址	子网掩码	默认网关	首选 DNS
192.168.98.190	255.255.255.0	192.168.98.1	192.168.98.1

2. 配置静态路由。

静态路由参数示例如下表所示。

策略名称	目标网络	子网掩码	默认网关	接口
内网访问	172.16.100.0	255.255.255.0	192.168.98.1	WAN2

进入「更多」>「高级路由」>「静态路由」页面，点击 **新增**，配置静态路由参数，点击 **保存**。

新增静态路由

策略名称

内网访问

目标网络

172 . 16 . 100 . 0

子网掩码

255 . 255 . 255 . 0

默认网关

192 . 168 . 98 . 1

接口

WAN2

取消

保存

----完成

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。

### 8.1.4 路由表

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「高级路由」>「路由表」。

在这里，您可以查看路由器的详细路由信息。

路由表			
目标网络	子网掩码	默认网关	接口
0.0.0.0	0.0.0.0	172.16.200.1	WAN
10.10.96.0	255.255.224.0	0.0.0.0	LAN
172.16.200.1	255.255.255.255	0.0.0.0	WAN
192.168.0.0	255.255.255.0	0.0.0.0	LAN

#### 参数说明

标题项	说明
目标网络	<p>目的网络的 IP 地址。目标网络和子网掩码均为“0.0.0.0”表示默认路由。</p> <p> <b>提示</b></p> <p>当在路由表中找不到与数据包的目的地址精确匹配的路由时，路由器会选择默认路由来转发该数据包。</p>
子网掩码	<p>目的网络的子网掩码。</p>
默认网关	<p>数据包从路由器的接口出去后，下一跳路由的入口 IP 地址。</p> <p>默认网关为“0.0.0.0”表示直连路由，即该目标网络是路由器接口直连的网络。</p>
接口	<p>数据从路由器出去的接口。</p>

## 8.1.5 策略路由

### 概述

策略路由，也叫做基于策略的路由，是指在决定一个 IP 包的下一跳转发地址时，不是简单的根据目的或源 IP 地址来决定，而是综合考虑多种因素决定。本路由器的策略路由通过对源网络、目的网络、目的端口、协议和 WAN 口的设置，更加精确的控制路由器进行选路。

策略路由设置完成后，路由器将满足该策略条件的数据包通过指定的 WAN 口转发。

### 配置策略路由

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「高级路由」>「策略路由」。

在这里，您可以配置策略路由。点击 **新增** 可以新建策略路由。

策略路由

新增

策略名称	源IP地址段/掩码	源端口	目的IP地址段/掩码	目的端口	协议	接口	开销	状态 ↑	操作
------	-----------	-----	------------	------	----	----	----	------	----

新增策略路由

策略名称

源IP地址段/掩码

源端口

目的IP地址段/掩码

目的端口

协议

接口

开销

取消

保存

### 参数说明

标题项	说明
策略名称	策略路由的策略名称。
源 IP 地址段/掩码	要进行精确路由转发的源 IP 地址段。

标题项	说明
源端口	要进行精确路由转发的源端口号。
目的 IP 地址段/掩码	数据包被转发到的目的 IP 地址段。
目的端口	数据包被转发到的目标网络的端口号。
协议	数据包的协议类型。
接口	策略生效的物理接口，满足策略路由条件的数据包将由该接口转发出去。
开销	该策略的优先级，值越小，策略路由优先级越高。
状态	策略的状态。
操作	<p>可对策略进行如下操作：</p> <ul style="list-style-type: none"> <li>- 点击<a href="#">编辑</a>可以修改策略。</li> <li>- 点击<a href="#">停用/启用</a>可以停用或启用策略。</li> <li>- 点击<a href="#">删除</a>可以删除策略。</li> </ul>

## 策略路由配置举例

### 组网需求

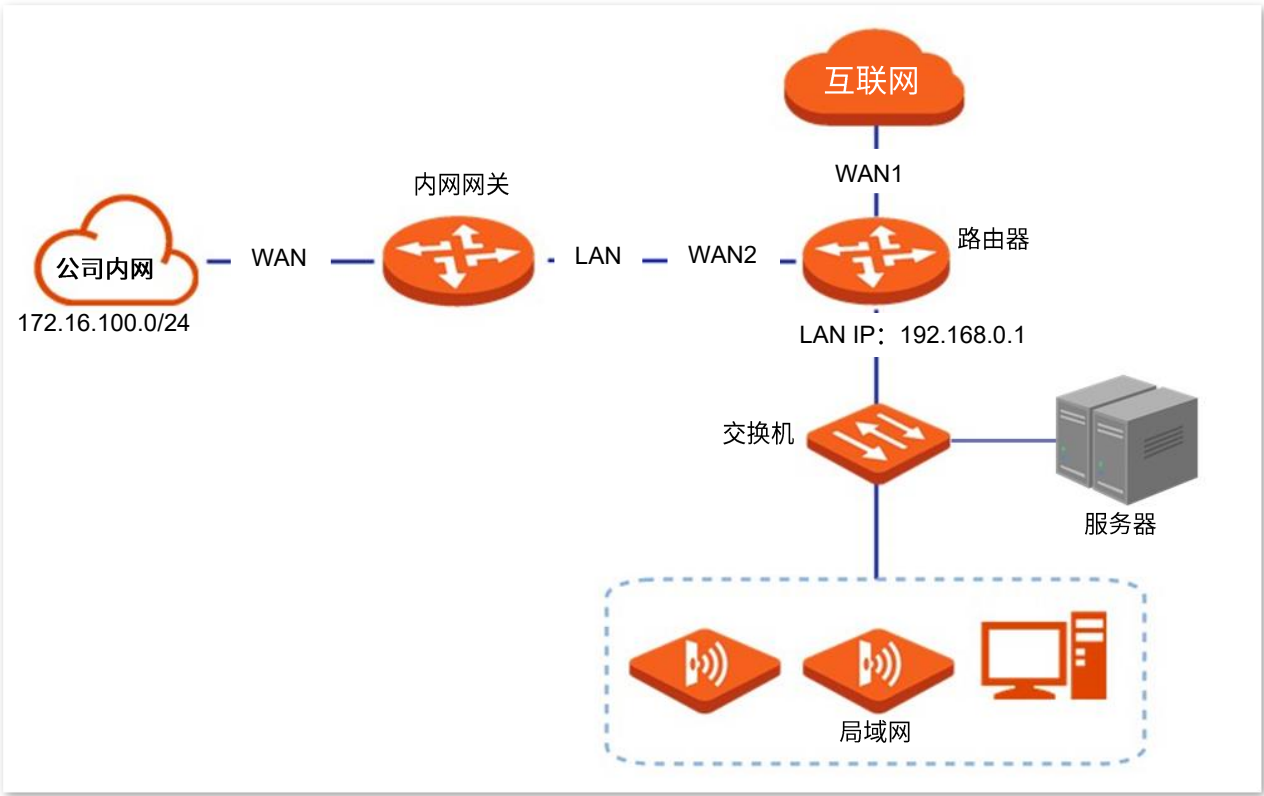
某企业使用路由器进行网络搭建，路由器已通过宽带拨号接入互联网。现企业内网搭建了一个 Web 服务器，与互联网在不同的网络。企业内网的接入方式为动态 IP。

要求：局域网地址为 192.168.0.2~192.168.0.254 的用户能同时访问互联网和公司内网的 Web 服务器。

### 方案设计

可以采用路由器的策略路由功能实现上述需求。





配置步骤



**步骤 1** 登录路由器 Web 管理页面。

**步骤 2** 启用 2 个 WAN 口。

1. 点击「网络」>「联网设置」。
2. 设置“WAN 口个数”为“2”。
3. 确认提示信息后，点击 **确定**。路由器将重启，稍等片刻，路由器重启完成。

**WAN口个数**

接口 千兆网口

WAN口个数

端口状态

1	2	3	4
WAN	WAN/LAN	WAN/LAN	LAN
WAN 1	WAN 2	LAN 3	LAN 4

**步骤 3** 配置 WAN2 口联网。

- 1. 点击「网络」>「联网设置」。
- 2. 在 WAN2 处选择“联网方式”为“动态 IP”，点击 **连接**。

WAN 1

WAN 2

连接设置

联网方式

动态IP

首选DNS

.(.)

(可选)

备用DNS

.(.)

(可选)

联网状态

联网中...

连接

断开

稍等片刻，当 WAN2 口的联网状态显示“**已联网**”时，WAN2 口联网成功。

**步骤 4** 配置策略路由。

策略路由参数示例如下表所示。

策略名称	源 IP 地址段/掩码	源端口	目的 IP 地址段/掩码	目的端口	协议	接口	开销
Web 服务器访问	192.168.0.0/24	1~65535	172.16.100.0/24	1~65535	ALL	WAN2	10

进入「更多」>「高级路由」>「策略路由」页面，点击 **新增**，配置策略路由参数，点击 **保存**。

新增策略路由

策略名称

Web服务器访问

源IP地址段/掩码

192.168.0.0 / 24

源端口

1 - 65535

目的IP地址段/掩码

172.16.100.0 / 24

目的端口

1 - 65535

协议

ALL

接口

WAN2

开销

10

取消

保存

----完成

验证配置

局域网地址为 192.168.0.2~192.168.0.254 的用户能同时访问互联网和公司内网的 Web 服务器。

## 8.2 虚拟服务

### 8.2.1 DMZ 主机

#### 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。例如：某台电脑正在进行视频会议或在线游戏，可将该电脑设置为 DMZ 主机使视频会议和在线游戏更加顺畅。另外，在互联网用户需要访问局域网资源时，也可将该服务器设置为 DMZ 主机。



- 将设备设置成 DMZ 主机后，该设备相当于完全暴露于外网，路由器的防火墙对该设备不再起作用。
- 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。
- DMZ 主机上的安全软件、杀毒软件以及系统自带防火墙，可能会影响 DMZ 主机功能，使用本功能时，请暂时关闭。不使用 DMZ 主机时，建议关闭该功能，并且打开 DMZ 主机上的防火墙、安全卫士和杀毒软件。

#### 配置 DMZ 主机

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「虚拟服务」>「DMZ」。

路由器默认已为各 WAN 接口创建了相应的 DMZ 策略，状态为“已停用”，您根据实际需要修改相应的 DMZ 策略。

DMZ <span>?</span>				
接口	DMZ主机IP地址	VPN端口过滤	状态 ↑	操作
WAN1	-	开启	已停用	<a href="#">编辑</a> <a href="#">启用</a>

#### 参数说明

标题项	说明
接口	DMZ 策略生效的 WAN 接口。
DMZ 主机 IP 地址	要设置为 DMZ 主机的局域网设备的 IP 地址。

标题项	说明
	开启后，启用 DMZ 功能时，由路由器的 VPN 服务响应外网的 VPN 请求。
VPN 端口过滤	 <p>路由器已开启 VPN 功能的情况下，开启 DMZ 主机功能时，请同时开启“VPN 端口过滤”功能。</p>
状态	DMZ 策略的状态。
操作	<p>可对策略进行如下操作：</p> <ul style="list-style-type: none"> <li>- 点击<a href="#">编辑</a>可以修改策略。</li> <li>- 点击<a href="#">停用/启用</a>可以停用或启用策略。</li> </ul>

## DMZ 配置举例

### 组网需求

某企业使用企业级无线路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。现在需要将企业内部的 Web 服务器开放给互联网用户，使员工不在公司时也能访问企业内部网络。

### 方案设计

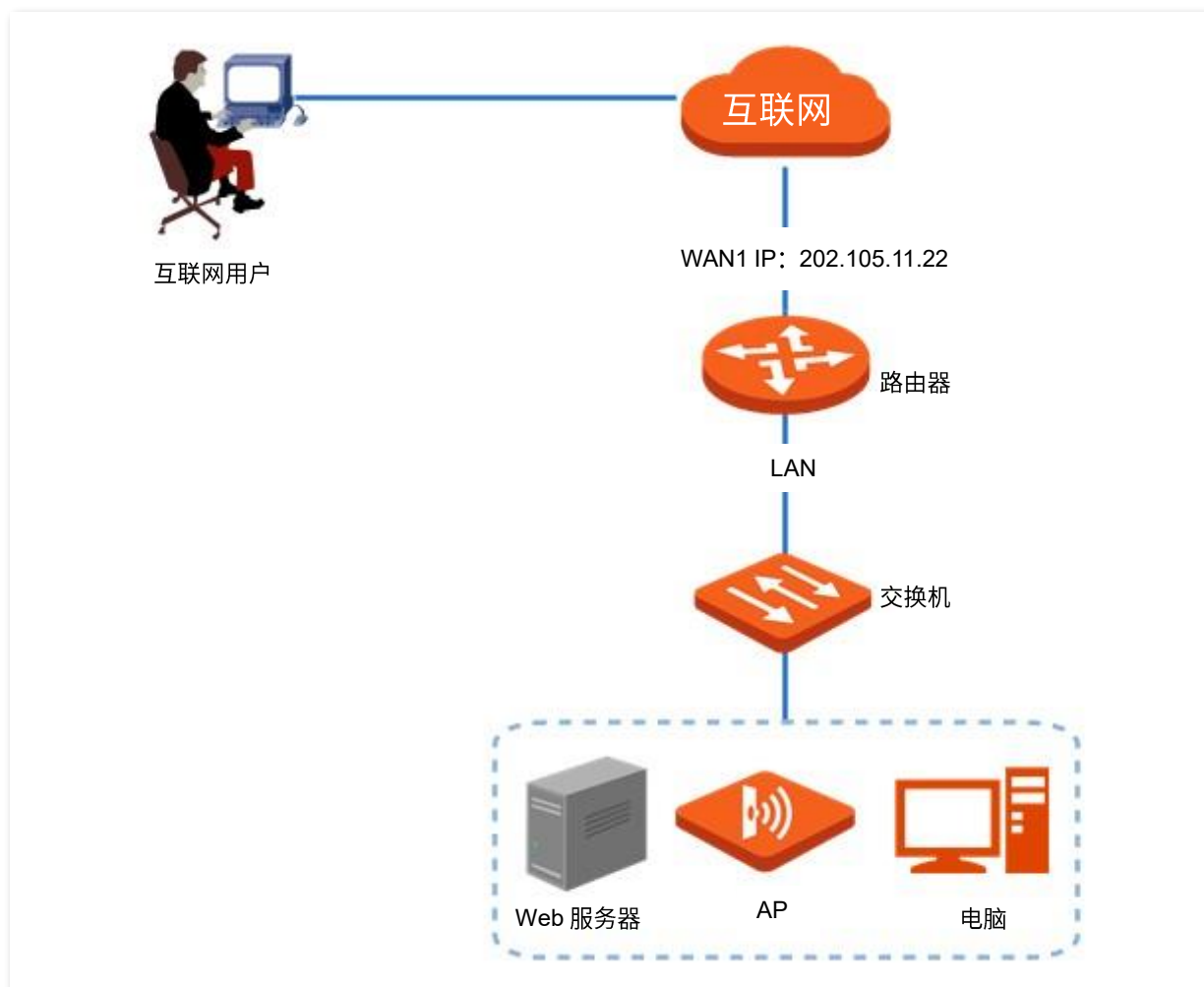
- 使用 DMZ 主机功能实现互联网用户访问企业内部 Web 服务器的需求。
- 使用静态 IP 分配功能防止因 Web 服务器地址改变导致互联网用户访问企业内部 Web 服务器失败。

假设 Web 服务器信息如下：

- 服务器地址：192.168.0.250
- 服务器主机 MAC 地址：C8:9C:DC:60:54:69
- 服务端口：9999



- 配置前请确保路由器 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址或互联网服务提供商分配的内网 IP 地址（以 100 开头），将导致功能无法实现。IPv4 常用的地址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。
- 互联网服务提供商可能不会支持未经报备的使用默认端口号 80 访问的 Web 服务。因此，在使用 DMZ 主机功能时，建议将内网服务端口设为非熟知端口（1024~65535），如 9999，以确保可以正常访问。



## 配置步骤

配置 DMZ 主机 > 给 DMZ 主机分配固定 IP 地址

**步骤 1** [登录路由器 Web 管理页面](#)。

**步骤 2** 配置 DMZ 主机。

1. 点击「更多」>「虚拟服务」>「DMZ」。找到相应的 WAN 口，点击[编辑](#)。

DMZ <span>?</span>			
接口	DMZ主机IP地址	状态 ↓	操作
WAN1	-	已停用	<a href="#">编辑</a> <a href="#">启用</a>

2. 输入局域网内要设置为 DMZ 主机的设备的 IP 地址，本例为“192.168.0.250”。
3. 点击 [保存](#)。

编辑WAN1 DMZ

接口

WAN1

DMZ主机IP地址

192 . 168 . 0 . 250

取消

保存

4. 点击启用。

DMZ			
接口	DMZ主机IP地址	状态 ↓	操作
WAN1	192.168.0.250	已停用	<a href="#">编辑</a> <a href="#">启用</a>

步骤 3 给 DMZ 主机分配固定 IP 地址。

DHCP 静态分配规则参数示例如下所示。

终端名称：Web 服务器	固定分配给服务器主机的 IP 地址：192.168.0.250
服务器主机的 MAC 地址：C8:9C:DC:60:54:69	规则备注信息：Web 服务器地址

1. 点击「网络」>「DHCP 静态分配」，然后点击 新增 。

DHCP静态分配

新增

删除

导入

导出

搜索

<input type="checkbox"/>	终端名称	终端类型	IP地址 ↑	MAC地址	备注	状态	操作
--------------------------	------	------	--------	-------	----	----	----

2. 配置 DHCP 静态分配规则的相关参数后，点击 保存 。

新增DHCP静态分配

终端名称

Web服务器

IP地址

192 . 168 . 0 . 250

MAC地址

C8:9C:DC:60:54:69

备注

Web服务器地址

(可选)

取消

保存

---完成

验证配置

互联网上的用户使用“内网服务应用层协议名称://对应 WAN 口当前的 IP 地址”可以成功访问内网服务器。  
如果内网服务端口不是默认端口号，访问格式为“内网服务应用层协议名称://对应 WAN 口当前的 IP 地址:

内网服务端口”。

在本例中，访问地址为“http://202.105.11.22:9999”。

您可以在「系统」页面的[连接状态](#)模块找到路由器 WAN 口当前 IP 地址。

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

## 8.2.2 DDNS

### 概述

DDNS，Dynamic Domain Name Server，动态域名服务。当服务运行时，路由器上的 DDNS 客户端将路由器当前的 WAN 口 IP 地址传送给 DDNS 服务器，然后服务器更新数据库中域名与 IP 地址的映射关系，实现动态域名解析。

通过 DDNS 功能，可以将路由器动态变化的 WAN 口 IP 地址（公网 IP 地址）映射到一个固定的域名上。DDNS 功能通常与端口映射、DMZ 主机等功能结合使用，使外网用户可以通过域名访问路由器局域网服务器或路由器管理页面，无需再关注路由器的 WAN 口 IP 地址变化。

### 配置 DDNS

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「虚拟服务」>「DDNS」。

路由器默认已为 WAN 接口创建了相应的 DDNS 策略，状态为“未启用”。您根据实际情况修改相应的 DDNS 策略。

DDNS						
接口	连接状态	服务提供商	用户名	域名	状态 ↓	操作
WAN1	未连接	3322.org	-	-	已停用	<a href="#">编辑</a> <a href="#">启用</a>

#### 参数说明

标题项	说明
接口	DDNS 策略生效的 WAN 接口。
连接状态	DDNS 服务的运行状态。
服务提供商	DDNS 的服务提供商。



标题项	说明
用户名	登录 DDNS 服务的用户名。
域名	在 DDNS 服务商处申请的域名信息。设置为除 oray 外的其他 DDNS 提供商时，需要手动输入在对应网站上申请的域名。
状态	DDNS 策略的状态。
操作	<p>可对策略进行如下操作：</p> <ul style="list-style-type: none"> <li>- 点击<a href="#">编辑</a>可以修改策略。</li> <li>- 点击<a href="#">停用/启用</a>可以停用或启用策略。</li> </ul>

## DDNS 配置举例

### 组网需求

某企业使用企业级无线路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。现需要将企业内部的 Web 服务器开放给互联网用户，使员工不在公司时也能访问企业内部网络。

### 方案设计

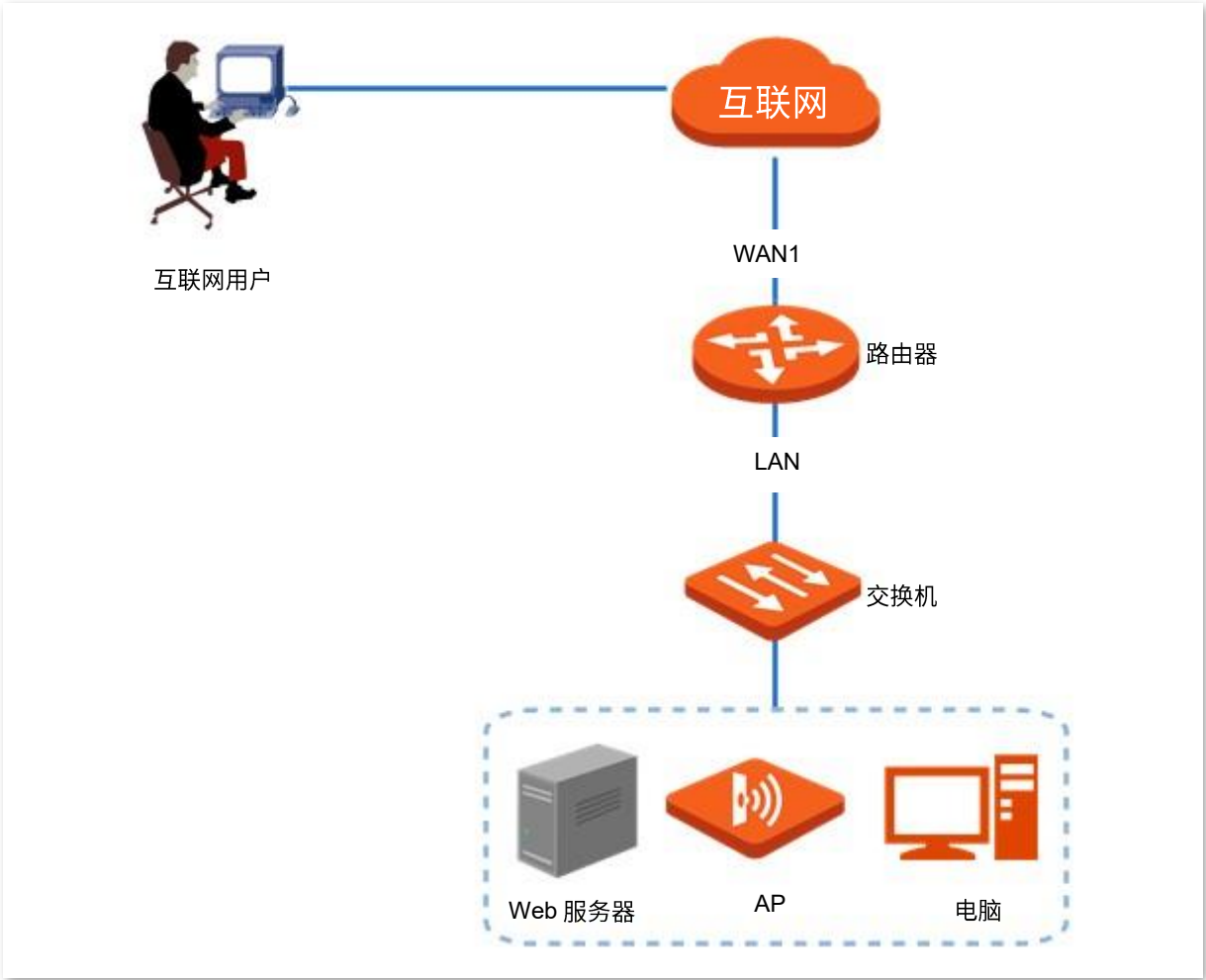
- 使用端口映射功能实现互联网用户访问企业内部 Web 服务器的需求。
- 使用 DDNS 功能让互联网用户可以通过固定域名访问企业内部 Web 服务器，防止因 WAN 口 IP 地址变化导致访问失败。
- 使用静态 IP 分配功能防止因 Web 服务器地址改变导致互联网用户访问企业内部 Web 服务器失败。

假设 Web 服务器信息如下：

- 服务器地址：192.168.0.250
- 服务器主机 MAC 地址：C8:9C:DC:60:54:69
- 服务端口：9999



- 配置前请确保路由器 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址或互联网服务提供商分配的内网 IP 地址（以 100 开头），将导致功能无法实现。IPv4 常用的地址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。
- 互联网服务提供商可能不会支持未经报备的使用默认端口号 80 访问的 Web 服务。因此，在设置端口映射时，建议将外网端口设为非熟知端口（1024~65535），如 9999，以确保可以正常访问。
- 内网端口和外网端口可设置为不同的端口号。



配置步骤

配置端口映射

给服务器主机分配固定 IP 地址

配置 DDNS

**步骤 1** 登录路由器 Web 管理页面。

**步骤 2** 配置端口映射。

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

端口映射 ?

端口映射 ☒ 开启 ☐ 关闭

新增

内网IP地址	内网端口	外网端口	协议	接口	备注	状态 ↓	操作
192.168.0.250	9999	9999	TCP	WAN1	-	已启用	<a href="#">编辑</a> <a href="#">停用</a> <a href="#">删除</a>

步骤 3 给服务器主机分配固定 IP 地址。

DHCP 静态分配规则参数示例如下所示。

终端名称：Web 服务器	固定分配给服务器主机的 IP 地址：192.168.0.250
服务器主机的 MAC 地址：C8:9C:DC:60:54:69	规则备注信息：Web 服务器地址

1. 点击「网络」>「DHCP 静态分配」，然后点击 **新增**。



2. 配置 DHCP 静态分配规则的相关参数后，点击 **保存**。

步骤 4 配置 DDNS。

1. 注册域名。

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

2. [登录路由器 Web 管理页面](#)，设置 DDNS。

- (1) 点击「更多」>「虚拟服务」>「DDNS」，点击对应 WAN 口规则后的 **编辑**，本例为“WAN1”。

DDNS						
接口	连接状态	服务提供商	用户名	域名	状态 ↓	操作
WAN2	未连接	3322.org	-	-	已停用	<a href="#">编辑</a> <a href="#">启用</a>

- (2) 选择您申请域名的 DDNS 提供商，本例为“3322”。

- (3) 输入您在 DDNS 服务提供商网站注册的用户名及对应登录密码，本例分别为“zhangsan”和“zhangsan”。
- (4) 输入您从 DDNS 服务提供商网站申请的域名，本例为“zhangsan.3322.org”。
- (5) 点击 **保存**。

编辑WAN1 DDNS

接口: WAN1

服务提供商: 3322.org [去注册](#)

用户名: zhangsan

密码: .....

域名: zhangsan.3322.org

[取消](#) [保存](#)

3. 点击**启用**。

DDNS						
接口	连接状态	服务提供商	用户名	域名	状态 ↓	操作
WAN1	未连接	3322.org	zhangsan	zhangsan.3322.org	已停用	<a href="#">编辑</a> <a href="#">启用</a>

DDNS 服务配置完成，刷新一下页面，稍等片刻。当 WAN1 口“连接状态”显示为“**已连接**”时，连接成功。

DDNS						
接口	连接状态	服务提供商	用户名	域名	状态 ↓	操作
WAN1	已连接	3322.org	-	-	已启用	<a href="#">编辑</a> <a href="#">停用</a>

---完成

## 验证配置

互联网上的用户使用“内网服务应用层协议名称://对应 WAN 口域名”可以成功访问内网服务器。添加端口映射规则时，如果设置的外网端口号不是内网服务的默认端口号，访问格式为“内网服务应用层协议名称://对应 WAN 口域名:外网端口”。

在本例中，访问地址为“http://zhangsan.3322.org:9999”。



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

- 确保您填写的内网端口是正确的相应服务端口。
  - 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。
-

### 8.2.3 DNS 劫持

#### 概述

DNS，Domain Name Server，域名服务器。用于管理域名与 IP 地址之间的关系，将域名和 IP 地址相互映射。

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

#### 配置 DNS 劫持

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「虚拟服务」>「DNS 劫持」。

在这里，您可以根据实际需要配置 DNS 劫持策略。



#### 参数说明

标题项	说明
域名	要解析为固定 IP 地址的域名。
映射 IP 地址	DNS 劫持后域名解析的 IP 地址，即用户访问指定域名时，会解析到该 IP 地址。
接口	数据从路由器出去的接口。
状态	DNS 劫持策略的状态。
操作	<p>可对策略进行如下操作：</p> <ul style="list-style-type: none"><li>- 点击<a href="#">编辑</a>可以修改策略。</li><li>- 点击<a href="#">停用/启用</a>可以停用或启用策略。</li><li>- 点击<a href="#">删除</a>可以删除策略。</li></ul>

## DNS 劫持配置举例

### 组网需求

某企业使用路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。现要求局域网用户访问淘宝（taobao.com）、京东（jd.com）等网站时，访问的是路由器的 Web 管理页面。

### 方案设计

可以采用路由器的 DNS 劫持功能实现上述需求。假设路由器的 IP 地址为 192.168.0.1。

### 配置步骤

**步骤 1** 登录路由器 Web 管理页面。

**步骤 2** 点击「更多」>「虚拟服务」>「DNS 劫持」，然后点击 **新增**。

**步骤 3** 配置 DNS 劫持规则的各项参数后，点击 **保存**。

1. 输入淘宝的域名地址，本例为“taobao.com”。
2. 输入映射的路由器 IP 地址，本例为“192.168.0.1”。



新增DNS劫持

域名: taobao.com

映射IP地址: 192 . 168 . 0 . 1

接口: 不指定

取消 保存

**步骤 4** 参考步骤 2~3 新增一条域名为京东（jd.com）的 DNS 劫持策略。

DNS劫持				
新增				
域名	映射IP地址	接口	状态 ↓	操作
jd.com	192.168.0.1	不指定	已启用	编辑 停用 删除
taobao.com	192.168.0.1	不指定	已启用	编辑 停用 删除

----完成

### 验证配置

局域网设备访问淘宝（taobao.com）、京东（jd.com）网站时，始终是访问到路由器 Web 管理页面。

## 8.2.4 IP 劫持

### 概述

启用 IP 劫持后，局域网内的用户访问 IP 地址：服务端口时，直接劫持到映射 IP 地址对应的端口服务。

常见服务端口：443（HTTPS 协议网页服务）、80（HTTP 协议网页服务）、21（FTP 服务）等。

### 配置 IP 劫持

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「虚拟服务」>「IP 劫持」。

在这里，点击 **新增**，您可以根据实际需要配置 IP 劫持策略。



### 参数说明

标题项	说明
目的 IP 地址	需要劫持访问的 IP 地址。
映射 IP 地址	劫持后访问的 IP 地址，即用户访问“目的 IP 地址:端口”时，都会解析到该 IP 地址。
端口	<p>“映射 IP 地址”指定服务对应的端口号。访问指定服务端口时，才会劫持到“映射 IP 地址”。</p> <p> <b>提示</b></p> <p>0 表示所有的端口。</p>
接口	数据从路由器出去的接口。
状态	IP 劫持策略的状态。
操作	<p>可对策略进行如下操作：</p> <ul style="list-style-type: none"><li>- 点击<a href="#">编辑</a>可以修改策略。</li><li>- 点击<a href="#">停用/启用</a>可以停用或启用策略。</li><li>- 点击<a href="#">删除</a>可以删除策略。</li></ul>



## IP 劫持配置举例

### 组网需求

某企业使用路由器进行网络搭建，且已接入互联网，可以为局域网用户提供上网服务。现要求局域网用户访问 1.1.1.1 网址时，访问的是路由器的 Web 管理页面。

### 方案设计

可以采用路由器的 IP 劫持功能实现上述需求。假设路由器的管理 IP 地址为 192.168.0.1，HTTPS 网页服务对应的端口号为 443。

### 配置步骤

**步骤 1** 登录路由器 Web 管理页面。

**步骤 2** 点击「更多」>「虚拟服务」>「IP 劫持」，然后点击 **新增**。

**步骤 3** 输入目的 IP 地址，本例为“1.1.1.1”。

**步骤 4** 输入映射的路由器 IP 地址，本例为“192.168.0.1”。

**步骤 5** 输入端口号，本例为“443”。

**步骤 6** 点击 **保存**。



新增IP劫持

目的IP地址	1 . 1 . 1 . 1
映射IP地址	192 . 168 . 0 . 1
端口	443 
接口	不指定 

**取消** **保存**

----完成

### 验证配置

局域网设备访问 1.1.1.1:443 网址时，可以访问到路由器的 Web 管理页面。

## 8.2.5 UPnP

### 概述

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

### 开启 UPnP

进入页面: [登录路由器 Web 管理页面](#), 点击「更多」>「虚拟服务」>「UPnP」。

UPnP 功能默认关闭, 在这里, 您可以开启 UPnP 功能。

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

UPnP					
UPnP <input checked="" type="radio"/> 开启 <input type="radio"/> 关闭					
远程主机	外网端口	内部主机	内网端口段	协议	描述
anywhere	54322	192.168.0.148	12345	UDP	MiniTP SDK
anywhere	54322	192.168.0.148	54321	TCP	MiniTP SDK

## 8.2.6 端口映射

### 概述

默认情况下，广域网中的用户不能访问局域网内的设备。通过端口映射功能，您可以开放路由器的一个或多个服务端口（TCP 或 UDP），并以 IP 地址和内网端口映射到指定的局域网服务器，之后，路由器将广域网中对此服务端口的请求定位到该局域网服务器上。这样，广域网中的用户就能够访问局域网服务器，局域网也能避免受到侵袭。

### 配置端口映射

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「虚拟服务」>「端口映射」。

在这里，您可以根据实际情况配置端口映射策略。

端口映射功能默认关闭，开启后显示如下。

端口映射

端口映射 ☒ 开启 ☐ 关闭

新增

内网IP地址	内网端口	外网端口	协议	接口	备注	状态 ↓	操作
暂无数据							

### 参数说明

标题项	说明
内网 IP 地址	内网服务器的 IP 地址。
内网端口	内网服务器的服务端口。
外网端口	路由器开放给广域网用户访问的端口。
协议	内网服务的协议类型。设置时，如果不确定服务的协议类型，可以选择“TCP&UDP”。
接口	内网服务映射的 WAN 口，即广域网用户访问局域网服务器时使用的 WAN 口。
备注	端口映射策略的备注信息。
状态	策略的状态。

标题项	说明
	可对策略进行如下操作：
操作	<ul style="list-style-type: none"> <li>- 点击<a href="#">编辑</a>可以修改策略。</li> <li>- 点击<a href="#">停用/启用</a>可以停用或启用策略。</li> <li>- 点击<a href="#">删除</a>可以删除策略。</li> </ul>

## 端口映射配置举例

### 组网需求

某企业使用企业级无线路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。现在需要将企业内部的 Web 服务器开放给互联网用户，使员工不在公司时也能访问企业内部网络。

### 方案设计

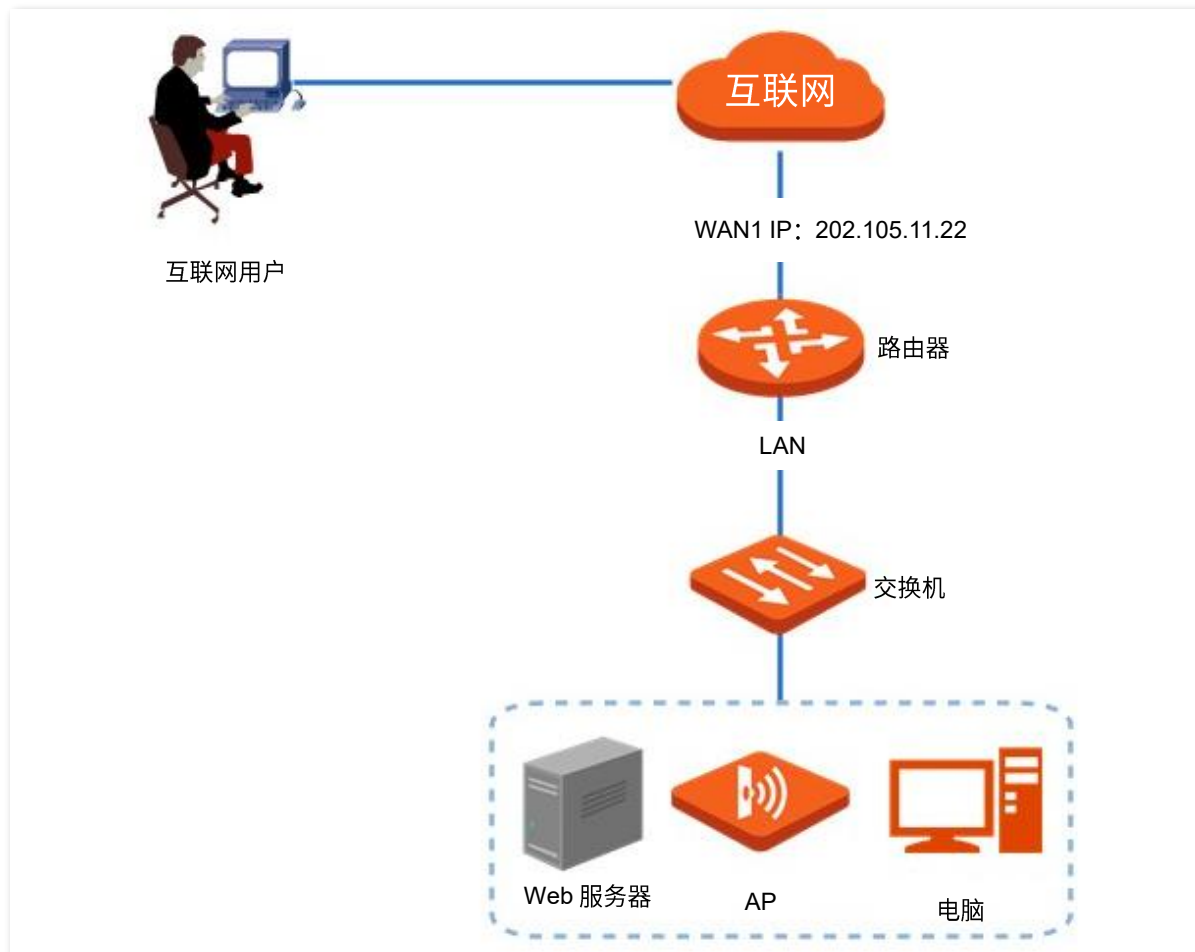
- 使用端口映射功能实现互联网用户访问企业内部 Web 服务器的需求。假设路由器开放的外网端口为 9999。
- 使用静态 IP 分配功能防止因 Web 服务器 IP 地址改变导致互联网用户访问企业内部 Web 服务器失败。

假设 Web 服务器信息如下：

- 服务器地址：192.168.0.250
- 服务器主机 MAC 地址：C8:9C:DC:60:54:69
- 服务端口：9999



- 配置前请确保路由器 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址或互联网服务提供商分配的内网 IP 地址（以 100 开头），将导致功能无法实现。IPv4 常用的地址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。
- 互联网服务提供商可能不会支持未经报备的使用默认端口号 80 访问的 Web 服务。因此，在设置端口映射时，建议将外网端口设为非熟知端口（1024~65535），如 9999，以确保可以正常访问。
- 内网端口和外网端口可设置为不同的端口号。



## 配置步骤

配置端口映射 → 给服务器主机分配固定 IP 地址

**步骤 1** [登录路由器 Web 管理页面](#)。

**步骤 2** 配置端口映射。

端口映射规则参数示例如下所示。

内网 IP 地址：192.168.0.250

内网端口（Web 服务端口）：9999

外网端口：9999

协议：TCP

接口：WAN1

1. 点击「更多」>「虚拟服务」>「端口映射」。
2. 开启“端口映射”功能后，点击 **新增**。
3. 配置端口映射规则的相关参数后，点击 **保存**。如下图示。

新增端口映射

内网IP地址

192 . 168 . 0 . 250

内网端口

9999

外网端口

9999

协议

TCP

接口

WAN1

备注

(可选)

取消

保存

端口映射规则配置完成，如下图示。

端口映射

端口映射

开启

关闭

新增

内网IP地址	内网端口	外网端口	协议	接口	备注	状态 ↓	操作
192.168.0.250	9999	9999	TCP	WAN1	-	已启用	<div>编辑</div> <div>停用</div> <div>删除</div>

步骤 3 给服务器主机分配固定 IP 地址。

DHCP 静态分配规则参数示例如下所示。

终端名称：Web 服务器	固定分配给服务器主机的 IP 地址：192.168.0.250
服务器主机的 MAC 地址：C8:9C:DC:60:54:69	规则备注信息：Web 服务器地址

1. 点击「网络」>「DHCP 静态分配」，然后点击 新增 。

DHCP静态分配

新增

删除

导入

导出

搜索

终端名称

终端类型

IP地址 ↑

MAC地址

备注

状态

操作

2. 配置 DHCP 静态分配规则的相关参数后，点击 保存 。



----完成

### 验证配置

互联网上的用户使用“内网服务应用层协议名称://对应 WAN 口当前的 IP 地址”可以成功访问内网服务器。如果设置的外网端口号不是内网服务的默认端口号，访问格式为“内网服务应用层协议名称://对应 WAN 口当前的 IP 地址:外网端口”。

在本例中，访问地址为“http://202.105.11.22:9999”。

您可以在「系统」页面的[连接状态](#)模块找到路由器 WAN 口当前 IP 地址。

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



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

- 确保您填写的内网端口是正确的相应服务端口。
- 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。

## 8.3 维护服务

### 8.3.1 远程 WEB 管理

#### 概述

一般情况下，只有接到路由器 LAN 口或无线网络的设备才能登录路由器的管理页面。通过远程 WEB 管理功能，使您在有特殊需要时（如远程技术支持），可以通过 WAN 口远程访问路由器的管理页面。

#### 配置远程 WEB 管理

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「维护服务」>「远程 WEB 管理」。

在这里，您可以开启或关闭远程 WEB 管理，也可以限定能够远程登录到本路由器的主机。

远程 Web 管理默认关闭，开启后，页面显示如下。

远程WEB管理

远程WEB管理

☒ 开启

☐ 关闭

指定接口

WAN1

远程主机的IP地址

所有地址

远程管理地址

http://o95ju9jc.cloud.tendacn.net:8080

复制

保存

#### 参数说明

标题项	说明
远程 WEB 管理	开启/关闭远程 WEB 管理功能。
指定接口	选择路由器的 WAN 口，即远程访问路由器管理页面时所使用的 WAN 口。



标题项	说明
	可以远程访问路由器管理页面的设备的 IP 地址。
远程主机的 IP 地址	<ul style="list-style-type: none"> <li>- 所有地址：互联网上任意 IP 地址的设备都能访问路由器的管理页面。为了网络安全，不建议选择此项。</li> <li>- 指定地址：只有指定 IP 地址的设备能远程访问路由器的管理页面。如果该设备在局域网，则应填入该设备的网关的 IP 地址（公网 IP 地址）。</li> </ul>
远程管理地址	远程管理路由器时使用的域名。开启“远程 WEB 管理”功能后，互联网用户可以使用此域名登录到路由器管理页面。

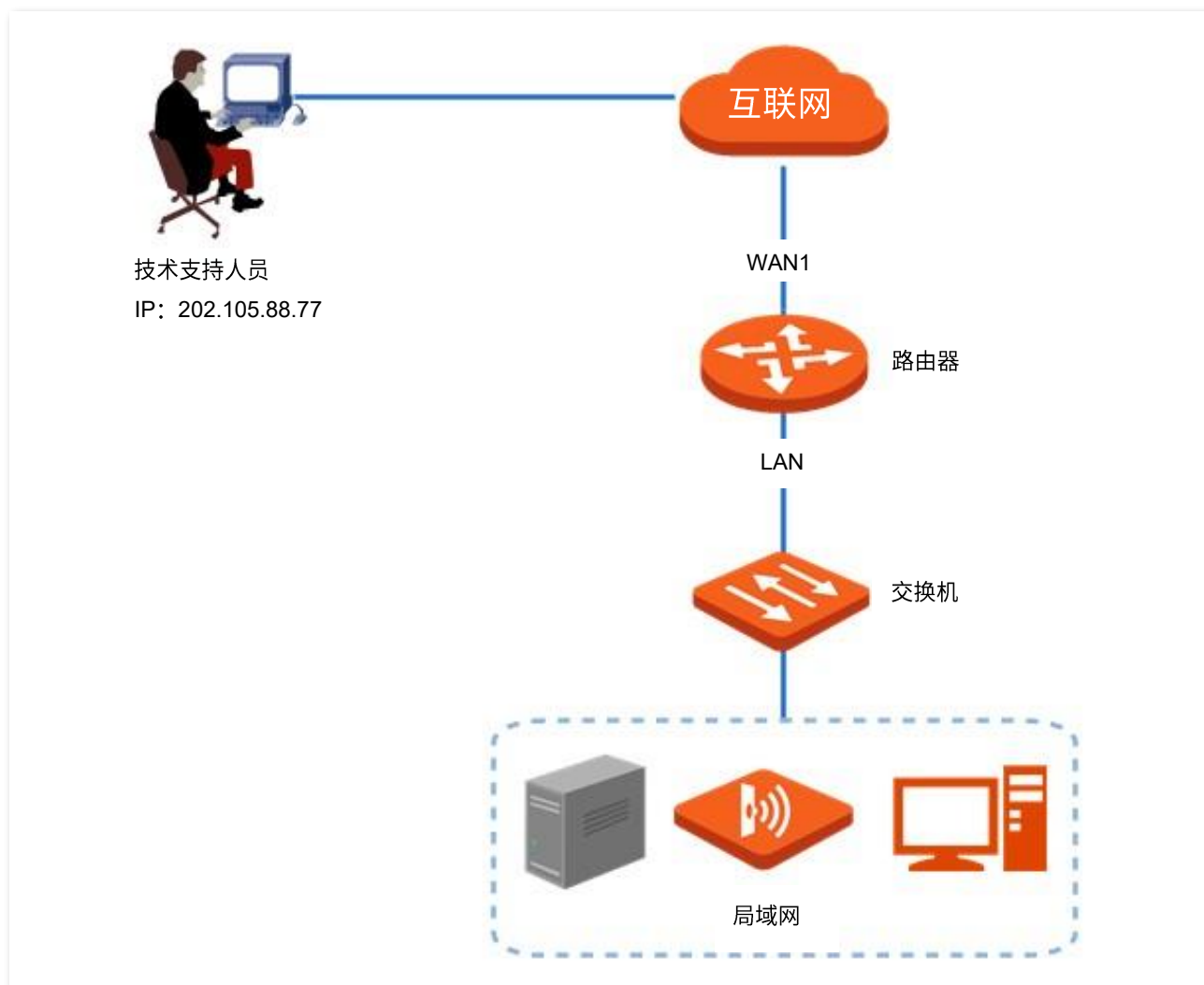
## 远程 WEB 管理配置举例

### 组网需求

某企业使用企业级无线路由器进行网络搭建，网络管理员在设置网络时遇到问题，需要 Tenda 技术支持远程登录到路由器管理页面分析并解决。

### 方案设计

可以采用路由器的远程 WEB 管理功能实现上述需求。



## 配置步骤

**步骤 1** [登录路由器 Web 管理页面](#)。

**步骤 2** 点击「更多」>「维护服务」>「远程 WEB 管理」。

**步骤 3** 开启“远程 WEB 管理”功能。

**步骤 4** 选择远程访问路由器时所使用的 WAN 口，本例为“WAN1”。

**步骤 5** 选择“指定地址”，然后输入 Tenda 技术支持的电脑的 IP 地址，本例为“202.105.88.77”。

**步骤 6** 点击 **保存**。

### 远程WEB管理

远程WEB管理

☒ 开启 ☐ 关闭

指定接口

WAN1

远程主机的IP地址

指定地址

202 . 105 . 88 . 77

远程管理地址

http://o95ju9jc.cloud.tendacn.net:8080

复制

保存

----完成

## 验证配置

Tenda 技术支持在其电脑（IP 地址为 202.105.88.77）上访问 “http://o95juq6q.cloud.tendacn.net:8080”，即可登录路由器管理页面并对其进行管理。

### 8.3.2 安全设置

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「维护服务」>「安全设置」。

在这里，您可以进行路由器安全设置。

安全设置

防WAN口Ping

开启

●

关闭

内网DDoS攻击防御

开启

●

关闭

ARP攻击防御

开启

●

关闭

二元绑定

开启

●

关闭

Web闲置超时时间

60分钟

▼

保存

#### 参数说明

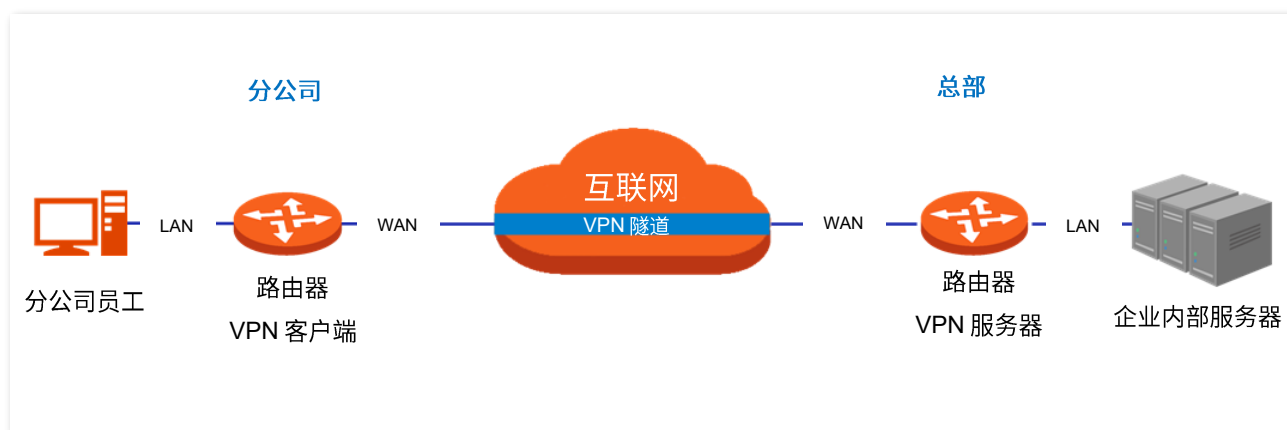
标题项	说明
防 WAN 口 Ping	开启/关闭防 WAN 口 Ping 功能。 开启后，广域网主机 Ping 路由器 WAN 口 IP 地址时，路由器可以自动忽略该 Ping 请求，防止暴露自己，同时防范外部的 Ping 攻击。
内网 DDoS 攻击防御	开启/关闭内网 DDoS 攻击防御功能。 DDoS 攻击，即分布式拒绝服务（Distributed Denial of Service）攻击。利用 DDoS 攻击，攻击者可以消耗目标系统资源，使该目标系统无法提供正常服务。
ARP 攻击防御	开启/关闭 ARP 攻击防御功能。 开启后，路由器可以识别局域网的 ARP 欺骗，并记录攻击者的 MAC 地址。
二元绑定	开启后，仅“DHCP 静态分配”列表中的设备才可以上网。
Web 闲置超时时间	当您登录到路由器的管理页面后，如果在所设置的“WEB 闲置超时时间”内没有任何操作，系统将自动退出登录，保障网络安全。

## 8.4 VPN 服务

### 8.4.1 概述

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

VPN 的典型网络拓扑图如下。



本路由器支持的 VPN 服务有：

- [PPTP/L2TP VPN 客户端](#)
- [IPSec](#)

### 8.4.2 VPN 客户端

#### 配置 VPN 客户端

本路由器可以作为 PPTP/L2TP 客户端连接到 PPTP/L2TP 服务器。

进入页面：[登录路由器 Web 管理页面](#)，点击「更多」>「VPN 客户端」。

VPN 客户端默认关闭，开启后，页面显示如下。

VPN客户端

VPN客户端

☒ 开启 ☐ 关闭

客户端类型

☒ PPTP ☐ L2TP

WAN口

WAN1

服务器IP地址/域名

用户名

密码

加密

☐ 开启 ☒ 关闭

VPN代理上网

☐ 开启 ☒ 关闭

服务器内网网段

服务器内网子网掩码

状态

未连接

保存

参数说明

标题项	说明
VPN 客户端	开启/关闭 VPN 客户端功能。开启后，路由器作为 VPN 客户端。
客户端类型	<p>路由器使用的 VPN 协议类型，PPTP 或 L2TP。PPTP 和 L2TP 都是二层 VPN 隧道协议，使用 PPP（点到点协议）进行数据封装，并都为数据增添额外首部。</p> <p>- PPTP：要连接的 VPN 服务器是 PPTP 服务器时，选择此项。</p> <p>- L2TP：要连接的 VPN 服务器是 L2TP 服务器时，选择此项。</p>
WAN 口	路由器进行 VPN 拨号时使用的 WAN 口。
服务器 IP 地址/域名	要连接的 VPN 服务器的 IP 地址或域名，一般是对端 VPN 路由器上开启了“PPTP/L2TP 服务器”功能的 WAN 口的 IP 地址或域名。
用户名	VPN 服务器分配给 VPN 客户端的用户名和密码。
密码	

标题项	说明
加密	根据 VPN 服务器配置选择是否启用数据加密。请和服务器配置保持一致，否则不能正常通信。只有 PPTP VPN 才支持此选项。
VPN 代理上网	开启后，局域网内的用户通过 VPN 服务器端路由器上网。
服务器内网网段	VPN 服务器端局域网的网段。
服务器内网子网掩码	VPN 服务器端局域网的子网掩码。
状态	当前 VPN 客户端的连接状态。

## PPTP/L2TP VPN 配置举例

### 组网需求

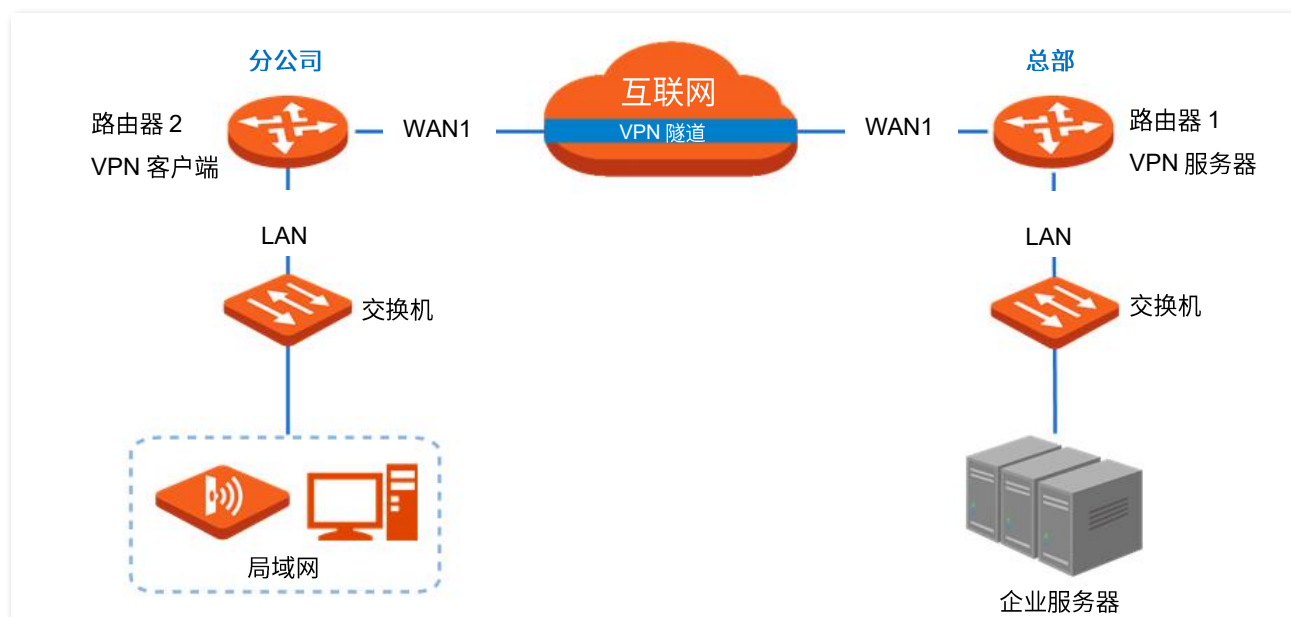
某企业分公司使用企业级无线路由器进行网络搭建，并成功接入互联网。分公司员工需要经过互联网访问企业总部内部局域网资源，如，内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

企业总部使用具备 VPN 服务器功能的企业级路由器进行网络搭建，已配置 PPTP VPN 服务器，并成功接入互联网。

### 方案设计

可以通过设置“VPN 客户端”功能实现上述需求。假设：

- PPTP 服务器与客户端建立隧道的 WAN 口地址为 113.88.112.220
- PPTP 服务器分配的用户名和密码均为 admin1



## 配置步骤

**步骤 1** 登录路由器 Web 管理页面。

**步骤 2** 点击「更多」>「VPN 客户端」。

**步骤 3** 开启“VPN 客户端”。

**步骤 4** 客户端类型保持默认为 PPTP，WAN 口保持默认为 WAN1。

**步骤 5** 输入 VPN 服务器侧作为隧道出口的 WAN 口的 IP 地址或域名，本例为“113.88.112.220”。

**步骤 6** 输入 VPN 客户端进行 VPN 拨号时使用的用户名和密码，本例均为“admin1”。

**步骤 7** 加密方式保持默认为关闭，VPN 代理上网选择开启。

**步骤 8** 点击 **保存**。

VPN客户端

VPN客户端 ☒ 开启 ☐ 关闭

客户端类型 ☒ PPTP ☐ L2TP

WAN口 WAN1

服务器IP地址/域名 113.88.112.220

用户名 admin

密码 .....

加密 ☐ 开启 ☒ 关闭

VPN代理上网 ☒ 开启 ☐ 关闭

状态 未连接

保存

----完成

当页面的状态显示为“已连接”时，VPN 连接成功。之后，分公司和总部的员工就可以通过互联网安全访问对方的局域网资源了。

## 验证配置

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

- FTP 服务器 IP 地址为 192.168.0.104
- FTP 服务端口为 21



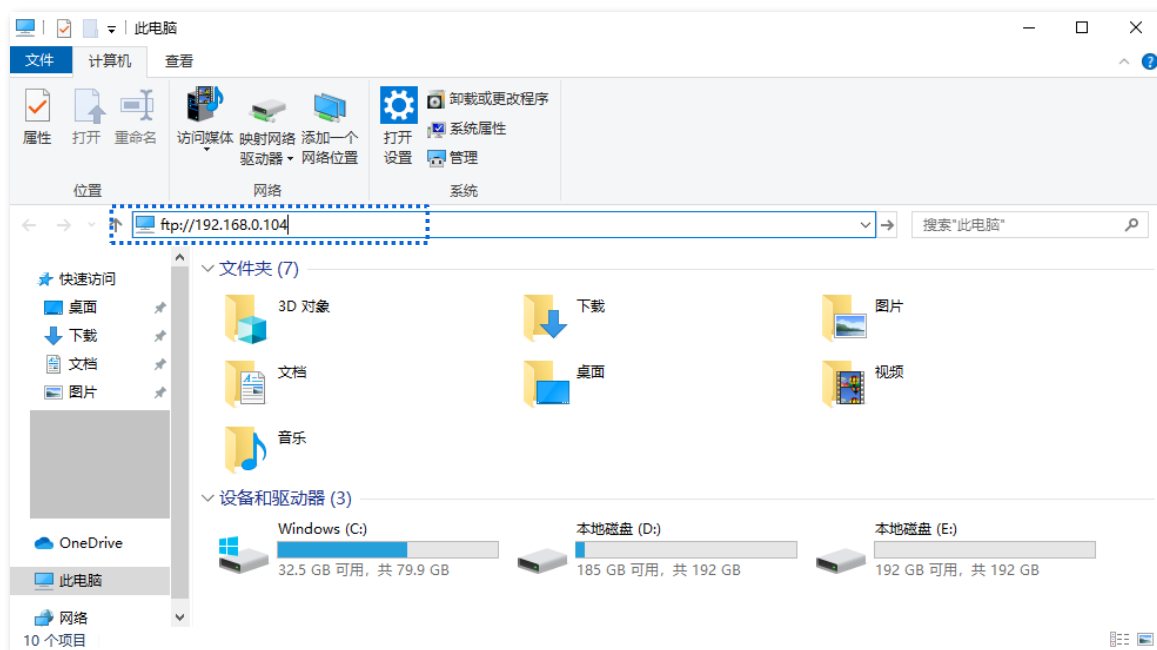
- FTP 服务器登录用户名和密码均为 zhangsan

当分公司员工访问总部项目资料时，步骤如下：

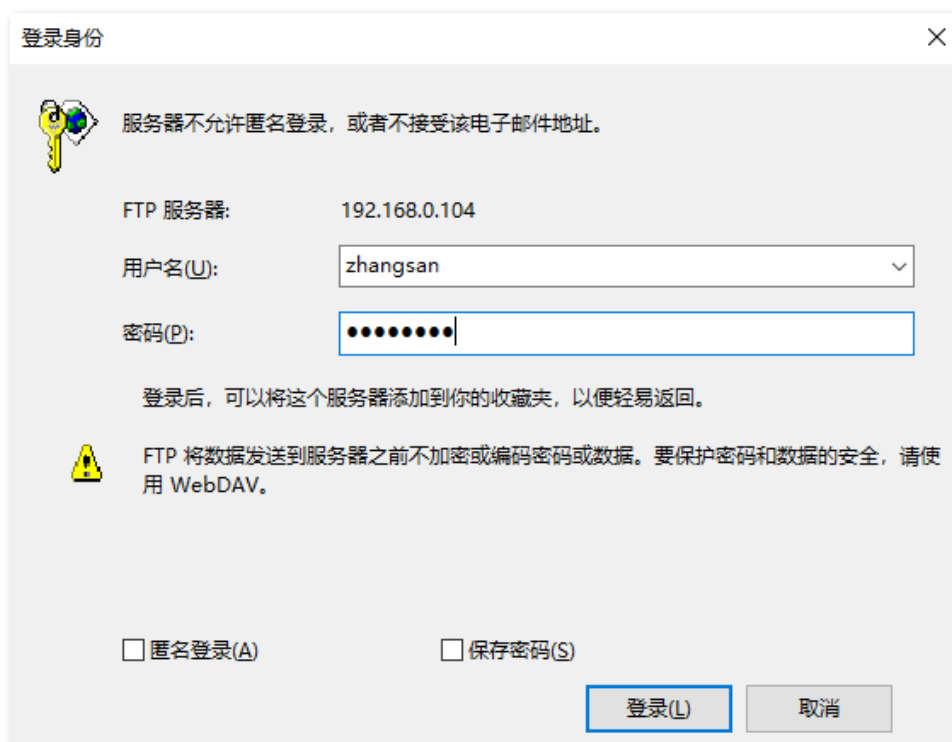
**步骤 1** 在浏览器或“我的电脑”使用“局域网服务应用层协议名称://服务器 IP 地址”，可以成功访问局域网资源。本例为 <ftp://192.168.0.104>。



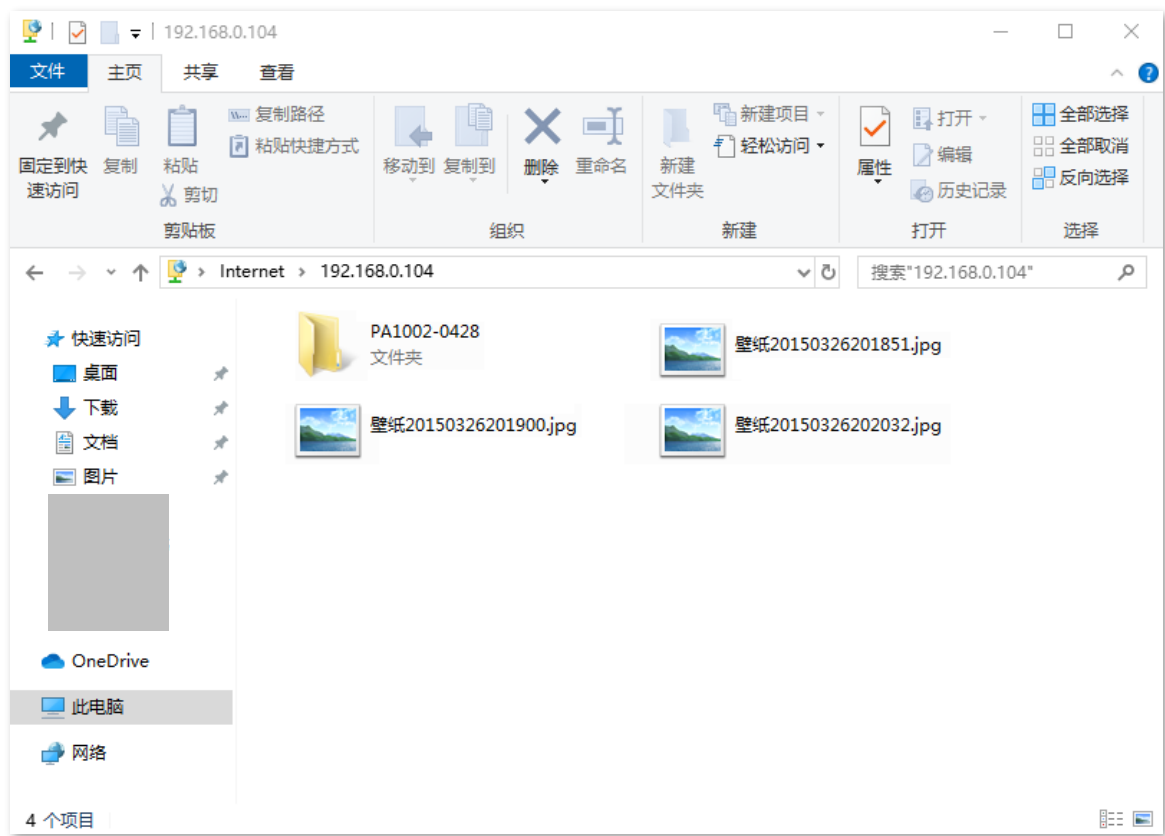
如果局域网服务端口不是默认端口号，访问格式为“局域网服务应用层协议名称://服务器 IP 地址:局域网服务端口”。



**步骤 2** 输入登录用户名和密码，本例均为“zhangsan”，然后点击 **登录**。



访问成功。



### 8.4.3 IPSec

#### 概述

IPSec（IP Security，IP 安全性）是一系列协议的集合，用来实现在互联网上安全、保密地传送数据。

IPSec 相关概念如下：

■ 封装模式

封装模式，即 IPSec 传输的数据的封装模式。IPSec 支持“隧道模式”和“传输模式”两种封装模式。

- 隧道（Tunnel）模式：增加新的 IP 头，通常用于两个安全网关之间的通讯。用户的整个 IP 数据包被用来计算 AH（Authentication Header，鉴别首部）或 ESP（Encapsulating Security Payload，封装安全载荷）头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。
- 传输（Transport）模式：不改变原有的 IP 头部，通常用于主机和主机之间的通信。只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。

协议 \ 模式	隧道模式	传输模式
AH	IP   AH   Data	IP   AH   IP   Data
ESP	IP   ESP   Data   ESP-T	IP   ESP   IP   Data   ESP-T
AH +ESP	IP   AH   ESP   Data   ESP-T	IP   AH   ESP   IP   Data   ESP-T

■ 安全网关

指具有 IPSec 功能的网关设备（安全加密路由器），安全网关之间可以利用 IPSec 对数据进行安全保护，保证数据不被偷窥和篡改。

■ IPSec 对等体

IPSec 的两个端点被称为 IPSec 对等体，要在两个对等体（安全网关）之间安全传输数据，首先要在两者之间建立安全联盟（Security Association，SA）。

■ SA

SA 是通信对等体间对某些要素的约定。如，使用哪种协议（AH、ESP 还是两者结合）、协议的封装模式（传输模式、隧道模式）、加密算法（DES、3DES、AES）、特定流中保护数据的共享密钥以及密钥的生命周期等。SA 具有以下特征：

- 由{ SPI（Security Parameter Index，安全参数索引），IP 目的地址，安全协议标识符}三元组唯一标识。
- 它决定了对报文进行何种处理：协议、算法、密钥。

- SA 是单向的，在两个对等体之间的双向通信，最少需要两个 SA 来分别对两个方向的数据流进行安全保护。另外，如果两个对等体希望同时使用 AH 和 ESP 来进行安全通信，则每个对等体都会针对每一种协议来构建一个独立的 SA。
- SA 可以手工建立或由 IKE (Internet Key Exchange, 互联网密钥交换) 协商生成。IKE 协议分为 IKEv1 和 IKEv2 两个版本，本路由器支持 IKEv1，下文中涉及的 IKE 均指 IKEv1。
  - 手动建立：配置复杂，创建 SA 所需的全部信息必须手动配置，且不支持一些高级特性（如：定时更新密钥）。此时，SA 没有生命周期限制，除非手动删除，否则永不过期，因此有安全隐患。一般用于小型静态环境中，或通信的对等体设备数量较少的情况。
  - IKE 自动协商：配置简单，只需要配置 IKE 协商安全策略的信息，即可由 IKE 自动协商来创建和维护 SA。此时，SA 有生命周期，会定时更新，增强了安全性。一般用于中、大型动态网络环境。

## ■ 建立 SA 的方式

- 手动建立

手动配置 SA 所需的全部信息，包括认证算法、认证密钥、加密算法、加密密钥、SPI 值等。

- IKE 自动协商

自动协商时，为了保证信息的私密性，IPSec 通信双方需要使用彼此都知道的信息来对数据进行加密和解密，所以在通信建立之初双方需要协商安全性密钥，这一过程便由 IKE 完成。

IKE 是 ISAKMP、Oakley、SKEME 这三个协议的混合体。

- ISAKMP: Internet Security Association and Key Management Protocol，互联网安全性关联和密钥管理协议，该协议为交换密钥和 SA 协商提供了一个框架。
- Oakley: 密钥确定协议，该协议描述了密钥交换的具体机制。
- SKEME: 安全密钥交换机制，该协议描述了与 Oakley 不同的另一种密钥交换机制。

IKE 协商过程分为两个阶段：

- 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。

具体完成过程如下：

- 1) 协商确认一系列算法等安全提议，确保对等体双方使用相同的安全提议。
- 2) 根据预共享密钥和协商的安全提议计算出 DH (Diffie-Hellman) 公共值，用于密钥交换。
- 3) 对等体验证，本路由器通过预共享密钥方式来验证对等体合法性。

- 阶段 2

在阶段 1 建立的 ISAKMP SA 上为 IPSec 协商具体的 SA，建立一条用于 IP 数据安全传输的 IPSec SA。

新增 IPSec 连接---隧道模式

[登录路由器 Web 管理页面](#)，进入「更多」>「IPSec」页面，点击 **新增**，然后在出现的页面配置各项参数，点击 **保存**。

本路由器支持“隧道模式”和“传输模式”两种封装模式，默认为“隧道模式”，如下所示。

新增IPSec

IPSec

☒ 开启 ☐ 关闭

WAN口

WAN1

封装模式

隧道模式

隧道名称

协商模式

初始者模式

隧道协议

ESP

远端网关地址

IP地址或域名

本地内网网段/掩码

192.168.100.0/24

!

远端内网网段/掩码

192.168.100.0/24

!

密钥协商方式

自动协商

认证方式

共享密钥方式

预共享密钥

DPD检测

开启

DPD检测周期

10

秒 !

点击隐藏

取消

保存

## 参数说明

标题项	说明
IPSec	开启/关闭 IPSec 功能。
WAN 口	IPSec 生效的 WAN 口，IPSec 对端设备的“远端网关地址”需填为此接口的 IP 地址。
封装模式	<p>IPSec 数据的封装模式。</p> <ul style="list-style-type: none"> <li>- 隧道模式：通常用于两个安全网关之间的通讯。</li> <li>- 传输模式：通常用于主机和主机、主机与网关之间的通信。</li> </ul>
隧道名称	该 IPSec 连接的名称。
协商模式	<p>IPSec 隧道的协商模式。</p> <ul style="list-style-type: none"> <li>- 初始者模式：主动向对端发起连接。</li> <li>- 响应者模式：等待对端发起连接。</li> </ul> <p> <b>注意</b></p> <p>请勿将 IPSec 隧道两端都设置为“响应者模式”，否则会导致 IPSec 隧道建立失败。</p>
隧道协议	<p>为 IPSec 提供安全服务的协议。</p> <ul style="list-style-type: none"> <li>- AH：Authentication Header，鉴别首部。该协议主要提供数据完整性校验功能，若数据报文在传输过程中被篡改，则接收方将在完整性验证时丢弃该报文。</li> <li>- ESP：Encapsulating Security Payload，封装安全性载荷。该协议可以对数据的完整性进行检查，还对数据进行加密，这样，即使报文在传输过程中被截获，截取方也难以获取到真实信息。</li> <li>- AH+ESP：同时使用上述两种协议。</li> </ul>
远端网关地址	<p>IPSec 隧道对端网关的 WAN 口 IP 地址或域名。</p> <p> <b>注意</b></p> <p>设置为域名时，需要在对端网关上设置 DDNS 功能，确保对端网关 WAN 口 IP 地址发生变化时，也不影响 IPSec 隧道的使用。</p>
本地内网网段/掩码	本路由器局域网的网段/前缀长度。例如：本路由器的 LAN 口 IP 地址为 192.168.0.1，子网掩码为 255.255.255.0，则本地内网网段/前缀长度可填为 192.168.0.0/24。
远端内网网段/掩码	IPSec 隧道对端网关局域网的网段/前缀长度。若对端是一台特定主机，则此参数设置为“该设备的 IP 地址/32”。

标题项	说明
密钥协商方式	<p>建立 IPsec 安全隧道的密钥协商方式。本路由器支持“<a href="#">自动协商</a>”和“<a href="#">手动设置</a>”。</p> <ul style="list-style-type: none"><li>- 自动协商：默认模式。通过 IKE 自动建立 SA，并进行动态维护、删除，降低了手工配置的复杂度，简化 IPsec 的使用、管理工作。自动建立的 SA 有生命周期，会定时更新，增强了安全性。</li><li>- 手动设置：用户手动设置加密/认证算法及密钥来建立 SA。手动建立的 SA 没有生命周期限制，除非手动删除，否则永不过期，因此有安全隐患。该方式常用于调试阶段。</li></ul>

### 密钥协商方式--自动协商

自动协商时，为了保证信息的私密性，IPsec 通信双方需要使用彼此都知道的信息来对数据进行加密和解密，所以在通信建立之初双方需要协商安全性密钥，这一过程便由 IKE 完成。IKE 是 ISAKMP、Oakley、SKEME 这三个协议的混合体。

- ISAKMP：Internet Security Association and Key Management Protocol，互联网安全性关联和密钥管理协议，该协议为交换密钥和 SA 协商提供了一个框架。
- Oakley：密钥确定协议，该协议描述了密钥交换的具体机制。
- SKEME：安全密钥交换机制，该协议描述了与 Oakley 不同的另一种密钥交换机制。

IKE 协商过程分为两个阶段：

**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。

密钥协商方式为“自动协商”时，如下图。

密钥协商方式

自动协商

认证方式

共享密钥方式

预共享密钥

DPD检测

开启

DPD检测周期

10

秒 ⓘ

## 参数说明

标题项	说明
认证方式	显示为“共享密钥方式”，表示 IPSec 双方事先通过某种方式协商好一个双方共享的密钥字符串。
预共享密钥	输入协商时所用的预共享密钥，需要与对端网关设备保持一致。最长为 128 字符。
DPD 检测	开启/关闭对等体检测功能。 通过 DPD 检测可以检测远端的隧道站点是否有效。
DPD 检测周期	发送 DPD 报文的周期。 路由器会按照设置的周期定时发送 DPD 报文。如果 DPD 报文在有效时间内没有得到远端的确认，则重新初始化本地到远端的 IPSec SA。

点击[显示高级设置](#)可显示自动协商的高级参数。点击后，页面如下图所示。



点击隐藏

阶段1

模式

Main

加密算法

DES

完整性验证算法

SHA1

Diffie-Hellman分组

768

本地ID类型

IP地址

对端ID类型

IP地址

密钥生命周期

3600

阶段2

PFS

开启

关闭

加密算法

DES

完整性验证算法

SHA1

Diffie-Hellman分组

768

密钥生命周期

3600

参数说明

标题项	说明
	IKE 阶段 1 的交换模式，该交换模式必须与对端设置相同。
模式	<div><div>- Main：主模式，此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。</div><div>- Aggressive：野蛮模式，又称主动模式，此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。</div></div>

标题项	说明
加密算法	<p>应用于 IKE 会话的加密算法。路由器支持以下加密算法：</p> <ul style="list-style-type: none"> <li>- 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。</li> <li>- AES（Advanced Encryption Standard，高级加密标准）：AES 128/192/256 表示使用长度为 128/192/256 bit 的密钥进行加密。</li> </ul>
完整性验证算法	<p>应用于 IKE 会话的验证算法。路由器支持以下验证算法：</p> <ul style="list-style-type: none"> <li>- 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。</li> <li>- 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。</li> </ul>
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。
本地 ID 类型	<p>本地网关标识。</p> <ul style="list-style-type: none"> <li>- IP 地址：本地路由器使用对应 WAN 口 IP 地址与对端网关协商。</li> <li>- FQDN：Fully Qualified Domain Name，完全合格域名。此时需在“本地 ID”输入框中输入任意字符串，用于与对端网关协商。“本地 ID”与远端网关的“对端 ID”必须相同。</li> </ul> <p> <b>注意</b></p> <p>“本地 ID 类型”与“对端 ID 类型”的设置需一致，此时建议将模式改为 Aggressive（野蛮模式）。</p>
对端 ID 类型	<p>对端网关标识。</p> <ul style="list-style-type: none"> <li>- IP 地址：本地网关默认对端网关使用其 WAN 口 IP 地址进行协商。</li> <li>- FQDN：Fully Qualified Domain Name，完全合格域名。此时需在“对端 ID”输入框中输入任意字符串，用于与本地网关协商。“对端 ID”与远端网关的“本地 ID”必须相同。</li> </ul> <p> <b>注意</b></p> <p>“本地 ID 类型”与“对端 ID 类型”的设置需一致，此时建议将模式改为 Aggressive（野蛮模式）。</p>
密钥生命周期	IPSec SA 的生存时间。
PFS	<p>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。</p> <p>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。</p>

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（以隧道协议为“AH+ESP”时为例）。

密钥协商方式	手动设置
ESP加密算法	DES
ESP加密密钥	
ESP认证算法	MD5
ESP认证密钥	
ESP外出SPI	
ESP进入SPI	
AH认证算法	MD5
AH认证密钥	
AH外出SPI	
AH进入SPI	

参数说明

标题项	说明
	当隧道协议选择“ESP”时需设置 ESP 加密算法。路由器支持以下加密算法：
ESP 加密算法	<div><div>- DES：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。</div><div>- AES：AES128/192/256 表示使用长度为 128/192/256bit 的密钥进行加密。</div></div>
ESP 加密密钥	ESP 加密密钥。IPSec 通信双方设置需保持一致。
	当隧道协议选择“ESP”时，需设置 ESP 认证算法；当隧道协议选择“AH”时，需设置 AH 认证算法。路由器支持以下验证算法：
ESP/AH 认证算法	<div><div>- MD5：对一段消息产生 128bit 的消息摘要，防止消息被篡改。</div><div>- SHA1：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。</div></div>

标题项	说明
ESP/AH 认证密钥	当隧道协议选择“ESP”时，需设置 ESP 认证密钥；当隧道协议选择“AH”时，需设置 AH 认证密钥。  IPSec 通信双方设置需保持一致。
ESP/AH 外出 SPI	外出 SPI 参数。  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	进入 SPI 参数。  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。

## 新增 IPSec 连接---传输模式

在「更多」>「IPSec」页面，点击 **新增**，然后在出现的页面封装模式选择“传输模式”，并配置其他各项参数，点击 **保存**。如下所示。

新增IPSec

IPSec

☒ 开启 ☐ 关闭

WAN口

WAN1

封装模式

传输模式

隧道名称

协商模式

初始者模式

加密算法

3DES

完整性验证算法

SHA1

预共享密钥

取消

保存

## 参数说明

标题项	说明
IPSec	开启/关闭 IPSec 功能。
WAN 口	IPSec 生效的 WAN 口，IPSec 对端设备的“远端网关地址”需填为此接口的 IP 地址。
封装模式	<p>IPSec 数据的封装模式。</p> <ul style="list-style-type: none"> <li>- 隧道模式：通常用于两个安全网关之间的通讯。</li> <li>- 传输模式：通常用于主机和主机、主机与网关之间的通信。</li> </ul>
隧道名称	该 IPSec 连接的名称。
协商模式	<p>IPSec 隧道的协商模式。</p> <ul style="list-style-type: none"> <li>- 初始者模式：主动向对端发起连接。</li> <li>- 响应者模式：等待对端发起连接。</li> </ul> <p> <b>注意</b></p> <p>请勿将 IPSec 隧道两端都设置为“响应者模式”，否则会导致 IPSec 隧道建立失败。</p>
加密算法	<p>应用于 IKE 会话的加密算法。路由器支持以下加密算法：</p> <ul style="list-style-type: none"> <li>- 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。</li> <li>- AES（Advanced Encryption Standard，高级加密标准）：AES 128/192/256 表示使用长度为 128/192/256 bit 的密钥进行加密。</li> </ul>
完整性验证算法	<p>应用于 IKE 会话的验证算法。路由器支持以下验证算法：</p> <ul style="list-style-type: none"> <li>- 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。</li> <li>- 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。</li> </ul>
预共享密钥	输入协商时所用的预共享密钥，需要与对端网关设备保持一致。最长为 128 字符。

## IPSec VPN 配置举例

### 组网需求

某企业总部和分公司都使用企业级无线路由器进行网络搭建，并成功接入互联网。分公司员工需要经过互联网访问公司内部局域网资源，如，内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

### 方案设计

在 2 台路由器上均建立 IPSec 隧道，实现远端用户经互联网安全访问企业内部局域网的需求。

假设将路由器 1 部署在总部，基本信息如下：

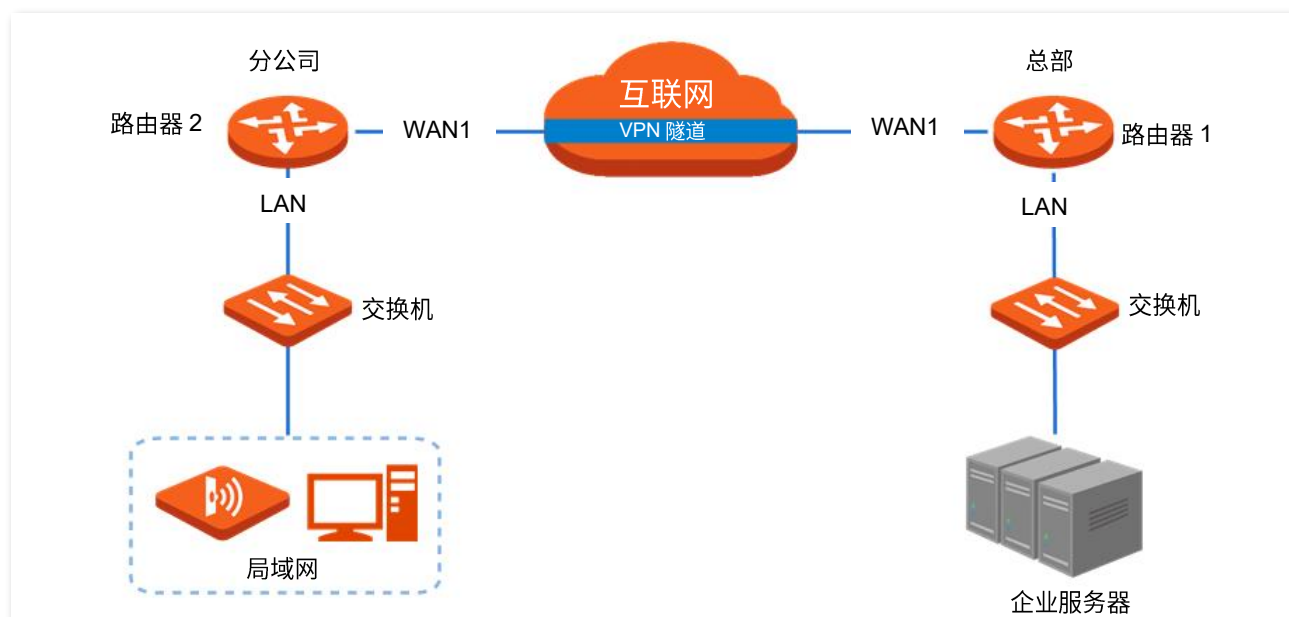
- 建立 IPSec 隧道的接口为 WAN1。
- WAN1 IP 地址为 202.105.11.22。
- 局域网网络为 192.168.0.0/24。

假设将路由器 2 部署在分公司，基本信息如下：

- 建立 IPSec 隧道的接口为 WAN1。
- WAN1 IP 地址为 202.105.88.77。
- 局域网网络为 192.168.1.0/24。

假设两台路由器的 IPSec 连接基本信息如下：

- 封装模式为隧道模式。
- 密钥协商方式为自动协商。
- 预共享密钥为 UmXmL9UK。



### 配置步骤

设置路由器 1

设置路由器 2



配置过程中，如果需要设置 IPSec 连接的高级选项，请保持两台路由器的设置参数一致。

## 步骤 1 设置路由器 1。

1. [登录路由器 1 的 Web 管理页面](#)。
2. 点击「更多」>「IPSec」。
3. 点击 **新增**。



4. 在出现的页面进行如下配置，然后点击 **保存**。
  - (1) 选择本条 IPSec 隧道绑定的 WAN 口，本例为“WAN1”。
  - (2) 选择“封装模式”为“隧道模式”。
  - (3) 为本条隧道设置一个名称，如“IPSec\_1”。
  - (4) 设置“远端网关地址”为对端路由器上 IPSec 隧道绑定的 WAN 口的 IP 地址，本例为“202.105.88.77”。
  - (5) 输入本路由器内网的网段/前缀长度，本例为“192.168.0.0/24”。
  - (6) 输入对端路由器内网的网段/前缀长度，本例为“192.168.1.0/24”。
  - (7) 设置协商时所用的预共享密钥，本例为“UmXmL9UK”。

新增IPSec

IPSec

开启

关闭

\*

WAN口

WAN1

\*

封装模式

隧道模式

\*

隧道名称

IPSec\_1

协商模式

初始者模式

隧道协议

ESP

\*

远端网关地址

202.105.88.77

\*

本地内网网段/掩码

192.168.0.0/24

\*

远端内网网段/掩码

192.168.1.0/24

密钥协商方式

自动协商

认证方式

共享密钥方式

\*

预共享密钥

UmXmL9UK

DPD检测

开启

DPD检测周期

10

秒

路由器 1 的 IPSec 添加完成，如下图示。

IPSec							
<div>新增</div> <div>删除</div>							
<input type="checkbox"/>	隧道状态	WAN口	隧道名称	封装模式	隧道协议	远端网关地址	状态
<input type="checkbox"/>	未连接	WAN1	IPSec_1	隧道模式	ESP	202.105.88.77	已启用
		<div>编辑</div> <div>停用</div> <div>删除</div>					

步骤 2 设置路由器 2。

1. [登录路由器 2 的 Web 管理页面](#)。
2. 点击「更多」>「IPSec」。
3. 点击 

新增

。





4. 在出现的页面进行如下配置后，点击 **保存**。
- (1) 选择本条 IPsec 隧道绑定的 WAN 口，本例为“WAN1”。
  - (2) 选择“封装模式”为“隧道模式”。
  - (3) 为本条隧道设置一个名称，如“IPsec\_1”。
  - (4) 设置“远端网关地址”为对端路由器上 IPsec 隧道绑定的 WAN 口的 IP 地址，本例为“202.105.11.22”。
  - (5) 输入本路由器内网的网段/前缀长度，本例为“192.168.1.0/24”。
  - (6) 输入对端路由器内网的网段/前缀长度，本例为“192.168.0.0/24”。
  - (7) 输入协商时所用的预共享密钥，本例为“UmXmL9UK”。

IPSec

开启

关闭

\*

WAN口

WAN1

\*

封装模式

隧道模式

\*

隧道名称

IPSec\_1

协商模式

初始者模式

隧道协议

ESP

\*

远端网关地址

202.105.11.22

\*

本地内网网段/掩码

192.168.1.0/24

\*

远端内网网段/掩码

192.168.0.0/24

密钥协商方式

自动协商

认证方式

共享密钥方式

\*

预共享密钥

UmXmL9UK

DPD检测

开启

DPD检测周期

10

秒

路由器 2 的 IPSec 添加完成，如下图示。

IPSec							
<div>新增 删除</div>							
<input type="checkbox"/>	隧道状态	WAN口	隧道名称	封装模式	隧道协议	远端网关地址	状态
<input type="checkbox"/>	未连接	WAN1	IPSec_1	隧道模式	ESP	202.105.11.22	已启用
<div>编辑 停用 删除</div>							

----完成

## 验证配置

当规则的“隧道状态”显示为“已连接”时，IPSec 隧道建立成功。之后，分公司和总部的员工就可以通过互联网安全访问对方的局域网资源了。

IPSec

新增

删除

<input type="checkbox"/>	隧道状态	WAN口	隧道名称	封装模式	隧道协议	远端网关地址	状态	操作
<input type="checkbox"/>	已连接	WAN1	IPSec_1	隧道模式	ESP	202.105.11.22	已启用	<a href="#">编辑</a> <a href="#">停用</a> <a href="#">删除</a>

## 8.5 IPv6

### 8.5.1 概述

IPv6（Internet Protocol Version 6，互联网协议第 6 版）是网络层协议的第二代标准协议，属于 IPv4 的升级版，解决了许多当前 IPv4 在地址空间等方面的不足之处。

### IPv6 地址

IPv6 地址总长度为 128 比特，通常分为 8 组，每组为 4 个十六进制数的形式，每组十六进制数间用冒号分隔。一个 IPv6 地址可以分为如下两部分：

- 网络前缀：n 比特，相当于 IPv4 地址中的网络 ID。
- 接口标识：128-n 比特，相当于 IPv4 地址中的主机 ID。

### 基本概念

#### ■ DHCPv6

IPv6 动态主机配置协议 DHCPv6（Dynamic Host Configuration Protocol for IPv6），属于有状态 IPv6 地址自动配置协议。DHCPv6 服务器可以给主机分配 IPv6 地址/前缀和其他网络配置参数。

#### ■ SLAAC

IPv6 的另一种动态主机配置协议 SLAAC（Stateless address autoconfiguration），属于无状态地址自动配置协议。主机通过路由通告（RA）方式自动生成 IPv6 地址/前缀和其他网络配置参数。

## 8.5.2 外网

进入页面：[登录到路由器 Web 管理页面](#)，点击「更多」>「IPv6」>「外网」。

在这里，您可以配置对应 WAN 口的 IPv6 地址信息。路由器 WAN 口支持两种 IPv6 地址获取方式，请根据上级设备的配置选择地址获取方式。

如果	请选择
上级设备的 LAN 口配置的 IP 地址分配方式为 DHCPv6、SLAAC 或 DHCPv6+SLAA	
上级设备为网络运营商设备，且运营商提供支持 IPv6 业务的宽带账号和宽带密码	<a href="#">自动配置</a>
上级设备为网络运营商设备，且运营商未提供具体上网参数	
上级设备不分配 IP 地址	
上级设备为网络运营商设备，且运营商提供了一组用于上网的固定 IPv6 地址，包括 IP 地址、子网掩码、默认网关、DNS 服务器信息	<a href="#">手动设定</a>



如果 WAN 口直连运营商网络，请确保您已开通 IPv6 互联网服务。如果不确定，请先与您的网络运营商联系。

### 自动配置

自动配置，即 WAN 口通过 DHCPv6 或 SLAAC 方式自动获取 IPv6 地址上网信息。WAN 口 IPv6 参数配置完成后，您可以在右侧“连接状态”模块查看 IPv6 联网状态。下图仅供参考。

外网

WAN1

WAN2

状态

开启

关闭

IPv6地址获取方式

自动配置

DNS获取方式

手动设定

首选DNS

备用DNS

(可选)

保存

连接状态

物理连接

联网状态

联网时长

IPv6地址

子网前缀长度

默认网关

首选DNS

备用DNS

参数说明

标题项	说明
模式设定	状态 <div>开启/关闭对应 WAN 口的 IPv6 功能。</div>
	IPv6 地址获取方式 <div>请选择自动配置。</div>
	DNS 获取方式 <div>对应 WAN 口获取 DNS 服务器地址的方式。<div><div>- 自动配置：通过 DHCPv6 或 SLAAC 方式自动获取 DNS 服务器地址。</div><div>- 手动设定：手动输入 DNS 服务器地址。</div></div></div>
	首选 DNS <div>请输入正确的 IPv6 DNS 服务器地址。</div>
	备用 DNS <div><div>提示</div><div>如果只有一个 DNS 地址，“备用 DNS”可以不填。</div></div>
连接状态	物理连接 <div>对应 WAN 口当前的速率和双工模式。</div>
	联网状态 <div>对应 WAN 口的连接状态。<div><div>- 已联网：路由器 WAN 口已插网线，并已经获得 IPv6 地址信息。</div><div>- 联网中...：路由器正在连接到上级网络设备。</div><div>- 未连接：未连接或连接失败，请检查网线连接状态、联网信息设置或咨询相应的网络运营商。</div></div></div>
	联网时长 <div>对应 WAN 口最近一次成功接入 IPv6 网络的时长。</div>
	IPv6 地址 <div>对应 WAN 口的 IPv6 全球单播地址。</div>

标题项	说明
子网前缀长度	IPv6 地址的网络前缀位数。
默认网关	对应 WAN 口的 IPv6 网关地址。
首选 DNS	对应 WAN 口的首选/备用 IPv6 DNS 服务器地址。
备用 DNS	

## 手动设定

手动设定，即手动输入网络运营商提供的 IPv6 地址信息上网。

外网

WAN1

模式设定

状态

开启关闭

IPv6地址获取方式

手动设定

IPv6地址 / 

0

IPv6默认网关

DNS获取方式

手动设定

首选DNS

备用DNS (可选)

保存

连接状态

物理连接

100Mbps全双工

联网状态

未连接

联网时长

0秒

IPv6地址

-

子网前缀长度

-

默认网关

-

首选DNS

-

备用DNS

-

## 参数说明

标题项	说明
模式设定	状态 <div>开启/关闭对应 WAN 口的 IPv6 功能。</div>
	IPv6 地址获取方式 <div>请选择手动设定。</div>
	IPv6 地址 <div>请输入网络运营商提供的 IPv6 全球单播地址。</div>
	IPv6 默认网关 <div>请输入网络运营商提供的 IPv6 网关地址。</div>

标题项	说明
DNS 获取方式	对应 WAN 口获取 IPv6 DNS 服务器地址的方式。 仅支持“手动设定”，即，手动输入 IPv6 DNS 服务器地址。
首选 DNS	请输入正确的 IPv6 DNS 服务器地址。
备用 DNS	如果只有一个 DNS 地址，“备用 DNS”可以不填。
物理连接	对应 WAN 口当前的速率和双工模式。
联网状态	<p>路由器对应 WAN 口的连接状态。</p> <ul style="list-style-type: none"> <li>- 已联网：路由器 WAN 口已插网线，并已经获得 IPv6 地址信息。</li> <li>- 联网中...：路由器正在连接到上级网络设备。</li> <li>- 未连接：未连接或连接失败，请检查网线连接状态、联网信息设置或咨询相应的网络运营商。</li> </ul>
联网时长	对应 WAN 口最近一次成功接入 IPv6 网络的时长。
IPv6 地址	对应 WAN 口的 IPv6 全球单播地址。
子网前缀长度	IPv6 地址的网络前缀位数。
默认网关	对应 WAN 口的 IPv6 网关地址。
首选 DNS	对应 WAN 口的首选/备用 IPv6 DNS 服务器地址。
备用 DNS	

### 8.5.3 局域网

进入页面：[登录到路由器 Web 管理页面](#)，点击「更多」>「IPv6」>「局域网」。

在这里，您可以配置对应 VLAN 接口的 IPv6 地址信息，实现局域网内多台共享您办理的宽带服务上网。

VLAN 接口默认关闭 IPv6 功能，开启后，如下图所示。

局域网

VLAN接口

VLAN\_Default

▼

状态

☒ 开启

☐ 关闭

IPv6地址获取方式

自动配置

▼

前缀代理接口

--未选择--

▼

IPv6地址前缀

::

/

64

IPv6地址

地址分配方式

SLAAC

▼

首选寿命

6300

秒

有效寿命

7200

秒

首选DNS

(可选)

备用DNS

(可选)

保存

参数说明

标题项	说明
VLAN 接口	需配置 IPv6 功能的 VLAN 接口。
状态	开启/关闭该 VLAN 接口的 IPv6 功能
IPv6 地址获取方式	<div>VLAN 接口获取 IP 地址的方式。</div> <div><div>- 自动配置：VLAN 接口的 IPv6 地址前缀由“前缀代理接口”从上级设备处获取，接口地址由路由器根据标准自动生成。</div><div>- 手动配置：手动设置 VLAN 接口的 IP 地址前缀、完整的 IPv6 地址及地址分配方式。</div></div>
前缀代理接口	VLAN 接口的 IPv6 地址前缀由该 WAN 口从上级设备处获取。“IPv6 地址获取方式”为“自动配置”时需要选择此项。
IPv6 地址前缀	VLAN 接口的 IPv6 地址前缀。
IPv6 地址	VLAN 接口完整的 IPv6 地址。



标题项	说明
地址分配方式	<p>路由器给局域网客户端分配 IPv6 地址的方式。</p> <ul style="list-style-type: none"> <li>- DHCPv6: 客户端直接从 DHCPv6 服务器获取全部的 IPv6 地址信息，包括 DNS 服务器等。</li> <li>- SLAAC: 客户端通过路由通告（RA）方式自动生成 IPv6 地址信息，包括 IPv6 地址、DNS 服务器等。</li> <li>- SLAAC+DHCPv6: 客户端通过路由通告（RA）方式自动生成 IPv6 地址，从 DHCPv6 服务器获取其他地址信息，如 DNS 服务器等。</li> </ul>
开始地址	DHCPv6 服务器可分配的 IPv6 地址地址范围。
结束地址	地址分配方式为 DHCPv6 时需要配置此项。
首选寿命	IPv6 地址租借期限的首选生命期。如果客户端在首选生命周期时间内未收到路由通告（RA），则会将该 IPv6 地址废止，不再使用该 IPv6 地址建立新的连接，但接收目的地址为该 IPv6 地址的报文。
有效寿命	IPv6 地址租借期限的有效生命期。到期后该 IPv6 地址将被删除，变成无效地址，断开所有会话。
首选 DNS	分配给客户端的首选/备用 DNS 服务器 IP 地址。
备用 DNS	<p> 注意</p> <p>为了使局域网设备能够正常上网，请务必确保修改的首选 DNS 是正确的 DNS 服务器或 DNS 代理的 IP 地址。</p>

# 9 系统工具

## 9.1 系统时间

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「系统时间」。

在这里，您可以设置路由器的系统时间。

为了保证路由器基于时间的功能正常生效，需要确保路由器的系统时间准确。路由器支持[与网络时间同步](#)和[手动设置系统时间](#)两种时间设置方式，默认为“与网络时间同步”。

### 9.1.1 与网络时间同步

使用此方式时，系统时间自动同步互联网上的时间服务器。只要路由器成功连接到互联网就能自动校准其系统时间，无需重新设置。

设置完成后刷新一下页面，您可以查看路由器的当前时间是否校对准确。

系统时间

当前时间

2023-07-27 16:22:05

设置时间

☒ 与网络时间同步

☐ 手动设置系统时间

同步周期

1小时

选择时区

(GMT+08:00) 北京, 重庆, 等

保存

#### 参数说明

标题项	说明
当前时间	路由器当前的系统时间。
设置时间	路由器系统时间的设置方式，选择与网络时间同步。
同步周期	路由器向互联网上的时间服务器校对系统时间的时间间隔。

标题项	说明
选择时区	选择路由器当前所在地区的标准时区。

### 9.1.2 手动设置系统时间

使用此方式时，路由器每次重启后，您都需要重新设置系统时间。选择“手动设置系统时间”时，页面展开的相关参数如下图所示。

设置完成后刷新一下页面，您可以查看路由器的当前时间是否校对准确。

系统时间

当前时间

2023-07-27 16:22:42

设置时间

☐

与网络时间同步

☒

手动设置系统时间


日期时间

2023-07-27 16:17:09

同步当前电脑时间

保存

#### 参数说明

标题项	说明
当前时间	路由器当前的系统时间。
设置时间	路由器系统时间的设置方式，选择手动设置系统时间。
日期时间	点击  选择正确的时间，也可以点击 <b>同步当前电脑时间</b> 将正在管理路由器的电脑的时间同步到路由器。

## 9.2 排障工具

### 9.2.1 Ping

Ping 用于检测网络的连通性和连通质量。

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「排障工具」。

在这里，您可以通过 Ping 工具检测网络连通性和连通质量。

假设要检测路由器到 QQ 官网（www.qq.com）的链路是否畅通。

执行 Ping：

**步骤 1** [登录到路由器 Web 管理页面](#)，点击「工具」>「排障工具」。

**步骤 2** 选择“工具”为“Ping”。

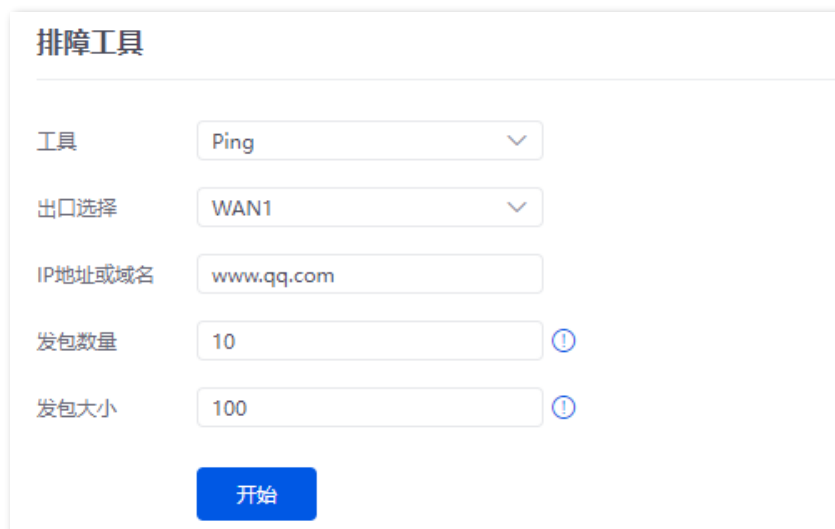
**步骤 3** 选择数据出去的接口，本例为“WAN1”。

**步骤 4** 输入目的 IP 地址或域名，本例为“www.qq.com”。

**步骤 5** 设置 ping 发送的数据包的个数，如“10”。

**步骤 6** 设置 ping 发送的数据包的大小，如“100”。

**步骤 7** 点击 **开始**。



The screenshot shows the '排障工具' (Troubleshooting Tools) section of a router's web management interface. It contains a form for configuring a Ping test. The form has five rows of input fields: '工具' (Tool) with a dropdown menu set to 'Ping'; '出口选择' (Exit Selection) with a dropdown menu set to 'WAN1'; 'IP地址或域名' (IP Address or Domain Name) with a text input field containing 'www.qq.com'; '发包数量' (Number of Packets) with a text input field containing '10' and a help icon; and '发包大小' (Packet Size) with a text input field containing '100' and a help icon. At the bottom of the form is a blue button labeled '开始' (Start).

----完成

## 参数说明

标题项	说明
出口选择	选择数据出去的接口。
IP 地址或域名	要检测的目的 IP 地址或域名。
发包数量	ping 发送的数据包的个数。
发包大小	ping 发送的数据包的大小。

稍后，诊断结果将显示在页面下方。如下图所示。

## 诊断结果

```
PING ins-r23tsuuf.ias.tencent-cloud.net (61.241.54.232) from 192.168.96.47 eth0: 100(128) bytes of data.
108 bytes from 61.241.54.232: icmp_seq=1 ttl=55 time=6.56 ms
108 bytes from 61.241.54.232: icmp_seq=2 ttl=55 time=6.06 ms
108 bytes from 61.241.54.232: icmp_seq=3 ttl=55 time=6.12 ms
108 bytes from 61.241.54.232: icmp_seq=4 ttl=55 time=6.14 ms
108 bytes from 61.241.54.232: icmp_seq=5 ttl=55 time=6.40 ms
108 bytes from 61.241.54.232: icmp_seq=6 ttl=55 time=6.11 ms
108 bytes from 61.241.54.232: icmp_seq=7 ttl=55 time=6.32 ms
108 bytes from 61.241.54.232: icmp_seq=8 ttl=55 time=10.6 ms
108 bytes from 61.241.54.232: icmp_seq=9 ttl=55 time=6.22 ms
108 bytes from 61.241.54.232: icmp_seq=10 ttl=55 time=6.07 ms

--- ins-r23tsuuf.ias.tencent-cloud.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 861ms
rtt min/avg/max/mdev = 6.061/6.661/10.630/1.334 ms
```

## 9.2.2 Tracert

Tracert 用于检测数据包从路由器到目标主机所经过的路由。

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「排障工具」。

在这里，您可以通过 Tracert 工具检测数据包到达目标地址所经过的路由。

假设要检测路由器到 QQ 官网（www.qq.com）所经过的路由。

执行 Tracert：

**步骤 1** [登录到路由器 Web 管理页面](#)，点击「工具」>「排障工具」。

- 步骤 2** 选择“工具”为“Tracert”。
- 步骤 3** 选择数据出去的接口，本例为“WAN1”。
- 步骤 4** 输入目的 IP 地址或域名，本例为“www.qq.com”。
- 步骤 5** 点击 **开始**。

排障工具

工具

Tracert

出口选择

WAN1

IP地址或域名

www.qq.com

开始

----完成

参数说明

标题项	说明
出口选择	选择数据出去的接口。
IP 地址或域名	要检测的目的 IP 地址或域名。

稍后，诊断结果将显示在页面下方。如下图示例。

诊断结果

```
tracert to www.qq.com (61.241.54.232), 30 hops max, 60 byte packets
1 _gateway (192.168.96.1) 9.363 ms 9.912 ms 10.783 ms
2 192.168.254.2 (192.168.254.2) 0.968 ms 0.950 ms 0.940 ms
3 58.250.161.1 (58.250.161.1) 7.301 ms 8.066 ms 8.053 ms
4 120.80.145.69 (120.80.145.69) 4.975 ms * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 61.241.54.232 (61.241.54.232) 5.939 ms 5.904 ms 5.888 ms
```

### 9.2.3 抓包工具

抓包工具，可以将网络中传送的数据包完全截获下来提供分析。

在进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「排障工具」。

在这里，您可以通过抓包工具对某一接口特定的数据包进行抓取。

假设要截获路由器 LAN4 口的所有类型数据包，LAN4 口 IP 地址为 192.168.0.250，属于 VLAN\_Default。

执行抓包：

**步骤 1** [登录到路由器 Web 管理页面](#)，点击「工具」>「排障工具」。


**步骤 2** 选择“工具”为“抓包工具”。

**步骤 3** 选择要截获数据的 VLAN 接口，本例为“VLAN\_Default”。

**步骤 4** 输入 LAN4 口 IP 地址，本例为“192.168.0.250”。

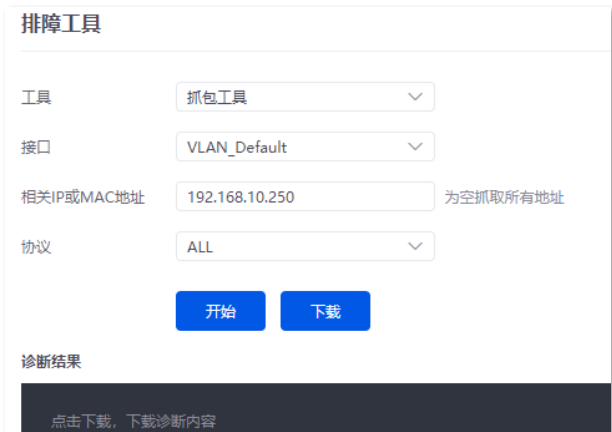
**步骤 5** 选择数据协议类型，本例为“ALL”。

**步骤 6** 点击 **开始**。



**步骤 7** 抓包过程中，可根据需要点击 **结束**。

**步骤 8** 点击 **下载**。pcap 类型的文件将下载到本地电脑，可以用抓包软件（WireShark）打开查看。



---完成

参数说明

标题项	说明
接口	要截获数据的 VLAN 接口。
相关 IP 或 MAC 地址	<p>接口连接的设备的 IP 或 MAC 地址。为空表示抓取 VLAN 下所有接口的数据报文。</p> <p> <b>提示</b></p> <p>如果所填的 IP 地址或 MAC 地址在网络中不存在，或不在所设置的 VLAN 接口下，则不会截获到报文。</p>
协议	<p>数据协议类型。ALL 表示包括 ICMP、TCP、UDP 和 ARP 四种协议。</p> <ul style="list-style-type: none"><li>- ICMP：Internet Control Message Protocol，即 Internet 控制报文协议。用于在 IP 主机、路由器之间传递控制消息，包括网络通不通、主机是否可达、路由是否可用等。</li><li>- TCP：Transmission Control Protocol，即面向连接的通信协议。通过三次握手建立连接，通讯完成时要拆除连接，只能用于端到端的通讯，如 Telnet、FTP。</li><li>- UDP：User Datagram Protocol，即用户数据报协议。UDP 数据包括目的端口和源端口信息，通讯不需要连接，可以实现广播发送。使用 UDP 的服务包括 DNS、SNMP 等。</li><li>- ARP：Address Resolution Protocol，即地址解析协议，是根据 IP 地址获取物理地址的一个 TCP/IP 协议。</li></ul>

9.2.4 系统诊断

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「排障工具」。

在这里，您可以执行系统诊断，查看系统所有进程的状态信息。

执行系统诊断：

**步骤 1** [登录到路由器 Web 管理页面](#)，点击「工具」>「排障工具」。

**步骤 2** 选择“工具”为“系统诊断”。

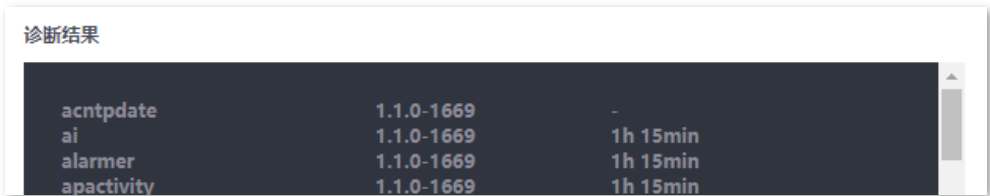
**步骤 3** 点击 **开始**。





----完成

稍等片刻，结果将会显示在下方区域，拉动滚动条可以查看更多信息，如下图示。



## 9.2.5 接口信息

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「排障工具」。

在这里，您可以查看设备接口信息，包括物理接口、桥接口、隧道接口、VLAN 虚拟接口。桥接口和 VLAN 虚拟接口在创建 VLAN 接口时生成，但 VLAN 为 1 时不生成 VLAN 虚拟接口；隧道接口在创建 SSID 策略时生成。

执行步骤：

**步骤 1** [登录到路由器 Web 管理页面](#)，点击「工具」>「排障工具」。

**步骤 2** 选择“工具”为“接口信息”。

**步骤 3** 点击 **开始**。



----完成

稍等片刻，结果将会显示在下方区域，拉动滚动条可以查看更多信息，如下图示。

## 诊断结果

```
br0    Link encap:Ethernet  HWaddr D8:38:0D:3D:7D:E0  
        inet addr:192.168.0.252  Bcast:192.168.0.255  Mask:255.255.255.0  
        inet6 addr: fe80::da38:dff:fe3d:7de0/64 Scope:Link  
        UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1  
        RX packets:717185 errors:0 dropped:1326 overruns:0 frame:0  
        TX packets:183431 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1000
```

### 9.3 日志中心

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「日志中心」。

在这里，您可以查看路由器记录的日志信息。

日志中心记录了路由器的系统日志、操作日志和运行日志。如遇网络故障，可以利用路由器的日志信息进行问题排查。

#### 9.3.1 系统日志

系统日志记录系统运行相关日志信息，如 DHCP 日志、拨号日志等。点击下拉框选择相应日志类型即可查看。

系统日志 <span>?</span>				
<div><div>全部导出</div><div>全部删除</div></div>		系统日志	2023-07-31 → 2023-07-31	<div>搜索</div>
序号	发生时间 ↓	日志内容	操作者	功能模块
1	2023-07-31 17:00:56	Sync time success!	system	system
2	2023-07-31 16:53:10	Sync time success!	system	system
3	2023-07-31 16:47:06	Sync time success!	system	system
4	2023-07-31 15:56:53	Sync time success!	system	system
5	2023-07-31 14:56:48	Sync time success!	system	system
6	2023-07-31 14:26:05	Sync time success!	system	system
7	2023-07-31 13:25:55	Sync time success!	system	system
8	2023-07-31 12:25:45	Sync time success!	system	system
9	2023-07-31 11:25:40	Sync time success!	system	system
10	2023-07-31 10:25:29	Sync time success!	system	system

日志记录时间以路由器的系统时间为准，为确保日志记录时间准确，请先准确设置路由器的系统时间。可以到[系统时间](#)页面校准路由器的系统时间。

#### 9.3.2 操作日志

操作日志记录用户对路由器进行的操作，如登录日志、配置变更等。点击下拉框选择相应日志类型即可查看。

操作日志 <span>?</span>				
<div><div>全部导出</div><div>全部删除</div></div>		登录日志	2023-07-27 → 2023-07-27	<div>搜索</div>
序号	发生时间 ↓	日志内容	操作者	功能模块
1	2023-07-27 15:13:10	192.168.0.164 login webservice success.	admin	login

日志记录时间以路由器的系统时间为准，为确保日志记录时间准确，请先准确设置路由器的系统时间。可以到[系统时间](#)页面校准路由器的系统时间。

### 9.3.3 运行日志

运行日志记录系统进程运行、接口状态等信息。点击下拉框选择相应日志类型即可查看。

运行日志

全部导出

全部删除

接口状态日志

2023-07-31 → 2023-07-31

搜索

序号	发生时间 ↓	日志内容	操作者	功能模块
1	2023-07-31 08:36:33	WAN2 is UP.	system	interface
2	2023-07-31 08:36:29	WAN2 is DOWN.	system	interface

日志记录时间以路由器的系统时间为准，为确保日志记录时间准确，请先准确设置路由器的系统时间。可以到[系统时间](#)页面校准路由器的系统时间。

## 9.4 系统维护

### 9.4.1 设备信息

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「系统维护」>「设备信息」。

在这里，您可以查看路由器的基本信息，包括 CPU 使用率、内存使用率、系统时间和系统运行时长。

设备信息

CPU使用率

7%

内存使用率

50%

系统时间

2023-07-27 16:37:46

系统运行时长

1天 1小时 17分钟 53秒

## 9.4.2 配置备份与恢复

### 概述

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

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

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「系统维护」>「配置备份与恢复」。

在这里，您可以对路由器进行备份和恢复操作。

### 备份配置

**步骤 1** [登录到路由器 Web 管理页面](#)。

**步骤 2** 点击「工具」>「系统维护」>「配置备份与恢复」。

**步骤 3** 点击 **导出**。



——完成

浏览器将下载文件名为 RouterCfm.cfg 的配置文件。



提示

若页面出现类似“由于此类型的文件可能会损坏你的设备，RouterCfm.cfg 被阻止。”的提示，请选择“保留”。

### 恢复配置

**步骤 1** [登录到路由器 Web 管理页面](#)。

**步骤 2** 点击「工具」>「系统维护」>「配置备份与恢复」。

**步骤 3** 点击 **浏览**，选择并加载之前备份的配置文件。



**步骤 4** 点击 **导入**。



**步骤 5** 确认提示信息后，点击 **确定**。

---完成

将出现恢复进度提示，请耐心等待。进度条显示 100%时，路由器配置恢复完成。

## 9.4.3 恢复出厂设置

### 概述

当局域网用户不能访问互联网，且无法定位问题原因时；或您需要登录路由器的管理页面，却忘记登录密码时，可以将路由器恢复出厂设置后重新设置。路由器支持[软件恢复出厂设置](#)和[硬件恢复出厂设置](#)两种方式。

恢复出厂设置后，路由器的 LAN 口 IP 地址为 192.168.0.1。



注意

- 恢复出厂设置后，路由器的所有设置将会恢复到出厂状态，您需要重新设置路由器才能上网。请谨慎操作。
- 为避免损坏路由器，恢复出厂设置过程中，请确保路由器供电正常。

### 软件恢复出厂设置

**步骤 1** [登录到路由器 Web 管理页面](#)。

**步骤 2** 点击「工具」>「系统维护」>「恢复出厂设置」。

**步骤 3** 点击 **恢复出厂**。



**步骤 4** 确认提示信息后，点击 **确定**。

---完成

将出现恢复出厂进度提示，请耐心等待。进度条显示 100%时，路由器恢复出厂完成，请重新设置路由器。

### 硬件恢复出厂设置

使用此方式时，您无需进入路由器管理页面就可以将路由器恢复出厂设置。操作方法如下：

路由器 SYS 灯闪烁状态下，用针状物按住机身上的 **Reset/扩展按钮** 约 8 秒，待指示灯全亮时松开。当 SYS 灯重新闪烁时，路由器恢复出厂设置成功。

## 9.5 升级服务

### 9.5.1 概述

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「升级服务」。

在这里，您可以对路由器进行软件升级和特征库升级，获得更好的用户体验。

- 系统软件升级：您可以通过升级路由器软件，体验更多功能，获得更好的用户体验。支持“本地升级”和“在线升级”两种升级方式。默认为“本地升级”。
- 特征库升级：更新路由器的特征库。升级特征库不会对路由器系统软件产生影响。支持“本地升级”和“在线升级”两种升级方式。默认为“本地升级”。

#### 参数说明

标题项	说明
本地升级	先访问 Tenda 官方网站 <a href="http://www.tenda.com.cn">www.tenda.com.cn</a> ，搜索相应产品型号，下载升级文件到本地电脑，然后再进行升级。
在线升级	联网后，路由器系统自动检测是否有新的升级文件，并显示检测结果。如果检测到新的软件版本，您可以根据需要进行升级。升级时，点击 <b>升级</b> ，系统将自动下载升级文件，并进行升级。

### 9.5.2 系统软件本地升级



注意

- 为避免路由器损坏，请使用正确的升级文件进行升级。一般情况下，软件升级文件的文件后缀为.bin。
- 升级过程中，请勿断开路由器电源。

**步骤 1** 访问 Tenda 官网 [www.tenda.com.cn](http://www.tenda.com.cn)，下载对应型号路由器的软件升级文件到本地电脑并解压。

**步骤 2** [登录到路由器 Web 管理页面](#)，点击「工具」>「升级服务」>「系统软件升级」。

**步骤 3** 选择“升级方式”为“本地升级”。

**步骤 4** 点击 **浏览**，找到并载入相应目录下的升级软件，然后点击 **升级**。



### 系统软件升级

当前软件版本

V16.01.0.5(1357)

升级方式

☒ 本地升级 ☐ 在线升级

升级文件路径

US\_W18EV2.0

浏览

升级

**步骤 5** 确认提示信息后，点击 **确定**。

----完成

等待进度条走完即可。进度条走完后，您可重新登录路由器，进入「工具」>「升级服务」>「系统软件升级」页面，查看路由器当前的软件版本号来确认是否升级成功。



提示

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

## 9.5.3 特征库本地升级



- 为避免路由器损坏，请使用正确的升级文件进行升级。一般情况下，特征库升级文件的文件后缀为.bin。
- 升级过程中，请勿断开路由器电源。

**步骤 1** 访问 Tenda 官网 [www.tenda.com.cn](http://www.tenda.com.cn)，下载对应型号的路由器最新的特征库文件并存放到本地电脑。

**步骤 2** [登录到路由器 Web 管理页面](#)，点击「系统工具」>「升级服务」>「特征库升级」。

**步骤 3** 选择“升级方式”为“本地升级”。

**步骤 4** 点击 [浏览](#)，找到并载入相应目录下的特征库文件，然后点击 [升级](#)。

特征库升级

当前软件版本 v1.0

升级方式 ☒ 本地升级 ☐ 在线升级

升级文件路径  浏览

升级

----完成

等待进度条走完即可。进度条走完后，您可重新登录路由器，进入「系统工具」>「升级服务」>「特征库升级」页面，查看当前的特征库版本号来确认是否升级成功。

## 9.6 重启

### 9.6.1 立即重启

您可以立即重启路由器，使某些配置生效，或者提升运行性能。重启过程中将断开当前网络连接，过程约 1 分钟。请在网络相对空闲时重启。

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「重启服务」>「重启」。

在这里，您可以点击 [重启设备](#)，来立即重启路由器。



## 9.6.2 定时重启

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「重启服务」>「定时重启」。

在这里，您可以设置路由器在空闲时间周期性地定时自动重启，预防路由器长时间运行导致其出现性能下降、不稳定等现象。



定时重启时间以路由器的系统时间为准，为避免重启时间出错，请确保路由器的[系统时间](#)准确。

定时重启步骤：

- 步骤 1** [登录到路由器 Web 管理页面](#)。
- 步骤 2** 点击「工具」>「重启服务」>「定时重启」。
- 步骤 3** 开启定时重启功能。
- 步骤 4** 选择路由器自动重启的时间点，如“03:00”。
- 步骤 5** 设置重启日期，如“星期四”。
- 步骤 6** 点击 **保存**。



----完成

如上图设置完成后，每个星期四的凌晨 3 点，路由器将自动重启。

## 9.7 系统账号

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「系统账号」。

在这里，您可以添加/修改/删除管理员账号和访客账号。



### 参数说明

标题项	说明
	登录路由器 Web 管理页面的账号类型。
角色	<ul style="list-style-type: none"><li>- 管理员：使用此账号登录路由器后，您可以查看、配置路由器的所有功能。</li><li>- 访客：使用此账号登录路由器后，您可以查看路由器除系统账号信息之外的其他功能配置。</li></ul>
密码	设置账号对应的登录密码。
确认密码	
备注	账户的备注信息。
登录 IP 限制	设置后，只有该 IP 地址或 IP 地址段的用户可以使用该账号登录设备管理页面，不设置则不限制 IP 地址。

## 9.8 诊断

进入页面：[登录到路由器 Web 管理页面](#)，点击「工具」>「诊断」。

在这里，您可以点击 **诊断** 对路由器 WAN 口进行联网诊断。

诊断

网口选择

WAN1

▼

WAN口诊断

宽带拨号, 已插入网线, 已联网

DNS诊断

正常

延时诊断

6ms

HTTP访问诊断

正常

诊断

参数说明

标题项	说明
网口选择	需要诊断的 WAN 口。
WAN 口诊断	检查 WAN 口的上网方式、接线情况及联网状态。
DNS 诊断	检查 WAN 口是否能够正常解析域名。
延时诊断	检查 WAN 口的网络延迟情况。
HTTP 访问诊断	检查 WAN 口是否能够正常收到 HTTP 响应。

# 附录

## 缩略语

缩略语	全称
AES	高级加密标准（Advanced Encryption Standard）
AH	鉴别首部（Authentication Header）
APSD	自动省电模式（Automatic Power Save Delivery）
ARP	地址解析协议（Address Resolution Protocol）
CPU	中央处理器（Central Processing Unit）
DDNS	动态域名服务（Dynamic Domain Name Server）
DDoS	分布式拒绝服务（Distributed Denial of Service）
DES	数据加密标准（Data Encryption Standard）
DHCP	动态主机配置协议（Dynamic Host Configuration Protocol）
DMZ	非军事区（Demilitarized zone）
DNS	域名系统（Domain Name System）
DPD	失效对等体检测（Dead Peer Detection）
ESP	封装安全载荷（Encapsulating Security Payload）
FQDN	完全合格域名（Fully Qualified Domain Name）
FTP	文件传输协议（File Transfer Protocol）
GMT	格林威治时间（Greenwich Mean Time）

缩略语	全称
HTTP	超文本传送协议（HyperText Transfer Protocol）
HTTPS	超文本传输安全协议（Hypertext Transfer Protocol Secure）
ICMP	网际控制报文协议（Internet Control Message Protocol）
IKE	互联网密钥交换（Internet Key Exchange）
IP	互联网协议（Internet Protocol）
IPv6	互联网协议第 6 版（Internet Protocol Version 6）
IPSec	互联网安全协议（Internet Protocol Security）
ISAKMP	互联网安全性关联和密钥管理协议（Internet Security Association and Key Management Protocol）
ISP	互联网服务提供商（Internet Service Provider）
LAN	局域网（Local Area Network）
L2TP	二层隧道协议（Layer 2 Tunneling Protocol）
MAC	媒体接入控制（Medium Access Control）
MTU	最大传输单元（Maximum Transmission Unit）
NAT	网络地址转换（Network Address Translation）
PFS	完全前向保密（Perfect Forward Secrecy）
PPP	点对点协议（Point to Point Protocol）
PPTP	点对点隧道协议（Point to Point Tunneling Protocol）
SA	安全联盟（Security Association）
SHA	安全散列算法（Secure Hash Algorithm）
SLAAC	无状态地址自动配置（Stateless address autoconfiguration）
SMTP	简单邮件传输协议（Simple Mail Transfer Protocol）
SSID	服务集标识符（Service Set Identifier）

缩略语	全称
SSL	安全套接层(Secure Sockets Layer)
SPI	安全参数索引 (Security Parameter Index)
TCP	传输控制协议 (Transmission Control Protocol)
UDP	用户数据报协议 (User Datagram Protocol)
URL	统一资源定位符 (Uniform Resource Locator)
UPnP	通用即插即用 (Universal Plug and Play)
VLAN	虚拟局域网 (Virtual Local Area Network)
VPN	虚拟专用网络 (Virtual Private Network)
WAN	广域网 (Wide Area Network)
WMM	无线多媒体 (Wi-Fi multi-media)
WPA	Wi-Fi 网络安全接入 (Wi-Fi Protected Access)
WPA-PSK	WPA 预共享密钥 (WPA-Preshared Key)