

The logo for TP-LINK, featuring the brand name in a bold, black, sans-serif font. A registered trademark symbol (®) is located at the top right of the 'K'.

150M 室外高功率无线接入器

TL-WA7210N

详细配置指南

声明

Copyright © 2014 普联技术有限公司

版权所有，保留所有权利

未经普联技术有限公司明确书面许可，任何单位或个人不得擅自仿制、复制、誊抄或转译本书部分或全部内容。不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。

TP-LINK® 为普联技术有限公司注册商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。

目录

第 1 章	产品概述	1
1.1	产品简介	1
1.2	主要特性	1
1.3	本书约定	2
第 2 章	硬件描述	3
2.1	前面板示意图	3
2.2	后面板	4
2.3	系统需求	4
2.4	安装环境	4
第 3 章	快速安装指南	5
3.1	硬件连接	5
3.1.1	AP 客户端路由模式	5
3.1.2	AP 路由模式	5
3.1.3	接入点模式	6
3.1.4	多 SSID 模式	6
3.1.5	中继模式	7
3.1.6	桥接模式	7
3.1.7	客户端模式	8
3.2	建立正确的网络连接	8
3.3	快速安装指南	11
3.3.1	AP 客户端路由	13
3.3.2	AP 路由	16
3.3.3	接入点	19
3.3.4	多 SSID	20
3.3.5	中继	23
3.3.6	桥接	26
3.3.7	客户端	29
第 4 章	接入点模式、多 SSID 模式、中继模式、桥接模式和客户端模式	32
4.1	登录	32
4.2	运行状态	32
4.3	设置向导	33
4.4	工作模式	33

4.5	网络参数.....	34
4.6	无线设置.....	34
4.6.1	无线基本设置.....	35
4.6.2	无线安全设置.....	36
4.6.3	无线 MAC 地址过滤.....	40
4.6.4	无线高级设置.....	42
4.6.5	天线对准.....	43
4.6.6	无线距离设置.....	43
4.6.7	无线流量监测.....	44
4.6.8	无线主机状态.....	45
4.7	DHCP 服务器.....	45
4.7.1	DHCP 服务.....	45
4.7.2	客户端列表.....	46
4.7.3	静态地址分配.....	47
4.8	系统工具.....	48
4.8.1	SNMP.....	48
4.8.2	时间设置.....	49
4.8.3	诊断工具.....	50
4.8.4	看门狗.....	51
4.8.5	简单速率测试.....	52
4.8.6	软件升级.....	52
4.8.7	恢复出厂设置.....	53
4.8.8	备份和载入配置.....	53
4.8.9	重启设备.....	54
4.8.10	修改登录口令.....	55
4.8.11	系统日志.....	55
4.8.12	流量统计.....	56
第 5 章	AP 客户端路由模式和 AP 路由模式.....	58
5.1	登录.....	58
5.2	运行状态.....	58
5.3	设置向导.....	59
5.4	工作模式.....	59
5.5	网络参数.....	60
5.5.1	WAN 口设置.....	60
5.5.2	MAC 地址克隆.....	67

5.5.3	LAN 口设置	68
5.6	无线设置	68
5.6.1	无线基本设置	69
5.6.2	无线安全设置	71
5.6.3	无线 MAC 地址过滤	74
5.6.4	无线高级设置	76
5.6.5	天线对准	77
5.6.6	无线距离设置	77
5.6.7	无线流量监测	78
5.6.8	无线主机状态	78
5.7	DHCP 服务器	79
5.7.1	DHCP 设置服务	79
5.7.2	客户端列表	80
5.7.3	静态地址分配	80
5.8	转发规则	81
5.8.1	虚拟服务器	82
5.8.2	特殊应用程序	83
5.8.3	DMZ 主机	84
5.8.4	UPnP 设置	85
5.9	防火墙设置	85
5.9.1	安全设置	86
5.9.2	高级安全设置	86
5.9.3	局域网 WEB 管理	88
5.9.4	远端 WEB 管理	89
5.10	家长控制	90
5.11	访问控制	92
5.11.1	控制规则	93
5.11.2	主机列表	96
5.11.3	访问目标	96
5.11.4	日程计划	97
5.12	路由功能	98
5.12.1	静态路由表	99
5.12.2	系统路由表	99
5.13	IP 带宽控制	100
5.13.1	控制设置	100

5.13.2	控制规则	101
5.14	IP 与 MAC 绑定	102
5.14.1	静态 ARP 绑定设置	102
5.14.2	ARP 映射表	103
5.15	动态 DNS	103
5.16	系统工具	105
5.16.1	时间设置	105
5.16.2	诊断工具	106
5.16.3	软件升级	107
5.16.4	恢复出厂设置	108
5.16.5	备份和载入配置	108
5.16.6	重启设备	109
5.16.7	修改登录口令	110
5.16.8	系统日志	110
5.16.9	流量统计	111
附录 A: FAQ	113
附录 B: IE 浏览器设置	116
附录 C: POE 的使用	119
附录 D: 规格参数	121

第1章 产品概述

1.1 产品简介

TL-WA7210N 150M 室外高功率无线接入器能帮助移动用户或难以实施布线工程的用户轻松地访问网络，将有线以太网扩展到整幢大楼或整个园区。此款无线接入器具有高性能的网桥、漫游以及基于 Web 的配置和管理的特性，能很好地满足小企业与家庭用户日益增长的需求，让用户随时随地访问文件、电子邮件与互联网。

TL-WA7210N 150M 室外高功率无线接入器为不同用户提供 7 种网络接入模式：AP 客户端路由、AP 路由、接入点、多 SSID、中继、桥接和客户端等工作模式。在 AP 客户端路由模式下，可以视为无线网接入端，以无线方式通过无线网络服务提供商（WISP， Wireless Internet Service Provider）接入互联网。在 AP 路由模式下，可以通过 ADSL/Cable Modem 接入互联网，局域网以无线方式传输数据。

TL-WA7210N 150M 室外高功率无线接入器提供多重安全防护措施，可以有效保护用户的无线上网安全。它支持 SSID 广播控制，有效的防止 SSID 广播泄密，支持 64/128/152 位 WEP 加密，WPA/WPA2、WPA-PSK/WPA2-PSK 等加密与安全机制，同时支持 VPN 穿透技术，可以保证数据在无线网络传输中的安全。

TL-WA7210N 150M 室外高功率无线接入器符合 IEEE 802.11n, IEEE 802.11g 和 IEEE 802.11b 标准，提供 150Mbps 的无线传输速率，无线传输范围甚至可以扩展到数十公里。

1.2 主要特性

- 符合 IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u 无线标准
- 无线传输速率达到 150Mbps
- 支持 AP 客户端路由、AP 路由、接入点、多 SSID、中继、桥接和客户端等工作模式
- 高传输功率和优质的接收灵敏度
- 支持专为 WISP 设计的客户端路由模式
- 支持 Passive POE 供电
- 支持 WDS 模式
- 支持远距离通信，无线传输距离达 2 千米以上
- 支持天线校准
- 提供无线传输速率监控来指示当前无线传输速率
- 支持二层用户隔离
- 支持看门狗功能
- 支持速度检测
- 支持远程管理
- 支持输出功率调节
- 支持 PPPoE、静态 IP、动态 IP 方式接入互联网

- 内置 NAT 和 DHCP 服务器，支持静态地址分配
- 支持 UPnP、动态 DNS、静态路由、VPN 穿透
- 支持虚拟服务器、特殊应用程序和 DMZ 主机
- 内置防火墙，支持 IP 地址过滤、域名过滤和 MAC 地址过滤
- 提供 WLAN ACL
- 支持数据的载入和备份以及软件升级
- 支持 Web 管理

1.3 本书约定

在本手册中，所提到的 AP、TL-WA7210N 或设备，如无特别说明，系指 TL-WA7210N 150M 室外高功率无线接入器。

图片界面都配有相关参数，这些参数主要是为您正确配置产品参数提供参考。实际产品的配置参数并没有提供，您可以根据实际需要设置这些参数。

第2章 硬件描述

2.1 前面板

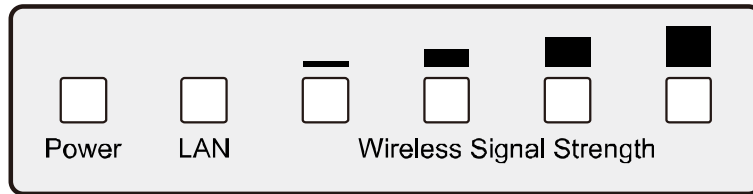


图 2-1 前面板示意图

指示灯：

指示灯	状态	说明	
Power	常灭	没有上电	
	常亮	已经上电	
LAN	常灭	端口没有连接上	
	常亮	端口已正常连接到设备但没有数据传输	
	闪烁	端口正在进行数据传输	
Wireless Signal Strength	常灭	没有无线信号	只适用于如下模式： AP 客户端路由，中继，桥接和客户端模式
	常亮	指示无线信号强度	

注意：

Wireless Signal Strength 指示灯：

- 在接入点，AP 路由和多 SSID 模式下，4 个指示灯均会常亮
- AP 客户端路由，中继，桥接和客户端模式下，当无线信号强度（RSSI）值达到相应值，对应的指示灯才会被点亮。

4 个无线信号强度指示灯的 RSSI 值分别对应 0db、14db、21db、29db，当无线信号强度达到这些数值时对应的指示灯就会点亮。

2.2 后面板

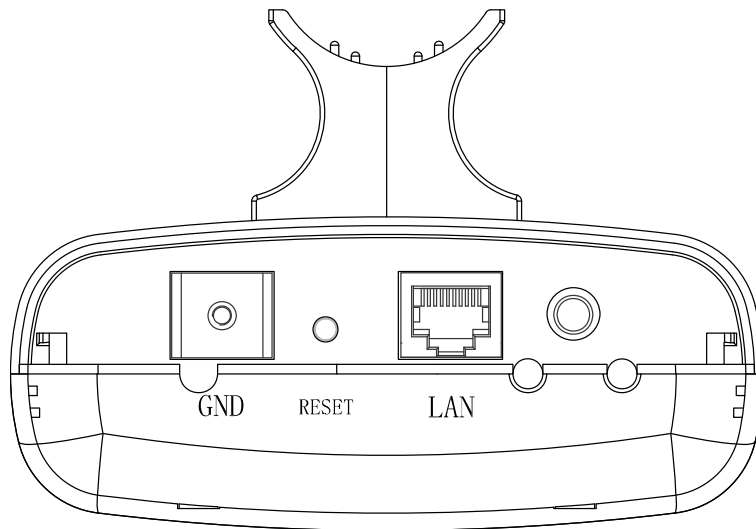



图 2-2 后面板示意图

从右至左观看，按钮与端口说明如下：

- ：与外界天线连接的插孔。您可以通过此接口扩展连接外部天线。此 AP 的天线是内置的，一般情况下无需连接外部天线。
- LAN：该端口用来连接 POE 供电设备。
- RESET：
 - 将本设备恢复出厂设置有两种方法：
 - 可以在**系统工具**→**恢复出厂设置**页面将设备恢复出厂设置。
 - 使用RESET按钮：在通电状态下，持续按压RESET按钮并至少等待五秒钟，当前面板图 2-1中除Power指示灯外其他指示灯闪烁后，AP将重启。

注意：

在AP完全启动之前，保证设备持续供电。

2.3 系统需求

- PC 的以太网连接设备（无线网卡或有线网卡及网线）
- 支持 TCP/IP 协议的操作系统
- Web 浏览器，如 Microsoft Internet Explorer 5.0、Netscape Navigator 6.0 或以上的版本
- 如果 AP 工作在 AP 客户端路由模式下，您还需要无线网络接入服务
- 如果 AP 工作在 AP 路由模式下，您还需要宽带 Internet 服务（DSL/Cable/Ethernet 接入）

2.4 安装环境

- 工作温度：-30℃~70℃
- 工作湿度：10%到 90% RH 不凝结

第3章 快速安装指南

本章介绍如何连接AP并成功接入Internet网络。更多高级配置说明，请阅读[第4章](#)和[第5章](#)内容。

3.1 硬件连接

请遵循以下步骤来安装 AP：

1. 关闭计算机、电缆/DSL 调制解调器和 AP。
2. 保证无线网络运营商（WISP）已提供无线网络接入服务。
3. 将 AP 尽量放在可以良好接收 WISP 信号的地方。
4. 调整 AP 的位置保证其接收到最佳无线信号。

完成上述步骤后，请根据 AP 的工作模式选择相应的安装流程。本 AP 支持 7 种模式：AP 客户端路由、AP 路由、接入点、多 SSID、中继、桥接和客户端模式。

3.1.1 AP 客户端路由模式

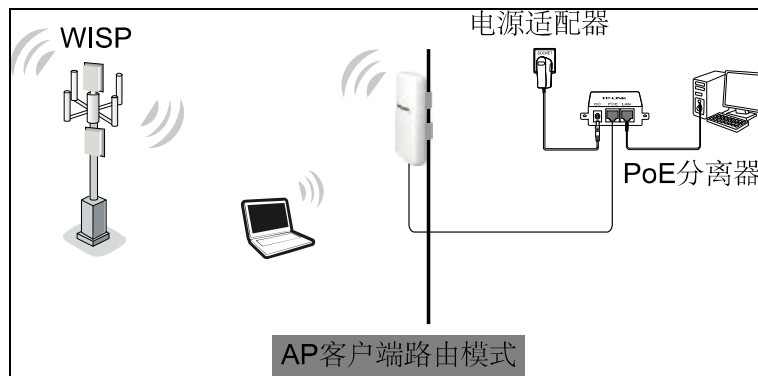


图 3-1 AP 客户端路由模式下 TL-WA7210N 的硬件连接

1. 将以太网线一端接入 TL-WA7210N 的 LAN 口，另一端连接到 POE 设备的 POE 端口。
2. 将以太网线一端接入计算机，另一端接入 POE 设备的 LAN 口。
3. 将电源适配器接入 POE 设备的 DC 插孔，另一端插入电源插座。
4. 打开计算机和笔记本。

3.1.2 AP路由模式

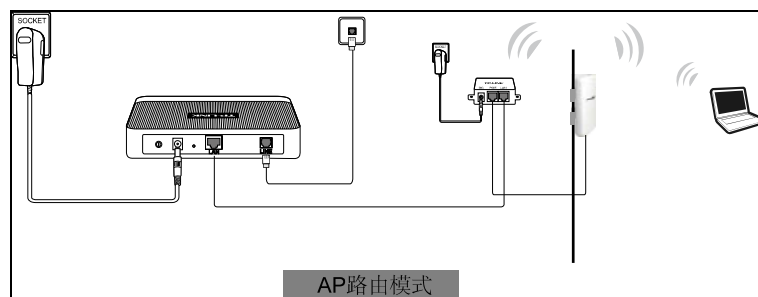


图 3-2 AP 路由模式下 TL-WA7210N 的硬件连接

1. 将以太网线一端接入 TL-WA7210N 的 LAN 口，另一端连接到 POE 设备的 POE 端口。
2. 将以太网线一端接入电缆/DSL 点调制解调器，另一端接入 POE 设备的 LAN 口。

3. 将电源适配器接入 POE 设备的 DC 插孔，另一端插入电源插座。
4. 打开计算机和网络中的其他连接设备（比如 ADSL 调制解调器）。

 **注意：**

在此模式下，POE设备的LAN口作为WAN口工作。

3.1.3 接入点模式

此工作模式下可以允许提供无线网络供无线设备接入。

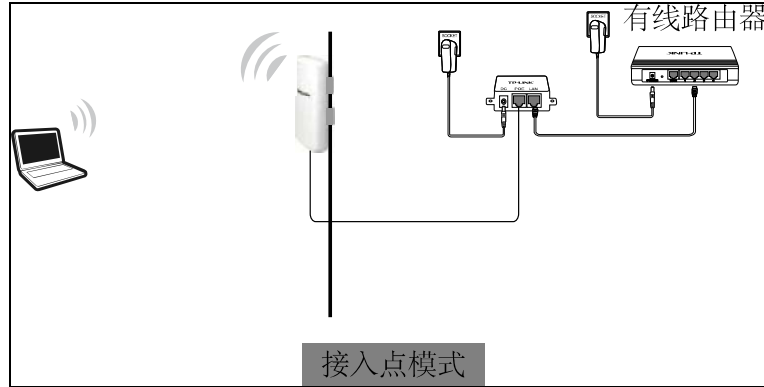


图 3-3 接入点模式下 TL-WA7210N 的硬件连接

1. 将以太网线一端接入 TL-WA7210N 的 LAN 口，另一端连接到 POE 设备的 POE 端口。
2. 将以太网线一端接入 POE 设备的 LAN 口，另一端接入到有线网络端口。
3. 将电源适配器接入 POE 设备的 DC 插孔，另一端插入电源插座。
4. 打开计算机和网络中的其他连接设备（比如有线路由器）。

3.1.4 多SSID模式

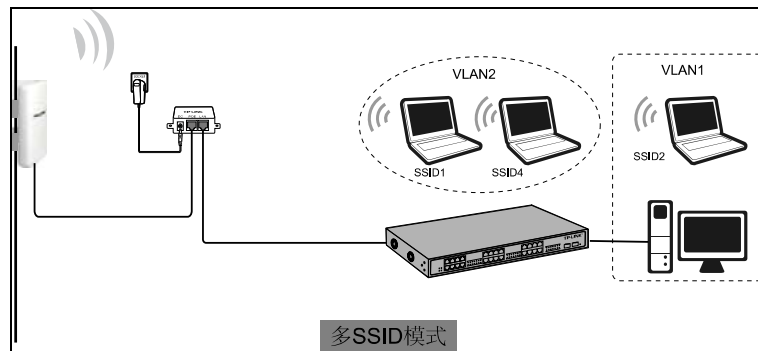


图 3-4 多 SSID 模式下 TL-WA7210N 的硬件连接

1. 将以太网线一端接入 TL-WA7210N 的 LAN 口，另一端连接到 POE 设备的 POE 端口。
2. 将以太网线一端接入 POE 设备的 LAN 口，另一端接入到有线网络端口。
3. 将电源适配器接入 POE 设备的 DC 插孔，另一端插入电源插座。
4. 打开计算机和网络中的其他连接设备（比如交换机）。

3.1.5 中继模式

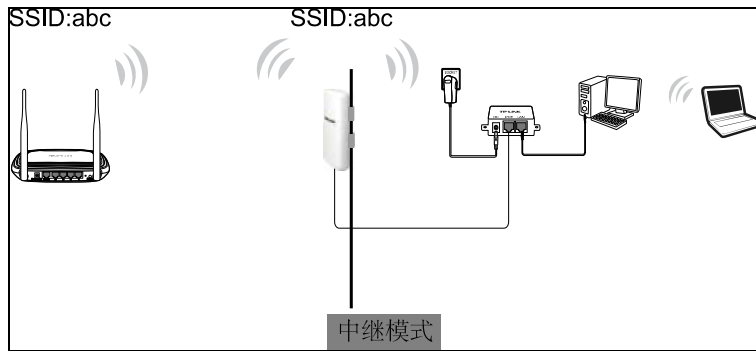


图 3-5 中继模式下 TL-WA7210N 的硬件连接

1. 将以太网线一端接入 TL-WA7210N 的 LAN 口，另一端连接到 POE 设备的 POE 端口。
2. 将电源适配器接入 POE 设备的 DC 插孔，另一端插入电源插座。
3. 打开计算机和网络中的其他连接设备（比如路由器）。

👉 注意：

WDS中继模式与普通中继模式都可以用来扩展另外一台AP或无线路由器的无线信号覆盖范围。在WDS中继模式下，WDS关联功能是开启的；在普通中继模式下，WDS关联是关闭的。

3.1.6 桥接模式

桥接模式需要两台设备。

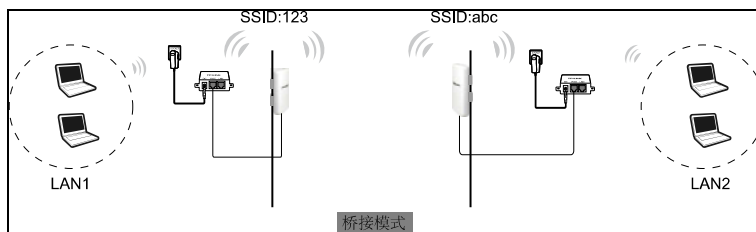


图 3-6 桥接模式下 TL-WA7210N 的硬件连接

1. 将以太网线一端接入 TL-WA7210N 的 LAN 口，另一端连接到 POE 设备的 POE 端口。
2. 将电源适配器接入 POE 设备的 DC 插孔，另一端插入电源插座。
3. 打开计算机。

👉 注意：

推荐先用以以太网线连接计算机/笔记本与设备的 LAN 口，然后从计算机/笔记本上登录设备，设置其模式为桥接模式。

3.1.7 客户端模式

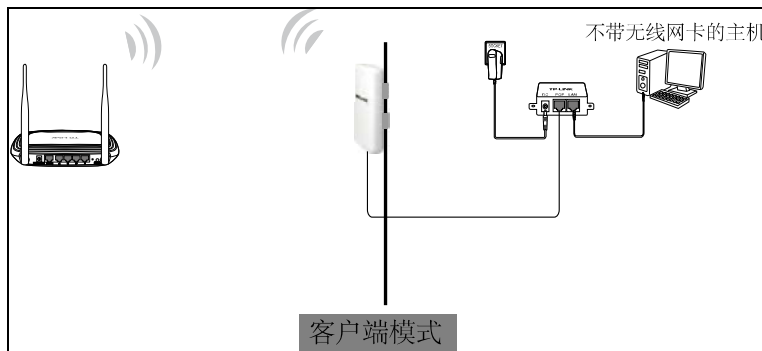


图 3-7 客户端模式下 TL-WA7210N 的硬件连接

1. 将以太网线一端接入 TL-WA7210N 的 LAN 口，另一端连接到 POE 设备的 POE 端口。
2. 将以太网线一端接入 POE 设备的 LAN 口，另一端接入到计算机。
3. 将电源适配器接入 POE 设备的 DC 插孔，另一端插入电源插座。
4. 打开计算机与其他连接设备（比如路由器）。

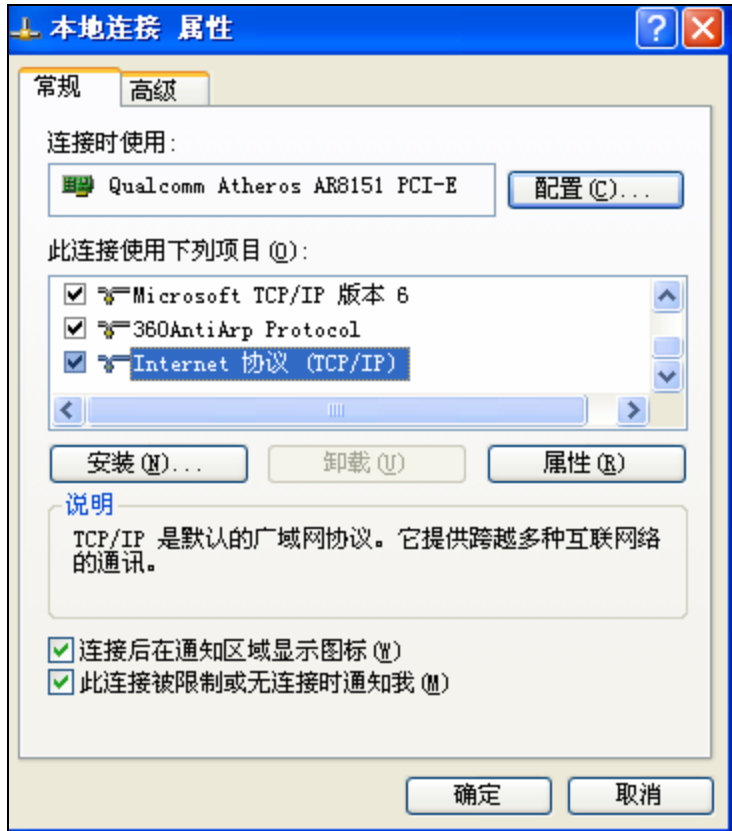
3.2 建立正确的网络连接

本设备默认 LAN 口 IP 地址是 192.168.1.254，默认子网掩码是 255.255.255.0。这些值可以根据实际需要而改变，但本手册中将按默认值说明。本节以 Windows XP 系统为例，介绍计算机参数的设置步骤。

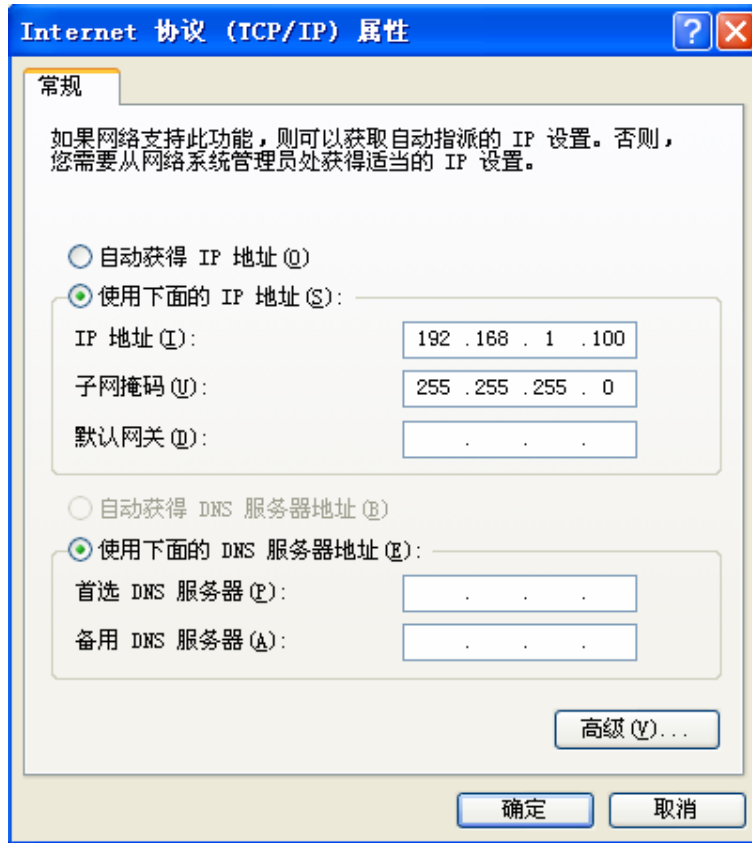
1. 点击开始→控制面板→网络连接→本地连接，右键点击“本地连接”，选择属性，打开“本地连接属性”页面。



2. 双击 Internet 协议(TCP/IP)。



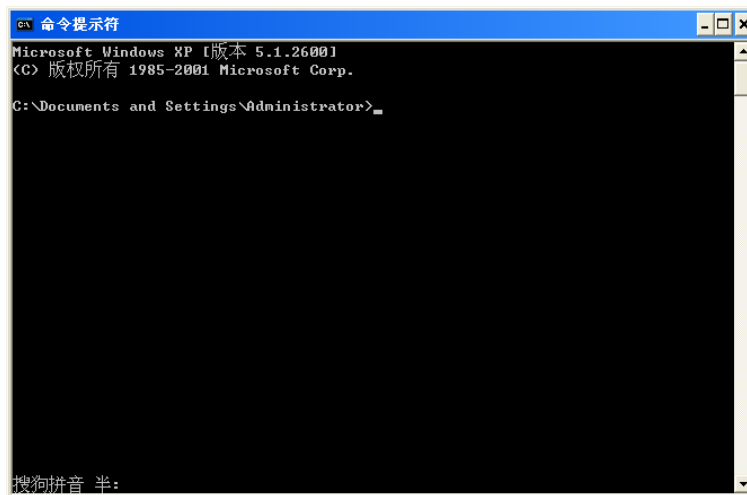
- 3. 选择使用下面的 IP 地址，在 IP 地址栏输入：192.168.1. ×（×为从 2~253 之间的任一整数，在此以 100 为例），在子网掩码栏输入：255.255.255.0， 点击确定保存配置。



 **提示：**

Windows 98 或更早版本的操作系统，以上设置可能需要重启计算机。

4. 使用 Ping 命令检查计算机和路由器之间是否连通。在 Windows XP 环境中，点击开始—运行，在随后出现的运行窗口输入“cmd”命令，回车或点击**确定**进入下图所示界面。



5. 输入命令：Ping 192.168.1.254，回车。

如果屏幕显示为：

```
Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

计算机已与路由器成功建立连接。

如果屏幕显示为：

```
Pinging 192.168.1.254 with 32 bytes of data: :
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

这说明设备还未安装好，请按照下列顺序检查：

1) 硬件连接是否正确？

AP 面板上 LAN 口的指示灯和计算机上的网卡指示灯必须亮。

2) 计算机的 TCP/IP 设置是否正确？

计算机的 IP 地址可以按照前面介绍的自动获取方式，也可以从 AP 自动获取。若从 AP 自动获取，此时 AP 的 DHCP 模式必须开启，见章节 [4.7 DHCP 服务器](#) 或 [5.7 DHCP 服务器](#)，然后计算机在 **Internet 协议(TCP/IP)** 的界面选择“**自动获取IP地址**”。

3.3 快速安装指南

本产品提供基于 WEB 浏览器的配置工具。为了能顺利通过本路由器连接互联网，首先请设置 WEB 浏览器，具体设置步骤请参阅 [附录B IE 浏览器设置](#)。

打开网页浏览器，在浏览器的地址栏中输入路由器的 IP 地址：192.168.1.254，将会看到图 3-8 所示登录界面，输入用户名和密码（用户名和密码的出厂默认值均为 **admin**），点击 **确定** 按钮。

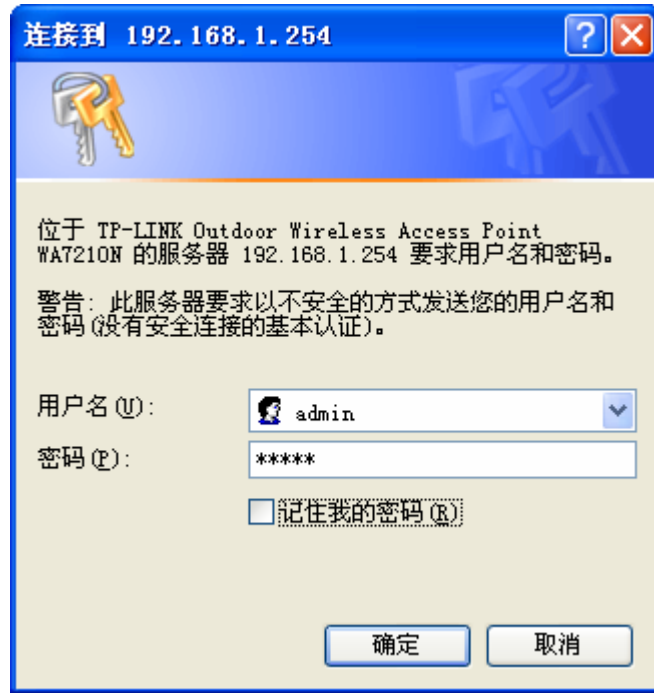


图 3-8 登录界面

浏览器会弹出如图 3-9 所示的设置向导页面。如果没有自动弹出此页面，可以点击页面左侧的**设置向导**菜单将它激活。

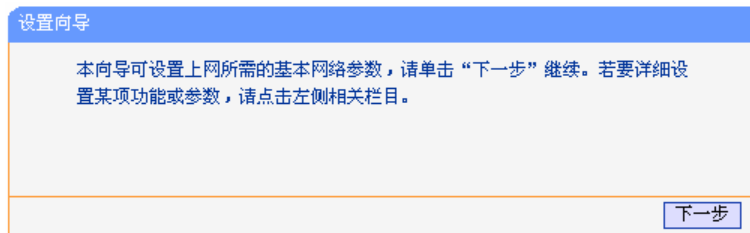


图 3-9 设置向导

点击下一步，弹出**设置向导-工作模式**页面，如图 3-10。

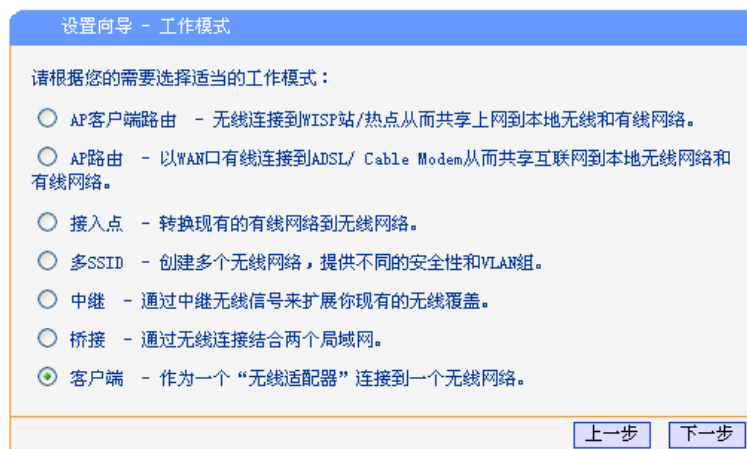


图 3-10 设置向导-工作模式

AP 支持 7 种接入模式：**AP 客户端路由**、**AP 路由**、**接入点**、**多 SSID**、**中继**、**桥接**和**客户端模式**。

➤ AP 客户端路由模式

该模式下，设备能够让多个用户共享来自WISP的互连网络。LAN端的设备通过无线端口从WISP共享一样的互联网IP地址。在AP客户端路由模式下，当连接WISP时，无线端口作为WAN口工作，而有线端口作为LAN口工作。

➤ AP 路由模式

该模式下，设备能够让多个用户共享来自ADSL/Cable调制器提供的互连网络。无线端口共享同样的IP到ISP，而这个IP通过有线WAN口获取。AP路由模式下，无线端口作为一个LAN端工作。

➤ 接入点模式

该模式下，AP作为无线网络中心接入到有线局域网中，从而扩展有线局域网覆盖范围。

➤ 多SSID模式

该模式下，AP能虚拟多个SSID供用户接入，同时，对连接到不同SSID的设备进行VLAN标记。

➤ 中继模式

该模式下，AP用于扩展另外一台AP或无线路由器的无线信号覆盖范围。一般该模式用于其他AP或者无线路由器支持WDS的情况下。

➤ 桥接模式

该模式下，AP可以将不超过4个局域网通过无线网络连接起来。

➤ 客户端模式

该模式下，AP设备的功能类似于无线网卡，可以用来连接WISP或者无线路由器。

3.3.1 AP 客户端路由

若选择了 **AP 客户端路由** 模式，请按以下步骤配置设备：

1. 在图 3-10中点击下一步，然后弹出**上网方式**页面，如图 3-11：

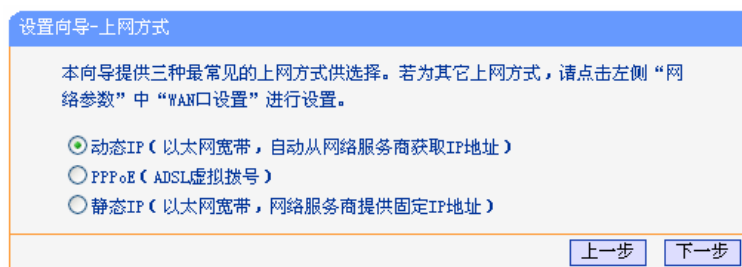


图 3-11 设置向导-上网方式

- **动态 IP**-当设备连接到 DHCP 服务器，或者您的网络服务商提供 DHCP 连接时，请选择此模式。在这个模式下设备将自动从 DHCP 服务器或者 WISP（无线互联网服务提供商）获取 IP 地址。

在图 3-11中选择动态IP，点击**下一步**，将会弹出无线设置页面，如图 3-12所示。

图 3-12 设置向导-WISP 主机设置

- **WISP 主机无线名称**- 您的设备作为客户端想要接入的 AP 的 SSID。您也可以用**搜索**功能找到这个 SSID 并加入。
 - **WISP 主机物理地址**- 您的设备作为客户端想要接入的 AP 的 MAC 地址。您也可以用**搜索**功能找到这个 MAC 地址并加入。
 - **搜索**- 搜索工作在当前信道中的 AP。
 - **传输功率**- 有六种不同的传输功率可供选择。
 - **无线安全模式**- 此安全选项应该根据前端 AP 的安全配置来选择。建议与前端 AP 的安全模式保持一致。
 - **无线密钥**- 如果您的设备想要接入的 AP 所设置的密码。
- **PPPoE**-如果您是利用 ADSL 来拨号上网，您应该选择这种上网方式。在这个模式下您需要填入网络服务商提供的帐户和口令。
- 1) 在图 3-11中选择PPPoE，点击**下一步**，将弹出如下页面：

图 3-13 设置向导-PPPoE

- 2) 输入网络服务商提供的帐户和口令，点击**下一步**，将弹出无线设置页面图 3-12。
- **静态 IP**- 此模式下您应该手动输入网络供应商提供的基本网络参数，包括 **IP 地址**、**子网掩码**、**网关**、**DNS 服务器**等。
- 1) 在图 3-11选择**静态IP**，点击**下一步**，弹出如下页面：

设置向导-静态IP

请在下框中填入网络服务商提供的基本网络参数，如遗忘请咨询网络服务商。

IP地址：

子网掩码：

网关：

DNS服务器：

备用DNS服务器： (可选)

图 3-14 设置向导-静态 IP

- **IP 地址**- 在此填入本路由器对外网用户（以及网络服务商）的 WAN 口 IP 地址。
- **子网掩码**- WAN IP 下的子网掩码，一般为 255.255.255.0。
- **网关**- 在此填入默认网关地址。
- **DNS 服务器**- 在此填入 DNS 服务器的 IP。
- **备用 DNS 服务器**- 在此填入 WISP 提供的另一 DNS 服务器地址，可选。

 **注意：**

静态 IP 参数需要由您的无线网络服务商提供。

- 2) 填完必须的网络参数之后，点击**下一步**，将弹出无线设置页面，如图 3-12所示。
2. 在图 3-12中点击**搜索**，将弹出AP列表页面，选择目标AP，点击**连接**之后将会返回上一页面，如果该AP设置了密码的话您还需要输入密码，然后点击**下一步**。

AP列表

扫描到的AP的信息如下： 64

ID	BSSID	SSID	信号强度	信道	是否加密	选择
1	40-16-9F-AA-AA-E5		37dB	1	WPA/WPA2-PSK	连接
2	00-0A-EB-13-17-02	300_2g	44dB	1	WPA/WPA2	连接
3	00-13-4E-0B-2A-7B	CU_3dEn	45dB	1	WPA-PSK	连接
4	00-13-4E-0B-2A-7C	CU_vap0_3dEn	46dB	1	WPA-PSK	连接
5	00-13-4E-0B-2A-7D	CU_vap1_3dEn	46dB	1	WPA-PSK	连接
6	00-13-4E-0B-2A-7E	CU_vap2_3dEn	45dB	1	WPA-PSK	连接
7	6C-FD-B9-95-6A-DA	Eltek-956ADA	48dB	1	WPA2-PSK	连接
8	E0-05-C5-86-A3-F1	TP-LINK_1750_2.4G	33dB	1	否	连接
9	00-14-78-00-00-08	TP-LINK_2.4G_11gbug	36dB	1	否	连接
10	40-16-9F-BF-50-F2	TP-LINK_BF50F2	48dB	1	否	连接
11	40-16-9F-BF-51-4C	TP-LINK_BF514C	61dB	1	否	连接
12	94-27-19-E7-84-AB	TP-LINK_E784AB	34dB	1	否	连接
13	EC-17-2F-F8-30-7E	TP-LINK_F8307E	51dB	1	WPA2-PSK	连接
14	00-14-78-00-00-01	TP-LINK_FFFFFFFF	49dB	1	否	连接
15	00-5E-AA-08-01-05	abc	69dB	1	WPA/WPA2-PSK	连接
16	00-24-23-E0-22-71	only_test	34dB	3	WPA-PSK	连接
17	6C-FD-B9-95-6A-E4	Eltek-956AE4	34dB	4	WPA2-PSK	连接
18	00-06-0D-02-0A-02	CU_0gc9	38dB	5	否	连接

图 3-15 AP 列表

3. 在弹出的**本地无线 AP 设置**页面里，输入**本地无线名称**。默认情况下，本地无线网络的安全设置将和 WISP 保持一致。然后点击**下一步**。

设置向导 - 本地无线 AP 设置

本地无线名称： (也叫做 SSID)

为本地无线网络使用与远程 WISP 主机相同的安全设置。

图 3-16 设置向导

如果不勾选**为本地无线网络使用与远程 WISP 主机相同的安全设置**，您将可以在下面的页面中选择本地无线网络的**无线安全模式**并设置**无线密钥**。

设置向导 - 本地无线 AP 设置

本地无线名称： (也叫做 SSID)

为本地无线网络使用与远程 WISP 主机相同的安全设置。

无线安全模式：

无线密钥：

您可以输入 8 到 63 个 ASCII 字符或 8 到 64 个十六进制字符。

图 3-17 设置向导-本地无线 AP 设置

当完成上述的无线设置之后，您将会看到**结束**页面，如图 3-18 所示。请检查您所配置的参数，如有错误，请点击**上一步**返回重新设置。若配置确认无误，请点击**完成**或**重启**按钮使配置生效。

设置向导 - 结束

确认您所设定的配置。如果有什么问题，请按“上一步”按钮重新设置。
确认后，请单击“完成”或“重启”按钮使配置生效。

无线设置

工作模式：	AP 客户端路由
互联网连接类型	动态 IP
桥接 AP 无线名称：	MERCURY_030405
桥接 AP 物理地址：	00-01-02-03-04-05
无线安全模式：	无
本地无线名称 (SSID)：	TP-LINK_721002
无线信道：	6
无线安全模式：	无
传输功率：	27 dBm

图 3-18 设置向导-结束

3.3.2 AP 路由

当你选择了 **AP 路由** 模式，请按以下步骤配置设备：

1. 在图 3-10 中点击**下一步**，然后弹出**上网方式**页面，如图 3-19：

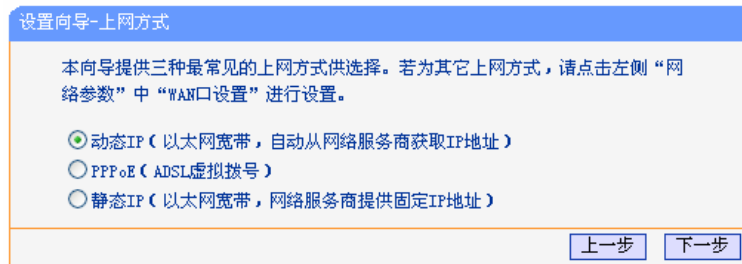


图 3-19 设置向导-上网方式

- **动态 IP**-当设备连接到 DHCP 服务器，或者您的网络服务商提供 DHCP 连接时，请选择此模式。在这个模式下设备将自动从 DHCP 服务器获取 IP 地址。

在图 3-19中选择动态IP，点击下一步，将会弹出无线设置页面，如图 3-20所示。

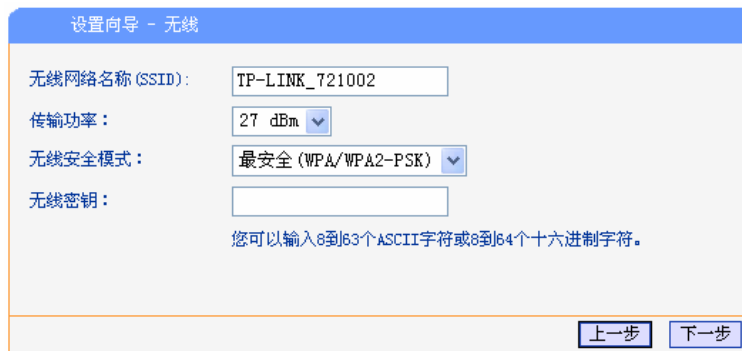


图 3-20 设置向导-无线设置

- **无线网络名称(SSID)**- 输入一串字符串来命名您的无线网络。最多可输入 32 位字符。您网络中的无线设备都需连入到此网络中。无线网络名称默认设置为 TP-LINK_XXXXXX（XXXXXX 是本台设备 MAC 地址的最后六位），它的唯一性可以保证您无线网络的安全。但我们仍然建议您更改您的无线网络名称（SSID）。此无线网络名称是区分大小写的，例如，MYSSID 和 MySsid 是两个不同的网络名。
- **传输功率**-有六种不同的传输功率可供选择。
- **无线安全模式**- 您可以从如下安全模式中选择一种：
 - 最安全（WPA/WPA2-PSK）- 基于共享密钥的 WPA 加密模式。
 - 安全（WEP）-基于非共享密钥的 WEP 加密模式。
 - 无- 关闭无线安全功能。此时无线设备不需要密码验证就能连入此设备。
- **认证类型**- 如果安全模式是 WEP，必须选择根 AP 的认证类型。
- **密钥格式**-如果安全模式是 WEP，必须选择 WEP 密钥的格式。
- **WEP 密钥序号**- 如果安全模式是 WEP，必须选择 WEP 密钥的序号。
- **无线密码**- 如果您的设备所连入的 AP 需要密码验证，此处需填入这个密码。
- **PPPoE**-如果您是利用 ADSL 来拨号上网，您应该选择这种上网方式。在这个模式下您需要填入网络服务商提供的帐户和口令。
 - 1) 在图 3-19中选择PPPoE，点击下一步，将弹出如下页面：

图 3-21 设置向导-PPPoE

2) 输入网络服务商提供的帐户和口令，点击**下一步**，将弹出页面图 3-20。

- **静态 IP**- 此模式下您应该手动输入网络供应商提供的基本网络参数，包括 **IP 地址**、**子网掩码**、**网关**、**DNS 服务器**等。

在图 3-19选择**静态IP**，点击**下一步**，弹出如下页面：

图 3-22 设置向导-静态 IP

- **IP 地址**- 在此填入本路由器对外网用户（以及网络服务商）的 WAN 口 IP 地址。
- **子网掩码**- WAN 口 IP 下的子网掩码，一般为 255.255.255.0。
- **网关**- 在此填入默认网关地址。
- **DNS 服务器**- 在此填入 DNS 服务器的 IP。
- **备用 DNS 服务器**- 在此填入 WISP 提供的另一 DNS 服务器地址，可选。

注意：

静态 IP 参数需要由您的无线网络服务商提供。

填完必须的网络参数之后，点击**下一步**，将弹出无线配置界面图 3-20。

2. 当您完成了图 3-20的无线设置之后，点击**下一步**，将弹出**结束**页面，您可以在此界面上点击**重启**来完成配置。



图 3-23 设置向导-结束

3.3.3 接入点

当你选择了接入点模式，请按以下步骤配置设备：

1. 在图 3-10中点击下一步，将弹出无线设置页面如图 3-24，为您的无线网络选一个易记的SSID，无线安全模式选择最安全（WPA/WPA2-PSK）并在下一行输入无线密钥来防止对此设备进行的未经授权的访问。然后点击下一步。

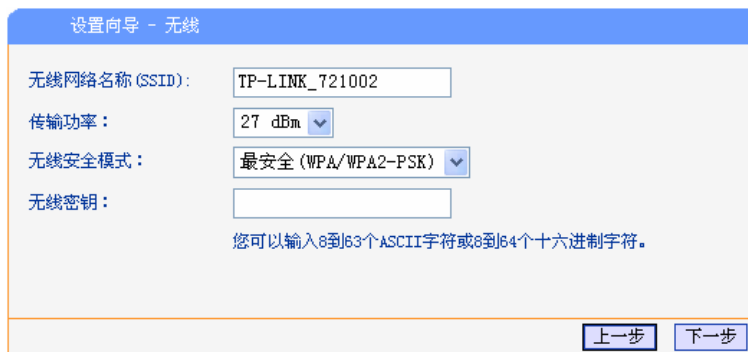


图 3-24 设置向导-无线

- **无线网络名称(SSID)**- 输入一串字符串来命名您的无线网络。最多可输入 32 位字符。您网络中的无线设备都需连入到此网络中。无线网络的名称默认设置为 TP-LINK_xxxxxx（xxxxxx 是本平台设备 MAC 地址的最后六位），它的唯一性可以保证您无线网络的安全。但我们仍然建议您更改您的无线网络名称（SSID）。此无线网络名称是区分大小写的，例如，MYSSID 和 MySsid 是两个不同的网络名。
- **传输功率**-有六种不同的传输功率可供选择。
- **无线安全模式**- 您可以从如下安全模式中选择一种：
 - **最安全 (WPA/WPA2-PSK)** - 基于共享密钥的 WPA 加密模式。
 - **安全 (WEP)** -基于非共享密钥的 WEP 加密模式。
 - **无**- 关闭无线安全功能。此时无线设备不需要密码验证就能连入此设备。
- **认证类型**- 如果安全模式是 WEP，必须选择根 AP 的认证类型。
- **密钥格式**-如果安全模式是 WEP，必须选择 WEP 密钥的格式。
- **WEP 密钥序号**- 如果安全模式是 WEP，必须选择 WEP 密钥的序号。

- **无线密钥**- 如果您的设备所连入的 AP 需要密码验证，此处需填入这个密码。

注意：

本设备的无线信号的覆盖范围很大程度上取决于它所安装的地理位置。为达到最佳效果，请在设备安装时遵循以下原则：

- 尽量选择高处，比如一个较高的架子上。
- 远离潜在的干扰源，比如电脑，微波炉和无绳电话等。
- 天线处于直立位置。
- 远离大的金属表面。

若不遵循以上原则将导致本设备性能下降，或导致该区域内的无线设备无法连接到本设备。

2. 在弹出的网络设置页面里，建议您保持当前的默认设置不变，点击**下一步**。

设置向导 - 网络

DHCP服务器： 不启用 启用

在大多数情况下，你的根AP /路由器启用了DHCP服务器功能，我们强烈建议您在此设备上禁用DHCP服务器功能以避免无法预测的问题。

IP地址：

子网掩码：

我们建议您配置这个AP使用相同的IP子网和子网掩码，但与根AP/路由不同的IP地址。

改变登入账号： 否 是

图 3-25 设置向导-网络

3. 当您完成图 3-25中的网络设置，点击**下一步**后将弹出如下页面，在此页面上点击**重启**来完成配置过程。

设置向导 - 结束

确认您所设定的配置。如果有什么问题，请按“上一步”按钮重新设置。
确认后，请单击“完成”或“重启”按钮使配置生效。

无线设置

工作模式：	接入点
无线网络名称 (SSID)：	TP-LINK_721002
无线安全模式：	最安全 (WPA/WPA2-PSK)
无线密钥：	12345678
传输功率：	27 dBm

网络设置

登入账户：	admin/ admin
LAN IP地址：	192.168.1.254
DHCP服务器：	不开启

图 3-26 设置向导-结束

3.3.4 多SSID

当你选择了**多 SSID** 模式，请按以下步骤配置设备：

1. 在图 3-10中点击下一步，将弹出无线设置页面如图 3-27，勾选开启VLAN功能，创建不同的 SSID并依据您对无线网络安全的要求来分别为他们设置对应的密码。点击保存键来使每个 SSID下的设置生效，然后点击下一步。

 **注意:**

本设备的无线信号的覆盖范围很大程度上取决于它所安装的地理位置。为达到最佳效果，请在设备安装时遵循以下原则：

- 尽量选择高处，比如一个较高的架子上。
- 远离潜在的干扰源，比如电脑，微波炉和无绳电话等。
- 天线处于直立位置。
- 远离大的金属表面。

若不遵循以上原则将导致本设备性能下降，或导致该区域内的无线设备无法连接到本设备。



设置向导 - 无线

开启 VLAN功能

SSID1: TP-LINK_721002 VLAN ID: 1

SSID2: TP-LINK_721002_2 VLAN ID: 1

SSID3: TP-LINK_721002_3 VLAN ID: 1

SSID4: TP-LINK_721002_4 VLAN ID: 1

传输功率: 27 dBm

SSID: TP-LINK_721002

无线安全模式: 最安全 (WPA/WPA2-PSK)

无线密钥:

您可以输入8到63个ASCII字符或8到64个十六进制字符。

保存

上一步 下一步

图 3-27 设置向导-无线

- **开启 VLAN 功能**- 开启或者关闭 VLAN。本 AP 设备最多支持 4 个 VLAN。VLAN 中的所有无线主机都能连接到本设备中。本 AP 设备可以和支持 802.1Q VLAN 的交换机一起工作。如果交换机开启了 TAG VLAN 功能，则除了无线主机以外的其他主机，必须处在与 SSID1 相同的 VLAN 下才能连入本 AP。如果一台主机直接连入本 AP 的 LAN 口，请确保这台主机的网卡支持 TAG 功能，否则这台主机将无法连接到 AP。
- **SSID**- 无线网络名称(SSID)- 输入一串字符串来命名您的无线网络。最多可输入 32 位字符。您网络中的无线设备都需连入到此网络中。在多 SSID 模式下，您可以为“SSID1”~“SSID4”分别指定 SSID。
- **VLAN ID**- VLAN 的 ID 号，取值范围为 1-4095。只有处于同一个 VLAN 中，无线主机和有线主机才能相互通信。如果开启了 VLAN 功能，当 AP 设备转发数据包时，从 LAN 发出的数据包将会被添加 IEEE 802.1Q VLAN TAG 标记，此数据包的 VLAN ID 即为发送它的交换机端口所在的 VLAN。
- **传输功率**-有六种不同的传输功率可供选择。

- **无线安全模式**- 您可以从如下安全模式中选择一种：
 - **最安全 (WPA/WPA2-PSK)** - 基于共享密钥的 WPA 加密模式。
 - **安全 (WEP)** -基于非共享密钥的 WEP 加密模式。
 - **无**- 关闭无线安全功能。此时无线设备不需要密码验证就能连入此设备。
 - **认证类型**- 如果安全模式是 WEP，必须选择根 AP 的认证类型。
 - **密钥格式**-如果安全模式是 WEP，必须选择 WEP 密钥的格式。
 - **WEP 密钥序号**- 如果安全模式是 WEP，必须选择 WEP 密钥的序号。
 - **无线密钥**- 如果您的设备所连入的 AP 需要密码验证，此处需填入这个密码。
 - **保存**- 保存选中 SSID 下的安全配置。
2. 在弹出的网络设置页面中，建议您保持当前的默认设置不变，点击**下一步**。

设置向导 - 网络

DHCP服务器： 不启用 启用

在大多数情况下，你的根AP /路由器启用了DHCP服务器功能，我们强烈建议您在此设备上禁用DHCP服务器功能以避免无法预测的问题。

IP地址：

子网掩码：

我们建议您配置这个AP使用相同的IP子网和子网掩码，但与根AP/路由不同的IP地址。

改变登入账号： 否 是

图 3-28 设置向导-网络

3. 当您完成图 3-28中的设置，点击**下一步**，将会出现下图的界面，您可以点击**重启**按钮来使配置生效。

设置向导 - 结束

确认您所设定的配置。如果有什么问题，请按“上一步”按钮重新设置。
确认后，请单击“完成”或“重启”按钮使配置生效。

无线设置

工作模式：多SSID

SSID1：TP-LINK_721002

无线安全模式：最安全 (WPA/WPA2-PSK)

无线密钥：12345678

SSID2：不开启

SSID3：不开启

SSID4：不开启

传输功率：27dBm

网络设置

登入账户：admin/ admin

LAN IP地址：192.168.1.254

DHCP服务器：不开启

上一步 重启

图 3-29 设置向导-结束

3.3.5 中继

当你选择了**中继**模式，请按以下步骤配置设备：

1. 在图 3-10中点击**下一步**，将弹出无线设置页面如图 3-30，点击**搜索**按钮来扫描整个无线网络。

设置向导 - 无线

中继模式： 普通中继 WDS中继

前端AP无线名称： (也叫做SSID)

前端AP物理地址：

搜索

点击“搜索”按钮扫描无线网络，并选择目标设置。

传输功率：

无线安全模式：最安全 (WPA/WPA2-PSK)

所有的安全设置，例如无线密钥应该符合前端AP/路由器。

无线密钥：

您可以输入8到63个ASCII字符或8到64个十六进制字符。

上一步 下一步

图 3-30 设置向导-无线

- **中继模式**- 您可以从如下中继模式中选择一种：
 - **普通中继** – 在普通中继模式下，未开启了 WDS 功能的 AP 将中转来自它所关联的前端 AP 的数据。此时 AP 功能也同时开启。无线中继功能让更大范围内的无线主机能与根 AP 进行通信。
 - **WDS 中继** – 在 WDS 中继模式下，开启了 WDS 功能的 AP 将中转来自它所关联的前端 AP 的数据。此时 AP 功能也同时开启。无线中继功能让更大范围内的无线主机能与根 AP 进行通信。

- **前端 AP 无线名称**- 本设备作为客户端所要连入的前端 AP 的 SSID。您可以通过搜索功能来选择所连入的 AP 的 SSID。
- **前端 AP 物理地址**-本设备作为客户端所要连入的前端 AP 的 MAC 地址。您可以通过搜索功能来选择所连入的 AP 的 MAC 地址。
- **搜索**- 点击此按钮来搜索无线网络中的 AP。
- **传输功率**-有六种不同的传输功率可供选择。
- **无线安全模式**- 您可以从如下安全模式中选择一种：
 - **最安全 (WPA/WPA2-PSK)** - 基于共享密钥的 WPA 加密模式。
 - **安全 (WEP)** -基于非共享密钥的 WEP 加密模式。
 - **无**- 关闭无线安全功能。此时无线设备不需要密码验证就能连入此设备。
- **认证类型**- 如果安全模式是 WEP，必须选择根 AP 的认证类型。
- **密钥格式**-如果安全模式是 WEP，必须选择 WEP 密钥的格式。
- **WEP 密钥序号**- 如果安全模式是 WEP，必须选择 WEP 密钥的序号。
- **无线密钥**- 如果您的设备所连入的 AP 需要密码验证，此处需填入这个密码。

 **注意:**

本设备的无线信号的覆盖范围很大程度上取决于它所安装的地理位置。为达到最佳效果，请在设备安装时遵循以下原则：

- 尽量选择高处，比如一个较高的架子上。
- 远离潜在的干扰源，比如电脑，微波炉和无绳电话等。
- 天线处于直立位置。
- 远离大的金属表面。

若不遵循以上原则将导致本设备性能下降，或导致该区域内的无线设备无法连接到本设备。

2. AP列表界面如图 3-31所示，选择您要连入的前端AP的BSSID（与它的MAC地址相同）并点击**连接**。

AP列表

扫描到的AP的信息如下： 64

ID	BSSID	SSID	信号强度	信道	是否加密	选择
1	40-16-9F-AA-AA-E5		17dB	1	WPA/WPA2-PSK	连接
2	00-13-4E-0B-2A-7B	CU_3dEn	44dB	1	WPA-PSK	连接
3	00-13-4E-0B-2A-7C	CU_vap0_3dEn	44dB	1	WPA-PSK	连接
4	00-13-4E-0B-2A-7D	CU_vap1_3dEn	45dB	1	WPA-PSK	连接
5	00-13-4E-0B-2A-7E	CU_vap2_3dEn	43dB	1	WPA-PSK	连接
6	8C-FD-B9-95-8A-DA	Eltek-956ADA	40dB	1	WPA2-PSK	连接
7	02-10-18-01-00-01	TP-LINK_010001	0dB	1	WPA2-PSK	连接
8	00-23-79-11-22-33	TP-LINK_112233	37dB	1	否	连接
9	E0-05-C5-72-10-08	TP-LINK_721008	57dB	1	否	连接
10	EC-88-8F-97-37-E6	TP-LINK_9737E6	24dB	1	WPA/WPA2-PSK	连接
11	40-16-9F-BF-50-F0	TP-LINK_BF50F0	59dB	1	否	连接
12	94-27-19-E7-84-AB	TP-LINK_E784AB	33dB	1	否	连接
13	00-0A-EB-70-00-50	TP-LINK_PocketAP_700050	32dB	1	WPA/WPA2-PSK	连接
14	90-F6-52-57-6B-2A	tiger-lion	21dB	1	否	连接
15	08-19-A6-60-15-D8	ChinaNet-LPNV	24dB	2	WPA/WPA2-PSK	连接
16	40-16-9F-BF-50-F2	TP-LINK_BF50F2	55dB	2	否	连接
17	46-16-9F-BF-50-F2	TP-LINK_BF50F2_01	57dB	2	否	连接

图 3-31 AP 列表

您将返回到图 3-30所示的无线页面，此时无线安全模式已经被选定，请确认并输入与前端ap或者路由器相同的密码，然后点击下一步。

- 随后弹出网络的设置页面如图 3-32所示，建议您保持当前的默认设置不变，点击下一步。

设置向导 - 网络

DHCP服务器： 不启用 启用

在大多数情况下，你的根AP /路由器启用了DHCP服务器功能，我们强烈建议您在此设备上禁用DHCP服务器功能以避免无法预测的问题。

IP地址：

子网掩码：

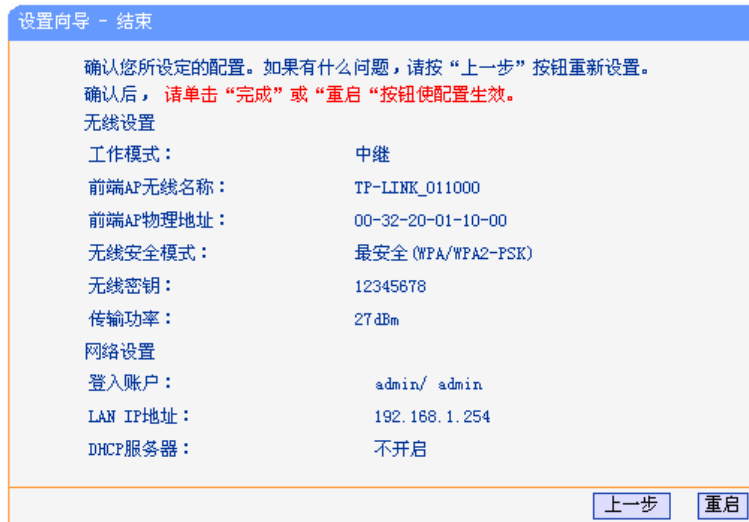
我们建议您配置这个AP使用相同的IP子网和子网掩码，但与根AP/路由不同的IP地址。

改变登入账号： 否 是

[上一步](#) [下一步](#)

图 3-32 设置向导-网络

- 在弹出的结束页面里，点击**重启**按钮来使设置生效，如图 3-33所示



设置向导 - 结束

确认您所设定的配置。如果有什么问题，请按“上一步”按钮重新设置。
确认后，请单击“完成”或“重启”按钮使配置生效。

无线设置

工作模式： 中继

前端AP无线名称： TP-LINK_011000

前端AP物理地址： 00-32-20-01-10-00

无线安全模式： 最安全(WPA/WPA2-PSK)

无线密钥： 12345678

传输功率： 27dBm

网络设置

登入账户： admin/ admin

LAN IP地址： 192.168.1.254

DHCP服务器： 不开启

上一步 重启

图 3-33 设置向导-结束

3.3.6 桥接

当你选择了桥接模式，请按以下步骤配置设备：

1. 在图 3-10中点击下一步，将弹出无线桥接页面图 3-34，点击**搜索**按钮来扫描整个无线网络。



设置向导 - 无线桥接设置

桥接AP无线名称： (也叫做SSID)

桥接AP物理地址：

搜索

点击“搜索”按钮扫描无线网络，并选择目标设置。

传输功率：

信道：

无线安全模式：

所有的安全设置，例如无线密钥应该符合前端AP/路由器。

无线密钥：

您可以输入8到63个ASCII字符或8到64个十六进制字符。

上一步 下一步

图 3-34 设置向导-无线桥接设置

- **桥接 AP 无线名称**- 本设备作为客户端所要连入的前端 AP 的 SSID。您可以通过**搜索**功能来选择所连入的 AP 的 SSID。
- **桥接 AP 物理地址**-本设备作为客户端所要连入的前端 AP 的 MAC 地址。您可以通过搜索功能来选择所连入的 AP 的 MAC 地址。
- **搜索**- 点击此按钮来搜索无线网络中的 AP。
- **传输功率**-有六种不同的传输功率可供选择。
- **无线安全模式**- 您可以从如下安全模式中选择一种：
 - **最安全 (WPA/WPA2-PSK)** - 基于共享密钥的 WPA 加密模式。
 - **安全 (WEP)** -基于非共享密钥的 WEP 加密模式。

- 无- 关闭无线安全功能。此时无线设备不需要密码验证就能连入此设备。
- 认证类型- 如果安全模式是 WEP，必须选择根 AP 的认证类型。
- 密钥格式-如果安全模式是 WEP，必须选择 WEP 密钥的格式。
- WEP 密钥序号- 如果安全模式是 WEP，必须选择 WEP 密钥的序号。
- 无线密钥- 如果您的设备所连入的 AP 需要密码验证，此处需填入这个密码。

 **注意:**

本设备的无线信号的覆盖范围很大程度上取决于它所安装的地理位置。为达到最佳效果，请在设备安装时遵循以下原则：

- 尽量选择高处，比如一个较高的架子上。
- 远离潜在的干扰源，比如电脑，微波炉和无绳电话等。
- 天线处于直立位置。
- 远离大的金属表面。

若不遵循以上原则将导致本设备性能下降，或导致该区域内的无线设备无法连接到本设备。

2. AP列表界面如图 3-35所示，选择您要连入的前端AP的BSSID（与它的MAC地址相同）并点击连接。

ID	BSSID	SSID	信号强度	信道	是否加密	选择
1	40-16-9F-AA-AA-E5		29dB	1	WPA/WPA2-PSK	连接
2	8C-21-0A-82-6A-B8	Alcatel	19dB	1	WPA/WPA2-PSK	连接
3	00-11-22-33-44-55	CU_3344	19dB	1	WPA-PSK	连接
4	00-13-4E-0B-2A-7B	CU_3dEn	47dB	1	WPA-PSK	连接
5	00-13-4E-0B-2A-7C	CU_vap0_3dEn	47dB	1	WPA-PSK	连接
6	00-13-4E-0B-2A-7D	CU_vap1_3dEn	46dB	1	WPA-PSK	连接
7	00-13-4E-0B-2A-7E	CU_vap2_3dEn	49dB	1	WPA-PSK	连接
8	00-0A-EB-07-40-09	TP-LINK_074009	25dB	1	否	连接
9	00-14-78-88-88-E0	TP-LINK_8888DF	24dB	1	否	连接
10	EC-88-8F-97-37-E6	TP-LINK_9737E6	22dB	1	WPA/WPA2-PSK	连接
11	40-16-9F-BF-50-F0	TP-LINK_BF50F0	61dB	1	否	连接
12	94-27-19-E7-84-AB	TP-LINK_E784AB	30dB	1	否	连接
13	AA-00-01-02-03-05	TP-LINK_FFFFFFFF	24dB	1	否	连接
14	08-19-A6-60-15-D8	ChinaNet-LPNV	19dB	2	WPA/WPA2-PSK	连接
15	40-16-9F-BF-50-F2	TP-LINK_BF50F2	50dB	2	否	连接
16	46-16-9F-BF-50-F2	TP-LINK_BF50F2_01	50dB	2	否	连接
17	4A-16-9F-BF-50-F2	TP-LINK_BF50F2_02	50dB	2	否	连接

图 3-35 AP 列表

您将返回到图 3-34所示的无线页面，此时无线安全模式已经被选定，请确认并输入与前端AP或者路由器相同的密码，然后点击下一步。

3. 在弹出的本地无线 AP 设置页面里，输入 本地无线名称。默认情况下，本地无线网络的安全设置将和前端 AP 保持一致。然后点击下一步。

图 3-36 设置向导-本地无线 AP 设置

4. 随后弹出网络的设置页面如图 3-37所示，建议您保持当前的默认设置不变，点击下一步。

图 3-37 设置向导-网络

5. 当您完成图 3-37中的设置，点击下一步，将会出现下图的界面图 3-38，您可以点击**重启**按钮来使配置生效。

图 3-38 设置向导-结束

3.3.7 客户端

当你选择了**客户端**模式，请按以下步骤配置设备：

1. 在图 3-10中点击**下一步**，将弹出无线设置页面如图 3-39，点击**搜索**按钮来扫描整个无线网络。

设置向导 - 无线

前端AP无线名称： (也叫做SSID)

前端AP物理地址：

搜索

点击“搜索”按钮扫描无线网络，并选择目标设置。

传输功率：

无线安全模式：

所有的安全设置，例如无线密钥应该符合前端AP/路由器。

无线密钥：

您可以输入8到63个ASCII字符或8到64个十六进制字符。

图 3-39 设置向导-无线

- **前端 AP 无线名称**- 本设备作为客户端所要连入的前端 AP 的 SSID。您可以通过搜索功能来选择所连入的 AP 的 SSID。
- **前端 AP 物理地址**-本设备作为客户端所要连入的前端 AP 的 MAC 地址。您可以通过搜索功能来选择所连入的 AP 的 MAC 地址。
- **搜索**- 点击此按钮来搜索无线网络中的 AP。
- **传输功率**-有六种不同的传输功率可供选择。
- **无线安全模式**- 您可以从如下安全模式中选择一种：
 - **最安全 (WPA/WPA2-PSK)** - 基于共享密钥的 WPA 加密模式。
 - **安全 (WEP)** -基于非共享密钥的 WEP 加密模式。
 - **无**- 关闭无线安全功能。此时无线设备不需要密码验证就能连入此设备。
- **认证类型**- 如果安全模式是 WEP，必须选择根 AP 的认证类型。
- **密钥格式**-如果安全模式是 WEP，必须选择 WEP 密钥的格式。
- **WEP 密钥序号**- 如果安全模式是 WEP，必须选择 WEP 密钥的序号。
- **无线密钥**- 如果您的设备所连入的 AP 需要密码验证，此处需填入这个密码。

注意：

本设备的无线信号的覆盖范围很大程度上取决于它所安装的地理位置。为达到最佳效果，请在设备安装时遵循以下原则：

- 尽量选择高处，比如一个较高的架子上。
- 远离潜在的干扰源，比如电脑，微波炉和无绳电话等。
- 天线处于直立位置。
- 远离大的金属表面。

若不遵循以上原则将导致本设备性能下降，或导致该区域内的无线设备无法连接到本设备。

2. AP列表界面如图 3-40所示，选择您要连入的前端AP的BSSID（与它的MAC地址相同）并点击连接。

ID	BSSID	SSID	信号强度	信道	是否加密	选择
1	40-16-9F-AA-AA-E5		29dB	1	WPA/WPA2-PSK	连接
2	8C-21-0A-82-6A-B8	Alcatel	19dB	1	WPA/WPA2-PSK	连接
3	00-11-22-33-44-55	CU_3344	19dB	1	WPA-PSK	连接
4	00-13-4E-0B-2A-7B	CU_3dEn	47dB	1	WPA-PSK	连接
5	00-13-4E-0B-2A-7C	CU_vap0_3dEn	47dB	1	WPA-PSK	连接
6	00-13-4E-0B-2A-7D	CU_vap1_3dEn	48dB	1	WPA-PSK	连接
7	00-13-4E-0B-2A-7E	CU_vap2_3dEn	49dB	1	WPA-PSK	连接
8	00-0A-EB-07-40-09	TP-LINK_074009	25dB	1	否	连接
9	00-14-78-88-88-E0	TP-LINK_8888DF	24dB	1	否	连接
10	EC-88-8F-97-37-E6	TP-LINK_9737E6	22dB	1	WPA/WPA2-PSK	连接
11	40-16-9F-BF-50-F0	TP-LINK_BF50F0	61dB	1	否	连接
12	94-27-19-E7-84-AB	TP-LINK_E784AB	30dB	1	否	连接
13	AA-00-01-02-03-05	TP-LINK_FFFFFFFF	24dB	1	否	连接
14	08-19-A6-60-15-D8	ChinaNet-LPNV	19dB	2	WPA/WPA2-PSK	连接
15	40-16-9F-BF-50-F2	TP-LINK_BF50F2	50dB	2	否	连接
16	46-16-9F-BF-50-F2	TP-LINK_BF50F2_01	50dB	2	否	连接
17	4A-16-9F-BF-50-F2	TP-LINK_BF50F2_02	50dB	2	否	连接

图 3-40 AP 列表

您将返回到图 3-39所示的无线页面，此时无线安全模式已经被选定，请确认并输入与前端AP或者路由器相同的密码，然后点击下一步。

3. 在弹出网络的设置页面如图 3-41所示，建议您保持当前的默认设置不变，点击下一步。

设置向导 - 网络

DHCP服务器： 不启用 启用

在大多数情况下，你的根AP /路由器启用了DHCP服务器功能，我们强烈建议您在此设备上禁用DHCP服务器功能以避免无法预测的问题。

IP地址：

子网掩码：

我们建议您配置这个AP使用相同的IP子网和子网掩码，但与根AP/路由不同的IP地址。

改变登入账号： 否 是

图 3-41 设置向导-网络

4. 当您完成图 3-41中的设置，点击下一步，将会出现图 3-42的界面，您可以点击**重启**按钮来使配置生效。



图 3-42 设置向导-结束

第4章 接入点模式、多SSID模式、中继模式、桥接模式和客户端模式

本章介绍在接入点模式、多 SSID 模式、中继模式、桥接模式和客户端模式等工作模式下，如何使用 Web 管理页面配置 AP 的高级功能，在下面的说明书中，我们以接入点工作模式为例。

4.1 登录

启动AP并成功登录AP管理页面后，在左侧菜单栏中，共有如下七个菜单：**运行状态**，**设置向导**，**工作模式**，**网络参数**，**无线设置**，**DHCP服务器**和**系统工具**。点击某个菜单项，即可进行相应的功能设置。下面将详细讲解各个菜单的功能。

4.2 运行状态

选择菜单**运行状态**，可以查看AP当前的状态信息。

版本信息		
当前软件版本：	3.18.0 Build 130829 Rel.32571n	
当前硬件版本：	WA7210N v1 00000000	

有线状态		
MAC 地址：	E0-05-C5-5F-CC-90	
IP地址：	192.168.1.254	
子网掩码：	255.255.255.0	

无线状态		
运行模式：	接入点	
SSID：	TP-LINK_721002	
信道：	1	
模式：	11bgn mixed	
频段带宽：	自动	
MAC 地址：	E0-05-C5-5F-CC-90	

流量统计			
	接收	发送	
字节数：	0	975317	
数据包数：	0	3521	

运行时间：	0 天 00:02:22	刷新
-------	--------------	--------------------

图 4-1 运行状态

1. 有线状态

此处显示 AP 当前 LAN 口的设置状态，包括 MAC 地址、IP 地址和子网掩码。

2. 无线状态

此处显示 AP 当前的无线设置状态，包括无线功能、SSID、信道、模式、频段带宽、MAC 地址等信息。

3. 流量统计

此处显示 AP 当前的数据传输状态。

4. 运行时间

此处显示 AP 当前的运行时间。

4.3 设置向导

请参见 [3.3: "快速安装指南"](#)。

4.4 工作模式

本页用来选择 AP 的工作模式。本设备有 7 个工作模式供您选择：**AP 客户端路由**、**AP 路由**、**接入点**、**多 SSID**、**中继**、**桥接**和**客户端**模式，请选择一个您需要的工作模式，并且点击**保存**。

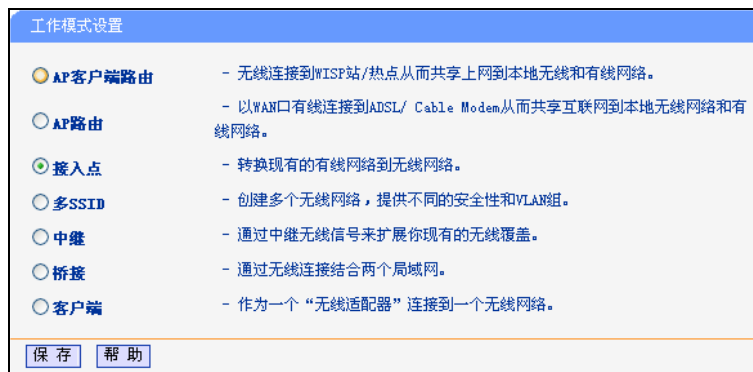


图 4-2 工作模式设置

➤ AP 客户端路由模式

该模式下，设备能够让多个用户共享来自WISP的互连网络。LAN端的设备通过无线端口从WISP共享一样的互联网IP地址。在AP客户端路由模式下，当连接WISP时，无线端口作为WAN口工作，而有线端口作为LAN口工作。

➤ AP 路由模式

该模式下，设备能够让多个用户共享来自ADSL/Cable调制器提供的互连网络。无线端口共享同样的IP到ISP，而这个IP通过有线WAN口获取。AP路由模式下，无线端口作为一个LAN端工作。

➤ 接入点模式

该模式下，AP作为无线网络中心接入到有线局域网中，从而扩展有线局域网覆盖范围。

➤ 多SSID模式

该模式下，AP能虚拟多个SSID供用户接入，同时，对连接到不同SSID的设备进行VLAN标记。

➤ 中继模式

该模式下，AP用于扩展另外一台AP或无线路由器的无线信号覆盖范围。一般该模式用于其他AP或者无线路由器支持WDS的情况下。

➤ 桥接模式

该模式下，AP可以将不超过4个局域网通过无线网络连接起来。

➤ 客户端模式

该模式下，AP设备的功能类似于无线网卡，可以用来连接WISP或者无线路由器。

4.5 网络参数

点击**网络参数**，在图 4-3中手动配置AP的网络参数。

The screenshot shows a web-based configuration interface for the LAN port. The title bar is labeled 'LAN'. The configuration fields are as follows:

- MAC地址: EO-05-C5-5F-CC-90
- 类型: 静态IP (dropdown menu)
- IP地址: 192.168.1.254
- 子网掩码: 255.255.255.0 (dropdown menu)
- 默认网关: 0.0.0.0
- IGMP代理: 开启 (dropdown menu)

At the bottom of the form, there are two buttons: '保存' (Save) and '帮助' (Help).

图 4-3 LAN 口设置

- MAC 地址:** AP 在局域网中的 MAC 地址，用来标识局域网，此值不可更改。
- 类型:** 选择动态 IP（DHCP）来从 DHCP 服务器获取 IP 地址，或者选择静态 IP 手动配置 IP 地址。
- IP 地址:** 输入 AP 的 IP 地址，格式为点分十进制（默认为 192.168.1.254）。
- 子网掩码:** 输入 AP 的子网掩码，通常为 255.255.255.0。
- 默认网关:** 输入 AP 的网关，此处要与 AP 的 IP 地址在同一个子网中。
- IGMP代理:** IGMP（Internet Group Management Protocol，Internet组管理协议）应用于IPTV组播数据。该设备支持可开关的IGMP代理功能和IGMP侦听功能。

👉 注意:

- 1) 如果改变LAN口IP地址，您必须使用新的IP地址登录AP的web页面。
- 2) 如果新的IP地址与原来的IP地址不在同一网段，DHCP服务器的地址池需要重新配置才能生效。
- 3) 如果新的IP地址与原来的IP地址不在同一网段，虚拟服务器和开放主机（DMZ host）的地址也将随之改变。
- 4) 保存配置后，设备将会自动重启。

4.6 无线设置

无线设置功能，可以安全方便的启用 AP 的无线功能进行网络连接。

无线设置菜单下有 8 个子菜单：无线基本设置，无线安全设置，无线 MAC 地址过滤，无线高级设置，天线对准，无线距离设置，无线流量监测和无线主机状态。

- 无线设置

- 无线基本设置
- 无线安全设置
- 无线MAC地址过滤
- 无线高级设置
- 天线对准
- 无线距离设置
- 无线流量监测
- 无线主机状态

点击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.6.1 无线基本设置

点击无线设置→无线基本设置，可以在图 4-5中进行无线网络的基本设置。

图 4-5 接入点模式下的无线基本设置

开启 VLAN:

若工作模式是多 SSID 模式，则在此选择是否开启 VLAN 功能并勾选 SSID 来配置对应的无线网络名称。

无线设置 - 多SSID

开启 VLAN

SSID1: TP-LINK_721002 VLAN ID: 1

SSID2: TP-LINK_721002_2 VLAN ID: 1

SSID3: TP-LINK_721002_3 VLAN ID: 1

SSID4: TP-LINK_721002_4 VLAN ID: 1

传输功率: 27 dBm

信道: 自动

模式: 11bgn mixed

信道带宽: 自动

开启无线功能

开启SSID广播

保存 帮助

图 4-6 多 SSID 模式下的无线基本设置

无线网络名称 (SSID)： 输入一串字符串来命名您的无线网络。最多可输入 32 位字符。您网络中的无线设备都需连入到此网络中。无线网络名称默认设置为 TP-LINK_xxxxxx (xxxxxx 是本台设备 MAC 地址的最后六位)，它的唯一性可以保证您无线网络的安全。但我们仍然建议您更改您的无线网络名称 (SSID)。此无线网络名称是区分大小写的，例如，MYSSID 和 MySsid 是两个不同的网络名。

传输功率： 有六种不同的传输功率可供选择。

信道： 以无线信号作为传输媒体的数据信号传送的通道，选择范围从 1 到 13。除非发现您的设备与附近其他 AP 设备产生信道冲突，否则此处不需要更改。如果选择“自动”，设备将根据当前各个频段的信号强度，选择干扰较小的频率段。

模式： 用于设置 AP 的无线工作模式，包括 11b only, 11g only, 11n only, 11bg mixed, 11bgn mixed。

信道带宽： 选择要使用的频段带宽。

开启无线功能： 开启或关闭无线功能。

开启 SSID 广播： 开启或关闭无线网络名称的广播功能。

完成更改后，点击保存按钮，AP 会自动重启使当前的设置生效。

4.6.2 无线安全设置

点击无线设置→无线安全设置，可以在界面图 4-7中设置无线网络安全选项。

无线网络安全设置

本页面设置路由器无线网络的安全认证选项。
安全提示：为保障网络安全，强烈推荐开启安全设置，并使用WPA/WPA2 - 个人版 AES加密方法。

不开启无线安全

WPA/WPA2 - 个人版 (推荐)

认证类型：

加密算法：

密码：
 (8-63个ASCII码字符或8-64个十六进制字符)

组密钥更新周期：
 (单位为秒，最小值为30，不更新则为0)

WPA/WPA2 - 企业版

认证类型：

加密算法：

Radius服务器IP：

Radius端口： (1-65535, 0表示默认端口:1812)

Radius密码：

组密钥更新周期：
 (单位为秒，最小值为30，不更新则为0)

WEP

认证类型：

WEP密钥格式：

密钥选择	WEP密钥	密钥类型
Key 1: <input checked="" type="radio"/>	<input type="text"/>	禁用 <input type="text"/>
Key 2: <input type="radio"/>	<input type="text"/>	禁用 <input type="text"/>
Key 3: <input type="radio"/>	<input type="text"/>	禁用 <input type="text"/>
Key 4: <input type="radio"/>	<input type="text"/>	禁用 <input type="text"/>

图 4-7 接入点模式下的无线安全设置

选择的 SSID: 如果设备的工作模式是多 SSID，从下拉框中选择一条 SSID 来进行配置。

无线网络安全设置

本页设置路由器无线网络的安全认证选项。
安全提示：为保障网络安全，强烈推荐开启安全设置，并使用WPA/WPA2 - 个人版 AES加密方法。

选择的SSID： TP-LINK_721002

不开启无线安全

WPA/WPA2 - 个人版 (推荐)

认证类型： 自动

加密算法： 自动

密码： 11111111
(8-63个ASCII码字符或8-64个十六进制字符)

组密钥更新周期： 30
(单位为秒，最小值为30，不更新则为0)

WPA/WPA2 - 企业版

认证类型： 自动

加密算法： 自动

Radius服务器IP：

Radius端口： 1812 (1-65535, 0表示默认端口：1812)

Radius密码：

组密钥更新周期： 0
(单位为秒，最小值为30，不更新则为0)

保存 帮助

图 4-8 多 SSID 模式下的无线安全设置

在无线网络安全设置页面，可以选择是否关闭无线安全功能。

- 如果您无需开启无线安全功能，请勾选**不开启无线安全**以关闭无线安全功能。如果关闭此功能，其他无线站点不需要任何认证就可以连接本地AP。
- 如果您要开启无线安全功能，则请选择页面中三种安全类型中的一种进行无线安全设置。

本页面提供了三种无线安全类型：**WPA/WPA2-个人版（推荐）**、**WPA/WPA2-企业版**和**WEP**。不同的安全类型下，安全设置项不同，下面将详细介绍。

1. WPA/WPA2-个人版（推荐）

WPA/WPA2个人版是基于共享密钥的WPA模式，安全性很高，设置也比较简单，适合普通家庭用户和小型企业使用。

认证类型: 自动选择 - 根据主机请求自动选择使用WPA-个人版还是WPA2-个人版的安全模式。

WPA-个人版 - 使用WPA-个人版的安全模式。

WPA2-个人版 - 使用WPA2-个人版的安全模式。

加密算法: 该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为自动，选择该项后，AP将根据实际需要自动选择TKIP或AES加密方式。

密码: 该项是WPA-PSK/WPA2-PSK的初始设置密钥, 设置时, 要求为8-63个ASCII字符或8-64个十六进制字符。

组密钥更新周期: 该项设置广播和组播密钥的定时更新周期, 以秒为单位, 最小值为30, 若该值为0, 则表示不进行更新。

 **注意:**

若 AP 进行了无线安全设置, 则该无线网络内的所有主机都必须根据此处的安全设置进行相应的设置, 如密码设置必须完全一样, 否则将不能成功的通过无线连接到本 AP。

2. WPA/WPA2-企业版

WPA/WPA2-企业版是一种比WEP强大的加密算法, 选择这种安全类型, AP将采用Radius服务器进行身份认证并得到密钥的WPA或WPA2安全模式。由于要架设一台专用的认证服务器, 代价比较昂贵且维护也很复杂, 所以不推荐普通用户使用此安全类型。

认证模式: 该项用来选择系统采用的安全模式, 即自动、WPA、WPA2。

- ◆ 自动: 若选择该项, AP会根据主机请求自动选择WPA或WPA2安全模式。
- ◆ WPA: 若选择该项, AP将采用WPA的安全模式。
- ◆ WPA2: 若选择该项, AP将采用WPA2的安全模式。

加密算法: 该项用来选择对无线数据进行加密的安全算法, 选项有Automatic、TKIP、AES。默认选项为Automatic, 选择该项后, AP将根据实际需要自动选择TKIP或AES加密方式。

Radius服务器IP: Radius服务器用来对无线网络内的主机进行身份认证, 此项用来设置该服务器的IP地址。

Radius端口: Radius服务器用来对无线网络内的主机进行身份认证, 此项用来设置该Radius认证服务采用的端口号。

Radius密码: 该项用来设置访问Radius服务的密码。

组密钥更新周期: 该项设置广播和组播密钥的定时更新周期, 以秒为单位, 最小值为30, 若该值为0, 则表示不进行更新。

3. WEP

WEP是Wired Equivalent Privacy的缩写, 它是一种基本的加密方法, 其安全性不如另外两种安全类型高。选择WEP安全类型, AP将使用802.11基本的WEP安全模式。

认证类型: 该项用来选择系统采用的安全模式, 包括自动、开放系统、共享密钥。

- ◆ 自动: 若选择该项, AP会根据主机请求自动选择开放系统或共享密钥方式。
- ◆ 开放系统: 若选择该项, AP将采用开放系统方式。此时, 无线网络内的主机可以在不提供认证密码的前提下, 通过认证并关联上无线网络, 但是若要传输数据, 必须提供正确的密码。
- ◆ 共享密钥: 若选择该项, AP将采用共享密钥方式。此时, 无线网络内的主机必须提供正确的密码才能通过认证, 否则无法关联上无线网络, 更无法进行数据传输。

密钥格式选择： 该项用来选择即将设置的密钥的形式，包括16进制、ASCII码。若采用16进制，则密钥字符只能为0-9，A、B、C、D、E、F；若采用ASCII码，则密钥字符可以是键盘上的任意字符。

WEP 密钥、密钥类型：

这两项用来选择密钥，设置具体的密钥值和选择密钥的类型，密钥的长度受密钥类型的影响。选择64位密钥需输入16进制字符10个，或者ASCII码字符5个。选择128位密钥需输入16进制字符26个，或者ASCII码字符13个。选择152位密钥需输入16进制字符32个，或者ASCII码字符16个。

- **WEP密钥：**在此输入WEP密钥，注意长度和有效字符范围。如果没有设置任何密钥，无线数据将不进行加密。
- **密钥类型：**可以选择使用64位、128位或152位的WEP密钥，选择“禁用”将不使用该密钥。

注意：

关于密钥选择中的4个密钥，可以只使用其一，也可以多个同时使用。无论哪种情况，客户端网卡上密钥的设置都必须与之一一对应。

4.6.3 无线MAC地址过滤

MAC 地址是网卡的物理地址，它就像是网卡的身份证，在网络中进行网卡的识别都是通过这个地址进行的。通常说的计算机的 MAC 地址也即计算机上网卡的 MAC 地址。

无线 MAC 地址过滤功能就是通过 MAC 地址来控制计算机能否接入无线网络，从而有效控制无线网络内用户的上网权限。

MAC 地址过滤功能通过 MAC 地址允许或拒绝无线网络中的计算机访问广域网，有效控制无线网络内用户的上网权限。利用按钮**添加新条目**来增加新的过滤规则；或者通过“**编辑**”、“**删除**”链接来修改或删除旧的过滤规则。

点击**无线设置**→**无线MAC地址过滤**，配置MAC地址过滤规则，来效控制无线网络内用户的上网权限。如图 4-9。

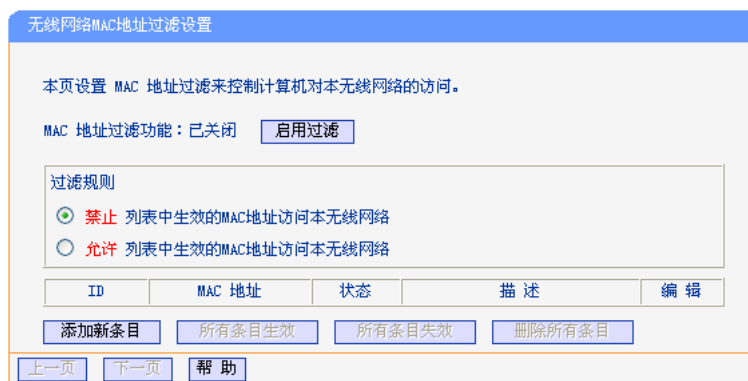


图 4-9 无线 MAC 地址过滤

选择的 SSID： 如果工作模式是多 SSID 模式，则在此下拉框中选择一条 SSID 进行配置。

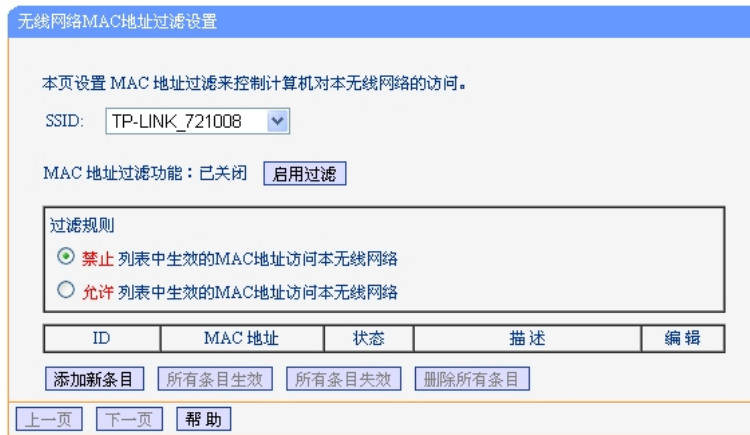


图 4-10 多 SSID 模式下无线 MAC 地址过滤

- 启用过滤：** 点击此按钮以开启无线网络的访问控制功能。
- 禁止：** 勾选以禁止列表中生效的 MAC 地址访问无线网络。
- 允许：** 勾选以允许列表中生效的 MAC 地址访问无线网络。
- MAC 地址：** AP 需要进行访问控制的无线主机的 MAC 地址。
- 状态：** 此条条目的状态，生效或失效。
- 描述：** 对此个无线主机的简单描述。
- 编辑：** 对表中的条目进行编辑或者删除。
- 添加新条目：** 点击该按钮，可以添加新的过滤条目。
- 所有条目生效：** 点击该按钮，可以将列表中的所有条目的状态设置为“生效”。
- 所有条目失效：** 点击该按钮，可以将列表中的所有条目的状态设为“失效”。
- 删除所有条目：** 点击该按钮，可以删除该列表中的所有条目。

请按照以下步骤创建 MAC 地址过滤条目。

首先，您必须决定未知无线客户端是否可以接入本 AP 的无线网络。如果未知无线客户端可以接入，请在过滤规则里选择**禁止列表中生效的 MAC 地址访问无线网络**；如果不允许未知无线客户端接入，请选择**允许列表中生效的 MAC 地址访问无线网络**。

点击**添加新条目**按钮，添加MAC地址过滤规则条目。然后**无线网络MAC地址过滤设置**页面将会弹出，如图 4-11所示。



图 4-11 添加或修改无线 MAC 地址过滤条目

MAC Address: 填写需要进行访问限制的无线网络内的主机 MAC 地址。MAC 地址的格式为：XX-XX-XX-XX-XX-XX（X 是任意十六进制数字），如 00-0A-EB-B0-00-0B。

描述: 为无线客户端添加简单的描述信息。如：无线主机 A。

状态: 选择是否启用本条目。**生效**或者**失效**。

举例：如果您希望 MAC 地址为 00-0A-EB-00-07-BE 的主机 A 可以访问无线网络，其他位置主机不能访问无线网络。您可以按照以下步骤进行配置：

1. 点击**启用过滤**按钮。
2. 在**过滤规则**处选择**允许列表**中**生效**的 MAC 地址访问无线网络。
3. 确认列表中没有任何生效的条目，如果有，将该条目状态改为**失效**或删除该条目，也可以点击**删除所有条目**按钮，将列表中的条目清空。
4. 点击**添加新条目**按钮，在 **MAC 地址**处填写 00-0A-EB-00-07-BE，在**描述**处填写无线主机 A，在**状态**处选择**生效**。设置完成后，点击**保存**按钮和**返回**按钮。

过滤规则表格显示如下：

ID	MAC 地址	状态	描述	编辑
1	00-0A-EB-00-07-BE	生效	无线主机A	编辑 删除

注意：

如果启用MAC地址过滤规则，并在**过滤规则**处选择**允许列表**中**生效**的MAC地址访问无线网络，而表中没有启用任何条目，这时没有任何无线客户端可以接入无线网络。

4.6.4 无线高级设置

选择**无线设置**→**无线高级设置**来设置本设备的部分高级功能，如图 4-12所示。由于各模式下本页面的配置项基本相同，下文中我们以接入点模式为例来说明。



图 4-12 无线高级设置

天线设置: 设置天线的极化方向，可以设置为垂直天线，水平天线和外部天线三种。

Beacon 时槽: 表示 AP 发送 Beacon 帧的发包间隔，AP 通过发送 Beacon 广播来进行无线网络连接的同步。可以设置为（40-1000）内的值，单位为毫秒（ms），默认值为 100。

RTS 时槽: 为数据包指定 RTS 阈值，当数据包长度超过 RTS 阈值时，路由器就会发送 RTS 到目的站点来进行协商，默认值为 2346。

- 分片阈值:** 为数据包指定分段阈值。当数据包的长度超过分段阈值时，会被自动分成多个数据包。过多的数据包将会造成网络性能降低，所以分段阈值不应设置过低，默认值为 2346。
- DTIM 阈值:** 该值在 1 至 255 之间，指定传输指示消息(DTIM, Delivery Traffic Indication Message) 的间隔，DTIM 是一种倒数计时作业，用以告知下一个要接收广播及多播的客户端窗口。当路由器已经为相关联的客户端缓存了广播或者多播信息时，它会在 Beacon 中夹带有下一个 DTIM 时槽的信息；当客户端听到 Beacon 讯号时，就会接收该广播和组播信息。DTIM 单位为 Beacon 时槽，默认值为 1，表示 DTIM 阈值与 Beacon 时槽相同。。
- 开启WMM:** 开启WMM后路由器具有无线服务质量(QoS)功能，可以对音频、视频数据优先处理，保证音频、视频数据的优先传输。推荐勾选此项。
- 开启Short GI:** 选择此项可以使路由器接收和发送短帧间隔数据包，提高路由器的传输速率，推荐勾选。
- 开启 AP 隔离:** 打开 AP 隔离，选择此项可以隔离关联到 AP 的各个无线主机。在开启 WDS/桥接功能时，此功能失效。

注意:

如果您不熟悉本页面上的配置条目，请保持它们的默认配置不变，否则可能引起无线网络的工作性能下降。

4.6.5 天线对准

点击**无线设置**→**天线对准**，当您改变天线的方向时，可以在本页看到 AP 的信号强度变化。

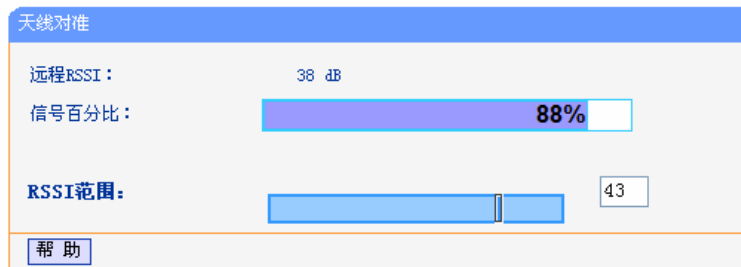


图 4-13 天线校准

- 远程RSSI:** 显示AP的信号强度值。
- 信号百分比:** 显示RSSI和RSSI 范围的比值，单位是百分比。
- RSSI 范围:** 您可以拖动滑块设置RSSI 范围值。如果RSSI 范围值减小，颜色变化对信号的波动将更敏感。滑块实际上是改变了指示器的最大值

注意:

只有**中继模式**、**桥接模式**、**客户端模式**和**AP 客户端路由模式**下，并与前端 AP 建立连接后，此功能才能生效。

4.6.6 无线距离设置

点击**无线设置**→**无线距离设置**，可以调整本设备的无线传输距离，它决定了户外无线网络连接的稳定性。输入无线传输距离，AP 会自动调整数据包的 ACK 超时时间。

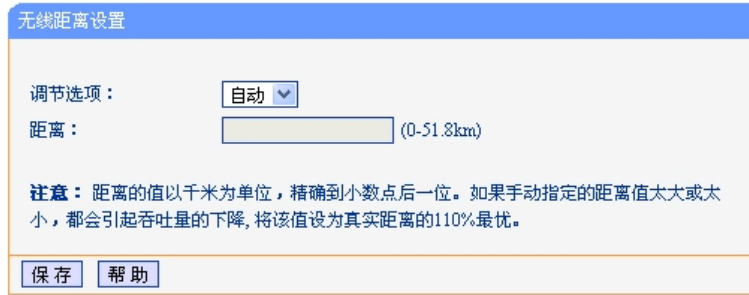


图 4-14 无线距离设置

调节选项： 如果AP在户外使用，请保持默认设置。您也可以手动设置距离。如果AP在室内使用，请使用室内模式。

距离： 输入无线传输距离，精确到小数点后一位，单位为千米。如果本距离太短或太长，将会导致无线传输信号和传输性能低下。此处最好填写真实距离的110%。

点击**保存**使配置生效。

4.6.7 无线流量监测

点击**无线设置**→**无线流量监测**，可以在图 4-15的界面中开始或停止无线通信的流量监测。



图 4-15 无线流量监测

速率： 流量单位。

运行时间： 流量监控功能运行的时间。

发送速率： 无线发射速率信息。

接收速率： 无线接收速率信息。

点击**开始**按钮开始无线流量监测。

点击**停止**按钮结束无线流量监测。

4.6.8 无线主机状态

点击**无线设置**→**无线主机状态**，查看当前连接到无线网络中的所有主机的基本信息。如图 4-16。

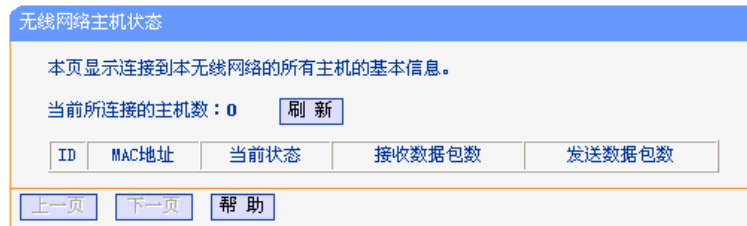


图 4-16 无线网络主机状态

MAC 地址: 显示当前已经连接到无线网络的主机的MAC地址。

当前状态: 此项显示当前主机的运行状态。

接收数据包数: 显示收到的数据包数目。

发送数据包数: 显示发送的数据包数目。

在本页无法进行任何修改，点击**刷新**按钮刷新当前无线连接状态。如果无线连接数目超过一页，点击**下一页**按钮，进入下一页；点击**上一页**按钮，返回上一页。

🔔 注意:

本页数据会每隔5秒自动刷新。

4.7 DHCP服务器

DHCP 指动态主机控制协议（Dynamic Host Configuration Protocol）。本 AP 具有 DHCP 服务功能，能够为所有接入 AP 并且应用 DHCP 服务的网络设备自动分配 IP 参数。

DHCP 菜单下有 3 个子菜单：**DHCP 服务**，**客户端列表**和**静态地址分配**。



点击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.7.1 DHCP服务

点击**DHCP服务器**→**DHCP 服务**，将看到DHCP服务界面，如图 4-18。开启DHCP服务器功能后，AP将会自动配置局域网中各主机的TCP/IP协议。

图 4-18 DHCP 设置

- DHCP 服务器:** 选择是否启用DHCP服务器功能，默认为不启用。
- 地址池开始/结束地址:** 分别输入开始地址和结束地址。完成设置后，DHCP服务器分配给内网主机的IP地址将介于这两个地址之间。开始地址默认值为192.168.1.100，结束地址默认值为192.168.1.199。
- 地址租期:** 即DHCP服务器给内网主机分配的IP地址的有效使用时间。在该段时间内，服务器不会将该IP地址分配给其它主机。
- 网关:** 可选项。应填入AP的LAN口的IP地址，缺省为0.0.0.0。
- 缺省域名:** 可选项。应填入本地网域名，缺省为空。
- 主 DNS 服务器:** 可选项。可以填入 ISP 提供的 DNS 服务器或保持缺省，若不清楚可咨询 ISP。
- 备用DNS服务器:** 可选项。如果ISP提供给您了两个DNS服务器，则您可以把另一个DNS服务器的IP地址填于此处。

完成更改后，点击**保存**按钮并重启AP使设置生效。

注意:

为了使用本路由器的DHCP服务器功能，局域网中各计算机的TCP/IP协议必须设置为“自动获得IP地址”。此功能需要重启AP才能生效。

4.7.2 客户端列表

点击**DHCP服务器**→**客户端列表**，可以查看客户端主机的相关信息；点击**刷新**按钮可以更新表中信息，如图 4-19。

ID	客户端名	MAC 地址	IP 地址	有效时间
1	android-5eac29e0f0a3dc35	38-AA-3C-CA-DE-DF	192.168.1.101	01:59:55

图 4-19 DHCP 客户端列表

- 客户端名：** 显示获得IP地址的客户端计算机的名称。
- MAC地址：** 显示获得IP地址的客户端计算机的MAC地址。
- IP地址：** 显示DHCP服务器分配给客户端主机的IP地址。
- 有效时间：** 指客户端主机获得的IP地址距到期所剩的时间。每个IP地址都有一定的租用时间，客户端软件会在租期到期前自动续约。

4.7.3 静态地址分配

点击**DHCP服务器**→**静态地址分配**，本页可以为指定MAC地址的计算机预留IP地址。当该计算机请求DHCP服务器分配IP地址时，DHCP服务器将给它分配表中预留的IP地址。如图 4-20。

静态地址分配

本页设置DHCP服务器的静态地址分配功能。

ID	MAC地址	IP地址	状态	编辑
1	00-13-BF-9C-24-65	192.168.1.24	生效	编辑 删除

图 4-20 静态地址分配

- MAC 地址：** 显示预留静态IP地址的计算机的MAC地址。
- IP地址：** 显示预留给内网主机的IP地址。
- 状态：** 显示该条目是否生效。只有状态为生效时，本条目的设置才生效。
- 编辑：** 修改或删除本条目。

添加预留 IP 地址：

1. 点击**添加新条目**按钮弹出如图 4-21的页面。
2. 输入 MAC 地址（MAC 地址默认格式为 XX-XX-XX-XX-XX-XX）和您需要预留的 IP 地址。
3. 状态设置为**生效**。
4. 点击**保存**按钮，使配置生效。

静态地址分配

本页设置DHCP服务器的静态地址分配功能。

MAC地址：

IP地址：

状态：

图 4-21 添加或修改预留 IP 地址条目

修改预留 IP 地址：

1. 选择需要修改的条目，点击**编辑**按钮。如果您想要删除该条目，请点击**删除**按钮。
2. 点击**保存**按钮使配置生效。

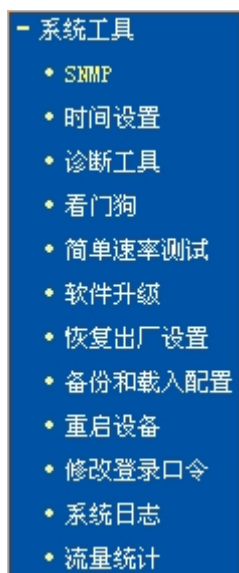
点击**删除所有条目**按钮，删除所有条目。

 **注意：**

所有配置将重启后生效。

4.8 系统工具

系统工具帮助您优化设备的配置。在系统工具菜单下有 12 个子菜单：**SNMP**、时间设置、诊断工具、看门狗、简单速率测试、软件升级、恢复出厂设置、备份和载入配置、重启路由器、修改登录口令、系统日志和流量统计。



点击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.8.1 SNMP

SNMP 允许网管通过在设备中的 SNMP 代理来获取设备的流量信息和传输情况。简单网管协议（SNMP）目前网络中应用最为广泛的网络管理协议，它提供了一个管理框架来监控和维护互联网设备。使用本功能，在下面页面中设置 SNMP 的相关参数。如图 4-22。



图 4-22 SNMP 设置

SNMP 服务： 您可以在此处选择开启或者关闭 SNMP 服务。当服务启用时，SNMP 代理收集本设备的信息，响应来自一个或多个管理系统的信息请求。

系统联系人： 本管理节点的管理员的联系信息。

- 系统名称：** 本管理节点的名称。
- 系统位置：** 本管理节点的物理位置。
- 只读团体名：** 团体(Community)是指为管理目的而集合在一起的主机群。只读团体(RO Community)对设备的 SNMP 信息只有读权限。默认的只读团体名为 public。
- 只读可信区：** 此处定义可以作为只读团体读取设备 SNMP 信息的主机的 IP 地址(如 10.10.10.1)或所在的子网。子网用“IP 地址/位数”的格式表示(如 10.10.10.0/24)。默认值为 0.0.0.0, 表示所有主机均可读取设备的 SNMP 信息。
- 读写团体名：** 读写团体(RW Community)对设备的 SNMP 信息具有读写权限。默认的读写团体名为 private。
- 读写可信区：** 此处定义可以作为读写团体读写设备 SNMP 信息的主机的 IP 地址(如 10.10.10.1)或所在的子网。子网用“IP 地址/位数”的格式表示(如 10.10.10.0/24)。默认值为 0.0.0.0, 表示允许所有主机读写设备的 SNMP 信息。

注意：

通过定义团体，可以实现仅允许同一团体内的管理系统和代理进行通讯。团体名可以看作网络主机组的共享密码。因此，为保障安全性，我们建议您在启用 SNMP 服务前先修改默认的团体名。如果团体名为空，则代理不会对任何出现的团体名作出响应。

4.8.2 时间设置

点击**系统工具**→**时间设置**，可以在图 4-23 界面中设置AP的系统时间。设置系统时间有两种方式，手动设置系统时间和通过互联网获取标准的GMT时间。

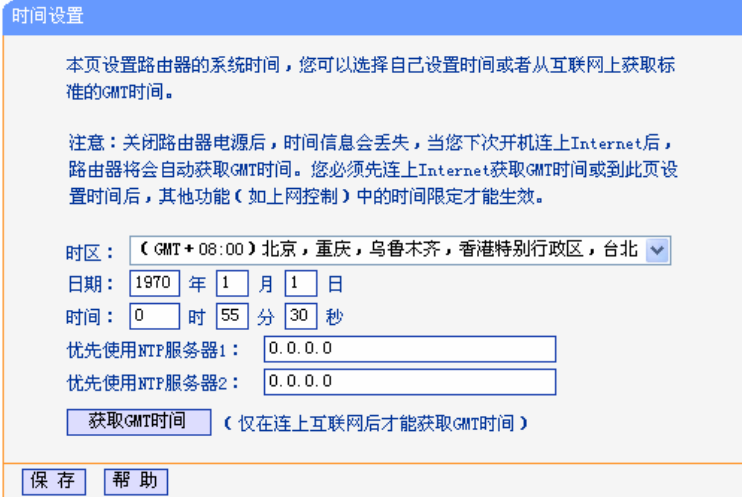


图 4-23 时间设置

- 时区：** 该项用来手动设置系统时间，请先选择您的时区。
- 日期：** 填写本地的日期，格式为月/日/年。
- 时间：** 填写本地时间，格式为时/分/秒。

优先使用 NTP 服务器 1/2:

该项用来设置 NTP 服务器的 IP 地址(最多可以输入两个)。NTP 服务器是网络时间服务器，用于同步互联网上的计算机时间。AP 内置了一些常用的 NTP 服务器地址，一旦与 Internet 连接后，路由器可以自动获取系统时间。但是，若此处设置了该项，则当路由器获取 GMT 时间时，将优先从已设置的时间服务器上获取。

获取GMT时间:

首先请连接互联网，选择所在的时区，最后点击**获取GMT时间**按钮即可从互联网上获取标准的GMT时间。

注意:

1. NTP (Network Time Protocol, 网络时间协议) 用来为路由器、交换机和工作站之间提供时间同步。时间同步的作用是可以将多台网络设备上的相关事件记录联系起来，有助于分析复杂的故障和安全事件等。
2. 关闭AP电源后，时间信息会丢失，只有当下次开机连上Internet后，AP会自动获取GMT时间。
3. 必须先通过Internet获取GMT时间或在此页手动设置系统时间后，AP其他功能(如防火墙)中的时间限定才能生效。

4.8.3 诊断工具

在本页面可以使用 ping 或者 tracert，诊断 AP 的连接状态。

图 4-24 诊断工具

选择操作:

选择 Ping 或 Tracert 操作。检测 AP 的连接状态。其中 Ping 功能用来检测 AP 和被测主机是否已连通及连接延时等，而 Tracert 功能用来检测 AP 要连通被测主机时需经过的其它路由器的个数。

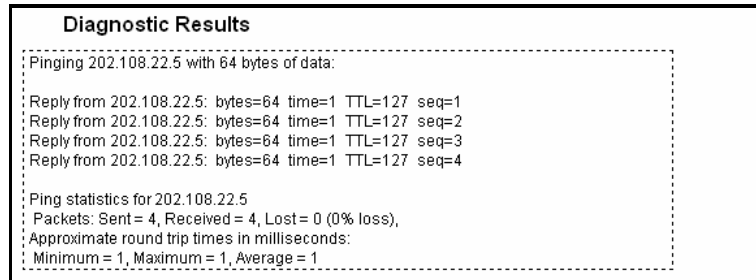
IP 地址/域名:

目的 IP 地址或域名。

- Ping 包数目：** Ping 操作发出的 Ping 包数目。
- Ping 包大小：** Ping 操作发出的 Ping 包的大小。
- Ping 超时：** 设置 Ping 操作的超时时间。
- Tracert 跳数：** 设置 Tracert 的跳数。

点击开始按钮来启动诊断，诊断结果页面中将显示诊断的结果。

如果诊断结果与下图类似，则说明网络连接正常。



注意：

1. 本功能在同一时间内只支持一个用户使用。
2. Ping/Tracert的目的地址可以是IP地址或者域名。如果对IP地址的Ping/Tracert操作成功，但是对相应的域名的Ping/Tracert操作失败，则问题可能是域名解析失败。请确认您输出的目的域名能够被DNS（Domain Name System, 域名系统）正确地解析。

4.8.4 看门狗

看门狗功能使 AP 通过连续 Ping 用户定义的 IP 地址，持续监测与远程主机的特殊连接。如果在用户定义的设置下不能 Ping 通，AP 将会自动重启。

点击**系统工具**→**开门狗**，您可以在图 4-25界面中配置看门狗功能。



图 4-25 开门狗功能

- 开启开门狗功能：** 勾选启用看门狗功能。
- 目标 IP 地址：** 看门狗发送 Ping 数据包的目的主机的 IP 地址。
- 发包周期：** 发送两个连续 Ping 数据包的时间间隔。
- 启动延迟：** AP 重启之后到发送第一个 Ping 数据包之前的时间延迟。
- 最大丢包数量：** 目的主机连续没有响应的 Ping 数据包的最大数目，如果超过这个值，设备将会自动重启

4.8.5 简单速率测试

速率测试帮助您检测设备与当前网络中任意可达的 IP 地址的连接速率，专门用于搭建远距离无线连接的环境中，也可以用于粗略估计两个设备间的预留带宽。

点击**系统工具**→**简单速率测试**，可以在图 4-26中配置速率测试功能。

图 4-26 网络速率测试

目标 IP: 远程设备的 IP 地址。

发射: 估算发送的数据量。

接收: 估算接受的数据量。

当获取到足够的信息之后，请点击**开始测试**来启动一次新的测试。您也可以在测试过程中随时按**终止测试**按钮来终止当前的测试。

4.8.6 软件升级

点击**系统工具**→**软件升级**，可以在图 4-27界面中升级本设备的软件版本以获得更多的功能和更为稳定的性能。

图 4-27 软件升级

软件升级步骤：

- 第一步：登录本公司的网站（<http://www.tp-link.com.cn>），下载最新版本的软件。
- 第二步：点击**浏览**按钮选择下载的文件，或在“文件”栏内填入已下载升级软件文件的全路径文件名。
- 第三步：点击**升级**进行软件升级。
- 第四步：升级完成后，设备将自动重启。

注意：

1. 升级软件后，路由器可能会恢复到出厂默认设置，现有的所有设置信息将丢失，建议在升级软件之前备份现有设置信息。
2. 升级时请选择与当前硬件版本一致的软件。升级过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。当升级结束后，路由器将会自动重启。

当前软件版本： 显示设备当前的软件版本。

当前硬件版本： 显示设备当前的硬件版本。

4.8.7 恢复出厂设置

点击**系统工具**→**恢复出厂设置**，可以将设备的所有设置恢复到出厂时的默认状态。恢复出厂设置后，设备将自动重启，恢复出厂设置页面如图 4-28。

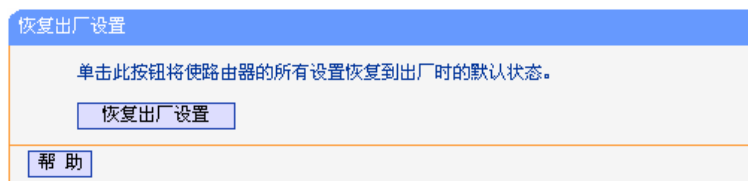


图 4-28 恢复出厂设置

点击**恢复出厂设置**按钮，路由器的所有设置将恢复到出厂时的默认状态。其中：

- 默认的用户名：admin
- 默认的密码：admin
- 默认的IP地址：192.168.1.254
- 默认的子网掩码：255.255.255.0

注意：

恢复出厂设置后，您之前的配置信息将丢失。

4.8.8 备份和载入配置

配置备份功能可以将路由器的设置以文件形式保存到电脑中，以备下次使用；在升级路由器软件或在载入新的配置文件前备份路由器的原有配置，可以有效防止升级软件或载入新配置文件过程中丢失原有配置的问题。

配置载入功能则可以将先前保存的或已编辑好的配置文件重新载入。

如果需要为多台路由器配置相同的设置，则可以先配置一台路由器，保存其配置文件后，再将其载入到其它的路由器中，这样可以有效节省配置时间。

点击**系统工具**→**备份和载入配置**，可以在图 4-29中备份或载入AP的配置文件。

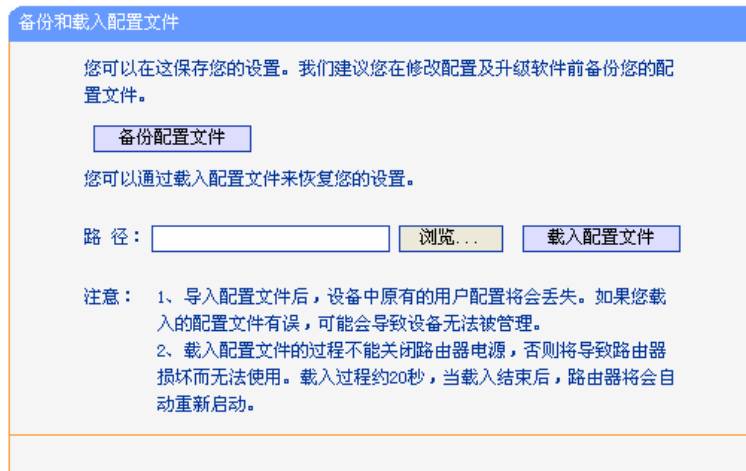


图 4-29 备份和载入配置

点击**备份配置文件**按钮来将当前所有的配置以文件的形式存入您的本地电脑。

点击**载入配置文件**按钮来将先前保存的或已编辑好的配置文件重新载入。

☞ 注意：

1. 载入配置文件后，设备中原有的配置信息将会丢失，所以在导入配置文件前请先备份配置。如果您载入的配置文件有误，可重新载入先前备份的文件。
2. 配置文件载入的过程中不能关闭接入器电源，否则将导致接入器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，AP将会自动重新启动。如果载入有错，请根据提示信息自己选择是否保存配置，最好重启AP。

4.8.9 重启设备

点击**系统工具**→**重启设备**，可以将AP重新启动，如图 4-30。



图 4-30 重启设备

点击**重启设备**按钮来重启设备。

本 AP 的某些设置需要在设备重新启动后才能生效，包括：

- 修改 LAN 口的基本网络参数（设备将自动重启）
- 修改 DHCP 的相关设置
- 修改无线配置
- 修改 Web 管理端口
- 升级设备的软件（设备将自动重启）
- 恢复 AP 的出厂设置（设备将自动重启）
- 载入配置文件（设备将自动重启）

4.8.10 修改登录口令

点击**系统工具**→**修改登录口令**，可以在图 4-31界面中修改登录AP管理界面的用户名和密码。修改完成后，点击**保存**按钮即可。

图 4-31 修改登陆口令

出于安全考虑，我们强烈推荐您更改初始系统管理员的口令。如果忘了系统口令，请将路由器恢复到出厂设置。

👉 注意：

系统管理员的口令长度应该在 0-14 位之间。且不含空格键。请输入两次新口令来确认。

输入完成后点击**保存**按钮。

要清除全部信息请点击**清空**按钮。

4.8.11 系统日志

点击**系统工具**→**系统日志**，可以在下图 4-32中查看AP的日志信息。该界面记录了AP的系统日志，可以通过查询日志了解网络情况和快速定位设备故障。

索引	时间	类型	级别	日志内容
2	1st day 00:00:16	DHCP	NOTICE	DHCP server started
1	1st day 00:00:07	其他	INFO	System started

Time = 1970-01-01 3:52:45 13966s
H-Ver = TL-WA7210N v1.0 00000000 : S-Ver = 1.0.0 Build 20130730 Rel. 33181
L = 192.168.0.254 : M = 255.255.255.0
W1 = DHCP : Y = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0

图 4-32 系统日志

通过邮件定时发送日志功能： 设置是否启用邮件发送日志功能。

邮件发送设置： 设置邮件的收/发邮箱地址、SMTP 服务器地址、验证信息以及自动发送功能的时间表。

图 4-33 邮件发送设置

➤ 邮件帐户设置

发信邮箱地址:

设备使用的邮件帐户，设备通过该帐户发送邮件。

收信邮箱地址:

发送邮件的目的邮箱，最终该邮箱会收到发送的邮件。

SMTP 服务器地址:

提供 SMTP 服务的服务器地址，各大邮件门户网站均提供该服务器，例如 163 邮箱的 SMTP 服务器地址是 smtp.163.com。如果不清楚该地址可以登录相关的邮件网站查询帮助页面。

启用验证:

需要用户名/密码登录的邮箱基本上都需要启用验证。

用户名:

登录邮箱的用户名(不含@后面的字段)。

密码和密码确认:

登录邮箱用的密码。

➤ 定时自动发送日志功能

启用功能:

开启定时器，让日志自动通过邮件发送。

每天发送:

给出一天其中的一个时间点，路由器每天在该时间点会自动发送包含当前日志的邮件。

间隔发送:

给出一段间隔时间，路由器将在功能启动/系统启动后立即发送一封包含当前日志的邮件，并每经过这段间隔时间就发送一次邮件。

4.8.12 流量统计

点击系统工具→流量统计，可以在图 4-34中查看AP的流量信息。点击刷新按钮，可以更新流量统计表；本页分别对设备总的的数据流量以及最近一段时间间隔内的数据流量进行统计。

图 4-34 流量统计

当前流量统计状态： 显示流量统计功能是否开启，默认为关闭。

数据包统计时间间隔： 设置数据包统计时间间隔。默认为 10 秒，请在 5-60 秒之间选择。

分类规则下拉框选择流量统计表中的排序规则。包括：**按 IP 地址排序**、**按总流量数据包排序**、**按总流量字节数排序**、**按当前流量数据包排序**、**按当前流量字节数排序**。

统计表：

IP 地址		被统计主机的 IP 地址，此处也会显示该主机的 MAC 地址。
总流量	数据包数	设备接受和发送的数据包总数。
	字节数	设备接受和发送的字节总数。
当前流量	数据包数	设备在用户指定的数据包统计时间间隔中收、发数据的包的个数。
	字节数	设备在用户指定的数据包统计时间间隔中收、发数据的字节数。
	ICMP Tx	设备在用户指定的数据包统计时间间隔中每秒发送到广域网的 ICMP 包的个数。统计数字表现为：当前发送速率/历史最高发送速率。
	UDP Tx	设备在用户指定的数据包统计时间间隔中每秒发送到广域网的 UDP 包的个数。统计数字表现为：当前发送速率/历史最高发送速率。
	SYN Tx	设备在用户指定的数据包统计时间间隔中每秒发送到广域网的 TCP SYN 包的个数。统计数字表现为：当前发送速率/历史最高发送速率。

第5章 AP客户端路由模式和AP路由模式

本章介绍了在 AP 客户端路由模式和 AP 路由模式下，如何使用 Web 管理页面配置设备的高级功能。在下面的说明书中，我们以 AP 客户端路由工作模式为例。

5.1 登录

启动设备并成功登录设备管理页面后，在左侧菜单栏中，共有如下七个菜单：**运行状态**，**设置向导**，**工作模式**，**网络参数**，**无线设置**，**DHCP服务器**和**系统工具**。点击某个菜单项，即可进行相应的功能设置。下面将详细讲解各个菜单的功能。

5.2 运行状态

选择菜单**运行状态**，可以查看设备当前的状态信息。

版本信息		
当前软件版本：	3.18.0 Build 130829 Rel.32571n	
当前硬件版本：	WA7210N v1 00000000	

LAN口状态		
MAC 地址：	E0-05-C5-5F-CC-90	
IP地址：	192.168.1.254	
子网掩码：	255.255.255.0	

无线状态		
无线功能：	开启	
SSID号：	TP-LINK_721002	
信道：	1	
模式：	11bgn mixed	
频段带宽：	自动	
最大发送速率：	150Mbps	
MAC 地址：	E0-05-C5-5F-CC-90	
客户端状态：	扫描...	

WAN口状态		
MAC地址：	E0-05-C5-5F-CC-91	
IP地址：	192.168.0.122	静态IP
子网掩码：	255.255.255.0	
默认网关：	192.168.0.1	
DNS服务器：	192.168.0.1 , 0.0.0.0	

WAN口流量统计		
	接收	发送
字节数：	0	0
数据包数：	0	0

运行时间：	0 天 00:04:03	<input type="button" value="刷新"/>
-------	--------------	-----------------------------------

图 5-1 运行状态

- 版本信息:** 此处显示路由器当前的软硬件版本号。可以在**系统工具**→**软件升级**界面升级软件版本。
- LAN 口状态:** 此处显示路由器当前 LAN 口的 MAC 地址、IP 地址和子网掩码。其中 IP 地址和子网掩码可以在**网络参数**→**LAN 口设置**界面中进行设置。
- 无线状态:** 此处显示路由器当前的无线设置状态，包括无线功能、SSID 号、信道、模式、频段带宽、最大发送速率、MAC 地址和客户端状态等信息。
- WAN 口状态:** 此处显示路由器当前 WAN 口的 MAC 地址、IP 地址、子网掩码、网关和 DNS 服务器地址。可以在**网络参数**→**WAN 口设置**界面中进行相关设置。
- WAN 口流量统计:** 此处显示当前 WAN 口接收和发送的数据流量信息。
- 运行时间:** 此处显示路由器当前的运行时间。

5.3 设置向导

请参见 [3.3: "快速安装指南"](#)。

5.4 工作模式

本页用来选择 AP 的工作模式。本设备有 7 个工作模式供您选择：**AP 客户端路由**、**AP 路由**、**AP、多 SSID**、**中继**、**桥接**和**客户端模式**，请选择一个您需要的工作模式，并且点击**保存**。

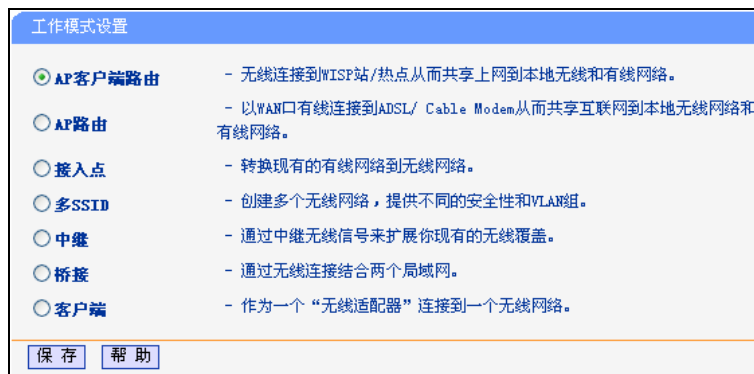


图 5-2 工作模式设置

➤ AP 客户端路由模式

该模式下，设备能够让多个用户共享来自 WISP 的互联网。LAN 端的设备通过无线端口从 WISP 共享一样的互联网 IP 地址。在 AP 客户端路由模式下，当连接 WISP 时，无线端口作为 WAN 口工作，而有线端口作为 LAN 口工作。

➤ AP 路由模式

该模式下，设备能够让多个用户共享来自 ADSL/Cable 调制解调器提供的互联网。无线端口共享同样的 IP 到 ISP，而这个 IP 通过有线 WAN 口获取。AP 路由模式下，无线端口作为一个 LAN 端工作

➤ 接入点模式

该模式下，AP 作为无线网络中心接入到有线局域网中，从而扩展有线局域网覆盖范围。

➤ 多 SSID 模式

该模式下，AP 能虚拟多个 SSID 供用户接入，同时，对连接到不同 SSID 的设备进行 VLAN 标记。

➤ 中继模式

该模式下，AP用于扩展另外一台AP或无线路由器的无线信号覆盖范围。一般该模式用于其他AP或者无线路由器支持WDS的情况下。

➤ 桥接模式

该模式下，AP可以将不超过4个局域网通过无线网络连接起来；

➤ 客户端模式

该模式下，AP设备的功能类似于无线网卡，可以用来连接WISP或者无线路由器。

5.5 网络参数

在网络参数功能中，可以根据组网需要设置路由器在局域网中的 IP 地址，并根据 ISP 提供的网络参数方便快捷地设置路由器 WAN 口参数，使局域网计算机能够共享 ISP 提供的网络服务。

选择菜单**网络参数**，可以看到：



点击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.5.1 WAN口设置

WAN 是广域网(Wide Area Network)的缩写。在对 WAN 口参数的设置中，可以根据 ISP 提供的连接类型方便快捷地设置路由器，使局域网计算机共享 ISP 提供的网络服务。在此设置中各种参数均由 ISP 提供，当参数不明确时请咨询 ISP。

选择菜单**网络参数**→**WAN口设置**，可以在随后出现的界面中配置WAN口的网络参数。本路由器支持6种上网方式：动态IP、静态IP、PPPoE、L2TP、PPTP和DHCP+，请咨询ISP提供哪种上网方式并获取相关参数。你也可以点击页面上的“自动检测”按钮，让路由器检测合适的上网方式。

1. 静态 IP

当ISP提供的上网方式为静态IP时，ISP会提供IP地址、子网掩码、网关和DNS服务器等WAN IP 信息时，请选择**静态IP**。如图 5-3所示。具体设置时，若不清楚，请咨询ISP。

The image shows the "WAN口设置" (WAN Port Settings) configuration page. The "WAN口连接类型" (WAN Port Connection Type) is set to "静态IP" (Static IP). The "自动检测" (Auto Detect) button is visible. The configuration fields are as follows:

WAN口连接类型：	静态IP	自动检测
IP 地址：	0.0.0.0	
子网掩码：	0.0.0.0	
网关：	0.0.0.0	
数据包MTU (字节)：	1500	(默认是1500, 如非必要, 请勿修改)
DNS服务器：	0.0.0.0	
备用DNS服务器：	0.0.0.0	(可选)

At the bottom, there are "保存" (Save) and "帮助" (Help) buttons.

图 5-3 WAN 口设置-静态 IP

- IP地址：** 输入ISP提供的IP地址信息，必填项。
- 子网掩码：** 输入ISP提供的子网掩码，必填项。根据不同的网络类型子网掩码不同，一般为255.255.255.0(C类)。
- 网关：** 输入ISP提供的网关参数。
- 数据包MTU：** MTU全称为最大数据传输单元，缺省为1500。请向ISP咨询是否需要更改。如非特别需要，一般不要更改。
- DNS服务器、备用DNS服务器：** ISP一般至少会提供一个DNS(域名服务器)地址，若提供了两个DNS地址则将其中一个填入“备用DNS服务器”栏。

完成更改后，点击**保存**按钮。

2. 动态 IP

选择**动态IP**，路由器将从ISP(网络服务提供商)自动获取IP地址。当ISP未提供任何IP网络参数时，请选择这种连接方式。如图 5-4。

图 5-4 WAN 口设置-动态 IP

- 更新：** 点击**更新**按钮，可以查看路由器从ISP的DHCP服务器上动态得到IP地址、子网掩码、网关以及DNS服务器。
- 释放：** 点击**释放**按钮，路由器将发送DHCP释放请求给ISP的DHCP服务器，释放IP地址、子网掩码、网关以及DNS服务器设置。
- 数据包MTU：** MTU全称为最大数据传输单元，缺省为1500。请向ISP咨询是否需要更改。如非特别需要，一般不要更改。
- DNS服务器、备用DNS服务器：**

显示从ISP处自动获取的DNS服务器地址。当需要使用已有的DNS服务器时，勾选“手动设置DNS服务器”，并在此处输入DNS服务器和备用DNS服务器(选填)的IP地址。路由器将优先连接手动设置的DNS服务器。

主机名： 设置路由器的主机名。ISP的DHCP服务器可以通过主机名识别您的身份。

单播方式获取IP： 少数ISP的DHCP服务器不支持广播请求方式，如果在网络连接正常的情况下无法获取IP地址，请选择此项。

完成更改后，点击**保存**按钮。

3. PPPoE

如果ISP提供的是**PPPoE**(以太网上的点到点连接)，ISP会提供上网帐号和上网口令。具体设置时，若不清楚，请咨询ISP。如图 5-5。

图 5-5 WAN 口设置-PPPoE

上网账号： 请正确输入ISP提供的上网账号，必须填写。

上网口令： 请正确输入ISP提供的上网口令，必须填写。

确认口令： 请再次输入ISP提供的上网口令，必须填写。

第二连接： 如果ISP还提供了以动态IP或静态IP的方式连接到局域网的连接，请选择“动态IP”或“静态IP”来启动这个连接。

按需连接： 若选择按需连接模式，当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。对于采用按使用时间进行计费的用户，选择按需连接可以有效节省上网费用。

自动断线等待时间： 如果自动断线等待时间T不等于0(默认时间为15分钟)，则在检测到连续T分钟内没有网络访问流量时自动断开网络连接，保护上网资源。此项设置仅对“按需连接”和“手动连接”生效。

自动连接: 在开机后系统自动连接网络。在使用过程中，如果由于外部原因网络被断开，系统就会主动尝试连接，直到成功连接。若网络服务是包月交费形式，推荐选择该项连接方式。

定时连接: 系统在连接时段的开始时刻主动进行网络连接，在终止时刻自动断开网络连接。选择此连接模式，可以有效控制内网用户的上网时间。

手动连接: 开机或断线后，在此处或个人计算机中手动拨号连接。若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若网络服务是按时间交费，选择手动连接可有效节省上网费用。

连接/断线: 点击此按钮，可进行即时的连接/断线操作。

若需要进一步设置，可以点击**高级设置**按钮，在下图5-6界面中进行高级设置。

PPPoE高级设置

数据包MTU(字节): 1480 (默认是1480, 如非必要, 请勿修改)

服务名: (如非必要, 请勿填写)

服务器名: (如非必要, 请勿填写)

使用ISP指定的IP地址

ISP指定的IP地址: 0.0.0.0

在线检测间隔时间: 0 秒 (0 ~ 120 秒, 0 表示不发送)

手动设置DNS服务器

DNS服务器: 0.0.0.0

备用DNS服务器: 0.0.0.0 (可选)

返回

保存 帮助

图 5-6 WAN 口设置-PPPoE-高级设置

数据包MTU: 填入网络数据包的MTU值，缺省为1480，如非特别需要，一般不要更改。

服务名、服务器名称: 如果不是ISP特别要求，请不要填写这两项。

使用ISP指定IP地址: 该项仅适用于静态PPPoE。如果ISP提供上网帐号和口令时，还提供了IP地址，请选中此选择框，并输入PPPoE连接的静态IP地址。

在线检测间隔时间: 设置该值后，路由器将根据指定的时间间隔发送检测信号，以检测服务器是否在线。如果该值为0，则表示不发送检测信号。

DNS服务器、备用DNS服务器:

该处显示从ISP处自动获得的DNS服务器地址。当需要使用已有的DNS服务器时，请选择“手动设置DNS服务器”，并手动输入DNS服务器和备用DNS服务器IP地址(至少设置一个)。连接时，路由器将优先使用手动设置的DNS服务器。

完成更改后，点击**保存**按钮。

4. L2TP

如果ISP提供的是**L2TP**上网方式，ISP会提供上网帐号和上网口令。具体设置时，若不清楚，请咨询ISP。如图 5-7。

WAN口设置

WAN口连接类型：

上网帐号：

上网口令：

动态 IP 静态 IP

服务器 IP /域名：

IP 地址：

子网掩码：

网关：

DNS：

Internet IP：

Internet DNS：

数据包MTU(字节)： (缺省值为1460, 如非必要, 请勿修改)

根据您的需要, 请选择对应的连接模式:

自动断线等待时间： 分 (0 表示不自动断线)

按需连接, 在有访问数据时自动进行连接

自动连接, 在开机和断线后自动连接

手动连接, 由用户手动连接

图 5-7 WAN 口设置-L2TP

- 上网帐号：**请正确输入ISP提供的上网帐号，必须填写。
- 上网口令：**请正确输入ISP提供的上网口令，必须填写。
- 连接/断线：**点击此按钮，可进行即时的连接/断线操作。
- 动态或静态IP：**如果ISP分配了IP地址、子网掩码、网关和DNS服务器地址，请选择使用静态IP。否则使用动态IP。
- 服务器IP/域名：**输入由ISP提供的服务器IP或者域名。
- IP地址：**当选择使用静态IP时，请输入拨号时使用的IP地址。
- 子网掩码：**当选择使用静态IP时，请输入ISP提供的子网掩码。
- 网关：**当选择使用静态IP时，请输入ISP提供的网关IP地址。
- DNS：**当选择使用静态IP时，请输入ISP提供的DNS服务器地址。
- Internet IP：**从ISP的L2TP服务器得到的因特网IP地址。
- Internet DNS：**从ISP的L2TP服务器得到的DNS服务器地址。
- 数据包MTU：**填入网络数据包的MTU值，缺省为1460，如非特别需要，一般不要更改。
- 按需连接：**当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若网络服务是按时间交费，可以选择该项连接方式。

自动连接: 开机后系统自动连接网络。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间(30秒)尝试连接，直到成功连接为止。若网络服务是包月交费形式，可以选择该项连接方式。

手动连接: 开机或断线后，在此处或个人计算机中手动拨号连接。若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若网络服务是按时间交费，选择该连接方式可有效节省上网费用。

完成更改后，点击**保存**按钮。

5. PPTP

如果ISP提供的上网方式是PPTP，ISP会提供上网账号和上网口令。具体设置时，若不清楚，请咨询ISP。如图 5-8。

The screenshot shows the 'WAN口设置' (WAN Port Settings) window. The 'WAN口连接类型' (WAN Port Connection Type) is set to 'PPTP'. The '上网帐号' (Username) field contains 'username' and the '上网口令' (Password) field is masked with dots. There are '连接' (Connect), '断线' (Disconnect), and '未连接' (Not Connected) buttons. The '动态 IP' (Dynamic IP) radio button is selected. Below are fields for '服务器 IP /域名' (Server IP/Domain), 'IP 地址' (IP Address), '子网掩码' (Subnet Mask), '网关' (Gateway), and 'DNS'. The 'Internet IP' and 'Internet DNS' fields are also present. The '数据包MTU(字节)' (Packet MTU) is set to 1420. At the bottom, there is a section for '根据您的需要，请选择对应的连接模式' (Select the corresponding connection mode according to your needs) with three options: '按需连接' (Selected), '自动连接' (Auto-connect), and '手动连接' (Manual connect). The '自动断线等待时间' (Auto-disconnect wait time) is set to 15 minutes.

图 5-8 WAN 口设置-PPTP

上网帐号: 请正确输入ISP提供的上网帐号，必须填写。

上网口令: 请正确输入ISP提供的上网口令，必须填写。

连接/断线: 点击此按钮，可进行即时的连接/断线操作。

动态或静态IP: 如果ISP分配了IP地址、子网掩码、网关和DNS服务器地址，请选择使用静态IP。否则使用动态IP。

服务器IP/域名: 输入由ISP提供的服务器IP或者域名。

IP地址: 当选择使用静态IP时，请输入拨号时使用的IP地址。

子网掩码: 当选择使用静态IP时，请输入ISP提供的子网掩码。

- 网关:** 当选择使用静态IP时, 请输入ISP提供的网关IP地址。
- DNS:** 当选择使用静态IP时, 请输入ISP提供的DNS服务器地址
- Internet IP:** 从ISP的PPTP服务器得到的因特网IP地址。
- Internet DNS:** 从ISP的PPTP服务器得到的DNS服务器地址
- 数据包MTU:** 填入网络数据包的MTU值, 缺省为1420, 如非特别需要, 一般不要更改。
- 按需连接:** 当有来自局域网的网络访问请求时, 系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时, 系统会自动断开连接。若网络服务是按时间交费, 可以选择该项连接方式。
- 自动连接:** 开机后系统自动连接网络。在使用过程中, 如果由于外部原因, 网络被断开, 系统则会每隔一段时间(30秒)尝试连接, 直到成功连接为止。若网络服务是包月交费形式, 可以选择该项连接方式。
- 手动连接:** 开机或断线后, 在此处或个人计算机中手动拨号连接。若在指定时间内(自动断线等待时间)没有任何网络请求时, 系统会自动断开连接。若网络服务是按时间交费, 选择该连接方式可有效节省上网费用。

完成更改后, 点击**保存**按钮。

6. DHCP+

如果ISP提供的是**DHCP+**上网方式, ISP会提供上网帐号和上网口令。具体设置时, 若不清楚, 请咨询ISP。如图 5-9。

The screenshot shows the 'WAN口设置' (WAN Port Settings) window. The 'WAN口连接类型' (WAN Port Connection Type) is set to 'DHCP+'. The '上网帐号' (Internet Account) and '上网口令' (Internet Password) fields are empty. The 'IP地址' (IP Address), '子网掩码' (Subnet Mask), '网关' (Gateway), '首选DNS服务器' (Preferred DNS Server), and '备用DNS服务器' (Backup DNS Server) are all set to '0.0.0.0'. The '数据包MTU (字节)' (Packet MTU) is set to '1500' with a note '(缺省值为1500, 如非必要, 请勿更改)'. The '认证服务器' (Authentication Server) is set to '218.29.0.227' with a note '(缺省为 218.29.0.227)'. Under '根据您的需要, 请选择对应连接模式:', the '手动连接, 由用户手动进行连接。' (Manual connection, manual connection by user) option is selected. At the bottom, there are buttons for '连接' (Connect), '断线' (Disconnect), and '未连接' (Not connected), along with '保存' (Save) and '帮助' (Help) buttons.

图 5-9 WAN 口设置-DHCP+

上网帐号: 请正确输入ISP提供的上网帐号, 必须填写。

上网口令: 请正确输入ISP提供的上网口令, 必须填写。

- IP地址:** 从ISP的DHCP+服务器动态得到的IP地址。
- 子网掩码:** 从ISP的DHCP+服务器动态得到的子网掩码。
- 网关:** 从ISP的DHCP+服务器动态得到的网关。
- 首选DNS服务器:** 从ISP的DHCP+服务器动态得到的首选DNS服务器。
- 备用DNS服务器:** 从ISP的DHCP+服务器动态得到的备用DNS服务器。
- 数据包MTU:** 填入网络数据包的MTU值, 缺省为1500, 如非特别需要, 一般不要更改。
- 自动连接:** 开机后系统自动连接网络。在使用过程中, 如果由于外部原因, 网络被断开, 系统则会每隔一段时间(10秒)尝试连接, 直到成功连接为止。
- 手动连接:** 开机或断线后, 在此处或个人计算机中手动拨号连接。若在指定时间内(自动断线等待时间)没有任何网络请求时, 系统会自动断开连接。若网络服务是按时间交费, 选择该连接方式可有效节省上网费用。
- 连接/断线:** 点击此按钮, 可进行即时的连接/断线操作。
- 完成更改后, 点击**保存**按钮。

5.5.2 MAC地址克隆

选择菜单**网络参数**→**MAC地址克隆**, 可以在下图 5-10界面中设置路由器对广域网的MAC地址。

图 5-10 MAC 地址克隆

- MAC地址:** 此项默认为路由器WAN口的MAC地址。若ISP提供了一个MAC地址并要求对路由器WAN口的MAC地址进行绑定, 只要将提供的值输入到“MAC地址”栏。除非ISP有特别要求, 否则不建议更改MAC地址。
- 当前管理PC的MAC地址:** 该处显示当前正在管理路由器的计算机的MAC地址。
- 恢复出厂MAC:** 点击此按钮, 您即可恢复本路由器对广域网的MAC地址为出厂时的默认设置。
- 克隆MAC地址:** 点击此按钮, 可将当前管理PC的MAC地址克隆到“MAC地址”栏内。若ISP提供服务时要求进行MAC地址克隆, 则应进行该项操作, 否则无须克隆MAC地址。

完成更改后, 点击**保存**按钮, 路由器会自动重启。

注意：

只有局域网中的计算机才能使用“克隆 MAC 地址”功能。

5.5.3 LAN口设置

选择菜单**网络参数**→**LAN口设置**，在图 5-11界面中配置LAN接口的网络参数。如果需要，可以更改LAN接口IP地址以配合实际网络环境的需要。

图 5-11 LAN 口设置

- MAC地址：**本路由器对局域网的MAC地址，用来标识局域网。
- IP地址：**输入本路由器对局域网的IP地址。局域网中所有计算机的IP地址必须与此IP地址处于同一网段，且默认网关必须为此IP地址。IP地址的出厂默认值为192.168.1.254，为C类IP地址，适用于数量不超过200台计算机的小型网络，可以根据组网需要改变它。
- 子网掩码：**选择路由器对局域网的子网掩码。C类IP地址对应子网掩码为255.255.255.0，为保证网络连接正常，请不要改变子网掩码。可以根据实际的局域网类型以及IP地址类型选择不同的子网掩码。
- IGMP代理：**IGMP (Internet Group Management Protocol, Internet组管理协议) 应用于IPTV组播数据。该设备支持可开关的IGMP代理功能和IGMP侦听功能。

完成更改后，点击**保存**按钮，路由器会自动重启。

注意：

1. 如果改变了路由器LAN口IP地址，必须用新的IP地址才能登录路由器的WEB管理界面，并且局域网中所有计算机的默认网关必须设置为该IP地址才能正常上网。
2. 局域网中所有计算机的子网掩码必须与此处子网掩码设置相同。
3. 若您所设置的新的LAN口IP地址与原来的LAN口IP地址不在同一网段，则路由器的动态IP服务将会自动更改到新LAN口IP所在的网段，但是虚拟服务器和DMZ主机功能将失效。如果您希望启用这些功能，请重新对其进行设置。

5.6 无线设置

无线设置功能，可以安全方便的启用 AP 的无线功能进行网络连接。

无线设置菜单下有 8 个子菜单：**无线基本设置**，**无线安全设置**，**无线 MAC 地址过滤**，**无线高级设置**，**无限对准**，**无线距离监测**，**无线流量监测**和**无线主机状态**。

- 无线设置

- 无线基本设置
- 无线安全设置
- 无线MAC地址过滤
- 无线高级设置
- 天线对准
- 无线距离设置
- 无线流量监测
- 无线主机状态

点击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.6.1 无线基本设置

点击无线设置→无线基本设置，可以在无线设置中进行无线网络的基本设置（图 5-13和图 5-14）。

 **注意：**

AP路由模式和AP客户端路由模式下的无线设置界面不同，如图 5-13和图 5-14

1. AP 路由模式下的无线设置



图 5-13 AP 路由模式下的无线设置

无线网络名称（SSID）： 输入一串字符串来命名您的无线网络。最多可输入 32 位字符。您网络中的无线设备都需连入到此网络中。无线网络名称默认设置为 TP-LINK_XXXXXX（XXXXXX 是本台设备 MAC 地址的最后六位），它的唯一性可以保证您无线网络的安全。但我们仍然建议您更改您的无线网络名称（SSID）。此无线网络名称是区分大小写的，例如，MYSSID 和 MySsid 是两个不同的网络名。

传输功率： 有六种不同的传输功率可供选择。

信道： 以无线信号作为传输媒体的数据信号传送的通道，选择范围从 1 到 13。除非发现您的设备与附近其他 AP 设备产生信道冲突，否则此处不需要更改。如果选择“自动”，设备将根据当前各个频段的信号强度，选择干扰较小的频率段。

模式： 用于设置 AP 的无线工作模式，包括 11b only, 11g only, 11n only, 11bg mixed, 11bgn mixed。

信道带宽： 选择要使用的频段带宽。

开启无线功能： 开启或关闭无线功能。

开启 SSID 广播： 开启或关闭无线网络名称的广播功能。

完成更改后，点击**保存**按钮，设备会自动重启使当前的设置生效。

2. AP 客户端路由模式下的无线设置

图 5-14 AP 客户端路由模式下的无线设置

WISP 主机无线名称： 本设备作为客户端想要接入的 AP 的 SSID。您也可以用**搜索**功能找到这个 SSID 并加入。

WISP 主机物理地址： 本设备作为客户端想要接入的 AP 的 MAC 地址。您也可以用搜索功能找到这个 MAC 地址并加入。

搜索： 搜索工作在当前信道中的 AP。

密钥类型： 您可以从如下安全模式中选择一种：

- 最安全 (WPA/WPA2-PSK) - 基于共享密钥的 WPA 加密模式。
- 安全 (WEP) - 基于非共享密钥的 WEP 加密模式。
- 无- 关闭无线安全功能。此时无线设备不需要密码验证就能连入此设备。

认证类型： 如果安全模式是 WEP，必须选择根 AP 的认证类型。

密钥格式： 如果安全模式是 WEP，必须选择 WEP 密钥的格式。

WEP 密钥序号： 如果安全模式是 WEP，必须选择 WEP 密钥的序号。

密钥： 如果本设备所连入的 AP 需要密码验证，此处需填入这个密码。

本地无线名称（SSID）：

输入一串字符串来命名您的无线网络。最多可输入 32 位字符。您网络中的无线设备都需连入到此网络中。无线网络的名称默认设置为 TP-LINK_XXXXXX（XXXXXX 是本台设备 MAC 地址的最后六位），它的唯一性可以保证您无线网络的安全。但我们仍然建议您更改您的无线网络名称（SSID）。此无线网络名称是区分大小写的，例如，MYSSID 和 MySsid 是两个不同的网络名。

传输功率： 有六种不同的传输功率可供选择。

开启无线功能： 开启或关闭无线功能。

开启 SSID 广播： 开启或关闭无线网络名称的广播功能。

禁止本地无线接入： 勾选此项后本地无线网络中的设备将无法无线接入到本路由器。

在图 5-14 的设置页面中选择**搜索**，将会弹出 AP 列表，如图 5-15 所示。找到您所要接入的 AP 的 SSID，点击对应的**连接**以连入到该 AP 中。

ID	BSSID	SSID	信号强度	信道	是否加密	选择
1	40-16-9F-AA-AA-E5		14dB	1	WPA/WPA2-PSK	连接
2	00-11-22-33-44-55	CU_3344	0dB	1	否	连接
3	12-11-22-33-44-55	CU_3344_01	3dB	1	WPA-PSK	连接
4	22-11-22-33-44-55	CU_3344_02	0dB	1	WPA-PSK	连接
5	32-11-22-33-44-55	CU_3344_03	9dB	1	WPA-PSK	连接
6	EC-17-2F-F8-30-7E	CU_F830	34dB	1	WPA-PSK	连接
7	0C-4C-39-1D-00-7F	ChinaNet-KDmc	11dB	1	WPA/WPA2-PSK	连接
8	70-72-3C-D4-38-74	Jason	20dB	1	WPA-PSK	连接
9	0C-37-DC-F9-DB-61	MobileWiFi-db61	0dB	1	WPA-PSK	连接
10	38-83-45-67-38-26	PocketAP_123	21dB	1	WPA/WPA2-PSK	连接
11	EC-88-8F-01-01-90	TL-SC2000N	7dB	1	WPA/WPA2-PSK	连接
12	28-2C-B2-93-B3-C0	TL-WR841N	5dB	1	否	连接
13	00-0A-EB-07-40-09	TP-LINK_074009	12dB	1	否	连接
14	00-19-66-CA-8B-07	TP-LINK_07_aaa	21dB	1	WPA/WPA2-PSK	连接
15	00-0A-EB-89-80-22	TP-LINK_2_4GHz_898022	5dB	1	WPA2-PSK	连接
16	50-32-EF-5A-E1-FF	TP-LINK_5AE1FF	25dB	1	否	连接
17	EC-88-8F-97-37-E6	TP-LINK_9737E6	6dB	1	WPA/WPA2-PSK	连接

图 5-15 AP 列表

完成更改后，点击**保存**按钮，路由器会自动重启使当前的设置生效。

5.6.2 无线安全设置

点击**无线设置**→**无线安全设置**，可以在图 5-16 界面中设置无线网络安全选项。

图 5-16 无线网络安全设置

在无线网络安全设置页面，可以选择是否关闭无线安全功能。

- 如果您无需开启无线安全功能，请勾选**不启用无线安全**以关闭无线安全功能。如果关闭此功能，其他无线站点不需要任何认证就可以连接本地AP。
- 如果您要开启无线安全功能，则请选择页面中三种安全类型中的一种进行无线安全设置。

本页面提供了三种无线安全类型：**WPA/WPA2-个人版**、**WPA/WPA2-企业版**和**WEP**。不同的安全类型下，安全设置项不同，下面将详细介绍。

1. WPA/WPA2-个人版（推荐）

WPA/WPA2个人版是基于共享密钥的WPA模式，安全性很高，设置也比较简单，适合普通家庭用户和小型企业使用。

认证类型： **自动选择** - 根据主机请求自动选择使用WPA-个人版还是WPA2-个人版的安全模式。

WPA-个人版 - 使用WPA-个人版的安全模式。

WPA2-个人版 - 使用WPA2-个人版的安全模式。

- 加密算法:** 该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为自动，选择该项后，AP将根据实际需要自动选择TKIP或AES加密方式。
- PSK密码:** 该项是WPA-PSK/WPA2-PSK的初始设置密钥，设置时，要求为8-63个ASCII字符或8-64个十六进制字符。
- 组密钥更新周期:** 该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为30，若该值为0，则表示不进行更新。

 **注意:**

若设备进行了无线安全设置，则该无线网络内的所有主机都必须根据此处的安全设置进行相应的设置，如密码设置必须完全一样，否则将不能成功的通过无线连接到本设备。

2. WPA/WPA2-企业版

WPA/WPA2-企业版是一种比WEP强大的加密算法，选择这种安全类型，AP将采用Radius服务器进行身份认证并得到密钥的WPA或WPA2安全模式。由于要架设一台专用的认证服务器，代价比较昂贵且维护也很复杂，所以不推荐普通用户使用此安全类型。

- 认证模式:** 该项用来选择系统采用的安全模式，即自动、WPA、WPA2。
- **自动:** 若选择该项，AP会根据主机请求自动选择WPA或WPA2安全模式。
 - **WPA:** 若选择该项，AP将采用WPA的安全模式。
 - **WPA2:** 若选择该项，AP将采用WPA2的安全模式。
- 加密算法:** 该项用来选择对无线数据进行加密的安全算法，选项有Automatic、TKIP、AES。默认选项为Automatic，选择该项后，AP将根据实际需要自动选择TKIP或AES加密方式。
- Radius服务器IP:** Radius服务器用来对无线网络内的主机进行身份认证，此项用来设置该服务器的IP地址。
- Radius端口:** Radius服务器用来对无线网络内的主机进行身份认证，此项用来设置该Radius认证服务采用的端口号。
- Radius密码:** 该项用来设置访问Radius服务的密码。
- 组密钥更新周期:** 该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为30，若该值为0，则表示不进行更新。

3. WEP

WEP是Wired Equivalent Privacy的缩写，它是一种基本的加密方法，其安全性不如另外两种安全类型高。选择WEP安全类型，AP将使用802.11基本的WEP安全模式。

- 认证类型:** 该项用来选择系统采用的安全模式，包括自动、开放系统、共享密钥。
- **自动:** 若选择该项，AP会根据主机请求自动选择开放系统或共享密钥方式。
 - **开放系统:** 若选择该项，AP将采用开放系统方式。此时，无线网络内的主机可以在不提供认证密码的前提下，通过认证并关联上无线网络，但是若要进行数据传输，必须提供正确的密码。

- **共享密钥：**若选择该项，AP将采用共享密钥方式。此时，无线网络内的主机必须提供正确的密码才能通过认证，否则无法关联上无线网络，更无法进行数据传输。

密钥格式选择： 该项用来选择即将设置的密钥的形式，包括16进制、ASCII码。若采用16进制，则密钥字符只能为0-9，A、B、C、D、E、F；若采用ASCII码，则密钥字符可以是键盘上的任意字符。

密钥选择、WEP 密钥、密钥类型：

这三项用来选择密钥，设置具体的密钥值和选择密钥的类型，密钥的长度受密钥类型的影响。选择64位密钥需输入16进制字符10个，或者ASCII码字符5个。选择128位密钥需输入16进制字符26个，或者ASCII码字符13个。选择152位密钥需输入16进制字符32个，或者ASCII码字符16个。

- **WEP密钥：**在此输入WEP密钥，注意长度和有效字符范围。如果没有设置任何密钥，无线数据将不进行加密。
- **密钥类型：**可以选择使用64位、128位或152位的WEP密钥，选择“禁用”将不使用该密钥。

注意：

关于密钥选择中的4个密钥，可以只使用其一，也可以多个同时使用。无论哪种情况，客户端网卡上密钥的设置都必须与之一一对应。

5.6.3 无线MAC地址过滤

MAC 地址是网卡的物理地址，它就像是网卡的身份证，在网络中进行网卡的识别都是通过这个地址进行的。通常说的计算机的 MAC 地址也即计算机上网卡的 MAC 地址。

无线 MAC 地址过滤功能就是通过 MAC 地址来控制计算机能否接入无线网络，从而有效控制无线网络内用户的上网权限。

MAC 地址过滤功能通过 MAC 地址允许或拒绝无线网络中的计算机访问广域网，有效控制无线网络内用户的上网权限。利用按钮**添加新条目**来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则。

点击**无线设置**→**无线MAC地址过滤**，配置MAC地址过滤规则，来控制无线网络内用户的上网权限。如图 5-17。

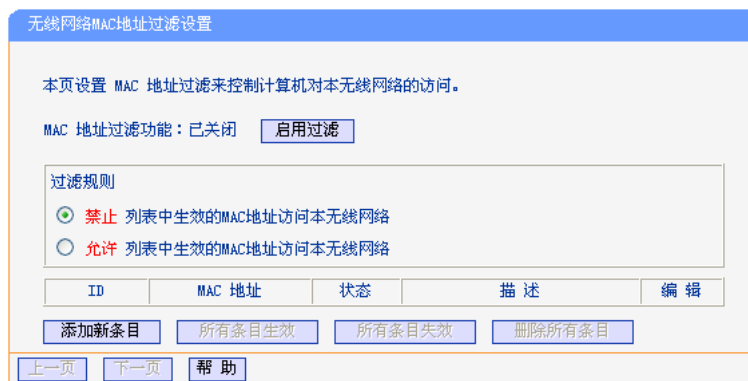


图 5-17 无线 MAC 地址过滤

启用过滤： 点击此按钮以开启无线网络的访问控制功能。

- 禁止：** 勾选以禁止列表中生效的 MAC 地址访问无线网络。
- 允许：** 勾选以允许列表中生效的 MAC 地址访问无线网络。
- MAC 地址：** 本设备需要进行访问控制的无线主机的 MAC 地址。
- 状态：** 此条条目的状态，生效或失效。
- 描述：** 对此个无线主机的简单描述。
- 编辑：** 对表中的条目进行编辑或者删除。
- 添加新条目：** 点击该按钮，可以添加新的过滤条目。
- 所有条目生效：** 点击该按钮，可以将列表中的所有条目的状态设置为“生效”。
- 所有条目失效：** 点击该按钮，可以将列表中的所有条目的状态设为“失效”。
- 删除所有条目：** 点击该按钮，可以删除该列表中的所有条目。

请按照以下步骤创建 MAC 地址过滤条目。

首先，您必须决定未知无线客户端是否可以接入本 AP 的无线网络。如果未知无线客户端可以接入，请在过滤规则里选择**禁止列表中生效的 MAC 地址访问无线网络**；如果不允许未知无线客户端接入，请选择**允许列表中生效的 MAC 地址访问无线网络**。

点击**添加新条目**按钮，添加MAC地址过滤规则条目。然后**无线网络MAC地址过滤设置**页面将会弹出，如图 5-18所示。

图 5-18 添加或修改无线 MAC 地址过滤条目

- MAC Address：** 填写需要进行访问限制的无线网络内的主机 MAC 地址。MAC 地址的格式为：XX-XX-XX-XX-XX-XX（X 是任意十六进制数字），如 00-0A-EB-B0-00-0B。
- 描述：** 为无线客户端添加简单的描述信息。如：无线主机 A。
- 状态：** 选择是否启用本条目。**生效**或者**失效**。

举例：如果您希望 MAC 地址为 00-0A-EB-00-07-BE 的主机 A 可以访问无线网络，其他位置主机不能访问无线网络。您可以按照以下步骤进行配置：

1. 点击**启用过滤**按钮。
2. 在**过滤规则**处选择**允许列表中生效的 MAC 地址访问无线网络**。
3. 确认列表中没有任何生效的条目，如果有，将该条目状态改为**失效**或删除该条目，也可以点击**删除所有条目**按钮，将列表中的条目清空。

4. 点击**添加新条目**按钮，在 **MAC 地址** 处填写 00-0A-EB-00-07-BE，在**描述**处填写无线主机 A，在**状态**处选择**生效**。设置完成后，点击**保存**按钮和**返回**按钮。

过滤规则表格显示如下：

ID	MAC 地址	状态	描述	编辑
1	00-0A-EB-00-07-BE	生效	无线主机A	编辑 删除

注意：

如果启用MAC地址过滤规则，并在**过滤规则**处选择**允许列表**中生效的MAC地址访问无线网络，而表中没有启用任何条目，这时没有任何无线客户端可以接入无线网络。

5.6.4 无线高级设置

选择**无线设置**→**无线高级设置**来设置本设备的部分高级功能，如图 5-19所示。由于各模式下本页面的配置项基本相同，下文中我们以AP客户端路由模式为例来说明。



图 5-19 无线高级设置

- 天线设置：** 设置天线的极化方向，可以设置为垂直天线，水平天线和外部天线三种。
- Beacon 时槽：** 表示设备发送 Beacon 帧的发包间隔，设备通过发送 Beacon 广播来进行无线网络连接的同步。可以设置为（40-1000）内的值，单位为毫秒（ms），默认值为 100。
- RTS 时槽：** 为数据包指定 RTS 阈值，当数据包长度超过 RTS 阈值时，路由器就会发送 RTS 到目的站点来进行协商，默认值为 2346。
- 分片阈值：** 为数据包指定分段阈值。当数据包的长度超过分段阈值时，会被自动分成多个数据包。过多的数据包将会造成网络性能降低，所以分段阈值不应设置过低，默认值为 2346。
- DTIM 阈值：** 该值在 1 至 255 之间，指定传输指示消息(DTIM, Delivery Traffic Indication Message) 的间隔，DTIM 是一种倒数计时作业，用以告知下一个要接收广播及多播的客户端窗口。当路由器已经为相关联的客户端缓存了广播或者多播信息时，它会在 Beacon 中夹带有下一个 DTIM 时槽的信息；当客户端听到 Beacon 讯号时，就会接收该广播和组播信息。DTIM 单位为 Beacon 时槽，默认值为 1，表示 DTIM 阈值与 Beacon 时槽相同。
- 开启WMM：** 开启WMM后路由器具有无线服务质量(QoS)功能，可以对音频、视频数据优先处理，保证音频、视频数据的优先传输。推荐勾选此项。

开启Short GI: 选择此项可以使路由器接收和发送短帧间隔数据包，提高路由器的传输速率，推荐勾选。

开启AP隔离: 打开AP隔离，选择此项可以隔离关联到AP的各个无线主机。如果开启AP隔离，那么关联到本路由器的无线客户端之间无法互相访问。

完成更改后，点击**保存**按钮。

注意:

如果您不熟悉本页面上的配置条目，请保持它们的默认配置不变，否则可能引起无线网络的工作性能下降。

5.6.5 天线对准

点击**无线设置**→**天线对准**，当您改变天线的方向时，可以在本页看到设备的信号强度变化。

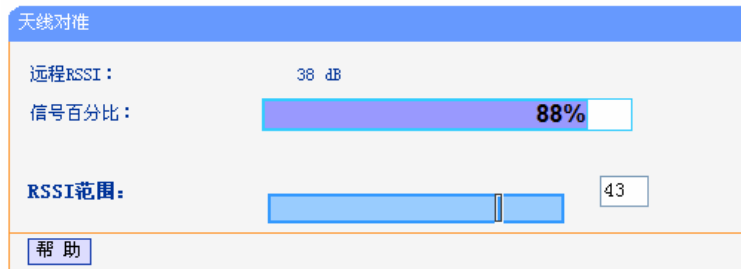


图 5-20 天线校准

远程RSSI: 显示设备的信号强度值。

信号百分比: 显示RSSI和RSSI 范围的比值，单位是百分比。

RSSI 范围: 您可以拖动滑块设置RSSI 范围值。如果RSSI 范围值减小，颜色变化对信号的波动将更敏感。滑块实际上是改变了指示器的最大值

注意:

只有**中继模式**、**桥接模式**、**客户端模式**和**AP 客户端路由模式**下，并与前端 AP 建立连接后，此功能才能生效。

5.6.6 无线距离设置

点击**无线设置**→**无线距离设置**，可以调整本设备的无线传输距离，它决定了户外无线网络连接的稳定性。输入无线传输距离，设备会自动调整数据包的 ACK 超时时间。

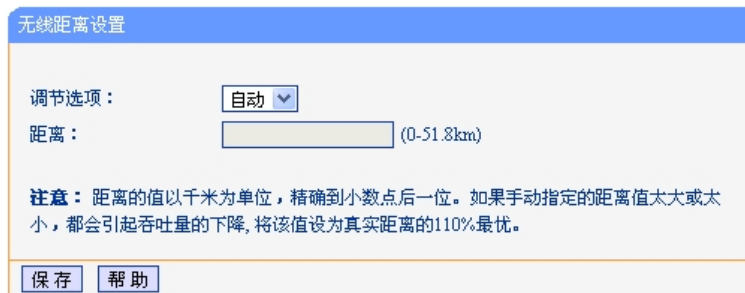


图 5-21 无线距离监测

调节选项: 如果设备在户外使用, 请保持默认设置。您也可以手动设置距离。如果设备在室内使用, 请使用室内模式。

距离: 输入无线传输距离, 精确到小数点后一位, 单位为千米。如果本距离太短或太长, 将会导致无线传输信号和传输性能低下。此处最好填写真实距离的110%。

点击**保存**使配置生效。

5.6.7 无线流量监测

点击**无线设置**→**无线流量监测**, 可以在图 5-22界面中开始或停止无线通信的流量监测。



图 5-22 无线流量监测

速率: 流量单位。

运行时间: 流量监控功能运行的时间。

发送速率: 无线发射速率信息。

接收速率: 无线接收速率信息。

点击**开始**按钮开始无线流量监测。

点击**停止**按钮结束无线流量监测。

5.6.8 无线主机状态

点击**无线设置**→**无线主机状态**, 查看当前连接到无线网络中的所有主机的基本信息。如图 5-23。

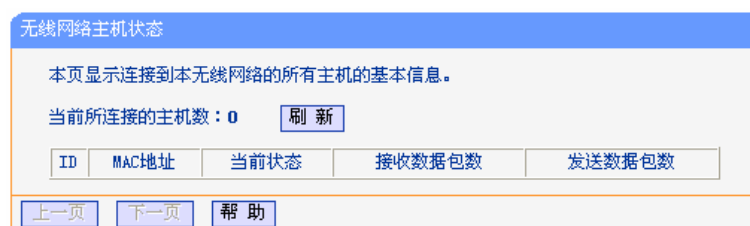


图 5-23 无线网络主机状态

MAC 地址： 显示当前已经连接到无线网络的主机的MAC地址。

当前状态： 此项显示当前主机的运行状态。

接收数据包数： 显示收到的数据包数目。

发送数据包数： 显示发送的数据包数目。

在本页无法进行任何修改，点击**刷新**按钮刷新当前无线连接状态。如果无线连接数目超过一页，点击**下一页**按钮，进入下一页；点击**上一页**按钮，返回上一页。

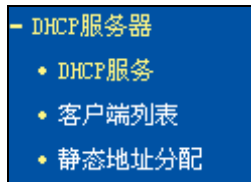
 **注意：**

本页数据会每隔5秒自动刷新。

5.7 DHCP服务器

DHCP 指动态主机控制协议（Dynamic Host Configuration Protocol）。本设备具有 DHCP 服务功能，能够为所有接入设备并且应用 DHCP 服务的网络设备自动分配 IP 参数。

DHCP 菜单下有 3 个子菜单：**DHCP 服务**，**客户端列表**和**静态地址分配**。



点击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.7.1 DHCP设置服务

点击**DHCP服务器**→**DHCP服务**，将看到DHCP服务界面，如图 5-25。开启DHCP服务器功能后，AP将会自动配置局域网中各主机的TCP/IP协议。


 该截图显示了DHCP服务的配置界面。标题为“DHCP服务”。

本路由器内建的DHCP服务器能自动配置局域网中各计算机的TCP/IP协议。

DHCP服务器： 不启用 启用

地址池开始地址：

地址池结束地址：

地址租期： 分钟（1~2880分钟，缺省为120分钟）

网关：（可选）

缺省域名：（可选）

主DNS服务器：（可选）

备用DNS服务器：（可选）

底部有“保存”和“帮助”按钮。

图 5-25 DHCP 服务

DHCP 服务器： 选择是否启用DHCP服务器功能，默认为不启用。

地址池开始/结束地址： 分别输入开始地址和结束地址。完成设置后，DHCP服务器分配给内网主机的IP地址将介于这两个地址之间。开始地址默认值为192.168.1.100，结束地址默认值为192.168.100.199。

- 地址租期：** 即DHCP服务器给内网主机分配的IP地址的有效使用时间。在该段时间内，服务器不会将该IP地址分配给其它主机。
- 网关：** 可选项。应填入AP的LAN口的IP地址，缺省为0.0.0.0。
- 缺省域名：** 可选项。应填入本地网域名，缺省为空。
- 主 DNS 服务器：** 可选项。可以填入 ISP 提供的 DNS 服务器或保持缺省，若不清楚可咨询 ISP。
- 备用DNS服务器：** 可选项。如果ISP提供给您了两个DNS服务器，则您可以把另一个DNS服务器的IP地址填于此处。

完成更改后，点击**保存按钮**并重启AP使设置生效。

注意：

为了使用本路由器的DHCP服务器功能，局域网中各计算机的TCP/IP协议必须设置为“自动获得IP地址”。此功能需要重启AP才能生效。

5.7.2 客户端列表

点击**DHCP服务器**→**客户端列表**，可以查看客户端主机的相关信息；点击**刷新按钮**可以更新表中信息，如图 5-26。

ID	客户端名	MAC 地址	IP 地址	有效时间
1	android-5eac29e0f0a3dc35	38-AA-3C-CA-DE-DF	192.168.1.101	01:59:55

刷新

图 5-26 DHCP 客户端列表

- 客户端名：** 显示获得IP地址的客户端计算机的名称。
- MAC地址：** 显示获得IP地址的客户端计算机的MAC地址。
- IP地址：** 显示DHCP服务器分配给客户端主机的IP地址。
- 有效时间：** 指客户端主机获得的IP地址距到期所剩的时间。每个IP地址都有一定的租用时间，客户端软件会在租期到期前自动续约。

5.7.3 静态地址分配

点击**DHCP服务器**→**静态地址分配**，本页可以为指定MAC地址的计算机预留IP地址。当该计算机请求DHCP服务器分配IP地址时，DHCP服务器将给它分配表中预留的IP地址。如图 5-27。

ID	MAC地址	IP地址	状态	编辑
1	00-13-8F-9C-24-65	192.168.1.24	生效	编辑 删除

添加新条目 **使所有条目生效** **使所有条目失效** **删除所有条目**

上一页 **下一页** **帮助**

图 5-27 静态地址分配

- MAC 地址：** 显示预留静态IP地址的计算机的MAC地址。

- IP地址：** 显示预留给内网主机的IP地址。
- 状态：** 显示该条目是否生效。只有状态为生效时，本条目的设置才生效。
- 编辑：** 修改或删除本条目。

添加预留 IP 地址：

1. 点击**添加新条目**按钮弹出如图 5-28的页面。
2. 输入 MAC 地址（MAC 地址默认格式为 XX-XX-XX-XX-XX-XX）和您需要预留的 IP 地址。
3. 状态设置为**生效**。
4. 点击**保存** 按钮，使配置生效。

图 5-28 添加或修改预留 IP 地址条目

修改预留 IP 地址：

1. 选择需要修改的条目，点击**编辑**按钮。如果您想要删除该条目，请点击**删除**按钮。
2. 点击**保存** 按钮使配置生效。

点击**删除所有条目**按钮，删除所有条目。

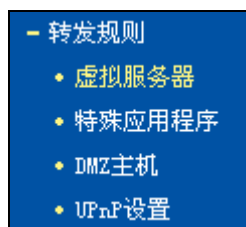
 **注意：**

所有配置将重启后生效。

5.8 转发规则

通过转发规则功能，远程用户可以访问局域网服务器的资源。在局域网用户运行某些特殊应用程序（如 Internet 网络游戏、视频会议、网络电话）时，还可以建立用户端与因特网服务器之间的连接。

选择菜单**转发规则**，可以看到：



点击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.8.1 虚拟服务器

通过将本路由器配置为虚拟服务器，可以使远程用户访问局域网内部的服务器，如 Web、FTP、邮件服务器等。

为保证局域网的安全，默认情况下，路由器会将局域网主机的 IP 地址隐藏起来，使因特网计算机无法主动与局域网计算机建立连接。因此，若要使因特网用户能够访问局域网内的服务器，需要设置虚拟服务器条目。

“虚拟服务器”定义了路由器的因特网服务端口与局域网服务器 IP 地址之间的对应关系。因特网所有对此端口的服务请求都会转发给通过 IP 地址指定的局域网服务器，这样既保证了因特网用户成功访问局域网中的服务器，又不影响局域网内部的网络安全。

选择菜单**转发规则**→**虚拟服务器**，可以在图 5-29 界面中设置虚拟服务器条目。



图 5-29 虚拟服务器

点击**添加新条目**按钮，可以在图 5-30 所示界面中设置新的虚拟服务器条目。

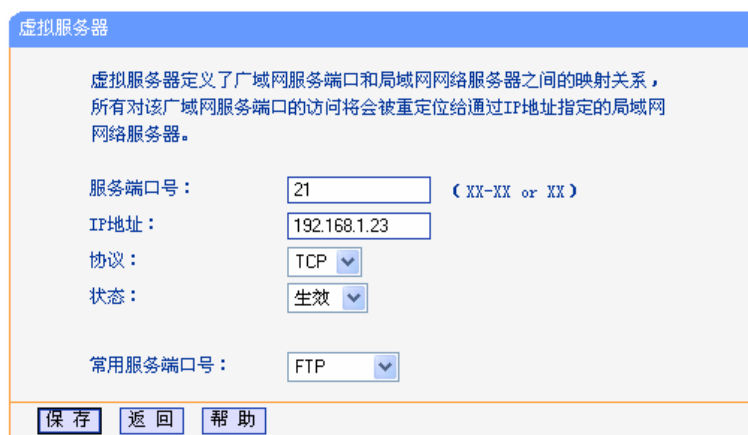


图 5-30 设置虚拟服务器条目

服务端口号： 设置路由器向因特网开放的服务端口。因特网用户通过向该端口发送请求来获取服务。可输入单个端口值或连续的端口段。端口段输入格式为“开始端口-结束端口”。

IP 地址： 输入局域网服务器的静态 IP 地址。通过此 IP 地址，路由器会将与服务端口的访问请求转到局域网服务器上。

协议： 选择此虚拟服务所采用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。

状态： 设置该条目是否生效。只有状态为生效时，本条目的设置才有效。

常用服务端口号：选择服务器提供的服务类型，系统会自动将该服务的服务端口号和协议添加到上述对应项中。对于“常用服务端口号”中没有列出的服务，则需要手动输入服务端口号和协议的相关信息。

举例：假如您有一些大型文件要共享给因特网的朋友，而由于文件太大，传输起来不方便，这时您可以将自己的计算机建成 FTP 服务器，然后利用本路由器的虚拟服务器功能使朋友可以访问您计算机中的这些文件。假设 FTP 服务器（即您的计算机）的静态 IP 地址为 192.168.1.23，希望朋友能够通过默认端口 21 访问此服务器，且采用 TCP 协议，那么，请按如下步骤进行设置：

1. 在图 5-29 所示的“虚拟服务器”页面点击**添加新条目**按钮。
2. 按图 5-30所示进行设置。其中的服务端口号和协议，可以手动输入，也可以通过在“常用服务端口号”中选择“FTP”，端口号“21”和协议“TCP”将自动填入到相应设置框中。
3. 点击**保存**按钮，可以看到设置完成后的虚拟服务列表如图 5-29所示。

当朋友访问此 FTP 服务器时，只需在浏览器中输入 ftp://xxx.xxx.xxx.xxx:21 即可。其中，“xxx.xxx.xxx.xxx”是本路由器的 WAN 口 IP 地址，如：当路由器 WAN 口 IP 为 172.32.90.1 时，需在浏览器中输入 ftp://172.32.90.1:21。

注意：

如果设置了服务端口为80的虚拟服务器，则需要将**防火墙设置→远端WEB管理**的“WEB管理端口”设置为80以外的值，如88，否则会跟路由器远程服务端口发生冲突，因特网用户对此端口的访问将默认为对路由器的访问，而不会转到局域网服务器上，从而导致虚拟服务器不起作用。

5.8.2 特殊应用程序

特殊应用程序功能，可以使某些需要多条连接的应用程序，如 Internet 网络游戏、视频会议、网络电话等能够与网络服务器建立正常连接。

对于此类特殊的应用程序，在客户端向因特网服务器主动发起连接的同时，也需要服务器向客户端发起连接。但在缺省情况下，因特网服务器向局域网客户端发起的连接请求都会被路由器拒绝，导致连接中断。

通过设置**特殊应用程序**，当局域网中有此类请求时，应用程序向触发端口发起连接，会触发路由器打开所有开放端口来为正常连接提供保证。

选择菜单**转发规则→特殊应用程序**，可以在图 5-31所示界面中查看和编辑特殊应用程序条目。



图 5-31 特殊应用程序

点击**添加新条目**按钮，可以在图 5-32所示界面中设置新的特殊应用程序条目。

图 5-32 设置特殊应用程序条目

- 触发端口：** 该端口是应用程序首先发起连接的端口，只有在该端口上发起连接，开放端口中的所有端口才可以开放。
- 触发协议：** 触发端口上使用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。
- 开放端口：** 当应用程序向触发端口上成功发起连接后，触发对应的开放端口，因特网服务器可通过开放端口与内网计算机连接。可输入单个端口值或端口段。端口段输入格式为“开始端口-结束端口”，不同的端口段用“,”隔开。
- 开放协议：** 开放端口上使用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。
- 状态：** 设置该条目是否生效。只有状态为生效时，本条目的设置才有效。
- 常用应用程序：** 选择需要设置的应用程序，系统会自动将该应用程序的触发端口号和开放端口号添加到上述对应项中。对于“常用应用程序”中没有列出的程序，需要手动输入触发端口和开放端口的相关信息。

5.8.3 DMZ主机

局域网中设置 DMZ (Demilitarized Zone, 非军事区) 主机后，该主机将完全暴露给广域网，可以实现双向无限制通信。

DMZ 主机实际上就是一个开放了所有端口的虚拟服务器，当需要设置的虚拟服务器的开放端口不确定时，可以把它设置成 DMZ 主机。

选择菜单**转发规则**→**DMZ主机**，可以在图 5-33 界面中设置 DMZ(非军事区)主机。

图 5-33 DMZ 主机

DMZ 状态: 选择是否启用 DMZ 主机功能。

DMZ 主机 IP 地址:

输入要设置为 DMZ 主机的局域网计算机的静态 IP 地址。

完成设置后，点击**保存**按钮。

5.8.4 UPnP设置

依靠UPnP(Universal Plug and Play)协议，局域网中的计算机可以请求路由器进行特定的端口转换，使得外部计算机能够在需要时访问内部计算机上的资源，例如，Windows XP和Windows ME系统上安装的MSN Messenger，在使用音频和视频通话时就可以利用UPnP协议，这样原本受限于NAT的功能便可以恢复正常使用。

选择菜单**转发规则**→**UPnP设置**，可以在图 5-34界面中查看UPnP信息。

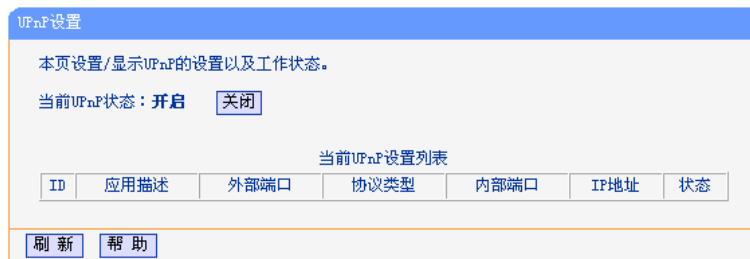


图 5-34 UPnP 设置

应用描述: 显示应用程序通过 UPnP 向路由器请求端口转换时给出的描述。

外部端口: 显示端口转换时使用的路由器端口号。

协议类型: 显示进行端口转换时采用的协议类型。

内部端口: 显示需要进行端口转换的局域网计算机端口号。

IP 地址: 显示需要进行端口转换的局域网计算机 IP 地址。

状态: 显示该条目是否已经启用。

使用时点击**开启**按钮即可，端口转换信息由应用程序发出请求时提供，无需进行任何设置。点击**刷新**按钮可以看到当前正在使用本功能的应用程序的端口转换相关信息。

注意:

1. 因为现阶段版本的UPnP协议的安全性还未得充分保证，不使用时请关闭UPnP功能。
2. 只有支持UPnP协议的应用程序才能使用本功能。
3. UPnP功能需要操作系统的支持(如Windows ME/ XP/ Vista)。

5.9 防火墙设置

选择菜单**防火墙设置**，您可以看到：

- 防火墙设置
 - 安全设置
 - 高级安全设置
 - 局域网WEB管理
 - 远端WEB管理

点击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.9.1 安全设置

选择菜单**防火墙设置**→**安全设置**，您可以在图 5-35界面中对以下安全功能的开启与关闭进行设置。

图 5-35 安全设置

- **状态检测防火墙(SPI):** SPI 防火墙当开启时拒绝所有来自外网的请求，只有是对内网请求回应的连接并符合已建立状态数据库的包才能通过防火墙进入内网。SPI 默认打开。如果您需要将内网中的所有主机暴露给外网，那么可将其关闭。
- **虚拟专用网络(VPN):** VPN 提供了通过广域网 (WAN) (例如，互联网) 在远程计算机间安全通信的方法。如果内网主机需要使用VPN协议(如PPTP、L2TP、IPSec)通过路由器连接到远程VPN 网络，那么应开启相应的 VPN 穿透功能。
- **应用层网关(ALG):** ALG 支持某些采用“控制/数据”模式的应用层协议(如 FTP、TFTP、H323 等)在通过 NAT 网关时作网络地址和端口的转换。推荐打开。

5.9.2 高级安全设置

选择菜单**防火墙设置**→**高级安全设置**，可以在下图 5-36界面中开启DoS(拒绝服务)攻击防范。完成更改后，点击**保存**按钮。

DoS攻击的目的是用极大量的虚拟信息流耗尽目标主机的资源。受害者被迫全力处理虚假信息流，从而影响对正常信息流的处理。如果DoS攻击始发于多个源地址，则称为分布式拒绝服务(DDoS)攻击。通常DoS与DDoS攻击中的源地址都是欺骗性的。开启DoS攻击防范后，若某主机向目标主机发送某种数据包的速率大于设定值，那么该主机将被列入“DoS被禁主机列表”而不能上网，从而很好地防止了DoS攻击。

图 5-36 高级安全设置

- 数据包统计时间间隔:** 设置对数据包进行统计的时间间隔。如果统计得到发往同一目标IP地址的某种数据包(例如UDP FLOOD)达到了指定的阈值，那么系统将认为UDP-FLOOD攻击已经发生。如果UDP-FLOOD过滤已经开启，那么路由器将会停止接收该类型的数据包，从而达到防范攻击的目的。此处的值和系统工具→流量统计中的“数据包统计时间间隔”是一样的，一处的更改将引起另一处作同样的更改。
- DoS攻击防范:** 该项是开启下面各种攻击防范的总开关，只有选择此项后，以下的几种防范措施才能生效。
- 开启ICMP-FLOOD攻击过滤:** 若需要防范ICMP-FLOOD攻击，请选择此项。
- ICMP-FLOOD数据包阈值:** 当开启ICMP-FLOOD功能后，如果在指定时间间隔内发往同一目标IP地址的ICMP包达到了设定值，防范措施将立即启动。
- 开启UDP-FLOOD攻击过滤:** 若需要防范UDP-FLOOD，请选择此项。
- UDP-FLOOD数据包阈值:** 当开启UDP-FLOOD功能后，如果在指定时间间隔内发往同一目标IP地址的UDP包达到了设定值，防范措施则立即启动。
- 开启TCP-SYN-FLOOD攻击过滤:** 若需要防范TCP-SYN-FLOOD，请选择此项。

TCP-SYN-FLOOD数据包阈值:

当开启TCP-SYN-FLOOD功能后，如果在指定时间间隔内发往同一目标IP地址的TCP的SYN包达到了设定值，防范措施则立即启动。

忽略来自WAN口的Ping: 若开启该功能，广域网的计算机将不能Ping通路由器。

禁止来自LAN口的Ping包通过路由器:

若开启该功能，局域网的计算机将不能Ping通广域网中的计算机。

DoS被禁主机列表:

点击该按钮，可以查看被禁止的计算机列表，如图5-37。点击**刷新**按钮可以更新列表信息。若希望被禁计算机能够重新上网，可以点击**删除**按钮；若需要释放所有被禁计算机，可以点击**清空**按钮。

Index	主机IP地址	主机MAC地址	修改	删除
1	192.168.1.101	00-13-8F-AA-6D-77		

图 5-37 DoS 被禁主机列表

完成更改后，点击**保存**按钮。

注意:

只有在开启了**系统工具**→**流量统计**中的流量统计功能后，DoS 攻击防范才能正常生效。

5.9.3 局域网WEB管理

选择菜单**防火墙设置**→**局域网WEB管理**，您可以在图 5-38界面中管理局域网内计算机对本WEB页面的访问权限。完成更改后，点击**保存**按钮。

为了更好地对局域网中的计算机进行控制，您可以通过局域网 WEB 管理功能来限制局域网中计算机对本 WEB 管理页面的访问。

本路由器默认允许局域网中的所有计算机登陆路由器执行 WEB 管理，如果您选择“仅允许列表中的 MAC 地址访问本 WEB 管理页面”，并在列表中添加可以执行 WEB 管理的计算机的 MAC 地址，那么仅有在列表中的计算机才能访问路由器的 WEB 管理页面，而局域网中的其他计算机将被拒绝访问本路由器。

点击**添加**按钮即可把当前管理 PC 的 MAC 地址复制到列表中。

图 5-38 局域网 WEB 管理

5.9.4 远端WEB管理

远端 WEB 管理功能允许用户通过 Web 浏览器（如 Internet Explorer 等）从广域网登录此管理页面配置管理路由器。

选择菜单**防火墙设置**→**远端WEB管理**。远端WEB管理功能可以允许用户通过WEB浏览器从广域网配置路由器。可以在下图 5-39界面中设置管理IP地址和端口。

图 5-39 远端 WEB 管理

WEB 管理端口： 用于访问宽带路由器的 WEB 管理端口号。

远端 WEB 管理 IP 地址： 广域网中可以访问该路由器执行远端 WEB 管理的计算机 IP 地址。

完成更改后，点击**保存**按钮。

注意：

1. 路由器默认的WEB管理端口为80，如果改变了默认的WEB管理端口（例如改为8080，推荐修改为1024以后的端口，以免与知名端口冲突），则必须用“IP地址:端口”的方式登录路由器WEB管理界面，例如http://192.168.1.254:8080。此功能需要重启路由器才能生效。
2. 路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理，如果改变了默认的远端WEB管理IP地址（例如改为202.96.12.8），则广域网中只有具有指定IP地址（例如202.96.12.8）的计算机才能登录路由器执行远端WEB管理。如果将远端WEB管理IP地址设为255.255.255.255，那么，广域网中所有的计算机都可以登录路由器执行远端WEB管理。

举例：如果希望广域网中IP地址为202.96.134.13的计算机能够访问宽带路由器，执行远端WEB管理功能，WEB管理端口为80。则可以进行如下设置：

1. 设置WEB管理端口为“80”。
2. 设置远端WEB管理IP地址为“255.255.255.255”或“202.96.134.13”。

这样，该计算机访问路由器管理界面时应该输入路由器WAN口IP地址即可。

5.10 家长控制

通过**家长控制**功能，可以对小孩的上网时间和访问的网站进行控制。

家长控制功能可以选择局域网中的一台PC（Personal Computer，即个人电脑）作为家长PC，家长PC可以不受限制地正常上网，而其他所有PC只能根据控制列表中的规则在指定的时间访问指定的网站。若某台非家长PC不在控制列表中，则此PC将无法上网。

家长控制只能使局域网中的一台PC不受控制，而且受控PC能够访问的网站数量很有限。若想放宽受控条件，如使更多的PC不受控制或使受控PC能访问更多的网站，那么请参阅[5.11 访问控制](#)部分。

选择菜单**家长控制**，可以在图 5-40界面中设置家长控制条目。

图 5-40 家长控制设置

家长控制： 选择是否开启家长控制功能。开启此功能后，只有家长PC可以正常上网，其他PC均会受到控制。

家长PC的MAC地址：

设定家长PC，即不受控制的PC的MAC地址。

当前管理PC的MAC地址：

此处显示当前正在操作的PC的MAC地址，点击其后的**设为家长PC**按钮可以把此MAC地址复制到“家长PC的MAC地址”一栏中。

完成更改后，点击**保存**按钮使设置生效。

点击**增加单个条目**按钮，可以在图5-41界面中设置家长控制条目。

图 5-41 家长控制规则设置

小孩 PC 的 MAC 地址:

受控制的 PC 的 MAC 地址，为空则表示对局域网中所有的非家长 PC 应用此控制规则。

当前局域网中 PC 的 MAC 地址:

此处列出了当前局域网中所有 PC 的 MAC 地址及其对应的 IP 地址，可通过 IP 地址选择要控制的一台 PC，选择后该 PC 对应的 MAC 地址会自动复制到“小孩 PC 的 MAC 地址”一栏中。

给允许的网站列表一个描述:

为方便识别，请在此处输入对允许小孩访问的网站列表的一个简单描述，不同控制条目的描述不能相同。

允许小孩访问的网站域名:

可以填写 8 个允许的网站完整域名或域名的关键字，如果在此处填入某一个字符串（例如：yahoo），则含有该字符串的域名（www.yahoo.com、www.yahoo.com.cn）都可以被匹配。

希望在哪些时候生效:

允许小孩访问以上网站的时间段。如果已经在**访问控制**→**日程计划**中设置好了时间，请直接在下拉列表中选择，否则请先保存设置，然后点击**日程计划**进入日程

计划设置对话框进行设置。有关日程计划的设置请参阅本文档[5.11.4 日程计划](#)部分。

状态： 以上设置是否生效。

完成更改后，点击**保存**按钮。

举例：假如家长PC的MAC地址为00-19-66-80-54-37，小孩PC的MAC地址为00-19-66-80-53-CF，为了不影响学习，希望小孩只能在周六全天及周日上午的8：00—11：30访问雅虎（www.yahoo.com.cn）及谷歌网站（www.google.com.cn），而家长自己不受任何控制，那么请按以下步骤进行设置：

1. 在“家长控制”中启用家长控制功能；若“当前管理PC的MAC地址”为00-19-66-80-54-37，则点击**设为家长PC**按钮，否则手动填入家长PC的MAC地址“00-19-66-80-54-37”。
2. 在**访问控制**→**日程计划**中添加两条新的日程计划，分为命名为“周六全天”、“周日上午”，时间分别设置为“星期六、全天—24小时”、“星期天、开始时间：0800、结束时间：1130”。设置保存后的结果如图5-42所示。



图 5-42 日程计划设置示例

3. 返回“家长控制设置”界面，点击**增加单个条目**按钮，按图5-41所示进行设置。
4. 保存设置。重复第3步，并将第3步中的“给允许的网站列表一个描述”改为“雅虎&谷歌_2”、“希望在哪些时候生效”改为“周日上午”，点击**保存**按钮。

完成以上设置之后，看到的规则列表将是：

ID	MAC 地址	网站列表	日程计划	状态	配置
1	00-19-66-80-53-CF	雅虎&谷歌_1	周六全天	生效	编辑 删除
2	00-19-66-80-53-CF	雅虎&谷歌_2	周日上午	生效	编辑 删除

5.11 访问控制

通过访问控制功能，可以控制局域网内主机的上网行为，使其上网时间和访问的网站受到一定规则的限制，如控制某台主机只能在某个时段登录某些网站，或在某个时间段不能登录这些网站等。

与**家长控制**相比，**访问控制**功能显得更灵活。**访问控制**可以通过一台主机控制一台或几台局域网内的其他主机。如果家中有孩子，访问控制和家长控制功能都可以有效的控制孩子的上网范围和上网时间，使孩子能够更健康的使用互联网。但访问控制的应用较为广泛，如果您家有三台电脑，那么**访问控制**功能可以在控制孩子使用电脑的同时对另一台电脑不作控制。

选择菜单**访问控制**，可以看到：

- 访问控制

- 控制规则
- 主机列表
- 访问目标
- 日程计划

点击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.11.1 控制规则

通过规则管理，可以设置和管理局域网内主机上网的规则，允许或禁止“主机列表”中的主机在“日程计划”时间段内访问“访问目标”网站。

选择菜单**访问控制**→**控制规则**，可以在下图5-43所示面中设置对内网主机上网行为的控制规则。

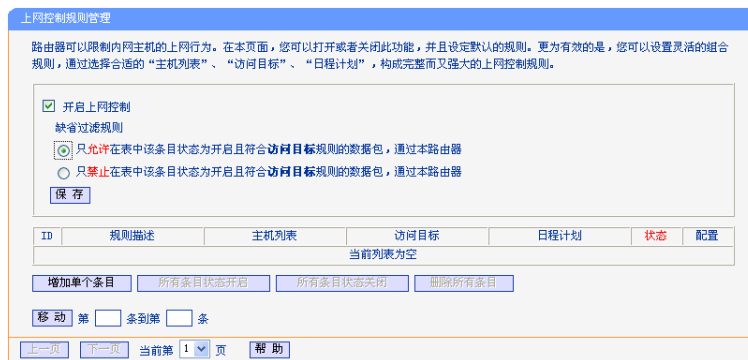


图 5-43 访问控制规则管理

开启上网控制：选中则开启访问控制功能，若不选中则规则无效。

缺省过滤规则：只允许在表中该条目状态为开启且符合访问目标规则的数据包，通过本路由器--选择此项，则凡是和已设置状态开启的访问控制规则相符的数据包，均可以通过本路由器。

只允许在表中该条目状态为开启且符合访问目标规则的数据包，通过本路由器--选择此项，则凡是和已设置状态开启的访问控制规则相符的数据包，均不能通过本路由器。

移动：通过该按钮来调整各条控制规则的顺序，以达到不同的控制优先级(ID序号越靠前则优先级越高)。

完成更改后，点击**保存**按钮。

点击**增加单个条目**按钮，可以在下图5-44界面中设置新的访问控制条目。

图 5-44 访问控制规则设置

规则描述: 对该访问控制条目的简单描述，此描述必须是唯一的，如“周末 8:00-12:00”，用于标识设置的上网规则。

主机列表: 此条目为要控制的内网主机。如果已在**访问控制**→**主机列表**中设置好了要控制的主机的信息，请直接在下拉列表中选择，否则请点击[点击此处添加主机列表](#)进入主机列表设置对话框进行设置。有关主机列表的设置请参阅本文档[5.11.2 主机列表](#)部分。

访问目标: 允许或禁止“主机列表”中的主机访问的网站域名或IP地址。如果已在**访问控制**→**访问目标**中设置好了访问目标信息，请直接在下拉列表中选择，否则请点击[点击此处添加访问目标](#)进入访问目标设置对话框进行设置。有关访问目标的设置请参阅本文档[5.11.3 访问目标](#)部分。

日程计划: 允许或禁止“主机列表”中的主机访问目标网站的时间段。如果已在**访问控制**→**日程计划**中设置好了时间，请直接在下拉列表中选择，否则请点击[点击此处添加日程计划](#)进入日程计划设置对话框进行设置。有关日程计划的设置请参阅本文档[5.11.4 日程计划](#)部分。

生效: 该访问控制条目是否生效。

完成更改后，点击**保存**按钮。

举例: 周一到周五为小明学习的时间，在此期间有必要禁止他的电脑上网。因此，需要限制局域网中IP地址为192.168.1.88的计算机（该计算机的主人为小明）只能在周末上网，而局域网中的其它主机（假设IP地址为192.168.1.89—192.168.1.91）不受任何控制，请按照以下步骤进行设置：

1. 在**主机列表**中添加两个条目，其一：主机名为“小明的计算机”，IP地址为192.168.1.88；其二：主机名为“其他计算机”，IP地址为192.168.1.89—192.168.1.91。
2. 在**日程计划**设置中，输入日程描述“周末全天”，勾选“星期六”、“星期天”和“全天-24小时”，如图 5-45，点击**保存**完成设置。

图 5-45 日程计划设置

- 回到图5-43所示的“访问控制规则管理”界面，启用访问控制功能，选择缺省过滤规则为“凡是符合已生效访问控制规则的数据包，允许通过本路由器”，点击**保存**按钮。
- 点击**增加单个条目**按钮，按下图进行设置并保存。

图 5-46 访问控制规则设置示例一

- 再次在图5-43所示界面中点击**增加单个条目**按钮，按图5-47所示进行设置并保存。

图 5-47 访问控制规则设置示例二

完成以上设置之后，规则列表将是：

ID	规则描述	主机列表	访问目标	日程计划	生效	配置
1	允许小明周末上网	小明的计算机	任意	周末全天	<input checked="" type="checkbox"/>	编辑 删除
2	允许其他主机上网	其他计算机	任意	永久	<input checked="" type="checkbox"/>	编辑 删除

图 5-48 规则列表

5.11.2 主机列表

主机列表列举了需要遵守访问控制规则的主机信息，包括主机名，主机信息等。在主机列表设置中，可以增加，编辑和删除相应的主机列表。

选择菜单**访问控制**→**主机列表**，如图5-49，可以在设置受控的内网主机列表。



图 5-49 主机列表设置

点击**增加单个条目**按钮，可以在下图 5-50界面中设置新的受上网规则控制的主机信息。

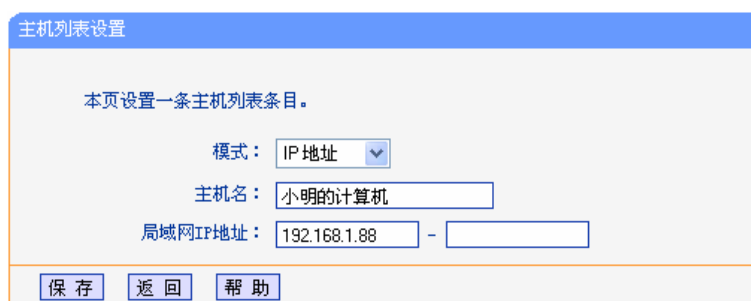


图 5-50 主机列表设置示例

模式: 选择标识受控主机身份的模式，有IP地址和MAC地址两个选项。

主机名: 给受控主机的一个简单描述，不同主机列表条目中的主机名不能相同。

局域网IP地址/MAC地址:

如果选择的模式为IP地址，请在此输入一台受控主机的IP地址或IP地址连续的多台受控主机的首尾IP地址。如果选择的模式为MAC地址，请在此输入受控主机的MAC地址。

完成更改后，点击**保存**按钮。此时图 5-49所示界面的列表中将显示刚刚设置的主机条目的信息。点击**删除所有条目**按钮，可以一次性删除列表中的所有条目。删除所有条目后，则原先设置的访问控制规则对相应主机失效。

5.11.3 访问目标

访问目标显示了主机上网访问的目标网站或目标 IP 地址，如“www.baidu.com”，“192.168.1.71”等。

选择菜单**访问控制**→**访问目标**，可以在图5-51界面中设置允许或禁止受控主机访问的目标信息。



图 5-51 访问目标设置

点击**增加单个条目**按钮，可以在图 5-52 界面中设置新的访问目标的信息。

图 5-52 访问目标列表设置—IP 地址模式

模式：选择描述访问目标信息的模式，有IP地址和网站域名两个选项。如果选择了网站域名模式，设置页面将如图5-53所示。

目标描述：给访问目标的一个简单描述，此描述必须是唯一的。

目标IP地址：输入一个访问目标的IP地址或连续的访问目标IP地址段。

目标端口：允许或限制访问的目标IP地址的服务端口，可以为一个端口号或连续的端口段。如果不清楚目标端口号，可以在“常用服务端口号”的下拉列表中通过选择服务来自动填入。

协议：访问目标的服务器所使用的协议。如果不清楚采用的协议，推荐选择ALL。

常用服务端口号：下拉列表中列举了一些常用的服务端口，从中选择需要的服务，则该服务对应的端口号会自动填入上面的“目标端口”输入框中。

图 5-53 访问目标列表设置—网站域名模式

网站域名：在域名模式下，可以为列表设置4个网站完整域名或域名的关键字，如果在此处填入某一个字符串（例如：**yahoo**），则含有该字符串的域名（**www.yahoo.com**、**www.yahoo.com.cn**）都可以被匹配。

完成更改后，点击**保存**按钮。

5.11.4 日程计划

在“日程计划”中，可以设置上网规则生效的时间。此处的时间包括日期和时间段。日期可以为一个星期的某几天，也可以为每天。时间段可以设为某两个时间点间的时间段，也可以为“全天 24 小时”。

选择菜单访问控制→日程计划，可以在图5-54界面中设置允许或禁止受控主机上网的时间段。

☞ 注意:

在设置之前，请确保路由器的时间是正确的，有关路由器的时间设置请参阅本文档 [5.16.1 时间设置部分](#)。



图 5-54 日程计划设置

点击**增加单个条目**按钮，可以在下图 5-55界面中设置新的日程计划。

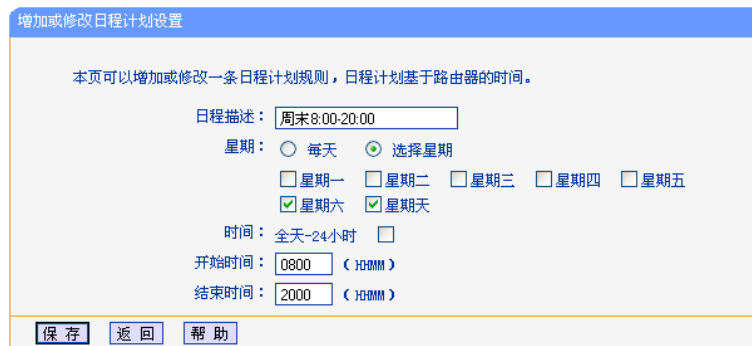


图 5-55 日程计划设置示例

日程描述: 给日程计划的简单描述，此描述必须是唯一的，例如“周末8：00-20：00”。

星期: 点选“每天”，可以将时间设置为每天，点选“选择星期”，则可将时间设置为每个星期的某几天。

时间: 如果要设置为全天，请直接选择“全天-24小时”，否则请在开始时间、结束时间中输入具体时间，注意时间格式为HHMM，即前两位为小时，后两位为分钟。

完成更改后，点击**保存**按钮。

5.12 路由功能

静态路由是一种特殊的路由，由网络管理员手动配置。在网络中使用合适的静态路由可以减少路由选路造成的网络开销，提高数据包的转发速度。

静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

通过设定目的 IP 地址、子网掩码和网关地址可以确定一个路由条目。其中目的 IP 地址和子网掩码用来确定一个目标网络/计算机，然后路由器会将数据包发往相应静态路由条目的网关，并由该网关转发数据包。

☞ 注意:

当路由器周围的网络环境较复杂，或者没有完全了解周围网络的拓扑结构时，请慎用此功能。

5.12.1 静态路由表

选择菜单路由功能→静态路由表，可以在下图 5-56 的界面中设置静态路由信息。



图 5-56 静态路由表

点击添加新条目按钮，可以在下图中添加静态路由条目。如图 5-57。

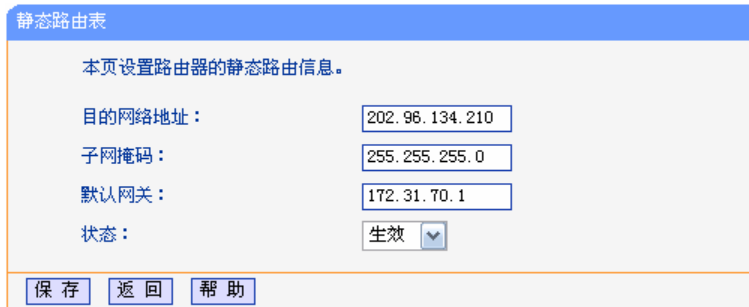


图 5-57 添加静态路由条目

目的 IP 地址： 用来标识希望访问的目标地址或目标网络，此 IP 地址不能和路由器的 WAN 口或 LAN 口 IP 地址处于同一网段。

子网掩码： 该项与目的 IP 地址一起来标识目标网络。

默认网关： 数据包被指定发往的下一个节点的 IP 地址，此 IP 地址必须和路由器的 WAN 口或 LAN 口 IP 地址处于同一网段。

状态： 显示该条目是否生效。只有状态为生效时，此路由条目才起作用。

5.12.2 系统路由表

系统路由表显示了所有正在使用的路由表条目，每条路由表条目由目的 IP 地址，子网掩码，网关和网络接口组成。点击刷新按钮可以刷新路由表，如图 5-58。

ID	目的网络地址	子网掩码	网关	接口
1	10.0.0.0	255.255.255.0	0.0.0.0	WAN
2	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
3	0.0.0.0	0.0.0.0	10.0.0.101	WAN

刷新 帮助

图 5-58 系统路由表

目的网络地址： 静态路由条目所指定的目的主机或网络的网络地址。

子网掩码： 子网掩码决定了目的 IP 地址的网络号和主机号。

网关： 连接路由器和目的主机或网络的网关设备的网络地址。

网络接口： 网络接口显示目的 IP 地址位于 LAN 与 WLAN(内部有线和无线网络)，或者 WAN(外部网络)。

5.13 IP带宽控制

带宽控制功能可以实现对局域网计算机上网带宽的控制。在带宽资源不足的情况下，通过对各类数据包的带宽进行控制，可以实现带宽的合理分配，达到有效利用现有带宽的目的。通过 IP 带宽控制功能，可以设置局域网内计算机的带宽上下限，保证每台计算机都能通畅地共享网络，并在网络空闲时充分利用网络带宽。

选择菜单 **IP 带宽控制**，可以看到：



点击菜单中的子项即可进行具体的设置，下面将详细讲解各子项的功能和设置方法。

5.13.1 控制设置

带宽设置分为“上行总带宽”和“下行总带宽”。上行总带宽是指所有内网计算机同时上传数据时占用的总带宽，由 ISP 提供的大小决定。下行总带宽则指所有内网计算机同时下载数据时占用的总带宽。通常 ISP 提供的带宽指的是“下行总带宽”，如“1M”等。通过**控制设置**，可以对上行、下行总带宽分别进行设置。

选择**IP带宽控制**→**控制设置**，可以进入下图 5-59所示界面。

IP带宽控制设置

本页对IP带宽控制的开启与关闭进行设置。只有IP带宽控制的总开关是开启的时候，后续的“IP带宽控制规则”才能够生效，反之，则失效。

注意：1、带宽的换算关系为：1Mbps = 1024Kbps；
2、选择宽带线路类型及填写带宽大小时，请根据实际情况进行选择 and 填写，如不清楚，请咨询您的带宽提供商（如电信、网通等）；
3、修改下面的配置项后，请点击“保存”按钮，使配置项生效。

开启IP带宽控制

请选择您的宽带线路类型： ADSL线路 其它线路

上行总带宽： Kbps

下行总带宽： Kbps

图 5-59 IP 带宽控制设置

- **开启 IP 带宽控制：** 选择是否开启 QoS 功能，只有此处开启时，后续的“QoS 规则”设置才能够生效。
- **带宽线路类型：** 选择申请的带宽线路类型，此处仅区分 ADSL 线路和其它线路。
- **上行总带宽：** 输入希望路由器通过 WAN 口提供的上传速率，最大值为 100000Kbps。
- **下行总带宽：** 输入希望路由器通过 WAN 口提供的下载速率，最大值为 100000Kbps。

👉 注意：

为了使IP带宽控制达到最佳效果，请正确设置线路类型，并向ISP了解线路的上行/下行总带宽。

5.13.2 控制规则

在控制规则中，可以设置局域网计算机的上下行带宽参数，满足局域网中每台主机的上网需求。选择**IP带宽控制**→**控制规则**，进入下图 5-60所示界面。控制规则分为控制规则列表和控制规则配置。

ID	描述	上行带宽 (Kbps)		下行带宽 (Kbps)		启用	配置
		最小	最大	最小	最大		
1	192.168.1.10 - 192.168.1.250/80 - 85/TCP	400	1000	400	1000	<input checked="" type="checkbox"/>	编辑 删除

图 5-60 IP 带宽控制规则列表

- **下行总带宽：**输入希望路由器通过 WAN 口提供的下载速率，最大值为 100000Kbps。
- **ID：**规则序号。
- **描述：**显示描述的信息，包括地址段，传输层的端口段和协议。
- **上行带宽：**表示主机发送数据时占用的带宽，此处显示 WAN 口允许的最大上传速度限制和最小上传速度保证，为 0 时表示采用缺省值。输入范围为 0-100000Kbps。
- **下行带宽：**表示主机接受数据时占用的带宽，此处显示 WAN 口允许的最大下载速度限制和最小下载速度保证，为 0 时表示采用缺省值。输入范围为 0-100000 Kbps。
- **启用：**显示规则的状态，选中该复选框则表示该规则生效。
- **配置：**对相应的规则进行编辑或删除。

当点击控制规则列表中的**添加新条目**或**编辑**按钮时，将进入图5-61设置界面。在控制规则配置中，可以创建新的IP带宽控制规则或修改已存在的规则，配置结果将在图5-60中显示。

图 5-61 带宽控制规则配置

- **启用：**选择是否启用该规则。
- **IP 地址段：**输入内部主机的地址范围。当全部为空或为 0.0.0.0 时表示该域无效。
- **端口段：**通过设置端口段，可以限制主机访问网络的端口范围。一般浏览网页的端口为“80”，而登录 QQ 的端口则为 1500 左右。可以在此输入内部主机访问外部服务器的端口范围，当全部为空或为 0 时表示该域无效。普通用户可以不用设置“端口段”。

- **协议：**输入传输层采用的协议类型，这里有 ALL(任意匹配)、TCP 和 UDP；该域只有在端口段选中下才有效。
- **上行带宽、下行带宽：**上行带宽表示主机发送数据时占用的带宽，下行带宽则表示主机接受数据时占用的带宽。通常，上行带宽远远小于下行带宽，下行带宽的设置则需参考总带宽和主机数量，以及内网计算机的上网需求。

5.14 IP与MAC绑定

选择菜单 **IP 与 MAC 绑定**，可以看到：



点击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.14.1 静态ARP绑定设置

静态 ARP 绑定，即 IP 与 MAC 绑定，是防止 ARP 攻击本路由器的有效方法。

路由器在局域网内传输 IP 数据包时是靠 MAC 地址来识别目标的，因此 IP 地址与 MAC 地址必须一一对应，这些对应关系靠 ARP 映射表来维护。ARP 攻击可以用伪造的信息更新路由器的 ARP 映射表，破坏表中 IP 地址与 MAC 地址的对应关系，使路由器无法与相应的主机进行通信。

静态 ARP 绑定将主机的 IP 地址与相应的 MAC 地址进行绑定，可以有效防止 ARP 列表被错误的 IP MAC 对应信息更替。

选择菜单 **IP 与 MAC 绑定**→**静态 ARP 绑定设置**，可以在下图界面中设置静态 ARP 绑定条目。

图 5-62 静态 ARP 绑定设置

ARP 绑定： 该项用来开启 ARP 绑定功能，只有选择“启用”时，列表中的设置才能生效。

MAC 地址： 该项显示被绑定计算机的 MAC 地址。

IP 地址： 该项显示被绑定计算机的 IP 地址。

绑定： 该项显示条目状态，只有选中该项，该条绑定条目才能生效。

举例： 如果希望将某台计算机的IP地址和MAC地址进行绑定，其IP地址为192.168.1.100，MAC地址为90-2B-34-63-59-68，请按照如下步骤设置：

1. 在图 5-62界面中点击**增加单个条目**。

2. 在下图 5-63中按照下图界面设置MAC地址和IP地址。

图 5-63 添加静态 ARP 绑定条目

3. 设置完成后，选中“绑定”，并点击**保存**按钮。

5.14.2 ARP映射表

如前所述，IP 数据包在局域网内传输时是靠 MAC 地址来识别目标的，IP 地址与 MAC 地址必须一一对应，ARP 映射表用来存储与维护 IP/MAC 对应信息。

选择菜单**IP与MAC绑定**→**ARP映射表**，可以在图 5-64界面中查看ARP绑定条目信息。

ID	MAC地址	IP地址	状态	配置
1	00-25-22-4A-91-85	192.168.1.122	已绑定	导入 删除

图 5-64 ARP 映射表

导入： 该项用来将指定映射条目添加到静态 ARP 列表中。

全部导入： 该项用来将 ARP 映射列表中的所有条目添加到静态 ARP 列表中。

全部绑定： 将当前 ARP 映射列表中所有条目的状态设置为绑定，注意该按钮只有在启用了 ARP 绑定功能后才能点击。

刷新： 点击该按钮，可以更新 ARP 映射列表中的条目信息。

注意：

1. 在进行导入操作时，如果该条目与ARP静态绑定表中的某条目冲突，则会显示冲突提示，不会添加该条目；
2. 在进行全部导入操作时，如果同样存在冲突条目，则系统会忽略冲突条目，将其它没有冲突的条目添加到ARP静态绑定列表中。

5.15 动态DNS

选择菜单**动态 DNS**，可以看到：



点击**动态 DNS**，可以进行相应的功能设置，下面将详细讲解动态 DNS 的功能。

动态DNS又名DDNS，它的主要功能是实现固定域名到动态IP地址之间的解析。对于使用动态IP地址的用户，在每次上网得到新的IP地址后，安装在计算机上的动态域名软件就会将该IP地址发送到由DDNS服务商提供的动态域名解析服务器，并更新域名解析数据库。当Internet上的其他用户需要访问这个域名的时候，动态域名解析服务器就会返回正确的IP地址。这样，大多数不使用固定IP地址的用户，也可以通过动态域名解析服务经济、高效地构建自身的网络系统。

选择服务提供者“花生壳(www.oray.net)”，可以在下图 5-65界面中设置DDNS。在注册成功后，可以用注册的用户名和密码登录到DDNS服务器上。当连接状态显示成功之后（如图 5-66），互联网上的其它计算机就可以通过域名的方式访问路由器或虚拟服务器了。

图 5-65 花生壳 DDNS 设置

图 5-66 连接成功

- 服务商链接：** 如果未在 DDNS 上注册，请选择该选项进行注册。
- 服务提供者：** 该项是提供 DDNS 的服务器。请根据需要选择所需的服务类型。
- 用户名、密码：** 请正确填写在 DDNS 上注册的用户名和密码。
- 启用 DDNS：** 该项用来启用花生壳 DDNS 服务。
- 登录/退出：** 点击该按钮，可以登录/退出 DDNS 服务。

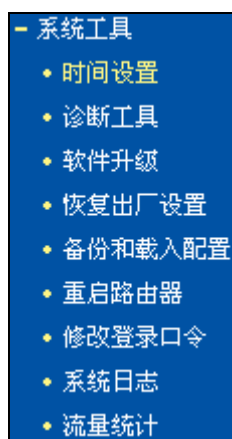
图 5-66为注册成功后，用注册的Oray护照和密码登录到DDNS服务器上的连接成功示意图。当连接状态显示成功后，互联网上的其它主机就可以通过域名信息中的域名来访问路由器或虚拟服务器。

提示：

若希望将局域网中的服务器向互联网开放，还需要在转发规则功能中设置相应的端口映射，具体设置请参考[5.8 转发规则](#)部分。

5.16 系统工具

系统工具帮助您优化设备的配置。在系统工具菜单下有 12 个子菜单：**SNMP**、时间设置、诊断工具、看门狗、简单速率测试、软件升级、恢复出厂设置、备份和载入配置、重启路由器、修改登录口令、系统日志和流量统计。



点击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.16.1 时间设置

点击**系统工具**→**时间设置**，可以在图 5-68界面中设置AP的系统时间。设置系统时间有两种方式，手动设置系统时间和通过互联网获取标准的GMT时间。

时间设置

本页设置路由器的系统时间，您可以选择自己设置时间或者从互联网上获取标准的GMT时间。

注意：关闭路由器电源后，时间信息会丢失，当您下次开机连上Internet后，路由器将会自动获取GMT时间。您必须先连上Internet获取GMT时间或到此页设置时间后，其他功能（如上网控制）中的时间限定才能生效。

时区：

日期：年月日

时间：时分秒

优先使用NTP服务器1：

优先使用NTP服务器2：

（仅在连上互联网后才能获取GMT时间）

图 5-68 时间设置

时区： 该项用来手动设置系统时间，请先选择您的时区。

日期: 填写本地的日期, 格式为月/日/年。

时间: 填写本地时间, 格式为时/分/秒。

优先使用 NTP 服务器 1/2:

该项用来设置 NTP 服务器的 IP 地址(最多可以输入两个)。NTP 服务器是网络时间服务器, 用于同步互联网上的计算机时间。AP 内置了一些常用的 NTP 服务器地址, 一旦与 Internet 连接后, 路由器可以自动获取系统时间。但是, 若此处设置了该项, 则当路由器获取 GMT 时间时, 将优先从已设置的时间服务器上获取。

获取GMT时间: 首先请连接互联网, 选择所在的时区, 最后点击**获取GMT时间**按钮即可从互联网上获取标准的GMT时间。

注意:

1. NTP (Network Time Protocol, 网络时间协议) 用来为路由器、交换机和工作站之间提供时间同步。时间同步的作用是可以将多台网络设备上的相关事件记录联系起来, 有助于分析复杂的故障和安全事件等。
2. 关闭AP电源后, 时间信息会丢失, 只有当下次开机连上Internet后, AP会自动获取GMT时间。
3. 必须先通过Internet获取GMT时间或在此页手动设置系统时间后, AP其他功能(如防火墙)中的时间限定才能生效。

5.16.2 诊断工具

在本页面可以使用 ping 或者 tracert, 诊断 AP 的连接状态。



图 5-69 诊断工具

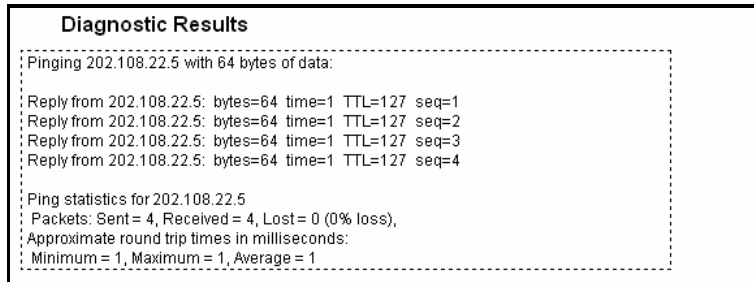
选择操作: 选择 Ping 或 Tracert 操作。

IP 地址/域名: 目的 IP 地址或域名。

- Ping 包数目：** Ping 操作发出的 Ping 包数目。
- Ping 包大小：** Ping 操作发出的 Ping 包的大小。
- Ping 超时：** 设置 Ping 操作的超时时间。
- Tracert 跳数：** 设置 Tracert 的跳数。

点击**开始**按钮来启动诊断，诊断结果页面中将显示诊断的结果。

如果诊断结果与下图类似，则说明网络连接正常。



注意：

1. 本功能在同一时间内只支持一个用户使用。
2. Ping/Tracert的目的地址可以是IP地址或者域名。如果对IP地址的Ping/Tracert操作成功，但是对相应的域名的Ping/Tracert操作失败，则问题可能是域名解析失败。请确认您输出的目的域名能够被DNS（Domain Name System, 域名系统）正确地解析。

5.16.3 软件升级

点击**系统工具**→**软件升级**，可以在图 5-70界面中升级本设备的软件版本以获得更多的功能和更为稳定的性能。

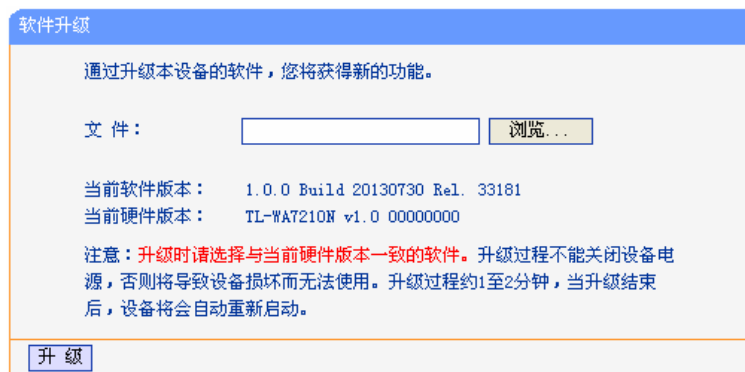


图 5-70 软件升级

软件升级步骤：

- 第一步：登录本公司的网站（<http://www.tp-link.com.cn>），下载最新版本的软件。
- 第二步：点击**浏览**按钮选择下载的文件，或在“文件”栏内填入已下载升级软件文件的全路径文件名。
- 第三步：点击**升级**进行软件升级。
- 第四步：升级完成后，设备将自动重启。

 **注意：**

1. 升级软件后，路由器可能会恢复到出厂默认设置，现有的所有设置信息将丢失，建议在升级软件之前备份现有设置信息。
2. 升级时请选择与当前硬件版本一致的软件。升级过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。当升级结束后，路由器将会自动重启。

当前软件版本： 显示设备当前的软件版本。

当前硬件版本： 显示设备当前的硬件版本。

5.16.4 恢复出厂设置

点击**系统工具**→**恢复出厂设置**，可以将设备的所有设置恢复到出厂时的默认状态。恢复出厂设置后，设备将自动重启，恢复出厂设置页面如图 5-71。

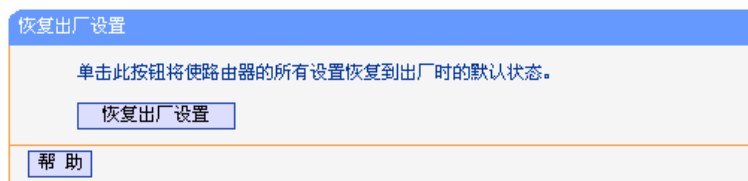


图 5-71 恢复出厂设置

点击**恢复出厂设置**按钮，路由器的所有设置将恢复到出厂时的默认状态。其中：

- 默认的用户名：admin
- 默认的密码：admin
- 默认的IP地址：192.168.1.254
- 默认的子网掩码：255.255.255.0

 **注意：**

恢复出厂设置后，您之前的配置信息将丢失。

5.16.5 备份和载入配置

配置备份功能可以将路由器的设置以文件形式保存到电脑中，以备下次使用；在升级路由器软件或在载入新的配置文件前备份路由器的原有配置，可以有效防止升级软件或载入新配置文件过程中丢失原有配置的问题。

配置载入功能则可以将先前保存的或已编辑好的配置文件重新载入。

如果需要为多台路由器配置相同的设置，则可以先配置一台路由器，保存其配置文件后，再将其载入到其它的路由器中，这样可以有效节省配置时间。

点击**系统工具**→**备份和载入配置**，可以在图 5-72中备份或载入设备的配置文件。

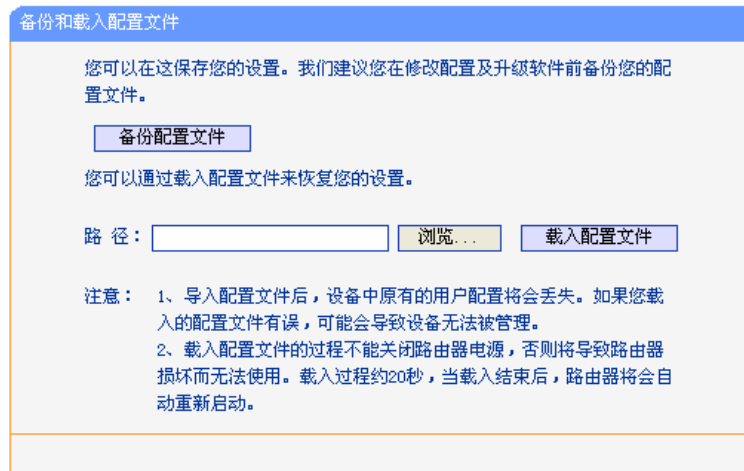


图 5-72 备份和载入配置

点击**备份配置文件**按钮来将当前所有的配置以文件的形式存入您的本地电脑。

点击**载入配置文件**按钮来将先前保存的或已编辑好的配置文件重新载入。

☞ 注意：

1. 载入配置文件后，设备中原有的配置信息将会丢失，所以在导入配置文件前请先备份配置。如果您载入的配置文件有误，可重新载入先前备份的文件。
2. 配置文件载入的过程中不能关闭接入器电源，否则将导致接入器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，AP将会自动重新启动。如果载入有错，请根据提示信息自己选择是否保存配置，最好重启AP。

5.16.6 重启设备

点击**系统工具**→**重启设备**，可以将设备重新启动，如图 5-73。



图 5-73 重启设备

点击**重启设备**按钮来重启设备。

本 AP 的某些设置需要在设备重新启动后才能生效，包括：

- 修改 LAN 口的基本网络参数（设备将自动重启）
- 修改 DHCP 的相关设置
- 修改无线配置
- 修改 Web 管理端口
- 升级设备的软件（设备将自动重启）
- 恢复 AP 的出厂设置（设备将自动重启）
- 载入配置文件（设备将自动重启）

5.16.7 修改登录口令

点击**系统工具**→**修改登录口令**，可以在图 5-74界面中修改登录AP管理界面的用户名和密码。修改完成后，点击**保存**按钮即可。

图 5-74 修改登陆口令

出于安全考虑，我们强烈推荐您更改初始系统管理员的口令。如果忘了系统口令，请将路由器恢复到出厂设置。

注意：

系统管理员的口令长度应该在 0-14 位之间。且不含空格键。请输入两次新口令来确认。

输入完成后点击**保存**按钮。

要清除全部信息请点击**清空**按钮。

5.16.8 系统日志

点击**系统工具**→**系统日志**，可以在下图 5-75中查看设备的日志信息。该界面记录了设备的系统日志，可以通过查询日志了解网络情况和快速定位设备故障。

图 5-75 系统日志

通过邮件定时发送日志功能： 设置是否启用邮件发送日志功能。

邮件发送设置： 设置邮件的收/发邮箱地址、SMTP 服务器地址、验证信息以及自动发送功能的时间表。

图 5-76 邮件发送设置

➤ 邮件帐户设置

发信邮箱地址:

设备使用的邮件帐户，设备通过该帐户发送邮件。

收信邮箱地址:

发送邮件的目的邮箱，最终该邮箱会收到发送的邮件。

SMTP 服务器地址:

提供 SMTP 服务的服务器地址，各大邮件门户网站均提供该服务器，例如 163 邮箱的 SMTP 服务器地址是 smtp.163.com。如果不清楚该地址可以登录相关的邮件网站查询帮助页面。

启用验证:

需要用户名/密码登录的邮箱基本上都需要启用验证。

用户名:

登录邮箱的用户名(不含@后面的字段)。

密码和密码确认:

登录邮箱用的密码。

➤ 定时自动发送日志功能

启用功能:

开启定时器，让日志自动通过邮件发送。

每天发送:

给出一天其中的一个时间点，路由器每天在该时间点会自动发送包含当前日志的邮件。

间隔发送:

给出一段间隔时间，路由器将在功能启动/系统启动后立即发送一封包含当前日志的邮件，并每经过这段间隔时间就发送一次邮件。

5.16.9 流量统计

点击系统工具→流量统计，可以在图 5-77中查看AP的流量信息。点击刷新按钮，可以更新流量统计表；本页分别对设备总的的数据流量以及最近一段时间间隔内的数据流量进行统计。

图 5-77 流量统计

当前流量统计状态： 显示流量统计功能是否开启，默认为关闭。

数据包统计时间间隔： 设置数据包统计时间间隔。默认为 10 秒，请在 5-60 秒之间选择。

分类规则下拉框选择流量统计表中的排序规则。包括：**按 IP 地址排序、按总流量数据包排序、按总流量字节数排序、按当前流量数据包排序、按当前流量字节数排序。**

统计表：

IP 地址		被统计主机的 IP 地址，此处也会显示该主机的 MAC 地址。
总流量	数据包数	设备接受和发送的数据包总数。
	字节数	设备接受和发送的字节总数。
当前流量	数据包数	设备在用户指定的数据包统计时间间隔中收、发数据的包的个数。
	字节数	设备在用户指定的数据包统计时间间隔中收、发数据的字节数。
	ICMP Tx	设备在用户指定的数据包统计时间间隔中每秒发送到广域网的 ICMP 包的个数。统计数字表现为：当前发送速率/历史最高发送速率。
	UDP Tx	设备在用户指定的数据包统计时间间隔中每秒发送到广域网的 UDP 包的个数。统计数字表现为：当前发送速率/历史最高发送速率。
	SYN Tx	设备在用户指定的数据包统计时间间隔中每秒发送到广域网的 TCP SYN 包的个数。统计数字表现为：当前发送速率/历史最高发送速率。

附录 A: FAQ

1. 忘记了登录AP的用户名和密码怎么办（如何将路由器复位）？

忘记了登录 AP 的用户名和密码只能将 AP 恢复到出厂默认设置，即复位。在 AP 的后面板上有一个标识为 **RESET** 的圆孔，这就是**复位键**。在通电状态下，持续按压 **RESET** 按钮，并至少等待五秒钟，当最右边的 LED 指示灯闪烁后，AP 将重启。

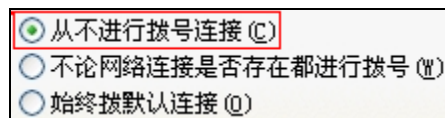
注意：复位后 AP 默认登录 IP 为 **192.168.1.254**，默认用户名/密码是 **admin/admin**。登录时，请确保计算机的 IP 地址在 192.168.1.X（X 为 2 到 253 之间的任意整数）网段。

2. 登录不了AP的管理界面怎么办？

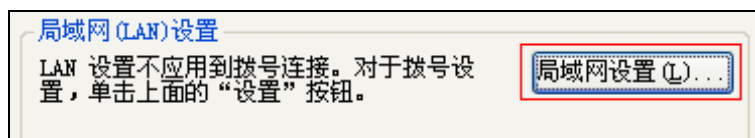
- 1) 请确保计算机连接在 AP 的 LAN 口；
- 2) 请确认计算机的 IP 地址与 AP 登录 IP 地址处于同一网段；如 AP 默认登录 IP 地址为 192.168.1.254，则计算机 IP 地址须为 192.168.1.X（X 为 2 到 253 之间的任意整数）；
- 3) 如果您修改了 AP 的 WEB 管理端口（默认为 80），则登录路由器管理界面时应输入 http://LAN 口 IP:端口号，如 http:192.168.1.254:88；
- 4) 请确保浏览器设置为从“不进行拨号连接”并且没有设置代理服务器；

方法如下（以 IE 浏览器为例）：

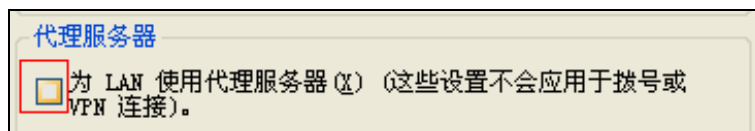
依次选择工具—Internet 选项—连接，选择“从不进行拨号连接”：



点击局域网设置：



如下图设置：



- 5) 可尝试更换其它计算机进行登录；

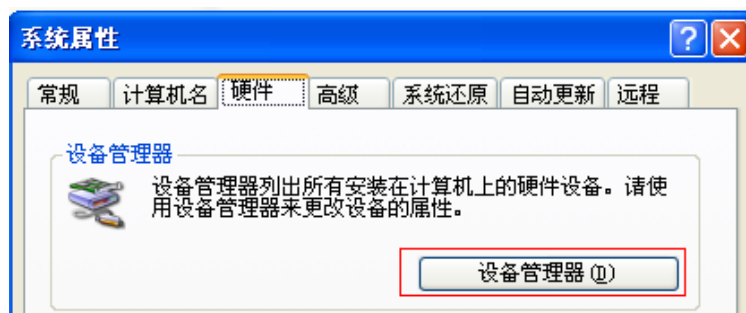
若上述提示不能帮助您登录到 AP，请将 AP 恢复出厂设置并重新操作。

3. 为什么我的笔记本电脑搜索不到无线信号？

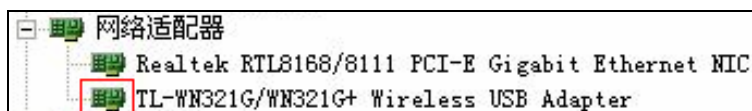
- 1) 如果是笔记本电脑内置的无线网卡，请确认无线功能开关已打开（建议联系笔记本电脑厂商或查阅相关说明书）；
- 2) 在设备管理器中查看无线网卡驱动是否成功安装以及无线网卡是否已启用；

方法如下：

右键点击桌面上的**我的电脑**，选择**属性-硬件-设备管理器**



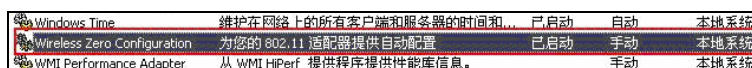
如下图中的绿色标识表示网卡驱动已安装成功且启用



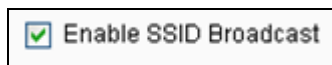
3) 检查笔记本电脑的无线服务是否开启；

方法如下（以 Windows XP 为例）：

右键点击桌面上**我的电脑**，选择**管理**。在计算机管理中选择“服务和应用程序”，再在“服务”页面里面查看“Wireless Zero Configuration”的状态



4) 请确认 AP 的无线功能已开启且允许 SSID 广播。



5) 尝试近距离是否可以搜索到无线信号，避免因障碍物太多导致信号衰减严重；

若上述提示不能帮助到您，请确认其它的无线网卡是否可以连接到该 AP。如果都不可以，请将 AP 恢复到出厂设置。

4. 为什么我的笔记本电脑搜到无线信号却连接不上？

- 1) 请确认尝试连接的无线信号的名称与 AP 设置的 SSID 号一致；
- 2) 请确认无线信号的强度，如果信号较弱，建议调整 AP 的位置或近距离连接；
- 3) 请确认 AP 是否设置加密，如果已设置加密，检查无线网卡与 AP 的加密设置是否一致；
- 4) 删除电脑上的无线网卡原有配置文件，重新进行连接；
- 5) 咨询笔记本电脑或无线网卡的厂商，按照相关的指导操作无线网卡进行连接；

若仍然无法连接，请将 AP 恢复到出厂设置并重新设置。

5. 如何判断我的上网方式？

一般情况下，我们可以通过如下几种简单的方法来辨别常见的上网方式：

- 1) ADSL 虚拟拨号（PPPoE）：宽带服务商只提供了一个用户名和密码（帐号和口令），不接路由器时需拨号上网；
- 2) 静态 IP 地址：宽带服务商提供了相关的 IP 地址和网关等信息，不用路由器时需要配置相关参数才可以上网；
- 3) 动态 IP 地址：宽带服务商没有提供任何参数，计算机不需要做任何设置。

6. 忘记无线加密的密钥怎么办？

一般来说有以下两种方法：

- 1) 使用网线连接计算机和 AP，通过有线的方式登录无线路由器并查看**无线安全设置**的相关参数；
- 2) 将 AP 恢复到出厂设置。

7. 有线使用正常，为什么无线上不了网？

一般情况下，如果使用有线连接可以正常上网，那么说明 AP 的配置基本上是正常的。请从下面几个方面排除故障：

- 1) 检查无线网卡和 AP 是否连接成功，（即检查用无线方式能否登录 AP 管理界面）；
- 2) 确认连接到了正确的 AP（根据 SSID 号判断）；
- 3) 检查无线网络连接是否配置了正确的 IP 地址、网关和 DNS 服务器地址；
- 4) 检查一下 AP 安全设置中是否有设置过滤；

8. 为什么QQ正常，却打不开网页？

- 1) 检查网络连接是否配置了正确的 DNS 服务器地址（可以咨询当地运营商或者登录路由器的管理界面，在**工作状态**→**WAN 口状态**→**DNS 服务器**处查看）；
- 2) 检查浏览器设置为从不进行拨号连接并且没有设置代理服务器；
- 3) 更换一个浏览器（如 Firefox）进行访问。

9. 无线信号受哪些因素的影响？

- 1) 无线局域网采用的是微波传输，微波的最大特点就是绕射能力非常弱。家庭中最主要的障碍物就是墙壁，它不仅阻挡无线信号还能把电磁的能量吸收掉，因此身处在墙后面的无线接收设备只能接到很微弱的信号，或没有收到信号。
- 2) 微波炉、蓝牙设备、无绳电话、电冰箱等的强大磁场会使无线网络信号受到影响。
- 3) 如果在无线环境中存在多台无线设备还有可能存在频道冲突，无线信号串扰的问题。
- 4) 距离无线设备及电缆线路 100 米内的无线电发射塔、电焊机、电车或高压电力变压器等强信号干扰源，也可能对无线信号或设备产生强干扰。
- 5) 室外传播时天气情况对无线信号的影响也很大，雷雨天或天气比较阴沉的时候信号衰减比较厉害，晴天里信号能传输的距离会比较远。

10. 如何改善信号传输质量？

- 1) 为 AP 选择一个最佳的放置地点。这个放置地点的要求如下：一、位置应偏高一些，以便在较高地方向下辐射，减少障碍物的阻拦，尽量减少信号盲区；二、位置地点选择时应使信号尽量少穿越隔墙，最好使房间中的无线客户端能与无线 AP 可视。
- 2) 修改频道，减少无线串扰。注意：设置自己无线信号发射频道时也要尽量保证离别人的无线信号频道 5 个以上。
- 3) 减少家用电器干扰，保证信号畅通无阻。放置无线 AP 时尽量远离上述设备。
- 4) 如果 AP 天线是可拆卸的，可以通过更换天线达到增强无线信号的目的。

附录 B: IE浏览器设置

2. 打开 IE 浏览器，选择菜单工具→Internet 选项...，如图 1 所示。



图 1

3. 在 Internet 选项界面中点击“连接”，勾选“从不进行拨号连接”，或将“拨号和虚拟专用网络设置”中的设置内容全部删除(即将下图中的“宽带连接（默认）”删除)，如图 2 示。

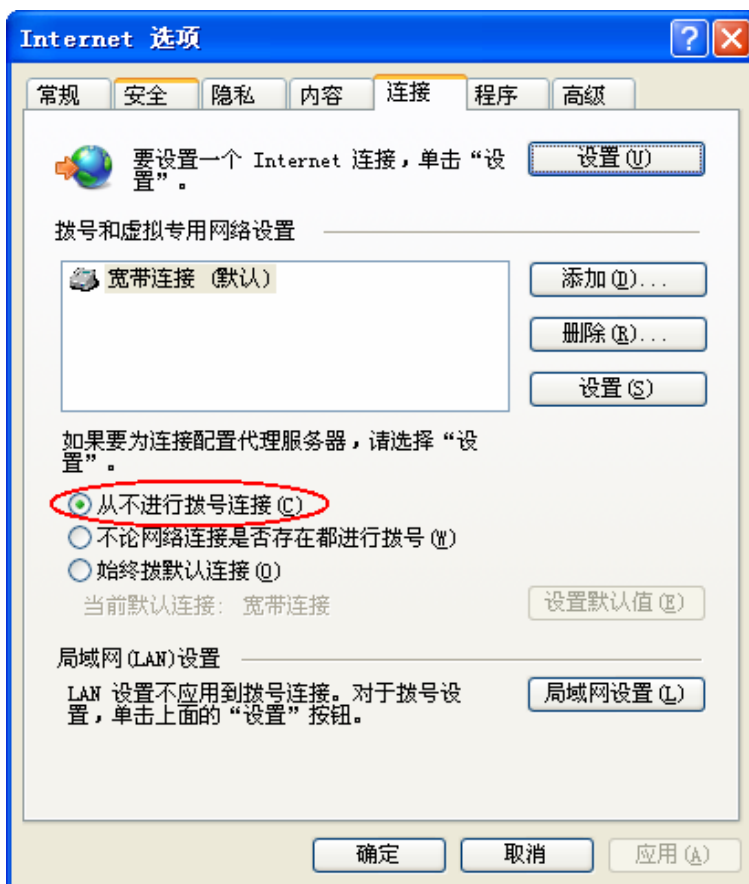


图 2

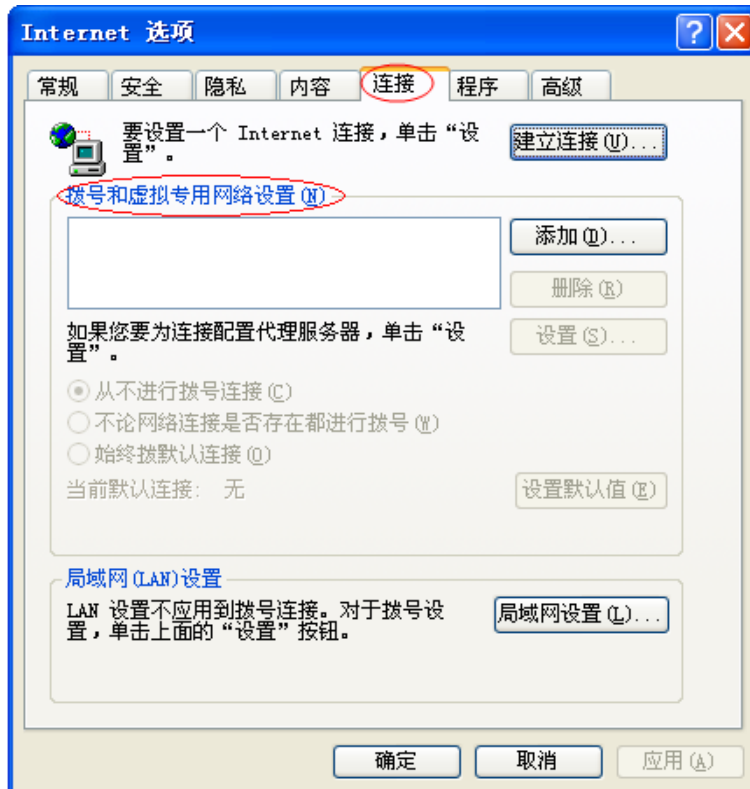


图 3

4. 点击图 3 中的局域网设置...按钮，确保“代理服务器”下的复选框处于非选中状态，如下图界面所示，点击确定按钮返回。

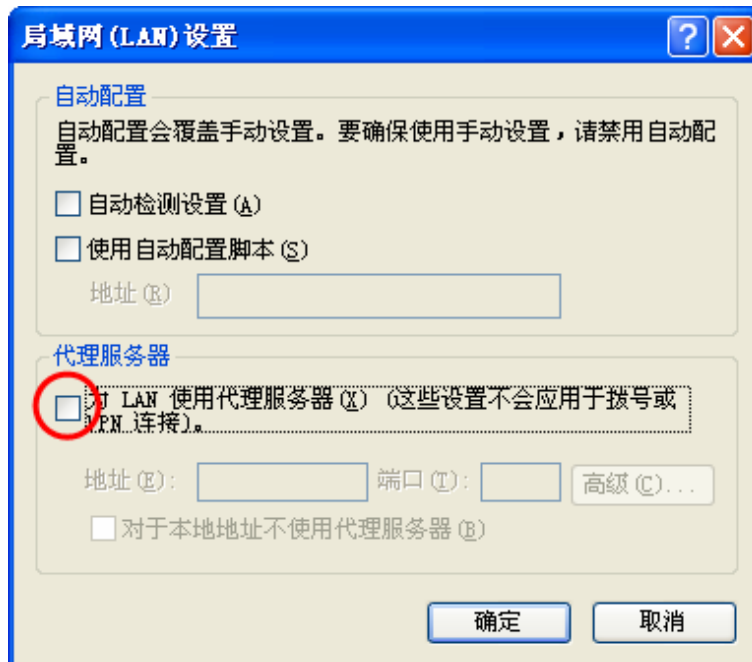


图 4

5. 回到 IE 浏览器界面，选择菜单文件，点击下拉菜单中的脱机工作将该项将前面的“√”去掉，如下图示。若该项前面没有“√”符号则表示脱机工作没有启用，不用设置。

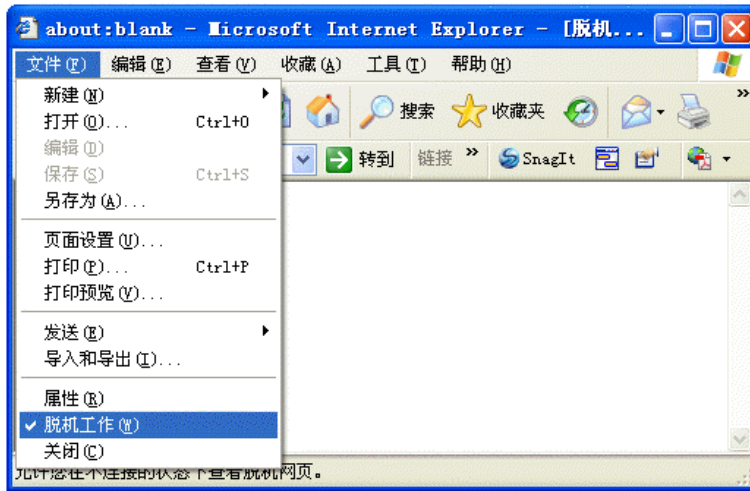


图 5

附录 C: POE的使用

A. 简介

POE 设备使您不再受电源适配器位置的限制，在一定范围内，可以随意放置 AP 产品。

B. 接口说明

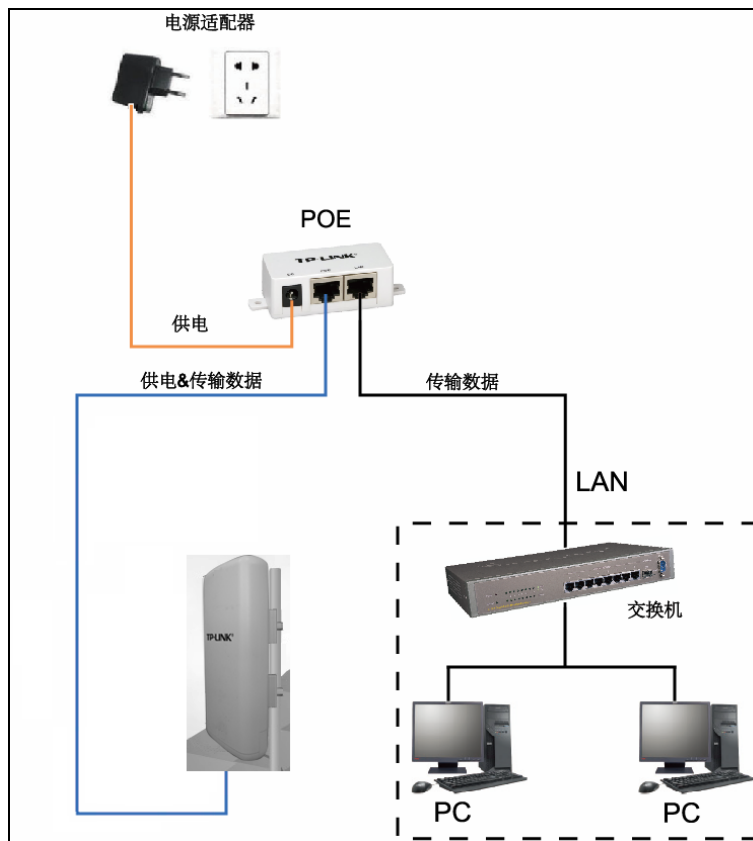


- **DC:** 电源插孔，连接电源适配器。
- **POE:** POE 口，连接到 AP 的 LAN 口。
- **LAN:** LAN 口，连接到局域网用于数据传输。

C. 硬件连接

请按以下步骤将 POE 接入网络：

1. 关闭所有的网络设备，包括计算机、交换机、POE 和 AP。
2. 将以太网线一端接入交换机，另一端接入 POE 设备的 LAN 口。
3. 将电源适配器接入 POE 设备的 DC 插孔，另一端插入电源插座。
4. 将以太网线一端接入 AP，另一端接入 POE 设备的 POE 接口。



注意：

1. 连接 POE 的以太网线对长度有一定限制，具体数据请查看下表。表格所列数据已通过 TP-LINK 检测，但实际当中也会因环境、网线质量等因素的影响而变化。

机型	电源适配器	POE 以太网线长度
TL-WA501G+	输出: 9VDC/0.6A	≤40 米
TL-WA701N	输出: 9VDC/0.85A	≤40 米
TL-WA801N	输出: 12VDC/1A	≤60 米
TL-WA7210N	输出: 12VDC/1A	≤60 米

2. 如果您需要连接 POE 设备的网线长度上限高达 100 米，请选择 TP-LINK 的 48V POE 配套产品，如：TL-POE200、TL-POE150S 和 TL-POE10R。
3. 为保证 POE 设备正常使用，请使用配套的电源适配器。
4. Passive POE 并不是标准 PoE（802.3af），请与支持 Passive PoE 的设备配套使用。

附录 D: 规格参数

基本参数	
支持的标准和协议	IEEE 802.3, 802.3u, 802.11b, 802.11g and 802.11n, TCP/IP, DHCP
安全认证	FCC, CE
端口	一个10/100M 自协商RJ45端口, 支持POE供电设备。
网络介质	10Base-T: 3类或3类以上 UTP 100Base-TX: 5类 UTP
无线参数	
无线传输速率	最高可达150Mbps
无线数据加密	64/128/152-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK
物理和环境参数	
工作温度	-30°C~70°C
工作湿度	10% 到 90% RH不凝结
储存温度	-40°C~70°C(-40°F~158°F)
储存湿度	5% 到 90% RH不凝结