



TP-LINK®

室外 **2.4GHz** 高功率无线客户端设备

TL-WA5210G

详细配置指南

声明

Copyright © 2010 深圳市普联技术有限公司

版权所有，保留所有权利

未经深圳市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® 为深圳市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	指示灯.....	3
2.2	后面板和按钮.....	3
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
3.2	建立正确的网络连接.....	5
3.3	快速安装指南.....	7
第 4 章	AP Client Router 和 AP Router 工作模式	11
4.1	Login（登录）.....	11
4.2	Status（运行状态）.....	11
4.3	Quick Setup（快速安装）.....	13
4.4	Operation Mode（工作模式）.....	13
4.5	Network（网络参数）.....	13
4.5.1	LAN（LAN 口设置）.....	14
4.5.2	WAN（WAN 口设置）.....	14
4.5.3	MAC Clone（MAC 地址克隆）.....	18
4.6	Wireless（无线设置）.....	19
4.6.1	Basic Settings（基本设置）.....	20
4.6.2	Wireless Mode（无线模式）.....	20
4.6.3	Security Settings（安全设置）.....	22
4.6.4	MAC Filtering（无线 MAC 地址过滤）.....	25
4.6.5	Wireless Statistics（无线信息统计）.....	27
4.6.6	Distance Setting（距离设置）.....	28
4.6.7	Antenna Alignment（天线校准）.....	28
4.6.8	Throughput Monitor（吞吐量监控）.....	29
4.7	DHCP.....	30

4.7.1	DHCP Settings (DHCP 设置)	30
4.7.2	DHCP Clients List (DHCP 客户端列表)	31
4.7.3	Address Reservation (静态地址分配)	31
4.8	Wireless settings (无线高级设置)	32
4.9	Forwarding (转发规则)	33
4.9.1	Virtual Servers (虚拟服务器)	33
4.9.2	Port Triggering (端口触发)	35
4.9.3	DMZ (DMZ 主机)	36
4.9.4	UPnP (UPnP 设置)	37
4.10	Security (安全功能)	38
4.10.1	Firewall (防火墙)	38
4.10.2	IP Address Filtering (IP 地址过滤)	39
4.10.3	Domain Filtering (域名过滤)	40
4.10.4	MAC Address Filtering (MAC 地址过滤)	42
4.10.5	Remote Management (远程 WEB 管理)	43
4.10.6	Advanced Security (高级安全功能)	43
4.11	Static Routing (静态路由表)	45
4.12	IP & MAC Binding (IP、MAC 地址绑定)	46
4.12.1	Binding Setting (绑定设置)	46
4.12.2	ARP List (ARP 列表)	47
4.13	Dynamic DNS (动态 DNS)	48
4.13.1	Dyndns.org DDNS	48
4.13.2	Oray.net DDNS	49
4.13.3	Comexe.cn DDNS	50
4.14	SNMP	51
4.14.1	Community Setting (团体设置)	51
4.14.2	SNMP System Setting (SNMP 系统设置)	52
4.15	System Tools (管理工具)	53
4.15.1	Time (时间设置)	53
4.15.2	Firmware (软件升级)	54
4.15.3	Factory Defaults (恢复出厂设置)	55
4.15.4	Backup & Restore (备份和载入配置)	55
4.15.5	Ping Watch Dog (看门狗)	56
4.15.6	Speed Test (速率检测)	56
4.15.7	Reboot (重启)	57

4.15.8	Password (修改登录口令)	58
4.15.9	Syslog (系统日志)	58
4.15.10	Statistics (流量统计)	59
第 5 章	AP 工作模式	60
5.1	Login (登录)	60
5.2	Status (系统状态)	60
5.3	Quick Setup (快速安装)	61
5.4	Operation Mode (工作模式)	62
5.5	Network (网络参数)	62
5.6	Wireless (无线设置)	63
5.6.1	Basic Settings (基本设置)	63
5.6.2	Wireless Mode (无线模式)	64
5.6.3	Security Settings (无线安全设置)	69
5.6.4	MAC Filtering (无线 MAC 地址过滤)	72
5.6.5	Wireless Statistics (无线信息统计)	74
5.6.6	Distance Setting (距离设置)	75
5.6.7	Antenna Alignment (天线校准)	75
5.6.8	Throughput Monitor (吞吐量监控)	76
5.7	DHCP	77
5.7.1	DHCP Settings (DHCP 设置)	77
5.7.2	DHCP Clients List (DHCP 客户端列表)	78
5.7.3	Address Reservation (静态地址分配)	79
5.8	Wireless settings (无线高级设置)	80
5.9	SNMP	81
5.9.1	Community Setting (团体设置)	81
5.9.2	SNMP System Setting (SNMP 系统设置)	81
5.10	System Tools (系统工具)	82
5.10.1	Firmware (软件升级)	82
5.10.2	Factory Defaults (恢复出厂设置)	83
5.10.3	Backup & Restore (备份和载入配置)	84
5.10.4	Ping Watch Dog (看门狗)	84
5.10.5	Speed Test (速率检测)	85
5.10.6	Reboot (重启)	86
5.10.7	Password (修改登录口令)	87
5.10.8	Syslog (系统日志)	87

Appendix A: FAQ	88
Appendix B: IE 浏览器设置.....	91
Appendix C: POE 的使用.....	94
Appendix D: 规格参数.....	96

第1章 产品概述

1.1 产品简介

TL-WA5210G 室外 2.4GHz 高功率无线客户端设备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。它功能齐全、性能优越、设置方便，是您组建无线局域网的最佳选择。

TL-WA5210G 室外 2.4GHz 高功率无线客户端设备为不同用户提供 3 种网络接入模式：AP client router、AP router 和 AP 模式。在 AP client router 模式下，可以视为无线网接入端，以无线方式接入互联网。在 AP router 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。在 AP 模式下，设备又可以工作在多种模式，例如 AP、Client、WDS Bridge、Repeater 模式。

TL-WA5210G 2.4GHz 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-WA5210G 室外 2.4GHz 高功率无线客户端设备符合 IEEE 802.11g 和 IEEE 802.11b 标准，提供 54Mbps 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 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u 无线标准
- 无线传输速率达到 54Mbps
- 支持 AP Client Router、AP Router 和 AP operation 三种工作模式
- 高传输功率和优质的接收灵敏度。
- 支持专为 WISP 设计的 Client Router 模式
- 支持 Passive POE 供电
- 支持 WDS 模式。
- 支持远距离通信，使无线传输距离可达 50 千米
- 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-WA5210G 或设备，如无特别说明，系指 TL-WA5210G 室外 2.4GHz 高功率无线客户端设备。

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 指示灯

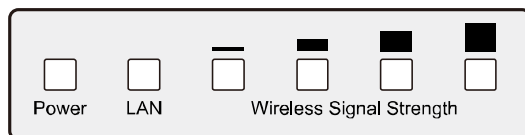


图 2-1 前面板示意图

从左至右观看。

指示灯	状态	说明	
Power	灭	没有上电	
	亮	已经上电	
LAN	灭	端口没有连接上	
	亮	端口已正常连接	
	闪烁	端口正在进行数据传输	
Wireless Signal Strength	灭	没有无线信号	Client 或 Repeater 模式下
	亮	指示无线信号强度	

注意：

Wireless Signal Strength 指示灯：

- 在 AP 或 Bridge 模式下，4 个指示灯均会常亮
- 在 Client 或 Repeater 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。RSSI 值可以在 Wireless Advanced Settings 页面进行配置。如图 4-26

例如如果 RSSI 值为 30，则 4 个无线信号强度指示灯的 RSSI 值分别对应 15、25、35、45，则 RSSI 值为 15 和 25 的两个 LED 指示灯会点亮。

2.2 后面板和按钮

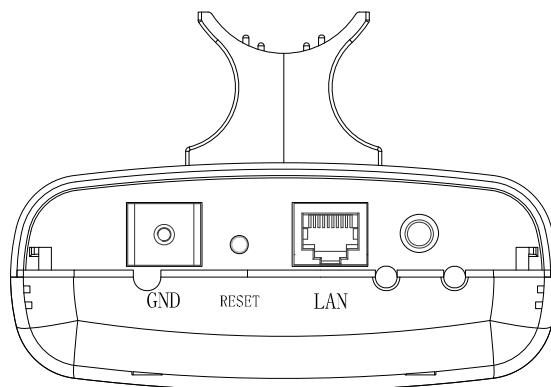



图 2-2 后面板示意图

从右至左观看。

- : 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。
- 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 **System Tools > Factory Default** 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, 当最右边的 LED 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 client router 模式下, 您还需要无线网络接入服务
- 如果 AP 工作在 AP router 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°C~70°C
- 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，请阅读第四章内容。

3.1 硬件连接

AP的基本连接如图 3-1所示，请遵循以下步骤安装设备：

1. 保证无线网络运营商（WISP）已提供无线网络接入服务。
2. 将 AP 尽量放在可以良好接收 WISP 信号的地方。
3. 用网线将计算机直接连接到 AP 的 LAN 口。
4. 调整 AP 的位置保证其接收到最佳无线信号。
5. 接通电源，您可以通过计算机登录 AP 的 Web 管理页面配置 AP。

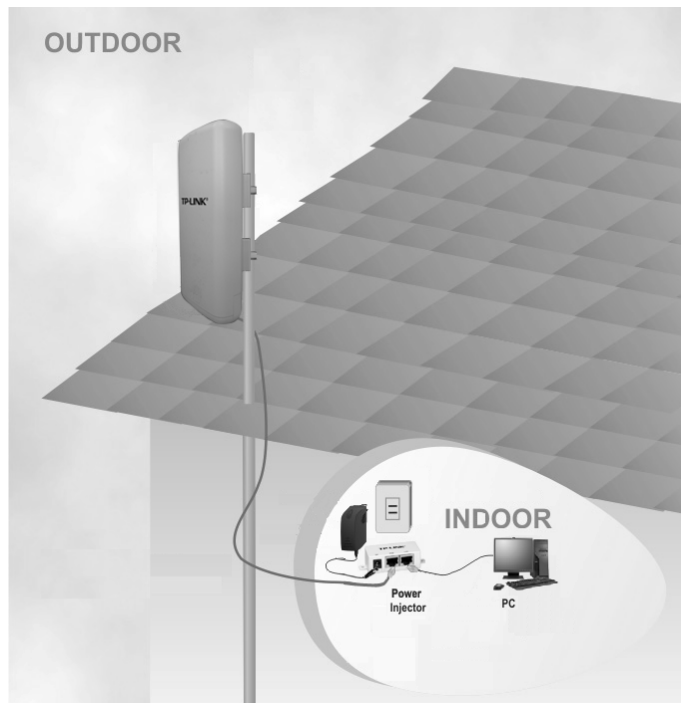


图 3-1

3.2 建立正确的网络连接

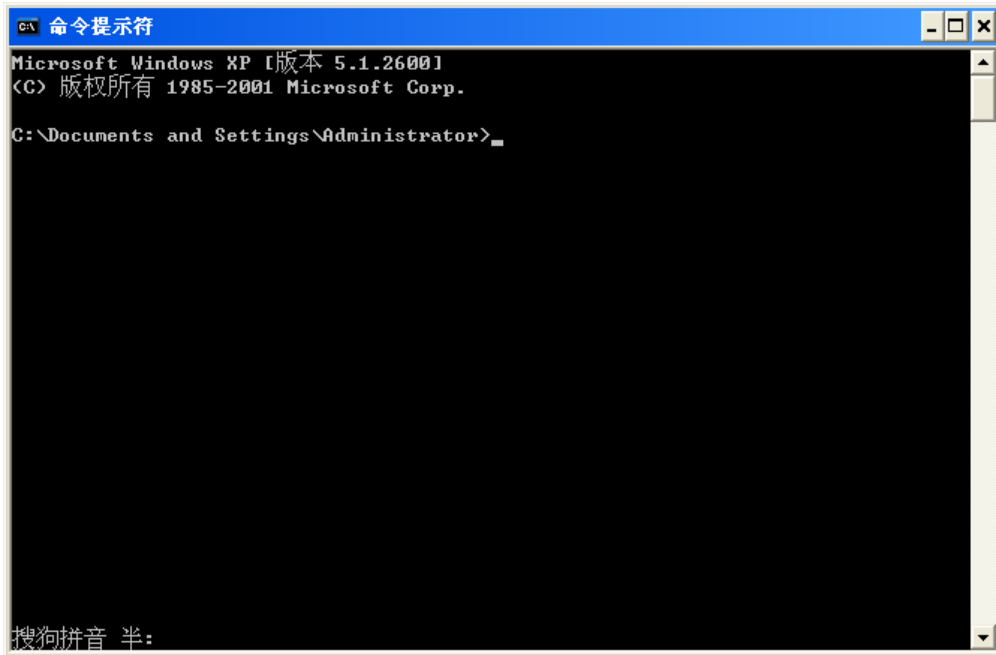
本设备默认 LAN 口 IP 地址是 192.168.1.254，默认子网掩码是 255.255.255.0。这些值可以根据实际需要而改变，但本手册中将按默认值说明。本节以 Windows XP 系统为例，介绍计算机参数的设置步骤。

1. 右键单击桌面上的“网上邻居”图标，选择**属性**，在打开的“网络连接”页面中，右键单击“本地连接”，选择**状态**，打开“本地连接 状态”页面，然后按下图所示进行操作。

 **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。

2. 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。



3. 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？

若计算机的 IP 地址为前面介绍的自动获取方式，则无须进行设置。若手动设置 IP，请注意如果 AP 的 IP 地址为 192.168.1.254，那么计算机 IP 地址必须为 192.168.1.X（X 是 2 到 253

之间的任意整数), 子网掩码须设置为 255.255.255.0, 默认网关须设置为 192.168.1.254。

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, 将会看到下图 3-2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), 单击OK按钮。

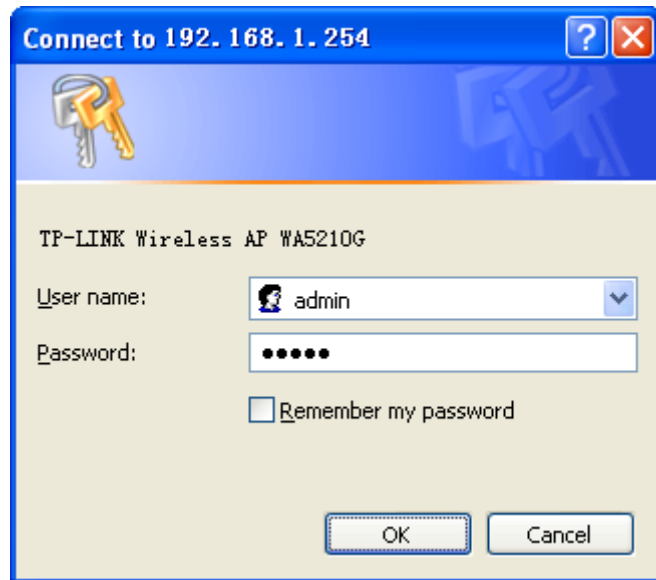


图 3-2 登录界面

浏览器会弹出如下图 3-3所示的设置向导页面。如果没有自动弹出此页面, 可以单击页面左侧的**Quick Setup**菜单将它激活。

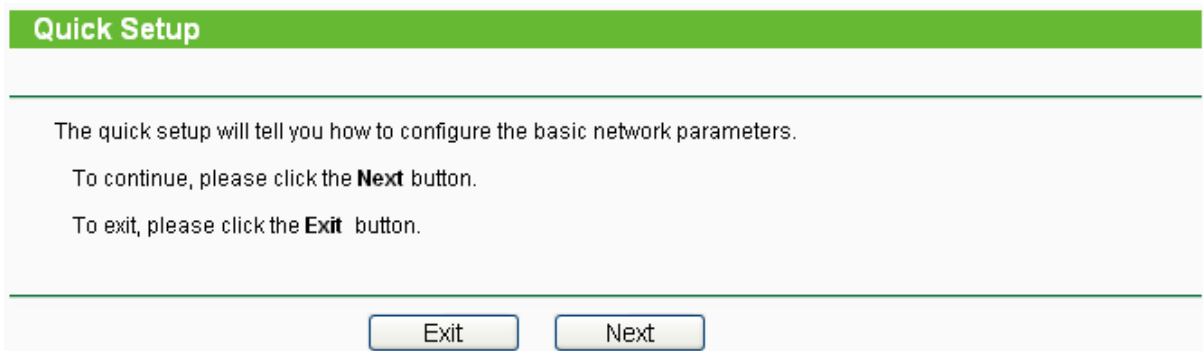


图 3-3 Quick Setup

单击 **Next**, 弹出**Choose Operation mode**页面, 如图 3-4。

图 3-4 Choose Operation mode

注意：

AP支持3种接入模式：**AP Client Router**、**AP Router** 和 **AP**模式。在**AP Client Router**模式下，有WISP的支持，**AP**可以直接以无线方式接入互联网；在**AP Router**模式下，**AP**可以通过ADSL/Cable Modem接入互联网；在**AP**模式下，可以允许多个无线客户端接入无线局域网。在不同模式下，您可以参照以下步骤快速配置设备。

A. 当您选择 **AP Client Router** 或 **AP Router** 模式，请按照以下步骤配置 AP：

1. 在图 3-4中点击 **Next**，然后弹出**Choose WAN Connection Type** 页面，如图 3-5:

图 3-5 Choose WAN Connection Type

在 **AP Client Router** and **AP Router** 模式下，有 3 种最常用的上网方式，请根据 ISP 提供的上网方式进行选择。

2. 单击 **Next** 填写 ISP 提供的网络参数。
 - a) 如果您的上网方式为PPPoE，即ADSL虚拟拨号方式，ISP会给你提供上网帐号和口令，在下图 3-6所示页面中输入ISP提供的ADSL上网账号和口令。

图 3-6 Quick Setup - PPPoE

- b) 如果您的上网方式为"**Dynamic IP**", 您可以自动从网络服务商获取 IP 地址, 无须做任何设置。单击 **Next** 即可。
- c) 如果您的上网方式为"**Static IP**", 网络服务商会给您提供IP地址参数, 您需要在下图 3-7所示页面中输入ISP提供的参数, 若有不明白的地方请咨询网络服务商。

图 3-7 Quick Setup - Static IP

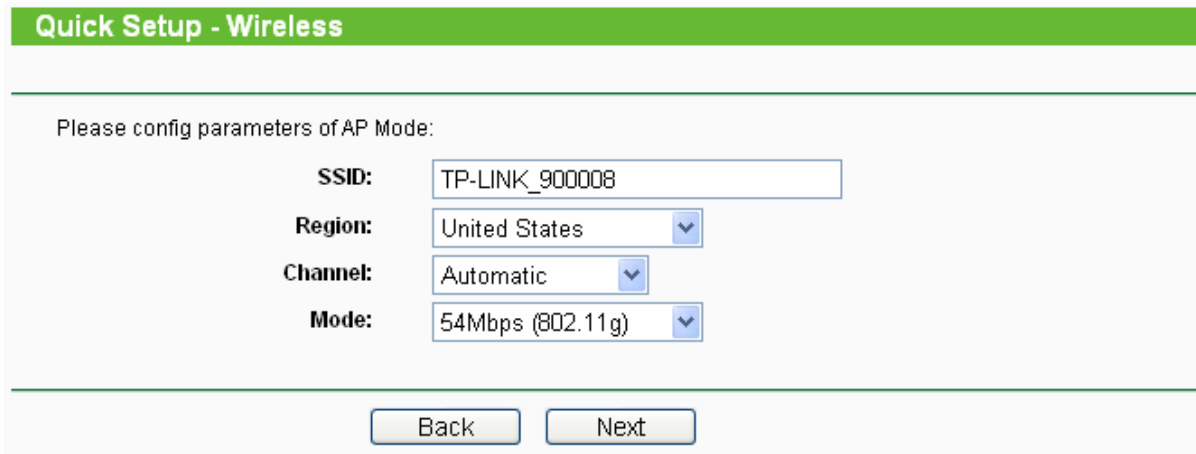
3. 然后点击 **Next** 按钮, 弹出 Wireless settings 页面。

图 3-8 Quick Setup - Wireless settings

在本页, 您需要配置以下无线参数:

 **注意:**

不同模式下 **Quick Setup > Wireless** 页面有所不同。如果您选择 **AP Router** 模式, 您将会看到如下页面。



Quick Setup - Wireless

Please config parameters of AP Mode:

SSID:

Region:

Channel:

Mode:

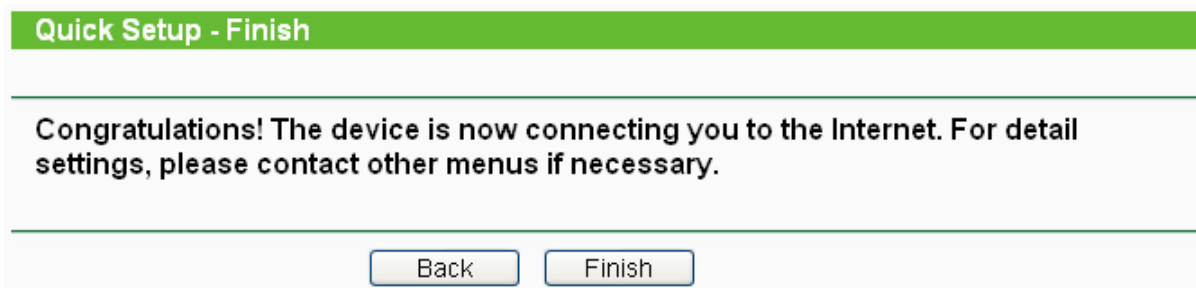
图 3-9 Quick Setup - Wireless settings

- SSID:** 设置任意一个字符串来标明您的无线网络。（字母大小写表意不同）
- Region:** 选择您所在的地区。
- Channel:** 设置路由器的无线信号频段，推荐您选择 **Automatic**。
- Mode:** 设置 AP 的无线工作模式。

这里只是无线参数的基本设置，更高级的配置请参见 [Section 4.6: "Wireless"](#)。

B. 当您选择 **AP**模式，如图 3-4 ，您将直接进入图 3-9所示的页面。

点击 **Next** 您将看到 **Finish** 页面。单击 **Finish** 结束 **Quick Setup**，AP 将自动重启使设置生效。



Quick Setup - Finish

Congratulations! The device is now connecting you to the Internet. For detail settings, please contact other menus if necessary.

图 3-10 Quick Setup - Finish

第4章 AP Client Router和AP Router工作模式

本章介绍在 AP Client Router 和 AP Router 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 AP Client Router 模式为例。

4.1 Login（登录）

启动AP并成功登录AP管理页面后，在左侧菜单栏中，共有如下几个菜单：**Status, Quick Setup, Operation Mode, Network, Wireless, DHCP, Wireless Settings, Forwarding, Security, Static Routing, IP & MAC Binding, Dynamic DNS, SNMP** 和 **System Tools**。单击某个菜单项，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 Status（运行状态）

选择菜单**Status**，可以查看AP当前的状态信息。

Status

Firmware Version: 4.4.0 Build 100120 Rel.52294n
Hardware Version: WA5210G v1 081640EF

LAN

MAC Address: 00-0A-EB-90-00-08
IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0

Wireless

Wireless Radio: Enable
Signal:
SSID: TP-LINK_900008
Channel: 4
Mode: 11Mbps (802.11b)
MAC Address: 00-0A-EB-90-00-09

WAN

MAC Address: 00-0A-EB-90-00-09
IP Address: 0.0.0.0 Dynamic IP
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0 [Obtaining network parameters...](#)
DNS Server: 0.0.0.0, 0.0.0.0

Traffic Statistics

	Received	Sent
Bytes:	0	0
Packets:	0	0

System Up Time: 0 day(s) 00:16:13

图 4-1 Status

LAN: 此处显示 AP 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 **Network > LAN** 界面中进行设置。

Wireless: 此处显示 AP 当前的无线设置状态，包括 SSID、信道和频段带宽等信息。您可以在 **Wireless > Basic Settings** 界面进行相关设置。

WAN: 此处显示 AP 当前 WAN 口的 MAC 地址、IP 地址、子网掩码、网关和 DNS

服务器地址。您可以在 **Network > WAN** 界面中进行相关设置。

Traffic Statistics: 此处显示 AP 当前的数据传输状态。

System Up Time: 此处显示 AP 当前的运行时间。

4.3 Quick Setup（快速安装）

请参见 [3.2: "快速安装指南"](#)。

4.4 Operation Mode（工作模式）

本页用来选择 AP 的工作模式。本设备有 3 个工作模式供您选择：**AP Client Router**、**AP Router** 和 **AP** 模式，请选择一个您需要的，并且点击 **Save** 保存。

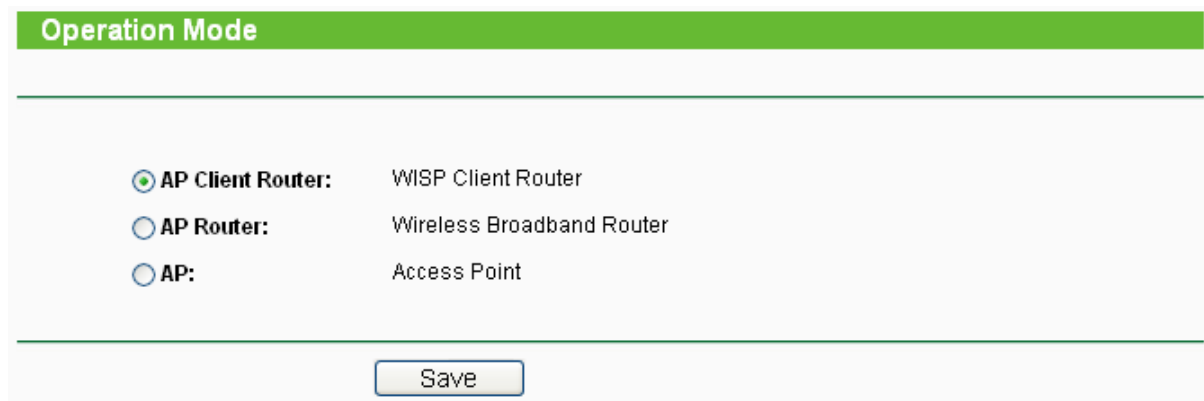


图 4-2 Operation Mode

AP Client Router: 在本模式下，有 WISP 的支持，无线设备可以通过 AP 以无线的方式直接接入互联网，以太网端口通过无线端口直接从 WISP 处获取相同的 IP 地址，无线端口相当于普通无线路由器的 WAN 口，以太网端口相当于 LAN 口。

AP Router: 在本模式下，设备允许用户通过 ADSL/Cable Modem 设备连接互联网，无线端口通过以太网 WAN 口从 ISP 处获取相同的 IP 地址，无线端口相当于一个 LAN 口。

AP: 在本模式下，设备允许多个无线客户端通过 WIFI 接入无线局域网，以太网端口和无线端口均相当于 LAN 口。

4.5 Network（网络参数）

Network 功能，可以根据组网需要设置 AP 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 AP 的 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 **Network**，可以看到：

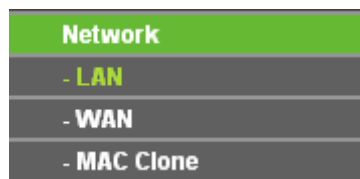


图 4-3 the Network menu

4.5.1 LAN（LAN口设置）

选择菜单 **Network > LAN** 可以在本页配置 LAN 口参数。

图 4-4 LAN

- MAC Address:** AP 在局域网中的 MAC 地址，用来标识局域网。
- IP Address:** 输入 AP 在局域网中的 IP 地址（默认为 192.168.1.254）。
- Subnet Mask:** 输入 AP 对局域网的子网掩码，通常为 255.255.255.0。

 **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，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) 如果新的 LAN 口 IP 地址不在同一网关内，虚拟服务器和 DMZ 主机也会同时做出相应的改变。

4.5.2 WAN（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，您可以根据 ISP 提供的连接类型方便快捷地设置 AP，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 和 PPPoE，请咨询 ISP 提供哪种上网方式同时提供相关参数。

1. 当 ISP 未提供任何 IP 网络参数时，请选择 **Dynamic IP**。如图 4-5 所示。选择 **Dynamic IP**，AP 将从 ISP 自动获取 IP 地址。

WAN

WAN Connection Type:

Host Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Obtaining network parameters...

MTU Size (in bytes): (The default is 1500. Do not change it unless necessary.)

Use These DNS Servers

Primary DNS:

Secondary DNS: (Optional)

Get IP with Unicast DHCP (It is usually not required.)

图 4-5 WAN – Dynamic IP

- MTU Size:** 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。
- Use These DNS Servers:** AP 会从 ISP 处自动获取 DNS 服务器地址。当您需要使用已有的 DNS 服务器时，勾选“**Use These DNS Servers**”，并在此处输入 DNS 服务器和备用 DNS 服务器(选填)的 IP 地址。AP 将优先连接手动设置的 DNS 服务器。
- Get IP with Unicast DHCP:** 少数 ISP 的 DHCP 服务器不支持广播，如果您不能正常获取 IP 地址，可以勾选此项。
2. 当ISP提供给您IP地址、子网掩码、网关和DNS服务器等信息时，请选择Static IP。如图 4-6所示。具体设置时，若不清楚上述参数，请咨询ISP。

WAN

WAN Connection Type:	Static IP	
IP Address:	0.0.0.0	
Subnet Mask:	0.0.0.0	
Default Gateway:	0.0.0.0	(Optional)
MTU Size (in bytes):	1500	(The default is 1500. Do not change it unless necessary.)
Primary DNS:	0.0.0.0	(Optional)
Secondary DNS:	0.0.0.0	(Optional)

图 4-6 WAN - Static IP

- IP Address:** 输入 ISP 提供的 IP 地址信息，必填项。
- Subnet Mask:** 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。
- Default Gateway:** 输入 ISP 提供的网关参数。
- MTU Size:** 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。
- Primary(Secondary)DNS:** 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。
3. 如果ISP提供的上网方式是PPPoE(以太网上的点到点连接)，ISP会提供上网账号和上网口令，请选择PPPoE。如图 4-7。具体设置时，若不清楚此参数，请咨询ISP。

图 4-7 WAN - PPPoE

- User Name/Password:** 请正确输入ISP提供的上网账号和上网口令，必须填写。
- Connect on Demand:** 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交费的用户，选择按需连接可以有效节省上网费用。
- Max Idle Time:** 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。
- Connect Automatically:** 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。若您的网络服务是包月交费形式，可以选择该项连接方式。
- Time-based Connecting:** 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。
- Connect Manually:** 开机或断线后，您需要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。若您的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:** 单击此按钮，可进行即时的连接/断线操作。

 **注意:**

您必须在**System Tools > Time**页面配置系统时间后，才能使**Time-based Connecting**配置生效。若需要进一步设置，可以点击**Advanced Settings**按钮，在下图 4-8界面中进行高级设置。

PPPoE Advanced Settings

MTU Size (in bytes):	<input type="text" value="1480"/>	(The default is 1480, do not change unless necessary.)
Service Name:	<input type="text"/>	
AC Name:	<input type="text"/>	
	<input type="checkbox"/>	Use IP address specified by ISP
ISP Specified IP Address:	<input type="text" value="0.0.0.0"/>	
Detect Online Interval:	<input type="text" value="0"/>	Seconds (0 ~ 120 seconds, the default is 0, 0 means not detecting.)
	<input type="checkbox"/>	Use the following DNS Servers
Primary DNS:	<input type="text" value="0.0.0.0"/>	
Secondary DNS:	<input type="text" value="0.0.0.0"/>	(Optional)
<input type="button" value="Save"/> <input type="button" value="Back"/>		

图 4-8 PPPoE Advanced Settings

Packet 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。

Service Name/AC Name: 如果不是ISP特别要求，请不要填写这两项。

ISP Specified IP Address:

该项仅适用于静态PPPoE。如果ISP提供上网账号和口令时，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。

Detect Online Interval: 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 IP address: 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。

4.5.3 MAC Clone (MAC地址克隆)

MAC地址克隆是将AP的MAC地址克隆为管理计算机的MAC地址来解决某些ISP要求登记您计算机的MAC地址的情况。如非特殊要求，此页不需要配置。

选择菜单**Network > MAC Clone**地址克隆，可以在下图 4-9界面中设置路由器对广域网的MAC地址。

图 4-9 MAC Address Clone

WAN MAC Address: 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。

Your PC's MAC Address:

该处显示当前正在管理路由器的计算机的MAC地址。

Restore Factory MAC: 单击此按钮，即可恢复MAC地址为出厂时的默认值。

Clone MAC Address To: 单击此按钮，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。

注意:

只有局域网中的计算机才能使用“MAC地址克隆”功能。

4.6 Wireless（无线设置）

Wireless 功能，可以安全方便的启用 AP 的无线功能进行网络连接。

Wireless菜单下有 8 个子菜单(如图 4-10): **Basic Settings, Wireless Mode, Security Settings, MAC Filtering, Wireless Statistics, Distance Setting, Antenna Alignment** 和 **Throughput Monitor**。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

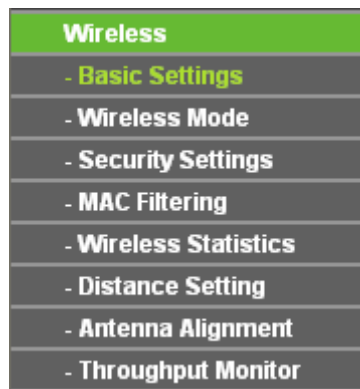


图 4-10 Wireless menu

4.6.1 Basic Settings（基本设置）

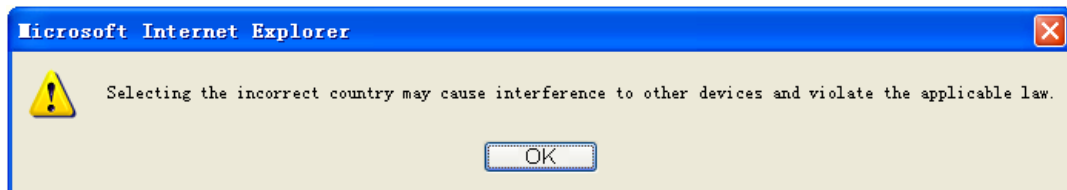
点击 **Wireless > Basic Settings**，可以在图 4-11中进行无线网络的基本设置。

图 4-11 Wireless Settings in AP Client Router mode

SSID: 即 Service Set Identification，用于标识无线网络的名称。您可以在这里输入一个喜欢的名称，它将显示在无线网卡搜索到的无线网络列表中。（区分大小写）

Region: 选择您所在的地区。为设备的无线功能制定使用区域，来解决在某些地区除了菜单中罗列的区域外使用无线功能是非法的问题。如果您所在的地区没有罗列在菜单中，请联系当地的政府。

当选择您所在的区域后，点击 **Save** 按钮，将会显示如下图所示的对话框，点击 **OK**。



注意:

由于法律制约，北美地区没有region的选项。

Channel: 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。

Mode: 该项用于设置 AP 的无线工作模式。

完成更改后，点击 **Save** 按钮，AP 会自动重启使当前的设置生效。

4.6.2 Wireless Mode（无线模式）

点击 **Wireless > Wireless Mode**，可以在图 4-12中选择设备的无线模式。

Wireless Mode Settings

Access Point

Enable SSID Broadcast

Client

SSID:

MAC of AP:

Repeater

MAC of AP:

Universal Repeater

MAC of AP:

Bridge (Point to Point)

With AP Mode

MAC of AP:

Bridge (Point to Multi-Point)

With AP Mode

MAC of AP1:

MAC of AP2:

MAC of AP3:

MAC of AP4:

MAC of AP5:

MAC of AP6:

Note: The current security method may be invalid after changing the wireless mode.

图 4-12 Wireless Mode

注意：

在AP Client Router模式下，仅Client模式可以选择。在AP Router模式下，仅Access Point模式可以选择。

Access Point: Access Point 模式允许无线接入点和 AP 客户端接入路由器。

Enable SSID Broadcast:

开启后无线客户端将可以通过搜索无线 SSID 来发现本 AP。

Client: 在 Client 模式下，AP 将成将等同于一个无线网卡，可以连入其他无线网络。

SSID: 您可以填入一个已有的 SSID，指定接入该无线网络。

MAC of AP: 您可以填入一个已有的 AP MAC 地址，指定接入该 AP 的无线网络。

完成更改后，点击 **Save** 按钮，AP 会自动重启使当前的设置生效。

您还可以单击 **Survey** 按钮，从扫描到的 AP 列表中选择一个接入点，点击 **Connect** 连接，页面将自动返回到基本设置页，此时可以保存设置并重启，以使修改生效。

AP List						
AP Count: 33						
ID	BSSID	SSID	Signal	Channel	Security	Choose
1	00-1D-0F-01-06-18	TP-LINK_010618	31 dB	2	OFF	Connect
2	00-19-E0-94-51-F4	TP-LINK	20 dB	1	ON	Connect
3	00-27-19-C4-BC-58	TP-LINK_C4BC58	19 dB	2	OFF	Connect
4	00-0A-EB-00-01-C1	TP-LINK_0001C1	13 dB	9	ON	Connect
5	00-27-19-C4-BE-8E	TP-LINK_C4BE8E	23 dB	8	OFF	Connect
6	00-0A-EB-CE-1E-1B	TP-LINK_CE1E1B	27 dB	5	OFF	Connect

图 4-13 AP List

BSSID: 显示已有 AP 的 BSSID，通常为 AP 的 MAC 地址。

SSID: 显示已有 AP 的 SSID。

Signal: 显示从已有 AP 处接收到的信号强度。

Channel: 显示已有 AP 的无线数据传输通道。

Security: 显示已有 AP 的安全模式是否开启。

Choose: 从列表中选择一个已有 AP 来接入网络。

 **注意:**

如果您想要配置本 AP 的其他无线模式，您可以在 **Operation Mode** 页面中改变 AP 工作模式。（如图 4-2）

4.6.3 Security Settings（安全设置）

单击 **Wireless > Security Settings**，可以在图 4-14 界面中设置无线网络安全选项。

Wireless Security

Disable Security

WEP

Type:

WEP Key Format:

Key Selected	WEP Key	Key Type
Key 1: <input checked="" type="radio"/>	<input type="text"/>	Disabled <input type="text" value="v"/>
Key 2: <input type="radio"/>	<input type="text"/>	Disabled <input type="text" value="v"/>
Key 3: <input type="radio"/>	<input type="text"/>	Disabled <input type="text" value="v"/>
Key 4: <input type="radio"/>	<input type="text"/>	Disabled <input type="text" value="v"/>

WPA/WPA2

Version:

Encryption:

Radius Server IP:

Radius Port: (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: (in second, minimum is 30, 0 means no update)

WPA-PSK/WPA2-PSK

Version:

Encryption:

PSK Passphrase:

(The Passphrase is between 8 and 63 characters long)

Group Key Update Period: (in second, minimum is 30, 0 means no update, only be valid in AP mode.)

Note: Some security mode can not be selected since it can not be supported by the current wireless mode.

图 4-14 Wireless Security

在 **Wireless > Security Settings** 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**Disable Security**以关闭无线安全功能。
- 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：WEP、WPA/WPA2 以及 WPA-PSK/WPA2-PSK。不同的安全类型下，安全设置项不同，下面将详细介绍。

1. WPA-PSK/WPA2-PSK

WPA-PSK/WPA2-PSK安全类型其实是WPA/WPA2的一种简化版本，它是基于共享密钥的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。

Version: 该项用来选择系统采用的安全模式，即Automatic、WPA-PSK、WPA2-PSK。

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

Encryption: 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 Passphrase: 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。

Group Key Update Period:

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

WPA/WPA2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。

Version: 该项用来选择系统采用的安全模式，即Automatic、WPA、WPA2。

- **Automatic:** 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。

Encryption: 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: 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 Port: 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 Password: 该项用来设置访问Radius服务的密码。

Group Key Update Period:

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。

Type: 该项用来选择系统采用的安全模式，包括Automatic、Shared Key、Open System。

- **Automatic:** 若选择该项，AP会根据主机请求自动选择Open System或Shared Key方式。
- **Open System:** 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。
- **Shared Key:** 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。

WEP Key Format: 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 Key、Key Type:

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。

密钥长度说明：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。

 **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。

4.6.4 MAC Filtering（无线MAC地址过滤）

MAC Filtering 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。

单击**Wireless > MAC Filtering**，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 4-15。

图 4-15 Wireless MAC address Filtering

- Add New...:** 点击该按钮，可以添加新的过滤条目。
- Enabled All:** 点击该按钮，可以将列表中的所有条目的状态设置为“生效”。
- Disabled All:** 点击该按钮，可以将列表中的所有条目的状态设为“失效”。
- Delete All:** 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，请选择 **Allow the stations not specified by any enabled entries in the list to access**；如果不允许未知无线客户端接入，请选择 **Deny the stations not specified by any enabled entries in the list to access**。

点击 **Add New...** 按钮，添加 MAC 地址过滤规则条目。然后 **Add or Modify Wireless MAC Address Filtering entry** 页面将会弹出，如图 4-16 所示。

图 4-16 Add or Modify Wireless MAC Address Filtering entry

- 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。
- Status:** 选择是否启用本条目。**Enabled**（启用）或 **Disabled**（不启用）。
- Privilege:** 选择 MAC 地址过滤规则，您可以选择 **Allow**（允许）或 **Deny**（拒绝）。

Description: 为无线客户端添加简单的描述信息。如：Wireless station A。

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，MAC 地址为 00-0A-EB-00-07-5F 的主机 B 以及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. 为本规则点击 **Enable** 按钮。
2. 在 **Filtering Rules** 处选择 **Deny the stations not specified by any enabled entries in the list to access**。
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 **Disabled** 或删除该条目，也可以点击 **Delete All** 按钮，将列表中的条目清空。
4. 点击 **Add New...**按钮，在 **MAC Address** 处填写 00-0A-EB-00-07-BE，在 **Description** 处填写 wireless station A，在 **Privilege** 处选择 **Allow**，在 **Status** 处选择 **Enabled**。设置完成后，点击 **Save** 按钮和 **Return** 按钮。
5. 点击 **Add New...**按钮，在 **MAC Address** 处填写 00-0A-EB-00-07-5F，在 **Description** 处填写 wireless station B，在 **Privilege** 处选择 **Deny**，在 **Status** 处选择 **Enabled**。设置完成后，点击 **Save** 按钮和 **Return** 按钮。

过滤规则表格显示如下：

ID	MAC Address	Status	Privilege	Description	Modify
1	00-0A-EB-00-07-BE	Enabled	allow	Wireless Station B	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	deny	Wireless Station B	Modify Delete

 **注意：**

- 1) 如果您在 **Filtering Rules** 处选择 **Allow the stations not specified by any enabled entries in the list to access**，wireless station B 仍然不能接入无线网络，但是其他不在列表中的无线接入站将可以接入无线网络。
- 2) 如果启用 MAC 地址过滤规则，并在 **Filtering Rules** 处选择 **Deny the stations not specified by any enabled entries in the list to access**，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。

4.6.5 Wireless Statistics（无线信息统计）

单击 **Wireless > Wireless Statistics**，查看当前连接到无线网络中的所有主机的基本信息。如图 4-17。

Wireless Statistics				
Current Connected Wireless Stations numbers:		1	<input type="button" value="Refresh"/>	
ID	MAC Address	Current Status	Received Packets	Sent Packets
1	00-0A-EB-90-00-09	AP-DOWN	0	32088
<input type="button" value="Previous"/>		<input type="button" value="Next"/>		

图 4-17 The router attached wireless stations

MAC Address: 显示当前已经连接到无线网络的主机的MAC地址。

Current Status: 此项显示当前主机的运行状态。

Received Packets: 显示收到的数据包数目。

Sent Packets: 显示发送的数据包数目。

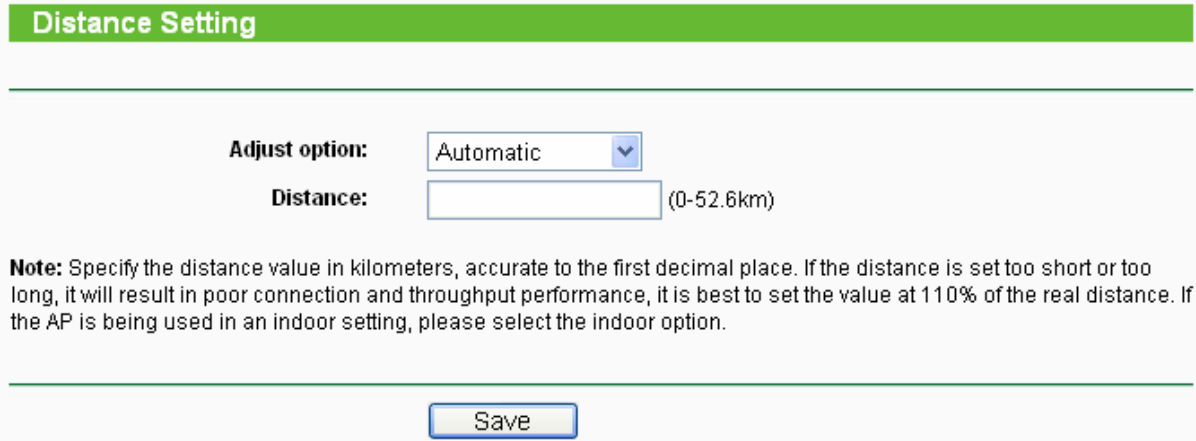
在本页无法进行任何修改，点击 **Refresh** 按钮刷新当前无线连接状态。如果无线连接数目超过一页，点击 **Next** 按钮，进入下一页；点击 **Previous** 按钮，返回上一页。

 **注意：**

本页数据会每隔 5 秒自动刷新。

4.6.6 Distance Setting（距离设置）

单击 **Wireless > Distance Setting**，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。



Adjust option: Automatic

Distance: (0-52.6km)

Note: Specify the distance value in kilometers, accurate to the first decimal place. If the distance is set too short or too long, it will result in poor connection and throughput performance, it is best to set the value at 110% of the real distance. If the AP is being used in an indoor setting, please select the indoor option.

Save

图 4-18 Distance Setting

Adjust option: 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。

Distance: 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%。如果AP在室内使用，请使用indoor模式。

点击 **Save** 使配置生效。

4.6.7 Antenna Alignment（天线校准）

单击 **Wireless > Antenna Alignment**，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。

Antenna Alignment

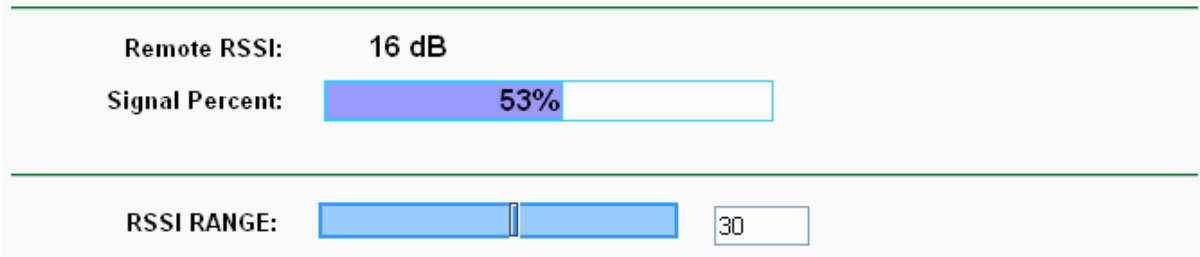


图 4-19 Antenna Alignment

Remote AP RSSI: 显示AP的信号强度值。

Signal percent: 显示RSSI和RSSI RANGE的百分比。

RSSI RANGE: 您可以拖动滑块设置RSSI RANGE值。如果RSSI RANGE值减小，信号强度指示条的变化将更敏感。滑块实际上是改变了指示器的最大值。

注意:

本功能只在已连接 AP 工作在 client 模式下才生效。

4.6.8 Throughput Monitor（吞吐量监控）

单击 **Wireless > Throughput Monitor**，可以在下图 4-20 界面中开始或停止无线通信的流量检测。界面中所有速率单位都为bps，即bit/s。

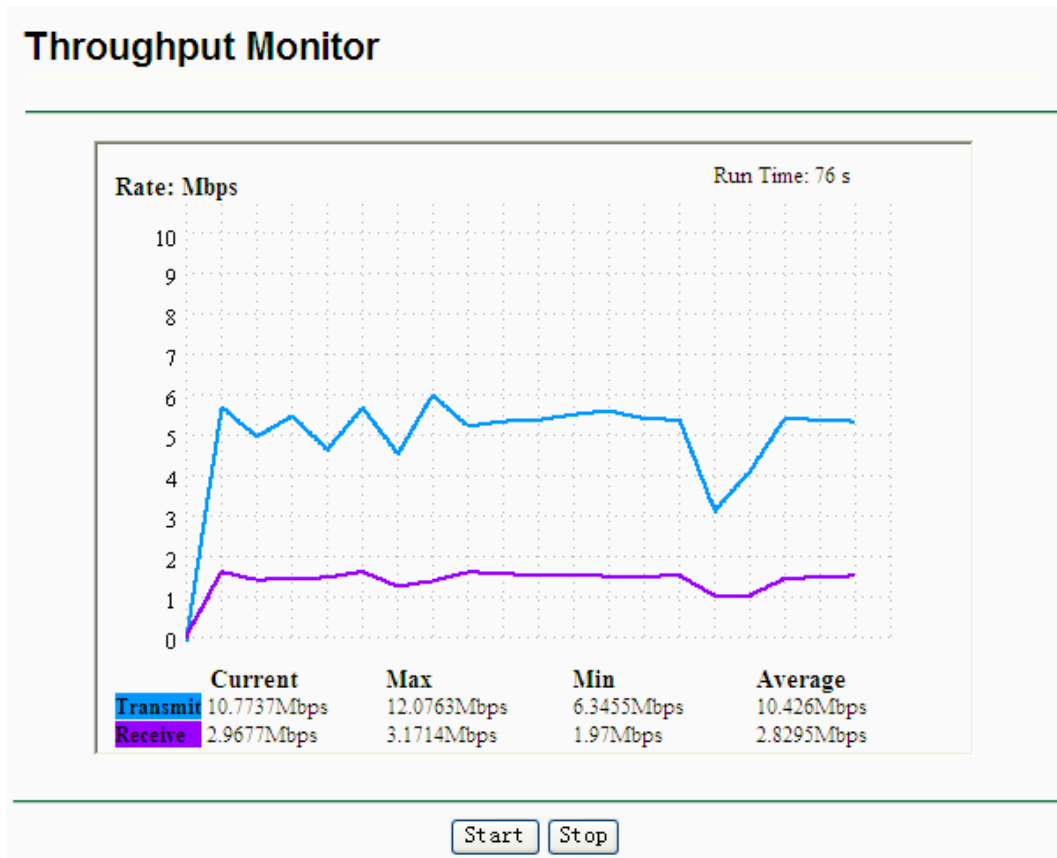


图 4-20 Wireless Throughput

4.7 DHCP

DHCP 指动态主机控制协议(Dynamic Host Configuration Protocol)。本 AP 中有一个内置的 DHCP 服务器，可以实现局域网内的计算机 IP 地址的自动分配。

DHCP 菜单下有 3 个子菜单(如图 4-21): **DHCP Settings**, **DHCP Clients List** 和 **Address Reservation**。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

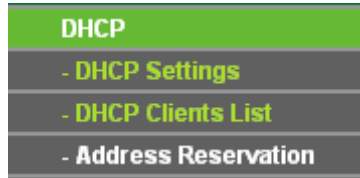


图 4-21 The DHCP menu

4.7.1 DHCP Settings (DHCP设置)

单击 **DHCP > DHCP Settings**，将看到DHCP设置界面，如图 4-22。

 A screenshot of the "DHCP Settings" configuration page. The page has a green header with the title "DHCP Settings". Below the header, there are several configuration fields:

- DHCP Server:** Radio buttons for "Disable" (selected) and "Enable".
- Start IP Address:** Text input field containing "192.168.1.100".
- End IP Address:** Text input field containing "192.168.1.199".
- Address Lease Time:** Text input field containing "120", followed by "minutes (1~2880 minutes, the default value is 120)".
- Default Gateway:** Text input field containing "0.0.0.0" with "(optional)" to its right.
- Default Domain:** Text input field with "(optional)" to its right.
- Primary DNS:** Text input field containing "0.0.0.0" with "(optional)" to its right.
- Secondary DNS:** Text input field containing "0.0.0.0" with "(optional)" to its right.

 At the bottom of the form is a "Save" button.

图 4-22 DHCP Settings

- DHCP Server:** 选择是否启用DHCP服务器功能，默认为启用（Enable）。
- Start/End IP Address:** 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。
- Address Lease Time:** 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。
- Default Gateway (optional):** 可选项。应填入AP的LAN口的IP地址，缺省为192.168.1.254。
- Default Domain (optional):** 可选项。应填入本地网域名，缺省为空。
- Primary/Secondary DNS (optional):** 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。

完成更改后，单击**Save**按钮并重启AP使设置生效。

4.7.2 DHCP Clients List (DHCP客户端列表)

单击**DHCP > DHCP Clients List**，可以查看客户端主机的相关信息；单击**Refresh**按钮可以更新表中信息，如图 4-23。

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	microsoft	00-19-66-CB-45-66	192.168.1.100	01:56:59

图 4-23 DHCP Clients List

- Client Name:** 显示获得IP地址的客户端计算机的名称。
- MAC Address:** 显示获得IP地址的客户端计算机的MAC地址。
- Assigned IP:** 显示DHCP服务器分配给客户端主机的IP地址。
- Lease Time:** 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 Address Reservation (静态地址分配)

单击 **DHCP > Address Reservation**，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 4-24。

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>				
<input type="button" value="Previous"/> <input type="button" value="Next"/>				

图 4-24 Address Reservation

- MAC Address:** 显示预留静态IP地址的计算机的MAC地址。
- Reserved IP Address:** 显示预留给内网主机的IP地址。
- Status:** 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。
- Modify:** 修改或删除本条目。

添加预留 IP 地址：

1. 点击**Add New...**按钮弹出如图 4-25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. 点击 **Save** 按钮，使配置生效。

图 4-25 Add or Modify an Address Reservation Entry

修改预留 IP 地址：

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

点击 **Delete All** 按钮，删除所有条目。

 **注意：**

所有配置将重启后生效。

4.8 Wireless settings（无线高级设置）

单击 **Wireless Settings**，可以在图 4-26 中设置无线的高级功能。

图 4-26 Wireless settings

Enable WMM: WMM功能可以保证在数据包的高质量传输。推荐您开启此功能。

Enable AP Isolation: 选择此项可以隔离关联到接入器的各个无线客户端。

Disable short preamble:

屏蔽短前导，只使用长前导。推荐您保持默认设置。

RTS threshold:

RTS/CTS起始值。决定发送RTS/CTS数据包大小的起始值。

Fragmentation Threshold:

分片阈值。为数据包指定分段阈值，当数据包长度超过此值时会被自动分成多个数据包。

Beacon Interval:

Beacon时槽。设置Beacon帧的发包间隔。

Power:

发射功率。选择是否勾选**Obey Regulatory Power**，不勾选可能导致与其他设备相冲突，干扰可用网络。

Antenna Settings:

设置天线的方向。

Signal LED Thresholds: LED指示灯的RSSI阈值。

4.9 Forwarding（转发规则）

在Forwarding 菜单下有 4 个子菜单(如图 4-27): **Virtual Servers**, **Port Triggering**, **DMZ** 和 **UPnP**。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

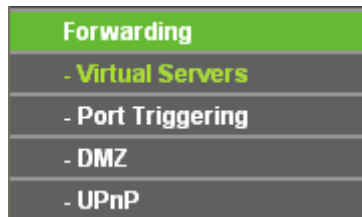


图 4-27 The Forwarding menu

4.9.1 Virtual Servers（虚拟服务器）

通过将本 AP 配置为虚拟服务器（Virtual Servers），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，AP 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 AP 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。

单击**Forwarding > Virtual Servers**，可以在图 4-28所示界面中设置虚拟服务器。

Virtual Servers					
ID	Service Ports	IP Address	Protocol	Status	Modify
1	21	192.168.1.101	TCP	Enabled	Modify Delete

图 4-28 Virtual Servers

Service Port: 显示AP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。端口段输入格式为“开始端口-结束端口”。

IP Address: 显示局域网服务器的静态IP地址。

Protocol: 显示此虚拟服务所采用的协议。可选项有TCP、UDP和ALL。

Status: 显示该条目是否生效。只有状态为生效时（Enable），本条目的设置才有效。

Modify: 对现有条目进行修改。

请按照以下步骤创建 Virtual Servers:

1. 在virtual servers页面点击Add New...按钮，弹出如图 4-29页面。
2. 在 Common Service Port 列表中选择您所需要的服务，对于“Common Service Port”中没有列出的服务，需要手动输入服务端口号和协议的相关信息。
3. 在 **Server IP Address** 处填写局域网服务器的静态 IP 地址。通过此 IP 地址，AP 会将与服务端口的访问请求转到局域网服务器上。
4. 在 **Protocol** 处，选择此虚拟服务所采用的协议，若对采用的协议不清楚，推荐选择 ALL。
5. 在 **Status** 处选择 **Enable**，开启虚拟服务器。
6. 点击 **Save** 按钮保存设置。

Add or Modify a Virtual Server Entry	
Service Port:	<input type="text" value="21"/> (XX-XX or XX)
IP Address:	<input type="text" value="192.168.1.101"/>
Protocol:	<input type="text" value="TCP"/> ▼
Status:	<input type="text" value="Enabled"/> ▼
Common Service Port:	<input type="text" value="FTP"/> ▼

图 4-29 Add or Modify a Virtual Server Entry

Common Service Port: 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“**Common Service Port**”中没有列出的服务，需要手动输入服务端口号和协议的相关信息。

 **注意:**

1. 如果您的主机或服务器有一个以上的虚拟服务器，请将所有虚拟服务器的 IP 地址均输入该主机或服务器的 IP 地址。
2. 如果设置了服务端口为 80 的虚拟服务器，则需要将 **System Tools > Remote Management** 的“**Web management port**”设置为 80 以外的值，如 8080，否则会与 AP 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 AP 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。

4.9.2 Port Triggering (端口触发)

端口触发功能，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 **Port Triggering**，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 AP 打开所有开放端口来为正常连接提供保证。

单击 **Forwarding > Port Triggering**，可在图 4-30 的界面中设置端口触发功能。

Port Triggering						
ID	Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status	Modify
1	554	ALL	6970-6999	ALL	Enabled	Modify Delete

图 4-30 Port Triggering

单击 **Add New...** 按钮，可以在下图 4-31 所示界面中设置新的特殊应用程序条目。

Add or Modify a Port Triggering Entry

Trigger Port:	<input type="text" value="554"/>
Trigger Protocol:	<input type="text" value="ALL"/>
Incoming Ports:	<input type="text" value="6970-6999"/>
Incoming Protocol:	<input type="text" value="ALL"/>
Status:	<input type="text" value="Enabled"/>
Common Applications:	<input type="text" value="Quick Time 4"/>

图 4-31 Add or Modify a Triggering Entry

- Trigger Port:** 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。
- Trigger Protocol:** 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。
- Incoming Ports Range:** 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。
- Incoming Protocol:** 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。
- Status:** 设置该条目是否生效。只有状态为**Enable**时，本条目的设置才有效。
- Common Applications:** 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“**Common Applications**”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。

4.9.3 DMZ (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 Virtual Servers，当需要设置的 Virtual Servers 的 Service Port 不确定时，可以把它设置成 DMZ 主机。

单击**Forwarding > DMZ**，可以在图 4-32所示界面中设置DMZ主机。

图 4-32 DMZ

Current DMZ Status: 选择是否启用 DMZ 主机功能。

DMZ Host IP Address: 输入要设置为 DMZ 主机的局域网计算机的静态 IP 地址。

点击 **Save** 按钮使设置生效。

因特网用户访问 DMZ 主机的方法与访问虚拟服务器的方法相同。

注意:

1. 添加DMZ主机可能会给该主机带来不安全因素，因此不要轻易使用这一选项。
2. DMZ主机的优先级低于Virtual Servers，因特网用户对AP同一端口的访问将优先转发到Virtual Servers所对应的局域网服务器上。

4.9.4 UPnP (UPnP设置)

依靠 UPnP(Universal Plug and Play, 通用即插即用)协议功能，局域网中的主机可以请求 AP 自动进行端口转换,使得外部主机能够在需要时访问内部主机上的资源,如 Windows XP 和 Windows ME 系统上安装的 MSN Messenger 或迅雷、BT、PPLive 等支持 UPnP 协议的应用程序。

单击**Forwarding >UPnP**，可以在图 4-33中查看UPnP信息。

图 4-33 UPnP Settings

Current UPnP Status 选择是否启用 UPnP 功能。

App Description: 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。

External Port: 显示端口转换时使用的路由器端口号。

Protocol: 显示进行端口转换时采用的协议类型。

Internal Port: 显示需要进行端口转换的局域网主机端口号。

IP Address: 显示需要进行端口转换的局域网主机 IP 地址。

Status: 显示该条目是否已经启用。

4.10 Security（安全功能）

Security用来保护您的网络，在Security菜单下有 6 个子菜单(如图 4-34)：**Firewall**、**IP Address Filtering**、**Domain Filtering**、**MAC Address Filtering**、**Remote Management**和**Advanced Security**。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。



图 4-34 The Security menu

4.10.1 Firewall（防火墙）

本节介绍防火墙的各个过滤功能的开启与关闭设置。只有防火墙的总开关是开启的时候，后续的“IP Address Filtering”、“Domain Filtering”、“MAC Address Filtering”才能够生效。

单击**Security > Firewall**，可以在图 4-35中设置防火墙功能。

 A screenshot of the "Firewall" configuration page. The page has a green header bar with the word "Firewall" in white. Below the header, there are several configuration options, each with a checkbox:

- Enable Firewall (the general firewall switch)
- Enable IP Address Filtering

 Under "Enable IP Address Filtering", there is a section titled "Default IP Address Filtering Rules:" with two radio button options:

- Allow the packets not specified by any filtering rules to pass through the device
- Deny the packets not specified by any filtering rules to pass through the device

 Below these are two more checkbox options:

- Enable Domain Filtering
- Enable MAC Address Filtering

 Under "Enable MAC Address Filtering", there is a section titled "Default MAC Address Filtering Rules:" with two radio button options:

- Allow these PCs with enabled rules to access the Internet
- Deny these PCs with enabled rules to access the Internet

 At the bottom of the page, there is a "Save" button.

图 4-35 Firewall Settings

Enable Firewall: 请选择是否开启防火墙功能。这是防火墙的总开关，当该开关关闭时，后续的“IP Address Filtering”、“Domain Filtering”、“MAC Filtering”将全部失效。

Enable IP Address Filtering:

请选择是否开启 IP Address Filtering 功能，只有选择该项时，IP Address Filtering 设置才能生效。

Enable Domain Filtering:

请选择是否开启防火墙的 Domain Filtering 功能，只有选择该项时，Domain Filtering 设置才能生效。

Enable MAC Filtering: 请选择是否开启防火墙的 MAC Address Filtering 功能，只有选择该项时，MAC Address Filtering 设置才能生效。

点击 **Save** 按钮使设置生效。

4.10.2 IP Address Filtering (IP地址过滤)

单击 **Security > IP Address Filtering**，可以在图 4-36中设置IP地址过滤功能。

图 4-36 IP address Filtering

Add New...: 点击该按钮，可以添加新的过滤条目。

Enabled All: 点击该按钮，可以将列表中的所有过滤条目的状态设置为“生效”。

Disabled All: 点击该按钮，可以将列表中的所有过滤条目的状态设为“失效”。

Delete All: 点击该按钮，可以删除该列表中的所有过滤条目。

Move: 通过条目序号，可以将某条记录移动到另一个位置，以达到不同的过滤优先级。

如果禁用该功能，请保持默认设置。如果设置IP地址过滤功能，首先您需要在图 4-35中开启防火墙，然后在图 4-36中启用（Enable）该功能，然后点击**Add New...**按钮，将弹出如图 4-37所示界面。

Add or Modify an IP Address Filtering Entry

Effective time:	<input type="text" value="0000"/> - <input type="text" value="2400"/>
LAN IP Address:	<input type="text"/> - <input type="text"/>
LAN Port:	<input type="text"/> - <input type="text"/>
WAN IP Address:	<input type="text"/> - <input type="text"/>
WAN Port:	<input type="text"/> - <input type="text"/>
Protocol:	<input type="text" value="ALL"/> ▼
Action:	<input type="text" value="Deny"/> ▼
Status:	<input type="text" value="Enabled"/> ▼

图 4-37 Add or Modify an IP Address Filtering Entry

- Effective Time:** 设置规则生效的起始时间和终止时间。格式为 hhmm，例如 0803，表示 8 时 3 分。
- LAN IP Address:** 设置局域网中被控制的计算机的 IP 地址，为空表示对局域网中所有计算机进行控制。
- LAN Port:** 设置局域网中被控制的计算机的服务端口，为空表示对该计算机所有服务端口进行控制。
- WAN IP Address:** 设置广域网中被控制的网站的 IP 地址，为空表示对整个广域网进行控制。
- WAN Port:** 设置广域网中被控制的网站的服务端口，为空表示对该网站的所有服务端口进行控制。
- Protocol:** 设置被控制的数据包所使用的协议。
- Action:** 设置符合本条目设置规则的数据包是否可以通过 AP。
- Status:** 选择是否使本条过滤规则生效。

点击 **Save** 按钮使设置生效。

举例: 如果您想设置局域网中 IP 地址为 192.168.1.7 的计算机不能收发邮件; IP 地址为 192.168.1.8 的计算机不能访问 IP 为 202.96.134.12 的网站，对局域网中的其它计算机则不做任何限制。您需要配置如下条目:

ID	Effective time	LAN IP Address	LAN Port	WAN IP Address	WAN Port	Protocol	Action	Status	Modify
1	0000-2400	192.168.1.7	-	-	25	ALL	Deny	Enabled	Modify Delete
2	0000-2400	192.168.1.7	-	-	110	ALL	Deny	Enabled	Modify Delete
3	0000-2400	192.168.1.8	-	202.96.134.12	-	ALL	Deny	Enabled	Modify Delete

4.10.3 Domain Filtering (域名过滤)

单击 **Security > Domain Filtering**，可以在图 4-38 中设置域名过滤功能。

Domain Filtering

Firewall Settings (You can change them on Firewall page)

Enable Firewall: **Disabled**

Enable Domain Filtering: **Disabled**

ID	Effective time	Domain Name	Status	Modify
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>				
<input type="button" value="Previous"/> <input type="button" value="Next"/>				

图 4-38 Domain Filtering

- Add New...:** 点击该按钮，可以添加新的过滤条目。
- Enabled All:** 点击该按钮，可以将列表中的所有过滤条目的状态设置为“生效”。
- Disabled All:** 点击该按钮，可以将列表中的所有过滤条目的状态设为“失效”。
- Delete All:** 点击该按钮，可以删除该列表中的所有过滤条目。

在添加域名过滤条目之前，您需要在图 4-35 中开启防火墙，然后在图 4-38 中启用（Enable）该功能，然后点击 **Add New...** 按钮，将弹出如图 4-39 所示界面。

Add or Modify an Domain Filtering Entry

Effective Time: -

Domain Name:

Status: ▼

图 4-39 Add or Modify a Domain Filtering entry

- Effective Time:** 设置规则生效的起始时间和终止时间。例如，如果您输入 0803 – 1705，表示规则生效时间从 08:03 到 17:05。
- Domain Name:** 设置希望控制的域名。留空表示广域网中的所有域名。如 www.xxyy.com.cn, .net。
- Status:** 选择是否使本条过滤规则生效。

点击 **Save** 按钮使设置生效。

举例：如果您想阻止局域网中的计算机登录 www.xxyy.com.cn、www.aabbcc.com 和以.net 结尾的域名，其他域名不做限制。您需要配置如下条目：

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.xxyy.com.cn	Enabled	Modify Delete
2	0000-2400	www.aabbcc.com	Enabled	Modify Delete
3	0000-2400	.net	Enabled	Modify Delete

4.10.4 MAC Address Filtering (MAC地址过滤)

单击**Security > Domain Filtering**，可以在图 4-40中设置MAC地址过滤功能。

MAC Address Filtering

Firewall Settings (You can change them on Firewall page)

Enable Firewall: **Disabled**

Enable MAC Address Filtering: **Disabled**

Default Filtering Rules: **Deny** these PCs with the enabled rules to access the Internet.

ID	MAC Address	Description	Status	Modify
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>				

图 4-40 MAC address Filtering

- Add New...:** 点击该按钮，可以添加新的过滤条目。
- Enabled All:** 点击该按钮，可以将列表中的所有过滤条目的状态设置为“生效”。
- Disabled All:** 点击该按钮，可以将列表中的所有过滤条目的状态设为“失效”。
- Delete All:** 点击该按钮，可以删除该列表中的所有过滤条目。

在添加MAC地址过滤条目之前，您需要在图 4-35中开启防火墙，然后在图 4-40中启用（Enable）该功能，然后点击**Add New...**按钮，将弹出如图 4-41所示界面。

Add or Modify a MAC Address Filtering Entry

MAC Address:

Description:

Status:

图 4-41 Add or Modify a MAC Address Filtering entry

MAC Address: 设置希望控制的计算机的 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 00-0E-AE-B0-00-0B。

Description: 设置对该计算机的适当描述。例如 John's PC。

Status: 选择是否使本条过滤规则生效。

点击 **Save** 按钮使设置生效。

举例: 如果您想阻止 MAC 地址为 00-0A-EB-00-07-BE 和 00-0A-EB-00-07-5F 的计算机访问广域网。您需要配置如下条目:

ID	MAC Address	Description	Status	Modify
1	00-0A-EB-00-07-BE	John's PC	Enabled	Modify Delete
2	00-0A-EB-00-07-5F	Alice's PC	Enabled	Modify Delete

4.10.5 Remote Management (远程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。

点击 **Security > Remote Management**, 可以在图 4-42 中设置远端 WEB 管理功能。

图 4-42 Remote Management

Web Management Port: 用于访问 AP 的 WEB 管理端口号。AP 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 88), 则必须用 “http://IP 地址: 端口” 的方式 (例如 http://192.168.1.254:88) 才能登录 AP 执行 WEB 界面管理。此功能需要重启 AP 后才生效。

Remote Management IP Address:

广域网中可以访问该 AP 执行远端 WEB 管理的计算机 IP 地址。AP 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 AP 执行远端 WEB 管理。如果改变了默认的远端 WEB 管理 IP 地址, 则广域网中只有具有该指定 IP 地址的计算机才能登录 AP 执行远端 WEB 管理。如果改为 255.255.255.255, 则广域网中所有主机都可以登录 AP 执行远端 WEB 管理。

点击 **Save** 按钮使设置生效。

4.10.6 Advanced Security (高级安全功能)

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所设置的值，那么该主机将被列入“Blocked DoS Host Table”而不能上网，从而很好地防止了 DoS 攻击。

点击 **Security > Advanced Security**，可以在图 4-43 中设置 DoS 攻击防范功能。

图 4-43 Advanced Security settings

Packets Statistic interval: 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。

DoS protection: 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。

Enable ICMP-FLOOD Attack Filtering:

若需要防范 ICMP-FLOOD 攻击，请选择此项。

ICMP-FLOOD Packets threshold:

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。

Enable UDP-FLOOD Filtering:

若需要防范UDP-FLOOD，请选择此项。

UDP-FLOOD Packets threshold:

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。

Enable TCP-SYN-FLOOD Attack Filtering:

若需要防范TCP-SYN-FLOOD，请选择此项。

TCP-SYN-FLOOD Packets threshold:

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。

Ignore Ping Packet from WAN Port:

若开启该功能，广域网的计算机将不能Ping通AP。

Forbid Ping Packet from LAN Port:

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。

Blocked DoS Host Table: 点击该按钮，你可以查看被禁止的主机列表。

点击 **Save** 按钮使设置生效。

4.11 Static Routing（静态路由表）

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/主机，然后AP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。

可以在图 4-44中设置静态路由功能。

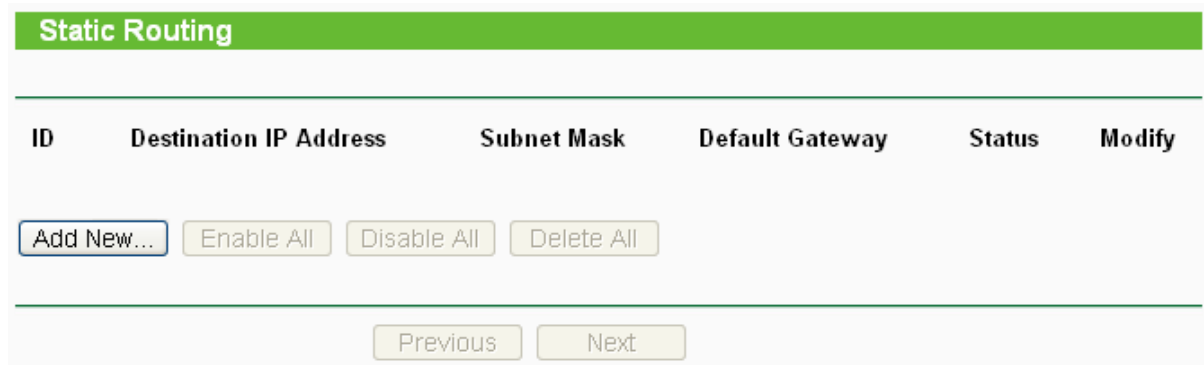


图 4-44 Static Routing

Add New...: 点击该按钮，可以添加新的过滤条目。

Enabled All: 点击该按钮，可以将列表中的所有过滤条目的状态设置为“生效”。

Disabled All: 点击该按钮，可以将列表中的所有过滤条目的状态设为“失效”。

Delete All: 点击该按钮，可以删除该列表中的所有过滤条目。

点击**Add New**按钮，你可以在下图中添加静态路由条目。如图 4-45。

图 4-45 Add or Modify a Static Route Entry

Destination IP Address: 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。

Subnet Mask: 该项与目的 IP 地址一起来标识目标网络。

Default Gateway: 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。

Status: 显示该条目是否生效。只有状态为生效（**Enabled**）时，此路由条目才起作用。

4.12 IP & MAC Binding (IP、MAC地址绑定)

IP & MAC Binding，可以有效防止 ARP 攻击，维护局域网用户的上网安全。

在IP & MAC Binding菜单下有 2 个子菜单(如图 4-46): **Binding Setting**和**ARP List**。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

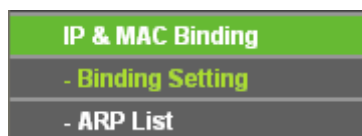


图 4-46 the IP & MAC Binding menu

4.12.1 Binding Setting (绑定设置)

静态 ARP 绑定，即 IP 与 MAC 绑定，是防止 ARP 攻击本 AP 的有效方法。

AP 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 AP 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。

点击**IP & MAC Binding > Binding Setting**，可以在图 4-47所示界面中设置静态ARP绑定条目。

ARP Binding: Disable Enable

ID	MAC Address	IP Address	Bind	Modify
1	00-0A-EB-00-07-BE	192.168.1.101	<input checked="" type="checkbox"/>	Modify Delete

Page 1

图 4-47 Binding Setting

ARP Binding: 选择是否开启ARP绑定功能，只有选择“Enable”并单击**Save**后，列表中的设置才能生效。

单击**Add New...**按钮，可以在图 4-48所示界面中设置新的静态ARP绑定条目。

Bind:

MAC Address:

IP Address:

图 4-48 IP & MAC Binding Setting (Add & Modify)

Bind: 设置本条目状态，只有选中该项，该条绑定条目才能生效。

MAC Address: 输入被绑定主机的 MAC 地址。

IP Address: 输入被绑定主机的 IP 地址。

4.12.2 ARP List (ARP列表)

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 映射表就是用来存储与维护这些对应信息的。

单击**IP & MAC Binding > ARP List**，可以在图 4-49所示界面中查看ARP条目信息。

ARP List				
ID	MAC Address	IP Address	Status	Configure
1	00-19-66-CB-45-66	192.168.1.93	Unbound	Load Delete
2	00-0A-EB-00-07-BE	192.168.1.101	Bound	Load Delete

图 4-49 ARP List

MAC Address: 被绑定主机的 MAC 地址。

IP Address: 被绑定主机的 IP 地址。

Status: 选择本条目是否生效。

Load: 将相应条目的ARP信息添加到图 4-47界面的静态ARP绑定列表中。

Load All: 将当前ARP映射列表中所有条目的信息添加到图 4-47界面的静态ARP绑定列表中。

Bind All: 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。

4.13 Dynamic DNS (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。如果AP的WAN口IP地址为动态获取的，通过此功能可使互联网上的其它主机用固定域名的方式访问AP或虚拟服务器。

动态DNS功能对于使用动态IP地址的用户，在每次上网得到新的IP地址后，AP内置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。此功能对于大多数不使用固定IP地址的用户，也可以经济、高效地构建自身的服务网络。

在使用本功能之前，您需要在DDNS服务商处注册，如www.dyndns.org、www.oray.net或者www.comexe.cn，注册后DDNS服务商会给您提供密码。

4.13.1 Dyndns.org DDNS

如果您在Service Provider处选择www.dyndns.org，将会弹出图 4-50所示页面。

DDNS

Service Provider: DynDNS (www.dyndns.org) [Go to register...](#)

User Name:

Password:

Domain Name:

Enable DDNS

Connection Status: DDNS not launching!

图 4-50 DynDNS.org DDNS Settings

User Name、Password: 请正确填写在DDNS上注册的用户名和密码。

Domain Name: 填写动态DNS服务商提供的域名。

Enable DDNS: 勾选启用DDNS服务。

Connection Status: 查看DDNS服务器的连接状态。

Login/Logout: 点击该按钮，可以登录/退出DDNS服务。

4.13.2 Oray.net DDNS

如果您在**Service Provider**处选择www.oray.net，将会弹出图 4-51所示页面。

DDNS

Service Provider: PeanutHull (www.oray.net) [Go to register...](#)

User Name:

Password:

Enable DDNS

Connection Status: DDNS not launching!

Service Type: ---

Domain Name: ---

图 4-51 Oray.net DDNS Settings

User Name、Password: 请正确填写在DDNS上注册的用户名和密码。

Enable DDNS: 勾选启用DDNS服务。

Connection Status: 查看DDNS服务器的连接状态。

Domain Name: 查看动态DNS服务商提供的域名。

Login/Logout: 点击该按钮，可以登录/退出DDNS服务。

4.13.3 Comexe.cn DDNS

如果您在**Service Provider**处选择www.comexe.cn，将会弹出图 4-52所示页面。

DDNS

Service Provider: Comexe (www.comexe.cn) [Go to register...](#)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name:

Password:

Enable DDNS

Connection Status: DDNS not launching!

图 4-52 Comexe.cn DDNS Settings

- Domain Name:** 填写动态DNS服务商提供的域名。
- User Name、Password:** 请正确填写在DDNS上注册的用户名和密码。
- Enable DDNS:** 勾选启用DDNS服务。
- Connection Status:** 查看DDNS服务器的连接状态。
- Login/Logout:** 点击该按钮，可以登录/退出DDNS服务。

4.14 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，选择启用功能，并在下面页面中设置参数。如图 4-53。



图 4-53 SNMP Settings

4.14.1 Community Setting（团体设置）

单击 **SNMP > Community Setting**，可以在图 4-54中设置SNMP团体。

Community List				
Num	Community	Access Mode	Status	Status
1	public	Read Only	Disable	Modify
2	public	Read Only	Disable	Modify
3	public	Read Only	Disable	Modify
4	public	Read Only	Disable	Modify

图 4-54 Community Setting

- Num:** 显示团体名的序号。
- Community:** 设备连接SNMP管理端软件的登录密码。
- Access Mode:** 选择团体名的权限。Read Only表示团体对SNMP信息只有读取权限；Read&Write表示团体对SNMP信息具有读写权限。
- Status:** 选择是否启用相应团体名。
- Modify:** 修改本条目。
- Enabled All:** 点击该按钮，可以将列表中的所有条目的状态设置为“生效”。
- Disabled All:** 点击该按钮，可以将列表中的所有条目的状态设为“失效”。

4.14.2 SNMP System Setting (SNMP系统设置)

点击SNMP > SNMP Setting，可以在图 4-55中设置SNMP系统参数。

SNMP System Settings	
System Contact:	<input type="text"/>
System Name:	<input type="text"/>
System Location:	<input type="text"/>
<input type="button" value="Save"/>	

图 4-55 SNMP System Setting

- System Contact:** SNMP系统的管理员联系信息。
- System Name:** 本设备的系统名称。
- System Location:** 本设备的联系人位置信息。

4.15 System Tools（管理工具）

System Tools帮助您优化设备的配置。在System Tools菜单下有 10 个子菜单(如图 4-56)：**Time**、**Firmware**、**Factory Defaults**、**Backup & Restore**、**Ping Watch Dog**、**Speed Test**、**Reboot**、**Password**、**Syslog** 和 **Statistics**。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。



图 4-56 The System Tools menu

4.15.1 Time（时间设置）

单击**System Tools > Time**，可以在下图 4-57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。

 The "Time Settings" page has a green header. Below it, there are several configuration sections:

- Time Zone:** A dropdown menu showing "(GMT+08:00) Beijing, Hong Kong, Perth, Singapore".
- Date:** Three input boxes for month (1), day (1), and year (2006), with "(MM/DD/YY)" to the right.
- Time:** Three input boxes for hour (9), minute (5), and second (11), with "(HH/MM/SS)" to the right.
- Using Daylight Saving Time:** An unchecked checkbox.
- DST begin:** Three input boxes for month, day, and hour, with "(MM/DD/HH)" to the right.
- DST end:** Three input boxes for month, day, and hour, with "(MM/DD/HH)" to the right.
- Preferable NTP Server:** Two input boxes, both containing "0.0.0.0". Below them is a "Get GMT" button with the text "(Get GMT when connected to Internet)".

 At the bottom of the page is a "Save" button.

图 4-57 Time settings

Preferable NTP Server:

该项用来设置NTP Server的IP地址(最多可以输入两个)。NTP Server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 Server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。

Date: 填写本地的日期，格式为月/日/年。

Time: 填写本地时间，格式为时/分/秒。

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

 **注意:**

1. 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。
2. 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。

4.15.2 Firmware（软件升级）

点击**System Tools > Firmware**，可以在下图 4-58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。

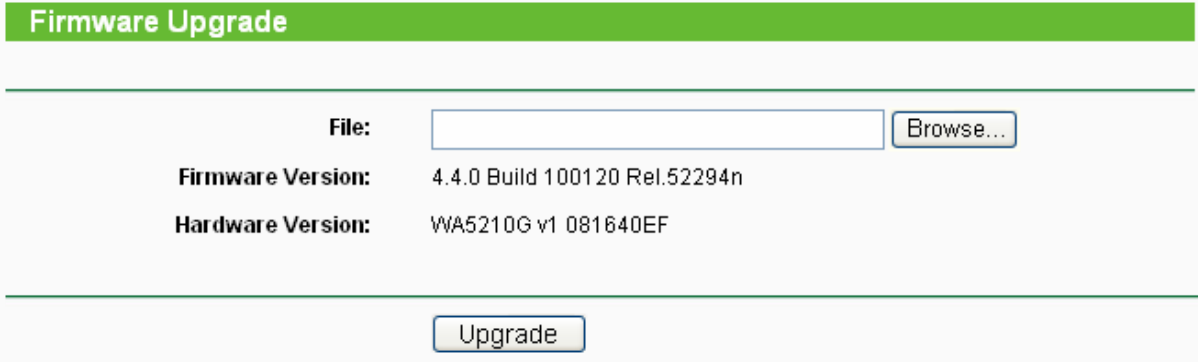


图 4-58 Firmware Upgrade

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 **Browse** 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：单击 **Upgrade** 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。

Firmware Version: 显示设备当前的软件版本。

Hardware Version: 显示设备当前的硬件版本。

4.15.3 Factory Defaults（恢复出厂设置）

点击**System Tools > Factory Default**，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 4-59。

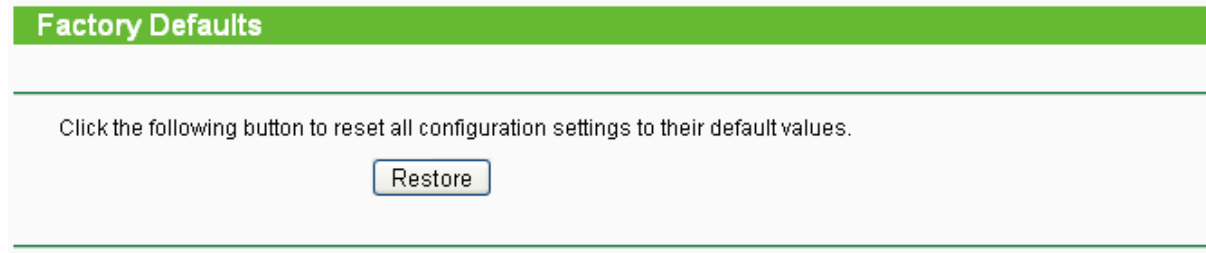


图 4-59 Restore Factory Default

单击**Restore**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。

4.15.4 Backup & Restore（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**System Tools > Backup & Restore**，可以在下图 4-60中备份或载入AP的配置文件。



图 4-60 Save or Restore the Configuration

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。

4.15.5 Ping Watch Dog（看门狗）

看门狗功能使接入器通过连续 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 **System Tools > Ping Watch Dog**，您可以在下图 4-61 界面中配置看门狗功能。

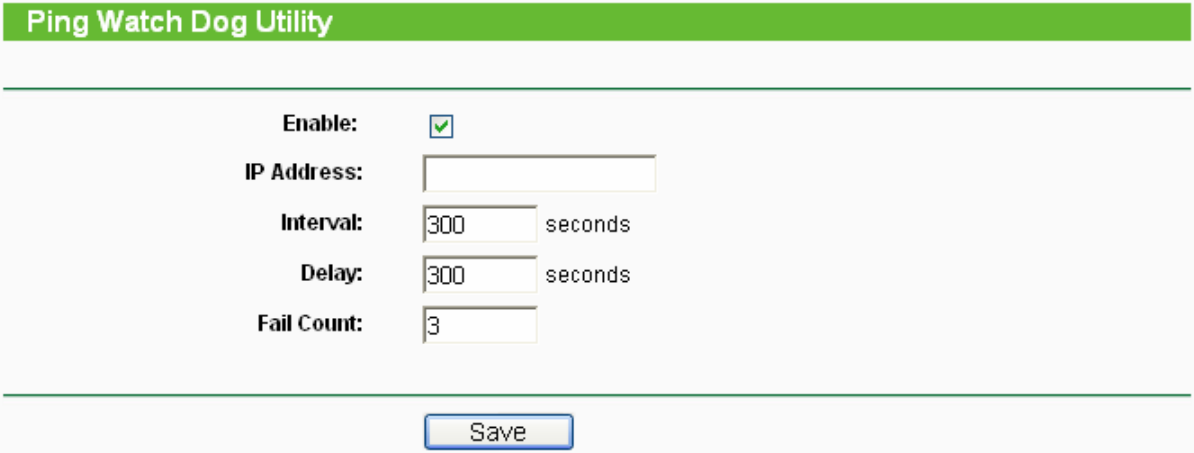


图 4-61 Ping Watch Dog Utility

- Enable:** 勾选启用看门狗功能。
- IP Address:** 看门狗发送 Ping 数据包的目的主机的 IP 地址。
- Interval:** 发送两个连续 Ping 数据包的时间间隔。
- Delay:** AP 重启之后到发送第一个 Ping 数据包之前的时间延迟。
- Fail Count:** 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

4.15.6 Speed Test（速率检测）

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。如果远程设备也是 **TL-WA5210G**，您可以在 **Advance options** 页面输入远程设备的用户名和密码，获取精确的预留带宽值。

点击 **System > Speed Test**，可以在图 4-62 中配置速率测试功能。

图 4-62 Speed Test

- Destination IP:** 远程设备的 IP 地址
- User、Password:** 远程设备的登录账号名和密码。如果您想要获得精确的测试数据，请正确填写。反正则留空。
- Advanced options:** 勾选是否进行高级设置。如果您需要精确测试数据，请勾选此项。
- Direction:** 速率测试时的三种传输方向选项。**transmit** 测试输出带宽；**receive** 测试输入带宽；**both** 测试输出带宽和输入带宽。
- Duration:** 填写测试持续时间。
- Data amount:** 在整个测试过程中的发送的最大数据包数。

注意:

1. 如果User或Password错误，设备将自动转换为基本测试，即高级配置将会失效。
2. 如果指定Duration和Data amount，超出设置值后测试将自动停止。

4.15.7 Reboot（重启）

点击**System Tools > Reboot**，可以将AP重新启动，如图 4-63。

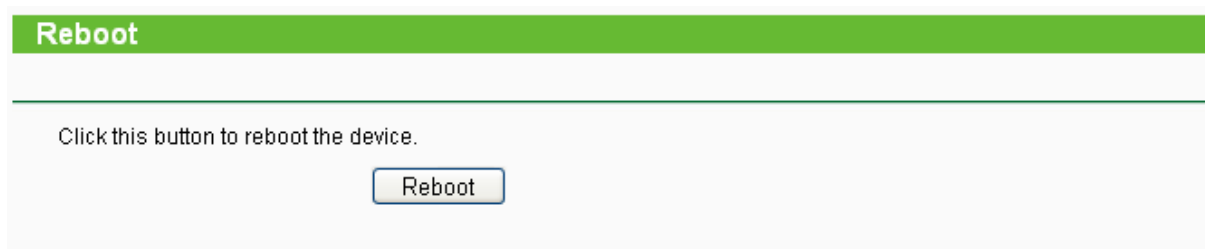


图 4-63 Reboot the AP

本 AP 的某些设置需要在路由器重新启动后才能生效。

- 对 AP 进行软件升级
- 恢复 AP 的出厂设置
- 修改 LAN 口的基本网络参数
- 设置 DHCP 服务功能
- 设置 DHCP 服务器的静态地址分配功能

手动重启的方法：单击图 4-63 中的 **Reboot** 按钮。

4.15.8 Password（修改登录口令）

点击 **System Tools > Password**，可以在下图 4-64 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 **Save** 按钮即可。

图 4-64 Password

注意：

出于安全考虑，我们强烈推荐您更改初始系统管理员的用户名及密码。如果忘了系统密码，请将路由器恢复到出厂设置。

4.15.9 Syslog（系统日志）

点击 **System Tools > System Log**，可以在下图 4-65 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。

图 4-65 System Log

4.15.10 Statistics (流量统计)

点击**System Tools > Statistics**，可以在下图 4-66中查看AP的流量信息。单击**Refresh**按钮，可以更新流量统计表；单击AP数据流量统计表中对应条目后的**Reset**，可以将该条目当前的流量数据全部清零，并重新开始统计；单击**Delete**，可以删除指定的流量统计信息。

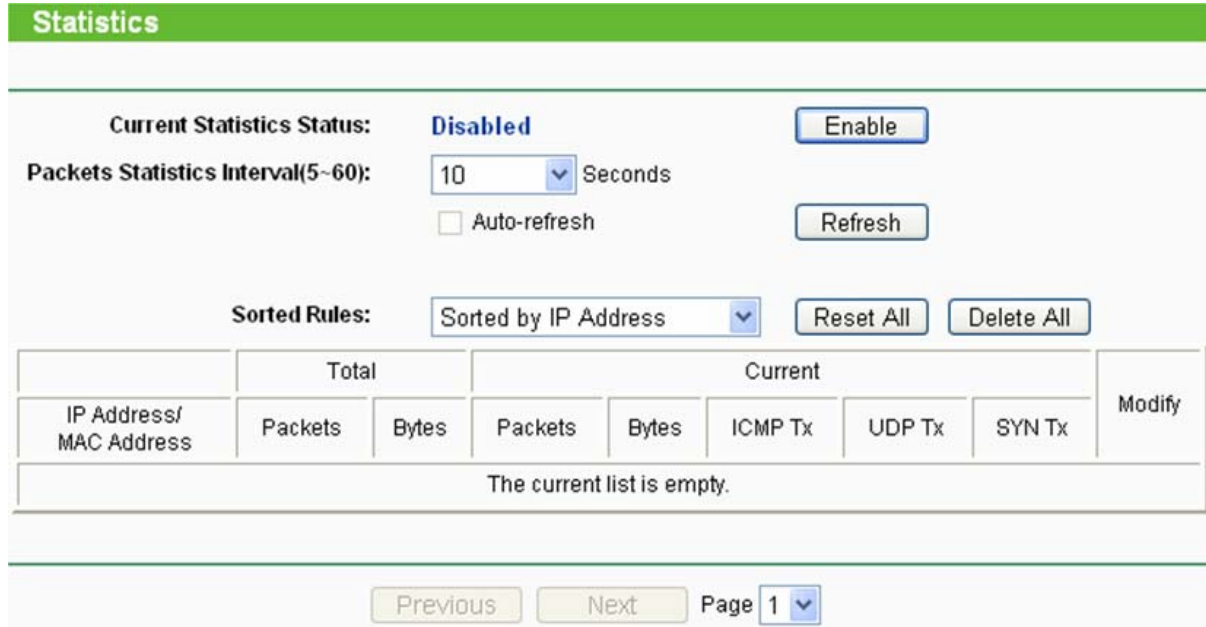


图 4-66 Statistics

Current Statistics Status: 显示流量统计功能是否开启，默认为关闭。如果关闭此功能，Security settings 处的 DoS protection 功能将失效。

Packets Statistics Interval: 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。

Sorted Rules: 此处列出分类规则。

统计表:

IP Address		被统计主机的 IP 地址，此处也会显示该主机的 MAC 地址。
Total	Packets	接受和发送的数据包总数。
	Bytes	接受和发送的字节总数。
Current	Packets	每秒接受和发送的数据包数。
	Bytes	每秒接受和发送的字节数。
	ICMP Tx	WAN 口每秒发送的 ICMP 数据包数。
	UDP Tx	WAN 口每秒发送的 UDP 数据包数。
	TCP SYN Tx	WAN 口每秒发送的 TCP SYN 数据包数。

第5章 AP 工作模式

本章介绍了在 AP 工作模式下，如何使用 Web 管理页面配置 AP 的高级功能。

5.1 Login（登录）

启动AP并成功登录AP管理页面后，在左侧菜单栏中，共有如下几个菜单：**Status**、**Quick Setup**、**Operation Mode**、**Network**、**Wireless**、**DHCP**、**Wireless Settings**、**SNMP**和**System Tools**。。单击某个菜单项，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 Status（系统状态）

选择菜单 **Status**，可以查看 AP 当前的状态信息。

Status

Firmware Version: 4.4.1 Build 100222 Rel.56698n
Hardware Version: WA5210G v1 081640EF

Wired

MAC Address: 00-0A-EB-90-00-08
IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0

Wireless

Operating Mode: Access Point
SSID: TP-LINK_900008
Channel: 1
Mode: 54Mbps (802.11g)
MAC Address: 00-0A-EB-90-00-08

Traffic Statistics

	Received	Sent
Bytes:	0	1404
Packets:	0	24

System Up Time: 0 day(s) 00:02:28

图 5-1 Status

- Wired:** 此处显示 AP 当前的 MAC 地址、IP 地址和子网掩码。
- Wireless:** 此处显示 AP 当前的无线设置状态，包括 SSID、信道和频段带宽等信息。您可以在 **Wireless > Basic Settings** 界面进行相关设置。
- Traffic Statistics:** 此处显示 AP 当前的数据传输状态。
- System Up Time:** 此处显示 AP 当前的运行时间。

5.3 Quick Setup（快速安装）

请参见 [3.2: "快速安装指南"](#)。

5.4 Operation Mode（工作模式）

本页用来选择 AP 的工作模式。本设备有 3 个工作模式供您选择：**AP Client Router**、**AP Router** 和 **AP** 模式，请选择一个您需要的，并且点击 **Save** 保存。

图 5-2 Operation Mode

AP Client Router: 在本模式下，有 WISP 的支持，无线设备可以通过 AP 以无线的方式直接接入互联网，以太网端口通过无线端口直接从 WISP 处获取相同的 IP 地址，无线端口相当于 WAN 口，以太网端口相当于 LAN 口。

AP Router: 在本模式下，设备允许用户通过 ADSL/Cable Modem 设备连接互联网，无线端口通过以太网 WAN 口从 ISP 处获取相同的 IP 地址，无线端口相当于一个 LAN 口。

AP: 在本模式下，设备允许多个无线客户端通过 WIFI 接入无线局域网，以太网端口和无线端口均相当于 LAN 口。

5.5 Network（网络参数）

点击 **Network**，在图 5-3 中配置 AP 的网络地址。

图 5-3 Network

IP Address: 输入 AP 的 IP 地址（默认为 192.168.1.254）。

Subnet Mask: 输入 AP 的子网掩码，通常为 255.255.255.0。

Gateway: 输入 AP 的网关，此处要与 IP 地址相同。

MAC Address: AP 在局域网中的 MAC 地址，用来标识局域网。

 **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) 保存配置后，设备将会自动重启。

5.6 Wireless（无线设置）

Wireless 功能，可以安全方便的启用 AP 的无线功能进行网络连接。

Wireless菜单下有 8 个子菜单(如图 5-4): **Basic Settings, Wireless Mode, Security Settings, MAC Filtering, Wireless Statistics, Distance Setting, Antenna Alignment** 和 **Throughput Monitor**。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

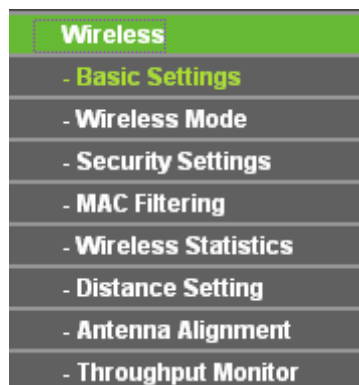


图 5-4 Wireless menu

5.6.1 Basic Settings（基本设置）

单击 **Wireless > Basic Settings**，可以在图 5-5中进行无线网络的基本设置。

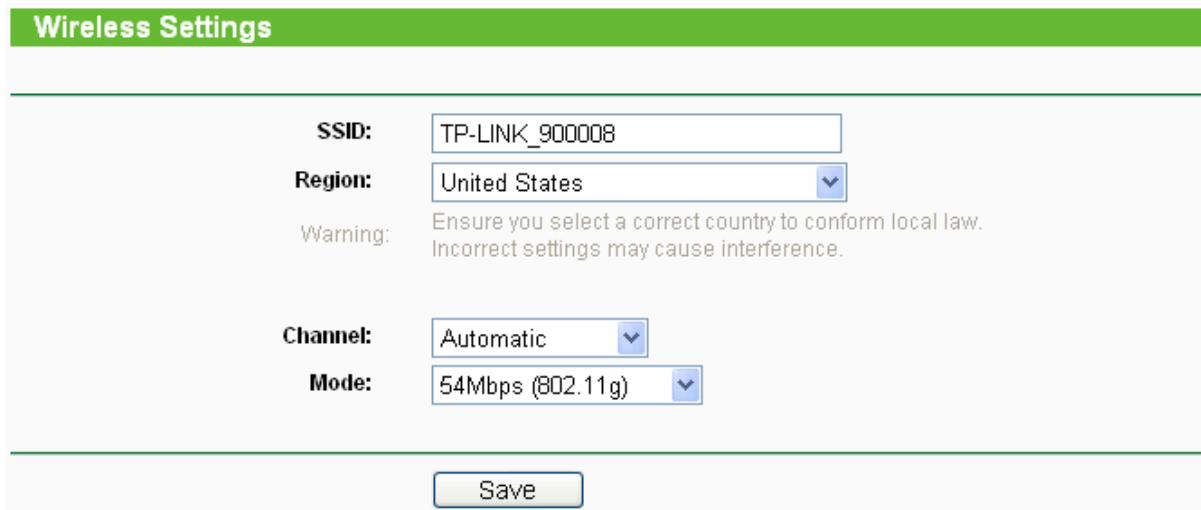
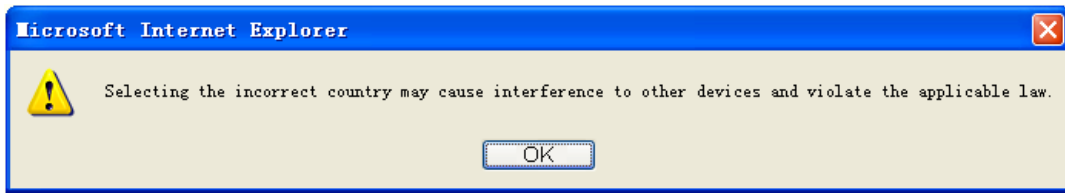


图 5-5 Wireless Settings in AP mode

- SSID:** 即 Service Set Identification，用于标识无线网络的名称。您可以在这里输入一个喜欢的名称，它将显示在无线网卡搜索到的无线网络列表中。（区分大小写）
- Region:** 选择您所在的地区。为设备的无线功能制定使用区域，来解决在某些地区除了菜

中罗列的区域外使用无线功能是非法的问题。如果您所在的地区没有罗列在菜单中，请联系当地的政府。

当选择您所在的区域后，点击 **Save** 按钮，将会显示如下图所示的对话框，点击 **OK**。



注意：

由于法律制约，北美地区没有region的选项。

Channel: 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。

Mode: 该项用于设置 AP 的无线工作模式。

完成更改后，点击 **Save** 按钮，AP 会自动重启使当前的设置生效。

5.6.2 Wireless Mode（无线模式）

点击**Wireless > Wireless Mode**，可以在图 5-6中选择设备的无线模式。

Wireless Mode Settings

 Access Point Enable SSID Broadcast Client Enable WDS SSID: TP-LINK_900008 MAC of AP: RepeaterMAC of AP: Universal RepeaterMAC of AP: Bridge (Point to Point) With AP ModeMAC of AP: Bridge (Point to Multi-Point) With AP ModeMAC of AP1: MAC of AP2: MAC of AP3: MAC of AP4: MAC of AP5: MAC of AP6:

Note: The current security method may be invalid after changing the wireless mode.

图 5-6 Wireless Mode

注意：

AP提供5个工作模式：Access Point、Client、Repeater、Bridge (point to point)和Bridge (point to Multi-point)。

Access Point: Access Point 模式允许无线接入点和 AP 客户端接入路由器。

Enable SSID Broadcast:

开启后无线客户端将可以通过搜索无线 SSID 来发现本 AP。

Client: 在 Client 模式下，AP 将成将等同于一个无线网卡，可以连入其他无线网络。

Enable WDS: 开启后，接入器将使用 4 地址包格式与 AP 通信，否则使用 3 地址包格式。

SSID: 您可以填入一个已有的 SSID，指定接入该无线网络。

MAC of AP: 您可以填入一个已有的 AP MAC 地址，指定接入该 AP 的无线网络。

Repeater: 该模式下接入器会转发来自指定的远端 AP 数据，从而扩大无线的覆盖范围。您可以填入一个已有的 AP MAC 地址，指定转发该 AP 的数据。

Universal Repeater:

该模式与 Repeater 模式相似，可扩大无线网络的覆盖范围，且兼容性更佳。您可以填入一个已有的 AP MAC 地址，指定转发该 AP 的数据。

完成更改后，点击 **Save** 按钮，AP 会自动重启使当前的设置生效。

您还可以单击“Survey”按钮，从扫描到的 AP 列表选择一个接入点，点击“Connect”连接，页面将自动返回到基本设置页，此时可以保存设置并重启，以使修改生效。

注意：

如果可达的 AP 不支持 WDS 功能，您可以选择不开启 WDS 的 Client 模式或者 Repeater 模式与之相连。

下面是如何搭建无线转发网络的例子，请参照以下步骤：

1. 配置 TL-WA5210G 室外 2.4GHz 高功率无线客户端设备的工作模式。

- 配置 AP1 为 Access Point 模式。
- 配置 AP2 为 Repeater 模式，并在 MAC of AP 处填写 AP1 的 MAC 地址。
- 配置 AP3 为 Repeater 模式，并在 MAC of AP 处填写 AP2 的 MAC 地址。

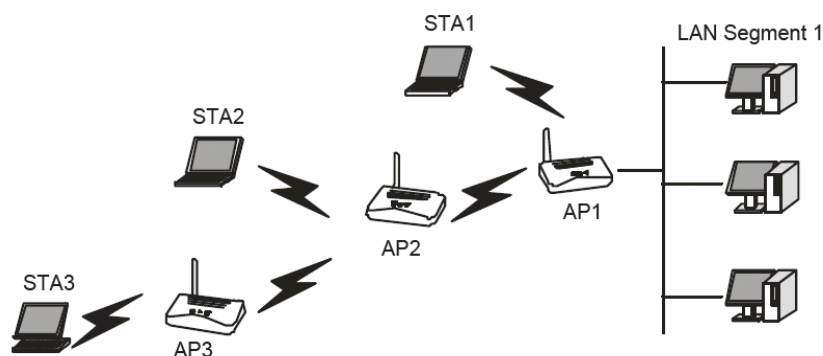


图 5-7 Wireless repeating

2. 检查所有设备的无线安全参数。

3. 检查网络的连通性。任意网段的计算机均能连接互联网或者可以与其他三个无线网段的计算机共享文件和打印机。

注意：

您可以在 Repeater 模式下重复增加 TL-WA5210G 室外 2.4GHz 高功率无线客户端设备。但是由于设备是以半双工模式通信的，所以带宽会随着设备的增加而减少。同时您也可以使用无线天线增加无线网络覆盖范围。

Bridge (Point to Point):

一对一桥接模式，用于连接两个局域网。

With AP mode: 如果您选择此项，您的 AP 工作在 Bridge (Point to Point)模式下同时支持 AP 模式。

下面是如何创建一对一网桥的例子，请参照以下步骤：

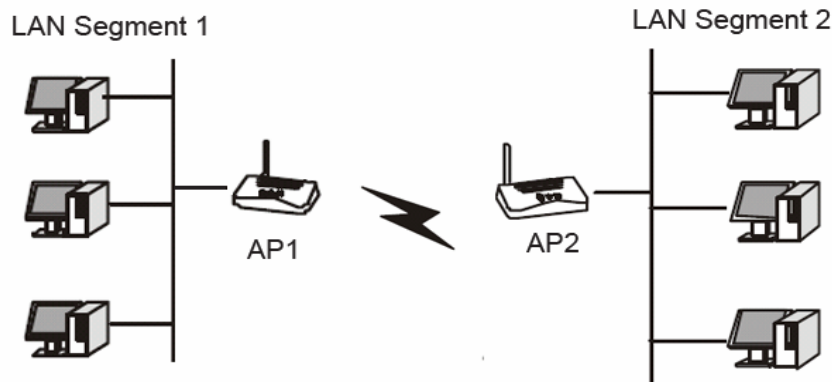


图 5-8 Point to Point Bridge

1. 配置 LAN1 的 TL-WA5210G (AP1) 为 Point-to-Point Bridge 模式。
2. 配置 LAN2 的 TL-WA5210G (AP2) 为 Point-to-Point Bridge 模式。AP1 必须在 MAC of AP 处填写 AP2 的 MAC 地址同时 AP2 必须在 MAC of AP 处填写 AP1 的 MAC 地址。
3. 检查两个 AP 必须在同一信道内并开启安全设置。
4. 检查两个网段的连通性。任意网段内的计算机均可连接互联网或者与其他计算机共享文件和打印机。

Bridge (Point to Multi-Point):

该模式允许接入器桥接不超过 6 个 AP，用于连接多个局域网。

With AP mode: 如果您选择此项，您的 AP 工作在 Bridge (Point to Point)模式下同时支持 AP 模式。

下面是如何创建一对多网桥的例子，请参照以下步骤：

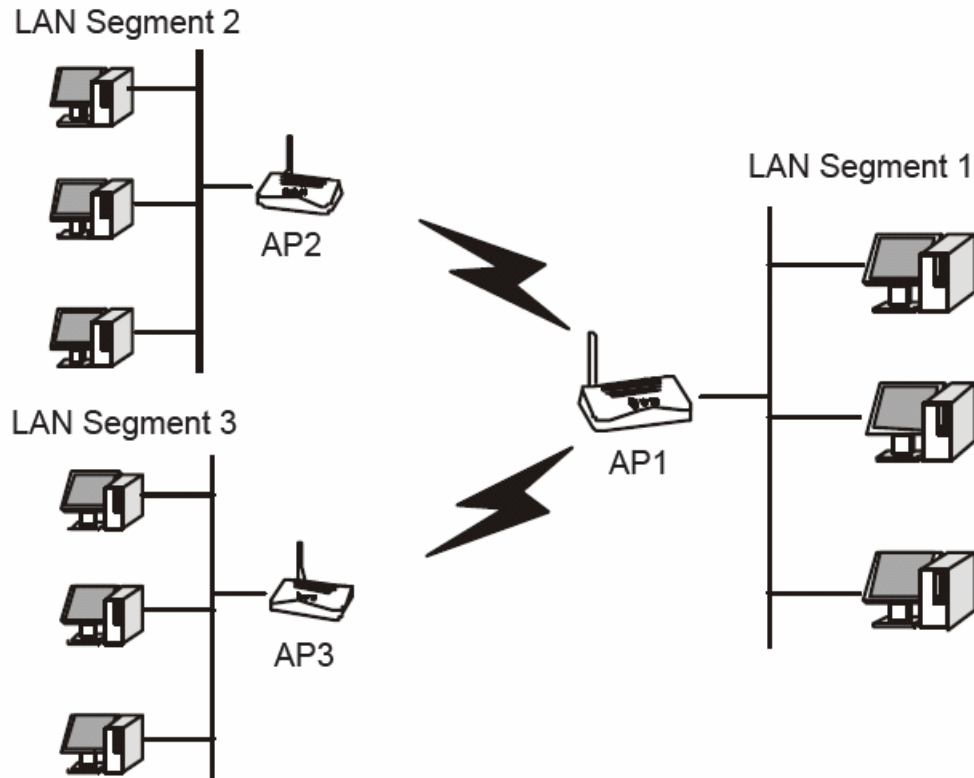


图 5-9 Point to Multi-point Bridge

1. 配置 TL-WA5210G 室外 2.4GHz 高功率无线客户端设备的工作模式。
 - 由于处在网络中心, AP1选择Point-to-Multi-Point Bridge 模式, 并在MAC of AP处填写AP2和AP3的MAC地址。
 - 配置AP2为Point-to-Point Bridge 模式, 并在MAC of AP处填写AP1的MAC地址。
 - 配置AP3为Point-to-Point Bridge 模式, 并在MAC of AP处填写AP1的MAC地址。
2. 对所有设备检查以下方面。
 - 所有AP必须工作在同一信道内并开启安全设置。
 - 所有Point-to-Point模式的AP必须在MAC of AP处填写AP1的MAC地址, AP1必须在MAC of AP处填写其他全部Point-to-Point 模式的AP的MAC地址。
3. 检查网络连通性。
 - 任意网段内的计算机均可连接互联网或者与其他计算机共享文件和打印机。

在上面例子中, 无线工作站不能连接 TL-WA5210G 室外 2.4GHz 高功率无线客户端设备, 如果您需要无线接入站登录任意局域网中, 您可以在任意局域网中添加一个工作在 Wireless Access Point 模式下的 TL-WA5210G 室外 2.4GHz 高功率无线客户端设备

您还可以单击“Survey”按钮, 从扫描到的 AP 列表中选择接入点, 单击“Connect”连接, 页面将自动返回到基本设置页, 此时可以保存设置并重启, 以使修改生效。

AP List

AP Count: 53

ID	BSSID	SSID	Signal	Channel	Security	Choose
1	00-21-27-4B-23-78	TP-LINK_4B2378	28 dB	11	OFF	Connect
2	00-1D-0F-98-2B-08	TP-LINK	25 dB	11	ON	Connect
3	00-08-01-00-00-80	AKING	18 dB	11	OFF	Connect

图 5-10 AP List

5.6.3 Security Settings（无线安全设置）

单击**Wireless > Security Settings**，可以在图 5-11界面中设置无线网络安全选项。

Wireless Security

Disable Security

WEP

Type:

WEP Key Format:

Key Selected	WEP Key	Key Type
Key 1: <input checked="" type="radio"/>	<input type="text"/>	Disabled <input type="text" value="Disabled"/>
Key 2: <input type="radio"/>	<input type="text"/>	Disabled <input type="text" value="Disabled"/>
Key 3: <input type="radio"/>	<input type="text"/>	Disabled <input type="text" value="Disabled"/>
Key 4: <input type="radio"/>	<input type="text"/>	Disabled <input type="text" value="Disabled"/>

WPA/WPA2

Version:

Encryption:

Radius Server IP:

Radius Port: (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: (in second, minimum is 30, 0 means no update)

WPA-PSK/WPA2-PSK

Version:

Encryption:

PSK Passphrase:

(The Passphrase is between 8 and 63 characters long)

Group Key Update Period: (in second, minimum is 30, 0 means no update, only be valid in AP mode.)

Note: Some security mode can not be selected since it can not be supported by the current wireless mode.

图 5-11 Wireless Security

在 **Wireless > Security Settings** 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**Disable Security**以关闭无线安全功能。
- 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：**WEP**、**WPA/WPA2** 以及 **WPA-PSK/WPA2-PSK**。不同的安全类型下，安全设置项不同，下面将详细介绍。

1. WPA-PSK/WPA2-PSK

WPA-PSK/WPA2-PSK安全类型其实是**WPA/WPA2**的一种简化版本，它是基于共享密钥的**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。

Version: 该项用来选择系统采用的安全模式，即**Automatic**、**WPA-PSK**、**WPA2-PSK**。

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

Encryption: 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 Passphrase: 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。

Group Key Update Period:

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

WPA/WPA2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。

Version: 该项用来选择系统采用的安全模式，即Automatic、WPA、WPA2。

- **Automatic:** 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。

Encryption: 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: 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 Port: 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 Password: 该项用来设置访问Radius服务的密码。

Group Key Update Period:

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。

Type: 该项用来选择系统采用的安全模式，包括Automatic、Shared Key、Open System。

- **Automatic:** 若选择该项，AP会根据主机请求自动选择Open System或Shared Key方式。
- **Open System:** 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。
- **Shared Key:** 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。

WEP Key Format: 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 Key、Key Type:

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。

密钥长度说明：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。

 **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。

5.6.4 MAC Filtering（无线MAC地址过滤）

MAC Filtering 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。

单击**Wireless > MAC Filtering**，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 5-12。

图 5-12 Wireless MAC address Filtering

Add New...: 点击该按钮，可以添加新的过滤条目。

Enabled All: 点击该按钮，可以将列表中的所有条目的状态设置为“生效”。

Disabled All: 点击该按钮，可以将列表中的所有条目的状态设为“失效”。

Delete All: 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，请选择 **Allow the stations not specified by any enabled entries in the list to access**；如果不允许未知无线客户端接入，请选择 **Deny the stations not specified by any enabled entries in the list to access**。

点击 **Add New...** 按钮，添加 MAC 地址过滤规则条目。然后 **Add or Modify Wireless MAC Address Filtering entry** 页面将会弹出，如图 5-13 所示。

图 5-13 Add or Modify Wireless MAC Address Filtering entry

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。

Status: 选择是否启用本条目。**Enabled**（启用）或 **Disabled**（不启用）。

Privilege: 选择 MAC 地址过滤规则，您可以选择 **Allow**（允许）或 **Deny**（拒绝）。

Description: 为无线客户端添加简单的描述信息。如：Wireless station A。

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，MAC 地址为 00-0A-EB-00-07-5F 的主机 B 以及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. 为本规则点击 **Enable** 按钮。
2. 在 **Filtering Rules** 处选择 **Deny the stations not specified by any enabled entries in the list to access**。
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 **Disabled** 或删除该条目，也可以点击 **Delete All** 按钮，将列表中的条目清空。
4. 点击 **Add New...**按钮，在 **MAC Address** 处填写 00-0A-EB-00-07-BE，在 **Description** 处填写 wireless station A，在 **Privilege** 处选择 **Allow**，在 **Status** 处选择 **Enabled**。设置完成后，点击 **Save** 按钮和 **Return** 按钮。
5. 点击 **Add New...**按钮，在 **MAC Address** 处填写 00-0A-EB-00-07-5F，在 **Description** 处填写 wireless station B，在 **Privilege** 处选择 **Deny**，在 **Status** 处选择 **Enabled**。设置完成后，点击 **Save** 按钮和 **Return** 按钮。

过滤规则表格显示如下：

ID	MAC Address	Status	Privilege	Description	Modify
1	00-0A-EB-00-07-BE	Enabled	allow	Wireless Station B	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	deny	Wireless Station B	Modify Delete

注意：

- 1) 如果您在 **Filtering Rules** 处选择 **Allow the stations not specified by any enabled entries in the list to access**，wireless station B 仍然不能接入无线网络，但是其他不在列表中的无线接入站将可以接入无线网络。
- 2) 如果启用 MAC 地址过滤规则，并在 **Filtering Rules** 处选择 **Deny the stations not specified by any enabled entries in the list to access**，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。

5.6.5 Wireless Statistics（无线信息统计）

单击 **Wireless > Wireless Statistics**，查看当前连接到无线网络中的所有主机的基本信息。如图 5-14。

Wireless Statistics				
Current Connected Wireless Stations numbers:		1	<input type="button" value="Refresh"/>	
ID	MAC Address	Current Status	Received Packets	Sent Packets
1	00-0A-EB-90-00-09	AP-DOWN	0	32088
<input type="button" value="Previous"/>		<input type="button" value="Next"/>		

图 5-14 The router attached wireless stations

MAC Address: 显示当前已经连接到无线网络的主机的MAC地址。

Current Status: 此项显示当前主机的运行状态。

Received Packets: 显示收到的数据包数目。

Sent Packets: 显示发送的数据包数目。

在本页无法进行任何修改，点击 **Refresh** 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 **Next** 按钮，进入下一页；点击 **Previous** 按钮，返回上一页。

 **注意：**

本页数据会每隔5秒自动刷新。

5.6.6 Distance Setting（距离设置）

单击 **Wireless > Distance Setting**，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。

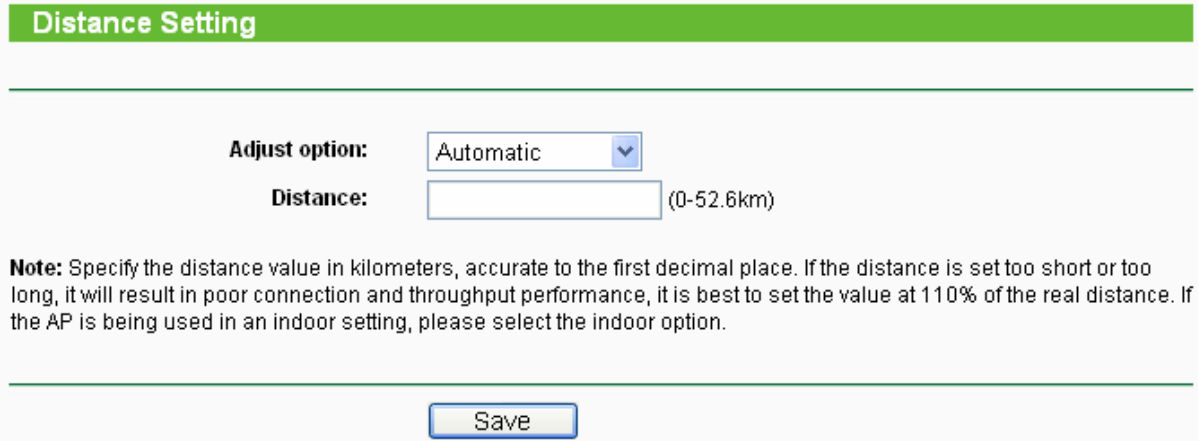


图 5-15 Distance Setting

Adjust option: 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。

Distance: 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%。如果AP在室内使用，请使用indoor模式。

点击 **Save** 使配置生效。

5.6.7 Antenna Alignment（天线校准）

单击 **Wireless > Antenna Alignment**，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。

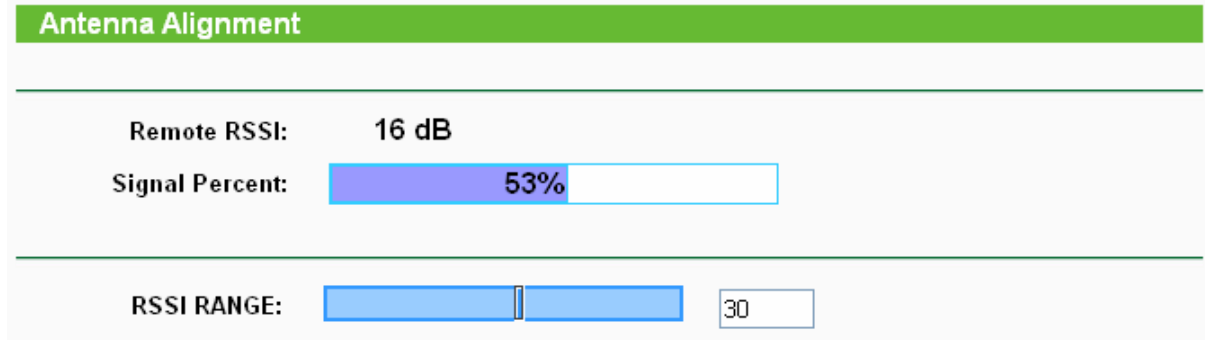


图 5-16 Antenna Alignment

Remote AP RSSI: 显示AP的信号强度值。

Signal percent: 显示RSSI和RSSI RANGE的百分比。

RSSI RANGE: 您可以拖动滑块设置RSSI RANGE值。如果RSSI RANGE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：

本功能只在已连接 AP 工作在 client 模式下才生效。

5.6.8 Throughput Monitor（吞吐量监控）

单击**Wireless > Throughput Monitor**，可以在下图 5-17界面中开始或停止无线通信的流量检测。界面中所有速率单位都为bps，即bit/s。

Throughput Monitor

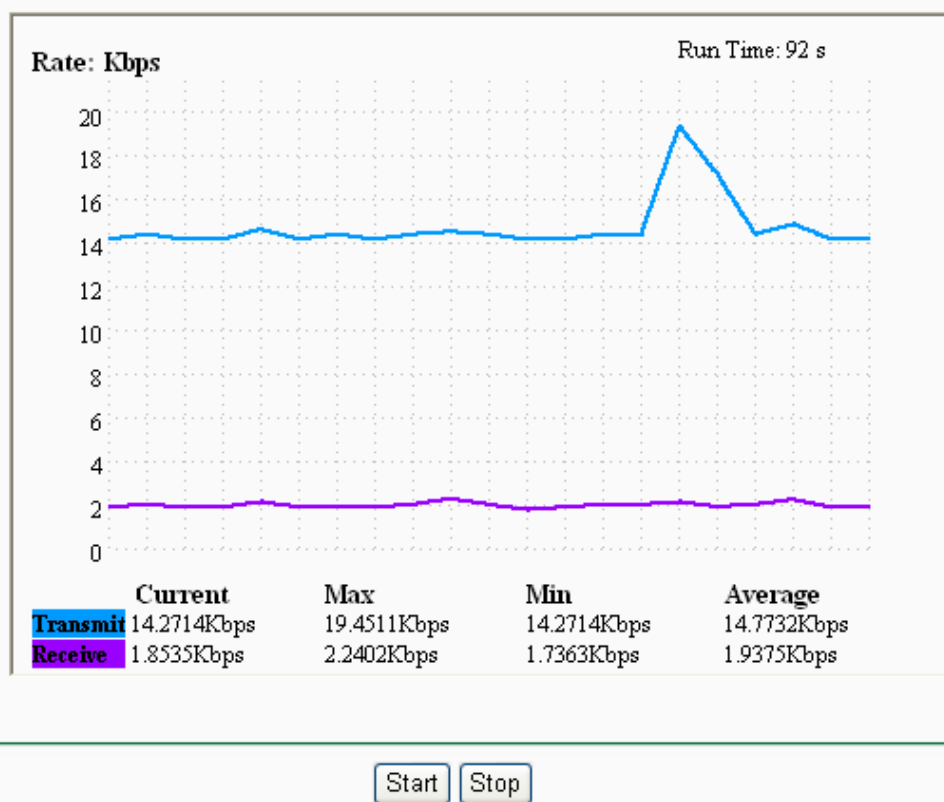


图 5-17 Wireless Throughput

5.7 DHCP

DHCP 指动态主机控制协议(Dynamic Host Configuration Protocol)。本 AP 中有一个内置的 DHCP 服务器，可以实现局域网内的计算机 IP 地址的自动分配。

DHCP 菜单下有 3 个子菜单(如图 5-18)：**DHCP Settings**、**DHCP Clients List** 和 **Address Reservation**。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

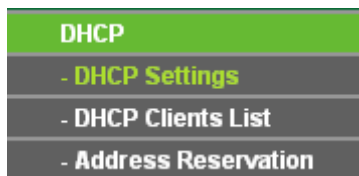


图 5-18 The DHCP menu

5.7.1 DHCP Settings (DHCP 设置)

单击 **DHCP > DHCP Settings**，将看到 DHCP 设置界面，如图 5-19。

DHCP Settings

DHCP Server: Disable Enable

Start IP Address:

End IP Address:

Address Lease Time: minutes (1~2880 minutes, the default value is 120)

Default Gateway: (optional)

Default Domain: (optional)

Primary DNS: (optional)

Secondary DNS: (optional)

图 5-19 DHCP Settings

- DHCP Server:** 选择是否启用DHCP服务器功能，默认为启用（Enable）。
- Start/End IP Address:** 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。
- Address Lease Time:** 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。
- Default Gateway (optional):** 可选项。应填入AP的LAN口的IP地址，缺省为192.168.1.254。
- Default Domain (optional):** 可选项。应填入本地网域名，缺省为空。
- Primary/Secondary DNS (optional):** 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。

完成更改后，点击**Save**按钮并重启AP使设置生效。

5.7.2 DHCP Clients List（DHCP客户端列表）

单击**DHCP > DHCP Clients List**，可以查看客户端主机的相关信息；单击**Refresh**按钮可以更新表中信息，如图 5-20。

DHCP Clients List

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	microsoft	00-19-66-CB-45-66	192.168.1.100	01:56:59

图 5-20 DHCP Clients List

Client Name: 显示获得IP地址的客户端计算机的名称。

- MAC Address:** 显示获得IP地址的客户端计算机的MAC地址。
- Assigned IP:** 显示DHCP服务器分配给客户端主机的IP地址。
- Lease Time:** 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 Address Reservation（静态地址分配）

单击 **DHCP > Address Reservation**，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 5-21。

ID	MAC Address	Reserved IP Address	Status	Modify
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>				
<input type="button" value="Previous"/> <input type="button" value="Next"/>				

图 5-21 Address Reservation

- MAC Address:** 显示预留静态IP地址的计算机的MAC地址。
- Reserved IP Address:** 显示预留给内网主机的IP地址。
- Status:** 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。
- Modify:** 修改或删除本条目。

添加预留 IP 地址：

1. 点击**Add New...**按钮弹出如图 4-25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. 点击 **Save** 按钮，使配置生效。

Add or Modify an Address Reservation Entry

MAC Address:

Reserved IP Address:

Status: ▼

图 5-22 Add or Modify an Address Reservation Entry

修改预留 IP 地址：

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

点击 **Delete All** 按钮，删除所有条目。

 **注意：**

所有配置将重启后生效。

5.8 Wireless settings（无线高级设置）

单击**Wireless Settings**，可以在图 5-23中设置无线的高级功能。

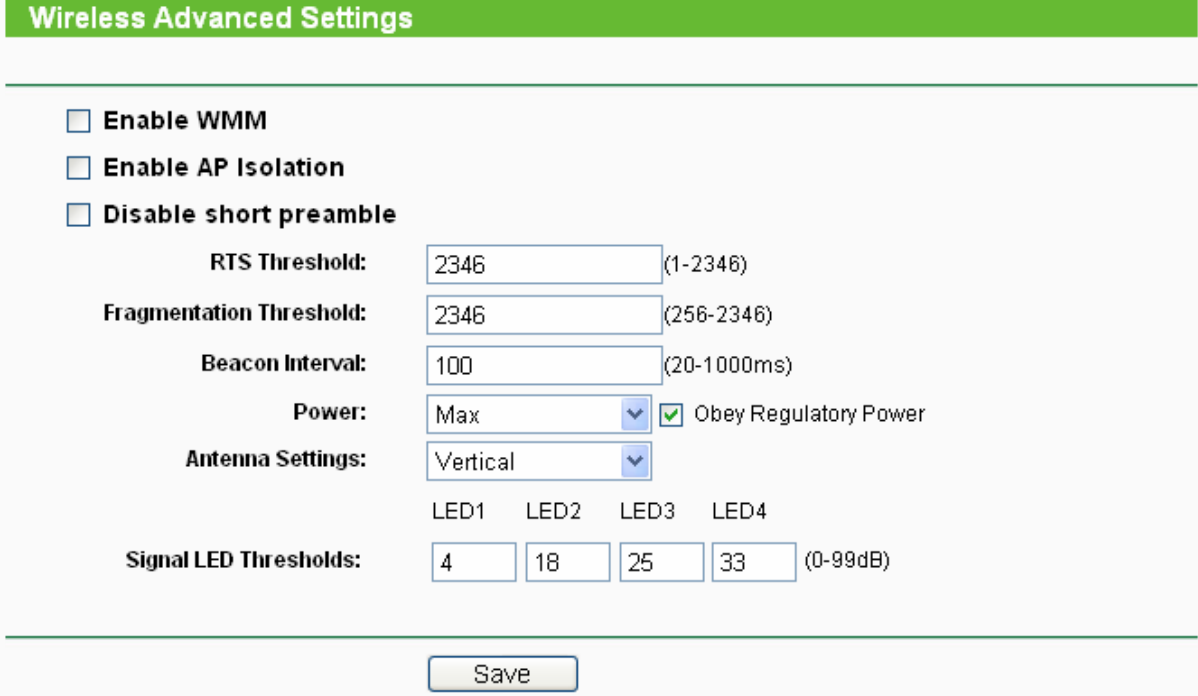


图 5-23 Wireless settings

Enable WMM: WMM功能可以保证在数据包的高质量传输。推荐您开启此功能。

Enable AP Isolation: 选择此项可以隔离关联到接入器的各个无线客户端。

Disable short preamble: 屏蔽短前导，只使用长前导。推荐您保持默认设置。

RTS threshold: RTS/CTS起始值。决定发送RTS/CTS数据包大小的起始值。

Fragmentation Threshold: 分片阈值。为数据包指定分段阈值，当数据包长度超过此值时会被自动分成多个数据包。

Beacon Interval: Beacon时槽。设置Beacon帧的发包间隔。

Power: 发射功率。选择是否勾选**Obey Regulatory Power**，不勾选可能导致与其他设备相冲突，干扰可用网络。

Antenna Settings: 设置天线的方向。

Signal LED Thresholds: LED指示灯的RSSI阈值。

5.9 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，选择启用功能，并在下面页面中设置参数。如图 5-24。



图 5-24 SNMP Settings

5.9.1 Community Setting（团体设置）

单击 **SNMP > Community Setting**，可以在图 5-25中设置SNMP团体。

Community List				
Num	Community	Access Mode	Status	Status
1	public	Read Only	Disable	Modify
2	public	Read Only	Disable	Modify
3	public	Read Only	Disable	Modify
4	public	Read Only	Disable	Modify

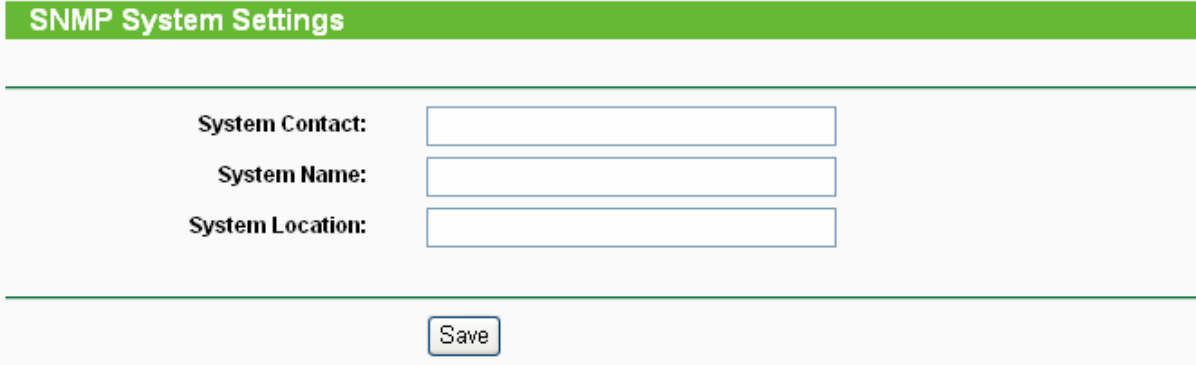
Enable All Disable All

图 5-25 Community Setting

- Num:** 显示团体名的序号。
- Community:** 设备连接SNMP管理端软件的登录密码。
- Access Mode:** 选择团体名的权限。Read Only表示团体对SNMP信息只有读取权限；Read&Write表示团体对SNMP信息具有读写权限。
- Status:** 选择是否启用相应团体名。
- Modify:** 修改本条目。
- Enabled All:** 点击该按钮，可以将列表中的所有条目的状态设置为“生效”。
- Disabled All:** 点击该按钮，可以将列表中的所有条目的状态设为“失效”。

5.9.2 SNMP System Setting（SNMP系统设置）

点击**SNMP > SNMP Setting**，可以在图 5-26中设置SNMP系统参数。



The image shows a web interface for 'SNMP System Settings'. It features a green header bar with the title 'SNMP System Settings'. Below the header, there are three input fields: 'System Contact:', 'System Name:', and 'System Location:'. Each field is represented by a rectangular text box. At the bottom of the form, there is a 'Save' button.

图 5-26 SNMP System Setting

System Contact: SNMP系统的管理员联系信息。

System Name: 本设备的系统名称。

System Location: 本设备的联系人位置信息。

5.10 System Tools（系统工具）

System Tools帮助您优化设备的配置。在System Tools菜单下有 8 个子菜单(如图 5-27): **Firmware**、**Factory Defaults**、**Backup & Restore**、**Ping Watch Dog**、**Speed Test**、**Reboot**、**Password**和**Syslog**。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。



图 5-27 The System Tools menu

5.10.1 Firmware（软件升级）

点击**System Tools > Firmware**，可以在下图 5-28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。

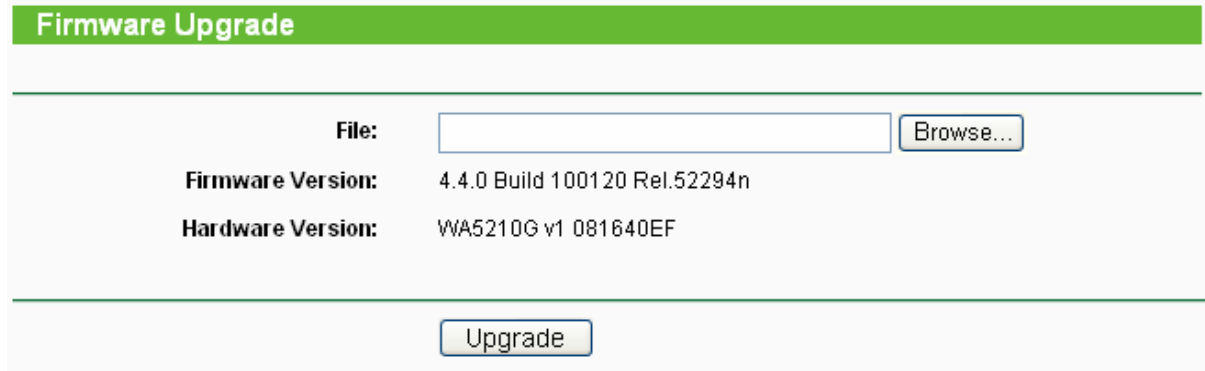


图 5-28 Firmware Upgrade

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 **Browse** 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：单击 **Upgrade** 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。

Firmware Version: 显示设备当前的软件版本。

Hardware Version: 显示设备当前的硬件版本。

5.10.2 Factory Defaults（恢复出厂设置）

点击 **System Tools > Factory Default**，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 5-29。

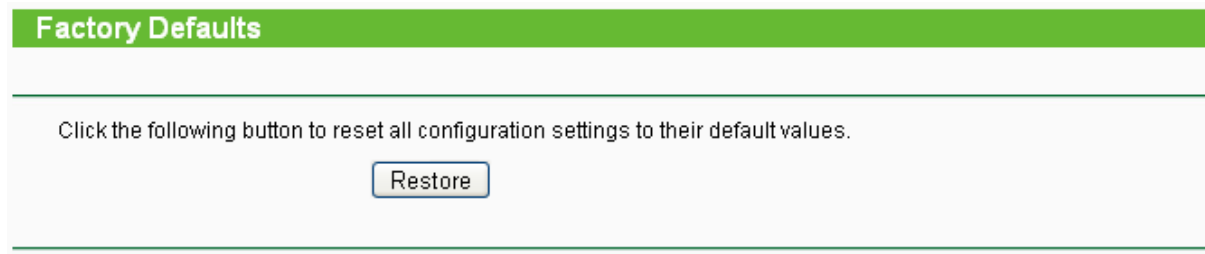


图 5-29 Restore Factory Default

单击 **Restore** 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。

5.10.3 Backup & Restore（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**System Tools > Backup & Restore**，可以在下图 5-30中备份或载入AP的配置文件。



图 5-30 Save or Restore the Configuration

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。

5.10.4 Ping Watch Dog（看门狗）

看门狗功能使接入器通过连续 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**System Tools > Ping Watch Dog**，您可以在下图 5-31界面中配置看门狗功能。

Ping Watch Dog Utility

Enable:

IP Address:

Interval: seconds

Delay: seconds

Fail Count:

图 5-31 Ping Watch Dog Utility

- Enable:** 勾选启用看门狗功能。
- IP Address:** 看门狗发送 Ping 数据包的目的主机的 IP 地址。
- Interval:** 发送两个连续 Ping 数据包的时间间隔。
- Delay:** AP 重启之后到发送第一个 Ping 数据包之前的时间延迟。
- Fail Count:** 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

5.10.5 Speed Test (速率检测)

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。如果远程设备也是 **TL-WA5210G**，您可以在 **Advance options** 页面输入远程设备的用户名和密码，获取精确的预留带宽值。

点击 **System > Speed Test**，可以在图 5-32 中配置速率测试功能。

图 5-32 Speed Test

- Destination IP:** 远程设备的 IP 地址
- User、Password:** 远程设备的登录账号名和密码。如果您想要获得精确的测试数据，请正确填写。反正则留空。
- Advanced options:** 勾选是否进行高级设置。如果您需要精确测试数据，请勾选此项。
- Direction:** 速率测试时的三种传输方向选项。**transmit** 测试输出带宽；**receive** 测试输入带宽；**both** 测试输出带宽和输入带宽。
- Duration:** 填写测试持续时间。
- Data amount:** 在整个测试过程中的发送的最大数据包数。

注意:

1. 如果User或Password错误，设备将自动转换为基本测试，即高级配置将会失效。
2. 如果指定Duration和Data amount，超出设置值后测试将自动停止。

5.10.6 Reboot（重启）

点击**System Tools > Reboot**，可以将AP重新启动，如图 5-33。

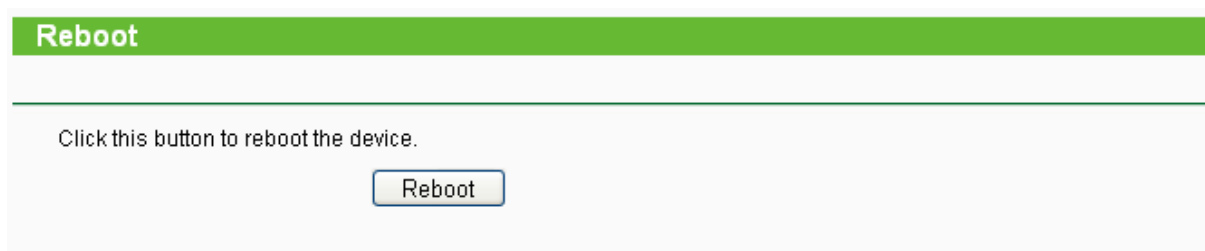


图 5-33 Reboot the AP

本 AP 的某些设置需要在路由器重新启动后才能生效。

- 对 AP 进行软件升级
- 恢复 AP 的出厂设置
- 修改 LAN 口的基本网络参数
- 设置 DHCP 服务功能
- 设置 DHCP 服务器的静态地址分配功能
- 手动重启的方法：单击图 5-33 中的 **Reboot** 按钮。

5.10.7 Password（修改登录口令）

点击 **System Tools > Password**，可以在下图 5-34 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 **Save** 按钮即可。

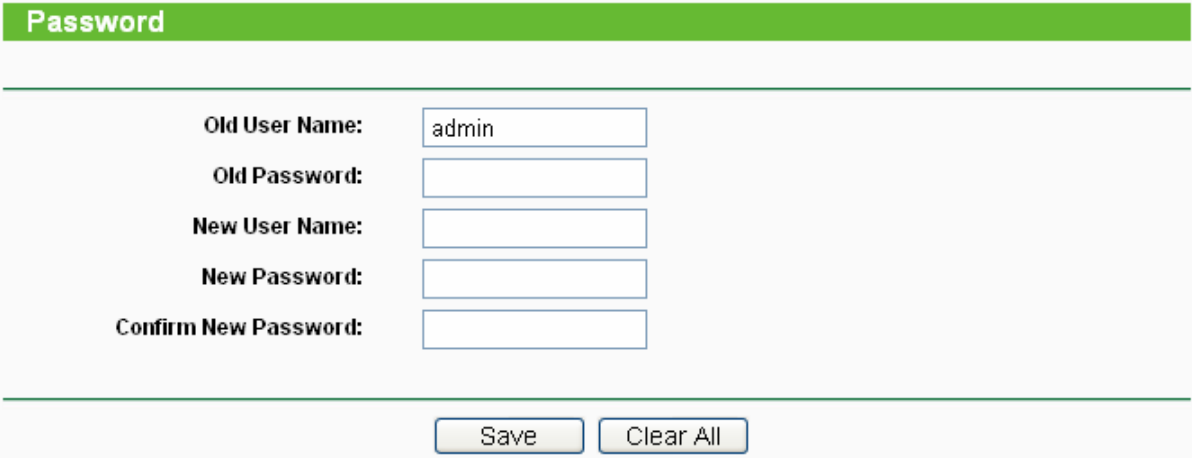


图 5-34 Password

👉 注意：

出于安全考虑，我们强烈推荐您更改初始系统管理员的用户名及密码。如果忘了系统密码，请将路由器恢复到出厂设置。

5.10.8 Syslog（系统日志）

点击 **System Tools > System Log**，可以在下图 5-35 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。




图 5-35 System Log

Appendix 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。

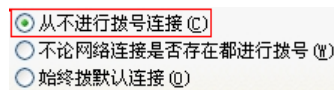
注意：复位后 AP 默认登录 IP 为 **192.168.1.254**，默认用户名/密码是 **admin/admin**。登录时，请确保计算机的 IP 地址在 192.168.1.X（X 为 2 到 253 之间的任意整数）网段。

2. 登录不了AP的管理界面怎么办？

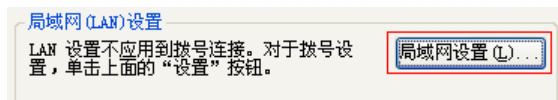
- 1) 请确保计算机连接在 AP 的 LAN 口；
- 2) 请确认计算机的 IP 地址与 AP 登录 IP 地址处于同一网段；如 AP 默认登录 IP 地址为 192.168.1.254，则计算机 IP 地址须为 192.168.1.X（X 为 2 到 253 之间的任意整数）；
- 3) 如果您修改了 AP 的 WEB 管理端口（默认为 80），则登录路由器管理界面时应输入 http://LAN 口 IP:端口号，如 http:192.168.1.254:88；
- 4) 请确保浏览器设置为从“不进行拨号连接”并且没有设置代理服务器；

方法如下（以 IE 浏览器为例）：

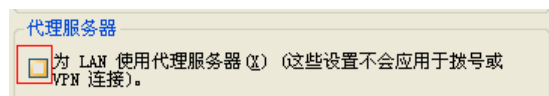
依次选择**工具—Internet 选项—连接**，选择“从不进行拨号连接”：



单击**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；

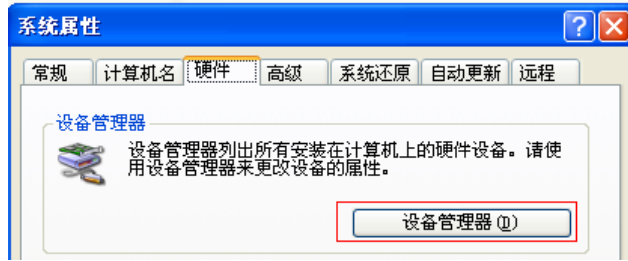
若上述提示不能帮助您登录到 AP，请将 AP 恢复出厂设置并重新操作。

3. 为什么我的笔记本电脑搜索不到无线信号？

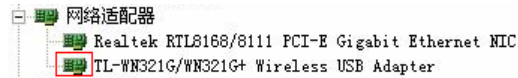
- 1) 如果是笔记本电脑内置的无线网卡，请确认无线功能开关已打开（建议联系笔记本电脑厂商或查阅相关说明书）；
- 2) 在设备管理器中查看无线网卡驱动是否成功安装以及无线网卡是否已启用；

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



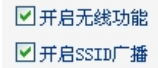
3) 检查笔记本电脑的无线服务是否开启：

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

Windows Time	维护在网络上的所有客户端和服务器的时间和...	已启动	自动	本地系统
Wireless Zero Configuration	为您的 802.11 适配器提供自动配置	已启动	手动	本地系统
WMI Performance Adapter	从 WMI HiPerf 提供程序提供性能库信息。		手动	本地系统

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 **Status > WAN > DNS Server** 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。

Appendix B: IE浏览器设置

2. 打开 IE 浏览器，选择菜单工具→Internet 选项...，如下图 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。

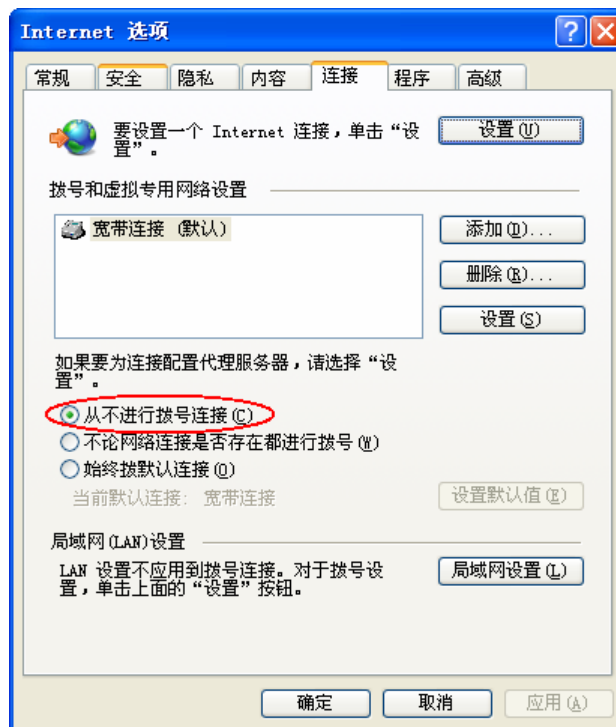


图 2



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，单击确定按钮返回。

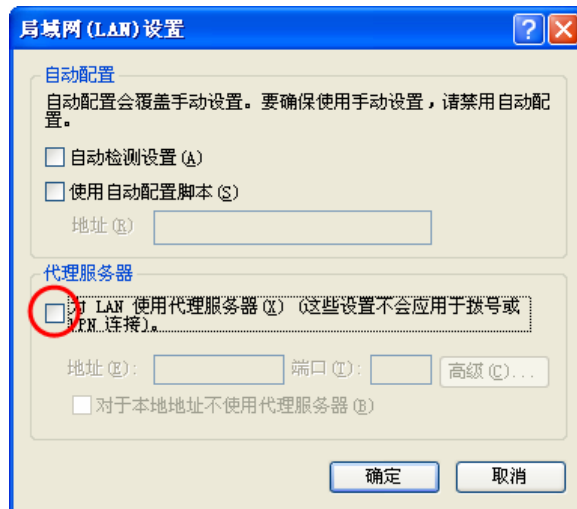


图 4

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

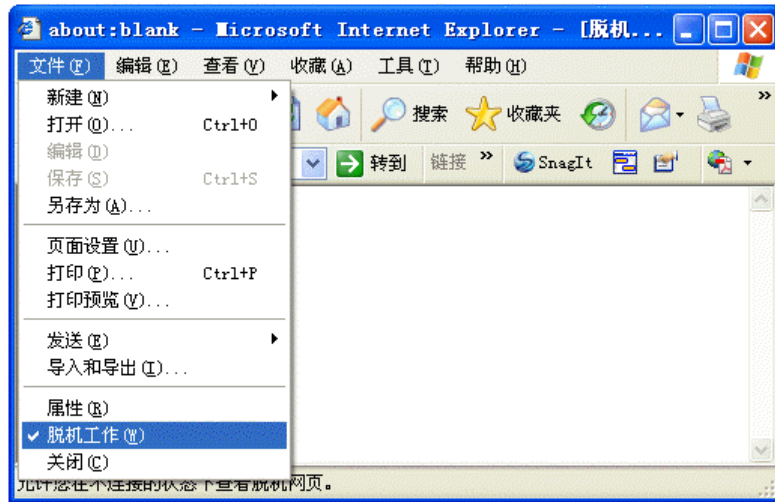


图 5

Appendix 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

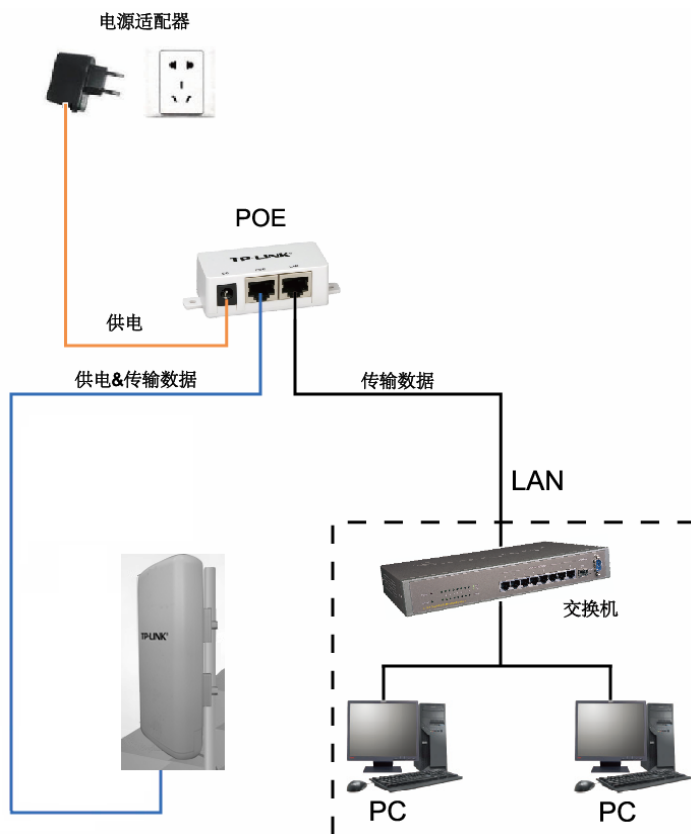


- **DC:** 电源插孔，连接电源适配器。
- **POE:** POE 口，连接到 AP 的 LAN 口。
- **LAN:** LAN 口，连接到局域网用于数据传输。

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-WA5210G	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。

Appendix D: 规格参数

基本参数	
支持的标准和协议	IEEE 802.3, 802.3u, 802.11b and 802.11g, TCP/IP, DHCP
安全认证	FCC, CE
端口	一个10/100M 自翻转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	54/48/36/24/18/12/9/6Mbps或11/5.5/3/2/1Mbps
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