AX3000 Wi-Fi6 强覆盖型吸顶式 AP i29

Web 配置指南

资料版本：V1.0

声明

前言

感谢选择腾达产品。开始使用本产品前，请先认真阅读本指南并妥善保存以备日后参考。

约定

本指南适用于腾达（Tenda）AX3000 Wi-Fi6 强覆盖型吸顶式 AP i29 产品。

本指南中，所提到的“AP”、“产品”等名词，如无特别说明，均指腾达（Tenda）AX3000 Wi-Fi6 强覆盖型吸顶式 AP i29。

本文可能用到的格式说明如下。

项目	格式	举例
菜单项	「」	选择「状态」菜单。
按钮	边框+底纹	点击 确定 。
连续菜单选择	>	进入「网络设置」>「LAN 口设置」页面。
窗口	【】	设置【SSID 流控策略】里面的参数。

本文档用到的标识说明如下。

标识	含义
注意	表示重要信息或需要特别关注的信息。若忽略此等信息，可能导致配置失效、数据丢失或设备故障。
提示	表示对配置操作进行补充与说明。

相关资料获取方式

AP 可以被 Tenda 无线控制器或支持“AP 管理”的 Tenda 路由器集中管理，详情请参考对应型号的无线控制器或路由器使用说明书。

访问腾达官方网站 www.tenda.com.cn，搜索对应产品型号，可获取最新的产品资料。

产品资料一览表

文档名称	概述
产品彩页	帮助您了解 AP 的基本参数。包括产品概述、产品特性、产品规格等。
快速安装指南	帮助您快速设置 AP 联网。包括 AP 的安装、上网设置指导、指示灯/接口/按钮说明、常见问题解答、保修条款等。
Web 配置指南	帮助您了解 AP 的更多功能配置。包括 AP 管理页面上的所有功能介绍。

技术支持

如需了解更多信息，请通过以下方式与我们联系。

腾达官网：www.tenda.com.cn

热线：400-6622-666　邮箱：tenda@tenda.com.cn　腾达微信公众号　腾达官方微博

修订记录

资料版本	修订内容	发布日期
V1.0	首次发行	2022-04-01

目录

1 登录 Web 管理界面

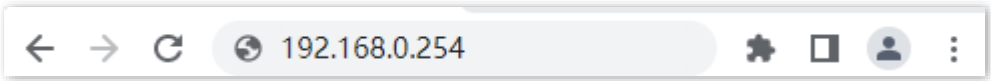
1.1 登录

步骤 1 用网线将管理电脑连接到 AP 或已连接 AP 的交换机。

步骤 2 设置电脑的 IP 地址，使其与 AP 的 IP 地址在同一网段。

例如：AP 的 IP 地址为 192.168.0.254，则电脑的 IP 地址可以设为“192.168.0.X”（X 为 2~253，且未被其它设备占用），子网掩码为“255.255.255.0”。

步骤 3 在电脑上打开浏览器，访问 AP 的 IP 地址（默认为“192.168.0.254”）。



步骤 4　输入登录用户名和密码，点击 登录 。

----完成

提示

若未出现上述页面，请尝试使用以下办法解决：

- 如果 AP 所在局域网有 DHCP 服务器，AP 可能自动从 DHCP 服务器获取了新的 IP 地址。这种情况下，请先到 DHCP 服务器的客户端列表中查看 AP 获得的 IP 地址，再用该 IP 地址登录 AP 的管理页面。
- 如果网络中部署了 Tenda 无线控制器（包括支持“AP 管理”的 Tenda 路由器），AP 可能已经被无线控制器管理，其 IP 地址已改变。请先登录到控制器管理页面，查看 AP 新的 IP 地址后，用新的 IP 地址登录 AP 的管理页面。
- 如果网络中部署了多台 AP，可能出现 AP 的 IP 地址冲突而导致无法登录 AP 管理页面的情况，请确保该 AP 连入网络前，其 IP 地址已修改为与网络中其他 AP 的 IP 地址不同。
- 将 AP 恢复出厂设置再使用默认 IP 地址登录。恢复出厂设置方法：AP 启动完成后，按住 AP 的复位按钮约 8 秒，然后等待约 8 秒（AP 恢复出厂设置并重启）即可。

成功登录到 AP 的管理页面，您可以开始配置 AP 了。

1.2 退出登录

登录到 AP 的管理页面后，如果在 WEB 闲置超时时间内没有任何操作，系统将自动退出登录。此外，您也可以点击页面右上方的 退出 ，安全地退出管理页面。

2 Web 界面简介

2.1 页面布局

AP 的管理页面共分为：一级导航栏、二级导航栏、页签和配置区四部分。如下图所示。

提示

管理页面上显示为灰色的功能或参数，表示 AP 不支持或在当前配置下不可修改。

序号	名称	说明
1	一级导航栏	以导航树、页签的形式组织 AP 的功能菜单。用户可以根据需要选择功能菜单，选择结果显示在配置区。
2	二级导航栏	
3	页签	
4	配置区	用户进行配置或查看配置的区域。

2.2 常用元素

AP 管理页面中常用元素的功能介绍如下表。

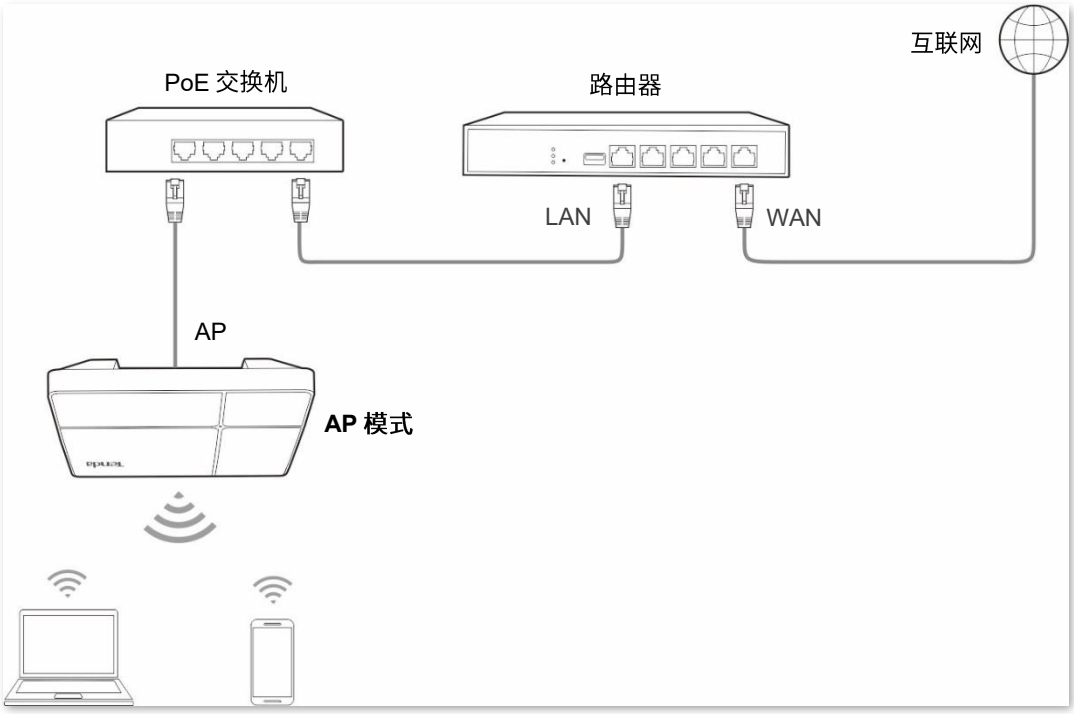
常用元素	说明
	用于刷新当前页面内容。
	用于保存当前页面配置，并使配置生效。
	用于取消当前页面未保存的配置，并恢复到修改前的配置。
	用于查看当前页面功能的帮助信息。

3 快速设置

3.1 概述

在「快速设置」模块，您可以快速设置 AP 的无线信息，使无线终端设备（如智能手机、平板电脑等）接入 AP 的无线网络后可以正常上网。

AP 仅支持工作在 AP 模式。AP 模式下，AP 通过网线接入互联网，将有线信号转变为无线信号，用于无线网络覆盖。AP 默认工作在此模式，应用拓扑图如下。



3.2 快速设置

提示

设置之前，请确保上级路由器已经联网成功。

步骤 1 点击「快速设置」。

步骤 2 选择要设置的无线频段，如“2.4GHz”。

步骤 3 点击“SSID”输入框，设置无线名称（主 SSID）。

步骤 4 选择无线网络的安全模式，并设置其展开参数。

步骤 5 点击 保存 。

步骤 6 如果还需要设置另一频段的无线网络，重新进行**步骤 2-5**。

----完成

使用智能手机等无线设备搜索并连接您设置的 SSID，输入无线密码（即您设置的密钥），即可上网。

参数说明

标题项	说明
无线频段	选择要设置的无线频段。
SSID	点击可修改所选频段下主网络的无线名称。
安全模式	无线网络的安全模式。点击超链接可了解对应安全模式详情。不加密、WEP、WPA-PSK、WPA2-PSK、WPA3-SAE、WPA3-SAE/WPA2-PSK、WPA/WPA2-PSK、WPA、WPA2。

4 状态

4.1 系统状态

在「状态」>「系统状态」页面中，您可以查看 AP 的系统状态和 LAN 口状态。

参数说明

标题项		说明
系统状态	设备名称	AP 的名称，您可以在 LAN 口设置页面修改设备名称。
	运行时间	AP 最近一次启动后连续运行的时长。
	系统时间	AP 当前的系统时间。
	软件版本	AP 系统软件的版本号。
	硬件版本	AP 硬件的版本号。
	无线客户端个数	当前接入到 AP 无线网络的设备数量。

标题项		说明
LAN 口状态	MAC 地址	AP 以太网口（LAN 口）的物理地址。
	IP 地址	AP 的 IP 地址，也是 AP 的管理 IP 地址，局域网内的用户可以使用该 IP 地址登录 AP 的管理页面。您可以在 LAN 口设置页面修改此 IP 地址。
	子网掩码	AP 的子网掩码。
	首选 DNS	AP 的首选 DNS 服务器 IP 地址。
	备用 DNS	AP 的备用 DNS 服务器 IP 地址。

4.2 无线状态

在「状态」>「无线状态」页面中，您可以查看 AP 各频段无线网络的射频状态和 SSID 状态。

参数说明

标题项		说明
射频状态	射频开关	AP 对应频段无线功能的开启/关闭状态。
	网络模式	AP 对应频段当前的无线网络模式。
	信道	AP 对应频段当前的工作信道。
SSID 状态	SSID	AP 对应频段所有的无线网络名称。
	MAC 地址	SSID 对应无线网络的物理地址。
	状态	SSID 对应无线网络的启用状态。
	安全模式	SSID 对应无线网络的安全模式。

4.3 报文统计

在「状态」>「报文统计」页面中，您可以查看 AP 各无线网络的报文统计信息。

SSID	总接收流量	总接收数据包（个）	总发送流量	总发送数据包（个）
Tenda_D00230	0.01MB	83	0.02MB	117
Tenda_D00231	0.00MB	0	0.00MB	0
Tenda_D00232	0.00MB	0	0.00MB	0
Tenda_D00233	0.00MB	0	0.00MB	0
Tenda_D00234	0.00MB	0	0.00MB	0
Tenda_D00235	0.00MB	0	0.00MB	0
Tenda_D00236	0.00MB	0	0.00MB	0

参数说明

标题项	说明
SSID	无线网络名称。
总接收流量	无线网络已接收的数据字节数。
总接收数据包（个）	无线网络已接收的数据包的个数。
总发送流量	无线网络已发送的数据字节数。
总发送数据包（个）	无线网络已发送的数据包的个数。

注意

本设备重启、关闭无线时，所有报文统计信息会清零。禁用 SSID 时，该无线网络的报文统计信息会清零。

4.4 客户端列表

在「状态」>「客户端列表」页面中，您可以查看 AP 当前的无线网络客户端连接情况。

参数说明

标题项	说明
SSID	从下拉列表菜单中选择无线网络名称，以查看该无线网络当前连接无线客户端的情况。
MAC 地址	无线客户端的 MAC 地址。
IP 地址	无线客户端的 IP 地址。
连接时间	无线客户端最近一次接入无线网络的时长。
发送速率	无线客户端当前的发送速率。
接收速率	无线客户端当前的接收速率。

5 网络设置

在「网络设置」>「LAN 口设置」页面中，您可以查看 AP 的 LAN 口 MAC 地址，还可以设置 AP 的 IP 地址相关信息、设备名称及端口驱动模式。

参数说明

标题项	说明
MAC 地址	AP 的 LAN 口物理地址。
IP 获取方式	AP 获取 IP 地址的方式。 - 静态 IP：手动指定 AP 的 IP 地址、子网掩码、默认网关、DNS 服务器。适用于网络中只需部署一台或几台 AP 的场景。 - DHCP（自动获取）：AP 从网络中的 DHCP 服务器自动获取其 IP 地址、子网掩码、网关地址、DNS 服务器。适用于网络中需要部署大量 AP 的场景。 提示 IP 获取方式为“DHCP（自动获取）”时，下次登录 AP 的管理页面前，您必须到网络中的 DHCP 服务器的客户端列表中查看 AP 获得的 IP 地址，再用该 IP 地址进行登录。

标题项	说明
IP 地址	AP 的 IP 地址，也是 AP 的管理 IP 地址，局域网用户可访问该 IP 地址登录到 AP 的管理页面。
子网掩码	AP 的子网掩码，用于定义设备网段的地址空间。
默认网关	AP 的默认网关。一般设置网关地址为出口路由器的 LAN 口 IP 地址。
首选 DNS	AP 的首选 DNS 服务器地址。 如果出口路由器有 DNS 代理功能，此处可填入出口路由器的 LAN 口 IP 地址。否则，请填入正确的 DNS 服务器的 IP 地址。
备用 DNS	AP 的备用 DNS 服务器地址，该选项可选填。 若有两个 DNS 服务器 IP 地址，可将另一个 IP 地址填在此处。
设备名称	该 AP 的名称。 建议修改设备名称为该 AP 的安装位置描述（如大厅），方便在管理多台相同型号的 AP 时，通过设备名称快速定位各 AP 设备。
端口驱动模式	AP PoE 供电接口（即，具备 PoE 受电功能的接口）的驱动模式。 - 标准：速率高，驱动距离较短。一般情况下，建议选择此模式。 - 增强：驱动距离远，但速率较低，一般协商为 10Mbps。 当连接 AP PoE 供电接口与对端设备的网线超过 100 米时，才建议尝试改为“增强”模式以提高网线驱动距离。同时，必须确保对端端口工作模式为“自协商”，否则可能导致 AP PoE 供电接口无法正常收发数据。

6 无线设置

6.1 SSID 设置

6.1.1 概述

在「无线设置」>「SSID 设置」页面中，您可以配置 AP 的 SSID 相关参数。

参数说明

标题项	说明
SSID	选择当前要设置的无线网络。 对应频段下，页面显示的第一个无线网络为该频段的主网络。

标题项	说明
状态	所选择无线网络的状态。 主 SSID 默认启用。其它无线网络默认禁用，可根据需要启用。
访客网络	启用后，该无线网络用户仅可访问因特网，无法访问局域网资源。
SSID 广播	禁用 SSID 广播后，AP 不广播该 SSID，周边的无线设备不能扫描到对应 SSID。此时，如果要连接到该无线网络，用户必须手动在无线设备上输入该 SSID，这在一定程度上增强了无线网络的安全性。
最大客户端数量	无线网络最多允许接入的无线设备数量。 若接入该无线网路的无线设备达到此值，除非某些设备断开连接，否则新的无线设备不能接入此无线网络。
SSID	点击此栏，可修改所选择无线网络的名称。 SSID 支持中文字符。
中文 SSID 编码格式	SSID 中的中文字符采用的编码格式。默认为 UTF-8。 如果 AP 同时设置多个中文 SSID，建议将部分 SSID 选择 UTF-8 编码格式，另部分选择 GB2312 编码格式，以兼容不同的无线客户端。
安全模式	无线网络的安全模式。点击超链接可了解对应安全模式详情。不加密、WEP、WPA-PSK、WPA2-PSK、WPA3-SAE、WPA3-SAE/WPA2-PSK、WPA/WPA2-PSK、WPA、WPA2。

安全模式

无线网络采用具有空中开放特性的无线电波作为数据传输介质，在没有采取必要措施的情况下，任何用户均可接入无线网络、使用网络资源或者窥探未经保护的数据。因此，在 WLAN 应用中必须对传输链路采取适当的加密保护手段，以确保通信安全。

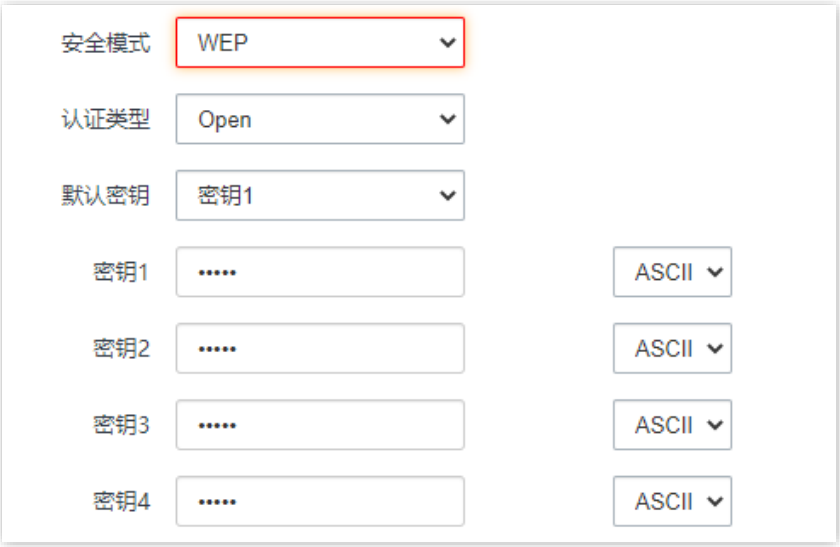
您可根据应用环境需求选择合适的安全模式：不加密、WEP、WPA-PSK、WPA2-PSK、WPA3-SAE、WPA3-SAE/WPA2-PSK、WPA/WPA2-PSK、WPA、WPA2。

- **不加密**

AP 的无线网络不加密，用户连接无线网络时，无需输入密码即可接入。为了保障网络安全，不建议选择此项。

- **WEP**

有线等效加密（Wired Equivalent Privacy）认证，使用一个静态的密钥来加密所有信息，只能提供和有线 LAN 同级的安全性。WEP 加密容易被破解，且无线速率最大只能达到 54Mbps，不建议使用此加密方式。



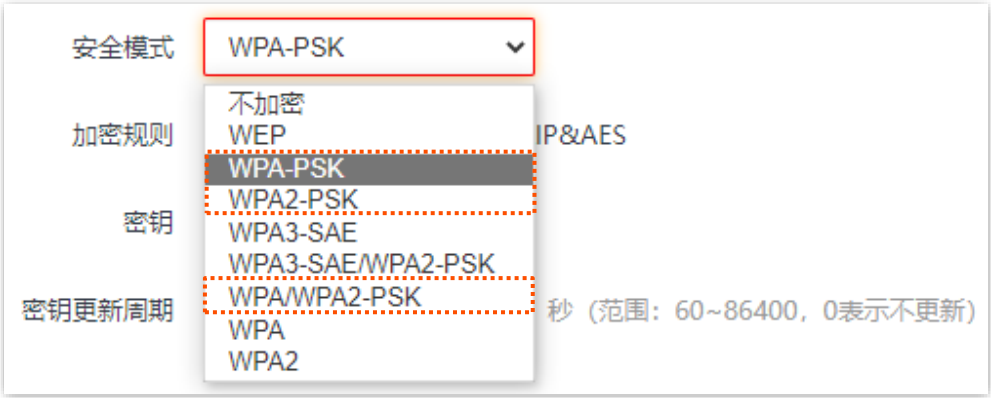
参数说明

标题项	说明
认证类型	WEP 加密时使用的认证方式：Open、Shared。两者加密过程完全一致，只是认证方式不同。 - Open：采用“空认证+WEP 加密”。无线设备无需经过认证，即可与无线网络进行关联，AP 只对传输数据进行 WEP 加密。 - Shared：采用“共享密钥认证+WEP 加密”。无线设备与无线网络进行关联时，需提供在 AP 上指定的 WEP 密钥，只有在双方 WEP 密钥一致的情况下，才能关联成功。
默认密钥	用于指定无线网络当前使用的 WEP 密钥。 如：默认密钥为“密钥 2”，则无线设备需要使用“密钥 2”的无线密码连接该无线网络。
密钥 1/2/3/4	WEP 密钥可以同时输入 4 个，但是只有“默认密钥”指定的密钥生效。密钥字符类型可以为 ASCII 或 Hex。 - ASCII：密钥可以输入 5 或 13 个 ASCII 码字符。 - Hex：密钥可以输入 10 或 26 位十六进制字符（0-9，a-f，A-F）。

- **WPA-PSK、WPA2-PSK、WPA/WPA2-PSK**

WPA/WPA2-PSK 表示 AP 同时兼容 WPA-PSK、WPA2-PSK。

上述 3 种安全模式都采用 WPA 预共享密钥（Pre-Shared Key，简称 PSK）认证，其设置的密钥只用来验证身份，数据加密密钥由 AP 基于加密规则 TKIP 或 AES 来自动生成，解决了 WEP 静态密钥的漏洞，适合一般家庭用户用于保证无线安全。但由于其用户认证和加密的共享密码（原始密钥）为人为设定，且所有接入同一 AP 的无线客户端的密钥完全相同，因此，其密钥难以管理并容易泄漏，不适合在安全要求非常严格的场合应用。



- **WPA3-SAE**

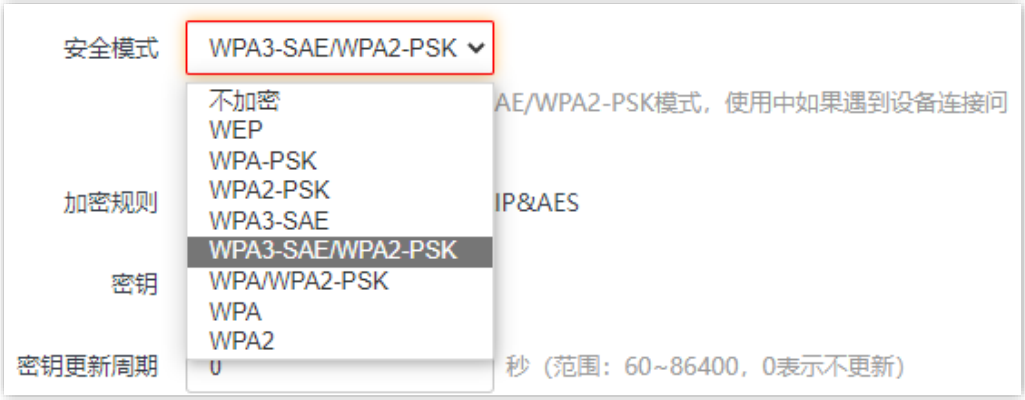
WPA 对等实体同时验证（Simultaneous Authentication of Equals，简称 SAE），WPA2-PSK 的升级版，提供更可靠的、基于密码的验证，使用 AES 加密规则。支持管理帧保护（PMF），可以抵御字典暴破攻击，防止信息泄露，用户无需再设置复杂而难记的密码。

提示

如果无线客户端不支持 WPA3-SAE 加密方式，或者 WiFi 使用体验不好，建议将安全模式设置为“WPA2-PSK”。

- **WPA3-SAE/WPA2-PSK**

表示 AP 同时兼容 WPA3-SAE、WPA2-PSK 两种安全模式。目前 WPA2 仍然被广泛使用，为了允许不支持 WPA3 的无线设备访问 WPA3 网络，AP 支持 WPA3-SAE 过渡模式，即 WPA3-SAE/WPA2-PSK 混合认证。可以兼顾兼容性和安全性需求。



参数说明

标题项	说明
安全模式	选择安全模式。 - WPA-PSK：无线网络采用 WPA-PSK 安全模式，有较好的兼容性。 - WPA2-PSK：无线网络采用 WPA2-PSK 安全模式，有更高的安全等级。 - WPA/WPA2-PSK：兼容 WPA-PSK 和 WPA2-PSK，此时，无线设备使用 WPA-PSK 和 WPA2-PSK 均可连接对应无线网络。 - WPA3-SAE：无线网络采用 WPA3-SAE 安全模式，为 WPA2-PSK 的升级版。 - WPA3-SAE/WPA2-PSK：兼容 WPA3-SAE 和 WPA2-PSK，此时，无线设备使用 WPA3-SAE 和 WPA2-PSK 均可连接对应无线网络。
加密规则	WPA 加密规则。您可参考以下说明选择合适的加密规则。 - AES：高级加密标准。 - TKIP：临时密钥完整性协议。相较于 AES，采用 TKIP 时，AP 只能使用较低的无线速率（最大 54Mbps）。 - TKIP&AES：兼容 TKIP 和 AES，无线客户端使用 TKIP 和 AES 均可连接。
密钥	WPA 预共享密钥，即无线客户端连接此无线网络时使用的密码。
密钥更新周期	WPA 数据加密密钥自动更新周期，较短的密钥更新周期可增强 WPA 数据安全性。 0 表示不更新。

- **WPA，WPA2**

为了改善 PSK 安全模式在密钥管理方面的不足，Wi-Fi 联盟提供了 WPA 企业版本（即 WPA、WPA2），它使用 802.1x 对用户进行认证并生成用于加密数据的根密钥，而不再使用手工设定的预共享密钥，但加密过程并没有区别。

由于采用了 802.1x 进行用户身份认证，每个用户的登录信息都由其自身进行管理，有效降低信息泄漏

的可能性。并且用户每次接入无线网络时的数据加密密钥都是通过 RADIUS 服务器动态分配的，攻击者难以获取加密密钥。因此，WPA、WPA2 极大地提高了网络的安全性，成为高安全无线网络的首选加密方式。

参数说明

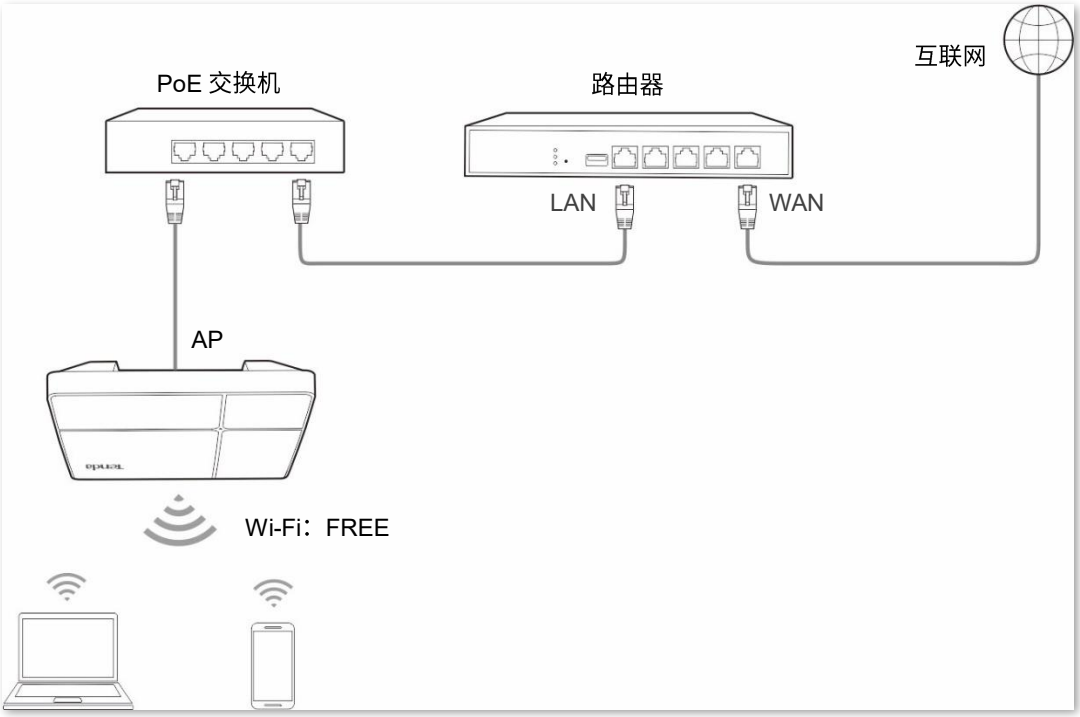
标题项	说明
安全模式	选择安全模式。 - WPA：无线网络采用 WPA 企业版安全模式。 - WPA2：无线网络采用 WPA2 企业版安全模式。
RADIUS 服务器	
RADIUS 端口	用于输入 RADIUS 服务器的 IP 地址/认证端口/共享密钥。
RADIUS 密码	
加密规则	选择 WPA 加密规则。 - AES：高级加密标准。 - TKIP：临时密钥完整性协议。相较于 AES，采用 TKIP 时，AP 只能使用较低的无线速率（最大 54Mbps）。 - TKIP&AES：兼容 TKIP 和 AES，无线客户端使用 TKIP 和 AES 均可连接。
密钥更新周期	WPA 数据加密密钥自动更新周期，较短的密钥更新周期可增强 WPA 数据安全性。 0 表示不更新。

6.1.2 SSID 设置举例

不加密无线网络配置举例

组网需求

酒店大厅进行无线组网，要求无线网络名称为 FREE，没有无线密码。



配置步骤

假设使用 AP 2.4GHz 频段的第 2 个 SSID 进行设置。

步骤 1　点击「无线设置」>「SSID 设置」。

步骤 2　点击“SSID”下拉框，选择第 2 个 SSID。

步骤 3　选择“状态”为“启用”。

步骤 4　修改“SSID”为“FREE”。

步骤 5　选择“安全模式”为“不加密”。

步骤 6　点击 保存 。

----完成

验证配置

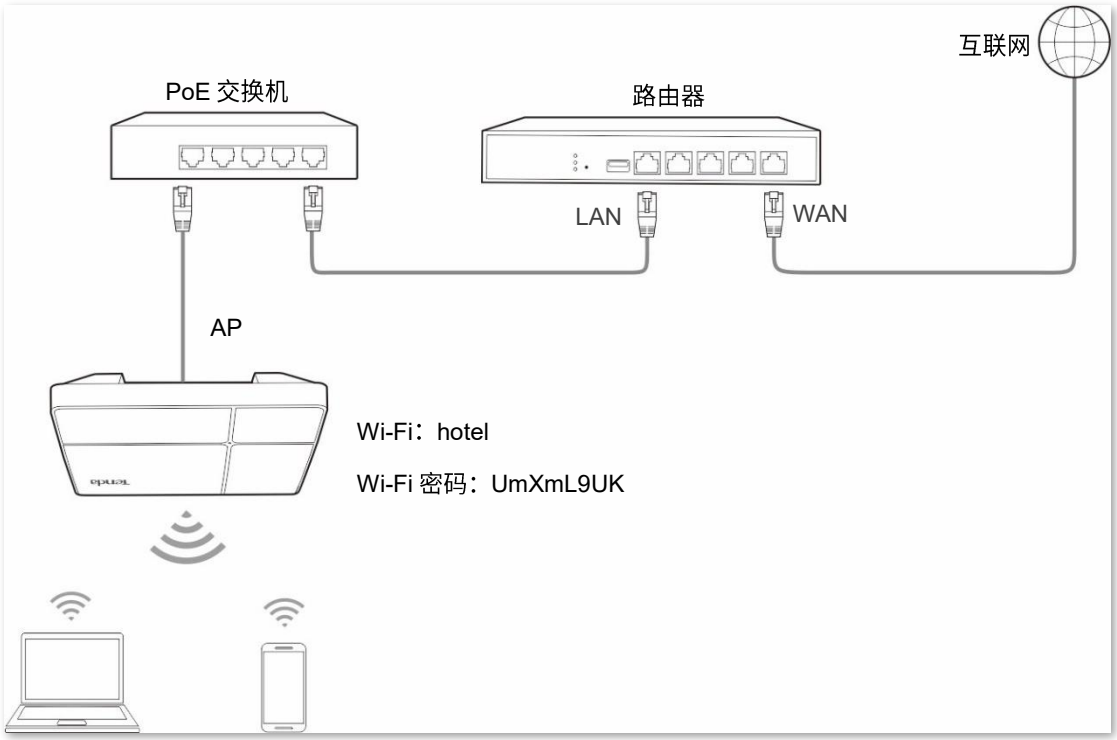
无线设备连接无线网络“FREE”，不需要输入无线密码即可连接成功。

WPA 个人加密无线网络配置举例

组网需求

某酒店进行无线组网，要求有一定安全性，且配置简单。

针对上述需求，建议采用 WPA-PSK、WPA2-PSK 或 WPA/WPA2-PSK 安全模式。假设：无线名称为 hotel，无线密码为 UmXmL9UK，具体如下图所示。



配置步骤

假设使用 AP 2.4GHz 频段的第 2 个 SSID 进行设置。

步骤 1　点击「无线设置」>「SSID 设置」。

步骤 2　点击“SSID”下拉框，选择第 2 个 SSID。

步骤 3　选择“状态”为“启用”。

步骤 4　修改“SSID”为“hotel”。

步骤 5　选择“安全模式为”“WPA2-PSK”，“加密规则”为“AES”。

步骤 6　设置“密钥”为“UmXmL9UK”。

步骤 7　点击 保存 。

----完成

验证配置

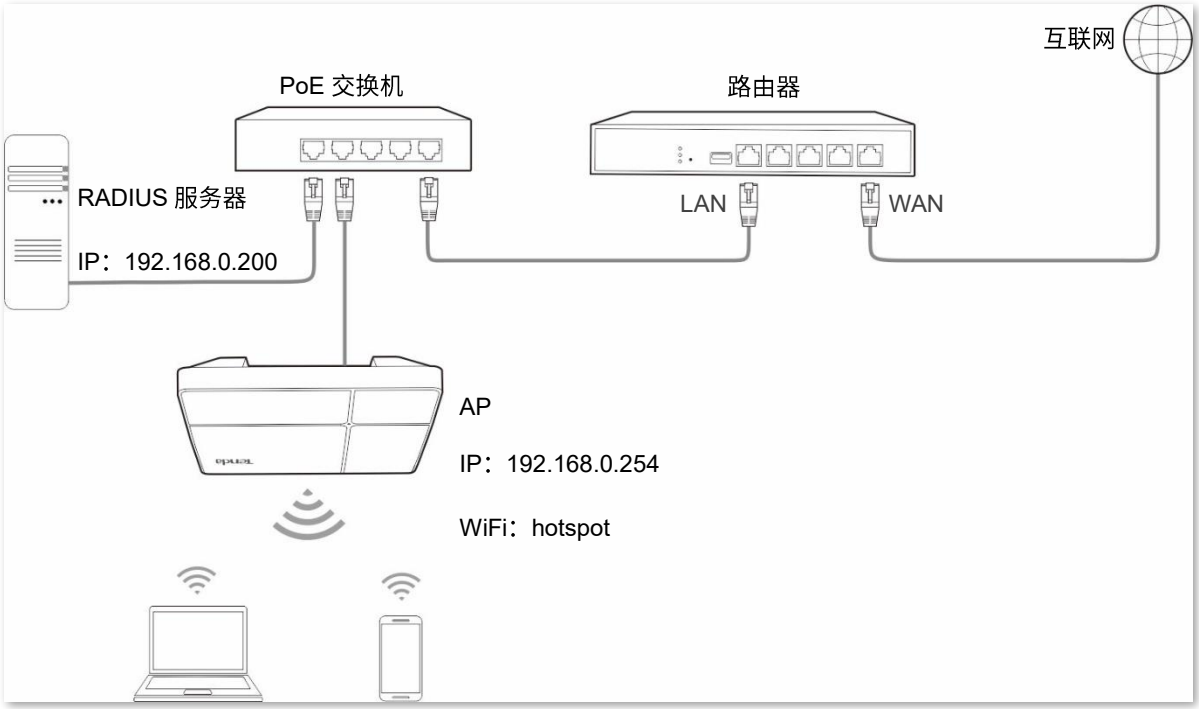
无线设备连接无线网络“hotel”时，输入无线密码“UmXmL9UK”即可连接成功。

WPA 企业加密无线网络配置举例

组网需求

某企业进行无线组网，要求无线网络具有极高的安全性，且网络中已架设专用的 RADIUS 服务器。针对上述需求，建议采用 WPA 或 WPA2 安全模式。

假设：RADIUS 服务器 IP 地址为 192.168.0.200，认证密钥为 UmXmL9UK，认证端口为 1812，无线名称为 hotspot。具体如下图所示。



配置步骤

一. 配置 AP

假设使用 AP 2.4GHz 频段的第 2 个 SSID 进行设置。

步骤 1　点击「无线设置」>「SSID 设置」。

步骤 2　点击“SSID”下拉框，选择第 2 个 SSID。

步骤 3　选择“状态”为“启用”。

步骤 4　修改“SSID”为“hotspot”。

步骤 5　选择“安全模式”为“WPA2”。

步骤 6　分别输入“RADIUS 服务器”为“192.168.0.200”、“端口”为“1812”、“密码”为“UmXmL9UK”。

步骤 7　选择“加密规则”为“AES”。

步骤 8　点击 保存 。

二. 配置 RADIUS 服务器

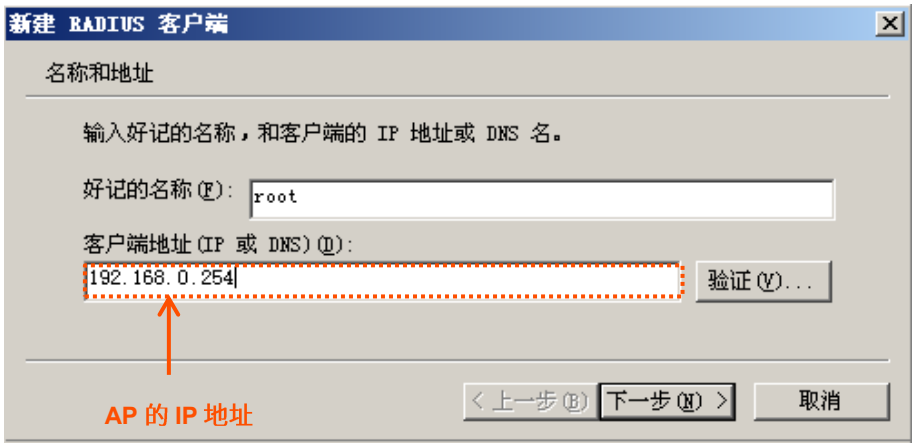
提示

以 Windows 2003 服务器上的 RADIUS 服务器为例说明。

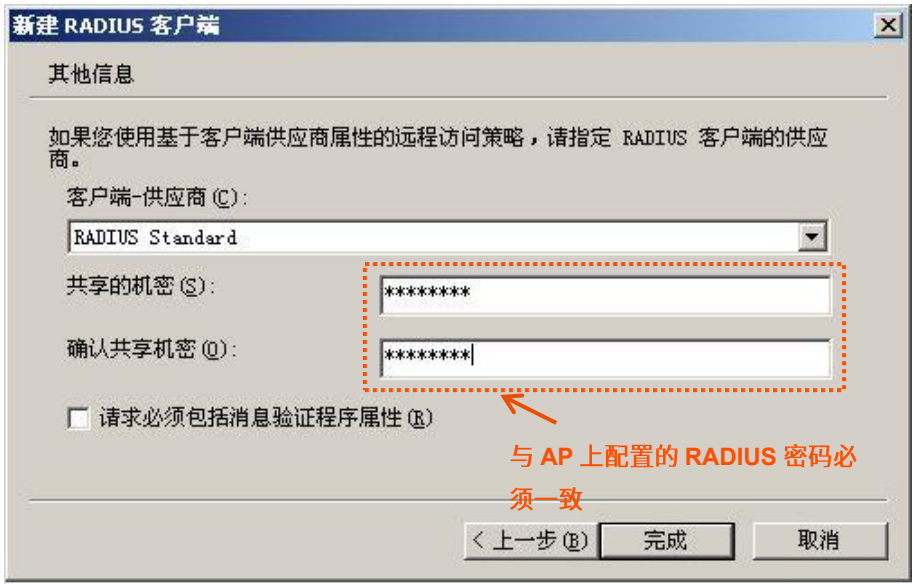
步骤 1 配置 RADIUS 客户端。

1. 在 Windows 2003 服务器操作系统的管理工具，双击“Internet 验证服务”，右键单击“RADIUS 客户端”，选择“新建 RADIUS 客户端”。

2. 设置 RADIUS 客户端名称（可以是 AP 的设备名称），输入 AP 的 IP 地址，点击 下一步 。



3. 在“共享的机密”和“确认共享机密”栏均输入：UmXmL9UK，点击 完成 。

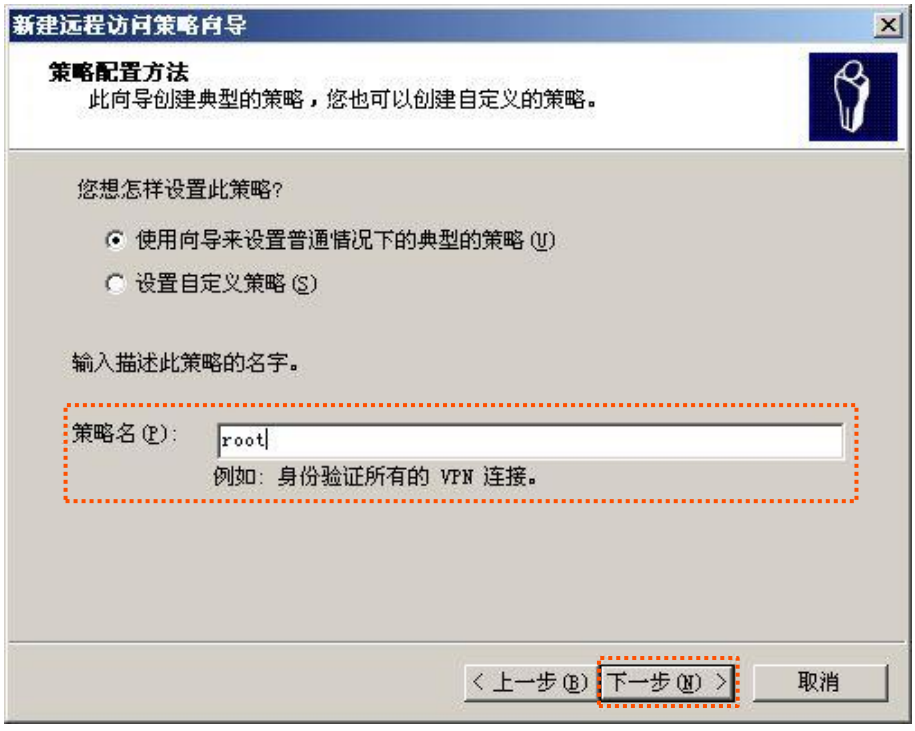


步骤 2 配置远程访问策略

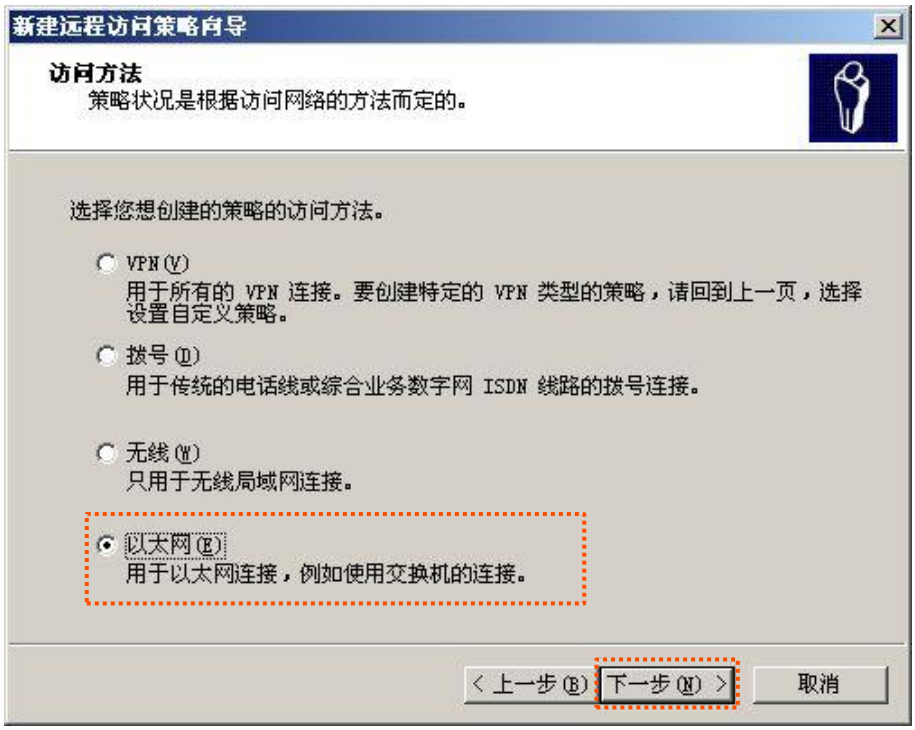
1. 右键单击“远程访问策略”，选择“新建远程访问策略”。

2. 弹出新建远程访问策略向导，点击 下一步 。

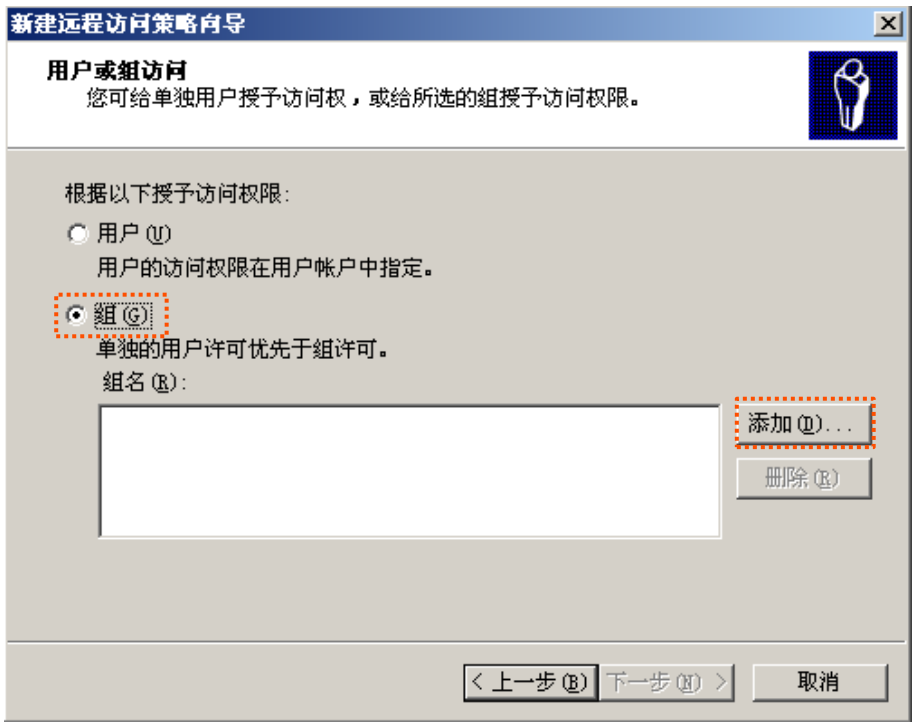
3. 设置策略名，点击 下一步 。



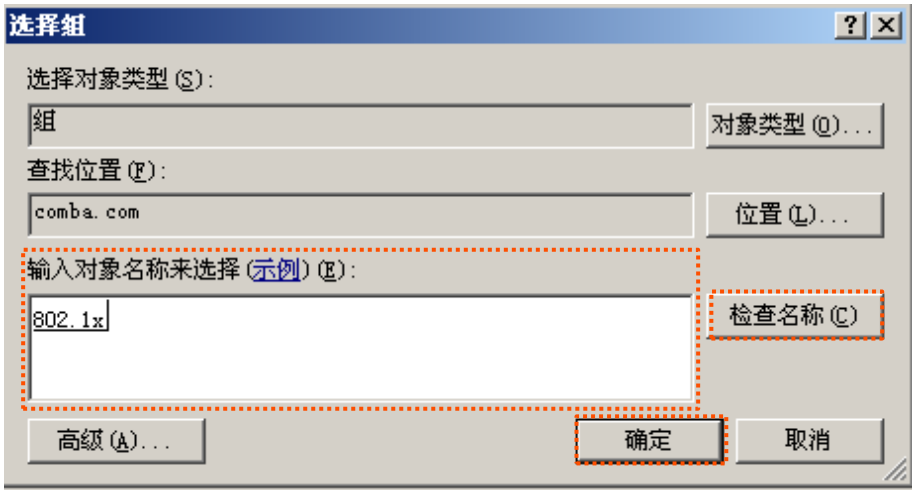
4. 选择“以太网”，点击 下一步 。



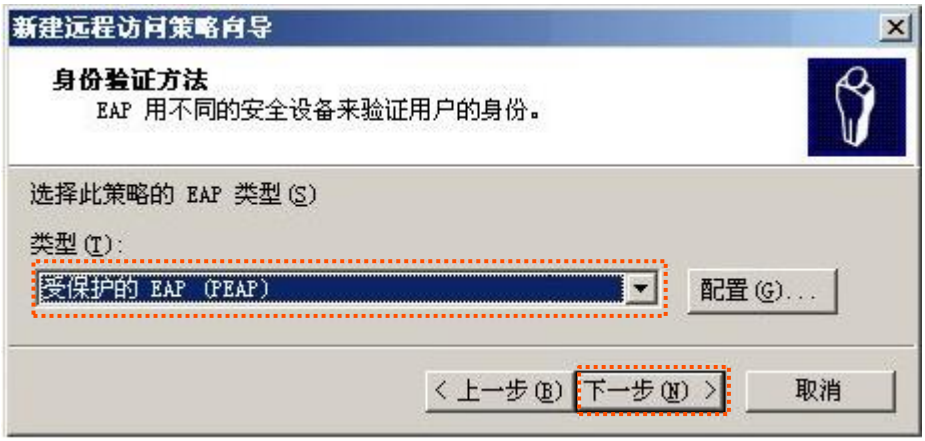
5. 选择“组”，点击 添加 。



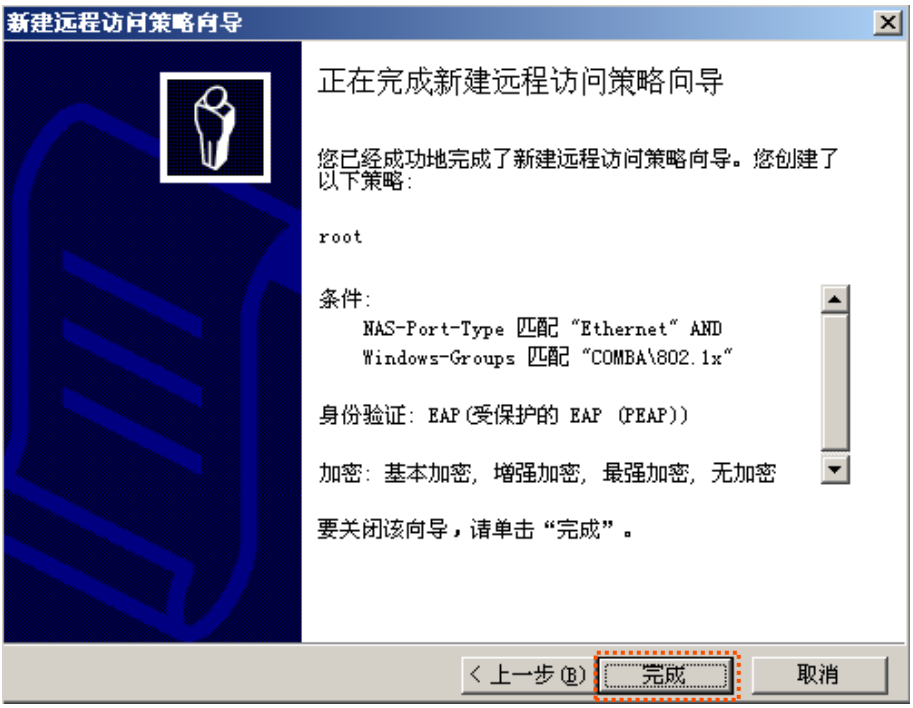
6. 在“输入对象名称来选择”中输入 802.1x，点击 检查名称 ，点击 确定 。



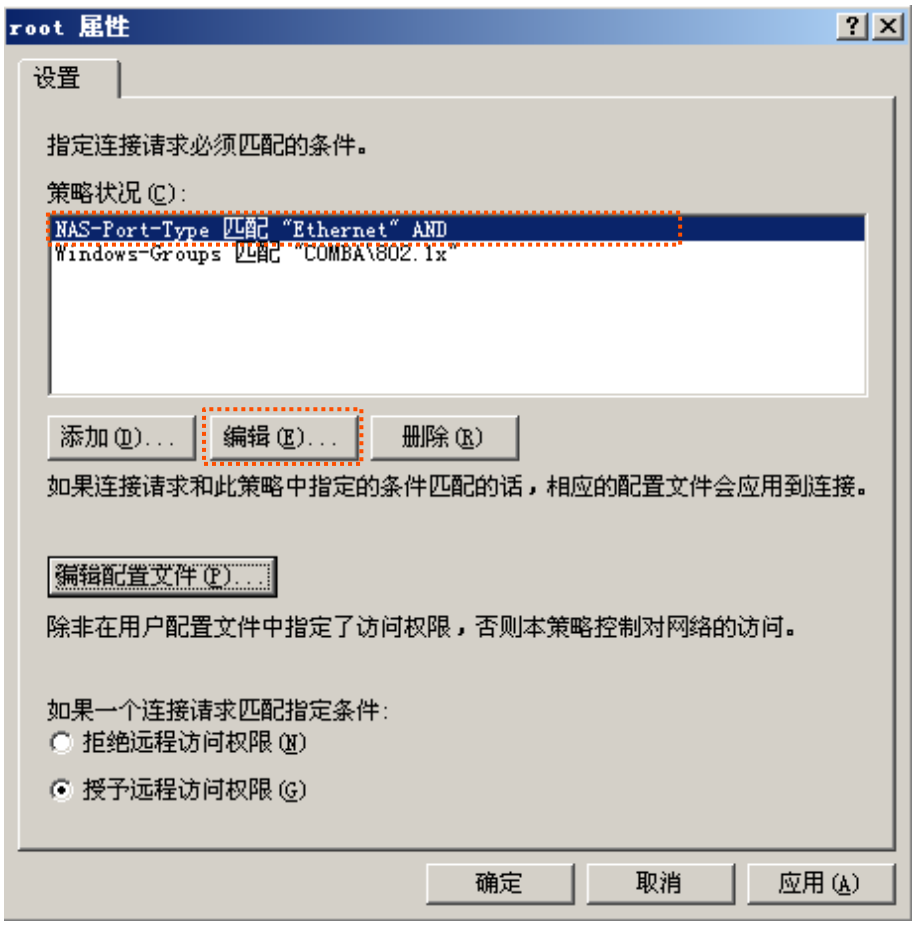
7. 选择“受保护的 EAP (PEAP)”，点击 下一步 。



8. 点击 完成 。

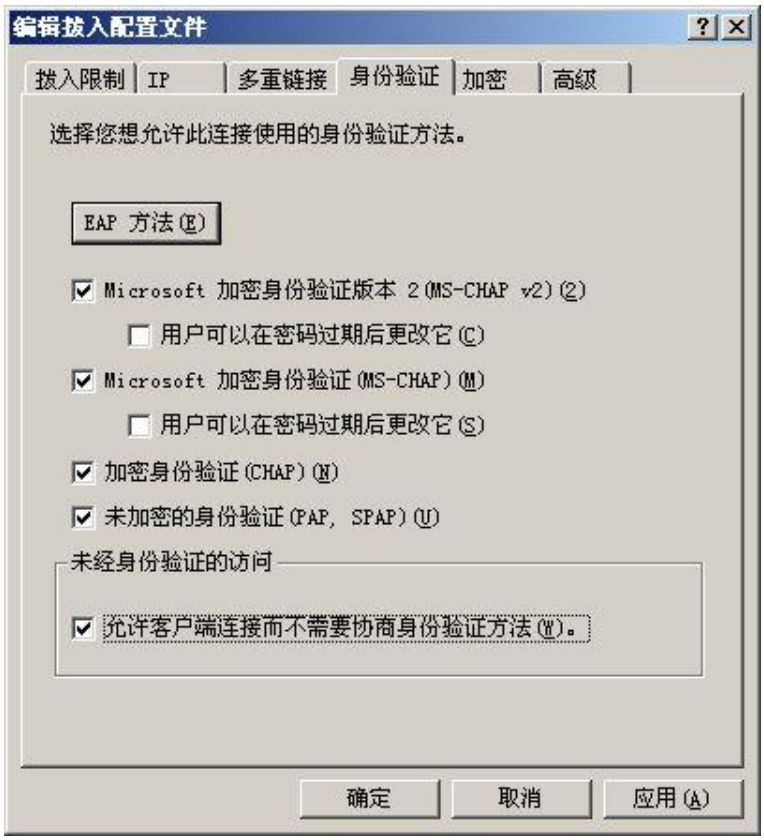


9. 选中 root，点击右键，选择“属性”，在打开的窗口中，选择“授予远程访问权限”，然后选择“NAS-Port-Type 匹配“Ethernet”AND”，点击 编辑 。

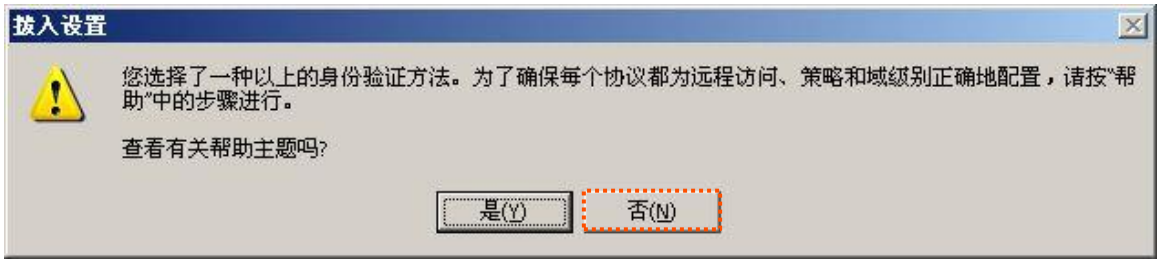


10. 在出现的窗口选择“无线-其它”，点击 添加>> ，然后点击 确定 。

11. 在返回的页面点击 编辑配置文件 ，在身份验证页面，进行下图所示配置，点击 确定 退出。



12. 在弹出的提示框，点击 否 ，确认返回。



步骤 3　配置用户信息

新建用户，并将用户添加到组 802.1x。

三. 配置用户设备

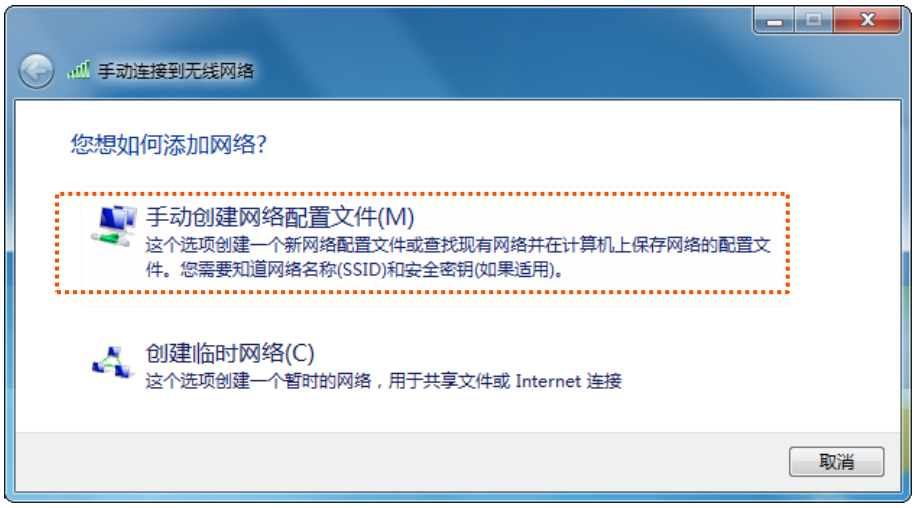
提示

本文以 Windows 7 系统为例说明。

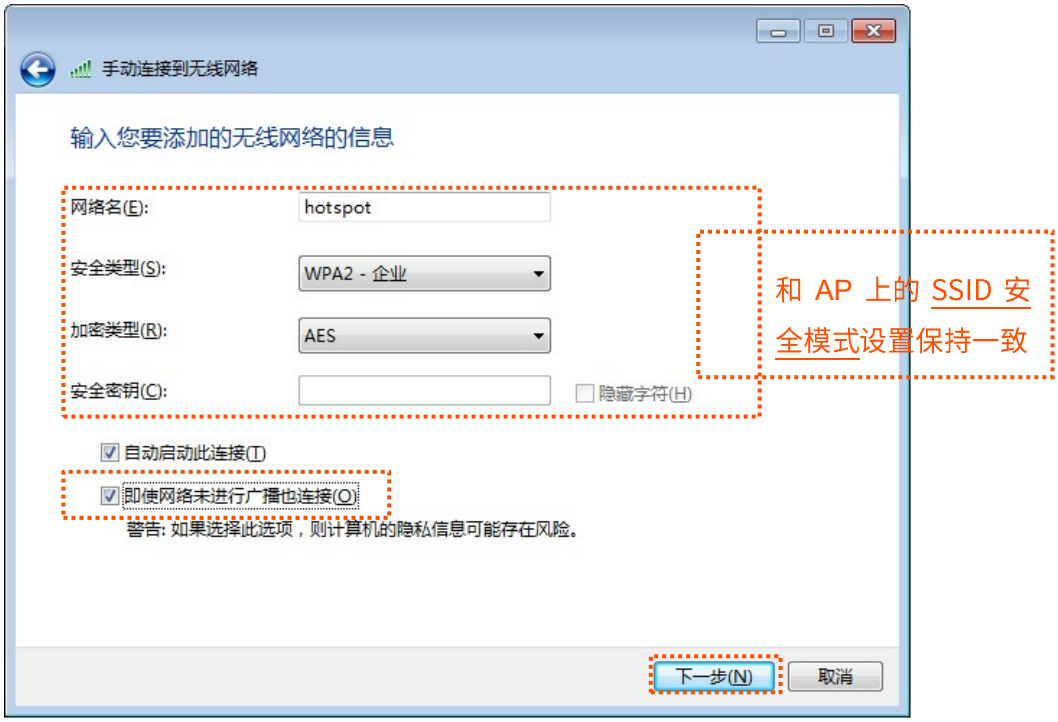
步骤 1　在「控制面板」>「网络和 Internet」>「网络和共享中心」页面，点击“管理无线网络”。

步骤 2　点击“添加”。

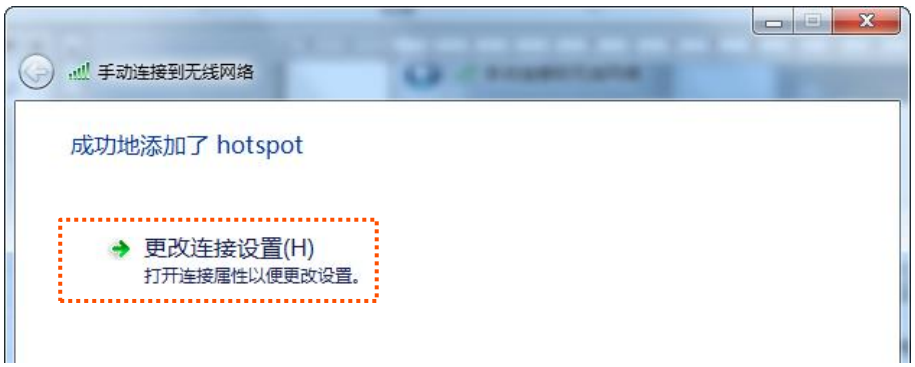
步骤 3　选择“手动创建网络配置文件（M）”。



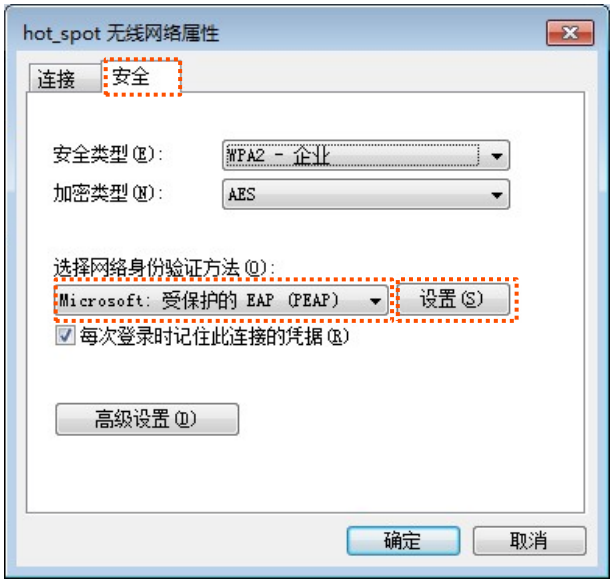
步骤 4　如下图所示输入无线网络信息，勾选“即使网络未进行广播也连接”，然后点击 下一步 。



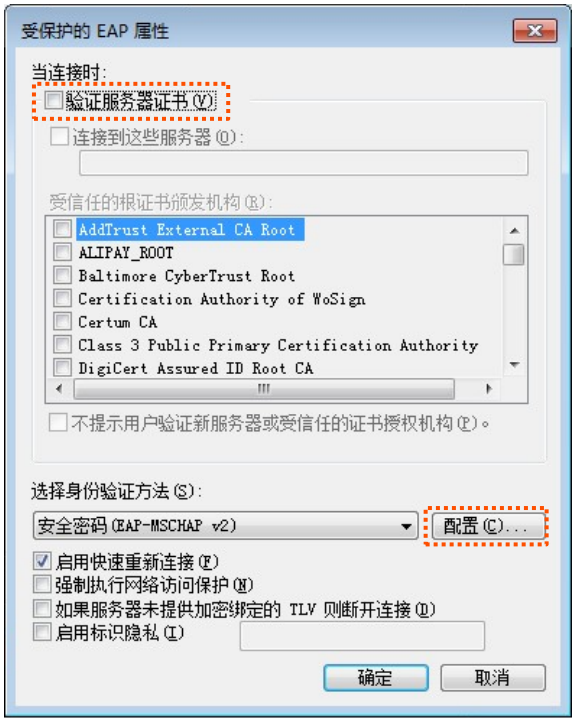
步骤 5　点击“更改连接设置（H）”。



步骤 6　选择“安全”页签，身份验证方法选择“Microsoft：受保护的 EAP（PEAP）”，然后点击 设置 。

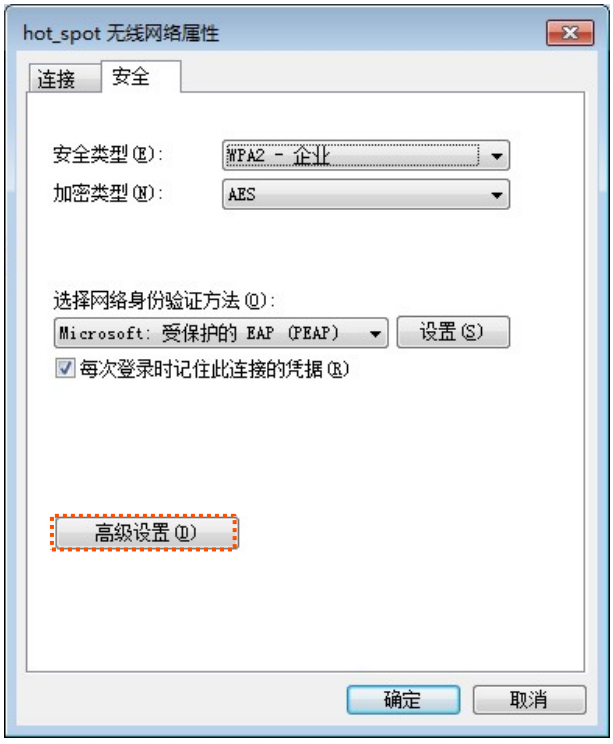


步骤 7　取消勾选“验证服务器证书”，然后点击 配置 。

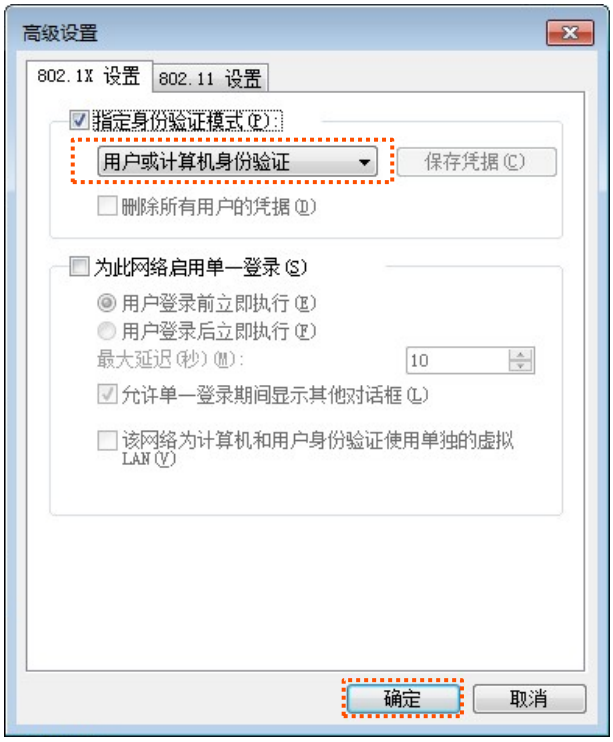


步骤 8　取消勾选“自动使用 Windows 登录名和密码”，点击 确定 。

步骤 9　点击 高级设置 。



步骤 10　指定身份验证模式为“用户或计算机身份验证”，然后点击 确定 。



步骤 11 点击 关闭 。

步骤 12 点击电脑桌面右下角，连接 AP 的无线网络，本例为“hotspot”。

步骤 13 当弹出用户名和密码输入框时，输入 RADIUS 服务器上添加的用户名/密码，然后点击 确定 。

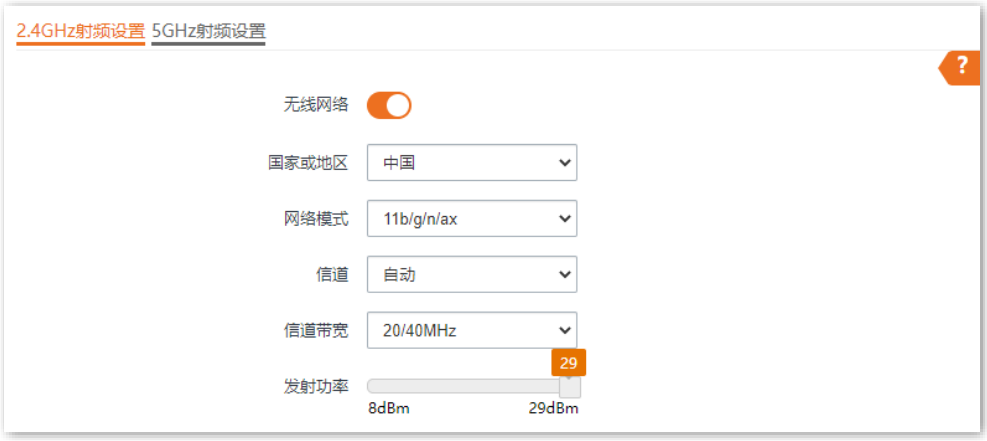
----完成

验证配置

用户设备连接无线网络“hotspot”成功。

6.2 射频设置

在「无线设置」>「射频设置」页面中，您可以修改 AP 的射频相关参数。



参数说明

标题项	说明
无线网络	开启/关闭 AP 相应频段的无线功能。
国家或地区	选择 AP 当前所在的国家或地区，以适应不同国家（或地区）对信道的管制要求。
网络模式	选择 AP 的无线网络模式。 您可以参考以下说明选择 2.4GHz 无线网络下的网络模式。 - 11b：此模式下，仅允许 802.11b 无线设备接入 AP 的 2.4GHz 无线网络。 - 11g：此模式下，仅允许 802.11g 无线设备接入 AP 的 2.4GHz 无线网络。 - 11b/g：此模式下，允许 802.11b、802.11g 无线设备接入 AP 的 2.4GHz 无线网络。 - 11b/g/n：此模式下，允许 802.11b、802.11g 以及工作在 2.4 GHz 的 802.11n 无线设备接入 AP 的 2.4GHz 无线网络。 - 11b/g/n/ax：此模式下，允许 802.11b、802.11g 以及工作在 2.4 GHz 的 802.11n、802.11ax 无线设备接入 AP 的 2.4GHz 无线网络。 您可以参考以下说明选择 5GHz 无线网络下的网络模式。 - 11a：此模式下，仅允许 802.11a 无线设备接入 AP 的 5GHz 无线网络。 - 11ac：此模式下，允许 802.11ac 无线设备接入 AP 的 5GHz 无线网络。 - 11a/n：此模式下，允许 802.11a 以及工作在 5GHz 的 802.11n 无线设备接入 AP 的 5GHz 无线网络。 - 11a/n/ac/ax：此模式下，允许 802.11a、802.11ac 以及工作在 5GHz 的 802.11n、802.11ax 无线设备接入 AP 的 5GHz 无线网络。

标题项	说明
信道	选择 AP 的工作信道。 “自动”表示 AP 根据周围环境情况自动调整工作信道。
信道带宽	选择 AP 的无线信道带宽。 - 20MHz：AP 只能使用 20MHz 的信道带宽。 - 40MHz：AP 只能使用 40MHz 的信道带宽。 - 20/40MHz：仅适用于 2.4GHz。AP 根据周围环境，自动调整其信道带宽为 20MHz 或 40MHz。 - 80MHz：仅适用于 5GHz。AP 只能使用 80MHz 的信道带宽。 - 160 MHz：仅适用于 5GHz。AP 使用 160MHz 的信道带宽。 - 20/40/80/160MHz：仅适用于 5GHz。AP 根据周围环境，自动调整信道带宽为 20MHz、40MHz、80MHz 或 160MHz。
发射功率	设置 AP 相应频段的无线发射功率。 发射功率越大，则无线覆盖范围越广。但适当的减少发射功率更有助于提高无线网络的性能和安全性。

6.3 射频优化

在「无线设置」>「射频优化」页面中，您可以修改 AP 的射频参数，优化性能。

注意

如果没有专业人士指导，建议不要进行此页面的相关设置，以免降低 AP 的无线性能！

参数说明

标题项	说明
Beacon 间隔	设置 AP 发送 Beacon 帧的时间间隔。 Beacon 帧按规定的时间间隔周期性发送，以公告无线网络的存在。一般来说：间隔越小，无线客户端接入 AP 的速度越快；间隔越大，无线网络数据传输效率越高。
接入信号强度阈值	设置 AP 可接受的无线设备信号强度，信号强度低于此值的设备将无法接入 AP。 当环境中存在多个 AP 时，正确设置接入信号强度限制可以确保无线设备主动连接到信号比较强的 AP。
5GHz 优先	启用后，如果 AP 接收到的终端 5GHz 信号强度不低于“5GHz 优先阈值”，则让双频用户优先连接到 AP 的 5GHz 网络。
5GHz 优先阈值	开启“5GHz 优先”时，如果 AP 在 5GHz 频段接收到的终端信号强度大于此阈值，则让终端优先连接 AP 的 5GHz 网络；如果小于此阈值，则让终端随机连接 AP 的 2.4GHz 和 5GHz 网络。
空口调度	启用后，可以让不同速率的用户获得相同的空口时间，提升高速率用户体验。
MU-MIMO	Multi-User Multiple-Input Multiple-Output，即多用户多入多出技术。启用后，AP 可以同时与多个终端设备进行通讯，从而提升通讯效率，避免 Wi-Fi 拥堵。

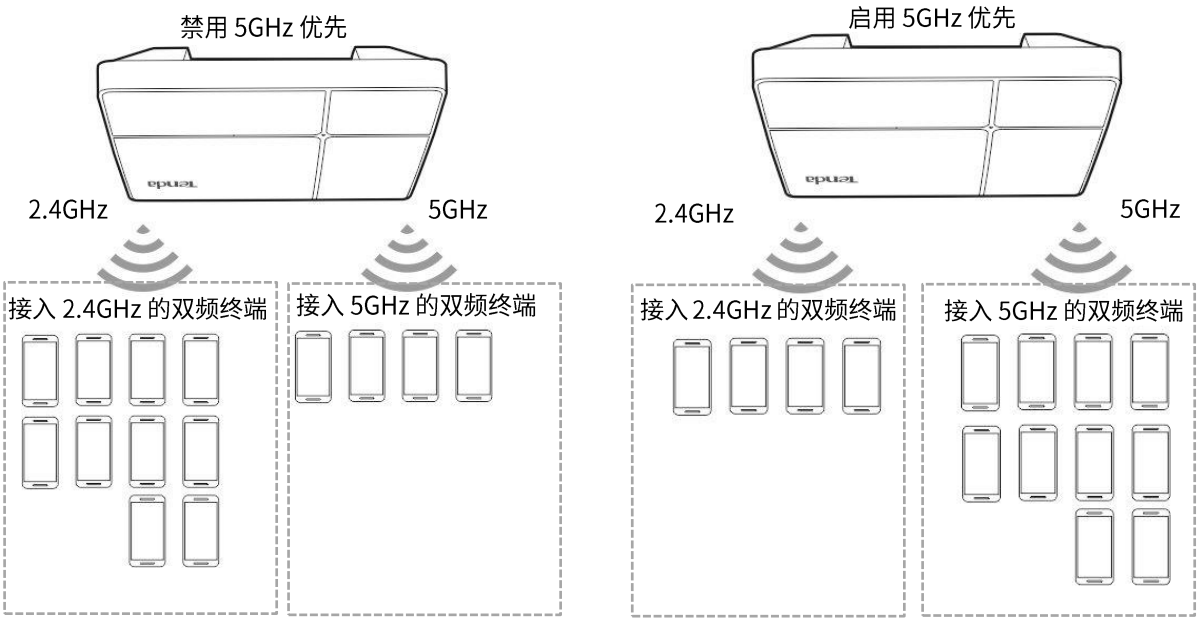
OFDMA	Orthogonal Frequency Division Multiple Access，即正交频分多址。启用后，可以让多个用户在同一时刻并行传输，提高数据传输速率、降低时延，提升用户上网体验。
客户端老化时间	设置客户端老化时间。无线设备连接到 AP 的 Wi-Fi 后，如果在该时间段内与 AP 没有进行数据通信，AP 将主动断开该无线设备。

- **5GHz 优先**

无线网络应用中，2.4GHz 频段比 5GHz 频段应用更为广泛，但 2.4GHz 频段只有 3 个不重叠的通信信道，信道相当拥挤，无线信号间的干扰也很大。实际上，5GHz 频段能提供更多不重叠的通信信道，在中国有至少 5 个，在有的国家更是多达二十多个。

随着无线网络的发展，越来越多的用户使用同时支持 2.4GHz 频段和 5GHz 频段的双频无线终端。然而，通常情况下，双频终端在接入无线网络的时候，默认都选择从 2.4GHz 频段接入，造成 2.4GHz 频段更加拥挤和 5GHz 频段的浪费。

5GHz 优先是指双频终端接入双频 AP 时，如果 AP 接收到的终端 5GHz 信号强度不低于“5GHz 优先阈值”，则让终端优先接入 5GHz 频段，从而达到将双频终端用户向 5GHz 频段上迁移的目的，减少 2.4GHz 频段上的负载和干扰，提升用户体验。



*假设 5GHz 频段的最大客户端数设置为 10

注意

5GHz 优先的前提是 AP 的 2.4GHz 和 5GHz 射频都开启，且在 2.4GHz 和 5GHz 频段配置的 SSID 相同，无线认证加密方式、密码也相同。

- **空口调度**

  传统的报文调度采用 FIFO（先进先出）方式。在无线混合速率环境下，高速用户传送能力强，频谱效率高，却占用的空口时间更少；而低速用户传送能力弱，频谱效率低，却占用的空口时间更多。这会降低每个 AP 的系统吞吐率，进而降低系统效率。

  空口调度通过公平地分配下行传输时间，使得高速用户和低速用户获得相同的下行传输时间，帮助高速用户传输更多的数据，从而使 AP 实现更高的系统吞吐率和用户接入数。

6.4 WMM 设置

6.4.1 概述

802.11 网络提供基于 CSMA/CA（Carrier Sense Multiple Access with Collision Avoidance，载波监听/冲突避免）信道竞争机制的无线接入服务，使得接入 WLAN 的所有客户端享有公平的信道竞争机会，承载在 WLAN 上的所有业务使用相同的信道竞争参数。但实际应用中，不同的业务在带宽、时延、抖动等方面的要求往往不同，需要 WLAN 能根据承载业务提供有区分的接入服务。

WMM 是一种无线 QoS 协议，用于保证高优先级的报文有优先的发送权利，从而保证语音、视频等应用在无线网络中有更好的服务质量。

在了解 WMM 之前，先认识以下常用术语。

- EDCA（Enhanced Distributed Channel Access，增强的分布式信道访问）是 WMM 定义的一套信道竞争机制，有利于高优先级的报文享有优先发送的权利和更多的带宽。
- AC（Access Category，接入类）。WMM 将 WLAN 数据按照优先级从高到低的顺序分为 AC-VO（语音流）、AC-VI（视频流）、AC-BE（尽力而为流）、AC-BK（背景流）四个接入类，每个接入类使用独立的优先级队列发送数据。WMM 保证越高优先级队列中的报文，抢占信道的能力越强。

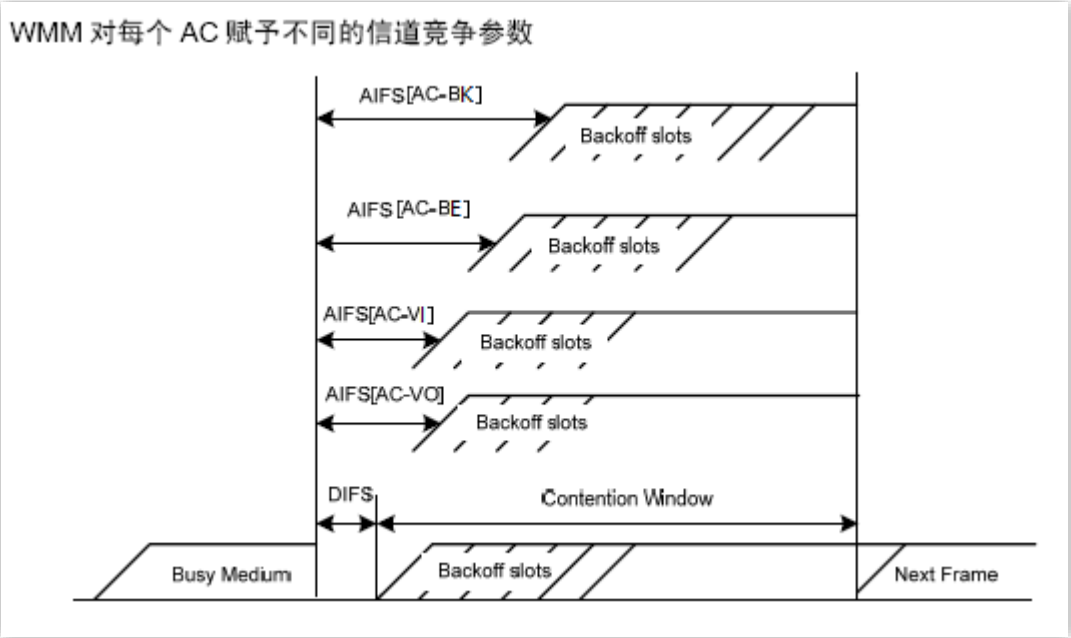
802.11 协议中，设备试图占用信道发送数据前，都会监听信道。当信道空闲时间大于或等于规定的空闲等待时间，设备在竞争窗口范围内随机选择退避时间进行退避。最先结束退避的设备竞争到信道。在 802.11 协议中，由于所有设备的空闲等待时间、竞争窗口都相同，所以整个网络设备的信道竞争机会相同。

- **EDCA 参数**

WMM 协议通过对 802.11 协议进行增强，改变了整个网络完全公平的竞争方式，将数据报文分为 4 个 AC，高优先级的 AC 占用信道的机会大于低优先级的 AC，从而使不同的 AC 能获得不同级别的服务。

WMM 协议对每个 AC 定义了一套信道竞争 EDCA 参数，EDCA 参数的含义如下所示。

- AIFSN（Arbitration Inter Frame Spacing Number，仲裁帧间隙数），在 802.11 协议中，空闲等待时长（DIFS）为固定值，而 WMM 针对不同 AC 可以配置不同的空闲等待时长，AIFSN 数值越大，用户的空闲等待时间越长，为下图中 AIFS 时间段。
- CWmin（最小竞争窗口指数）和 CWmax（最大竞争窗口指数)，决定了平均退避时间值，这两个数值越大，用户的平均退避时间越长，为下图中 Backoff slots 时间段。
- TXOP（Transmission Opportunity，传输机会），用户一次竞争成功后，可占用信道的最大时长。这个数值越大，用户一次能占用信道的时长越大，如果是 0，则每次占用信道后只能发送一个报文。



- **ACK 策略**

协议规定 ACK 策略有两种：Normal ACK 和 No ACK。

- No ACK（No Acknowledgment）策略是在无线报文传输过程中，不使用 ACK 报文进行接收确认的一种策略。No ACK 策略可以用于通信环境较好，干扰较小的应用场合，可以有效提高传输效率。但是如果在通信环境较差的场合使用 No ACK 策略，报文的发送方将不会对丢包进行重发，将导致丢包率增大的问题，反而导致整体性能的下降。
- Normal ACK 策略是指对于每个发送的单播报文，接收者在成功接收到发送报文后，都要发送 ACK 进行确认。

6.4.2 WMM 设置

提示

当 AP 的 2.4GHz 无线网络模式为 11b/g/n 或 11b/g/n/ax，5GHz 无线网络模式为 11a/n、11ac 或 11a/n/ac/ax 时，其相应频段的 WMM 功能无法禁用。

在「无线设置」>「WMM 设置」页面中，您可以禁用或启用 AP 对应频段的 WMM 功能。WMM 功能默认开启。

6.5 访问控制

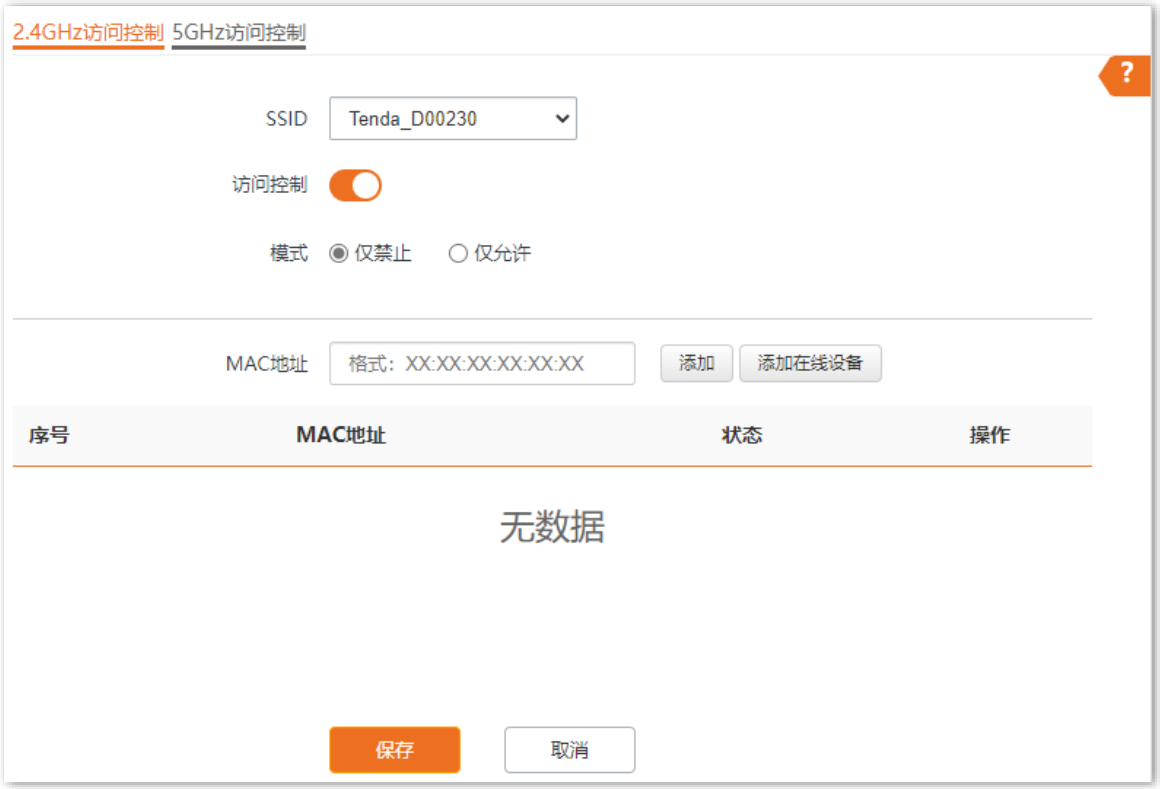
6.5.1 概述

在「无线设置」>「访问控制」页面，您可以通过设置访问控制规则，允许或禁止指定设备接入 AP 的无线网络。

AP 支持以下两种访问控制模式：

- 仅禁止：拒绝指定 MAC 地址的无线设备接入 AP 对应无线网络，允许其他无线设备接入。
- 仅允许：允许指定 MAC 地址的无线设备接入 AP 对应无线网络，拒绝其他无线设备接入。

访问控制功能默认关闭，开启后，页面如下图所示。



参数说明

标题项	说明
SSID	选择要限制无线设备连接的 SSID。
访问控制	启用/禁用访问控制功能。
模式	设置访问控制模式。 - 仅禁止：仅禁止访问控制列表中的无线设备接入该 SSID，允许其他无线设备接入该 SSID。 - 仅允许：仅允许访问控制列表中的无线设备接入该 SSID。
MAC 地址	客户端的 MAC 地址。
添加	点击可将 MAC 地址栏中指定的设备添加到访问控制列表。
添加在线设备	点击可快速添加列表中的无线设备到访问控制列表。
状态	规则的状态，可根据需要开启或关闭。
操作	点击 可以删除规则。

6.5.2 配置访问控制

步骤 1 点击「无线设置」>「访问控制」，并选择要限制用户使用的无线网络所在的频段页签。

步骤 2 点击“SSID”下拉框，选择要限制用户使用的 SSID。

步骤 3 点击滑块至 。

步骤 4 根据需要选择“模式”为“仅禁止”或“仅允许”。

步骤 5 在 MAC 地址输入框中，输入用户设备的 MAC 地址，然后点击 添加 。

提示

如果要限制的无线设备已连接上 AP，可以直接点击 添加在线设备 ，快速添加该无线设备的 MAC 地址到无线访问控制列表。

步骤 6 点击 保存 。

----完成

6.5.3 访问控制配置举例

组网需求

某企业进行无线组网，已专门在 5GHz 频段配置了无线网络 SSID “VIP”，现需要配置 AP，让该 SSID 仅供几个成员接入。

可以使用 AP 的无线访问控制功能实现上述需求。假设仅允许 3 台无线设备连接无线网络 “VIP”，MAC 地址分别为：D8:38:0D:00:00:01、D8:38:0D:00:00:02、D8:38:0D:00:00:03。

配置步骤

步骤 1　点击「无线设置」>「访问控制」，选择 “5GHz 访问控制” 页签。

步骤 2　在 “SSID” 下拉框中选择 “VIP” 。

步骤 3　点击滑块至  。

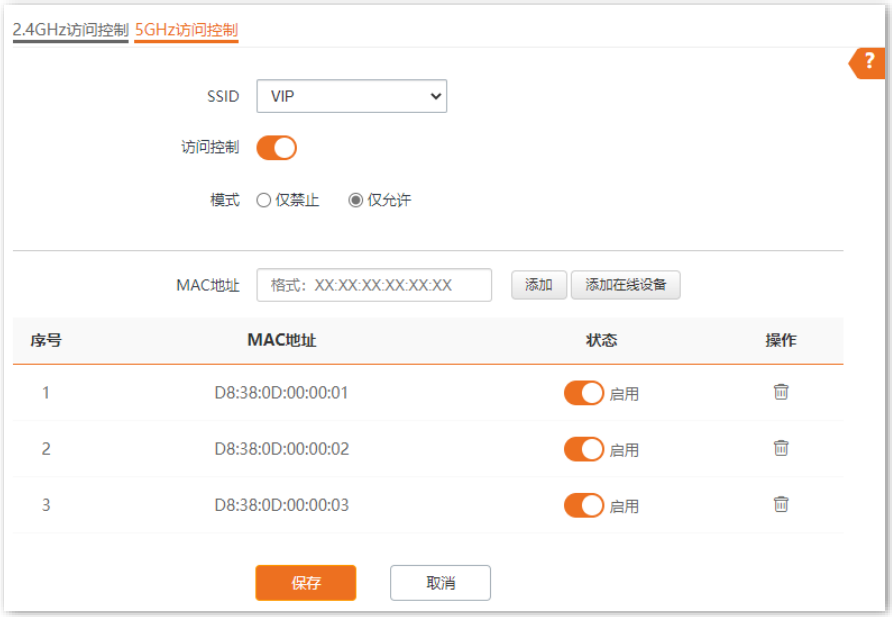
步骤 4　选择 “模式” 为 “仅允许” 。

步骤 5　在 MAC 地址输入框中，输入 “D8:38:0D:00:00:01” ，然后点击 添加 。重复本步骤，添加 MAC 地址 “D8:38:0D:00:00:02” 和 “D8:38:0D:00:00:03” 。

步骤 6　点击 保存 。

----完成

设置完成后，页面如下图示。



验证配置

只有上述 3 台无线设备才可以接入无线网络 “VIP”，其他设备无法接入该网络。

6.6 QVLAN 设置

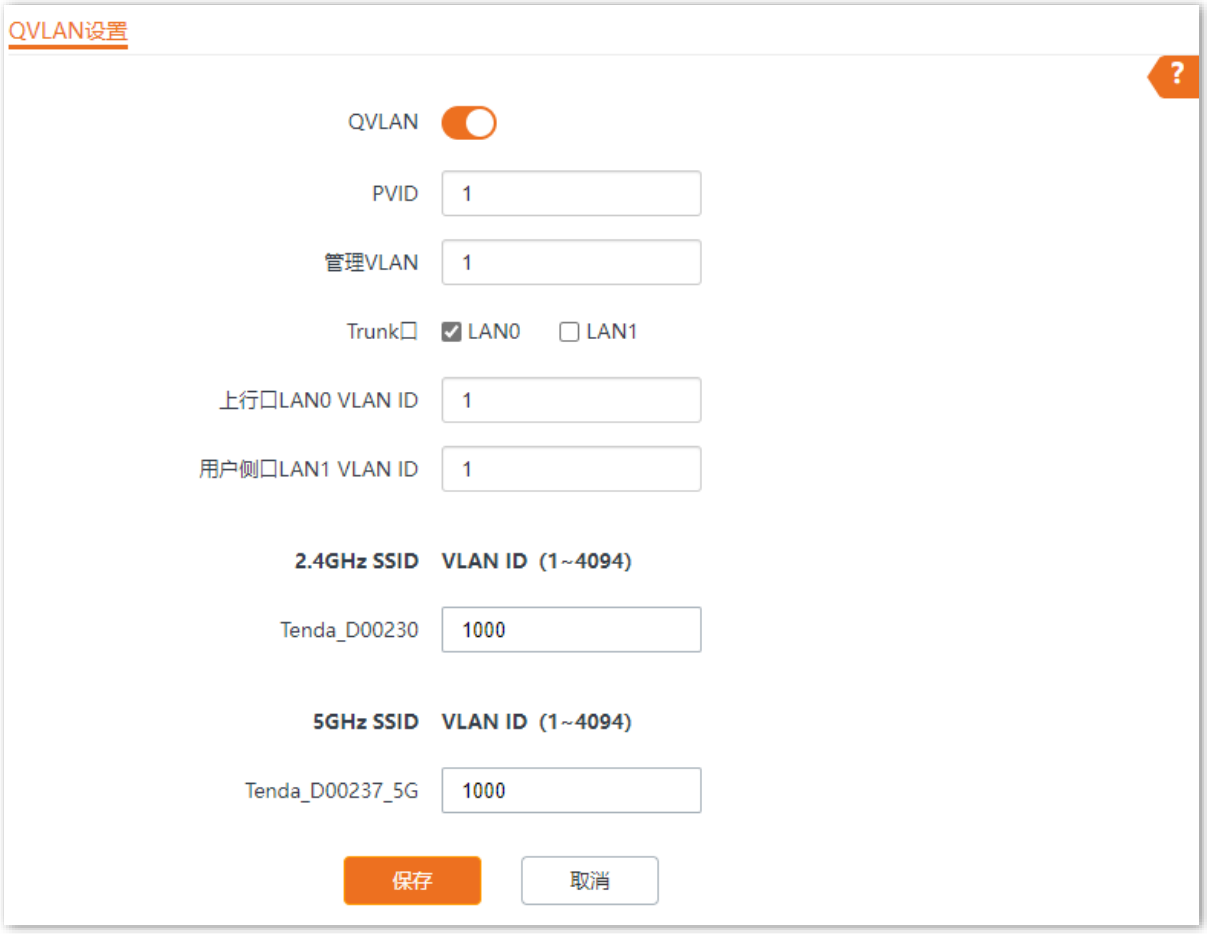
6.6.1 概述

AP 支持 IEEE 802.1q VLAN，可以在划分了 QVLAN 的网络环境使用。默认情况下，AP 关闭了 QVLAN 功能。

启用 QVLAN 后，对于进入端口的 Tag 数据，按数据中的 VID 转发到相应 VLAN 的其他端口；对于进入端口的 Untag 数据，按该端口的 PVID 转发到相应 VLAN 的其他端口。各链路类型端口对数据的接收和发送处理方式详见下表：

端口链路类型	接收数据处理		发送数据处理
	接收 Tag 数据	接收 Untag 数据	
Access	按 Tag 中的 VID 转发到相应 VLAN 的其他端口。	按该端口的 PVID 转发到相应 VLAN 的其他端口。	去掉报文的 Tag 发送。
Trunk			保留报文的 Tag 发送。

在「无线设置」>「QVLAN 设置」页面中，您可以根据需要设置各 SSID 的 VLAN ID。



参数说明

标题项	说明
QVLAN	开启/关闭 AP 的 802.1 Q VLAN 功能。
PVID	AP Trunk 口默认所属的 VLAN 的 ID。
管理 VLAN	AP 的管理 VLAN ID。 更改管理 VLAN 后，管理电脑或无线控制器需要重新连接到新的管理 VLAN，才能管理 AP。
Trunk 口	将选定的以太网口（有线 LAN 口）设置为 Trunk 口，默认为“LAN0”。Trunk 口允许所有 VLAN 通过。 注意 启用 802.1Q VLAN 功能时，至少要选择一个 LAN 口作为 Trunk 口。如果 AP 只有一个以太网口，则默认将该以太网口作为 Trunk 口。
上行口 LAN0 VLAN ID 用户侧口 LAN1 VLAN ID	AP 各以太网口，以及对应的 VLAN。 - LAN0：AP 的 PoE 供电、数据传输复用接口。 - LAN1：AP 的数据传输接口。 提示 未被设为 Trunk 口的以太网口视作 Access 口，可以设置其 VLAN ID。
2.4GHz SSID 5GHz SSID VLAN ID	显示 AP 2.4GHz/5GHz 频段当前已启用的 SSID，以及各 SSID 对应的 VLAN ID。 提示 启用 VLAN 后，SSID 所在的无线接口相当于一个 Access 口，其 PVID 与 VLAN ID 相同。

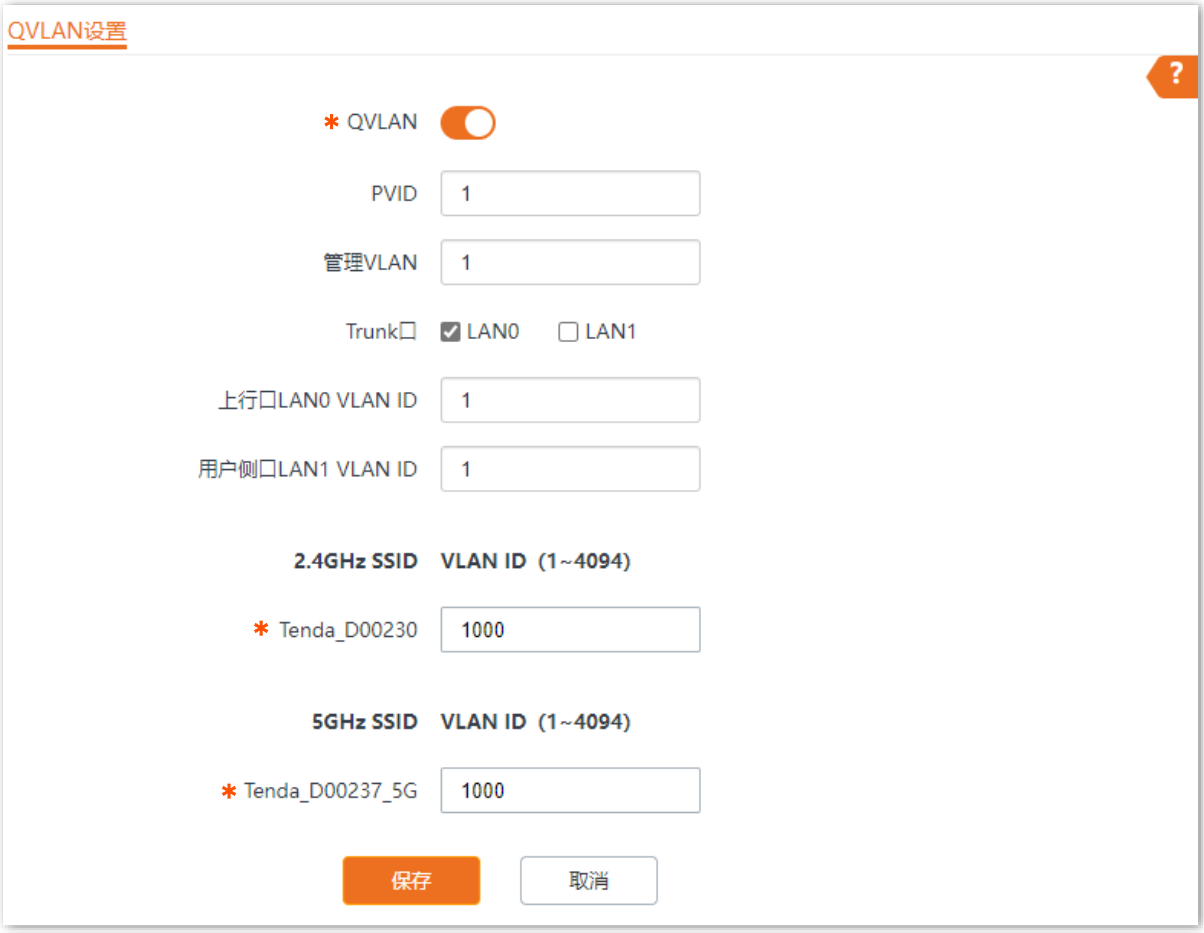
6.6.2 配置 QVLAN

步骤 1 点击「无线设置」>「QVLAN 设置」。

步骤 2 点击滑块至  。

步骤 3 根据需要修改各参数（一般仅需修改“2.4GHz SSID VLAN ID”、“5GHz SSID VLAN ID”）。

步骤 4 点击 保存 。



----完成

6.6.3 QVLAN 设置举例

组网需求

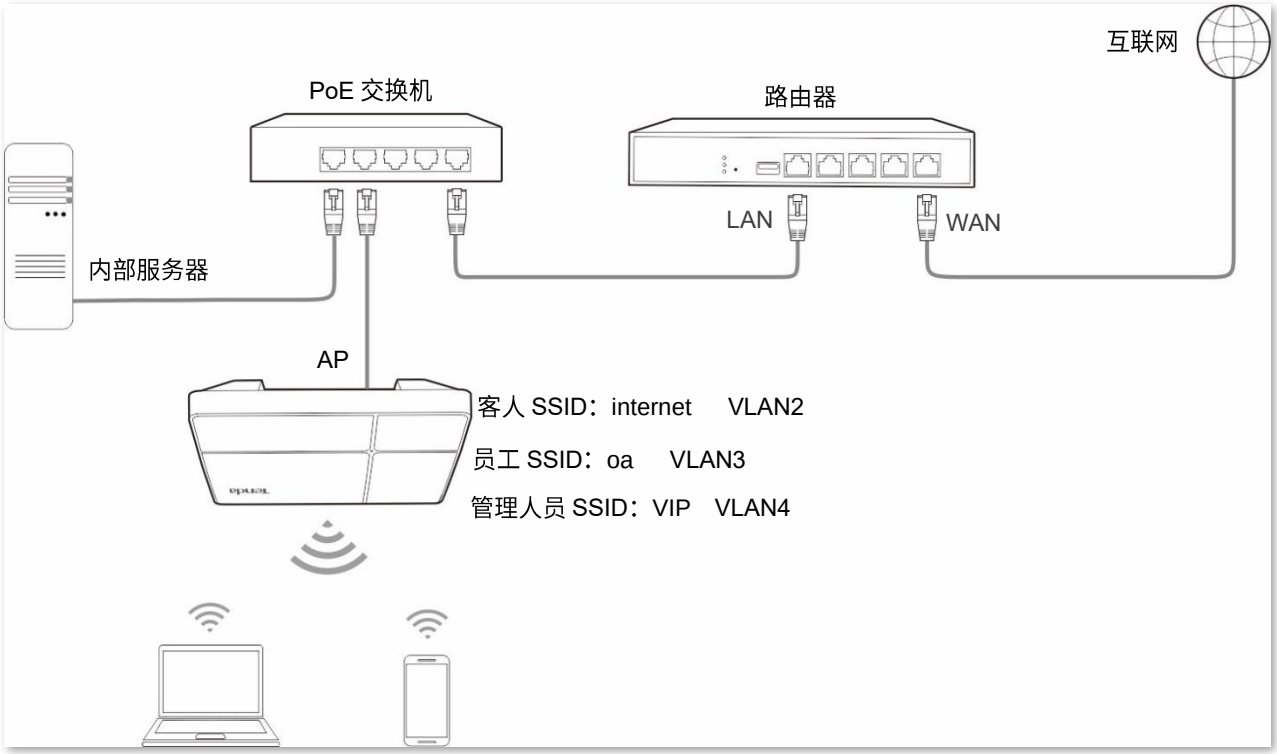
某酒店内要进行无线覆盖，需求如下：

- 客人接入无线网络时获得 VLAN2 的权限，只能访问互联网。
- 员工接入无线网络时获得 VLAN3 的权限，只能访问内网。
- 酒店管理人员接入无线网络时获得 VLAN4 的权限，既能访问内网也能访问互联网。

方案设计

- 使用 2.4GHz 无线频段，客人 SSID 为“internet”，员工 SSID 为“oa”，管理人员 SSID 为“VIP”。
- 在 AP 上为上述 SSID 配置对应的 VLAN。
- 在交换机上配置 VLAN 转发规则。

- 在路由器和内部服务器上配置 VLAN 转发规则。



配置步骤

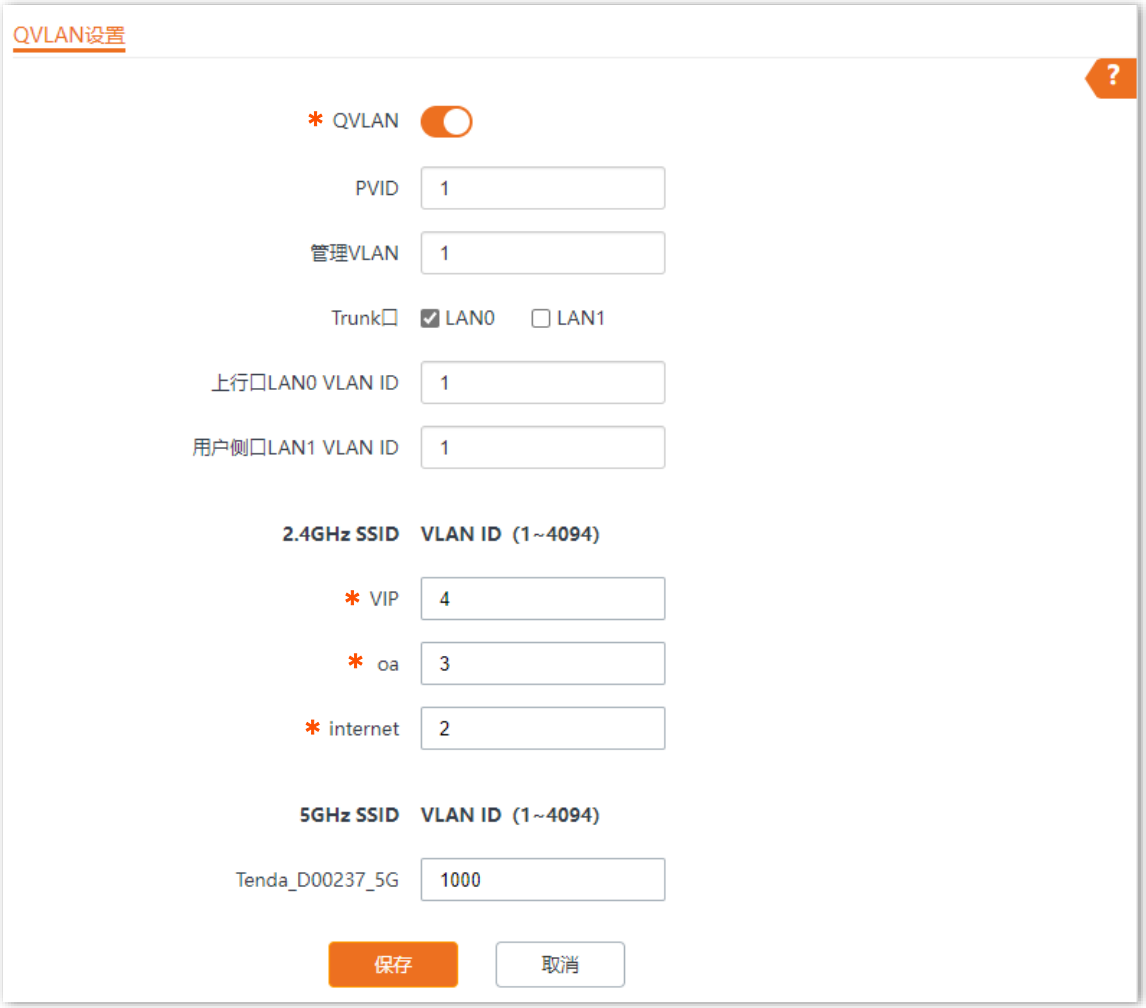
一. 配置 AP

步骤 1 点击「无线设置」>「QVLAN 设置」。

步骤 2 点击滑块至  。

步骤 3 修改 AP 2.4GHz 频段各 SSID 的 VLAN ID，其中，internet 的 VLAN ID 为“2”，oa 的 VLAN ID 为“3”，VIP 的 VLAN ID 为“4”。

步骤 4 点击 保存 。



步骤 5　确认提示信息后，点击 确定 。

等待 AP 自动重启完成即可。

二. 配置交换机

在交换机上划分 IEEE 802.1q VLAN，具体如下。

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
AP	1,2,3,4	Trunk	1
内部服务器	3,4	Trunk	1
路由器	2,4	Trunk	1

其他未提到的端口保持默认设置即可。具体配置方法请参考交换机的使用说明书。

三. 配置路由器和内部服务器

为保证接入到 AP 的无线客户端能正常上网，路由器和内部服务器需要支持并进行 QVLAN 配置。具体如下。

路由器：

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
交换机	2,4	Trunk	1

内部服务器：

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
交换机	3,4	Trunk	1

具体配置方法请参考对应设备的使用说明书。

----完成

验证配置

连接到“internet”的用户只能访问互联网；连接到“oa”的用户只能访问公司内网；连接“VIP”的用户既能访问内网也能访问互联网。

7 系统工具

7.1 时间管理

在「时间管理」模块，您可以设置 AP 的系统时间和 WEB 闲置超时时间。

7.1.1 系统时间

在「系统工具」>「时间管理」>「系统时间」页面中，您可以设置 AP 的系统时间。

为了保证 AP 基于时间的功能正常生效，需要确保 AP 的系统时间准确。AP 支持网络校时和手动设置两种时间校准方式。

网络校时

选择“网络校时”后，系统时间自动同步互联网上的时间服务器。只要 AP 成功连接至互联网就能自动校准其系统时间，AP 重启后也能自行校准，无需重新设置。AP 联网方法请参考 LAN 口设置。

参数说明

标题项	说明
时间设置	AP 系统时间的设置方式。

标题项	说明
时区	选择 AP 当前所在地区的标准时区。

手动设置

选择“手动设置”后，网络管理员需手动设置 AP 的系统时间。AP 每次重启后，您都需要重新设置其系统时间。

您可以手动输入日期与时间，也可以点击 复制本地时间 将当前正在管理 AP 的电脑的时间同步到 AP。

7.1.2 WEB 闲置超时时间

为了保障网络安全，当您登录到 AP 的管理页面后，如果在 WEB 闲置超时时间内没有任何操作，系统将自动退出登录。

在「系统工具」>「时间管理」>「WEB 闲置超时时间」页面中，您可以修改 WEB 闲置超时时间。默认 WEB 闲置超时时间为 5 分钟。

7.2 设备维护

在「系统工具」>「设备维护」页面，您可以重启 AP、将 AP 恢复出厂设置、升级 AP 的系统软件、备份或导入 AP 的配置、开启或关闭 AP 的指示灯。

7.2.1 重启设备

提示

AP 重启时，会断开当前所有连接。请在网络相对空闲的时候进行重启操作。

手动重启

当您设置的某项参数不能正常生效或 AP 不能正常使用时，可以尝试手动重启 AP 解决。

操作方法：进入「系统工具」>「设备维护」>「设备维护」页面，点击 重启 。

自定义重启

通过自定义重启功能，您可以设置 AP 定时自动重启，预防 AP 长时间运行导致其出现性能降低、不稳定等现象。AP 支持以下两种自动重启类型：

- 按间隔时间段重启：管理员设置好一个间隔时间，AP 将每隔这个“间隔时间”就自动重启一次。
- 定时重启：AP 在指定的日期和时间自动重启。

设置 AP 按间隔时间段重启

提示

定时重启时间以 AP 的系统时间为准，为避免重启时间出错，请确保 AP 的系统时间准确。

步骤 1 点击「系统工具」>「设备维护」>「自定义重启」。

步骤 2 点击滑块至 。

步骤 3 选择“类型”为“按间隔时间段重启”。

步骤 4 设置重启间隔时间，如“1440 分钟”。

步骤 5　点击 保存 。

----完成

如上图设置完成后，1 天后 AP 将自动重启。

设置 AP 定时重启

步骤 1　点击「系统工具」>「设备维护」>「自定义重启」。

步骤 2　点击滑块至 。

步骤 3　选择“类型”为“定时重启”。

步骤 4　选择定时重启的日期，如“周一至周五”。

步骤 5　设置定时重启的时间点，如“22:00”。

步骤 6　点击 保存 。

----完成

如上图设置完成后，每周一到周五的 22:00 点，AP 将自动重启。

7.2.2 恢复出厂设置

当 AP 出现无法定位的问题，或您忘记了登录 AP 管理页面的密码时，可以将 AP 恢复出厂设置后重新配置。

注意

- 恢复出厂设置后，AP 的所有设置将会被恢复到出厂状态，您需要重新设置 AP 才能上网，请谨慎使用恢复出厂设置操作。
- 为避免损坏 AP，恢复出厂设置过程中，请确保 AP 供电正常。
- 恢复出厂设置后，AP 的登录 IP 地址为 192.168.0.254，登录用户名/密码均为“admin”。

操作方法 1

AP 启动完成后，用针状物按住复位按钮（RESET）约 8 秒即可。

操作方法 2

在「系统工具」>「设备维护」>「设备维护」页面中，点击 恢复出厂设置 。

7.2.3 升级软件

通过软件升级，您可以体验更多功能，获得更好的用户体验。

注意

为了避免 AP 损坏，确保升级正确：

- 在升级之前，请务必确认新的软件适用于此 AP。
- 升级过程中，请确保 AP 供电正常。

软件升级步骤：

步骤 1 访问 Tenda 官方网站 www.tenda.com.cn，下载对应型号 AP 的升级文件到本地电脑并解压。通常情况下，升级文件格式为：.bin。

步骤 2 登录到 AP 的管理页面，进入「系统工具」>「设备维护」>「设备维护」。

步骤 3 点击 升级 。

步骤 4 在弹出的窗口中选择并上传升级文件。

----完成

页面会出现升级及重启进度条，请耐心等待。待进度条走完后，重新登录到 AP 的管理页面，然后进入「状态」>「系统状态」页面查看 AP 的“软件版本”，确认是否与刚才升级的软件版本相同，如果相同则升级成功，否则请重新升级。

提示

为了提高 AP 的稳定性，以及体验高版本软件的增值功能，AP 升级完成后，建议将 AP 恢复出厂设置，然后重新配置 AP。

7.2.4 备份/恢复

使用备份功能，可以将 AP 当前的配置信息保存到本地电脑；使用恢复功能，可以将 AP 配置还原到之前备份的配置。

当您对 AP 进行了大量的配置，使其在运行时拥有较好的状态/性能，或更符合对应环境的需求，此时建议对该配置进行备份；当您对 AP 进行了升级、恢复出厂设置等操作后，可以恢复备份的 AP 配置。

提示

如果您需要设置大量 AP，且这些 AP 的配置全部一致或大部分一致，也可以使用备份与恢复功能：先配置好 1 台 AP 并备份该 AP 的配置信息，之后将备份的配置信息导入（恢复）到其他 AP，从而节省配置时间，提高效率。

备份配置

步骤 1 点击「系统工具」>「设备维护」>「设备维护」。

步骤 2 点击 备份/恢复 。

步骤 3　点击 备份 。

----完成

浏览器将下载文件名为 APCfm.cfg 的配置文件。

提示

如果浏览器出现类似“此文件可能会损害您的计算机，是否保存”的提示时，请选择“是”。

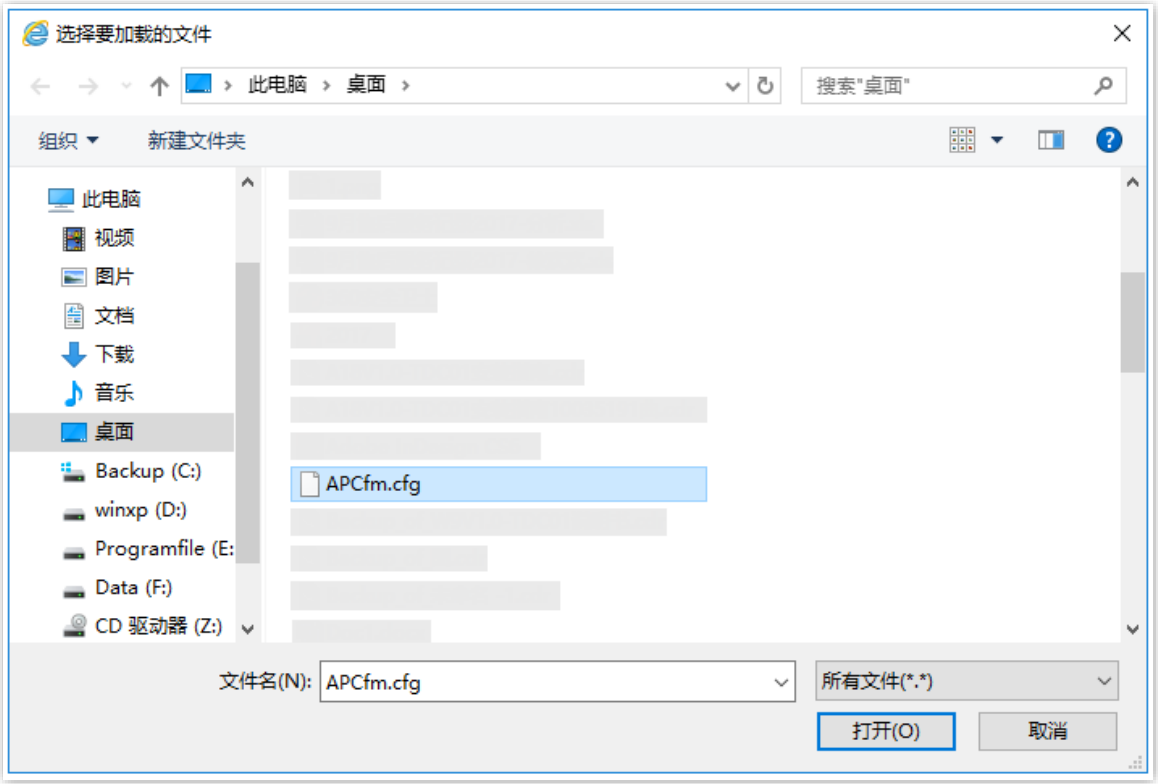
恢复配置

步骤 1　点击「系统工具」>「设备维护」>「设备维护」。

步骤 2　点击 备份/恢复 。

步骤 3　点击 恢复 。

步骤 4　选择并加载之前备份的配置文件。



----完成

页面会出现重启进度条，请耐心等待。进度条走完后，AP 恢复配置成功。

7.2.5 指示灯控制

指示灯控制功能用于关闭/开启 AP 的指示灯。默认情况下，AP 开启了指示灯。

关闭指示灯

在「系统工具」>「设备维护」>「设备维护」页面中，点击 关闭所有指示灯 。

设置完成后，AP 的指示灯熄灭，不再指示 AP 工作状态。

开启指示灯

在「系统工具」>「设备维护」>「设备维护」页面中，点击 开启所有指示灯 。

设置完成后，AP 的指示灯重新亮起，您可以根据指示灯判断 AP 的工作状态。

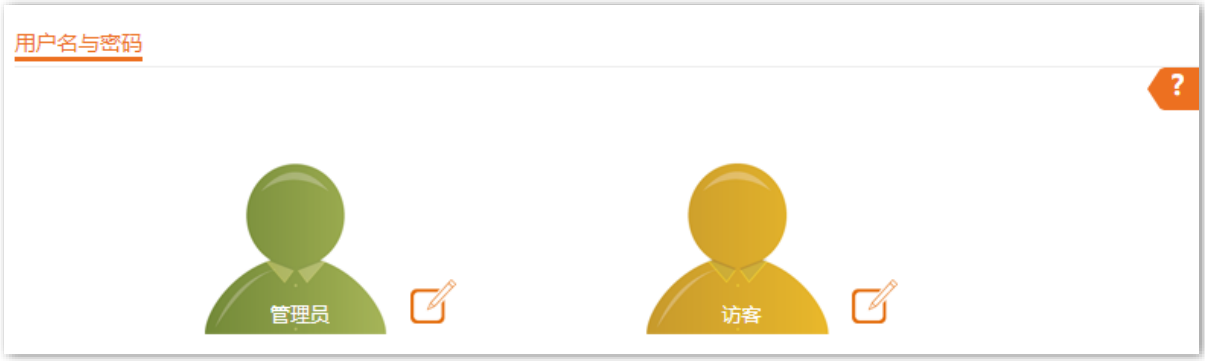
7.3 用户名与密码

7.3.1 概述

在「系统工具」>「用户名与密码」页面，您可以修改 AP 管理页面的登录账号信息，以防止非授权用户进入 AP 的管理页面更改设置，影响无线网络正常使用。

本 AP 支持管理员和访客两种权限的登录账号。

- 管理员：使用此账号登录到 AP 后，您可以查看、修改 AP 的配置。默认用户名与密码均为“admin”。
- 访客：使用此账号登录到 AP 后，您只能查看 AP 的配置信息，不能修改 AP 的配置。默认用户名与密码均为“user”，且默认禁用。



7.3.2 修改登录账户的用户名与密码

步骤 1 点击「系统工具」>「用户名与密码」。

步骤 2 点击待修改账户旁的 。

步骤 3 如果待修改账户为“访客”，则点击启用滑块至 ，否则下一步。

步骤 4 在“原密码”输入框中输入账户当前的密码。

步骤 5 在“新用户名”输入框中输入新的账户名称，如“123”。

步骤 6 在“新密码”输入框中输入新的账户密码。

步骤 7 在“确认新密码”输入框中再次输入新的账户密码。

步骤 8 点击 保存 。

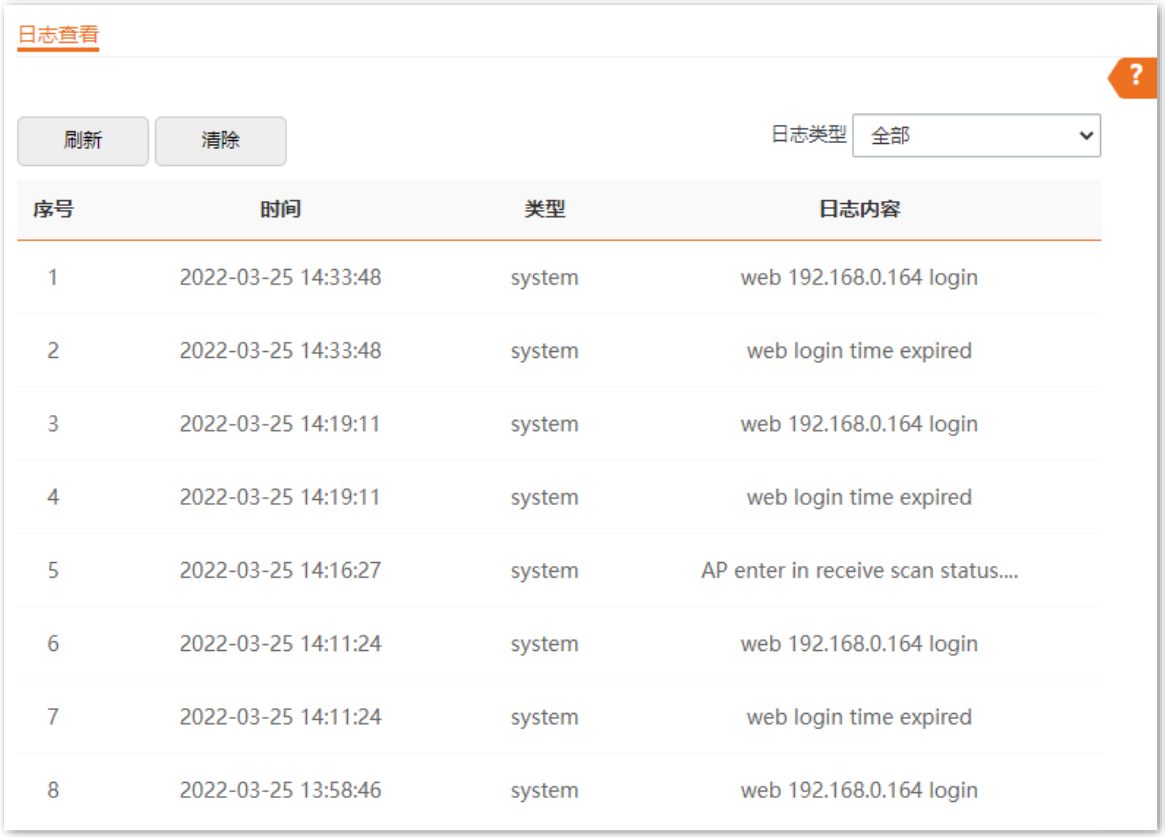
----完成

系统会跳转至登录页面，您可输入新密码，然后点击 登录 即可登录到 AP 的管理页面。

7.4 系统日志

AP 的系统日志记录了系统启动后出现的各种情况及用户对 AP 的操作记录。若遇网络故障，可以利用 AP 的系统日志信息进行问题排查。

在「系统工具」>「系统日志」>「日志查看」页面，您可以查看系统日志。



日志记录时间以 AP 的系统时间为准，请确保 AP 的系统时间准确。您可以到「系统工具」>「时间管理」>「系统时间」页面校准 AP 的系统时间。

AP 默认保存最新的 500 条日志信息，如果超过可显示的最大日志条数，设备会自动清除前面的日志。如果要查看 AP 最新的日志信息，请点击 刷新 ；如果要清空页面显示的日志信息，请点击 清除 。

注意

- AP 重启后，重启之前的日志信息将丢失。
- 断电后重新通电、配置 QVLAN、软件升级、恢复配置、恢复出厂设置等操作都会导致 AP 重启。

7.5 诊断工具

通过诊断工具，您可以用于检测网络的连通性和连通质量。

执行诊断：

假设要检测到百度服务器的链路是否畅通。

步骤 1 点击「系统工具」>「诊断工具」。

步骤 2 输入目标 IP 地址或域名，本例为“www.baidu.com”。

步骤 3 点击 ping 。

----完成

稍后，诊断结果将显示在下面的黑框中。如下图示例。

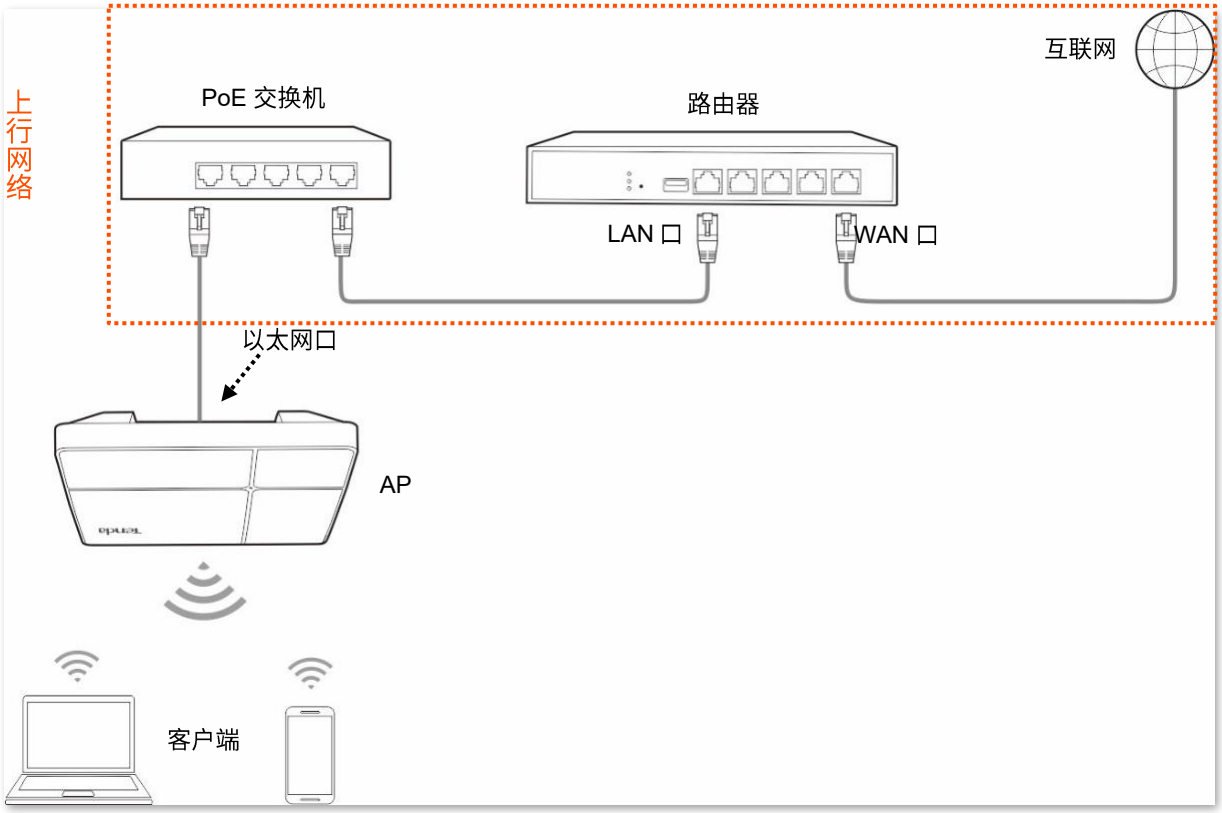
7.6 上行链路检测

7.6.1 概述

AP 模式时，AP 通过以太网口（LAN 口）接入上行网络，如果以太网口到上行网络之间的某些关键节点出现故障，则 AP 及关联到 AP 的无线客户端就无法继续访问上行网络。启用上行链路检测后，AP 会周期性地通过以太网口去 Ping 已配置的主机，如果所配置的 Ping 主机都无法到达，AP 将执行关闭射频或重启设备动作。

- 若 AP 执行关闭射频动作，无线客户端将无法搜索到该 AP 的 SSID，直至故障 AP 的上行网络连接恢复正常，AP 停止执行关闭射频动作，无线客户端才可以重新关联该 AP。这样保证了在无线客户端所关联的 AP 出现上行连接故障后，如果同一区域还有其他工作正常的 AP，无线客户端可以通过关联到其他工作正常的 AP 来接入上行网络。
- 若 AP 执行重启设备动作，设备重启后检查上行网络是否恢复正常，若仍未恢复，则在下一检测周期再次执行重启动作，直至故障 AP 的上行网络连接恢复正常，AP 停止执行重启动作。这样通过重启设备，一定程度上解决了因设备故障导致上行链路不通的问题。

上行链路检测组网如下图所示（上行接口为以太网口）。



7.6.2 配置上行链路检测

步骤 1 点击「系统工具」>「上行链路检测」。

步骤 2 点击滑块至  。

步骤 3 设置上行链路检测的执行动作。

步骤 4 在“上行链路地址 1”和“上行链路地址 2”输入框中输入 Ping 的目的主机地址，如 AP 以太网口直连的交换机或路由器 IP 地址。如果目的主机地址只有一个，则“上行链路地址 1”和“上行链路地址 2”都输入该目的主机地址。

步骤 5 设置执行上行链路检测的间隔时间，系统默认为“10 分钟”。

步骤 6 点击 保存 。

----完成

参数说明

标题项	说明
上行链路检测	开启/关闭 AP 的上行链路检测功能。
执行动作	设置上行链路检测的执行动作。开启 AP 的上行链路检测功能后可设置。 – 关闭射频：AP 执行关闭射频动作。 – 重启设备：AP 执行重启设备动作。
上行链路地址 1	输入 Ping 的目的主机地址。开启 AP 的上行链路检测功能后可设置。
上行链路地址 2	
检测间隔	设置执行上行链路检测的间隔时间。开启 AP 的上行链路检测功能后可设置。

附录

A 默认参数

AP 主要参数的默认设置如下表：

参数			默认设置
设备登录	管理 IP 地址		192.168.0.254
	用户名|密码	管理员	admin|admin
快速设置	工作模式		AP 模式
LAN 口设置	IP 获取方式		LAN 口 IP 地址默认获取方式为静态 IP 若 AP 所在局域网有 Tenda 无线控制器（包含支持“AP 管理”的 Tenda 路由器），AP 可能自动从无线控制器的 DHCP 服务器获取新的 IP 地址。这种情况下，请到无线控制器 DHCP 服务器的客户端列表中查看 AP 获取的 IP 地址
SSID 设置	SSID	2.4GHz	支持 7 个 SSID。SSID 为“Tenda_XXXXXX”，其中 XXXXXX 为 AP LAN 口 MAC 后六位~后六位+6，您可以到「无线设置」>「SSID 设置」页面查看 默认主 SSID 启用，其他 SSID 禁用
		5GHz	支持 4 个 SSID。SSID 为“Tenda_XXXXXX_5G”，其中 XXXXXX 为 AP LAN 口 MAC 后六位+6~后六位+9，您可以到「无线设置」>「SSID 设置」页面查看 默认主 SSID 启用，其他 SSID 禁用
射频设置	无线网络		开启

B 缩略语

缩略语	全称
AC	接入类（Access Category）
AC	无线控制器（Access Point Controller）
AES	高级加密标准（Advanced Encryption Standard）
AIFSN	仲裁帧间隙数（Arbitration Inter Frame Spacing Number）
AP	无线接入点（Access Point）
APSD	自动省电模式（Automatic Power Save Delivery）
DHCP	动态主机配置协议（Dynamic Host Configuration Protocol）
DNS	域名系统（Domain Name System）
EDCA	增强的分布式信道访问（Enhanced Distributed Channel Access）
ID	身份标识号码（Identity Document）
LAN	局域网（Local Area Network）
MIB	管理信息库（Management Information Base）
MU-MIMO	多用户多入多出技术（Multi-User Multiple-Input Multiple-Output）
OFDMA	正交频分多址（Orthogonal Frequency Division Multiple Access）
PoE	以太网供电（Power over Ethernet）
PSK	预共享密钥（Pre-Shared Key）
PVID	端口的虚拟局域网标识号（Port-base VLAN ID）
SAE	对等实体同时验证（Simultaneous Authentication of Equals）
SNMP	简单网络管理协议（Simple Network Management Protocol）
SSID	服务集标识符（Service Set Identifier）
TKIP	临时密钥完整性协议（Temporal Key Integrity Protocol）

缩略语	全称
TXOP	传输机会（Transmission Opportunity）
VLAN	虚拟局域网（Virtual Local Area Network）
WEP	有线等效加密（Wired Equivalent Privacy）
WMM	无线多媒体（Wi-Fi multi-media）
WPA	WiFi 网络安全接入（Wi-Fi Protected Access）