

WEB 管理手册

AP 系列无线接入点

RGOS11.1(5)B8P3

文档版本 : V1.0

版权声明

copyright © 2016 锐捷网络

保留对本文档及本声明的一切权利。

未得到锐捷网络的书面许可，任何单位和个人不得以任何方式或形式对本文档的部分内容或全部进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。



以上均为锐捷网络的商标。

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。

免责声明

您所购买的产品、服务或特性等应受商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，锐捷网络对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。锐捷网络保留在没有任何通知或者提示的情况下对文档内容进行修改的权利。

本手册仅作为使用指导。锐捷网络在编写本手册时已尽力保证其内容准确可靠，但并不确保手册内容完全没有错误或遗漏，本手册中的所有信息也不构成任何明示或暗示的担保。

前言

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

- 锐捷网络官方网站：<http://www.ruijie.com.cn/>
- 锐捷网络在线客服：<http://webchat.ruijie.com.cn>
- 锐捷网络官方网站服务与支持版块：<http://www.ruijie.com.cn/service.aspx>
- 7×24 小时技术服务热线：4008-111-000
- 锐捷网络技术论坛：<http://bbs.ruijie.com.cn/portal.php>
- 常见问题搜索：<http://www.ruijie.com.cn/service/known.aspx>
- 锐捷网络技术支持与反馈信箱：4008111000@ruijie.com.cn

本书约定

1. 命令行格式约定

命令行格式意义如下：

粗体：命令行关键字（命令中保持不变必须照输的部分）采用加粗字体表示。

斜体：命令行参数（命令中必须由实际值进行替代的部分）采用斜体表示

[]：表示用[]括起来的部分，在命令配置时是可选的。





{ x | y | ... }：表示从两个或多个选项中选取一个。

[x | y | ...]：表示从两个或多个选项中选取一个或者不选。

//：由双斜杠开始的行表示为注释行。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

-
-  警告标志。表示用户必须严格遵守的规则。如果忽视此类信息，可能导致人身危险或设备损坏。
 -  注意标志。表示用户必须了解的重要信息。如果忽视此类信息，可能导致功能失效或性能降低。
 -  说明标志。用于提供补充、申明、提示等。如果忽视此类信息，不会导致严重后果。
 -  产品/版本支持情况标志。用于提供产品或版本支持情况的说明。
-

3. 说明

- 本手册举例说明部分的端口类型同实际可能不符，实际操作中需要按照各产品所支持的端口类型进行配置。
- 本手册部分举例的显示信息中可能含有其它产品系列的内容（如产品型号、描述等），具体显示信息请以实际使用的设备信息为准。
- 本手册中涉及的路由器及路由器产品图标，代表了一般意义下的路由器，以及运行了路由协议的三层交换机。

1 AP-Eweb 功能配置

1.1 概述

WEB 管理通过使用浏览器（如 IE）访问 WEB 管理系统来管理 AP 设备。

WEB 管理包括 WEB 服务器和 WEB 客户端两部分。WEB 服务器集成在设备上，用来接收和处理客户端发来的请求，并把处理结果返回给客户端，WEB 客户端通常指网络浏览器，如 IE。

✔ 目前该文档仅适用于系列 AP 设备。

1.2 典型应用

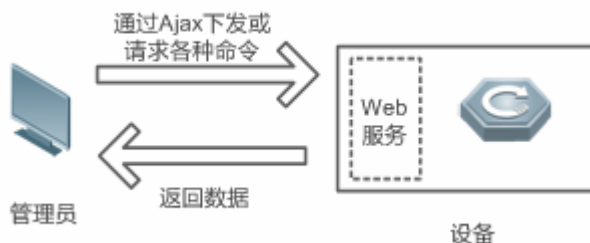
典型应用	场景描述
通过WEB管理设备	管理员通过浏览器访问设备，使用 WEB 管理系统对设备进行配置管理。

1.2.1 通过WEB管理设备

应用场景

如下图所示，管理员通过浏览器访问设备，使用 WEB 管理系统对设备进行配置。

图 1-1 应用拓扑



【注释】 Web 管理界面是通过拼接各种设备命令，然后通过 AJAX 请求到设备，设备根据命令返回相关数据。设备上有一个 WEB 服务，可以处理基本的 HTTP 协议请求。

功能部属

配置环境要求

客户端的要求：

- 网管使用 WEB 管理客户端的 WEB 浏览器登陆设备 WEB 管理界面对设备进行配置管理。客户端通常是指 PC，也可能是一些其它的移动终端设备，如笔记本电脑、IPAD 等。
- 浏览器：支持 IE7.0、IE8.0、IE9.0、IE10.0、IE11.0、Google chrome、火狐浏览器、以及部分基于 IE 内核的浏览器（如 360 安全浏览器）。使用其它浏览器登录 WEB 管理时，可能出现乱码或格式错误等异常。

- 分辨率：建议分辨率设置为 1024*768、1280*1024 及 1440*960，在其它分辨率下，页面字体和格式可能出现不对齐、不够美观等异常。

服务器的要求：

- AP 设备需要启动 WEB 服务。
- AP 设备需要配置 WEB 管理登录认证信息。
- AP 设备需要配置管理 IP 地址。

缺省配置

下表用来描述 WEB 管理的缺省配置。

功能特性	缺省值
WEB 服务	开启
设备 IP	192.168.110.1

缺省用户/密码	权限说明
admin / admin	超级管理员，拥有所有权限。

i 缺省账号没有修改密码的情况下没有保存在 show running-config 中

当WEB服务开启，并且IP地址配置正确即IP地址可达，可以直接在浏览器中输入可达IP地址，http://ip地址，如<http://192.168.110.1>，按回车出现如下页面：



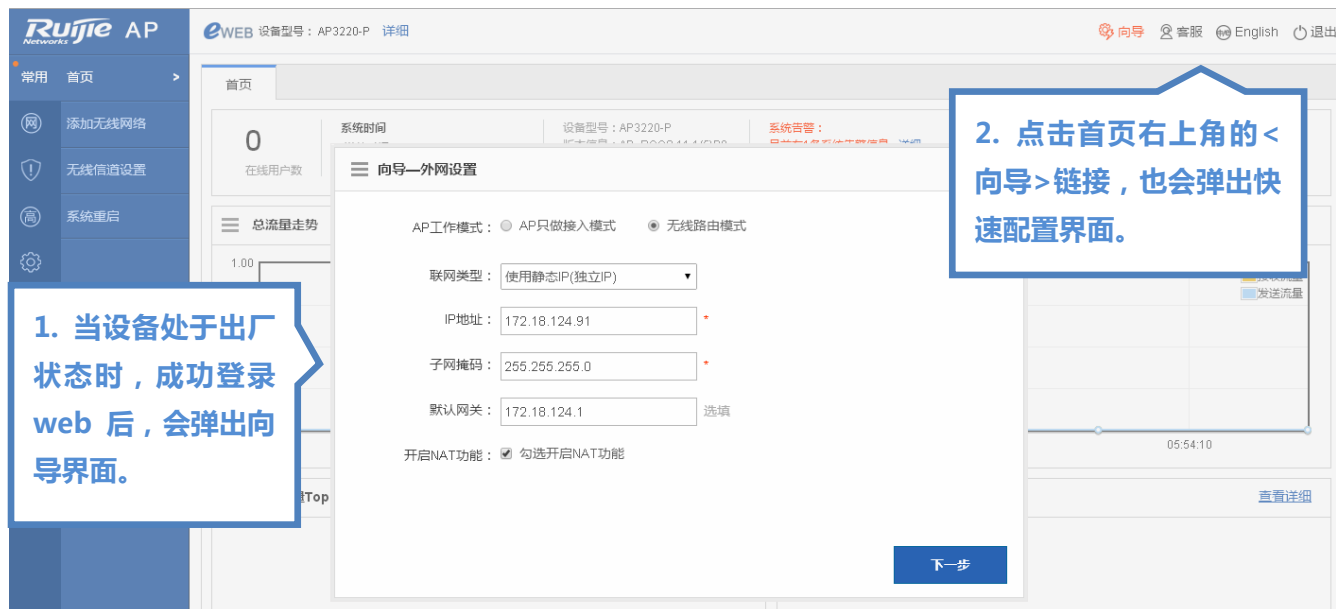
输入用户名和密码后点击<登录>。



1.3 AP-Eweb配置

1.3.1 快速配置

根据您的实际网络环境创建 WiFi 使得用户可以连上这个 WiFi 上网。



三

向导—外网设置

×

AP工作模式：

AP只做接入模式

无线路由

WiFi名称必填，其他配置项可选。

联网类型：

使用静态IP(独立IP)

IP地址：

172.18.124.91

*

子网掩码：

255.255.255.0

*

默认网关：

172.18.124.1

选填

开启NAT功能：

勾选开启NAT功能

点击显示查看密码

点击<完成配置>，完成操作。

下一步

三

向导—WiFi配置

×

WiFi名称：

Eweb_AAAA1

*

WiFi密码：

.....

显示密码

开启DHCP服务：

DHCP服务器配置在本AP上(AP来分配地址)

Vlan ID：

1

IP分配范围：

192.168.1

1

至

254

DHCP网关：

192.168.1.1

DNS服务器：

114.114.114.114

选填

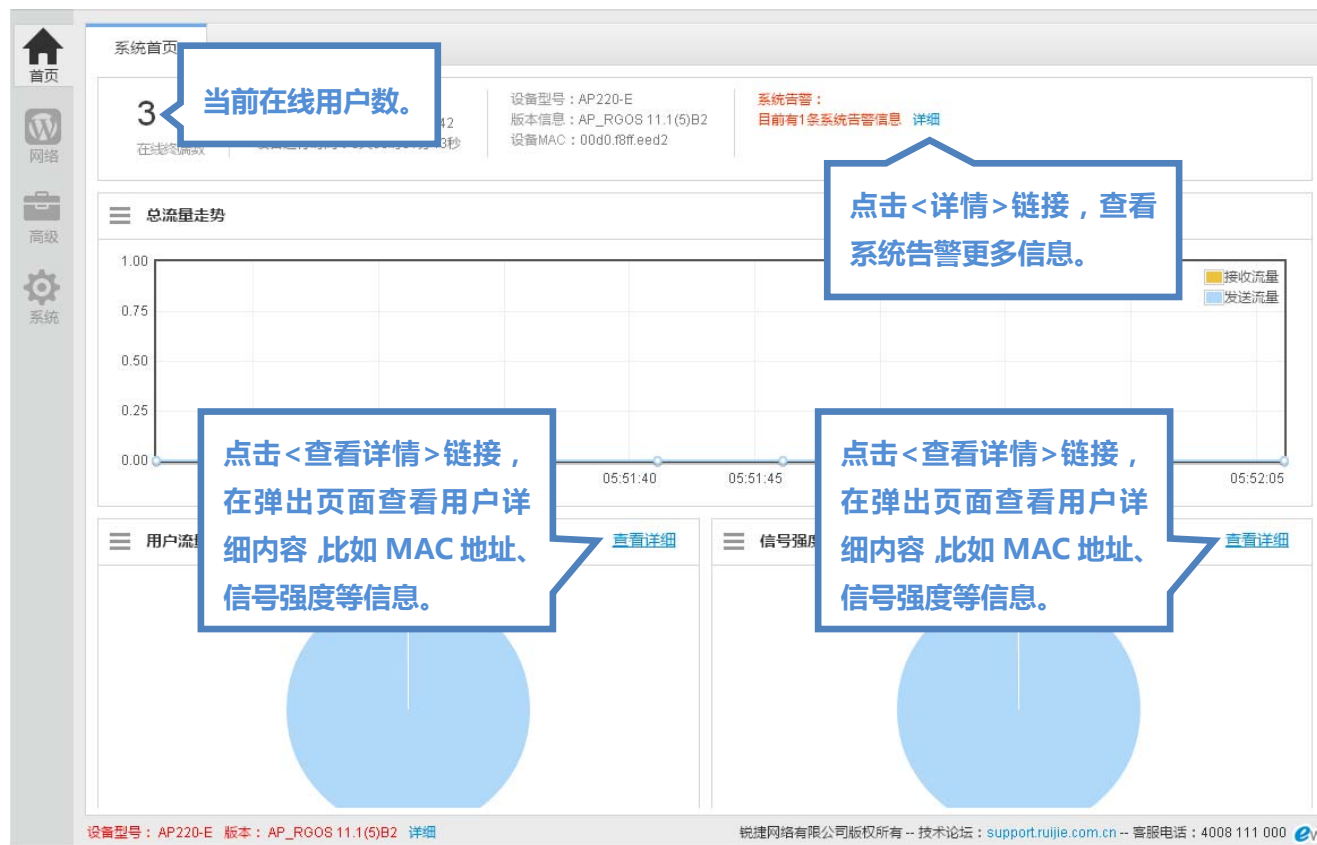
上一步

完成配置

1.3.2 常用

1.3.2.1 首页

“首页”可以让您一目了然查看 AP 设备的基本信息，如设备 MAC 地址、设备型号等，系统告警信息，AP 设备总流量趋势，可以了解全部管理 AP 的最新动态，每个管理 AP 对应的用户信息，时时了解终端用户信号强度分布情况。



1.3.2.2 添加无线网络

无线网络是为了让无线终端用户能够通过 wifi 接入 AP 进行上网。可以添加多个无线网络或删除无线网络。

添加无线网络的页面如下：

The screenshot shows the 'Add Wireless Network' (添加无线网络) configuration page. It includes fields for:

- WiFi Name:** Eweb_EED21
- Encryption Type:** WPA/WPA2-PSK(通用版)
- WiFi Password:** (masked with dots) with a 'Show Password' (显示密码) checkbox.

Below these fields is a section for 'Advanced Configuration' (高级配置) and two buttons: 'Save Settings' (保存设置) and 'Delete Network' (删除网络).

- 添加无线网络

1. 点击<+>按钮,打开一个新的网络页签。新增一个 WiFi。

2. 输入需要的配置项。

3. 点击<保存设置>提示“设置成功”后,完成操作。

- 编辑无线网络

1. 点击需要编辑的 WiFi 页签。

2. 输入需要的配置项。

3. 点击<保存设置>提示“设置成功”后,完成操作。

- 删除无线网络

点击<删除网络>按钮,弹出确认窗口,点击<确定>按钮,完成删除操作。。

1.3.2.3 无线信道设置

无线信道设置主要是调整设备发出无线 WiFi 的信号强度,可以设置 2G 和 5G 网络的信道等参数。

- 开启 2.4G 网络

无线信道设置

说明：如果感觉信号不稳定或感觉信号不强，可以试试切换信道（如下表）
注意：信号还跟天线是否拧紧，周围是否有障碍物有关。

开启2.4G网络：☒ ON

[【强制将2.4G转成5G】](#)

当前所在的国家：中国(CN)

无线信道：1 当前无线信道：1

无线频率带宽：20MHZ

信号强度：穿墙

无线最大用户数：32 可连接的最大无线用户数(范围1-128)

点击图标。可以打开和关闭 2.4G 网络。

点击链接，强制转换网络 5G。

- 开启 5G 网络

无线信道设置

说明：如果感觉信号不稳定或感觉信号不强，可以试试切换信道（如下表）
注意：信号还跟天线是否拧紧，周围是否有障碍物有关。

开启2.4G网络：☐ OFF

开启5G网络：☒ ON

[【强制将5G转成2.4G】](#)

当前所在的国家：中国(CN)

无线信道：149 当前无线信道：149

无线频率带宽：20MHZ

信号强度：穿墙

无线最大用户数：32 可连接的最大无线用户数(范围1-128)

保存设置

点击图标。可以打开和关闭 5G 网络。

点击链接，强制转换网络 2.4G。

1.3.2.4 系统重启

一键重启，方便快捷。

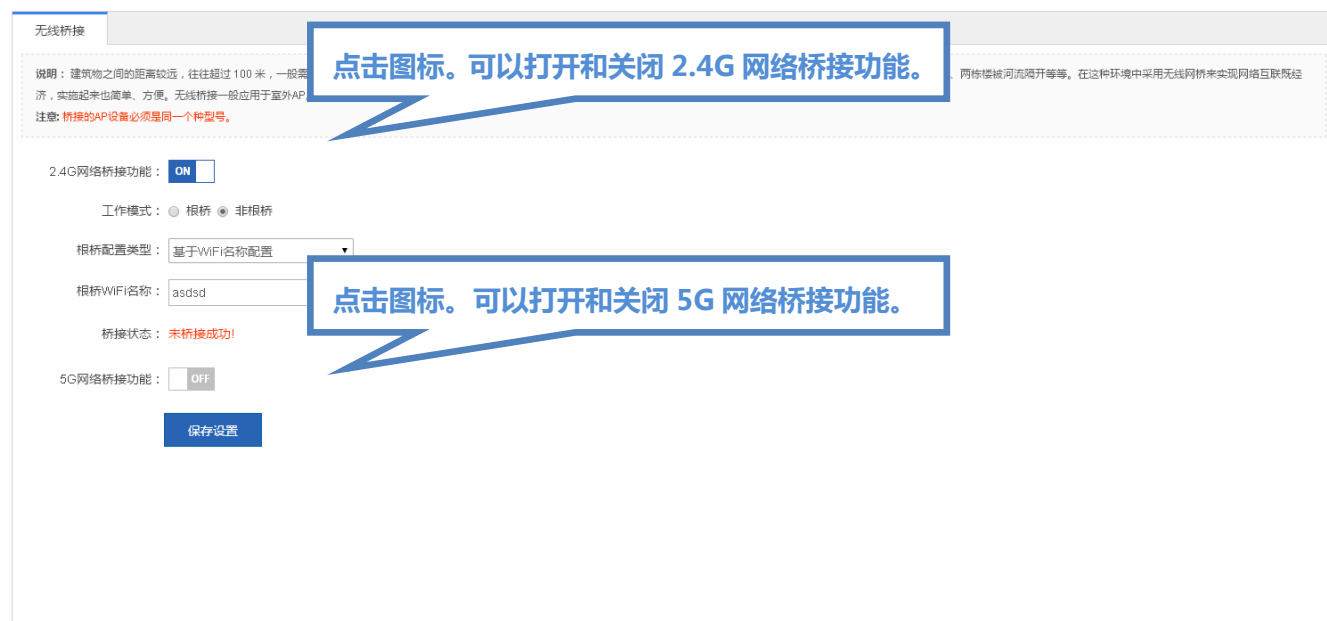


1.3.3 网络

1.3.3.1 无线桥接

多个 AP 通过无线桥接或中继的方式相连，从而达到连接分布网络和扩展无线信号的作用。AP 可以当做一个中继器，把前端的网络扩展出去，无线 wifi 发射更远，让更远的用户关联连接。无线桥接支持 2.4G 网络和 5G 网络桥接功能配置。

根据需要开启 2.4G 或者 5G 网络桥接功能，选择“工作模式”和“中心基站网络”，点击<保存配置>按钮，完成配置。



1.3.3.2 上网实名认证

Web 认证是一种对用户访问网络的权限进行控制的身份认证方法，这种认证方法不需要用户安装专用的客户端认证软件，使用普通的浏览器软件就可以进行身份认证。进行上网实名认证对用户的管理更加方便快捷。根据认证服务器所在位置分为外置 web 认证和内置 web 认证。

外置 web 认证

未认证用户使用浏览器上网时，接入设备会强制浏览器访问特定站点。在指定的 web 站点进行认证操作。当 portal（推送认证的 web 界面）在 AC 设备之外，单独的设备时是外置 web 认证。

The screenshot shows the 'External Web Authentication' configuration page. It includes fields for 'Server Type' (One-Generation, Two-Generation), 'Server IP Address' (2.2.2.2), 'Redirect Home' (http://2.2.2.2/index.html), 'Server Password' (11), 'SNMP Server' ([SNMP Server]), and 'Select to Enable Authentication' (Select to Enable Authentication). A 'Save Settings' button is at the bottom. Callouts highlight: 'Configure the IP address of the authentication server.', 'Redirect to the homepage, for users who have not been authenticated, it is necessary to redirect to the homepage to enter authentication.', 'SNMP server user and authentication server information exchange.', and 'Wireless management can be used for wifi addition and modification.'

内置 web 认证

未认证用户使用浏览器上网时，接入设备会强制浏览器访问特定站点。在指定的 web 站点进行认证操作。当 portal（推送认证的 web 界面）内嵌在 AC 设备中时是内置 web 认证。

The screenshot shows the 'Internal Web Authentication' configuration page. It includes fields for 'User Authentication Method' (Only use local authentication information), 'Internal Server Port' (8888), and 'Apply to Wifi' (Eweb_33AA1). A 'Save Settings' button is at the bottom. Callouts highlight: 'View local users, manage users, can add and modify users.', 'Online users, manage online users.', and 'Online users, manage online users.'

高级设置

Web 认证的高级设置，提供的是 Web 认证一些可选特性，这些可选特性对一代 Web 认证、二代 Web 认证均适用。这些可选特性在一些网络环境下能够帮助用户解决一些实际问题。

外置web认证

内置web认证

高级设置

最大HTTP会话数：

(范围:1-255，默认255) 防止同一个未认证用户发起过多的HTTP连接请求，需要限制未认证用户的最大HTTP会话数。

重定向超时时间：

(范围:1-10秒，默认3) 设置维持重定向连接的超时时间，防止未认证用户不发GET/HEAD报文，而又长时间占用TCP连接。

在线信息更新时间：

(范围:30-3600秒，默认180) 设置在线用户信息的更新时间间隔。

重定向HTTP端口：

(端口号范围:1-65535) 多个用“,”隔开，最多可配置10个。

MAC旁路认证应用：

(已配置1x认证的WIFI无法应用) 这是一种基于MAC地址的免客户端认证的方式，一般用于打印机等设备的认证。

免认证网络资源：

输入网络资源服务器的IP地址，所有用户（包括未认证用户）都可以访问该IP；最大允许配置50条规则。

IP地址：

掩码：

✕

+添加

免认证用户IP：

该用户可以直接上网，不需要认证。最大允许配置50条规则。

IP地址：

掩码：

✕

+添加

保存设置

清除设置

1.3.4 安全

1.3.4.1 反制非法AP

无线网络中可能存在非法 AP 设备非法 AP 可能存在安全漏洞或被攻击者操纵，因此会对用户网络的安全造成严重威胁或危害。在 AP 上开启反制功能可以对非法设备进行攻击使其他无线终端无法关联到非法设备。

反制非法 AP 配置

反制非法AP配置

被反制的非法AP列表

信任设备列表

说明：主动发现网
户接入到非法AP

点击图标。可以打开和关闭反制非法 AP 服务。

的桥接或未经授权的Ad-hoc设备)对这些非法设备进行反制，避免用

反制非法AP：

OFF

通过开关开启或者关闭 AP 的反制非法 AP 功能。

被反制的非法 AP 列表

反制非法AP配置 被反制的非法AP列表 信任设备列表

反制模式： 检测到非同一AC设备的AP设备 每一分钟刷新一次 清空非法AP 基于WiFi名称查询： 搜索

选择反制模式查看反制非法AP对应的wifi列表。

信道 速率(Mbps) 信号强度

无记录信息

显示: 10 条 共0条 首页 上一页 下一页 末页 1 确定

信任设备列表

当 AP 开启反制非法 AP 功能后，非授权的 AP 会被反制，而有些 AP 是信任设备，需进行特殊处理。可以进行配置信任设备的 MAC。

反制非法AP配置 被反制的非法AP列表 信任设备列表

说明：以下配置的MAC地址对应的设备将不会被认为是非法AP,是不会被反制的AP设备,是信任设备

信任设备MAC地址： + 增加MAC地址 点击添加多个信任设备的MAC地址。

信任厂商列表

厂商唯一标识符： + 增加MAC地址 多对多关系 厂商唯一标识符对应的WiFi名称： + 增加WiFi

保存设置 点击添加多个厂商的标识。 点击添加多个WiFi。

1.3.4.2 黑白名单

为了增加无线的安全性，可以控制无线用户的接入，通过将无线指定给某些特定用户使用或不给某些特定的用户使用。

禁止接入 WiFi 上网的用户数默认为 1024 个

允许接入 WiFi 上网的用户数默认为 1024 个

设置 MAC 控制类型，选择黑白名单。

黑白名单配置

说明：这里是设置是否允许无线用户接入WiFi上网；MAC地址是关联到AP设备的客户端（如：您的手机或笔记本电脑）的MAC地址！

名单类型：☐ 禁止以下MAC地址接入WiFi上网（黑名单） ☒ 仅允许以下MAC地址接入WiFi上网（白名单）

+ 添加白名单

✕ 删除选中白名单

📄 批量导入白名单

基于MAC地址查询

搜索

<input type="checkbox"/>	用户名	MAC地址	操作
<input type="checkbox"/>		0002.0002.0007	<div>编辑</div> <div>删除</div>
<input type="checkbox"/>		0002.0002.0008	<div>编辑</div> <div>删除</div>
<input type="checkbox"/>		0002.0002.0009	<div>编辑</div> <div>删除</div>
<input type="checkbox"/>		0002.0002.0010	<div>编辑</div> <div>删除</div>
<input type="checkbox"/>		0002.0002.0011	<div>编辑</div> <div>删除</div>
<input type="checkbox"/>		0002.0002.0014	<div>编辑</div> <div>删除</div>
<input type="checkbox"/>		0002.0002.0015	<div>编辑</div> <div>删除</div>
<input type="checkbox"/>		0002.0002.0078	<div>编辑</div> <div>删除</div>

显示: 10 条 共8条

⏪ 首页 ⏩ 上一页 1 下一页 ⏩ 末页

确定

当前设备的MAC地址：00d0.f822.33aa [\[基于WiFi控制无线用户上网\]](#)

清除所有白名单

点击<添加>图标，增加用户的MAC地址，可添加多个。

点击设置通过 WiFi 上网的用户。点击出现如下页面。

黑白名单配置

Eweb_33AA1

Eweb_33AA2

Eweb_33AA3

Eweb_33AA4

Eweb_33AA5

Eweb_33AA6

▼

说明：这里是设置是否允许无线用户接入WiFi上网；MAC地址是关联到AP设备的客户端（如：您的手机或笔记本电脑）的MAC地址！

名单类型：☒ 禁止以下MAC地址接入WiFi上网（黑名单） ☐ 仅允许以下MAC地址接入WiFi上网（白名单）

+ 添加黑名单

📄 批量导入黑名单

批量导入黑名单

说明：批量导入功能，建议先下载导入模板，然后按照模板填写数据后再导入。

csv [点击下载模板](#) 名单的容量为256

名单文件：

浏览...

导入

显示: 10 条 共0条

⏪ 下一页 ⏩ 末页

1

确定

当前设备的MAC地址：00d0.f822.33aa

批量导入黑名单配置

1.3.4.3 动态黑名单

将恶意攻击源添加到动态黑名单，防止其访问。

13

动态黑名单

说明：设置攻击检测方式

选择开启检测方式。

自动将攻击源添加到动态黑名单；生存时间到期之后，该攻击源会自动从黑名单中删除。

攻击检测方式：☐ 泛洪攻击检测

开启动态黑名单功能。

动态黑名单功能：☐ 开启

生存时间(秒)：300 * 范围(60-1200)

设置生存时间，超过该时间移除黑名单。

刷新列表

删除选中的数据

点击刷新列表

序号	MAC地址	生存时间	操作
无记录信息			

显示 10 条 共0条

首页 上一页 下一页 末页 1 确定

1.3.4.4 禁止内外网互访

为了网络安全及信息之间不被经意传递，可以设置内网用户之间不能通信，对一些特别用户(可以互访的用户)，可经过用户名、MAC 地址进行识别。

禁止内网用户互访

说明：在不影响用户正常上网的情况下对用户进行隔离，使之不能互访，保证了用户业务的安全。

开关，开启或者关闭内网用户互访。

禁止内网用户互访：☒

允许互访的用户MAC：

用户名：

MAC地址：0000.1111.2222 * 添加

点击 <添加> 图标，增加互访用户的 MAC 地址，可添加多个。

当前设备的MAC地址

点击 X 图标，删除某个用户的 MAC 地址。

保存设置

清除设置

1.3.4.5 防攻击/ARP表

在网络环境中经常发现一些恶意的攻击，这些攻击会给交换机带来过重的负担，引起交换机 CPU 利用率过高，导致交换机无法正常运行。

本地防攻击

本地防攻击

防火墙

ARP表项

ARP防攻击：☒ 开启ARP防攻击，防

[【ARP防攻击列表】](#)

点击链接查看被检测到 ARP 攻击的主机。

IP防扫描：☒ 开启IP防扫描，防

[【IP防扫描列表】](#)

点击链接查看被检测到 IP 扫描的主机。

ICMP防攻击：☒ 开启ICMP防攻击，防

[【ICMP防攻击列表】](#)

点击链接查看被检测到 ICMP 攻击的主机。

DHCPv4防攻击：☒ 开启DHCPv4防攻击，防

[【DHCPv4防攻击列表】](#)

点击链接查看被检测到 DHCPv4 攻击的主机。

DHCPv6防攻击：☒ 开启DHCPv6防攻击，防

[【DHCPv6防攻击列表】](#)

点击链接查看被检测到 DHCPv6 攻击的主机。

ND防攻击：☐ 开启ND防攻击配置。

应用带宽，每秒处理报文 不超过15个。

查看防攻击日志：[【本地防攻击日志】](#)

保存设置

恢复默认设置

📌 防火墙

是通过配置 ACL 规则，应用到对应的端口，或者 wifi，来限制特定的用户访问，或者限制用户访问特定的网络等。

本地防攻击

防火墙

ARP表项

+ 添加防火墙

✕ 删除防火墙

<input type="checkbox"/>	ACL号	应用于	过滤方向	操作
<input type="checkbox"/>	12	Gi0/7	收报文(In)	<div><div>编辑</div><div>删除</div></div>

显示

10

条 共1条

◀ 首页

◀ 上一页

1

下一页 ▶

末页 ▶▶

1

确定

● 添加防火墙



- 批量删除防火墙



- 编辑防火墙



- 删除防火墙



ARP 表项



● 动态转为静态绑定



● 解除静态绑定

本地防攻击

防火墙

ARP表项

动态>>静态绑定

解除静态绑定

2. 点击<解除静态绑定>图标批量解除静态绑定，完成操作。

	IP地址	MAC地址	类型	操作
<input type="checkbox"/>	192.168.26.22	14fe.5ba0.f8a7	静态绑定	解除静态绑定
<input type="checkbox"/>			动态绑定	动态>>静态绑定
<input type="checkbox"/>			动态绑定	动态>>静态绑定
<input type="checkbox"/>	172.18.124.23	b8ac.6f40.ad37	动态绑定	动态>>静态绑定

1. 在“ARP 列表”中选择一条或多条记录。

手工绑定

本地防攻击

防火墙

ARP表项

动态>>静态绑定

解除静态绑定

手工绑定

1. 点击<手工绑定>图标。

地址查询：

搜索

	IP地址	MAC地址	类型	操作
<input type="checkbox"/>	192.168.26.22			解除静态绑定
<input type="checkbox"/>	172.18.124.1			动态>>静态绑定
<input type="checkbox"/>	172.18.124.19			
<input type="checkbox"/>	172.18.124.23			动态>>静态绑定
<input type="checkbox"/>	172.18.124.24			动态>>静态绑定
				动态>>静态绑定
				动态>>静态绑定
				动态>>静态绑定

手工绑定ARP

IP地址：

MAC地址：

2. 填入 IP 地址和 MAC 地址。

3. 点击<确定>提示“设置成功”后，会显示在 ARP 列表中。

确定

取消

1.3.4.6 ACL列表

输入 ACL 在设备接口接收到报文时，检查报文是否与该接口输入ACL 的某一条ACE 相匹配；输出ACL 在设备准备从某一个接口输出报文时，检查报文是否与该接口输出ACL 的某一条ACE相匹配。

在制定不同的过滤规则时，多条规则可能同时被应用，也可能只应用其中几条。只要是符合某条ACE，就按照该ACE 定义的处理报文(Permit 或Deny)。

ACL 列表

ACL列表

ACL生效时间

ACL列表：12

添加ACL

删除ACL

+ 添加ACE规则

× 删除选中

	序号	源IP/通配符	源端口	访问控制	协议	目的IP/通配符	目的端口	生效时间	状态	操作
<input type="checkbox"/>	1	22.22.22.22/0.0.0		允许				所有时间	生效	编辑 移动
<input type="checkbox"/>	2	11.11.11.11/0.0.0		允许				所有时间	生效	编辑 移动

显示：10 条 共2条

◀ 首页

◀ 上一页

1

下一页 ▶

末页 ▶

1

确定

添加 ACL



● 删除 ACL



● 添加 ACE 规则



● 编辑 ACE 规则

ACL列表

ACL生效时间

ACL列表: 12

添加ACL

删除ACL

+ 添加ACE规则

✕ 删除选中

<input type="checkbox"/>	序号	源IP/通配符	源端口	访问控制	协议	目的IP/通配符	目的端口	生效时间	状态	操作
<input type="checkbox"/>	1	编辑ACE规则								编辑 移动
<input type="checkbox"/>	2									编辑 移动

显示: 10

ACL类型: 标准ACL (控制源地址)

ACL列表: 12

规则设置

访问控制: ☒ 允许 ☐ 禁止

生效时间: ---请选择生效时间---

☐ 任意IP地址: (IP地址任意是对所有的IP应用该规则)

1

确定

2. 弹窗口页面会显示该 ACE 的信息 对信息进行编辑。

1. 点击 “ACE 规则列表” 某个 ACE 中<编辑>按钮。

3. 点击<确定>提示 “设置成功” 后，完成操作。

确定

取消

● 删除 ACE 规则

ACL列表

ACL生效时间

ACL列表

+ 添加ACE规则

✕ 删除选中

<input type="checkbox"/>	序号	源IP/通配符	源端口	访问控制	协议	目的IP/通配符	目的端口	生效时间	状态	操作
<input type="checkbox"/>	1	22.22.22.22/0		允许	ALL			所有时间	生效	编辑 移动
<input type="checkbox"/>	2			禁止	ALL			所有时间	生效	编辑 移动

显示: 10

条 共2条

1. 在 “ACE 列表” 中选择一条或多条记录。

2. 点击<删除选中>图标，弹出确认窗口，点击<确定>按钮，完成删除操作。

1

确定

➤ ACL 生效时间

您可以使 ACL 基于时间运行，比如让 ACL 在一个星期的某些时间段内生效等。为了达到这个要求，您必须首先配置一个时间对象。

ACL列表

ACL生效时间

+ 添加时间对象

✕ 删除选中时间对象

<input type="checkbox"/>	时间对象	时间周期	时间段	操作
<input type="checkbox"/>	log	星期一 星期二 星期二 星期三 星期四	1:00-23:00 0:00-2:00	编辑 删除
<input type="checkbox"/>	上班	工作日	7:00-17:00	编辑 删除
<input type="checkbox"/>	周末	周末	0:00-23:59	编辑 删除

显示: 10

条 共3条

1

确定

● 添加时间对象

1. 点击<添加时间对象>图标。

2. 在弹窗中填入配置项。

3. 点击“完成配置”提示“设置成功”后，会显示在时间对象列表中。

时间对象	时间周期	时间段	操作
log	星期一 星期二 星期二 星期三 星期四	1:00-23:00 0:00-2:00	编辑 删除

● 批量删除时间对象

1. 在列表中选择要删除的时间对象。

2. 点击<删除选中时间对象>图标，弹出确认窗口，点击<确定>按钮，完成删除操作。

时间对象	时间周期	时间段	操作
log	星期二 星期三 星期四	0:00-2:00	编辑 删除
		7:00-17:00	编辑 删除
		0:00-23:59	编辑 删除

● 编辑时间对象

ACL列表 ACL生效时间

+ 添加时间对象 X 删除选中时间对象

时间对象	时间周期	时间段	操作
log	星期一-星期二 星期二-星期三-星期四	1:00-23:00 0:00-2:00	编辑 删除

显示 10 条

1. 点击列表中某个时间对象中<编辑>按钮。

2. 弹窗口页面会显示该时间对象的信息,对信息进行编辑。

3. 点击“完成配置”提示“设置成功”后,完成操作。

编辑时间对象

对象名: log

时间段: 星期一,星期二 1:00 ~ 23:00

+ 添加

完成配置 取消

- 删除时间对象

动态黑名单

说明: 设置攻击检测方式及开启动态黑名单功能后,当设备检测到攻击,会自动将攻击源添加到动态黑名单;生存时间到期之后,该攻击源会自动从黑名单中删除。

攻击检测方式: ☐ 泛洪攻击检测 ☐ 欺骗攻击检测 ☐ 弱初始化向量检测

动态黑名单功能: ☐ 开启

生存时间(秒): 300 * 范围(60-1200)

保存设置

刷新列表 X 删除选中的数据

序号	操作
无记录信息	

显示

1. 在列表中选择要删除的黑名单

2. 点击<删除选中数据>图标,弹出确认窗口,点击<确定>按钮,完成删除操作。

1 确定

1.3.5 高级

1.3.5.1 VLAN管理

VLAN管理

+ 添加VLAN

✕ 删除选中VLAN

<input type="checkbox"/>	VLAN ID	IPv4 IP	IPv4 掩码	IPv6地址/掩码	操作
<input type="checkbox"/>	1	172.18.124.76	255.255.255.0		<div>编辑</div>
<input type="checkbox"/>	2	3.3.3.3	255.255.255.0		<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	3	4.4.4.4	255.255.255.0		<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	4	5.5.5.5	255.255.255.0		<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	5				<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	11				<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	23				<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	32				<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	33				<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	34				<div>编辑</div> <div>删除</div>

显示: 10 条 共13条

◀ 首页

◀ 上一页

1 2

下一页 ▶

末页 ▶

1 确定

- 添加 VLAN

The screenshot displays the 'VLAN管理' (VLAN Management) interface. At the top, there are buttons for '+ 添加VLAN' (Add VLAN) and 'X 删除选中VLAN' (Delete Selected VLAN). Below this is a table with columns for selection, IPv4 address, IPv6 address, and actions (编辑, 删除). A modal window titled '添加VLAN' (Add VLAN) is open, showing fields for 'VLAN ID' (with a range of 1-4094) and 'IP 地址' (IP Address). Below these fields is a section for '高级设置' (Advanced Settings). At the bottom of the modal are '完成配置' (Finish Configuration) and '取消' (Cancel) buttons. Three blue callout boxes with white text provide instructions: 1. Click the '+ 添加 VLAN' button. 2. Fill in the configuration items in the modal. 3. Click '完成配置' to see the '设置成功' (Setup Successful) message and the 'VLAN 列表' (VLAN List).

1. 点击<添加 VLAN>按钮。

2. 在弹窗中填入配置项。

3. 点击<完成配置>提示“设置成功”后，会显示在“VLAN 列表”中。

- 批量删除 VLAN

VLAN管理

+ 添加VLAN X 删除选中VLAN

2. 点击<删除选中 VLAN>图标，弹出确认窗口，点击<确定>按钮，完成删除操作。

	VLAN ID	IPv4 IP	IPv4 掩码	操作
<input type="checkbox"/>	1	172.18.124.76	255.255.255.0	编辑
<input type="checkbox"/>	2	3.3.3.3	255.255.255.0	编辑 删除
<input type="checkbox"/>	3	4.4.4.4	255.255.255.0	编辑 删除
<input type="checkbox"/>	4	5.5.5.5	255.255.255.0	编辑 删除

1. 在列表中选择要删除的 VLAN 。

● 编辑 VLAN

VLAN管理

+ 添加VLAN X 删除选中VLAN

1. 点击列表中某个 VLAN 中<编辑>按钮。

2. 弹窗口页面会显示该 VLAN 的信息，对信息进行编辑。

3. 点击<完成配置>提示“设置成功”后，完成操作。

	VLAN ID	IPv4 IP	操作
<input type="checkbox"/>	1	172.18.124.76	编辑 删除
<input type="checkbox"/>			编辑 删除
<input type="checkbox"/>			编辑 删除
<input type="checkbox"/>			编辑 删除
<input type="checkbox"/>			编辑 删除
<input type="checkbox"/>			编辑 删除
<input type="checkbox"/>			编辑 删除
<input type="checkbox"/>			编辑 删除
<input type="checkbox"/>			编辑 删除
<input type="checkbox"/>			编辑 删除

编辑VLAN

VLAN ID: 2 * 范围1-4094

IP 地址: 3.3.3.3

>> 高级设置

完成配置 取消

显示: 10 条 共13条

首页 < 上一页 1 2 下一页 > 末页 1 确定

● 删除 VLAN

VLAN管理

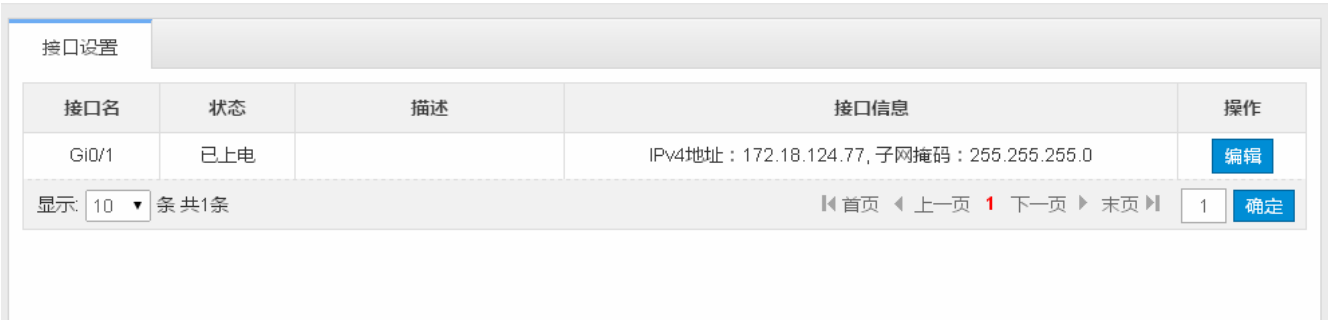
+ 添加VLAN X 删除选中VLAN

点击列表中某个 VLAN 中<删除>按钮，弹出确认窗口，点击<确定>按钮，完成删除操作。

	VLAN ID	IPv4 IP	IPv4 掩码	操作
<input type="checkbox"/>	1	172.18.124.76	255.255.255.0	
<input type="checkbox"/>	2	3.3.3.3	255.255.255.0	编辑 删除
<input type="checkbox"/>	3	4.4.4.4	255.255.255.0	编辑 删除
<input type="checkbox"/>	4	5.5.5.5	255.255.255.0	编辑 删除

1.3.5.2 接口设置

➤ 接口设置



- 编辑接口设置



1.3.5.3 路由管理



- 添加静态路由



- 添加默认路由



备注：路由选路分为主路由和备份路由，当主路由不能生效，比如主路由的接口没有活动时，就会走备份路由，备份路由也是按照配置的级别优先级来走。备份路由1的优先级比备份路由2的优先级来的高。

- 批量删除路由

路由管理

+ 添加静态路由 + 添加默认路由 × 删除选中路由

	目的网段	目的网段掩码	下一跳地址	出口	路由类型	操作
<input type="checkbox"/>	0.0.0.0	0.0.0.0	172.18.124.1		主路由	编辑 删除
<input type="checkbox"/>	0.0.0.0	0.0.0.0	3.6.6.6	VLAN 2	备份路由-2	编辑 删除
<input type="checkbox"/>	0.0.0.0	0.0.0.0	3.6.6.6	VLAN 2	备份路由-2	编辑 删除

显示: 10 条 共3条

首页 < 上一页 1 下一页 > 末页 1 确定

1. 在列表中选择要删除的路由。

2. 点击<删除选中路由>图标，弹出确认窗口，点击<确定>按钮，完成删除操作。

● 编辑路由

路由管理

+ 添加静态路由 + 添加默认路由 × 删除选中路由

编辑默认路由

1. 点击列表中某个路由中<编辑>按钮。

2. 弹窗口页面会显示该路由的信息，对信息进行编辑。

IP类型: ☒ IPv4 ☐ IPv6

路由出口: VLAN 2

下一跳地址: 3.6.6.6

路由选路: 备份路由-2

3. 点击<完成配置>提示“设置成功”后，完成操作。

完成配置 取消

● 删除路由

路由管理

+ 添加静态路由 + 添加默认路由 × 删除选中路由

	目的网段	目的网段掩码	下一跳地址	出口	路由类型	操作
<input type="checkbox"/>	0.0.0.0	0.0.0.0	172.18.124.1		主路由	编辑 删除
<input type="checkbox"/>	0.0.0.0	0.0.0.0	3.6.6.6	VLAN 2	备份路由-2	编辑 删除
<input type="checkbox"/>	0.0.0.0	0.0.0.0	6.3.3.3		备份路由-2	编辑 删除

显示: 10 条 共3条

首页 < 上一页 1 下一页 > 末页 1 确定

点击列表中某个路由中<删除>按钮，弹出确认窗口，点击<确定>按钮，完成删除操作。

1.3.5.4 DHCP配置

➤ DHCP 配置

DHCP配置

静态地址分配

客户端列表

+ 添加DHCP

✕ 删除选中DHCP

⊖ 不分配的IP段

DHCP服务开关：

ON

<input type="checkbox"/>	名称	地址范围	默认网关	租用时间	DNS	操作
<input type="checkbox"/>	33333	192.68.2.1-192.68.2.254	192.68.2.1	8小时		<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	1233455	152.3.6.1-152.3.6.254	152.3.6.1	8小时		<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	wzhy	2.2.2.1-2.2.2.254	2.2.2.1	8小时		<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	ttt	192.168.11.1-192.168.11.254	192.168.11.1	8小时		<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	www	192.168.8.1-192.168.8.254	192.168.8.1	8小时	192.168.58.110	<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	6	5.5.5.1-5.5.5.254	5.5.5.5	8小时		<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	2323	4.4.4.1-4.4.4.254	4.4.4.4	8小时		<div>编辑</div> <div>删除</div>
<input type="checkbox"/>	23	3.3.3.1-3.3.3.254	3.3.3.3	8小时		<div>编辑</div> <div>删除</div>

显示：

10

条 共8条

⏪ 首页

⏩ 上一页

1

下一页

末页

1

确定

● 添加 DHCP

DHCP配置

静态地址分配

客户端列表

+ 添加DHCP

✕ 添加DHCP

1. 点击<添加 DHCP>按钮。

2. 在弹窗中填入配置项。

3. 点击<完成配置>提示“设置成功”后，会显示在“DHCP 列表”中。

配置类型：

☒ IPv4

☐ IPv6

IP分配范围：1 至 254

默认网关：

租用时间：

8

小时

完成配置

取消

点击我，试试高级配置

● 批量删除 DHCP

DHCP配置 静态地址分配 客户端列表

+添加DHCP X删除选中DHCP

2. 点击<删除选中 DHCP>图标，弹出确认窗口，点击<确定>按钮，完成删除操作。

	名称	地址范围	租约时间	DNS	操作
<input type="checkbox"/>	33333	192.68.2.1-192.68.2.254	8小时		编辑 删除
<input type="checkbox"/>	1233455	152.3.6.1-152.3.6.254	8小时		编辑 删除
<input type="checkbox"/>	wzhvy	2.2.2.1-2.2.2.254	8小时		编辑 删除
<input type="checkbox"/>		11.1	8小时		编辑 删除

1. 在列表中选择要删除的 DHCP。

- 配置不分配的 IP 段

DHCP配置 静态地址分配 客户端列表

+添加DHCP X删除选中DHCP 不分配的IP段 DHCP服务开关: ON

1. 点击<不分配的 IP 段>按钮。

2. 在弹窗中填入配置项。

三 不分配的IP段

不分配的IP段：设置的IP地址将不会分配给客户。格式如：1.1.1.1-1.1.1.30,只填1.1.1.1代表单个IP。

不分配的IP段1: - +

3. 点击<完成配置>提示“设置成功”后，会显示在“DHCP列表”中。

完成配置 取消

DHCP配置 静态地址分配 客户端列表

+添加DHCP X删除选中DHCP 不分配的IP段 DHCP服务开关: ON

不分配的 IP 段。可以配置若干个 IP 段，IP 段内的 IP 将不会分配给用户。

三 不分配的IP段

不分配的IP段：设置的IP地址将不会分配给客户。格式如：1.1.1.1-1.1.1.30,只填1.1.1.1代表单个IP。

不分配的IP段1: - +

完成配置 取消

显示: 10 条 共8条

首页 上一页 1 下一页 末页 1 确定

- DHCP 服务开关



- 编辑 DHCP



- 删除 DHCP

DHCP配置 静态地址分配 客户端列表

+ 添加DHCP X 删除选中DHCP 不分配的IP段 DHCP服务开关: ☒ ON

<input type="checkbox"/>	名称	地址范围	默认网关	租用时间		
<input type="checkbox"/>	33333	192.68.2.1-192.68.2.254	192.68.2.1	8小时		
<input type="checkbox"/>	1233455	152.3.6.1-152.3.6.254	152.3.6.1	8小时	编辑	删除
<input type="checkbox"/>	wzhy	2.2.2.1-2.2.2.254	2.2.2.1	8小时	编辑	删除
<input type="checkbox"/>	ttt	192.168.11.1-192.168.11.254	192.168.11.1	8小时	编辑	删除

点击列表中某个 DHCP 中<删除>按钮，弹出确认窗口，点击<确定>按钮，完成删除操作。

静态地址分配

DHCP配置 静态地址分配 客户端列表

+ 添加静态地址 X 删除选中地址

<input type="checkbox"/>	客户名称	客户端IP	掩码	网关	客户端MAC	DNS服务器	操作
<input type="checkbox"/>	客户1	192.168.23.11	255.255.255.0		0002.0002.0020		编辑 删除
<input type="checkbox"/>	客户2	192.168.23.12	255.255.255.0		0002.0002.0021		编辑 删除

显示: 10 条 共2条

首页 上一页 1 下一页 末页 1 确定

添加静态地址

DHCP配置 静态地址分配 客户端列表

+ 添加静态地址 X 删除选中地址

1. 点击<添加静态地址>按钮。

2. 在弹窗中填入配置项。

3. 点击<完成配置>提示“设置成功”后，会显示在“静态地址列表”中。

客户名称: *

客户端IP: *

子网掩码:

客户MAC地址: *

网关:

DNS:

完成配置 取消

批量删除静态地址



● 编辑静态地址



● 删除静态地址



➤ 客户端列表

DHCP配置 静态地址分配 客户端列表

✦ 把MAC地址绑定到动态获取的IP上 基于IP地址查询： 搜索

<input type="checkbox"/>	已分配的IP地址	MAC地址	地址租期	IP分配方式
无记录信息				

显示: 20 条 共0条

首页 上一页 下一页 末页 1 确定

- 绑定 MAC 地址到动态获取的 IP 上

DHCP配置 静态地址分配 客户端列表

✦ 把MAC地址绑定到动态获取的IP上 2. 点击<把 MAC 地址绑定到动态获取的 IP 上>图标，弹出确认窗口，点击<确定>按钮，完成操作。

<input type="checkbox"/>	已分配的IP地址	MAC地址	地址租期	IP分配方式
无记录信息				

1. 在列表中选择要删除的静态地址。

显示: 20 条 共0条

首页 上一页 下一页 末页 1 确定

- 基于 IP 地址查询客户端

DHCP配置 静态地址分配 客户端列表

✦ 把MAC地址绑定到动态获取的IP上 在输入框内输入要查询的 IP 地址。点击<搜索>按钮，列表中显示符合条件的搜索结果。

基于IP地址查询： 搜索

<input type="checkbox"/>	已分配的IP地址	MAC地址	地址租期	IP分配方式
无记录信息				

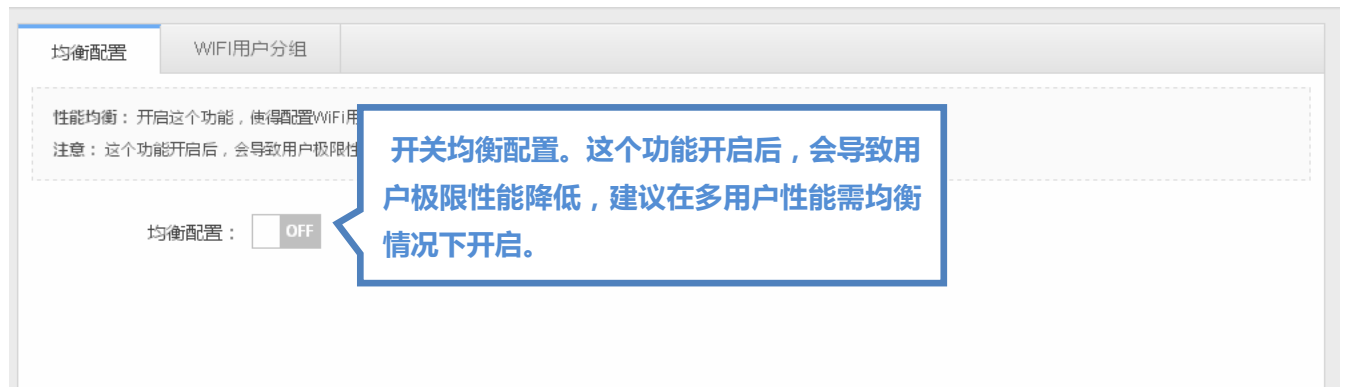
显示: 20 条 共0条

首页 上一页 下一页 末页 1 确定

1.3.5.5 电子书包配置

均衡配置

注意，您所使用的 AP 可能不支持该功能，请以实际的菜单项为准。



WIFI 用户分组



1.3.5.6 单播/组播

单播/组播

简单组播：一般用于教室内的广播教学，教师机（组播）和学生机在一个广播域内，组播（广播报文）直接在广播域内推送即可,组播报文不需要跨设备跨网段。

标准组播：一般场景是一个高校，有自己的组播视频服务器，然后通过标准组播方式向全校推送广播报文。

组播：

☐ 简单组播

☒ 标准组播

☐ 关闭组播

动态老化时间：

500

时间到了，组播表项如果没被更新，就老化删除了

忽略查询报文定时器：

☐ 开启

配置忽略查询报文重置端口老化定时器

定时间隔时间：

(范围：1-18000秒)

响应查询报文时间：

(范围：1-65535秒)

代理三层设备：

☐ 代理的IP地址

代理三层设备。勾选后需要配置三层设备的 IP 地址。

基于VLAN-ID开组播：

☐ 全部开启

选择需要开组播的 VLAN，可以选择全部开启。

☐ Vid=1 ☐ Vid=2

组播转单播：

☐ OFF

保存设置

1.3.5.7 端口映射

一般应用在将内网指定主机的指定端口映射到外网地址的指定端口上。**注意，您所使用的 AP 可能不支持该功能，请以实际的菜单项为准。**

端口映射

说明：一般应用在将内网指定主机的指定端口映射到外网地址的指定端口上。

+ 添加端口映射

✕ 删除选中的端口映射

<input type="checkbox"/>	映射关系	内网IP	内网端口	外网IP	外网端口	协议类型	接口	操作
<input type="checkbox"/>	端口映射	192.168.23.2	3333	192.168.112.2	6666	TCP	-	<div>编辑</div> <div>删除</div>

显示:

10

 条 共1条

⏪ 首页

⏩ 上一页

1

下一页

⏩ 末页

1

确定

- 添加端口映射

端口映射

说明：一般应用在将内网指定主机的指定端口映射到外网地址的指定端口上。

1. 点击<添加端口映射>图标。

2. 在弹窗中填入配置项。

显示: 10 条

内网IP: *

内网端口: * (1-65535)

外网IP: ☒ 输入地址: *

☐ 使用接口地址: Fa0/2 ▾

外网端口: * (1-65535)

协议类型: TCP ▾

3. 点击<完成配置>提示“设置成功”后，会显示在“端口映射列表”中。

完成配置 取消

操作: 编辑 删除

1 确定

- 批量删除端口映射

端口映射

说明：一般应用在将内网指定主机的指定端口映射到外网地址的指定端口上。

1. 在列表中选择要删除的 VLAN。

2. 点击<删除选中端口映射>图标，弹出确认窗口，点击<确定>按钮，完成删除操作。

映射关系	内网IP	内网端口	外网IP	外网端口	协议类型	操作
<input type="checkbox"/>	192.168.88.8	8888	192.168.148.8	6666	TCP	编辑 删除

显示: 10 条

1 确定

- 编辑端口映射



● 删除端口映射



1.3.6 系统

1.3.6.1 系统设置

▾ 系统时间

通过设备所在区设置系统时间，使得设备信息准确明了。

系统时间	修改密码	系统重启	恢复出厂设置	增强功能	SNMP	DNS
------	------	------	--------	------	------	-----

当前时间：2014年12月25日07:35:41

重新设置时间：2014-12-25 07:46

时区：UTC+4(毛里求斯时间)

时间同步：☐ 自动与Internet时间服务器同步(请保证配置了正确的DNS服务器)

保存设置

当需要配置时间和网络时间自动同步时，需要先设置 DNS 服务器。

修改密码

为了提高系统安全性，让信息交互更加安全，请您修改系统默认密码。

系统时间	修改密码	系统重启	恢复出厂设置	增强功能	SNMP	DNS
------	------	------	--------	------	------	-----

Web网管密码修改

用户名：admin

原密码：

新密码：

确认密码：

保存设置

输入原密码。

输入新密码。

重新输入新密码。

Telnet认证密码修改(当开启了web认证后必配,修改的是admin用户的密码)

用户名：admin

新密码：

确认密码：

保存设置

输入新密码。

重新输入新密码。

恢复出厂配置

清空配置信息，还原至最初状态。通过导入导出配置，对配置批量操作，更加方便用户操作。

系统时间 修改密码 系统重启 恢复出厂设置 增强功能 SNMP DNS

三 导入/导出配置

说明：导入过程中不能关闭或刷新浏览器。对于导入的配置：导入配置后，要启用新的配置，请在本页面重启设备否则配置不生效。

文件名： 未选择任何文件

导入的配置文件。

下载最新的配置文件。

三 恢复出厂设置

说明：恢复出厂设置，将删除当前所有配置。如果当前系统存在有用的配置，可先 [导出当前配置](#)。

清空配置信息，还原至初始状态。

[查看当前配置](#)

点击图标。在下面框中查看配置信息。

增强功能

为了便于管理设备，配置设备位置更好的盘查设备。设置超时时间，当离开长时间后 web 自动退出，保障您的系统安全。

系统时间 修改密码 系统重启 恢复出厂设置 增强功能 SNMP DNS

三 基本信息

WEB访问端口： (默认 8025-65535)

登录超时：

设备位置：

设置访问端口。WEB 浏览器访问时需要加上

设置安全超时时间。

设备位置，便于管理。

SNMP

SNMP 简单网络管理协议,它们提供了一种从网络上的设备中收集网络管理信息的方法.可以管理很多网络设备。

系统时间	修改密码	系统重启	恢复出厂设置	增强功能	SNMP	DNS
------	------	------	--------	------	------	-----

SNMP版本：☒ v2版本 ☐ v3版本

设备位置：

SNMP口令： *

Trap口令： Trap口令和SNMP口令一致

Trap接收主机： * 最多可配置9个Trap接收主机，IP之间请用“,”或者“回车换行符”隔开。

选择 SNMP 版本，配置字段不同。

➤ DNS

配置了 DNS 服务器，才能进行动态域名解析。

系统时间	修改密码	系统重启	恢复出厂设置	增强功能	SNMP	DNS
------	------	------	--------	------	------	-----

DNS服务器1： ×

DNS服务器2： +

点击 × 图标，删除 DNS 服务器。

点击 + 图标，添加 DNS 服务器。

1.3.6.2 系统升级

➤ 本地升级

将软件包主程序或者 web 包下载到本地，通过本地升级。

本地升级	WEB包在线升级
------	----------

说明：您可以到锐捷网络官方网站上下载对应型号的软件版本到本地，然后通过下面的方式升级到设备中。

提示：1、升级软件主程序时，可能会遇到整理flash从而导致页面暂时没响应，此时不能断电或者重启设备，直到提示升级成功。

文件： 未选择文件

点击选择需要升级的主程序或者 web 包。

点击<取消升级>按钮，升级过程中可以中断。

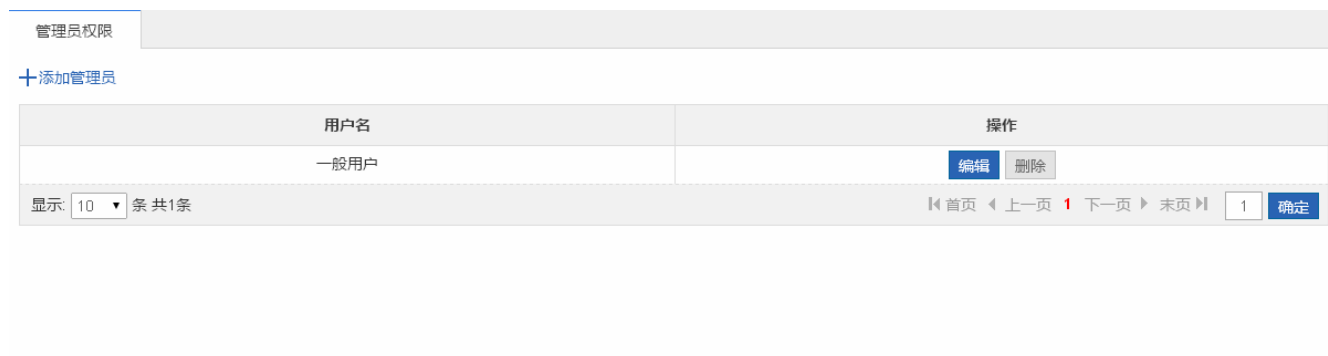
➤ WEB 包在线升级

无需下载 web 包，当配置设备可以上网后，可以通过在线进行升级 web 包。



1.3.6.3 管理员权限

一个系统中用户可以有多个，级别不同权限也不同，可以通过设置管理员权限查看页面。系统默认的用户有 admin



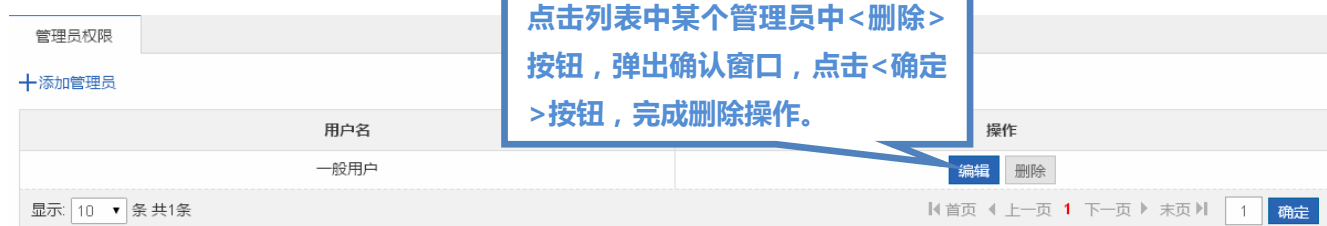
- 添加管理员



- 编辑管理员



● 删除管理员



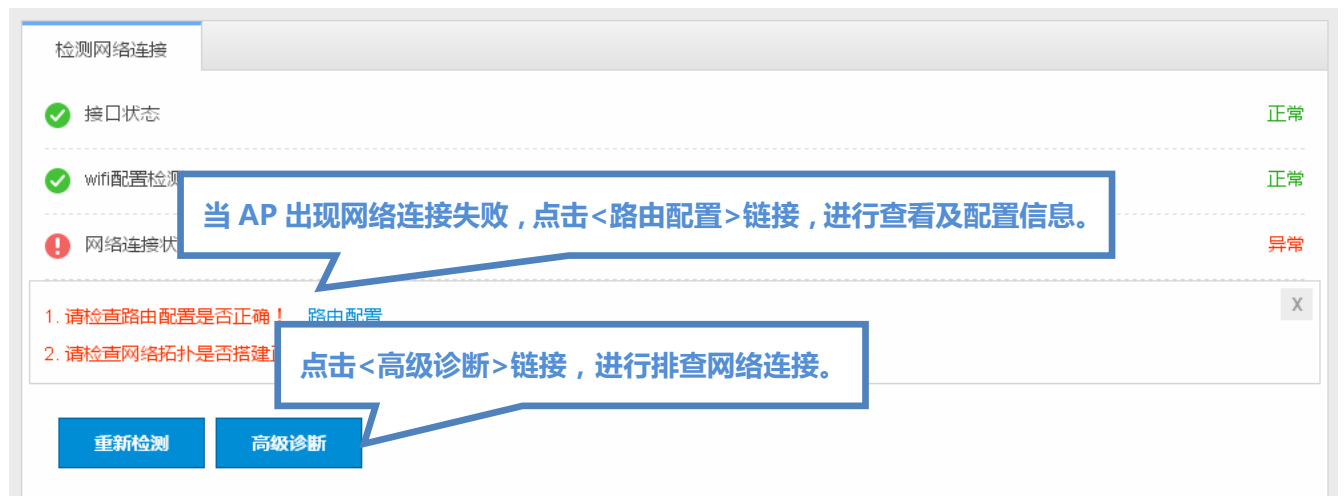
1.3.6.4 上传日志

设备本地的日志发送到对应的服务器上保存，保存历史查看方便查阅。



1.3.6.5 检测网络连接

当网络出现故障时，通过检测网络连接，有助于排查故障。



1.3.6.6 Web控制台



该控制台功能类似 telnet 功能，可以直接在上面做任何命令的配置。但是不支持 shell 模式下命令和 telnet 到 ap 的设备的功能。

1.3.6.7 胖瘦模式切换

根据 AP 的模式进行选择设置。



1.4 AP 手机适配

1.对于 AP 的 web 界面，我们提供了部分功能有手机适配，就是在手机上，能够正常的显示界面，手机适配只支持中文版本，且只支持 admin 管理员。手机适配支持功能有“首页”，“上网配置”，“信道配置”，“网络检测”，“DNS”，“版本信息”，“密码修改”，“重启”，“切为电脑版”，“退出”

1.4.1.1 首页

“首页”可以让您一目了然查看 AP 设备的基本信息，如、设备型号等，AP 设备总流量趋势，可以了解 AP 的用户数。



1.4.1.2 上网配置

点击菜单的“上网配置”或者首页的“上网配置”可以进入界面。

< EWEB-AP ≡

AP工作模式：

☐ AP只做接入模式

☒ 无线路由模式

联网类型：

使用静态IP(独立IP) ▾

IP地址：

172.18.124.91 *

子网掩码：

255.255.255.0 *

默认网关：

172.18.124.1

开启NAT功能：

☒ 勾选开启NAT功能

下一步

1.4.1.3 信道配置

无线信道设置主要是调整设备发出无线 WiFi 的信号强度，可以设置 2G 和 5G 网络的信道等参数。 点击菜单的“信道配置”或者首页的“信道配置”可以进入界面

<

EWEB-AP

≡

开启2.4G网络：

ON

[【强制将2.4G转成5G】](#)

当前所在的国家：

中国(CN)

▼

无线信道：

1

▼

当前无线信道：

1

无线频率带宽：

20MHZ

▼

信号强度：

自定义

▼

信号强度值：

4

无线最大用户数：

32

可连接的最大无线用户数(范围1-128)

开启5G网络：

ON

[【强制将5G转成2.4G】](#)

1.4.1.4 网络检测

点击菜单 “网络检测” 可以检测当前设备的网络情况，当网络出现故障时，通过检测网络连接，有助于排查故障。

<

EWEB-AP

≡

✔ 接口状态

正常

✔ wifi配置检测

正常

✔ 网络连接状态

正常

重新检测

1.4.1.5 DNS

点击 菜单 “DNS” 功能，配置 dns，配置了 DNS 服务器，才能进行动态域名解析。



1.4.1.6 胖瘦AP切换

点击菜单的“胖瘦 AP 切换”功能，可以弹出此页，选择 AP 的工作模式



1.4.1.7 版本信息

点击菜单的“版本信息”功能，可以弹出此页，可以显示当前设备的相关信息



1.4.1.8 密码修改

为了提高系统安全性，让信息交互更加安全，请您修改系统默认密码。点击菜单的“密码修改菜单”



The screenshot shows a mobile application interface for 'EWEB-AP'. At the top is a blue header bar with a back arrow on the left, the text 'EWEB-AP' in the center, and a hamburger menu icon on the right. Below the header, the title 'Web网管密码修改' (Web Network Management Password Modification) is displayed. The main content area contains the following elements: a label '用户名: admin' (Username: admin); three password input fields labeled '原密码:' (Original Password), '新密码:' (New Password), and '确认密码:' (Confirm Password), each with a red asterisk icon to its right; and a blue button labeled '保存设置' (Save Settings) at the bottom.

1.4.1.9 重启

一键重启，方便快捷。



恢复出厂

清空配置信息，还原至最初状态。通过导出配置，对配置批量操作，更加方便用户操作。



1.4.1.10 切换到电脑版

手机适配功能有限，用户可以切到电脑版，提供完整的功能。



<

EWEB-AP

≡

WiFi名称：

Eweb_AAAA1

*

WiFi密码：

☐ 显示密码

开启DHCP服务：

☒ DHCP服务器配置在本AP上(AP来分配地址)

Vlan ID：

1

IP分配范围：

192.168.1

1

至

254

DHCP网关：

192.168.1.1

DNS服务器：

114.114.114.114

上一步

完成设置

1.5 开启web服务器

AP 出厂情况下是开启 WEB 服务,，默认 IP: 192.168.110.1。下面介绍在 WEB 服务关闭的情况下，如何在 CLI 下打开。

配置项	相关命令	
配置 web 服务器	enable service web-server	开启 web 服务
	ip address	可选配置 IP 地址
	webmaster level username password	可选配置，登录 WEB 管理的账号密码信息

配置方法

▾ 开启 WEB 服务

- 必须配置。
- 在 AP 上配置。

▾ 配置 IP 地址

- 可选配置。

▾ 配置登录 WEB 管理的账号密码信息

- 可选配置。

- 开启 WEB 服务时，缺省创建管理员账号 admin/admin 与访客账号 guest/guest，这两个账号密码可以修改，同时用户也可以再创建其他的 WEB 管理账号。

检验方法

通过设置的 IP 地址和 web 管理的账号密码登陆 web 界面，查看是否可以正常登陆。

相关命令

启动 WEB 服务

- 【命令格式】 **enable service web-server [http | https | all]**
- 【参数说明】 **http | https | all**：打开相应的服务。**http** 为打开 HTTP 服务，**https** 为打开 HTTPS 服务，**all** 为同时打开 HTTP 和 HTTPS 服务。缺省为同时打开 HTTP 和 HTTPS 服务。
- 【命令模式】 全局模式

配置 IP 地址

- 【命令格式】 **ip address ip-address ip-mask**
- 【参数说明】 *ip-address*：ip 地址
ip-mask：网络掩码
- 【命令模式】 接口模式

配置登录 WEB 管理的账号密码信息

- 【命令格式】 **webmaster level privilege-level username name password { password | [0 | 7] encrypted-passw**
- 【参数说明】 *privilege-level*：用户绑定权限等级，分为 0/1/2 三个等级。缺省创建的超级管理员账号 admin 对应 0 级权限，访客账号 guest 对应 2 级，其他手动创建的账号对应 1 级。
name：静态 RP 的地址。
password：使用 ACL 限定该静态 RP 服务的组地址范围。缺省为所有组服务。
0 | 7：口令的加密类型，0 无加密，7 简单加密。缺省为 0。
encrypted-password：口令文本。
- 【命令模式】 全局模式
- 【使用指导】 -

配置举例

配置 WEB 服务器

- 【配置方法】
- 打开 web 服务。
 - 配置设备管理 IP，默认管理 VLAN 是 VLAN 1，配置 VLAN 1 的 IP，需要保证用户 PC 能够 ping 通管理 IP。

```
Ruijie# configure terminal
Ruijie(config)# enable service web-server
Ruijie(config)# webmaster level 0 username test password test
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# ip address 192.168.1.200 255.255.255.0
Ruijie(config)# end
```

【检验方法】 通过 **show running-config** 查看相关命令。

```
Ruijie(config)#show running-config
Building configuration...
Current configuration : 6312 bytes

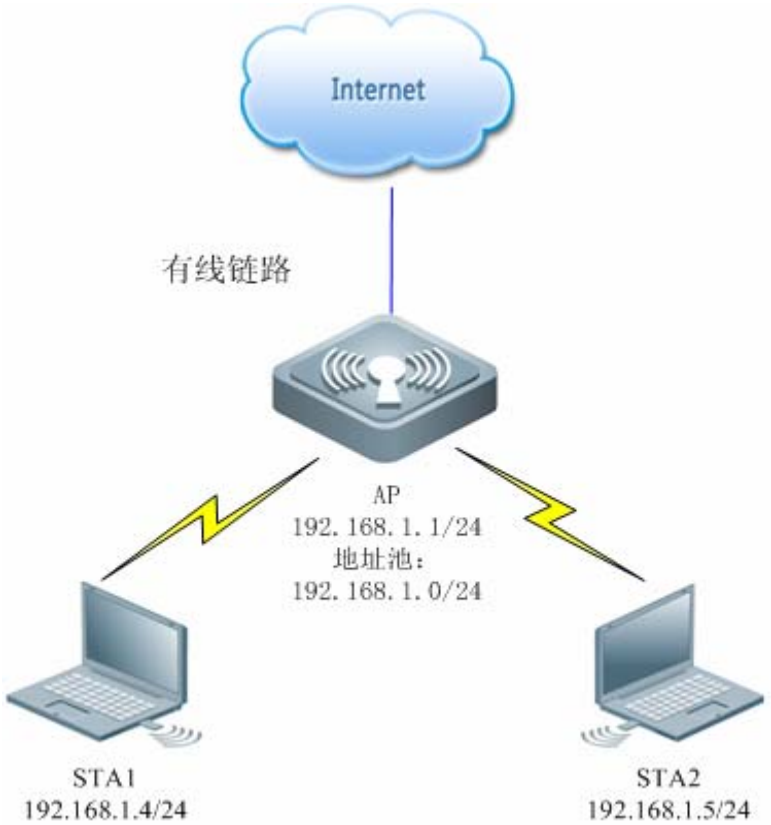
!
hostname ruijie
!
!
webmaster level 0 username test password test      //WEB 管理认证用户名与密码
http update mode auto-detect
!
!
interface VLAN 1
 ip address 192.168.1.200 255.255.255.0           //设备管理 IP
 no shutdown
!
line con 0
line vty 0 4
 login
!
!
End
```

1.6 WEB管理配置举例

1.6.1 搭建DHCP服务器在AP设备上的WLAN

ap 当做无线路由，作为胖 ap，搭建一个小型的网络，dhcp 服务器配置在 ap 设备上，拓扑如下图

图 1-1 拓扑图 1 ap 为路由模式



配置项	配置建议 & 相关命令	
搭建一个 dhcp 服务器在 ap 上的无线网络	<div><div></div>必须配置，用于搭建无线网络必要信息</div>	
	配置 wifi 名称	用户上网关联的无线信号
	配置 wifi 密码	用户上网关联无线信息输入密码，防止不必要蹭网
	配置 dhcp 信息	分配 ip 给无线用户

配置方法

1) 选择 AP 角色并设置联网方式

快速配置—外网设置

AP工作模式：☐ AP只做接入模式 ☒ 无线路由模式

联网类型：

使用静态IP(独立IP)

IP地址：

172.18.124.91

*

子网掩码：

255.255.255.0

*

默认网关：选填

开启NAT功能：☐ 勾选开启NAT功能

上一步

完成配置

ap 作为无线路由模式。

- 无线路由模式可以选择联网类型
- 使用静态 IP(独立 IP)类型

快速配置—外网设置

AP工作模式：☐ AP只做接入模式 ☒ 无线路由模式

联网类型：

IP地址： *

子网掩码： *

默认网关： 选填

开启NAT功能：☐ 勾选开启NAT功能

●

- 使用 PPPoE(ADSL 线路)

快速配置—外网设置

AP工作模式：☐ AP只做接入模式 ☒ 无线路由模式

联网类型：

上网账号： *

上网口令： *

PPPOE IP: 未获取

开启NAT功能：☒ 勾选开启NAT功能

●

- 使用 DHCP(动态 IP)

快速配置—外网设置

AP工作模式：☐ AP只做接入模式 ☒ 无线路由模式

联网类型：

默认网关： 选填

DHCP IP: 未获取

开启NAT功能：☐ 勾选开启NAT功能

2) 配置 wifi 名称 (可以填写简单易记得 wifi,如 zhangsan) wifi 名称最长不超过 32 字节。

图 1-2 ap 快速配置-ssid

快速配置—WiFi配置

WiFi名称：

WiFi密码： ☐ 显示密码

开启DHCP服务: ☒ DHCP服务器配置在本AP上(AP来分配地址)

Vlan ID：

IP分配范围： 至

DHCP网关：

DNS服务器： 选填

3) 安全配置

- 默认选择 wpa2 psk 加密方式，密码输入为 8-64 个字符，可使用英文、数字及部分特殊字符的组合。

图 1-3 ap 快速配置-安全配置

快速配置—WiFi配置

WiFi名称：

WiFi密码：

☐ 显示密码

开启DHCP服务：☒ DHCP服务器配置在本AP上(AP来分配地址)

Vlan ID：

IP分配范围： 至

DHCP网关：

DNS服务器： 选填

上一步

完成配置

4) dhcp 配置

图 1-4 ap 快速配置-dhcp 配置

快速配置—WiFi配置

WiFi名称： *

WiFi密码： ☐ 显示密码

开启DHCP服务: ☒ DHCP服务器配置在本AP上(AP来分配地址)

Vlan ID：

IP分配范围： 至

DHCP网关：

DNS服务器： 选填


上一步

完成配置

- 开启地址池：192.168.1.0/24
- DNS 服务器：192.168.58.110（根据实际情况而配）
- 点击完成配置

检验方法

- 用户关联 wifi 名称 Eweb_AAAA1 获得地址 ip 192.168.1.4
- 用户可以连上 wifi,然后通过 192.168.1.1 访问 web.

 注意：如果修改管理 IP,则用新的管理 IP 重新登录访问 Web

-