TP-LINK®

室外无线基站和CPE系列

TL-CPE210/TL-CPE510/TL-BS210/TL-BS510

用户手册

REV1.0.1

1910040458

声明

前言

本手册旨在帮助您正确使用室外无线基站和CPE系列产品。手册中详细介绍了该系列产品的使用方法，请在操作设备前，详细阅读本手册。

目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

本书约定

在本手册中，

- 所提到的“设备”、“本产品”“无线基站/CPE”等名词，如无特别说明，系指室外无线基站和CPE系列产品，即 TL-CPE210/TL-CPE510/TL-BS210/TL-BS510；所提到的“远程AP”系指本设备准备接入的远程的AP设备；所提到的“前端AP”、“前端设备”等名词系指本设备已经接入的无线AP或无线路由设备；所提到的“STA”、“站点”等名词系指接入到本设备的无线客户端。
- 正文中出现的<>尖括号标记的文字，表示Web页面的按钮名称，如<确定>。
- 正文中出现的**加粗**标记的文字，表示设备的各个功能的名称，如**端口配置**页面。
- 正文中出现的“”双引号标记的文字，表示配置页面上出现的名词，如“IP地址”。

本手册中使用的特殊图标说明如下：

图标	含义
注意：	该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
说明：	该图标表示此部分内容是对相应设置、步骤的补充说明。

目录

第1章 产品介绍

1.1 产品简介

300M 室外无线基站和 CPE 系列产品专门为室外无线网络覆盖提供有效的解决方案。该系列涵盖 2.4GHz 与 5GHz 两个频段的室外无线基站和 CPE 产品，并支持由 Pharos Control 软件统一管理，可以实现点对点、点对多点和室外无线覆盖等多种应用，从而满足农村、厂区等室外环境远距离无线传输以及公园、广场等环境无线覆盖需求。

300M 室外无线基站提供两个 RP-SMA-MALE 外置天线接口，既可外接高增益定向天线实现远距离传输，又可配合全向天线或扇区天线实现大范围无线覆盖；300M 室外无线 CPE 采用内置高增益定向天线和 802.11n MIMO 技术，提供 300Mbps 的无线传输速率。

300M 室外无线基站和 CPE 系列产品为不同用户提供 6 种工作模式：AP 模式、Client 模式、Repeater 模式、Bridge 模式、AP Router 模式、AP Client Router 模式。

300M 室外无线基站和 CPE 系列产品满足 4kV 雷电防护、15kV ESD 防护，同时采用 ASA 工程塑料壳体，无线基站符合 IP65 等级防尘、防水，无线 CPE 符合 IP55 等级防尘、防水。

该系列产品包含如下机型：

产品机型	产品名称	特点
TL-CPE210	2.4GHz 300M 9dBi 室外无线 CPE	内置高增益定向天线，常工作在 Client 或 AP Client Router 模式用于定向传输无线数据
TL-CPE510	5GHz 300M 13dBi 室外无线 CPE	
TL-BS210	2.4GHz 300M 室外无线基站	可外接定向或全向天线，常工作在 Access Point 或 AP Router 模式用于定向传输数据或实现大范围无线覆盖
TL-BS510	5GHz 300M 室外无线基站	

1.2 产品外观

室外无线基站和CPE系列产品的指示灯位于左侧面板上，如图 1-1所示（以TL-CPE210为例）。

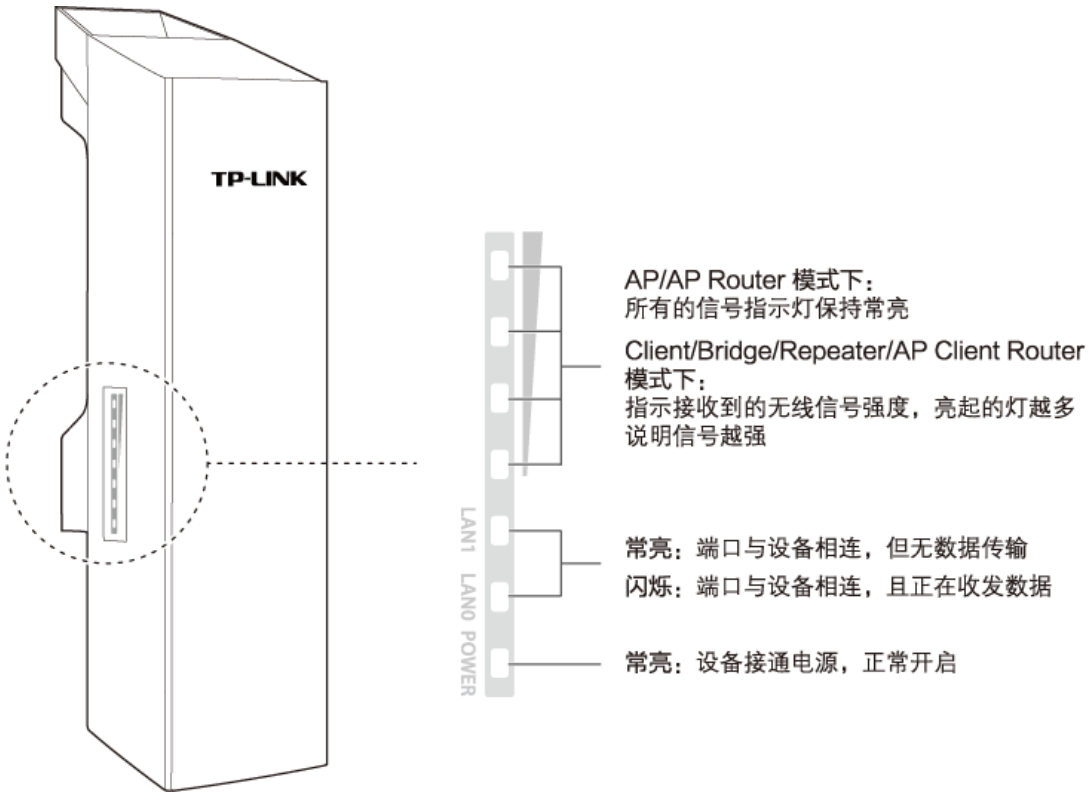


图 1-1 基站与CPE指示灯介绍

室外无线基站和 CPE 系列产品的接口和按键位于底部面板上，如图 1-2 所示（以 TL-CPE210 为例）。

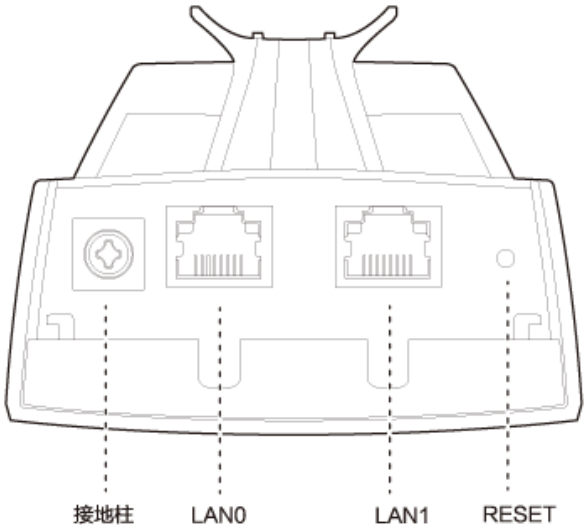


图 1-2 基站与CPE底部面板示意图

- 接地柱

  用于与地线相连进行接地。良好的接地是设备防静电和防雷的重要保障，本设备可通过两种方式接地，具体操作方法可参考《安装手册》。

- LAN0

  RJ45 端口，同时也是 PoE 输入端口。用于连接 PoE 适配器的 PoE 端口， 可同时传输数据和为本设备供电。

- LAN1

  RJ45 端口，同时也是 PoE 输出端口。可同时传输数据和为受电设备供电，供电电压为 24V。

  说明：

  LAN1 端口既可连接 PoE 设备，也可连接非 PoE 设备。当接入的为 PoE 设备需要通过 LAN1 端口供电时，请先登录 Web 管理界面，进入**管理维护**页面启用“LAN1 端口 PoE 供电”功能；当接入的为非 PoE 设备时，LAN1 端口将只传输数据，不会损坏您的设备。

- RESET

  复位键。在设备通电的情况下，长按 RESET 键约 8 秒至无线信号强度指示灯闪烁后松开，设备将自动恢复出厂设置并重启。

室外无线基站和 CPE 系列产品采用 24V/1A Passive PoE 供电，Passive PoE 适配器的指示灯、按键及接口如图 1-3 所示。

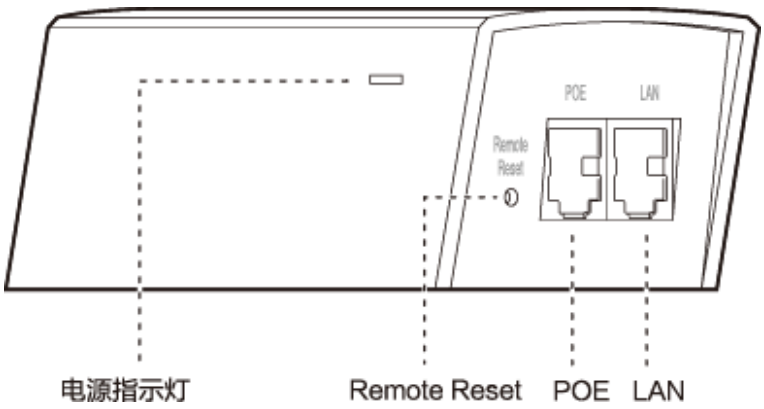


图 1-3 Passive PoE适配器示意图

- 电源指示灯

  指示当前工作电流的大小：绿色为 0~0.8A；红色为 0.8A~1A。

- Remote Reset

  远程复位键。在无线基站/CPE 通电的情况下，长按此 Remote Reset 键约 8 秒至无线基站/CPE 的无线信号强度指示灯闪烁后松开，无线基站/CPE 将自动恢复出厂设置并重启。

- POE

  POE 端口，用于连接无线基站/CPE 的 LAN0 端口。

- LAN

  LAN 端口。用于连接需要接入到无线基站/CPE 的网络设备，如计算机或交换机。

第2章 工作模式

室外无线基站和CPE系列产品支持六种工作模式：Access Point、Client、Repeater、Bridge、AP Router和AP Client Router。下面将分别介绍六种工作模式的典型应用场景，请根据需要选择一种工作模式，并参考《安装手册》进行硬件连接，相应的软件配置方法则请参考第4章 快速设置。

2.1 Access Point模式

Access Point 模式下，设备作为无线网络的中心节点，为无线客户端提供网络接入。Access Point 模式主要有三种常见的应用场景。此模式下还可开启“多 SSID”功能，设备可同时提供 4 个具有不同 SSID 和加密方式的无线网络。如需深入了解“多 SSID”功能，请参考 7.4 多 SSID。

➢ 场景一

在校园、小区、工业园区或公共场所等实现无线网络覆盖，组网图如图 2-1 所示。

本设备工作在 Access Point 模式，前端接入校园网、园区局域网等，在现有有线局域网的基础上提供无线接入点，为智能手机、平板电脑、笔记本电脑等无线客户端提供无线网络接入，丰富了局域网的接入方式。

特点：在现有的有线局域网基础上增加无线接入点，丰富了局域网的接入方式。

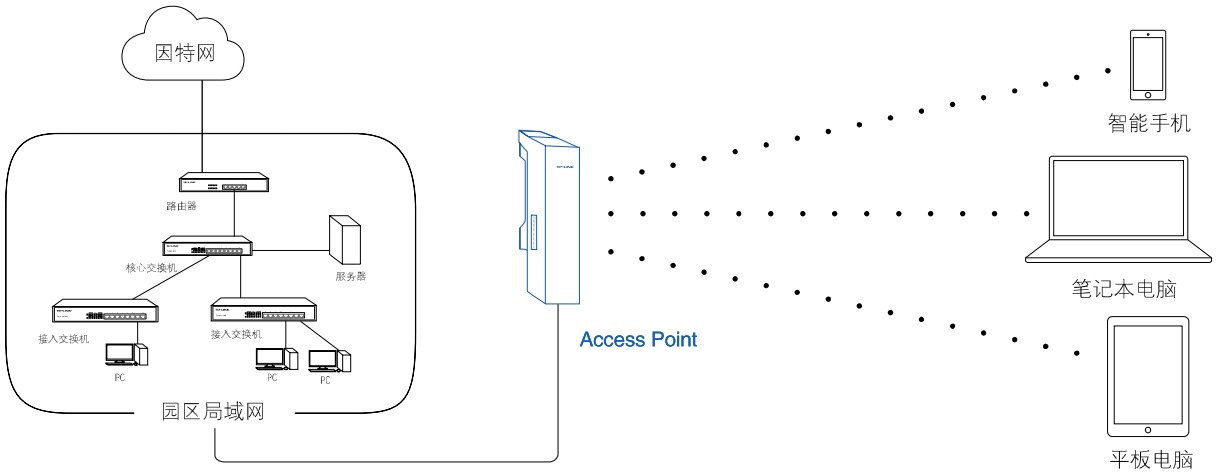


图 2-1 AP模式--场景一

➢ 场景二

在偏远的农村地区部署网络。

偏远地区的上网用户比较分散，布线麻烦而且昂贵。采用本设备部署网络，可实现远距离无线数据传输，省去布线的烦恼，降低施工成本。

如图 2-2所示，首先运营商可选择在其邻近且已经有有线网络覆盖的城镇搭建一个设备工作在Access Point模式，前端接入运营商网络；然后农村中的家庭用户只要在家中搭建一个设备工作在AP Client Router来接入Access Point的网络即可上网，使运营商可以突破传统的有线接入方式，节约运营成本。

特点：采用远距离无线方式传输数据，降低网络部署中的施工成本，为用户提供更丰富的接入方式。

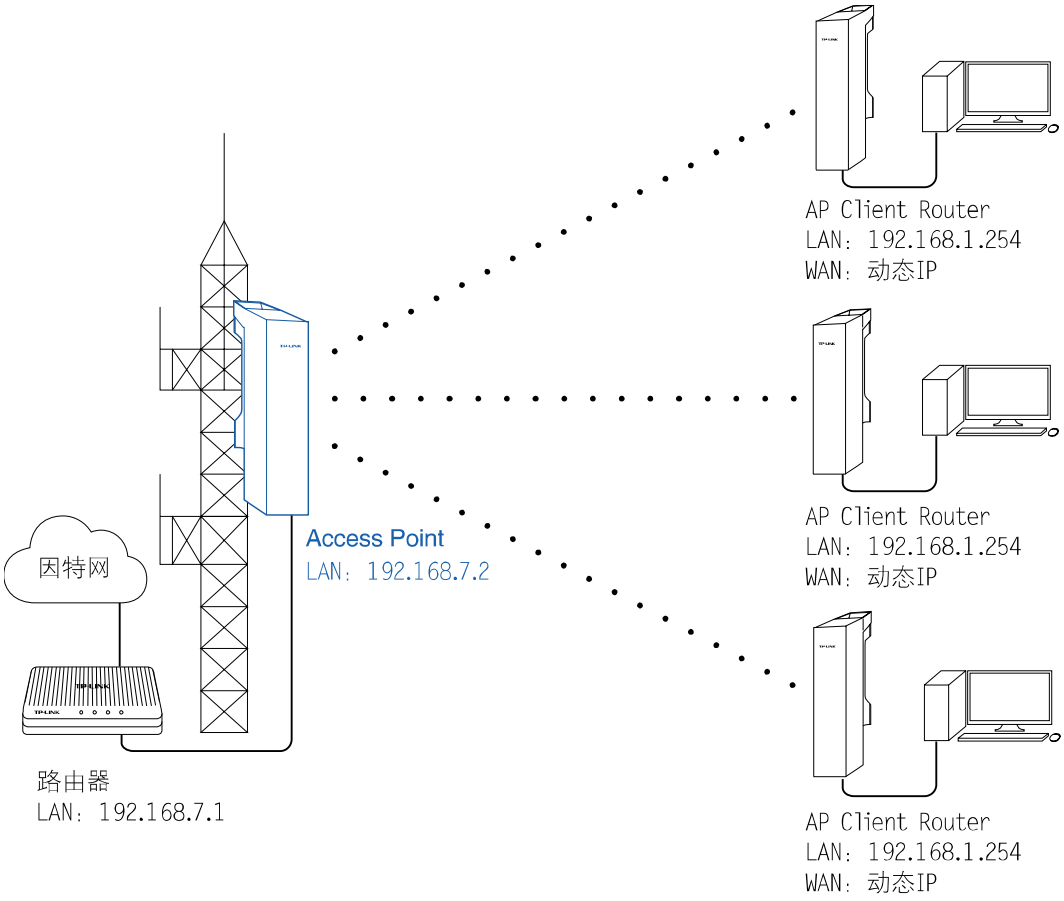


图 2-2 AP模式--场景二

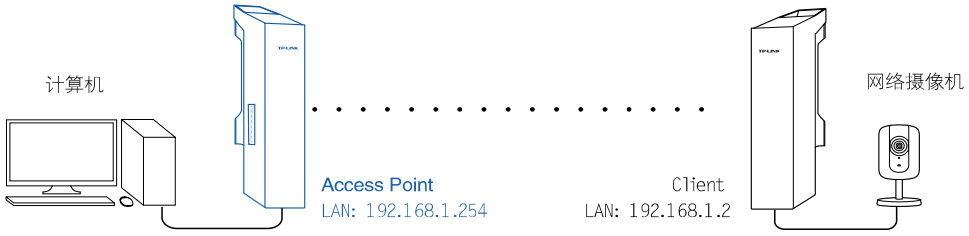
➢ 场景三

点对点组网进行视频监控，或者用于连接同一企业的两个办公区。

如图 2-3 所示，用于视频监控时，将工作在 Access Point 模式下的设备连接用于监控的计算机，而工作在 Client 模式下的设备连接网络摄像机；用于连接两个办公区时，则将工作在 Access Point 和 Client 模式下的本设备分别接入到两个办公区的接入交换机，从而连接两个办公网络。用户通过一对室外无线基站和 CPE 系列产品即可完成远距离无线组建局域网，实现两地互联互通，省去了传统布线的烦恼，是一种简单又经济的方案。

特点：点对点远距离组建局域网实现两地互联互通，省去传统布线烦恼。

视频监控：



连接两个办公区：

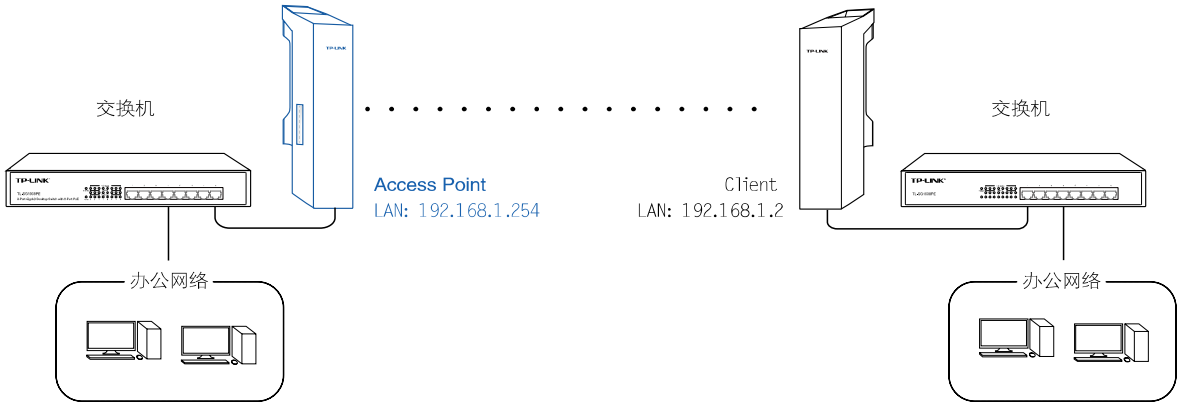


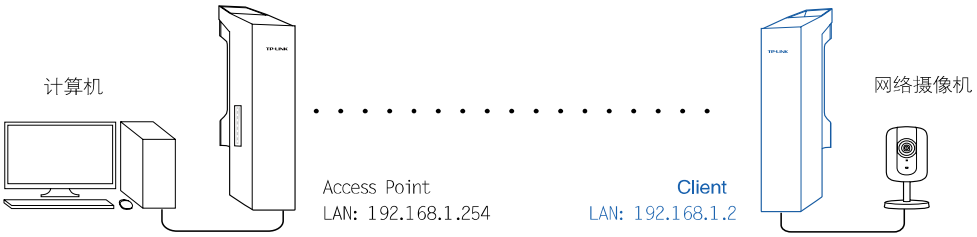
图 2-3 AP模式--场景三

2.2 Client模式

Client 模式下，设备相当于无线网卡，用来接收前端无线接入点的无线信号，这样有线设备通过连接到 Client 即可访问前端 AP 或基站提供的网络。

如图 2-4 所示，Client 最为常见的应用场景是与 Access Point 配合进行点对点组网，用于视频监控或者连接两个办公区，详细内容可参考 Access Point 模式的场景三。

视频监控：



连接两个办公区：

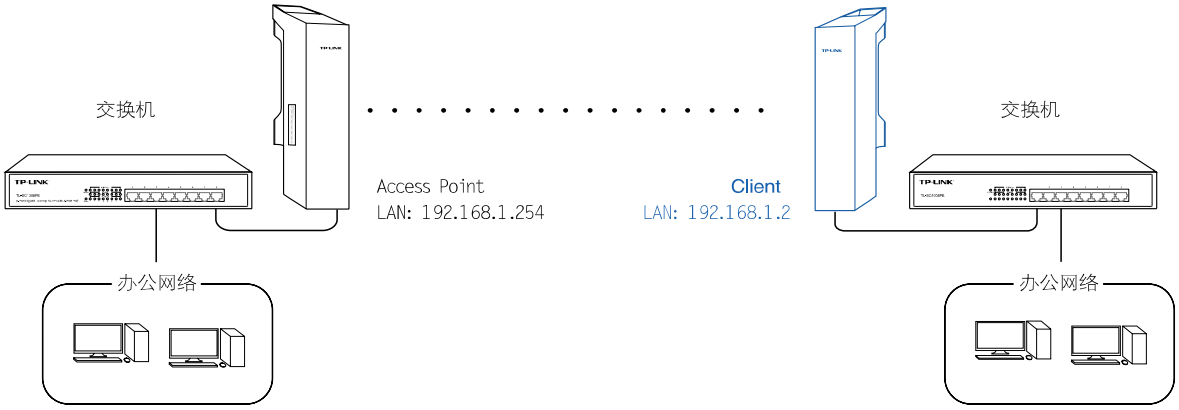


图 2-4 Client模式

2.3 Repeater模式

Repeater 模式下，设备用于增强已有的无线信号，从而延伸无线信号的覆盖范围，消除信号盲区。此模式下本设备提供的无线网络的 SSID 和加密方式与前端 AP 的完全相同。

➢ 场景一

用于消除信号盲区。

在面积比较大的校园、工业园区等场所部署无线网络时，仅用一台设备工作在 Access Point 模式下可能无法完全覆盖所有区域，存在信号盲区。此时，可以搭建一台或多台设备工作在 Repeater 模式下用于延伸无线信号的覆盖范围，消除信号盲区。

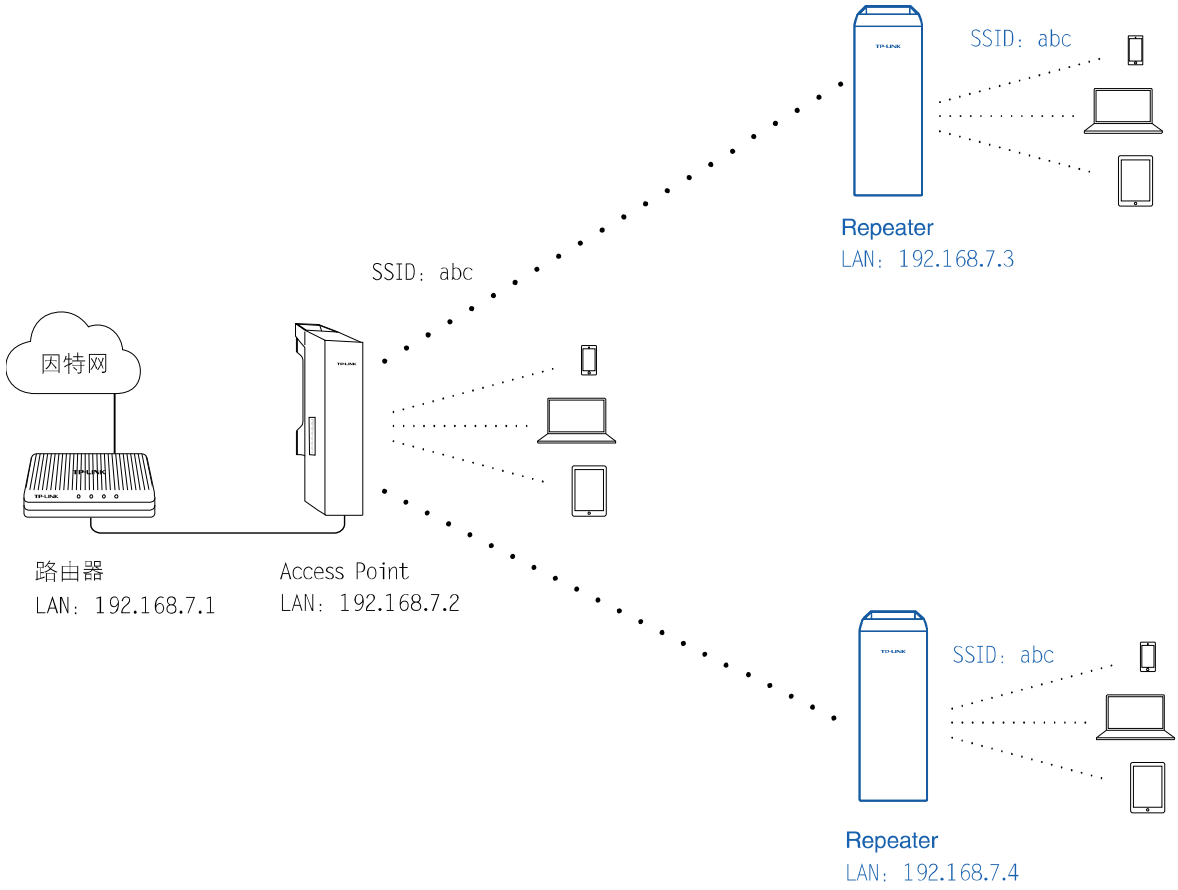


图 2-5 Repeater模式--场景一

➢ 场景二

用于为无线传输“接力”。

如图 2-6所示，当进行远距离无线传输时，若两地距离超过了CPE的最大传输范围，可在中间搭建一台设备工作在Repeater模式下为无线传输“接力”。

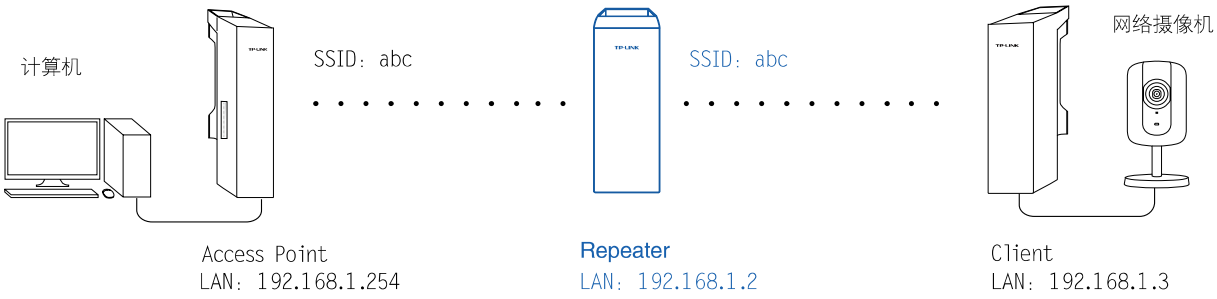
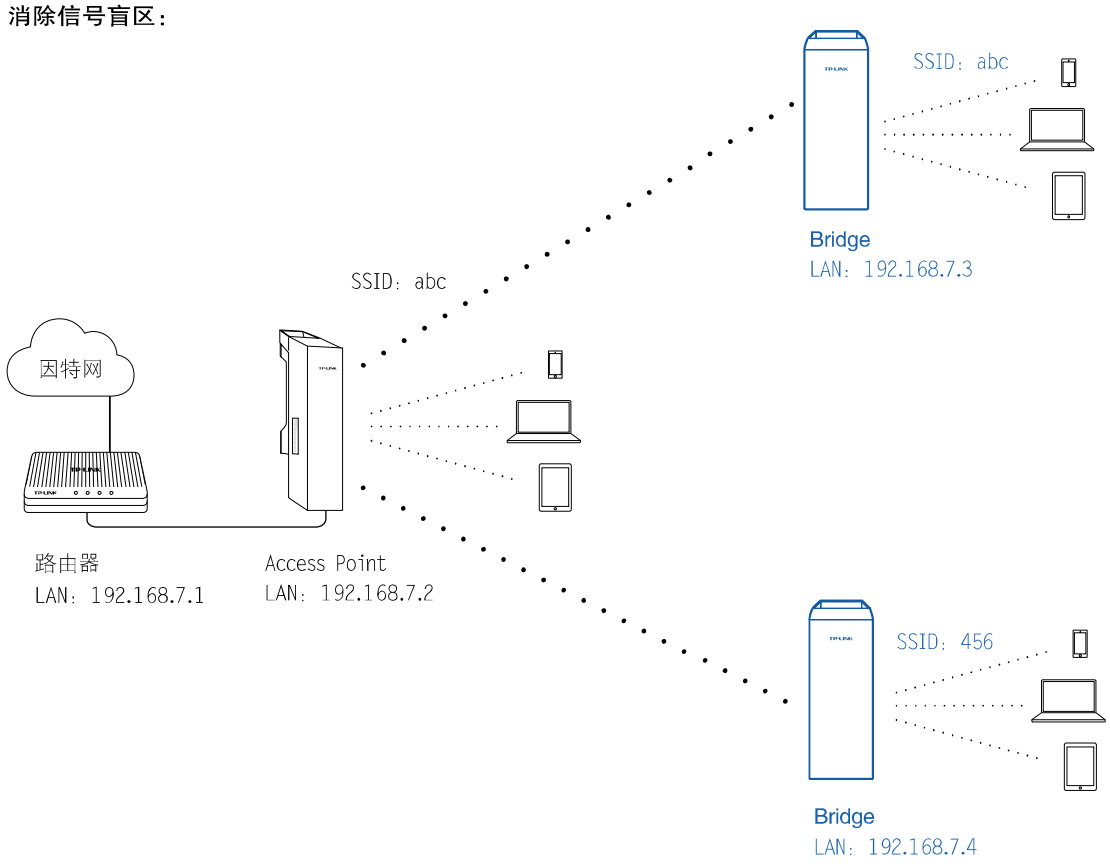


图 2-6 Repeater模式--场景二

2.4 Bridge模式

如图 2-7 所示，Bridge 模式与 Repeater 模式应用场景类似，也是用于增强已有的无线信号。与 Repeater 模式不同的是，Bridge 模式下还可以设置其无线网络的 SSID 和加密方式，不必与前端 AP 保持一致。

消除信号盲区：



为无线传输“接力”：

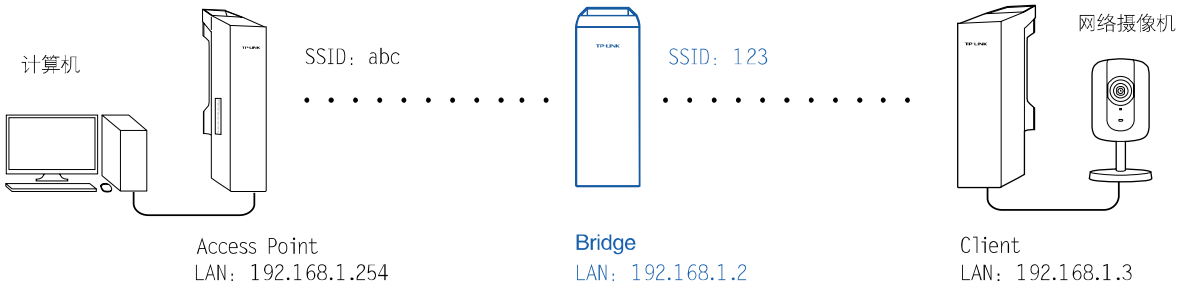


图 2-7 Bridge模式

2.5 AP Router模式

AP Router 模式下，设备与家用无线路由器类似，其前端接入调制解调器（猫），智能手机、笔记本电脑等无线客户端通过连接到本设备提供的无线网络即可共享广域网。不同之处在于，本设备的无线覆盖范围更广。其应用场景与 Access Point 的场景一类似，可以在校园、小区、工业园区或公共场所等实现无线网络覆盖。

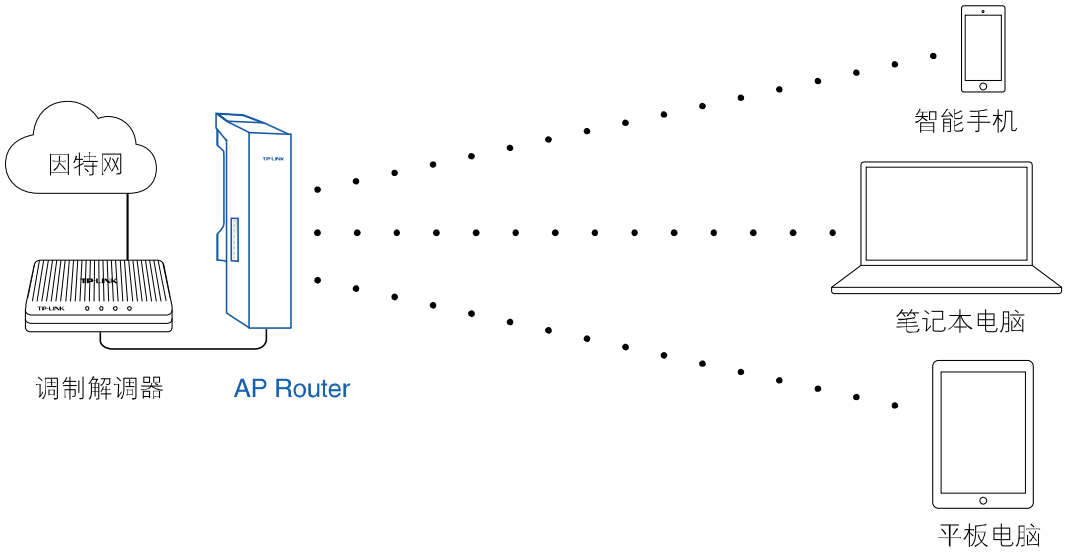


图 2-8 AP Router模式

2.6 AP Client Router模式

AP Client Router 模式下，本设备前端接入 WISP 提供的无线网络，再为后端的无线客户端提供无线网络服务，同时允许台式电脑等有线设备通过本设备的 LAN1 口或者 PoE 适配器的 LAN 口接入本设备。这样所有接入到本设备的用户就可以共享一个从 WISP 申请的帐户上网了。

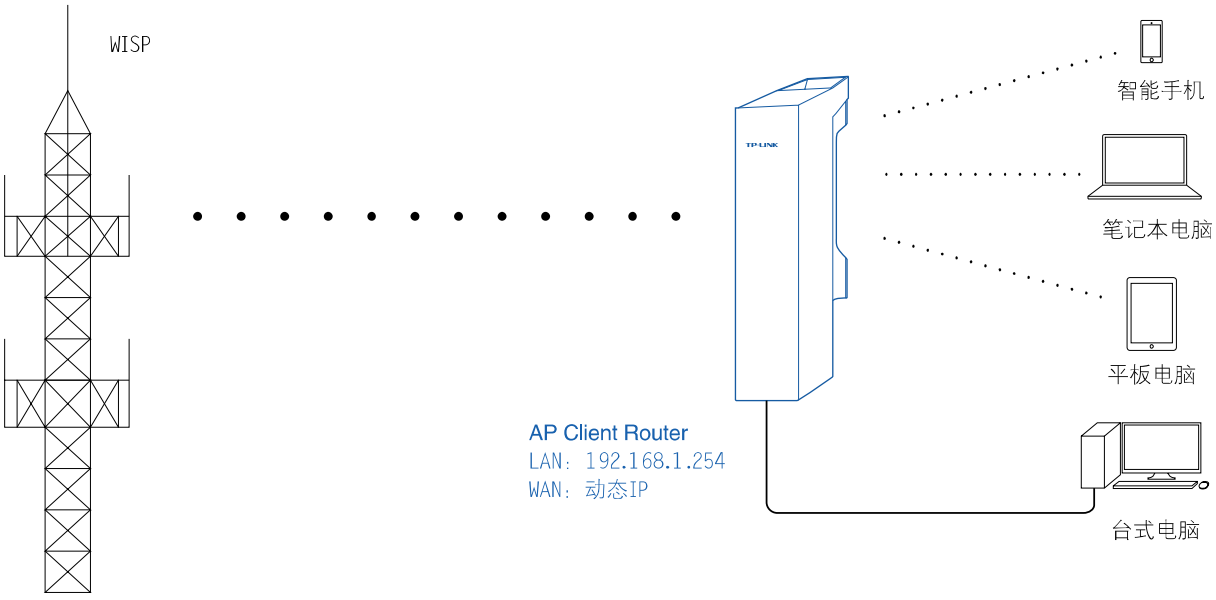


图 2-9 AP Client Router模式

第3章 登录Web页面

3.1 登录Web页面步骤

第一次登录时，请确认以下几点：

1) 设备已正常加电启动，并已与管理主机相连；

2) 管理主机已正确安装有线网卡及该网卡的驱动程序；

3) 管理主机IP地址已设为与本设备同一网段，即192.168.1.X（X为2至253之间的任意整数），子网掩码为255.255.255.0；

4) 为保证更好地体验Web页面显示效果，浏览器推荐使用Mozilla Firefox、Apple Safari、 Google Chrome或者IE 8.0及以上版本。

打开浏览器，在地址栏输入http://192.168.1.254登录设备的Web页面。

首次登录设备时页面如图 3-1所示。在此页面输入设备管理帐号的用户名和密码，出厂默认值为admin/admin。然后仔细阅读框内的使用条款并勾选“我同意该使用条款”，最后点击<登录>按钮。

图 3-1 登录页面

出于网络安全考虑，进行首次登录时，系统将弹出如图 3-2所示页面，您需要在该页面修改本设备管理帐号的用户名和密码。要求输入的用户名和密码长度不超过15个字符，不能包含空格且注意英文字母区分大小写。确认新密码后点击<完成>按钮完成修改。如图 3-2所示。

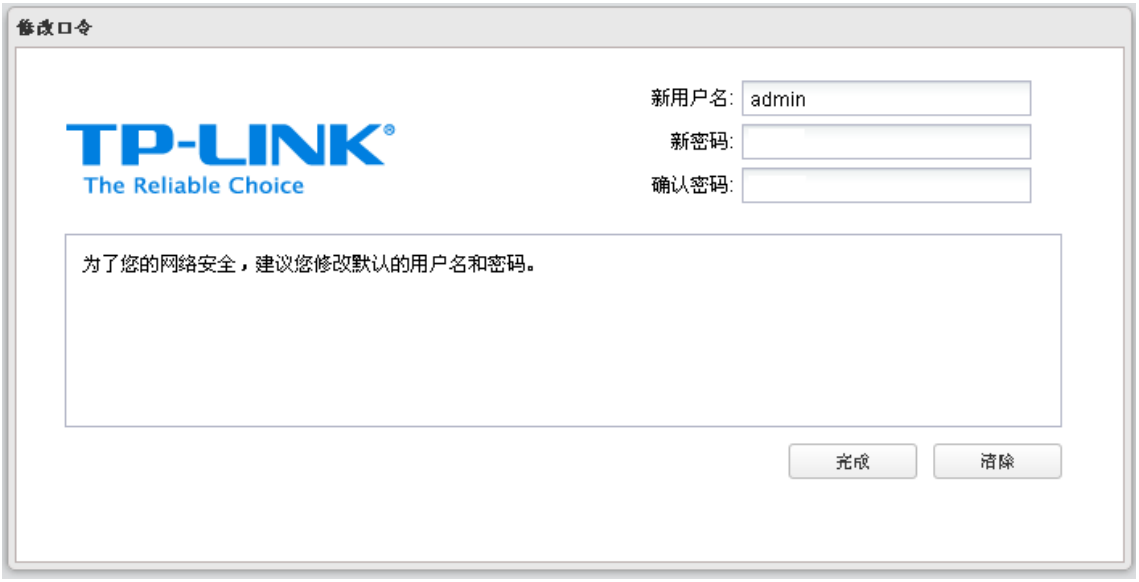


图 3-2 修改口令

成功登录后即进入系统状态页面，如图 3-3 所示。

图 3-3 初始页面

3.2 Web页面简介

室外无线基站和CPE系列典型的Web页面如图 3-4所示。

图 3-4 Web页面区域划分

从图中可以看到，页面主要由快速选择菜单、功能菜单区和功能设置区组成。

编号	页面元素	描述
A	快速选择区	包含“工作模式”和“小工具”两个下拉菜单，可以快速地配置设备的工作模式和使用 Ping、速度测试、频谱分析等工具。
B	功能菜单区	通过点击菜单的标题切换功能界面，进行相应的配置操作。
C	功能设置区	配置相应的功能。

第4章 快速设置

使用快速设置功能可以快速设置您需要的模式。以下将分别介绍六种工作模式的快速设置方法，设置过程中出现的参数，如无特别说明或特别需要，保持默认设置即可。

室外无线基站和CPE系列支持六种工作模式：Access Point、Client、Repeater、Bridge、AP Router和AP Client Router。

4.1 Access Point模式

Access Point 模式的配置步骤如下：

1. 进入**快速设置**页面，工作模式选择 Access Point，然后点击<下一步>按钮。

2. 将 IP 地址设置为与前端路由器处在同一网段，再输入子网掩码，然后点击<下一步>按钮。

3. 进入 **AP 设置**页面，设置 AP 模式基本参数。建议“加密方式”选择 WPA-PSK / WPA2-PSK 并在“PSK 密钥”一栏设置无线网络的密码，要求为 8-63 个 ASCII 字符（包含数字、英文字母及特殊符号，英文字母注意区分大小写）或者 64 个十六进制字符（包含 0-9、A-F 及 a-f，英

文字母不区分大小写)；“距离设置”请输入最远的客户端与本设备之间的距离 (如果您无法精确测量该距离，建议输入一个比实际距离稍微偏大的数值)；如果接入本设备的无线网络的客户端设备均为 TP-LINK 室外无线基站和 CPE 系列产品，建议启用 MAXtream 功能以提高无线传输性能。完成 AP 参数设置后点击<下一步>按钮。

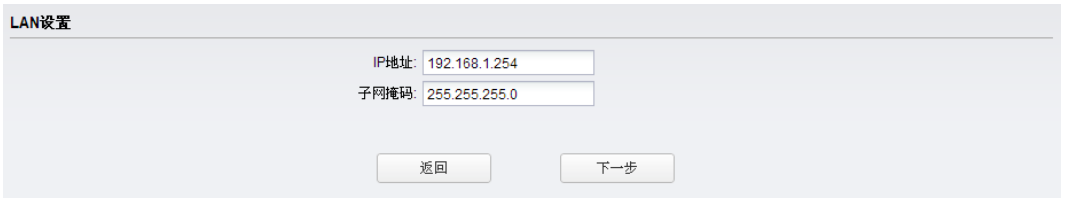
4. 完成上述步骤后，您将会看到**完成**页面，如下图所示。请检查您所配置的参数，如有错误，请点击<返回>重新设置。若配置确认无误，请点击<完成>按钮使配置生效。

4.2 Client模式

Client 模式的配置步骤如下：

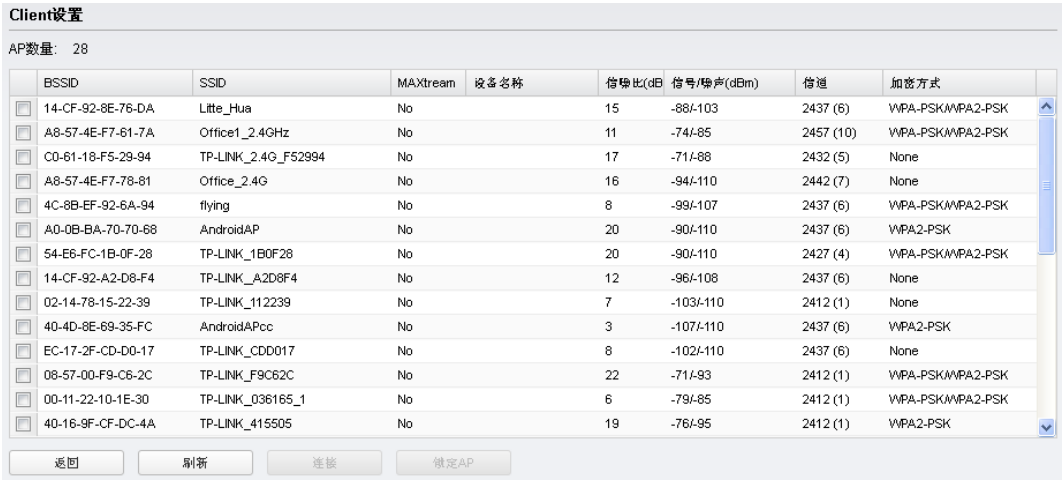
1. 进入**快速设置**页面，工作模式选择 Client，然后点击<下一步>按钮：

2. 进入 **LAN 设置**页面，将 IP 地址设置为与前端设备处在同一网段，再输入子网掩码，然后点击<下一步>按钮。



3. 进入 **Client 设置**页面，填写 Client 相关参数。

单击<扫描>按钮将出现可用的AP列表，如下图所示。选择一个目标AP，然后点击<连接>按钮，页面将自动返回到上图所示页面。如果您启用MAC地址锁定AP功能则可以唯一确定需要关联的远程AP 。“无线模式”、“信道带宽”、“加密方式”和“PSK密钥”请与接入的远程AP保持一致。“距离设置”则填写设备与远程AP的距离（如果您无法精确测量该距离，建议输入一个比实际距离稍微偏大的数值）。完成Client设置后点击<下一步>按钮。



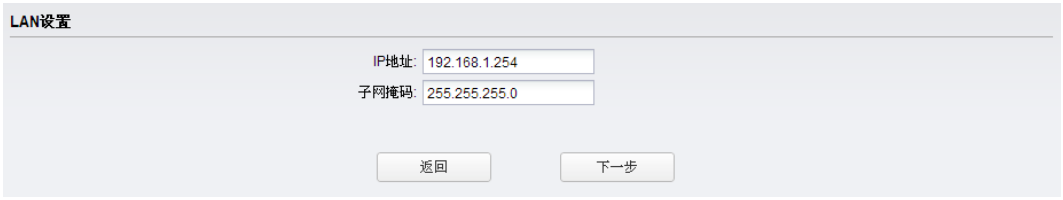
4. 完成上述步骤后，您将会看到**完成**页面，如下图所示。请检查您所配置的参数，如有错误，请点击<返回>重新设置。若配置确认无误，请点击<完成>按钮使配置生效。

4.3 Repeater模式

Repeater 模式的配置步骤如下：

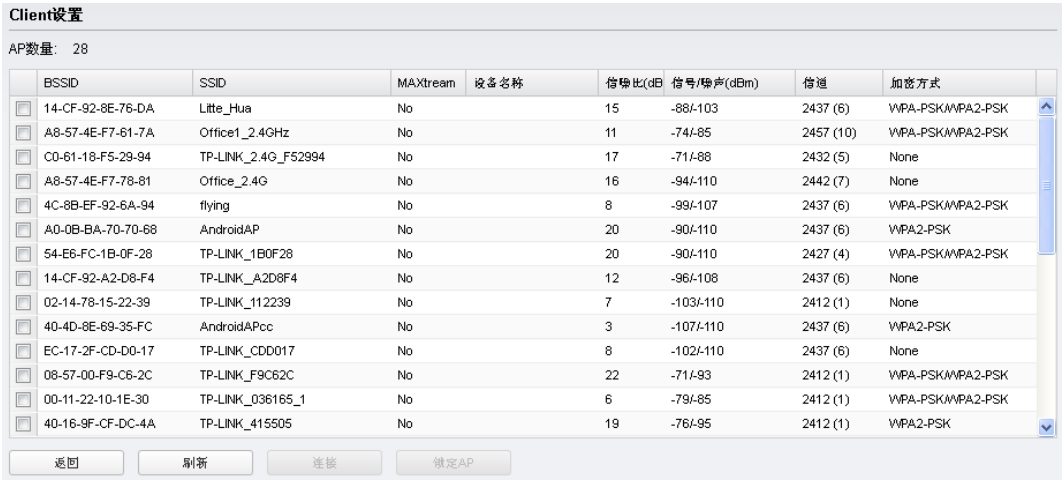
1. 进入**快速设置**页面，工作模式选择 Repeater，然后点击<下一步>按钮：

2. 进入 **LAN 设置**页面，将 IP 地址设置为与前端设备处在同一网段，再输入子网掩码，然后点击<下一步>按钮。



3. 进入 **Client 设置**页面，填写 Client 相关参数。

单击<扫描>按钮将出现可用的AP列表，如下图所示。选择一个目标AP，然后点击<连接>按钮，页面将自动返回到上图所示页面。建议启用“MAC地址锁定AP”功能，从而唯一确定需要关联的远程AP。“无线模式”、“信道带宽”、“加密方式”和“PSK密钥”请与接入的远程AP保持一致。“距离设置”则填写设备与远程AP的距离（如果您无法精确测量该距离，建议输入一个比实际距离稍微偏大的数值）。完成Client设置后点击<下一步>按钮。

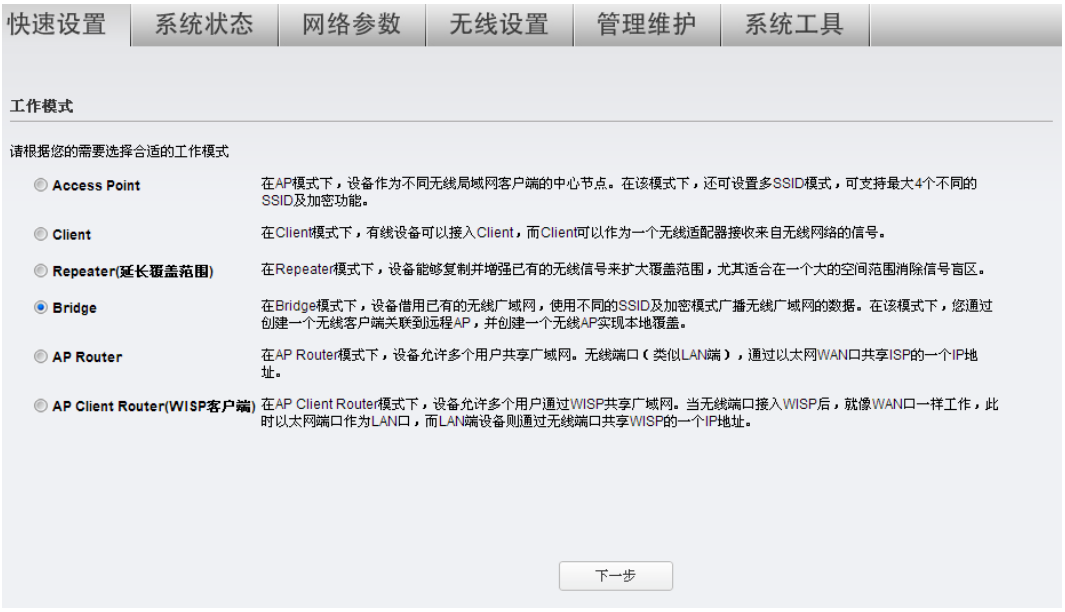


4. 完成上述步骤后，您将会看到**完成**页面，如下图所示。请检查您所配置的参数，如有错误，请点击<返回>重新设置。若配置确认无误，请点击<完成>按钮使配置生效。

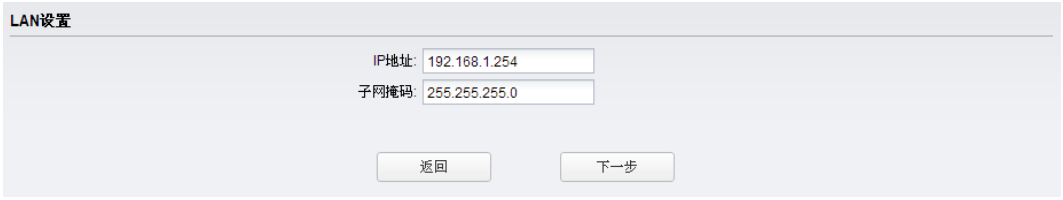
4.4 Bridge模式

Bridge 模式的配置步骤如下：

1. 进入**快速设置**页面，工作模式选择 Bridge，再点击<下一步>按钮：



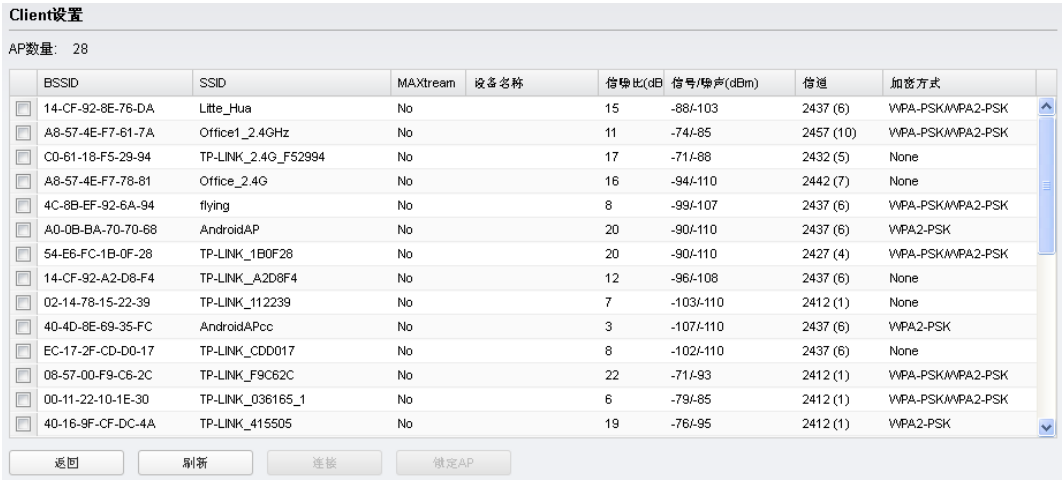
2. 进入 **LAN 设置**页面，将 IP 地址设置为与前端设备处在同一网段，再输入子网掩码，然后点击<下一步>按钮。



3. 进入 **Client 设置**页面，填写 Client 相关参数。

单击<扫描>按钮将出现可用的AP列表，如下图所示。选择一个目标AP，然后点击<连接>按钮，页面将自动返回到上图所示页面。建议启用“MAC地址锁定AP”功能，从而唯一确定需要关联的远程AP。“无线模式”、“信道带宽”、“加密方式”和“PSK密钥”请与接入的远程AP保持一

致。“距离设置”则填写设备与远程AP的距离（如果您无法精确测量该距离，建议输入一个比实际距离稍微偏大的数值）。完成Client设置后点击<下一步>按钮。



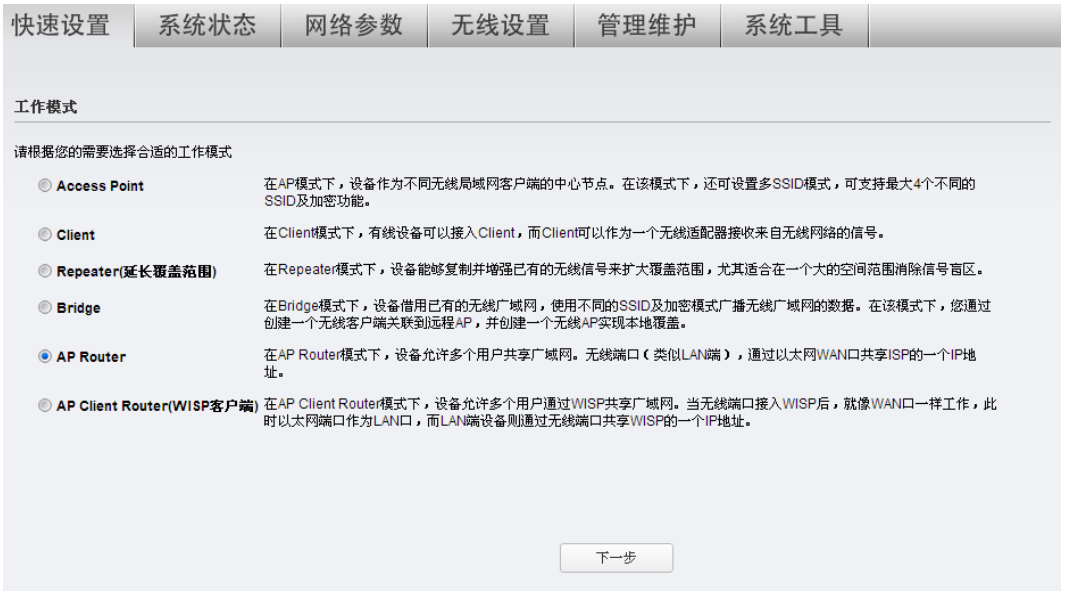
4. 进入 **AP 设置**页面，设置 AP 相关参数和加密信息。建议“加密方式”选择 WPA-PSK / WPA2-PSK 并在“PSK 密钥”一栏设置无线网络的密码，要求为 8-63 个 ASCII 字符（包含数字、英文字母及特殊符号，英文字母注意区分大小写）或者 64 个十六进制字符（包含 0-9、A-F 及 a-f，英文字母不区分大小写）。完成 AP 参数设置后点击<下一步>按钮。

5. 完成上述步骤后，您将会看到**完成**页面，如下图所示。请检查您所配置的参数，如有错误，请点击<返回>重新设置。若配置确认无误，请点击<完成>按钮使配置生效。

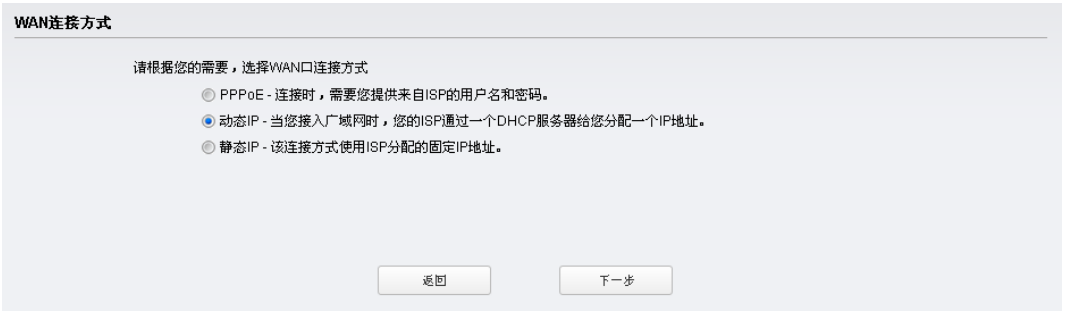
4.5 AP Router模式

AP Router 模式的配置步骤如下：

1. 进入**快速设置**页面，工作模式选择 AP Router，然后点击<下一步>按钮：



2. 进入 **WAN 连接方式**页面选择 WAN 口连接方式。



PPPoE、动态IP和静态IP为最常用的三种连接方式，请根据ISP提供的上网方式进行选择，然后点击<下一步>按钮填写ISP提供的网络参数。

- PPPoE（ADSL虚拟拨号）

如果您的上网方式为PPPoE，即ADSL虚拟拨号方式，ISP会给您提供上网帐号和口令，在下图所示页面中输入ISP提供的ADSL上网帐户用户名和密码，然后点击<下一步>按钮进入步骤3。

➢ 动态IP（以太网宽带，自动从ISP获取IP地址）

如果您的上网方式为动态IP，您可以自动从ISP获取IP地址，无需做任何设置，直接点击<下一步>按钮进入步骤3。

➢ 静态IP（以太网宽带，ISP提供固定IP地址）

如果您的上网方式为静态IP， ISP会给您提供IP地址参数，在下图所示页面中输入ISP提供的参数，如有不明白的地方请咨询ISP。WAN参数设置完成后点击<下一步>按钮进入步骤3。

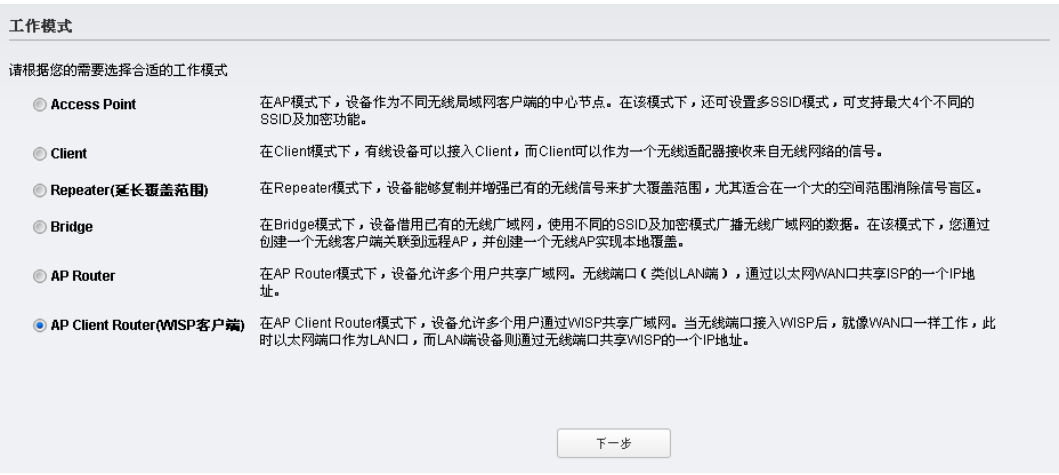
3. 进入 **AP 设置**页面，设置 AP 模式基本参数。建议“加密方式”选择 WPA-PSK / WPA2-PSK 并在“PSK 密钥”一栏设置无线网络的密码，要求为 8-63 个 ASCII 字符（包含数字、英文字母及特殊符号，英文字母注意区分大小写）或者 64 个十六进制字符（包含 0-9、A-F 及 a-f，英文字母不区分大小写）；“距离设置”请输入最远的客户端与本设备之间的距离（如果您无法精确测量该距离，建议输入一个比实际距离稍微偏大的数值）；如果接入本设备的无线网络的客户端设备均为 TP-LINK 室外无线基站和 CPE 系列产品，建议启用 MAXtream 功能以提高无线传输性能。完成 AP 参数设置后点击<下一步>按钮。

4. 完成上述步骤后，您将会看到**完成**页面，如下图所示。请检查您所配置的参数，如有错误，请点击<返回>重新设置。若配置确认无误，请点击<完成>按钮使配置生效。

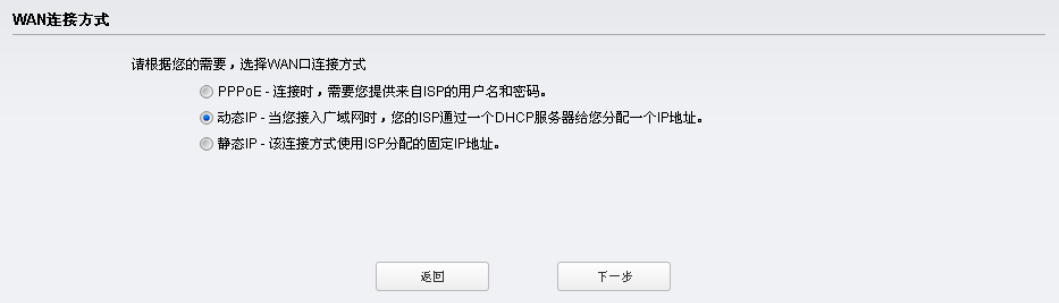
4.6 AP Client Router模式

AP Client Router 模式的配置步骤如下：

1. 进入**快速设置**页面，工作模式选择 AP Client Router，再点击<下一步>按钮：



2. 进入 **WAN 连接方式**页面选择 WAN 口连接方式。



PPPoE、动态IP和静态IP为最常用的三种连接方式，请根据ISP提供的上网方式进行选择，然后点击<下一步>按钮填写ISP提供的网络参数。

➢ PPPoE（ADSL虚拟拨号）

如果您的上网方式为PPPoE，即ADSL虚拟拨号方式，ISP会给您提供上网帐号和口令，在下图所示页面中输入ISP提供的ADSL上网帐户用户名和密码，然后点击<下一步>按钮进入步骤3。

➢ 动态IP（以太网宽带，自动从ISP获取IP地址）

如果您的上网方式为动态IP，您可以自动从ISP获取IP地址，无需做任何设置，直接点击<下一步>按钮进入步骤3。

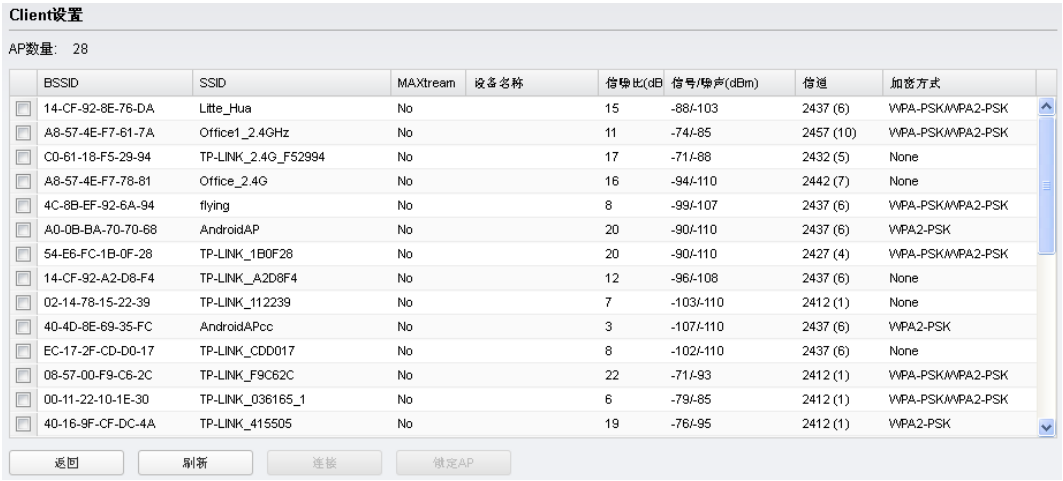
➢ 静态IP（以太网宽带，ISP提供固定IP地址）

如果您的上网方式为静态IP， ISP会给您提供IP地址参数，在下图所示页面中输入ISP提供的参数，如有不明白的地方请咨询ISP。WAN参数设置完成后点击<下一步>按钮进入步骤3。

3. 进入 **Client 设置**页面，填写 Client 相关参数。

单击<扫描>按钮将出现可用的AP列表，如下图所示。选择一个目标AP，然后点击<连接>按钮，页面将自动返回到上图所示页面。建议启用“MAC地址锁定AP”功能，从而唯一确定需要关联的远程AP。“无线模式”、“信道带宽”、“加密方式”和“PSK密钥”请与接入的远程AP保持一

致。“距离设置”则填写设备与远程AP的距离（如果您无法精确测量该距离，建议输入一个比实际距离稍微偏大的数值）。完成Client设置后点击<下一步>按钮。



4. 进入 **AP 设置**页面，设置 AP 模式基本参数。建议“加密方式”选择 WPA-PSK / WPA2-PSK 并在“PSK 密钥”一栏设置无线网络的密码，要求为 8-63 个 ASCII 字符（包含数字、英文字母及特殊符号，英文字母注意区分大小写）或者 64 个十六进制字符（包含 0-9、A-F 及 a-f，英文字母不区分大小写）。完成 AP 参数设置后点击<下一步>按钮。

5. 完成上述步骤后，您将会看到**完成**页面，如下图所示。请检查您所配置的参数，如有错误，请点击<返回>重新设置。若配置确认无误，请点击<完成>按钮使配置生效。

第5章 系统状态

系统状态页面显示了设备的系统信息、参数设置以及当前的运行状态。如图 5-1 所示。

图 5-1 系统状态

5.1 设备信息

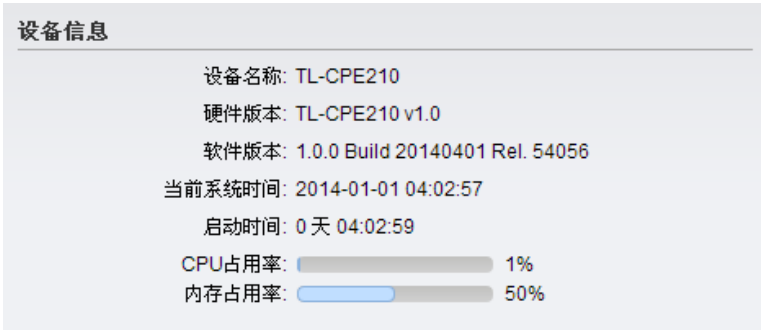


图 5-2 设备信息

设备名称：	显示当前设备的名称，如需自定义设备名称，请参考 9.1 设备。
硬件版本：	显示当前设备的硬件版本。
软件版本：	显示当前设备的软件版本，如需升级软件，请参考 9.5 软件升级。
当前系统时间：	显示设备的当前系统时间，如需更改系统时间，请参考 9.4 时间设置。
启动时间：	显示设备从本次启动后到当前的时长。
CPU占用率：	显示系统当前的 CPU 占用率。您可以通过该参数值来简单判断设备当前是否运行正常。
内存占用率：	显示系统当前的内存占用率。您可以通过该参数值来简单判断设备当前是否运行正常。

5.2 无线设置

图 5-3 无线设置

MAXtream：	显示是否已启用 MAXtream 功能。MAXtream 是 TP-LINK 自主研发的基于时分多路访问（TDMA）的无线信号传输技术，目标是在多站点接入的环境下，最大化吞吐量和最小化延迟时间。启用 MAXtream 同时还能解决“隐藏节点”问题。如果接入本设备的无线网络的客户端设备均为 TP-LINK 室外无线基站和 CPE 系列产品，建议启用 MAXtream 功能以提高无线传输性能。
区域：	显示您为当前设备配置的区域。
信道/频率：	显示设备当前使用的信道和频率，如需更改，请参考 7.1 基本设置。
信道带宽：	显示设备当前使用的信道带宽，如需更改，请参考 7.1 基本设置。
无线模式：	显示设备的无线模式，如需更改，请参考 7.1 基本设置。
最大发送速率：	显示设备的最大无线发送速率。
发射功率：	显示设备当前的发射功率，如需更改，请参考 7.1 基本设置。
传输距离：	显示设备与对端设备的距离，如需更改，请参考 7.6 无线高级设置。

5.3 无线信号质量

当设备工作在 Client、Repeater、Bridge 和 AP Client Router 模式下时，该区域显示的参数为设备接收到的无线信号状态参数；其余工作模式下该区域参数不适用，没有意义。

图 5-4 无线设置

信号强度：	显示设备当前接收到的前端 AP 的信号强度。
噪声强度：	显示设备当前接收到的无线电噪声。
信噪比：	显示设备当前接收到的有用信号和噪声之间的功率比。信噪比数值越大，说明当前系统通信质量越高。
CCQ（客户端链接质量）：	显示当前客户端链接质量。CCQ（客户端链接质量）是指当前有效传输带宽与理论上最大可用带宽的比值。CCQ 以百分比的形式反映了实际链路情况的好坏。

5.4 LAN

图 5-5 LAN

MAC地址：	显示设备的 MAC 地址。
IP地址：	显示 LAN 口的 IP 地址。
子网掩码：	显示 LAN 口的子网掩码。
端口0/端口1：	显示端口的连接状态和最大传输速率。

5.5 WAN

当设备工作在 AP Router 和 AP Client Router 模式下时，该区域显示的参数为设备 WAN 口的参数；其余工作模式下该区域所有的参数显示为 N/A，表示不适用。

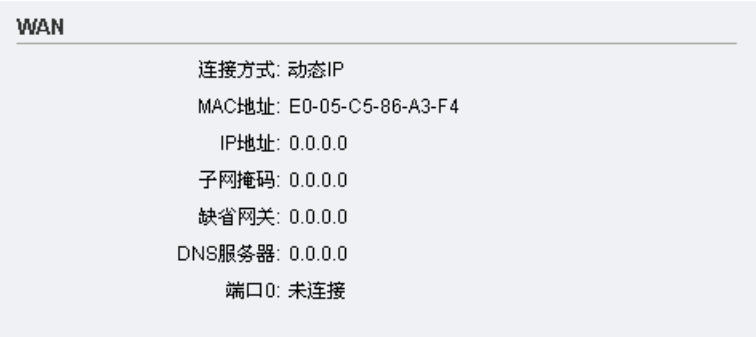


图 5-6 WAN

连接方式：	显示设备 WAN 口连接到因特网的方式。
MAC地址：	显示设备 WAN 口的 MAC 地址。
IP地址：	显示 WAN 口的 IP 地址。
子网掩码：	显示 WAN 口的子网掩码。
缺省网关：	显示 WAN 口的缺省网关地址。
DNS服务器：	显示 WAN 口的 DNS 服务器地址。

5.6 射频状态

图 5-7 射频状态

AP：	显示是否已启用 AP 功能。AP 功能的启用情况取决于设备的工作模式。一般情况下，Client 模式下 AP 为禁用状态，其余模式为启用状态。
MAC地址：	显示设备的 MAC 地址。
SSID：	显示设备的无线网络名称。
认证类型：	显示设备的无线网络的加密方式。
已接入的站点：	显示接入该 AP 的客户端数量。
Client：	显示是否已启用 Client 功能。Client 功能的启用情况取决于设备的工作模式。一般情况下，Client、Repeater、Bridger 和 AP Client Router 模式下 Client 为启用状态，其余模式为禁用状态。
MAC地址：	显示设备的 MAC 地址。
认证类型：	显示所接入的无线网络的加密方式。
WDS：	显示设备对 WDS 四地址数据帧的支持状态。
前端AP的BSSID：	显示前端 AP 的 BSSID，通常为前端 AP 的 MAC 地址。
前端AP的SSID：	显示前端 AP 的 SSID。

发送速率：	显示设备发送数据包的速率。
接收速率：	显示设备接收数据包的速率。
接入时间：	显示设备从本次接入前端 AP 到当前的时长。

5.7 监控

监控区可监控设备当前的吞吐量、无线客户端、接口、ARP表、路由表、DHCP客户端状态和动态WAN等，从而了解当前网络的整体状况。

状态监控条目切换方法：点击监控区上方的蓝色选择区域，带下划线的条目为当前的监控条目。

➢ 吞吐量

监控设备各个接口的吞吐量以了解设备的运行情况。点击监控图上方的下拉菜单，可选择监控的接口，不同的工作模式下提供的接口不尽相同，请根据实际情况进行监控。

图 5-8 监控吞吐量

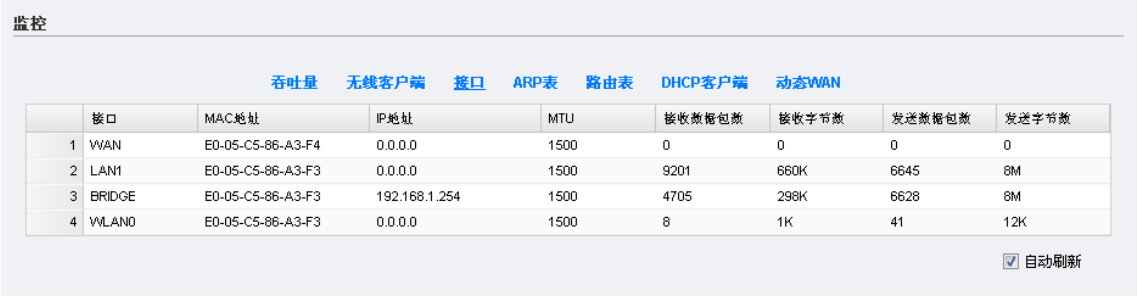
➢ 无线客户端

对于启用 AP 功能的几种模式（Access Point、Bridge、AP Router 和 AP Client Router 模式），可以通过监控无线客户端，查看关联到本设备的站点。

图 5-9 监控无线客户端

➢ 接口

监控各个接口的地址信息和数据传输速率等情况。



	接口	MAC地址	IP地址	MTU	接收数据包数	接收字节数	发送数据包数	发送字节数
1	WAN	E0-05-C5-86-A3-F4	0.0.0.0	1500	0	0	0	0
2	LAN1	E0-05-C5-86-A3-F3	0.0.0.0	1500	9201	660K	6645	8M
3	BRIDGE	E0-05-C5-86-A3-F3	192.168.1.254	1500	4705	298K	6628	8M
4	WLAN0	E0-05-C5-86-A3-F3	0.0.0.0	1500	8	1K	41	12K

图 5-10 监控接口

➢ ARP表

监控设备的 ARP 表。

	IP地址	MAC地址	接口
1	192.168.1.100	0C-37-DC-E5-99-02	BRIDGE
2	192.168.1.5	90-2B-34-63-59-CA	BRIDGE

图 5-11 监控ARP表

➢ 路由表

监控设备的路由表。

	目的IP地址	网关	子网掩码	接口
1	192.168.1.0	0.0.0.0	255.255.255.0	BRIDGE

图 5-12 监控路由表

➢ DHCP客户端

若设备开启了 DHCP 服务器功能，可在此处查看接入该设备的 DHCP 客户端。

	客户端名称	MAC地址	分配的IP地址	地址租期
1	android-7291290f4e631c30	0C-37-DC-E5-99-02	192.168.1.100	0 days 01:57:49

图 5-13 监控DHCP客户端

➢ 动态WAN

此监控条目仅在设备工作模式为 AP Router 或者 AP Client Route 时出现。当设备工作在 AP Router 或者 AP Client Router 模式下，且 WAN 连接方式为 PPPoE/L2TP/PPTP 或动态 IP 时，可在此处监控本设备分配到的 IP 参数。(图 5-14 以 WAN 连接方式为动态 IP 为例)

图 5-14 监控动态WAN

第6章 网络参数

网络参数页面主要用于配置设备的网络相关参数，不同工作模式下需要配置的条目有所不同，请根据设备的工作模式有选择性地查看本章节内容。

图 6-1 网络参数

6.1 WAN设置

WAN 设置仅在 AP Router 和 AP Client Router 模式下适用。不同的连接方式下，需要配置的参数有所不同，下面将介绍各种连接方式下的参数设置方法。

➢ 静态IP

若 ISP 提供了固定的 IP 地址参数，请选择此模式。该模式下，您需要手动输入 ISP 提供的基本网络参数，包括 IP 地址、子网掩码、网关、首选 DNS 服务器等。若不清楚，请咨询 ISP。

图 6-2 静态IP设置

IP地址：	输入 ISP 提供的 IP 地址，必填项。

子网掩码：	输入 ISP 提供的子网掩码，必填项。
网关：	输入 ISP 提供的网关参数，必填项。
首选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。
数据包MTU：	填入网络数据包的 MTU 值（最大传输单元），缺省为 1500。请向 ISP 咨询是否需要更改。如非特别需要，请保持默认值不变。
WAN口MAC地址：	可在此处设置 WAN 口的 MAC 地址。如果您的 ISP 将 IP 地址与您的主机或者之前的路由器的 MAC 地址进行了绑定，您可以在此处输入被绑定的 MAC 地址作为 WAN 口 MAC 地址。点击<恢复出厂 MAC 地址>按钮可将 WAN 口 MAC 地址恢复为出厂 MAC 地址；点击<克隆管理主机 MAC 地址>按钮可将设备的 WAN 口 MAC 地址设置为管理主机的 MAC 地址。
管理主机的MAC地址：	显示管理主机的 MAC 地址。

设置完成后，点击<确定>按钮使其生效。

➢ 动态IP

当设备连接到 DHCP 服务器，或者您的 ISP 提供 DHCP 连接时，请选择此模式。该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。

图 6-3 动态IP设置

数据包MTU：	填入网络数据包的 MTU 值（最大传输单元），缺省为 1500。请向 ISP 咨询是否需要更改。如非特别需要，请保持默认值不变。
手动设置DNS服务器：	动态 IP 模式下，系统会从 ISP 处自动获取 DNS 服务器地址。当需要使用已有的 DNS 服务器时，勾选“启用”可手动设置 DNS 服务器。勾选后请在下方输入首选 DNS 服务器和备用 DNS 服务器的 IP 地址，系统将优先连接手动设置的 DNS 服务器。

WAN口MAC地址：	可在此处设置 WAN 口的 MAC 地址。点击<恢复出厂 MAC 地址>按钮可将 WAN 口 MAC 地址恢复为出厂 MAC 地址；点击<克隆管理主机 MAC 地址>按钮可将设备的 WAN 口 MAC 地址设置为管理主机的 MAC 地址。
管理主机的MAC地址：	显示管理主机的 MAC 地址。

设置完成后，点击<确定>按钮使其生效。

➢ PPPoE

若您是利用 ADSL 来拨号上网，请选择此模式。该模式下您需要填入 ISP 提供的用户名和密码，并设置连接模式。若不清楚，请咨询 ISP。

图 6-4 PPPoE设置

用户名：	请正确输入 ISP 提供的上网帐户用户名，必填项。
密码：	请正确输入 ISP 提供的上网帐户密码，必填项。

连接模式：	请选择连接模式。 • 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；当在设定时间内（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。选用此模式后需要设置自动断线等待时间，默认为 15 分钟。对于采用按使用时间进行缴费的用户，选择按需连接可以有效节省上网费用。 • 自动连接：开机后系统将自动连接网络。在使用过程中，如果由于外部原因网络被断开，系统会主动尝试连接，直到连接成功。若网络服务是包月缴费方式，推荐选择该项连接方式。 • 定时连接：系统在连接时段的起始时刻主动进行网络连接，在结束时刻自动断开网络连接。选用此模式后需要设置起始时间和结束时间。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 PC 中手动拨号连接。若在指定时间（自动断线等待时间）内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。
数据包MTU：	填入网络数据包的 MTU 值（最大传输单元），缺省为 1480。请向 ISP 咨询是否需要更改。如非特别需要，请保持默认值不变。
服务名称/AC名称：	如果 ISP 未提供该项，则不必填写。
在线检测间隔：	设置该值后，本设备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。
使用ISP指定的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。
手动设置DNS服务器：	该模式下，系统会从 ISP 处自动获取 DNS 服务器地址。当需要使用已有的 DNS 服务器时，勾选“启用”可手动设置 DNS 服务器。勾选后请在下方输入首选 DNS 服务器和备用 DNS 服务器的 IP 地址，系统将优先连接手动设置的 DNS 服务器。
WAN口MAC地址：	可在此处设置 WAN 口的 MAC 地址。点击<恢复出厂 MAC 地址>按钮可将 WAN 口 MAC 地址恢复为出厂 MAC 地址；点击<克隆管理主机 MAC 地址>按钮可将设备的 WAN 口 MAC 地址设置为管理主机的 MAC 地址。
管理主机的MAC地址：	显示管理主机的 MAC 地址。

设置完成后，点击<确定>按钮使其生效。

➢ L2TP/PPTP

若 ISP 提供的上网方式为 L2TP 或者 PPTP，ISP 会提供服务器 IP/域名、用户名和密码，您还可以设置连接模式和备用连接方式。若不清楚，请咨询 ISP。

图 6-5 L2TP设置

服务器IP/域名：	请正确输入 ISP 提供的服务器 IP 地址或者域名。
用户名：	请正确输入 ISP 提供的上网帐户用户名，必填项。
密码：	请正确输入 ISP 提供的上网帐户密码，必填项。
连接模式：	请选择连接模式。 • 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；当在设定时间内（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。选用此模式后需要设置自动断线等待时间，默认为 15 分钟。对于采用按使用时间进行缴费的用户，选择按需连接可以有效节省上网费用。 • 自动连接：开机后系统将自动连接网络。在使用过程中，如果由于外部原因网络被断开，系统会主动尝试连接，直到连接成功。若网络服务是包月缴费方式，推荐选择该项连接方式。 • 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，选择手动连接可有效节省上网费用。
备用连接：	请选择备用的连接方式，可选项有“静态 IP”和“动态 IP”，相关连接方式的配置方法请对应参考静态 IP 和动态 IP。
数据包MTU：	填入网络数据包的 MTU 值（最大传输单元），L2TP 缺省为 1480，PPTP 缺省为 1420。请向 ISP 咨询是否需要更改。如非特别需要，请保持默认值不变。
WAN口MAC地址：	可在此处设置 WAN 口的 MAC 地址。点击<恢复出厂 MAC 地址>按钮可将 WAN 口 MAC 地址恢复为出厂 MAC 地址；点击<克隆管理主机 MAC 地址>按钮可将设备的 WAN 口 MAC 地址设置为管理主机的 MAC 地址。
管理主机的MAC地址：	显示管理主机的 MAC 地址。

设置完成后，点击<确定>按钮使其生效。

6.2 LAN设置

LAN设置区用于配置设备的LAN参数。

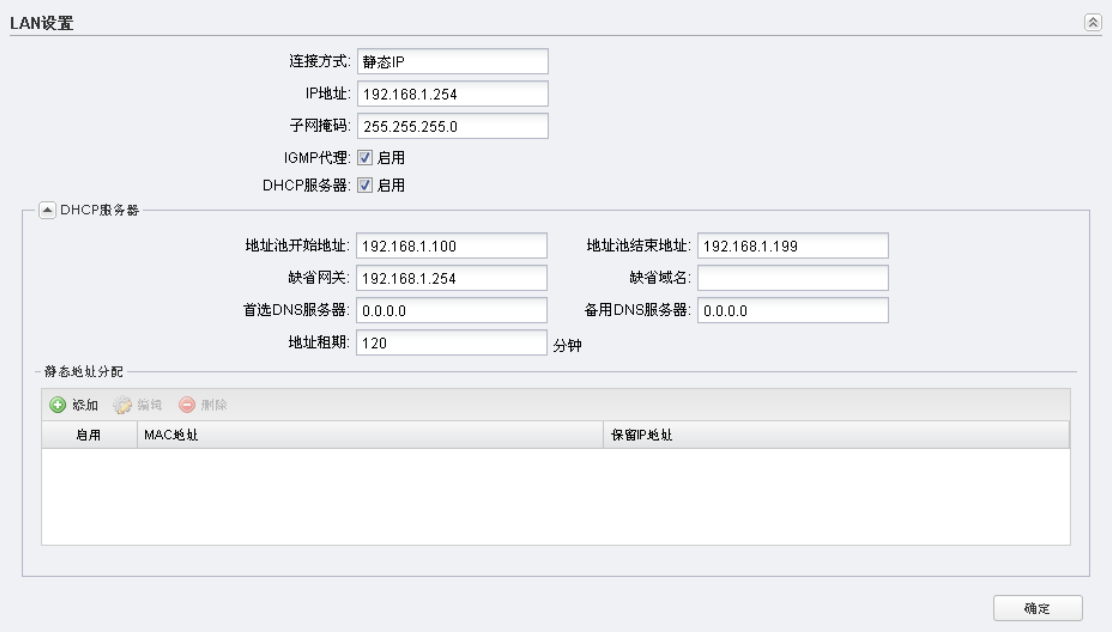


图 6-6 LAN设置

连接方式：	选择与前端 AP 或路由器的连接方式。 • 静态 IP：需填写一个固定的 IP 地址以接入前端网络设备。 • 动态 IP：由前端的 DHCP 服务器分配 IP 地址。AP Router 和 AP Client Router 模式不支持该连接方式。
IP地址：	若连接方式选择静态 IP，请在此处输入一个固定的 IP 地址。注意与前端网络设备保持在同一网段且保证不会与其他接入该网络的终端产生 IP 冲突。
子网掩码：	若连接方式选择静态 IP，请在此处输入设备的子网掩码。
回退IP：	若连接方式选择动态 IP，您可以启用回退 IP 功能。启用该功能后，如果设备无法连接 DHCP 服务器，则自动使用该回退 IP 作为 LAN 口 IP 地址。
回退IP地址：	指定回退 IP 的 IP 地址。
回退子网掩码：	指定回退 IP 的子网掩码。
IGMP代理：	IGMP(Internet Group Management Protocol，Internet 组管理协议)常用于 IPTV 组播数据。本设备支持可开关的 IGMP 代理功能和 IGMP 侦听功能。仅 AP Router 和 AP Client Router 模式支持该功能。

DHCP 服务器：	DHCP（Dynamic Host Configuration Protocol 动态主机控制协议）。启用 DHCP 服务器功能后，本设备能够为接入设备自动分配 IP 参数。
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 服务器分配给接入设备的 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。
缺省网关：	可选项。应填入本设备的 LAN 口的 IP 地址。
缺省域名：	可选项。应填入本地网域名，缺省为空。
首选DNS服务器：	可选项。可以填入 ISP 提供的 DNS 服务器或保持缺省，若不清楚请咨询 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。
地址租期：	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。
静态地址分配：	可以为内网中指定 MAC 地址的计算机保留 IP 地址，当该计算机请求 DHCP 服务器分配 IP 地址时，DHCP 服务器将为它分配保留的 IP 地址。点击<添加>按钮，再输入指定计算机的 MAC 地址和保留的 IP 地址即可。 

设置完成后，点击<确定>按钮使其生效。

6.3 转发规则

转发规则仅在 AP Router 和 AP Client Router 模式下适用。

我们在因特网上使用的 IP 地址为公网地址，而在局域网内一般使用私网地址。使用私网地址的主机不能直接访问因特网，而在因特网上也不能直接访问使用私网地址的主机。

私网主机访问因特网是由路由设备的 NAT（Network Address Translation，网络地址转换）技术实现的。NAT 可以将私网地址转换为公网地址，从而使需要与外部通讯的私网用户顺利访问因特网。NAT 是路由设备的基本功能，无需额外设置。

外部网络主动访问局域网主机，则可以通过设置 DMZ 主机、虚拟服务器等转发规则来实现。

图 6-7 静态IP设置

DMZ主机：

勾选“启用”后可开启 DMZ 主机。

DMZ（Demilitarized Zone，非军事区域，也叫隔离区）是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。局域网中设置 DMZ 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。

如下图所示，将出现“DMZ 主机 IP”填写项。请在此处输入 DMZ 主机的 IP 地址。注意被设置为 DMZ 主机的计算机应使用静态 IP 地址。

应用层网关：

可以勾选启用对应的应用层网关（ALG），推荐开启应用层网关。

普通 NAT 只能对报文的网络层首部和传输层首部进行地址转换，对报文的应用层字段则无能为力。应用层网关可以处理报文的应用层字段，在路由设备上把应用层字段中的私网 IP 信息修改为公网 IP 信息。本设备 ALG 支持的应用协议有：FTP、TFTP、H323 和 RTSP。

- FTP ALG：允许 FTP（File Transfer Protocol，文件传输协议）客户端和服务器穿透 NAT 传输数据；
- TFTP ALG：允许 TFTP（Trivial File Transfer Protocol,简单文件传输协议）客户端和服务器穿透 NAT 传输数据；
- H323 ALG：允许微软 IP 电话、视频会议等聊天客户端穿透 NAT 进行通信。
- RTSP ALG：允许一些媒体播放器客户端穿透 NAT 与流媒体服务器进行通信。

虚拟服务器：

勾选“启用”后可开启虚拟服务器功能。

为保证局域网的安全，默认情况下，路由设备会将局域网主机的 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。通过将路由设备配置为虚拟服务器，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。

“虚拟服务器”定义了本设备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。

如下图所示，勾选“启用”后将出现虚拟服务器的参数设置项，点击<添加>按钮并填写相关参数即可添加虚拟服务器条目。

虚拟服务器（续）：

- IP 地址：输入局域网服务器的静态 IP 地址。通过此 IP 地址，路由设备会将对服务端口的访问请求转到局域网服务器上。
- 内部端口： 指定局域网内虚拟服务器主机的实际服务端口，取值范围为 1-65535 之间的任意整数。
- 服务端口：设置路由设备向因特网开放的服务端口，取值范围为 1-65535 之间的任意整数。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”。
- 协议：选择此虚拟服务所采用的协议，可选项有 TCP、UDP 和 TCP/UDP。若对采用的协议不清楚，推荐选择 TCP/UDP。

勾选“启用”后可开启特殊应用程序功能。

由于防火墙的存在，一些如网络游戏、视频会议、网络电话、P2P 下载等应用程序需要通过设置转发规则才能正常工作，而这些应用程序又要求多个端口连接，针对单一端口的虚拟服务器功能已不能满足需求，此时就需要使用端口触发功能。当一个应用程序向触发端口发起连接时，对应开放端口中的所有端口就会打开，以备后续连接。

如下图所示，勾选“启用”后将出现特殊应用程序的参数设置项，点击<添加>按钮并填写相关参数即可添加特殊应用程序条目。

特殊应用程序：

- 开放端口：为应用程序提供服务的一个或多个端口，取值范围 1-65535。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，如“8600，8690-8696”。当触发端口上发起连接后，开放端口打开，之后应用程序便可以通过这些开放端口发起后续连接。
- 触发端口： 应用程序首先发起连接的端口，取值范围 1-65535。只有触发端口发起连接时，对应开放端口中的所有端口才可以开放，并为应用程序提供服务，否则开放端口中的所有端口是不会开放的。
- 协议： 设定在触发端口上使用的数据包协议类型。

勾选“启用”后可开启 UPnP。

UPnP（Universal Plug and Play，通用即插即用），是一组协议的统称。遵循该协议的不同设备或应用程序（如 BitComet 下载工具、MSN 等）可以自动发现对方并建立通信。

使用 UPnP 功能的前提：

1. 路由设备支持并开启 UPnP；
2. 操作系统支持 UPnP（可安装 UPnP 组件）；
3. 需要访问的设备或应用程序支持 UPnP。

满足以上条件后，局域网中的主机就可以根据软件的需要自动地在本设备上打开相应的端口，使得外部主机上的应用程序在需要时能够通过打开的端口访问内部主机上的资源，这样原本受限于 NAT 的功能便可以正常使用。

UPnP：

相对于虚拟服务器和特殊应用程序等转发规则而言，UPnP 的应用不需要用户手动设置任何规则，对于一些端口不固定的应用会更加方便。

如下图所示，启用 UPnP 功能后，可以在本页面查看当前的 UPnP 信息。

- 应用描述：显示对发起 UPnP 请求的应用程序的描述。
- 外部端口： 显示本设备为该应用程序开启的外部端口。
- 内部端口：显示本设备为该应用程序开启的内部端口。
- 协议：显示进行端口转换时采用的协议。
- IP 地址：发起 UPnP 请求的本地主机的 IP 地址。
- 状态：显示该端口状态。“启用”表明该端口被激活，“禁用”则表明端口被禁用。

设置完成后，点击<确定>按钮使其生效。

注意：

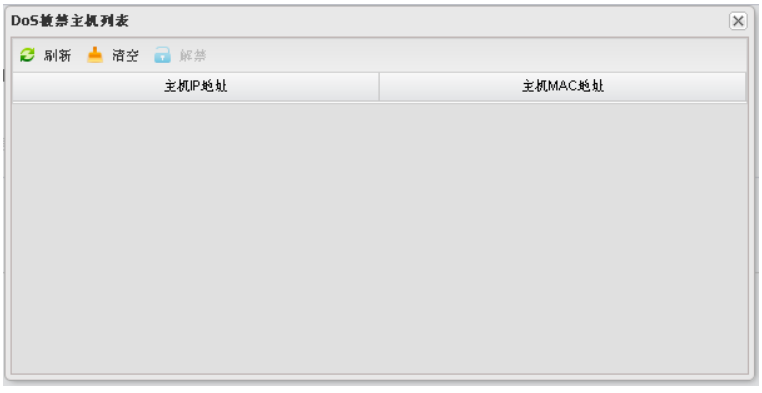
一些木马、病毒可能会利用 UPnP 服务打开特定的端口，使局域网主机成为黑客的攻击目标，因此需谨慎应用 UPnP 服务。

6.4 安全设置

安全设置功能仅在 AP Router 和 AP Client Router 模式下适用，主要用于开启防火墙、Ping 防护、VPN 穿透及 DoS 攻击防范等功能，防止广域网对本设备及局域网内主机进行攻击。

图 6-8 安全设置

防火墙：	可以勾选以开启 SPI 防火墙。 SPI 防火墙开启时会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 防火墙默认启用，当您希望 LAN 端的所有主机暴露到广域网中时，可关闭该功能。 如果您启用 SPI 防火墙的同时设置了“DMZ 主机”、“应用层网关”等转发规则，系统将优先满足转发规则功能。
Ping：	可以勾选以开启“防 WAN 口 Ping”或“防 LAN 口 Ping”功能。 • 防 WAN 口 Ping：勾选后，本设备将不会响应来自 WAN 口的 Ping 请求。 • 防 LAN 口 Ping：勾选后，本设备将不会响应来自 LAN 口的 Ping 请求。
VPN穿透：	可以勾选启用对应的 VPN 穿透功能。 VPN （Virtual Private Network，虚拟专用网络）功能是在公用网络上建立专用网络，进行加密通信。VPN 提供了通过广域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)通过本设备连接到远程 VPN 网络，那么应开启相应的 VPN 穿透功能。 • PPTP 穿透：若您采用的 VPN 的隧道协议为 PPTP，请勾选此项。 • L2TP 穿透：若您采用的 VPN 的隧道协议为 L2TP，请勾选此项。 • IPSec 穿透：若您采用的 VPN 的隧道协议为 IPSec，请勾选此项。

DoS攻击防范：	勾选“启用”后可开启 DoS 攻击防范功能。 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 攻击始发自多个源地址，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。
数据包统计时间间隔：	设置对数据包进行统计的时间间隔。
ICMP_FLOOD 攻击过滤：	可以勾选启用 ICMP_FLOOD 攻击过滤功能，勾选后可设置 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由同一主机发出的 ICMP 包达到了设定值，本设备将会立即停止转发来自该主机的 ICMP 包，并将该主机加入 DoS 被禁主机列表中，从而达到防范攻击的目的。
UDP_FLOOD 攻击过滤：	可以勾选启用 UDP_FLOOD 攻击过滤功能，勾选后可设置 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由同一主机发出的 UDP 包达到了设定值，本设备将会立即停止转发来自该主机的 UDP 包，并将该主机加入 DoS 被禁主机列表中，从而达到防范攻击的目的。
TCP_SYN_FLOOD 攻击过滤：	可以勾选启用 TCP_SYN_FLOOD 攻击过滤功能，勾选后可设置 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由同一主机发出的带 SYN 标志的 TCP 包达到了设定值，本设备将会立即停止转发来自该主机的带 SYN 标志的 TCP 包，并将该主机加入 DoS 被禁主机列表中，从而达到防范攻击的目的。
DoS被禁主机列表：	点击该按钮，可以查看因疑似发起 DoS 攻击而被禁止上网的计算机列表，如下图所示。点击<刷新>按钮可以更新列表信息。若被禁止上网的计算机已正常运行，不再对本设备发起攻击，则可以通过点击<解禁>按钮进行解禁；若需要释放所有被禁计算机，请点击<清空>按钮。 

设置完成后，点击<确定>按钮使其生效。

6.5 访问控制

访问控制功能仅在 AP Router 和 AP Client Router 模式下适用。

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。

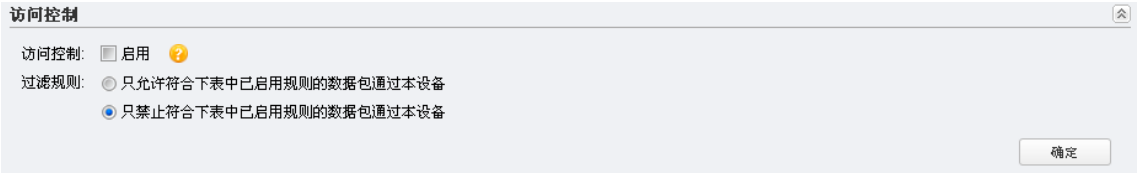


图 6-10 访问控制

访问控制：

可以勾选启用访问控制功能。如下图所示，勾选后将出现规则设置项，点击表格中的<添加>按钮可添加访问控制规则条目。

- 协议： 选择设置规则所依据的协议。
- 主机 IP 地址： 输入需要控制的内网主机的 IP 地址或者 IP 地址段。若为 IP 地址段，输入格式如“192.168.1.5-192.168.1.15”。
- 目的 IP 地址：输入允许或禁止内网主机访问的 IP 地址或者 IP 地址段。若为 IP 地址段，输入格式如“192.168.3.5-192.168.3.15”。
- 目的端口：若选择的协议为 TCP 或 UDP，可以在此处指定目的端口或端口范围。
- 生效时间：从下拉菜单中选择规则每周的生效时间。在下拉菜单中，灰色表示已被选中，若需删除该选项，再点击一次即可。
- 时间：输入规则每天的生效时间段，格式为 HH:MM-HH:MM。

过滤规则： 请在此处选择允许或是禁止符合表格中已启用规则的数据包通过本设备。

设置完成后，点击<确定>按钮使其生效。

6.6 静态路由

静态路由功能仅在 AP Router 和 AP Client Router 模式下适用。

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、子网掩码和下一跳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，然后本设备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。

图 6-11 静态路由

静态路由：

勾选“启用”后可开启静态路由功能。如下图所示，勾选后将出现静态路由设置项，点击表格中的<添加>按钮可添加静态路由条目。

- 目的网络 IP：用来标识希望访问的目标地址或目标网络，此 IP 地址不能和本设备的 WAN 口或 LAN 口 IP 地址处于同一网段。
- 子网掩码：该项与目标网络 IP 一起来标识目标网络。
- 下一跳：数据包被指定发往的下一个节点的 IP 地址，此 IP 地址必须和本设备的 WAN 口 IP 地址处于同一网段。

设置完成后，点击<确定>按钮使其生效。

6.7 带宽控制

带宽功能仅在 AP Router 和 AP Client Router 模式下适用。

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。

说明：

为了使带宽控制达到最佳效果，请先向 ISP 或 WISP 了解线路的上行/下行总带宽。

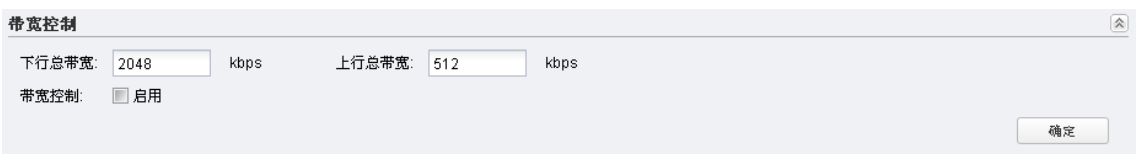


图 6-12 带宽控制

下行总带宽：	输入允许本设备通过 WAN 口提供的最大下载速率，取值范围 1-100000Kbps。此处设置的下行总带宽应小于 ISP 或 WISP 为您提供的下行总带宽。
上行总带宽：	输入允许本设备通过 WAN 口提供的最大上传速率，取值范围 1-100000Kbps。此处设置的上行总带宽应小于 ISP 或 WISP 为您提供的上行总带宽。
带宽控制：	勾选“启用”后可开启带宽控制功能。如下图所示，勾选后将出现带宽控制设置项，点击表格中的<添加>按钮可添加带宽控制条目。  • IP 地址范围：输入内部主机的 IP 地址范围，格式如“192.168.1.5-192.168.1.15”。 • 端口范围：输入内部主机访问外部服务器的端口范围。一般浏览网页的端口为“80”，而登录 QQ 的端口则为 1500 左右。 • 协议：输入传输层采用的协议类型，可选项为 TCP/UDP、TCP 和 UDP，若不清楚，请选择 TCP/UDP。 • 最小下行带宽：设置此 IP 地址范围内的主机接收数据时至少能使用的总带宽。 • 最大下行带宽：设置此 IP 地址范围内的主机接收数据时最多允许占用的总带宽。 • 最小上行带宽：设置此 IP 地址范围内的主机发送数据时至少能使用的总带宽。 • 最大上行带宽：设置此 IP 地址范围内的主机发送数据时最多允许占用的总带宽。

设置完成后，点击<确定>按钮使其生效。

6.8 IP地址与MAC地址绑定

启用 IP 地址与 MAC 地址绑定功能，可有效防止 ARP 攻击和 IP 盗用。

设备在局域网内传输 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，这些对应关系由 ARP 映射表来维护。ARP 攻击可以用伪造的信息更新设备的 ARP 映射表，破坏表中 IP 地址与 MAC 地址的对应关系，使设备无法与相应的主机进行通信。启用 IP 地址与 MAC 地址绑定功能后，绑定列表中的 IP 地址与 MAC 地址映射条目将不会过期或者被新的 ARP 数据更新，从而有效防止 ARP 攻击。

本设备的某些功能，如“访问控制”和“带宽控制”，是通过 IP 地址来识别接入本设备的用户的。在小型网络中， 为方便管理，网络管理员可以为每一位接入的用户分配一个静态 IP，再根据 IP 地

址制定访问控制和带宽控制规则，控制用户的上网行为及占用的带宽。部分用户可能会通过修改 IP 地址以获取更高的上网权限，启用 IP 地址与 MAC 地址绑定功能则可以有效防止 IP 盗用现象。

图 6-13 IP 地址与 MAC 地址绑定

IP 地址与 MAC 地址绑定：

勾选“启用”后可开启 IP 地址与 MAC 地址绑定功能。如下图所示，勾选后将出现绑定设置项，点击表格中的<添加>按钮可添加绑定条目。您也可以通过点击<导入>按钮从系统的 ARP 表中导入条目，导入的条目默认为“禁用”状态，需要手动开启。

- IP 地址：输入需要绑定的主机的 IP 地址。
- MAC 地址：输入需要绑定的主机的 MAC 地址。

设置完成后，点击<确定>按钮使其生效。

第7章 无线设置

无线设置页面主要用于配置设备的无线相关参数，不同工作模式下需要配置的条目有所不同，请根据设备的工作模式有选择性地查看本章节内容。

图 7-1 无线设置

7.1 基本设置

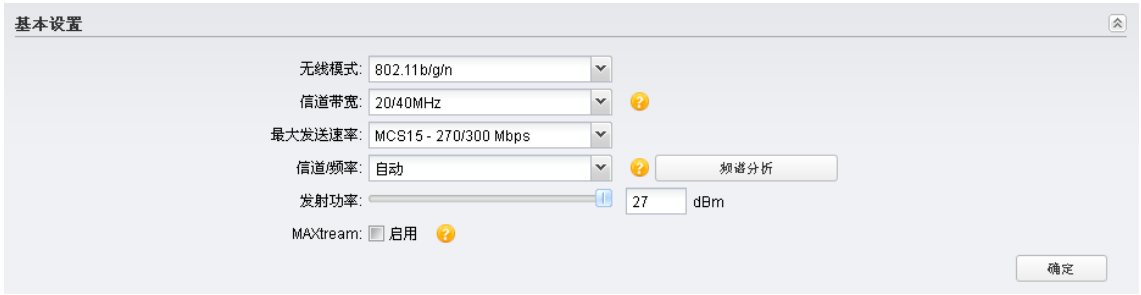


图 7-2 基本设置

无线模式：	选择无线网络采用的协议标准。 TL-CPE210/TL-BS210 为 2.4GHz 设备，支持 802.11b、802.11g、802.11n、802.11b/g 以及 802.11b/g/n 五种无线模式。建议选择 802.11b/g/n 混合模式，这样您的无线网络可以同时允许 11b、11g 和 11n 模式的客户端接入。 TL-CPE510/TL-BS510 为 5GHz 设备，支持 802.11a、802.11n 以及 802.11a/n 混合三种无线模式。建议选择 802.11a/n 混合模式，这样您的无线网络可以同时允许 11a 和 11n 模式的客户端接入。
信道带宽：	选择本设备使用的信道带宽，可选项有：5MHz、10 MHz、20 MHz 以及 20/40 MHz。20/40 MHz 表示优先选择使用 40 MHz，若 40 MHz 不可用则使用 20 MHz。 根据 IEEE 802.11n 标准，使用 40 MHz 的信道带宽能够增加无线吞吐量，但是，用户也可能基于如下原因选择较低的带宽： 1. 在受限的总带宽中，增加可用信道数； 2. 在相同的无线环境下，避免与其他设备占用的重叠信道相冲突； 3. 越低的带宽能够集中越高的发射功率，增加远距离传输中无线链路的稳定性； 4. 在 Client /Bridge /Repeater /AP Client Router 模式下，设备的信道带宽请与前端 AP 保持一致。 推荐使用频谱分析工具来帮助选择信道带宽。频谱分析工具的使用方法请参考 10.5 频谱分析。
最大发送速率：	设置设备的最大发送速率。
信道/频率：	选择设备使用的信道以提高无线性能。1/2412MHz 表示使用信道 1，频率为 2412MHz。推荐使用频谱分析工具来帮助选择信道。频谱分析工具的使用方法请参考 10.5 频谱分析。 TL-CPE210/TL-BS210 为 2.4GHz 设备，支持 1~13 共 13 个信道；TL-CPE510/TL-BS510 为 5GHz 设备，支持 149、153、157、161 和 165 共 5 个信道（信道带宽选择 20/40MHz 时不支持 165 信道）。
发射功率：	设置本设备的无线发射功率。可通过拉动滑动条进行设置，也可在直接输入框中手动输入 0-27 之间任意整数。
MAXtream：	仅在 AP 和 AP Router 模式下有此条目。 MAXtream 是 TP-LINK 自主研发的基于时分多路访问（TDMA）的无线信号传输技术，目标是在多站点接入的环境下，最大化吞吐量和最小化延迟时间。“隐藏节点”问题也能在 MAXtream 启用时被解决。 如果接入本设备的无线网络的客户端设备均为 TP-LINK 室外无线基站和 CPE 系列产品，建议启用 MAXtream 功能以提高无线传输性能。

MAXtream站点模式：	仅在 Client 模式下有此条目。 选择 MAXtream 站点模式，可选项为：自动判别、低延迟优先和高吞吐量优先。 若前端的 AP 设备为 TP-LINK 室外无线基站和 CPE 系列产品且启用了 MAXtream 功能，则本 Client 设备将自动成为其中的 MAXtream 站点。您可以根据您的网络需求选择“低延迟优先”或者“高吞吐量优先”模式，当您不能确定或者没有特殊需求时，请选择“自动判别”。

设置完成后，点击<确定>按钮使其生效。

7.2 Client设置

仅在Client、Repeater、Bridge和AP Client Router模式下适用。

图 7-3 Client 设置

无线射频：	仅在 Client 模式下有此条目。 即无线开关，启用无线射频后设备才能发送和接收无线信号。
远程AP的SSID：	可以手动输入远程 AP 的 SSID；也可以通过点击<扫描>按钮搜索目标无线网络，与其建立连接。
远程AP的MAC地址：	勾选<MAC 地址锁定 AP>后，可以在输入框内填写远程 AP 的 MAC 地址。 当同一区域存在两个或以上 SSID 相同的无线网络时，设备会选择信号最强的 AP 进行关联，启用 MAC 地址锁定 AP 功能则可以唯一确定需要关联的远程 AP。
WDS：	选择设备对 WDS 四地址数据帧的支持状态。 WDS（Wireless Distribution System，无线分布式系统）是 AP 之间通过无线连接实现多个无线局域网间互相通信的系统。在 WDS 技术中，数据帧使用了四个地址域，可以在链路层上做透明转发。WDS 技术需要前端设备支持四地址数据帧的转发，如果前端设备不支持，可以设置本设备使用三地址模式来转发数据帧，此模式下仅支持 ARP/IP/PPPOE 协议的数据帧在 AP 间的转发。 • 启用：使用四地址数据帧。 • 禁用：使用三地址数据帧。 • 自动：系统将自动探测前端设备对三四地址格式数据帧的支持情况，优先选择使用四地址格式。推荐选择此项。

认证类型：	选择本 Client 设备接入前端 AP 的认证类型。应与前端 AP 的认证类型保持一致，才能通过前端 AP 的验证，接入前端 AP 的无线网络。 • 无加密：若前端 AP 的认证类型为无加密，则选择此项。此时无需输入密码等参数。 • WPA-PSK：若前端 AP 的认证类型为 WPA-PSK，则选择此项。选择该选项后，需要输入 WPA 版本、加密方式及 PSK 密钥等参数，请与前端 AP 保持一致。 • WEP：若前端 AP 的认证类型为 WEP，则选择此项。选择该选项后，需要输入验证类型、密钥格式及 PSK 密钥等参数，请与前端 AP 保持一致。

设置完成后，点击<确定>按钮使其生效。

7.3 AP设置

仅在Access Point、AP Router、Bridge和AP Client Router模式下适用。

图 7-4 AP 设置

无线射频：	即无线开关，启用无线射频后，设备才能发发送和接收无线信号。
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。 SSID 默认设置为 TP-LINK_Outdoor_xxxxxx（xxxxxx 是本设备 MAC 地址的最后六位），推荐更改 SSID 以更方便地标识您的无线网络。
开启SSID广播：	勾选“开启 SSID 广播”后，AP 将在无线覆盖区域广播无线网络名称，这样在其覆盖范围内的主机就能搜索到并加入该无线网络。若未开启 SSID 广播，则需要接入该无线网络的主机无法搜索到其无线信号，只能手动输入 SSID 以接入该无线网络。
认证类型：	选择无线网络的安全认证类型。如果不需要对无线网络加密，能够让任意主机接入无线网络，则可以选择“无加密”；如果需要对无线网络加密，请选择界面中三种认证类型中的一种进行无线安全设置。 为保障网络安全，推荐加密无线网络。 本设备提供加密方式有：WPA-PSK、WPA 和 WEP，推荐使用 WPA-PSK 加密方式，不同的加密方式，设置项不同，下面将详细介绍。

设置完成后，点击<确定>按钮使其生效。

认证类型中的 WPA-PSK、WPA 和 WEP 加密方式详细介绍如下：

- WPA-PSK

WPA-PSK 认证类型是基于预共享密钥（Pre-shared key，PSK）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。WPA-PSK 认证类型有 WPA-PSK 和 WPA2-PSK 两个版本。

图 7-5 WPA-PSK

版本：	选择使用的 WPA 的版本，可选项有自动、WPA 和 WPA2。 • 自动：系统会根据主机请求自动选择 WPA-PSK 或 WPA2-PSK 安全模式。 • WPA：系统将采用 WPA-PSK 认证模式。 • WPA2：系统将采用 WPA2-PSK 认证模式。
加密方式：	选择对无线数据进行加密的安全算法，可选项有自动、TKIP、AES。默认选项为自动，选择该项后，系统将根据实际需要自动选择 TKIP 或 AES 加密方式。
PSK密钥：	设置 WPA-PSK/WPA2-PSK 密码，设置时，要求为 8-63 个 ASCII 字符（包含数字、英文字母及常见符号，英文字母注意区分大小写）或者 64 个十六进制字符（包含 0-9、A-F 及 a-f，不区分大小写）。
组密钥更新周期：	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。

- WPA

采用 WPA 认证类型，系统将采用 Radius 服务器进行身份认证并得到密钥的 WPA 或 WPA2 安全模式。WPA 认证类型的安全性非常高，需要架设专用的 Radius 服务器来生成不同的密钥给各个用户，价格比较昂贵维护也比较复杂，适合企业级用户使用。目前有 WPA 和 WPA2 两个版本。

图 7-6 WPA

版本：	选择使用的 WPA 的版本，可选项有自动、WPA 和 WPA2。 • 自动：系统会根据主机请求自动选择 WPA 或 WPA2 安全模式。 • WPA：系统将采用 WPA 认证模式。 • WPA2：系统将采用 WPA2 认证模式。
加密方式：	选择对无线数据进行加密的安全算法，可选项有自动、TKIP、AES。默认选项为自动，选择该项后，系统将根据实际需要自动选择 TKIP 或 AES 加密方式。 **说明：** 802.11n 模式下不支持 TKIP 加密算法，如果在 11n 模式下使用 TKIP 加密算法会导致 Client 设备无法正常接入本设备的无线网络，而在 11b/g/n（2.4GHz 频段）或 11a/n（5GHz 频段）模式下使用 TKIP 加密算法，本设备可能工作在较低的传输速率上。建议选择 AES 或自动选项。
Radius远程认证服务器IP地址/端口：	输入 Radius 服务器的 IP 地址和认证服务采用的端口号。
Radius远程认证服务器密码：	设置访问 Radius 服务器的密码。勾选“显示密码”，页面将显示输入的密码。
组密钥更新周期：	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。

- 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认证类型高。选择 WEP 认证类型，设备将使用 802.11 基本的 WEP 安全模式。

说明：

802.11n 不支持 WEP 加密方式，如果在 11n 模式下使用 WEP 加密方式会导致 Client 设备无法正常接入本设备的无线网络，而在 11b/g/n（2.4GHz 频段）或 11a/n（5GHz 频段）模式下使用 WEP 加密方式，本设备可能工作在较低的传输速率上。

图 7-7 WEP

验证类型：	该项用来选择系统采用的安全模式。 • 自动：选择该项后，设备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：选择该项后，设备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：选择该项后，设备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，也无法进行数据传输。
密钥格式：	该项用来选择即将设置的密钥的形式，包括 Hex（16 进制）和 ASCII 码。 • Hex：密钥字符可包含 0-9、A-F 和 a-f，英文字母不区分大小写。 • ASCII：密钥字符可包含数字、英文字母和特殊符号，注意英文字母区分大小写。
已选密钥：	可以预先配置 4 条密钥，并根据需要选择当前生效的 WEP 密钥。
WEP密钥：	请输入需要设置的密钥。密钥的长度和有效字符范围受密钥类型的影响。如果没有设置任何密钥，无线数据将不进行加密。
密钥类型：	可以选择禁用相应密钥，或者设置 64 位、128 位或 152 位的 WEP 密钥。 • 关闭：不使用该密钥。 • 64 位密钥：需输入 16 进制字符 10 个，或者 ASCII 码字符 5 个。 • 128 位密钥：需输入 16 进制字符 26 个，或者 ASCII 码字符 13 个。 • 152 位密钥：需输入 16 进制字符 32 个，或者 ASCII 码字符 16 个。

7.4 多SSID

仅在 Access Point 模式下适用。

本设备开启多 SSID 功能的同时也将开启其 VLAN 功能，可以和支持 802.1Q VLAN 的交换机一起工作。本设备可同时虚拟 4 个无线网络供用户接入，相应地，本设备可同时支持 4 个 VLAN。

当本设备与交换机协同工作时，对于来自无线客户端的数据包，一般情况下本设备会在数据包头部添加相应的 VLAN 标记，但是如果该无线客户端处在 VLAN1 中，本设备则不会给数据包添加 VLAN 标记。处在不同的 VLAN 中的设备不能直接通信，请在您的交换机上做好相应的 VLAN 设置。

对于直接有线接入到本设备的主机，本设备不会给来自该主机的数据包添加 VLAN 标记，该主机可以跟 VLAN1 中的无线客户端以及其他有线接入到本设备的主机通信。

图 7-8 多 SSID

多SSID：	勾选“启用”后可开启多 SSID 模式。 点击<添加>按钮并填写相关参数即可添加无线网络条目。 • SSID：输入需要添加的无线网络名称，最多可输入 32 位字符。 • VLAN：设置该无线网络所属的 VLAN，取值范围 1-4094。 • SSID 广播：选择是否广播该 SSID。 • AP 隔离：选择是否启用 AP 隔离功能。启用 AP 隔离后，系统将隔离接入到同一个无线网络中的各个无线主机，各无线主机之间不能直接通信。
SSID：	选择已添加的无线网络进行安全设置。
认证类型	对选中的无线网络，设置其认证类型。 • 无加密：如果不需要对无线网络加密，能够让任意主机接入无线网络，则可以选择该选项。 • WPA-PSK：系统将采用 WPA-PSK 加密方式对无线网络进行加密。请参考 7.3 AP 设置中的 WPA-PSK 填写相关参数。

设置完成后，点击<确定>按钮使其生效。

说明：

列表中第一个条目为默认存在的无线网络，此无线网络除了 VLAN 之外的参数都不能在列表中修改。如需修改此无线网络的 SSID 和 SSID 广播状态，请在“AP 设置”区域修改；如需修改其“AP 隔离”状态，请在“无线高级设置”区域修改。

7.5 无线MAC地址过滤

Client 模式下无此功能。

无线 MAC 地址过滤功能即通过 MAC 地址来控制客户端能否接入无线网络，从而有效控制无线网络内用户的上网权限。

图 7-9 无线MAC地址过滤

无线MAC地址过滤：	勾选“启用”后可开启无线 MAC 地址过滤功能。启用该功能后，将出现规则设置项，点击表格中的<添加>按钮可添加过滤规则条目。 • SSID：选择需要控制接入的无线网络。在 AP 模式下，若开启了多 SSID 模式，可以针对每个 SSID 标识的无线网络设置不同的过滤规则。 • MAC 地址：需要进行接入控制的无线主机的 MAC 地址。 • 备注：可以在此处输入对该过滤规则的描述信息。
过滤规则：	请在此处选择允许或是禁止符合表格中已启用规则的用户接入对应的无线网络。

设置完成后，点击<确定>按钮使其生效。

7.6 无线高级设置

图 7-10 无线高级设置

距离设置：	请输入 AP 与 STA（Station，站点）之间的距离，这个设置会很大程度上影响远距离无线传输性能。 如果设备作为 Client 设备，请输入设备与前端 AP 的距离；如果设备作为 AP 设备，则输入最远的客户端与本设备之间的距离。如果难以精确测量，在输入 AP 与 STA 的距离时，请输入一个比实际距离稍微偏大的数值。
Beacon时槽：	Beacon 帧是设备的广播包，用于发布设备支持的 SSID 无线网络。STA（Station，站）通过收到的 Beacon 帧判断该 SSID 是否还存在，如果长时间都没有收到该 SSID 的 Beacon 帧，则 STA 可以认为该 SSID 已经不存在，STA 就会自动断开与该 SSID 的连接，从而实现无线网络连接同步。 Beacon 时槽表示 AP 发送 Beacon 广播的频率。默认值为 100 毫秒，取值范围是 40-1000 毫秒。
RTS阈值：	为数据包指定 RTS（(Request to Send）阈值，当数据包长度超过 RTS 阈值时，系统就会发送 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间隔：	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。当系统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。
AP隔离：	勾选“启用”此项可以隔离关联到本设备中的各个无线主机。启用 AP 隔离后，系统将隔离接入到同一个无线网络中的各个无线主机，各无线主机之间不能直接通信。

Short GI：	勾选“启用”此项可以使设备接收和发送短帧间隔数据包，提高设备的传输速率，推荐勾选。
Wi-Fi多媒体（WMM）：	勾选“启用”此项后，设备具有无线 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。
Transmit Beamforming：	勾选“启用”后可开启 Transmit Beamforming 功能。 Transmit Beamforming（传输波束成形）是 MIMO 系统中一种可选的智能天线技术，通过精确调整每一路上信号的相位和幅度，使多路信号在接收端得以较好地叠加，成为一个加强的单一信号,从而有效提高信号质量，特别是在远距离传输上，效果尤为明显。推荐启用该功能。

设置完成后，点击<确定>按钮使其生效。

第8章 管理维护

管理维护页面主要用于实现对本设备的管理和维护。

图 8-1 管理维护

8.1 系统日志

系统日志主要用于记录系统中硬件、软件及系统问题的信息，监视系统中发生的事件。可以通过系统日志了解系统运行状态，检测错误发生的原因等。

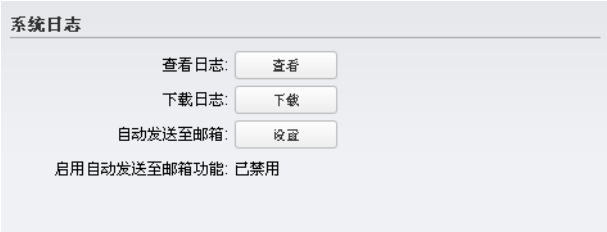


图 8-2 系统日志

查看日志：	点击<查看>按钮将弹出“系统日志”窗口，可查看自本次启动以来的系统日志。
下载日志：	点击<下载>按钮可将下载系统日志。
自动发送至邮箱：	可配置自动发送邮箱功能。点击<设置>按钮将弹出“自动发送至邮箱功能”窗口，可在该窗口输入发件人及收件人邮箱、填写 SMTP 服务器地址及身份验证信息等参数后启用自动发送至邮箱功能。
启用自动发送至邮箱功能：	显示当前是否已启用自动发送至邮箱功能。

设置完成后，点击<确定>按钮使其生效。

8.2 杂项

图 8-3 杂项

被Pharos Control发现：	Pharos Control 是 TP-LINK 自主研发的专门用于管理 TP-LINK 室外无线基站和 CPE 系列产品的管理软件。 勾选启用“被 Pharos Control 发现”功能后，可以让 Pharos Control 管理软件发现并管理该设备。
LAN1端口PoE供电：	勾选“启用”后可开启 LAN1 端口 PoE 供电功能。LAN1 口可为 PD 设备供电，当您希望使用 LAN1 端口对对端设备供电并进行数据传输时，请启用 LAN1 端口 PoE 供电功能。

设置完成后，点击<确定>按钮使其生效。

8.3 Ping看门狗

Ping 看门狗功能可以周期性地发送 Ping 包检测本设备与目的 IP 地址的网络连通性，从而判断本设备是否出现故障。如果判断为故障，系统将自动重启，从而保证设备和网络处于良好状态。

图 8-4 Ping 看门狗

Ping看门狗：	勾选“启用”后可开启 Ping 看门狗功能。
目标IP地址：	设备发送 Ping 包的目的 IP 地址。
发包周期：	设备发送 Ping 包的时间间隔，取值范围为 10～300 秒，默认值为 300 秒。
启动延迟：	系统启动后，延迟启用 Ping 看门狗功能的时间，取值范围为 60～300 秒，默认值为 300 秒。 设置此参数，可以避免系统启动过程中触发了 Ping 看门狗功能，而用户又无法登录管理界面修改配置，导致设备不停地重启。
最大丢包数：	若设置最大丢包数为 N，则当设备连续发送 N 个 Ping 包至目的 IP 地址，都没有收到应答时，设备将自动重启。取值范围为 1～65535，默认值为 3。

设置完成后，点击<确定>按钮使其生效。

8.4 动态DNS

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。

设备通过 PPPoE 方式、动态 IP、L2TP 或 PPTP 方式连接到因特网时，所获取到的 IP 地址是不固定的。这样，内网用户就无法通过广播本设备的 IP 地址来让因特网用户访问内网服务器。动态 DNS 功能可以解决这个问题。

DDNS 服务器维护着一个域名与 IP 地址的映射表。本设备开启动态 DNS 功能后，在每次上网获得新的 IP 地址时，都会将该 IP 地址发送到 DDNS 服务器，发起更新请求。DDNS 服务器收到请求后会更新域名与 IP 地址的映射关系。所以，无论本设备的 WAN 口 IP 地址如何改变，因特网上的用户仍可以通过固定的域名访问到本局域网内的服务器。这样，大多数不使用固定 IP 地址的用户，也可以通过 DDNS 服务高效、经济搭建自己的 Web 服务器了。

说明：

本设备的 DDNS 功能是作为 DDNS 服务的客户端工具，需要与 DDNS 服务器协同工作，使用该功能之前，请先向 DDNS 服务提供商（NO-IP、Dyndns 或 Comexe）申请注册一个域名。

图 8-5 动态DNS

服务提供者：	选择您的DDNS服务提供商。本设备支持NO-IP、Dyndns及Comexe三家DDNS服务提供商。
动态DNS：	勾选“启用”后可开启动态DNS服务。
用户名/密码：	请正确填写在DDNS上注册的用户名和密码。
域名：	填写您的动态域名。启用动态DNS服务后，即使您使用的是动态IP，Internet上的其他用户仍然可以通过这个固定的域名访问到您的网络。
连接状态：	显示与DDNS服务器的连接状态。

参数填写完毕后，请点击<登录>按钮与DDNS服务器建立连接。

8.5 Web服务器

可以在本设置区配置设备的Web服务器功能。本设备作为Web服务器，允许用户登录其Web管理界面对设备进行管理维护。

图 8-6 Web服务器

安全连接（HTTPS）：	Web 服务器的安全连接（HTTPS）模式默认为开启状态。
安全连接端口：	指定 HTTPS（安全连接）模式下 Web 服务器使用的服务端口，默认为 443。
服务端口：	指定 HTTP 模式下 Web 服务器使用的服务端口，默认为 80。
远程登录IP地址：	设置允许远程登录本设备 Web 管理界面的设备的 IP 地址。其中，0.0.0.0 表示禁止所有远端 IP 访问；255.255.255.255 表示允许所有远端 IP 访问。
WEB会话超时时间：	设置 WEB 会话超时时间。用户登录 Web 管理界面后，如果无操作时间大于 WEB 会话超时时间，则需重新登录。
MAC地址验证：	勾选“启用”可开启 MAC 地址验证功能。开启该功能后，只有 MAC 地址为列表中的主机才可以登录设备的 Web 管理界面管理设备。默认情况下该功能为禁用状态，局域网内的所有主机都可以登录设备的 Web 管理界面。
MAC1~MAC4：	输入可以登录 Web 管理界面的主机的 MAC 地址。

设置完成后，点击<确定>按钮使其生效。

8.6 SNMP代理

可以通过启用 SNMP 代理功能将本设备配置为 SNMP 代理。

简单网管协议（SNMP）是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。SNMP 的基本功能包括监视网络性能、检测分析网络差错和配置网络设备等。在网络正常工作时，SNMP 可实现统计、配置和测试等功能；当网络出故障时，可实现各种错误检测和恢复功能。

SNMP 包括三个网络元素：SNMP 管理者，SNMP 代理和 MIB 库（Management Information Base，管理信息库）。SNMP 管理者是运行在工作站的客户端程序，帮助网络管理员完成绝大多数的网络设备管理工作。SNMP 代理是驻留在被管理设备上的一个进程，负责接收和处理 SNMP 管理者发来的信息。被管理设备一般为主机、网桥、交换机、路由器等网络设备。MIB 库则是被管理对象的集合，定义了被管理对象的一系列属性，每个 SNMP 代理都有自己的 MIB。

将本设备设置成 SNMP 代理后，设备可以负责接收和处理来自 SNMP 管理者的请求报文。

图 8-7 SNMP代理

SNMP代理：	勾选“启用”后可开启 SNMP 代理功能。 启用后，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：	请输入本管理节点的管理员的联系信息。
系统名称：	请输入本管理节点的名称。
系统位置：	请输入本管理节点的物理位置。
只读团体名：	团体(Community)是指以管理为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)。
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)。

设置完成后，点击<确定>按钮使其生效。

说明：

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。

8.7 SSH服务器

本设备支持 SSH 服务器功能，可以使用 SSH 客户端软件通过 SSH 连接方式登录并管理设备。

SSH（Secure Shell，安全外壳）是建立在应用层和传输层基础上的安全协议。SSH 加密连接所提供的功能类似于一个 telnet 连接，但是传统的 telnet 远程管理方式在本质上是不安全的，因为它在网络上是使用明文传送口令和数据的，别有用心的人可以很容易的截获这些口令和数据。当通过一个不能保证安全的网络环境远程登录到设备时，SSH 功能可以提供强大的加密和认证安全保障，它可以对所有传输的数据进行加密，可以有效防止远程管理过程中的信息泄露问题。

图 8-8 SSH服务器

服务端口：	请输入服务端口号，SSH 服务默认使用 22 端口。
SSH登录：	勾选“启用”后可开启 SSH 服务器功能。
远程管理：	勾选“启用”后可以让远程的主机访问并使用 SSH 服务。

设置完成后，点击<确定>按钮使其生效。

8.8 无线信号灯阈值

可以在本设置区修改无线信号灯的点亮阈值。当设备接收到的无线信号强度达到所设定的阈值时，相应的无线信号灯将亮起。完成修改后，点击<确定>按钮使设置生效。设备出厂默认的阈值是我们根据经验预设的最优值，如无特别需要建议保持默认值不变。

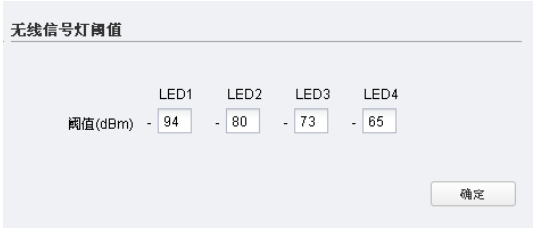


图 8-9 无线信号灯阈值

第9章 系统工具

系统工具页面主要用于配置设备的名称、位置、管理帐号和时间设置等基本信息，以及实现对设备的软件升级、配置管理等功能。

图 9-1 系统工具

9.1 设备

图 9-2 设备

设备名称：	即对该设备的描述，默认为设备的机型，您可以根据需要修改设备名称。
语言：	显示 Web 界面所使用的语言。

设置完成后，点击<确定>按钮使其生效。

9.2 位置

可以在该设置区输入本设备的物理位置，用经度和纬度来表示。位置参数填写完毕后请点击<确定>按钮使其生效。Pharos Control管理软件可以通过该位置参数获得当前设备的位置。

图 9-3 位置

9.3 管理帐号

可以在该设置区修改登录该设备的用户名和密码。

图 9-4 管理帐号

原用户名/原密码：	输入管理帐号的原用户名和密码，以获得修改管理帐号的权限。
新用户名/新密码：	输入管理帐号的新用户名和密码，要求输入的用户名和密码长度不超过 15 个字符，不能包含空格且注意英文字母区分大小写。
确认新密码：	再次输入新密码，以确认在上一栏输入的字符串为预想的新密码。

设置完成后，点击<确定>按钮使其生效。

9.4 时间设置

可以在时间设置区配置设备的系统时间。系统时间是设备工作时使用的时间，访问控制等功能的生效时间以此处为准。可以选择手动设置时间或者连接到一个 NTP(网络时间协议)服务器获取 GMT 时间，也可以获取当前管理 PC 的时间作为设备的系统时间。

图 9-5 时间设置

时区：	选择设备所在的时区。
日期：	设置当前日期，格式为 YYYY/MM/DD。
时间：	设置当前的时间，格式为 HH:MM:SS。
首选NTP服务器/ 备用NTP服务器：	若选择通过 NTP 服务器获取 GMT 时间，请在此处输入 NTP 服务器的 IP 地址。

说明：

对于日期和时间，您可以手动设置；也可以通过点击<获取管理主机时间>按钮从管理主机中自动获取当前日期/时间；如果您配置了 NTP 服务器，还可以通过点击<获取 GMT>按钮获取 GMT 时间（格林尼治标准时间）。

设置完成后，点击<确定>按钮使其生效。

9.5 软件升级

可以在本设置区升级系统文件，系统升级后将获得更完善的功能。请登录TP-LINK官方网站http://www.tp-link.com.cn下载最新版本的系统文件，然后点击本设置页面中的<浏览>按钮选择下载的文件，最后点击<导入>按钮进行升级。

图 9-6 软件升级

注意：

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电源，否则将导致设备损坏而无法使用。当升级结束后，系统将会自动重启。

9.6 配置管理

配置管理区主要实现对设备的配置文件的管理，包括备份配置、导入配置、恢复出厂配置等功能。

备份配置功能可以将设备当前的配置以文件的保存到电脑中，方便日后通过该文件恢复配置：在升级软件或在载入新的配置文件前备份设备的原有配置，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。

导入配置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。如果需要为多台型号相同的设备配置相同的设置，则可以先配置一台设备，保存其配置文件后，再将其载入到其它的设备中，这样可以有效节省配置时间。

图 9-7 配置管理

备份配置：	点击<备份>按钮可将设备当前的配置保存到电脑。建议软件升级前先进行备份。
导入配置：	点击<浏览>按钮，选择目标配置文件，再点击<导入>按钮将配置文件导入设备。导入配置后设备将自动重启。
恢复出厂配置：	点击<恢复>按钮可将设备恢复为出厂配置状态，所有配置数据将被清除。
重启设备：	点击<重启>按钮可重启设备。

注意：

1. 导入配置可能需要较长时间，此期间请耐心等待，不要操作设备。
2. 配置文件载入的过程中请不要关闭设备电源，否则可能导致文件载入失败，设备恢复出厂设置。

第10章 小工具

本设备提供了Ping、Traceroute、速度测试、扫描和频谱分析等用于监控和管理网络的小工具，分散于Web管理界面的各个标签页中。另外，也可以通过点击快速选择区的“小工具”下拉菜单，快速选择您需要的小工具。

图 10-1 小工具

10.1 Ping

Ping 功能可以检测设备与其他网络设备之间是否可达，方便网络管理员检查网络的连通性，定位网络故障。

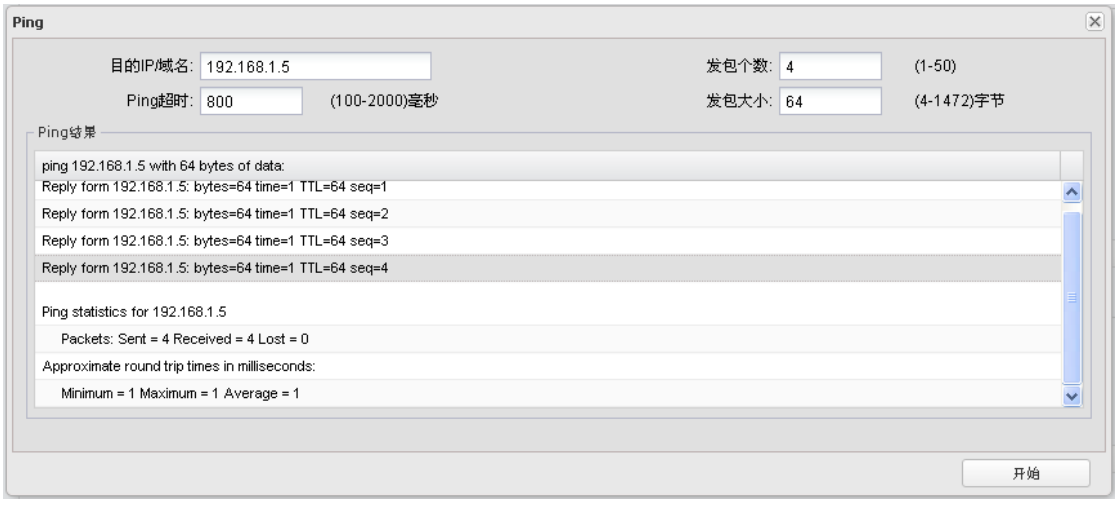


图 10-2 Ping

目的IP/域名：	输入需要测试的目标节点的 IP 地址或域名。
发包个数：	输入 Ping 检测中发送的检测包的数量。建议使用默认值。
Ping超时：	设置 Ping 检测的超时时间。设备发送检测包后，如果超过此超时时间仍未收到目标设备返回的报文，则判断为目标设备不可达。建议使用默认值。
发包大小：	指定 Ping 检测中发送的检测包大小。建议使用默认值。

填写完以上参数后，点击<开始>按钮开始检测，检测结果将显示在“Ping 结果”页面中。

10.2 Traceroute

Traceroute 即路由跟踪，可以查看设备到目标节点所经过的路由器。当网络出现故障时，可以使用该功能定位出现故障的网络节点。

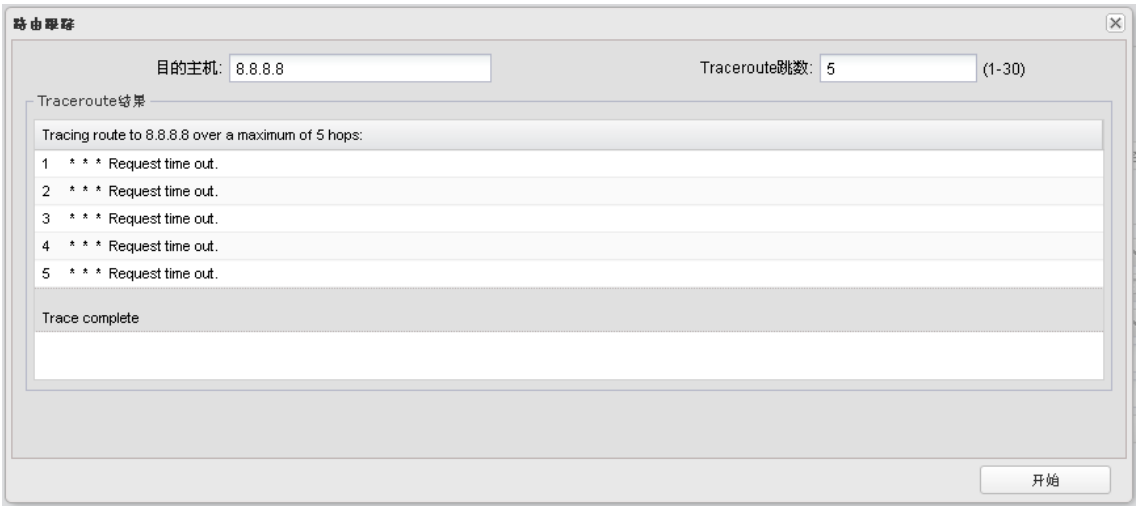


图 10-3 Traceroute

目的主机：	输入需要测试的目标节点的 IP 地址或域名。
Traceroute跳数：	设置发送的检测报文的最大跳数。假设最大跳数为 N，则设备只跟踪与自己相离 N 跳（即 N 台路由器）以内可达的设备。

填写完以上参数后，点击<开始>按钮开始检测，检测结果将显示在“Traceroute 结果”页面中。

10.3 速度测试

速度测试工具用于检测同一网络内两台设备（TP-LINK 室外无线基站和 CPE 系列产品）之间的连接速度。测试过程中，需要将其中一台设备配置为服务器，另外一台设备则配置为客户端。客户端向服务器发起测速请求，服务器被动接受客户端发起的测速请求，测试结果最终显示在客户端的“速度测试”页面上。

对于服务器，只需在“速度测试”页面开启服务器功能后点击<开始>按钮即可，无需配置参数。如图 10-4 所示。

图 10-4 速度测试--服务器

对于客户端，在“速度测试”页面开启服务器功能，需要配置相关参数。如图 10-5 所示。

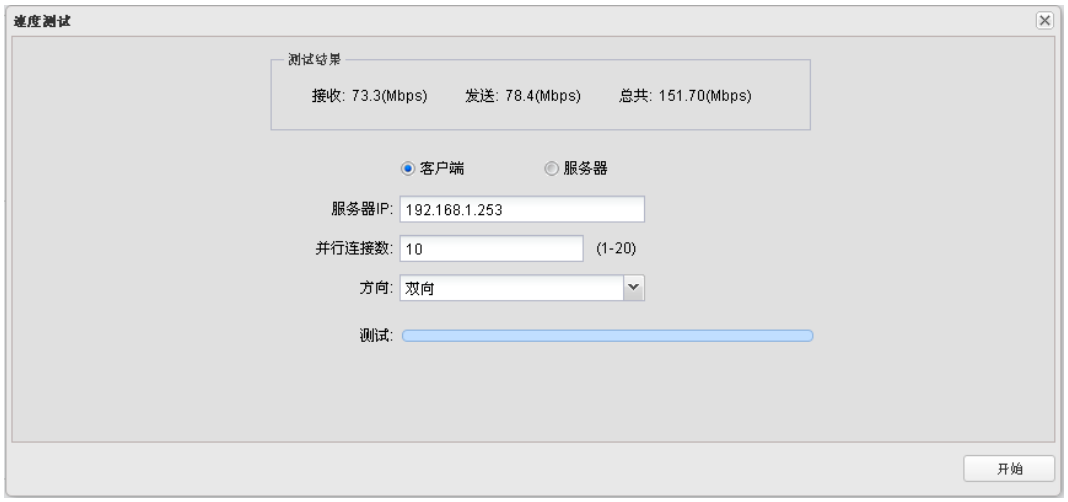


图 10-5 速度测试--客户端

服务器IP：	输入服务器的 IP 地址。
并行连接数：	设置发起测速连接的条目数，取值范围为 1-20。
方向：	设置测速方向。 • 单向：测试数据包从客户端到服务器的发送速率。 • 双向：同时测试数据包的发送速率和接收速率。

填写完以上参数后，点击<开始>按钮开始检测，检测结果将显示在“测试结果”页面中。

10.4 扫描

扫描工具用于搜索周围可用的无线网络。点击<扫描>按钮，将弹出如图 10-6 所示的 AP 信息列表。

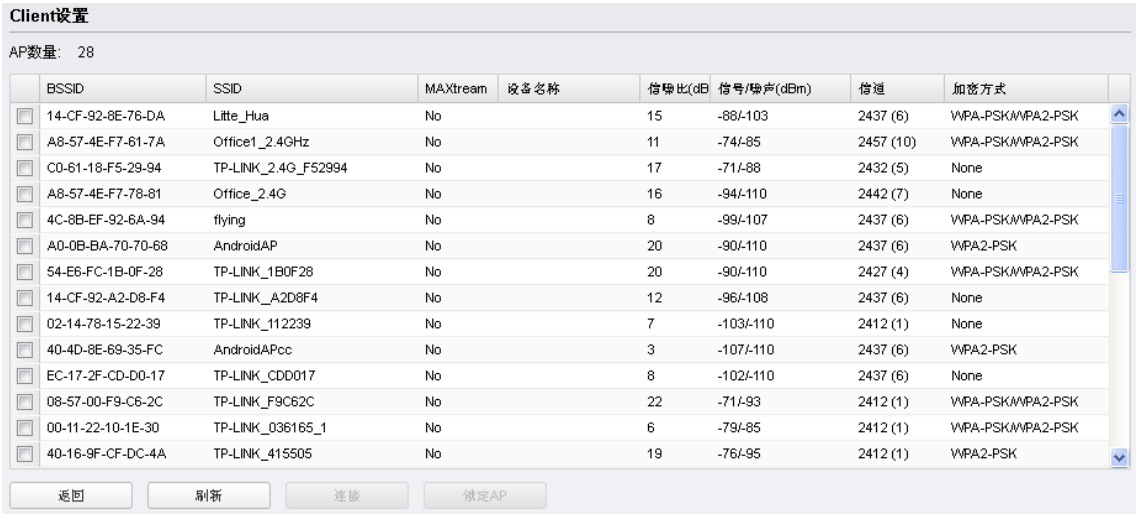


图 10-6 扫描

10.5 频谱分析

频谱分析工具是帮助您选择信道及信道带宽的好助手。您可以通过频谱分析查看周围的无线噪声的分布情况， 从而选择噪声强度较低的频段作为设备的工作频段。

使用步骤：

1. 点击<频谱分析>按钮，将弹出如下图所示窗口，点击<是>进入频谱分析界面。

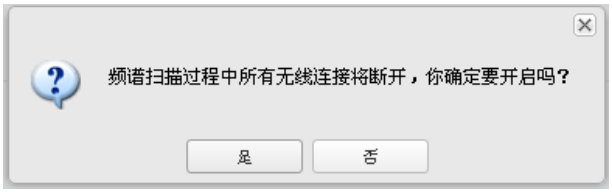


图 10-7 频谱分析--提示窗口

2. 点击右下角的<开始>按钮开始分析，任意一段时间后，点击<结束>按钮查看稳定的图像。

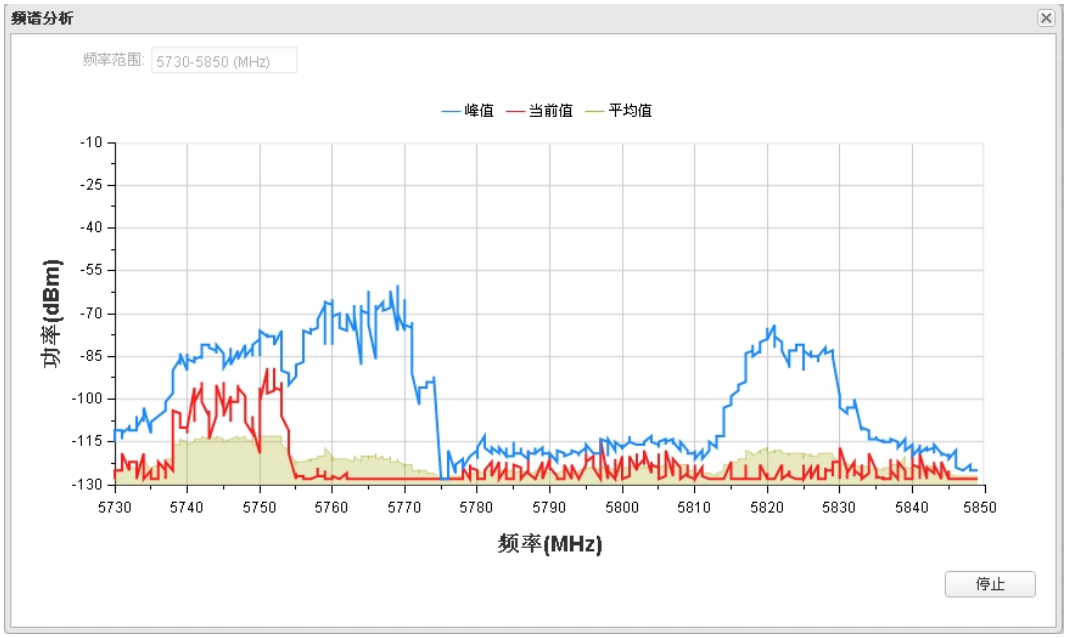


图 10-8 频谱分析--结果显示

3. 在选择信道时应该尽量避开干扰较大的频段。图 10-8 中 5735~5775MHz 和 5815~5835MHz 都存在着较强的干扰，建议选择 157/5785MHz 信道或者 161/5805MHz 信道。

附录A　硬件参数规格

产品型号		TL-CPE210	TL-CPE510	TL-BS210	TL-BS510
安装方式		抱杆安装			
处理器		Qualcomm Atheros MIPS 工业级处理器，主频 560MHz			
内存		64MB DDR2			
Flash		8MB			
无线	无线标准	802.11b/g/n	802.11a/n	802.11b/g/n	802.11a/n
	专有协议	Pharos MAXtream TDMA			
	工作频段	2.4~2.4835GHz	5.725~5.85GHz	2.4~2.4835GHz	5.725~5.85GHz
	最大发射功率	27dBm/500mw		30dBm/1w	
	天线接口	无		2 个 RP-SMA-MALE 接口	
	天线	内置 9dBi 双极化天线	内置 13dBi 双极化天线	无	
接口		1 个 10/100Mbps 屏蔽 RJ45 端口（LAN0/POE） 1 个 10/100Mbps 屏蔽 RJ45 端口（LAN1）			
供电方式		24V/1A Passive PoE 供电，供电距离达 60 米			
指示灯		PWR、LAN0、LAN1、4 个信号强度指示灯			
使用环境		工作温度：–30℃~70℃；　工作湿度：10%～90%RH 不凝结			
		存储温度：–40℃～70℃；　存储湿度：5%～90%RH 不凝结			
环境防护		6kV 雷电防护	4kV 雷电防护	6kV 雷电防护	6kV 雷电防护
		15kV ESD 防护			
		ASA 工程塑料壳体，IP55 等级防尘、防水		ASA 工程塑料壳体，IP65 等级防尘、防水	

附录B　软件参数规格

室外无线基站和 CPE 系列产品软件规格相同，详细内容如下：

参数项	参数内容
无线模式	AP、Client、Bridge、Repeater、AP Router、AP Client Router(WISP Client)
网络设置	• WAN 口连接: 静态 IP、动态 IP、PPPoE、L2TP、PPTP • LAN 口连接: 静态 IP、动态 IP、DHCP • 转发规则: DMZ、ALG、UPnP、虚拟服务器、端口触发 • 网络安全: SPI 防火墙、Ping 禁止、VPN、DoS 防攻击 • 接入控制 • 静态路由 • 带宽控制 • IP–MAC 绑定
无线设置	• Pharos MAXtream TDMA 技术 • 802.11b/g/n 模式 • 自动信道选择 • 发射功率调整 • 动态频率选择(DFS) • WDS • 无线安全: WPA/WPA2、WPA–PSK/WPA2–PSK (AES/TKIP)加密、64/128/152 位 WEP 加密 • SSID 广播/隐藏 • 多 SSID、SSID 与 Tag VLAN 映射(仅 AP 模式) • 距离设置、ACK 超时设置 • 无线 MAC 地址过滤 • 高级设置:Beacon 时槽、RTS 阈值、分片阈值、DTIM 间隔、AP 隔离、Short GI、WMM
管理维护	• 由 Pharos Control 集中管理软件统一管理 • HTTP/HTTPS WEB 管理 • 系统日志 • SNMP 代理(v2c) • Ping 看门狗 • 动态 DDNS • SSH 服务器

参数项	参数内容
系统工具	• 系统状态:信号强度、噪声强度、传输 CCQ、CPU 占用率、内存占用率 • 状态监控: 吞吐量/无线客户端/接口/ARP/路由/WAN/DHCP 服务器 • 频谱分析 • 速率测试 • Ping • Traceroute
系统优化	• IGMP Snooping 优化、多播代理 • 硬件看门狗