无线 AP

操作手册

关于本产品

本手册描述的产品仅供中国大陆地区销售和使用。本产品只能在购买地所在国家或地区享受售后服务及维保方案。

关于本手册

本手册仅作为相关产品的指导说明，可能与实际产品存在差异，请以实物为准。因产品版本升级或其他需要，海康威视可能对本手册进行更新，如您需要最新版手册，请您登录海康威视官网查阅（www.hikvision.com）。

海康威视建议您在专业人员的指导下使用本手册。

商标声明

- HIKVISION 海康威视为海康威视的注册商标。
- 本手册涉及的其他商标由其所有人各自拥有。

责任声明

- 在法律允许的最大范围内，本手册以及所描述的产品（包含其硬件、软件、固件等）均“按照现状”提供，可能存在瑕疵或错误。海康威视不提供任何形式的明示或默示保证，包括但不限于适销性、质量满意度、适合特定目的等保证；亦不对使用本手册或使用海康威视产品导致的任何特殊、附带、偶然或间接的损害进行赔偿，包括但不限于商业利润损失、系统故障、数据或文档丢失产生的损失。
- 您知悉互联网的开放性特点，您将产品接入互联网可能存在网络攻击、黑客攻击、病毒感染等风险，海康威视不对因此造成的产品工作异常、信息泄露等问题承担责任，但海康威视将及时为您提供产品相关技术支持。
- 使用本产品时，请您严格遵循适用的法律法规，避免侵犯第三方权利，包括但不限于公开权、知识产权、数据权利或其他隐私权。您亦不得将本产品用于大规模杀伤性武器、生化武器、核爆炸或任何不安全的核能利用或侵犯人权的用途。
- 如本手册内容与适用的法律相冲突，则以法律规定为准。

前　言

本节内容的目的是确保用户通过本手册能够正确使用产品，以避免操作中的危险或财产损失。在使用此产品之前，请认真阅读产品手册并妥善保存以备日后参考。

资料获取

访问本公司官网（www.hikvision.com）获取说明书、应用工具和开发资料。

概述

本手册适用于以下型号的 HIKVISION 无线 AP：DS-3WA12-E、DS-3WA12-S。文中若无特别说明，产品图片以 DS-3WA12-E 为例。

符号约定

对于文档中出现的符号，说明如下所示。

符号	说明
 说明	说明类文字，表示对正文的补充和解释。
 注意	注意类文字，表示提醒用户一些重要的操作或者防范潜在的伤害和财产损失危险。
 警告	警告类文字，表示有潜在风险，如果不加避免，有可能造成伤害事故、设备损坏或业务中断。
 危险	危险类文字，表示有高度潜在风险，如果不加避免，有可能造成人员伤亡的重大危险。

目 录

第1章 登录 Web 管理页面

1.1 登录

如果您是首次使用 AP 或已将 AP 恢复出厂设置，请参考 AP 的安装手册。否则，请参考下文。用网线将管理电脑连接到 AP 或已连接 AP 的交换机。

步骤1 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”。

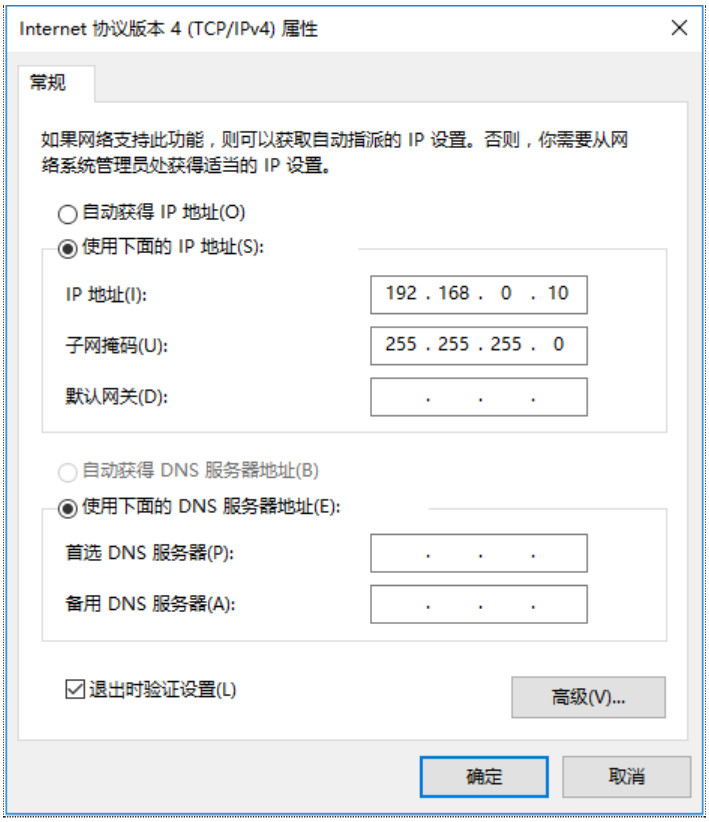


图1-1 电脑的 IP 地址

步骤2 在电脑上打开浏览器，访问 AP 的 IP 地址（默认为“192.168.0.254”）。

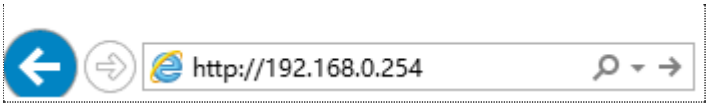


图1-2 浏览器访问

步骤3 在出现的页面设置 admin 用户的密码，然后点击 登录 。

图1-3 登录页面

说明

若未出现上述页面，请尝试使用以下办法解决：

- 如果网络中部署了 HIKVISION 无线控制器（包括支持“AP 管理”的网关路由器），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 的系统灯闪烁状态下，使用针状物按住 AP 的 Reset 按钮约 8 秒，待系统灯长亮时松开，当系统灯重新闪烁时，恢复出厂设置成功。

成功登录到 AP 的管理页面，您可以开始配置 AP 了。

图1-4 AP 的管理页面

1.2 退出登录

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。此外，您也可以点击管理页面右上角的 退出 ，安全地退出管理页面。

第2章 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。

图2-1 系统状态

说明

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。

表2-1 页面布局说明

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。

表2-2 常用元素

常用元素	说明
刷新	用于刷新当前页面内容。
保存	用于保存当前页面配置，并使配置生效。
取消	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

第3章 快速设置

通过「快速设置」模块，您可以快速设置 AP，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 支持两种工作模式：AP 模式、Client+AP 模式。

3.1 AP 模式

3.1.1 概述

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。

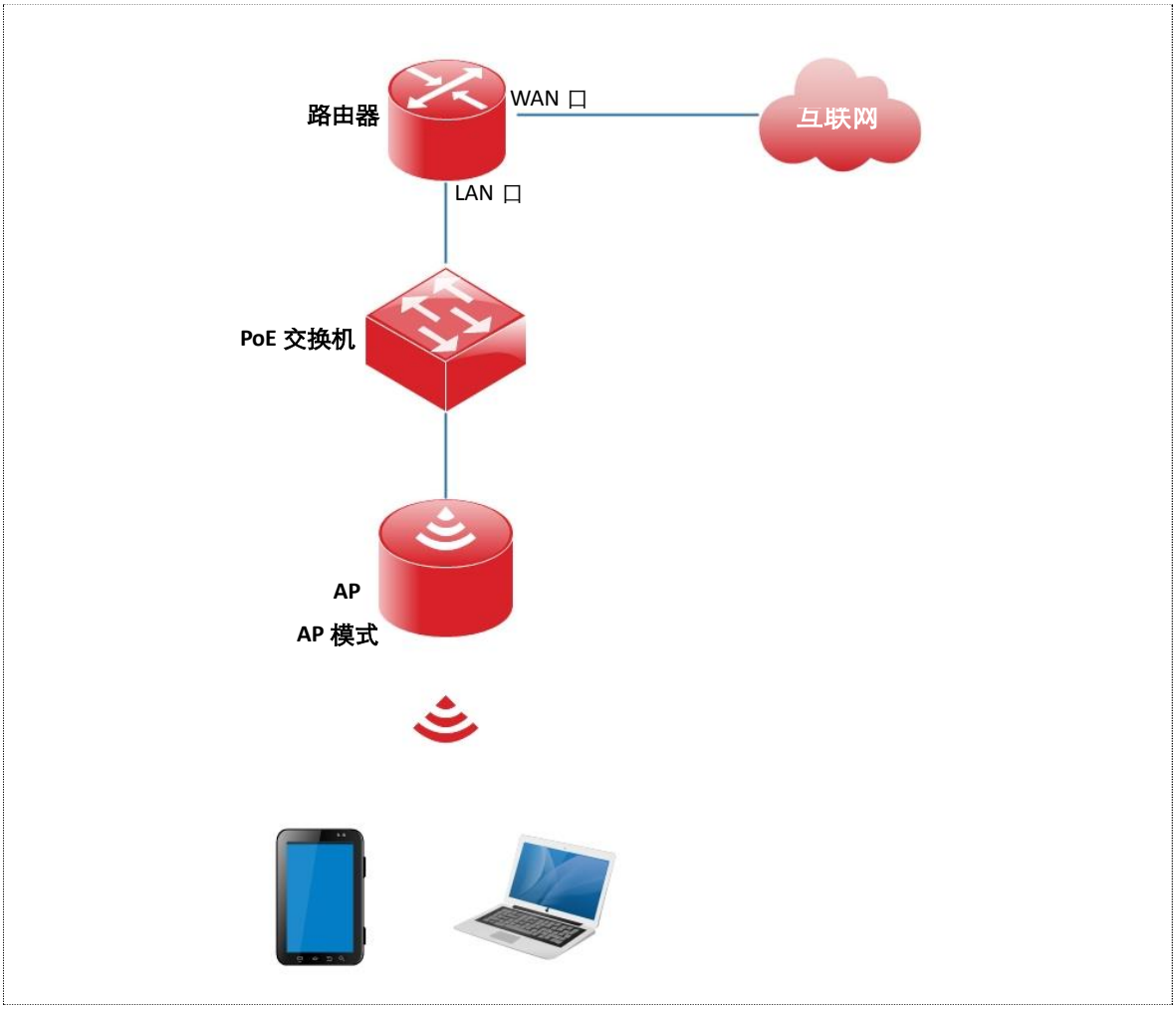


图3-1 AP 模式

3.1.2 设置 AP 模式

说明

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 选择“工作模式”为“AP 模式”。

步骤4 点击“SSID”输入框，设置无线名称（主 SSID）。

步骤5 选择无线网络的安全模式，并设置其展开参数。

步骤6 点击 保存 。

图3-2 AP 模式

步骤7 如果还需要设置另一频段的无线网络，重新进行步骤 2-6。

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。

表3-1 AP 模式的参数说明

标题项	说明
无线频段	选择要设置的无线频段。
工作模式	选择“AP 模式”，将现有的有线网络转换成无线网络。
SSID	点击可修改所选频段下主网络的无线名称。
安全模式	选择对应无线网络的安全模式。AP 支持如下几种安全模式。 ● 不加密：无线网络不加密，允许任意无线客户端接入。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。 ● WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK：WPA 预共享密钥认证，用户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，适合个人或家庭用户用于保证无线安全。Mixed WPA/WPA2-PSK 表示 AP 同时兼容 WPA-PSK、WPA2-PSK 两种安全模式。 ● WPA、WPA2：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，数据加密密钥由 AP 基于加密规则 TKIP 或 AE 来自动生成，适合企业等高安全要求的无线网络使用。

3.2 Client+AP 模式

3.2.1 概述

Client+AP 模式下，AP 通过无线桥接上级设备（无线路由器、AP 等）的无线网络，扩展无线网络覆盖范围。应用拓扑图如下。

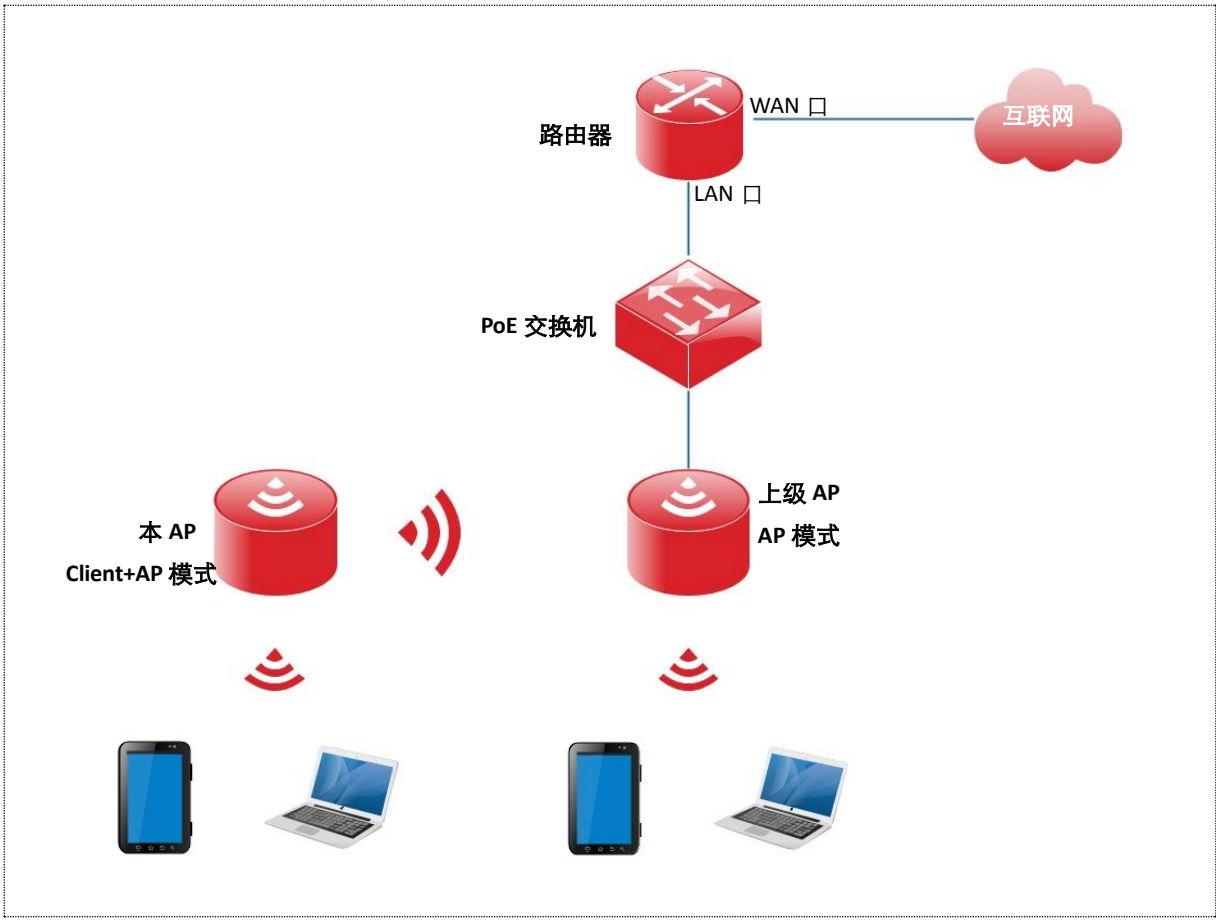


图3-3 Client+AP 模式

3.2.2 设置 Client+AP 模式

注意

设置之前，请确保上级 AP 已经联网成功。

步骤1 点击「快速设置」。

步骤2 选择要桥接的无线网络所在的频段，如“2.4GHz”。

步骤3 选择“工作模式”为“Client+AP 模式”。

步骤4 点击 扫描 。

图3-4 Client+AP 模式

步骤5 在出现的无线网络列表中，选择要扩展的无线网络。

说明

- 如果扫描不到无线网络，请进入「无线设置」>「射频设置」页面，确认您已开启无线，然后重新尝试。
- 选择无线网络后，AP 会自动填写所选择无线网络的 SSID，安全模式、信道。您只需手动填写“密钥”参数。

选择	SSID	MAC地址	信道带宽	信道	安全模式	信号强度
◉	HIKVISION_21A54	D8:38:0D:A8:8B:09	20MHz	6	Mixed WPA/WPA2-PSK...	
○	HIKVISION_21AC8	C8:3A:35:23:08:69	20MHz	1	WPA2-PSK/AES	
○	HIKVISION_A5A54	D8:38:0D:94:8E:C1	20MHz	3	不加密	

图3-5 无线网络列表

步骤6 点击 关闭扫描 。

步骤7 如果上级无线网络已加密，请填入对应的“密钥”。

步骤8 点击 保存 。

图3-6 Client+AP 模式参数设置

使用智能手机等无线设备搜索并连接 AP 的 SSID，输入无线密码（密钥），即可上网。

说明

登录到 AP 管理页面后，进入「无线设置」>「基本设置」页面，可查看 AP 的 SSID 和密钥。

表3-2 Client+AP 模式的参数说明

标题项	说明
无线频段	选择要设置的无线频段。
工作模式	选择 Client+AP 模式，桥接上级无线网络。
SSID	要桥接的网络的无线名称（SSID）。通过扫描选择时，会自动填充，无需手动设置。
安全模式	被桥接无线网络使用的安全模式。通过扫描选择时，会自动填充，无需手动设置。 AP 可以支持桥接如下安全模式的无线网络。 ● 不加密：无线网络不加密，允许任意无线客户端接入。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。 ● WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK：WPA 预共享密钥认证，用户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，适合个人或家庭用户用于保证无线安全。Mixed WPA/WPA2-PSK 表示 AP 同时兼容 WPA-PSK、WPA2-PSK 两种安全模式。 **说明** ● 如果待桥接的无线网络使用 WEP 安全模式时，需手动输入认证类型、默认密钥和密钥 x（x 为 1-4）。 ● 如果待桥接的无线网络使用 WPA-PSK、WPA2-PSK 和 Mixed WPA/WPA2-PSK 安全模式时，系统会自动填入加密规则，您只需手动输入密钥即可。

第4章 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。

图4-1 系统状态

表4-1 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。
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。

图4-2 无线状态

表4-2 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	显示 AP 对应频段所有的无线网络名称。
	MAC 地址	SSID 对应的物理地址。
	启用状态	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）
HIKVISION_21A54...	0.11MB	640	1.65MB	6633
HIKVISION_21A54...	0.00MB	0	0.00MB	0
HIKVISION_21A54...	0.00MB	0	0.00MB	0
HIKVISION_21A54...	0.00MB	0	0.00MB	0
HIKVISION_21A54...	0.00MB	0	0.00MB	0
HIKVISION_21A54...	0.00MB	0	0.00MB	0
HIKVISION_21A54...	0.00MB	0	0.00MB	0
HIKVISION_21A54...	0.00MB	0	0.00MB	0

图4-3 报文统计

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，还可以将已连接的客户端添加到黑名单。

序号	MAC地址	IP地址	终端类型	连接时间	发送速率	接收速率	加入黑名单
1	88:F8:72:62:54:E0	192.168.10.65	--	00:03:47	13Mbps	6Mbps	
2	46:2A:2A:56:07:C5	192.168.10.66	--	00:03:45	0Mbps	1Mbps	

图4-4 客户端列表

表4-3 参数说明

标题项	说明
SSID	要查看无线客户端连接情况的 SSID。
MAC 地址	无线客户端的 MAC 地址。
IP 地址	无线客户端的 IP 地址。
终端类型	无线客户端的操作系统类型。 **说明** 只有当 AP 开启了终端类型识别且终端访问过 HTTP 网站后，AP 才能识别该终端的操作系统类型。
连接时间	无线客户端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。
加入黑名单	点击，系统断开与无线客户端的连接，并将该客户端移入访问控制的黑名单中。

4.5 设备信息

在「状态」>「设备信息」页面中，您可以查看设备及软件的相关信息。


设备信息
设备名称 DS-3WA12-E
设备型号 DS-3WA12-E
设备序列号
固件版本号 V1.0.3 build 200714
设备MAC地址 C8:5A:35:21:A5:40
设备二维码:
扫一扫，添加设备

图4-5 设备信息

第5章 网络设置

5.1 LAN 口设置

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。

图5-1 LAN 口设置

表5-1 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。 **说明** **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。**
IP 地址	AP 的 IP 地址，也是 AP 的管理 IP 地址，局域网用户可使用该 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 背面网线接口的驱动模式。 ● 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 背面网线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 背面网线接口无法正常收发数据。

5.2 DHCP 服务器

5.2.1 概述

本 AP 提供了 DHCP 服务器，可以为局域网中的设备自动分配 IP 地址信息。本功能默认禁用。

说明

修改 LAN 口设置后，如果新的 LAN 口 IP 与原 LAN 口 IP 不在同一网段，系统将自动修改 AP 的 DHCP 地址池，使其和新的 LAN 口 IP 在同一网段。

5.2.2 配置 DHCP 服务器

步骤1 点击「网络设置」>「DHCP 服务器」>「DHCP 服务器」。

步骤2 点击滑块至  。

步骤3 配置各项参数（一般仅需修改“网关地址”、“首选 DNS”）。

步骤4 点击 保存 。

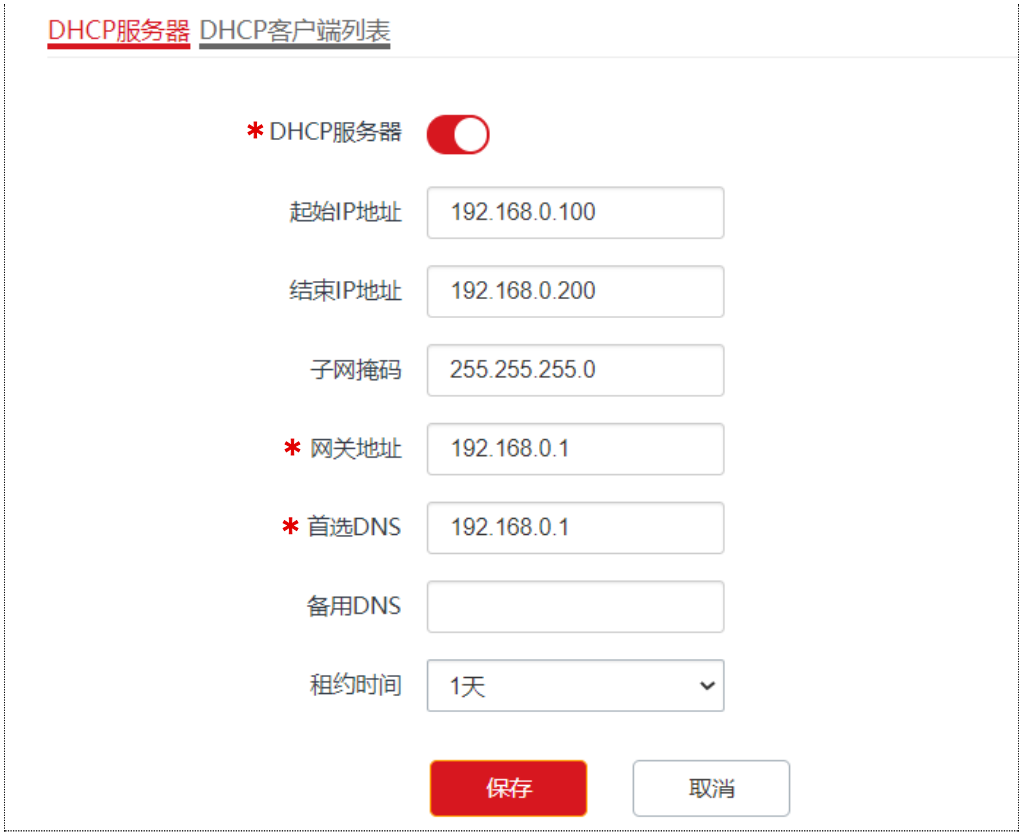


图5-2 DHCP 服务器

注意

如果网络中有其它 DHCP 服务器，为避免地址分配冲突，请确保 AP 的 DHCP 地址池和其它 DHCP 服务器的 DHCP 地址池没有重合。

表5-2 参数说明

标题项	说明
DHCP 服务器	启用/禁用 AP 的 DHCP 服务器功能。
IP 池开始地址	DHCP 服务器可分配的 IP 地址范围。起始 IP 地址默认为 192.168.0.100，结束 IP 地址默认为 192.168.0.200。
IP 池结束地址	
子网掩码	DHCP 服务器分配给客户端的子网掩码。
网关地址	DHCP 服务器分配给客户端的默认网关 IP 地址，一般为网络中路由器的 LAN 口 IP 地址。 **说明** 客户端访问本网段以外的服务器或主机时，数据必须通过网关进行转发。
首选 DNS 服务器	DHCP 服务器分配给客户端的首选 DNS 服务器 IP 地址。默认为 8.8.8.8。 **说明** 为了使局域网设备能够正常上网，请务必确保首选 DNS 是正确的 DNS 服务器或 DNS 代理的 IP 地址。
备用 DNS 服务器	DHCP 服务器分配给客户端的备用 DNS 服务器地址。此项可不填，表示 DHCP 服务器不分配此项。
租约时间	DHCP 服务器所分配给客户端的 IP 地址的有效时间。 当租约到达一半时，客户端会向 DHCP 服务器发送一个 DHCP Request，请求更新自己的租约。如果续约成功，则在续约申请的时间基础上续租；如果续约失败，则到了租期的 7/8 时，再重复一次续约过程。如果成功，则在续约申请的时间基础上续租，如果仍然失败，则租约到期后，客户端需要重新申请 IP 地址信息。 如无特殊需要，建议保持默认设置“1 天”。

5.2.3 查看 DHCP 客户端

在「网络设置」>「DHCP 服务器」>「DHCP 客户端列表」页面，您可以查看从本 AP 获取 IP 地址的设备的主机名称，IP 地址等信息。

图5-3 DHCP 客户端列表

如果要查看最新的 DHCP 客户端列表信息，请点击 刷新 。

5.3 高级设置

在「网络设置」>「高级设置」页面中，您可以设置平台接入方式、接入服务器 IP 及操作码。

图5-4 高级设置

表5-3 参数说明

标题项	说明
启用	勾选后，设备会接入萤石云平台。启用之前，请确保设备已经接入互联网。
平台接入方式	当前版本仅支持萤石云。
接入服务器 IP	萤石云平台的服务器 IP。用户也可自定义接入服务器的 IP。
连接状态	设备连接到萤石云平台的状态。
操作码	用户通过海康云管 APP 添加设备时，设备定义的验证用户对该设备具有所有权的凭证。默认初始值为验证码。用户也可以自行设置 6~12 位大小写字母和数字组合的操作码。

第6章 无线设置

6.1 SSID 设置

6.1.1 概述

AP 的「SSID 设置」模块用于配置 AP 的 SSID 相关参数。

图6-1 SSID 设置

表6-1 参数说明

标题项	说明
SSID	选择当前要设置的 SSID。 AP 的 2.4GHz 频段支持 8 个 SSID，5GHz 频段支持 4 个 SSID。对应频段下，页面显示的第一个 SSID 为该频段的主 SSID。
启用状态	所选择 SSID 的状态。 主 SSID 默认启用。其它 SSID 默认禁用，可根据需要启用。
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 SSID 的无线网络，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。
客户端隔离	启用后，连接到同一 SSID 的所有无线客户端完全隔离，只能访问 AP 连接的有线网络。适用于酒店、机场等公共热点的架设，让接入的无线用户保持隔离，提高网络安全性。
SSID 隔离	启用后，连接到设备不同 SSID 的无线客户端之间不能互相通信，可增强无线网络的安全性。
组播转单播	启用后，将组播数据流以单播的形式只转发给无线网络下组播数据的真正接收者，节省无线资源，提供可靠传输并减少延迟。
最大客户端数量	所选择 SSID 最多允许接入的无线设备数量。 若接入该 SSID 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 SSID。
SSID	点击此栏，可修改所选择的 SSID（无线网络名称）。 SSID 支持中文字符。
中文 SSID 编码格式	该 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	所选择 SSID 的安全模式。AP 支持的安全模式有：不加密、WEP、WPA-PSK、WPA2-PSK、Mixed 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。

针对不同应用环境需求，AP 提供以下安全模式：不加密、WEP、WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK、WPA、WPA2。

- 不加密

AP 的无线网络不加密，允许任意无线客户端接入。为了保障网络安全，不建议选择此项。

- WEP

WEP（有线等效加密）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。

图6-2 WEP

表6-2 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 SSID 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 SSID 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 SSID 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 SSID。
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、Mixed WPA/WPA2-PSK

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

上述 3 种安全模式都采用预共享密钥认证，其设置的密钥只用来验证身份，数据加密密钥由 AP 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 的无线用户的密钥完全相同，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。

图6-3 WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK

表6-3 参数说明

标题项	说明
安全模式	选择安全模式。 ● WPA-PSK：此时，SSID 对应的无线网络采用 WPA-PSK 安全模式。 ● WPA2-PSK：此时，SSID 对应的无线网络采用 WPA2-PSK 安全模式。 ● Mixed 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 SSID。
加密规则	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。
密钥	预共享密钥。
密钥更新周期	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。

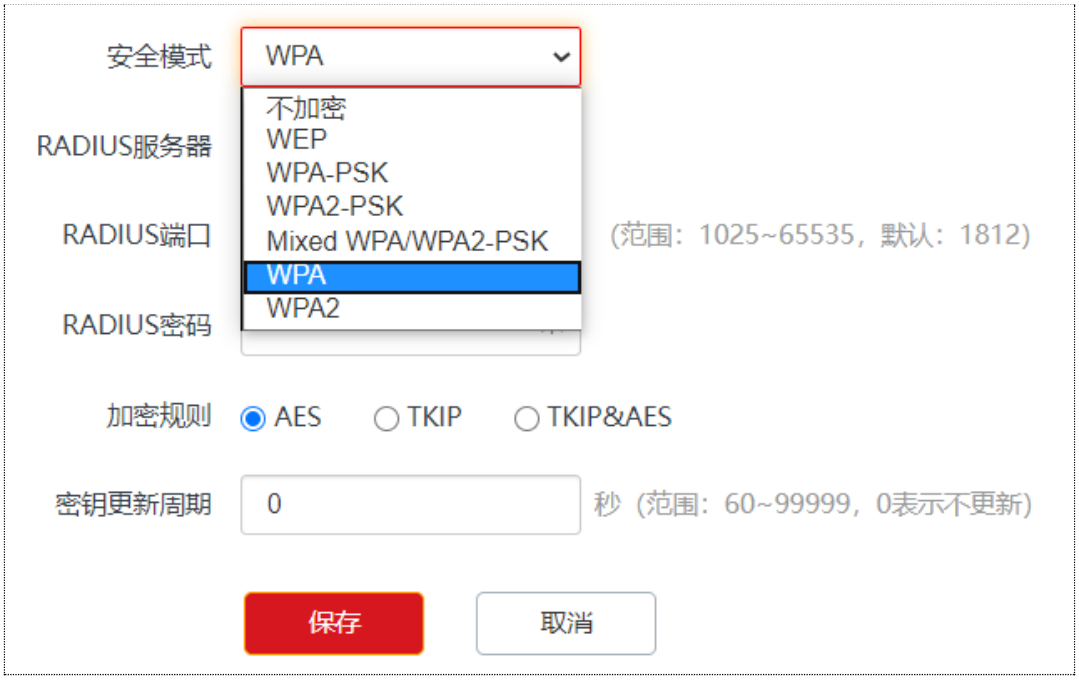


图6-4 WPA、WPA2

表6-4 参数说明

标题项	说明
安全模式	选择安全模式。 ● WPA：此时，SSID 对应的无线网络采用 WPA 企业版安全模式。 ● WPA2：此时，SSID 对应的无线网络采用 WPA2 企业版安全模式。
RADIUS 服务器	用于输入 RADIUS 服务器的 IP 地址/认证端口/共享密钥。
RADIUS 端口	
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。 ● 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

● 组网要求

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。

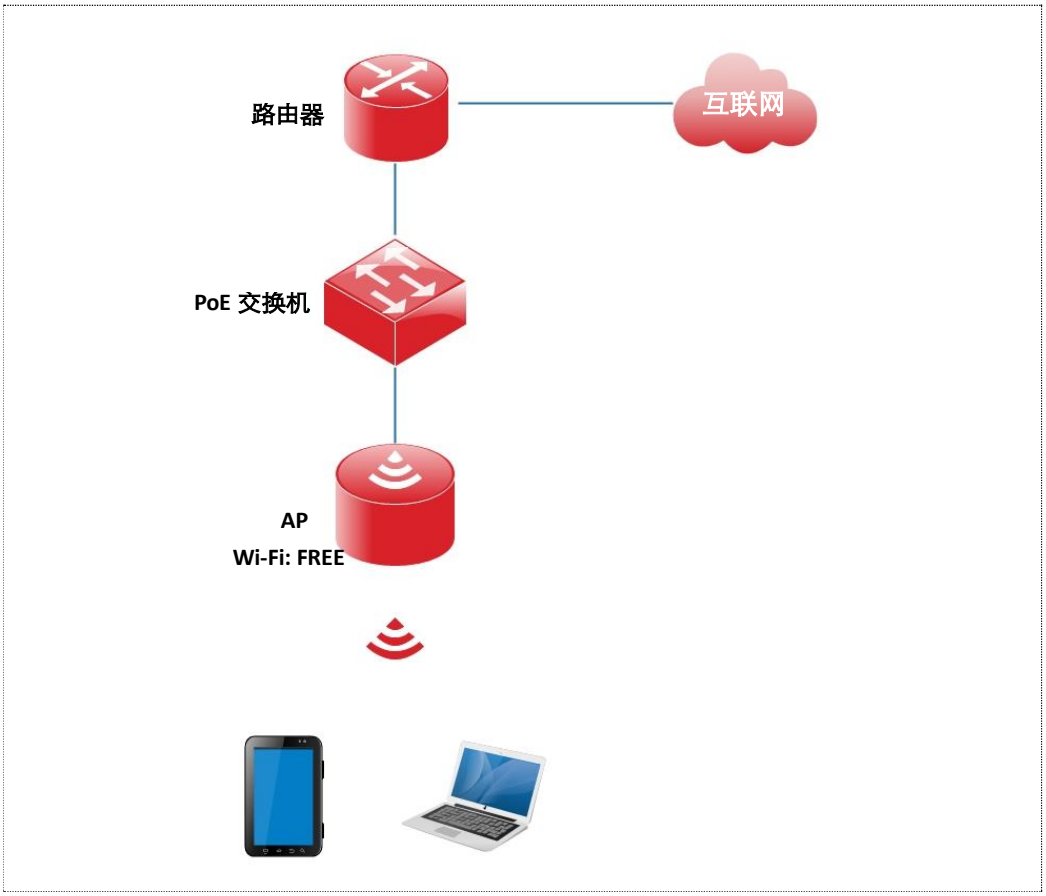


图6-5 不加密

● 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“启用状态”为“启用”。

步骤4 修改“SSID”为“FREE”。

步骤5 选择“安全模式”“不加密”。

步骤6 点击 保存 。

图6-6 SSID 设置

● 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

● 组网要求

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 Mixed WPA/WPA2-PSK 安全模式。假设：无线名称为 hotel，无线密码为 87654321，具体如下图所示。

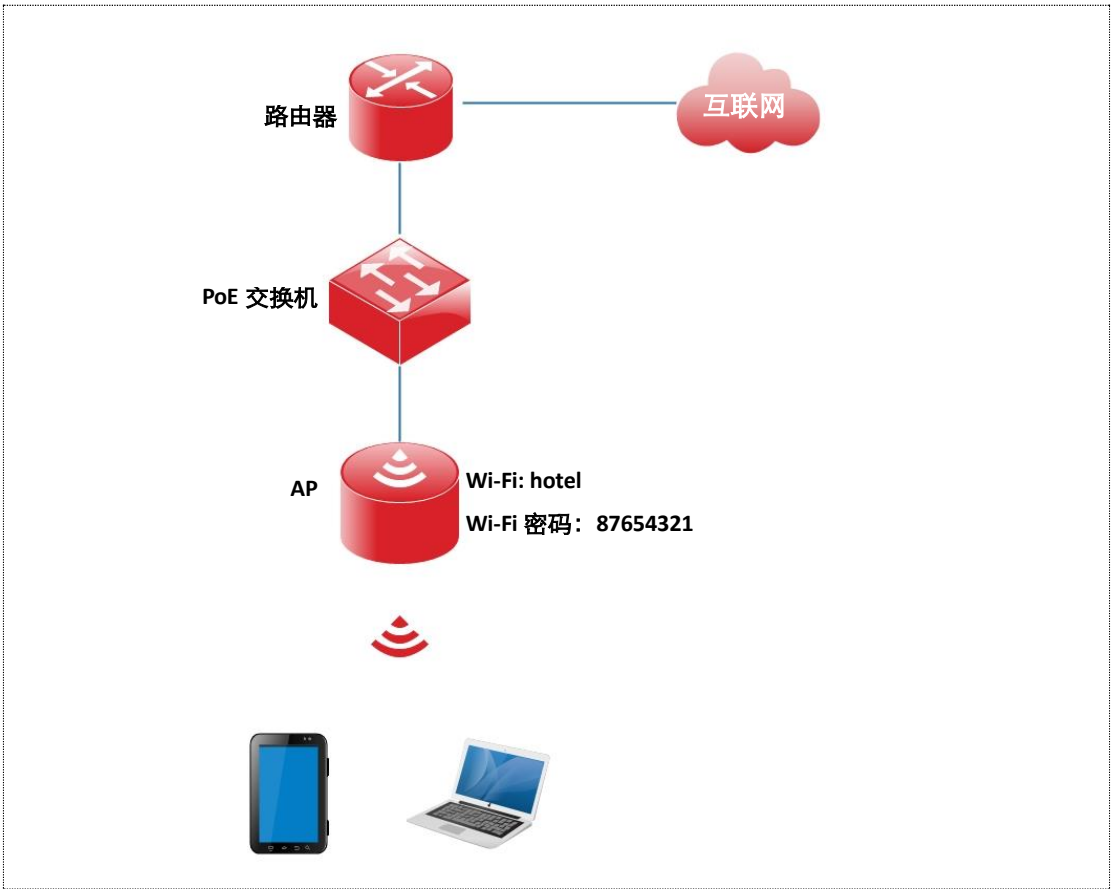


图6-7 WPA 个人加密

● 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“启用状态”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“87654321”。

步骤7 点击 保存 。

图6-8 SSID 设置

● 验证配置

无线设备连接无线网络“hotel”时，输入无线密码“87654321”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 12345678，认证端口为 1812，无线名称为 hotspot。具体如下图所示。

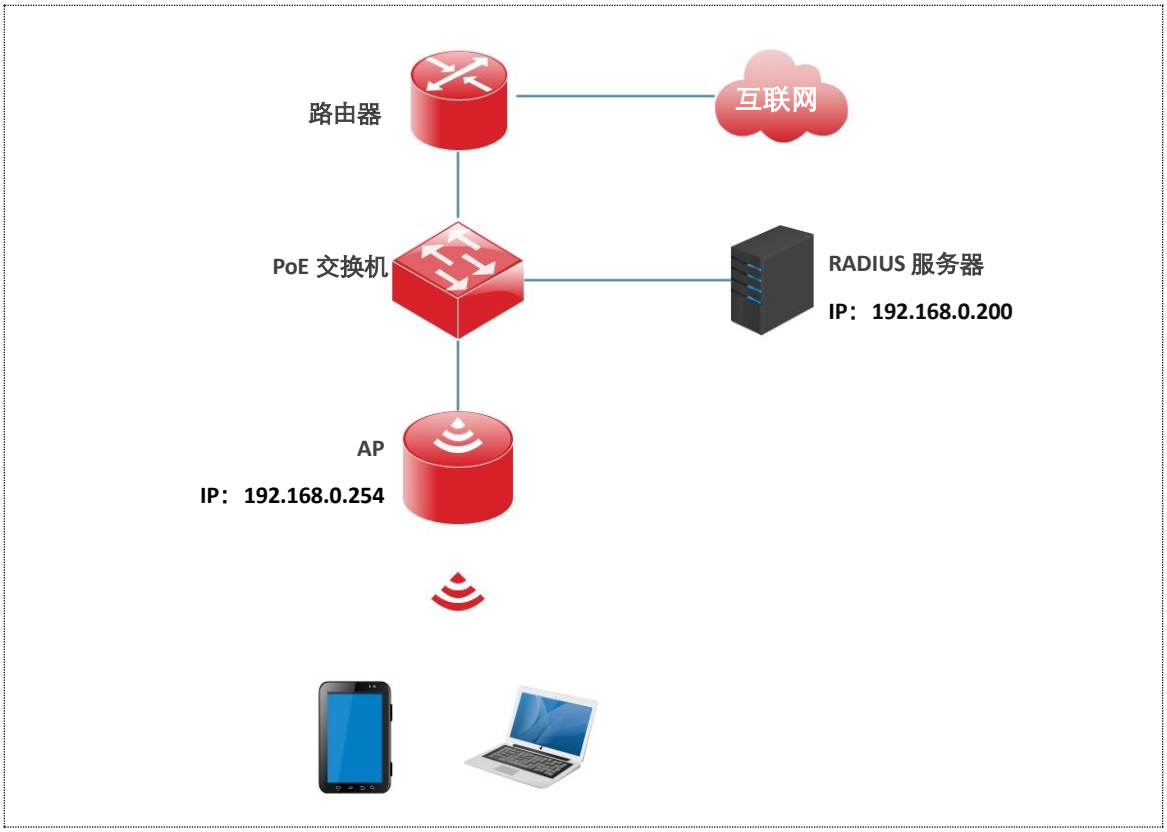


图6-9 WPA 企业加密

● 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“启用状态”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“12345678”。

步骤7 选择“加密规则”为“AES”。

步骤8 点击 保存 。

图6-10 SSID 设置

二、配置 RADIUS 服务器

说明

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”。

图6-11 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 。

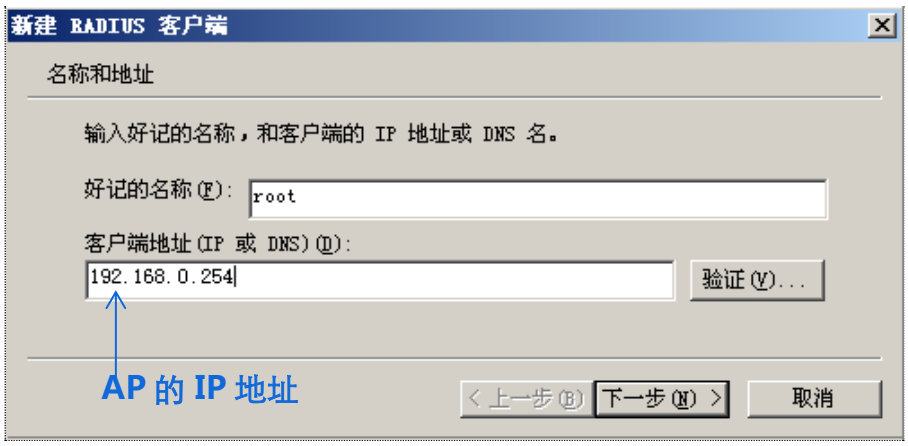


图6-12 输入 AP 的 IP 地址

3. 在“共享的机密”和“确认共享机密”栏均输入：12345678，点击 完成 。

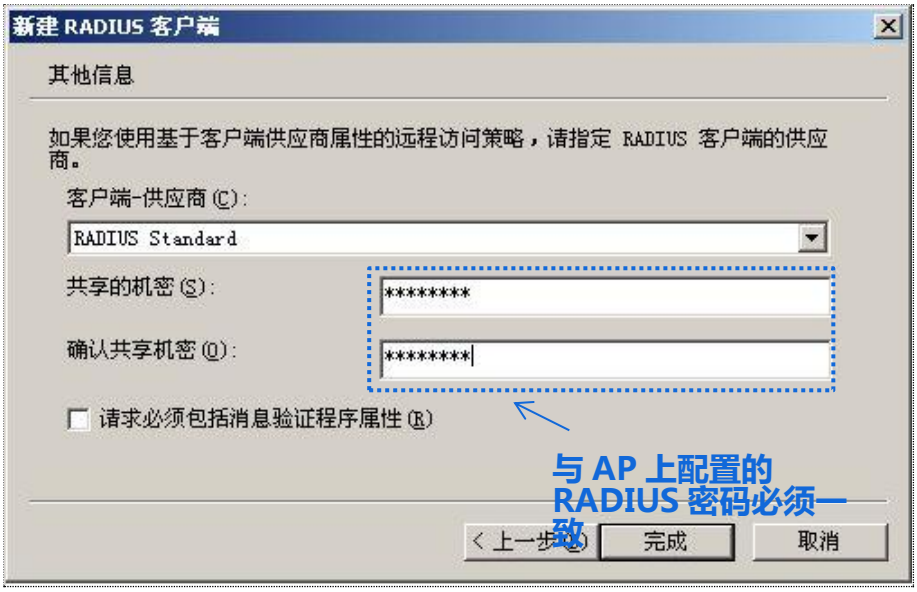


图6-13 输入 RADUIS 密码

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”。

图6-14 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 。

图6-15 新建向导

3. 设置策略名，点击 下一步 。

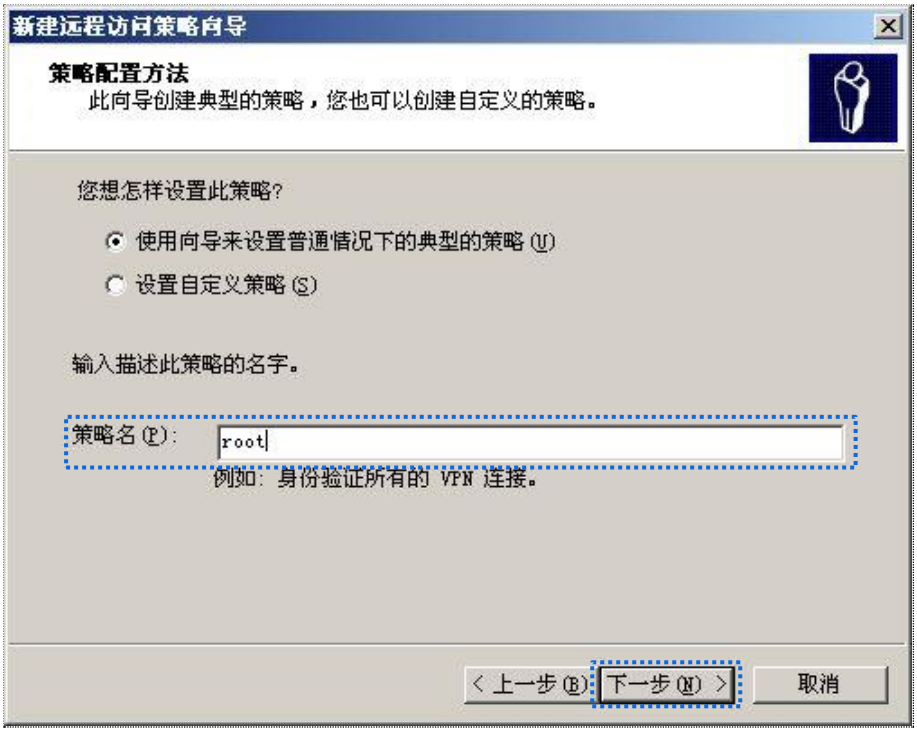


图6-16 设置策略名

4. 选择“以太网”，点击 下一步 。

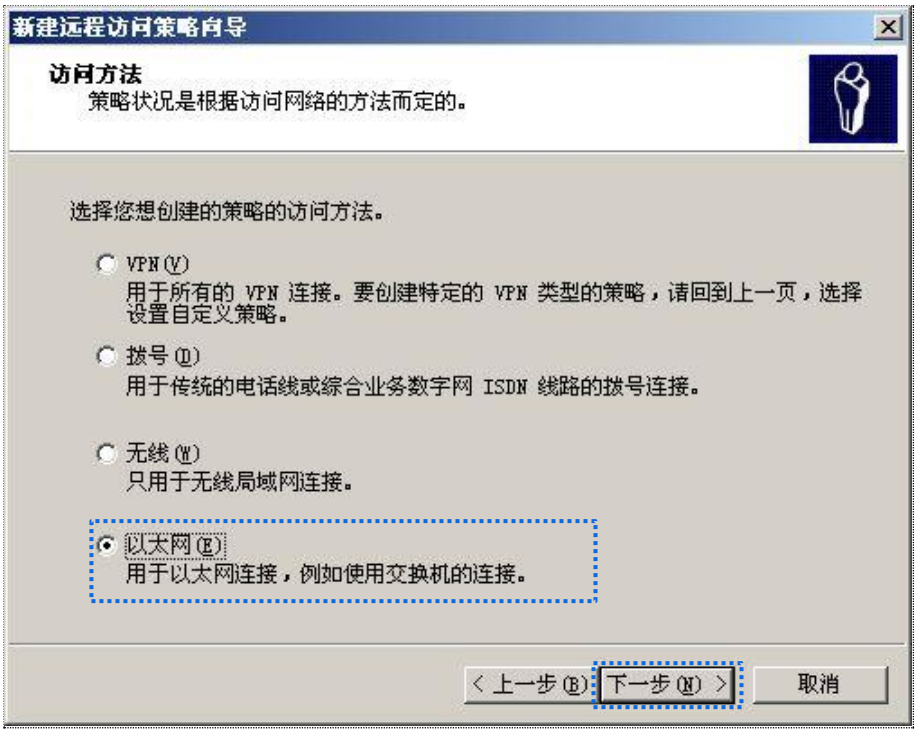


图6-17 以太网

5. 选择“组”，点击 添加 。

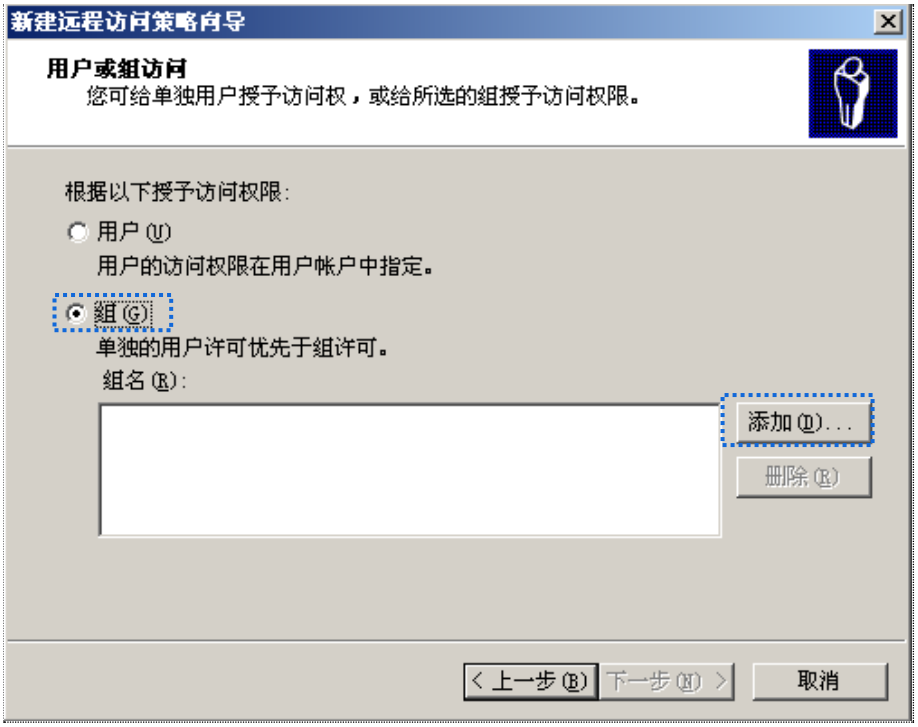


图6-18 选择组

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 。

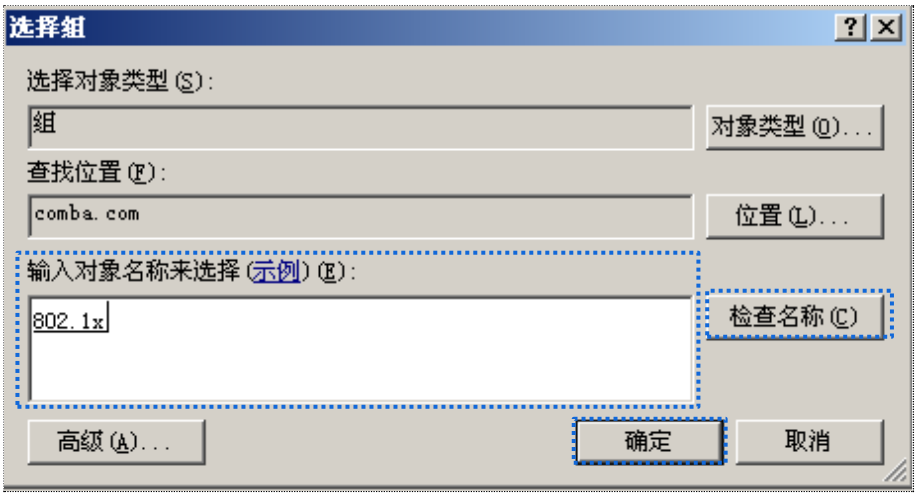


图6-19 检查 802.1x 名称

7. 选择受保护的 EAP (PEAP)，点击 下一步 。

图6-20 选择 EAP 类型

8. 点击 完成 。

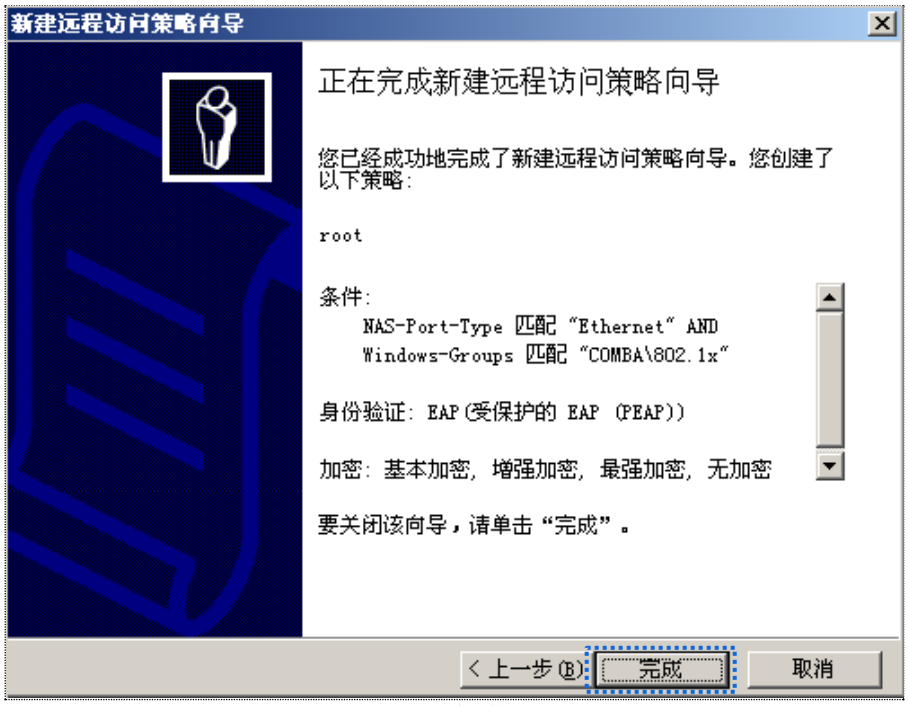


图6-21 完成向导

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 。

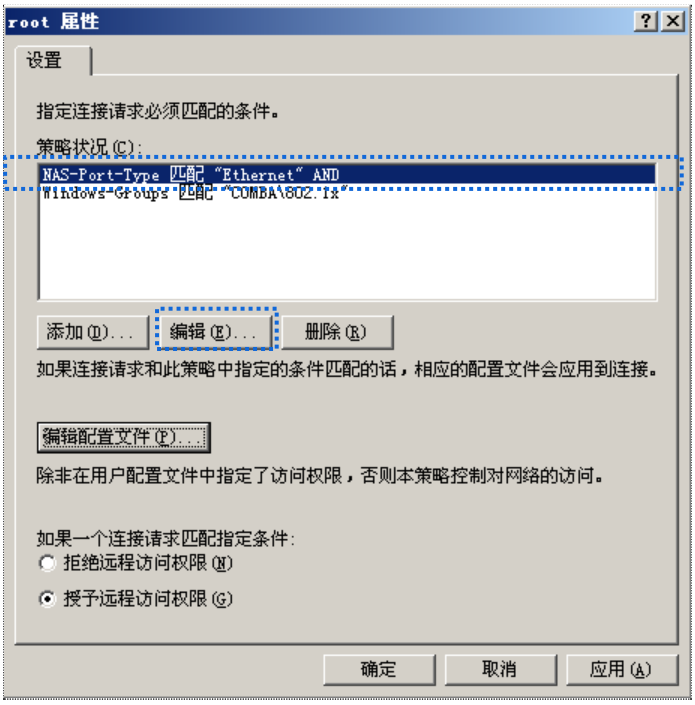


图6-22 修改属性

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

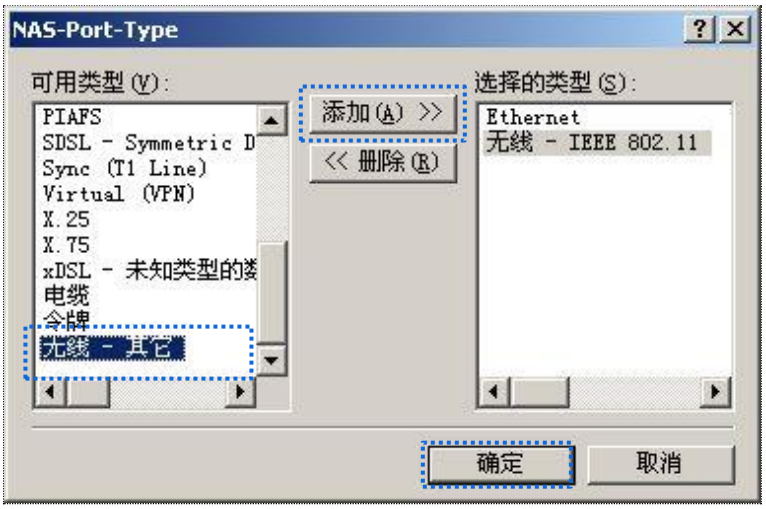


图6-23 添加选择的类型

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。

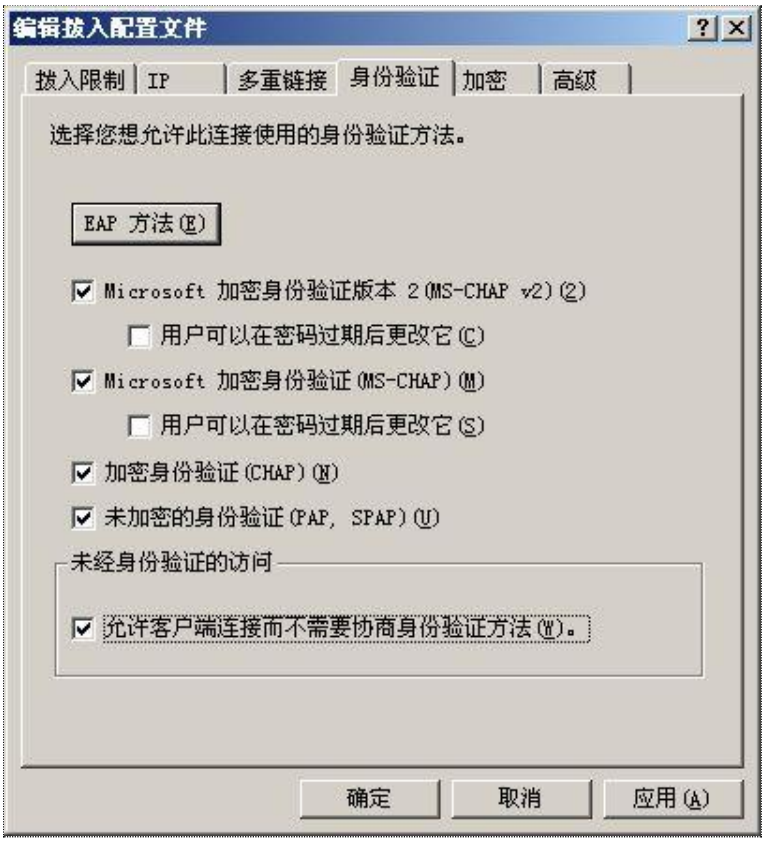


图6-24 配置身份验证

12. 在弹出的提示框，点击 否 ，确认返回。

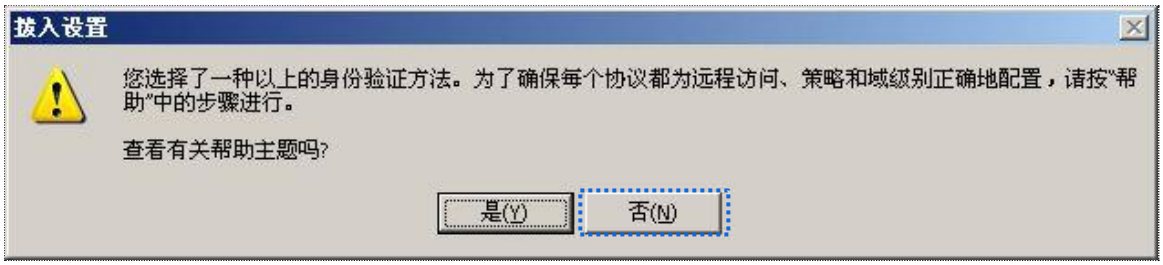


图6-25 跳过查看主题

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

说明

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”。

图6-26 进入管理无线网络

步骤2 点击“添加”。

图6-27 添加

步骤3 选择“手动创建网络配置文件（M）”。

图6-28 手动创建网络配置文件

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 。

图6-29 输入无线网络信息

步骤5 点击“更改连接设置（H）”。

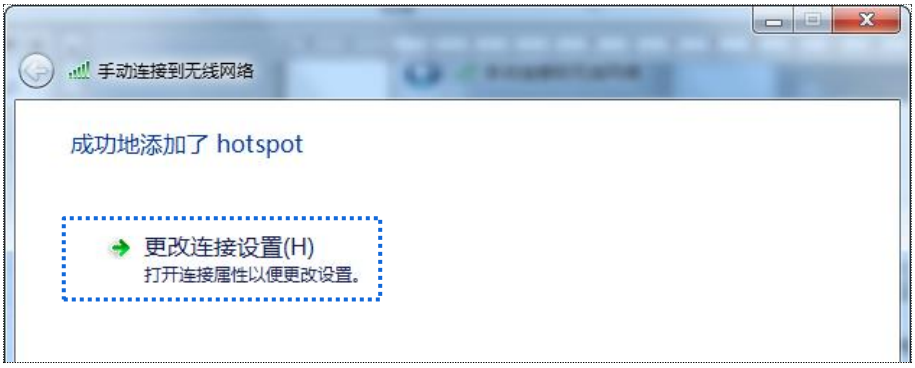


图6-30 更改连接设置

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 。

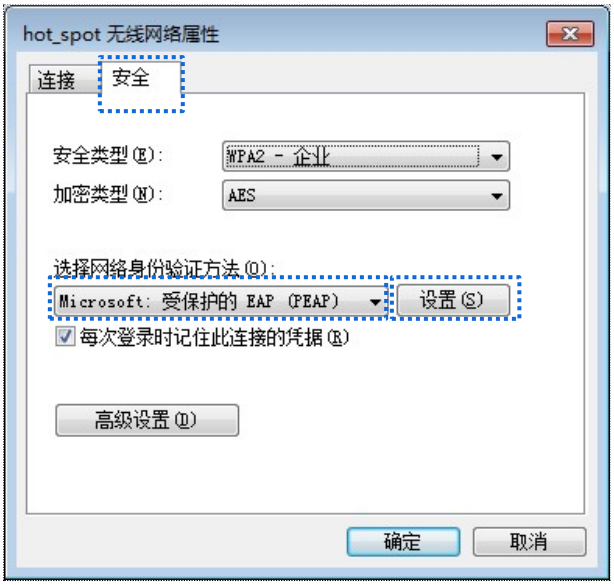


图6-31 选择网络身份验证方法

步骤7 取消勾选“验证服务器证书”，然后点击 配置 。

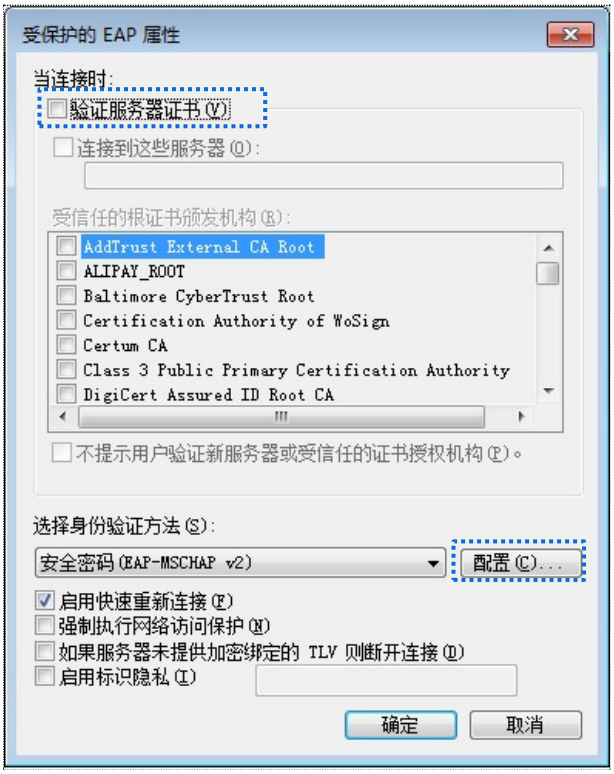


图6-32 取消验证服务器证书

步骤8 取消勾选“自动使用 Windows 登录名和密码”，点击 确定 。

图6-33 取消自动使用 Windows 登录名和密码

步骤9 点击 高级设置 。

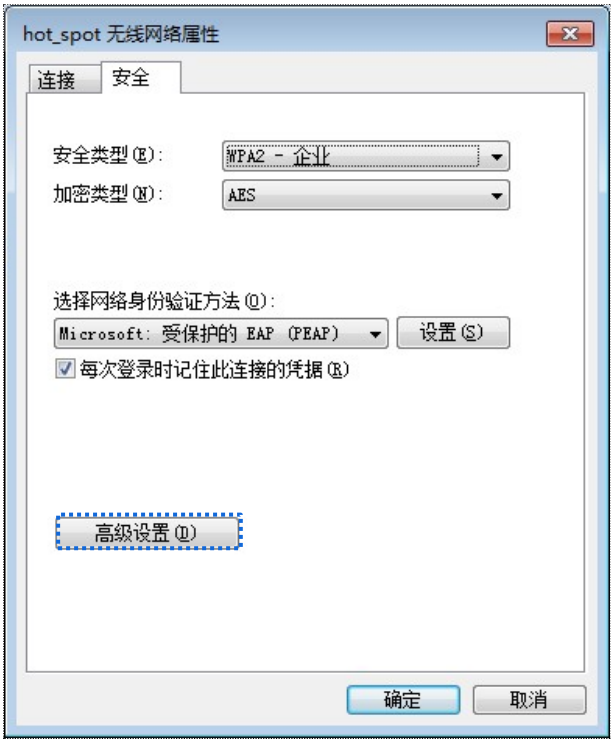


图6-34 高级设置

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 。

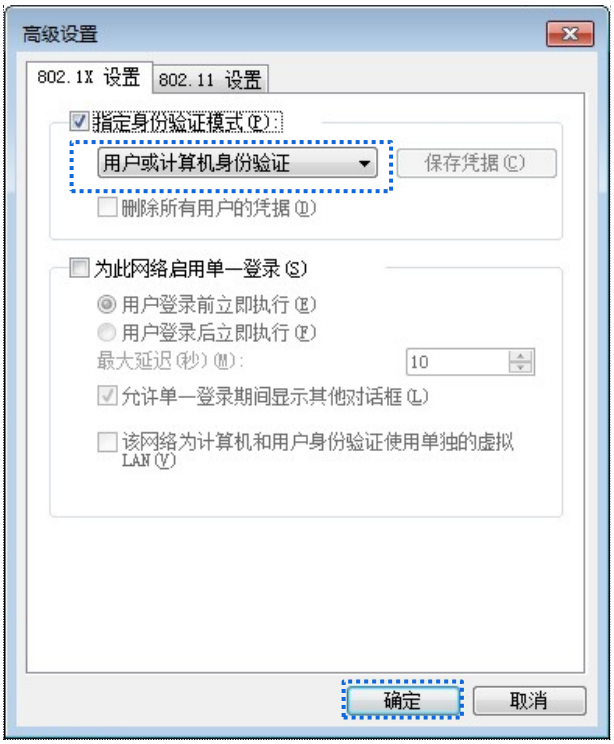


图6-35 指定身份验证模式

步骤11 点击 关闭 。

图6-36 关闭成功页

图6-37 用户设备完成

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

图6-38 连接 WiFi

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 。

图6-39 身份验证

----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。


2.4GHz射频设置
5GHz射频设置
无线网络
国家或地区
中国
网络模式
11b/g/n
信道
自动
信道带宽
20MHz
锁定信道
发射功率
低
中
高
锁定功率
无线前导码
长前导码
短前导码
Short GI
启用
禁用
探测广播报文回复抑制
启用
禁用
保存
取消

图6-40 射频设置

表6-5 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。在未勾选“锁定信道”的情况下可以设置。
网络模式	选择无线网络模式。在未勾选“锁定信道”的情况下可以设置。 2.4GHz 可选择 11b、11g、11b/g、11b/g/n，5GHz 可选择 11a、11ac、11a/n。 ● 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。 ● 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，允许工作在 5GHz 的 802.11a 和 802.11n 无线设备接入 AP 的 5GHz 无线网络。
信道	选择 AP 的工作信道。在未“锁定信道”的情况下可以设置。 “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	选择无线信道带宽。AP 工作在 11b/g/n、11ac、11a/n 模式，且未“锁定信道”的情况下可以设置。 ● 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：AP 根据周围环境，自动调整其信道带宽为 20MHz 或 40MHz。 ● 80MHz：AP 只能使用 80MHz 的信道带宽。
锁定信道	启用后，不可设置与信道相关的参数，包括国家或地区、网络模式、信道、信道带宽和扩展信道。
发射功率	设置 AP 相应频段的无线发射功率。

标题项	说明
	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。
锁定功率	启用后，将锁定该频段的当前发射功率值，使其不可更改。
无线前导码	无线前导码是位于数据包起始处的一组 bit 位，接收者可以据此同步并准备接收实际的数据。 默认为长前导码，可以兼容网络中一些比较老的客户端网卡。如果要使网络同步性能更好，可以选择短前导码。
Short GI	Short Guard Interval，短保护间隔。 无线信号在空间传输时会因多径等因素在接收侧形成时延，如果后面的数据块发送过快，会对前一个数据块形成干扰，短保护间隔可以用来规避这个干扰。使用 Short GI 时，可提高 10%的无线吞吐量。
探测广播报文回复抑制	无线设备默认都在不停的进行广播探测扫描，利用 Probe Request（探测请求）帧扫描所在区域的无线网络，Probe Request 帧包含 SSID 字段。AP 接收到该报文后会根据此来判断对方能否加入网络，并回应 Probe Response 报文（包含 Beacon 帧所有参数），消耗大量的无线资源。 启用本功能后，AP 不回复 SSID 为空的探测请求，有效节省无线资源。

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！


2.4GHz射频优化
5GHz射频优化
Beacon间隔
100
ms （范围：40~999，默认：100）
Fragment阈值
2346
（范围：256~2346，默认：2346）
RTS门限
2347
（范围：1~2347，默认：2347）
DTIM间隔
1
（范围：1~255，默认：1）
接入信号强度阈值
-90
dBm （范围：-90~-60，默认：-90）
穿墙能力
强覆盖
高密度
空口调度
启用
禁用
抗干扰模式
3（环境干扰很大时选择
（范围：0~3，默认：3）
APSD
启用
禁用
客户端老化时间
10分钟
强制速率
1 2 5.5 6 9 11 12 18 24 36 48 54
全选
支持速率
1 2 5.5 6 9 11 12 18 24 36 48 54
全选
保存
取消

图6-41 射频优化

表6-6 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。
Fragment 阈值	设置帧的分片门限值。 分片的基本原理是将一个大的帧分成更小的分片，每个分片独立地传输和确认。当帧的实际大小超过指定的分片门限值时，该帧被分片传输。 在误码率较高的环境下，可以把分片阈值适当降低，这样，如果传输失败，只有未成功发送的部分需要重新发送，从而提高帧传输的吞吐量。 在无干扰环境下，适当提高分片阈值，可以减少确认帧的次数，以提高帧传输的吞吐量。
RTS 门限	启用冲突避免（RTS/CTS）机制所要求的帧的长度门限值。单位：字节。当帧的长度超过这个门限时，使用 RTS/CTS 机制，降低发生冲突的可能性。 RTS 门限需要进行权衡后合理设置：如果设得较小，则会增加 RTS 帧的发送频率，消耗更多的带宽；但 RTS 帧发送得越频繁，无线网络从冲突中恢复得就越快。在高密度无线网络环境可以降低此门限值，以减少冲突发生的概率。 使用冲突避免机制会占用一定的网络带宽，所以只在传输高于 RTS 门限的数据帧时才使用，对于小于 RTS 门限的数据帧不启动该机制。
DTIM 间隔	DTIM（Delivery Traffic Indication Message）帧的发送间隔。单位：Beacon。 DTIM 会由此值倒数至 0，当 DTIM 计数达到 0 时，AP 才会发送缓存中的多播帧或广播帧。 例如：DTIM 间隔=1，表示每隔一个 Beacon 的时间间隔，AP 将发送所有暂时缓存的数据帧。
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。
穿墙能力	设置 AP 的穿墙能力。

标题项	说明
	● 强覆盖：常用于 AP 部署密度较低的场景，如办公室、仓库、医院等，使用此模式可以扩大 AP 的覆盖范围。 ● 高密度：常用于 AP 部署密度较高的场景，如会场、展厅、宴会厅、体育场馆、高校教室、候机厅等，使用此模式可以有效减少 AP 相互之间的干扰。
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，则让终端连接 AP 的 2.4GHz 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。
抗干扰模式	选择 AP 的抗干扰模式。 ● 0：禁用干扰抑制。 ● 1：启用弱干扰抑制，适用于环境干扰较小的场景。 ● 2：启用中等干扰抑制，适用于环境干扰较大的场景。 ● 3：启用强干扰抑制，适用于环境干扰很大的场景。
APSD	Automatic Power Save Delivery，自动省电模式。是 Wi-Fi 联盟的 WMM 省电认证协议。启用 WMM 后，开启“APSD”能降低 AP 的电能消耗。
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。
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 没有数据通信，AP 将主动断开该无线设备。
强制速率	表示 AP 强制的一组速率。对于强制速率集，无线设备必须支持，否则将无法连接到无线网络。
支持速率	表示 AP 支持的一组速率。对于支持速率集，无线设备可以支持（此时无线客户端可以在满足强制速率的前提下选择更高的速率与 AP 进行连接），也可以不支持。

● 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 频段的浪费的现象。

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。

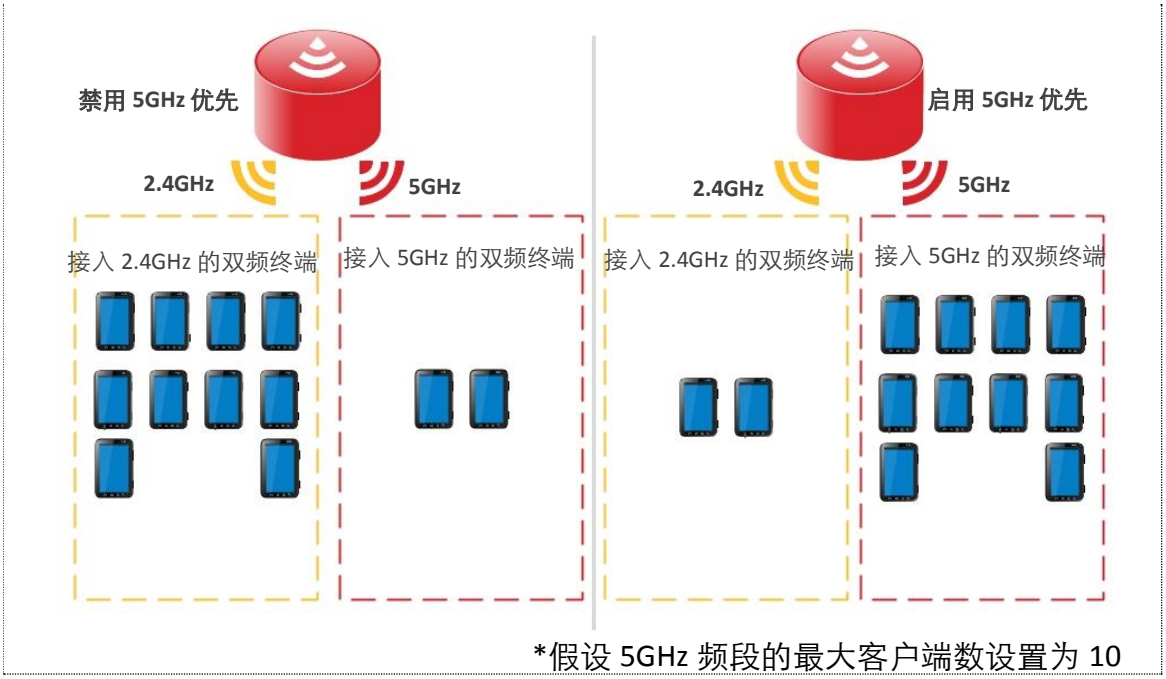


图6-42 5GHz 优先

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，却占用了更多的空口时间，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 频谱分析

在「无线设置」>「射频设置」页面，您可以进行频谱分析和信道扫描。

● 频谱分析

通过频谱分析功能，您可以查看各个信道的信号个数及信道利用率，然后选择一个利用率较低的信道来作为 AP 的工作信道，以提升无线传输效率。

信道	1	2	3	4	5	6	7	8	9	10	11	12	13
信号个数	15	4	2	8	5	14	6	5	5	7	9	3	7
信道利用率（%）	70	24	13	44	30	67	35	30	30	40	50	20	39

图6-43 频谱分析

- 信道利用率的底色为绿色，代表信道情况良好。
- 信道利用率的底色为黄色，代表信道拥挤。
- 信道利用率的底色为红色，代表信道非常拥挤，基本不可用。

● 信道扫描

通过信道扫描，您可以查看 AP 周围环境中其他无线网络的基本情况，例如 SSID、MAC、信道带宽和信号强度等信息。

序号	SSID	MAC地址	信道带宽	信道	安全模式	信号强度
1	HIKVISION_21A54	D8:38:0D:A8:8B:09	20MHz	6	Mixed WPA/WPA2-PSK...	
2	HIKVISION_21AC8	D8:38:0D:94:8E:C1	20MHz	3	WPA2-PSK/AES	

图6-44 信道扫描

6.5 WMM 设置

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，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)，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。

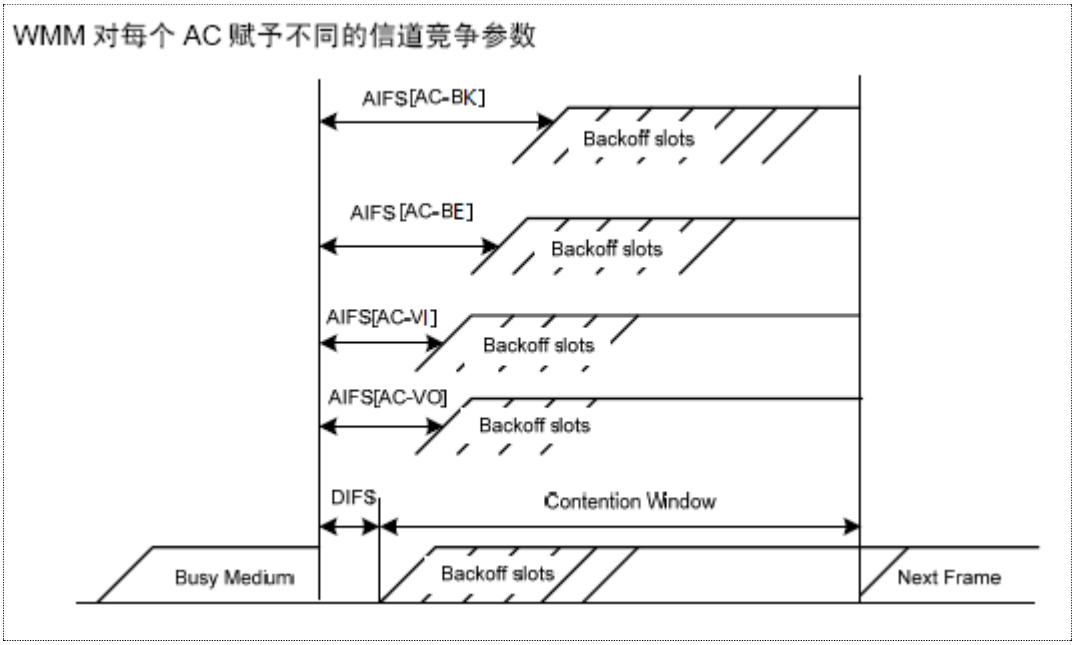


图6-45 AC 的信道竞争参数

- 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。

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

图6-46 WMM 设置

表6-7 参数说明

标题项	说明
优化模式	AP 支持以下 3 种 WMM 优化模式。 ● 一般用户场景：通常情况下，当同时接入 AP 的用户数不超过 10 人时，建议选择此优化模式，以获取更高的吞吐量。 ● 密集用户场景：通常情况下，当同时接入 AP 的用户数在 10 人以上时，建议选择此优化模式，以保障更高的用户容量。 ● 自定义：用户自定义 WMM EDCA 参数，进行精细优化。
No ACK	● 勾选复选框：表示采用 No ACK 策略。 ● 不勾选复选框：表示采用 Normal ACK 策略。
EDCA 参数	详细说明请参考 EDAC 概述内容。

6.6 访问控制

6.6.1 概述

在「无线设置」>「访问控制」页面，您通过无线访问控制功能，可以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：

- 白名单：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。
- 黑名单：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。

访问控制功能默认关闭，开启后，页面如下图所示。

图6-47 访问控制

表6-8 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。 ● 白名单：仅允许访问控制列表中的无线设备接入该 SSID。 ● 黑名单：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。
MAC 地址	客户端的 MAC 地址。

6.6.2 配置无线访问控制

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“黑名单”或“白名单”。

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 。

说明

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 。

图6-48 无线访问控制

6.6.3 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：C8:3A:35:00:00:01、C8:3A:35:00:00:02、C8:3A:35:00:00:03。

● 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“白名单”。

步骤5 在 MAC 地址输入框中，输入“C8:3A:35:00:00:01”，然后点击 添加 。重复本步骤，添加 MAC 地址“C8:3A:35:00:00:02”和“C8:3A:35:00:00:03”。

步骤6 点击 保存 。

设置完成后，页面如下图示。

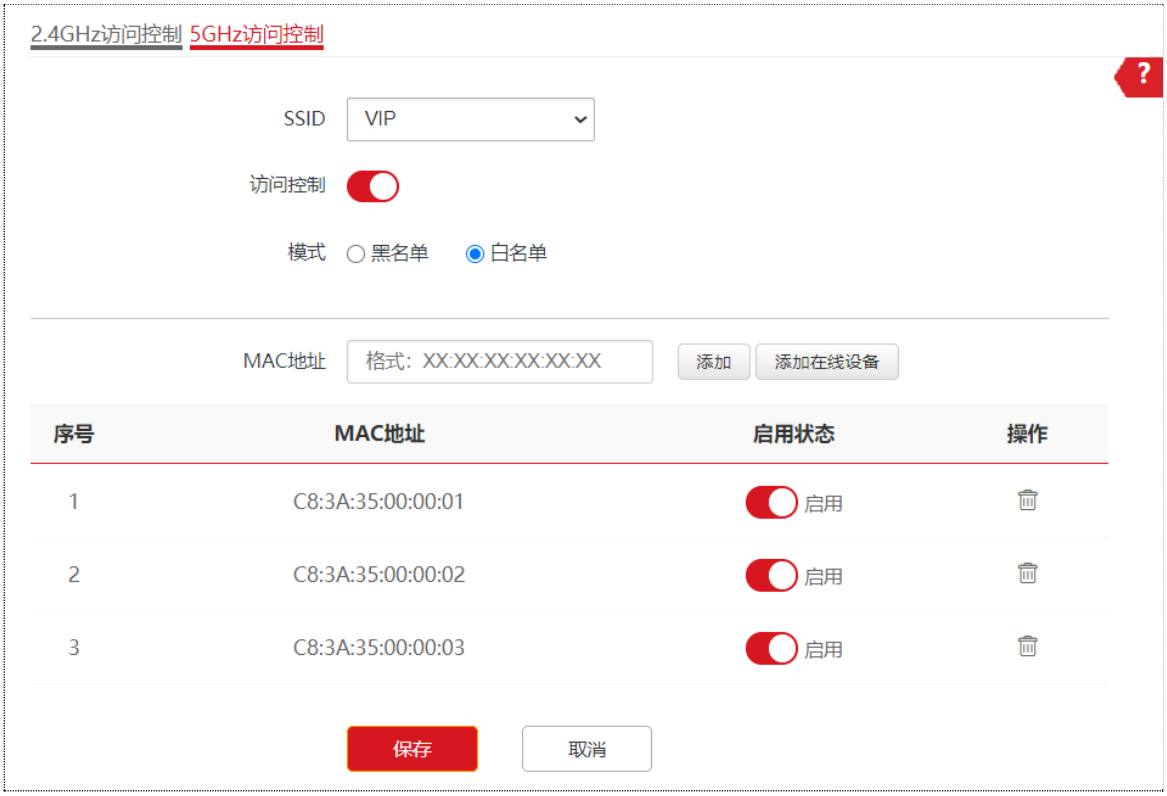


图6-49 白名单

- 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。

6.7 高级设置

在「无线设置」>「高级设置」页面中，您可以配置终端类型识别、广播报文过滤功能。

- 终端类型识别

识别接入 AP Wi-Fi 的无线设备的操作系统类型，让无线网络的管理更有效。AP 可以识别的终端类型包括：Android、iOS、WPhone、Windows、macOS。

- 广播报文过滤

默认情况下，AP 会转发很多有线网络的无效广播报文，这可能会影响正常业务数据的传递。使用广播数据过滤功能，您可以对广播报文转发进行分类过滤，减少空口资源浪费，进而保证正常业务数据的带宽。

- IPC 一键连接

开启某一 SSID 的 IPC 一键连接功能后，海康的网络摄像机可以自动连接到该无线网络。

注意

只有支持 IPC 一键连接功能的海康网络摄像机才能自动连接到无线网络。

图6-50 高级设置

表6-9 参数说明

标题项	说明
终端类型识别	启用该功能，且终端设备访问了 http 网站后，AP 可以识别终端设备的操作系统类型。可以在「状态」>「客户端列表」页面查看连接到 AP 的无线设备的操作系统类型。
广播报文过滤	启用后，AP 可以过滤广播报文，以减少空口资源浪费，从而保证正常业务数据的带宽。
过滤设置	启用“广播报文过滤”时支持。 ● 不含 DHCP 和 ARP：过滤掉除 DHCP 和 ARP 广播包以外的所有其他广播或组播数据。 ● 不含 ARP：过滤掉除 ARP 广播包以外的所有其他广播或组播数据。
IPC 一键连接	开启某一 SSID 的该功能后，海康的网络摄像机可以自动连接到该无线网络。

6.8 QVLAN 设置

6.8.1 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。

配置了 802.1Q VLAN 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：

<table>
<tr><th rowspan="2">端口链路类型</th><th colspan="2">接收数据处理</th><th rowspan="2">发送数据处理</th></tr>
<tr><th>接收 Tag 数据</th><th>接收 Untag 数据</th></tr>
<tr><td>Access</td><td rowspan="2">按Tag中的VID转发到相应 VLAN 的其他端口。</td><td rowspan="2">按该端口的 PVID 转发到相应 VLAN 的其他端口。</td><td>去掉报文的 Tag 再发送。</td></tr>
<tr><td>Trunk</td><td>VID = 端口 PVID，去掉 Tag 发送。
VID ≠ 端口 PVID，保留 Tag 发送。</td></tr>
</table>

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。

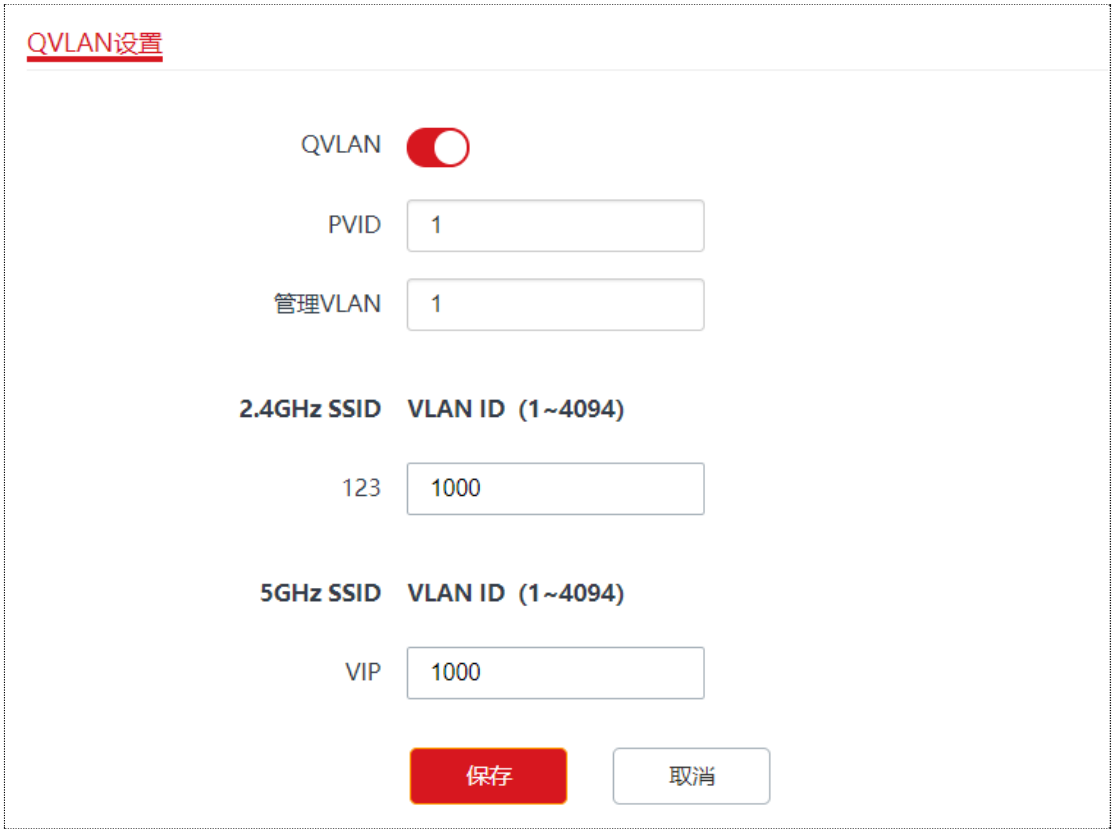


图6-51 QVLAN 设置

表6-10 参数说明

标题项	说明
QVLAN	开启/关闭 AP 的 802.1Q VLAN 功能。
PVID	AP Trunk 口默认所属的 VLAN 的 ID。启用 QVLAN 功能后，AP 的 LAN 口为 Trunk 口。Trunk 口允许所有 VLAN 通过。
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。
2.4GHz SSID	显示 AP 2.4GHz 频段当前已启用的 SSID。
5GHz SSID	显示 AP 5GHz 频段当前已启用的 SSID。
VLAN ID	SSID 对应的 VLAN ID。 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。

6.8.2 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 。

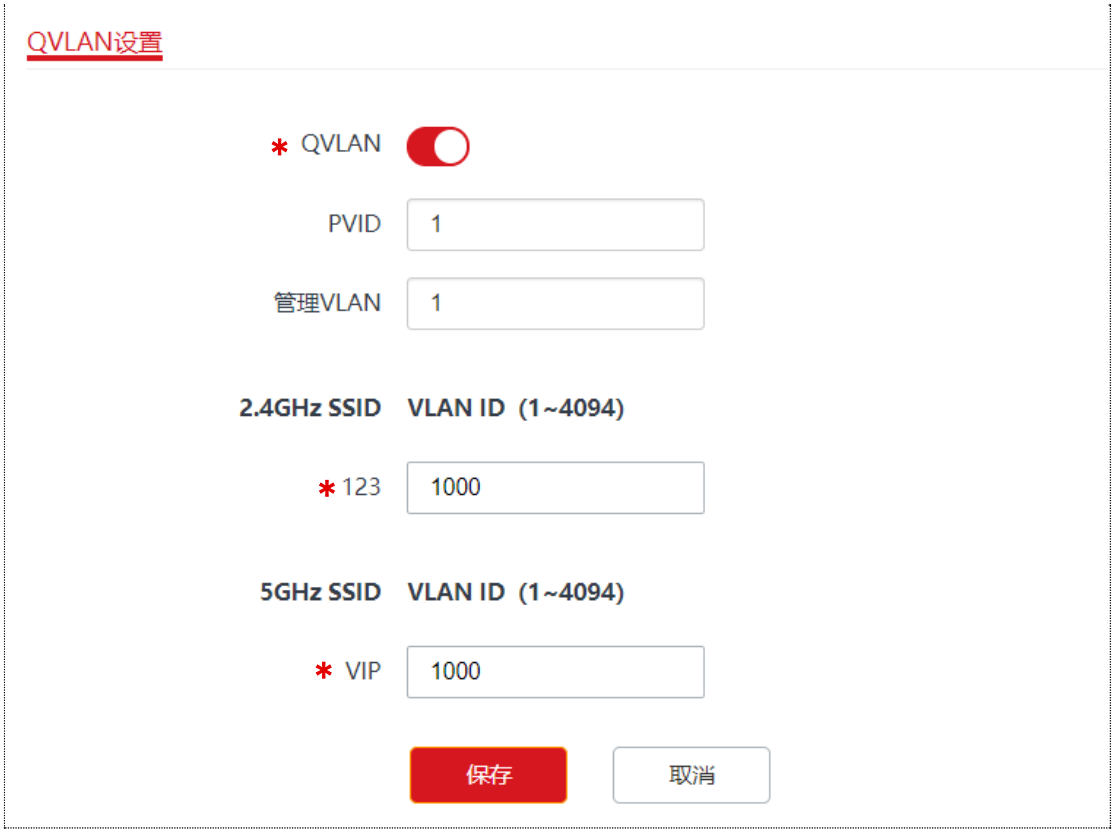


图6-52 配置 QVLAN

6.8.3 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 0 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。

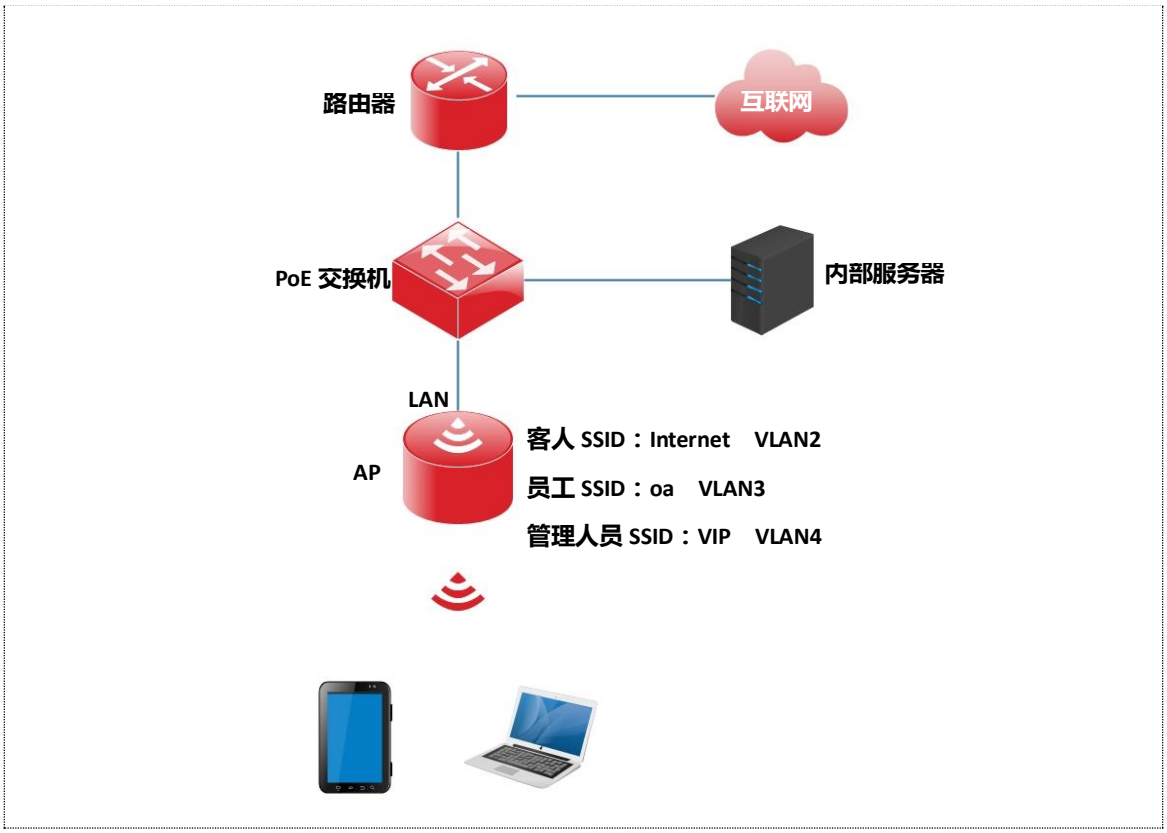


图6-53 QVLAN 配置举例

● 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 。

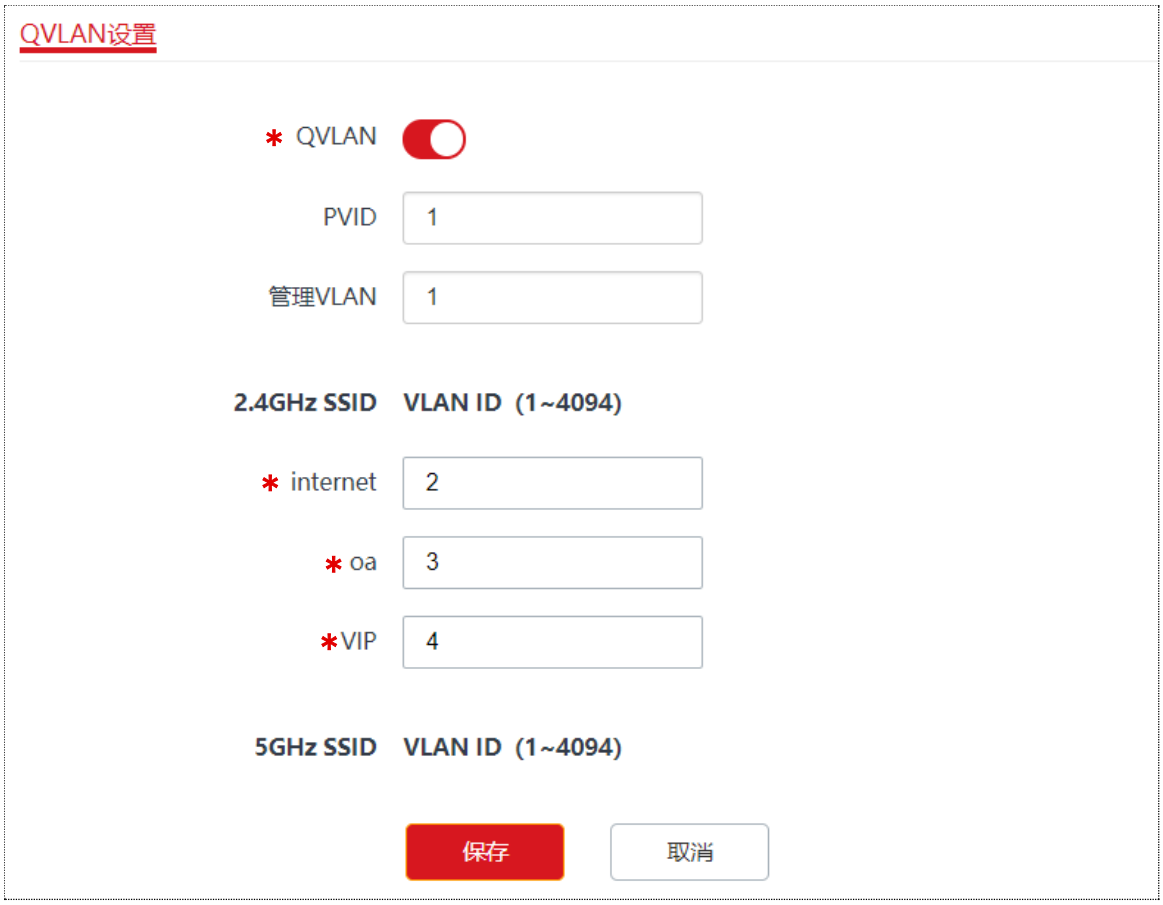


图6-54 配置 QVLAN

步骤5 确认提示信息后，点击 确定 。

二、配置交换机

在交换机上划分 IEEE 802.1Q VLAN，具体如下。

表6-11 配置交换机的 VLAN

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。

表6-12 配置路由器的 VLAN

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

表6-13 配置内部服务器的 VLAN

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。

- 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。

第7章 高级设置

7.1 部署模式

网络中需要部署大量 AP 时，推荐在网络中搭建无线控制器，实现 AP 的集中管理。

使用无线控制器集中管理 AP 时，有以下两种部署模式：本地部署、云部署（胖 AP）。

- 本地部署

当无线网络相对集中且规模较大时，建议 AP 使用“本地部署”模式，由本地网络中的无线控制器（从 AC 模式）集中管理。本地部署模式组网拓扑图如下。

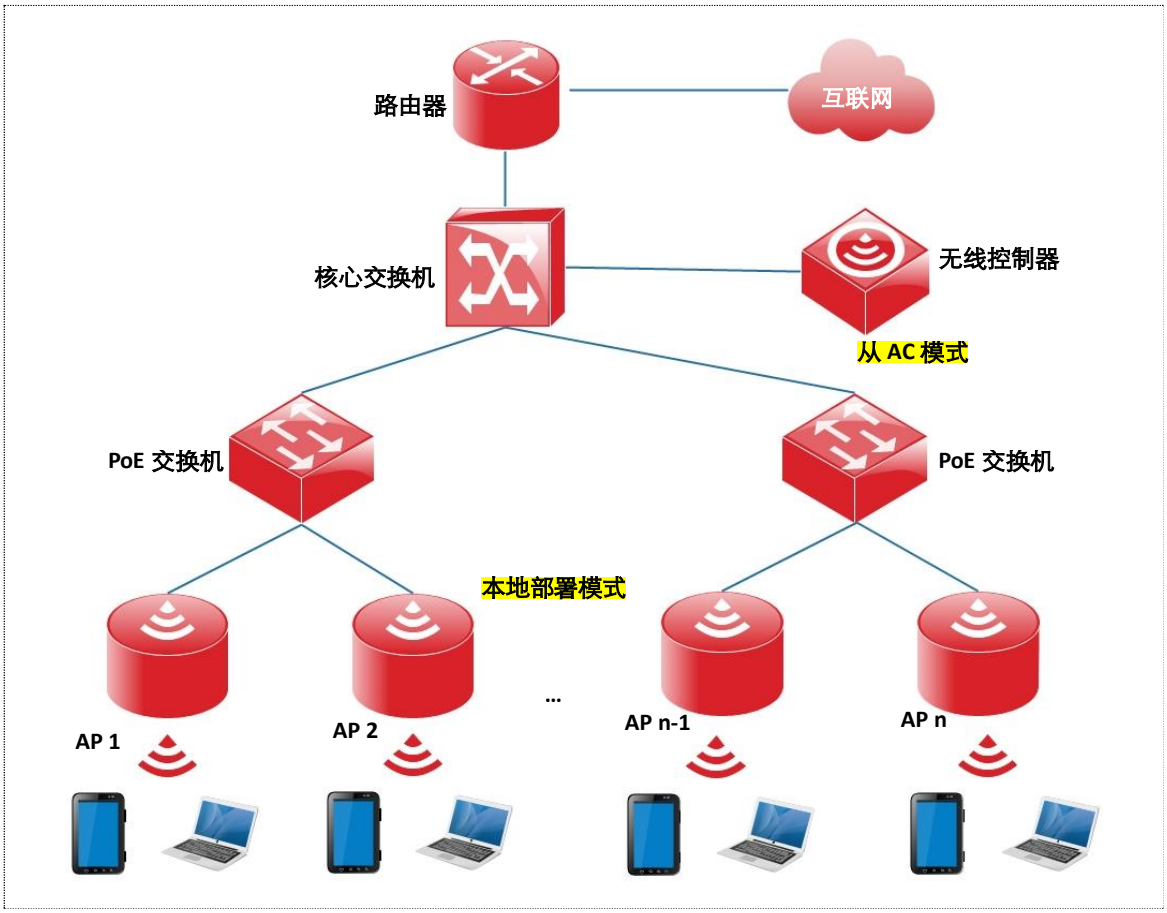
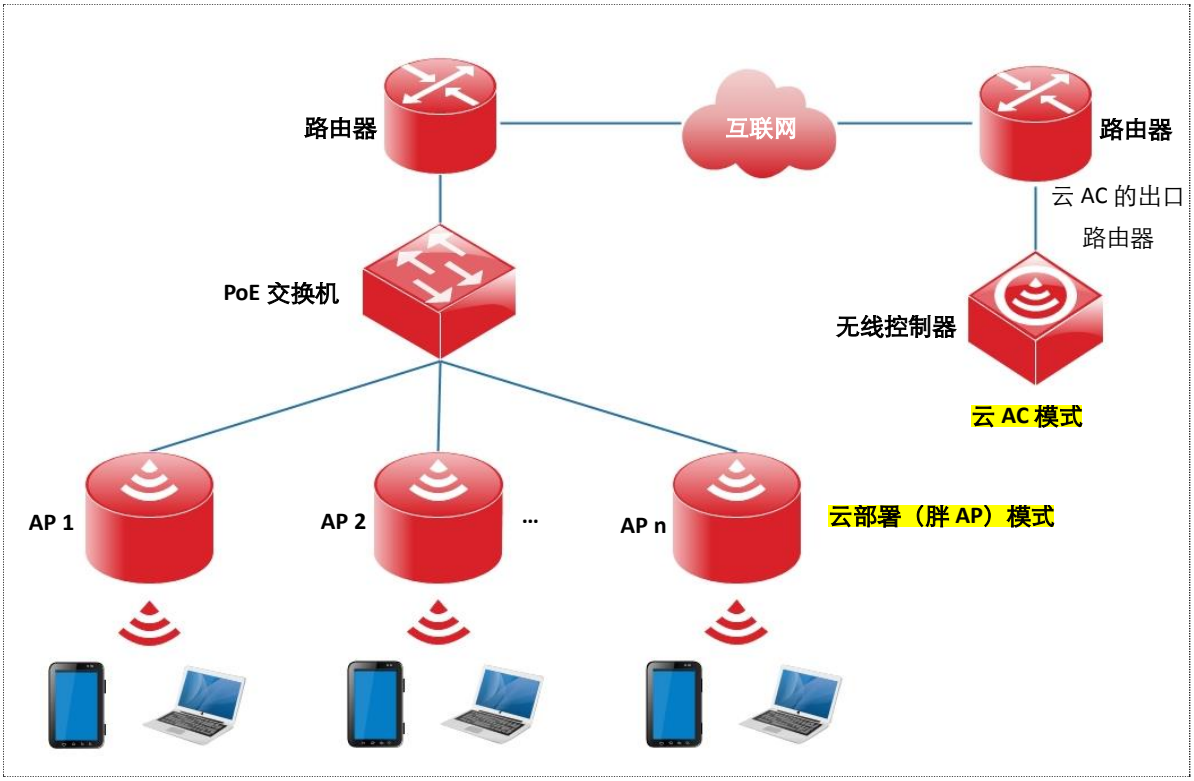


图7-1 本地部署

- 云部署（胖 AP）

当无线网络分散在各地，总体规模较大、但各处规模较小时，建议 AP 使用“云部署（胖 AP）”模式，由互联网上的无线控制器（云 AC 模式）集中管理分散在各地的云 AP。云部署（胖 AP）模式组网拓扑图如下。



在「高级设置」>「部署模式」页面中，您可以配置 AP 的部署模式。默认为“本地部署”，选择“云部署（胖 AP）”时，如下所示。

图7-2 部署模式

表7-1 参数说明

标题项	说明
部署模式	● 本地部署：AP 只能被本地局域网中的无线控制器（AC）管理。 ● 云部署（胖 AP）：AP 只能被指定 IP 地址的远程 AC（位于互联网或其他网络中的 AC）管理。
设备名称	AP 的名称描述。当网络中存在多台本型号设备时，不同的设备名称可以帮助您区分各设备。
云 AC 地址	远程 AC 的出口路由器的 WAN 口 IP 地址（必须是公网 IP 地址）或该 IP 地址绑定的域名。
云 AC 管理端口	远程 AC 的出口路由器已开放的端口号，用于管理本 AP。
云 AC 升级端口	远程 AC 的出口路由器已开放的端口号，用于升级本 AP。

7.2 SNMP

7.2.1 概述

利用 SNMP（Simple Network Management Protocol，简单网络管理协议），一个管理工作站可以远程管理所有支持这种协议的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件警告等。

SNMP 能够屏蔽不同设备的物理差异，实现对不同厂商设备的自动化管理。

● SNMP 的管理框架

SNMP 管理框架包含三个组成部分：SNMP 管理者，SNMP 代理，MIB 库（Management Information Base）。

- SNMP 管理者：一个利用 SNMP 协议对网络节点进行控制和监视的系统。其中网络环境中最常见的 SNMP 管理者被称为网络管理系统（NMS，Network Management System）。网络管理系统既可以指一台专门用来进行网络管理的服务器，也可以指某个网络设备中执行管理功能的一个应用程序。
- SNMP 代理：被管理设备中的一个软件模块，用来维护被管理设备的管理信息数据并可在需要时把管理数据汇报给一个 SNMP 管理系统。
- MIB 库：被管理对象的集合。它定义了被管理对象的一系列的属性：对象的名字、对象的访问权限和对象的数据类型等。每个 SNMP 代理都有自己的 MIB。SNMP 管理者根据权限可以对 MIB 中的对象进行读/写操作。

SNMP 管理者是 SNMP 网络的管理者，SNMP 代理是 SNMP 网络的被管理者，它们之间通过 SNMP 协议来交互管理信息。

- SNMP 基本操作

本 AP 中，SNMP 提供以下两种基本操作来实现 SNMP 管理者和 SNMP 代理的交互。

– Get 操作：SNMP 管理者使用该操作查询 SNMP 代理的一个或多个对象的值。

– Set 操作：SNMP 管理者使用该操作重新设置 MIB 库中的一个或多个对象的值。

- SNMP 协议版本

本 AP 兼容 SNMP v1、SNMP v2c 版本，采用团体名认证。SNMP 团体名（Community）用来定义 SNMP 代理和 SNMP 管理者的关系。如果 SNMP 报文携带的团体名没有得到设备的认可，该报文将被丢弃。团体名起到了类似于密码的作用，用来限制 SNMP 管理者对 SNMP 代理的访问。

SNMP v2c 它在兼容 SNMP v1 的同时又扩充了 SNMP v1 的功能：提供了更多的操作类型（GetBulk 和 InformRequest）；支持更多的数据类型（Counter64 等）；提供了更丰富的错误代码，能够更细致地区分错误。

- MIB 库简介

MIB 是以树状结构进行组织的。树的节点表示被管理对象，它可以用从根开始的一串表示路径的数字唯一地识别，这串数字称为 OID（Object Identifier，对象标识符）。MIB 的结构如图所示。图中，A 的 OID 为（1.3.6.1.2.1.1），B 的 OID 为（1.3.6.1.2.1.2）。

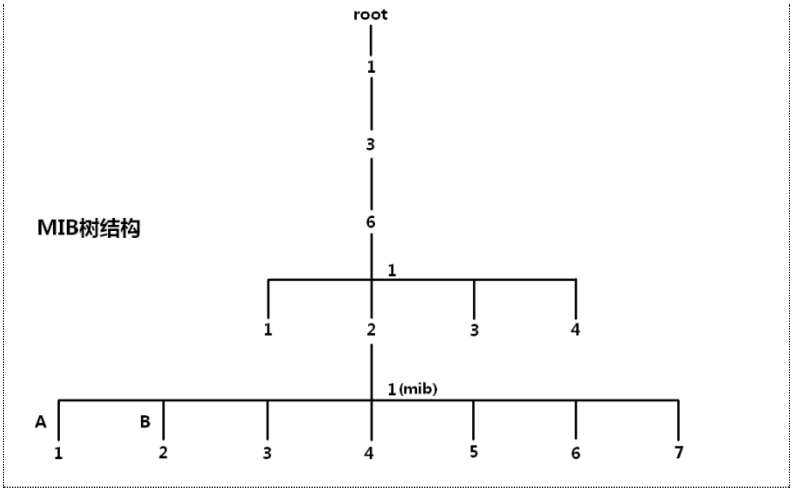


图7-3 MIB 树结构

在「高级设置」>「SNMP」页面中，您可以配置 AP 的 SNMP 代理。

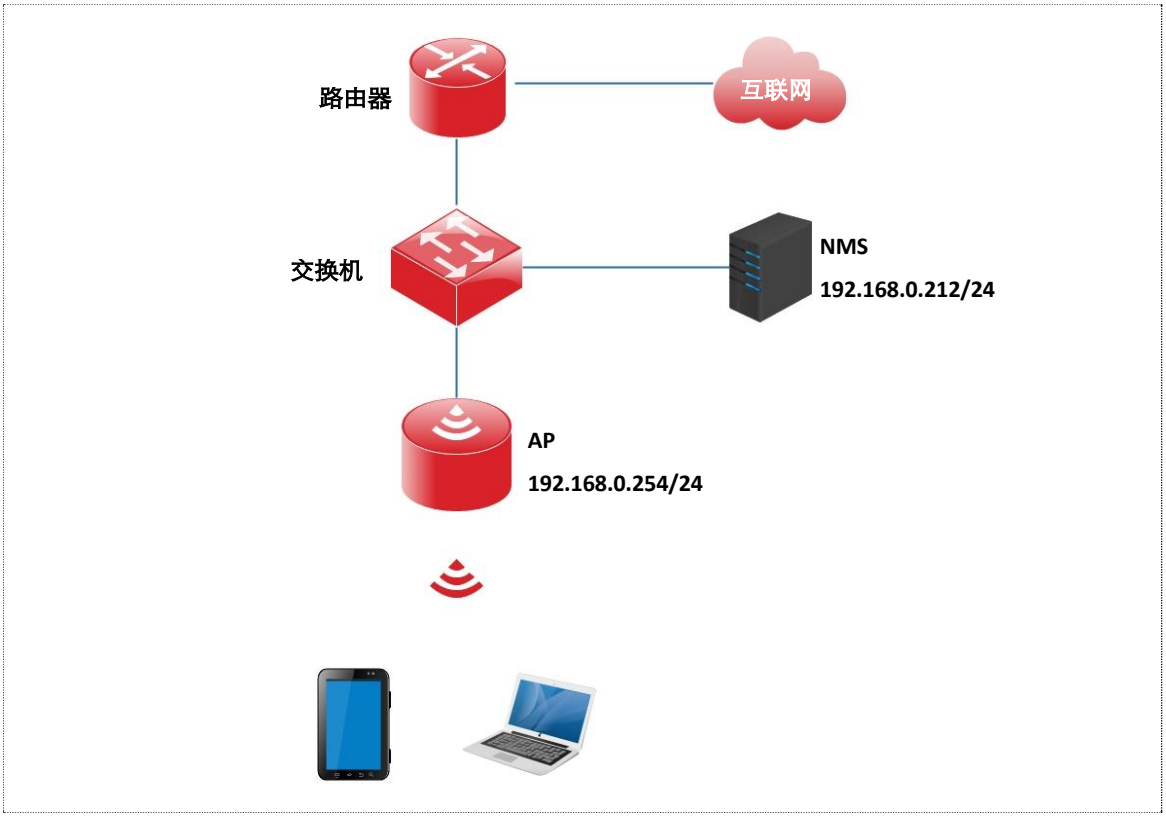
图7-4 SNMP

表7-2 参数说明

标题项	说明
SNMP 代理	开启/关闭 AP 的 SNMP 代理功能。 SNMP 管理者和 SNMP 代理上的 SNMP 版本必须相同，才能成功互访。目前，AP 中的 SNMP 代理支持 SNMP v1 版本、SNMP v2c 版本。
管理员	AP 的管理员的名字。可根据实际情况修改。
设备名称	AP 的设备名称。 **说明** **建议修改设备名称，使您在使用 SNMP 管理 AP 时，能快速识别出对应的 AP 设备。**
位置	AP 的安装位置。可根据实际情况修改。
读 Community	只读团体名，是 SNMP 管理者和 SNMP 代理之间的读操作口令。 本 SNMP 代理允许 SNMP 管理者用“读 Community”对 AP MIB 中的变量进行读操作。
读/写 Community	读/写团体名，是 SNMP 管理者和 SNMP 代理之间的读写操作口令。 本 SNMP 代理允许 SNMP 管理者用“读/写 Community”对 AP MIB 中的变量进行读和写操作。

7.2.2 SNMP 配置举例

- 组网要求
  - AP 与 NMS 通过以太网相连，AP 的 IP 地址为 192.168.0.254/24，NMS 的 IP 地址为 192.168.0.212/24。
  - NMS 通过 SNMP v1 或者 SNMP v2c 对 AP 进行监控管理。



- 配置步骤

一、配置 AP

假设管理员为“zhangsan”，读 Community 为“zhangsan”，读/写 Community 为“zhangsan123”。

步骤1 点击「高级设置」>「SNMP」。

步骤2 点击滑块至  。

步骤3 设置 SNMP 相关参数

1. 设置“管理员”为“zhangsan”。
2. 设置“位置”为“ShenZhen”。
3. 设置“读 Community”为“zhangsan”。
4. 设置“读/写 Community”为“zhangsan123”。

步骤4 点击 保存 。

图7-5 配置 SNMP 代理

二、配置 NMS

在使用 SNMP v1/v2c 版本的 NMS 上，设置“读 Community”和“读/写 Community”，注意需要与 AP 配置保持一致。具体设置方法请参考 NMS 的配套手册。

- 验证设置

完成上述设置后，NMS 可以和 AP 上的 SNMP 代理建立 SNMP 连接，能够通过 MIB 节点查询、设置 SNMP 代理上某些参数。

第8章 系统工具

8.1 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。

8.1.1 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，默认为“手动设置”。

- 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。

图8-1 网络校时

表8-1 参数说明

标题项	说明
时间设置	AP 系统时间的设置方式。
校时周期	AP 自动从互联网上的时间服务器同步的时间间隔。
选择时区	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。

图8-2 手动设置

8.1.2 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。

图8-3 WEB 闲置超时时间

8.2 设备维护

8.2.1 设备维护

在「系统工具」>「设备维护」>「设备维护」页面，您可以重启设备、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 的指示灯的操作。

- 重启设备

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 。

图8-4 重启设备

- 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。

说明

- 恢复出厂设置后，AP 的所有设置将会被清除，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。

操作方法 1:

AP 的指示灯闪烁状态下，按住 AP 的复位按钮约 8 秒，待指示灯长亮时松开。

当 AP 的指示灯重新闪烁时，恢复出厂设置成功。

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 。

当 AP 的指示灯重新闪烁时，恢复出厂设置成功。

图8-5 恢复出厂设置

- 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。

说明

为了避免 AP 损坏，确保升级正确：

- 恢复出厂设置后，AP 的所有设置将会被清除，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。

软件升级步骤：

步骤1 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2 点击 升级 。

图8-6 升级软件

步骤3 在弹出的窗口中选择并上传升级文件。

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。

说明

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。

- 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。

说明

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 。

图8-7 备份/恢复

步骤3 点击 备份 。

图8-8 备份

浏览器将下载文件名为 HikAp.cfg 的配置文件。

说明

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 。

图8-9 备份/恢复

步骤3 点击 恢复 。

图8-10 恢复

步骤4 选择并加载之前备份的配置文件。

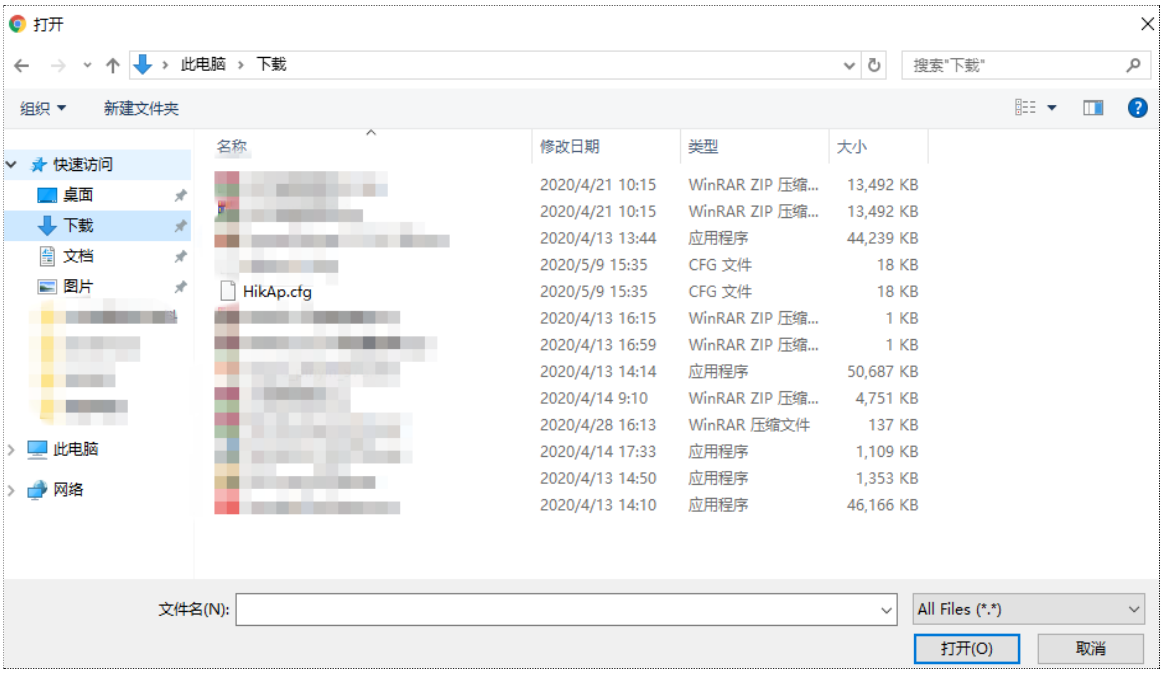


图8-11 加载备份文件

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。

- 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 。

图8-12 关闭指示灯

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 。

图8-13 开启指示灯

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。

8.2.2 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

说明

定时重启时间以路由器的系统时间为准，为避免重启时间出错，请确保路由器的系统时间准确。

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 。

图8-14 按间隔时间段重启

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 。

图8-15 定时重启

如上图设置完成后，每周一到周五的 22:00 点，AP 将自动重启。

8.3 用户名与密码

8.3.1 概述

在「系统工具」>「用户名与密码」页面，您可以修改 AP 管理页面登录账号（admin）的密码，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。

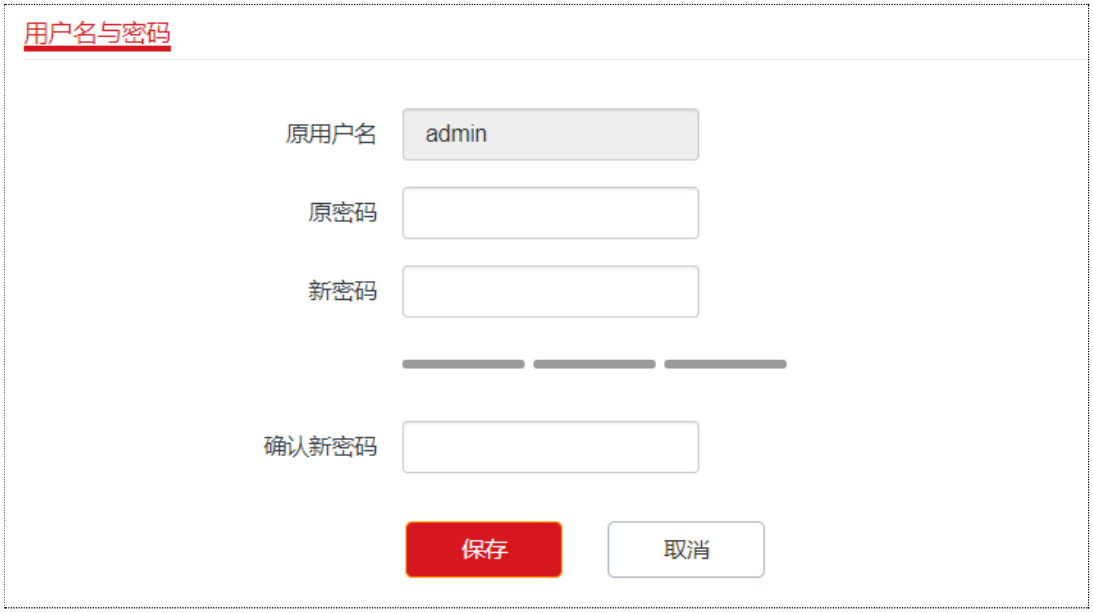


图8-16 用户名与密码

8.3.2 修改 admin 用户的密码

步骤1 点击「系统工具」>「用户名与密码」。

步骤2 在“原密码”输入框中输入账户当前的密码。

步骤3 在“新密码”输入框中输入新的账户密码。

步骤4 在“确认新密码”输入框中再次输入新的账户密码。

步骤5 点击 保存 。

图8-17 修改密码

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

8.4 系统日志

在 AP 的「系统日志」模块，您可以查看 AP 的系统日志、设置日志服务器和设置 Web 界面显示日志记录条数。

8.4.1 日志查看

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。

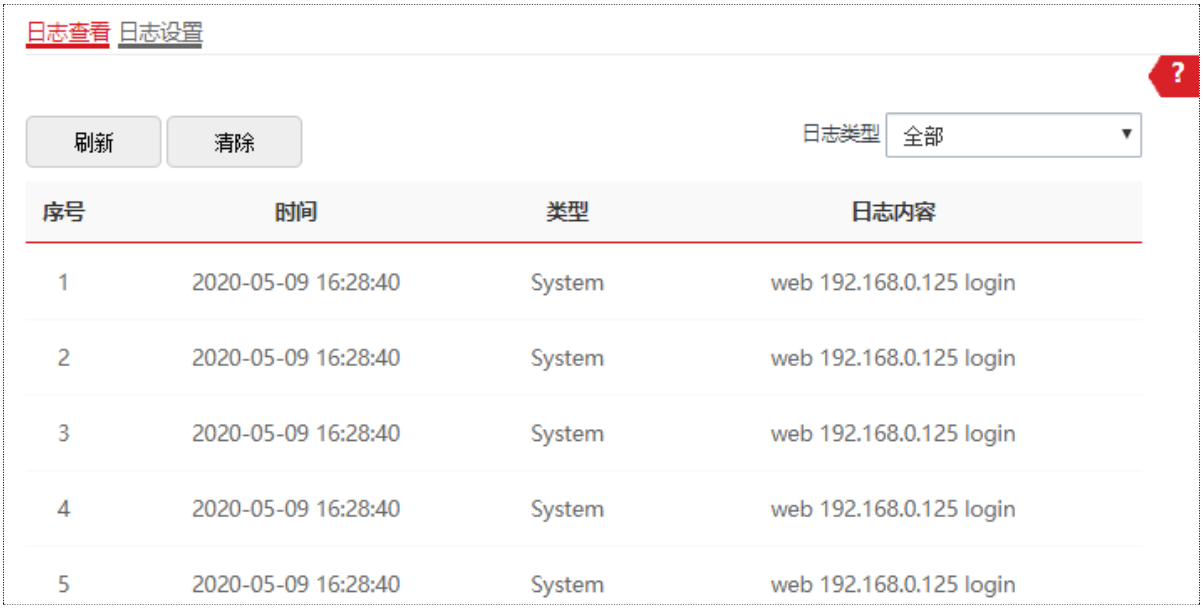


图8-18 查看日志

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 200 条日志信息。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 重启后会自动清除重启之前的日志信息，导致 AP 重启的操作有断电后重新通电、配置 QVLAN、升级软件、恢复配置、恢复出厂设置等。

8.4.2 日志设置

在「系统工具」>「系统日志」>「日志设置」页面，您可以设置日志记录条数和日志服务器。

设置日志服务器后，AP 会将系统日志同步发送到您设置的日志服务器，您可以在该日志服务器上查看 AP 的所有历史日志信息。

图8-19 设置日志服务参数

表8-2 参数说明

标题项	说明
日志服务	启用/禁用日志服务功能。默认禁用。 只有启用日志服务功能后，才可以进行修改日志记录条数和设置日志服务器的操作。
记录条数	最多可显示的日志条数。
日志服务器 IP 地址	日志服务器的 IP 地址。 为了保证系统日志能发送到日志服务器，请在「网络设置」>「LAN 口设置」页面设置本 AP 的 IP 地址、子网掩码和网关，使 AP 和日志服务器之间路由可达。
日志服务器端口	日志服务使用的端口（默认端口号为 514）。应与日志服务器设置的端口保持一致。
启用状态	日志服务器规则的启用状态。
操作	可对日志服务器进行如下操作： ● 点击可修改日志服务器的 IP 地址、端口和启用状态。 ● 点击可以删除对应的日志服务器。
添加	点击可以添加日志服务器。

添加日志服务器

步骤1 点击「系统工具」>「系统日志」>「日志设置」。

步骤2 点击滑块至。

步骤3 点击 添加 。

图8-20 开启日志服务

步骤4 在弹出的窗口中进行如下操作。

1. 输入日志服务器的 IP 地址。
2. 输入日志服务器发送/接收系统日志时使用的 UDP 端口号，一般为“514”。
3. 选择“启用状态”为“启用”。
4. 点击 添加 。

图8-21 日志服务器

步骤5 点击 保存 。

8.5 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 AP 到 www.baidu.com 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 。

图8-22 ping

稍后，诊断结果将显示在下面的黑框中。如下图示例。

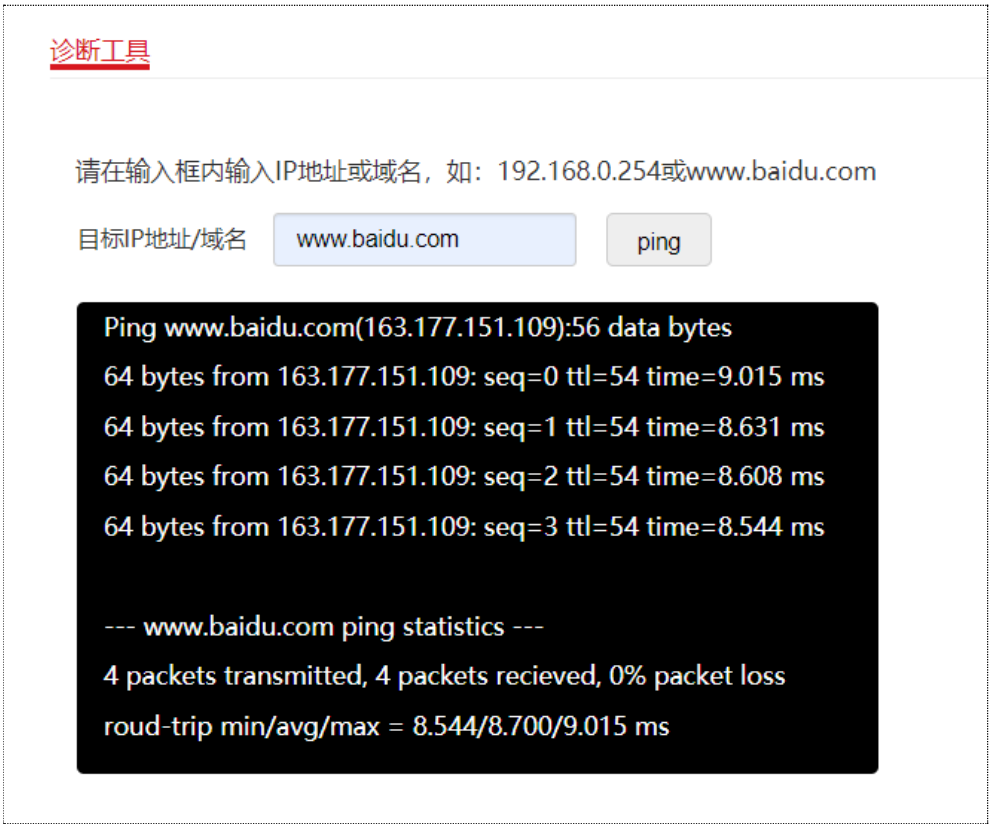


图8-23 ping 结果

8.6 上行链路检测

8.6.1 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 将停止提供无线接入服务，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，无线客户端才可以重新关联该 AP。

上行链接检测功能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。

上行链路检测组网如下图所示（上行接口为以太网口）。

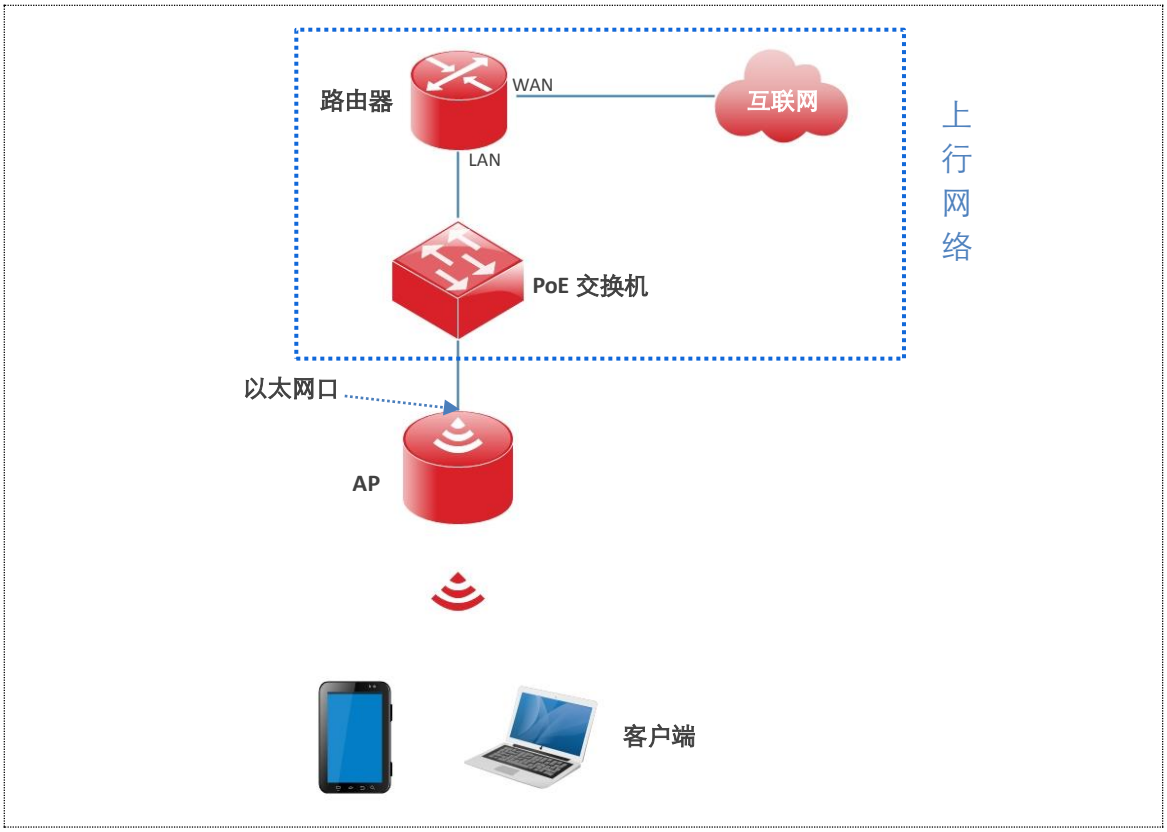


图8-24 上行链路检测

8.6.2 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 在“Ping 主机 1”和“Ping 主机 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“Ping 主机 1”和“Ping 主机 2”都输入该目的主机地址。

步骤4 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5 点击 保存 。


上行链路检测
?
上行链路检测
ping主机1
ping主机2
ping间隔
10
分钟（范围：10~100，默认：10）
保存
取消

附录A 默认参数

表8-3 AP 的主要参数

参数			默认设置
设备登录	管理 IP 地址		192.168.0.254
	用户名|密码		admin|无
快速设置	工作模式		AP 模式
LAN 口设置	IP 获取方式		静态 IP
	IP 地址		192.168.0.254
	子网掩码		255.255.255.0
DHCP 服务器			禁用
SSID 设置	SSID	2.4GHz	支持 8 个 SSID SSID 为“HIKVISION_XXXXXX”。其中，XXXXXX 为 AP LAN 口 MAC 后六位~后六位+7 默认主 SSID 启用，其他 SSID 禁用
		5GHz	支持 4 个 SSID SSID 为“HIKVISION_XXXXXX_5G”。其中，XXXXXX 为 AP LAN 口 MAC 后六位+8~后六位+11 默认主 SSID 启用，其他 SSID 禁用
射频设置	无线网络		开启
	网络模式	2.4GHz	11b/g/n
		5GHz	11ac
	信道带宽	2.4GHz	20MHz
		5GHz	80MHz

附录B 缩略语

表8-4 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）
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）
PoE	以太网供电（Power over Ethernet）
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）
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）
WPA	WiFi 网络安全接入（Wi-Fi Protected Access）

限制物质或元素标识表

《电器电子产品有害物质限制使用管理办法》限制物质或元素标识表

部分名称	《电器电子产品有害物质限制使用管理办法》限制物质或元素					
	铅(Pb)	汞(Hg)	镉(Cd)	六价铬(CrⅥ)	多溴联苯(PBB)	多溴二苯醚(PBDE)
金属部件	×	O	O	O	O	O
塑料部件	O	O	O	O	O	O
玻璃部件	×	O	O	O	O	O
线路板	×	O	O	O	O	O
电源（如果有）	×	O	O	O	O	O
附件	×	O	O	O	O	O
本表格依据 SJ/T 11364-2014 的规定编制。						
O 表示该有害物质在该部件所有均质材料中的含量均在 GB/T 26572-2011 规定的限量要求下。						
×表示该有害物质至少在该部件某一均质材料中的含量超出 GB/T 26572-2011 规定的限量要求，且目前业界没有成熟的替代方案，符合欧盟 RoHS 指令环保要求。						

本产品超过使用期限或者经过维修无法正常工作后，不应随意丢弃，请交由有废电器电子产品处理资格的企业处理，正确的方法请查阅国家或当地有关废弃电器电子产品处理的规定。

产品质量合格证
Qualification Card
PASS

保修服务

感谢您选用本产品，为了您能够充分享有完善的售后服务支持，请您在购买后认真阅读本产品保修卡的说明并妥善保存。
我们将按照海康威视产品标准保修承诺为您提供售后服务，售后服务政策明细请查看海康威视官网。部分信息摘录如下:
1. 保修期自产品首次购买之日起算，购买日以购买产品的发票日期为准。如无有效发票，则保修期将自产品出厂日推算。产品发票日期晚于产品实际交付日的，保修期自产品实际交付日起算。保修期限参考售后服务政策中的《海康威视产品标准保修期》执行。
2. 不保修范围(仅摘录部分,具体请见售后服务政策):
①超出规定的保修期限的;
②因误用、意外、改装、不适当的物理或操作环境、自然灾害、电涌及不当维护或保管导致的故障或损坏;
③第三方产品、软件、服务或行为导致的故障或损坏;
④产品使用过程中发生的正常脱色、磨损和消耗;
⑤产品可以不间断或无错误地正常运行;
⑥数据丢失或损坏;
⑦消耗零部件，除非是因材料或工艺缺陷而发生的故障;
⑧不能出示产品有效保修凭证和有效原始购物发票或收据，产品原序列号标签有涂改、替换、撕毁的现象、产品没有序列号或保修凭证上的产品型号或编号与产品实物不相符合的;
⑨未按随附的说明、操作手册使用产品，或者产品未用于预定功能或环境，海康威视经证实后确定您违反操作手册的任何其他情况。
3. 海康威视不对销售商或任何第三方对您的额外承诺负责，您应向这些第三方要求兑现。
用户名称：_____
详细地址：_____
电话：_____
产品型号（Model）：_____
产品编号（S/N）：_____
购买日期：___ 年__ 月__ 日
销售商：_____
电话：_____

注意:
1. 凭此卡享受保修期内的免费保修及保修期外的优惠性服务。
2. 本保修卡仅适用于本保修卡内产品，由销售单位盖章后方有效。
3. 特殊项目的产品保修条款以具体购销合同为准。

杭州海康威视数字技术股份有限公司
HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD.

www.hikvision.com
服务热线：400-800-5998