www.ip-com.com.cn

使用说明书

300Mbps无线面板式AP · W30AP

IP-COM

无线网络解决方案专家

版权声明

前言

感谢选择 IP-COM 产品。开始使用本产品前，请先阅读本说明书。

约定

本文可能用到的格式说明如下。

项目	格式	举例
菜单项	「」	选择「开始」菜单。
按钮	边框+底纹	点击 确定 。
连续菜单选择	>	进入「状态」>「无线状态」页面。

本文可能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	表示有助于节省时间或资源的方法。

缩略语

缩略语	全称
AP	Access Point
AC	Access Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
SSID	Service Set Identifier
VLAN	Virtual Local Area Network

更多信息

如需获取更多信息，请访问 IP-COM 官方网站：http://www.ip-com.com.cn。

技术支持

如需技术支持，请通过以下方式与我们联系。

40066-50066	ip-com@ip-com.com.cn	http://www.ip-com.com.cn

目录

1 产品介绍

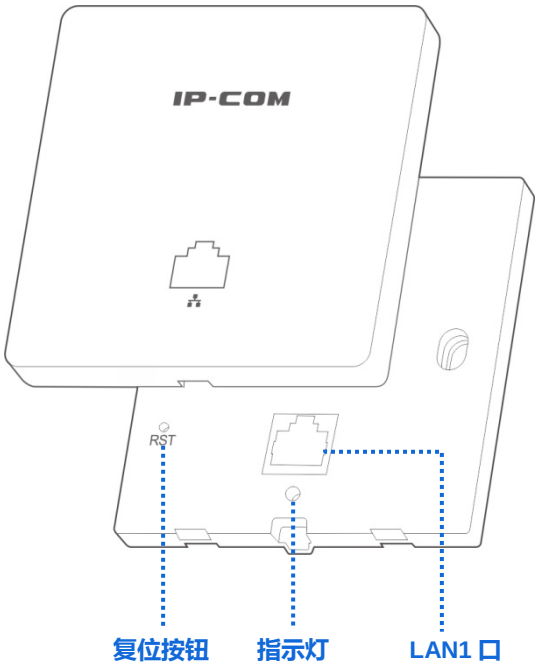
1.1 简介

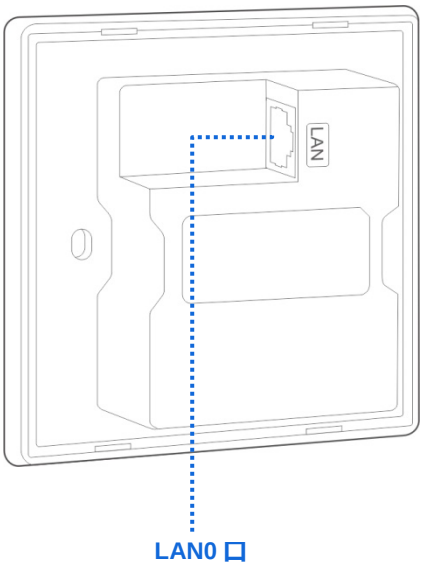
IP-COM 无线面板式 AP 产品 W30AP V4.0 提供 300Mbps 的无线数据传输速率，支持 IEEE 802.3af 标准 PoE 供电，可通过自身管理页面或 IP-COM 无线控制器（或带“AC 管理”功能的路由器）进行管理，采用入墙设计，适合别墅/大户型家庭、酒店进行无线覆盖。

1.2 外观

介绍 AP 的 按钮&指示灯&接口 、贴纸 。

1.2.1 按钮&指示灯&接口





- **复位按钮**

揭开 AP 外盖后可见。通电状态下，用针状物按住 8 秒后松开，AP 恢复出厂设置。

- **指示灯**

指示灯	闪烁：工作正常。
	不亮：未上电，已关闭指示灯显示，或出现故障。

- **LAN1 口**

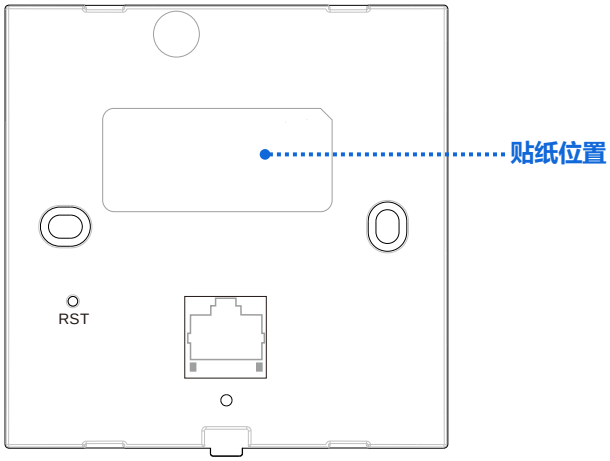
数据传输接口，10/100M 自适应，位于 AP 正面。用于连接电脑、交换机等。

- **LAN0 口**

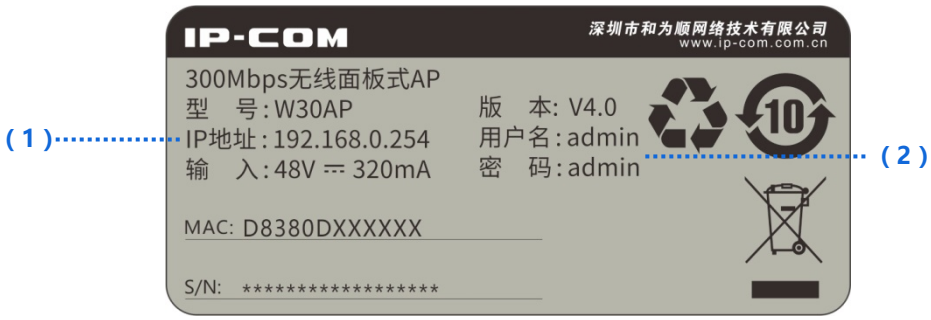
PoE 供电、数据传输复用接口，10/100M 自适应，位于 AP 背面。用网线连接到符合 IEEE 802.3af 标准的 PoE 交换机或 PoE 供电设备给 AP 供电。

1.2.2 贴纸

揭开 AP 外盖即可看见贴纸，具体位置如下图所示。



贴纸说明：



（1）：AP 默认（初始）的 IP 地址，首次使用 AP 时，可使用此地址登录 AP 的管理页面。

（2）：AP 管理页面的默认登录用户名和登录密码。

2 应用场景

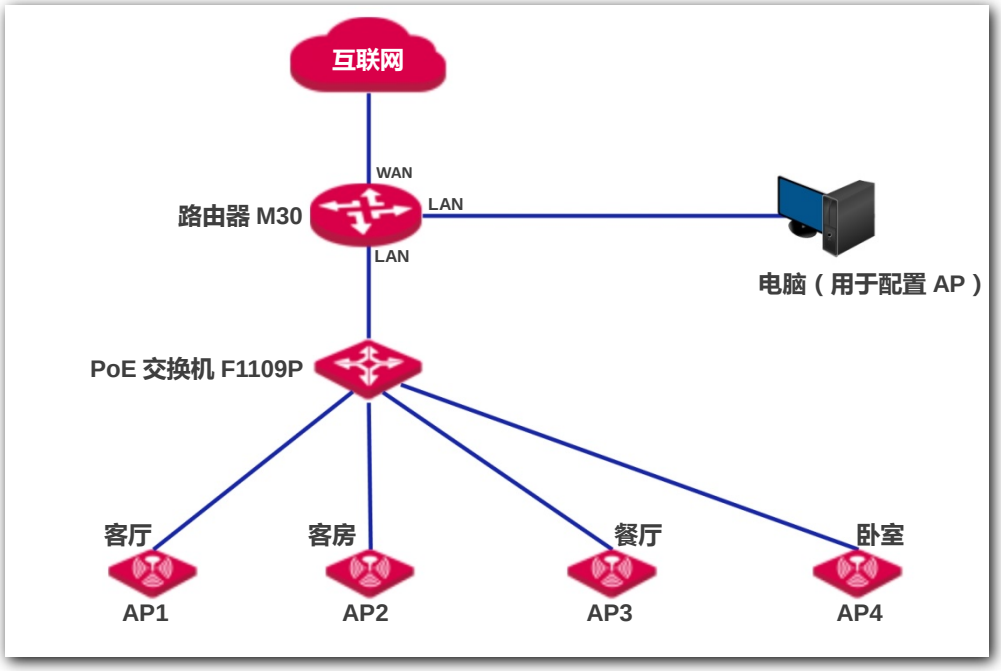
2.1 大户型/别墅家庭无线组网

2.1.1 搭配支持 AC 管理功能的 IP-COM 路由器

对于大户型/别墅家庭用户，推荐使用 IP-COM 大户型/别墅无线套装：1 台有线路由器（如 M30）+1 台 PoE 交换机（如 F1109P）+4~8 台 W30AP。安装时，每个房间部署 1 台 AP，将路由器、交换机都安装在弱电箱内。设置步骤如下所示。

步骤 1：连接设备。

路由器 WAN 口连接到 ADSL 猫或光猫，路由器 LAN 口连接 PoE 交换机的 Uplink 口，AP 背面接口 LAN0 通过墙壁内暗线连接到 PoE 交换机的 PoE 口。具体连接图示如下。



步骤 2：登录路由器管理页面。

电脑有线连接至路由器的 LAN 口。打开浏览器，在地址栏输入路由器的管理 IP（默认为 **192.168.0.252**），回车。在出现的页面设置您的登录密码，点击 登录 进入路由器的管理页面。

步骤 3：设置 AP。

在路由器的「AC 管理」模块，开启 **AC 管理**，修改第一条规则的 **SSID**（无线网络名称，如 IP-COM），认证类型选择 **WPA2-PSK**，并设置无线**密码**（如 12345678），点击 确定 保存配置。

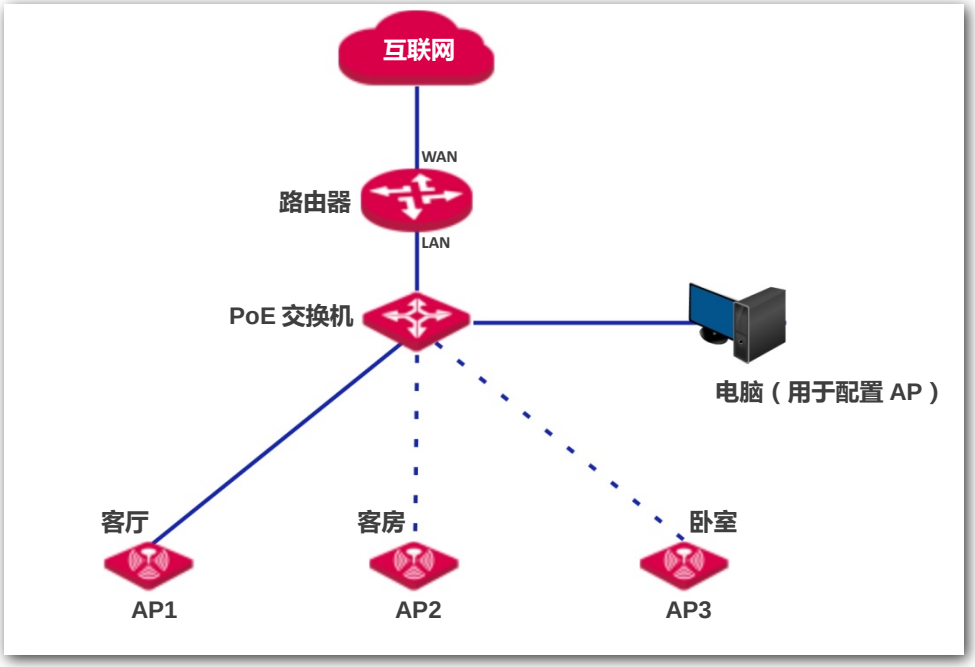
稍等片刻，网络中的 AP 会自动从路由器获得无线网络名称和无线密码。更多配置说明请访问 IP-COM 官网 http://www.ip-com.com.cn下载相应型号路由器的使用说明书。

2.1.2 搭配其他路由器

如果搭配的是其他路由器，请按以下步骤操作。

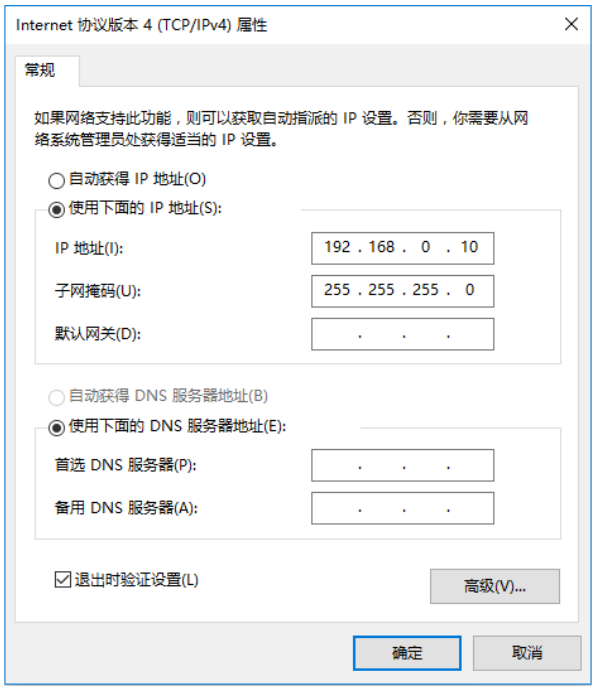
步骤 1：连接设备。

如下图所示，请先只接 1 台 AP（如 AP1）到 PoE 交换机，设置完成后再接另一台进行设置，以此类推。（为了避免 IP 地址冲突引起网络故障，设置时，必须 修改 AP 的 IP 地址 ）



步骤 2：设置电脑的 IP 地址。（以 Windows 7 系统为例）

用网线将电脑连接到 PoE 交换机。右键单击电脑桌面右下角的网络图标，点击**打开网络和共享中心**>**本地连接**>**属性**，双击 **Internet 协议版本 4（TCP/IPv4）**，选择**使用下面的 IP 地址**，设置 IP 地址为 **192.168.0.X**（X 为 2~253），子网掩码为 **255.255.255.0**，点击 确定 。



步骤 3：登录 AP 的管理页面。

打开电脑上的浏览器，在地址栏输入 AP 的管理 IP（默认为 **192.168.0.254**），回车。在出现的页面输入用户名和密码（默认均为 **admin**），点击 登录 进入 AP 的管理页面。

步骤 4：设置 AP1。

1. 在「快速设置」页面选择 **AP 模式**，设置 **SSID**（无线网络名称，如 IP-COM），安全模式设为 **WPA2-PSK**，**AES**，设置**密钥**（无线密码，如 12345678），点击 **保存** 。

2. 转到「网络设置」>「LAN 口设置」页面，修改 **IP 地址**的最后一段，避免与后续接入的 AP 的 IP 地址冲突，如 192.168.0.201，点击 **保存**。

步骤 5：设置其他 AP。

接入另一台 AP 到 PoE 交换机，参考**步骤 3**>**步骤 4** 进行设置。其中，SSID 和密钥设置完全相同，IP 地址设置必须不同。以此类推。

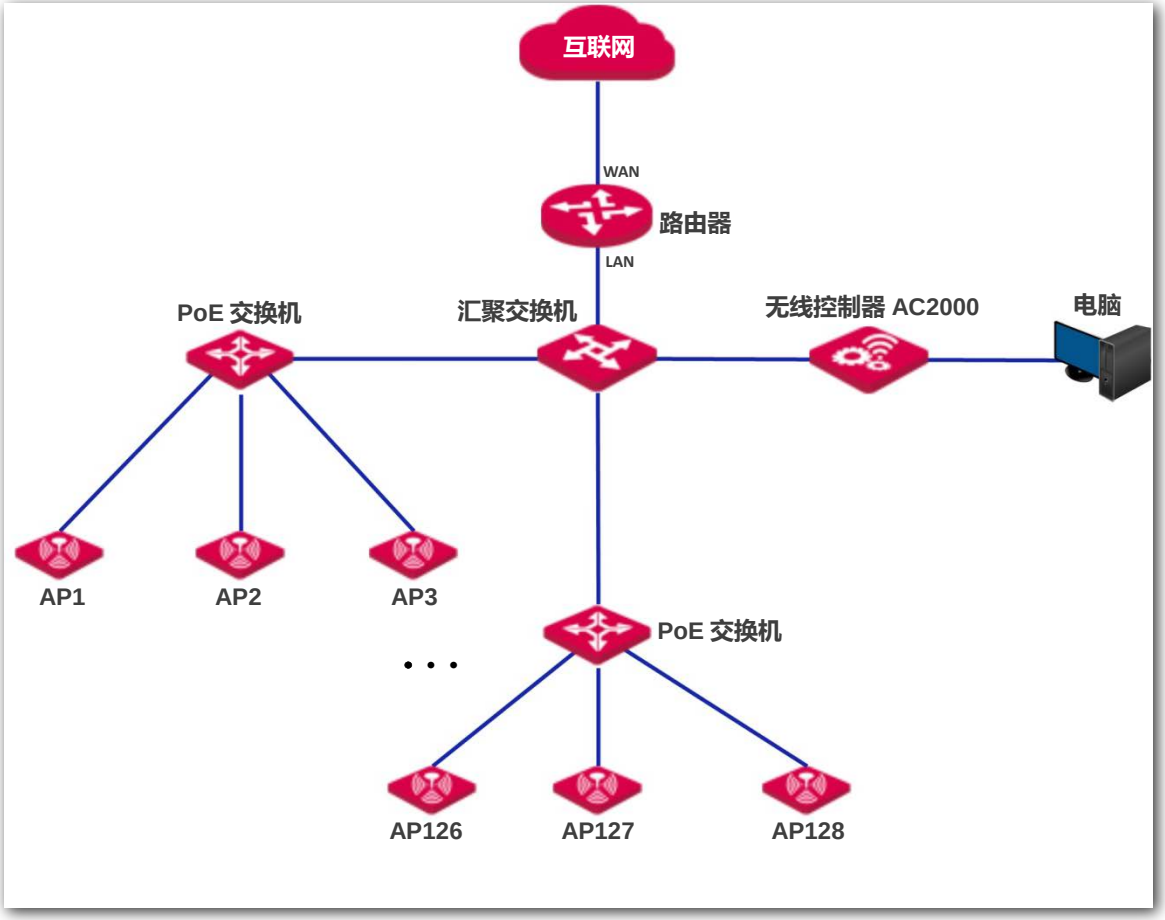
更多配置说明请参考本说明书第 **4** 章及以后内容。

2.2 酒店无线组网

由于酒店里安装的 AP 数量多，管理更复杂，需要在网络中部署 IP-COM 无线控制器(如 AC2000)，通过它集中设置和管理所有 AP。具体操作步骤如下。

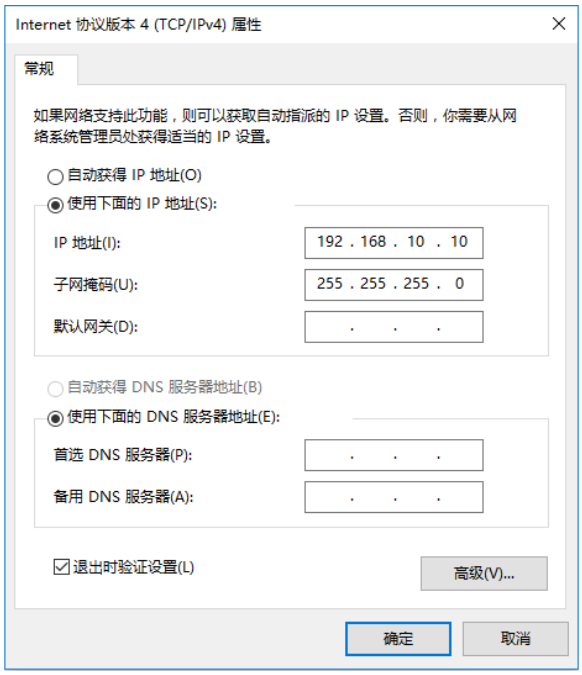
步骤 1：连接设备。

参考如下图示连接好各设备。



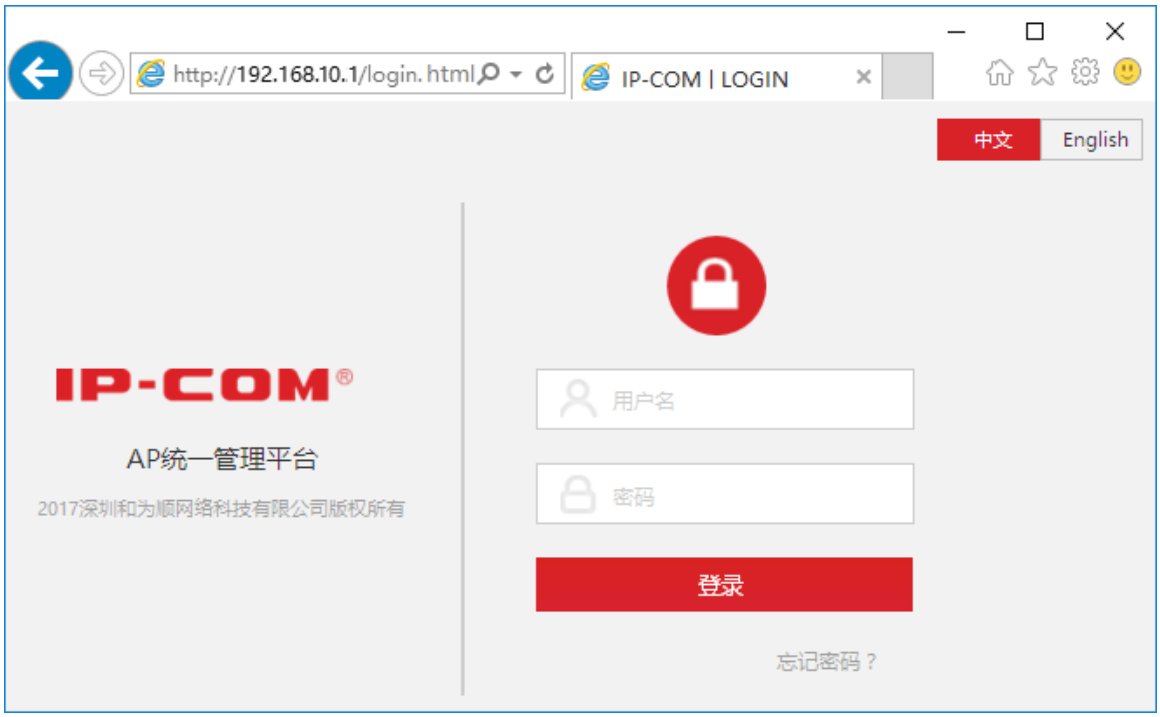
步骤 2：设置电脑的 IP 地址。（以 Windows 7 系统为例）

用网线将电脑连接到无线控制器。右键单击电脑桌面右下角的网络图标，点击**打开网络和共享中心**>**本地连接**>**属性**，双击 **Internet 协议版本 4 (TCP/IPv4)**，选择**使用下面的 IP 地址**，设置 IP 地址为 **192.168.10.X**（X 为 2~253），子网掩码为 **255.255.255.0**，点击 确定 。



步骤 3：登录无线控制器的管理页面。

打开电脑上的浏览器，在地址栏输入无线控制器的管理 IP（默认为 **192.168.10.1**），回车。在出现的页面输入用户名/密码（默认均为 **admin**），点击 登录 进入无线控制器的管理页面。



步骤 4：设置 AP。

在无线控制器的管理页面，点击 修改默认策略的 **SSID**（无线网络名称，如 IP-COM）、**加密方式**

（如 WPA2-PSK，AES）、**无线密码**（认证密钥，如 12345678），然后保存配置。

稍等片刻，网络中的 AP 会自动从无线控制器获得无线网络名称和无线密码。更多配置说明请访问 IP-COM 官网 http://www.ip-com.com.cn下载相应型号无线控制器的使用说明书。

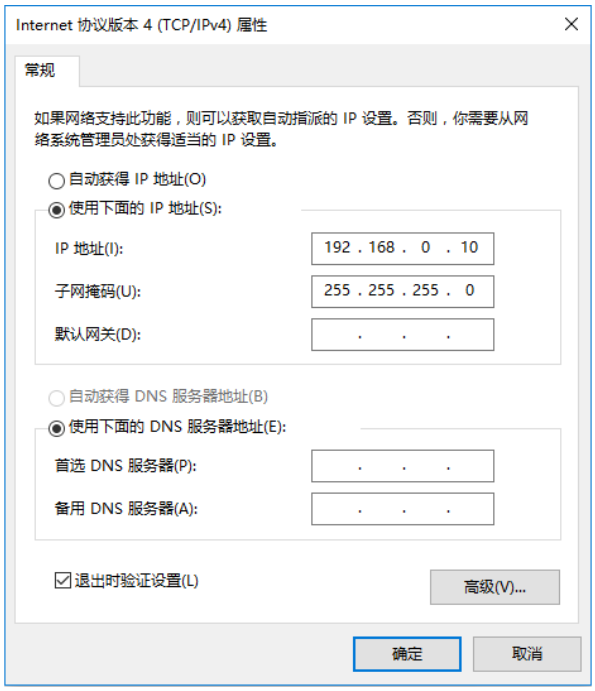
本说明书的后续内容，主要介绍登录到 AP 的管理页面设置 AP。

3 设备登录

3.1 登录 AP 的管理页面

使用浏览器就可以登录到 AP 的管理页面，步骤如下：

1. 用网线将管理电脑接到 AP（或 AP 连接的交换机）。
2. 设置电脑的本地连接 IP 地址为“192.168.0.X”（X 为 2~253），子网掩码为“255.255.255.0”。



3. 打开电脑上的浏览器（如 IE），访问 AP 的管理 IP（默认为“192.168.0.254”），进入 AP 的登录页面。
4. 输入登录用户名/密码（默认均为“admin”），点击 登录 。

提示

若未出现上述页面，请查看附录 A-常见问题解答的 问 1。

----完成

成功登录到 AP 的管理页面后，您就可以开始配置 AP 了。

3.2 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，您也可以直接关闭浏览器，退出管理页面。

3.3 管理页面布局

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。

3.4 管理页面常用按钮

以下是 AP 管理页面中常用按钮的功能介绍。

常用按钮	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。

常用按钮	说明
恢复	用于取消当前页面未保存的配置，并恢复到修改前的配置。
帮 助	点击可查看对应页面设置帮助信息。

4 快速设置

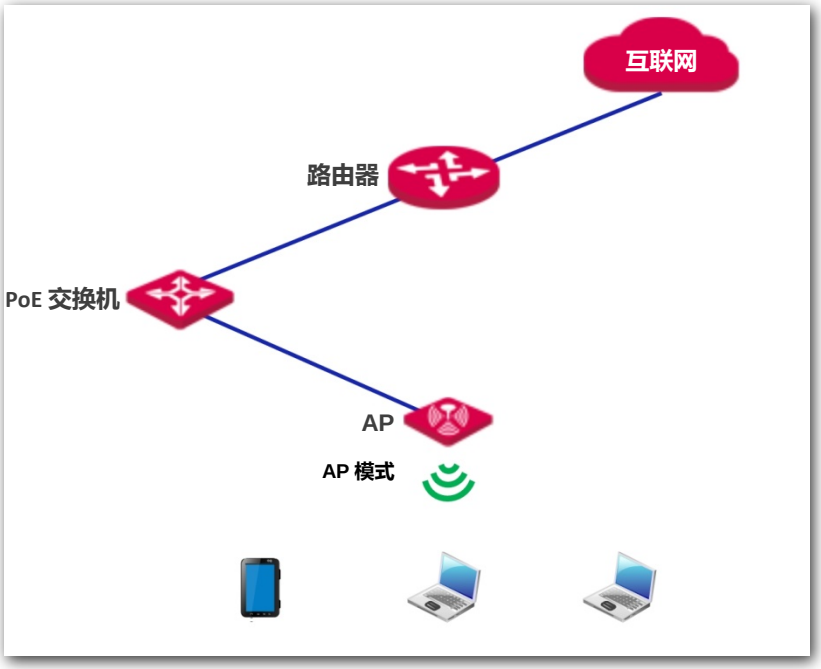
4.1 概述

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、Pad 等）连接 AP 的 Wi-Fi 可以正常上网。

本 AP 支持两种工作模式：AP 模式、Client+AP 模式。

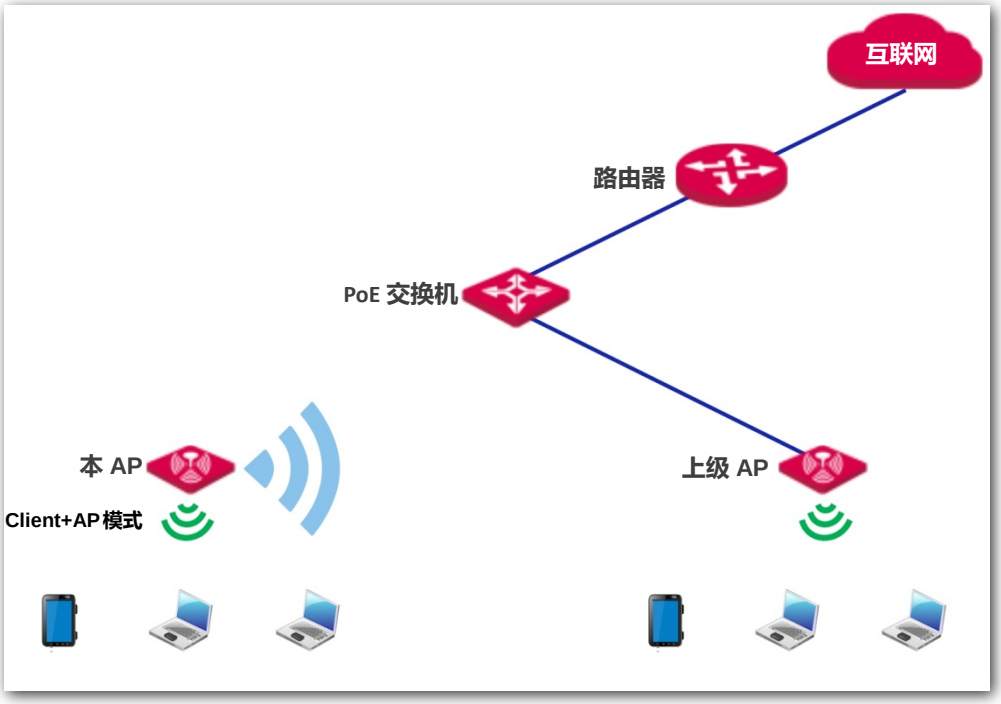
- **AP 模式**

AP 默认工作在此模式。此时，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。应用拓扑图如下。



- **Client+AP 模式**

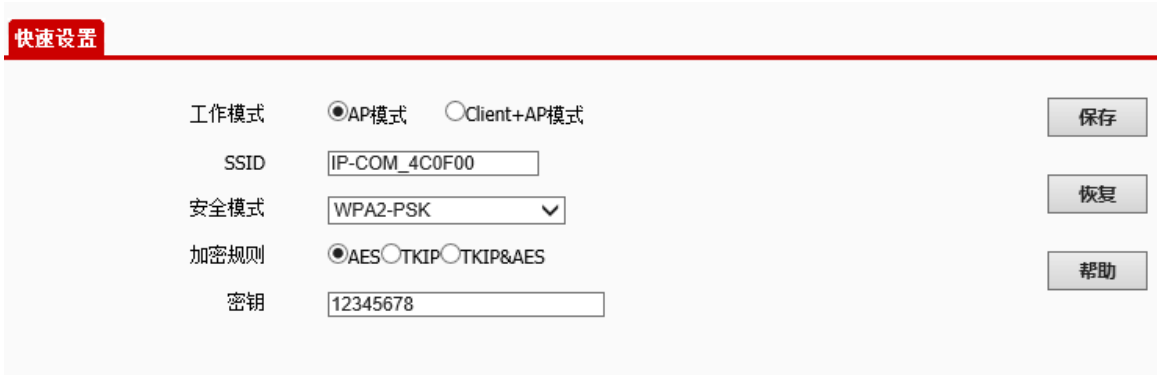
此时，AP 通过无线桥接上级设备（如：无线路由器、AP 等）的信号，扩展上级无线信号的覆盖范围。应用拓扑图如下。



4.2 快速设置

4.2.1 AP 模式

1. 进入 AP 的「快速设置」页面。
2. 工作模式：选择“AP 模式”。
3. SSID：点击输入框，修改 AP 主网络的无线网络名称（主 SSID）。
4. 安全模式：选择所需安全模式（建议选择“WPA2-PSK”>“AES”），并设置对应的展开参数。
5. 点击 **保存** 。



参数说明

标题项	说明
工作模式	选择 AP 的工作模式：AP 模式或 Client+AP 模式。
SSID	点击可修改 AP 主网络的无线网络名称，即 AP 的主 SSID。
安全模式	选择无线网络的安全模式。支持：不加密、WEP、WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK、WPA、WPA2。点击超链接可以了解对应安全模式的详细说明。

----完成

之后，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（密钥），即可上网。

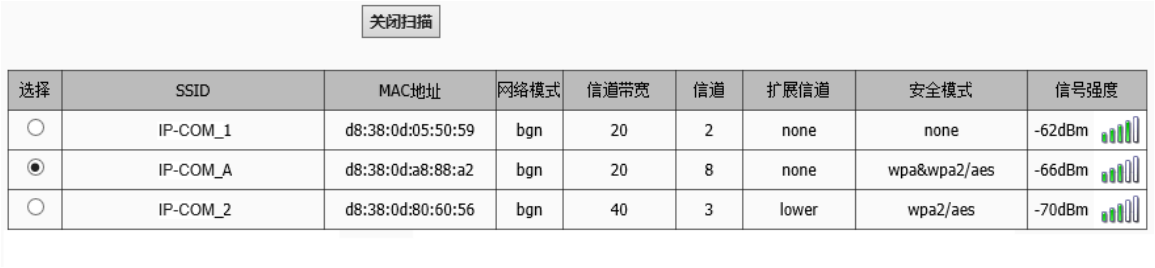
4.2.2 Client+AP 模式

1. 进入**本 AP** 的「快速设置」页面。
2. 工作模式：选择“Client+AP 模式”。
3. 点击 **扫描** 。

4. 在出现的无线网络列表中，选择要扩展的无线网络。

提示

- 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 会自动识别并填写所选择无线网络的以下参数：SSID，安全模式、信道。但对于“密钥”、“RADIUS 服务器”、“RADIUS 端口”、“RADIUS 密码”参数，则需要手动填写。



选择	SSID	MAC地址	网络模式	信道带宽	信道	扩展信道	安全模式	信号强度
○	IP-COM_1	d8:38:0d:05:50:59	bgn	20	2	none	none	-62dBm
◉	IP-COM_A	d8:38:0d:a8:88:a2	bgn	20	8	none	wpa&wpa2/aes	-66dBm
○	IP-COM_2	d8:38:0d:80:60:56	bgn	40	3	lower	wpa2/aes	-70dBm

5. 如果上级无线网络已加密，请填入对应的“密钥”或“RADIUS 服务器”、“RADIUS 端口”、“RADIUS 密码”。
6. 点击 **保存** 。

----完成

之后，使用智能手机等无线设备搜索并连接本 AP 的 SSID（进入「状态」>「无线状态」页面，可查看本 AP 的 SSID），输入无线密码（密钥），即可上网。

5 状态

5.1 系统状态

进入页面：点击「状态」>「系统状态」。

在这里，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
设备名称	该台 AP 的名称。 独特的设备名称有助于您快速区分各 AP 设备。您可以在「网络设置」>「LAN 口设置」页面修改设备名称。
系统时间	AP 当前的系统时间。
运行时间	AP 最近一次启动后连续运行的时长。

标题项	说明
无线客户端个数	当前接入 AP Wi-Fi 的无线设备个数。
软件版本号	AP 系统软件的版本号。
硬件版本号	AP 硬件的版本号。
MAC 地址	AP 以太网口（LAN 口）的物理地址。当您用网线连接 AP 和其他设备时，AP 使用本 MAC 地址和其他设备进行通信。
IP 地址	AP 的 IP 地址，也是 AP 的管理 IP 地址。 局域网用户访问本 IP，可以登录到 AP 的管理页面。您可以在「网络设置」>「LAN 口设置」页面修改此 IP 地址。
子网掩码	AP IP 地址的子网掩码。
首选 DNS 服务器	AP 的首选 DNS 服务器 IP 地址。
备用 DNS 服务器	AP 的备用 DNS 服务器 IP 地址。

5.2 无线状态

进入页面：点击「状态」>「无线状态」。

在这里，您可以查看 AP 射频的概要设置情况及 SSID 状态。

射频状态	
射频开关	无线已开启
网络模式	b/g/n
信道	3

SSID状态			
SSID	MAC地址	启用状态	安全模式
IP-COM_4C0F00	D8:38:0D:4C:0F:01	启用	不加密
IP-COM_4C0F01	D8:38:0D:4C:0F:02	禁用	不加密

参数说明

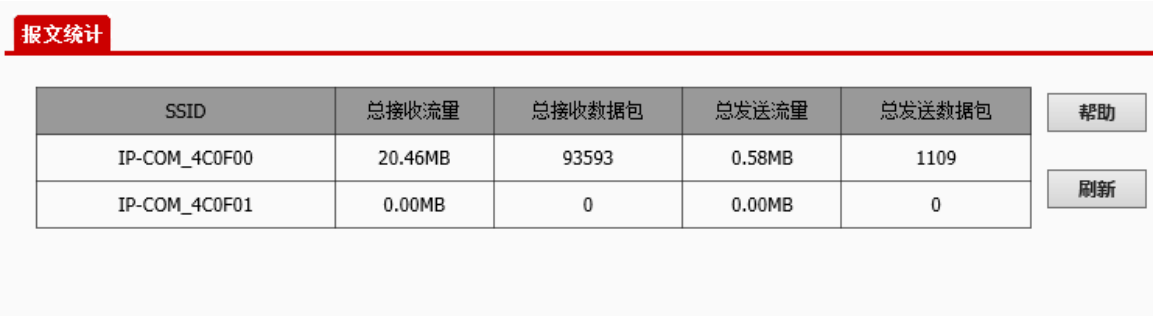
标题项		说明
射频状态	射频开关	AP 无线功能的开启/关闭状态。
	网络模式	AP 当前的无线网络模式。

标题项		说明
	信道	AP 当前的工作信道。
SSID 状态	SSID	显示 AP 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 对应无线网络的状态。
	安全模式	SSID 对应无线网络的安全模式。

5.3 报文统计

进入页面：点击「状态」>「报文统计」。

在这里，您可以查看 AP 各无线网络的历史报文统计信息。如果要查看最新的报文统计信息，请点击 **刷新** 。



SSID	总接收流量	总接收数据包	总发送流量	总发送数据包
IP-COM_4C0F00	20.46MB	93593	0.58MB	1109
IP-COM_4C0F01	0.00MB	0	0.00MB	0

5.4 客户端列表

进入页面：点击「状态」>「客户端列表」。

在这里，您可以查看 AP 各 SSID 的无线客户端连接信息。

序号	MAC地址	IP	连接时间	发送速率	接收速度
1	CC:08:8D:8E:9F:A6	192.168.110.161	00时02分17秒	58.5Mbps	1Mbps

页面默认显示 主 SSID的无线客户端连接信息。如果要查看其它 SSID 的无线客户端连接情况，请点击页面右上角的下拉菜单，选择要查看的 SSID 即可。

6 网络设置

6.1 LAN 口设置

进入页面：点击「网络设置」。

在这里，您可以查看 AP 的 LAN 口 MAC 地址，设置 AP 的名称、端口驱动能力、IP 获取方式及相关信息。

参数说明

标题项	说明
MAC 地址	AP 的 LAN 口 MAC 地址。 AP主 SSID默认为 IP-COM_XXXXXX，其中，XXXXXX 为此 MAC 后六位。
IP 获取方式	AP 的 IP 地址获取方式，默认为“手动设置”。 – 手动设置：手动指定 AP 的 IP 地址、子网掩码、网关地址、DNS 服务器信息。 – 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 服务器信息。 提示 IP 获取方式设置为“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

标题项	说明
	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 登录到 AP 的管理页面。默认为“192.168.0.254”。 如果要让 AP 联网，一般需要设置此 IP 使其与网络中的出口路由器的 LAN 口 IP 地址在同一网段。
子网掩码	AP IP 地址的子网掩码，默认为“255.255.255.0”。
网关地址	AP 的默认网关。 如果要让 AP 联网，一般需要设置网关地址为网络中出口路由器的 LAN 口 IP 地址。
首选 DNS 服务器	AP 的首选 DNS 服务器地址。 若网络中的出口路由器有 DNS 代理功能，此地址可以是出口路由器的 LAN 口 IP 地址。若网络中的出口路由器无 DNS 代理功能，请填入正确的 DNS 服务器的 IP 地址。
备用 DNS 服务器	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	该台 AP 的名称，默认为 AP 的型号，如 W30AP V4.0 的设备名称为“W30APV4.0”。 建议修改设备名称为该台 AP 的安装位置描述（如主卧），方便管理 AP 时，通过设备名称快速定位 AP。
端口驱动能力	AP LAN0 口的驱动模式。 – 标准模式：速率高，驱动距离较短。一般情况下，建议选择此模式。 – 增强模式：驱动距离远，但速率较低，一般协商为 10Mbps。 当连接 AP 的 LAN0 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 的 LAN0 口无法正常收发数据。

6.2 修改 LAN IP

6.2.1 手动设置 IP

由网络管理员手动指定 AP 的 IP 地址、子网掩码、网关地址、首选/备用 DNS 服务器，建议仅在网络中只需部署少量（一台或几台）AP 时使用本设置方式。

设置步骤：

1. 进入「网络设置」>「LAN 口设置」页面。
2. IP 获取方式：选择“手动设置”。

3. 设置 IP 地址、子网掩码、网关地址、首选/备用 DNS 服务器（一般仅需设置“IP 地址”、“网关地址”、“首选 DNS 服务器”）。
4. 点击 **保存** 。

----完成

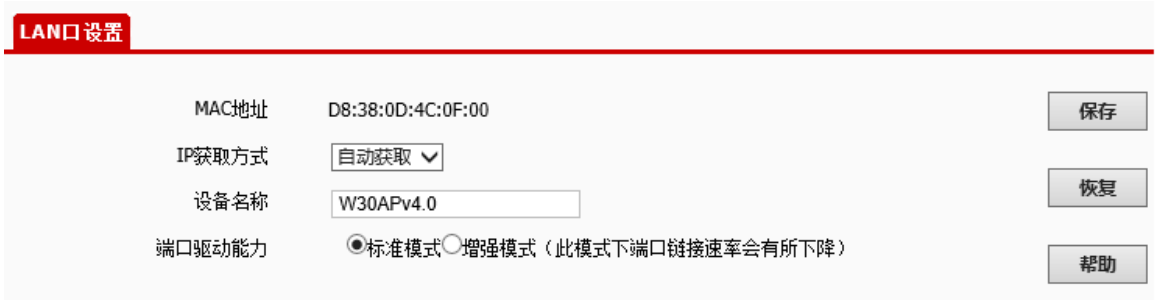
设置完成后，如果新的 IP 地址与原 IP 地址在同一网段，访问新的 IP 地址就能登录到 AP 的管理页面；如果新的 IP 地址与原 IP 地址不在同一网段，需要更改 管理电脑 的 IP 地址使其和新的 IP 在相同网段，并访问新的 IP 地址才能重新登录到 AP 的管理页面。

6.2.2 自动获取 IP

AP 自动从网络中的 DHCP 服务器获取 IP 地址、子网掩码、网关地址、首选/备用 DNS 服务器。如果网络中需要部署大量 AP，使用此方式可避免 IP 地址冲突，并有效减少网管人员的工作量。

设置步骤：

1. 进入「网络设置」>「LAN 口设置」页面。
2. IP 获取方式：选择“自动获取”。
3. 点击 **保存** 。



----完成

设置完成后，如果需要重新登录 AP 的管理页面，请先到 DHCP 服务器的客户端列表中查看 AP 获得的 IP 地址，再确保 管理电脑 的 IP 地址和该 IP 地址在相同网段，之后访问该 IP 地址进行登录。

6.3 DHCP 服务器

6.3.1 概述

本 AP 提供了 DHCP 服务器，可以为局域网中的客户端计算机自动分配 IP 地址信息。默认情况下，AP 禁用了 DHCP 服务器功能。

提示

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，系统将自动修改本 AP 的 DHCP 地址池，使其和新的 LAN 口 IP 在同一网段。

6.3.2 配置 DHCP 服务器

1. 进入「网络设置」>「DHCP 服务器」页面。
2. 配置各项参数（一般仅需修改“DHCP 服务器”、“网关地址”、“首选 DNS 服务器”）。
3. 点击 **保存** 。

----完成

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。默认禁用。
起始 IP 地址	DHCP 地址池（即 DHCP 服务器可分配的 IP 地址范围）的开始 IP 地址，默认为 192.168.0.100。
结束 IP 地址	DHCP 地址池的结束 IP 地址，默认为 192.168.0.200。 提示 起始 IP 地址和结束 IP 地址必须与 AP 的 IP 地址在同一网段。
租期	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”。
子网掩码	DHCP 服务器分配给客户端的子网掩码，默认为 255.255.255.0。
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。默认为 192.168.0.254。 提示 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 192.168.0.254。 提示 为了使局域网计算机能够正常上网，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。

注意

如果网络中已存在其它的 DHCP 服务器，为避免地址分配冲突，请确保 AP 的 IP 池地址段和其它 DHCP 服务器的 IP 池地址段没有重合！

6.3.3 查看 DHCP 用户列表

当 AP 启用 DHCP 服务器时，借助 DHCP 用户列表，您可以了解局域网中从本 DHCP 服务器获取 IP 地址的计算机的详细信息：主机名、IP 地址、MAC 地址、租期。

进入页面：点击「网络设置」>「DHCP 服务器」>「DHCP 用户列表」。

序号	主机名	IP地址	MAC地址	租期
1	iPhone	192.168.0.200	cc:08:8d:8e:9f:a6	23:59:38

如果要查看最新的 DHCP 用户列表信息，请点击 **刷新** 。

7 无线设置

7.1 基本设置

7.1.1 概述

AP 的「基本设置」模块用于配置 AP 的 SSID 相关参数。

广播 SSID

AP 广播其 SSID 时，周围的无线用户可以扫描到该 SSID。禁用“广播 SSID”后，AP 不广播其 SSID，周围的无线用户也就扫描不到该 SSID，此时，如果要连接到该 SSID 的无线网络，首先必须手动在无线客户端上输入该 SSID，这在一定程度上增强了无线网络的安全性。

需要注意的是：禁用“广播 SSID”后，如果黑客利用其他手段获得 SSID，仍然可以接入目标网络。

客户端隔离

类似于有线网络的 VLAN，将连接到同一 SSID 的所有无线用户完全隔离，使其只能访问 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。

组播转单播

当前无线用户日益增多，而无线/有线带宽资源却相当有限，为了有效的解决单点发送、多点接收的问题，组播技术被大规模应用于网络，节省了带宽，有效地避免了网络拥塞。

然而，由于无线网络的开放性，如果在某个无线接口上存在大量用户，但只有一个用户是组播数据的真正接收者，传统的组播技术会将数据发送至该无线接口下所有用户，无形中占用了有限的无线资源，可能导致无线信道拥塞；同时对于 802.11 网络来说，组播流转发并不安全。

AP 的组播转单播特性，可以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

最大客户端数量参数用于限制接入 SSID 对应无线网络的无线用户数量，当连上该 SSID 的无线用户数达到此值后，该 SSID 不再接受新的无线连接请求。设置最大客户端数量可以避免 AP 一些 SSID 负载过大导致用户体验不佳，而另外一些 SSID 却闲置带宽的情况。

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，本系列 AP 提供以下安全模式：不加密、WEP、WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK、WPA、WPA2 供用户选择。

- **不加密**

即不加密无线网络，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），WEP 使用一个静态的密钥来加密所有通信，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，不建议用户使用此加密方式。

- **WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK**

属于 WPA/WPA2 个人模式，其中，Mixed WPA/WPA2-PSK 兼容 WPA-PSK、WPA2-PSK。

三者都采用预共享密钥认证，用户设置的密钥只用来验证身份，数据加密密钥由 AP 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。

- **WPA、WPA2**

为了改善 WPA/WPA2 个人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 来进行用户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，但加密过程则没有区别。

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，有效减少信息泄漏的可能性。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，并成为高安全无线网络的首选接入方式。

7.1.2 修改基本设置

如果要修改某 SSID 的相关设置，请按如下步骤操作：

1. 进入「无线设置」>「基本设置」页面。
2. 在第 1 行，选择要修改相关参数的 SSID。
3. 根据需要修改各参数（一般只需修改“启用”、“SSID”以及“安全模式”相关设置）。
4. 点击 **保存** 。

----完成

参数说明

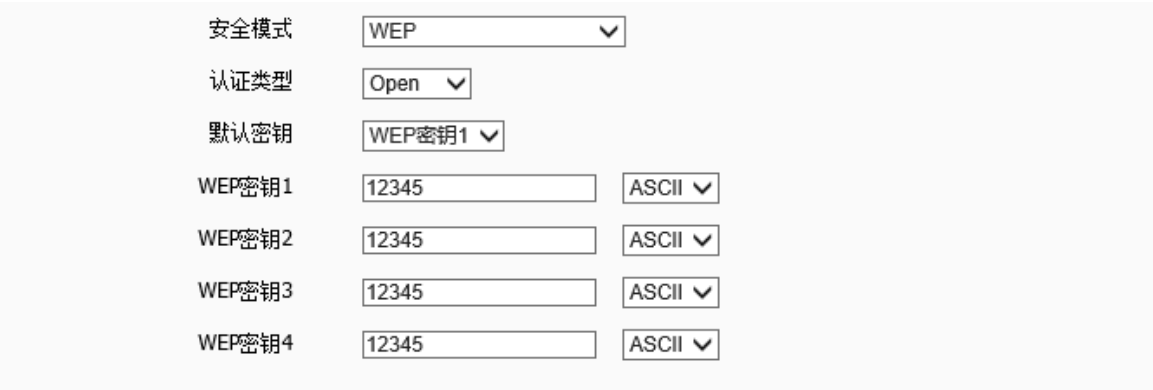
标题项	说明
SSID	选择当前要设置的 SSID。 AP 支持 2 个 SSID，其中，页面显示的第 1 个 SSID 为 AP 的主 SSID。
启用	启用/禁用所选择的 SSID。 主 SSID默认启用。其它 SSID 默认禁用，可根据需要启用。
广播 SSID	所选择 SSID 的广播状态。 – 启用：AP 广播该 SSID，周围无线设备可以扫描到该 SSID。 – 禁用 :AP 不广播该 SSID ,无线设备连接该 SSID 的 Wi-Fi 时 ,需要正确输入该 SSID。 提示 AP 支持“自动隐藏 SSID”。即，如果当前接入该 SSID 的无线设备数量达到了设置的 最大

标题项	说明
	客户端数量，AP 将不广播该 SSID。
客户端隔离	– 启用：连接在所选择 SSID 下的设备之间不能互相通信，可增强无线网络的安全性。 – 禁用：连接在所选择 SSID 下的设备之间能互相通信。默认为“禁用”。
组播转单播	– 启用：启用组播转单播功能。 – 禁用：禁用组播转单播功能。
最大客户端数量	所选择 SSID 允许同时接入的无线设备的最大数量。 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。 已启用的 SSID 的最大客户端数量总和不能超过 128。
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（汉字）。
中文 SSID 编码格式	该 SSID 中的中文字符采用的编码格式，仅当 SSID 中含有中文字符时此项设置有效。默认为 UTF-8。 如果 AP 同时启用 2 个中文 SSID，建议一个 SSID 选择 UTF-8，另一个选择 GB2312，以支持任意无线客户端识别并连接。
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。点击超链接可以了解对应安全模式的详细说明。

■ 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

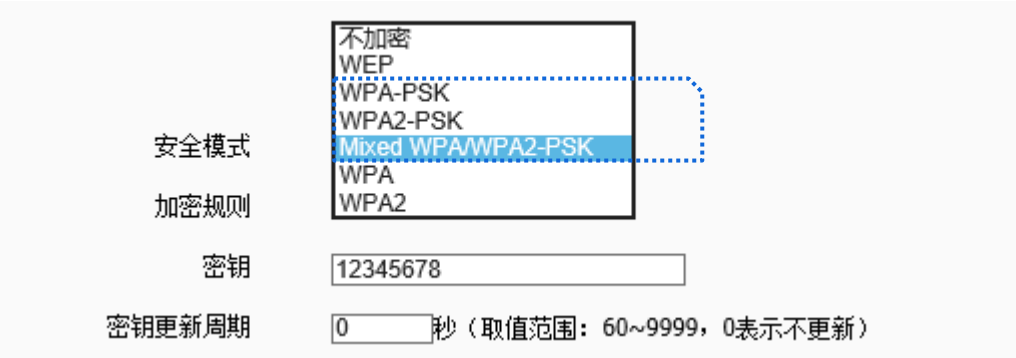


参数说明

标题项	说明
认证类型	WEP 加密时使用的认证方式：Open、Shared 或 802.1x。三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

标题项	说明
	联，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。 – 802.1x：采用“802.1x 身份认证+WEP 加密”。802.1x 协议仅仅关注端口的打开与关闭，合法用户接入时，打开端口；非法用户接入或没有用户接入时，端口处于关闭状态。
默认密钥	Open 和 Shared 认证时，用于指定对应 SSID 当前使用的 WEP 密钥。 如：默认密钥为“WEP 密钥 2”，则无线设备需要使用“WEP 密钥 2”设置的无线密码连接对应 SSID。
ASCII	Open 或 Shared 认证时，可选择的密钥字符类型之一。 此时，WEP 密钥可以输入 5 或 13 个 ASCII 字符。
Hex	Open 或 Shared 认证时，可选择的密钥字符类型之一。 此时，WEP 密钥可以输入 10 或 26 个十六进制数（0-9，a-f，A-F）。
RADIUS 服务器	802.1x 认证时设置。 进行身份认证的 RADIUS 服务器的 IP 地址/认证端口/共享密钥。
RADIUS 端口	
RADIUS 密码	

WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK



参数说明

标题项	说明
安全模式	WPA/WPA2 个人级安全模式：WPA-PSK、WPA2-PSK 或 Mixed WPA/WPA2-PSK。 – 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，WPA-PSK 只可选择“AES”或“TKIP”；WPA2-PSK 和 Mixed WPA/WPA2-PSK 还可选择“TKIP&AES”。

标题项	说明
	– AES：高级加密标准。 – TKIP：时间密钥完整性协议。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。可输入 8~63 个 ASCII 码或 8~64 个十六进制数。
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。 为 0 表示不更新。

■ WPA、WPA2

参数说明

标题项	说明
安全模式	选择安全模式：WPA 或 WPA2。 – WPA：此时，SSID 对应的无线网络采用 WPA 安全模式。 – WPA2：此时，SSID 对应的无线网络采用 WPA2 安全模式。
RADIUS 服务器	进行身份认证的 RADIUS 服务器的 IP 地址。
RADIUS 端口	RADIUS 服务器使用的认证端口。
RADIUS 密码	RADIUS 服务器设置的共享密钥。
加密规则	选择 WPA 加密规则：AES、TKIP 或 TKIP&AES。 – AES：高级加密标准。 – TKIP：时间密钥完整性协议。 – 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。

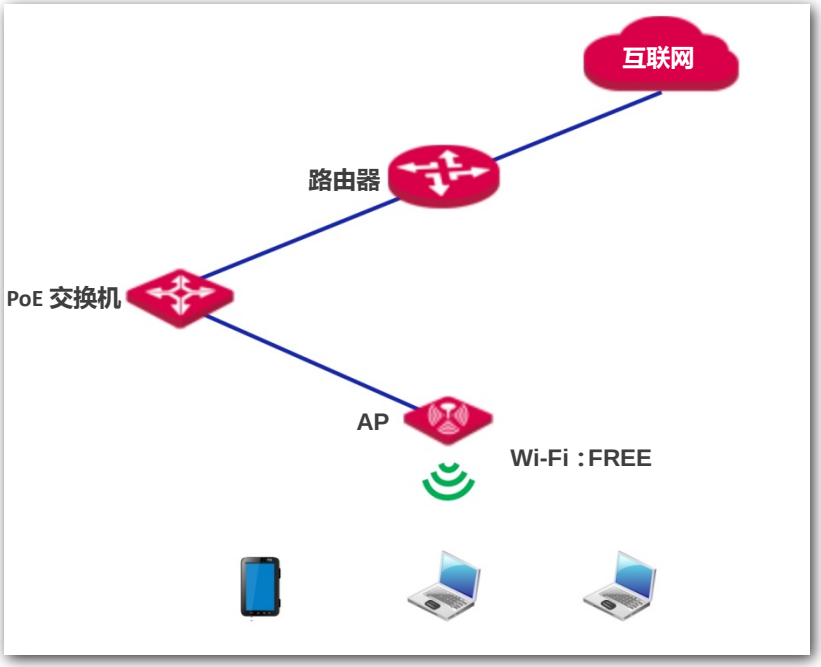
标题项	说明
	为 0 表示不更新。

7.1.3 基本设置举例

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：客人连接 Wi-Fi 即可上网，不需要无线密码。



配置步骤

假设使用 AP 的第 2 个 SSID 进行设置。

1. 进入「无线设置」>「基本设置」页面。
2. SSID：点击下拉框，选择第 2 个 SSID。
3. 启用：勾选复选框。
4. SSID：修改为“FREE”。
5. 安全模式：选择“不加密”。
6. 点击 **保存** 。

----完成

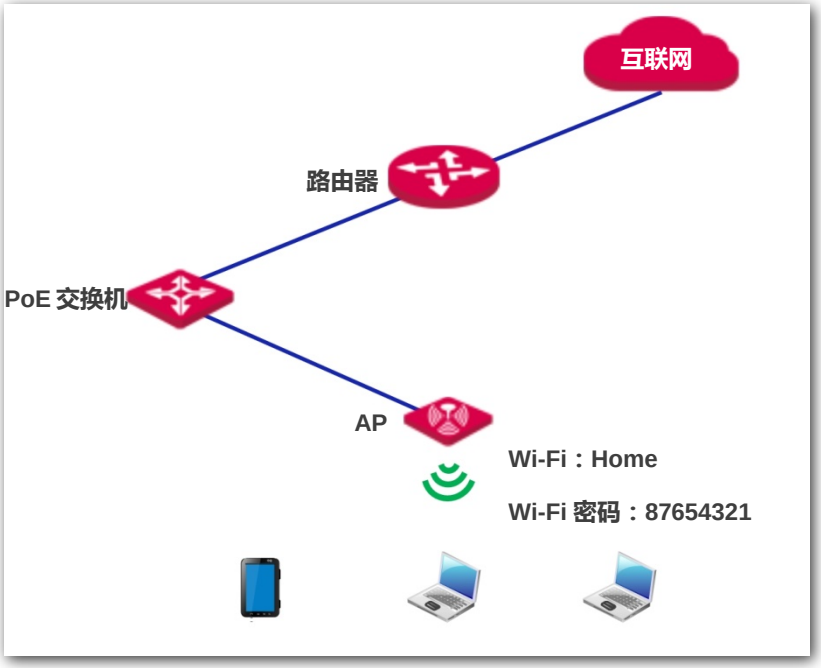
验证配置

无线设备连接无线网络“FREE”，不需要输入无线密码就可以连接成功。

WPA/WPA2-PSK 加密无线网络配置举例

组网需求

家用的无线网络，要求有一定安全性，且配置简单。针对上述需求，建议采用 WPA/WPA2 个人级安全模式。具体如下图所示。



配置步骤

假设使用 AP 的第 2 个 SSID 进行设置。

1. 进入「无线设置」>「基本设置」页面。
2. SSID：点击下拉框，选择第 2 个 SSID。
3. 启用：勾选复选框。
4. SSID：修改为“Home”。
5. 安全模式：建议选择“WPA2-PSK”>“AES”。
6. 密钥：修改为“87654321”。
7. 点击 **保存** 。

----完成

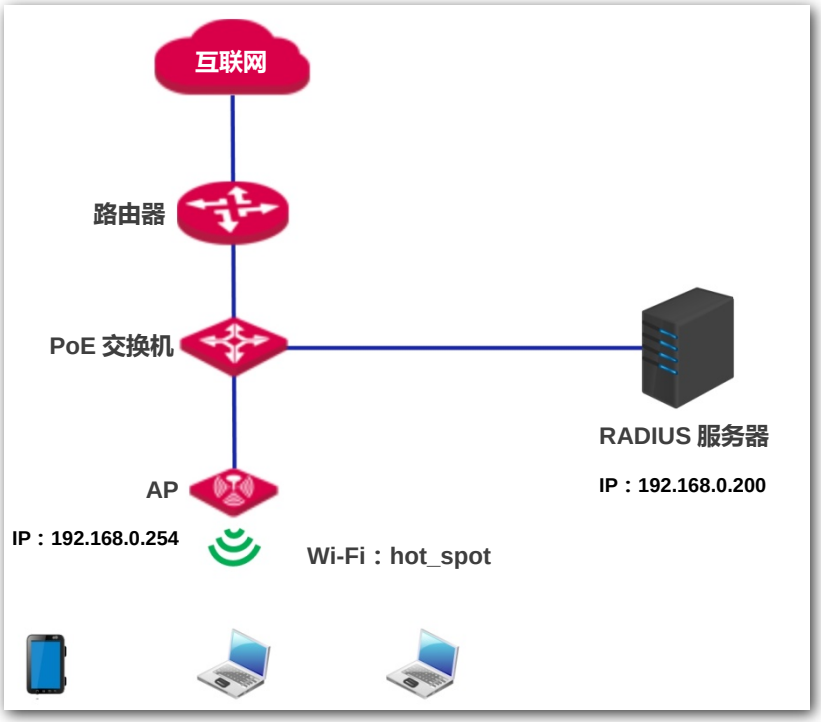
验证配置

无线设备连接无线网络“Home”时，输入无线密码“87654321”即可连接成功。

WPA/WPA2 加密无线网络配置举例

组网需求

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，无需考虑成本及维护问题。针对上述需求，建议采用 WPA 或 WPA2 安全模式。具体如下图所示。



配置步骤

一、配置 AP

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。

假设使用 AP 的第 2 个 SSID 进行设置。

1. 进入「无线设置」>「基本设置」页面。
2. SSID：选择第 2 个 SSID。
3. 启用：勾选复选框。
4. SSID：修改为“hot_spot”。
5. 安全模式：建议选择“WPA2”。
6. RADIUS 服务器/端口/密码：分别输入“192.168.0.200”、“1812”、“12345678”。
7. 加密规则：建议选择“AES”。
8. 点击 **保存** 。

----完成

二、配置 RADIUS 服务器

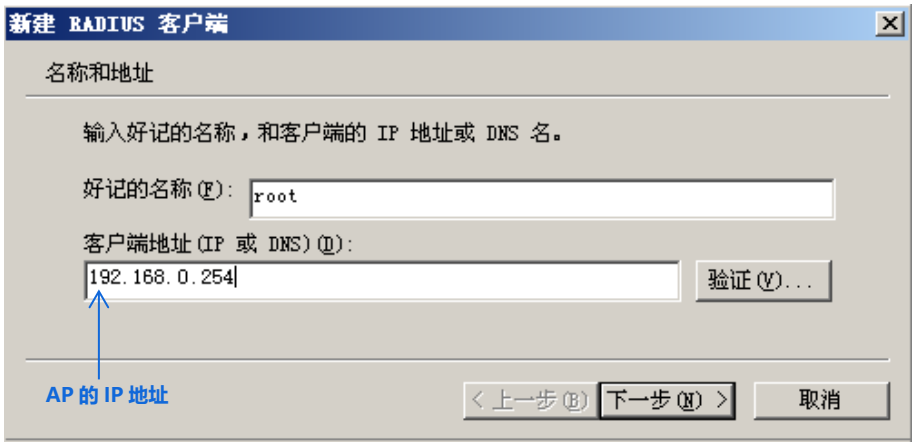
提示

以 Windows 2003 服务器上的 RADIUS 服务器为例说明。

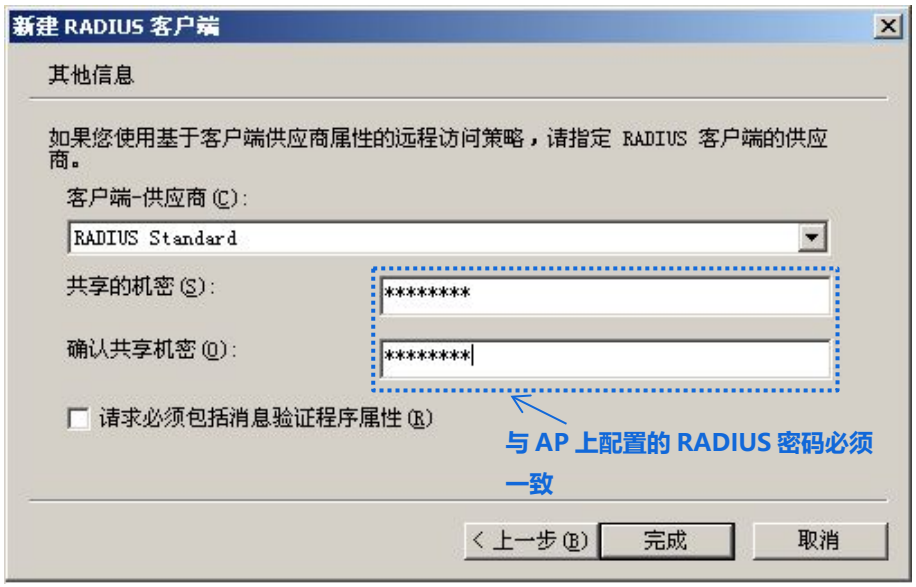
1. 配置 RADIUS 客户端。

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”。

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 。



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

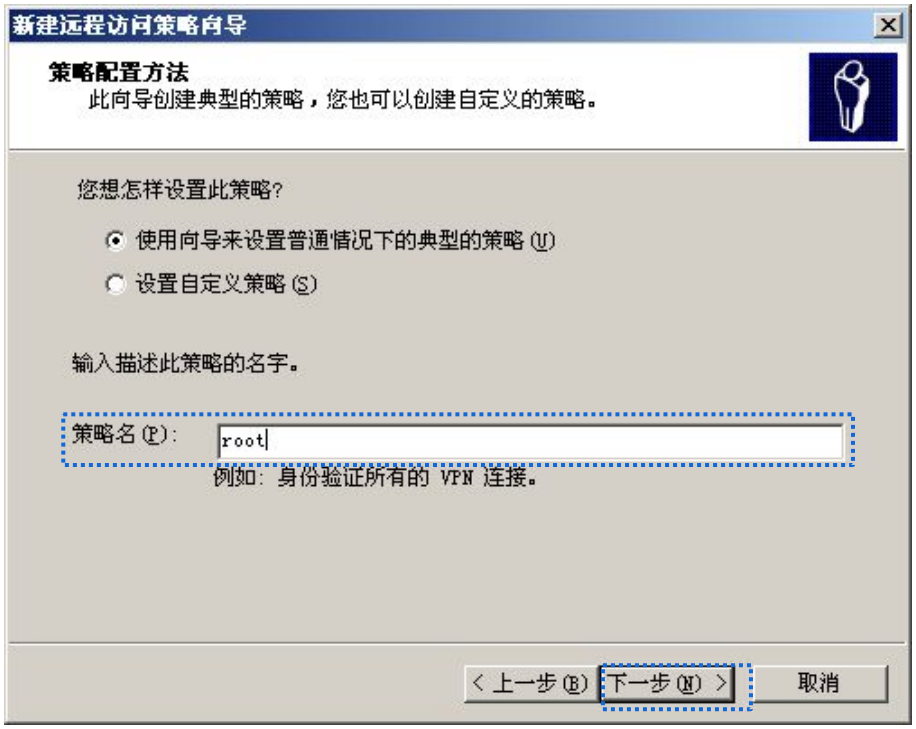


2. 配置远程访问策略。

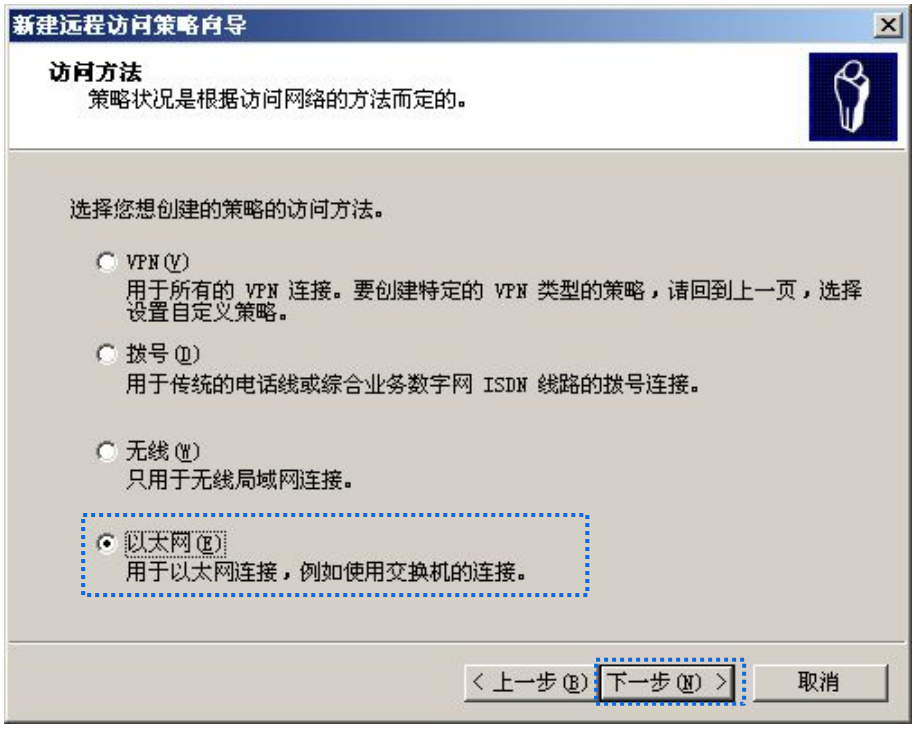
右键单击“远程访问策略”，选择“新建远程访问策略”。

弹出新建远程访问策略向导，点击 下一步 。

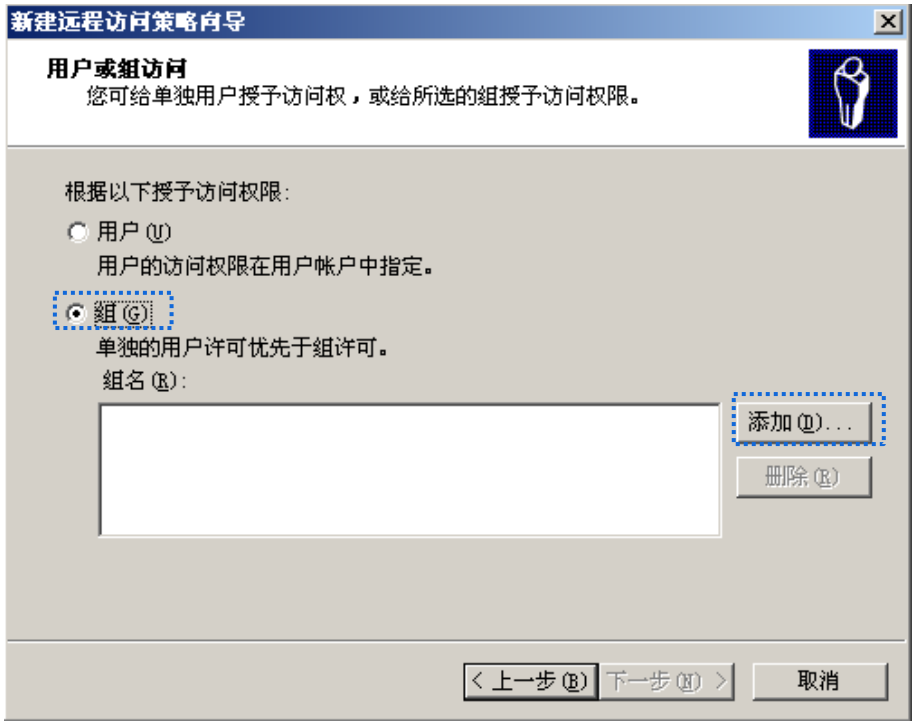
设置策略名，点击 下一步 。



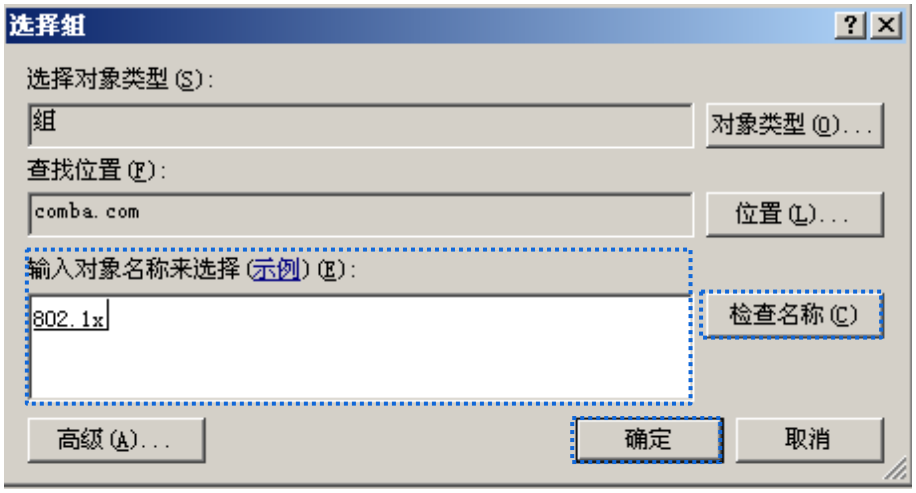
选择“以太网”，点击 下一步 。



选择“组”，点击 添加 。

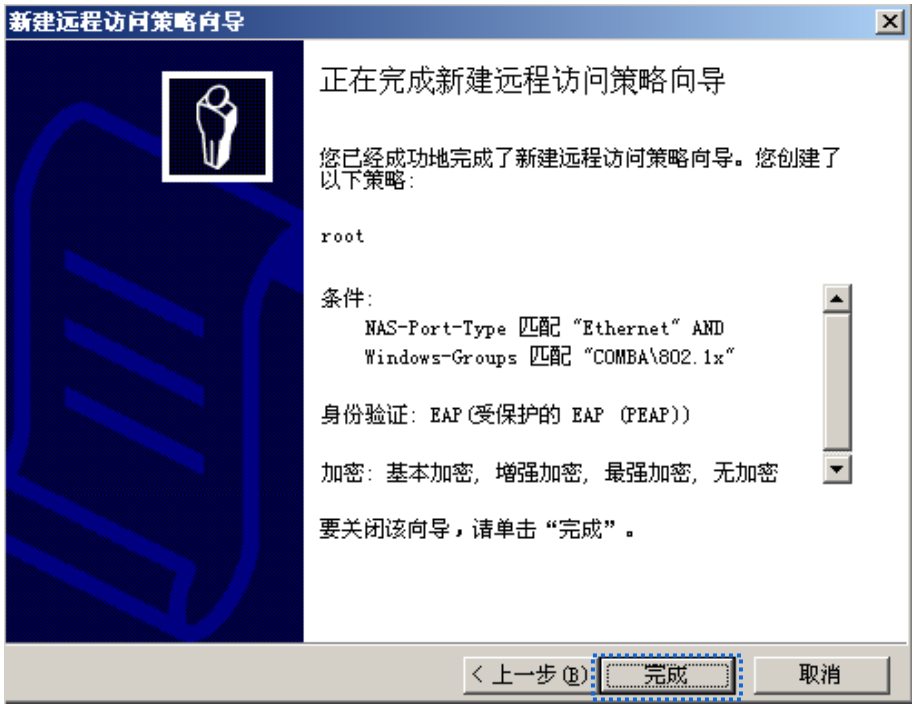


在“输入对象名称来选择”中输入 802.1x，点击 检查名称 ，点击 确定 。

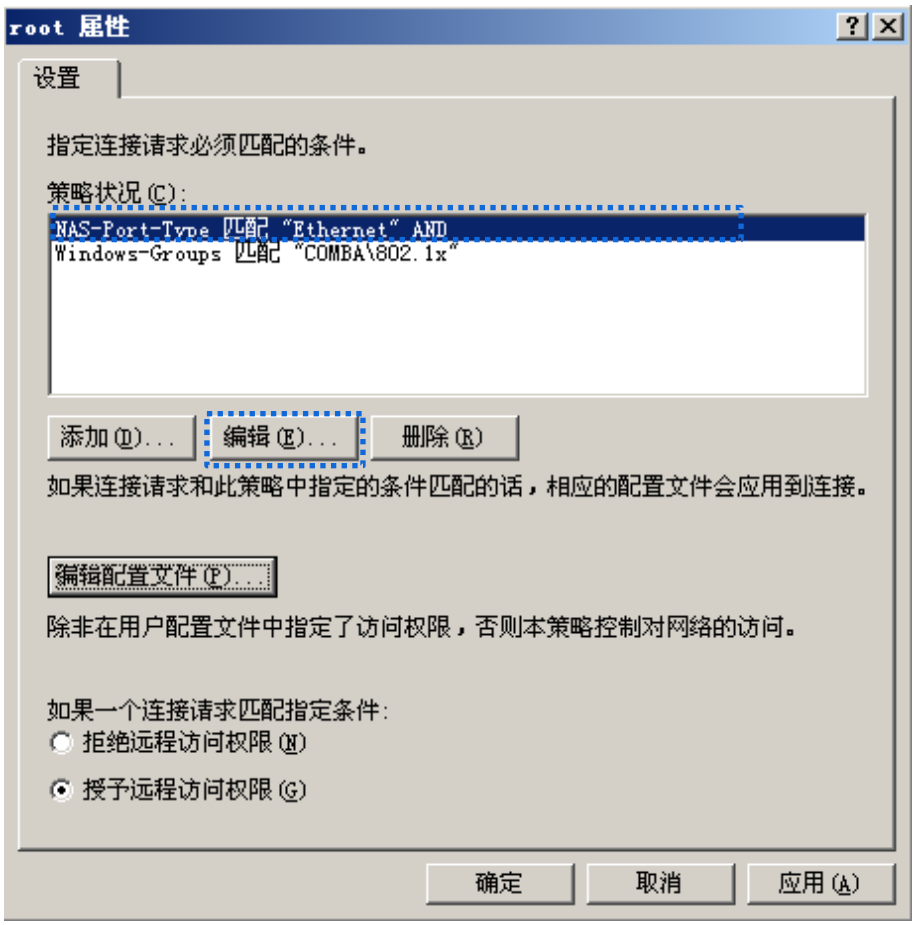


选择受保护的 EAP (PEAP)，点击 下一步 完成操作。

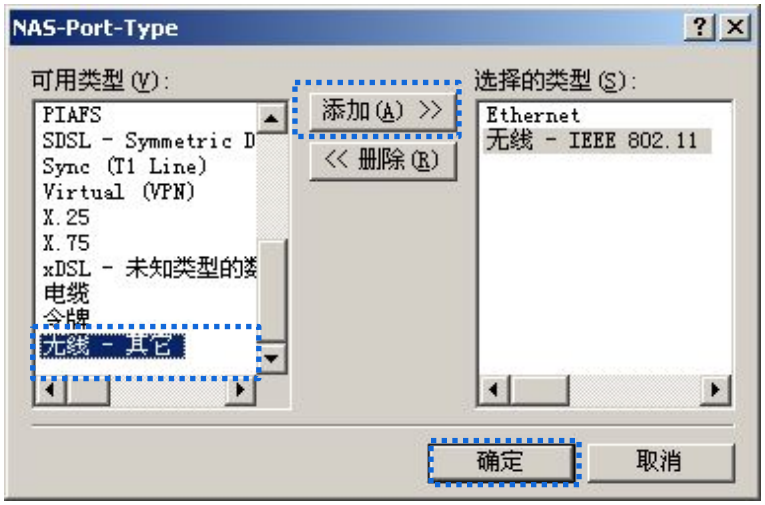
完成新建远程访问策略向导操作。



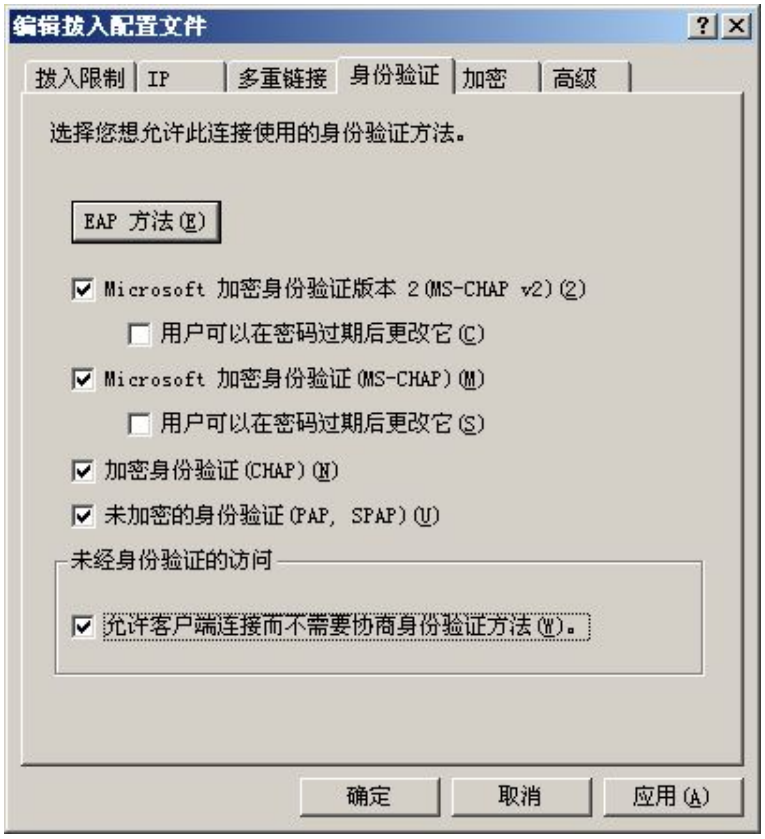
选中 root，点击右键，选择“属性”，在打开的窗口中，选择“授予远程访问权限”，然后选择“NAS-Port-Type 匹配“Ethernet”AND”，点击 编辑 。



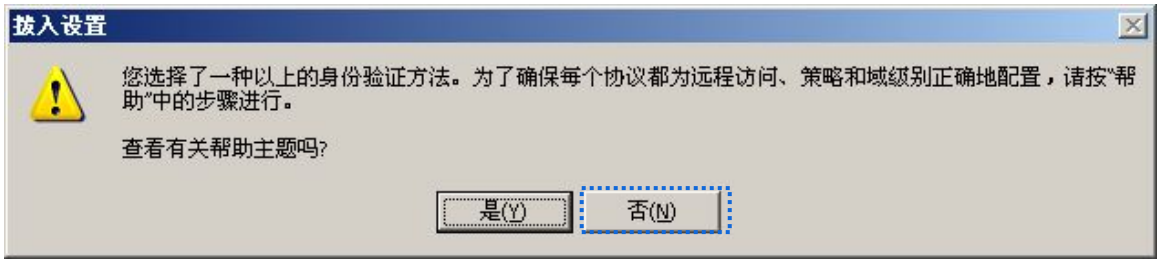
在出现的窗口选择“无线-其它”，点击 添加>> ，然后点击 确定 。



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。



在弹出的提示框，点击 否 ，确认返回。



3. 配置用户信息。

新建用户，并将用户添加到组 802.1x。

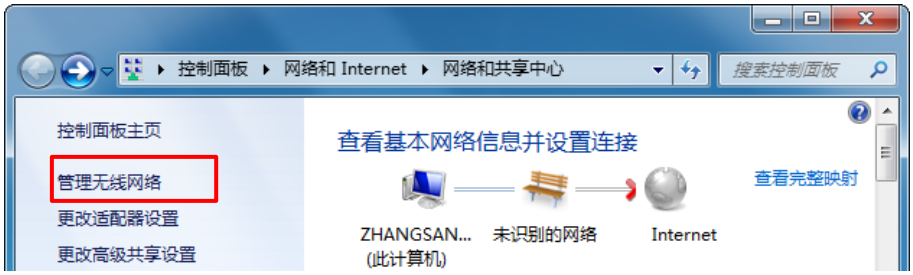
----完成

三、配置用户设备

提示

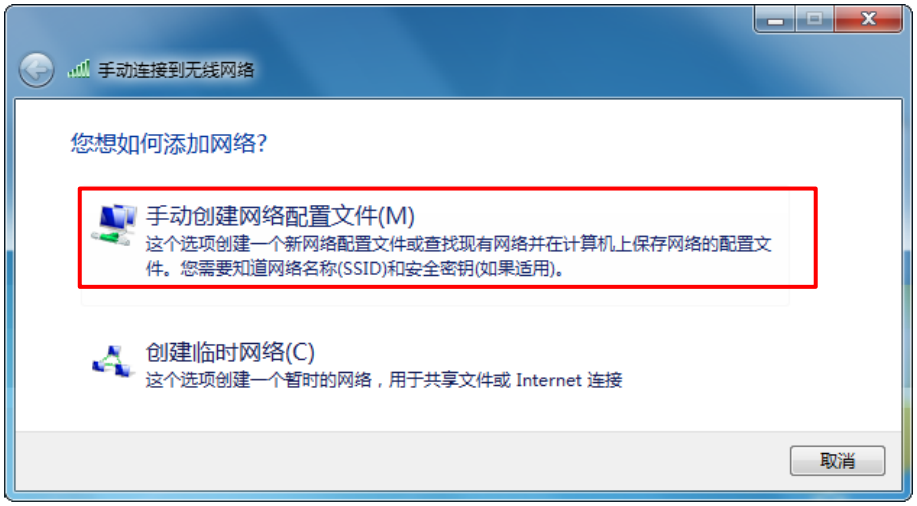
本文以 Windows 7 系统为例说明。

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”。

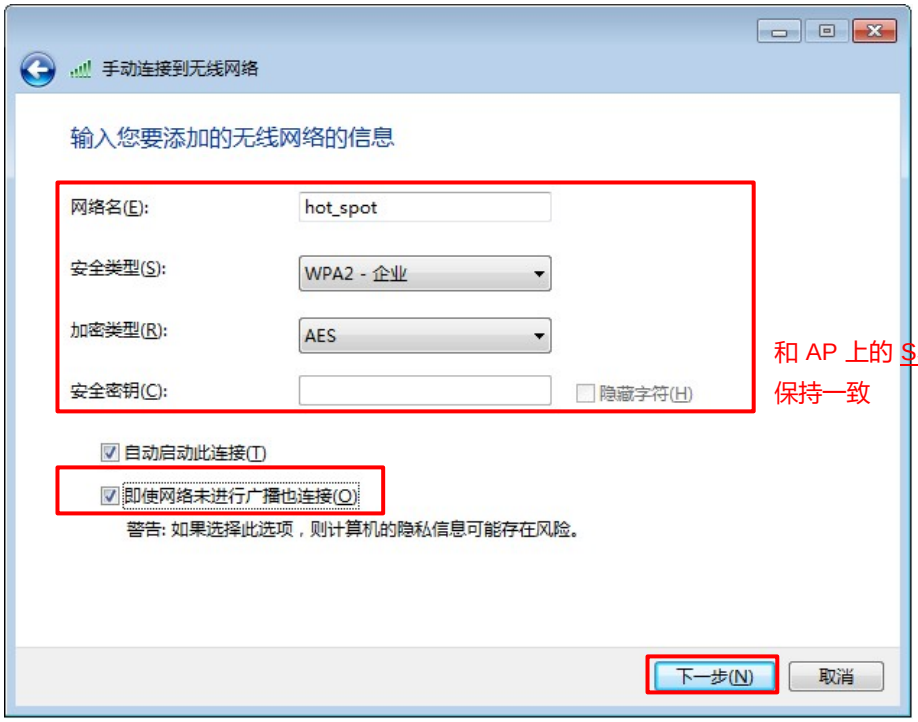


点击“添加”。

选择“手动创建网络配置文件（M）”。

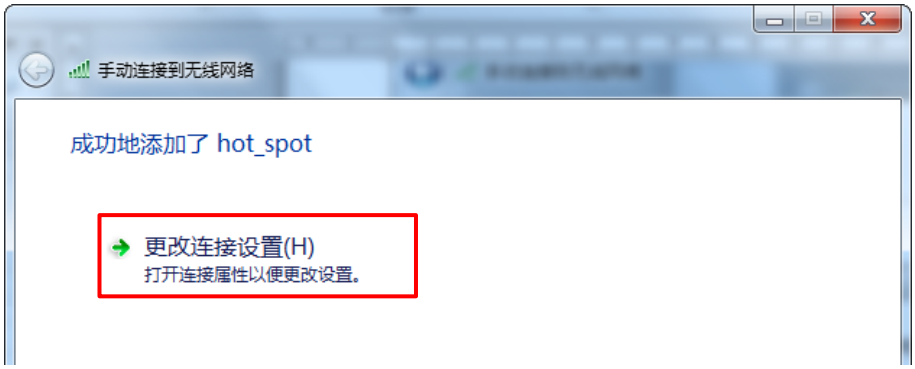


如下图所示输入无线网络信息，勾选“即使网络未进行广播也连接”，然后点击 下一步 。

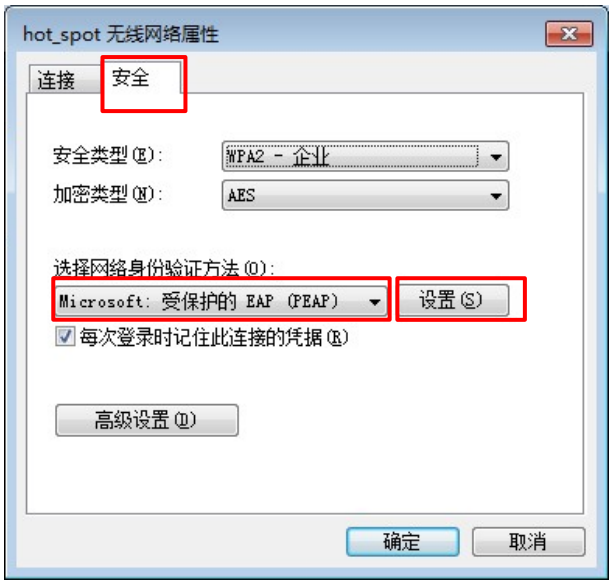


和 AP 上的 SSID 安全模式设置保持一致

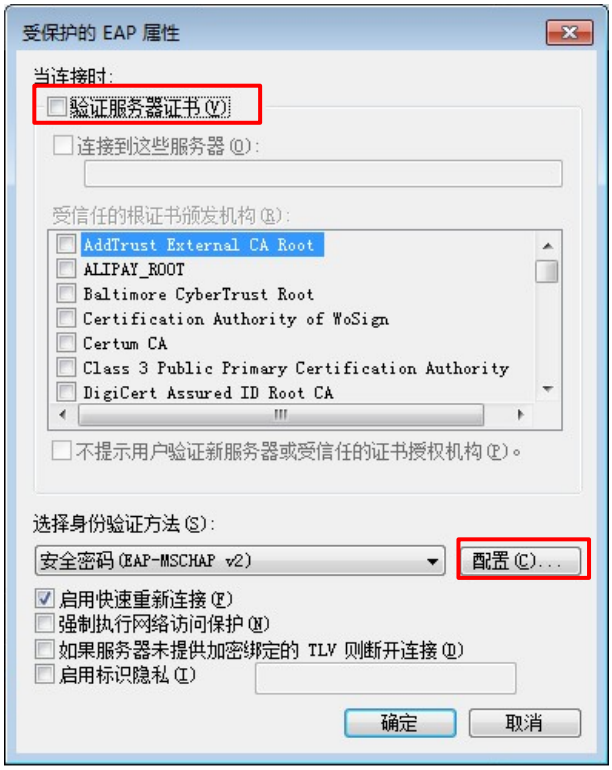
点击“更改连接设置（H）”。



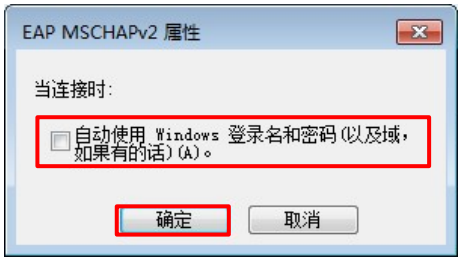
选择“安全”页签，身份验证方法选择“Microsoft：受保护的 EAP（PEAP）”，然后点击 设置 。



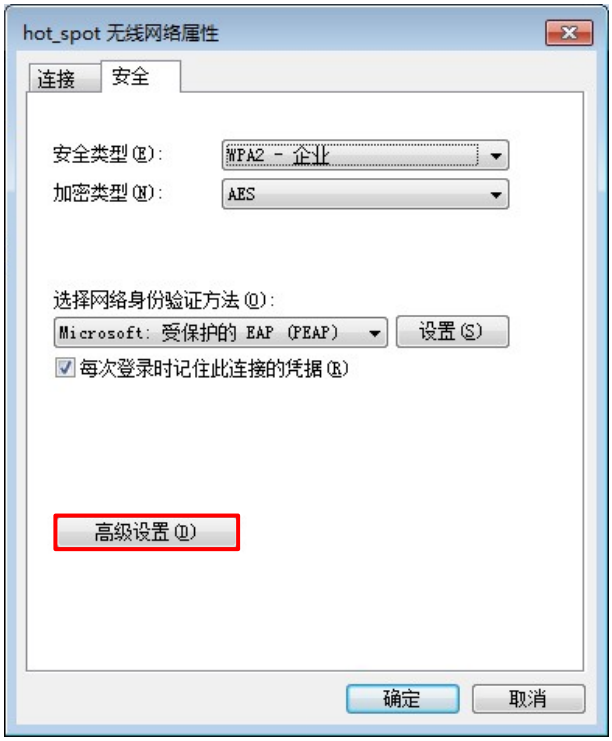
取消“验证服务器证书”，然后点击 配置 。



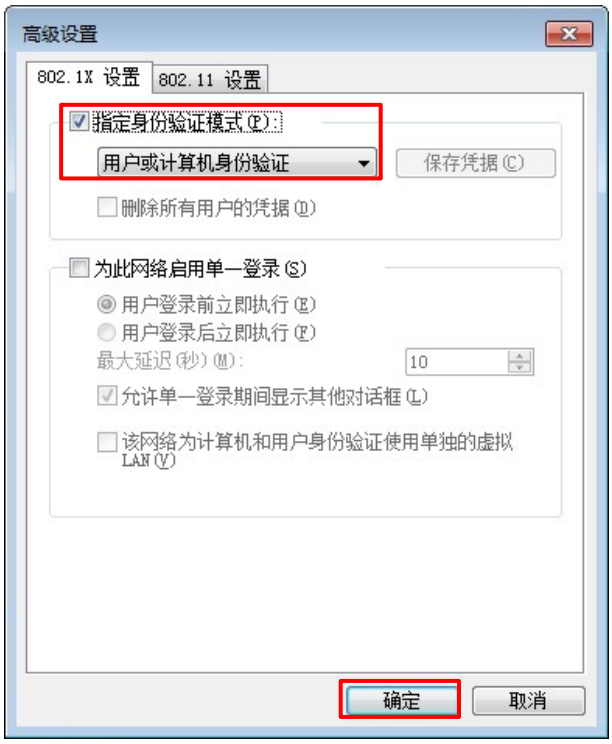
取消“自动使用 windows 登录名和密码”，点击 确定 。



点击 高级设置 。



指定身份验证模式为“用户或计算机身份认证”，然后点击 确定 。



点击 关闭 。

然后，在电脑桌面右下角连接 AP 的无线网络，本例为“hot_spot”。

当弹出用户名/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 。

验证配置

用户设备连接无线网络“hot_spot”成功。

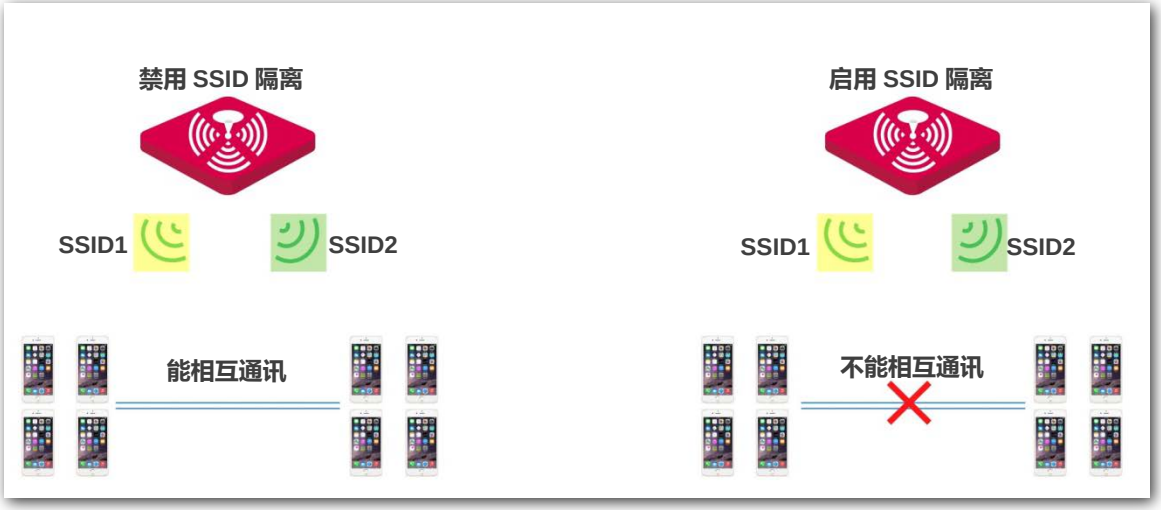
7.2 射频状态

7.2.1 概述

AP 的「射频状态」模块用于配置 AP 的射频相关参数，如，国家或地区、网络模式、信道、SSID 隔离等。下文简要说明一下 SSID 隔离功能。

SSID 隔离

将 连接到同一 AP 但不同 SSID 的无线用户隔离。如 :用户 1 连上 AP 的 SSID1 ,用户 2 连上 SSID2，则启用“SSID 隔离”后，用户 1 和用户 2 之间不能相互通讯。



7.2.2 修改射频设置

1. 进入「无线设置」>「射频状态」页面。
2. 根据需要修改各参数（一般只需修改“开启无线”、“信道”、“锁定信道”）。
3. 点击 **保存** 。

----完成

参数说明

标题项	说明
开启无线	用于开启/关闭 AP 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。默认为“中国”。
网络模式	选择无线网络模式。可选择 11b 模式、11g 模式、11b/g 模式、11b/g/n 模式。在未“锁定信道”的情况下可以设置。 – 11b 模式：AP 使用 11b 模式，此时，仅允许 802.11b 的无线设备连接到本 AP。 – 11g 模式：AP 使用 11g 模式，此时，仅允许 802.11g 的无线设备连接到本 AP。 – 11b/g 模式：AP 使用 11b/g 混合模式，此时，802.11b、802.11g 的无线设备可以连接到本 AP。 – 11b/g/n 模式：AP 使用 11b/g/n 混合模式，此时，802.11b、802.11g 以及工作在 2.4 GHz 的 802.11n 无线设备均可连接到本 AP。
信道	选择 AP 的工作信道。在未“锁定信道”的情况下可以设置。 Auto：表示 AP 根据周围环境情况自动调整工作信道。
信道带宽	AP 工作在 11b/g/n 模式，且未“锁定信道”的情况下可以设置，用于选择无线信道带宽。 – 20：AP 限制只能使用 20MHz 的信道带宽。 – 40：AP 优先使用 40MHz 的信道带宽，如果环境实在恶劣，将自动改为使用 20MHz 的信道带宽。 – 20/40：AP 根据周围环境，自动调整信道带宽为 20MHz 或 40MHz。
扩展信道	信道带宽为“40”或“20/40”，且未“锁定信道”的情况下可以设置，用于确定 AP 工作的频率段。
锁定信道	勾选后，将锁定 AP 的信道。信道锁定后，不可设置与信道相关的参数（国家或地区、网络

标题项	说明
	模式、信道、信道带宽、扩展信道）。
SSID 隔离	连接在 AP 不同 SSID 下的无线设备间的隔离状态。 – 禁用：连接在不同 SSID 下的无线设备之间能互相通信。 – 启用 :连接在不同 SSID 下的无线设备之间不能互相通信，可增强无线网络的安全性。
APSD	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，启用“APSD”能降低 AP 的电能消耗。默认禁用。
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。

7.3 信道扫描

7.3.1 概述

借助 “信道扫描” 功能 ,您可以对 AP 周围环境中的其它无线信号有一个大致了解 ,如 SSID、MAC、信道、信号强度等信息。之后，您就可以选择一个比较空闲的信道（如较少 AP 使用的信道）作为 AP 的工作信道，以提升无线传输效率。

7.3.2 执行信道扫描

1. 进入「无线设置」>「信道扫描」页面。
2. 点击 **扫描** 。

----完成

扫描结果如下图示例。

序号	SSID	MAC地址	网络模式	信道	信道带宽	安全模式	信号强度
1	IP-COM_E65616	d8:38:0d:e6:56:17	bgn	9	20	none	-30dBm
2	Guest	d8:38:0d:ee:ef:cd	bgn	11	20	wpa&wpa2/aes	-54dBm
3	VIP	d8:38:0d:2b:78:b0	bgn	6	40	wpa&wpa2/aes	-58dBm
4	IP-COM_000555	d8:38:0d:1e:ae:85	bgn	8	20	wpa&wpa2/aes	-58dBm
5	IP-COM_A8823C	d8:38:0d:a8:88:a2	bgn	5	20	wpa&wpa2/aes	-58dBm
6	IP-COM_772211	d8:38:0d:77:22:12	bgn	11	20	none	-62dBm
7	IP-COM_F61234	d8:38:0d:f6:12:34	bgn	2	20	none	-66dBm
8	IP-COM	d8:38:0d:1e:b6:c3	bgn	8	20	none	-70dBm

7.4 WMM 设置

7.4.1 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，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。

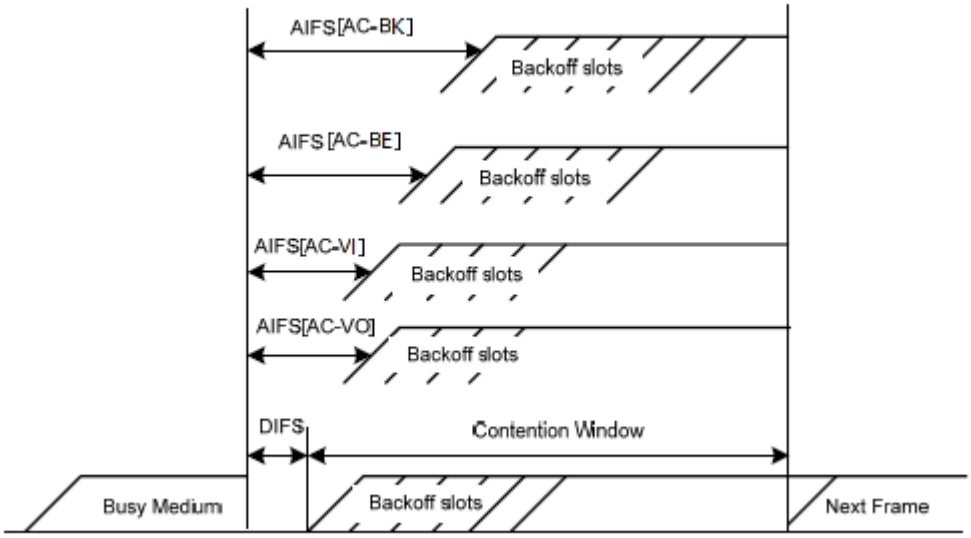
- **EDCA 参数**

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。

WMM 对每个 AC 赋予不同的信道竞争参数



- **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。

7.4.2 修改 WMM 设置

AP 默认启用了 WMM 功能，场景优化模式为“密集用户场景”。如果要修改 WMM 设置，请参考以下步骤。

1. 进入「无线设置」>「WMM 设置」页面。
2. WMM：选择“启用”。
3. 场景优化模式：根据需要，选择 WMM 优化模式。
4. 当场景优化模式选择为“自定义”时，请根据需要设置各项 WMM 参数。
5. 点击 **保存** 。

----完成

参数说明

标题项	说明
WMM	– 启用：启用 WMM 功能。 – 禁用：禁用 WMM 功能。
场景优化模式	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 的用户数等于或少于 10 人时，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 第 7.4.1 节 内容。

7.5 高级设置

7.5.1 概述

AP 的「高级设置」模块用于配置 AP 的射频性能优化参数，包括：Beacon 间隔、Fragment 阈值、RTS 门限、DTIM 间隔、接入信号强度限制、功率、无线前导码。

7.5.2 修改高级设置

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，以免降低无线性能！

1. 进入「无线设置」>「高级设置」页面。
2. 根据需要修改各参数。
3. 点击 **保存** 。

----完成

参数说明

标题项	说明
Beacon 间隔	发送 Beacon 帧的时间间隔，取值范围：20~999，单位：ms。 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。取值范围：256~2346，默认 2346，单位：字节。 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

标题项	说明
	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。 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。取值范围：1~2347，单位：字节。 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，取值范围：1~255，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包。
接入信号强度限制	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该 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。
功率	设置无线发射功率。在未“锁定功率”的情况下可以设置。 发射功率越大，则无线覆盖范围更广。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	勾选后，将锁定 AP 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。 默认长导码，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，可以选择短导码。

7.6 无线访问控制

7.6.1 概述

无线访问控制，即通过设置 MAC 地址过滤规则，限制可以使用 AP Wi-Fi 的用户。对于被限制使用 Wi-Fi 的用户，不能连接上对应 Wi-Fi。

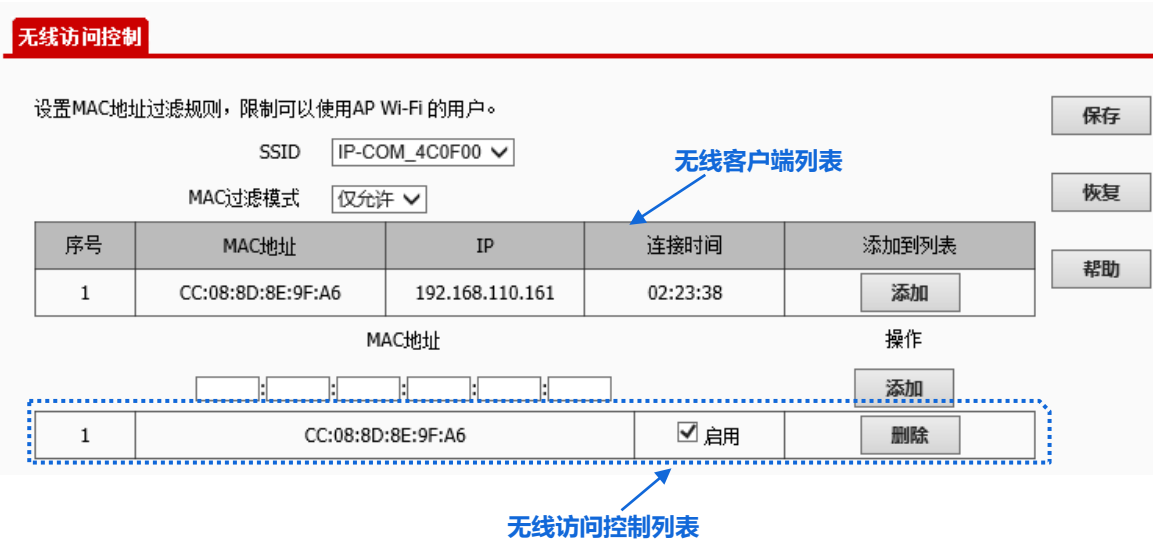
本 AP 支持三种 MAC 过滤模式：禁用、仅允许、仅禁止。

- 禁用：禁用无线访问控制功能。此时，任何无线设备都能使用 Wi-Fi。
- 仅允许：允许指定 MAC 地址的无线设备使用 Wi-Fi，拒绝其他无线设备使用。
- 仅禁止：拒绝指定 MAC 地址的无线设备使用 Wi-Fi，允许其他无线设备使用。

7.6.2 配置无线访问控制

1. 进入「无线设置」>「无线访问控制」页面。
2. SSID：选择要限制用户使用 Wi-Fi 的 SSID。
3. MAC 过滤模式：根据需要选择“禁用”、“仅允许”或“仅禁止”。
4. 当 MAC 过滤模式选择为“仅允许”或“仅禁止”时，在出现的 MAC 地址输入栏输入 MAC 地址，然后点击 **添加** 。

   如果要限制的无线设备已连接上 AP，还可以直接在无线客户端列表中的对应栏点击 **添加** ，快速添加该无线设备的 MAC 地址到无线访问控制列表。
5. 点击 **保存** 。



参数说明

标题项	说明
SSID	选择要限制无线设备连接的 SSID。
MAC 过滤模式	设置 MAC 地址过滤模式。 – 禁用：禁用无线访问控制功能。 – 仅允许：仅允许访问控制列表中的无线设备连接该 SSID。 – 仅禁止：仅禁止访问控制列表中的无线设备连接该 SSID，允许其他无线设备连接该 SSID。

7.6.3 无线访问控制配置举例

组网需求

大户型家庭进行无线组网，已专门配置了家用网络 SSID“Home”，现需要配置 AP，让该 SSID 仅供家庭成员接入。

可以使用 AP 的无线访问控制功能实现上述需求。假设家庭无线设备有三台，MAC 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

1. 进入「无线设置」>「无线访问控制」页面。
2. SSID：选择“Home”。
3. MAC 地址过滤模式：选择“仅允许”。
4. MAC地址 输入“C8:3A:35:00:00:01”，点击 **添加** 。重复本步骤，添加MAC“C8:3A:35:00:00:02”、“C8:3A:35:00:00:03”。
5. 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家庭网络“Home”，其他设备无法连接到该网络。

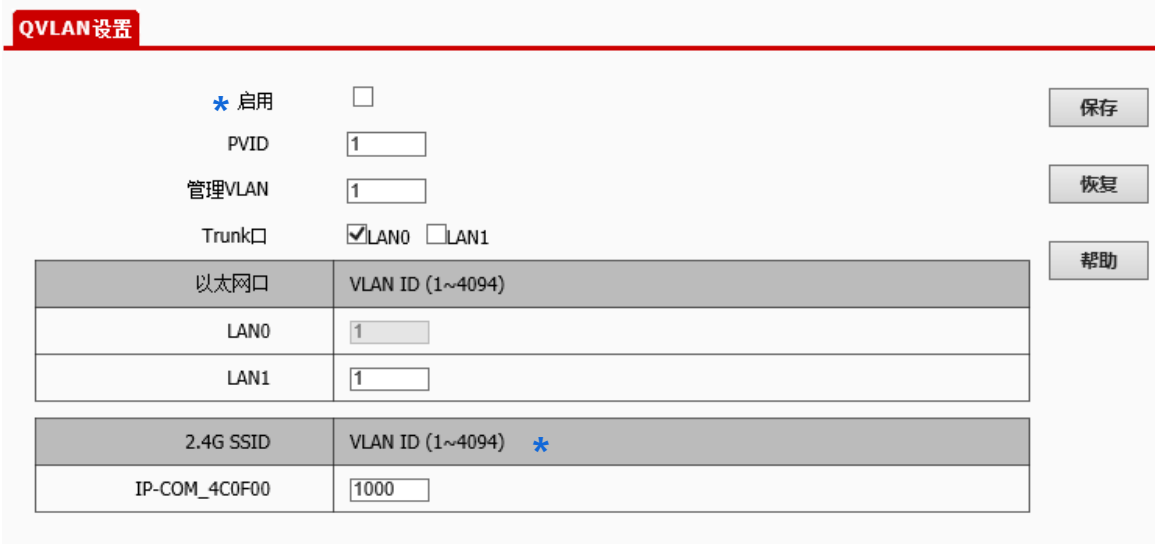
7.7 QVLAN

7.7.1 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。

7.7.2 配置 QVLAN

1. 进入「无线设置」>「QVLAN」页面。
2. 根据需要修改各参数（一般仅需修改“启用”、“2.4G SSID VLAN ID”）。
3. 点击 **保存** 。



----完成

参数说明

标题项	说明
启用	启用/禁用 AP 的 802.1Q VLAN 功能，默认禁用。
PVID	AP Trunk 口默认所属的 VLAN 的 ID，默认为“1”。
管理 VLAN	AP 的管理 VLAN ID，默认为“1”。 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	选择作为 AP Trunk 口的以太网口（有线 LAN 口），默认为“LAN0”。Trunk 口允许所有 VLAN 通过。

标题项	说明
	注意 启用 802.1Q VLAN 功能时，至少要选择一个 LAN 口作为 Trunk 口。 LAN0 对应 AP 的背面接口（PoE 供电、数据传输复用接口），LAN1 对应 AP 的正面接口（数据传输接口）。
以太网口	显示 AP 的以太网口：LAN0、LAN1。
VLAN ID	以太网口作为 Access 口时，对应的 VLAN ID。
2.4G SSID	显示 AP 当前已启用的 SSID。
VLAN ID	SSID 对应的 VLAN ID，默认均为“1000”，设置范围为 1~4094。 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。

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：

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 再发送。
Trunk			VID = 端口 PVID，去掉 Tag 发送。 VID ≠ 端口 PVID，保留 Tag 发送。

7.7.3 QVLAN 设置举例

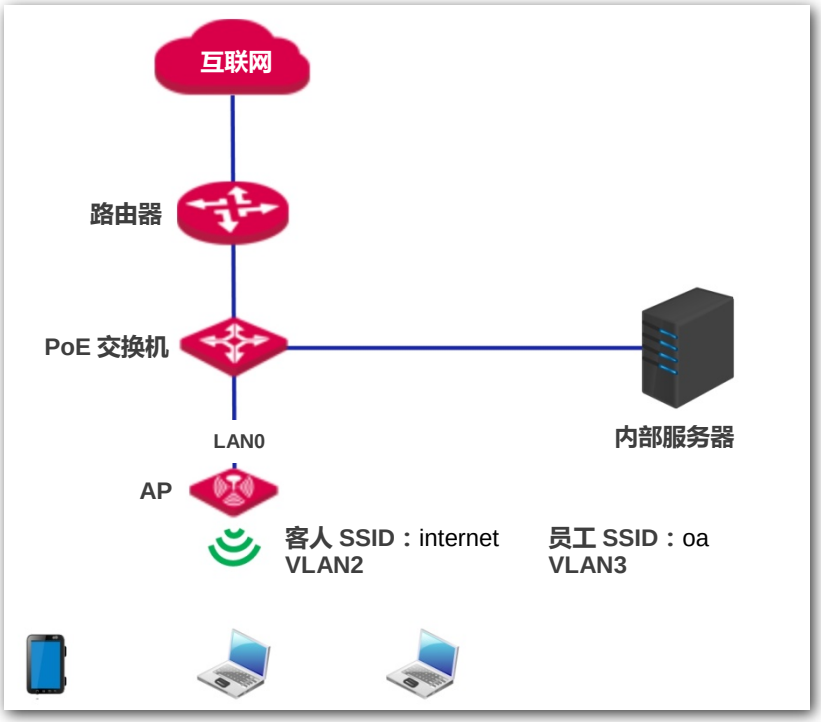
组网需求

某酒店内需要实现无线覆盖，需求如下：

- 客人接入无线网络时获得 VLAN 2 的权限，只能访问互联网。
- 员工接入无线网络时获得 VLAN 3 的权限，只能访问内网。

假设：客人 SSID 为“internet”，员工 SSID 为“oa”。

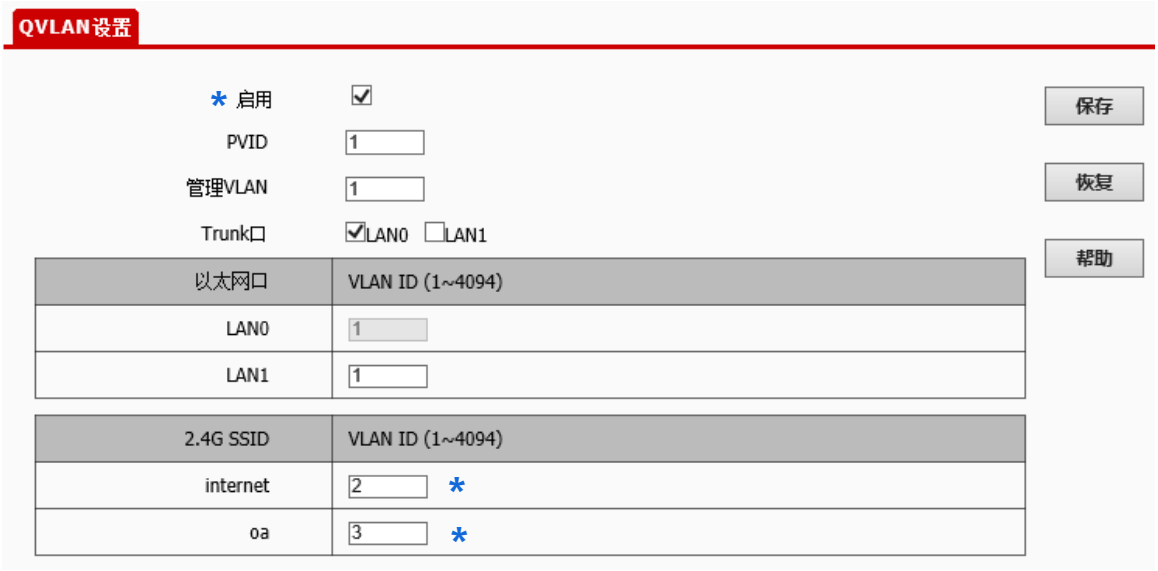
网络拓扑



配置步骤

一、配置 AP

1. 登录到 AP 的管理页面，转到「无线设置」>「QVLAN 设置」页面。
2. 启用：勾选复选框。
3. 修改 AP 各 SSID 的 VLAN ID，其中，internet 的 VLAN ID 为“2”，oa 的 VLAN ID 为“3”。
4. 点击 **保存** 。



----完成

等待 AP 自动重新启动即可。

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	Trunk	1
内部服务器	3	Access	3
路由器	2	Access	2

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。

验证配置

连接到“internet”的无线用户只能访问互联网；连接到“oa”的无线用户只能访问公司内网。

8 SNMP

8.1 概述

SNMP（Simple Network Management Protocol，简单网络管理协议）是目前 TCP/IP 网络中应用最为广泛的网络管理协议。利用 SNMP，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。

8.1.1 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。

8.1.2 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。

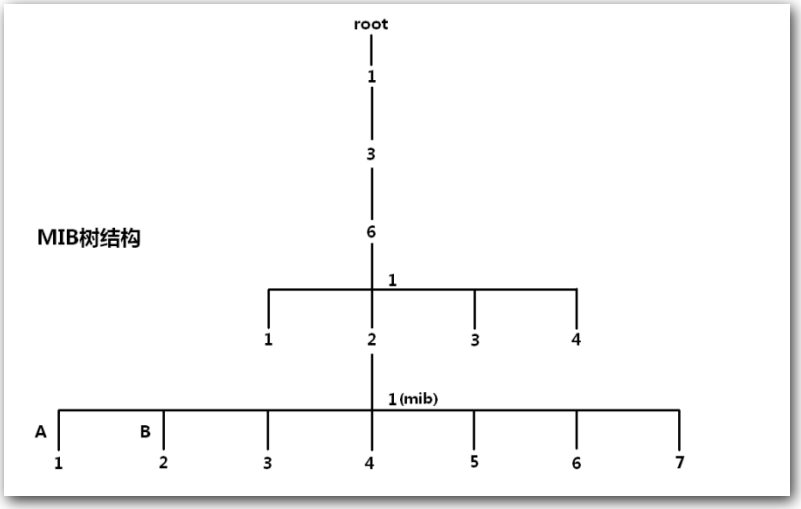
8.1.3 SNMP 协议版本

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。

8.1.4 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）。



8.2 配置 SNMP

1. 进入「SNMP」页面，选择“启用”SNMP 代理。
2. 设置 SNMP 相关参数。
3. 点击 **保存** 。

----完成

参数说明

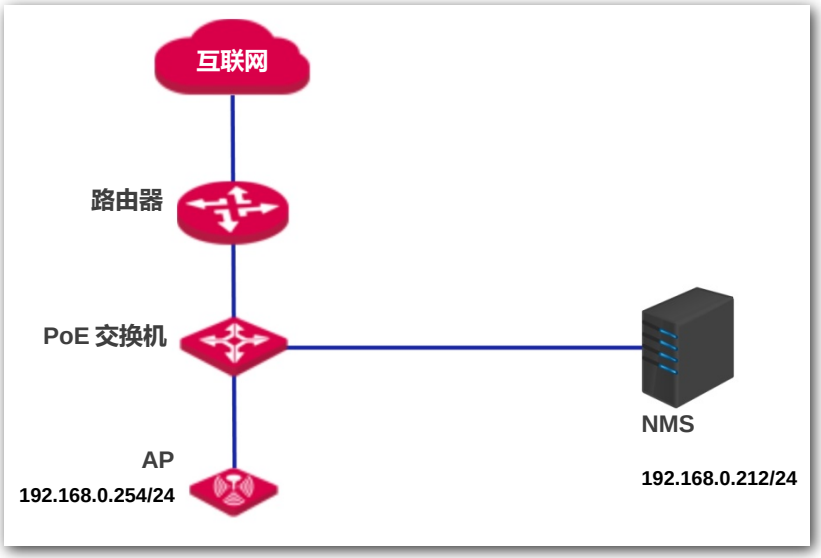
标题项	说明
SNMP 代理	禁用/启用 AP 的 SNMP 代理功能。默认为禁用。 SNMP 管理者和 SNMP 代理上的 SNMP 版本必须相同，才能成功互访。目前，AP 中的 SNMP 代理支持 SNMP v1 版本、SNMP v2c 版本。
管理员	AP 的管理员的名字，默认为“Administrator”。可根据实际情况修改。
设备名称	AP 的设备名称，默认为 AP 的产品型号。如 W30AP V4.0 的设备名称默认为“W30APV4.0”。 提示 建议修改设备名称，使您在使用 SNMP 管理 AP 时，能快速识别出对应的 AP 设备。
位置	AP 的安装位置，默认为“ShenZhen”。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，默认为“public”。 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，默认为“private”。 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。

8.3 SNMP 配置举例

组网需求

- 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”。

1. 登录 AP 的管理页面，再转到「SNMP」页面。
2. SNMP 代理：选择“启用”。
3. 设置 SNMP 相关参数：管理员、设备名称、位置、读 Community、读/写 Community。
4. 点击 **保存** 。

----完成

二、配置 NMS

在使用 SNMP v1/v2c 版本的 NMS 上，设置“只读 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。

验证配置

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 代理上某些参数的值。

9 部署模式

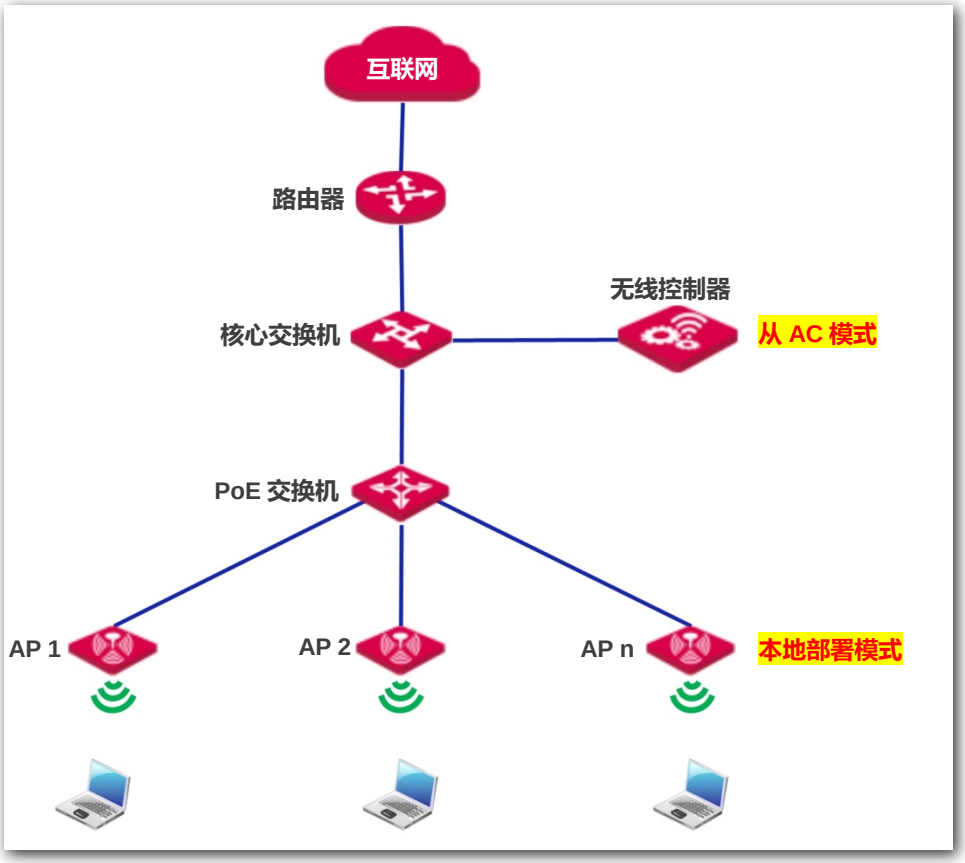
9.1 概述

网络中需要部署大量 AP 时，推荐在网络中搭建 IP-COM 无线控制器（AC1000/2000/3000，本文以 AC2000 为例说明），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。

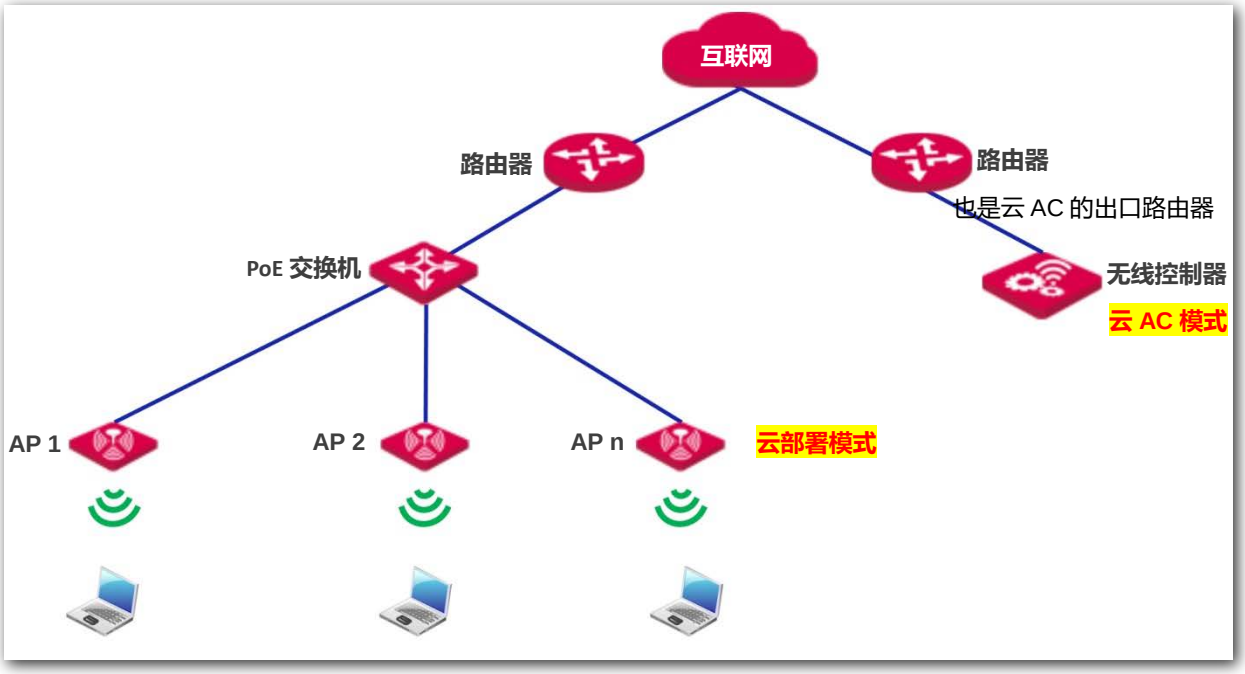
- **本地部署**

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。



- **云部署**

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”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。云部署模式组网拓扑图如下。



9.2 配置部署模式

AP 的部署模式默认为“本地部署”。

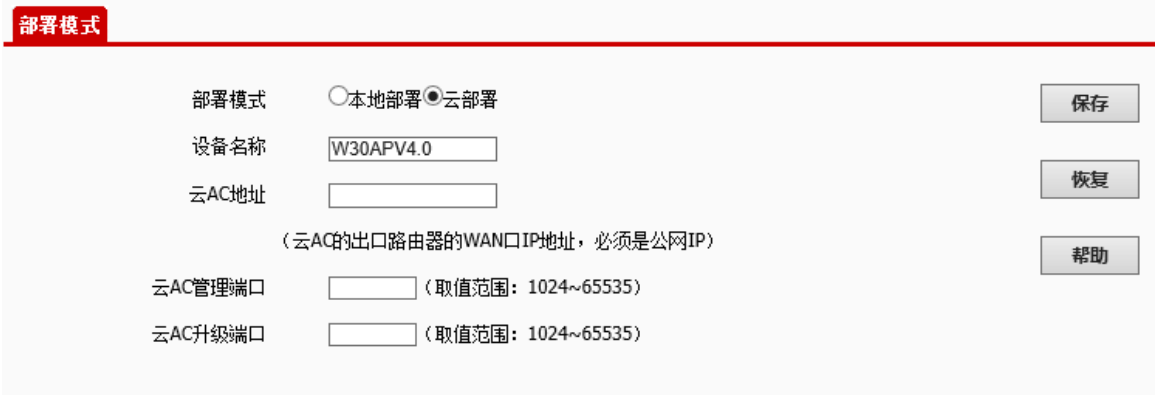
9.2.1 配置本地部署

1. 进入「部署模式」页面，选择部署模式为“本地部署”。
2. 点击 **保存** 。

----完成

9.2.2 配置云部署

1. 进入「部署模式」页面，选择部署模式为“云部署”。
2. 设置以下参数：设备名称、云 AC 地址、云 AC 管理端口、云 AC 升级端口。
3. 点击 **保存** 。



----完成

参数说明

标题项	说明
部署模式	AP 的部署管理模式，默认为“本地部署”。 – 本地部署：此时，AP 只能被本地网络中的 AC（即，位于同一局域网的 AC）管理。 – 云部署：此时，AP 只能被云 AC 管理。转换为云部署模式时，还需设置下述参数。
设备名称	AP 的名称，默认为对应 AP 的产品型号。 建议修改 AP 的设备名称，可以为该台 AP 的安装位置描述（如卧室），方便网络管理员对 AP 进行管理时，通过设备名称快速定位该 AP。
云 AC 地址	云 AC 出口路由器的公网 IP 地址或绑定的域名。
云 AC 管理端口	云 AC 出口路由器开放的端口号，用于管理云 AP。
云 AC 升级端口	云 AC 出口路由器开放的端口号，用于升级云 AP。

10 系统工具

10.1 软件升级

通过软件升级，可以使 AP 获得新增功能或更稳定的性能。

注意

为了确保升级正确，避免 AP 损坏，请在升级之前，务必确认新的软件适用于此 AP；升级过程中，请勿断开 AP 电源。

软件升级步骤：

1. 登陆 IP-COM 官方网站 www.ip-com.com.cn，下载对应型号 AP 更高版本的升级文件到本地电脑并解压。
2. 登录到 AP 的管理页面，转到「系统工具」>「软件升级」页面。
3. 点击 浏览... ，从本地电脑选择要加载的 AP 的升级文件。
4. 点击 **升级** 。

----完成

将出现进度条，等待进度条走完即可。进度条走完后，您可重新登录 AP，进入「状态」>「系统状态」页面，查看 AP 的“软件版本”，判断 AP 软件是否升级成功。

提示

为了更好的体验高版本软件的稳定性及增值功能，AP 升级完成后，建议将 AP 恢复出厂设置，然后重新配置 AP。

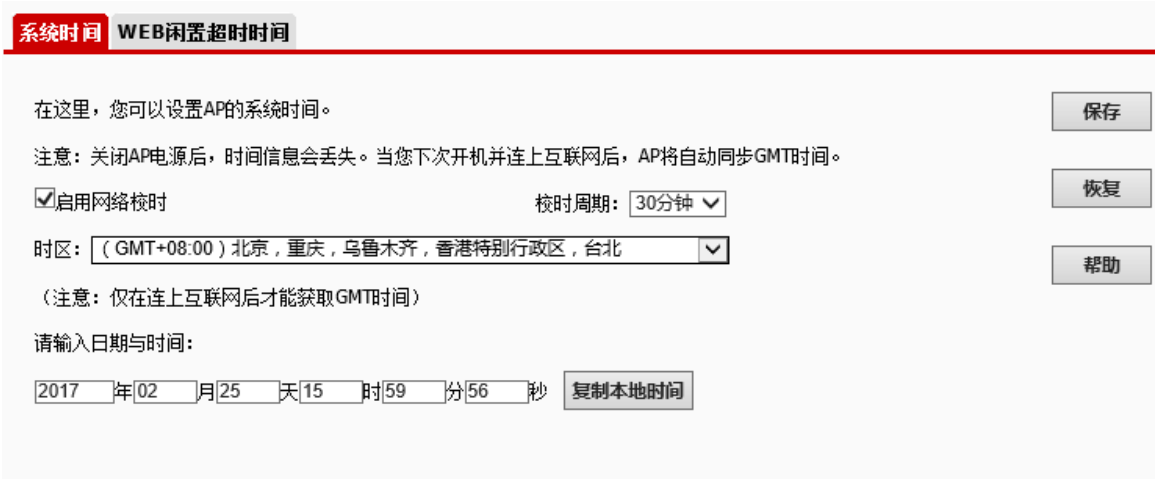
10.2 时间管理

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 。

10.2.1 系统时间

为了保证 AP 的日志记录、自定义重启等功能时间执行准确，需要确保 AP 的系统时间准确。

进入页面：点击「系统工具」>「时间管理」>「系统时间」。



AP 支持“网络校时”和“手动设置时间”两种时间设置方式，默认为“网络校时”。

网络校时

系统自动从互联网上的时间服务器同步时间。使用此方式时，只要 AP 成功连接至互联网就能自动校准其系统时间，即使 AP 经历重启，也能自行校准，无需网络管理员重新设置。

AP 联网方法请参考 LAN 口设置 。

网络校时设置步骤：

1. 进入「系统工具」>「时间管理」>「系统时间」页面。
2. 勾选“启用网络校时”复选框。
3. 校时周期 选择 AP 向互联网上的时间服务器校对系统时间的时间间隔 建议保持默认“30 分钟”。

4. 时区：选择 AP 当前所在地区的 GMT 标准时区，如中国需选择“（GMT+08:00）北京，重庆，乌鲁木齐，香港特别行政区，台北”。
5. 点击 **保存** 。

----完成

手动设置时间

网络管理员手动设置 AP 的系统时间。如果使用此方式，则 AP 每次重启后，您都需要重新设置其系统时间。

设置步骤：

1. 进入「系统工具」>「时间管理」>「系统时间」页面。
2. 输入正确的日期时间，或点击 **复制本地时间** 将当前正在管理 AP 的电脑的时间同步到 AP（需确保该电脑的时间正确）。
3. 点击 **保存** 。

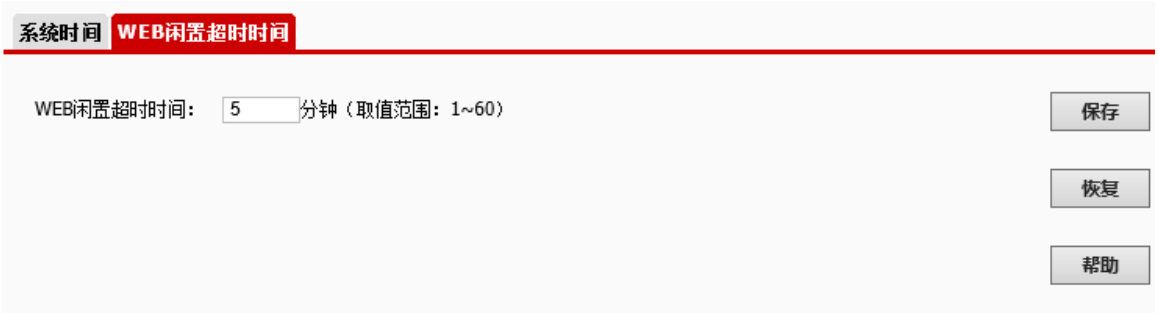
----完成

10.2.2 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，如果在所设置的“WEB 闲置超时时间”内没有任何操作，系统将自动退出登录。默认 WEB 闲置超时时间为 5 分钟。

修改 WEB 闲置超时时间：

1. 进入「系统工具」>「时间管理」>「WEB 闲置超时时间」页面。
2. 根据需要修改 WEB 闲置超时时间。
3. 点击 **保存** 。



----完成

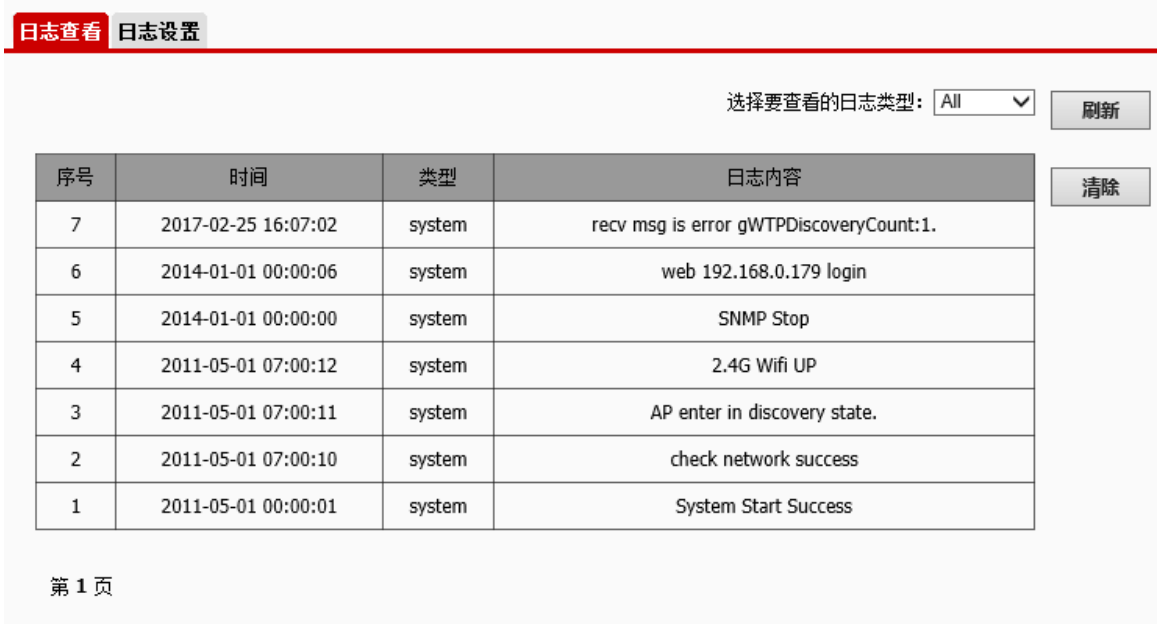
10.3 日志查看

在 AP 的「日志查看」模块，您可以进行：日志查看、日志设置。

10.3.1 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。

进入页面：点击「系统工具」>「日志查看」>「日志查看」。



序号	时间	类型	日志内容
7	2017-02-25 16:07:02	system	recv msg is error gWTPDiscoveryCount:1.
6	2014-01-01 00:00:06	system	web 192.168.0.179 login
5	2014-01-01 00:00:00	system	SNMP Stop
4	2011-05-01 07:00:12	system	2.4G Wifi UP
3	2011-05-01 07:00:11	system	AP enter in discovery state.
2	2011-05-01 07:00:10	system	check network success
1	2011-05-01 00:00:01	system	System Start Success

日志记录时间以 AP 的系统时间为准，如果要让日志记录时间准确，请先确保 AP 的系统时间准确。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。

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。
- 断电后重新上电、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。

10.3.2 日志设置

进入页面：点击「系统工具」>「日志查看」>「日志设置」。

在这里，您可以进行日志条数和日志服务器设置。

3.2.1 设置日志条数

AP 的管理页面默认最多可显示 150 条日志，您可以根据需要修改。

设置步骤：

1. 进入「系统工具」>「日志查看」>「日志设置」页面。
2. 日志条数设置：根据需要修改，范围为 100~300。
3. 点击 **保存** 。

----完成

3.2.2 设置日志服务器

您可以设置日志服务器，让 AP 将系统日志同步发送到网络中您设置的日志服务器，之后，您就可以到该日志服务器上查看 AP 的所有历史日志信息。

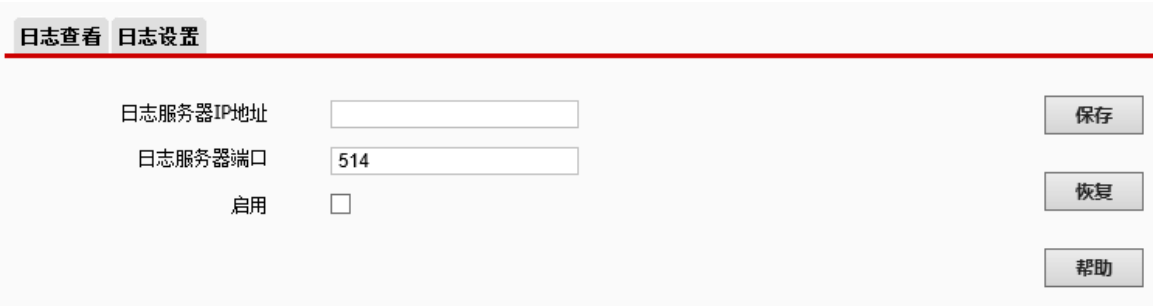
注意

为了保证系统日志能发送到日志服务器，需要在「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。

添加日志服务器

1. 进入「系统工具」>「日志查看」>「日志设置」页面。
2. 点击 **添加** 。

3. 在出现的页面设置下述参数。
   - 日志服务器 IP 地址：输入日志服务器的 IP 地址。
   - 日志服务器端口：设置发送/接收系统日志时所用到的 UDP 端口号，建议保持默认“514”。
   - 启用：勾选复选框，启用对应的日志服务器。
4. 点击 **保存** 。



5. 勾选“启用日志服务器功能”。
6. 点击 **保存** 。

----完成

完成配置后，页面如下图示例。

修改日志服务器

1. 进入「系统工具」>「日志查看」>「日志设置」页面。
2. 点击日志服务器列表操作栏中对应的 **修改** 。
3. 根据需要修改各参数。
4. 点击 **保存** 。

   ----完成

删除日志服务器

1. 进入「系统工具」>「日志查看」>「日志设置」页面。
2. 点击日志服务器列表操作栏中对应的 **删除** 。

   ----完成

10.4 配置管理

AP 的「配置管理」模块提供了以下功能：备份与恢复、恢复出厂设置。

10.4.1 备份与恢复

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。

如，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

1. 进入「系统工具」>「配置管理」>「备份与恢复」页面。
2. 点击 **备份** ，之后按页面提示操作。

----完成

4.1.2 恢复

1. 进入「系统工具」>「配置管理」>「备份与恢复」页面。
2. 点击 **浏览...** ，选择并加载之前备份的配置文件。
3. 点击 **恢复** ，之后按页面提示操作。

----完成

10.4.2 恢复出厂设置

当 AP 出现无法定位的问题或您需要登录 AP 的管理页面但却忘记登录密码时，可以将 AP 恢复出厂设置后重新设置。AP 支持“软件恢复出厂设置”和“硬件恢复出厂设置”两种恢复出厂设置方式。

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”。

注意

- 恢复出厂设置意味着 AP 的所有设置将会丢失，您需要重新设置 AP 才能上网。若非万不得已，不建议将 AP 恢复出厂设置。
- 为避免损坏 AP，恢复出厂设置过程中，请确保 AP 供电正常。

软件恢复出厂设置

1. 进入 AP 的「系统工具」>「配置管理」>「恢复出厂设置」页面。
2. 点击 **恢复出厂设置** 。

----完成

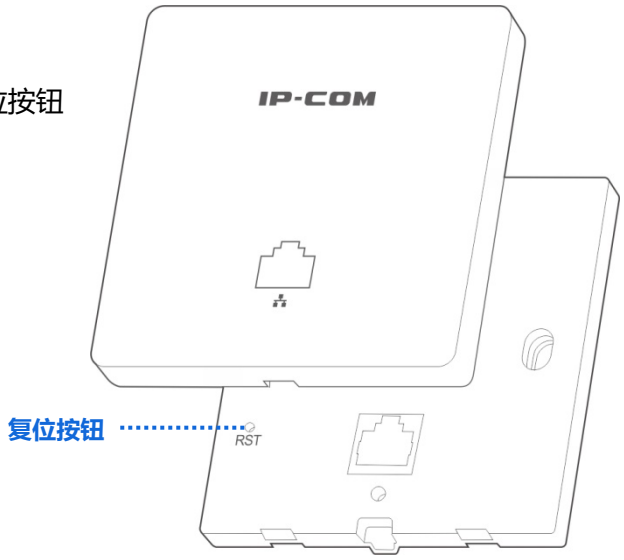
硬件恢复出厂设置

使用此方式时，您无需进入 AP 的管理页面就可以将 AP 恢复出厂设置。

操作方法：

1. AP 通电状态下，用针状物按住机身上的复位按钮 8 秒后松开。
2. 等待约 1 分钟即可。

----完成



10.5 用户名与密码

进入页面：点击「系统工具」>「用户名与密码」。

在这里，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。

参数说明

标题项	说明
账号类型	– 管理员：使用此账号登录 AP 时，您可以查看、修改 AP 的配置。 – 普通用户：使用此账号登录 AP 时，您只能查看 AP 的配置信息，不能修改 AP 配置。
用户名	账号的名称。 默认情况下，AP 有一个管理员账号，一个普通用户账号。其中，管理员的用户名和密码均为“admin”，普通用户的用户名和密码均为“user”。
启用	账号的启用状态。 – 管理员账号永远保持为“启用”状态。 – 普通用户默认为“启用”，可以根据需要禁用。
操作	修改：点击可修改对应账号的用户名/密码。 删除：点击可删除普通用户。 添加：删除普通用户后，点击本按钮可以重新添加普通用户。 注意 进行修改、删除、添加操作后，需要点击 保存 。

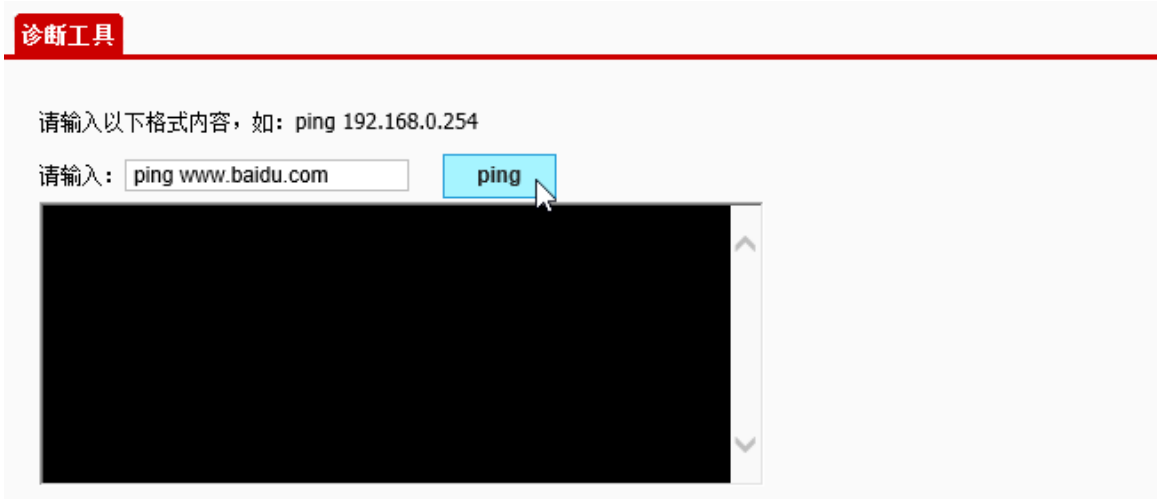
10.6 诊断工具

当网络出现故障时，借助 AP 提供的诊断工具，您可以快速地定位出网络具体是在哪个节点出现了故障。

执行诊断：

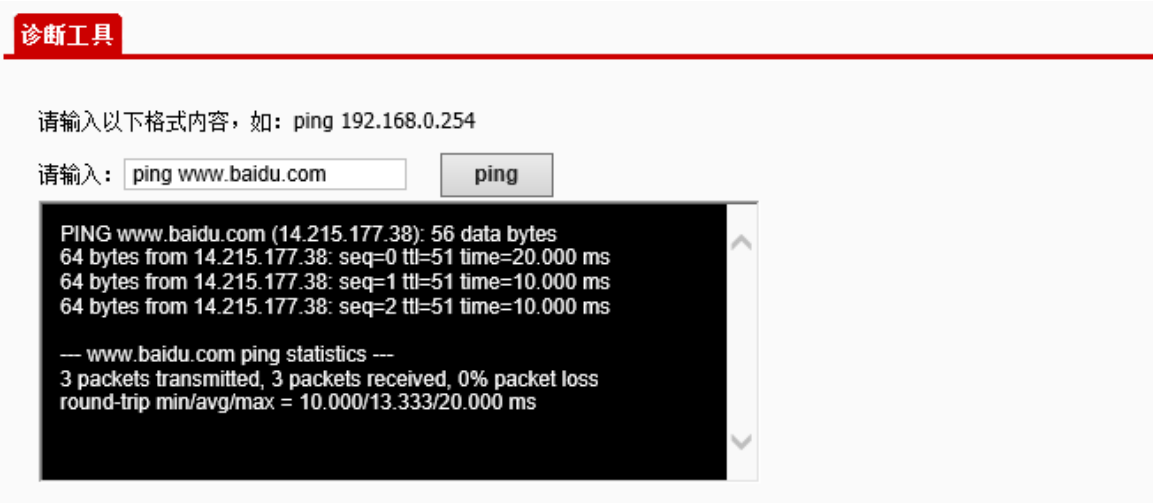
假设要检测访问百度链路是否畅通。

1. 进入「系统工具」>「诊断工具」页面。
2. 请输入：输入格式“ping 要检测的 IP 地址或域名”，本例为“ping www.baidu.com”。
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。



10.7 设备重启

在「设备重启」模块，您可以设置：设备重启、自定义重启。

提示

AP 重启时，会自动断开所有连接。请在网络相对空闲的时候进行重启操作。

10.7.1 设备重启

当您设置的某项参数不能正常生效时，可以尝试手动重启 AP 解决。

设置步骤：

1. 进入「系统工具」>「设备重启」页面。
2. 点击 **重启** 。

----完成

10.7.2 自定义重启

使用自定义重启功能，可以定时地自动重启 AP，预防长时间地运行 AP 导致 WLAN 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 在每周指定的日期和时间自动重启。

设置 AP 按间隔时间段重启

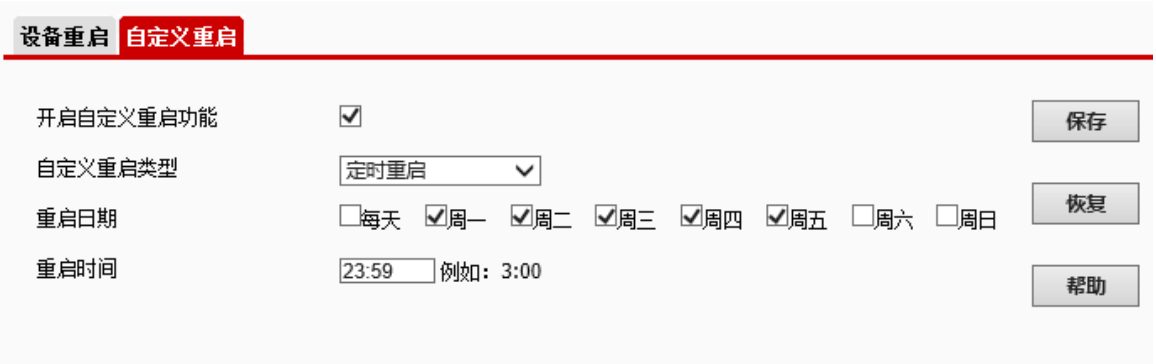
1. 进入「系统工具」>「设备重启」>「自定义重启」页面。
2. 开启自定义重启功能：勾选复选框。

3. 自定义类型：选择“按间隔时间段重启”。
4. 间隔时间：设置重启间隔时间，如“1440 分钟”。
5. 点击 **保存** 。

----完成

设置 AP 定时重启

1. 进入「系统工具」>「设备重启」>「自定义重启」页面。
2. 开启自定义重启功能：勾选复选框。
3. 自定义类型：选择“定时重启”。
4. 日期：选择定时重启的日期，如“周一 ~ 周五”。
5. 时间：设置定时重启的时间点，如“23:59”。
6. 点击 **保存** 。



----完成

10.8 LED 灯控制

AP 提供了 LED 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 LED 灯。

关闭 LED 灯：

1. 进入「系统工具」>「LED 灯控制」页面。
2. 点击 **关闭所有指示灯** 。

----完成

开启 LED 灯：

1. 进入「系统工具」>「LED 灯控制」页面。
2. 点击 **开启所有指示灯** 。

----完成

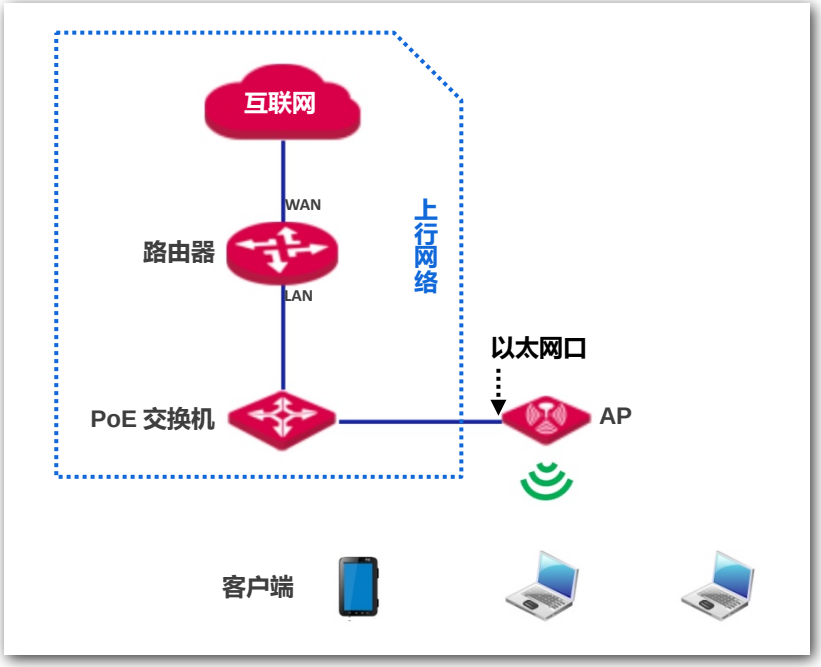
10.9 上行链路检测

10.9.1 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。启用上行链路检测时，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，无线客户端将可以重新关联该 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）。



10.9.2 配置上行链路检测

1. 进入「系统工具」>「上行链路检测」页面。
2. 上行链路检测：勾选“启用”复选框。
3. Ping 主机 1 或 Ping 主机 2：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。
4. Ping 间隔：设置执行上行链路检测的间隔时间。

5. 点击 **保存** 。


上行链路检测
上行链路检测
启用
Ping 主机1
Ping 主机2
Ping 间隔
10
分钟（取值范围：10~100）
保存
恢复
帮助

----完成

附录

常见问题解答

问 1：输入 192.168.0.254 登录不了 AP 的管理页面，怎么办？

答：请分别从以下几个方面检查：

- 确认管理电脑的 IP 地址为 192.168.0.X（X 为 2~253）。
- 清空浏览器的缓存或使用别的浏览器进行尝试。
- 关闭电脑的防火墙或使用别的电脑进行尝试。
- 若网络中同时接了至少两台 AP，且没有搭建无线控制器（包括带“AC 管理”功能的路由器），请先只接一台 AP 到 PoE 交换机，修改该 AP 的 IP 地址后，再接入另一台 AP 进行设置。以此类推。
- 可能 AP 已被无线控制器管理，其 IP 已不是 192.168.0.254。请先登录到控制器管理页面，查看 AP 新的 IP，然后用新的 IP 登录 AP 的管理页面。
- 若经过上述操作仍无法登录，请将 AP 恢复出厂设置再重新操作。

问 2：无线控制器扫描不到 AP，怎么办？

答：请分别从以下几个方面检查：

- 确认设备连接正确，且 AP 已正常启动。
- 若网络已划分 VLAN，确认无线控制器已添加了对应的 VLAN。
- 重新启动 AP 或将 AP 恢复出厂设置再尝试扫描。

问 2：想进入 AP 的管理页面，但忘记了登录用户名和密码怎么办？

答：请先使用默认登录信息（IP 为“192.168.0.254”，用户名为“admin”，密码为“admin”）尝试登录。如果不行，请将 AP 恢复出厂设置后，再使用默认登录信息登录。

问 3：不能登录 AP 管理页面的情况下，怎么将 AP 恢复出厂设置？

答：AP 通电状态下，使用尖状物持续按住 AP 机身上的**复位按钮** 8 秒后松开，等待约 1 分钟即可。AP 恢复出厂设置后，需要重新配置参数。

问 4：连接 AP 后，电脑出现“IP 地址与网络上的其他系统有冲突”提示信息，怎么办？

答：请分别从以下几个方面检查：

- 确保局域网内的电脑没有占用 AP 的 IP 地址，AP 出厂默认的 IP 地址是 192.168.0.254。
- 请确保局域网内为电脑静态设置的 IP 没有其它电脑使用。

更多问题请访问我们的网站 www.ip-com.com.cn或者发送 e-mail 到 ip-com@ip-com.com.cn或者打电话到 40066-50066，我们会及时给您解决。

默认参数

出厂时，AP 的各项参数默认设置如下：

参数			默认设置
设备登录	管理 IP		192.168.0.254
	用户名|密码	管理员	admin|admin
		普通用户	user|user
快速设置	工作模式		AP 模式
LAN 口设置	IP 获取方式		手动设置
	IP 地址		192.168.0.254
	子网掩码		255.255.255.0
	网关地址		192.168.0.1
	首选 DNS 服务器		8.8.8.8
	备用 DNS 服务器		8.8.4.4
	设备名称		AP 的产品型号，如 W30AP V4.0 的设备名称默认为“W30APV4.0”
	端口驱动能力		标准模式
DHCP 服务器	DHCP 服务器		禁用
	起始 IP 地址		192.168.0.100
	结束 IP 地址		192.168.0.200
	租期		1 天
	子网掩码		255.255.255.0
	网关地址		192.168.0.1
	首选 DNS 服务器		8.8.8.8
	备用 DNS 服务器		8.8.4.4
基本设置	SSID		支持 2 个 SSID SSID 为“IP-COM_XXXXXX”。其中，XXXXXX 为 AP LAN 口 MAC 后六位~后六位+1 默认 主 SSID启用，其他 SSID 禁用
	广播 SSID		启用
	客户端隔离		禁用

参数		默认设置
	组播转单播	禁用
	最大客户端数量	16
	中文 SSID 编码格式	UTF-8
	安全模式	不加密
射频状态	无线状态	开启
	国家或地区	中国
	网络模式	11b/g/n 混合模式
	信道	Auto
	信道带宽	20MHz
	锁定信道	开启
	SSID 隔离	禁用
	APSD	禁用
	客户端老化时间	5 分钟
WMM 设置	WMM	启用
	场景优化模式	密集用户场景（10 人以上）
高级设置	Beacon 间隔	100ms
	Fragment 阈值	2346
	RTS 门限	2347
	DTIM 间隔	1
	接入信号强度限制	-90dBm
	功率	18dBm
	锁定功率	启用
	无线前导码	长导码
无线访问控制		禁用
QVLAN	QVLAN 启用状态	禁用
	PVID	1
	管理 VLAN	1
	Trunk 口	LAN0
	以太网口 VLAN ID	1

参数			默认设置
	2.4G SSID VLAN ID		1000
SNMP	SNMP 代理		禁用
	管理员		Administrator
	设备名称		AP 的产品型号，如 W30AP V4.0 的设备名称默认为“W30APV4.0”
	位置		ShenZhen
	读 Community		public
	读/写 Community		private
部署模式			本地部署
系统工具	时间管理	系统时间	启用网络校时 时区：（GMT+08:00）北京，重庆，乌鲁木齐，香港特别行政区，台北
		WEB 闲置超时时间	5 分钟
	显示日志条数		150 条
	日志服务器		未添加
	自定义重启		禁用
	LED 灯控制		启用 LED 灯显示
	上行链路检测		禁用

电子信息产品有毒有害物质申明

电子信息产品有毒有害物质申明

部件名称	有毒有害物质或元素					
	铅（pb）	汞（Hg）	镉（Cd）	六价铬（Cr6+）	多溴联苯（PBB）	多溴二苯醚（PBDE）
结构件	×	○	○	○	○	○
单板/电路模块	×	○	○	○	○	○
电源适配器	×	○	○	○	○	○
线缆	×	○	○	○	○	○
连接器	×	○	○	○	○	○
附件	×	○	○	○	○	○

1. “○”表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T11363-2006标准规定的限量要求以下。
2. “X”表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T11363-2006标准规定的限量要求。
3. 由于中国限量标准中没有豁免条例，故标识为“X”并不一定表示为对人体有害。
4. 对生产制造的产品，可能包含这些欧洲豁免的物质。
5. 在所售产品中可能包含所有部件也可能不包含所有部件。