IP-COM®

使用说明书

F190AP

900M FAT/FIT室内无线接入设备

声明

前言

感谢您购买 IP-COM 产品！阅读此说明书将有助于您配置、管理、维护本产品。

目标读者

本说明书的目标读者为熟悉网络基础知识，了解网络术语的技术人员。

本书约定

本说明书中，所提到的“AP”、“本设备”、“本产品”、“设备”等名词，如无特别说明，均指 IP-COM 900M FAT/FIT 室内无线接入设备 F190AP。

本说明书主要指导安装 AP 和 AP 作为 FAT AP 时的设备管理方法。如果 AP 作为 FIT AP，您要对 AP 进行统一管理，请登录到 IP-COM 官方网站 www.ip-com.com.cn 后，点击『服务支持』→『下载中心』，找到 CW3024 有线无线一体化控制器的产品说明书参考操作。

本说明书中的符号格式约定如下：

文字描述	代替符号	举例
按钮	边框+底纹	点击“保存”按钮可简化为点击 保存
菜单项	『』	菜单项“基本设置”可简化为『基本设置』
连续菜单选择	→	进入『状态』→『系统日志』页面

本说明书使用的标识含义如下：

标识	含义
注意	提醒您在操作设备过程中需要注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。
提示	对操作内容的描述进行必要的补充和说明。

内容简介

本说明书各章节内容安排如下：

章节	内容
第 I 部分 产品介绍	介绍 AP 的外观及功能特性
第 II 部分 设备安装	介绍 AP 安装注意事项及安装步骤

章节	内容
第Ⅲ部分 设备管理入门	介绍如何通过 Web 网管管理 AP 及 AP Web 网管的基础操作
第Ⅳ部分 设备管理	介绍通过 Web 网管设置 AP 各功能的具体方法
第Ⅴ部分 附录	介绍 AP 常见问题处理方法、技术规格、有毒有害物质清单

相关资料获取方式

您可以登录到 IP-COM 官方网站 www.ip-com.com.cn 获取最新的产品资料。点击『技术支持』→『相关下载』，找到对应的产品即可。

技术支持

网址：http://www.ip-com.com.cn

技术支持邮箱：ip-com@ip-com.com.cn

技术支持热线电话：400-665-0066

目录

第 I 部分

产品介绍

简介

F190AP 是深圳市和为顺网络技术有限公司(以下简称 IP-COM 公司)自主研发的室内大范围覆盖型无线接入点，专为酒店、学校、企业无线等多房间覆盖而设计。

F190AP 工作在 2.4GHz、5GHz 频段，采用 MIMO、OFDM 等技术，最高可提供 900Mbps 的无线数据传输速率。内置 3 根双频 MIMO 天线，能提供更大的覆盖范围和更强的信号穿透力，室内有效覆盖距离可达 80-100 米，有效覆盖房间数量可达 10-16 个；基于吸顶式设计，美观大方，可直接安装在墙壁和天花板上；支持非标准 PoE 供电，可保证用户在不改变原有电力网络的基础上实现大范围无线覆盖。同时,F190AP 支持 CW3024 有线无线一体化交换机管理，这使得用户不需改变原有网络架构就可以对网络进行无线扩展。

特性

- 3X3 MIMO 设计，无线并发速度最高可达 900Mbps；
- 双端口千兆设计，PoE 口还支持非标准 PoE（自带电源适配器和 PoE 注入器）供电；
- 水滴式外形设计，保证信号最强覆盖；
- 胖瘦一体化设计，支持 FAT 和 FIT 模式切换；
- 双频网络接入，支持 2.4GHz、5GHz 并发工作；
- 外置全铝散热器；
- 节能设计，软件内置功率可调节功能。

包装

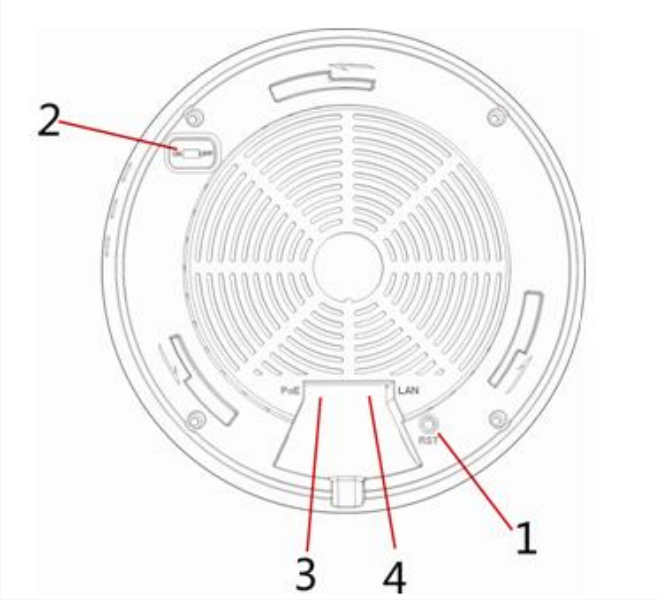
请小心打开产品包装盒，检查包装盒内应有以下物品：

- 设备主机*1
- 底盘*1
- 电源适配器*1
- 注入器*1
- 网线*1
- 螺丝*5
- 快速安装指南*1
- 保修卡*1

如果发现有损坏或配件短缺，请持原包装及配件与经销商联系更换。

外观

1 接口、按钮



1⇉系统复位按钮，通电状态下，持续按住 7 秒后放开，可将设备设置恢复到出厂状态。

2⇉指示灯显示开关，拨动开关，可开启/关闭指示灯显示。

3⇉PoE 网口，使用网线连接已连接电源适配器的注入器的 AP 端口给 AP 供电。

4⇉LAN 口，10/100/1000Mbps 自适应，可使用网线连接到计算机，交换机等以太网设备。

2 贴纸

1⇉设备未从上级网络设备获取到 IP 地址时的 LAN 口 IP 地址，可使用该地址进入设备 Web 网管页面。

2⇉使用 Http/s（Web 网管）、Telnet、SSH、串行端口管理设备时的默认登录用户名/密码。

3⇉设备的电源规格。

第 II 部分

设备安装

1 安装准备

安装设备前，请根据本节内容做好准备工作。

1.1 安全注意事项

- 未得到 IP-COM 允许，请不要随意拆卸设备机壳。
- 请将设备放置在干燥、平稳的地方，避免设备接触液体和滑落。
- 请保持设备洁净无灰尘。

1.2 检查安装环境

设备必须在室内使用，将其安装在天花板上时，需要满足以下条件：

- 设备和用户终端间的障碍物（如：墙壁）尽量最少。
- 安装位置远离可能产生射频噪声的电子设备或装置（如：微波炉）。
- 安装位置尽量隐蔽，不妨碍居民的日常工作和生活。

注意

严禁在积水、渗水、滴漏、结露等环境下安装，并需避免线缆凝水、渗水而造成水滴沿着线缆流入设备。

为保证设备良好运行，安装环境还需满足以下条件：

项目	要求
温度	0℃ ~ 45℃
湿度	10% ~ 90%（无凝结）

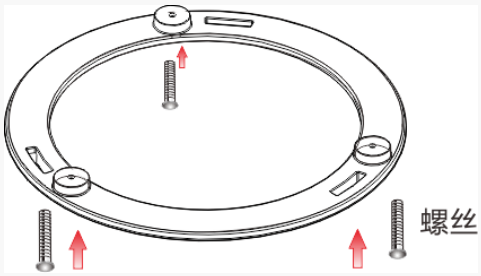
1.3 准备安装工具

安装设备过程中，可能会用到以下安装工具，请自备。

2 硬件安装

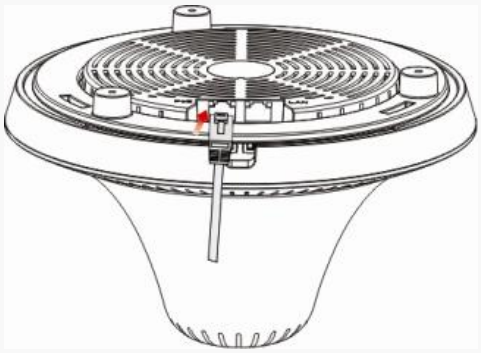
步骤 1：底盘安装。

1. 将底盘贴在天花板墙面，画出需要安装螺钉的孔的位置标记，用冲击钻打出 3 个直径 5.0mm 的孔，所钻的孔与底盘上的孔成对应关系；
2. 插入膨胀螺管到墙面上已钻好的孔中，用橡胶锤敲打膨胀螺管一端，直到将膨胀螺管全部敲入墙面；
3. 把底盘的螺钉孔对准膨胀螺管孔，并将螺钉从相应的安装孔穿过；
4. 调整底盘的位置，并将螺钉拧紧。

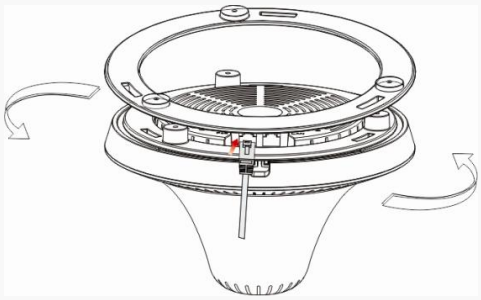


步骤 2：主机安装。

1. 将网线（建议使用 5 类或 5 类以上的网线）的一端接到设备主机的 PoE 接口；

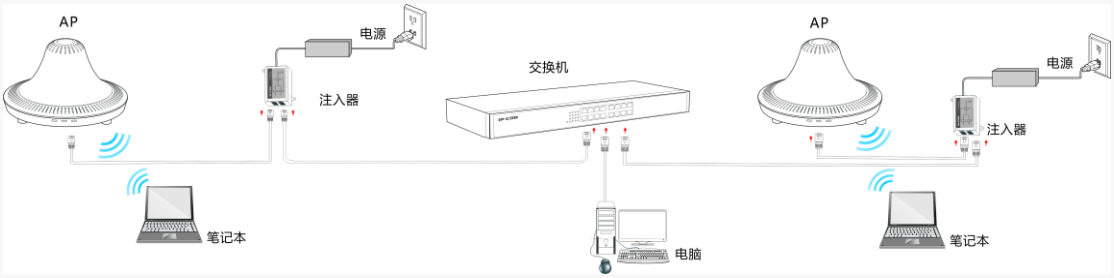


2. 将设备主机悬挂在底盘上；



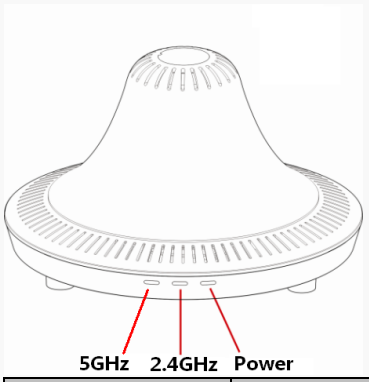
步骤 3：电源安装。

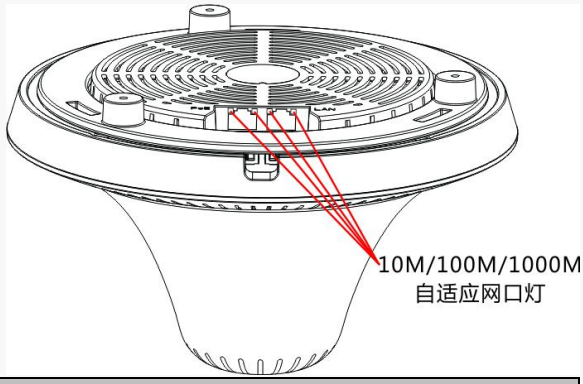
1. 将连接设备 PoE 接口的网线的另一端连接到注入器的 AP 端口；
2. 用网线连接 PoE 注入器的 Switch 口和交换机；
3. 连接注入器的电源，检查网络连接拓扑图。



3 上电检查

设备上电后，您可根据以下指示灯说明确认设备是否工作良好。





指示灯	颜色	状态	说明	
Power	绿色	常亮	设备已上电	
	绿色	闪烁	系统运行正常	
	/	不亮	设备未上电或已关闭指示灯或出现故障	
2.4GHz	绿色	常亮	2.4G 无线功能已开启	
	绿色	闪烁	2.4G 无线正在传输数据	
	/	不亮	2.4G 无线功能未开启或已关闭指示灯	
5GHz	绿色	常亮	5G 无线功能已开启	
	绿色	闪烁	5G 无线正在传输数据	
	/	不亮	5G 无线功能未开启或已关闭指示灯	
10M/100M/1000M 自适应网口灯	绿色/橙色	绿色亮	端口已连接，速率为 1000Mbps	
		橙色亮	端口已连接，连接速率为 100Mbps 或 10Mbps	
	/	不亮	PoE 口	端口未连接或端口只进行了 PoE 供电，无数据传输
			LAN 口	端口未连接

第Ⅲ部分

设备管理入门

1 Web 网管概述

为了方便网络管理员对 AP 进行操作和维护，本 AP 提供了 Web 网管功能。管理员可以使用 Web 页面直观地管理和维护网络设备。Web 网管的运行环境如下图所示。

2 登录 Web 网管

AP 出厂时已经默认启用了 HTTP 服务，并且设置有默认的 Web 登录信息，您可以直接使用默认登录信息通过浏览器登录 AP 的 Web 网管页面。默认的 Web 登录信息包括：

- 用户名：admin
- 密码：admin
- LAN 口 IP 地址：192.168.0.254

注意

- 默认情况下，AP LAN 口的连接类型为 DHCP，即，如果上级网络存在 DHCP 服务器，AP 将从上级网络动态地获取其 LAN 口 IP 地址信息。此时，您需要先进入上级网络设备查看其给 AP 分配的 IP 地址。
- 如果 AP 未从上级网络获取到 IP 地址，则其 LAN 口 IP 为 192.168.0.254。

采用 Web 方式登录设备的步骤如下：

步骤 1：用网线将计算机接在 AP 连接的交换机上或直接接在 AP 的 LAN 口。默认情况下，AP 所有端口均属于 VLAN 1。

步骤 2：将计算机的 IP 地址设置为和 AP 的 LAN 口 IP 在同一网段的不同 IP 地址。

步骤 3：启动计算机上的浏览器，在浏览器地址栏中输入 AP 的 LAN 口 IP 地址后，敲回车。

步骤 4：进入 AP Web 网管登录页面，输入用户名“admin”、密码“admin”，点击 登录 。

登录到 Web 网管后，您可进入『基本设置』页面修改管理员密码；进入『服务』→『Web 服务器』页面修改 HTTP 服务设置；进入『管理』→『以太网设置』页面修改 LAN 口 IP 地址，以增强设备安全性。

3 退出 Web 网管

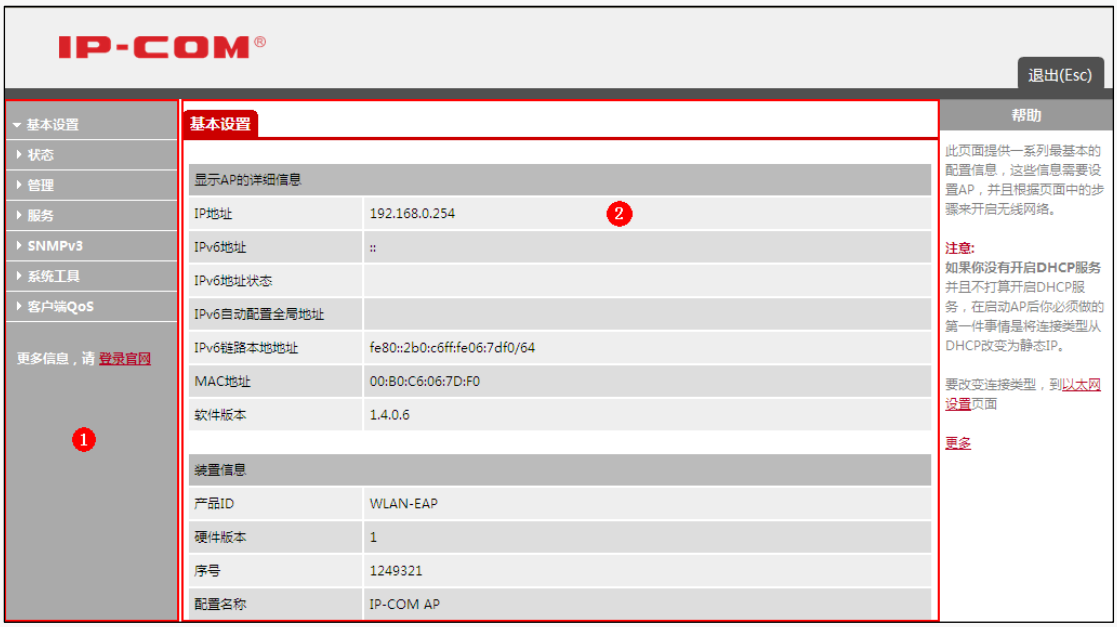
在 Web 网管页面上点击右上角的 退出（Esc） ，即可退出 Web 网管。退出 Web 网管时，系统不会自动保存当前配置。因此，建议用户在退出 Web 网管前先保存当前配置。

注意

直接关闭浏览器时，已登录到设备上的用户并不能自动退出登录。

4 Web 网管页面布局介绍

Web 网管页面共分为：导航栏和配置区两部分，如下图所示。



1⇉导航栏：以导航树的形式组织设备的 Web 网管功能菜单。用户在导航栏中可以方便地选择功能菜单，选择结果显示在配置区中。

2⇉配置区：用户进行配置和查看的区域。

注意

设备不支持的 Web 网管功能不会显示在 Web 网管导航区，请以设备软件的实际情况为准。

5 Web 网管页面常用元素

常用元素	说明
更新 保存	用于使当前页面的配置内容生效。
恢复 下载	用于对证书文件或配置文件进行导入导出。
添加	用于新增一条规则。
删除	用于删除一条规则。
取消	用于取消当前页面的配置内容。
刷新	用于刷新当前页面显示内容。
重置	用于将配置信息恢复到默认值。
重启	用于将 AP 进行重新启动。
切换	一般用在升级页面中，主要用于更换主次升级镜像。
软件升级	用于更新 AP 软件版本。
退出(Esc)	用于退出登录 Web 网管。
更多	可点击展开详细的帮助信息。

6 Web 网管使用限制

- Web 网管支持的操作系统包括：Windows XP/2000/Vista/7/8、Windows Server 2003 企业版、Windows Server 2003 标准版、Linux 和 MAC OS。
- Web 网管支持的浏览器包括：Microsoft Internet Explorer 8.0 SP2 及以上版本、Mozilla Firefox 3.0 及以上版本、Google Chrome 2.0.174.0 及以上版本、Opera 9.64 及以上版本、Safari 3.1.1 及以上版本。
- Web 网管不支持浏览器自带的后退、前进、刷新等按钮。使用这些按钮可能会导致 Web 页面显示不正常。
- 由于 Windows 操作系统自带的防火墙会对 TCP 连接数进行限制，使用 Web 网管时偶尔会出现无法打开 Web 网管页面的情况。为避免这种情况，建议关闭 Windows 自带的防火墙。
- 设备的软件版本变化后，在通过 Web 网管登录设备时，建议先清除浏览器的缓存数据，

否则 Web 网管的内容可能无法正确显示。

7 Web 网管使用常见问题举例

问题：无法正常通过 Web 网管访问设备。

问题现象：

用户可以 Ping 通设备，可以通过 Telnet 登录到设备上，HTTP 服务已经启用，并且使用的操作系统和浏览器版本都符合 Web 网管的要求。但是，无法正常访问设备的 Web 网管。

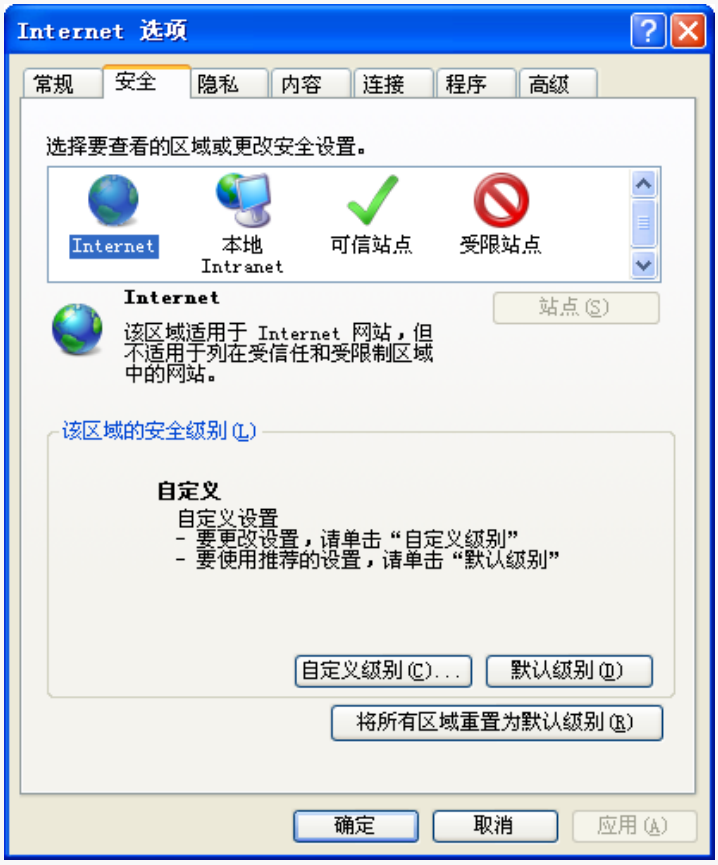
问题分析：

- 使用 Microsoft Internet Explorer 浏览器时，可能是以下功能未改为启用状态：对标记为可安全执行脚本的 ActiveX 控件执行脚本、运行 ActiveX 控件和插件、活动脚本。
- 使用 Mozilla Firefox 浏览器时，可能是 JavaScript 未启用。

Internet Explorer 浏览器处理过程：

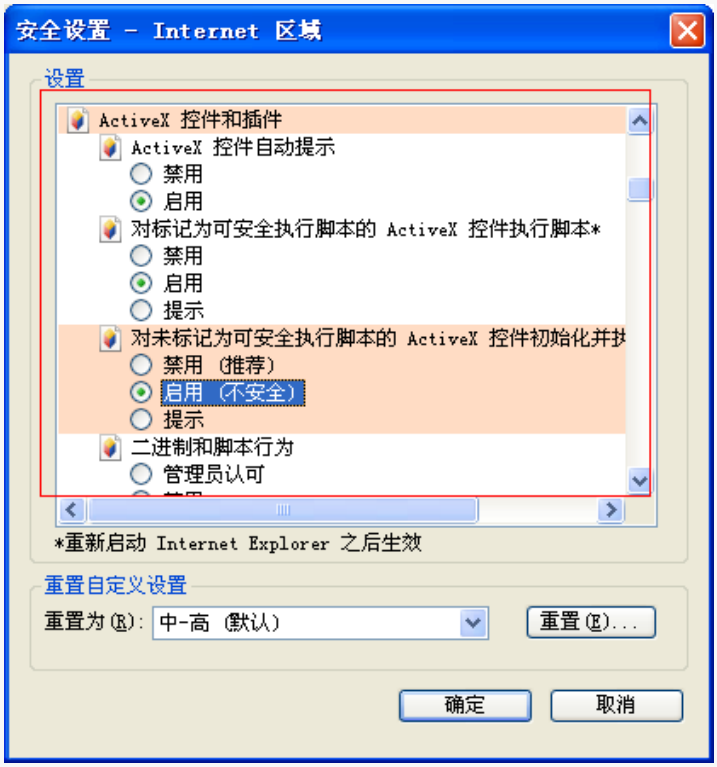
步骤 1：启动 Internet Explorer 浏览器，选择『工具』→『Internet 选项』；

步骤 2：点击“安全”页签，选中要访问的站点所在的区域，如下图所示；



步骤 3：点击 自定义级别 ，弹出“安全设置”对话框；

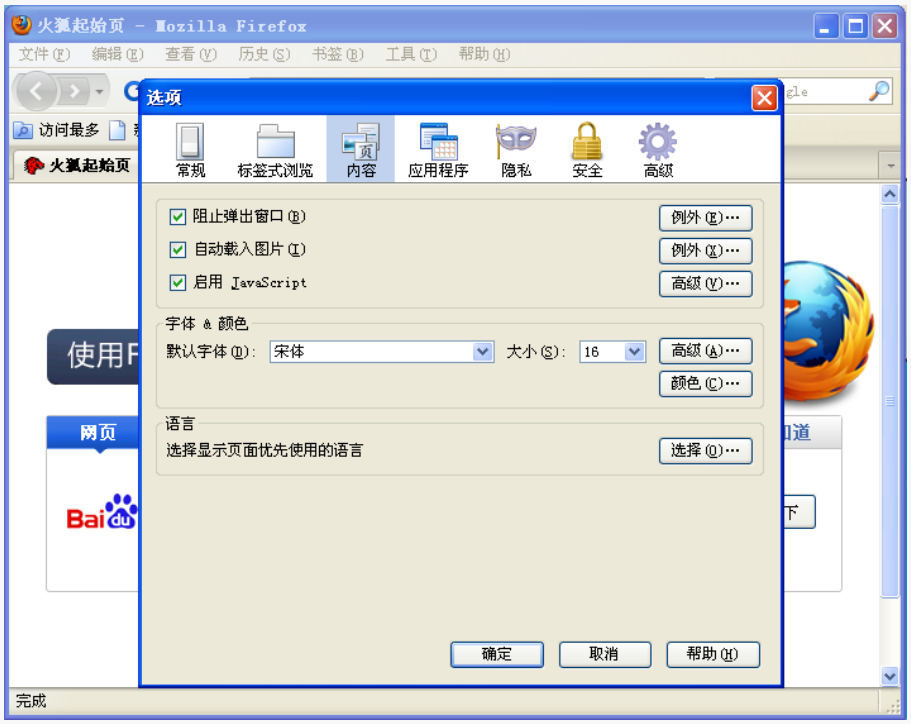
步骤 4：启用“对标记为可安全执行脚本的 ActiveX 控件执行脚本”、运行“ActiveX 控件和插件”、“活动脚本”后，点击 确定 。



Firefox 浏览器处理过程：

步骤 1：启动 Firefox 浏览器，选择『工具』→『选项』；

步骤 2：点击“内容”页签，选中“启用 JavaScript”前的复选框，点击 确定 。



第Ⅳ部分

设备管理

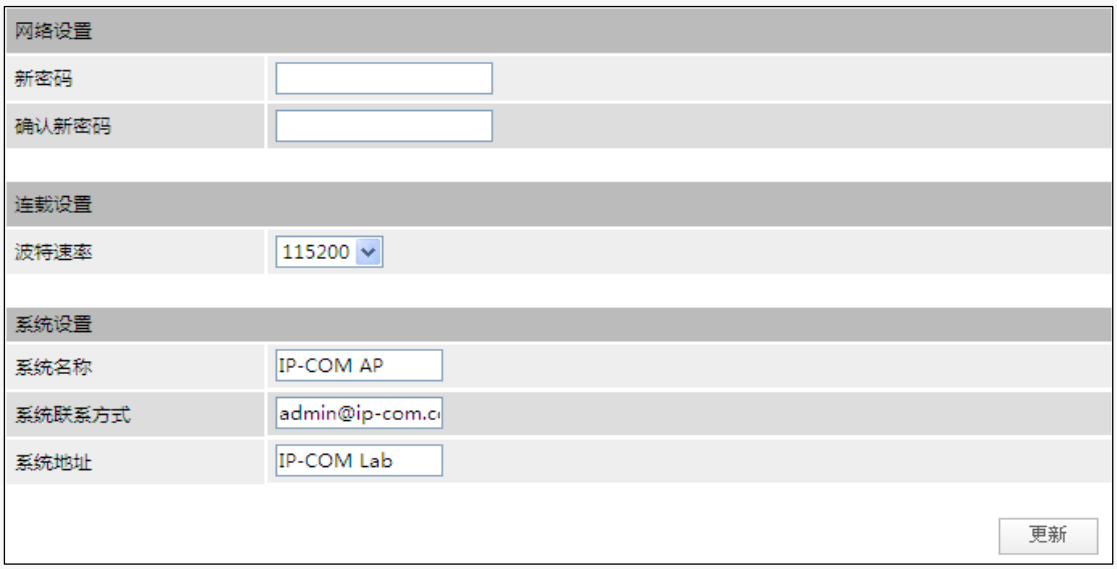
基本设置

显示 AP 当前最基本的配置信息。点击『基本设置』进入页面。

以下是对页面各参数的说明：

标题项	说明
IP 地址	显示 AP 的 IP 地址。
IPv6 地址	显示 AP 的 IPv6 地址。
IPv6 地址状态	显示分配到 AP 管理接口的静态 IPv6 地址的操作状态。可能的取值为“Operational”或“Tentative”。 **注意** 如果未手动设置或自动从 DHCPv6 服务器获得 IPv6 地址，本字段将显示为空白。
IPv6 自动配置全局地址	显示 AP 的 IPv6 自动配置全局地址。
IPv6 链路本地地址	显示 AP 的 IPv6 链路本地地址。该地址是由 IPv6 邻居发现过程分配的为本地物理链路所使用的 IPv6 地址，是不可配置的。
MAC 地址	显示 AP 的 MAC 地址。该 MAC 地址与管理接口关联，AP 通过其被外部其他网络识别。
软件版本	显示 AP 当前安装的软件的版本信息。
产品 ID	标识 AP 的硬件模型。

硬件版本	标识 AP 的硬件版本。
序号	显示 AP 的序列号。
配置名称	标识硬件类型的通用名称。
配置描述	提供关于产品的硬件信息。



以下是对页面各参数的说明：

标题项	说明
新密码	输入新的管理员密码。为防止他人看到您的密码，输入字符显示为暗文。 **管理员密码**：您在使用 Http/s、Telnet、SSH、串行端口登录到 AP 进行管理时需输入的密码。它必须是一个长度不超过 8 个字符的字母、数字字符串，不能含特殊字符或空格。 **注意** 作为保护您的无线网络的比较重要的第一步，我们建议您更改默认的管理员密码（admin）。
确认新密码	重新输入新的管理员密码，以确认密码更改。
波特速率	为串行端口连接选择一个波特率。通过一个串行连接（控制台）连接到 AP 命令行接口（CLI），AP 上的波特率必须和终端或终端仿真器的波特率相匹配。波特率值可选择：9600、19200、38400、57600、115200。
系统名称	输入的 AP 的名称。这个名字只出现在基本设置页面，用于帮助 AP 的管理员确定 AP。最多可使用 64 个字母、数字字符，例如 My AP。
系统联系方式	输入与 AP 相关的联系人名称，电子邮件地址，或电话号码。
系统地址	输入的 AP 的物理位置，例如：A 会议室。

状态

本节可帮助用户了解 AP 的状态和概要信息，包括以下 6 部分内容：

接口状态：查看 AP 当前的有线接口和无线接口设置概要信息。

无线客户端关联信息：查看当前连上 AP 的无线客户端状态和流量统计信息。

各接口报文统计：查看 AP 各接口的数据流量统计信息。

AP 无线报文统计：查看 AP 无线接口的数据流量统计信息。

管理型 AP 配置信息：查看 AP 设置为可管理模式（FIT AP）时，上级管理型交换机的 IP 地址及端口。

系统日志：设置 AP 的日志记录选项，查看 AP 近期产生的系统日志信息。

1 接口状态

显示 AP 当前有线接口和无线接口的设置概要信息。如果您需要改变设置，请点击『状态』→『接口状态』进入页面后，再点击有线设置或射频设置后的编辑链接到对应页面进行设置。

1.1 有线设置

以下是对页面各参数的说明：

标题项	说明
有线设置	点击编辑，可跳转至以太网设置页面，对 AP 的 LAN 进行配置。
MAC 地址	显示以太网 LAN 口的 MAC 地址。

VLAN ID	管理 VLAN ID，与您访问 AP 管理界面时使用的 IP 地址相关联。默认值为 1。
IP 地址	显示 LAN 口的 IP 地址。
子网掩码	显示 LAN 口 IP 地址对应的子网掩码。
IPv6 地址	本 AP 支持 IPv6，此处显示 LAN 口的 IPv6 地址。
IPv6 自动配置全局地址	如果 AP 被自动分配了一个或多个 IPv6 地址，这些地址将会被显示到此列表中。
IPv6 链路本地地址	显示 AP 的 IPv6 链路本地地址（以 fe80 开头）。
IPv6-DNS-1	显示 AP 的主 IPv6 DNS 地址。
IPv6-DNS-2	显示 AP 的次 Ipv6 DNS 地址。
DNS-1	显示 AP 的主 IPv4 DNS 地址。
DNS-2	显示 AP 的次 IPv4 DNS 地址。
默认网关	显示 AP 的默认网关地址。
默认 IPv6 网关	显示 AP 默认的 Ipv6 网关地址。

1.2 射频设置

以下是对页面各参数的说明：

标题项	说明
射频设置	点击编辑，可跳转至射频设置页面，对 AP 的射频参数进行设置。
MAC 地址	显示对应的无线接口（无线 1，无线 2）的 MAC 地址。 MAC 地址是由制造商分配的唯一标识一个接口的地址，您不能更改。
模式	显示对应的无线接口物理层(PHY)使用的无线标准模式： ➢ IEEE 802.11b/g：802.11b 和 802.11g 客户端能够连接到 AP。 ➢ IEEE 802.11b/g/n：工作在 2.4GHz 频段的 802.11b，802.11g，和 802.11n 客户端能够连接到 AP。 ➢ IEEE 802.11a：仅 802.11a 客户端可以连接到 AP。 ➢ IEEE 802.11a/n：工作在 5GHz 频段的 802.11a，802.11n 客户端可以连接到 AP。此模式仅适用于无线 1。
信道	显示对应的无线接口的当前工作频段。
信道带宽	显示当前无线信道正在使用的带宽。

2 无线客户端关联信息

显示关联上 AP 的无线客户端的状态及流量统计信息。点击『状态』→『无线客户端关联信息』进入页面。

以下是对此页面各显示参数的说明：

标题项	说明
网络	客户端关联的 VAP。例如：wlan0vap2 表明客户端关联上了无线 1 的 VAP2。 **注意** wlan0 表示客户端关联到无线 1（5G）的 VAP0，wlan1 表示客户端关联到无线 2（2.4G）的 VAP0。
客户端	客户端的 MAC 地址。
认证状态	客户端的认证状态。
关联状态	客户端的关联状态。
接收	AP 从无线客户端接收的数据包的数量和接收的字节数，以及接收后被丢弃的数据包的数量和字节数量。
发送	从 AP 发送至无线客户端的数据包的数量和字节数，以及传输中被丢弃的数据包的数量和字节数量。

3 各接口报文统计

显示 AP 各接口的详细数据包统计信息。点击『状态』→『各接口报文统计』进入页面。

接口	状态	MAC地址	VLAN ID	名称 (SSID)
LAN	up	00:B0:C6:20:12:18	1	-
isatap0	down	-	1	-
wlan0:vap0	up	00:B0:C6:20:12:18	1	IP-COM_5G_201218
wlan0:vap1	down		1	Virtual Access Point 1

发送

接口	数据包总数	字节总数	丢失的数据包总数	丢失的字节总数	错误
LAN	5906	4241484	0	0	0
isatap0	0	0	0	0	0
isatap0	0	0	0	0	0
wlan0:vap0	281	43756	0	0	0
wlan0:vap1	0	0	0	0	0

接收

接口	数据包总数	字节总数	丢失的数据包总数	丢失的字节总数	错误
LAN	5118	721650	0	0	0
isatap0	0	0	0	0	0
wlan0:vap0	0	0	0	0	0
wlan0:vap1	0	0	0	0	0

以下是对各页面显示参数的说明：

标题项	说明
接口	AP 的接口名称及编号。 LAN：以太网接口　　Vap0：无线主 SSID 接口 Vap1-15：无线各次 SSID 接口　　Wlan0wds0-3：WDS 桥接时的无线接口
状态	各接口的状态。 Up：接口当前状态为开启　　down：接口当前状态为关闭
MAC 地址	各接口的硬件地址，用于标识各个物理接口。
VLAN ID	各接口所属的 VALN。
名称（SSID）	各接口的名称，无线接口显示为 SSID。
数据包总数	各接口接收或发送的数据包个数。
字节总数	各接口接收或发送的数据字节数。
丢失的字节总数	各接口接收或发送时丢弃的数据字节总数。
错误	各接口接收或发送时产生的错误数据包的个数。

4 AP 无线报文统计

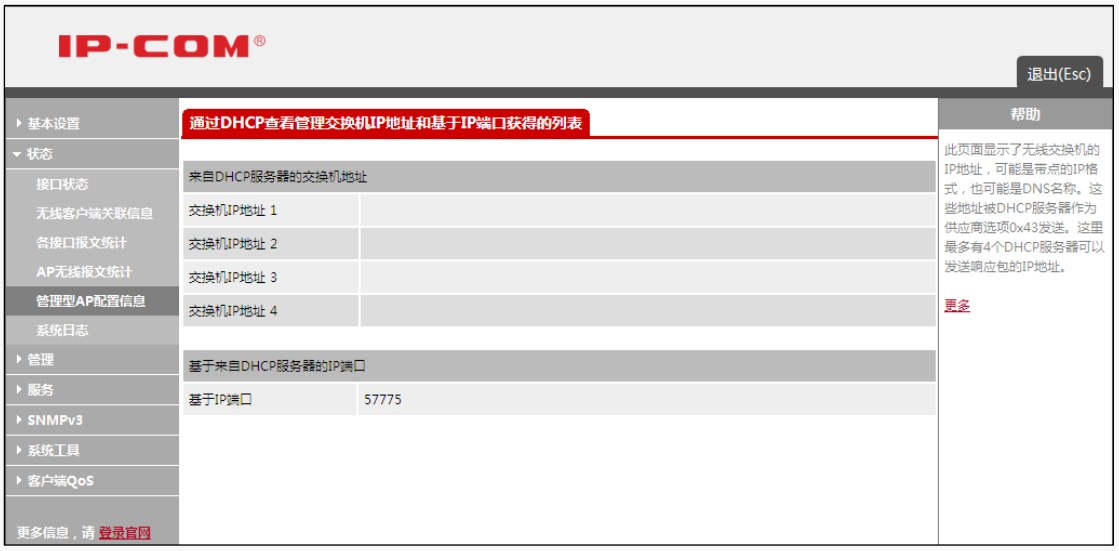
显示 AP 无线接口的数据包详细统计信息。点击『状态』→『AP 无线报文统计』进入页面。

以下是对各页面显示参数的说明：

标题项	说明
无线	选择查看无线 1（5G）还是无线 2（2.4G）的统计信息。 以下各显示信息均基于此处所选择的无线类型。
WLAN 接收数据包	接收到的数据包个数。
WLAN 接收字节	接收到的字节数。
WLAN 发送数据包	发送的数据包个数。
WLAN 发送字节	发送的字节数。
WLAN 接收时丢弃的数据包	接收到后丢弃的数据包个数。
WLAN 接收时丢弃的字节	接收到后丢弃的数据字节数。
WLAN 发送时丢弃的数据包	发送时丢弃的数据包个数。
WLAN 发送时丢弃的字节	发送时丢弃的数据字节数。
接收到的分片	已接收的类型数据或管理 MPDU 帧的数量。
已传输的分片	已发送的单播或多播数据、管理 MPDU 的数量。
接收的多播帧	已接收的多播 MSDU 帧的数量。
发送的多播帧	已发送的多播 MSDU 帧的数量。
复帧计数	收到的相同帧的个数。
传输失败次数	MSDU 发送失败的次数。
发送重试次数	一次或多次重试后成功发送 MSDU 的次数。
多个重试次数	一次以上重试后成功发送 MSDU 的次数。
RTS 成功次数	接收到响应 RTS 帧的 CTS 帧数量。
RTS 失败次数	未接收到响应 RTS 帧的 CTS 帧数量。
ACK 失败次数	未接收到的预期的 ACK 帧数量。
FCS 错误次数	在收到的 MPDU 帧中检测到 FCS 错误的次数。
发送帧次数	成功发送的 MSDU 数。
WEP 不可解密次数	接收到的加密帧的数量，以及发送方关键配置表示该帧本不应该被加密或由于接收站未实现隐私选项，该帧被丢弃。

5 管理型 AP 配置信息

显示 AP 设置为可管理模式时，FASTPATH 统一无线交换机的 IP 地址及端口。点击『状态』→『管理型 AP 配置信息』进入页面。



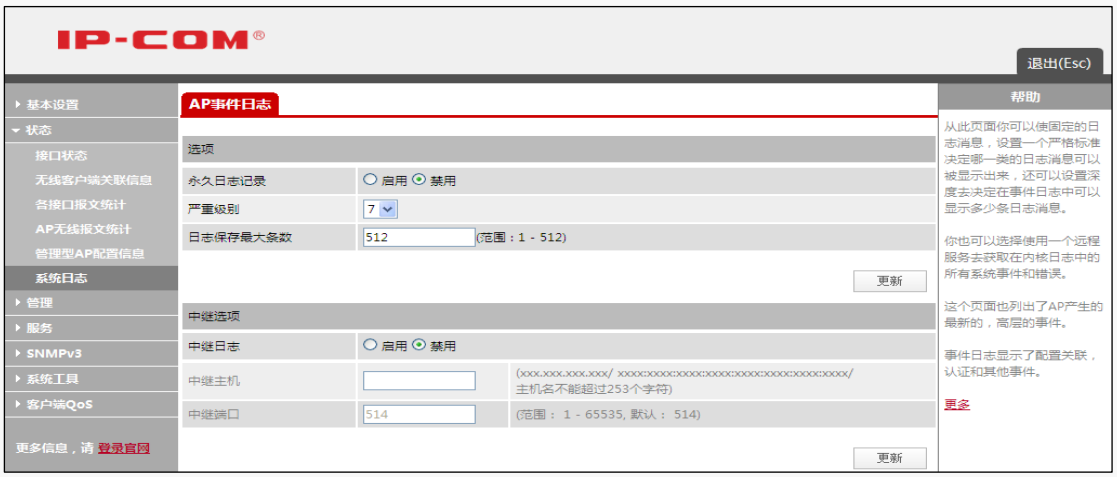
以下是对各页面显示参数的说明：

标题项	说明
交换机 IP 地址 1-4	AP 发现的 FASTPATH 统一无线交换机的 IP 地址，最多可发现 4 个。
基于 IP 端口	AP 与 FASTPATH 统一无线交换机通信的端口号，由 DHCP 选项 43 分配。

6 系统日志

本页可设置 AP 的日志记录参数，还可以查看到 AP 近期记录的日志信息。点击『状态』→『系统日志』进入页面。

6.1 日志选项设置

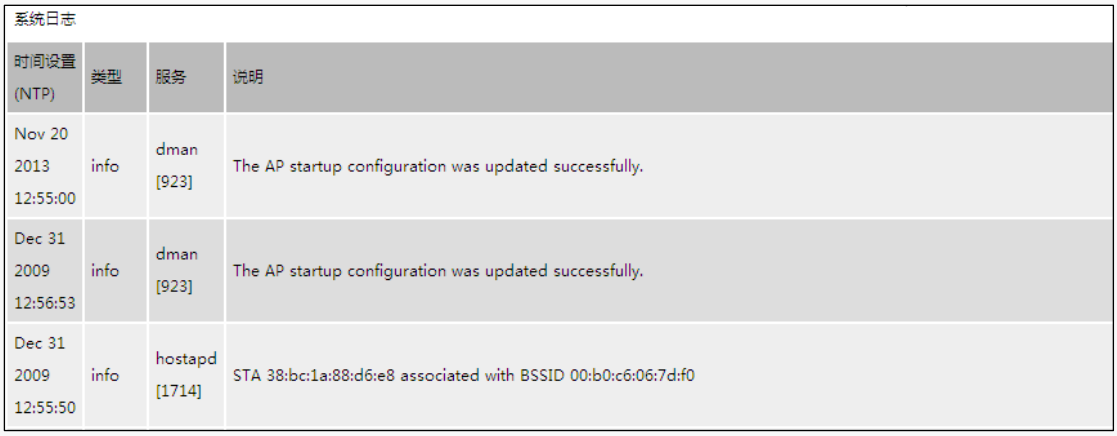


以下是对页面各参数的说明：

标题项	说明
永久日志记录	将日志信息保存在非易失性存储器（闪存）中，当 AP 重启时，日志不会被删除。（最大只可保存 128 条） **注意** 启用永久日志记录可能耗尽设备闪存，降低网络性能。您应该只在调试故障时启用永久日志记录。完成故障调试后，请禁用永久日志记录。
严重级别	设置系统日志的严重程度，高于此级别的将会被保存下来。具体日志级别定义请点击 Web 页面上的更多，查看更加详细的介绍。
日志保存最大条数	设置可保存的日志最大条目数。取值范围<1-512>。
中继日志	是否允许 AP 将其产生的系统日志同步到远程日志服务器上。
中继主机	输入指定的日志服务器的 IP 地址。
中继端口	日志服务器使用的端口号。

6.2 系统日志

显示近期记录的系统日志信息。


系统日志

时间设置(NTP)	类型	服务	说明
Nov 20 2013 12:55:00	info	dman [923]	The AP startup configuration was updated successfully.
Dec 31 2009 12:56:53	info	dman [923]	The AP startup configuration was updated successfully.
Dec 31 2009 12:55:50	info	hostapd [1714]	STA 38:bc:1a:88:d6:e8 associated with BSSID 00:b0:c6:06:7d:f0

管理

本节实现对 AP 的功能进行管理，包括以下 10 部分内容：

以太网设置：设置 AP 的以太网（即有线接口）参数。

VAP：设置虚拟接入点参数。

管理 IPv6：设置管理接口的 IPv6 地址信息。

IPv6 隧道：进行基于 ISATAP（站内自动隧道寻址协议）的 IPv6 隧道配置。

射频设置：设置无线射频参数，调试 AP 的性能。

WDS：设置 WDS，连接两个或多个独立的 LAN 或 WLAN，组建一个互通的网络实现数据访问。

MAC 认证：控制计算机通过 AP 访问网络的权限。

负载均衡：平衡分配区域中多个无线客户端对多个 AP 的使用。

管理型 AP：管理 AP 的胖（FAT）、瘦（FIT）、WDS 模式，设置相关参数。

管理 ACL：控制计算机对 AP 进行 Web 管理的权限。

1 以太网设置

设置 AP 的以太网（有线接口）参数。点击『管理』→『以太网设置』进入设置页面。

1.1 以太网设置概述

以太网设置，管理 AP 的以太网 LAN 口设置信息。默认情况下，AP 的 LAN 口连接类型为 DHCP，即自动从网络中的 DHCP 服务器获取其 LAN 口 IP 地址信息。默认管理 VLAN ID 为 1（默认的 Untagged VLAN），这意味着：如果您的网络上已经配置有一个与此 VLAN ID 不同的管理 VLAN，您必须更改 AP 的管理 VLAN ID 和其一致，才能对 AP 进行管理。

1.2 以太网设置参数说明

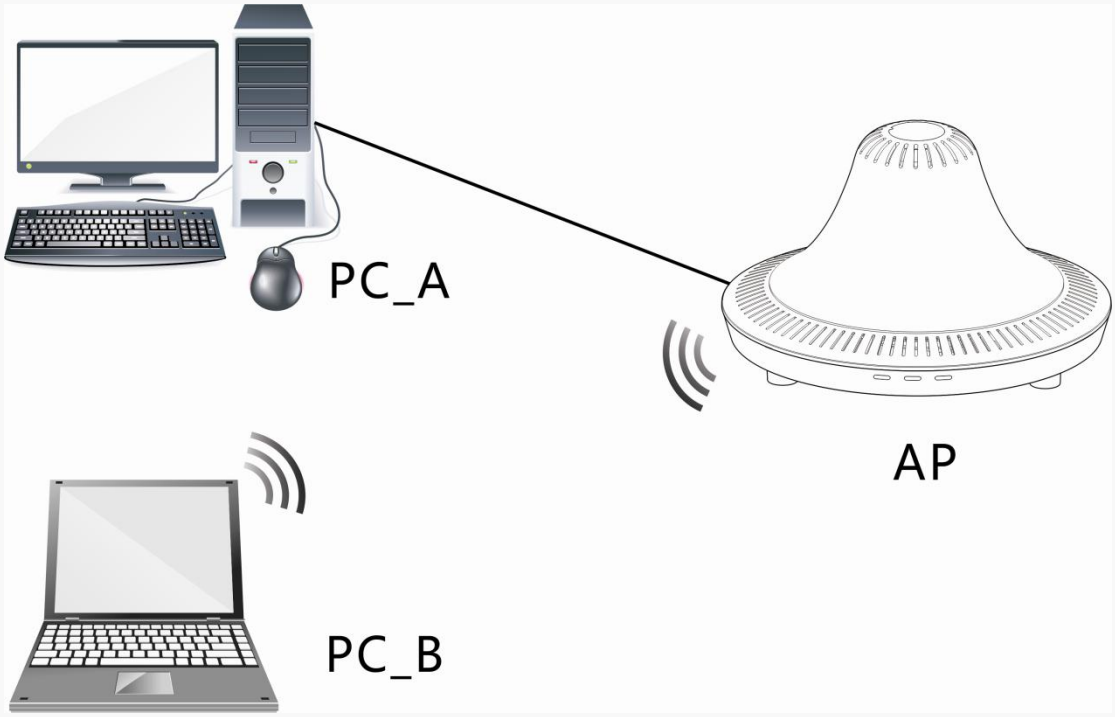
以下是对页面各参数的说明：

标题项	说明
主机名	设置 AP 的主机名。该主机名将出现在串口、telnet 及 SSH 管理 AP 时的命令行接口。主机名有以下要求： ➢ 长度必须在 1-63 个字符之间。 ➢ 有效字符为大写、小写字母，数字和连字符。 ➢ 第一个字符必须是字母（a-z 或 A-Z），最后一个字符不能为连字符。
MAC 地址	显示 AP LAN 口的 MAC 地址。
管理 VLAN ID	AP 的 LAN 口 IP 地址对应的 VLAN ID。默认管理 VLAN ID 为 1，取值范围<1-4094>。
Untagged VLAN	未标记的 VLAN。禁用时，所有的流量将会被打上一个 VLAN ID 标记。 默认情况下，AP 上所有的流量都会被剥去 tag，除非您禁用 untagged VLAN。
Untagged VLAN ID	该字段指定的 VLAN 上的流量将不会打上 VLAN ID 标记。取值范围<1-4094>。
连接类型	**DHCP**：AP 从 DHCP 服务器自动获取其 IP，子网掩码，DNS，网关信息。 **静态 IP**：您必须手动填写 AP 的 IP，子网掩码，DNS，默认网关信息。
静态 IP 地址	连接类型为静态 IP 时，在此输入 AP 的 LAN 口 IP 地址。
子网掩码	连接类型为静态 IP 时，在此输入 AP 的 LAN 口子网掩码。
默认网关	连接类型为静态 IP 时，在此输入 AP 的默认网关。
DNS 域名服务器	选择并设置 AP 的 DNS 模式。 **动态**：DNS 服务器的 IP 地址通过 DHCP 自动分配。此选项仅当您指定 DHCP 作为连接类型时可用。 **手动**：您必须分配静态 IP 地址解析域名。

1.3 以太网设置典型配置举例

组网需求：如下图所示，AP（IP 地址为 192.168.0.254/24）与 PC_A（IP 地址为 192.168.1.15/24）通过以太网相连。

现要实现如下需求：通过以太网设置将 AP 的管理 IP 地址更改为 192.168.1.12。

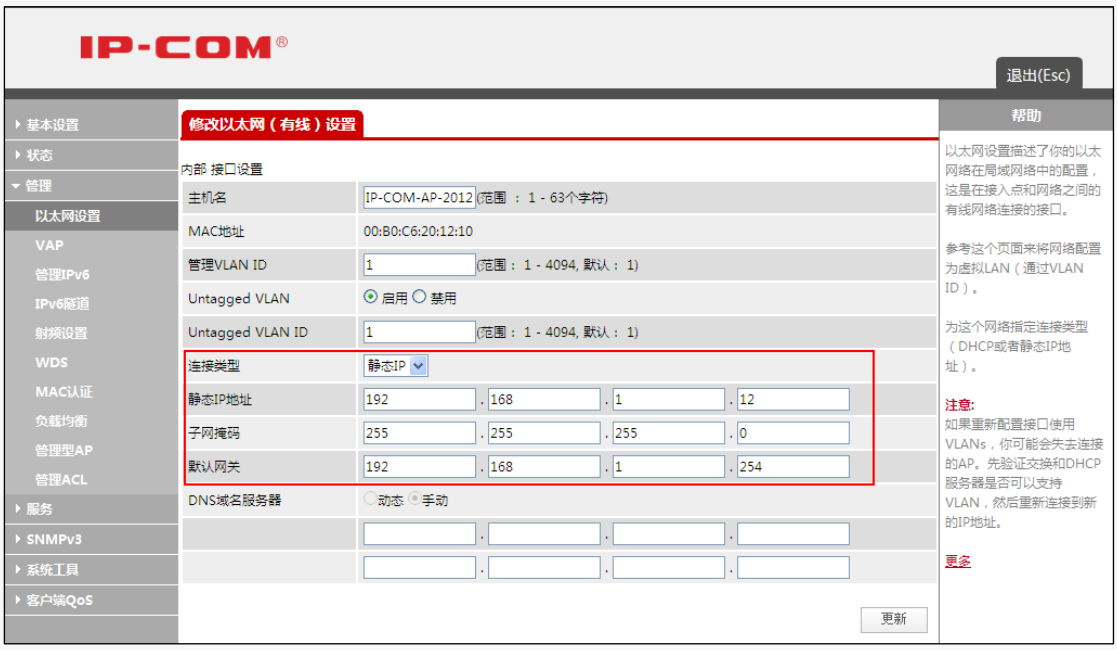


设置步骤：

步骤 1：进入『管理』→『以太网设置』页面。

步骤 2：选择连接类型为“静态 IP”，设置 IP 地址为“192.168.1.12”，设置默认网关为“192.168.1.254”。

步骤 3：点击 更新 ，保存配置信息。



步骤 4：PC_A 在其浏览器地址栏中输入 192.168.1.12 进入 AP 的 Web 网管界面。

2 VAP

本节设置 VAP（虚拟接入点）。点击『管理』→『VAP』进入页面。

2.1 VAP 概述

VAP 将无线局域网划分成相当于以太网 VLAN 的多个广播域，即，将多个虚拟 AP 模拟到一个物理的 AP 上，每个无线类型最多支持 16 个 VAP。

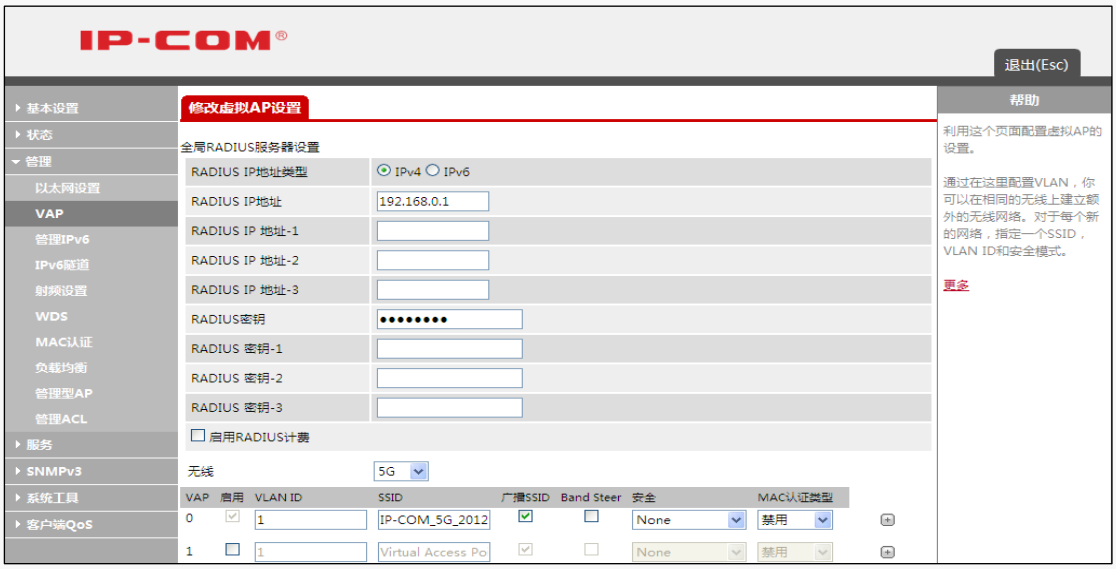
每个 VAP 均可以有一个独特的 SSID，多个不同的 SSID 使单个 AP 在网络上的其他系统看来像拥有两个或多个 AP。通过配置 VAP，您可以更好地控制影响网络性能的广播和组播流量。

您可以为每个 VAP 指定一个唯一的 VLAN，也可以配置多个 VAP 使用相同的 VLAN，所有 VAP 的默认 VLAN ID 均为 1。AP 会根据您在『管理』→『VAP』页面配置的或使用外部 RADIUS 服务器分配的 VLAN ID，给无线客户端的流量打上对应的 VLAN ID 标签。如果您使用的是外部 RADIUS 服务器，您可以在一个 VAP 上配置多个 VLAN，当客户端进行关联和认证时，外部 RADIUS 服务器将无线客户端分配给 VLAN。

您最多可以配置四个全局 IPv4 或 IPv6 RADIUS 服务器。其中一台服务器作为主服务器，其他则作为备份服务器。您可以配置每个 VAP 均使用全局 RADIUS 服务器设置（默认设置），也可以基于每个 VAP 配置 RADIUS 服务器组，您还可以为每个 VAP 单独配置 RADIUS 服务器设置。例如，您配置一个 VAP 使用 IPv6 RADIUS 服务器，其他的 VAP 使用全局 IPv4 RADIUS 服务器的设置。

如果无线客户端使用的安全模式不能与 RADIUS 服务器进行通信，或者 RADIUS 服务器不提供 VLAN 信息，您可以给每个 VAP 分配一个 VLAN ID，AP 将 VLAN 分配给通过该 VAP 连接它的所有的无线客户端。

2.2 VAP 参数说明



以下是对页面各参数的说明：

标题项	说明
RADIUS IP 地址类型	指定 RADIUS 服务器使用的 IP 地址类型。 **提示** 您可以切换地址类型，配置 IPv4 和 IPv6 全局 RADIUS 地址，但 AP 只和您选中的地址类型的一个或多个 RADIUS 服务器联系。
RADIUS IP/IPv6 地址	输入全局 RADIUS 服务器的 IPv4 或 IPv6 地址。默认情况下，每个 VAP 均使用您在此定义的全局 RADIUS 服务器。当第一个无线客户端尝试与 AP 进行认证时，AP 发送认证请求到全局服务器。 如果全局服务器响应认证请求，AP 将继续使用此 RADIUS 服务器作为全局服务器，认证请求被发送到您在此指定的地址。 如果在前一个字段中选择了 IPv4 RADIUS IP 地址类型选项，请在此输入全局 RADIUS 服务器的 IP 地址，例如 192.168.10.23。 如果在前一个字段中选择了 IPv6 RADIUS IP 地址类型选项，请输入全局 RADIUS 服务器的 IPv6 地址，例如 2001:0db8:1234::abcd。
RADIUS IP/IPv6 地址 1-3	输入备份 RADIUS 服务器的 IP 或 IPv6 地址。 如果与全局 RADIUS 服务器认证失败，则依次尝试向此处填写的备份 RADIUS 服务器进行认证。
RADIUS 密钥	输入全局 RADIUS 服务器的共享密钥。最多可包含 63 个字符，可以是标准的字母，数字和特殊字符。区分大小写。

	您输入的文字会显示为“*”字符，以防他人看到您键入的密钥。 您必须在 AP 和 RADIUS 服务器上配置相同的密钥。
RADIUS 密钥 1-3	输入与配置的备份 RADIUS 服务器关联的 RADIUS 密钥。 RADIUS IP/IPv6 地址-1 的服务器使用 RADIUS 密钥-1，RADIUS IP/IPv6 地址-2 的服务器使用 RADIUS 密钥-2，以此类推。
启用 RADIUS 计费	选择此选项可以跟踪和衡量一个特定用户的资源消耗，如系统时间，发送和接收的数据量等等。 勾选时，全局 RADIUS 服务器和备份服务器均会启用计费。
无线（Radio）	选择要配置的无线。VAP 是在每个无线上独立配置的。
VAP	每个无线最多可以配置 16 个 VAP。VAP0 是物理无线接口(physical radio interface)，只有禁用无线（Radio）时才能禁用 VAP0。
启用	启用/禁用网络。禁用指定网络后，该网络的 VLAN ID 一并丢失。
VLAN ID	当无线客户端通过此 VAP 连接到 AP，AP 会给所有来自该无线客户端的流量打上此 VLAN ID 标记，除非您输入 untagged VLAN ID，或使用一个 RADIUS 服务器将无线客户端分配到 VLAN。VLAN ID 取值范围<1-4094>。 如果您使用基于 RADIUS 的客户端认证，您可以选择添加 Tunnel-Type、Tunnel-Medium-Type、Tunnel-Private-Group-ID 属性到 RADIUS 或 AAA 服务器上相应的字段为客户端配置 VLAN。 RADIUS 服务器分配的 VLAN ID 将覆盖 VAP 页面上配置的 VLAN ID。在以太网设置页面，您可以配置 untagged 和管理 VLAN ID。
SSID	输入无线网络名称。SSID 是由字母、数字组成的字符串，最多允许 32 个字符。 多个 VAP 的 SSID 可以设置为相同的，也可以设置为各自不同。 **注意** 如果您是用无线连接到您正在管理的 AP，重设 SSID 会使您丢失与 AP 的连接。保存设置后，您需要重新连接到新的 SSID。
广播 SSID	指定是否允许 AP 在其 Beacon 帧中广播 SSID，默认启用。当 VAP 不广播其 SSID 时，它的无线网络名称不会显示在客户端的可用网络列表中，客户端在请求连接之前必须输入它的 SSID。 **注意** 禁止 SSID 广播提供了一个非常小的保护级别，它足以防止客户端意外连接到您的网络，但它阻止不了黑客甚至最简单的企图连接或监视未加密的流量。

Band steer	Load balance clients to higher capacity 5GHz band.
安全	为该 VAP 选择一个安全模式，可选的项有：None、Static WEP、WPA Personal、IEEE 802.1X、WPA Enterprise。 **注意** 您在此设置的安全模式是专用于此 VAP 的。如果您选择“None”以外的安全模式，将会显示其他字段，字段解释见下文。
MAC 认证类型	配置一个 MAC 地址全局列表，允许或拒绝列表中的 MAC 地址访问网络。此功能的下拉菜单允许您选择 MAC 地址认证使用的类型： ➢ 禁用：不使用 MAC 地址认证。 ➢ 本地：使用您在 MAC 认证页面上配置的 MAC 认证列表。 ➢ RADIUS：使用外部 RADIUS 服务器上的 MAC 认证列表。

None(Plain-text)

该模式意味着 AP 发送或接收的任何数据都是没有经过加密的。它在最初的网络配置或解决故障时可能是有用的，但我们不建议在内部网络上经常使用，因为它不安全。

Static WEP

有线等效加密(WEP)是一种 802.11 无线网络数据加密协议，其用以保护数据的 RC4 密码属于对称性流密码。使用有线等效加密后，无线网络上所有的无线站点和接入点都配置一个静态的 64 位（40 位密钥+24 位的初始化向量（IV））或 128 位（104 位密钥+24 位 IV）共享密钥对数据进行加密。

如果要使用 WEP，您需要在『管理』→『射频设置』页面，修改无线模式为 802.11a 或 802.11b/g。

WEP 不是最安全的模式，但它比 None(Plain-text)提供了更多的保护，因为它防止网络外的用户轻易嗅探出未加密的无线流量。

以下是对 Static WEP 参数的说明：

标题项	说明
传输密钥索引	选择密钥索引，表明 AP 将使用哪个 WEP 密钥对它传输的数据进行加密。 可用密钥索引范围为 1-4。默认值是 1。
密钥长度	指定密钥长度：64 位或 128 位。
密钥类型	指定可输入的密钥类型：ASCII 码或十六进制字符。
WEP 加密	在文本框中输入密钥字符串，输入字符类型取决于选择的密钥类型： ➢ ASCII：包括大小写字母，数字和特殊符号，如@，＃。 ➢ 十六进制：包括数字 0 到 9 和字母 A 到 F。 最多可以指定 4 个 WEP 密钥。 客户端站点必须将“传输密钥索引”、该密钥索引对应的“WEP 加密密钥”设置为和 AP 设置一致才能和 AP 进行通信。 **所需字符**：WEP 密钥输入框中允许输入的字符个数。该值由您选择的密钥长度和密钥类型决定并自动更新。例如，如果您使用 128 bits 的 ASCII 码，您必须输入 26 个字符的 WEP 密钥。
认证	定义了使用 Static WEP 安全模式时，客户端站点与 AP 关联的方法。 可选的认证算法有：开放式系统和共享密钥。
开放式系统	无论客户端是否具有正确的 WEP 密钥，均允许与 AP 关联。该算法适用于 plain-text，IEEE 802.1X，和 WPA 模式。 **注意** 只是允许客户端关联，并不保证它可以与 AP 交换流量。客户端必须有正确的 WEP 密钥，才能够成功地访问、解密来自 AP 的数据，以及向 AP 发送可读数据。
共享密钥	要求客户端必须有正确的 WEP 密钥才可以与 AP 关联。此时，WEP 密钥不正确的客户端，将无法与 AP 关联。
开放式系统和共享密钥	同时选择时： ➢ 配置使用共享密钥模式的客户端站点，必须具有有效的 WEP 密钥才可以与 AP 关联。 ➢ 配置使用开放式系统的客户端站点（共享密钥模式未启用）将能够与 AP 关联，即使他们没有正确的 WEP 密钥。

IEEE 802.1X

IEEE 802.1X 是一种基于端口的网络接入控制协议（Port Based Network Access Control Protocol）。“基于端口的网络接入控制”是指在 AP 的端口这一级对所接入的客户端进行认证和控制。连接在端口上的客户端如果能通过认证，就可以访问 AP 的 WLAN 中的资源；如果

不能通过认证，则无法访问 WLAN 中的资源。

IEEE 802.1X 提供动态生成的密钥，密钥定期更新。此时，AP 需要一个支持 EAP 的 RADIUS 服务器对客户端进行认证，如 Microsoft Internet 验证服务器。因要与 Windows 客户端一起工作，故认证服务器必须支持受保护的 EAP（PEAP）和 MSCHAP V2。

如果要使用 IEEE 802.1X，您需要在『管理』→『射频设置』页面，修改无线模式为 802.11a 或 802.11b/g。

以下是对 IEEE 802.1X 参数的说明：

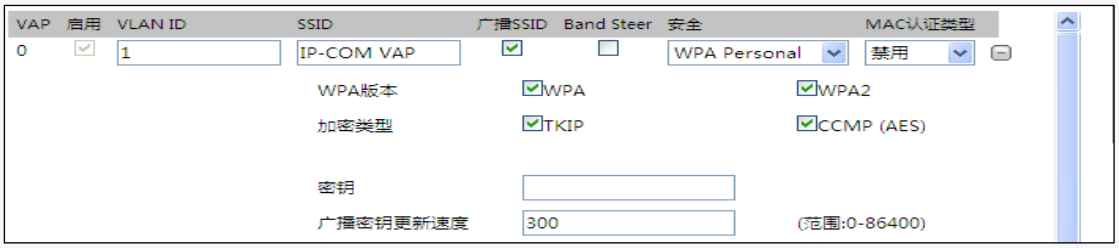
标题项	说明
使用全局 RADIUS 服务器设置	默认情况下，所有 VAP 均使用您在本页上方为 AP 定义的全局 RADIUS。您也可以配置每个 VAP 使用一组不同的 RADIUS 服务器。 ➢ 要使用全局 RADIUS 服务器设置，确保复选框已选中。 ➢ 要在 VAP 使用独立的 RADIUS 服务器，清除该复选框并在下面对应的输入框中输入 RADIUS 服务器的 IP 地址和密钥。
RADIUS IP 地址类型	指定 RADIUS 服务器使用的 IP 版本。
RADIUS IP/IPv6 地址	输入该 VAP 的主 RADIUS 服务器的 IPv4 或 IPv6 地址。 ➢ 如果在前一个字段中选择了 IPv4 RADIUS IP 地址类型选项，输入主 RADIUS 服务器的 IP 地址，例如 192.168.10.23。 ➢ 如果选择了 IPv6 RADIUS IP 地址类型选项，输入主 RADIUS 服务器的 IPv6 地址，例如 2001:0db8:1234::abcd。

RADIUS IP/IPv6 地址 1-3	此 VAP 最多可输入 3 个备份的 RADIUS 服务器。 ➢ 如果您选择了 IPv4 RADIUS IP 地址类型，请输入 RADIUS 服务器的 IP 地址。 ➢ 如果您选择了 IPv6 RADIUS IP 地址类型，请输入 RADIUS 服务器的 IPv6 地址。 **注意** 如果与主服务器认证失败，则依次尝试与每个备份服务器进行认证。
RADIUS 密钥	输入主 RADIUS 服务器的共享密钥。最多可以使用 63 个标准的字母（区分大小写），数字和特殊字符。 您输入的文字会显示为“*”字符，以防他人看到您键入的密钥。 AP 和 RADIUS 服务器上必须配置相同的密钥。
RADIUS 密钥 1-3	输入与配置的备份 RADIUS 服务器关联的 RADIUS 密钥。 RADIUS IP 地址-1 的服务器使用 RADIUS 密钥-1，RADIUS IP 地址-2 的服务器使用 RADIUS 密钥-2，以此类推。
启用 RADIUS 计费	选择此选项可以跟踪和衡量一个特定用户的资源消耗，如系统时间，发送和接收的数据量，等等。 如果启用 RADIUS 计费，主 RADIUS 服务器和备份服务器均会启用它。
广播密钥更新速度	为关联到此 VAP 的客户端设置广播密钥更新周期，默认为 300。取值范围<0-86400>，单位秒，为 0 表示广播密钥不更新。
会话密钥更新速度	为关联到此 VAP 的每个客户端设置会话（单播）密钥更新周期。取值范围<0-86400>，单位秒，为 0 表示会话密钥不更新。

WPA Personal（WPA 个人版）

WPA 基于 IEEE 802.11i 草案三制定，WPA2 则是基于 IEEE 802.11i 正式规范制定，比 WPA 具有更高的安全性及规范性。

两者均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 的无线客户端的密钥完全相同，因此，其密钥难于管理并容易泄漏，不适合在安全要求非常严格的场合应用。



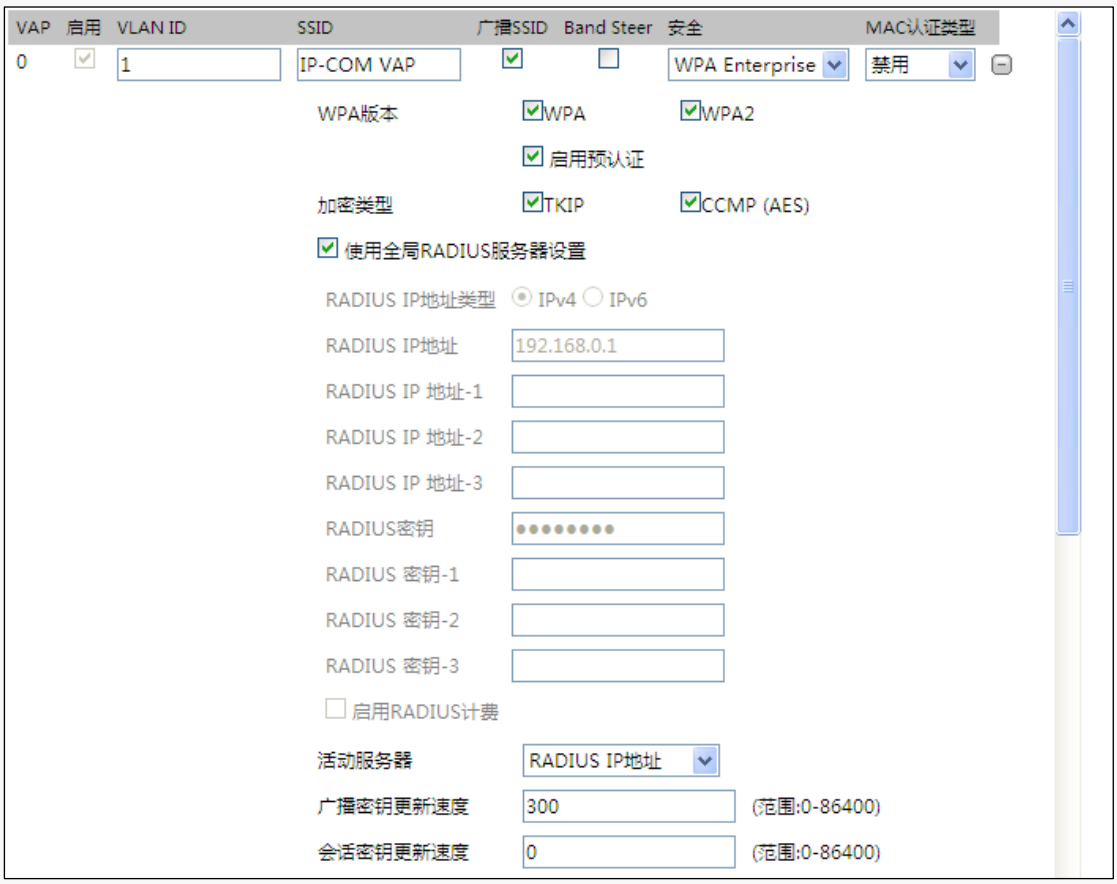
以下是对 WPA Personal 参数的说明：

标题项	说明
WPA 版本	选择您要支持的客户端站点的 WPA 类型。 **WPA**：如果网络上的所有客户端站点均支持 WPA，不支持 WPA2，请选择 WPA。 **WPA2**：如果网络上的所有客户端站点均支持 WPA2，建议使用 WPA2，按照 IEEE 802.11i 标准，它提供了最佳的安全性。 **WPA 和 WPA2**：如果网络上有混合的客户端，一些支持 WPA2，一些仅支持 WPA，那么选择两个复选框。使 WPA 和 WPA2 客户端都可以关联和认证，但对支持 WPA2 的客户端使用更强大的 WPA2 安全。WPA 允许更多的互操作性，以安全为代价。
加密类型	选择您要使用的密码类型：TKIP 或 CCMP(AES)或 TKIP 和 CCMP(AES)。 WPA 客户端必须满足以下条件之一才能与 AP 关联： ➢ 一个有效的 TKIP 密钥。 ➢ 一个有效的的 CCMP（AES）密钥。 未配置使用 WPA Personal 的客户端将无法与 AP 关联。
密钥	WPA Personal 的预共享密钥，是一个至少 8 个字符，最多 63 个字符的字符串。可接受的字符包括大小写字母，数字和特殊符号，如@，＃。
广播密钥更新速度	输入一个值为关联到此 VAP 的客户端设置广播密钥更新周期，默认为 300。 取值范围<0-86400>，单位秒，为 0 表示广播密钥不更新。

WPA Enterprise

为了改善 WPA-Personal 在密钥管理方面的不足，WiFi 联盟提供了 WPA Enterprise，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，攻击者难于获取加密密钥。因此，WPA Enterprise 极大的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。



以下是对 WPA Enterprise 参数的说明：

标题项	说明
WPA 版本	选择您要支持的客户端站点类型： **WPA**：如果网络上所有客户端站点均支持 WPA，不支持 WPA2，请选择 WPA。 **WPA2**：如果网络上的所有客户端站点均支持 WPA2，建议使用 WPA2，按照 IEEE 802.11i 标准，它提供了最佳的安全性。 **WPA 和 WPA2**：如果网络上有混合的客户端，一些支持 WPA2，一些仅支持 WPA，那么选择两个复选框，使 WPA 和 WPA2 客户端都可以关联和认证。这样，支持 WPA2 的客户端更安全，WPA 允许更多的互操作性，但以安全为代价。
启用预认证	如果您在选择 WPA 版本时，选择了仅 WPA2 或 WPA 和 WPA2，您可以启用 WPA2 客户端预认证。此功能可以帮助加快连接到多个 AP 的漫游客户端认证。 如果您想 WPA2 无线客户端发送预认证数据包，勾选“启用预认证”。预认证信息将被从客户端目前正在使用的 AP 中继到目标 AP。 如果您选择 WPA，则此选项不适用，因为 WPA 不支持此功能。
密码类型	选择您要使用的密码类型：TKIP、CCMP(AES)、TKIP 和 CCMP(AES)。 默认情况下，TKIP 和 CCMP 均被选中。此时，配置使用 WPA RADIUS 的客户

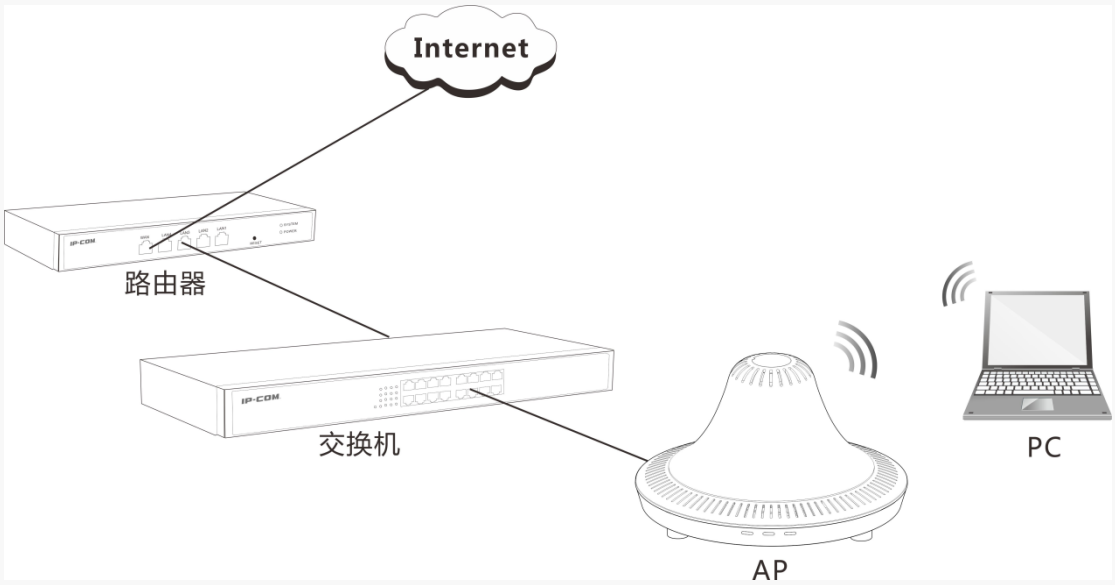
	端必须具备下列条件之一： ➢ 一个有效的 TKIP RADIUS IP 地址和 RADIUS 密钥。 ➢ 一个有效的 CCMP（AES）IP 地址和 RADIUS 密钥。
使用全局 RADIUS 服务器设置	默认情况下，所有 VAP 均使用您在本页上方为 AP 定义的全局 RADIUS 服务器。您也可以配置每个 VAP 使用一组不同的 RADIUS 服务器。 ➢ 要使用全局 RADIUS 服务器设置，确保该复选框已选中。 ➢ 要在 VAP 使用独立的 RADIUS 服务器，清除该复选框并在对应的输入框中输入 RADIUS 服务器的 IP 地址和密钥。
RADIUS IP 地址类型	指定 RADIUS 服务器使用的 IP 版本。
RADIUS IP/IPv6 地址	输入该 VAP 的主 RADIUS 服务器的 IPv4 或 IPv6 地址： ➢ 如果在前一个字段中选择了 IPv4 RADIUS IP 地址类型，输入主 RADIUS 服务器的 IPv4 地址，例如 192.168.10.23。 ➢ 如果在前一个字段中选择了 IPv6 RADIUS IP 地址类型，输入主 RADIUS 服务器的 IPv6 地址，例如 2001:0db8:1234::abcd。
RADIUS IP/IPv6 地址 1-3	最多可为此 VAP 输入 3 个 IPv4 或 IPv6 地址的备份 RADIUS 服务器。 ➢ IPv4 RADIUS IP 地址类型时，请输入 RADIUS 服务器的 IP 地址。 ➢ IPv6 RADIUS IP 地址类型时，请输入 RADIUS 服务器的 IPv6 地址。 **注意** 若和主 RADIUS 服务器认证失败，则按顺序向每个配置好的备份服务器认证。
RADIUS 密钥	输入主 RADIUS 服务器的共享密钥。最多可以使用 63 个标准的字母（区分大小写），数字和特殊字符。 您必须在 AP 和您的 RADIUS 服务器上配置相同的密钥。 您输入的文字会显示为“*”字符，以防他人看到您键入的 RADIUS 密钥。
RADIUS 密钥 1-3	输入与配置的备份 RADIUS 服务器关联的 RADIUS 密钥。 RADIUS IP 地址-1 的服务器使用 RADIUS 密钥-1，RADIUS IP 地址-2 的服务器使用 RADIUS 密钥-2，以此类推。
启用 RADIUS 计费	选择此选项可以跟踪和衡量一个特定用户的资源消耗，如系统时间，发送和接收的数据量，等等。 如果您启用 RADIUS 计费，主 RADIUS 服务器和备份服务器也会启用它。
广播密钥更新速度	为关联到此 VAP 的客户端设置广播密钥更新周期，默认为 300。

	取值范围<0-86400>，单位秒，为 0 表示广播密钥不更新。
会话密钥更新速度	为关联到此 VAP 的每个客户端设置会话（单播）密钥更新周期。 取值范围<0-86400>，单位秒，为 0 表示会话密钥不更新。

2.3 FAT AP 的无线典型配置举例

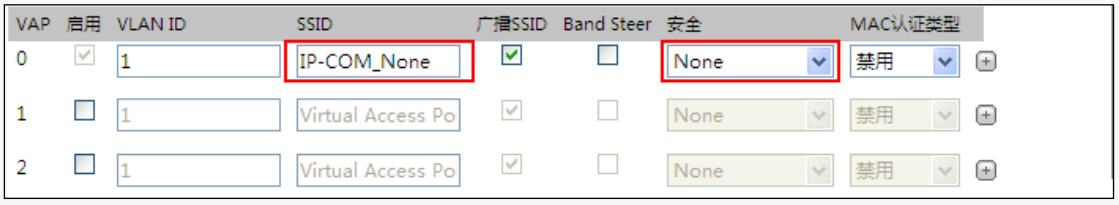
组网需求：某部门为了保证工作人员可以随时随地访问部门内部的网络资源，需要通过部署 AP 实现移动办公。

假设：AP 的 Lan 口 IP 地址为 192.168.0.254，可上网路由器的 Lan 口 IP 地址为 192.168.1.1，DNS 地址为 8.8.8.8。



不加密方式下设置步骤：

步骤 1：进入『管理』→『VAP』页面，配置好相关的 SSID，如“IP-COM_None”，选择安全为“None”，点击 更新 保存设置。

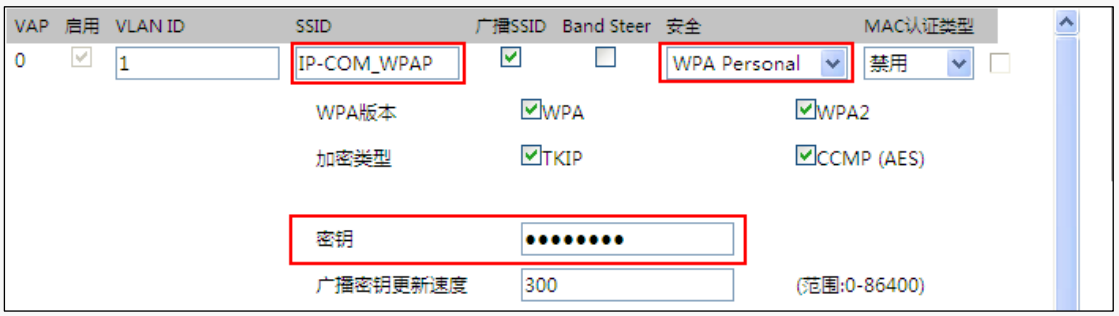


步骤 2：配置客户端的无线网卡 IP 地址：192.168.1.X（X 为 2-254，局域网内不能出现相同的 IP 地址），子网掩码：255.255.255.0，默认网关：192.168.1.1，首选 DNS 服务器：8.8.8.8。

步骤 3：客户端直接连接 AP 的无线（SSID：IP-COM_None）。

WPA Personal 认证方式下设置步骤：

步骤 1：进入『管理』→『VAP』页面，配置好相关的 SSID，如“IP-COM_WPAP”，选择安全为“WPA Personal”，设置密钥，如“12345678”，点击 更新 保存设置。



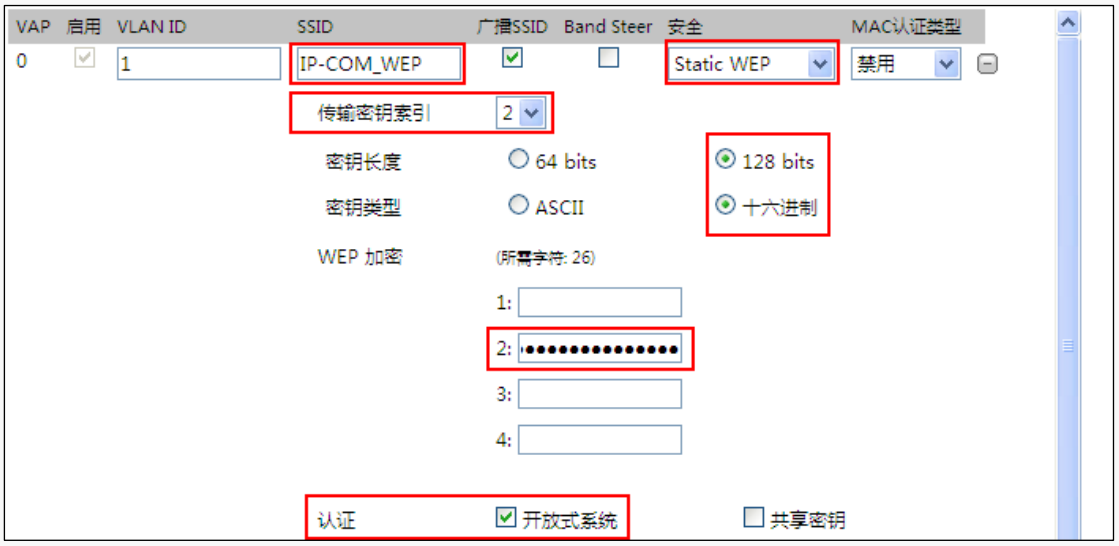
步骤 2：配置客户端的无线网卡 IP 地址：192.168.1.X（X 为 2-254，局域网内不能出现相同的 IP 地址），子网掩码：255.255.255.0，默认网关：192.168.1.1，首选 DNS 服务器：8.8.8.8。

步骤 3：客户端使用 WPA2-PSK/AES，密码 12345678 连接 AP 的无线（SSID：IP-COM_WPAP）。

WEP 认证方式下的设置步骤：

步骤 1：进入『管理』→『VAP』页面，配置好相关的 SSID，如“IP-COM_WEP”，选择安全为“Static WEP”。

步骤 2：设置传输密钥索引，如“2”，设置密钥长度，如“128 bits”，选择密钥类型，如“十六进制”，在 2 输入框输入密钥，如“1234567890abcde1234567890a”，设置认证，如“开放式系统”点击 更新 保存设置。



步骤 3：配置客户端的无线网卡 IP 地址：192.168.1.X（X 为 2-254，局域网内不能出现相同的 IP 地址），子网掩码：255.255.255.0，默认网关：192.168.1.1，首选 DNS 服务器：8.8.8.8。

步骤 4：客户端使用开放式认证，密钥索引 2，密码 1234567890abcde1234567890a 连接 AP 的无线（SSID：IP-COM_WEP）。

3 管理 IPv6

本节设置管理接口的 IPv6 地址信息。点击『管理』→『管理 IPv6』进入页面。

3.1 管理 IPv6 参数说明

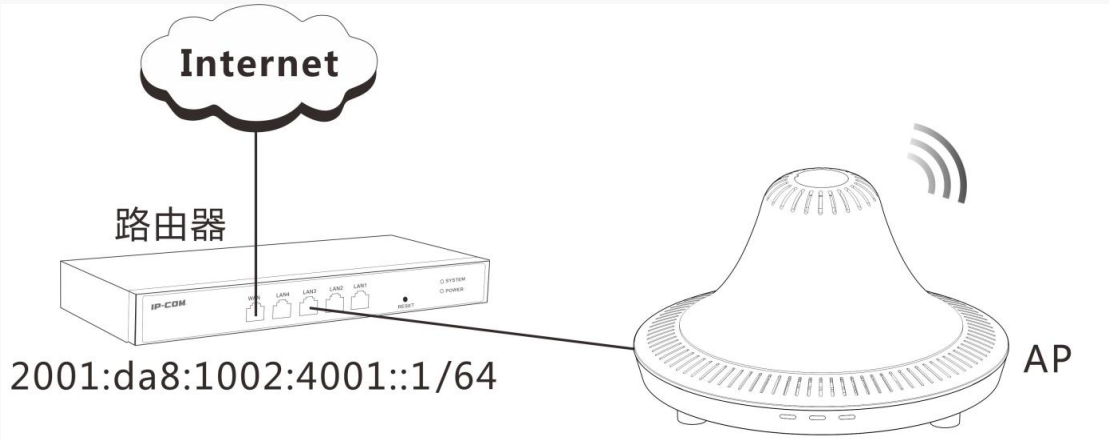
以下是对页面各参数的说明：

标题项	说明
IPv6 连接类型	**DHCPv6**：AP 从 DHCPv6 服务器自动获得 IPv6 地址，DNS 和网关信息。 **Static IPv6**：手动设置 AP 的 IPv6 地址，DNS 和网关信息。
IPv6 管理模式	启用或禁用 IPv6 管理。
IPv6 自动配置管理模式	启用/禁用 IPv6 自动地址配置。启用时，AP 通过处理 LAN 端口上接收的路由器通告自动配置 IPv6 地址和网关。 **注意** AP 可以有多个自动配置的 IPv6 地址。
静态 IPv6 地址	输入静态 IPv6 地址。即使地址已经自动配置了，AP 也可以有一个静态 IPv6 地址。
静态 IPv6 地址前缀长度	输入静态 IPv6 前缀长度。取值范围<0-128>。
静态 IPv6 地址状态	显示分配到 AP 管理端口的静态 IPv6 地址的状态。可能为“Operational”和“Tentative”。
IPv6 自动配置全局地址	在此列出 AP 已经自动获得的一个或多个 IPv6 地址。
IPv6 链路本地地址	显示本地物理链路层使用的 IPv6 链路本地地址。 链路本地地址由 IPv6 邻居发现过程分配，是不可配置的。

默认 IPv6 网关	输入默认 IPv6 网关。
IPv6 DNS 服务器	选择 IPv6 域名服务器地址获取方式： ➢ 动态：通过 DHCPv6 自动分配 DNS 服务器的 IPv6 地址。 ➢ 手动：您必须手动填写静态 IPv6 地址来解析域名。 **注意** 动态模式选项仅在您将连接类型指定为 DHCPv6 时可用。

3.2 静态 IPv6 配置举例

组网需求：具体如下图。假设上级路由器支持 IPv6。

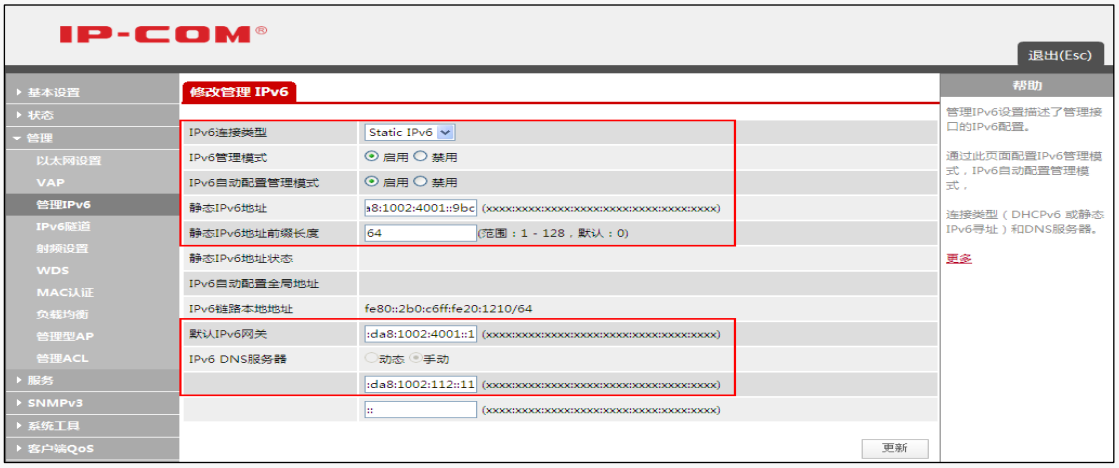


配置步骤：

步骤 1：进入『管理』→『管理 IPv6』页面。

步骤 2：设置以下 IPv6 参数后，点击 更新 ，保存设置。

- IPv6 连接类型：Static IPv6
- IPv6 管理模式：启用
- IPv6 自动配置管理模式：启用
- 静态 IPv6 地址，与上级路由同一网段的 IPv6 地址，如 2001:da8:1002:4001::9bc
- 静态 IPv6 地址前缀长度：与上级路由一致（64）
- 默认 IPv6 网关：路由网关（2001:da8:1002:4001::1）
- IPv6 DNS 服务器：手动
- 首选 DNS 服务器：本地的 DNS 服务器（2001:da8:1002:112::11）
- 备份 DNS 服务器：可选填



4 IPv6 隧道

本节设置 IPv6 隧道。点击『管理』→『IPv6 隧道』进入页面。

4.1 ISATAP 概述

ISATAP(Intra-Site Automatic Tunnel Addressing Protocol，站内自动隧道寻址协议)连接网络上的双栈（IPv6/IPv4 节点)。ISATAP 将 IPv4 网络视作 IPv6 的链路层，支持类似 Non-Broadcast Multiple Access(NBMA)模式的自动隧道化机制。

4.2 IPv6 隧道参数说明

以下是对页面各参数的说明：

标题项	说明
ISATAP 状态	启用/禁用 ISATAP 隧道。
ISATAP 可用主机	指定 ISATAP 路由器的 IP 地址或 DNS 名称。默认值为 isatap。

ISATAP 查询间隔	在知道 ISATAP 路由器的 IP 地址之前，隧道的 DNS 查询间隔。 取值范围<120-3600>，单位为秒。默认值为 120 秒，您也可以自定义该时间间隔。
ISATAP 征集间隔	当没有活动 ISATAP 路由器的时候，ISATAP 路由器征集信息之间间隔。 取值范围<120-3600>，单位为秒。默认值为 120 秒，您也可以自定义该时间间隔。
ISATAP IPv6 链路本地地址	显示 ISATAP 接口的 IPv6 链路本地地址。
ISATAP IPv6 全局地址	显示 ISATAP 接口的全局 IPv6 地址。

5 射频设置

本节设置 AP 的射频参数。点击『管理』→『射频设置』进入页面。

5.1 射频设置概述

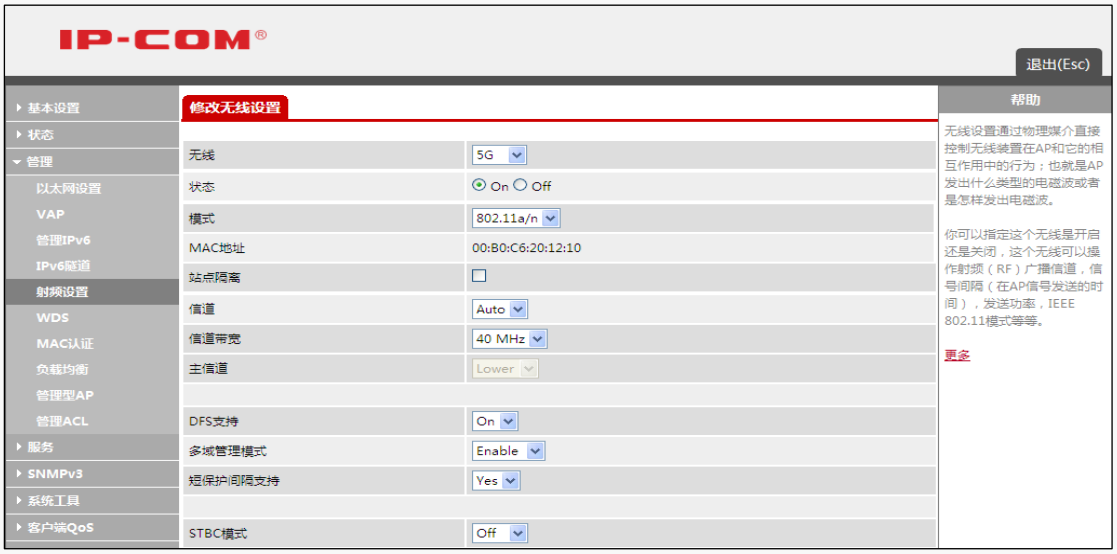
射频设置直接控制 AP 中的射频设备的行为及其与物理介质的相互作用，即，AP 如何发射电磁波及发射什么类型的电磁波。

根据您所选择的无线类型（5G 或 2.4G），页面将显示不同的设置，页面显示的设置仅适用于您选择的那个无线。如果 5G 和 2.4G 的射频参数均需进行设置，请先将其中一个无线的射频参数设置完成后，点击 更新 保存设置；再选择并设置另一个无线，设置完成后同样需要点击 更新 保存设置。

注意

更改某些参数可能会导致 AP 重启，此时，无线客户端将暂时失去连接。建议您在 WLAN 流量较低时对此部分参数进行更改。

5.2 射频设置参数说明



以下是对一些射频设置参数的说明：

标题项	说明
无线	选择要配置的无线类型：5G 表示无线 1，2.4G 表示无线 2。此表中其余设置适用于您在此选择的无线类型。 **注意** 确保对 5G 和 2.4G 的无线都进行配置。
状态	启用/禁用无线功能。 ➢ On：启用无线功能，默认选择 On。 ➢ Off：禁用无线功能，禁用后，所有与该无线相关的功能都将禁止。
模式	无线使用的物理层（PHY）标准，可选的模式取决于您选择的无线类型。 ➢ 802.11a：仅允许 802.11a 客户端连接到 AP。 ➢ 802.11a/n：工作在 5G 频段的 802.11a 和 802.11n 客户端均可连接至 AP。 ➢ 802.11b/g：802.11b、802.11g 的客户端可以连接到 AP； ➢ 802.11b/g/n：工作在 2.4G 频段的 802.11b，802.11g 和 802.11n 客户端均可连接至 AP。 **注意** 5G 无线默认为 802.11a/n 模式；2.4G 无线默认为 11b/g/n 模式。
MAC 地址	显示该无线类型的对应的无线接口 MAC 地址（VAP0 的 MAC）。

站点隔离	勾选后，同一 SSID 下的客户端之间不能相互访问。
信道	指定射频的工作信道，可以从下拉列表中选择其它有效的工作信道。 **auto**：自动选择信道模式。选择此模式后，AP 会评估无线网络中的信道质量，自动选择质量最优的信道作为工作信道。
信道带宽	除其他模式可用的传统的 20MHz 信道外，802.11n 规范允许 40MHz 宽的信道。40MHz 信道可实现更高的数据传输速率，但可用于其它 2.4GHz 和 5GHz 设备的信道变的更少。 设置为 20MHz 时，限制只能使用 20MHz 的信道带宽。
主信道	此设置仅在 40MHz 信道带宽时适用。 ➢ Upper：设置主信道为 40MHz 中上面的 20MHz 信道，可选择的信道为 5-13。 ➢ Lower：设置主信道为 40MHz 中下面的 20MHz 信道，可选择的信道为 1-9。
DFS 支持	动态频率选择（DFS）支持，仅在 5G 无线类型时适用。 DFS 是一种要求无线设备共享频谱，避免在 5G 频段上与雷达系统同信到操作的机制。DFS 基于监管领域的要求变化，它由 AP 的国家代码设置决定。 5G 无线启用 DFS 支持时，监管领域要求在信道上进行雷达探测，802.11h 的 DFS 和 TPC（传输功率控制）特点被激活。
多域管理模式（世界模式）	➢ Enable：AP 在 Beacon 帧和 probe response 帧中携带国家代码，此时允许客户端在任何国家代码中操作而不需要重新配置。默认为 Enable。 ➢ Disable：AP 不在 Beacon 帧中携带国家代码，这仅适用于 2.4GHz 无线类型；工作在 5GHz 频段的无线，由于 AP 软件配置支持 802.11h，国家代码信息将在 Beacon 帧中广播。
短保护间隔支持	开启/关闭短保护间隔（Short Guard Interval，Short GI）支持功能。 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。 ➢ 802.11a/g 的 GI 时长为 800ns。 ➢ 802.11n 可以配置使用 Short GI，Short GI 时长为 400ns。 **提示** 使用 Short GI 时，可提高 10%的无线吞吐量。

STBC 模式	STBC 模式仅在选择的无线模式包括 802.11n 时适用。 空时分组编码(Space Time Block Coding，STBC)是一项 802.11n 技术，旨在提高数据传输的可靠性。数据流在多天线中传输，因此接收系统在多数据流中可以有一个更好的选择。 ➢ On：AP 支持在多天线中同时传输相同的数据流。 ➢ Off：AP 不支持在多天线中传输相同的数据流。 ➢ Auto：AP 根据数据流情况自动选择开启与不开启 STBC 模式。 **提示** 默认 STBC 为 On，建议开启 STBC 模式以提高无线吞吐量。

以下是对页面各参数的说明：

标题项	说明
保护	保护可保证 802.11n 不干扰传统站点或应用。默认为启用（Auto）。 ➢ Auto：如果传统设备处于 AP 覆盖范围内，则保护机制被激活。 ➢ Off：在 AP 覆盖范围内的传统客户端或 AP 将会受到 802.11n 传输的影响。 保护机制也适用于 802.11b/g 模式，此时，它保护 802.11b 的客户端或 AP 不受到 802.11g 传输的影响。 **提示** 保护机制不会影响客户端关联 AP 的能力。

信标间隔	发送 Beacon 帧的时间间隔。默认为 100ms。 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。
DTIM 周期	DTIM（Delivery Traffic Indication Map，延迟传输指示映射）帧之间的 Beacon 间隔数。取值范围<1-255>，单位：beacon。 DTIM 会由此周期倒数至 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：如果 DTIM 周期为 1，则客户端将在每个 Beacon 帧中均对 AP 上的缓冲数据进行检查；如果 DTIM 周期为 10，客户端将每隔 10 个 Beacon 检查一次。
分片阈值	指定帧的分片门限值。取值范围<256-2346>，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。当数据包的实际大小超过指定的分片门限值时，该数据包被分片传输。 ➢ 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 阈值	启用冲突避免机制所要求的帧的长度门限值。当帧的实际长度大于设置的门限值时，启用冲突避免机制，以避免数据发送冲突。取值范围<0-2347>。 RTS 阈值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 阈值的数据帧不启动该机制。
最多站点数	允许同时与 AP 关联的客户端的最大个数。取值范围<1-200>。
发射功率	设置发射功率的百分比值。默认值为 100%。 发射功率越大，则 AP 的覆盖范围更广。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。
固定的组播速率	选择您想要 AP 支持的组播流量传输速率。 Auto：自动在支持速率集和所有客户端都支持的速率中选取一个速率，作为 BSS 中的多播帧的发送速率。

Legacy Rate Sets	设置您想要 AP 支持的传输速率集和 AP 公告的基本速率集。 **支持速率**：表示 AP 支持的一组速率。选中多个速率时，AP 会根据错误率以及客户端站点与 AP 之间的距离等因素，自动选择最有效率的速率。 **基本速率**：表示 AP 为达到与网络上的其他接入点和客户端站点建立通信的目的，而公告到网络上的速率。通常更有效的是，AP 广播其支持的速率集的子集。
广播/多播速率限制	**速率限制**：填写您所需要的多播或广播速率，取值范围<1-300>。 **速率限制突发**：设置组播/广播数据包使无线组播通道达到极限的个数。

6 WDS

WDS（Wireless Distribution System，无线分布式系统）：通过无线链路连接两个或者多个独立的有线或者无线局域网，组建一个互通的网络实现数据访问。

提示

AP 从独立模式切换到管理模式时，将自动禁用 WDS 功能。

6.1 WDS 概述

802.11 无线技术已经在家庭、SOHO、企业等得到广泛地应用，用户已经能通过无线局域网方便地访问 Internet。传统网络应用中，AP 必须连接到已有的有线网络，才能提供无线用户的网络访问服务，从而导致最终部署成本较高，大面积无线覆盖时需要大量的时间等问题。

WDS 技术可以在一些复杂的环境中方便快捷地建设无线局域网。WDS 网络的优点包括：

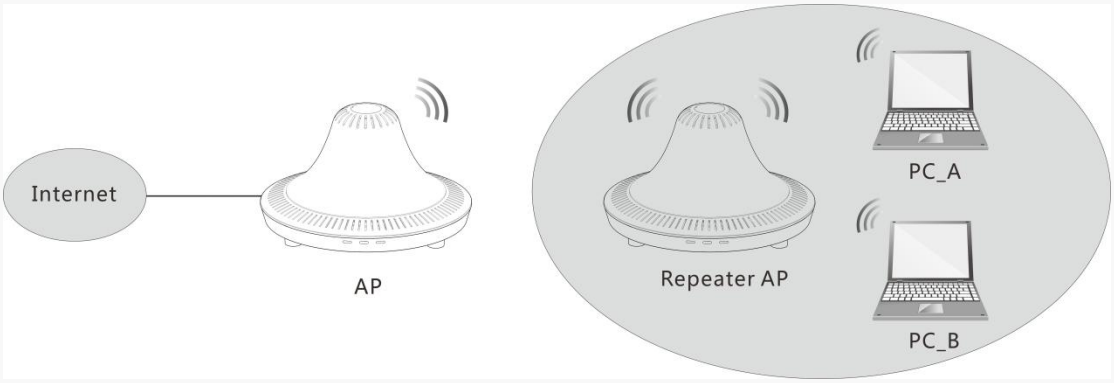
- 通过无线网桥连接两个独立的局域网段，并且在他们之间提供数据传输。
- 低成本，高性能。
- 扩展性好，并且无需铺设新的有线连接和部署更多的 AP。
- 适用于公司，大型仓储，制造等领域。

根据实际应用需求，WDS 网络可以提供了以下两种拓扑。通过在每个 AP 的 WDS 模式下配置对端 AP 的 MAC 地址来实现，详细配置请参见6.3 WDS 点到点典型配置举例。

点到点桥接

此时，AP 通过 WDS 链路与另一台 AP 建立桥接，同时还提供无线接入服务。也就是说：AP 不但创建无线网络，还通过 WDS 桥接将无线网络接入到已有网络中。

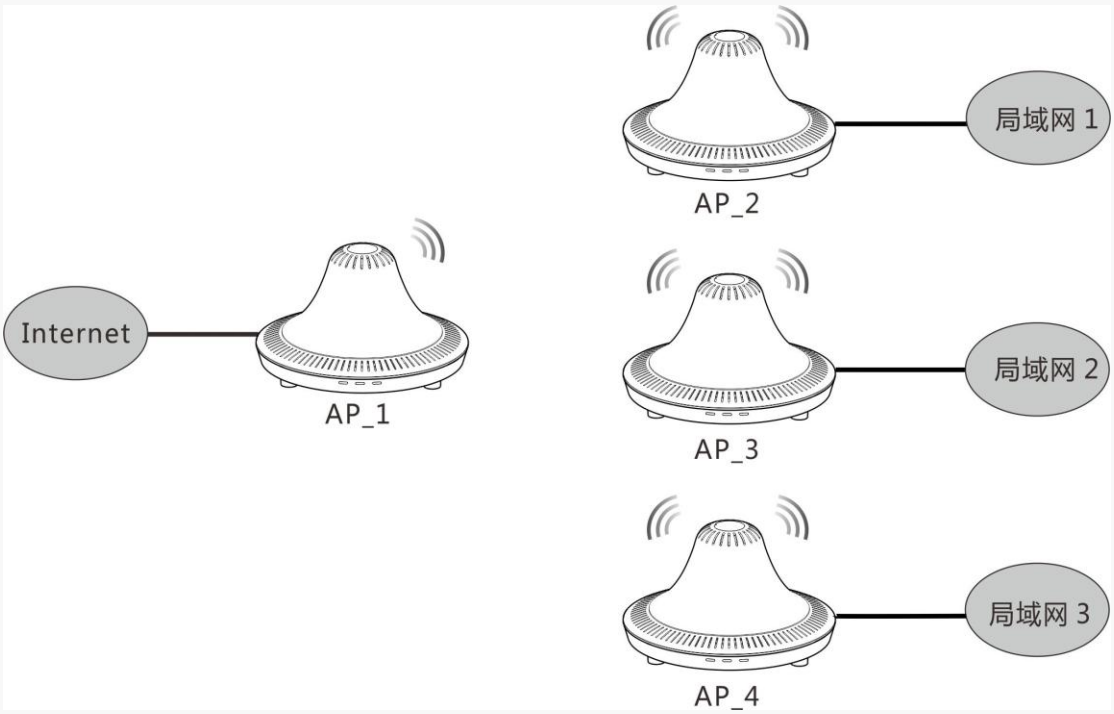
以下图为例，Repeater AP 虽然不直接接入有线网络，但是可以为 PC_A 和 PC_B 提供访问有线网络的服务。从应用的角度来看，通过网络中部署了 Repeater AP，延长了无线通信的距离，进而扩大了无线网络的覆盖范围。



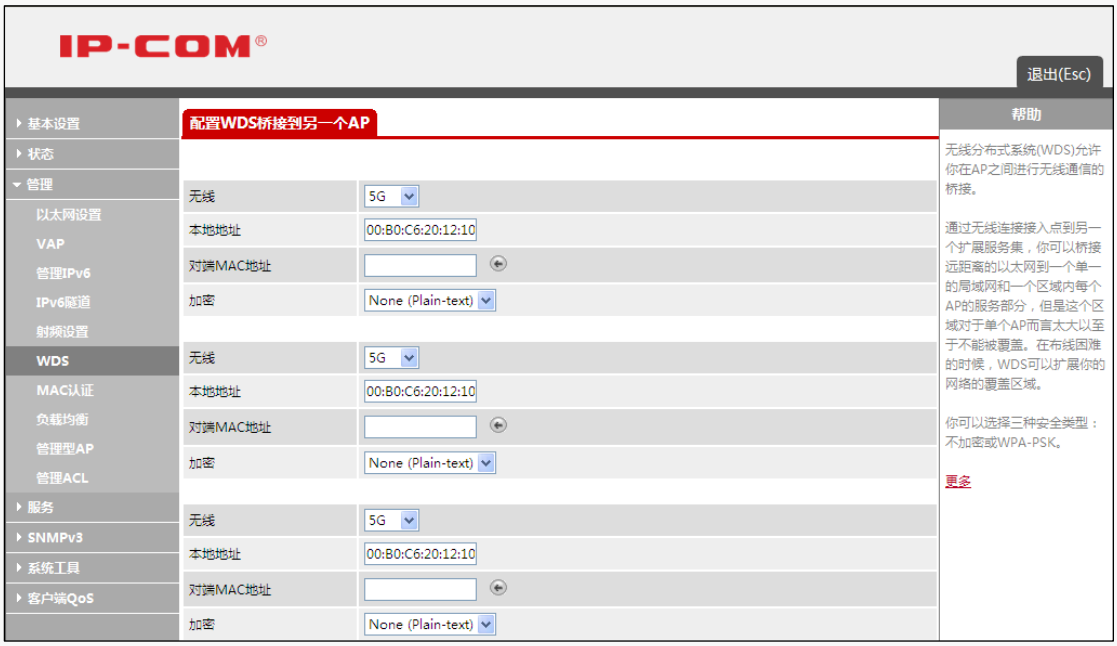
点到多点桥接

此时，一台 AP 作为中心 AP，其他所有的 AP 都只和中心 AP 建立无线桥接，实现多个网络的互联。该组网方式可以方便地解决多个网络孤岛需要连接到已有网络的要求，但是多个分支网络的互通都要通过中心桥接 AP 进行数据转发。

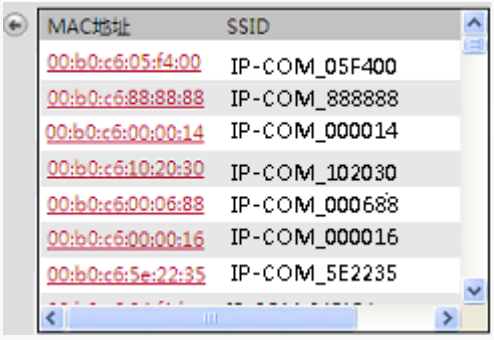
点到多点桥接组网应用拓扑示例如下图。

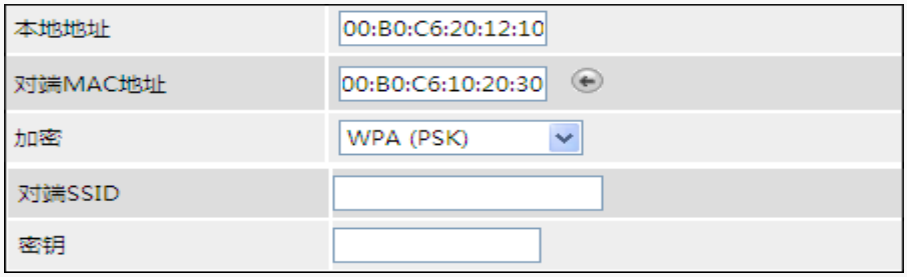


6.2 WDS 参数说明



以下是对页面各参数的说明：

标题项	说明
无线	选择进行 WDS 桥接的无线类型：5G 或 2.4G。 **注意** 以下其它的选项设置均适用于您在此选择的无线类型。
本地地址	显示 AP 的 MAC 地址。 对于每个点对点的 WDS 链路，本地地址反映了您所选择的无线类型的内部接口地址。
对端 MAC 地址	输入对端桥接 AP 的 MAC 地址，如果您不清楚，点击 图标扫描周围信号，出现如下页面：  在扫描列表里选择您想连接的 AP，点击 MAC 地址将您想连接的 AP 的 MAC 地址添加到地址栏中。之后，点击 更新 完成操作。

加密	None(Plain-text):WDS 不加密。 **WPA（PSK）**：如果您要对 WDS 链路加密，请选择 WPS(PSK)，出现如下页面：  **注意** 1. 选择 WPA（PSK）时需要输入对端桥接 AP 的 SSID 与密钥。 2. 如果 WDS 链路配置了 WPA-PSK，则您进行 WDS 的无线类型的 VAP0 必须设置为 WPA-PSK。
对端 SSID	为您已创建的 WDS 链路输入一个适当的名称。可以是不超过 32 个字符的任何字母数字的组合。 **注意** WDS 链路的另一端的 AP 也需要输入相同的 SSID。如果 WDS 连接的两个 AP 的 SSID 不一样，它们将无法通信和交换数据。
密钥	输入 WDS 链路唯一的共享密钥。WPA-PSK 密钥是一个 8-63 个字符的字符串。可接受的字符包括：大小写字母，数字和特殊字符，如@，＃。 **注意** WDS 链路另一端的 AP 也必须输入这个独特的共享密钥。如果两个 AP 的密钥不一样，它们将无法通信和交换数据。

6.3 WDS 点到点典型配置举例

组网需求：

室外环境中存在两个独立的局域网，如下图所示，现要实现这两个局域网的互通。

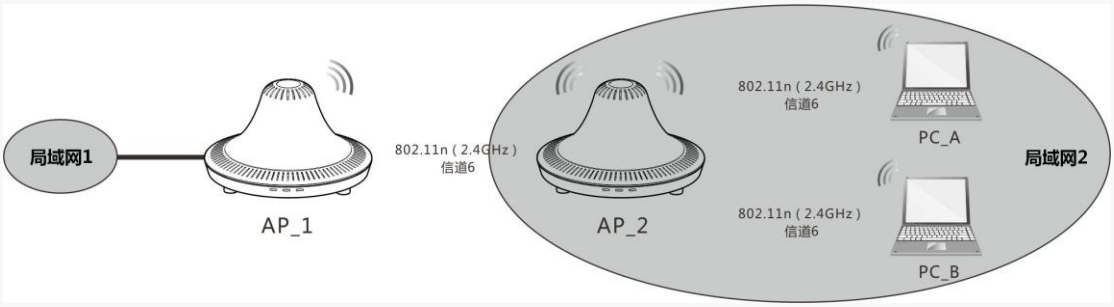
组网分析：

如果采用有线方式连接这两个局域网，需要使用挖沟开渠等方式铺设线缆，这样做工期长、开销大。此时，可以采用 WDS 链路连接这两个局域网，实现两个局域网之间的互通。

具体部署方式如下：

- AP_1 接入有线局域网（假设默认网关和 DNS 服务器 IP 均为：192.168.1.254），作为 Repeater 的 AP_2 通过 WDS 链路与 AP_1 建立连接，同时为 PC 提供无线接入服务。
- 手动指定 AP_1、AP_2 均使用固定信道 6，通过 802.11n(2.4GHz)射频模式使 AP_1 和 AP_2 之间形成 WDS 链路。

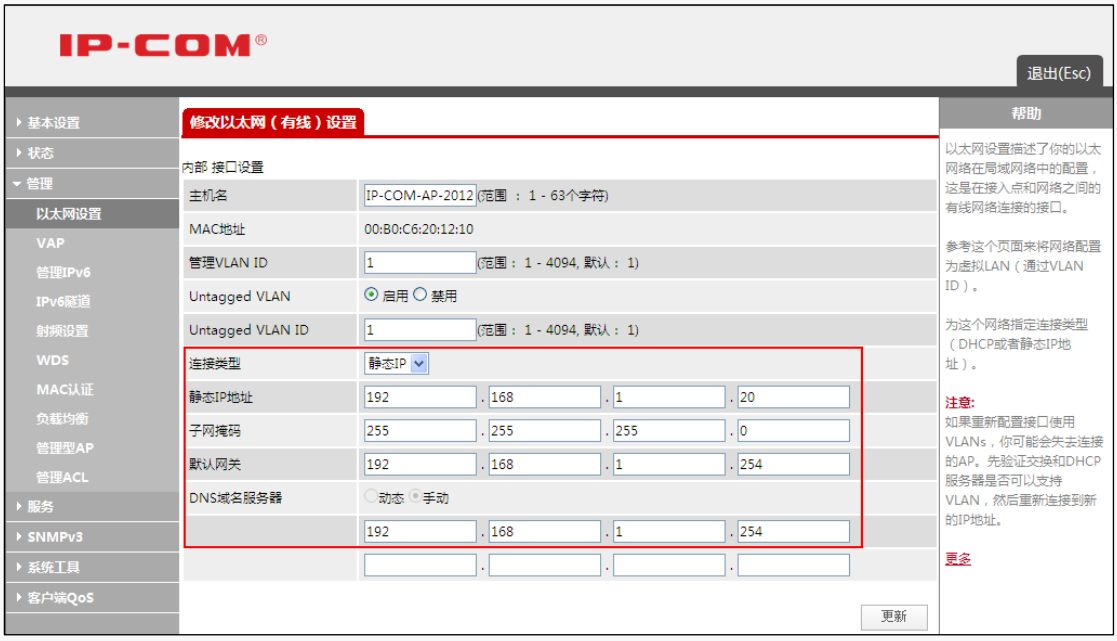
- 为了保证 WDS 链路的安全性，设置预共享密钥为“12345678”。
- 为了避免局域网 IP 地址冲突，并更方便 PC 对 AP_1 和 AP_2 同时进行管理，将 AP_1 和 AP_2 的 IP 地址设置为同网段的不同 IP 地址。如 AP_1：192.168.1.20，AP_2：192.168.1.10。



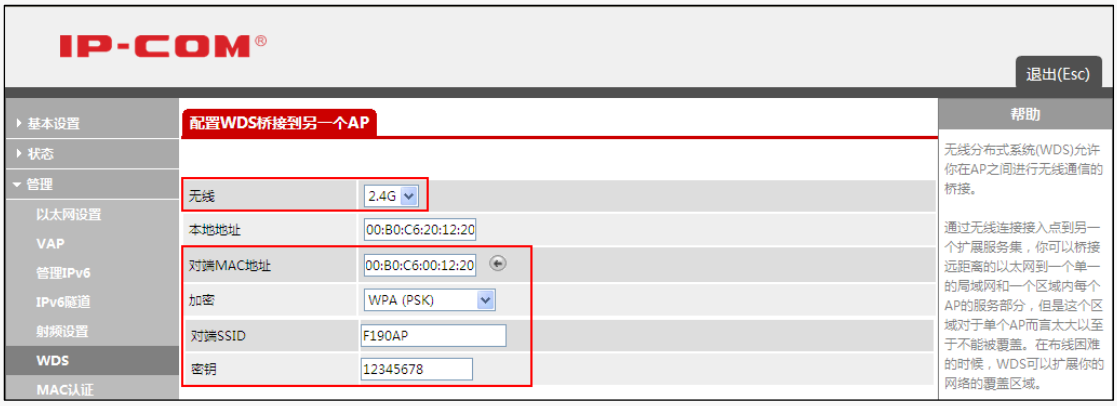
设置步骤：

步骤 1：配置 AP_1。

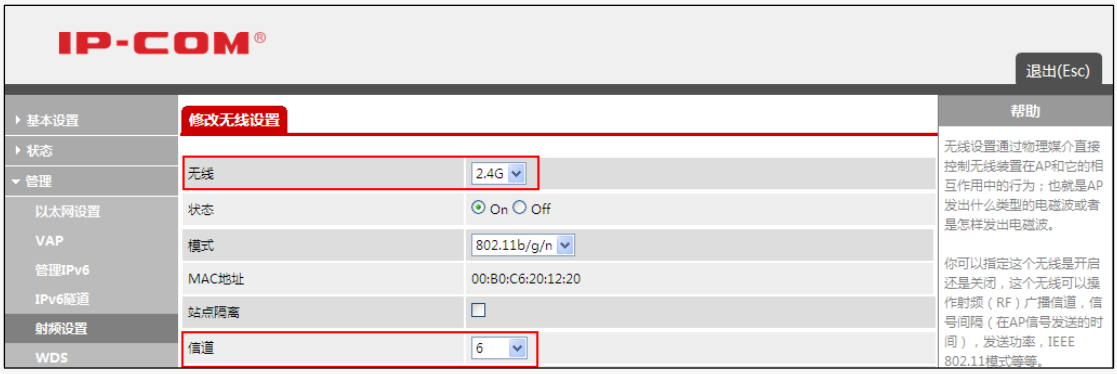
1. 配置 AP_1 的接口 IP 地址：进入『管理』→『以太网设置』页面，选择静态 IP，并配置 IP 地址，点击 更新 ；



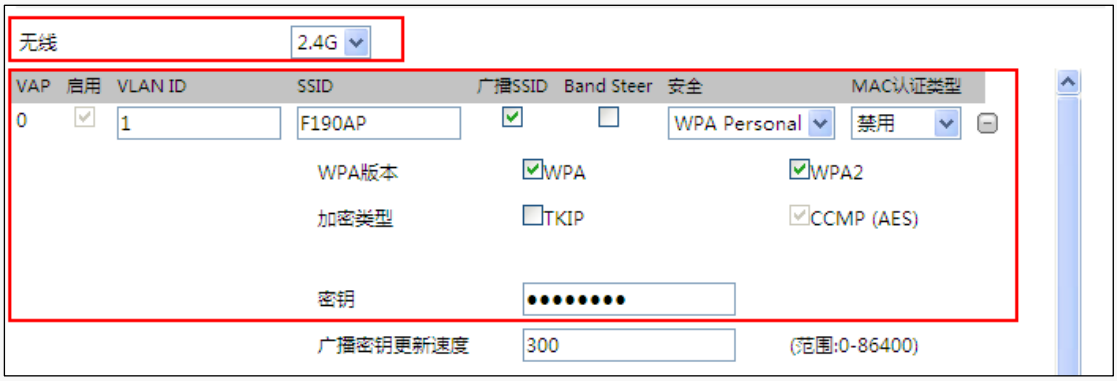
2. 配置 WDS：进入『管理→『WDS』页面，进行如下设置后，点击 更新 ；
   - 选择无线类型：2.4GHz
   - 输入对端 MAC 地址，如：00:B0:C6:00:12:20
   - 选择 WPA(PSK)加密
   - 输入对端 SSID，如：F190AP
   - 设置密钥，如：12345678



❸ 手动指定信道：进入『管理』→『射频设置』页面，选择 2.4G 无线，在信道下拉框中选择使用的信道 6，点击 更新 ；



❹ 手动指定 SSID：进入『管理』→『VAP』页面，选择 2.4G 无线后，在 VAP0 SSID 输入框中输入 F190AP，选择安全：WPA Personal，WPA 版本：WPA、WPA2，密钥：12345678，点击 更新 。



步骤 2：配置 AP_2。AP_2 的配置步骤和 AP_1 相同，此处不再重复。

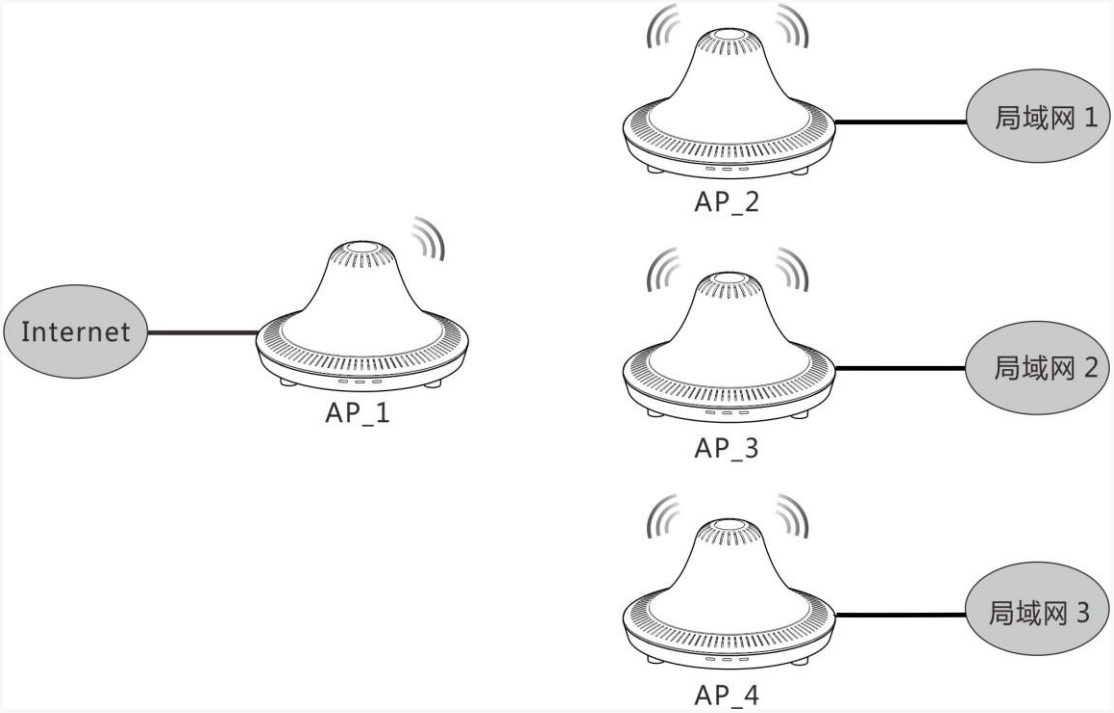
验证配置结果：在 AP_1 端主机 ping 通 AP_2 IP 192.168.1.10。

配置注意事项：

- WDS 功能需要两台 AP 均支持此功能，而且 SSID、信道、加密方式和密码必须与对端 AP 的相同。
- 如果需要对无线客户接入进行安全认证，设置完成保存后，需要重新启动 AP，才能使 WDS 设备之间正常通讯。

6.4 WDS 点到多点典型配置举例

组网需求：要求在 AP_1 分别和 AP_2，AP_3，AP_4 建立 WDS 链路。



配置思路：WDS 点到多点配置和普通无线 WDS 配置基本相同，但需要注意以下几点：

- 在 AP_1 的『管理』→『WDS』下配置邻居 AP_2、AP_3、AP_4 的 MAC 地址。
- 允许建立的最大 WDS 链路数为 4。

配置步骤：WDS 点到多点配置和普通无线 WDS 配置相同，具体配置步骤请参见 6.3 WDS 点到点典型配置举例中配置 AP_1 步骤。

验证配置结果：在 AP_1 端主机能 ping 通 AP_2、AP_3、AP_4 的 IP 地址。

配置注意事项：

- WDS 功能需要进行 WDS 的 AP 均支持此功能，而且 SSID、信道、加密方式和密码必须与对端 AP 的相同。
- 如果需要对无线客户接入进行安全认证，设置完成保存后，需要重新启动 AP，才能使 WDS 设备之间正常通讯。

7 MAC 认证

本节设置 AP 的 MAC 认证。点击『管理』→『MAC 认证』进入页面。

7.1 MAC 认证概述

MAC 认证，根据无线客户端的 MAC 地址来判断是否允许其通过无线连上 AP 访问网络。进行 MAC 认证前，您需要在 AP 或外部 RADIUS 服务器上配置全局 MAC 地址列表，然后，在 AP 的

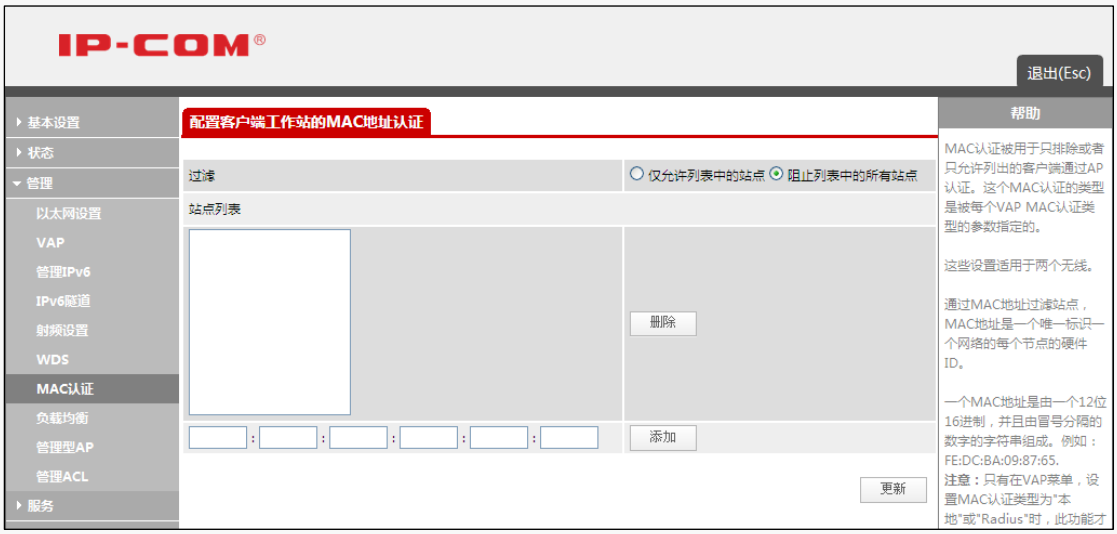
Web 网管上设置过滤规则，允许或拒绝指定 MAC 地址的无线客户端访问网络。

设置过滤规则后，当无线客户端尝试连接 AP 时，AP 根据您在『管理』→『VAP』页面设置的 MAC 认证类型，在对应的本地站点列表（您在『管理』→『MAC 认证』页面配置的 MAC 地址列表）或外部 RADIUS 服务器上查询无线客户端的 MAC 地址，执行您所设置的过滤规则。

注意

- MAC 地址认证规则和站点适用于 AP 上的所有无线类型及 VAP。
- 要使用 MAC 认证功能，必须在『管理』→『无线基本设置』页面设置 MAC 认证类型为“本地”或“RADIUS”。

7.2 MAC 认证参数说明



以下是对页面各参数的说明：

标题项	说明
过滤	设置 MAC 地址过滤规则。 ➢ 仅允许列表中的站点：拒绝任何不在站点列表中的站点通过 AP 访问网络。 ➢ 阻止列表中的所有站点：仅拒绝出现在站点列表中的站点通过 AP 访问网络；其他站点允许访问网络。 **注意** 此处设置的过滤规则对于本地站点列表中的站点和外部 RADIUS 服务器上的站点列表中的站点均适用。

站点列表	设置要控制其通过 AP 访问网络的本地站点列表。 ➢ 要添加一个 MAC 地址到本地站点列表，请在下面的文本框中输入 48 位 MAC 地址，点击 添加 。 ➢ 要从站点列表中删除 MAC 地址，选择它的 48 位 MAC 地址，点击 删除 。 根据您在上字段设置的过滤规则，将允许或拒绝列表中的站点访问网络。 **注意** AP 最多允许添加 512 个 MAC 地址到站点列表。

如果您使用的 MAC 认证类型为 RADIUS，您必须在外部 RADIUS 服务器上配置站点列表。站点列表包含无线客户端 MAC 地址条目，列表格式描述见下表。

RADIUS 服务器属性	描述	值
用户名（1）	客户端站点的 MAC 地址	有效的客户端 MAC 地址
用户密码（2）	用于查找客户端 MAC 的全局固定密码	NOPASSWORD

7.3 MAC 认证配置举例

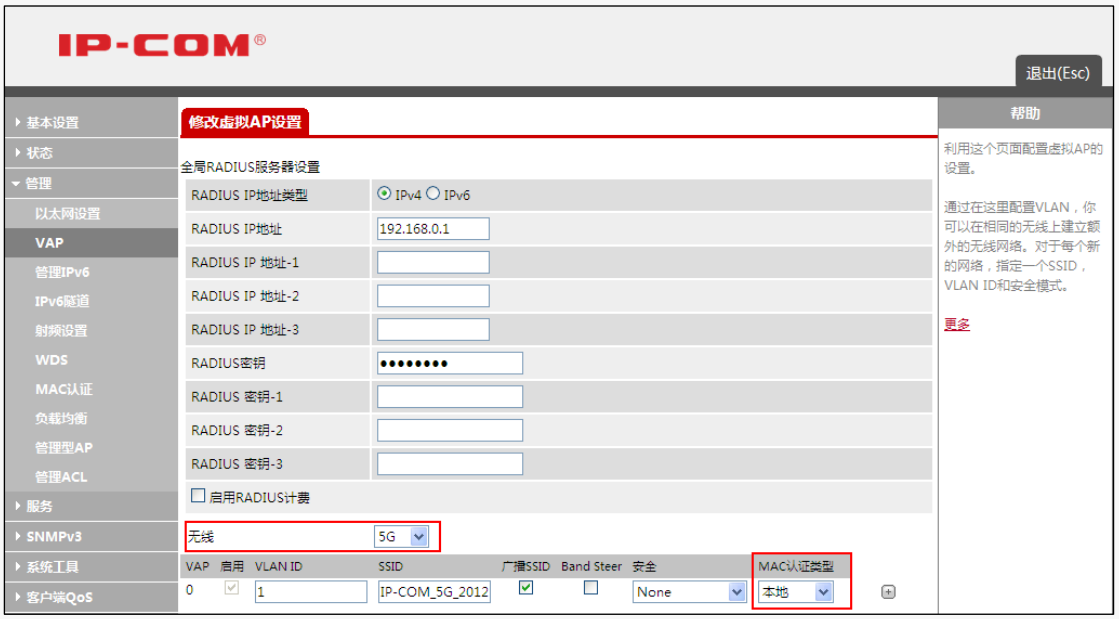
在『管理』→『VAP』页面设置的 MAC 地址认证类型分为以下三种：

- 禁用：不启用 MAC 认证功能。
- 本地：直接在 AP 上完成对用户的认证。无线用户接入网络时，根据 AP 上的本地站点列表和 MAC 地址过滤策略判断是否允许其接入 AP 的无线网络。
- RADIUS：AP 作为 RADIUS 客户端，与 RADIUS 服务器配合完成 MAC 地址认证操作。无线用户接入时，如果 AP 发现当前接入的客户端为未知客户端，AP 就将该认证请求转发到 RADIUS 服务器，由 RADIUS 服务器完成对该用户的认证，并下发相应的授权信息。

本地 MAC 认证组网拓扑图：

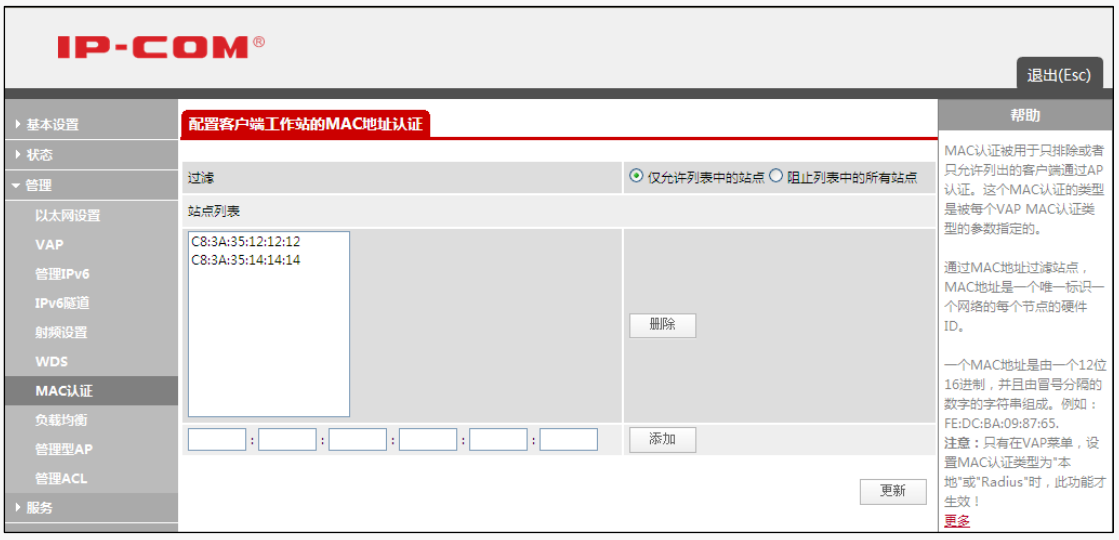
本地 MAC 认证配置步骤：

步骤 1：进入『管理』→『VAP』页面，选择无线类型，如“5G”，之后，将您想要进行 MAC 地址认证的 VAP 的 MAC 认证类型设置为“本地”，最后，点击 更新 保存配置。



步骤 2：进入『管理』→『MAC 认证』页面，选择过滤模式。

以“仅允许站点中的列表”为例，在输入框中输入 MAC 地址，比如：C8:3A:35:12:12:12，点击 添加 。再输入 C8:3A:35:14:14:14，点击 添加 。最后，点击 更新 保存配置。



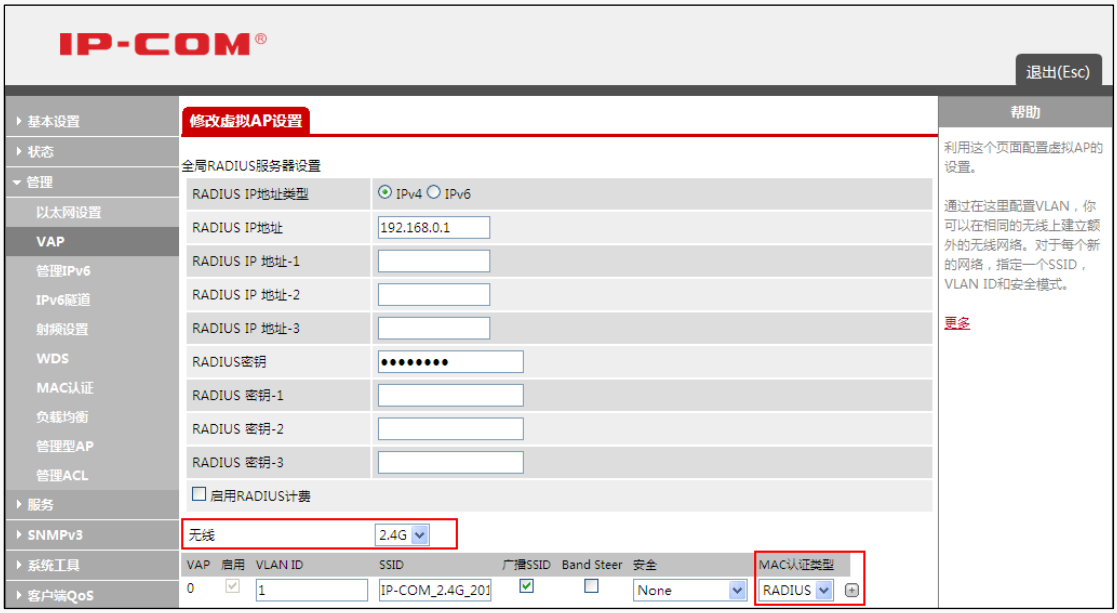
测试结果：

在组网拓扑图中可验证，MAC 地址为“C8:3A:35:12:12:12”的无线客户端可连接上 AP 访问网络，而 MAC 地址为“C8:3A:35:1F:1F:1F”的用户不能连接上 AP。

通过 RADIUS 服务器进行 MAC 地址认证，拓扑图如下：

配置步骤：

步骤 1：进入『管理』→『VAP』页面，选择无线类型，如“2.4G”，之后，将您想要进行 MAC 地址认证的 VAP 的 MAC 认证类型设置为“RADIUS”。最后，点击 更新 保存配置。



步骤 2：在 Radius 服务器上，用户名、密码填写需要允许或禁止接入 AP 的 PC 的 MAC 地址。

提示

采用 RADIUS 服务器进行 MAC 地址认证时，可以通过在各无线服务下分别指定各自的 domain 域，将不同 SSID 的 MAC 地址认证用户信息发送到不同的远端 RADIUS 服务器。

8 负载均衡

本节设置负载均衡。点击『管理』→『负载均衡』进入页面。

8.1 负载均衡概述

负载均衡，通过设置 AP 的网络利用率阈值控制客户端与 AP 关联、解除关联，使您可以确保无线网络上的所有 AP 平衡共享，不会出现单个 AP 过载的现象，进而保持无线网络的速度和性能。

提示

负载均衡设置适用于所有的无线（5G 或 2.4G）。

8.2 负载均衡参数说明

以下是对页面各参数的说明：

标题项	说明
负载均衡	启用或禁用负载均衡功能。默认为禁用。
无线关联下带宽使用	当 AP 停止接受新的客户端关联之前，允许的无线网络带宽利用率百分比。 默认值是 0，表示允许所有新关联而不管利用率如何。

注意

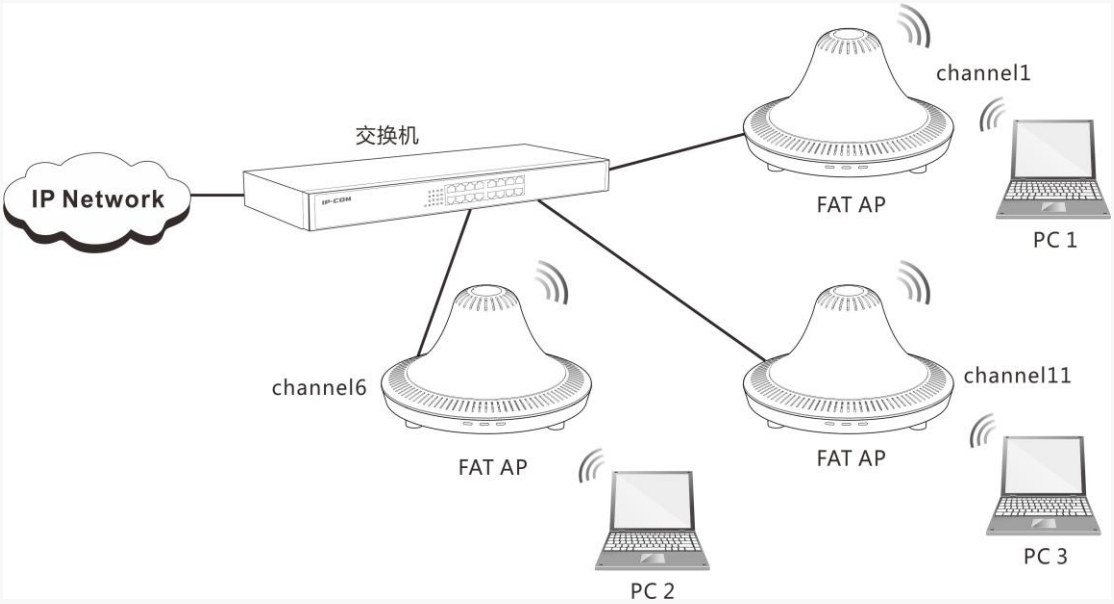
更改设置可能会导致 AP 终止运行并重新启动系统，无线客户端将暂时失去连接，我们建议您在 WLAN 流量低时更改 AP 的设置。

8.3 负载均衡典型配置举例

组网需求：某酒店为了满足多媒体应用的高带宽要求，需要部署多个无线 AP，让 Wi-Fi 覆盖酒店每个角落。

具体要求：

- 所有 AP 提供 SSID 为 Free 的明文方式的无线接入服务。
- 为避免某个 AP 流量过大，影响用户正常使用，甚至造成该 AP 负载过大死机而其它 AP 空闲，需要将所有 AP 配置负载均衡，无线关联下带宽使用超过 80%后不再接受关联。
- 为避免干扰，所有 AP 规划为蜂窝式信道，错开为 1、6、11。
- 为让 AP 能最大性能的提供服务，将发射功率设置为最高 100%。



配置 AP：

步骤 1：将所有 AP 的 IP 地址配置为不同。进入『管理』→『以太网设置』页面配置 AP 的 IP 地址。

步骤 2：配置无线服务。进入『管理』→『VAP』页面，设置 SSID 为 Free。

步骤 3：手动指定信道。进入『管理』→『射频设置』页面，在信道下拉框中选择 AP 需要使用的信道 1、6 或 11。

步骤 4：配置负载均衡。进入『管理』→『负载均衡』页面，选择“启用”负载均衡，在“无线关联下带宽使用”输入框中输入 80。

9 管理型 AP

本节配置 AP 的工作模式（独立模式/管理模式、WDS 模式）及其相关参数。点击『管理』→『管理型 AP』进入页面。

9.1 管理型 AP 概述

本 AP 可以工作在两种模式下：独立模式（胖 AP）或管理模式（瘦 AP）。

- 独立模式：AP 作为网络中的一个单独的 AP，您可以使用 Web 网管、Telnet，SSH 或 SNMP 对它进行管理。
- 管理模式：AP 作为 FASTPATH 统一无线系统的一部分，您可以使用 FASTPATH 统一无线交换机对它进行管理。此时，Web 网管，Telnet，SSH，SNMP 服务都被禁用。

在『管理』→『管理型 AP』页面，您最多可以配置 4 个可用于管理 AP 的 FASTPATH 统一无线交换机的 IP 地址。交换机和 AP 必须发现彼此，才能对 AP 进行管理。

注意

默认情况下，AP 工作在管理模式。

9.2 管理型 AP 参数说明

以下是对页面各参数的说明：

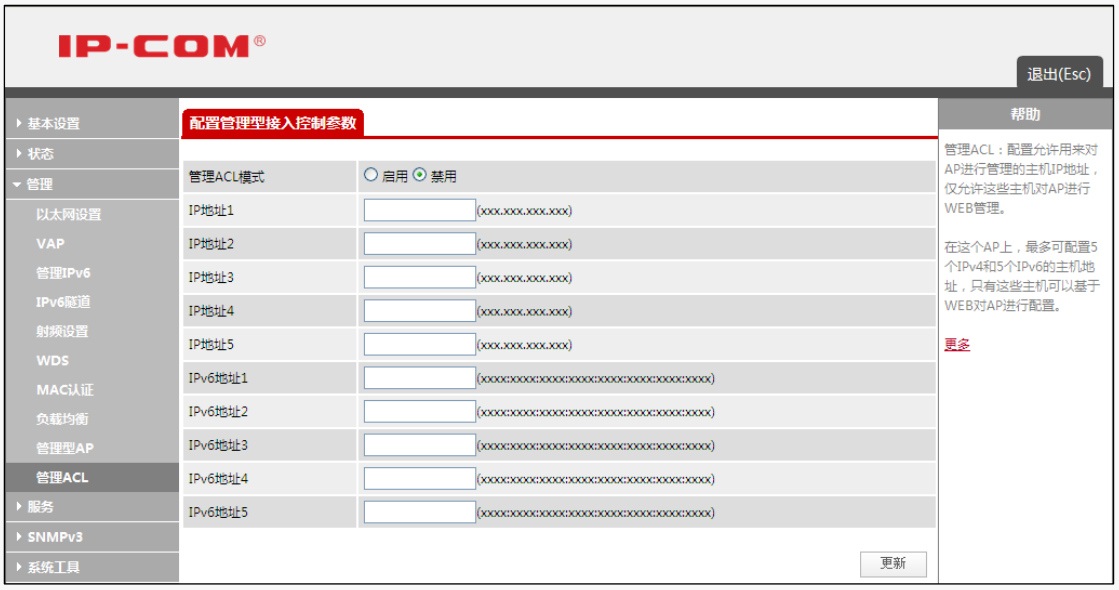
标题项	说明
管理型 AP 的管理模式	启用/禁用 AP 和无线交换机互相发现。 ➢ 启用：允许 AP 和交换机互相发现。如果 AP 成功与无线交换机进行认证，AP 将工作在管理模式。 ➢ 禁用：不允许 AP 和交换机互相发现，此时 AP 相当于工作在独立模式。
交换机的 IP 地址	启用“管理型 AP 的管理模式”后，最多可以配置 4 个用于管理 AP 的 FASTPATH 统一无线交换机的 IPv4 地址。 配置完成重启 AP 后，则被添加 IP 地址的 FASTPATH 统一无线交换机就能发现这个 AP，并允许对它进行相应的操作，如下发配置。

	注意 AP 首先尝试连接交换机 IP 地址 1。
基于 IP 端口	无线功能所使用的起始 IP 端口号。 10 个连续的端口号范围，只有范围中的第一个数字可以配置。默认值是 57775（到 57784）。
通行语句	8-63 个字符的认证密码，用于交换机对 AP 进行认证。 **注意** 交换机和 AP 上配置的认证密码必须相同。
WDS 管理模式	指定在 WDS 组中，AP 是充当根 AP 还是卫星 AP。 ➢ 根 AP：指连接到 FASTPATH 统一无线交换机的 AP。 ➢ 卫星 AP：指通过 WDS 连接到根 AP 的 AP，实际没有直接与交换机进行通信。
WDS 管理以太网端口	当 AP 成为了 WDS 组的一部分时，用于指定卫星 AP 上的以太网端口（AP 上的 LAN 口）是启用还是禁用。 **提示** 仅当有一个有线工作组连接到 AP 时，您才应该启用以太网接口。
WDS 组密码	用于卫星 AP 与根 AP 建立 WDS 连接时进行 WPA2 Personal 认证的密码。

10 管理 ACL

管理 ACL（访问控制列表），用来设置用户对 AP 的 Web 管理权限。启用管理 ACL 模式后，只有在此添加 IP 地址的主机有权限对 AP 进行 Web 管理,其他未授权的主机不能访问 AP 的 Web 网管页面。

点击『管理』→『管理 ACL』进入设置页面。



以下是对页面各参数的说明：

标题项	说明
IP 地址	使用点分十进制格式的 IPv4 地址，如：192.168.10.10
IPv6 地址	使用标准的 IPv6 地址，如：2001:0db8:1234::abcd

服务

本节设置 AP 的管理方式、参数，QoS 和时间管理，包括以下 6 部分内容：

Web 服务：设置 AP 的 Web 网管参数。

SNMP：设置 AP 的 SNMP 代理参数及 SNMP Trap 相关信息。

SSH：设置是否允许用户使用 SSH 协议对 AP 进行管理。

远程登录：设置是否允许用户远程登录（Telnet）到 AP 进行管理。

QoS：设置 AP 的 QoS 管理参数。

时间设置（NTP）：设置 AP 的系统时间。

1 Web 服务

设置 AP 的 Web 网管参数。点击『服务』→『Web 服务』进入页面。

提示

Web 网管登录的用户名为 admin，密码为您在『基本设置』页面设置的密码，默认为 admin。

以下是对页面各参数的说明：

标题项	说明
HTTPS 服务器状态	启用/禁用通过安全的 HTTP 服务器（HTTPS）访问 AP。
HTTP 服务器状态	启用/禁用通过 HTTP 服务器访问 AP。 **提示** 本设置与 HTTPS 服务器状态设置是互不相干的。
HTTP 端口	指定通过 HTTP 访问 AP 时所使用的端口号。 默认 HTTP 端口为 80，取值范围<1025-65535>。
HTTPS 端口	指定通过 HTTPS 访问 AP 时所使用的端口号。

	默认 HTTPS 端口为 443，取值范围<1025-65535>。
最大会话数	当用户登录到 AP 的 Web 网管时，便创建了一个会话。会话将被保持，直到用户注销或该会话超时。 输入可以同时存在的 Web 会话数，包括 HTTP 和 HTTPS。取值范围<1-10>。如果达到最大会话数，下一个试图登录到 AP Web 网管的用户将收到关于会话限制的错误消息。
会话超时（分钟）	设置用户登录到 Web 网管的闲置超时时间。单位：分钟，取值范围：<1-1440>。 如果在超时时间内，用户未在 Web 页面上进行任何操作，系统将会强制该用户下线。

以下是对页面参数的说明：

标题项	说明
生成 HTTP SSL 证书	点击右边对应的 保存，可生成一个新的 SSL 证书。
HTTP SSL 证书文件状态	显示当前 SSL 证书的有效期及发布者。
获取当前的 HTTP SSL 证书	采用 HTTP 或 TFTP 方式将当前的 SSL 证书下载至本地计算机。 HTTP：点击 下载，证书将会被自动下载至本地计算机。

	TFTP：需设置 SSL 证书文件名及本地 TFTP 服务器的 IP，同时确保本地计算机已开启 TFTP 服务器并已做好相应配置。
从一台电脑或者 TFTP 服务器上传 HTTP SSL 证书	采用 HTTP 或 TFTP 服务器方式上传一个 HTTP SSL 证书。 HTTP：点击 浏览 ，选择本地计算机上保存的 SSL 证书后，点击 确定 ，将会自动上传。 TFTP：需输入 SSL 证书文件名及本地 TFTP 服务器 IP，同时确保本地计算机已开启 TFTP 服务器并已做好相应配置。

2 SNMP

本 AP 带有 SNMP Agent 功能，您可以使用 NMS 对 AP 进行统一管理（概述见 1 SNMP 概述）。点击『服务』→『SNMP』进入页面，设置 SNMP Agent 相关参数和 Trap 操作功能。

2.1 SNMP 参数说明

以下是对页面各参数的说明：

标题项	说明
SNMP	指定 AP 上的 SNMP Agent（SNMP 代理）的状态：启用/禁用。 **注意** SNMP 是全局 SNMP 参数，适用于 SNMPv1，SNMPv2c 和 SNMPv3。禁用 SNMP 时，所有 SNMP 应用将不能生效。
只读团体名称（允许 SNMP get 操作）	输入只读团体名称，可以是任何包含 1~256 个字符的字母，数字字符串。 团体名称有着相当于密码的功能，如果发送方知道该密码则该请求通过认证。它作为一个简单的认证机制，来限制网络上可以向 SNMP 代理请求数据的设备。

端口号的 SNMP 代理监听	输入您要 SNMP 代理侦听请求的端口号。取值范围<1-65535>。 默认情况下，SNMP 代理只监听来自端口 161 的请求。 **注意** SNMP 代理监听端口是全局 SNMP 参数，适用于 SNMPv1，SNMPv2c 和 SNMPv3。
允许 SNMP 设置请求	选择是否允许 SNMP 在 AP 上进行设置的请求。 启用 SNMP 设置请求意味着网络上的设备可以通过 AP 上的 SNMP 代理对 AP 系统 MIB 库进行配置更改。
读-写团体名称 （允许 SNMP set 操作）	如果您已经启用了 SNMP 设置请求，您可以设置读-写团体名称。 团体名称与密码类似，只有来自以该团体名标识自己的主机的请求会被 AP 接受。 团体名称可以是任何字母，数字格式。有效范围是 1-256 个字符。
限制仅对指定主机或子网的 SNMP 请求来源	启用/禁用限制允许的 SNMP 请求的来源： ➢ 启用：限制允许的 SNMP 请求来源。 ➢ 禁用：允许任何来源提交 SNMP 请求。
网络管理系统的主机名称，地址，或子网	指定可对 AP 执行 get 和 set 请求的 IPv4 计算机的地址信息。 格式：地址/掩码、地址/掩码_长度。其中，地址为 IP 地址，掩码_长度为掩码位的数量。
网络管理系统的 IPv6 主机名称，地址或子网	指定可对 AP 执行 get 和 set 请求的 IPv6 计算机的地址信息。

以下是对页面各参数的说明：

标题项	说明
trap 团体名称	输入 trap 团体名称，可以是由任何 1-256 个字母，数字组成的字符串，不允许特殊字符。 从 AP 发送的 trap 消息将会以此处提供的字符串作为团体名称。
主机名或 IP 地址	输入接收 SNMP trap 消息的计算机的主机名或 IP 地址，最多可以添加 3 个主机名或 IP 地址。 由于 SNMP trap 是由 SNMP 代理随机发送的，因此指定 SNMP trap 具体应该被发送到哪很重要。 主机名有效字符个数为<1-256>。例如：snmptraps.foo.com.

2.2 SNMP 部分参数配置举例

开启 SNMP Agent 步骤：选择启用 SNMP 后，点击 更新 ，完成设置。

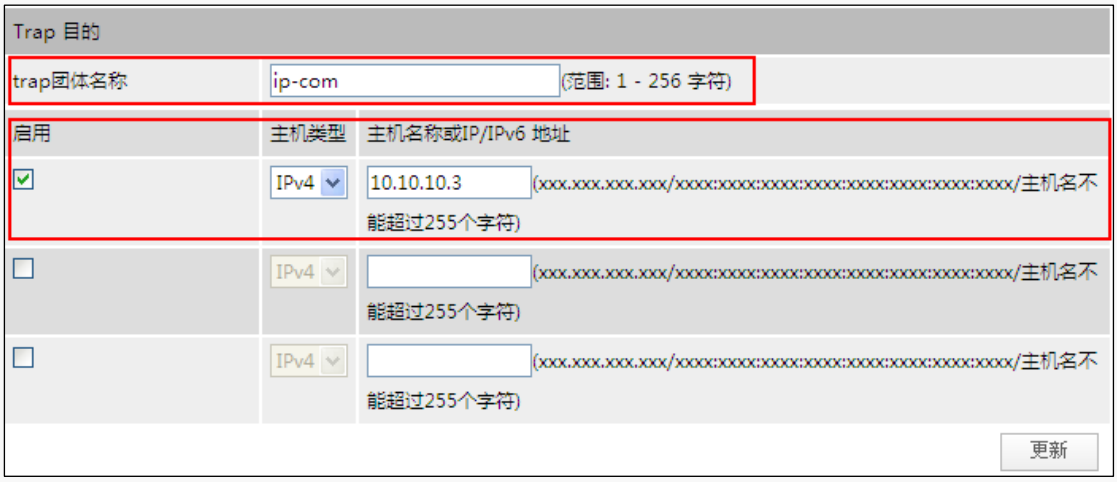
创建 SNMP 团体步骤：设置只读团体名称，允许 SNMP 设置请求，读-写团体名称（假设分别为 public，private），之后，点击 更新 保存设置。

配置 SNMP trap 功能步骤：

步骤 1：设置 trap 团体名称（假设为 ip-com）。

步骤 2：勾选启用，选择接收 trap 消息的主机的 IP 地址类型，接收 trap 消息的主机名称或 IP/IPv6 地址。（假设主机类型为 IPv4，IP 地址为 10.10.10.3）

步骤 3：点击 更新，保存设置。



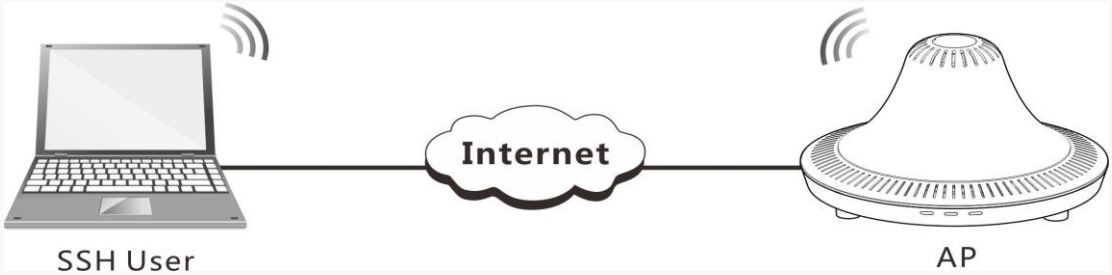
3 SSH

SSH 是 Secure Shell（安全外壳）的简称。Secure Shell 是一个程序，这个程序可以通过网络登录到另一台计算机，在远程机器上执行命令，将文件从一台机器移动到另一台，它在不安全的信道上提供了强大的认证和安全通信。

您可以启用或禁用 SSH 状态。点击『服务』→『SSH』进入 AP 的 SSH 服务设置页面。

SSH 配置举例

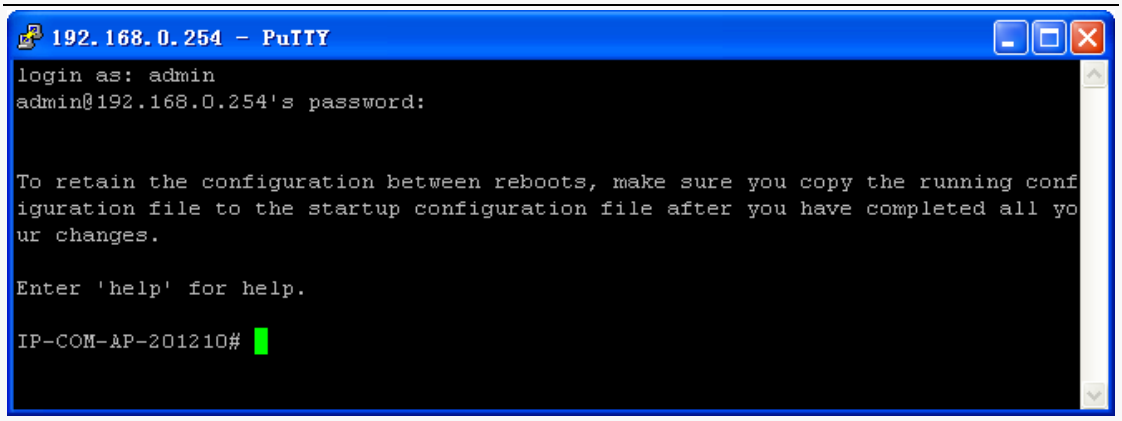
组网拓扑图如下：用户可以连通到 AP。



配置情况：启用 SSH 状态，客户端使用 putty 软件登录进 AP 进行配置。

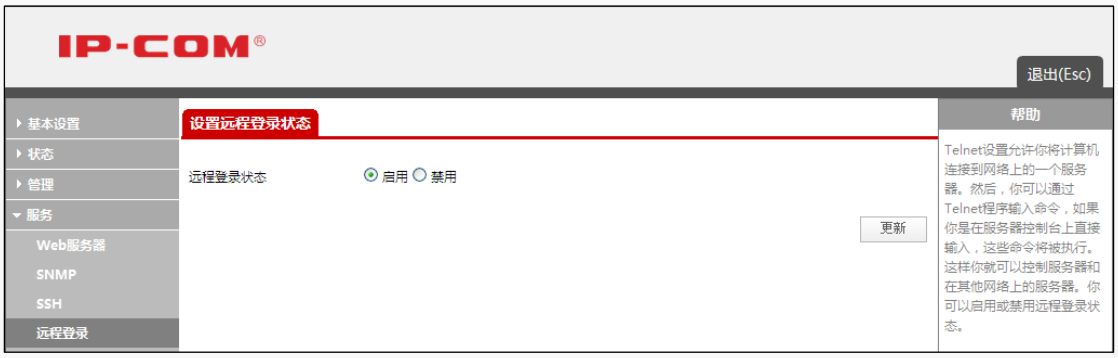
提示

SSH 登录的用户名为 admin，密码为您在『基本设置』页面设置的密码，默认为 admin。



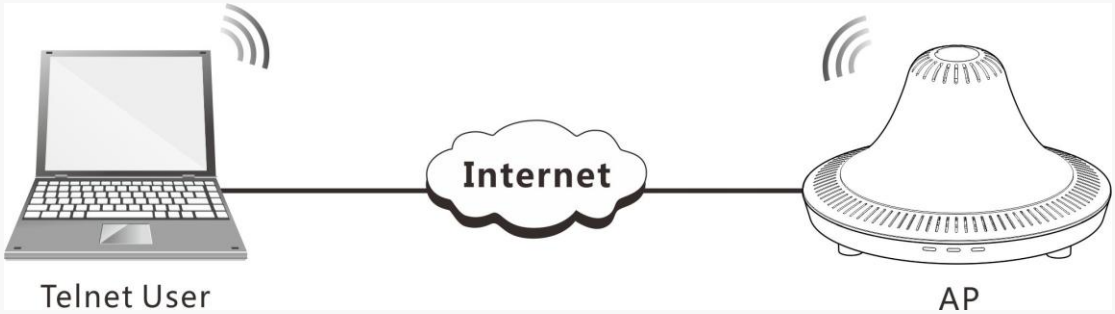
4 远程登录

远程登录允许您使用 telnet 登录到 AP 进行配置。您可以启用或禁用远程登录状态，点击『服务』→『远程登录』进入设置页面。



远程登录配置举例

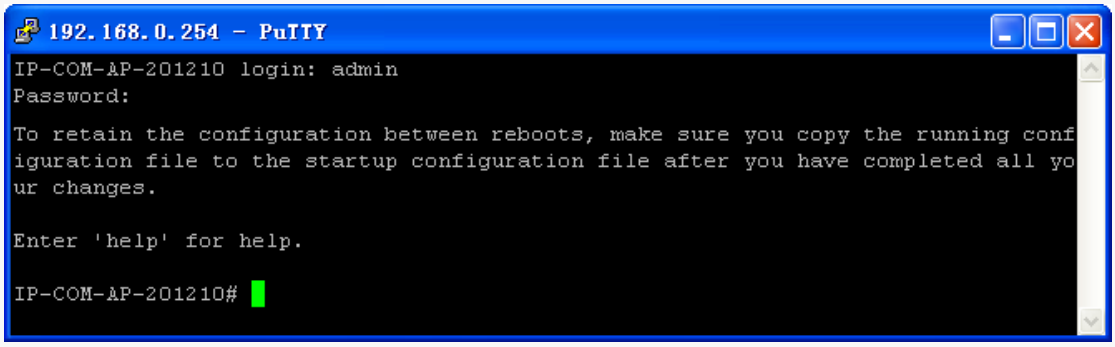
组网拓扑图如下：用户可以连通到 AP。



配置情况：启用远程登录状态，客户端使用 putty 软件登录进 AP 进行配置。

提示

Telnet 登录的用户名为 admin，密码为您在『基本设置』页面设置的密码，默认为 admin。



5 QoS

本节设置 QoS（Quality of Service，服务质量）参数。点击『服务』→『QoS』进入页面。

5.1 QoS 概述

QoS 允许您为不同类型的无线流量（如 VoIP，音频，视频和流媒体以及传统的 IP 数据）指定不同的队列参数，以增加无线吞吐量，提高无线性能。

AP 的 QoS 设置，包括对不同类型的无线流量的现有队列的参数设置，并有效地指定用于传输的最小和最大等待时间(通过竞争窗口)。这里描述的设置仅适用于 AP 上的数据传输行为，不适用于客户端工作站。

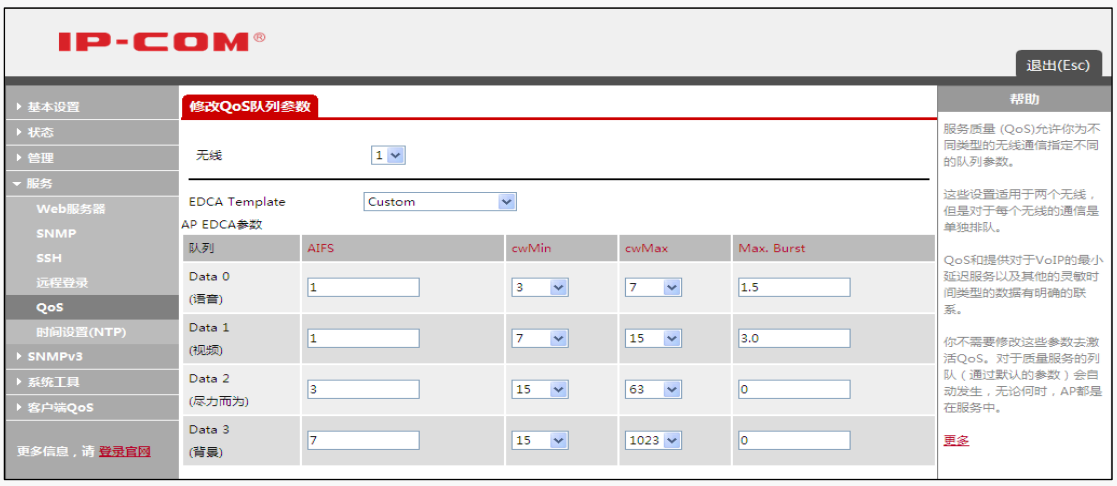
AP EDCA（Enhanced Distributed Channel Access）参数影响从 AP 到客户端站点的流量，站点 EDCA 参数影响从客户端站点到 AP 的流量。

AP 和站点 EDCA 参数的缺省值均采用 Wi-Fi 联盟在 WMM 规范中建议的值。一般情况下，采用缺省设置即可。

注意

QoS 设置适用于两个无线模式，但每一个无线的流量独立进行排队。

5.2 QoS 参数说明



以下是对页面各参数的说明：

标题项	说明
无线	选择查看或配置 QoS 的无线类型：1（5GHz）或 2（2.4GHz）。
EDCA Template	AP 已经定义了三种 EDCA 参数模板，您可以根据需要选择： ➢ Default：默认模式，上下行数据优先级没有进行特定的配置。 ➢ Optimized for Voice：语音优先模式，经过 AP 的上下行数据优先级顺序是：语音、视频、传统的 IP 数据、FTP 数据传输等。 ➢ Custom（自定义设置）：由您自定义配置各项参数来决定经过 AP 的上下行数据优先级。
AP EDCA 参数	
队列	为从 AP 发送到站点的不同类型数据定义队列： ➢ Data0（语音）：高优先级队列，最小延迟。对时间敏感的数据，如 VoIP 和流媒体会被自动发送到该队列。 ➢ Data1（视频）：高优先级队列，最小延迟。对时间敏感的视频数据将被自动发送到该队列。 ➢ Data2（尽力而为）：中等优先级队列，中等吞吐量和延迟。最传统的 IP 数据被发送到该队列。 ➢ Data3（背景）：最低优先级队列，高吞吐量。需要最大吞吐量和对时间不敏感的数据发送到该队列（如 FTP 数据）。
AIFS（帧间间隔）	指定数据帧的等待时间。单位：slot，取值范围<1-255>。
cwMin（最小竞争窗口）	此参数是输入的算法，用于确定传输重试的初始随机退避等待时间（窗口）。 指定的最小竞争窗口值是范围上限（单位：毫秒），初始随机退避等待时间从该范围确定。 生成的第一个随机数是一个介于 0 和 cwMin 之间的数字。 如果第一随机退避等待时间在数据帧被发送之前终止，则重试计数器递增，且随机退避时间翻倍。翻倍将继续，直到随机退避时间达到 cwMax 定义的值。 有效 cwMin 值为 1，3，7，15，31，63，127，255，511，1024。cwMin 必须小于 cwMax。
cwMax（最大竞争窗口）	指定最大竞争窗口，其值是双倍随机退避值的上限（单位：毫

	秒）。此倍增将继续，直到该数据帧被发送，或达到最大竞争窗口大小。 一旦达到最大竞争窗口大小，重试将继续下去，直到达到允许的最大重试次数。 有效 cwMax 值为 1，3，7，15，31，63，127，255，511，1024。cwMax 必须大于 cwMin。
MaxBurst(最大突发长度)	指定无线网络上允许的突发数据包的最大突发长度。单位：毫秒，取值范围<0.0-999>。 数据包突发是传输多个无首部信息的帧，减少开销以获得更高的吞吐量和更好的性能。

以下是对一些页面参数的说明：

标题项	说明
Wi-Fi 多媒体（WMM）	启用 WMM 时（默认为启用）： ➢ 无线介质访问的 QoS 优先级和协调也随即启用； ➢ AP 上的 QoS 设置控制 AP 的上下行流量； 禁用 WMM 时： ➢ 停用从站点到 AP 的上行流量（站点 EDCA 参数）QoS 控制； ➢ 您仍然可以设置一些从 AP 到客户端工作站的下行流量参数（AP EDCA 参数）。
No Acknowledgement	选择 On，指定 AP 不承认使用 QoSNoAck 作为服务类型值的帧。
APSD	选择 On，启用自动省电（APSD）电源管理方法。如果 VoIP 电话通过 AP 访问网络，建议使用 APSD。
站点 EDCA 参数	
AIFS（帧间间隔）	指定数据帧的等待时间。单位：slot，取值范围<1-255>。

cwMin（最小竞争窗口）	此参数是输入的算法，用于确定传输重试的初始随机退避等待时间（窗口）。 指定的最小竞争窗口值是范围上限（单位：毫秒），初始随机退避等待时间从该范围确定。 生成的第一个随机数是一个介于 0 和 cwMin 之间的数字。 如果第一随机退避等待时间在数据帧被发送之前终止，则重试计数器递增，且随机退避时间翻倍。翻倍将继续，直到随机退避时间达到 cwMax 定义的值。
cwMax（最大竞争窗口）	指定最大竞争窗口，其值是随机退避值上限的两倍（单位：毫秒）。此倍增将继续，直到该数据帧被发送，或达到最大竞争窗口大小。 一旦达到最大竞争窗口大小，重试将继续下去，直到达到允许的最大重试次数。
TXOP 限制	TXOP 是 WME 客户端站点有权在无线介质上向统一接入点发起传输时的一个时间间隔。 TXOP 限制单位：毫秒，最大取值为 65535。

6 时间设置（NTP）

本节设置 AP 的系统时间。点击『服务』→『时间设置』进入页面。

6.1 时间设置（NTP）概述

网络时间协议（NTP）是用于在网络上同步计算机时钟时间的 Internet 标准协议。NTP 服务器发送 UTC 至客户端，客户端定期向服务器发送时间请求，使用返回的时间戳来调整其时钟。

6.2 时间设置（NTP）参数说明

以下是对页面各参数的说明：

标题项	说明
设置系统时间	设置系统时间后，AP 能在日志信息和会话信息中提供正确的时间。 ➢ 使用网络时间协议（NTP）：NTP 为 AP 提供了一种从网络上的服务器获取和维护时间的方法，用户可以设置网络上的 IPv4/IPv6 地址或者域名的 NTP 时间服务器。 ➢ 手动：用户自己手动设置系统日期、系统时间、时区。
时区	从下拉菜单中选择您当地的时区。默认时区为 China。
DST 调整	选择使系统为夏令时（DST）调整的时间，选择此字段时，将显示配置夏令时的字段。
DST 开始（24 小时）	配置系统时间中开始夏令时的日期和时间。
DST 结束（24 小时）	配置系统时间中结束夏令时的日期和时间。
DST 偏移（分钟）	选择抵消 DST 的分钟数。默认为 60 分钟。

6.3 时间设置（NTP）配置举例

手动设置步骤:手动设置当前时间：年、月、日、分，点击 更新 使配置生效。

使用网络时间协议（NTP）设置步骤：

步骤 1：选择“使用网络时间协议（NTP）”；

步骤 2：设置网络时间服务器 IP 地址或者名称，如 64.236.96.53 或 s2k.time.edu.cn；

步骤 3：点击 更新 使配置生效。

设置完成后，等待 1 分钟左右，可以看到系统时间（24HR）与当前时间一致。表明 IP 地址或者名称可以使用，且功能已经生效。

SNMPv3

本节详细介绍如何使用 SNMP 协议对 AP 进行统一管理。

1 SNMP 概述

SNMP（Simple Network Management Protocol，简单网络管理协议）是一种简单的、SNMP 管理进程和代理进程之间的请求-应答协议，可使用它实现对网络中来自不同厂家的网络设备的自动化管理。

SNMP 网络元素主要由三个关键元件组成：网络管理站（NMS，Network Management Station），被管理设备（managed device）和代理者（Agent）。SNMP 协议是 NMS 和 Agent 之间的通信协议。

NMS 和 Agent 上的 SNMP 版本配置必须相同，才能成功互访。目前，设备的 SNMP Agent 支持 SNMP v1、SNMP v2c 和 SNMP v3 三种版本。

- SNMP v1：采用团体名（Community Name）认证。团体名用来定义 SNMP NMS 和 SNMP Agent 的关系，起到了类似于密码的作用，用来限制 SNMP NMS 对 SNMP Agent 的访问。如果 SNMP 报文携带的团体名没有得到 AP 的认可，该报文将被丢弃。
- SNMP v2c：采用团体名认证。SNMP v2c 兼容 SNMP v1 还扩充了 SNMP v1 的功能：提供更多的操作类型（GetBulk 和 InformRequest）；支持更多的数据类型（Counter64 等）；提供更丰富的错误代码，能够更细致地区分错误。
- SNMP v3：提供了基于用户的安全模型（USM，User-Based Security Model）的认证机制。用户可以设置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为 SNMP NMS 对 SNMP Agent 之间的通信提供更高安全性。

2 SNMP 配置任务简介

本小节介绍各版本 SNMP 的配置任务及任务的配置顺序。

2.1 配置 SNMPv1 和 SNMPv2c

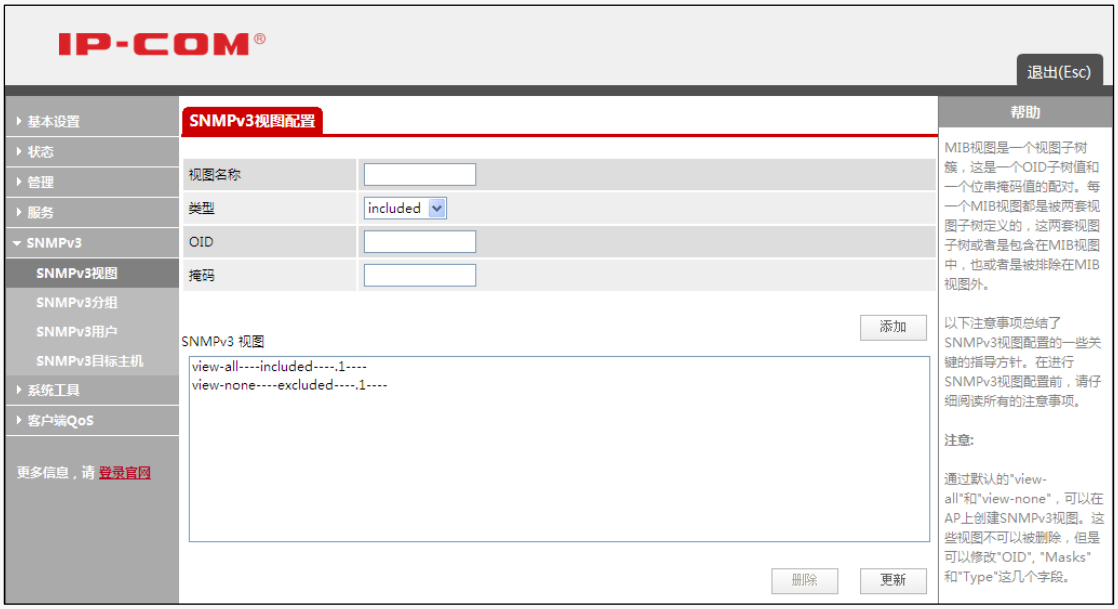
顺序	配置任务	说明	详细配置
1	启用 SNMP	必选	2.2 SNMP 部分参数配置举例
2	配置 MIB 视图	可选	3 SNMPv3 视图
3	创建 SNMP 团体	必选	2.2 SNMP 部分参数配置举例
4	配置 SNMP Trap	可选	2.2 SNMP 部分参数配置举例

2.2 配置 SNMPv3

顺序	配置任务	说明	详细配置
1	启用 SNMP	必选	2.2 SNMP 部分参数配置举例
2	配置 MIB 视图	可选	3 SNMPv3 视图
3	创建 SNMPv3 分组	必选	4 SNMPv3 分组
4	配置 SNMPv3 目标主机	可选	6 SNMPv3 目标主机

3 SNMPv3 视图

MIB 视图是一组视图子树或一个视图子树族，您可以创建 MIB 视图，控制 SNMPv3 用户可以访问的 OID 范围。点击『SNMPv3』→『SNMPv3 视图』进入页面。



配置 MIB 视图步骤：

步骤 1：配置视图名称，类型，OID。

步骤 2：点击 添加 ，添加好一条视图实例后，点击 更新 。

以下是对页面各参数的说明：

标题项	说明
视图名称	输入 MIB 视图名称。视图名称最多可以由 32 个数字和字母组成。
类型	指定要包括（included）或排除（excluded）的视图子树或视图子树族。
OID	输入视图子树要包括或排除的 OID 字符串。 例如：OID 字符串 1.3.6.1.2.1.1 指定了系统子树。

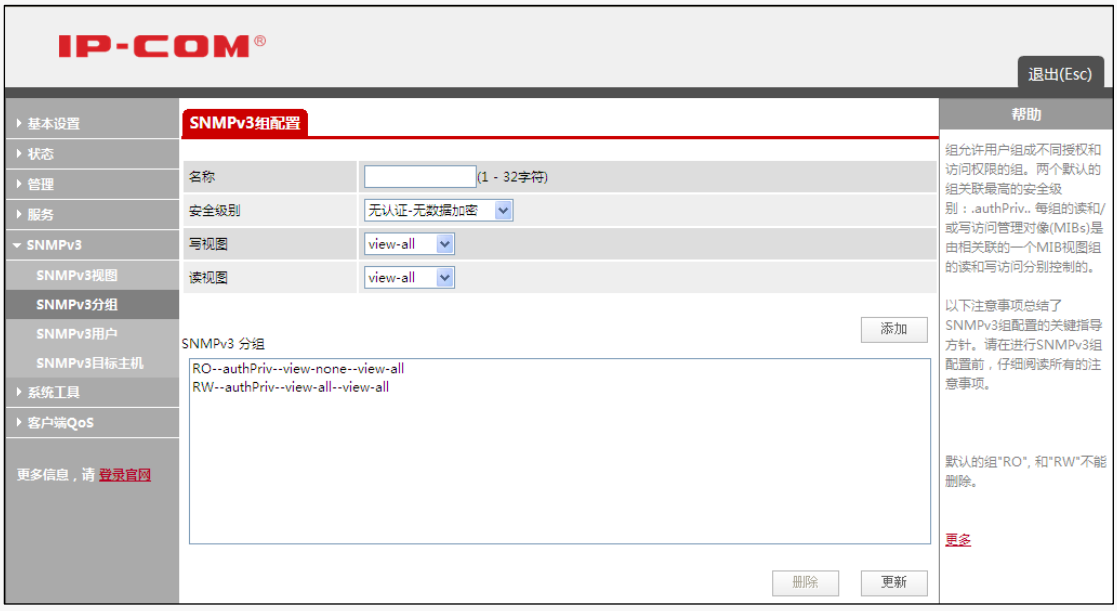
掩码	掩码格式为 xx.xx.xx（.）...或 XX:XX:XX(:)....。掩码长度为 16 个字节，每个字节由 2 个 16 进制字符组成。 例如：OID 掩码 FA.80 是 11111010.10000000。 视图子树族(family of view subtrees)以更有效的方式控制允许访问一个表中的某一行。
SNMPv3 视图	显示 AP 上的 MIB 视图。 要删除某个视图，选择该视图后，点击 删除 后，点击 更新 。

4 SNMPv3 分组

SNMPv3 分组，允许您将 SNMP 用户合并到不同授权和访问权限的组。默认情况下，AP 有 RO 和 RW 分组，这两个组中的用户均使用 MD5 密钥进行身份验证，DES 密钥进行数据加密，您必须定义 MD5 和 DES 密钥。RO 和 RW 分组的不同点如下：

- RO：只读组。该组的用户对默认的 MIB 视图只有只读访问权限；
- RW：读/写组。该组的用户对默认的 MIB 视图拥有读和写的访问权限；

点击『SNMPv3』→『SNMPV3 分组』进入设置页面。



配置 SNMPv3 分组步骤：

步骤 1：配置分组名称，安全级别，写视图，读视图。

步骤 2：点击 添加 加入一条组实例后，点击 更新 保存配置。

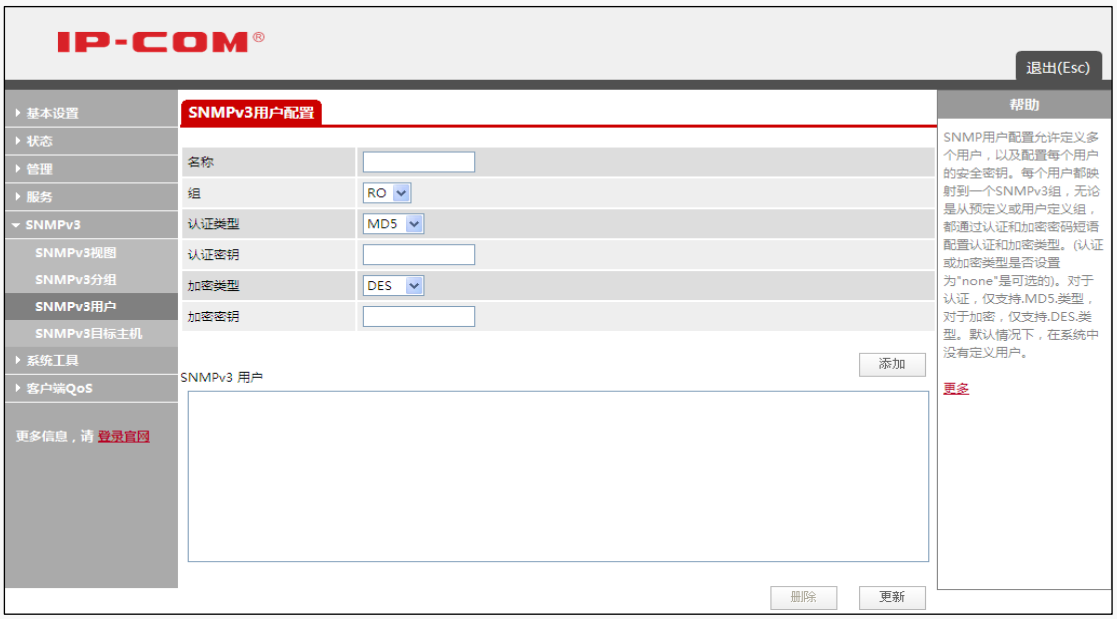
以下是对页面各参数的说明：

标题项	说明
名称	为该组指定一个用于识别的名称，默认组名为 RW 和 RO。组名最多可以由

	32 个数字和字母组成。
安全级别	为该组选择一个安全级别： ➢ 无认证-无数据加密：无安全性。 ➢ 身份认证-无数据加密：用户发送 SNMP 报文时，使用 MD5 密钥进行身份认证，不使用 DES 密钥进行数据加密。 ➢ 身份认证-数据加密：用户发送 SNMP 报文时，使用 MD5 密钥进行身份认证，并使用 DES 密钥进行数据加密。 **注意** 对于要求身份验证，加密或同时要求两者的组，您必须在『SNMPv3 用户』页面定义 MD5 和 DES 密钥。
写视图	为分组选择管理对象（MIB）写访问： ➢ write-all：该组可以创建，修改，删除 MIB。 ➢ write-none：该组不能创建，修改或删除 MIB。
读视图	为分组选择管理对象（MIB）读访问： ➢ view-all：该组允许查看和读取所有 MIB。 ➢ view-none：该组不能查看或读取 MIB。
SNMPv3 分组	显示默认的和您在 AP 上定义的组。

5 SNMPv3 用户

您可以定义多个用户，为每个用户关联所需的安全级别，并配置安全密钥。仅支持 MD5 认证和 DES 加密。点击『SNMPv3』→『SNMPv3 用户』进入设置页面。



创建 SNMPv3 用户步骤：

步骤 1：配置 SNMPv3 用户名称，所属分组，认证类型（密钥），加密类型（密钥）。

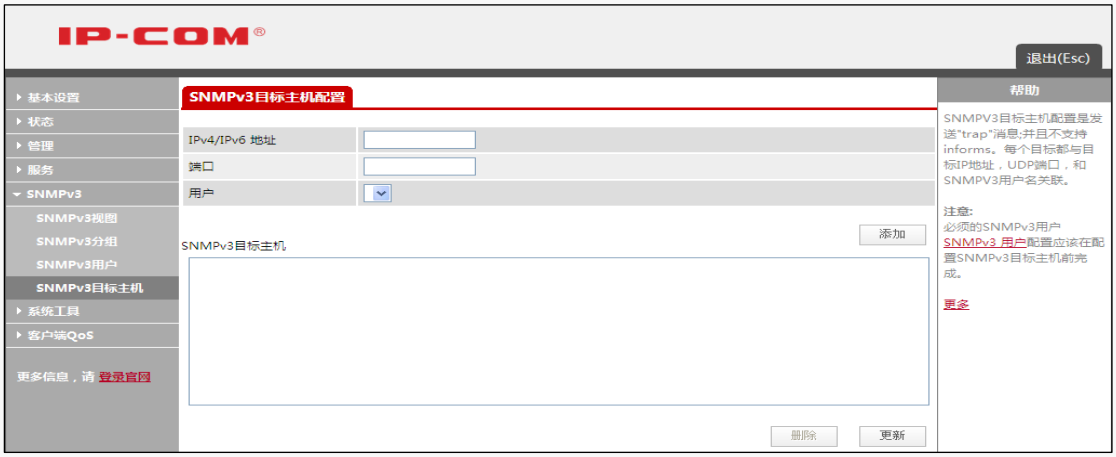
步骤 2：点击 添加 新增一条用户配置实例，点击 保存 。

以下是对页面各参数的说明：

标题项	说明
名称	输入用于识别该 SNMPv3 用户的用户名。最多可以由 32 个数字和字母组成。
组	将用户映射到分组。默认分组为 RW 和 RO，您还可以在『SNMPv3 分组』页面自定义分组。
认证类型	选择对来自该用户的 SNMP 请求执行的认证类型： ➢ MD5：对来自该用户的 SNMPv3 请求执行 MD5 认证。 ➢ None：对来自该用户的 SNMPv3 请求不执行认证。
认证密钥	认证类型为 MD5 时，输入一个密码启用 SNMP 代理对用户发送的请求进行认证。密码长度必须是 8～32 个字符。
加密类型	选择该用户的 SNMP 请求的数据加密类型： ➢ DES：该用户的 SNMPv3 请求进行 DES 加密。 ➢ None：该用户的 SNMPv3 请求不进行加密。
加密密钥	DES 加密时，输入加密 SNMP 请求的密钥。密码长度必须是 8～32 个字符。
SNMPv3 用户	显示您在 AP 上定义的用户。 要删除某个用户，选择该用户，点击 删除 后，点击 更新 。

6 SNMPv3 目标主机

配置 SNMPv3 目标主机，以允许 AP 的 SNMP 代理发送 SNMPv3 trap 消息。点击『SNMPv3』→『SNMP 目标主机』进入设置页面。



配置 SNMPv3 目标主机步骤：

步骤 1：IPv4/IPv6 地址，配置接收 SNMPv3 trap 消息的主机的 IPv4/IPv6 地址。

步骤 2：端口，配置发送 trap 消息的端口。

步骤 3：用户，选择您在『SNMPv3』→『SNMPv3 用户』页面定义的与目标相关联的用户。

步骤 4：点击 添加 ，添加一条实例后，点击 更新 。

以下是对页面各参数的说明：

标题项	说明
IPv4/IPv6 地址	输入接收 trap 消息的远程 SNMP 管理器的 IP 地址。
端口	输入用于发送 SNMP trap 消息的 UDP 端口。
用户	选择与目标相关联 SNMP 用户名称。
SNMPv3 目标	显示您配置的 SNMPv3 目标主机。 要删除一个目标主机，选择该目标主机，点击 删除 后，点击 更新 。

7 SNMP 典型配置举例

组网需求：如下图所示，NMS（IP 地址为 10.10.10.2/24）与 AP（IP 地址为 10.10.10.3/24）通过以太网相连。

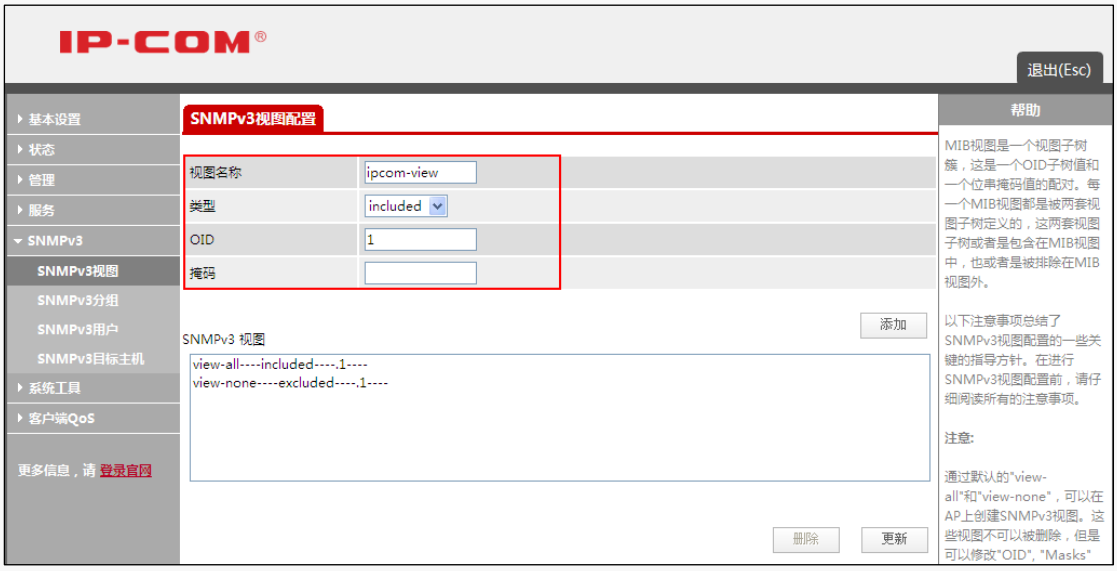
现要实现如下需求：

- NMS 通过 SNMPv3 对 AP 的接口状态进行监控管理。
- AP 对 SNMP 请求无身份认证和数据加密方面的要求。
- AP 在发生故障或者出错时，能够主动向 NMS 报告情况。

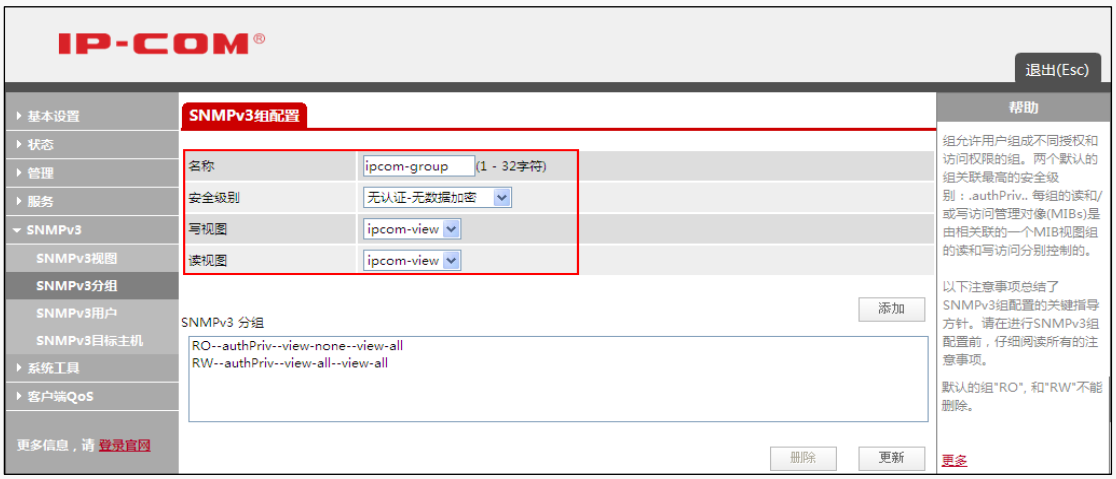
配置步骤：

步骤 1：开启 SNMP Agent。进入『服务』→『SNMP』页面，启用 SNMP 后，点击 更新 。

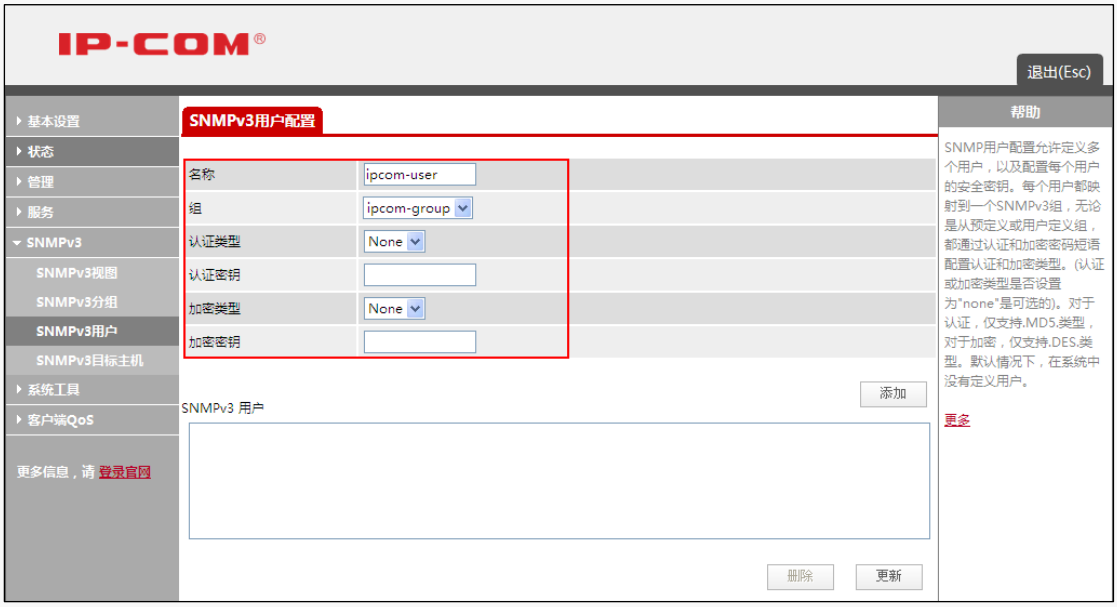
步骤 2：配置 SNMP 视图。进入『SNMPv3』→『SNMPv3 视图』页面，配置视图名称为 ipcom-view，类型为 included，OID 为 1，点击 添加 ，添加一条实例，点击 更新 。



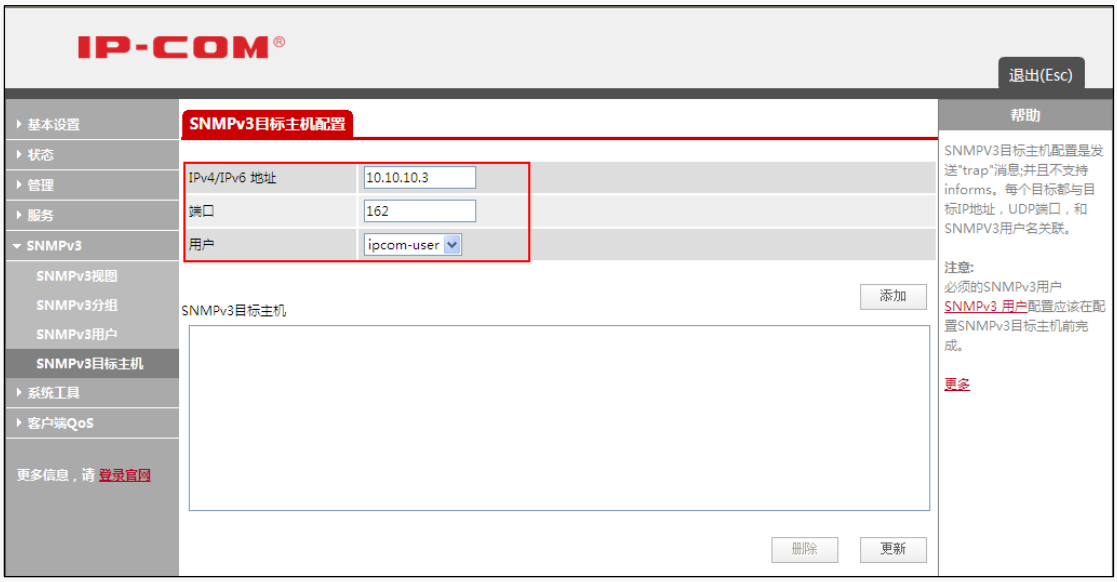
步骤 3：配置 SNMP 组。进入『SNMPv3』→『SNMPv3 分组』页面，输入组名称为 ipcom-group，选择写视图和读视图均为 ipcom-view，点击 添加 ，添加一条实例，点击 更新 。



步骤 4：配置 SNMP 用户。进入『SNMPv3』→『SNMPv3 用户』页面，输入用户名称为 ipcom-user，选择用户所在组为 ipcom-group，点击 添加 ，添加一条实例，点击 更新 。



步骤 5：开启 SNMP Agent 发送 SNMP Trap 消息功能。进入『SNMPv3』→『SNMP 目标主机』页面，输入 IPv4/IPv6 地址为 10.10.10.3，输入端口为 162，选择用户为 ipcom-user，点击 添加 后，点击 更新 保存配置。



系统工具

本节介绍如何维护 AP，包括以下 3 部分内容：

配置管理：管理 AP 配置文件，包括备份、还原 AP 配置、恢复出厂设置及重启 AP。

软件升级：介绍如何将 AP 软件升级。

数据包捕获：进行数据包捕获，设置数据包捕获参数。

1 配置管理

配置管理模块提供以下 4 种功能：

恢复出厂配置：将 AP 配置恢复至出厂状态。

配置备份：将设备当前的配置文件备份到用户的计算机上保存。

配置恢复：将保存到当前用户计算机上的配置文件上传到 AP。

重启 AP。

点击『系统工具』→『配置管理』进入页面。

1.1 恢复出厂设置

软件恢复法：点击恢复出厂设置后的 重置 ，之后按提示操作即可。

硬件恢复法：通电状态下，持续按住 AP 上的系统复位（RST）按钮 7 秒后放开，等待 AP 自动重启成功（Power 灯闪烁，2.4GHz 和 5GHz 灯亮起）即可。

1.2 配置备份

如果您对 AP 进行了大量重要的配置，建议将配置进行备份。本 AP 支持 HTTP 和 TFTP 两种方式将 AP 当前的配置文件备份至本地计算机。默认为 HTTP。

- HTTP：请点击 下载 ，之后按提示保存配置文件即可。
- TFTP：请为配置文件命名，并填写好 TFTP 服务器的 IP 地址后，再点击 下载 。

注意

选择 TFTP 时，请确认本地计算机上已开启 TFTP 服务器，且 TFTP 服务器参数配置正确。

1.3 配置恢复

配置恢复功能可将 AP 的配置还原到之前备份的配置。本 AP 支持 HTTP 和 TFTP 两种方式将配置文件上传至 AP。默认为 HTTP。

- HTTP：请点击 浏览 ，选择保存在本地计算机上的配置文件后，再点击 恢复 ，等待 AP 读取上传的配置文件并自动重启成功即可。
- TFTP：请填写配置文件的文件名以及 TFTP 服务器的 IP 地址后，再点击 恢复 ，等待 AP 读取上传的配置文件并自动重启成功即可。

注意

选择 TFTP 时，请确认本地计算机上已开启 TFTP 服务器，且 TFTP 服务器参数配置正确。

1.4 重启 AP

重启 AP 可使您对 AP 的进行的配置生效，某些时候，还能解决一些如死锁、登录不了 AP Web 网管的问题。

重启方法：点击本页的 重启 ，之后按页面提示操作即可。

注意

重启会导致所有连接到 AP 的通信暂时断开。重启成功后，AP 会自动跳转至 Web 网管的登录认证页面。

2 软件升级

您可以登录到 IP-COM 官网：www.ip-com.com.cn 下载 F190AP 更高版本的升级软件，进行软件升级，以获得更多增值功能以及更加稳定的性能。

点击『系统工具』→『软件升级』进入 F190AP 软件升级页面。

以下是对页面各参数的说明：

标题项	说明
主镜像	显示用于引导、启动 AP 的主系统文件版本。
次镜像	用于引导、启动 AP 的备用系统文件。如果主镜像加载失败，将自动启用次镜像来启动 AP。 您也可以点击 切换，手动切换系统的镜像文件。
上传方法	可选择 HTTP 或 TFTP 的方式将升级软件上传至 AP。默认为 HTTP。 ➢ HTTP 升级方式：点击 浏览，选择存放在本地计算机上的升级文件后，点击 软件升级，之后按页面提示操作即可。 ➢ TFTP 升级方式：请先填写好升级软件的文件名、TFTP 服务器的地址后，点击 软件升级，之后按页面提示操作即可。 **注意** 1. 选择 TFTP 时，请确认本地计算机上已开启 TFTP 服务器，且 TFTP 服务器参数配置正确。 2. 上传新的软件后，系统重新启动，新的软件将成为主镜像。如果升级失败，原来的软件仍然作为主镜像。 3. 软件升级过程需要等待一段时间，此时请不要在 Web 网管页面上进行任何操作，否则可能会导致软件升级中断。

3 数据包捕获

本 AP 可以对覆盖区内的无线报文及以太网报文进行侦听捕获，方便网络管理员将数据包下载至本地计算机，进行故障排查、优化分析。

点击『系统工具』→『数据包捕获』进入数据包捕获设置页面。

3.1 数据包捕获概述

本 AP 支持两种操作模式的数据包捕获：数据包文件捕获、远程数据包捕获。

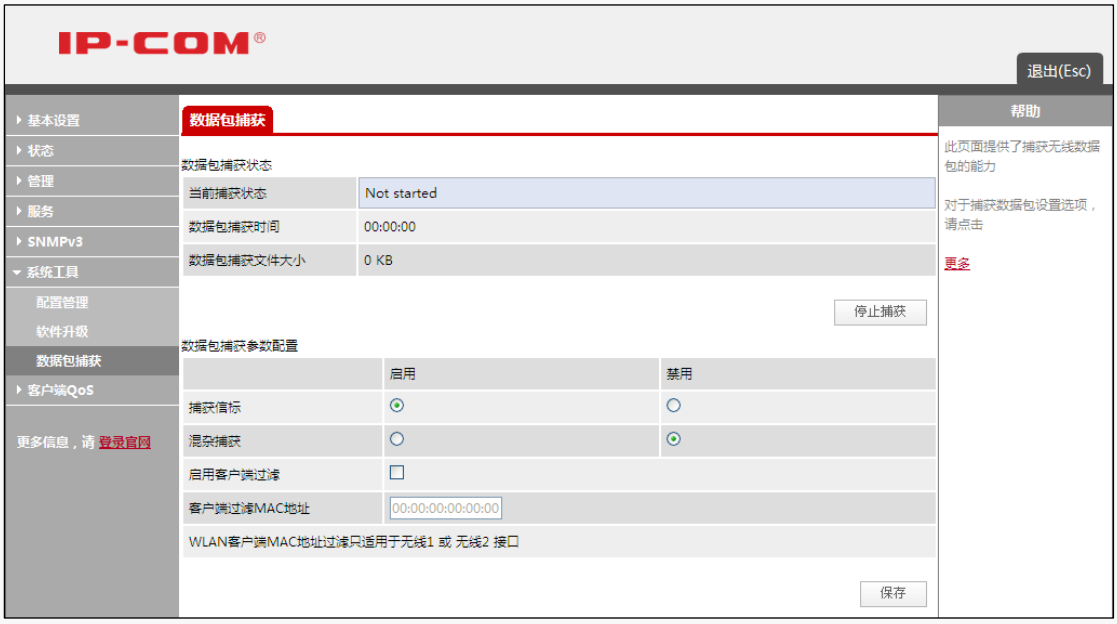
数据包文件捕获：捕获到的数据包保存在 AP 的 RAM 存储器中。捕获完成后，用户可通过 HTTP 或 TFTP 的方式下载 pcap 格式的数据包文件到本地计算机，并在本地计算机上使用 Wireshark、OmniPeek 等工具进行分析。

远程数据包捕获：将捕获的数据包实时重定向至正在运行 Wireshark 工具的远程计算机上。

本 AP 可以捕捉到以下类型的数据包：

- 无线接口接收和发送的 IEEE 802.11 数据包。
- 以太网接口接收和发送的 IEEE 802.3 数据包。
- 内部逻辑接口，如 VAPS 和 WDS 接口，传输的和接收到的 IEEE 802.3 数据包。

3.2 数据包捕获全局参数说明



以下是对数据包捕获的全局参数的说明：

标题项	说明
当前捕获状态	显示数据包当前的捕获动态，各动态及其解释如下： ➢ Not started：未开启数据包捕获。 ➢ File capture in progress：正在进行数据包文件捕获。 ➢ Remote capture in progress：正在进行远程捕获。 ➢ Stopped due to administrative action：管理员停止了捕获。 ➢ Stopped due to file size limit：因超过文件大小限制而停止捕获。 ➢ Stopped due to timeout：因超过时间限制而停止捕获。
数据包捕获时间	显示当时的（已经过去的）捕获时间。

数据包捕获文件大小	显示捕获到的数据包文件大小。
捕获信标	设置是否捕获 Beacon 帧。
混杂捕获	设置无线接口是否工作在混杂模式。 ➢ 禁用：只捕获含本地网卡地址的单播包、组播包以及广播包。 ➢ 启用：除捕获上述类型的数据包外，还捕获与本网卡地址不吻合的组播包。 **注意** 在混杂模式下，无线接收信道上的所有流量，包括不是发给该 AP 的。此时，AP 将继续服务关联的客户端，目的地址不是该 AP 的数据包不会被转发。一旦捕获完成，无线恢复到非混杂模式。
启用客户端过滤	是否仅捕获源地址或目的地址与设置的 MAC 地址相匹配的无线帧。 **注意** 本选项仅适用于无线接口捕获。
客户端过滤 MAC 地址	设置仅捕获源地址或目的地址为此 MAC 地址的无线帧。

3.2 数据包文件捕获

数据包捕获设置步骤：

步骤 1：配置捕获接口，捕获时间及最大捕获文件大小，点击 保存 。

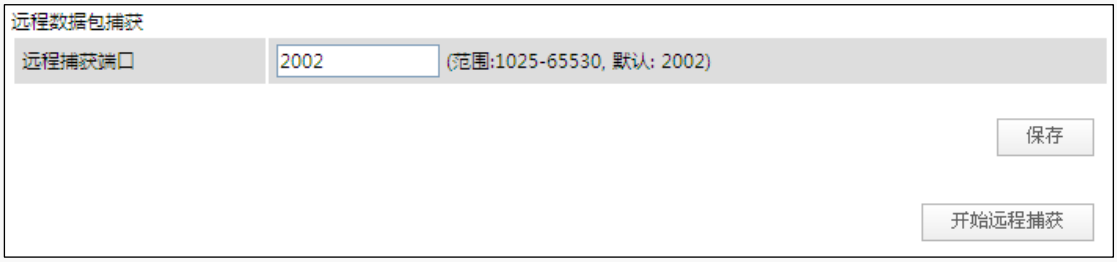
步骤 2：点击 开始文件捕获 。

以下是对各参数的说明：

标题项	说明
捕获接口	设置捕获接口，包括的捕获接口及其说明如下： ➢ Brtunk：vlan 桥接口。设置为此接口时，可捕获以太网、无线接口上的所有数据包。 ➢ eth0：以太网接口。设置为此接口时，可捕获以太网数据包。 ➢ Radio1：无线虚拟接口。设置为此接口时，将捕获包括主 SSID、

	次 SSID 接口上的无线数据包。 ➢ Wlan0：无线主 SSID 接口。设置为此接口时，可以捕获目的地址或源地址为主 SSID MAC 的无线数据包，且自动过滤掉 Beacon 包及其它广播包。 ➢ Wlan0vap1-Wlan0vap15：次 SSID 接口。只有启用次 SSID 时，此类接口才开启。 ➢ Wlan0wds0-Wlan0wds3：wds 桥接接口。只有启用 wds 桥接时，此类接口才开启。
捕获时间	指定捕获持续时间。
最大捕获文件的大小	指定允许捕获的数据包文件最大值。

3.3 远程数据包捕获

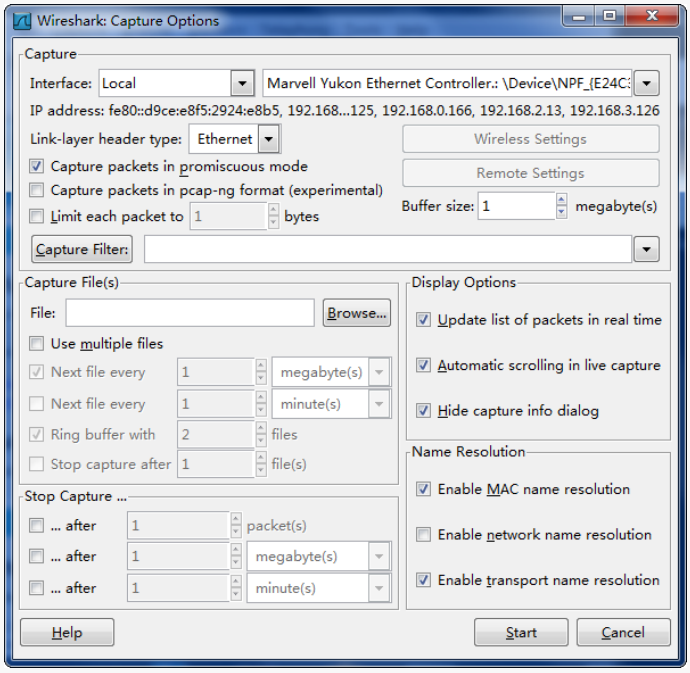


远程数据包捕获参考步骤：

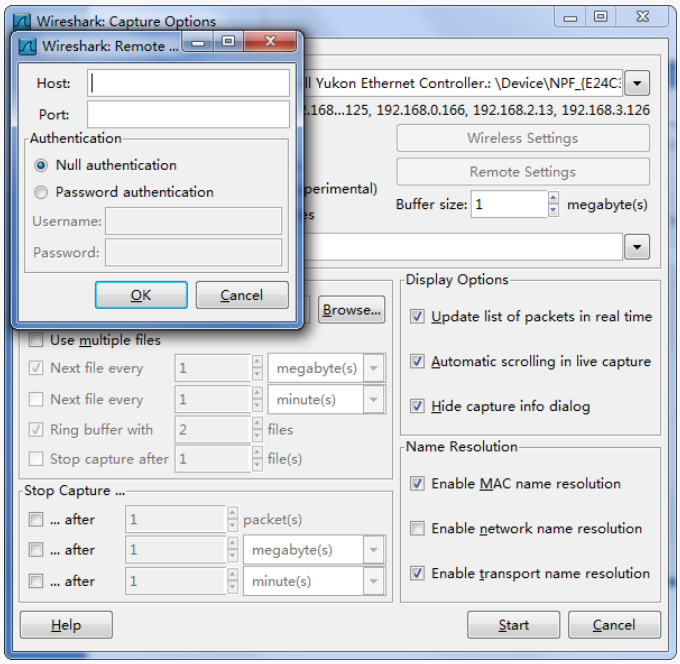
步骤 1：设置“远程捕获端口”（建议选择默认端口），点击 保存 ，点击 开始远程捕获 。

步骤 2：开启连接到 AP 的远程计算机上的 Wireshark 应用程序。

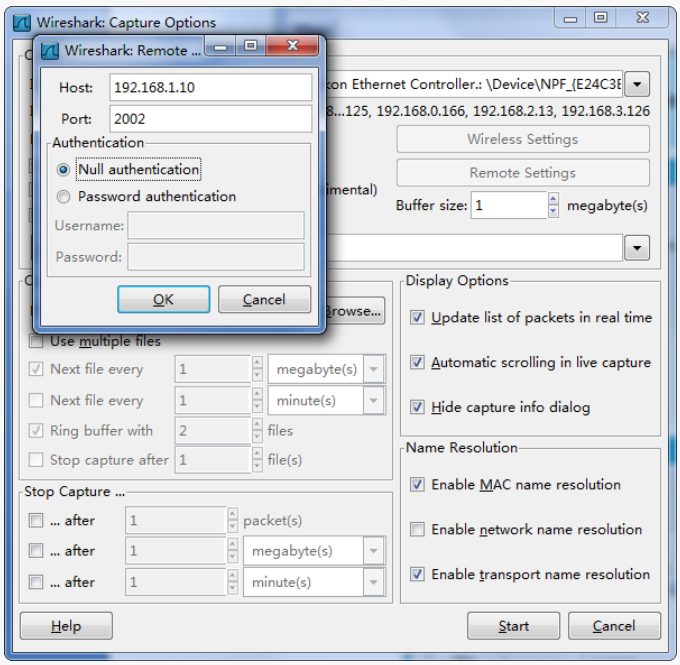
1 点击 Wireshark 工具导航栏上的“Capture”，选择“Options”，弹出如下图所示对话框；



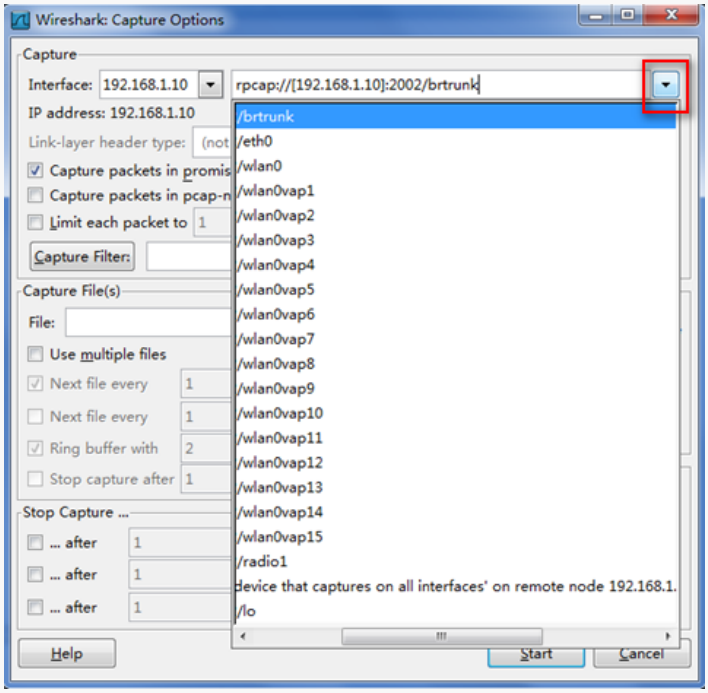
2 设置 Interface 为“Remote”；



3 在“Host”设置栏填写 AP 的 LAN 口 IP 地址，“Port”设置栏填写在 AP 上开启的远程捕获端口（此处假设 AP 的 LAN 口 IP 为 192.168.1.10，远程捕获端口为 2002）；



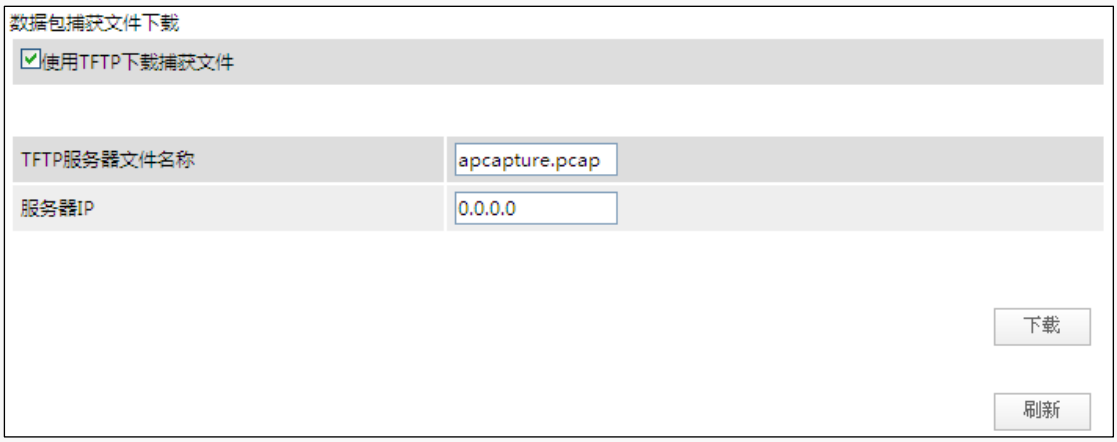
4 点击 OK，将弹出以下对话框，点击如图所示的下拉菜单，选择捕获的接口；



5 点击 Start，将开始正常捕获。

3.4 数据包捕获文件下载

此功能可将通过数据包文件捕获后，保存在 AP 的 RAM 存储器中的数据包文件下载至用户本地计算机。默认选择使用 TFTP 方式下载捕获文件。



- TFTP：请填写保存到 TFTP 服务器的文件名、TFTP 服务器 IP 地址。再点击 下载，捕获文件将传输至 TFTP 服务器。
- HTTP：此时请不勾选“使用 TFTP 下载捕获文件”，直接点击 下载。

客户端 QoS

本节介绍如何设置客户端 QoS 参数。点击『客户端 QoS』→『VAP QoS 参数』进入 AP 的客户端 QoS 设置页面。

1 QoS 概述

本小节简要介绍为何需要 QoS。

1.1 QoS 简介

QoS（Quality of Service，服务质量）是各种存在服务供需关系的场合中普遍存在的概念，它评估服务方满足客户服务需求的能力。评估通常不是精确的评分，而是注重分析在什么条件下服务是好的，在什么情况下还存在着不足，以便有针对性地做出改进。

在 Internet 中，QoS 所评估的就是网络转发分组的服务能力。由于网络提供的服务是多样的，因此，对 QoS 的评估可以基于不同方面，通常所说的 QoS，是对分组转发过程中为延迟、抖动、丢包率等核心需求提供支持的服务能力的评估。

1. 传统的分组转发业务

传统的 IP 网络无区别地对待所有的报文，采用 FIFO（First In First Out，先进先出）策略处理所有报文。即，根据报文到达时间的先后顺序分配转发所需要的资源，所有报文共享网络和设备的资源，至于得到资源的多少完全取决于报文到达的时机。这种服务策略称作 Best-Effort，它尽最大的努力将报文送到目的地，但对分组转发的延迟、抖动、丢包率和可靠性等需求不提供任何承诺和保证。

传统的 Best-Effort 服务策略只适合对带宽、延迟不敏感的 WWW、文件传输、e-mail 等业务。

2. 新业务引发的新需求

随着计算机网络的高速发展，越来越多的网络接入 Internet，越来越多的用户使用 Internet 作为数据传输的平台，开展各种应用。Internet 无论从规模、覆盖范围和用户数量上都拓展得非常快。

除了传统的 WWW、文件传输、e-mail 应用外，用户还尝试在 Internet 上拓展新业务，比如远程教学、远程医疗、可视电话、电视会议、视频点播等。企业用户也希望通过 VPN 技术，将分布在各地的分支机构连接起来，开展一些事务性应用，比如访问公司的数据库或通过 Telnet 管理远程设备。

这些新业务有一个共同特点，即对带宽、延迟、抖动等传输性能有着特殊的需求。比如电视会议、视频点播需要高带宽、低延迟和低抖动的保证。事务处理、Telnet 等关键任务虽然不一定要求高带宽，但非常注重低延迟，在拥塞发生时要求优先获得处理。

新业务的不断涌现对 IP 网络的服务能力提出了更高的要求，用户已不再满足于能够简单地将报文送达目的地，而是还希望在转发过程中得到更好的服务，诸如支持为用户提供专用带

宽、减少报文的丢失率、管理和避免网络拥塞、调控网络的流量、设置报文的优先级。所有这些，都要求网络应当具备更为完善的服务能力。

1.2 拥塞

传统网络所面临的服务质量问题，主要是由网络拥塞引起的。所谓的拥塞，是指由于供给资源相对不足造成分组转发速率下降、引入额外延迟的一种现象。

1．拥塞的产生

在 Internet 分组交换的复杂环境下，拥塞极为常见。以下图中的两种情况为例：

- 分组流从高速链路进入设备，由低速链路转发出去。
- 分组流从相同速率的多个端口同时进入网络设备，由一个相同速率的端口转发出去。如果流量以线速到达，那么就会出现资源的瓶颈而导致拥塞。

不仅仅是链路带宽的瓶颈会导致拥塞，任何用以正常转发处理的资源的不足，如可分配的处理器时间、缓冲区、内存资源的不足，都会造成拥塞。此外，在某个时间内对所到达的流量控制不力，使之超出了可分配的网络资源，也是引发网络拥塞的一个因素。

2．拥塞的影响

拥塞有可能会引发一系列的负面影响：

- 拥塞增加了报文传输的延迟和抖动，过高的延迟会引起报文重传。
- 拥塞使网络的有效吞吐率降低，造成网络资源的利用率降低。
- 拥塞加剧会耗费大量的网络资源（特别是存储资源），不合理的资源分配甚至可能导致系统陷入资源死锁而崩溃。

可见，拥塞使流量不能及时获得资源，是造成服务性能下降的源头。然而在分组交换以及多用户业务并存的复杂环境下，拥塞又是常见的，因此必须慎重加以对待。

3．对策

增加网络带宽是解决资源不足的一个直接途径，然而它并不能解决所有导致网络拥塞的问题。

解决网络拥塞问题的一个更有效的办法是在网络中增加流量控制和资源分配功能，为有不同服务需求的业务提供有区别的服务，正确地分配和使用资源。

在进行资源分配和流量控制的过程中，尽可能地控制好那些可能引发网络拥塞的直接或间接因素，减少拥塞发生的概率；在拥塞发生时，依据业务的性质及其需求特性权衡资源的分配，

将拥塞对 QoS 的影响减到最小。

2 客户端 QoS 参数说明

以下是对页面参数的说明：

标题项	说明
客户端 QoS 全局管理模式	在 AP 上启用或禁用客户端 QoS。 **提示** 此处更改的设置不会影响您在『服务』→『QoS』页面配置的 WMM 设置。
无线	选择要修改 VAP QoS 参数的无线类型：1（5G）或 2（2.4G）。
VAP	将您配置的客户端 QoS 设置应用到指定的 VAP，如 VAP0。 **提示** 当前选择的 VAP 的 QoS 设置不会影响到客户端通过其他 VAP 访问网络，如 VAP0 的规则对 VAP1 下的客户端不会造成任何影响，二者相互独立。
客户 QoS 模式	启用或禁用 VAP 菜单中选择的 VAP 的 QoS 操作。 **注意** 必须先启用客户端 QoS 全局管理模式，并在 VAP0-VAP15 上的其中一个 VAP 启用 QoS 规则，配置的规则才会在该 VAP 上被应用。
下行带宽限制	输入从 AP 到无线客户端所允许的最大传输速率，单位 bps（比特每秒）。 0 表示不对下行带宽作任何限制，建议配置下行带宽限制=N*8000bps，n=0, 1, 2, 3……
上行带宽限制	输入所允许的到 AP 的最大客户端传输速率，单位 bps（比特每秒）。 0 表示不对上行带宽作任何限制，建议配置上行带宽限制=N*8000bps，n=0, 1, 2, 3……

第Ⅴ部分

附录

常见问题处理

1. 电源系统故障处理

答：可以根据侧面板上的 Power 指示灯来判断 AP 电源系统是否故障。电源系统工作正常时，Power 指示灯应保持常亮或闪烁；若 Power 指示灯不亮，请进行如下检查：

- AP 电源线是否连接正确，开源开关是否为开启状态。
- AP 供电电源与 AP 所要求的电源是否匹配。
- AP 与注入器连接是否正确（AP 应接在注入器的的 AP 端口）。

2. 能 Ping 通设备，但登录设备 Web 网管不成功，也不能 Telnet 进入设备，是怎么回事？

答：您的设备当前可能已经转为 FIT 模式，Web 网管，Telnet，SSH，SNMP 服务已被禁用。此时，AP 作为 FASTPATH 统一无线系统的一部分，您可以使用 FASTPATH 统一无线交换机对它进行管理。

技术规格

1 硬件规格

项目	规格		
工作频段	802.11b/g/n：2.4GHz ~ 2.483GHz（中国） 802.11a/n：5.725GHz ~ 5.850GHz（中国）		
1000M 以太网口	2 个		
PoE	支持非标准 PoE 供电（采用自带电源适配器和 PoE 注入器供电）		
内置天线	内置硬件天线系统(工作频段：2.4G 和 5G，基础增益 7dBi)		
调制技术	OFDM ： BPSK@6/9Mbps 、 QPSK@12/18Mbps 、 16-QAM@24Mbps 、 64-QAM@48/54Mbps DSSS：DBPSK@1Mbps、DQPSK@2Mbps、CCK@5.5/11Mbps MIMO-OFDM：MCS 0-23		
2.4GHz 发送功率	11b	1Mbps ~ 11Mbps	26.5dBm ~27.5dBm
	11g	6Mbps ~ 9Mbps	26dBm
		12Mbps ~ 18Mbps	25dBm
		24Mbps ~ 36Mbps	24.5dBm
		48Mbps ~ 54Mbps	23.5dBm
	11n	MCS 0-32	23dBm ~ 26dBm
5GHz 发送功率	11a	20dBm	
	11n	20dBm	
2.4GHz 接收灵敏度	11b		-92dB
	11g		-83dB
	11n（HT20）		-83dB
	11n（HT40）		-80dB
5GHz 接收灵敏度	11a		-83dBm
	11n		-80dBm
可调功率粒度	1（百分比，范围：50 ~100）		

复位	支持
状态指示灯	Power：接通电源时常亮，系统启动后闪烁； 2.4GHz：默认常亮，数据传输时闪烁； 5GHz：默认常亮，数据传输时闪烁；
工作温度	0°C ～ 45°C
工作湿度	10% ～ 90%（无凝结）
整机功耗	<27W
EMC	B9254-2008、EN301 489、EN55022、FCC Part 15
尺寸	128.6mm×208.9mm(H×Φ)　　注：不包含天线接口和附件

2 软件规格

项目		规格
11n 支持	空间流数(Streams)	3
	工作频段	2.4GHz
	40MHZ	支持
	450Mbps(PHY)	支持
	空时分组码(STBC)	支持
WLAN 基础	建议每射频最大接入用户数	15
	虚拟 AP	16（实际应用中推荐每射频至多设置 5 个）
	open system/shared key 认证	支持
	广播 Probe 请求应答控制	支持
	WPA、WPA2-PSK	支持
	RTS/CTS	支持
	CTS-to-self	支持
	隐藏 SSID	支持
WLAN 扩展	STA 相关	支持 STA 异常下线检测、STA 老化、基

		于 STA 的统计和状态查询等
	接入用户数限制	支持
	多用户公平调度	支持
安全策略	加密	支持 64/128 位 WEP、动态 WEP、TKIP、CCMP(11n 推荐)加密
	802.11i	支持
	认证	支持 802.1X 认证、MAC 地址认证、PSK 认证、Portal 认证等。(根据应用不同可能需要 AC 无线控制器配合)
	用户隔离	支持无线用户二层隔离和基于 SSID 的无线用户隔离
	转发安全	支持报文过滤、MAC 地址过滤、广播风暴抑制等
	无线访问控制	支持/无线 MAC 认证
	SSID 与 VLAN 绑定	支持
AAA	Radius Client	支持
	认证服务器多域配置	支持
二三层功能	IP 地址设置	支持
	IPv6	支持
	ACL	支持(IPv4/IPv6)
	本地转发	支持基于 SSID+VLAN 的本地转发
	组播	IGMP Snooping/MLD Snooping
服务质量	802.11e	支持 WMM
	优先级	支持以太网口 802.1p 识别和标记
	QoS 策略映射	支持不同 SSID/VLAN 映射不同 QoS 策略
	用户带宽管理	可按每 STA 分配可用带宽，或按照 SSID 分配所有 STA 共享总带宽
	负载均衡	支持/基于流量
WDS	WDS	支持 P2P/P2MP、WDS 链路 PSK 认证与加

		密、邻居灵活发现
省电模式	非调度自动省电传送(U-APSD)	支持
	WMM Power Save	支持
管理维护	网络管理	SNMP V1/V2c/V3、Trap、HTTP(S)、SSH、Telnet、FTP/TFTP
	管理 SSID	支持
	日志功能	SYSLOG
	远程抓包分析	支持
	配置备份	支持

3 处理器和存储器

项目	规格
处理器	BCM53003
Flash	64MB
内存类型及容量	DDR2（128MB）

产品有毒有害物质清单

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。