

ATK-RM04 路由器使用手册

高性能 UART-ETH-WIFI 模块

使用手册

ALIENTEK

广州市星翼电子科技有限公司

修订历史

版本	日期	原因
V1.00	2013/10/24	第一次发布

目 录

1. 概述.....	1
1.1 模块简介.....	1
1.2 模块特性.....	1
2. 使用说明.....	2
2.1 登录管理.....	2
2.2 快速设置.....	5
2.2.1 Wizard	5
2.2.2 运作模式设置.....	6
2.3 网络设置.....	7
2.3.1 广域网络设置.....	7
2.3.2 局域网设置.....	10
2.3.3 DHCP 客户端列表	12
2.3.4 VPN Passthrough	13
2.3.5 高级路由选项.....	13
2.4 无线网络设置.....	14
2.4.1 基本设置.....	14
2.4.2 高级设置.....	16
2.4.3 安全设置.....	19
2.4.4 WDS.....	21
2.4.5 WPS.....	24
2.4.6 基地台扫描.....	24
2.4.7 客户端列表.....	25
2.4.8 统计资料.....	25
2.5 防火墙.....	25
2.5.1 MAC/IP/Port 过滤	25
2.5.2 Port 转送	27
2.5.3 DMZ 主机.....	28
2.5.4 系统安全设置.....	29
2.5.6 内容过滤.....	30
2.6 系统管理.....	31
2.6.1 管理.....	31
2.6.2 固件更新.....	32
2.6.3 设置管理.....	33
2.6.4 状态.....	34
3. 结构尺寸.....	34
4. 其他.....	35

1. 概述

1.1 模块简介

ATK-RM04 是 ALIENTEK 推出的一款高性能 UART-ETH-WIFI（串口-以太网-无线网）模块。ATK-RM04 模块板载 Hi-Link 公司的 HLK-RM04 模块，该模块支持路由器模式，可以直接当成一个无线宽带路由器使用。

作为无线宽带路由器，ATK-RM04 模块集有线/无线网络连接于一体，并支持网关和桥接，无线路由器，无线 AP 等四种工作模式，提供 2 个 RJ45 接口（一个 WAN 口，一个 LAN 口），支持端口速率、类型自动适应，满足你不同的网络需求。支持 11 n/b/g 的无线标准，最大无线信号文件传输速率高达 150Mbps。

模块路由器模式提供多方面的管理功能，可对系统、DHCP 服务器、虚拟服务器、DMZ 主机、防火墙、上网权限管理、静态路由表、UPnP 等进行管理，同时提供中文简体，中文繁体以及英文配置界面，界面友好和善，配置简单易用，即使你之前没有接触或使用过无线网络产品，依然可以通过安装设置向导来完成基本备置。

当今网络面临的难题是网络安全，尤其是无线网络，已经成为网络建设的重中之重。模块提供多重安全防护。具有 Wi-Fi 保护接入（WPA-PSK/WPA2 PSK）和 64/128-bit WEP 加密特性，可提升无线数据通信的安全等级。同时，还可以提供额外的安全特性，比如支持 WPS，可使用 PIN 或按键方式便捷设置更高等级安全连接。使未经认证的非法用户无计可施，最大限度的保护无线连接安全。支持 SSID 广播控制，支持基于 MAC 地址的访问控制，再配合强大的防火墙特性，可有效防止入侵，为无线通信提供更强的安全保护。

1.2 模块特性

ATK-RM04 无线宽带路由器功能特性：

- ◆ 支持 802.11n/b/g，最大传输速率可达 150Mbps；
- ◆ 网页用户界面支持免费软件升级功能；
- ◆ 支持备份和恢复配置文件；
- ◆ 支持 WDS 无线中继器功能，扩大无线网络覆盖区域；
- ◆ 支持外接天线，客户可根据自己需要，选择不同增益的外置天线；
- ◆ 支持多种路由器功能，如 DHCP 服务器与客户端，静态路由，虚拟服务器，DMZ，UPnP，VPN 穿透等等；
- ◆ 支持 PPPoE、动态 IP、静态 IP 接入方式。PPPoE 支持自动拨号，按需拨号以及手动拨号，满足不同用户的需求；
- ◆ 支持多种安全加密技术，如 64/128 位 WEP 数据加密，WPA/WPA2，WPS 无线配置及一键加密技术等等。内置防火墙可以预防黑客入侵；
- ◆ 支持隐藏无线 SSID 钥匙功能，可以保护用户信息数据安全，保障无线网络不被侵犯或者盗用；

2. 使用说明

2.1 登录管理

ATK-RM04 模块在路由器模式(即默认模式)下,是开启了所有端口的,包括 LAN/WLAN 口以及 WIFI。所以,我们要登录到 ATK-RM04 模块,可以有 2 种方法:

- 1, 通过 LAN 口。
- 2, 通过 WIFI。

这里我们重点介绍第一种方法:首先,设置电脑的 Internet 协议属性,设置为自动获取 IP 地址并自动获取 DNS,如图 2.1.1 所示:

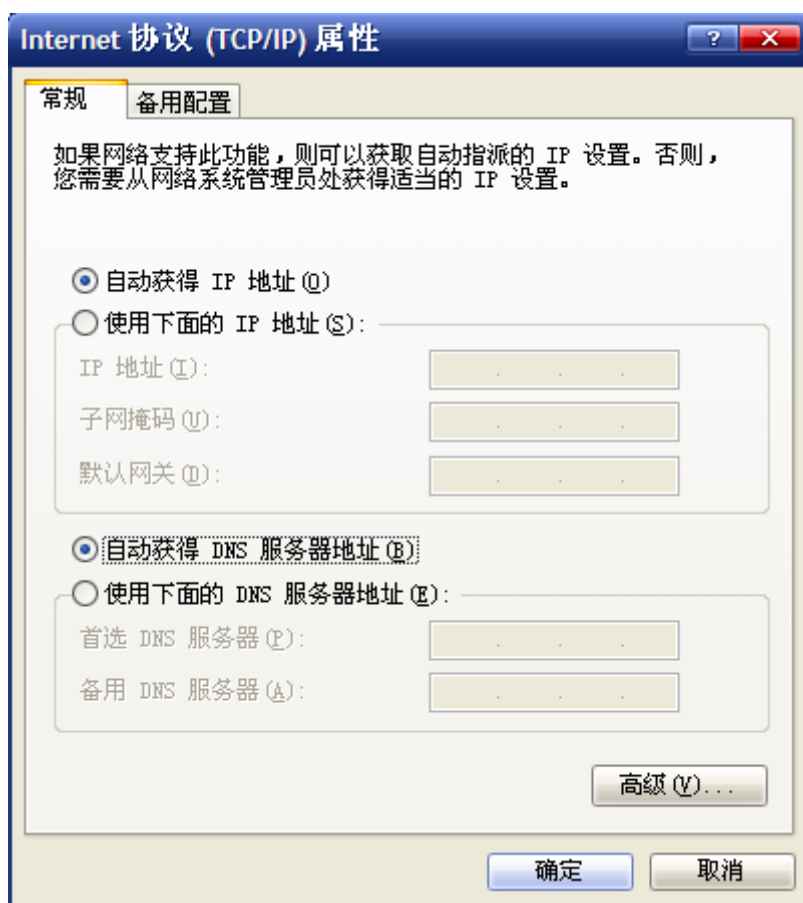


图 2.1.1 Internet 协议属性设置

点击确定,然后,找一根网线,连接电脑网口和 ATK-RM04 模块的 LAN 口(注意模块要先开机!!),此时可以看到电脑正在获取 IP 地址,稍等片刻后,电脑即可连上模块,如图 2.1.2 所示:



图 2.1.2 连接成功

至此，我们的电脑就和模块连接上了。通过 WIFI 的连接其实和第一种方法非常类似，只需要电脑开启 WIFI，然后就可以搜索到 ATK-RM04 的无线网络，输入密码：12345678，即可实现电脑 WIFI 连接模块（同样设置为自动获取 IP 和 DNS）。

注意：因为我们的模块默认是开启 DHCP 服务器功能的，所以电脑才可以自动从模块自动获取 IP 地址。如果自动获取 IP 地址失败，请检查模块是不是在默认状态，是否开启 DHCP 服务，可以让模块恢复出厂设置来排除这个问题。

在电脑与模块连接成功以后，我们在浏览器输入：192.168.16.254（路由器默认 IP 地址），点击回车，然后浏览器会弹出一个登录窗口，输入用户名和密码：admin/admin，即可登录，默认弹出的是串口配置界面，如图 2.1.3 所示：

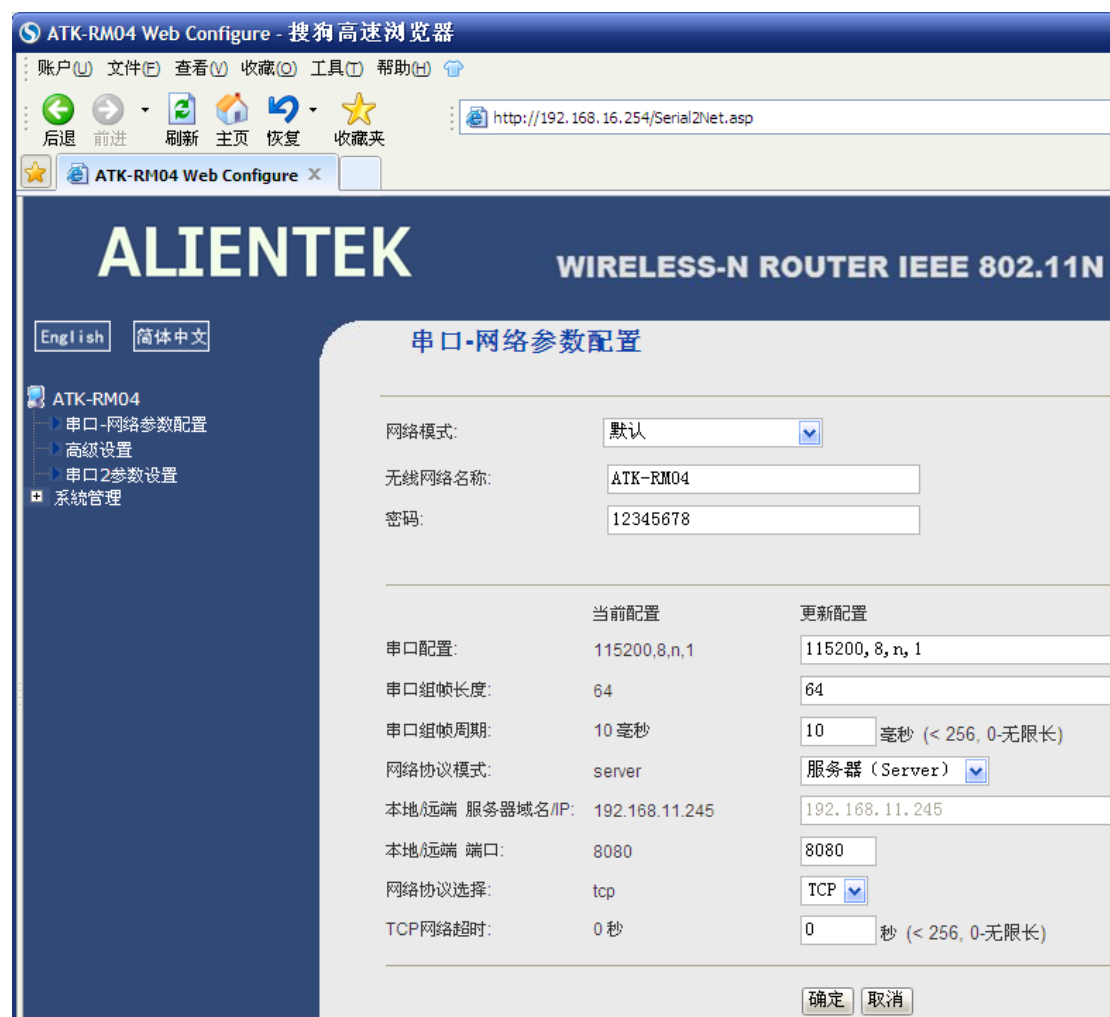


图 2.1.3 串口配置界面

然后，我们点击 ALIENTEK 图标，即可进入路由器设置界面，如图：2.1.4 所示：



图 2.1.4 路由器设置界面

至此，便成功登录到路由器设置界面了。另外，打开浏览器，在地址栏中输入地址：

192.168.16.254/home.asp，则可快速进入路由器设置界面。

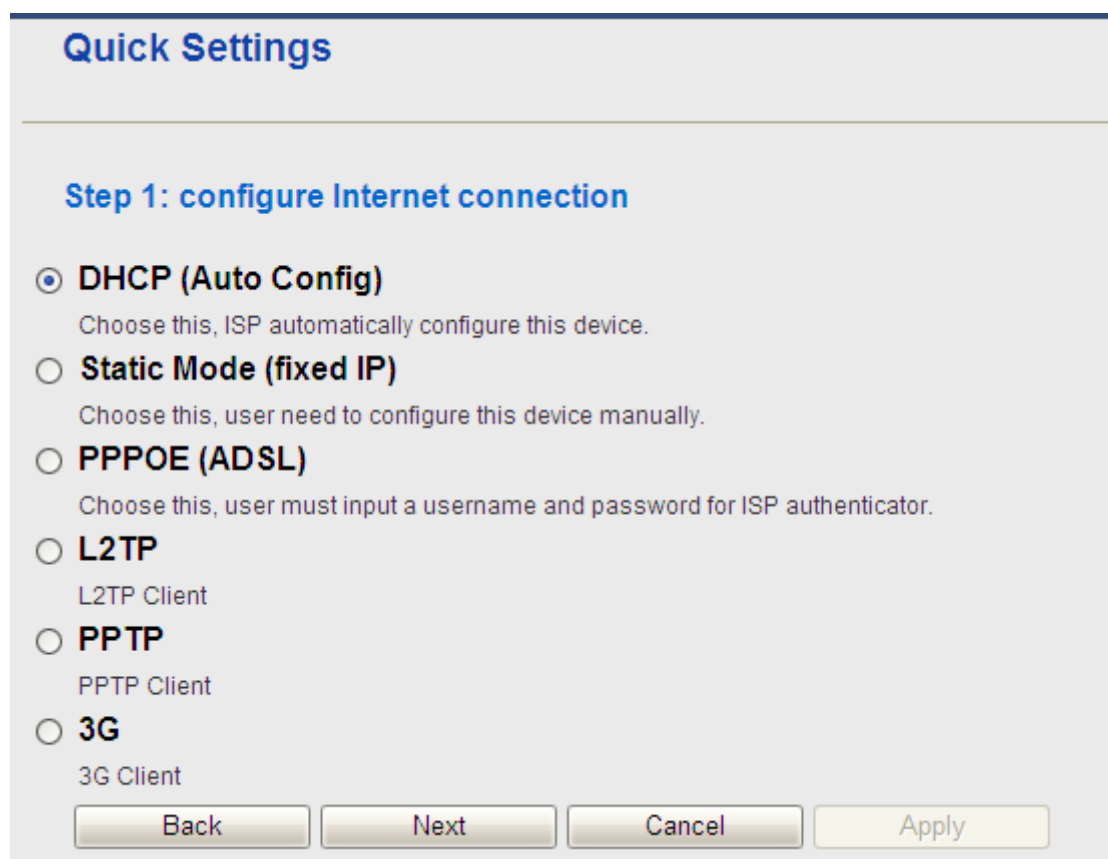
2.2 快速设置

模块提供多种功能并提供设置向导，即使您对路由器的使用不熟悉，也可以按照提示轻松自如的完成最基本设置。

2.2.1 Wizard

(1) 选择<Wizard>，进入快速设置界面，单击下一步开始对路由器进行设置。

(2) 本路由器支持六种常用的上网方式，如图 2.2.1.1 所示，请您根据自身情况进行选择，除了第一种方式之外，其他方式均需对接入互联网的相关项目进行设置。这些项目的参数由 ISP 服务商提供，如果你不了解，请咨询为您的 ISP 服务商。选择相应的上网方式后单击 Next。



Quick Settings

Step 1: configure Internet connection

☒ **DHCP (Auto Config)**
Choose this, ISP automatically configure this device.

☐ **Static Mode (fixed IP)**
Choose this, user need to configure this device manually.

☐ **PPPOE (ADSL)**
Choose this, user must input a username and password for ISP authenticator.

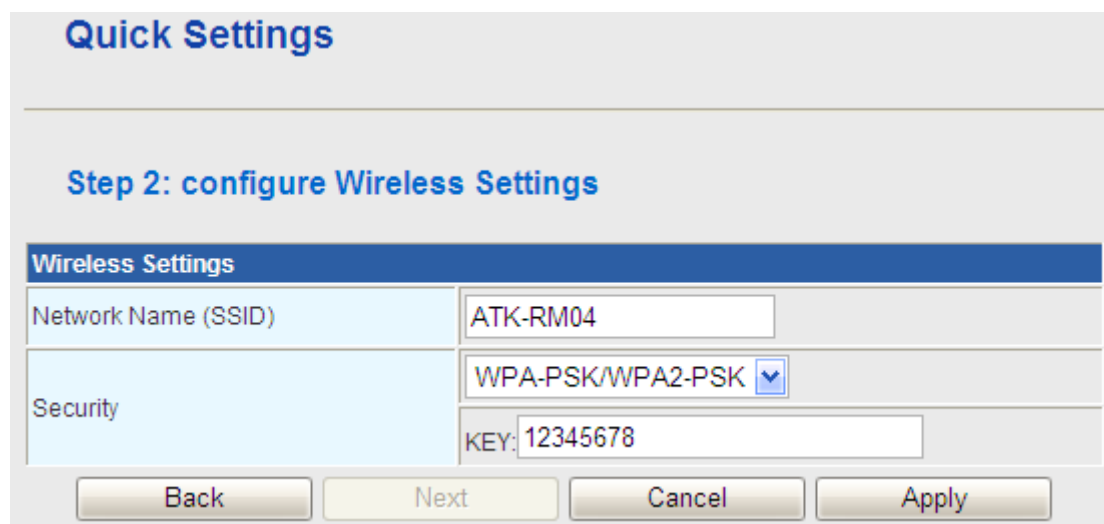
☐ **L2TP**
L2TP Client

☐ **PPTP**
PPTP Client

☐ **3G**
3G Client

图 2.2.1.1 选择上网方式

(3) 您还可以为您的无线网络设置定义网络名称和相应的加密安全机制，如图 2.2.1.2 所示，设置好之后，单击 Apply 按钮提交设置信息。系统重启后即完成对路由器基本的设置。



Quick Settings

Step 2: configure Wireless Settings

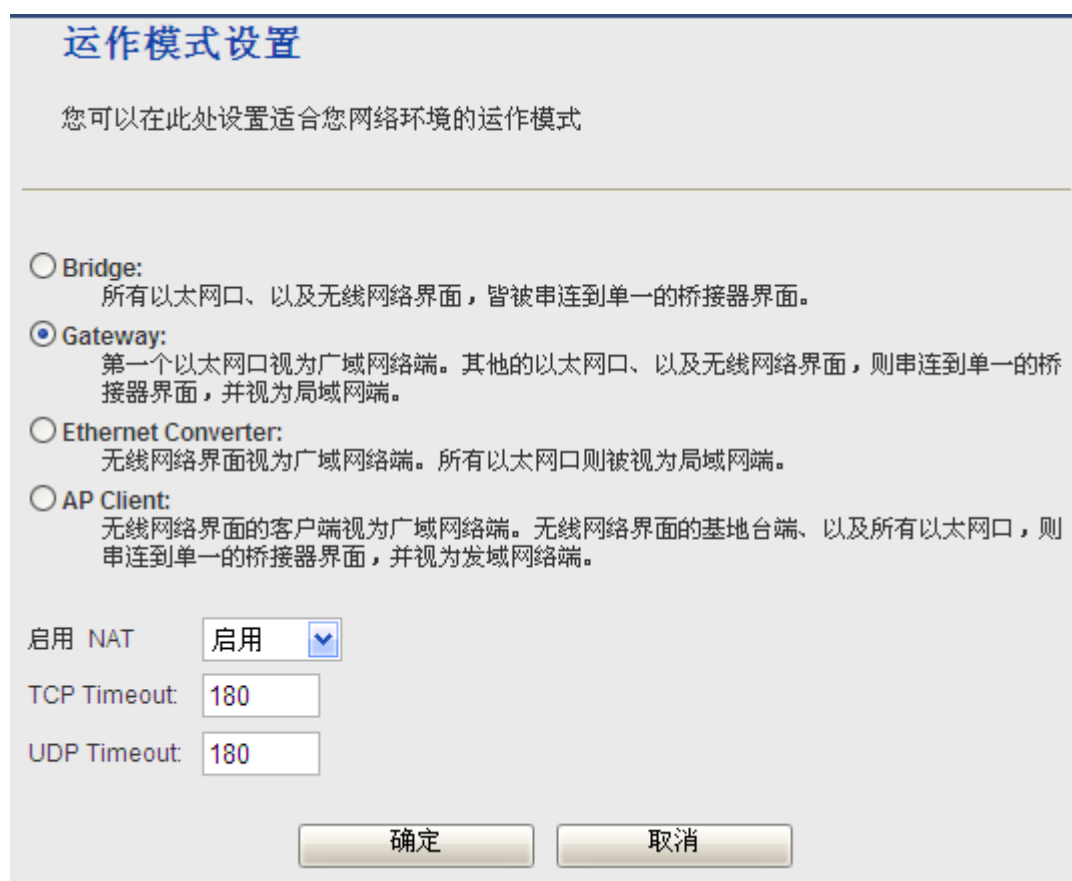
Wireless Settings	
Network Name (SSID)	ATK-RM04
Security	WPA-PSK/WPA2-PSK
	KEY: 12345678

Back Next Cancel Apply

图 2.2.1.2 无线参数设置

2.2.2 运作模式设置

ATK-RM04 模块作为无线路由器，拥有强大的功能：支持桥接（Bridge）、网关（Gateway）、以太网转换（Ethernet Converter）、AP 客户端（AP Client）四种运作模式，默认为网关模式。如图 2.2.2.1 所示：



运作模式设置

您可以在此处设置适合您网络环境的运作模式

☐ Bridge:
所有以太网口、以及无线网络界面，皆被串连到单一的桥接器界面。

☒ Gateway:
第一个以太网口视为广域网络端。其他的以太网口、以及无线网络界面，则串连到单一的桥接器界面，并视为局域网端。

☐ Ethernet Converter:
无线网络界面视为广域网络端。所有以太网口则被视为局域网端。

☐ AP Client:
无线网络界面的客户端视为广域网络端。无线网络界面的基地台端、以及所有以太网口，则串连到单一的桥接器界面，并视为局域网端。

启用 NAT

TCP Timeout:

UDP Timeout:

图 2.2.2.1 运作模式选择

桥接模式（Bridge）：

当你将路由器设置为桥接模式时，它即成为一台具备 WEB 管理功能无线的 AP，RJ45 接口变为 LAN 口，此时的路由器只具备交换机功能，不可以直接与广域网连

接，防火墙功能也不起作用。

网关模式 (Gateway):

网关模式，即默认模式。在此模式下，通过启用 NAT 功能，可以轻松的与互联网进行通信。

以太网转换 (Ethernet Converter):

无线网络为 WAN 口，此时，无线网络作为一个无线网卡连接到其他无线路由上，RJ45 作为 LAN 口，可以通过 RJ45 口上网

AP 客户端 (AP Client):

此时路由器是一个 AP，既可以连接到另外的无线路由器，本身也可以发起自己的网络，RJ45 口为 LAN 口。此功能可作为无线 WIFI 延伸用。

2.3 网络设置

2.3.1 广域网络设置

从 WAN 口连接到互联网(Internet)的相关参数。本路由器支持目前 ISP 所提供的常见连接方式，如静态 IP，动态自动获取 IP，PPPoE 等。你需要做的是在这里输入由 ISP 提供的相关参数即可。验证连接是否成功，除了直接浏览相关互联网网站外，也可以通过查看 Internet 配置的状态进行判别。

2.3.1.1 静态 IP(固定 IP)

静态 IP 模式设置如图 2.3.1.1.1 所示：

广域网络设置

您可以依您的环境选择适当的联机模式，并针对不同的联机模式设置参数。

广域网络联机模式: 静态 (固定 IP)

静态模式

IP 地址	192.168.1.108
子网掩码	255.255.255.0
预设网关	192.168.1.1
惯用 DNS 服务器	218.30.118.6
其他 DNS 服务器	114.114.114.114

MAC 复制

Enabled	停用
---------	----

确定 取消

图 2.3.1.1.1 广域网静态 IP 方式

- ◆ IP 地址：ISP 运营商提供的静态 IP 地址。
- ◆ 子网掩码：ISP 提供的子网掩码。
- ◆ 默认网关：填入 ISP 提供的网关地址。

- ◆ 首选 DNS 服务器：填入 ISP 提供的 DNS 服务器，不同地区 DNS 地址不同。
- ◆ 备用 DNS 服务器：填入 ISP 提供的 DNS 服务器，不同地区 DNS 地址不同。

2.3.1.2 动态 IP(自动获取 IP)

这种方式比较方便，无需进行设置，路由器自动从 ISP 运营商获取相关的信息参数，如 IP 地址、网关地址等。并随着 ISP 运营商网络状态改变而改变。如图 2.3.1.2.1 所示：

广域网络设置

您可以依您的环境选择适当的联机模式，并针对不同的联机模式设置参数。

广域网络联机模式: 动态 (自动取得)

DHCP 模式

网络名称 (optional)

MAC 复制

Enabled 停用

确定 取消

图 2.3.1.2.1 广域网动态 IP 方式

2.3.1.3 PPPoE(ADSL)

PPPoE 方式连接对于家庭使用或小型企业，是比较普遍的。如图 2.3.1.3.1 所示：

广域网络设置

您可以依您的环境选择适当的联机模式，并针对不同的联机模式设置参数。

广域网络联机模式: PPPoE (ADSL)

PPPoE 模式

使用者名称 pppoe_user

口令

确认口令

运行模式 永久连线

Keep Alive Mode: Redial Period 60 seconds

On demand Mode: Idle Time 5 minutes

MAC 复制

Enabled 停用

确定 取消

图 2.3.1.3.1 广域网 PPPoE 方式

- ◆ 上网账号：填入 ISP 提供的上网帐号，不清楚请向 ISP 询问。
- ◆ 密码及确认密码：填入 ISP 提供的密码，不清楚请向 ISP 询问。

- ◆ 运行模式：分为永久连接，动态需求，手动连接。
- ◆ 永久连接：若选择永久连接模式，则在开机后系统自动进行连接。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间（默认为 60 秒）尝试连接，直到成功连接为止。
- ◆ 动态需求：当局域网有网络访问请求时，系统会自动进行连接。若在设定时间内(空闲时间)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，可以选择该项连接方式，有效节省上网费用。
- ◆ 手动连接：选择该项，开机后需要用户手动拨号连接。

2.3.1.4 L2TP

L2TP 广域网连接方式如图 2.3.1.4.1 所示：

图 2.3.1.4.1 广域网 L2TP 方式

- ◆ 服务器 IP：填入 ISP 提供的 IP 地址，这是必须的。使用者名称：输入 L2TP 拨号时使用的上网账号，这是必须的，由运营商提供。
- ◆ 密码：输入 L2TP 拨号时使用的密码，这是必须的，由运营商提供。
- ◆ IP 地址模式：获取 IP 地址的方式，分为静态和动态两种。动态：前提是可以自动从 ISP 获取 IP 地址。静态：前提是拥有 ISP 提供的固定 IP 地址。
- ◆ IP 地址：当选择静态 IP 地址模式时，输入 ISP 提供的固定 IP 地址。
- ◆ 子网掩码：当选择静态 IP 地址模式时，输入 ISP 提供的子网掩码。
- ◆ 默认网关：当选择静态 IP 地址模式时，输入 ISP 提供的默认网关。
- ◆ 运行模式：分为永久连线，手动连线。永久连接：若选择永久连接模式，则在开机

后系统自动进行连接。在使用过程中，如果由于外部原因网络被断开，系统则会每隔一段时间尝试连接，直到成功连接为止。手动连接：选择该项，网络断开后，需手动提交进行重新拨号。

2.3.1.4 PPTP

PPTP 广域网连接方式如图 2.3.1.5.1 所示：

广域网络设置

您可以依您的环境选择适当的联机模式，并针对不同的联机模式设置参数。

广域网络联机模式：

PPTP

PPTP 模式	
服务器 IP	<div>pptp_server</div>
使用者名称	<div>pptp_user</div>
口令	<div>●●●●●●●●</div>
IP 地址模式	<div>静态</div>
IP 地址	<div>192.168.1.1</div>
子网掩码	<div>255.255.255.0</div>
预设网关	<div>192.168.1.254</div>
运行模式	<div>永久连线</div> <div>Keep Alive Mode: Redial Period <div>60</div> seconds</div>
MAC 复制	
Enabled	<div>停用</div>

确定

取消

图 2.3.1.5.1 广域网 PPTP 方式

选择 PPTP 上网方式，ISP 会给您提供上网账号和上网口令。若不清楚，请咨询 ISP。相关的参数设置同 L2TP 类似，请参考 L2TP 相关设置。

2.3.2 局域网设置

选择网络设置→局域网，即可配置局域网端口的有关参数。比如设定 LAN 口 IP 地址、子网掩码、DHCP 等。局域网设置界面如图 2.3.2.1 所示：

局域网设置	
IP 地址	192.168.16.254
子网掩码	255.255.255.0
局域网 2	<input type="radio"/> 启用 <input checked="" type="radio"/> 停用
局域网 2 IP 地址	
局域网 2 子网掩码	
MAC 地址	44:33:4C:B6:DD:E2
DHCP 类型	服务器 <input type="button" value="v"/>
起始 IP 地址	192.168.16.100
结束 IP 地址	192.168.16.200
子网掩码	255.255.255.0
惯用 DNS 服务器	192.168.16.254
其他 DNS 服务器	8.8.8.8
预设信关	192.168.16.254
释放时间	86400
静态指定	MAC: <input type="text"/> IP: <input type="text"/>
静态指定	MAC: <input type="text"/> IP: <input type="text"/>
静态指定	MAC: <input type="text"/> IP: <input type="text"/>
802.1d Spanning Tree	停用 <input type="button" value="v"/>
LLTD	停用 <input type="button" value="v"/>
IGMP Proxy	停用 <input type="button" value="v"/>
UPNP	停用 <input type="button" value="v"/>
PPPoE Relay	停用 <input type="button" value="v"/>
DNS Proxy	启用 <input type="button" value="v"/>
<input type="button" value="确定"/> <input type="button" value="取消"/>	

图 2.3.2.1 局域网设置

- ◆ IP 地址：本路由器对局域网的 IP 地址，出厂默认设置为 192.168.16.254 可根据需要进行变更。
- ◆ 子网掩码：本路由器对局域网的子网掩码，出厂默认设置为 255.255.255.0，你可

以根据实际的网络状态输入不同的子网掩码。

- ◆ 局域网 2：根据实际需求，启用或禁用路由器的第二个 LAN 口地址。启用之后，需要对接下来的局域网 2 的 IP 地址和局域网 2 的子网掩码进行设置。局域网 2 IP 地址：本路由器对局域网的第二个 IP 地址。局域网 2 子网掩码：本路由器对局域网的第二个子网掩码，此功能本路由器没有用到。
- ◆ MAC 地址：显示本路由器 LAN 口的 MAC 地址。
- ◆ DHCP 类型：通过路由器内置的 DHCP 服务器，实现自动为局域网中的计算机分配 IP 地址的功能。如需启用，选择 DHCP 类型为服务器，反之，选择停用。DHCP 服务器默认为开启。
- ◆ 起始 IP 地址：根据路由器的局域网 IP 地址设置 DHCP 服务器自动分配 IP 地址时的起始地址。
- ◆ 结束 IP 地址：根据路由器的局域网 IP 地址设置 DHCP 服务器自动分配 IP 地址时的结束地址。
- ◆ 子网掩码：根据起始地址、结束地址段设置相符的子网掩码。
- ◆ 惯用 DNS 服务器：可选项，可以填入 ISP 提供给您的 DNS 服务器。
- ◆ 其他 DNS 服务器：同上。
- ◆ 预设网关：根据路由器局域网 IP 地址设置 DHCP 服务器默认网关，本路由器局域网的默认 IP
- ◆ 释放时间：该项指 DHCP 服务器给客户端主机分配的动态 IP 地址的有效使用时间（以秒为单位）。默认为 86400 秒，即 24 个小时。在该段时间内，服务器不会将该 IP 地址分配给其它主机。您可以根据实际情况，设置合适的租用时间，可提高 DHCP 服务器对作废 IP 地址的回收效率。
- ◆ 802.1d Spanning Tree：启用此功能后，防止冗余结构的网络拓扑中产生回路，防止广播风暴的产生。
- ◆ LLTD：可以选择启用或停用，启用后，存在有 LLTP 客户端，则可以自动显示路由器信息。
- ◆ IGMP Proxy：启用此功能后，可以抑制二层组播泛滥，有效地获取和控制用户信息，在减少网络侧协议消息以降低网络负荷方面起到一定作用。默认为停用。
- ◆ UPNP：启用此功能后，路由器可为内网 P2P 软件提供自动端口映射，默认为停用。
- ◆ PPPoE Relay：启用此功能后，可以使本地的计算机在路由器的网关模式下直接单独进行 PPPoE 拨号，默认停用。
- ◆ DNS Proxy：是指在防火墙上启动 dns 代理功能，这样在局域网内部没有 dns 服务器时，局域网内部客户端可以通过防火墙连接到外部 dns 服务器，进行正确的 dns 解析后，可以访问 internet。

2.3.3 DHCP 客户端列表

通过选择网络设置→DHCP 客户端列表，可以查看局域网中使用 DHCP 自动分配 IP 地址的计算机的相关信息，如网络名称，MAC 地址，IP 地址，过期剩余时间。如图 2.3.3.1 所示：

DHCP 客户端列表			
您可以在这里检视所有 DHCP 客户端。			
DHCP 客户端			
网络名称	MAC 地址	IP 地址	过期
android_329f310	C8:7B:5B:85:82:82	192.168.16.100	23:08:50

图 2.3.3.1 DHCP 客户端列表

2.3.4 VPN Passthrough

VPN (Virtual Private Network)，它没有专用的网络物理连线，只是借助公用网络（如 Internet）建立一个临时的、安全的、模拟的点对点连接，咱们也可形象地把它称为“网络中的网络”（有点电视画中画的感觉）。V

VPN Passthrough 用来处理加密的 IPsec (ESP)或 PPTP (GRE)数据包不包含明文源端口和目标端口的情况。本路由器支持 IPsec、PPTP 和 L2TP 等三种 VPN 协议，如图 2.3.4.1 所示：

VPN Passthrough	
VPN passthrough 设置，包含: L2TP, IPsec, 以及 PPTP passthrough	
VPN Pass Through	
L2TP Passthrough	停用 <input type="button" value="v"/>
IPSec Passthrough	停用 <input type="button" value="v"/>
PPTP Passthrough	停用 <input type="button" value="v"/>
<input type="button" value="确定"/> <input type="button" value="取消"/>	

图 2.3.4.1 VPN Passthrough 设置

2.3.5 高级路由选项

如果需要为特定的主机增加特定的路由，可以使用本功能。在网络中使用合适的静态路由器可以减少路由选择问题和路由选择数据流的过载，提高数据包的转发速度。通过设定目的 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，之后路由器会通过网关将数据包发往指定的目标网络/主机。本路由器的高级路由选项如图 2.3.5.1 所示：

静态路由配置

您可以在这里新增/移除订制的静态路由规则,或者启用动态路由规则交换协议

新增静态路由规则

目标IP住址

类型

主机

网关IP住址

网络接口

局部网络

注解

提交

重置

当前的路由规则

编号	目标IP住址	子网掩码	网关IP住址	旗号	路由度量	参照	使用	网络接口	注解
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	局部网络(br0)	
2	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	局部网络(br0)	
3	192.168.1.0	255.255.255.0	0.0.0.0	1	0	0	0	广域网络(eth2.2)	
4	192.168.16.0	255.255.255.0	0.0.0.0	1	0	0	0	局部网络(br0)	
5	0.0.0.0	0.0.0.0	192.168.1.1	3	1	0	0	广域网络(eth2.2)	

删除

重置

图 2.3.5.1 高级路由选项

2.4 无线网络设置

2.4.1 基本设置

无线网络的基本设置如图 2.4.1.1 所示:

基本无线设置

您可以做基本的无线通讯设置，譬如：网络名称（服务集合标识符）和频道。基本设置项目可以做简单的无线存取节点设置。

无线网络	
驱动程序版本	2.6.0.1
无线电 开/关	<input type="button" value="RADIO OFF"/>
无线网络 开/关	<input type="button" value="WiFi OFF"/>
网络模式	11b/g/n mixed mode ▾
网络名称（服务集合标识符）	ATK-RM04 <input type="checkbox"/> 隐藏 <input type="checkbox"/> 分离 <input type="checkbox"/>
广播网络名称（服务集合标识符）	<input checked="" type="radio"/> 启用 <input type="radio"/> 停用
AP Isolation	<input type="radio"/> 启用 <input checked="" type="radio"/> 停用
基本服务集合标识符	44:33:4C:B6:DD:E2
频率（频道）	2412MHz (Channel 1) ▾
高吞吐量实体模块	
运作模式	<input checked="" type="radio"/> 混合模式 <input type="radio"/> Green Field
频道带宽	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
保护间隔	<input type="radio"/> 长 <input checked="" type="radio"/> 自动
MCS	自动 ▾
反转方向权限(RDG)	<input type="radio"/> 停用 <input checked="" type="radio"/> 启用
延伸频道	2432MHz (Channel 5) ▾
空时分组编码(STBC)	<input type="radio"/> 停用 <input checked="" type="radio"/> 启用
聚合MAC业务数据单元（A-MSDU）	<input checked="" type="radio"/> 停用 <input type="radio"/> 启用
自动单一区块确认	<input type="radio"/> 停用 <input checked="" type="radio"/> 启用
拒绝单一区块确认要求	<input checked="" type="radio"/> 停用 <input type="radio"/> 启用
HT Disallow TKIP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
20/40 Coexistence	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
其它	
高吞吐量传送数据流	1 ▾
高吞吐量接收数据流	1 ▾
<input type="button" value="确定"/> <input type="button" value="取消"/>	

图 2.4.1.1 基本无线设置

- ◆ 无线电开关：开启/关闭无线电。关闭后此无线路由不发射信号。
- ◆ 无线网络开关：关闭后此无线路由器隐藏 SSID。
- ◆ 网络模式：该项用于选择路由器的工作模式，可供选择的有：802.11b/g mixed mode、802.11b only、802.11g only、**802.11b/g/n mixed mode (默认)**、802.11n only (2.4G)。
- ◆ SSID(无线网络名称)：设置无线信号的网络名称。即无线局域网的名称。用来区分不同的网络，最多可以有 32 个字符。
- ◆ 广播网络名称：通过选择启用或停用规定路由器是否对 SSID 进行广播。选择“停用”，SSID 将被隐藏。无线客户端将无法扫描到设备的 SSID。客户端必须知道设备的 SSID 才能与设备进行通讯，默认为“启用”。
- ◆ 基本服务集合标识符：指站点的 MAC 地址。在一个无线接入点，一组无线工作站和一个无线局域网接入点(AP)组成一个基本服务装置(BSS)，BSS 中的每台计算机都必须配置相同的 BSSID，即无线接入点的无线标识。
- ◆ 频率(频道)：用于选择无线网络工作的频率段，可以设置为“自动选取”或“手动选择”。需要注意的是，不同的国家或地区，可使用的信道数有所差异。关于国家或地区设置，请转到高级设置。
- ◆ 运作模式：可以选择混合模式或单一模式。在混合模式下，以前的无线网卡可以识别并连接到 Pre-NAP，但吞吐量会受到一定影响。在单一模式下，能够达到高吞吐量，但是会影响向后兼容，以及系统的安全性。默认设置为混合模式。
- ◆ 频道带宽：可选择 20 或 20/40。默认设置为 20/40
- ◆ 保护间隔：可选择自动。默认设置为自动
- ◆ MCS：调制编码表(MCS) 是 802.11n 为表征 WLAN 的通讯速率而提出的一种表示形式。默认设置为自动
- ◆ 反转方向权限(RDG)：可以选择启用或者停用此权限。
- ◆ 延伸频道：选择所定义的频段的扩展频道。
- ◆ 空时分组码：可以选择启用或者停用，默认为启用。
- ◆ 聚合 MAC 业务数据单元(A-MSDU)：把多个 Ethernet 报文通过一定的方式聚合成一个较大的载荷。
- ◆ 自动单一区块确认：实现聚合交换序列，能够提高传输速率。
- ◆ 拒绝单一区块确认要求：默认设置为停用，能够提高传输速率。

2.4.2 高级设置

选择无线网络设置→高级设置，进入到无线高级设置的界面。高级设置包含无线高级参数设置项，例如：信标间隔、发射功率等。无线网络的高级设置如图 2.4.2.1 所示。

注意：如果你是一个高手，通过高级设置有助于你根据实际的网路状况进行配置优化。但如果你只是普通用户，请勿修改其中的内容，避免弄巧成拙。

高级无线设置

使用高级设置对无线执行细部设置。高级设置包含非基本设置项目，例如：信标间隔、控制传送速率、基本数据传输速率等。

高级无线	
BG保护模式	自动 <input type="button" value="v"/>
信标间隔	100 ms (范围 20 - 999, 默认 100)
数据信标比例 (传输量指示讯息)	1 ms (范围 1 - 255, 默认 1)
分割界限	2346 (范围 256 - 2346, 默认 2346)
传输请求界限	2347 (范围 1 - 2347, 默认 2347)
发射功率	100 (范围 1 - 100, 默认 100)
短前导码	<input checked="" type="radio"/> 启用 <input type="radio"/> 停用
短碰撞槽	<input checked="" type="radio"/> 启用 <input type="radio"/> 停用
传输突发	<input checked="" type="radio"/> 启用 <input type="radio"/> 停用
数据包聚合	<input checked="" type="radio"/> 启用 <input type="radio"/> 停用
支持IEEE 802.11H	<input type="radio"/> 启用 <input checked="" type="radio"/> 停用 (仅在A频带)
国家代码	无 <input type="button" value="v"/>

Wi-Fi多媒体 (WMM)	
Wi-Fi多媒体能力	<input checked="" type="radio"/> 启用 <input type="radio"/> 停用
直接联机能力	<input type="radio"/> 启用 <input checked="" type="radio"/> 停用
adv dls capable	<input type="radio"/> 启用 <input checked="" type="radio"/> 停用
Wi-Fi多媒体参数	<input type="button" value="Wi-Fi多媒体配置"/>

组播对单播转换器	
组播对单播	<input type="radio"/> 启用 <input checked="" type="radio"/> 停用

图 2.4.2.1 高级无线设置

- ◆ BG 保护模式：默认是自动，您可以选择开启或关闭。
- ◆ 信标间隔：设置无线基站发送无线信标帧以获取周围无线网络接入信息的间隔时间，默认值是 100ms。
- ◆ 数据信标比例：传输指示消息的间隔，用以告知下一个要接收广播和多播的客户端窗口，范围为 1~255，默认为 1ms。
- ◆ 分割界限：分割界限决定封包在传送前其数据被分割的大小尺寸。可使用的范围界于 256~2346。默认值为 2346 (注：分割界限以位为单位)。建议使用默认值，或将

默认值稍微调低一点。

- ◆ 传输请求界限: 合适传输请求机制可避免当两个站台位于同一个访问点范围内但彼此的范围不同时, 出现的隐藏节点问题。传输请求界限决定站台发出 RTS 的封包大小。其范围为 0~2347, 默认值为 2347。设置传输请求界限时, 须考量其利弊得失。低设定值将使 RTS 通知太过频繁而浪费频宽。但是, RTS 封包传送次数愈频繁, 系统从数据撞碰中恢复得愈快。建议使用默认值, 或将默认值稍微调低一点。
- ◆ 发射功率: 定义当前的机器 P 对于 SSID 的发射功率大小, 50 表示只发送总功率的一半; 默认为 100, 表示发送全部功率。
- ◆ 短前导码: 默认状态为停用, 即默认采用的是长型前导帧。你可以选择启用或者停用, 建议使用默认设置。
- ◆ 短碰撞槽: 默认设置为开启, 可以对其进行禁用, 建议使用默认设置。
- ◆ 传输突发: 属于 MAC 地址层的特性, 能够提高无线网络 TCP 传输的公平性。默认设置为开启, 可以对其进行禁用, 建议使用默认设置。
- ◆ 数据包聚合: 聚合技术把多个数据包组合在一起, 增强局域网数据包正确到达目的地, 以此提高传输效率。默认设置为开启, 可以对其进行禁用, 建议使用默认设置。
- ◆ 国家代码: 不同的国家或地区对无线的管控有所差别, 比如信道的使用数量, 美国使用 11 个信道频段, 日本使用 14 个信道频段。默认为无, 即不对其进行设置。你可以根据所在的国家或地区选择合适的国家代码以符合当地的规定。
- ◆ WiFi 多媒体能力: 设置 Wi-Fi 的多媒体质量服务(QoS) 能力, 开启此功能后, 机器将根据设定对不同类型的无线数据进行相应的优先处理。默认设置为开启。注: 为了实现 WMM 功能, 需要客户端与路由器双方配合, 因此无线客户端也必须也支持 WMM 功能。
- ◆ 直接联机能力: 直接联机能力。可选择启用或禁用此功能。默认禁用。
- ◆ WiFi 多媒体参数: 单击“Wi-Fi 多媒体设置”弹出 WMM 参数配置页面。如图 2.4.2.2 所示。

无线存取节点的Wi-Fi多媒体参数						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

客户端的Wi-Fi多媒体参数					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

图 2.4.2.2 Wi-Fi 多媒体配置

2.4.3 安全设置

选择无线网络设置→安全设置，此界面用来设置无线网络的安全加密。您可以选择需要加密的服务集合标识符（SSID），然后选择一种安全模式，并设定加密密钥，以防止未被授权无线客户端的连接访问。此外还可以通过设定基于MAC的访问策略允许或禁止非法连接。如图 2.4.3.1 所示：

无线网络安全/加密设置

设置无线网络的安全/加密以防止未被授权的存取與监听。

选择服务集合标识符

服务集合标识符的选定

ATK-RM04

"ATK-RM04"

安全模式

WPAPSKWPA2PSK

Wi-Fi保护访问（WPA）

WPA演算法

☐ TKIP ☒ AES ☐ TKIPAES

通行口令

12345678

私钥更新间距

3600

seconds (0 ~ 4194303)

访问策略

功能

停用

新增：

确定

取消

图 2.4.3.1 无线网络安全设置

下面分别介绍各安全模式的设置。

2.4.3.1 OPEN WEP

OPEN WEP 安全模式(OPENWEP/SHAREDWEP/WEPAUTO)设置如图 2.4.3.1.1 所示：

选择服务集合标识符			
服务集合标识符的选定		ATK-RM04 ▼	
"ATK-RM04"			
安全模式		OPENWEP ▼	
有线等效保密 (WEP)			
默认密钥		密钥 1 ▼	
WEP密钥	WEP密钥 1:	<input type="text"/>	Hex ▼
	WEP密钥 2:	<input type="text"/>	Hex ▼
	WEP密钥 3:	<input type="text"/>	Hex ▼
	WEP密钥 4:	<input type="text"/>	Hex ▼
访问策略			
功能		停用 ▼	
新增:		<input type="text"/>	
<input type="button" value="确定"/> <input type="button" value="取消"/>			

图 2.4.3.1.1 OPEN WEP 安全模式

- ◆ WEP 加密是无线加密中最早使用的加密技术，使用 64/128/152 位密钥为传输的数据加密。选用这种加密方式会使路由器工作在较低速率上，新的 802.11n 协议也不支持此加密方式，所以除非你的无线客户端与其他的加密方式不兼容，否则不建议使用此加密方式。
- ◆ 默认密钥：虽然可以同时设置 4 个密钥，但只可选择 1 个密钥在当下使用。因此须从四个密钥中选择需要使用的一个作为当下的密钥；
- ◆ WEP 密钥 1~4：根据不同的加密长度和密钥类型，设置不同的密钥。当选择密钥类型为十六进制型 (Hex) 时，密钥为 10 位或 26 位十六进制字符；当选择密钥类型为 ASCII 时，密钥为 5 位或 13 位 ASCII 码字符。

2.4.3.2 WPA-PSK

WPA-PSK，预共享密钥 Wi-Fi 保护访问，一种标准的新型加密技术，它提供比 WEP 更强大两种强大的加密方式，TKIP（暂时密钥集成协议）或 AES（高级加密标准），并且能动态改变密码。有效改善 WEP 安全特性，更有效抵御黑客的攻击，是目前最常用的加密方式之一。WPA-PSK 的设置界面如图 2.4.3.2.1 所示。

WPA 演算法：选择一种加密方式，AES 或者 TKIP。TKIP 通过一种散列算法将密码打乱，并且通过增加一种完整性检查特性，确保密码不被篡改。通行口令：设置密钥，合法的密钥长度为：8-63 个 ASCII 字符或 64 个十六进制数(0~9、a~f 或 A~F)私钥更新间距：输入密码更新时间间隔。

选择服务集合标识符	
服务集合标识符的选定	ATK-RM04 ▼
"ATK-RM04"	
安全模式	WPA-PSK ▼
Wi-Fi保护访问 (WPA)	
WPA演算法	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES
通行口令	12345678
私钥更新间距	3600 seconds (0 ~ 4194303)
访问策略	
功能	停用 ▼
新增：	
<div>确定</div> <div>取消</div>	

图 2.4.3.2.1 WPA-PSK 安全模式

2.4.3.3 WPA2-PSK

WPA2-PSK，即预共享密钥 Wi-Fi 保护访问，版本 2，其提供的加密方法较之 WPA-PSK 更为完善，但是需注意并非所有网卡都支持。设置方法可参考 WPA-PSK。

2.4.3.3 WPAPSKWPA2PSK

同时支持 WPA-PSK/WPA2-PSK 加密，客户端可以使用 WPA-PSK 或者 WPA2-PSK 来接入网络。设置方法可参考 WPA-PSK 或 WPA2-PSK。

注意：为了提高安全等级，请不要使用简单或容易记的密码。

访问策略提供了基于 MAC 对无线访问策略的设置，可以设置允许和拒绝所选的 MAC 地址的接入。在同一 SSID 下，只能采用“允许”和“拒绝”两种方式的其中一种。选择停用，不启用访问策略功能，停止对 MAC 列表的无线设备进行访问控制。选择允许，所添加的 MAC 地址就能够正常接入路由器，而没有在的 MAC 地址则无法正常接入。选择拒绝，则反之。通过 MAC 列表前的“Del”删除按钮可以删除相应的 MAC，但需单击最下方的确定按钮提交，机器重新启动后才能生效

2.4.4 WDS

选择“无线网络设置” - “WDS”进入无线分布式系统设置界面设置 WDS 的开启、模式选择等。

WDS，即无线分布式系统(Wireless Distribution System)。通过在无线设备上开启 WDS 功能，彼此之间建立 WDS 信任和通讯关系，延伸扩展无线信号，从而将无线网络覆盖更大的范围，大大方便了我们无线上网。

组建 WDS，需要注意：作为 WDS 成员须都具备 WDS 功能，每个访问点的工作频道不可设置“自动信道选择”，必须设置为相同的且指定的信道和工作模式；WDS 成员机器配置

为同一网段内的不同 IP 地址。如需 DHCP 功能，只开启其中一台机器 DHCP 功能，关闭其他机器的 DHCP 功能。此外，为了获得更好的兼容性，请尽量使用同一品牌同一系列型号产品进行连接。

ATK-RM04 支持三种连接方式：懒人（Lazy）模式、桥(Bridge)模式和中继(Repeater)模式。

懒人（ Lazy）模式

懒人模式不需要填写对方的 BSSID，本机器的 WDS 连接作为被动连接，需要对方填写了本机器的 BSSID 地址。因此对方机器的 WDS 模式只能为非 Lazy 模式(Bridge 或 Repeater 模式)，此外建立 WDS 连接机器需设置相同的实体模式、无线通道(且为指定的，不能选择 auto 项)和无线加密类型(不支持混合加密类型，如：WPAPSKWPA2PSK)，并将机器的配置为同一网段内的不同 IP 地址，只开启其中一台机器 DHCP 功能，关闭其他机器的 DHCP 功能。

懒人模式设置如图 2.4.4.1 所示：

无线分布式系统 (WDS)	
无线分布式系统模式	Lazy Mode
实体模式	CCK
加密型态	NONE
加密私钥	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	

Apply Cancel

图 2.4.4.1 懒人模式设置

实体模式：选择支持的实体模式（CCK、OFDM 和 HTMIX 其中一种）， WDS 连接的机器彼此的实体模式需一致。

加密方式：选择 WDS 连接的加密方式选择不加密(NONE)。支持三种加密方式：WEP、TKIP（暂时密钥集成协议）和 AES（对称分组密码体制）。最多可以设置 4 个不同 WDS 加密机制用于连接 4 个不同机器，实现一对多 WDS 连接。当 WDS 连接的机器之间所设置的加密方式一样时，连接才能生效。

加密私钥：根据所选的加密方式对应的密钥规则，在此处设置 WDS 密钥。无线 AP 的 MAC 地址：填写要建立 WDS 连接设备的 BSSID。最多可以填写 4 个不同的 BSSID，实现一对多 WDS 连接。

桥接（ Bridge）模式

桥接模式需要填写对方机器的 BSSID，本机 AP 的 SSID 则被屏蔽。无线客户端无法搜索到设置为桥接模式的路由器，但有线客户端可以通过该路由器的 LAN 口连接网络。

桥接模式设置如图 2.4.4.2 所示：

Wireless Distribution System

Wireless Distribution System Settings

无线分布式系统（WDS）

无线分布式系统模式	Bridge Mode
实体模式	CCK
加密型態	NONE
加密私钥	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
无线存取节点MAC地址	
AP MAC Address	
AP MAC Address	
AP MAC Address	

ApplyCancel

图 2.4.4.2 桥接模式设置

实体模式：选择支持的实体模式（CCK、OFDM 和 HTMIX 其中一种）， WDS 连接的机器彼此的实体模式需一致。

加密方式：选择 WDS 连接的加密方式选择不加密(NONE)。支持三种加密方式：WEP、TKIP（暂时密钥集成协议） 和 AES（对称分组密码体制）。最多可以设置 4 个不同 WDS 加密机制用于连接 4 个不同机器，实现一对多 WDS 连接。当 WDS 连接的机器之间所设置的加密方式一样时，连接才能生效。

加密私钥：根据所选的加密方式对应的密钥规则，在此处设置 WDS 密钥。无线 AP 的 MAC 地址：填写要建立 WDS 连接设备的 BSSID。最多可以填写 4 个不同的 BSSID，实现一对多 WDS 连接。

中继 (Repeater) 模式

中继模式也需要填写欲连接机器的 BSSID，与桥接模式所不同的是，无论是无线客户端还是有线客户端均可通过设置为中继模式的连接网络

2.4.5 WPS

WPS 是一项非专有的规范，它是由 Wi-Fi 联盟实施的认证项目。通过 WPS 能够简单、快捷地在无线网络客户端和设备之间建立加密连接，您不必选择加密方式和设置密钥，只需输入正确 PIN 码或者 PBC(或模块的 WPS/RST 按钮)来简易地设置 WPS。

2.4.6 基地台扫描

此功能只有当 ATK-RM04 工作在以太网转换的时候，才会出现，如图 2.4.6.1 所示：

扫描						
服务集合标识符	基本服务集合标识符	接收信号强度指示	频道	加密方式	认证方式	网络形态
<input type="radio"/> ALIENTEK	EC-17-2F-AC-21-E0	24%	1	AES	WPA2-PSK	Infrastructure

Disconnected 连结 重新扫描 新增联机设置档

图 2.4.6.1 基地台扫描

选中你要连接到的无线路由器，点击：连接，会出现如图 2.4.6.2 所示界面：

服务集合标识符: ALIENTEK

安全原则

安全模式: WPA2-Personal

Wi-Fi 保护访问 (WPA)

WPA 演算法: ☐ TKIP ☒ AES

通行口令:

确定 取消

图 2.4.6.2 连接到无线路由器

2.4.7 客户端列表

点击该功能，可以查看当前连接到无线路由器的客户端列表，如图 2.4.7.1 所示：

客户端列表

您能在此监视连结上这台无线存取节点的客户端。

无线网络							
MAC地址	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
C8:7B:5B:85:82:82	1	0	3	7	20M	1	0

图 2.4.7.1 客户端列表

2.4.8 统计资料

此功能用于查询无线状态信息，如图 2.4.8.1 所示：

AP Wireless Statistics

Wireless TX and RX Statistics

Transmit Statistics	
Tx Success	298
Tx Retry Count	50, PER=14.4%
Tx Fail after retry	0, PLR=0.0e+00
RTS Successfully Receive CTS	0
RTS Fail To Receive CTS	0
Receive Statistics	
Frames Received Successfully	2561
Frames Received With CRC Error	942, PER=26.9%
SNR	
SNR	41, n/a, n/a

Reset Counters

图 2.4.8.1 无线通信状态信息

2.5 防火墙

2.5.1 MAC/IP/Port 过滤

此功能用于路由器所带的客户端进行限制管理的，如果你需要限制路由器所带机器的上网情况，可以使用本功能。在使用本功能前首先得启用它并且选择一种默认策略(接受或抛弃)，表示不符合规则的数据包被接受或者拒绝。然后填写相应的过滤规则，注意并不是所有项都要填满，而是根据自己的需要填写相应选型。例如，要禁止 IP 为 192.168.16.146 的 IP 上网(其它都可以上网)，只需要使用默认策略为接受的策略，并在源 IP 地址一栏里填入

192.168.16.146 就可以了。运用本功能，能够提高用户局域网的安全性和可管理性。

MAC/IP/Port 过滤设置如图 2.5.1.1 所示：

MAC/IP/Port过滤设置

您可以建立防火墙规则来保护您的网路远离Internet病毒蠕虫恶意攻击。

基本设置

MAC/IP/Port过滤	停用 <input type="button" value="v"/>
默认原则 -- 未符合规则的数据包将被：	抛弃。 <input type="button" value="v"/>

MAC/IP/Port过滤设置

来源端MAC地址	<input type="text"/>
目的端IP地址	<input type="text"/>
来源端IP地址	<input type="text"/>
协议	None <input type="button" value="v"/>
目的端端口范围	<input type="text"/> - <input type="text"/>
来源端端口范围	<input type="text"/> - <input type="text"/>
执行动作	接受 <input type="button" value="v"/>
注解	<input type="text"/>

(The maximum rule count is 32.)

当前系统的MAC/IP/Port过滤规则：

编号	来源端MAC地址	目的端IP地址	来源端IP地址	协议	目的端端口范围	来源端端口范围	执行动作	注解	数据包计数
默认抛弃									-

图 2.5.1.1 MAC/IP/Port 过滤设置

- ◆ **MAC/IP/Port 过滤:** 如果您想启动该功能, 请选择“启用”, 默认停用;
默认原则: 对于不符合自定义的规则就按此策略执行, 可选择"抛弃"或者"接受".
MAC 地址: 填写你所要定义规则的 MAC 地址。
- ◆ **IP 地址:** 输入需要过滤的目的 IP 地址。
- ◆ **协议:** 选择被控制的数据包所使用的协议。
- ◆ **目的端口范围:** 输入需要控制的目的端口号, 起始端口号不能大于终止端口号。
- ◆ **来源端口范围:** 输入需要控制的来源端口号, 起始端口号不能大于终止端口号。
- ◆ **执行动作:** 所定义的规则是丢弃还是接受, 与默认策略相反。

2.5.2 Port 转送

即端口转发, 端口映射, 可以通过设置虚拟服务器, 将 WAN 口 IP 地址、外部端口号和局域网内服务器 IP 地址、内部端口建立映射关系, 为广域网用户访问局域网内部服务器提供的服务, 比如 Web 服务、Email 以及 FTP 等。缺省情况下, 为保证局域网的安全, 无线路由器会阻断从因特网主动发起的连接请求, 因此, 如果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。

端口转发设置如图 2.5.2.1 和 2.5.2.2 所示:

虚拟服务器设置

您可以建立虚拟服务器来提供网络服务。

虚拟服务器设置	
虚拟服务器设置	停用 <input type="button" value="v"/>
IP地址	<input type="text"/>
端口范围	<input type="text"/> - <input type="text"/>
协议	TCP&UDP <input type="button" value="v"/>
注解	<input type="text"/>

(The maximum rule count is 32.)

当前系统的虚拟服务器:

编号	IP地址	端口范围	协议	注解
<input type="button" value="选择删除"/> <input type="button" value="重设"/>				

图 2.5.2.1 端口转发设置 1

- ◆ **虚拟服务器设置:** 设置启用或停用虚拟服务器, 默认值是停用
- ◆ **IP 地址:** 输入您要设置为虚拟服务器的内网 IP 地址, 如 192.168.16.254
- ◆ **端口范围:** 映射的内网主机提供的服务端口段
- ◆ **协议:** 选择应用程序协议 (TCP/UDP/TCP&UDP), 默认为 TCP&UDP
- ◆ **注解:** 加入相关备注信息。

- ◆ 当前系统的虚拟服务器：显示当前已加入的虚拟服务器列表。

forward single port virtual server

forward single port virtual server setting

停用

IP地址

forward virtual server public port

forward virtual server private port

协议

TCP&UDP

注解

(The maximum rule count is 32.)

确定

重设

forward current single port virtual server

编号	IP地址	forward virtual server public port	forward virtual server private port	协议	注解
<div>选择删除</div> <div>重设</div>					

图 2.5.2.2 端口转发设置 2

- ◆ forward single port virtual server setting：设置启用或禁止单端口虚拟服务器，默认值是停用
 - ◆ IP 地址：输入您要设置为单端口虚拟服务器的内网 IP 地址
 - ◆ forward virtual server public port：客户端访问虚拟服务器所使用的端口。
 - ◆ forward virtual server private port：虚拟服务器上真实开放的服务端口。
 - ◆ 协议：选择应用程序协议（TCP/UDP/TCP&UDP），
 - ◆ 注解：加入相关备注信息
- 当前系统的单端口虚拟服务器：显示当前已加入的虚拟服务器列表

2.5.3 DMZ 主机

DMZ 主机实际上就是一个缺省的虚拟服务器，优先级低于虚拟服务器。如果无线路由器收到一个来自外部网络的连接请求时，它将首先根据外部请求的服务端口号，查找虚拟服务列表，如果有匹配的表项，就把请求消息发送到该表项对应的虚拟服务器上去；没有查到匹配的表项，则检查是否有匹配的 DMZ 主机，如果 DMZ 主机存在，就把请求消息全都转发到 DMZ 主机上去，否则丢弃。

具体设置，只需输入局域网指定 DMZ 主机的 IP 地址，然后选中启用并点击保存即可。需要注意的是：开启 DMZ 功能，该主机完全暴露给广域网，安全性降低。此外所访问 DMZ 主机的端口号应与 DMZ 实际开启的服务端口号一样。

DMZ 主机设置如图 2.5.3.1 所示：



DMZ设置

您可以建立一个隔离区（DMZ）来区分内部网络与Internet。

DMZ设置	
DMZ设置	停用
DMZ IP地址	<input type="text"/>

☐ TCP port 80除外

确定 重设

图 2.5.3.1 DMZ 主机设置

- ◆ DMZ 设置：启用或禁止 DMZ 主机。
- ◆ DMZ IP 地址(DMZ IP Address)：输入您想要公开的主机的 IP 地址。

2.5.4 系统安全设置

系统安全设置，如图 2.5.4.1 所示：



系统安全设置

您可以透过设置系统防火墙来保护路由器或无线接入点本身。

远程管理	
远程管理（經由广域网络）	允許

过滤广域网路的PING封包	
过滤广域网路的PING封包	停用

端口扫描	
防止端口扫描	停用

SYN Flood攻击	
防止SYN Flood攻击	停用

数据包状态检测 (SPI)	
SPI 防火墙	停用

确定 重设

图 2.5.4.1 系统安全设置

通过设置防火墙的系统安全设置，可以启用或者禁止远程管理实现允许或禁用来自 WAN 的计算机通过输入路由器 WAN 口 IP 地址登陆 WEB 进行管理；停用或启用过滤广域网络的 PING 封包功能响应或禁止来自 WAN 口的 Ping 请求；此外还可以停用或启用端口扫描、块溢出、SPI 防火墙等功能。需要注意的是启用相应的某些功能，如启用 SPI 防火墙功能，可能导致一些既定策略(如 IP/MAC/PORT 过滤)失效，请慎重使用。

2.5.6 内容过滤

内容过滤设置如图 2.5.6.1 所示：

内容过滤设置

您可以设置内容过滤规则来限制不适当的网页。

网页内容过滤

过滤

☐ Proxy ☐ Java ☐ ActiveX

确定

重设

网页 URL 过滤设置

当前系统的网页 URL 过滤规则：

编号	URL
<div>删除</div>	<div>重设</div>

新增URL过滤规则

URL:

新增

Reset

网页主机过滤设置

当前系统的网页主机过滤规则

编号	主机名(关键字)
<div>删除</div>	<div>重设</div>

当前系统的网页主机过滤规则：

关键字

新增

Reset

图 2.5.6.1 内容过滤设置

- ◆ 通过内容过滤设置界面，可以设定对所浏览的网页中包含的 Proxy, Java, ActiveX 内容进行过滤。

用户手册

www.alientek.com

30

- ◆ URL 过滤规则：实现禁止局域网的机器访问某一个网站或某类网站。当前系统的网页 URL 过滤规则：显示定义的 URL 过滤规则。如需撤销，将其选中，通过删除按钮即可删除；新增 URL 过滤规则：输入需要过滤的 URL 地址，点击新增按钮，实现禁止访问某一个网站。新增 URL 过滤规则将会在上一项中显示；
- ◆ 当前系统的网页主机过滤规则：显示定义的主机过滤规则。如需撤销，将其选中，通过删除按钮即可删除；新增网页主机过滤规则：输入需要过滤的主机名关键字，点击新增按钮，实现禁止访问某类网站。新增主机过滤规则将会在上一项中显示；

2.6 系统管理

2.6.1 管理

选择系统管理→管理，即可进行系统语言设置；系统的管理者账号和口令设置；动态域名服务设置，设置路由器的时间与 PC 的时间同步，或使用 NTP（网络时间协议）从服务器系统获取同步时间。

管理设置界面如图 2.6.1.1 所示。

- ◆ 选择语言：选择英文，简体中文和繁体中文其中一种语言，单击确认，即可完成语言的切换。
- ◆ 帐号：输入需更换的用户名，出厂默认为 admin。口令：输入此用户名的密码，出厂默认为 admin。注：如果忘了用户名和密码，可以让模块恢复默认设置，此时用户名和密码都将恢复默认值：admin/admin。
- ◆ 目前时间：显示当前系统时间。点击“主机同步”按钮，机器即可与当前管理主机同步时间。时区：选择系统所在时区。中国地区用户选择“(GMT+08: 00) 中国，中国香港”时间。
- ◆ 网络时间服务器：输入时间服务器的 URL 地址。中国地区的用户建议选择亚太地区的时间服务器。
- ◆ 网络时间校对（小时）：与时间服务器同步的间隔时间。
- ◆ 动态域名服务提供商：选择您使用的 DDNS 服务提供商。
- ◆ 帐号：请您输入在 DDNS 服务供应商上注册的用户名。口令：请您输入在 DDNS 服务供应商上注册的密码
- ◆ 动态域名服务：输入您使用的 DDNS 服务提供商注册的域名

系统管理

您可以在这里设置系统的管理者及口令等。

语言设置

选择语言	Simple Chinese
<div>确定</div> <div>取消</div>	

管理者设置

帐号	admin
口令	•••••
<div>确定</div> <div>取消</div>	

网络时间设置

当前时间	Wed Sep 11 14:54:31 UTC 20	主机同步
时区：	(GMT-11:00) 中途岛、萨摩亚	
网络时间服务器	ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw	
网络时间校准(小时)		
<div>确定</div> <div>取消</div>		

动态域名服务设置

动态域名服务提供商	无
帐号	
口令	
动态域名服务	
<div>确定</div> <div>取消</div>	

System Reboot

System Reboot Button	Reboot
----------------------	--------

图 2.6.1.1 管理设置界面

2.6.2 固件更新

选择系统管理→固件更新，即可进行固件升级更新。如图 2.6.2.1 所示：

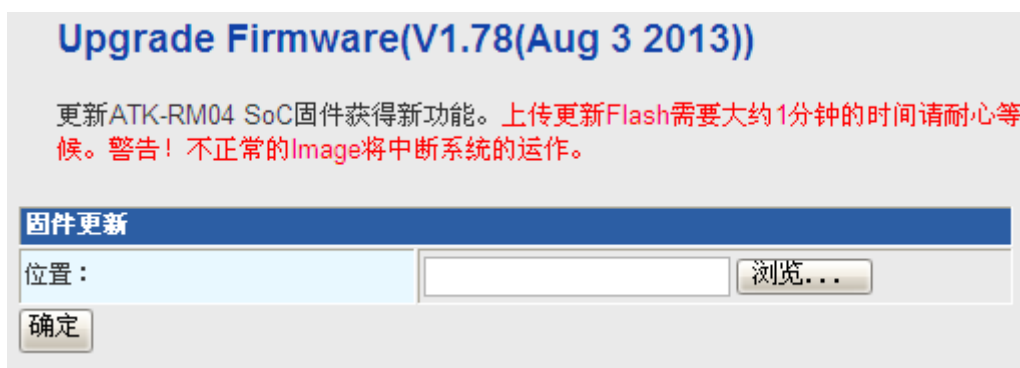


图 2.6.2.1 固件更新

点击“浏览”，选择将要更新的固件（.img 文件），然后点击“确定”，即可实现固件更新。

重要提示：软件升级期间切勿切断电源或中断网络连接，以免造成升级失败，甚至设备损坏。此外，固件千万别搞错了，否则模块可能被刷成砖头!!! 所以，不要乱刷固件。

2.6.3 设置管理

选择系统管理→设置管理，即可以导出配置文件保存系统设置，通过导入配置文件恢复系统设置，也可以将系统恢复至出厂值。设置管理如图 2.6.3.1 所示：

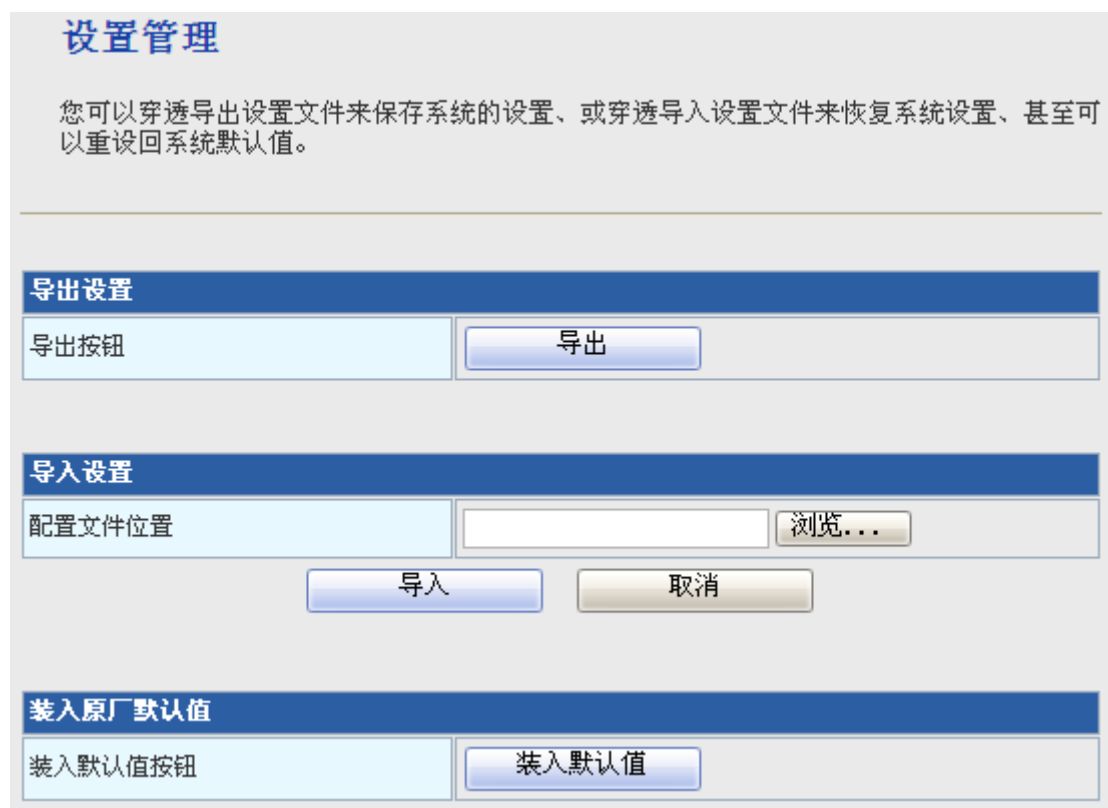


图 2.6.3.1 设置管理

导出设置：点击按钮将系统当前设置导出到指定位置，注意：导出配置时使用的默认文件名建议不做更改。

导入设置：点击浏览按钮，选择以前所导出的配置文件后，点击导入按钮，系统自动重启并加载配置文件，恢复之前的设置。装入原厂默认值：此按钮将所有设置恢复到默认出厂值。

注：导入配置以及恢复出厂设置前建议您保存当前配置。

2.6.4 状态

选择系统管理→状态，即可查看系统的 SDK 版本，正常运行时间，系统平台以及运行模式，Internet 配置信息和局域网信息。如图 2.6.4.1 所示：

无线存取节点状态

让我们可以看到ATK-RM04平台的状态。

系统信息	
SDK版本	V1.78(Aug 3 2013)
系统正常运行时间	15 hours, 34 mins, 19 secs
Operation Mode	Gateway Mode

Internet Configurations	
Connected Type	DHCP
WAN IP Address	192.168.1.110
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary Domain Name Server	218.30.118.6
Secondary Domain Name Server	114.114.114.114
MAC Address	44:33:4C:B1:D4:DD

Local Network	
Local IP Address	192.168.16.254
Local Netmask	255.255.255.0
MAC Address	44:33:4C:B1:D4:DC

Ethernet Port Status

not support

图 2.6.4.1 状态信息

3. 结构尺寸

ATK-RM04 模块的尺寸结构如图 3.1 所示：

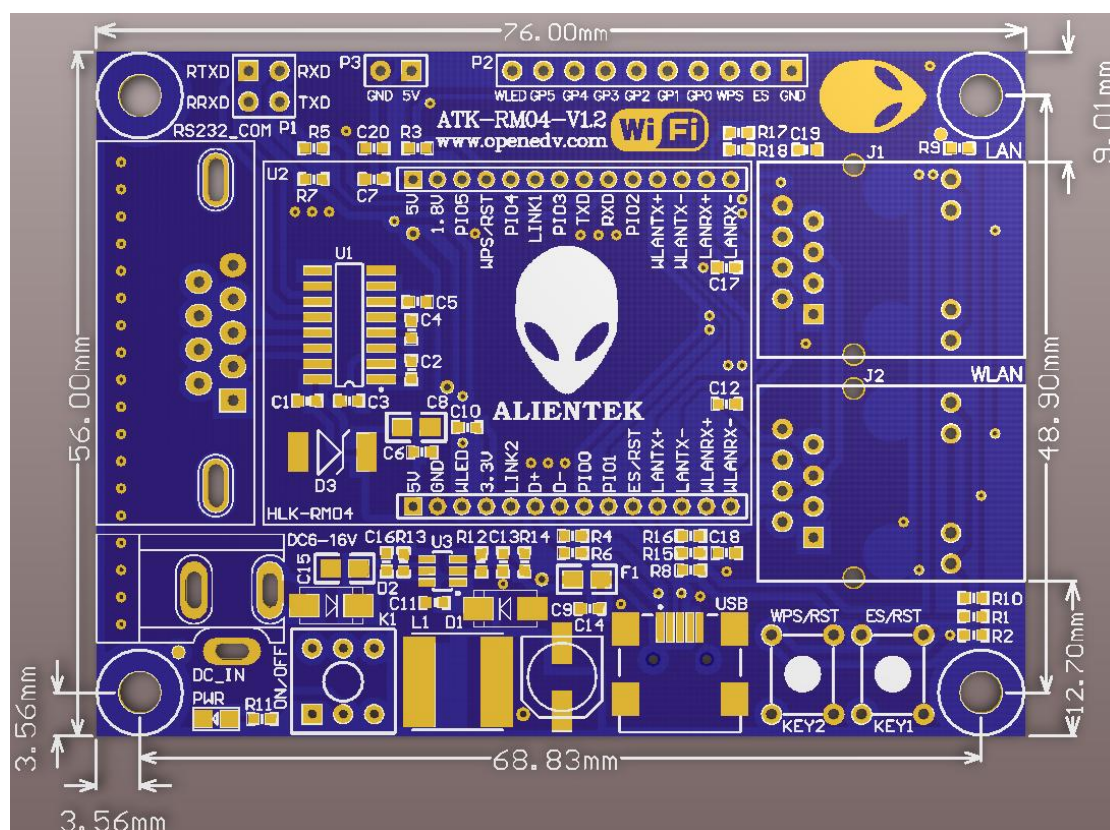


图 3.1 ATK-RM04 模块尺寸图

4. 其他

1、 购买地址:

官方店铺 1: <http://eboard.taobao.com>

官方店铺 2: <http://shop62103354.taobao.com>

2、资料下载

ATK-RM04 模块资料下载地址: <http://www.openedv.com/posts/list/23184.htm>

3、技术支持

公司网址: www.alientek.com

技术论坛: www.openedv.com

传真: 020-36773971

电话: 020-38271790

