

TP-LINK®

无线控制器

TL-AC10000

TL-AC1000

TL-AC500

TL-AC300

用户手册

REV2.1.0
1910040721

声明

Copyright © 2016 普联技术有限公司

版权所有, 保留所有权利

未经普联技术有限公司明确书面许可, 任何单位或个人不得擅自仿制、复制、誊抄或转译本手册部分或全部内容, 且不得以营利为目的进行任何方式 (电子、影印、录制等) 的传播。

TP-LINK[®]为普联技术有限公司注册商标。本手册提及的所有商标, 由各自所有人拥有。

本手册所提到的产品规格和资讯仅供参考, 如有内容更新, 恕不另行通知。除非有特殊约定, 本手册仅作为使用指导, 所作陈述均不构成任何形式的担保。

目录

前言	I
1 登录 Web 管理界面	1-1
1.1 登录准备	1-1
1.2 登录操作	1-1
1.3 登录成功	1-2
2 系统状态	2-1
2.1 运行状态	2-1
2.2 客户端状态	2-2
2.3 AP 状态	2-2
2.4 认证状态	2-3
2.4.1 认证状态	2-3
2.4.2 无感知认证用户	2-3
3 网络设置	3-1
3.1 接口设置	3-1
3.1.1 接口设置	3-1
3.1.2 接口流量统计	3-2
3.2 路由设置	3-3
3.2.1 静态路由	3-3
3.2.2 系统路由	3-4
3.3 DHCP 服务	3-4
3.3.1 DHCP 服务	3-4
3.3.2 客户端列表	3-6
3.3.3 静态地址分配	3-6
3.4 VLAN 设置	3-8
3.4.1 VLAN 简介	3-8
3.4.2 VLAN 设置	3-10

3.4.3	端口设置.....	3-12
3.5	交换机设置.....	3-12
3.5.1	端口统计.....	3-12
3.5.2	端口监控.....	3-14
3.5.3	端口流量限制.....	3-15
3.5.4	端口参数.....	3-16
3.5.5	端口状态.....	3-17
4	AP 管理.....	4-1
4.1	AP 设置.....	4-1
4.2	AP 升级.....	4-5
4.3	AP 数据库.....	4-6
4.4	负载均衡.....	4-7
5	射频管理.....	5-1
5.1	射频设置.....	5-1
5.2	速率设置.....	5-5
5.3	频谱导航.....	5-6
6	无线管理.....	6-1
6.1	无线服务.....	6-1
7	认证管理.....	7-1
7.1	MAC 认证.....	7-1
7.1.1	MAC 地址.....	7-2
7.1.2	MAC 认证.....	7-4
7.2	Portal 认证.....	7-5
7.2.1	跳转页面.....	7-5
7.2.2	Web 认证.....	7-8
7.2.3	微信连 Wi-Fi.....	7-12
7.2.4	一键上网.....	7-14
7.2.5	远程 portal.....	7-14

7.2.6	免认证策略.....	7-18
7.2.7	认证参数.....	7-21
7.3	用户管理.....	7-22
7.4	认证服务器.....	7-24
7.4.1	Radius 服务器.....	7-25
7.4.2	认证服务器.....	7-26
7.5	应用举例.....	7-28
7.5.1	一键上网.....	7-28
7.5.2	Web 认证.....	7-30
7.5.3	微信连 Wi-Fi.....	7-33
8	安全管理.....	8-1
8.1	广播风暴抑制.....	8-1
8.2	DHCP 防护.....	8-2
8.2.1	DHCP 防护.....	8-2
8.2.2	DHCP 服务器列表.....	8-3
8.3	ARP 防护.....	8-4
8.3.1	ARP 防护绑定.....	8-4
8.3.2	ARP 防护条目.....	8-5
9	链路备份.....	9-1
9.1	双链路备份.....	9-1
9.1.1	功能简介.....	9-1
9.1.2	双链路备份设置.....	9-3
10	系统工具.....	10-1
10.1	管理账号.....	10-1
10.1.1	管理账号.....	10-1
10.1.2	系统管理设置.....	10-1
10.2	设备管理.....	10-2
10.2.1	恢复出厂配置.....	10-2

10.2.2 备份与导入配置.....	10-3
10.2.3 重启设备.....	10-3
10.2.4 软件升级.....	10-4
10.3 诊断工具.....	10-4
10.4 时间设置.....	10-6
10.5 系统日志.....	10-8

前言

本手册旨在帮助用户正确使用无线控制器。内容包含对无线控制器产品性能特征的描述以及配置无线控制器的详细说明。请在操作前仔细阅读本手册。

目标读者


本手册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

正文中出现的符号约定

符号	含义
< >	尖括号。用尖括号标记的文字，表示界面的按键名称，如 < 保存 >。
“ ”	双引号。用双引号标记的文字，表示界面出现的除按键外名词，如“启用”。
【 】	方括号。用方括号标记的文字，表示键盘上的按键。

特殊图标约定

图标	含义
	说明图标。该图标表示此部分内容是对相应设置、步骤的补充说明。

其他约定

- 在本手册中，所提到的“AC”、“本产品”等名词，如无特别说明，系指无线控制器。
- 全文如无特殊说明，Web 界面以 TL-AC10000 机型为例介绍。

产品相关资料

我司官网提供丰富的产品资料，主要资料有可供网页阅读的产品介绍和规格参数信息；可供下载的《安装手册》、《用户手册》和《设备防雷安装手册》等多种文档。

如需获取最新产品资料，请登录我司官网 <http://www.tp-link.com.cn>。

阅读方式	资料名称	简介
仅供网页阅读	产品介绍	介绍设备主要性能特点
	规格参数	罗列设备硬件规格和软件功能
可在线阅读， 也可下载文档	《安装手册》	介绍设备的安装过程、启动以及常见故障处理
	《用户手册》	介绍设备各个功能应用
	《设备防雷安装手册》	介绍设备安装中如何做好防雷措施以避免设备雷击损坏

1 登录 Web 管理界面

1.1 登录准备

第一次登录时，需要确认以下几点：

- 1) 无线控制器已正常加电启动，任一物理端口已与管理主机相连。
- 2) 管理主机 IP 地址已设为与无线控制器接口同一网段，即 192.168.1.X（X 为 2 至 252 之间的任意整数），子网掩码为 255.255.255.0。
- 3) 管理主机已至少安装一种以下浏览器：IE 8.0 或以上版本，最新版本的 FireFox、Chrome 和 Safari 浏览器。
- 4) 为保证能更好地体验 Web 界面显示效果，建议将显示器的分辨率调整到 1024×768 或以上像素。

1.2 登录操作

- 1) 打开浏览器，在地址栏输入设备的默认管理地址 <http://192.168.1.253>，按下回车键。

图 1-1 输入管理地址



- 2) 首次登录需设置管理员账号，自定义用户名和密码，如下图所示，密码长度不得少于 6 位（包括英文字母、数字和符号的组合）。

图 1-2 首次登录界面

A screenshot of the TP-LINK first login interface. At the top is the TP-LINK logo. Below it is a red warning message: '为保证设备安全，请您务必设置管理员账号'. There are three input fields: '设置用户名:', '设置密码:', and '确认密码:'. Below the fields is a note: '注意：确认提交前请牢记您的管理员账户和密码，后续配置将必须使用该账户进行登录配置。如果您不慎遗忘该密码，只能在设备通电情况下按住Reset按钮并保持5秒以上来恢复出厂设置，以重新设置设备的所有参数。'. At the bottom is a blue '确认' button.

3) 完成管理员账号设置后，即可使用已设的用户名和密码登录，如下图所示。

图 1-3 登录界面



1.3 登录成功

成功登录后将看到无线控制器的 Web 管理界面，如下图所示。

图 1-4 Web 管理界面



界面右上角有 < 保存配置 > 和 < 退出登录 > 按钮。

表 1-1 主界面按键说明

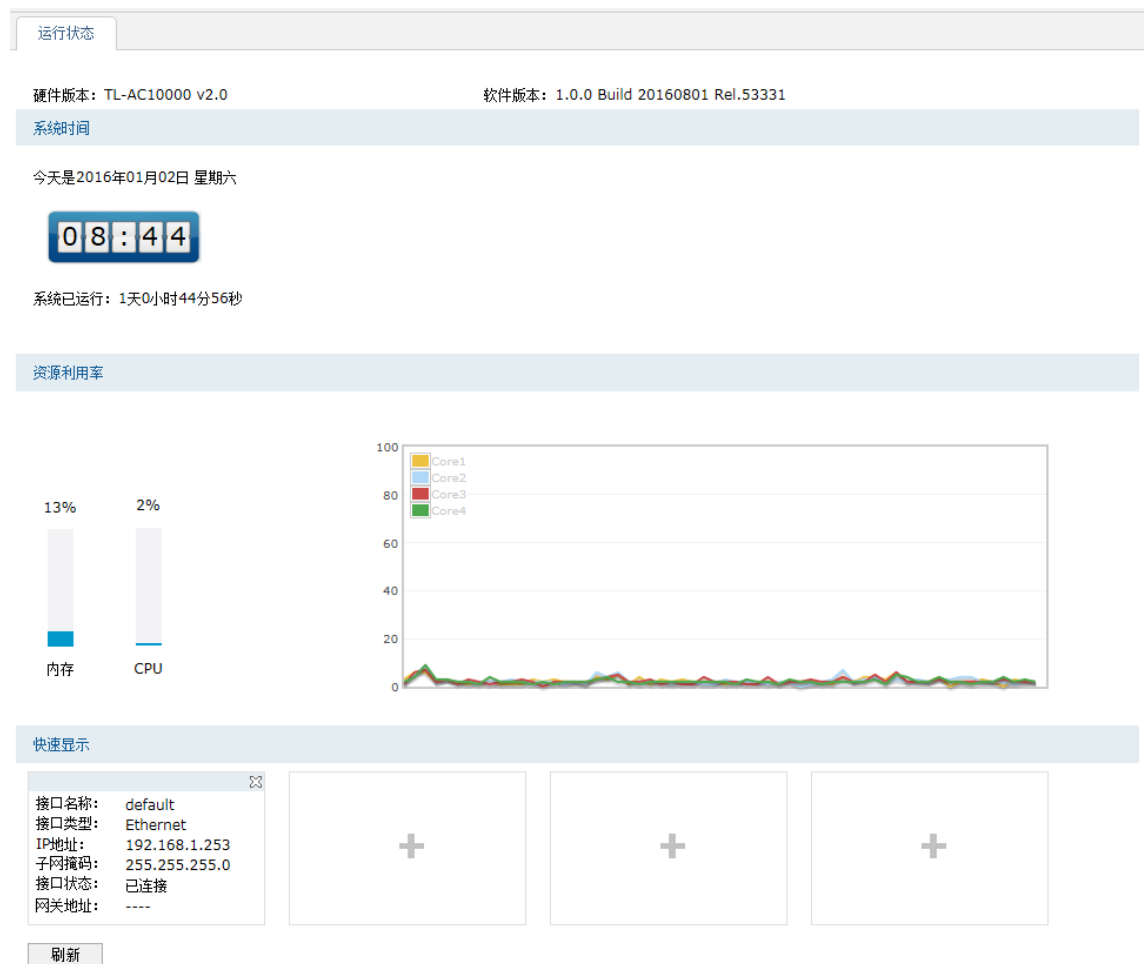
保存配置	保存最终的配置。 更改每一个配置后，< 新增 > 和 < 设置 > 按键只能使当前配置在设备未重启前生效；若需要在重启设备后配置依旧生效，则需要点击 < 保存配置 > 按钮。建议在断电重启前 < 保存配置 >，以免丢失配置信息。
退出登录	退出当前登录，返回登录界面。

2 系统状态

2.1 运行状态

进入界面：系统状态 >> 运行状态 >> 运行状态

图 2-1 运行状态界面



在**资源利用率**区域可以监测内存和 CPU 的利用率。CPU 利用率推荐值为 50% 左右，高于 85% 表示无线控制器处于高负载状态，高于 95% 表示满负载状态。当 CPU 利用率持续较高时，部分功能可能异常，此时可能是网络中出现异常，请进行排查。

在**快速显示**区域，点击各区域的 < + > 按键选择接口查看接口信息。

2.2 客户端状态

可以在此界面查看接入网络的客户端的信息。

进入界面：系统状态 >> 客户端状态 >> 客户端状态

图 2-2 客户端状态界面



2.3 AP 状态

可以在此界面查看接入无线控制器的 AP 的信息。如需设置 AP，请参考 [AP 管理](#)。

进入界面：系统状态 >> AP 状态 >> AP 状态

图 2-3 AP 状态界面



点击**射频列表**和 **SSID** 项的**详细信息**，将弹出对应项的详细信息界面。如需设置射频，请参考[射频管理](#)；如需设置无线服务，请参考[无线管理](#)。

图 2-4 射频列表详细信息界面



图 2-5 SSID 详细信息界面



2.4 认证状态

2.4.1 认证状态

可以在此界面查看接入网络的用户的认证状态。如需设置用户的认证方式，请参考[认证管理](#)。

进入界面：系统状态 >> 认证状态 >> 认证状态

图 2-6 认证状态界面



2.4.2 无感知认证用户

可以在此界面查看无感知认证用户的信息。

进入界面：系统状态 >> 认证状态 >> 无感知认证用户

图 2-7 无感知认证用户界面



3 网络设置

3.1 接口设置

3.1.1 接口设置

可以在此界面创建接口。创建接口必须保证有 VLAN 可供选择，如需设置 VLAN，请参考 [VLAN 设置](#)。

进入界面：网络设置 >> 接口设置 >> 接口设置

图 3-1 接口设置界面

The screenshot shows the '接口设置' (Interface Settings) page. At the top, there are tabs for '接口设置' and '接口流量统计'. Below the tabs is a search bar and a help icon. A toolbar contains '+ 新增' (Add), '- 删除' (Delete), and '🔍 搜索' (Search). The main content is a table with the following data:

<input type="checkbox"/>	序号	接口名称	连接状态	关联VLAN	IP地址	子网掩码	网关地址	MAC地址	设置
<input type="checkbox"/>	1	default	已连接 详细	1	192.168.1.253	255.255.255.0	---	00-14-78-00-00-00	

At the bottom right, there is a pagination control: '共1条, 每页: 10 条 | 当前: 1/1页, 1~1条 |' with navigation arrows and the page number '1'.

在此界面，可以对已有条目进行操作，序号为 1 的条目是系统预定义的一个接口，不可删除。点击 < 新增 > 按键可以添加新条目，新增接口界面如下图所示。

图 3-2 新增接口界面

The screenshot shows the '新增接口' (Add Interface) form with the following fields and options:

- 接口名称: (1-12个英文字符、数字或下划线)
- 关联VLAN: ▼
- 连接方式: ▼
- IP地址:
- 子网掩码:
- 网关地址: (可选)
- MTU: (576-1500)
- 首选DNS服务器: (可选)
- 备用DNS服务器: (可选)
- MAC地址:
- 备注: (可选, 1-50个字符)

At the bottom, there are two buttons: '确定' (Confirm) and '取消' (Cancel).

表 3-1 新增接口界面条目项说明

接口名称	自定义接口名称。
关联 VLAN	选择该接口指向的 VLAN。
连接方式	目前仅静态 IP 连接方式可选。
IP 地址	设置接口的 IP 地址。
子网掩码	设置接口的子网掩码。
网关地址	设置网关地址。
MTU	MTU (Maximum Transmission Unit, 最大传输单元), 可以设置数据包的最大长度。取值范围是 576-1500 之间的整数, 默认值为 1500。若 ISP 未提供 MTU 值, 请保持默认值不变。
首选 / 备用 DNS 服务器	输入 ISP 提供的 DNS 服务器, 若不清楚可以向 ISP 询问。当首选 DNS 服务器失效时客户端可以向备用 DNS 服务器申请域名解析。
MAC 地址	设置接口的 MAC 地址。
备注	设置条目备注, 以方便管理和查找。

说明:

若接口被 DHCP 服务或静态地址引用, 修改接口的 IP 网段会导致 DHCP 服务地址分配范围同步调整, 且与接口 IP 不在同一网段的静态地址无法分配。

3.1.2 接口流量统计

可以在此界面查看所有接口的流量统计信息。点击表头文字, 可以对该列进行升序 / 降序排序。

进入界面: 网络设置 >> 接口设置 >> 接口流量统计

图 3-3 接口流量统计界面

接口	发送速率(KB/s)	接收速率(KB/s)	发送包速率(Pkt/s)	接收包速率(Pkt/s)	发送总字节	接收总字节	发送总报文	接收总报文
default	1	2	9	9	10M	5M	40219	39340

共 1 条, 每页: 10 条 | 当前: 1/1 页, 1~1 条 |

如需要按指定内容排序, 请点击表头切换排序方式

3.2 路由设置

3.2.1 静态路由

可以在此界面设置静态路由条目。当数据包与静态路由条目匹配成功时，将按照条目的下一跳进行转发。

进入界面：网络设置 >> 路由设置 >> 静态路由

图 3-4 静态路由界面



在此界面，点击 < 新增 > 按键可以添加新条目，可对已有条目进行编辑、删除操作。

表 3-2 静态路由界面条目项说明

名称	路由条目的名称，不能重复。
目的地址	数据包要到达的目的网络的 IP 地址。
子网掩码	数据包要到达的目的网络的子网掩码。
下一跳	数据包将发往的下一个路由点。
出接口	数据包进行转发的接口。
Metric	路由条目的优先级，其数值越低优先级越高。默认值为 0，一般不需要修改。
可达性	路由条目的实际生效情况。 当出接口与下一跳相互匹配且 metric 值最小时，显示 < 可达 >; 当出接口与下一跳相互匹配但 metric 值非最小时，显示 < 备选 >; 当出接口与下一跳不匹配，或者条目被禁用时，显示 < 不可达 >。 仅当条目 < 可达 > 时，才是生效的。
状态	启用或禁用路由条目。
设置	编辑或删除条目。

3.2.2 系统路由

可以在此界面查看实际生效的系统路由表。

进入界面：网络设置 >> 路由设置 >> 系统路由

图 3-5 系统路由界面

The screenshot shows the 'System Routing' (系统路由) interface. It has two tabs: 'Static Routing' (静态路由) and 'System Routing' (系统路由). Below the tabs is a header 'System Routing Table' (系统路由表) with a search icon. A table displays the following data:

序号	目的地址	子网掩码	下一跳	出接口	Metric
1	127.0.0.0	255.0.0.0	0.0.0.0	loopback	0
2	192.168.1.0	255.255.255.0	0.0.0.0	default	0

Below the table, it indicates '共2条, 每页: 10 条 | 当前: 1/1页, 1~2条 |' with navigation buttons.

3.3 DHCP 服务

设备具有 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）服务功能，能够为所有接入无线控制器的 AP 或客户端自动分配 IP 参数。

3.3.1 DHCP 服务

可以在此界面配置 DHCP 服务器参数。

进入界面：网络设置 >> DHCP 服务 >> DHCP 服务

图 3-6 DHCP 服务界面

The screenshot shows the 'DHCP Service' (DHCP 服务) interface. It has three tabs: 'DHCP Service' (DHCP 服务), 'Client List' (客户端列表), and 'Static Address Allocation' (静态地址分配). Below the tabs is a 'Function Settings' (功能设置) section with a search icon. The 'IP Allocation Range' (IP分配范围) is set to 'Only for AP Allocation' (仅为AP分配). There is a 'Settings' (设置) button. Below is a 'DHCP Service List' (DHCP 服务列表) table:

序号	服务接口	开始地址	结束地址	地址租期	网关地址	首选DNS服务器	状态	设置
1	default	192.168.1.200	192.168.1.249	120	---	---	已启用	[Edit] [Delete]

Below the table, it indicates '共1条, 每页: 10 条 | 当前: 1/1页, 1~1条 |' with navigation buttons.

功能设置

在此区域可以配置 DHCP 的 IP 分配范围：

- 仅为 AP 分配：DHCP 服务器只能为 TP-LINK 系列 AP 分配 IP 地址。
- 为 AP 和用户终端分配：当网络中没有部署 DHCP 服务器为无线客户端分配 IP 地址时，可选择此项，无线控制器将为网络中的所有客户端分配 IP 地址。

DHCP 服务列表

在此区域可以对已有条目进行操作，序号为 1 的条目是系统预定义的 DHCP 服务。点击 <新增> 按钮可以添加新条目，新增 DHCP 服务界面如下图所示。

图 3-7 新增 DHCP 服务界面

The screenshot shows a configuration form for adding a DHCP service. The fields are as follows:

- 服务接口: A dropdown menu with a downward arrow.
- 开始地址: A text input field.
- 结束地址: A text input field.
- 地址租期: A text input field containing '120', followed by the unit '分钟 (2-2880)'.
- 网关地址: A text input field with '(可选)' to its right.
- 缺省域名: A text input field with '(可选)' to its right.
- 首选DNS服务器: A text input field with '(可选)' to its right.
- 备用DNS服务器: A text input field with '(可选)' to its right.
- 状态: A checkbox labeled '启用' (Enabled) which is checked.

At the bottom of the form are two buttons: '确定' (Confirm) and '取消' (Cancel).

表 3-3 新增 DHCP 服务界面条目项说明

服务接口	用于 DHCP 分配地址的服务接口。
开始 / 结束地址	DHCP 服务器自动分配的 IP 的开始 / 结束地址。 开始 / 结束地址必须与服务接口 IP 在同一网段，否则 DHCP 服务不生效。
地址租期	DHCP 服务器所分配的 IP 地址的有效使用时间，超时将重新分配。
网关地址	输入此地址池给客户端分配的默认网关。
缺省域名	输入本地网域名。
首选 / 备用 DNS 服务器	输入 ISP 提供的 DNS 服务器，若不清楚可以向 ISP 询问。当首选 DNS 服务器失效时客户端可以向备用 DNS 服务器申请域名解析。
状态	勾选“启用”后该条目生效。

3.3.2 客户端列表

可以在此界面查看已从无线控制器上获取 TCP/IP 网络参数的客户端的主机名、服务接口、MAC 地址、其获得的 IP 地址以及 IP 地址的剩余租期。

进入界面：网络设置 >> DHCP 服务 >> 客户端列表

图 3-8 客户端列表界面

客户端列表

搜索 刷新 自动刷新

序号	服务接口	主机名	MAC地址	IP地址	剩余租期
1	default	--	88-25-93-8C-84-5A	192.168.1.215	01:57:31

共 1 条, 每页: 10 条 | 当前: 1/1 页, 1~1 条 |

3.3.3 静态地址分配

可以在此界面为指定的 MAC 地址预留 IP 地址。当使用该 MAC 地址的设备向无线控制器的 DHCP 服务器请求分配 IP 时，服务器将为其分配预留的 IP 地址。

进入界面：网络设置 >> DHCP 服务 >> 静态地址分配

图 3-9 静态地址分配界面

备份静态地址条目

备份

导入静态地址条目

文件路径: 浏览

导入

注意：使用Excel软件打开csv文件时可能造成部分数值格式变化，从而显示不正确。如果使用Excel编辑csv文件，请设置单元格为文本格式。

静态地址分配

启用 禁用 新增 删除 搜索 全局搜索

<input type="checkbox"/>	序号	MAC地址	IP地址	备注	状态	设置
<input type="checkbox"/>	--	--	--	--	--	--

共 0 条, 每页: 10 条 | 当前: 0/0 页, 0~0 条 |

备份静态地址条目

点击 < 备份 > 按键可以备份所有的静态地址条目至 ANSI 编码格式的 CSV 文件中。备份的文件可直接通过“导入静态地址条目”功能重新添加到静态地址列表中。

导入静态地址条目

一次性导入多个静态地址条目配置方法：

- 1) 将需要设置的静态地址条目存为一份合法的 ANSI 编码格式的 CSV 文件。可以通过“备份静态地址条目”功能获取符合规则的 CSV 文件，以查看文件的正确格式。
- 2) 点击 < 浏览 > 按键选择文件路径，再点击 < 导入 > 按键导入该文件。



说明：

使用 Excel 软件打开 csv 文件时可能造成部分数值格式变化，从而显示不正确。如果使用 Excel 编辑 csv 文件，请设置单元格为文本格式。

静态地址分配

在此区域，可以对已有条目进行操作，点击 < 新增 > 按键可以添加新条目，新增静态地址分配界面如下图所示。

图 3-10 新增静态地址分配界面

MAC地址:

IP地址:

备注: (1-32个字符, 可选)

状态: 启用

表 3-4 新增静态地址分配界面条目项说明

MAC 地址	设置需要预留 IP 地址的 MAC 地址。
IP 地址	预留的 IP 地址。
备注	设置条目备注，以方便管理和查找。
状态	勾选“启用”后该条目生效。

3.4 VLAN 设置

3.4.1 VLAN 简介

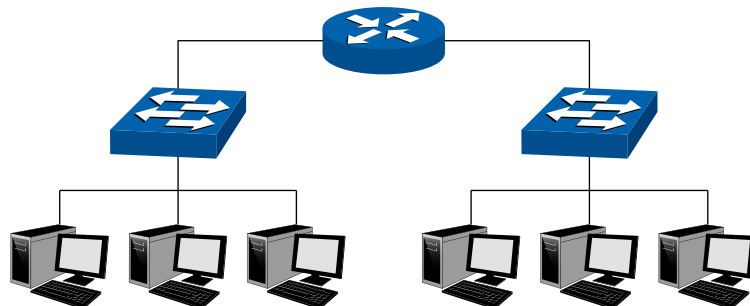
VLAN (Virtual Local Area Network, 虚拟局域网) 是一种将局域网设备从逻辑上划分成一个个网段, 从而实现虚拟工作组的数据交换技术, 这种技术通过在局域网数据帧上定义扩展字段, 来对物理网络进行逻辑上的分割, 从而限定局域网数据帧的转发范围, 缩小广播域。VLAN 技术主要应用于交换机、路由器和无线控制器等网络设备中。

产生背景

局域网的发展是 VLAN 产生的基础, 可以通过了解局域网的有关知识来了解 VLAN。

局域网 (Local Area Network) 是在一个局部的地理范围内 (如一个学校、工厂和公司内), 将各种计算机、共享设备和数据库等互相联接起来组成的一个封闭式的计算机通信网络。其通常是一个单独的广播域, 主要由 Hub、网桥或交换机等网络设备连接网络内的所有节点。处于同一个局域网的网络节点之间可以直接通信, 而处于不同局域网段的设备之间则必须经过路由器才能通信。下图为使用路由器构建的典型局域网环境。

图 3-11 典型局域网拓扑



然而随着网络的不断扩展, 接入设备逐渐增多, 网络结构也日趋复杂, 必须使用更多的路由器才能将不同的用户划分到各自的用户组 (广播域) 中, 在不同的局域网之间提供网络互联。但路由器数量的增多势必会导致网络延时逐渐加长, 网络数据传输速度下降。其次, 用户是按照物理连接被机械地划分到不同的用户组中, 而这种分割方式并没有考虑到用户的工作属性和网络需求。

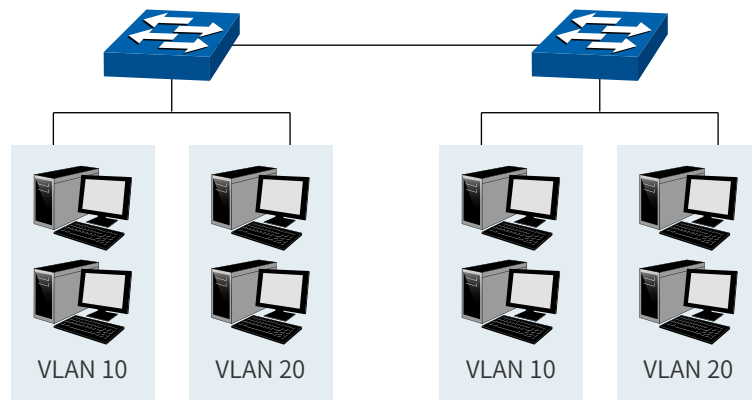
在这种情况下, VLAN 技术应运而生。利用 VLAN 技术, 可以根据用户的工作属性和网络需求, 在无线控制器或者交换机、路由器上划分 VLAN, 将用户划分到不同的工作组中, 为不同的工作组执行不同的策略。

同一个 VLAN 中的用户间通信就和在一个局域网内一样, 同一个 VLAN 中的广播只有 VLAN 中的成员才能听到, 而不会传输到其他的 VLAN 中去, 从而控制不必要的广播风暴的产生。同时, 若没有路由, 不同 VLAN 之间不能相互通信, 从而提高了不同工作组之间的信息安全性。网络管理员可以通过配置 VLAN 之间的路由来全面管理网络内部不同工作组之间的信息互访。

技术特点

以下是 VLAN 在实际网络应用中的常用基础拓扑。

图 3-12 VLAN 常用网络拓扑



VLAN 的划分不受物理位置的限制，不在同一物理位置范围的主机可以属于同一个 VLAN；一个 VLAN 包含的用户可以连接在同一台交换机上，也可以跨越交换机。在局域网中使用 VLAN 功能有如下优点：

- 快速创建虚拟工作组。使用 VLAN 功能可以快速创建虚拟工作组，只需网络管理者在控制台上进行简单的操作即可，而不必为项目需要将组成员的工作站集合在一起建立一个局域网。
- 增强网络安全。不同 VLAN 的设备不能互相访问，需要通过路由器或三层交换机等网络层设备对报文进行三层转发，从而确保一个 VLAN 的数据不会被其他 VLAN 的设备窃听。
- 提高网络性能。通过 VLAN 功能可以将广播帧限制在 VLAN 内，有效控制网络的广播风暴，节省了网络带宽，进而提高网络处理能力。
- 降低网络管理成本。同一个虚拟工作组的主机不会局限在某个物理范围内，简化了网络的管理，方便为不同区域用户建立工作组。当一个用户从一个位置移动到另一个位置时，使用合适的 VLAN 划分方法，就不需要重新配置网络属性。

802.1Q VLAN

IEEE 于 1999 年发布了用以规范 VLAN 实现的 IEEE Std 802.1Q 标准。藉以此标准，在局域网中的连接设备能够识别对方网络上建立的 VLAN 并执行相应的通信策略。

IEEE 802.1Q 协议标准为各种局域网网络结构定义了 VLAN 的 Tag 字段，不同网络结构中，连接设备可以通过共同的数据特征进行 VLAN 识别。

对于常见的以太网网络模型，其主要的报文封装格式类型有两种，分别为 Ethernet II 型和 802.2/802.3 型。对于这两种以太网报文的封装格式，IEEE 802.1Q 协议标准在数据帧首部的目的 MAC 地址（DA）和源 MAC 地址（SA）后定义了 VLAN Tag，用以标识 VLAN 的相关信息。Tag 字段的位置如下图所示。Tag 封装在 DA&SA 后，它包含四个字段，分别是 TPID（Tag

Protocol Identifier, 标签协议标识符)、Priority、CFI (Canonical Format Indicator, 标准格式指示位) 和 VLAN ID。

图 3-13 VLAN Tag 组成字段

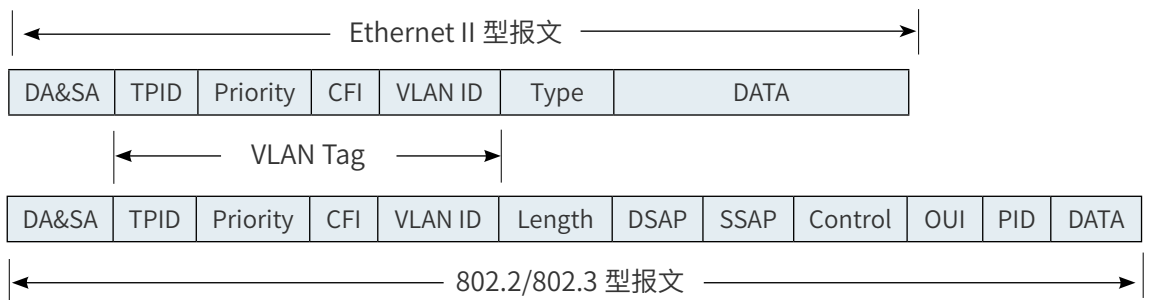


表 3-5 Tag 字段含义

TPID	默认值为 0x8100。当 TPID 字段为 0x8100 时，表示本数据帧带有 Tag。
Priority	数值为 0-7，表示数据包的传输优先级。当 VLAN ID 字段为 0 时表示此 Tag 是一个优先级 Tag，由 IEEE 802.1P 协议标准进行规范，详细请查看 IEEE 802.1P 协议标准。
CFI	数值为 0 或 1。以太网交换机中，CFI 总被设置为 0。用来表示 MAC 地址是否以标准格式进行封装。该字段长度为 1bit，取值为 0 表示 MAC 地址以标准格式进行封装，取 1 表示以非标准格式封装，缺省取值为 0。
VLAN ID	可设置范围为 1-4094。用来标识该报文所属 VLAN，简称 VID。当 VLAN ID 字段为 0 时表示此 Tag 是一个优先级 Tag；VLAN ID 字段全 1 为协议预留字段。

在 802.1Q VLAN 基础上，添加其他标识，可以有不同方法实现 VLAN，例如在 802.1Q VLAN 基础上添加 MAC 识别，从而实现基于 MAC 的 VLAN，此外，还有基于协议的 VLAN，基于 IP 地址的 VLAN，基于端口的 VLAN 等。无线控制器是基于端口实现的 VLAN。

PVID

PVID (Port VLAN ID)，通信设备每个物理接口的重要参数，表示端口默认所属的 VLAN。当设备的端口接收到的数据帧不带 VLAN Tag 时，设备会根据接收端口的 PVID 为该报文插入 VLAN Tag，并在端口的缺省 VLAN 中转发数据帧。PVID 主要有下面两个用途：

- 当设备收到不带 Tag 的数据帧时，将根据 PVID 为数据帧插入 VLAN Tag 并转发。
- PVID 指定了端口的缺省 VLAN ID，即默认广播域。当端口接收到 UL 包或广播包的时候，设备将这些数据包在该端口的缺省 VLAN 内广播。

3.4.2 VLAN 设置

在此界面可以设置报文中 Tag 字段的 VLAN ID 数值和端口的出口规则。

进入界面：网络设置 >> VLAN 设置 >> VLAN 设置

图 3-14 VLAN 设置界面



在此界面，可以对已有条目进行操作，序号为 1 的条目是系统预定义的一个 VLAN。点击 < 新增 > 按钮可以添加新条目，新增 VLAN 条目界面如下图所示。

图 3-15 新增 VLAN 界面

VLAN ID: (1-4094)

名称: (1-50个字符)

备注: (可选,1-50个字符)

选择端口成员

端口1 出口规则: UNTAG

端口2 出口规则: UNTAG

端口3 出口规则: UNTAG

端口4 出口规则: UNTAG

端口5 出口规则: UNTAG

表 3-6 新增 VLAN 界面条目项说明

VLAN ID	设置 Tag 字段的 VLAN ID 数值。
名称	输入一个名称来标识该 VLAN。
备注	添加对本条目的说明信息，非必填项。

选择端口成员

勾选端口后，可以选择 VLAN 端口成员的出口规则：

- TAG 表示输出的数据帧带有 tag 信息；
- UNTAG 表示输出的数据帧不带 tag 信息。

说明：

编辑或者删除 VLAN 条目，可能导致所属端口的 PVID 被修改。

3.4.3 端口设置

在此界面可以设置端口的 PVID。

进入界面：网络设置 >> VLAN 设置 >> 端口设置

图 3-16 端口设置界面

端口	PVID	所属VLAN
端口1	1	查询
端口2	1	查询
端口3	1	查询
端口4	1	查询
端口5	1	查询

设置

表 3-7 端口设置界面条目项说明

PVID	设置端口的 PVID。
所属 VLAN	点击“查询”，可以查看本端口所加入的 VLAN 信息。

3.5 交换机设置

3.5.1 端口统计

用于交换信息的数据包在数据链路层通常称为“帧”。可以通过此功能查看各个端口收发数据帧的统计信息。

进入界面：网络设置 >> 交换机设置 >> 端口统计

图 3-17 端口统计界面

参数		端口1	端口2	端口3	端口4	端口5
接收	单播帧	71243	0	0	0	15487
	广播帧	4537	0	0	0	50
	流控帧	0	0	0	0	0
	多播帧	18158	0	0	0	1271
	所有帧	16.7 MB	0 B	0 B	0 B	2.3 MB
发送	单播帧	74991	0	0	0	14965
	广播帧	59	0	0	0	4539
	流控帧	0	0	0	0	0
	多播帧	1277	0	0	0	18153
	所有帧	18.7 MB	0 B	0 B	0 B	7.5 MB
总计	过小帧	0	0	0	0	0
	正常帧	170265	0	0	0	54466
	过大帧	0	0	0	0	0

刷新 清空

表 3-8 端口统计界面条目项说明

单播帧	目的 MAC 地址为单播 MAC 地址的正常数据帧数目。
广播帧	目的 MAC 地址为广播 MAC 地址的正常数据帧数目。
流控帧	接收 / 发送的流量控制数据帧数目。
多播帧	目的 MAC 地址为多播 MAC 地址的正常数据帧数目。
过小帧	收到的长度小于 64 字节的数据帧数目（包含校验和错误的帧）。
正常帧	收到的长度在 64 字节到 1518 字节之间的数据帧数目（包含错误帧）。
过大帧	收到的长度大于 1518 字节的数据帧数目（包含错误帧）。

 说明：

- 错误帧：指校验和错误的帧。
- 最大帧长：设备支持的最大帧的大小，对于不带 Tag 标签的帧该值为 1518 字节，对于带 Tag 标签的帧该值为 1522 字节。

3.5.2 端口监控

可以在此开启和设置端口监控功能。被监控端口的报文会被自动复制到监控端口，以便网络管理人员实时查看被监控端口传输状况的详细资料，对其进行流量监控、性能分析和故障诊断。

进入界面：网络设置 >> 交换机设置 >> 端口监控

图 3-18 端口监控界面

端口统计 端口监控 端口流量限制 端口参数 端口状态

功能设置 ?

启用端口监控

监控模式: 输入输出监控

监控列表

监控端口	被监控端口
<input type="radio"/> 端口1	<input checked="" type="checkbox"/> 端口1
<input type="radio"/> 端口2	<input type="checkbox"/> 端口2
<input type="radio"/> 端口3	<input type="checkbox"/> 端口3
<input type="radio"/> 端口4	<input type="checkbox"/> 端口4
<input checked="" type="radio"/> 端口5	<input type="checkbox"/> 端口5

设置

功能设置

表 3-9 端口监控 - 功能设置界面条目项说明

启用端口监控	勾选即启用端口监控。推荐勾选，方便及时了解路由器端口报文信息。
监控模式	选择对数据包进行“输入监控”、“输出监控”或者“输入输出监控”。

监控列表

表 3-10 端口监控 - 监控列表界面条目项说明

监控端口	只能选择一个端口做监控端口。
被监控端口	被监控端口可以为多个，但不包含当前的监控端口。

应用举例

某企业网络出现异常状况，需要利用端口监控功能捕获网络中的所有数据进行分析。

可通过设置端口监控功能实现此需求。

设置界面：基本设置 >> 交换机设置 >> 端口监控

勾选“启用端口监控”，并选择“输入输出监控”的监控模式，设置端口 5 为监控端口，监控其它端口的输入输出数据，如下图所示。设置完成后，点击 < 设置 > 按钮。

图 3-19 端口监控应用举例界面

端口统计 端口监控 端口流量限制 端口参数 端口状态

功能设置 ?

启用端口监控

监控模式： 输入输出监控 ▼

监控列表

监控端口	被监控端口
<input type="radio"/> 端口1	<input checked="" type="checkbox"/> 端口1
<input type="radio"/> 端口2	<input checked="" type="checkbox"/> 端口2
<input type="radio"/> 端口3	<input checked="" type="checkbox"/> 端口3
<input type="radio"/> 端口4	<input checked="" type="checkbox"/> 端口4
<input checked="" type="radio"/> 端口5	<input type="checkbox"/> 端口5

设置

3.5.3 端口流量限制

可以在此开启各端口的流量限制功能并进行相应设置。

进入界面：网络设置 >> 交换机设置 >> 端口流量限制

图 3-20 端口流量限制界面

端口统计 端口监控 端口流量限制 端口参数 端口状态

功能设置 ?

端口	入口限制	入口限制速率(Mbps)	出口限制	出口限制速率(Mbps)
端口1	<input type="checkbox"/> 启用	1000	<input type="checkbox"/> 启用	1000
端口2	<input type="checkbox"/> 启用	1000	<input type="checkbox"/> 启用	1000
端口3	<input type="checkbox"/> 启用	1000	<input type="checkbox"/> 启用	1000
端口4	<input type="checkbox"/> 启用	1000	<input type="checkbox"/> 启用	1000
端口5	<input type="checkbox"/> 启用	1000	<input type="checkbox"/> 启用	1000

设置

表 3-11 端口流量限制界面条目项说明

入口限制	勾选“启用”后，后续设置的入口限制速率才会生效。
入口限制速率	设置入口限制速率。
出口限制	勾选“启用”，后续设置的出口限制速率才会生效。
出口限制速率	设置出口限制速率。

3.5.4 端口参数

可以在此启用各物理端口的流量控制，并根据需要设定其协商模式。

进入界面：网络设置 >> 交换机设置 >> 端口参数

图 3-21 端口参数界面



表 3-12 端口参数界面条目项说明

流量控制	推荐勾选“启用”以控制调节各端口数据包转发的速率，避免出现拥塞。
协商模式	有 10M 全 / 半双工、100M 全 / 半双工、1000M 全双工、自协商 6 种模式可选，择需使用。

3.5.5 端口状态

可以在此查看各个端口的基本状态。

进入界面：网络设置 >> 交换机设置 >> 端口状态

图 3-22 端口状态界面



端口	端口状态	连接速率	双工模式	流量控制
端口1	已连接	100M	全双工	已禁用
端口2	已断开	---	---	---
端口3	已断开	---	---	---
端口4	已断开	---	---	---
端口5	已连接	100M	全双工	已禁用

4 AP 管理

4.1 AP 设置

可以在此界面进行 AP 设置。

进入界面：AP 管理 >> AP 设置 >> AP 设置

图 4-1 AP 设置界面

全局设置

定时重启：若开启该功能，则在设定的时间到达时，所有已接入无线控制器的 AP 将重启。

自动固化：若开启该功能，则新 AP 连接到无线控制器上将生成已固化的 AP 条目。

分组列表

在此区域，可以对 AP 和模板进行分组管理。序号为 1 的条目是系统预定义的 AP 分组。不允许删除默认分组或非空分组。

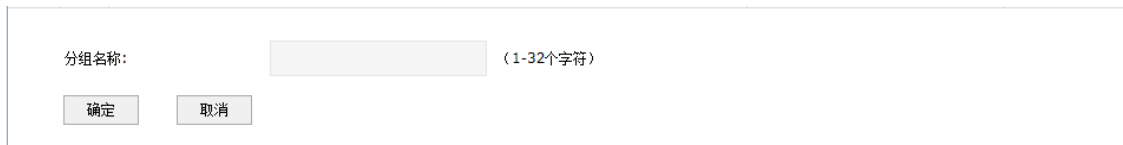
表 4-1 分组列表界面项说明

分组名称	显示分组名称。默认分组的名称后会加注“（默认分组）”字样。
分组统计信息	形如“X/Y, Z”，X 表示已经成功接入的 AP 数目，Y 表示分组中所有的 AP 数目，Z 表示分组中的模板数量。点击可以进入 分组详细列表 。
设置	点击 < 编辑 > 按键，可以编辑分组名称。

新增分组

点击图 4-1 中的 < 新增 > 按键可以添加新条目，新增分组界面如下图所示，需要自定义**分组名称**。

图 4-2 新增分组界面



该界面包含一个输入框，用于输入“分组名称”，右侧标注“(1-32个字符)”。下方有两个按钮：“确定”和“取消”。

分组详细列表

点击**分组统计信息**项显示的内容，如图 4-1 所示的 [1/1,0](#)，可以进入该分组详细列表界面，如下图所示。

图 4-3 分组详细列表界面

'default'的分组详细列表

[回到分组](#)
[修改分组](#)
[固化](#)
[新增](#)
[删除](#)
[批量编辑](#)
[搜索](#)
[组内搜索](#)
[刷新](#)

<input type="checkbox"/>	序号	名称	型号	硬件版本	软件版本	MAC地址	状态	设置
<input type="checkbox"/>	1	TL-AP300I-DC-0000	TL-AP300I-DC	1.1	1.0.7	88-25-93-8C-84-5A	运行	

共 1 条，每页：10 条 | 当前：1/1 页，1~1 条 | [<](#) [1](#) [>](#)

分组中的表项分为 AP 条目和 AP 模板两种类型，以下分别进行说明。

- AP 条目：用于对 AP 进行参数设置和管理。当一个 AP 接入之后，就会创建与其对应的 AP 条目。AP 条目有固化和未固化的区别。
 - 未固化的 AP 条目：AP 下线或 AC 重启后将消失，并且除“固化”外不能进行任何操作。未固化的 AP 条目名称后会加注“**(未固化)**”字样。
 - 已固化的 AP 条目：除非用户手动删除，否则一直存在。能够进行修改配置、修改分组、修改对应射频口配置和绑定无线服务等操作。
- AP 模板：用于设定某种硬件型号的 AP 的参数默认值，一种型号的 AP 只允许创建一个模板。当 AP 接入时，如果存在与其硬件型号匹配的 AP 模板，就会以其中的参数为默认值生成 AP 条目，且生成的 AP 条目位于模板所在的分组。AP 模板名称后会加注“**(模板)**”字样。

可以在此管理分组中的 AP 条目和 AP 模板，还可以对已有条目进行操作，下面对部分操作进行说明。

表 4-2 操作说明

修改分组	将表项移动到其他分组。不能移动未固化的 AP 条目。
------	----------------------------

固化

固化操作。只能对未固化的 AP 条目执行本操作。

点击图 4-3 中的 < 新增 > 按键可以添加新条目，新增 AP 条目界面如下图所示，新增 AP 模板界面与其类似，不单独介绍。

图 4-4 新增 AP 条目界面

名称:	<input type="text"/>	(1-50个字符)
型号:	<input type="text"/>	
硬件版本:	<input type="text"/>	
条目类型:	AP条目	
MAC地址:	<input type="text"/>	
AP保活时间:	30	(20-80秒)
客户端保活时间:	10	(3-1800秒)
客户端闲置时间:	3600	(60-86400秒)
AP离线自管理:	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭	
controller管理用户名:	admin	(1-31个字符)
controller管理密码:	tplink	(6-15个字符)
<input type="button" value="确定"/> <input type="button" value="取消"/>		

表 4-3 新增 AP 条目界面项说明

名称	<p>设置 AP 名称，方便用户识别和管理。</p> <p>新 AP 接入时产生的 AP 条目的名称格式为“X-NNNN”（X 为型号名或匹配的模板名，N 为数字且四位数字唯一）。为防止冲突，不允许用户自己配置的名称以“-NNNN(N 为数字)”的形式结尾。对于 HDAP 类型的 AP，其内部的两台 AP 会自动在名称末尾添加后缀名以进行区分，且后缀名不可编辑。当修改 HDAP 内部的某一台 AP 名称时，其修改也会同步到另一台 AP 上。</p>
型号	选择 AP 的硬件型号。
硬件版本	选择 AP 的硬件版本号。
条目类型	选择条目类型。
MAC 地址	AP 的 MAC 地址。不允许出现两条具有相同 MAC 地址的 AP 条目。此项仅 AP 条目可设，AP 模板不可设。
AP 保活时间	<p>设置 AP 的保活时间间隔。</p> <p>AP 与 AC 之间采用保活机制来确认隧道是否正常工作。正常情况下，AP 周期性发送回声请求（Echo Request）报文给 AC，AC 收到后发送回声应答（Echo Response）报文给 AP。如果 AC 在本端的 6 倍保活时间内没有收到回声请求，或者 AP 在自己的 6 倍保活时间内没有收到 AC 的回声应答，则 AC/AP 会主动断开连接。</p>

客户端保活时间	<p>设置客户端保活时间间隔。</p> <p>客户端保活机制用于检测客户端的异常下线。正常情况下，客户端下线时会向 AC 发送解关联报文，AC 收到之后就会删除客户端信息。如果客户端由于电源故障等原因异常下线就无法通知 AC，客户端的信息就会残留在 AC 的内存中，降低 AC 性能。因此，AP 会主动探测客户端是否存在，如果在保活时间内没有收到客户端的回复，就会通知 AC 删除客户端信息。</p>
客户端闲置时间	<p>AP 与客户端之间连接允许的最大闲置时间。如果 AP 在闲置时间内没有收到来自客户端的数据，那么该客户端将被删除。</p>
AP 离线自管理	<p>启用 AP 离线自管理，则即使该 AP 与 AC 的连接中断，也仍然可以接受新客户端的接入请求，但是该 AP 上配置的所有 Portal 认证条目将会失效。</p>
controller 管理用户名 /controller 管理密码	<p>设置 AP controller 管理软件的用户名和密码。在 AP 与 AC 关联以后，如果 AP 接受管理软件管理，需要使用此用户名和密码登录 AP。</p>

部分机型除了上述设置项还有一些特有的设置项，如下表所示。

表 4-4 AP 条目界面补充项说明

MAC 地址 2	<p>只有 HDAP 机型 (如 TL-HDAP1800C-PoE) 会显示该项。</p> <p>HDAP 内部的右侧 AP 的 MAC 地址，其大小固定为“MAC 地址 +2”。</p>
有线 LAN 口 VLAN ID	<p>只有具备额外有线 LAN 口的机型 (如 TL-AP300I-PoE) 会显示该项。</p> <p>设置 AP 额外有线 LAN 口的 VLAN ID，空表示不设置。</p>
AP 端口汇聚	<p>只有支持此功能的机型会显示该项。(如 TL-HDAP1800C-PoE 在后缀名为“_01”的 AP 中显示)</p> <p>将 AP 的多个物理端口绑定为一个逻辑端口来工作，以提高带宽。</p>

4.2 AP 升级

可以在此界面升级指定型号的 AP 软件版本。

进入界面：AP 管理 >> AP 升级 >> AP 升级

图 4-5 AP 升级界面

The screenshot shows the 'AP Upgrade' interface. At the top, there is a 'Version Upgrade Settings' section with a 'Upgrade Switch' set to 'Enabled' (radio button selected) and a 'Settings' button. Below this is the 'AP Version List' section, which contains a table with 10 columns: 'Serial Number', 'AP Model', 'Current Hardware Version', 'Current Software Version', 'Upgrade Start Time', 'Upgrade Progress', 'Upgrade Failure', 'Upgrade Status', and 'Software Management'. The table lists various AP models like TL-AP300C-PoE, TL-AP450C-PoE, etc. At the bottom right, there is a pagination bar showing 'Total 44 items, 10 items per page, current page 1/5, 1~10 items' and navigation buttons.

序号	AP型号	当前硬件版本	当前软件版本	升级开始时间	升级进度	升级失败	升级状态	软件管理
1	TL-AP300C-PoE	1.0/2.0/1.1/2.1	---	---	---	---	---	导入 删除
2	TL-AP450C-PoE	1.0/2.0/1.1/2.1	---	---	---	---	---	导入 删除
3	TL-AP600C-PoE	1.0/1.1	---	---	---	---	---	导入 删除
4	TL-AP1750C-PoE	1.0/1.1	---	---	---	---	---	导入 删除
5	TL-AP300I-PoE	1.0/1.1	---	---	---	---	---	导入 删除
6	TL-AP300I-DC	1.0/1.1	---	---	---	---	---	导入 删除
7	TL-AP300D	1.0/1.1	---	---	---	---	---	导入 删除
8	TL-AP450D	1.0/1.1	---	---	---	---	---	导入 删除
9	TL-AP300P	1.0/1.1	---	---	---	---	---	导入 删除
10	TL-AP451C	1.0/1.1	---	---	---	---	---	导入 删除

共44条， 每页： 10 条 | 当前： 1/5页， 1~10条 |
 < 1 2 3 4 5 >

版本升级设置

选择“启用”升级开关，并导入正确的升级软件和设置升级开始时间后，接入的 AP 将在到达升级时间后开始升级；“禁用”升级开关，还未开始升级的 AP 将会停止升级。

AP 版本列表

表 4-5 AP 升级界面项说明

AP 型号	显示 AP 型号的名称。
当前硬件版本	显示支持的该型号的硬件版本。
当前软件版本	显示当前导入的升级软件的版本号，若未导入，则显示为“---”。

升级开始时间	当上级文件上传成功后，输入升级开始的时间，点击 < 确认 > 按键生效设置。当“升级开关”处于开启状态时，到达设定的时间，此型号的 AP 设备将使用导入的 AP 升级软件进行升级。
升级进度	显示当前升级的进度，X/Y/Z 表示当前检测到有 Z 台该型号的 AP，其中有 Y 台需要升级，X 台已经升级成功。点击可以查看各个 AP 当前的升级状态。
升级失败	显示当前升级失败的 AP 个数，点击可以查看详细日志信息。
升级状态	显示当前 AP 型号的升级状态。点击可以查看该型号下的 AP 的具体升级状态信息。 <ul style="list-style-type: none"> ▪ 无需升级：当前 AP 型号下没有 AP 需要升级。 ▪ 等待升级：当前 AP 型号下的 AP 在等到升级。 ▪ 正在升级：当前 AP 型号下有 AP 正在升级。 ▪ 升级完成：当前 AP 型号下的所有 AP 都升级完成。 ▪ 升级中止：当前 AP 型号导入升级软件并且设置升级时间，当没到到达升级时间关闭升级开关，则该 AP 型号进入升级中止状态，或者该 AP 型号正在升级但是还有 AP 在等待升级时关闭升级开关，则该 AP 型号下正在升级的 AP 升级完成后进入升级中止状态；在升级中止状态下，开启升级开关，该 AP 型号重新进入正在升级状态或升级等待状态。
软件管理	可以进行如下操作： <ul style="list-style-type: none"> ▪ 导入：将外部的 AP 软件导入到系统中。 ▪ 删除：将系统中的 AP 软件删除。

说明：

- “升级进度”以及“升级失败”参数在设备重启后会被清空。
- 备份链路不会对 AP 进行升级。

4.3 AP 数据库

可以通过本界面导入 AP 数据库。当出现无线控制器无法管理最新 AP 机型的情况时，需要导入最新的 AP 数据库文件，以便识别新型 AP 设备。

进入界面：AP 管理 >> AP 数据库 >> AP 数据库

图 4-6 导入 AP 数据库界面

AP数据库

导入AP数据库 ?

当前数据库版本: 1.0.1

AP数据库文件路径: 浏览

导入

TP-LINK 官网 (<http://www.tp-link.com.cn>) 会不定期更新无线控制器的 AP 数据库文件，可将升级文件下载保存到本地。登录无线控制器后进入**导入 AP 数据库**界面，单击 < 浏览 > 按键，选择保存路径下的升级文件，单击 < 导入 > 按键进行数据库文件导入。

4.4 负载均衡

负载均衡适用于高密度无线网络环境中，可以准确地在无线网络中平衡 AP 设备的负载，保证该环境中客户端的合理接入，保证每个 AP 的性能和带宽得到最合理的使用。

下面通过简单的例子介绍负载均衡的工作过程，应用拓扑见下图：

图 4-7 负载均衡应用场景



客户端处在两个 AP 可以共同覆盖的网络中，当客户端向设备 A 发出关联请求时，如果同时满足以下两个条件：

- 设备 A 上连接的客户端数已经达到或超过负载均衡设定的**接入最大值**（图中以 20 为例）；
- 客户端还处于其他 AP 的无线网络范围内，设备 A 与其中至少一台 AP 上的客户端数差值达到或超过负载均衡设定的**差值上限**（图中以 4 为例， $20 - 16 \geq 4$ ）。

由于负载均衡功能，AC 将会拒绝客户端接入设备 A，使用户自动连接其他负载较小的 AP。这样，可以避免少量 AP 设备负载过大影响无线网络整体的运行效果。

如果客户端反复向设备 A 发起关联请求，且被拒绝请求的次数超过负载均衡设定的**最大失败次数**，在这种情况下，设备 A 会认为客户端不能连接到其它任何的 AP，将会接受该客户端的关联请求。

如果客户端的信号强度低于负载均衡设置的**RSSI 门限**（RSSI, Received Signal Strength Indication, 接收的信号强度指示），此弱信号客户端将不会参与负载均衡的计算。

进入界面：AP 管理 >> 负载均衡 >> 负载均衡

图 4-8 负载均衡界面

负载均衡

启用负载均衡功能 ?

负载均衡功能: 启用 禁用

负载均衡设置

负载均衡模式: 会话

门限: 20 用户数 (2-40, 缺省值=20)

差值门限: 4 用户数 (1-8, 缺省值=4)

最大失败次数: 10 (1-100, 缺省值=10)

RSSI 门限: -75 (-95-0, 缺省值=-75)

设置

启用负载均衡功能

勾选“启用”可以启用负载均衡功能，点击 < 设置 > 按键，**负载均衡设置**区域内的设置将生效。

负载均衡设置

表 4-6 负载均衡界面项说明

负载均衡模式	选择负载均衡模式。 会话模式：该模式使每一个 AP 分配的连接用户数尽可能平均。
门限	设定 AP 设备允许连接的最大客户端数目。当门限条件和差值门限条件均满足时，负载均衡会拒绝客户端接入此 AP。
差值门限	设定当前 AP 设备连接的客户端数目和其他 AP 连接的客户端数目之间的最大差值。当门限条件和差值门限条件均满足时，负载均衡会拒绝客户端接入此 AP。
最大失败次数	设定客户端尝试连接的最大失败次数。当被拒绝接入的客户端尝试连接此 AP 的次数超过最大失败次数时，AP 将会允许客户端接入。
RSSI 门限	设定参与负载均衡计算的客户端最小信号强度。忽略 RSSI 值低于 RSSI 门限的客户端，不将此客户端参与负载均衡的计算。

5 射频管理

5.1 射频设置

可以通过本界面查看 AP 射频的主要参数。

进入界面：射频管理 >> 射频设置 >> 射频设置

图 5-1 射频设置界面



列表中只显示选中分组下的 AP 的射频信息。点击列表设置栏中的 按钮可以编辑对应条目，编辑射频界面如下图所示。

图 5-2 编辑射频界面

AP名称:	TL-AP300I-DC-0000	(1-50个字符)
射频单元:	2.4GHz	
射频模式:	802.11b/g/n	
频段带宽:	自动	
信道:	自动	
动态信道切换 (DCS):	自动	
客户端在线切换:	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	
检查周期:	8	(3-180分钟, 默认值=8)
信道占用率门限:	50	(1-100, 默认值=50)
容限系数:	20	(1-45, 默认值=20)
发射功率:	Lv5	
关联最大用户数:	100	(1-100个用户)
天线:	内置天线	
分片门限:	2346	(必须是偶数, 256-2346字节)
beacon间隔:	100	(40-1000TU)
Airtime调度:	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	
RTS门限:	2346	(1-2347字节)
DTIM周期:	1	(1-255)
WMM:	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
响应广播探测:	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
Short GI:	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
弱信号限制:	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	
弱信号踢除:	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	
<input type="button" value="确定"/> <input type="button" value="取消"/> <input type="button" value="恢复缺省"/>		

表 5-1 编辑射频界面项说明

AP 名称	显示当前需要设置参数的 AP 名称。不可修改。
射频单元	显示当前需要设置参数的 AP 射频单元。不可修改。
射频模式	设置 AP 射频单元的工作模式。
频带带宽	当射频模式支持 11n 或者 11ac 时, 可设置频带带宽。
信道	以无线信号作为传输媒体的数据信号传送的通道。若选“自动”, 则设备会根据周围的环境自动选择一个合适的信道。
动态信道切换 (DCS)	<p>当信道设置为“自动”时方可配置。可选项有自动、手动和关闭。</p> <ul style="list-style-type: none"> 自动模式会在当前信道环境较差时自动切换到最优信道 (默认需 AP 处于无客户端连接状态才会切换)。 手动模式点击 < 重选信道 > 按钮可立即切换到最优信道 (无论是否有客户端连接)。 关闭时不会自动切换信道。

客户端在线切换	当 动态信道切换 (DCS) 设置为“自动”时方可配置。勾选此项后, AP 在有客户端连接时也会立即执行动态信道切换, 这将导致无线客户端断线重连, 影响用户使用, 请谨慎勾选。
检查周期	当 动态信道切换 (DCS) 设置为“自动”时方可配置。检查无线信道环境的周期。若发现当前信道环境较差, 则在检查周期到达时会触发信道切换。
信道占用率门限	当 动态信道切换 (DCS) 设置为“自动”时方可配置。信道占用率门限值。超过该值即认为当前信道环境较差。
容限系数	当 动态信道切换 (DCS) 设置为“自动”时方可配置。信道质量提升的门限值。高于该门限才会真正切换到新信道。
发射功率	设置 AP 射频单元的最大发射功率。
关联最大用户数	设置可以接入该 AP 射频单元的客户端的最大数目。
天线	设置 AP 射频单元的天线模式。
分片门限	当射频模式不含 11n 或者 11ac 时, 可设置无线帧数据包的分片门限, 此数值必须为偶数。 当数据包的长度超过分片门限时, 会被自动分成多个数据包。过多的数据包将会导致网络性能降低, 所以分片门限不应设置过低。
beacon 间隔	beacon 帧是设备的广播包, 用于发布设备支持的 SSID 无线网络。无线客户端通过收到的 beacon 帧判断该 SSID 是否还存在, 如果长时间都没有收到该 SSID 的 beacon 帧, 则客户端可以认为该 SSID 已经不存在, 客户端就会自动断开与该 SSID 的连接, 从而实现无线网络连接同步。 beacon 间隔表示设备发送 beacon 广播的实际间隔。单位: TU(Time Unit), 1TU=1024 微秒。
Airtime 调度	启用或禁用 Airtime 调度算法。
RTS 门限	启用 RTS (Request To Send, 要求发送) 机制所要求的无线帧的长度门限值。当无线帧长度超过该门限值时, 启用 RTS 机制。设置为 2347 表示关闭 RTS 功能。
DTIM 周期	设置信标的 DTIM 周期 (Delivery Traffic Indication Message, 数据待传指示信息)。
WMM	当射频模式不含 11n 或者 11ac 时, 可设置此项。 当射频模式支持 11n 或者 11ac 时, 此项不可设置, 且强制开启。 选择“启用”WMM 后, 设备具有无线服务质量功能, 可以对音频、视频数据优先处理, 保证音频、视频数据的优先传输。
响应广播探测	选择“启用”响应广播探测, AP 会响应客户端的广播探测请求。
Short GI	当射频模式支持 11n 或者 11ac 时, 可设置此项。 当射频模式不含 11n 或者 11ac 时, 此项不可设置, 且强制关闭。 选择“启用”Short GI (Short Guard Interval, 短保护间隔), 可以使设备接收和发送短帧间隔数据包, 提高设备的传输速率。

弱信号限制	选择“启用”弱信号限制，在右侧的文本框中输入客户端信号强度门限，可以禁止低于设置门限的客户端接入该无线网络。
弱信号踢除	选择“启用”弱信号踢除，在右侧的文本框中输入客户端信号强度门限，当客户端的信号强度低于设置门限时，踢除此客户端。

**说明：**

- 某些 AP 机型可能不支持动态信道切换（DCS）和 Airtime 调度的相关功能。
- 某些 AP 机型可能不支持 5GHz 的 BAND1 信道（36、40、44、48），即使可以设置为 BAND1 信道，但实际不生效，生效的信道可在 **AP 状态** 界面查看，界面进入方法：**系统状态 >> AP 状态 >> AP 状态**；
- 5GHz 射频单元下，只有在**频带带宽**设为 20MHz 时，才支持 165 信道；
- HDAP 机型两台 AP 的射频参数可能会联动变化。

5.2 速率设置

可以在此界面设置无线速率。

进入界面：射频管理 >> 速率设置 >> 速率设置

图 5-3 速率设置界面

速率设置
?

802.11a

强制速率： 6 9 12 18 24 36 48 54

支持速率： 6 9 12 18 24 36 48 54

组播速率： 6 9 12 18 24 36 48 54 自动

802.11b

强制速率： 1 2 5.5 11

支持速率： 1 2 5.5 11

组播速率： 1 2 5.5 11 自动

802.11g

强制速率： 1 2 5.5 6 9 11 12 18 24
 36 48 54

支持速率： 1 2 5.5 6 9 11 12 18 24
 36 48 54

组播速率： 1 2 5.5 6 9 11 12 18 24
 36 48 54 自动

802.11n

基本MCS索引：

支持MCS索引：

802.11ac

基本MCS集合：

支持MCS集合：

注意：

1. 对于已接入无线控制器的AP，如果开启了射频，需要重启AP或关闭再开启射频，设置的速率参数才会生效。
2. 如果11n的MCS索引值大于AP支持的最大值，则该AP的MCS索引生效值即为该AP支持的最大MCS索引值。

表 5-2 速率设置界面项说明

802.11a	<ul style="list-style-type: none"> 强制速率：客户端允许接入无线网络的基本速率集合，集合中至少设置一种速率，缺省值为 6Mbps、12 Mbps 和 24Mbps。 支持速率：扩展速率集合，该集合不能与强制速率集合有交集，缺省值为 9Mbps、18Mbps、36Mbps、48Mbps 和 54Mbps。 组播速率：用于发送多播报文的速率，该速率必须从强制速率集合中选取，设置为“自动”时，系统自动从强制速率集合中选取。
802.11b	<ul style="list-style-type: none"> 强制速率：客户端允许接入无线网络的基本速率集合，集合中至少设置一种速率，缺省值为 1Mbps 和 2Mbps。 支持速率：扩展速率集合，该集合不能与强制速率集合有交集，缺省值为 5.5Mbps 和 11Mbps。 组播速率：用于发送多播报文的速率，该速率必须从强制速率集合中选取，设置为“自动”时，系统自动从强制速率集合中选取。
802.11g	<ul style="list-style-type: none"> 强制速率：客户端允许接入无线网络的基本速率集合，集合中至少设置一种速率，缺省值为 1Mbps、2Mbps、5.5Mbps 和 11Mbps。 支持速率：扩展速率集合，该集合不能与强制速率集合有交集，缺省值为 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps 和 54Mbps。 组播速率：用于发送多播报文的速率，该速率必须从强制速率集合中选取，设置为“自动”时，系统自动从强制速率集合中选取。
802.11n	<ul style="list-style-type: none"> 基本 MCS 索引：客户端支持的最大 MCS 索引必须不小于该“基本 MCS 索引”值才能接入无线网络。缺省值为空。如果该值不为空，则非 11n 客户端不能接入 AP。 支持 MCS 索引：扩展 MCS 索引，该值不能小于“基本 MCS 索引”。
802.11ac	<ul style="list-style-type: none"> 基本 MCS 集合：客户端必须支持“基本 MCS 集合”对应的天线数和 MCS 索引范围，才能接入无线网络。缺省为空。如果该值不为空，则非 11ac 客户端不能接入 AP。 支持 MCS 集合：扩展 MCS 集合，该集合对应的天线数和 MCS 索引范围不能小于“基本 MCS 集合”对应的天线数和 MCS 索引范围。

说明：

- 对于已接入无线控制器的 AP，如果开启了射频，需要重启 AP 或关闭再开启射频，设置的速率参数才会生效。
- 如果 11n 的 MCS 索引值大于 AP 支持的最大值，则该 AP 的 MCS 索引生效值即为该 AP 支持的最大 MCS 索引值。

5.3 频谱导航

在实际无线网络环境中，某些客户端只能工作在 2.4G 频段上，也有一部分客户端可以同时支持 2.4G 和 5G 频段，如果支持双频的客户端都工作在 2.4G 频段上，会导致 2.4G 频段过载，5G 频段相对空余。为了避免频段资源的浪费，可以在设备上开启频谱导航功能。频谱导航功

能可以将支持双频工作的客户端优先接入 5G 频段，使得两个频段上的客户端数量相对均衡，从而提高整体网络性能。

下面通过简单的例子介绍频谱导航的工作过程，应用拓扑见下图：

图 5-4 频谱导航应用场景



一台双频 AP 的 2.4G 频段和 5G 频段 SSID 相同，当客户端向 AP 发起关联请求时：若客户端只支持单频 2.4G，则频谱导航功能不生效，客户端直接关联到 2.4G 频段上；若客户端支持双频，AP 则会将客户端优先引导至 5G 频段上；若客户端只支持单频 5G，则会直接关联到 5G 频段上。

当有新的支持双频的客户端想要连接到 AP 时，如果同时满足以下两个条件：

- AP 上 5G 频段连接的客户端数已经达到或超过频谱导航设定的**接入最大值**（图中以 40 为例）
- AP 上 5G 频段与 2.4G 频段上连接的客户端数差值达到或超过频谱导航设定的**差值上限**（图中以 4 为例， $40 - 36 \geq 4$ ）

由于频谱导航功能，AP 会拒绝客户端接入 5G 频段并允许客户端接入 2.4G 频段，即不会引导双频客户端优先接入 5G 频段。

如果客户端反复向 AP 的 5G 频段发起关联请求，且被拒绝请求的次数超过设定的**最大失败次数**，在这种情况下，AP 会认为客户端不能连接到 2.4G 频段，将会接受该客户端的 5G 频段关联请求。

进入界面：射频管理 >> 频谱导航 >> 频谱导航

图 5-5 频谱导航界面

频谱导航

启用频谱导航功能 ?

频谱导航: 启用 禁用

频谱导航设置

5G频段连接门限: 40 用户数(2-40)

差值门限: 4 用户数(1-8)

最大失败次数: 10 (0-100)

设置

启用频谱导航功能

勾选“启用”可以启用频谱导航功能，此时**频谱导航设置**区域内的设置生效。启用该功能时，请确保 2.4GHz 和 5GHz 的 SSID 设置相同。


频谱导航设置

表 5-3 频谱导航界面项说明

5G 频段连接门限	设定 AP 设备下允许连接到 5G 频段的最大客户端数目。当 5G 频段连接门限条件和差值门限条件均满足时，频谱导航会拒绝客户端接入 5G 频段。
差值门限	设定 AP 设备下 5G 频段客户端数目和 2.4G 频段客户端数目的最大差值。当 5G 频段连接门限条件和差值门限条件均满足时，频谱导航会拒绝客户端接入 5G 频段。
最大失败次数	设定客户端尝试连接的最大失败次数。当被拒绝接入的客户端尝试连接 5G 频段的次数超过最大失败次数时，AP 将会允许客户端接入 5GHz 频段。

6 无线管理

6.1 无线服务

可以在此界面设置和查看无线服务，并将无线服务绑定到射频。点击 < 新增 > 按键可以添加新条目，点击 <  > 按键会进入射频绑定列表界面。

进入界面：无线管理 >> 无线服务 >> 无线服务设置

图 6-1 无线服务设置界面



<input type="checkbox"/>	序号	SSID	描述	安全选项	状态	射频绑定	设置
<input type="checkbox"/>	1	中文[UTF-8]	---	---	已启用 		 

共 1 条，每页：10 条 | 当前：1/1 页，1~1 条 | 

新增无线服务条目

点击 < 新增 > 按键可以添加新条目，新增无线服务界面如下图所示。

图 6-2 新增无线服务界面



状态： 启用 禁用

SSID： (1-32个字符)

编码方式：

描述： (1-50个字符，可选)

无线网络内部隔离： 启用 禁用

安全选项：

带宽控制： 启用 禁用

控制模式：

最大上行带宽： KBps (1-131072000)

最大下行带宽： KBps (1-131072000)

表 6-1 新增无线服务界面项说明

状态	设置无线服务条目是否生效。
SSID	<p>SSID (Service Set Identifier, 服务集标识), 是无线局域网用于身份验证的登录名, 只有通过身份验证的用户才可以访问本无线网络。为便于标识, SSID 的名称应该尽量具有唯一性。</p> <p>本产品 SSID 设置支持中文字符, 当输入的 SSID 包含中文时, 将出现编码方式选项, 可选择 UTF-8 或 GBK 编码格式。最长可支持 32 个英文字符, 16 个 GBK 或者 10 个 UTF-8 中文字符。</p> <p>当 SSID 包含中文字符时, 选择单一编码格式, 会由于不同客户端机型和系统上的差异, 出现某些客户端可能无法正常搜索和显示 SSID 的情况。建议用户在使用中文 SSID 时, 设置两个使用相同无线网络名称但采用不同编码格式的无线网络。</p>
描述	设置该条目的描述信息, 以方便管理和查找。
无线网络内部隔离	启用此项, 使连接到同一个无线网络的客户端实现隔离, 客户端之间不能互相通信。该功能不能跨 AP 生效, 即通过不同 AP 接入相同无线网络的客户端之间不能实现隔离。
安全选项	<p>设置该 SSID 的安全选项。如果不需要对无线网络加密, 能够让任意主机接入无线网络, 则可以选择“关闭安全选项”; 如果需要对无线网络加密, 请选择界面中两种安全类型中的一种进行无线安全设置。为保障网络安全, 推荐启用安全设置。</p> <p>本设备提供的安全类型有: WPA-PSK/WPA2-PSK 和 WPA/WPA2, 推荐使用 WPA-PSK/WPA2-PSK AES 加密方法。</p> <p>不同的安全类型下, 安全设置项不同, 下面将详细介绍。</p>
带宽控制	设置客户端带宽控制功能是否生效。
控制模式	<p>启用带宽控制后可设, 设置客户端带宽控制模式。</p> <p>共享模式: 所有客户端均分共享带宽控制值;</p> <p>独占模式: 所有客户端独占带宽控制值。</p>
最大上行带宽	启用 带宽控制 后可设, 设置客户端带宽控制的最大上行带宽。
最大下行带宽	启用 带宽控制 后可设, 设置客户端带宽控制的最大下行带宽。

安全选项中的 WPA-PSK/WPA2-PSK 和 WPA/WPA2 加密方式详细介绍如下：

1 WPA-PSK/WPA2-PSK

WPA-PSK/WPA2-PSK 安全类型是基于共享密钥的 WPA 模式，安全性很高，设置也比较简单，适合普通家庭用户和小型企业使用。

图 6-3 WPA-PSK/WPA2-PSK 设置界面

安全选项:	WPA-PSK/WPA2-PSK	▼
认证类型:	自动	▼
加密算法:	自动	▼
组密钥更新周期:	86400	(30-604800) 秒, 不更新则为0
PSK密码:		(8-64个字符)

表 6-2 WPA-PSK/WPA2-PSK 设置界面项说明

认证类型	该项用来选择系统采用的安全模式，即自动、WPA-PSK、WPA2-PSK。默认选项为自动，无线控制器会根据主机请求自动选择 WPA-PSK 或 WPA2-PSK 安全模式。
加密算法	<p>该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。以下为选项的详细介绍。</p> <p>自动：选择该项后，无线控制器将根据网卡端的加密方式自动选择 TKIP 或 AES 加密方式。</p> <p>TKIP（Temporal Key Integrity Protocol，暂时密钥集成协议）：负责处理无线安全问题的加密部分。</p> <p>AES（Advanced Encryption Standard，高级加密标准）：是美国国家标准与技术研究所用于加密电子数据的规范。该算法汇聚了设计简单、密钥安装快、需要的内存空间少、在所有的平台上运行良好、支持并行处理并且可以抵抗所有已知攻击等优点。</p>
组密钥更新周期	该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为 30，若该值为 0，则表示不进行更新。
PSK 密码	该项是 WPA-PSK/WPA2-PSK 的初始设置密钥，设置时，要求为 8-63 个 ASCII 字符或 8-64 个十六进制字符。

2 WPA/WPA2

WPA/WPA2 是采用 Radius 服务器进行身份认证并得到密钥的 WPA 或 WPA2 安全模式。由于要架设一台专用的认证服务器，代价比较昂贵且维护也很复杂，所以在无线网络规模较小时不推荐使用此安全类型。

图 6-4 WPA/WPA2 设置界面

安全选项:	WPA/WPA2	▼
认证类型:	自动	▼
加密算法:	自动	▼
组密钥更新周期:	86400	(30-604800) 秒, 不更新则为0
Radius服务器IP:		
Radius端口:		(1024-65535)
Radius密码:		(1-64个英文字符)

表 6-3 WPA/WPA2 设置界面项说明

认证类型	该项用来选择系统采用的安全模式，即自动、WPA、WPA2。默认选项为自动，选择该项后，无线控制器会根据主机请求自动选择 WPA 或 WPA2 安全模式。
加密算法	<p>该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。以下为选项的详细介绍。</p> <p>自动：选择该项后，无线控制器将根据网卡端的加密方式自动选择 TKIP 或 AES 加密方式。</p> <p>TKIP（Temporal Key Integrity Protocol，暂时密钥集成协议）：负责处理无线安全问题的加密部分。</p> <p>AES（Advanced Encryption Standard，高级加密标准）：是美国国家标准与技术研究所用于加密电子数据的规范。该算法汇聚了设计简单、密钥安装快、需要的内存空间少、在所有的平台上运行良好、支持并行处理并且可以抵抗所有已知攻击等优点。</p>
组密钥更新周期	该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为 30，若该值为 0，则表示不进行更新。
Radius 服务器 IP	Radius 服务器用来对无线网络内的主机进行身份认证，此项用来设置该服务器的 IP 地址。
Radius 端口	Radius 服务器用来对无线网络内的主机进行身份认证，此项用来设置该 Radius 认证服务采用的端口号。
Radius 密码	该项用来设置访问 Radius 服务的密码。

说明:

- 无线网络内的主机若想连接该无线控制器，其无线参数必须与此处设置一致。
- 802.11n 不支持 TKIP 算法，如果在 11n 模式下使用 TKIP 加密会导致 STA 无法正常接入，而在 11b/g/n 模式下使用 TKIP 加密算法，传输速率只能达到 54Mbps。TKIP 是 WPA-PSK/WPA2-PSK 和 WPA/WPA2 加密方式中加密算法的选项。

射频绑定列表


新增的条目将出现在列表中，点击 <  > 按键会进入射频绑定列表界面，如下图所示。

图 6-5 射频绑定列表界面



The screenshot shows the 'Radio Binding List' interface. At the top, there are tabs for 'Wireless Service Settings' and 'Wireless Service Management'. Below the tabs, there are configuration fields for SSID (set to '中文[UTF-8]'), Select AP Group (set to 'default'), and Bind VLAN (set to '(1-4094, optional)'). There are also navigation buttons: 'Return to Wireless Service', 'Bind', 'Cancel Binding', 'Search', and 'Global Search'. The main part of the interface is a table with the following data:




<input type="checkbox"/>	序号	AP名称	射频单元	射频模式	绑定状态	绑定VLAN
<input type="checkbox"/>	1	TL-AP300I-DC-0000	1(2.4GHz)	802.11b/g/n	未绑定	---

At the bottom right, there is a pagination control: '共 1 条, 每页: 10 条 | 当前: 1/1 页, 1~1 条 |' with navigation arrows.

表 6-4 射频绑定列表界面项说明

SSID	显示当前执行射频绑定操作的无线网络名称。
选择 AP 分组	列表中只显示选中分组下的 AP 的射频信息。
绑定 VLAN	设置 VLAN ID。

表 6-5 射频绑定列表界面项操作说明

 绑定	勾选条目后，点击此按钮，可以把对应无线服务绑定到 AP 的射频上。 未固化的 AP，不允许执行绑定操作。固化操作：请至 AP 管理 >> AP 设置 >> AP 设置 界面，勾选“自动固化”。
 取消绑定	勾选条目后，点击此按钮，可以从 AP 射频上取消无线服务的绑定关系。
 返回无线服务	点击此按钮，将返回到无线服务界面。

7 认证管理

7.1 MAC 认证

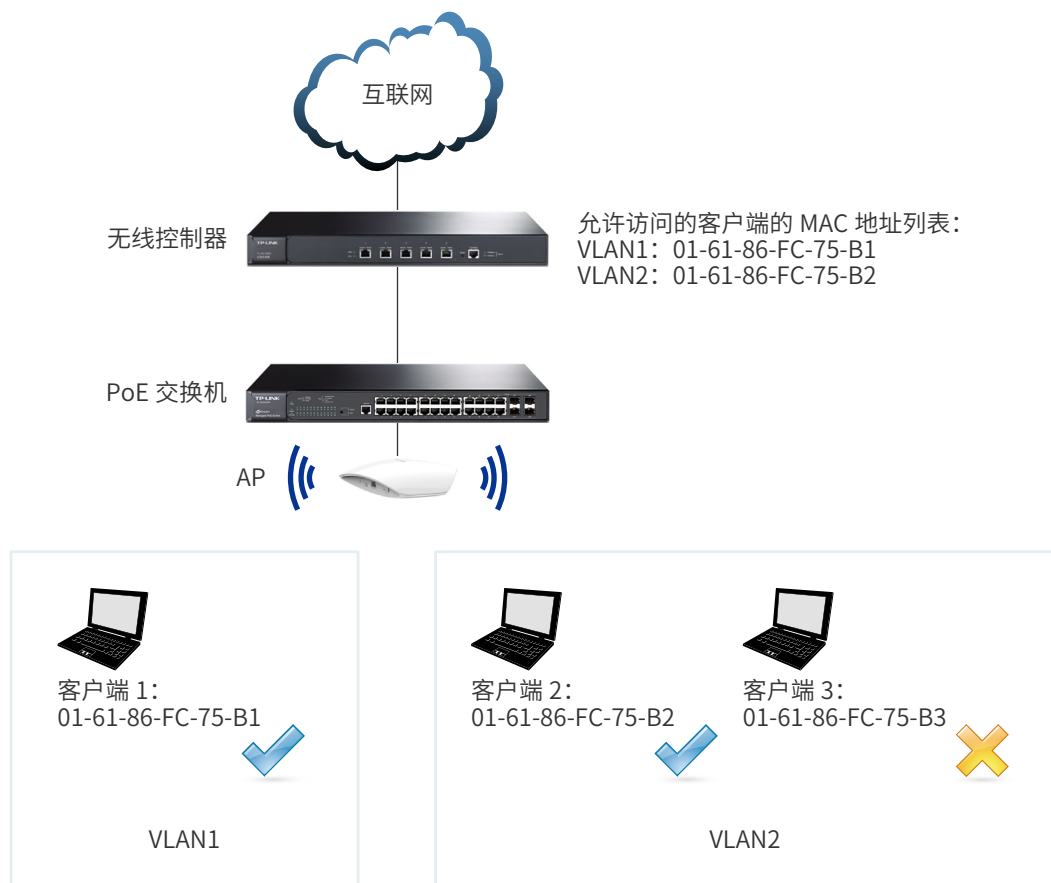
MAC 认证简介

MAC 认证是一种基于 VLAN 和 MAC 地址的认证方法，设备通过对用户 MAC 地址分组来管理用户的网络访问权限。

在无线网络应用中，MAC 认证需要预先获知允许访问无线网络的客户端的 MAC 地址。设备在首次检测到用户的 MAC 地址以后，立即启动对该用户的认证操作。用户无需安装任何客户端软件，认证过程中，用户也不需要进行任何操作。

无线控制器提供 MAC 认证功能，可以直接在设备上完成对用户的认证，认证拓扑如下图所示：

图 7-1 MAC 认证拓扑图



网络管理员预先在设备中配置允许访问网络的客户端的 MAC 地址，则当客户端请求接入网络时，只有存在于设备“允许访问的客户端的 MAC 地址列表”中的用户才可以认证，其他用户将被拒绝接入该网络。

配置 MAC 认证步骤

- 1) 设置允许通过认证的客户端的 MAC 地址。必须操作。配置界面：认证管理 >> MAC 认证 >> MAC 地址。
- 2) 创建应用 MAC 认证的认证服务。必须操作。配置界面：认证管理 >> MAC 认证 >> MAC 认证。

7.1.1 MAC 地址

可以通过本界面设置和查看允许通过认证的客户端的 MAC 地址。

进入界面：认证管理 >> MAC 认证 >> MAC 地址

图 7-2 MAC 地址界面

MAC认证 MAC地址

备份MAC地址信息 ?

备份

导入MAC地址信息

文件路径: 浏览

导入

注意：使用Excel软件打开csv文件时可能造成部分数值格式变化，从而显示不正确。如果使用Excel编辑csv文件，请设置单元格为文本格式。

MAC地址列表

+ 新增 - 删除 搜索 全局搜索

<input type="checkbox"/>	序号	名称	MAC地址	生效VLAN范围	设置
<input type="checkbox"/>	--	--	--	--	--

共0条, 每页: 10 条 | 当前: 0/0页, 0~0条 |

注意：生效VLAN范围中用0标识空VLAN，即当前所配置的MAC地址条目可在空VLAN中生效。若生效VLAN范围输入为空或者只输入0，则表示MAC地址只在空VLAN中生效。

备份 MAC 地址信息

点击 < 备份 > 按键可以备份所有的 MAC 地址条目至 ANSI 编码格式的 CSV 文件中。备份的文件可直接通过“导入 MAC 地址信息”功能重新添加到 MAC 地址列表中。

导入 MAC 地址信息

一次性添加多个 MAC 地址条目配置方法：

- 1) 将需要设置的 MAC 地址条目存为一份合法的 ANSI 编码格式的 CSV 文件。可以通过“备份 MAC 地址信息”功能获取符合规则的 CSV 文件，以查看文件的正确格式。
- 2) 点击 < 浏览 > 按键选择文件路径，再点击 < 导入 > 按键导入该文件。

说明：

使用 Excel 软件打开 csv 文件时可能造成部分数值格式变化，从而显示不正确。如果使用 Excel 编辑 csv 文件，请设置单元格为文本格式。

合法的条目内容如下：

- MAC 地址不冲突、名称不冲突，插入该条目。
- MAC 地址冲突、名称不冲突，更新已有条目。
- MAC 地址冲突、名称冲突，更新已有条目。

不合法的条目内容如下：

- MAC 地址不冲突、名称冲突，不更新已有条目。

MAC 地址列表

在此区域，可以对已有条目进行操作。点击 <新增> 按键可以添加新条目，新增 MAC 地址条目界面如下图所示。

图 7-3 新增 MAC 地址界面



新增 MAC 地址界面包含以下输入项：

- 名称：(1-50个字符)
- MAC地址：(XX-XX-XX-XX-XX-XX)
- 生效VLAN范围：(0-4094，可选，支持数字、区间，可用英文逗号间隔)

界面底部有“确定”和“取消”两个按钮。

表 7-1 新增 MAC 地址界面项说明

名称	自定义客户端名称。
MAC 地址	设置客户端的 MAC 地址。
生效 VLAN 范围	<p>设置 MAC 地址生效的 VLAN 范围，不同 MAC 地址的生效 VLAN 范围可重复。可输入范围 0-4094。0 用于标识空 VLAN，即当前配置的 MAC 地址条目在空 VLAN 中生效。支持数字、区间，并可用英文逗号间隔。输入格式如下：</p> <p>1</p> <p>11-20</p> <p>1,3,5,4090-4094</p>

7.1.2 MAC 认证

可以通过本界面对允许通过认证的客户端的 MAC 地址进行分组设置。

进入界面：认证管理 >> MAC 认证 >> MAC 认证

图 7-4 MAC 认证界面



在此界面，可以对已有条目进行操作。点击 <新增> 按键可以添加新条目，新增 MAC 认证条目界面如下图所示。

图 7-5 新增 MAC 认证界面

MAC认证名称: (1-50个字符)

生效VLAN范围: (1-4094, 可选, 支持数字、区间, 可用英文逗号间隔)

备注: (1-50个字符, 可选)

认证类型: 白名单 黑名单

状态: 启用 禁用

表 7-2 新增 MAC 认证界面项说明

MAC 认证名称	设置 MAC 认证的名称，不能与已有 MAC 认证名称重复。
生效 VLAN 范围	设置 MAC 认证条目生效的 VLAN 范围，不同 MAC 认证条目的生效 VLAN 范围不能冲突，必须是唯一的。可输入范围 1-4094。支持数字、区间，并可用英文逗号间隔。输入格式如下： 1 11-20 1,3,5,4090-4094
备注	设置该条目的备注，以方便管理和查找。
认证类型	白名单：生效 VLAN 范围中的 MAC 地址允许接入。 黑名单：生效 VLAN 范围中的 MAC 地址禁止接入。
状态	选择“启用”，在指定的 VLAN 范围中开启 MAC 认证功能。 选择“禁用”，在指定的 VLAN 范围中关闭 MAC 认证功能。

7.2 Portal 认证

无线控制器提供 Portal 认证服务，包括 Web 认证、微信连 Wi-Fi、一键上网和远程 Portal 认证方式，以及跳转页面、免认证策略和认证参数相关功能。

说明：

在进行 Portal 认证的相关设置之前，请先确保无线控制器管理 AP 的接口 IP 地址与待认证客户端的 IP 地址之间路由可达。

7.2.1 跳转页面

在此可通过图片上传、外部链接或使用默认模板，为后续的 Web 认证等认证过程设置跳转页面，满足推送广告，推广微信公众号等需求。

进入界面：认证管理 >> Portal 认证 >> 跳转页面

图 7-6 跳转页面设置界面



在此界面，可以对已有条目进行操作，点击 < 新增 > 按键可以添加新条目。

新增跳转页面，需要选择**认证页面类型**，本设备提供四种认证页面类型：Web 认证、微信连 Wi-Fi、一键上网和 Web 认证 + 微信连 Wi-Fi。其中，Web 认证和一键上网跳转页面设置内容相同；微信连 Wi-Fi 和 Web 认证 + 微信连 Wi-Fi 跳转页面设置内容相同。

» Web 认证 / 一键上网

图 7-7 新增跳转页面 -Web 认证

跳转页面名称:	<input type="text"/>	(1-50个英文字符、数字、下划线或减号)
认证页面类型:	Web认证 ▼	
页面标题:	<input type="text"/>	(1-50个字符)
背景图片:	<input type="button" value="上传"/> ...	
欢迎信息:	<input type="text"/>	(1-26个字符)
版权声明:	<input type="text"/>	(1-50个字符)
备注:	<input type="text"/>	(1-50个字符, 可选)
页面预览:	<input type="button" value="预览跳转页面"/>	

注意:
1、当条目已经被引用后, 不能再修改跳转页面名称和认证页面类型。

图 7-8 新增跳转页面 - 一键上网

跳转页面名称:	<input type="text"/>	(1-50个英文字符、数字、下划线或减号)
认证页面类型:	一键上网 ▼	
页面标题:	<input type="text"/>	(1-50个字符)
背景图片:	<input type="button" value="上传"/> ...	
欢迎信息:	<input type="text"/>	(1-26个字符)
版权声明:	<input type="text"/>	(1-50个字符)
备注:	<input type="text"/>	(1-50个字符, 可选)
页面预览:	<input type="button" value="预览跳转页面"/>	

注意:
1、当条目已经被引用后, 不能再修改跳转页面名称和认证页面类型。

表 7-3 新增跳转页面 -Web 认证 / 一键上网界面项说明

跳转页面名称	自定义跳转页面名称。
认证页面类型	选择认证页面类型。
页面标题	设置跳转页面的标题内容。
背景图片	上传跳转页面的背景图片。
欢迎信息	设置跳转页面的欢迎信息。
版权声明	设置跳转页面的版权信息。
备注	设置条目的备注信息, 以方便管理和查找。
页面预览	点击按键可预览设置的跳转页面。

» 微信连 Wi-Fi/Web 认证 + 微信连 Wi-Fi

图 7-9 新增跳转页面 - 微信连 Wi-Fi

跳转页面名称:	<input type="text"/>	(1-50个英文字符、数字、下划线或减号)
认证页面类型:	微信连WIFI ▼	
页面标题:	<input type="text"/>	(1-50个字符)
背景图片:	<input type="button" value="上传"/> ---	
欢迎信息:	<input type="text"/>	(1-26个字符)
版权声明:	<input type="text"/>	(1-50个字符)
Logo图片:	<input type="button" value="上传"/> ---	
Logo信息:	<input type="text"/>	(1-25个字符, 可选)
登录按钮提示文字:	<input type="text"/>	(1-15个字符)
备注:	<input type="text"/>	(1-50个字符, 可选)
页面预览:	<input type="button" value="预览跳转页面"/>	

注意:
1、当条目已经被引用后, 不能再修改跳转页面名称和认证页面类型。

图 7-10 新增跳转页面 -Web 认证 + 微信连 Wi-Fi

跳转页面名称:	<input type="text"/>	(1-50个英文字符、数字、下划线或减号)
认证页面类型:	Web认证+微信连WIFI ▼	
页面标题:	<input type="text"/>	(1-50个字符)
背景图片:	<input type="button" value="上传"/> ---	
欢迎信息:	<input type="text"/>	(1-26个字符)
版权声明:	<input type="text"/>	(1-50个字符)
Logo图片:	<input type="button" value="上传"/> ---	
Logo信息:	<input type="text"/>	(1-25个字符, 可选)
登录按钮提示文字:	<input type="text"/>	(1-15个字符)
备注:	<input type="text"/>	(1-50个字符, 可选)
页面预览:	<input type="button" value="预览跳转页面"/>	

注意:
1、当条目已经被引用后, 不能再修改跳转页面名称和认证页面类型。

表 7-4 新增跳转页面 - 微信连 Wi-Fi/Web 认证 + 微信连 Wi-Fi 界面项说明

跳转页面名称	自定义跳转页面名称。
认证页面类型	选择认证页面类型。
页面标题	设置跳转页面的标题内容。

背景图片	上传跳转页面的背景图片。
欢迎信息	设置跳转页面的欢迎信息。
版权声明	设置跳转页面的版权信息。
Logo 图片	上传跳转页面的 Logo 图片。
Logo 信息	设置跳转页面的 Logo 信息。
登录按钮提示文字	设置跳转页面的登录按钮提示文字。
备注	设置条目的备注信息，以方便管理和查找。
页面预览	点击按键可预览设置的跳转页面。

7.2.2 Web 认证

Web 认证简介

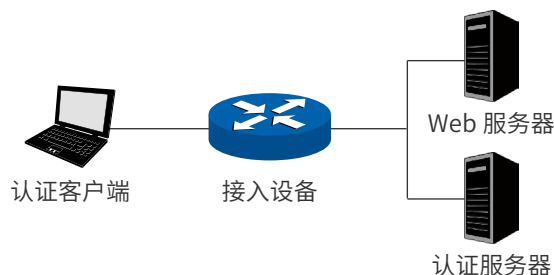
无线控制器提供 Web 认证功能，在采用 Web 认证的网络中，用户需要先登录认证页面，输入用户名和密码进行认证，认证成功后才可以访问网络资源。

用户主动访问预先设置的 Web 网站，这种认证方式称作主动认证。反之，如果用户试图通过 HTTP 访问其他网站，将被强制访问预先设置的 Web 网站，从而开始认证过程，这种认证方式称作强制认证。

Web 认证系统

Web 认证系统一般网络拓扑如下图所示：

图 7-11 Web 认证系统拓扑图



认证客户端

需要访问网络资源的未认证用户，将进行 Web 认证。

接入设备

宽带接入设备的统称，包括路由器、交换机和无线控制器等。主要作用有：

- 认证前，将用户的所有 HTTP 请求都重定向到 Web 服务器；

- 认证过程中，与认证服务器交互，完成用户的身份认证；
- 认证通过后，允许用户访问被管理员授权的网络资源。

Web 服务器

接收认证客户端的 Web 认证请求，提供基于 Web 认证的页面。Web 服务器可以是接入设备之外的独立实体，也可以是存在于接入设备之内的内嵌实体。

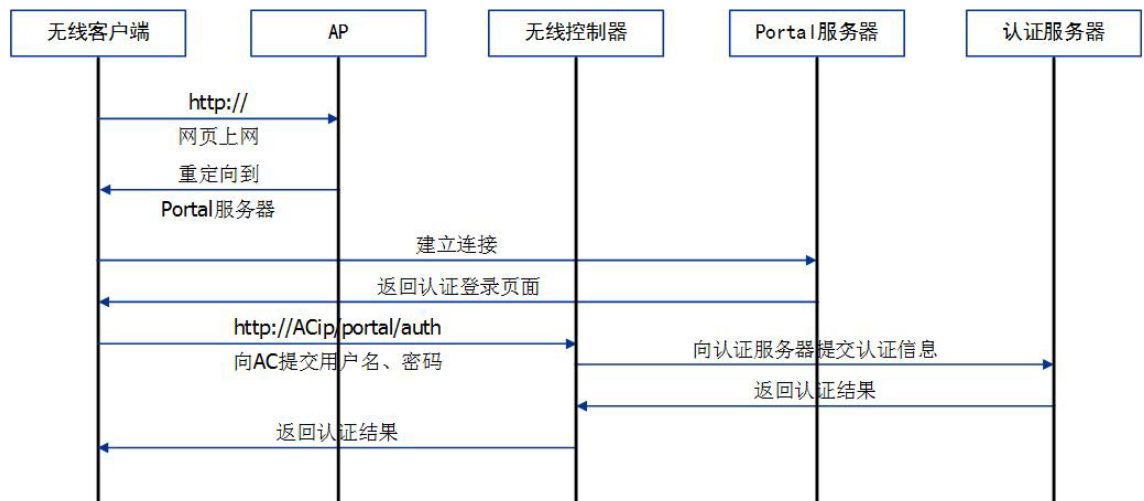
认证服务器

与接入设备进行交互，完成对用户的认证。认证服务器可以是接入设备之外的独立实体，也可以是存在于接入设备之内的内嵌实体。

Web 认证过程

Web 认证过程如下图所示：

图 7-12 Web 认证过程示意图



- 1) 认证客户端接入网络，未进行过认证，通过 HTTP 访问外网；
- 2) 接入设备返回重定向 URL，将认证客户端重定向到 Web 服务器；
- 3) 认证客户端访问 Web 服务器；
- 4) Web 服务器为认证客户端返回认证登录页面；
- 5) 认证客户端在认证登录页面输入用户名和密码，该信息将提交到接入设备；
- 6) 接入设备向认证服务器提交该用户的认证信息；
- 7) 认证服务器向接入设备返回认证结果；
- 8) 接入设备向认证客户端返回该认证结果。

Web 认证设置

可以通过本界面设置和查看 Web 认证相关内容。

进入界面：认证管理 >> Portal 认证 >> Web 认证

图 7-13 Web 认证界面



在此界面，可以对已有条目进行操作，点击 < 新增 > 按键可以添加新条目。

新增 Web 认证条目需要选择**认证服务器类型**，本设备提供两种认证服务器类型：本地服务器和远程服务器。

» 本地服务器

图 7-14 新增 Web 认证 - 本地服务器

状态： 启用 禁用

跳转页面名称：

VLAN ID： (1-4094, 可选)

认证服务器类型：

认证成功跳转链接：
(1-120个英文字符、数字或英文特殊字符, 可选)

认证失败跳转链接：
(1-120个英文字符、数字或英文特殊字符, 可选)

无感知认证： 开启 关闭

备注： (1-50个字符, 可选)

注意：
 1、如果配置了认证失败跳转链接，链接地址会自动加入免认证策略，无需用户配置。
 2、认证服务器类型为远程服务器时，若服务器配置了用户上网时间，则免费上网时长为服务器返回的时间，否则为本页面配置的免费上网时长。

表 7-5 新增 Web 认证 - 本地服务器界面项说明

状态	设置 Web 认证条目当前的启用状态。
----	---------------------

跳转页面名称	选择已经设置完成的 Web 认证的跳转页面模板。
VLAN ID	设置需要进行 Web 认证的 VLAN ID。
认证服务器类型	选择进行 Web 认证的服务器类型。
认证成功跳转链接	设置认证成功后跳转的 URL 地址。
认证失败跳转链接	设置认证失败后跳转的 URL 地址。如果配置了认证失败跳转链接，链接地址会自动加入免认证策略，无需用户配置。
无感知认证	若启用无感知认证，无感知认证用户再次接入 WLAN 时会自动进行认证。
备注	设置该条目的备注信息，以方便管理和查找。



说明：

当选择本地服务器认证时，需要在**用户管理**界面添加允许接入的用户的登录信息。具体设置方法请参考[用户管理](#)。

» 远程服务器

图 7-15 新增 Web 认证 - 远程服务器

状态： 启用 禁用

跳转页面名称：

VLAN ID： (1-4094，可选)

认证服务器类型：

认证服务器组：

免费上网时长： 分钟 (1-1440)

认证成功跳转链接：

(1-120个英文字符、数字或英文特殊字符，可选)

认证失败跳转链接：

(1-120个英文字符、数字或英文特殊字符，可选)

无感知认证： 开启 关闭

备注： (1-50个字符，可选)

注意：
 1、如果配置了认证失败跳转链接，链接地址会自动加入免认证策略，无需用户配置。
 2、认证服务器类型为远程服务器时，若服务器配置了用户上网时间，则免费上网时长为服务器返回的时间，否则为本页面配置的免费上网时长。

表 7-6 新增 Web 认证 – 远程服务器界面项说明

状态	设置 Web 认证条目当前的启用状态。
跳转页面名称	选择已经设置完成的 Web 认证的跳转页面模板。
VLAN ID	设置需要进行 Web 认证的 VLAN ID。
认证服务器类型	选择进行 Web 认证的服务器类型。
认证服务器组	选择进行 Web 认证的服务器组。服务器组具体设置方法请参考 认证服务器 。
免费上网时长	选择远程服务器进行认证时，若远程服务器配置了用户上网时间，则免费上网时长为服务器返回的时间；若远程服务器未进行相关设置，则为本页面配置的免费上网时长。
认证成功跳转链接	设置认证成功后跳转的 URL 地址。
认证失败跳转链接	设置认证失败后跳转的 URL 地址。如果配置了认证失败跳转链接，链接地址会自动加入免认证策略，无需用户配置。
无感知认证	若启用无感知认证，无感知认证用户再次接入 WLAN 时会自动进行认证。
备注	设置该条目的备注信息，以方便管理和查找。

7.2.3 微信连 Wi-Fi

无线控制器提供微信连 Wi-Fi 功能。商家可以根据需求对访问网络资源的用户进行认证，通过微信连 Wi-Fi 推广微信公众号并推送广告。

说明：

配置了微信连 Wi-Fi 认证的网络，需保证无线控制器可以访问互联网，无线客户端方能完成认证。

进入界面：认证管理 >> Portal 认证 >> 微信连 Wi-Fi

图 7-16 微信连 Wi-Fi 界面



在此界面，可以对已有条目进行操作，点击 < 新增 > 按键可以添加新条目，新增微信连 Wi-Fi 条目界面如下图所示。

图 7-17 新增微信连 Wi-Fi 界面

状态: 启用 禁用

跳转页面名称:

VLAN ID: (1-4094, 可选)

免费上网时长: 分钟 (1-1440)

ShopID: (1-32个数字或英文字母)

AppID: (1-32个数字或英文字母)

SecretKey: (1-32个数字或英文字母)

备注: (1-50个字符, 可选)

注意:
 1、配置了微信连WiFi认证条目，为了无线PC能够顺利完成认证，需要保证AC可以联网。
 2、微信公众号信息设置方法，请参阅：[微信连Wi-Fi功能使用指南](#)。

表 7-7 新增微信连 Wi-Fi 界面项说明

状态	设置微信连 Wi-Fi 认证条目当前的启用状态。
跳转页面名称	选择已经设置完成的微信连 Wi-Fi 认证的跳转页面模板。
VLAN ID	设置需要进行微信连 Wi-Fi 认证的 VLAN ID。
免费上网时长	设置微信连 Wi-Fi 认证用户可以免费上网的时长。
ShopID	设置微信连 Wi-Fi 门店 ID，可登陆微信公众号官网获取。
AppID	设置微信公众号 ID，可登陆微信公众号官网获取。
SecretKey	设置微信连 Wi-Fi 密钥，可登陆微信公众号官网获取。
备注	设置该条目的备注信息，以方便管理和查找。

7.2.4 一键上网

可以通过本界面设置和查看一键上网相关内容。

进入界面：认证管理 >> Portal 认证 >> 一键上网

图 7-18 一键上网界面



在此界面，可以对已有条目进行操作，点击 < 新增 > 按键可以添加新条目，新增一键上网条目界面如下图所示。

图 7-19 新增一键上网界面

表 7-8 新增一键上网界面项说明

状态	设置一键上网认证条目当前的启用状态。
跳转页面名称	选择已经设置完成的一键上网认证的跳转页面模板。
VLAN ID	设置需要进行一键上网认证的 VLAN ID。
免费上网时长	设置一键上网认证用户可以免费上网的时长。
备注	设置该条目的备注信息，以方便管理和查找。

7.2.5 远程 portal

可以通过本页面设置和查看远程 Portal 认证条目。

进入界面：认证管理 >> Portal 认证 >> 远程 Portal

图 7-20 远程 Portal 设置界面



在此界面，可以对已有条目进行操作，点击 < 新增 > 按键可以添加新条目。

新增远程 Portal 条目需要选择**认证服务器类型**，本设备提供两种认证服务器类型：本地服务器和远程服务器。

 说明：

使用远程 portal 认证时，用户需要自行提供远程 portal 认证页面。请参照 TP-LINK 官网 (<http://www.tp-link.com.cn/>) 提供的远程 portal 认证页面模板设计，或联系技术支持。

» 本地服务器

图 7-21 新增远程 Portal- 本地服务器

状态: 启用 禁用

跳转页面名称: (1-50个英文字符、数字、下划线或减号)

VLAN ID: (1-4094, 可选)

远程Portal地址:
(1-100个英文字符、数字或英文特殊字符)

认证服务器类型:

认证成功跳转链接:
(1-120个英文字符、数字或英文特殊字符, 可选)

认证失败跳转链接:
(1-120个英文字符、数字或英文特殊字符, 可选)

无感知认证: 开启 关闭

备注: (1-50个字符, 可选)

注意:
1、远程Portal地址和认证失败跳转链接会自动加入免认证策略, 无需用户配置。
2、认证服务器类型为远程服务器时, 若服务器配置了用户上网时间, 则免费上网时长为服务器返回的时间, 否则为本页面配置的免费上网时长。

表 7-9 新增远程 Portal- 本地服务器界面项说明

状态	设置远程 Portal 认证条目当前的启用状态。
跳转页面名称	自定义远程 Portal 认证的跳转页面模板名称。
VLAN ID	设置需要进行远程 Portal 认证的 VLAN ID。
远程 Portal 地址	输入远程 Portal 服务器的地址。该地址会自动加入免认证策略, 无需用户配置。
认证服务器类型	选择进行远程 Portal 认证的服务器类型。
认证成功跳转链接	设置认证成功后跳转的 URL 地址。
认证失败跳转链接	设置认证失败后跳转的 URL 地址。如果配置了认证失败跳转链接, 链接地址会自动加入免认证策略, 无需用户配置。
无感知认证	若启用无感知认证, 无感知认证用户再次接入 WLAN 时会自动进行认证。
备注	设置该条目的备注信息, 以方便管理和查找。

说明：

当选择本地服务器认证时，需要在**用户管理**界面添加允许接入的用户的登录信息。具体设置方法请参考[用户管理](#)。

» 远程服务器

图 7-22 新增远程 Portal- 远程服务器

状态：	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用	
跳转页面名称：	<input type="text"/>	(1-50个英文字符、数字、下划线或减号)
VLAN ID：	<input type="text"/>	(1-4094，可选)
远程Portal地址：	<input type="text"/>	(1-100个英文字符、数字或英文特殊字符)
认证服务器类型：	远程服务器	
认证服务器组：	---	
免费上网时长：	30	分钟 (1-1440)
认证成功跳转链接：	<input type="text"/>	(1-120个英文字符、数字或英文特殊字符，可选)
认证失败跳转链接：	<input type="text"/>	(1-120个英文字符、数字或英文特殊字符，可选)
无感知认证：	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭	
备注：	<input type="text"/>	(1-50个字符，可选)
<p>注意：</p> <p>1、远程Portal地址和认证失败跳转链接会自动加入免认证策略，无需用户配置。</p> <p>2、认证服务器类型为远程服务器时，若服务器配置了用户上网时间，则免费上网时长为服务器返回的时间，否则为本页面配置的免费上网时长。</p>		
<input type="button" value="确定"/> <input type="button" value="取消"/>		

表 7-10 新增远程 Portal- 远程服务器界面项说明

状态	设置远程 Portal 认证条目当前的启用状态。
跳转页面名称	自定义远程 Portal 认证的跳转页面模板名称。
VLAN ID	设置需要进行远程 Portal 认证的 VLAN ID。
远程 Portal 地址	输入远程 Portal 服务器的地址。该地址会自动加入免认证策略，无需用户配置。
认证服务器类型	选择进行远程 Portal 认证的服务器类型。
认证服务器组	选择进行远程 Portal 认证的服务器组。服务器组具体设置方法请参考 认证服务器 。

免费上网时长	选择远程服务器进行认证时，若远程服务器配置了用户上网时间，则免费上网时长为服务器返回的时间；若远程服务器未进行相关设置，则为本页面配置的免费上网时长。
认证成功跳转链接	设置认证成功后跳转的 URL 地址。
认证失败跳转链接	设置认证失败后跳转的 URL 地址。如果配置了认证失败跳转链接，链接地址会自动加入免认证策略，无需用户配置。
无感知认证	若启用无感知认证，无感知认证用户再次接入 WLAN 时会自动进行认证。
备注	设置该条目的备注信息，以方便管理和查找。

7.2.6 免认证策略

可以通过本界面设置和查看免认证策略。免认证策略可配置用户在 Portal 认证成功前能够免费访问的资源。

进入界面：认证管理 >> Portal 认证 >> 免认证策略

图 7-23 免认证策略界面

□	序号	策略名称	URL地址	源IP地址范围	目的IP地址范围	源端口	目的端口	服务协议	备注	状态	设置
--	1	dhcp client	---	---	---	68-68	67-67	UDP	---	已启用	---
--	2	dhcp server	---	---	---	67-67	68-68	UDP	---	已启用	---
--	3	dns client	---	---	---	---	53-53	UDP	---	已启用	---
--	4	dns server	---	---	---	53-53	---	UDP	---	已启用	---

在此界面，可以对已有条目进行操作。序号为 1-4 的条目是系统预定义的免认证策略，不可操作。点击 < 新增 > 按钮可以添加新条目。

新增免认证策略条目需要选择**匹配方式**，本设备支持两种匹配方式：五元组方式和 URL 方式。

» 五元组方式

主要依据 IP 地址范围、MAC 地址、VLAN ID、端口和服务协议设置策略，当需要限制的免认证参数种类较多时，推荐使用五元组方式。

图 7-24 免认证策略设置 - 五元组方式界面

策略名称:	<input type="text"/>	(1-50个字符)
匹配方式:	五元组方式	
源IP地址范围:	<input type="text"/> / <input type="text"/>	(可选)
源MAC地址:	<input type="text"/>	(XX-XX-XX-XX-XX-XX, 可选)
源VLAN:	<input type="text"/>	(1-4094, 可选)
源端口:	<input type="text"/> - <input type="text"/>	(1-65535, 可选)
目的IP地址范围:	<input type="text"/> / <input type="text"/>	(可选)
目的端口:	<input type="text"/> - <input type="text"/>	(1-65535, 可选)
服务协议:	UDP	
备注:	<input type="text"/>	(1-50个字符, 可选)
状态:	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
<p>注意:</p> <p>1、所有条件均为空的策略, 表示允许访问所有资源。</p> <p>2、仅当源端口或目的端口至少填写了一项, 服务协议才会生效。</p>		
<input type="button" value="确定"/>		<input type="button" value="取消"/>

表 7-11 新增五元组免认证策略界面项说明

策略名称	设置免认证策略的名称。
匹配方式	设置免认证策略的匹配方式。
源 IP 地址范围	设置免认证策略的源 IP 地址和网络掩码。
源 MAC 地址	设置免认证策略的源 MAC 地址。
源 VLAN	设置免认证策略的源 VLAN ID。
源端口	设置免认证策略的源端口范围。
目的 IP 地址范围	设置免认证策略的目的 IP 地址和网络掩码。
目的端口	设置免认证策略的目的端口范围。
服务协议	设置免认证策略的服务协议。仅当源端口或目的端口至少填写了一项, 服务协议才会生效。
备注	设置条目的备注, 以方便管理和查找。
状态	设置免认证策略是否生效。

» URL 方式

主要依据 URL 设置策略，当已知 URL 时，推荐使用 URL 方式。

图 7-25 免认证策略设置 -URL 方式界面

策略名称: (1-50个字符)

匹配方式:

URL地址: (1-128个字符)

源IP地址范围: / (可选)

源MAC地址: (XX-XX-XX-XX-XX-XX, 可选)

源VLAN: (1-4094, 可选)

备注: (1-50个字符, 可选)

状态: 启用 禁用

注意:
 1、所有条件均为空的策略，表示允许访问所有资源。
 2、仅当源端口或目的端口至少填写了一项，服务协议才会生效。

表 7-12 新增 URL 免认证策略界面项说明

策略名称	设置免认证策略的名称。
匹配方式	设置免认证策略的匹配方式。
URL 地址	选择 URL 免认证策略时，设置需要匹配的 URL 地址。
源 IP 地址范围	设置免认证策略的源 IP 地址和网络掩码。
源 MAC 地址	设置免认证策略的源 MAC 地址。
源 VLAN	设置免认证策略的源 VLAN ID。
备注	设置条目的备注，以方便管理和查找。
状态	设置免认证策略是否生效。



说明:

所有条件均为空的策略，表示允许访问所有资源。

7.2.7 认证参数

可以通过本界面设置和查看认证相关的全局参数。

进入界面：认证管理 >> Portal 认证 >> 认证参数

图 7-26 认证参数界面

表 7-13 认证参数界面项说明

认证老化 / 认证老化时间	勾选“认证老化”，可以设置认证老化时间。 当已认证客户端断开连接后，对应的认证条目的老化时间。客户端在老化时间内重新连接到 AP，不需要重新认证，超过老化时间后接入的客户端需要重新认证。
Portal 认证端口	用于 Portal 认证的服务端口，默认为 8080 端口。不能与其他的服务端口重复。

7.3 用户管理

可以在此界面设置无线控制器本地认证服务的用户身份信息。

进入界面：认证管理 >> 用户管理 >> 用户管理

图 7-27 用户管理界面

The screenshot shows the 'User Management' interface. At the top, there is a 'User Management' tab. Below it, there are three main sections: 'Backup User Information', 'Load User Information', and 'User Management Rule List'. The 'Backup User Information' section has a 'Backup' button. The 'Load User Information' section has a 'File:' input field, a 'Browse' button, and an 'Import' button. Below this is a note: '注意：使用Excel软件打开csv文件时可能造成部分数值格式变化，从而显示不正确。如果使用Excel编辑csv文件，请设置单元格为文本格式。' The 'User Management Rule List' section has a table with columns: '序号', '用户类型', '用户名', '有效期/上网时长', '免费时长', 'MAC地址', '备注', '状态', and '设置'. Above the table are icons for '启用', '禁用', '新增', '删除', '搜索', and '全局搜索'. Below the table is a pagination bar: '共0条，每页：10条 | 当前：0/0页，0~0条 |' with navigation arrows.

备份用户信息

点击 < 备份 > 按钮可以备份所有的本地用户条目至 ANSI 编码格式的 CSV 文件中。备份的文件可直接通过“加载用户信息”功能重新添加到用户列表中。

加载用户信息

一次性导入多个本地用户条目配置方法：

- 1) 将需要设置的用户条目存为一份合法的 ANSI 编码格式的 CSV 文件。可以通过“备份用户信息”功能获取符合规则的 CSV 文件，以查看文件的正确格式。
- 2) 点击 < 浏览 > 按钮选择文件路径，再点击 < 导入 > 按钮导入该文件。

说明：

使用 Excel 软件打开 csv 文件时可能造成部分数值格式变化，从而显示不正确。如果使用 Excel 编辑 csv 文件，请设置单元格为文本格式。

用户管理规则列表

在此区域，可以对已有条目进行操作，点击 < 新增 > 按键可以添加新条目，**用户类型**分为正式用户和免费用户。

» 正式用户

给用户提供连续自然天的上网服务，当账户有效期到期后，该账户无效。

图 7-28 新增正式用户界面

表 7-14 新增正式用户界面项说明

用户名	自定义用户名，不能与已有用户名重复。
密码	新增用户时，需要输入密码。修改用户配置时，可以输入新密码，不输入则表示不修改。
有效期 / 上网时长	设置账户有效的截止日期。
允许认证时间段	允许使用该用户名进行认证的时间段。
MAC 地址绑定方式	设置 MAC 绑定方式，有三种方式可供选择：不绑定、静态绑定和动态绑定。 <ul style="list-style-type: none"> 不绑定：不绑定认证客户端 MAC 地址。 静态绑定：手动输入认证客户端 MAC 地址，绑定对应用户名。 动态绑定：系统自动绑定第一个使用该用户名认证成功的客户端 MAC 地址。
同时登录用户数	仅当“MAC 地址绑定方式”为“不绑定”时，可设。允许同时使用该用户名认证的客户端最大数目。
姓名	设置客户姓名备注。
电话	设置客户电话备注。
备注	设置条目的备注，以方便管理和查找。

状态 设置该用户是否生效。

» 免费用户

给用户以“分钟”为时间单位的短时间上网服务，该账户可重复使用，用户免费上网时长到期后，使用该账户重新认证，即可再次上网。

图 7-29 新增免费用户界面

The screenshot shows a configuration form for adding a free user. The fields and their values are as follows:

- 用户类型: 免费用户 (dropdown menu)
- 用户名: (text input field)
- 密码: (password input field)
- 允许认证时间段: 00:00-24:00 (time range input)
- 免费时长: 30 (duration input)
- 同时登录用户数: 1 (concurrent users input)
- 备注: (text input field)
- 状态: 启用 禁用 (radio buttons)

Buttons for '确定' (OK) and '取消' (Cancel) are located at the bottom left.

表 7-15 新增免费用户界面项说明

用户名	自定义用户名，不能与已有用户名重复。
密码	新增用户时，需要输入密码。修改用户配置时，可以输入新密码，不输入则表示不修改。
允许认证时间段	允许使用该用户名进行认证的时间段。
免费时长	免费用户上网时间限制。
同时登录用户数	允许同时使用该用户名认证的客户端最大数目。
备注	设置条目的备注，以方便管理和查找。
状态	设置该用户是否生效。

7.4 认证服务器

无线控制器提供指定外部 Radius 服务器进行认证的功能。

外部 Radius 服务器认证，即当用户接入时，无线控制器将用户的身份认证信息提交给外部服务器，由外部服务器认证身份信息。

配置 Radius 认证服务器步骤

- 1) 设置 Radius 服务器。必须操作。配置界面：认证管理 >> 认证服务器 >> Radius 服务器。
- 2) 设置服务器组。必须操作。配置界面：认证管理 >> 认证服务器 >> 认证服务器。

7.4.1 Radius 服务器

可以通过本界面添加、修改或删除一个外部 Radius 服务器。Radius 支持认证服务和计费服务功能。

进入界面：认证管理 >> 认证服务器 >> Radius 服务器

图 7-30 设置 Radius 服务器界面

The screenshot shows the 'Radius 服务器' (Radius Servers) configuration page. At the top, there are tabs for '认证服务器' (Authentication Servers) and 'Radius 服务器' (Radius Servers). Below the tabs, there are buttons for '+ 新增' (Add), '- 删除' (Delete), and '搜索' (Search). A table with the following columns is displayed: 序号 (Serial Number), 名称 (Name), 地址 (Address), 认证端口 (Authentication Port), 计费端口 (Billing Port), 认证方式 (Authentication Method), and 设置 (Settings). The table contains one row with dashes '--' in all cells. Below the table, there is a pagination control showing '共0条, 每页: 10 条 | 当前: 0/0页, 0~0条 |' and navigation arrows.

在此界面，可以对已有条目进行操作，点击 < 新增 > 按键可以添加新条目，新增 Radius 服务器条目界面如下图所示。

图 7-31 新增 Radius 服务器界面

The screenshot shows the '新增 Radius 服务器' (Add Radius Server) form. It contains the following fields and their constraints:

- 服务器名称: (1-50个字符)
- 服务器地址: (IP地址或域名, 1-250个英文字符)
- 认证端口: 1812 (1024-65535)
- 计费端口: 0 (0, 1024-65535)
- 共享密钥: (1-120个字符)
- 重复发送次数: 3 (0-10次)
- 超时时间: 3 (1-60秒)
- NAS IP 地址: (可选)
- 认证方式: PAP (dropdown menu)

At the bottom, there are '确定' (Confirm) and '取消' (Cancel) buttons.

表 7-16 新增 Radius 服务器界面项说明

服务器名称	为配置的 Radius 服务器命名。
-------	--------------------

服务器地址	设置服务器的地址，IPv4 地址或者 DNS 域名。
认证端口	服务器监听认证报文的端口。
计费端口	服务器监听计费报文的端口，0 表示不启用计费功能。
共享密钥	Radius 服务器配置的共享密钥。
重复发送次数	当客户端发送请求后，如果没有收到回复，重复发送请求的次数。
超时时间	当客户端发送请求后，数据包超时时间。
NAS IP 地址	进行 Radius 认证或计费时，NAS-IP-Address 字段的 IP 地址值（一般填写 AC 与 Radius 服务器交互的实际 IP 地址，也可以为空）。
认证方式	选择使用的认证方式，有 PAP、CHAP、MSCHAP 和 MSCHAPv2。

7.4.2 认证服务器

可以通过本界面设置和查看认证服务器组。

进入界面：认证管理 >> 认证服务器 >> 认证服务器

图 7-32 认证服务器界面



在此界面，可以对已有条目进行操作，点击 < 新增 > 按键可以添加新条目，新增服务器组条目界面如下图所示。

图 7-33 新增服务器组界面

组名称: (1-50个字符)

协议类型: RADIUS

主服务器: ▼

备用服务器: ▼ (可选)

恢复时间: (30-1440分钟)

备注: (1-50个字符, 可选)

表 7-17 新增服务器组界面项说明

组名称	自定义认证服务器组名称，不能与已有服务器组名称重复。
协议类型	该组中认证服务器的类型，仅支持 Radius。
主服务器	选择特定类型的认证服务器为该组的主服务器，主服务器在认证过程中将优先被使用。
备用服务器	备用服务器在主服务器发生故障时启用。
恢复时间	当主服务器发生故障后，重新尝试使用主服务器的时间间隔。
备注	设置条目的备注，以方便管理和查找。

7.5 应用举例

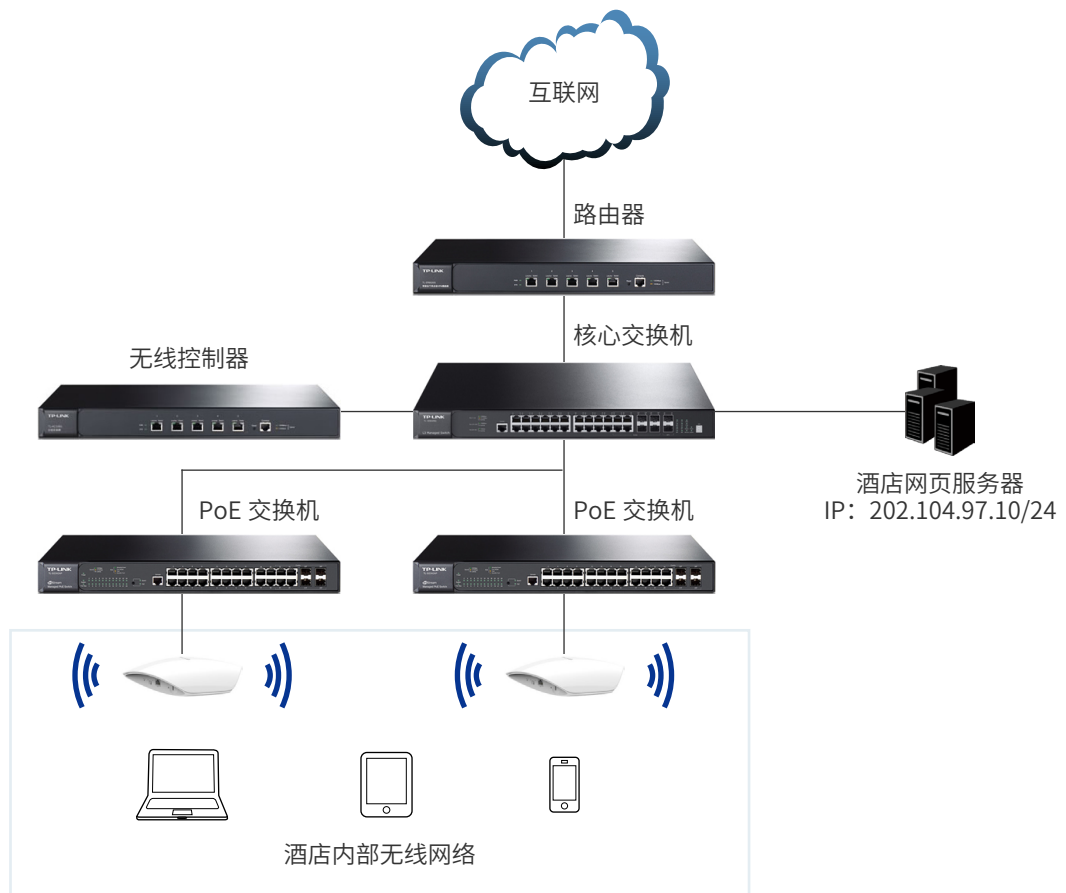
7.5.1 一键上网

应用场景

某酒店为顾客提供免费上网服务，并希望通过 Web 认证页面推送酒店宣传广告。可使用无线控制器一键上网认证功能实现需求。

网络拓扑

图 7-34 酒店无线网络应用拓扑



配置方法

1 设置一键上网跳转页面

进入页面：认证管理 >> Portal 认证 >> 跳转页面，点击 < 新增 > 按键，在设置页面选择“认证页面类型”为**一键上网**，可参考如下参数设置，背景图片选择制作好的酒店宣传图片上传到无线控制器上。

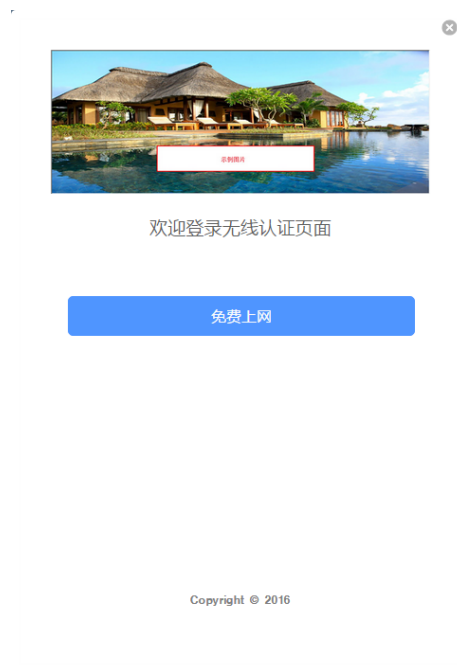
图 7-35 一键上网跳转页面设置

跳转页面名称:	OneClick	(1-50个英文字符、数字、下划线或减号)
认证页面类型:	一键上网	
页面标题:	XX酒店无线认证	(1-50个字符)
背景图片:	<input type="button" value="上传"/> <input type="button" value="上传成功"/>	
欢迎信息:	欢迎登录无线认证页面	(1-26个字符)
版权声明:	Copyright © 2016	(1-50个字符)
备注:	一键上网	(1-50个字符, 可选)
页面预览:	<input type="button" value="预览跳转页面"/>	

注意:
1、当条目已经被引用后, 不能再修改跳转页面名称和认证页面类型。

设置完成后, 点击 < 预览跳转页面 > 按键, 可以预览自定义的认证跳转页面, 如下图所示。

图 7-36 预览一键上网跳转页面



2 设置一键上网

进入页面: 认证管理 >> Portal 认证 >> 一键上网, 点击 < 新增 > 按键, 在一键上网设置页面选择启用一键上网, 可参考如下参数设置。

图 7-37 一键上网设置

状态:	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
跳转页面名称:	OneClick	
VLAN ID:	1	(1-4094, 可选)
免费上网时长:	30	分钟 (1-1440)
备注:	酒店无线认证	(1-50个字符, 可选)

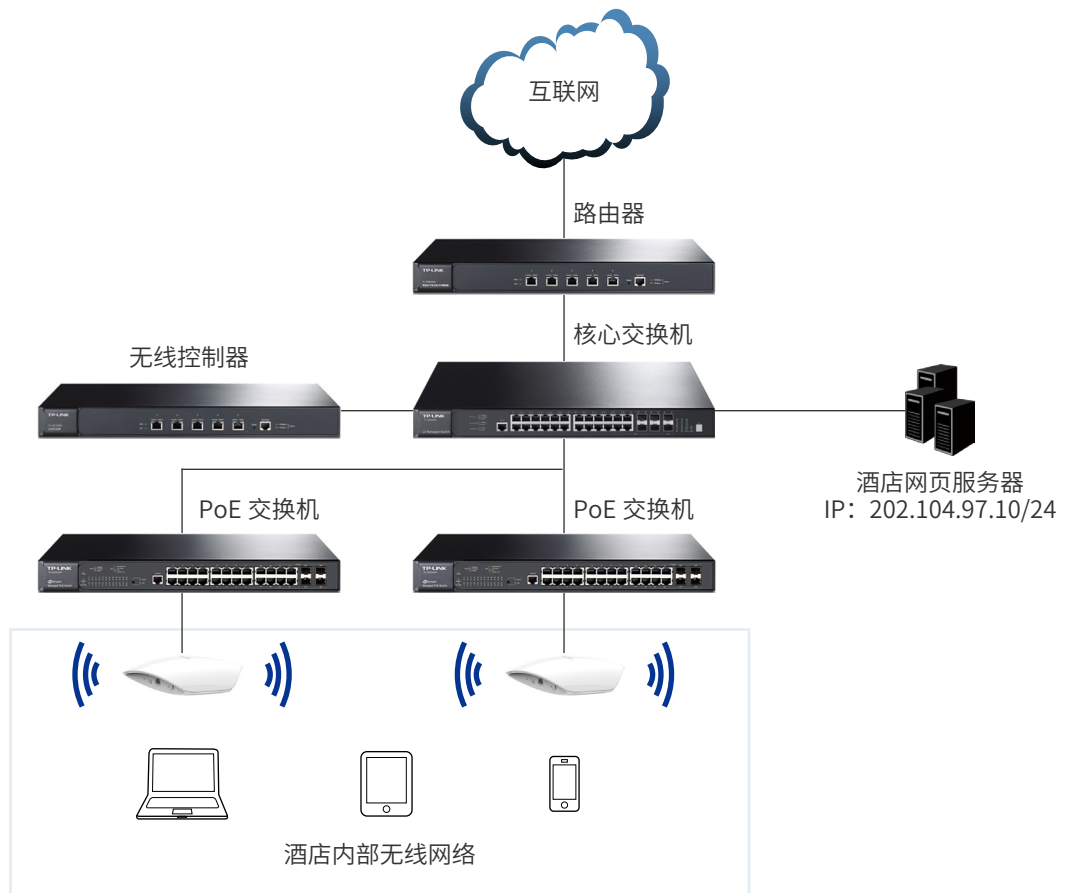
7.5.2 Web 认证

应用场景

某酒店组建无线局域网，满足酒店入住客人的上网需求，需要对接入网络的用户进行 Web 认证，在认证页面推送酒店宣传广告。可以使用无线控制器内置的 Web 服务器和本地认证服务器设置认证功能实现需求。

网络拓扑

图 7-38 酒店无线网络应用拓扑



配置方法

1 设置 Web 认证跳转页面

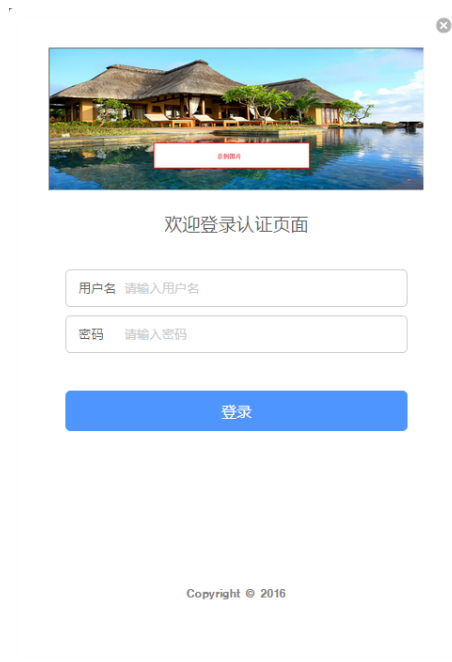
进入页面：认证管理 >> Portal 认证 >> 跳转页面，点击 < 新增 > 按键，在设置页面选择“认证页面类型”为 **Web 认证**，可参考如下参数设置，背景图片选择制作好的酒店宣传图片上传到无线控制器上。

图 7-39 Web 认证跳转页面设置

跳转页面名称:	Web	(1-50个英文字符、数字、下划线或减号)
认证页面类型:	Web认证	
页面标题:	XX酒店Web认证	(1-50个字符)
背景图片:	<input type="button" value="上传"/> 上传成功	
欢迎信息:	欢迎登录认证页面	(1-26个字符)
版权声明:	Copyright © 2016	(1-50个字符)
备注:	Web认证	(1-50个字符, 可选)
页面预览:	<input type="button" value="预览跳转页面"/>	
0		
注意:		
1、当条目已经被引用后, 不能再修改跳转页面名称和认证页面类型。		
<input type="button" value="确定"/> <input type="button" value="取消"/>		

设置完成后, 点击 < 预览跳转页面 > 按键, 可以预览自定义的认证跳转页面, 如下图所示。

图 7-40 预览 Web 认证跳转页面



2 设置 Web 认证

进入页面: 认证管理 >> Portal 认证 >> Web 认证, 点击 < 新增 > 按键, 在设置页面选择启用 Web 认证, 可参考如下参数设置。

图 7-41 Web 认证设置

状态:	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
跳转页面名称:	Web
VLAN ID:	1 (1-4094, 可选)
认证服务器类型:	本地服务器
认证成功跳转链接:	www.xxjjudian.com.cn (1-120个英文字符、数字或英文特殊字符, 可选)
认证失败跳转链接:	 (1-120个英文字符、数字或英文特殊字符, 可选)
无感知认证:	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭
备注:	Web认证 (1-50个字符, 可选)
注意: 1、如果配置了认证失败跳转链接, 链接地址会自动加入免认证策略, 无需用户配置。 2、认证服务器类型为远程服务器时, 若服务器配置了用户上网时间, 则免费上网时长为服务器返回的时间, 否则为本页面配置的免费上网时长。	
<input type="button" value="确定"/> <input type="button" value="取消"/>	

3 添加认证用户

在 Web 认证的相关参数设置完成后, 还需添加认证用户的账户信息, 为后续用户认证提供登录用户名和密码。

在添加以前, 需要确定好认证的账户总数, 在本例中按照以下需求进行设置:

- 1) 每个客房提供一个免费用户账号, 设置免费 2 小时上网, 超时需重新进行认证, 方便推送广告; 允许 3 个客户端同时使用这个账户, 方便同一房间的多位用户多台设备上网的需求。
- 2) 对于酒店的重要客户, 可以为每个客户单独设置一个正式用户账号, 按照入住日期, 设定上网的时限, 保证更为良好的上网环境。

进入页面: 认证管理 >> 用户管理 >> 用户管理, 点击 < 新增 > 按键, 在用户设置页面中, 添加认证用户账户, 下面以添加免费用户账户为例, 具体设置可参考如下的设置参数。

图 7-42 添加免费用户账户

用户类型:	免费用户
用户名:	user1 (1-100个英文字符、数字或英文特殊字符)
密码:	123456789 (1-100个英文字符、数字或英文特殊字符)
允许认证时段:	00:00-24:00 (格式: xx:xx-xx:xx)
免费时长:	120 分钟 (1-1440)
同时登录用户数:	3 (1-2048)
备注:	A708房间 (1-50个字符, 可选)
状态:	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
<input type="button" value="确定"/> <input type="button" value="取消"/>	

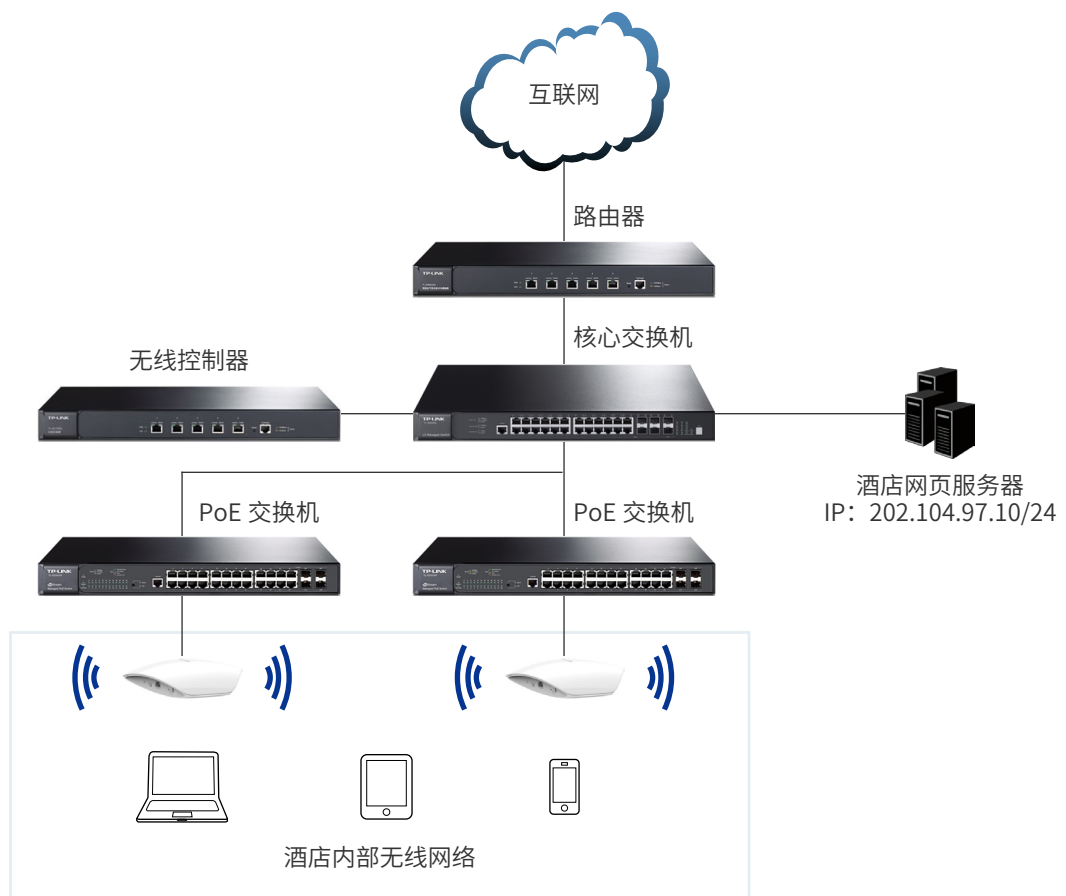
7.5.3 微信连 Wi-Fi

应用场景

某酒店组建无线局域网，需要对接入网络的用户进行微信连 Wi-Fi 认证，在认证页面推送酒店宣传图片，同时利用用户关注的微信公众号实现二次营销需求。可使用无线控制器微信连 Wi-Fi 功能实现需求。

网络拓扑

图 7-43 酒店无线网络应用拓扑



配置方法

1 微信公众号平台后台设置

以订阅号为例，在微信公众号平台后台进行如下设置：

- 1) 添加微信连 Wi-Fi 功能，如下图所示，点击 < 添加功能插件 > 后在插件库添加“微信连 Wi-Fi”功能。

图 7-44 添加微信连 Wi-Fi 功能



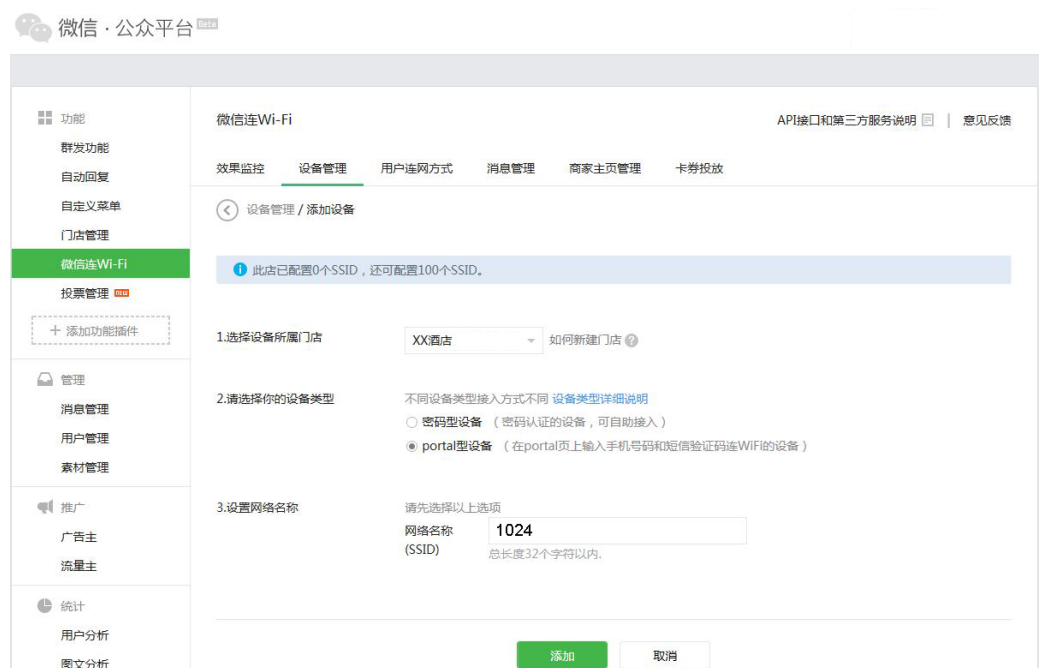
2) 新建门店，如下图所示，在门店管理功能界面可以新建门店。

图 7-45 新建门店



3) 在微信连 Wi-Fi 功能界面添加设备，如下图所示。

图 7-46 添加设备 1



4) 添加设备后会生成如下信息，这些信息在无线控制器上设置微信连 Wi-Fi 跳转页面时会用到。

图 7-47 添加设备 2



2 设置微信连 Wi-Fi 跳转页面

进入页面：认证管理 >> Portal 认证 >> 跳转页面，选择“认证页面类型”为**微信连 Wi-Fi**，可参考如下参数设置。

图 7-48 微信连 Wi-Fi 跳转页面设置

跳转页面名称:	1024	(1-50个英文字符、数字、下划线或减号)
认证页面类型:	微信连WIFI	
页面标题:	weixin	(1-50个字符)
背景图片:	<input type="button" value="上传"/> <input type="button" value="上传成功"/>	
欢迎信息:	欢迎使用微信连Wi-Fi	(1-26个字符)
版权声明:	Copyright © 2016	(1-50个字符)
Logo图片:	<input type="button" value="上传"/> <input type="button" value="上传成功"/>	
Logo信息:	XX酒店	(1-25个字符, 可选)
登录按钮提示文字:	登录	(1-15个字符)
备注:	微信连Wi-Fi	(1-50个字符, 可选)
页面预览:	<input type="button" value="预览跳转页面"/>	

注意:
1、当条目已经被引用后，不能再修改跳转页面名称和认证页面类型。

设置完成后，点击<预览跳转页面>按键，可以预览自定义的认证跳转页面，如下图所示。

图 7-49 预览微信连 Wi-Fi 跳转页面



3 设置微信连 Wi-Fi

进入页面：认证管理 >> Portal 认证 >> 微信连 Wi-Fi，点击 < 新增 > 按键，在设置页面选择启用微信连 Wi-Fi，可参考如下参数设置。

图 7-50 微信连 Wi-Fi 设置

状态:	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用	
跳转页面名称:	1024	
VLAN ID:	1	(1-4094, 可选)
免费上网时长:	30	分钟 (1-1440)
ShopID:	5971506	(1-32个数字或英文字母)
AppID:	wxec5aaae3151f232f	(1-32个数字或英文字母)
SecretKey:	4d31f6892cf7009626e6cea1b9de	(1-32个数字或英文字母)
备注:	微信连Wi-Fi	(1-50个字符, 可选)

注意:
 1、配置了微信连WIFI认证条目, 为了无线PC能够顺利完成认证, 需要保证AC可以联网。
 2、微信公众号信息设置方法, 请参阅: [微信连Wi-Fi功能使用指南](#)。

确定 取消

4 无线客户端上网步骤

不同厂商设备的操作界面可能有所不同，本手册仅以下文所述情况示意。

- 1) 使用 Wi-Fi 连接 SSID 为“1024”的无线网络，系统将自动跳转到认证页面，如下图所示。

图 7-51 跳转到认证页面



欢迎使用微信连Wi-Fi



Copyright © 2016

- 2) 点击 < 登录 >，进入微信连 Wi-Fi 页面，如下图所示。

图 7-52 微信连 Wi-Fi 页面



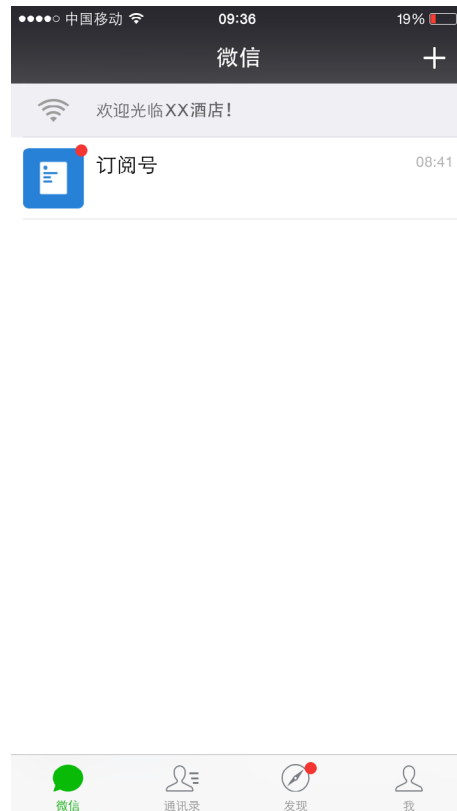
- 3) 点击 < 立即连接 >，可连接 Wi-Fi，如下图所示。

图 7-53 Wi-Fi 连接成功页面



4) Wi-Fi 连接成功后，即可上网，点击 <完成>，将进入微信页面，如下图所示。

图 7-54 微信页面



8 安全管理

8.1 广播风暴抑制

广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通讯，严重降低网络性能。广播风暴的判断标准为一个端口是否在短时间内连续收到许多个广播帧。广播风暴抑制是指用户可以限制端口上允许接收的广播流量大小，当该类流量超过用户设置的阈值后，系统将丢弃超出流量限制的广播帧，防止广播风暴的发生，从而保证网络的正常运行。

可以在此界面开启 AP 的广播风暴抑制功能，并设置广播风暴抑制速率。

进入界面：安全管理 >> 广播风暴抑制 >> 广播风暴抑制

图 8-1 广播风暴抑制设置界面

广播风暴抑制

广播风暴抑制

广播风暴抑制： 开启 关闭

广播风暴抑制速率：自定义

自定义速率：1024 (1-1024, 单位: Kbps)

设置

表 8-1 广播风暴抑制设置界面项说明

广播风暴抑制	选择开启或关闭 AP 的广播风暴抑制功能。
广播风暴抑制速率	选择广播风暴抑制速率。若选择“自定义”，则可自定义一个广播风暴抑制速率。

8.2 DHCP 防护

DHCP 防护，是指 AP 在接收到 DHCP 报文时检查其 IP 或 MAC，只允许绑定到该 AP 的 DHCP 服务器的报文通过。该功能可以防止无线客户端从非法 DHCP 服务器获取 IP。

8.2.1 DHCP 防护

可以在此界面启用或禁用每个 AP 的 DHCP 防护功能，也可以修改每个 AP 绑定的 DHCP 服务器。

进入界面：安全管理 >> DHCP 防护 >> DHCP 防护

图 8-2 DHCP 防护设置界面



列表中只显示选中分组下的 AP 的 DHCP 防护信息。点击 < > 按键会进入 DHCP 绑定列表界面，如下图所示。

图 8-3 DHCP 绑定列表界面



安全管理 >> DHCP 防护 >> DHCP 服务器列表界面中设置的条目会在此显示，可以选择 DHCP 服务器绑定到 AP。

8.2.2 DHCP 服务器列表

可以在此界面查看、新增、修改和删除 DHCP 服务器，以供 AP 绑定。

进入界面：安全管理 >> DHCP 防护 >> DHCP 服务器列表

图 8-4 DHCP 服务器列表界面



点击 < 新增 > 按键可以添加新条目，新增 DHCP 服务器界面如下图所示。

图 8-5 新增 DHCP 服务器界面

表 8-2 新增 DHCP 服务器界面项说明

服务器名称	设置 DHCP 服务器的名称，不能重复。
地址类型	选择 DHCP 服务器的地址类型，IP 或 MAC。
服务器地址	设置 DHCP 服务器的地址，不能重复。

8.3 ARP 防护

ARP 防护，是指 AP 在接收到 ARP 报文时检查其 IP 和 MAC，只有源 IP 和源 MAC 地址均匹配的数据报文才进行转发。该功能可以对 AP 有线口收到的 ARP 报文进行检测，防止 ARP 攻击，确保无线网络的稳定性。

8.3.1 ARP 防护绑定

可以在此界面查看已关联 AP 的 ARP 防护设置，单独或批量修改每个 AP 绑定的 ARP 防护条目。

进入界面：安全管理 >> ARP 防护 >> ARP 防护绑定

图 8-6 ARP 防护绑定设置界面



列表中只显示选中分组下的 AP 的 ARP 防护信息。点击 按键会进入 ARP 绑定列表界面，如下图所示。

图 8-7 ARP 绑定列表界面



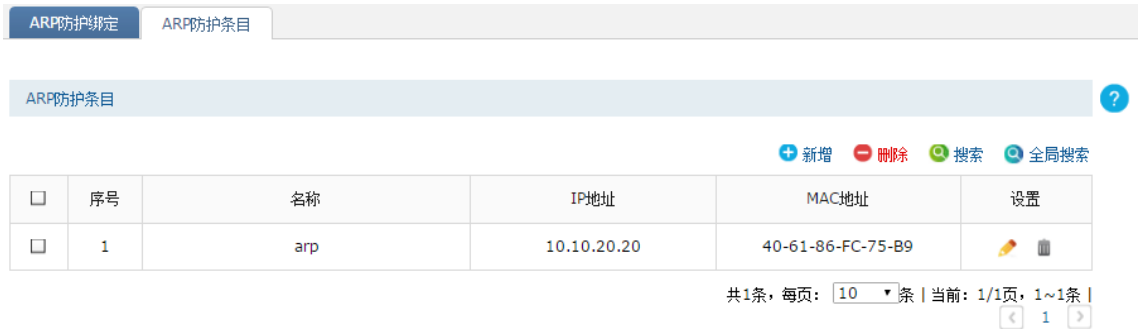
安全管理 >> ARP 防护 >> ARP 防护条目界面中设置的条目会在此显示，可以选择 ARP 防护条目绑定到 AP。

8.3.2 ARP 防护条目

可以在此界面查看、新增、修改和删除需要绑定设备的 IP 地址和 MAC 地址。一条 ARP 防护条目对应一台设备。

进入界面：安全管理 >> ARP 防护 >> ARP 防护条目

图 8-8 ARP 防护条目界面



点击 < 新增 > 按键可以添加新条目，新增 ARP 防护条目界面如下图所示。

图 8-9 新增 ARP 防护条目界面

表 8-3 新增 ARP 防护条目界面项说明

名称	设置 ARP 防护条目的名称，不能重复。
IP 地址	设置 ARP 防护条目的 IP 地址，一个 IP 地址可对应多个 MAC 地址。
MAC 地址	设置 ARP 防护条目的 MAC 地址，一个 MAC 地址可对应多个 IP 地址。



说明：

任意两条 ARP 防护条目的 IP 地址和 MAC 地址不能完全一样。

9 链路备份

9.1 双链路备份

9.1.1 功能简介

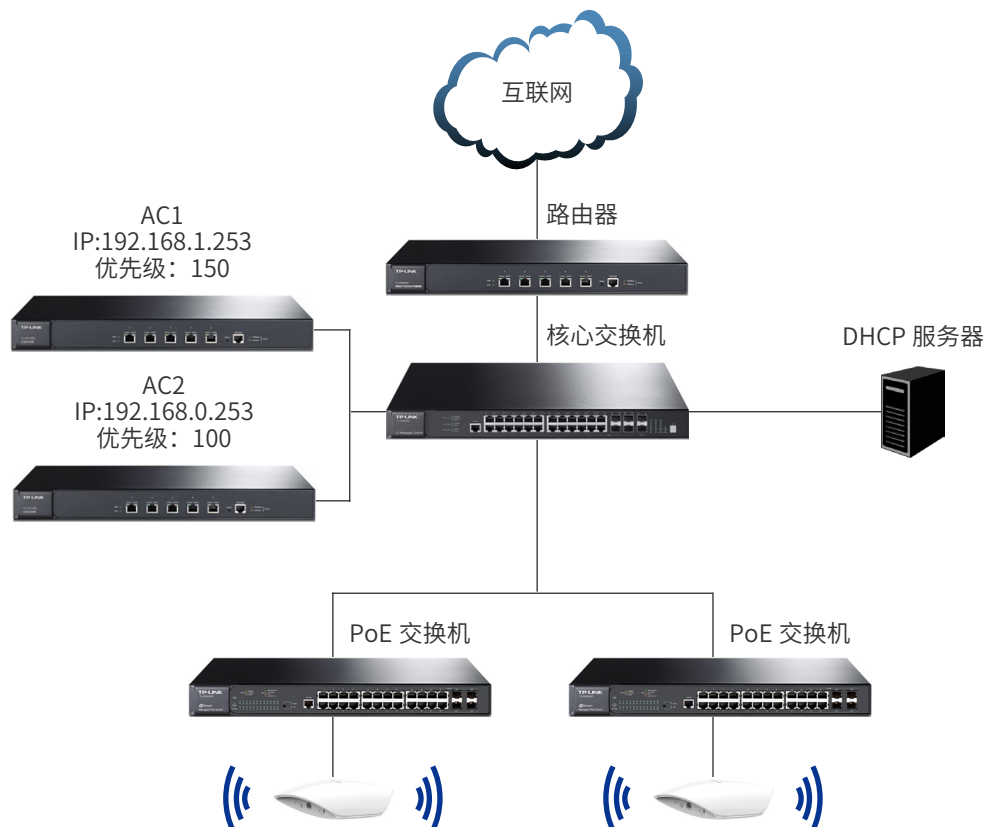
双链路备份功能适用于两台 AC 设备共同管理无线网络的应用场景。根据用户使用的 DHCP 服务器不同，有两种应用拓扑：[使用外部 DHCP 服务器](#)和[以 AC 为 DHCP 服务器](#)。推荐用户使用外部 DHCP 服务器，便于网络管理和维护。

使用外部 DHCP 服务器

当网络中有两台 AC 设备并且均可以正常管理所有的 AP，如果希望接入的 AP 设备优先接受某一台 AC 的管理，可将这台 AC 的**链路优先级**设置高于另一台 AC。

如下图所示，将无线控制器 AC1 的优先级设置为 150，将无线控制器 AC2 的优先级设置为 100。则 AC1 将作为主 AC 设备，可以管理所有 AP，而 AC2 将作为备份 AC。

图 9-1 使用外部 DHCP 服务器网络拓扑图



外部 DHCP 服务器配置方法

当 AP 获取地址时，需要服务器下发两台 AC 的 IP 地址。所以在 DHCP 服务器上，必须设置如下内容：

- 一条 **DHCP Option 60** 选项，内容为“TP-LINK”；
- 两条 **DHCP Option 138** 选项，分别填入两台 AC 的 IP 地址，使 AP 均能获取到所有的 AC IP 地址。

相关内容可参考我司技术支持网站上的指导：http://service.tp-link.com.cn/detail_article_504.html。

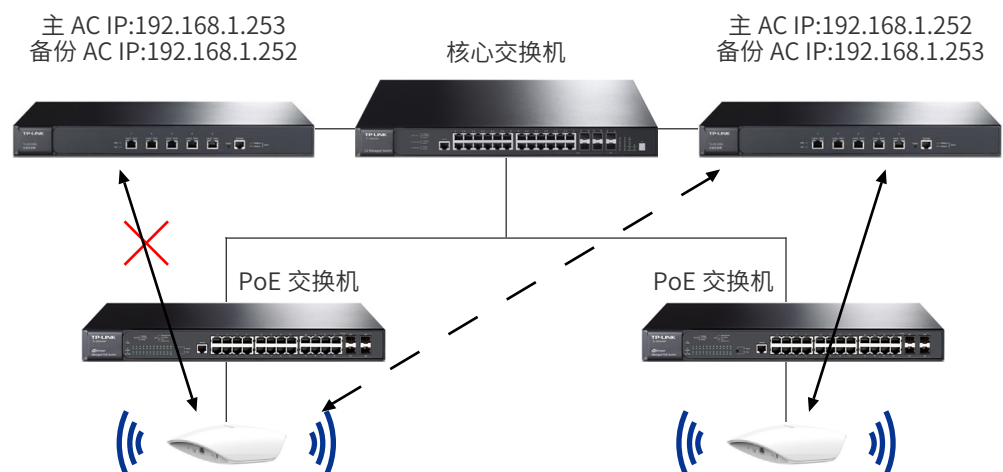
说明：

- 在配置外部 DHCP 前，请关闭所有 AC 的 DHCP 功能，以免出现 AP 获取地址异常的情况。
- 请在核心交换机上配置 DHCP 中继功能，确保 DHCP 的数据报文正常可达。

以 AC 为 DHCP 服务器

当网络中有两台 AC 设备并且均可以正常管理所有的 AP，如果希望在一台 AC 出现故障时，另一台 AC 能够自动接管 AP，则需要将两台 AC 的**对端地址**设置为对方的 IP 地址。这样，主链路的 AC 在分配 AP 设备 IP 地址时，会将备份 AC 的地址下发给 AP，AP 会同时与主备链路的 AC 进行关联。当主链路 AC 失效一段时间后，AP 会将备份链路升级为主链路，接受其管理，如下图所示。

图 9-2 以 AC 为 DHCP 服务器网络拓扑图



9.1.2 双链路备份设置

可以在此界面设置双链路功能和配置链路优先级。

进入界面：链路备份 >> 双链路备份 >> 双链路备份

图 9-3 双链路备份设置界面

双链路备份

双链路设置 ?

启用双链路

链路优先级: 0 (0-255)

对端地址: (x.x.x.x)

设置

注意:
1、修改双链路配置将使所有处于主链路状态的AP重启，处于备链路状态下的AP断开与本机的连接。当AP与AC重新建立连接之后，就会按照新的链路优先级重新选择主用AC和备份AC。

表 9-1 双链路备份设置界面项说明

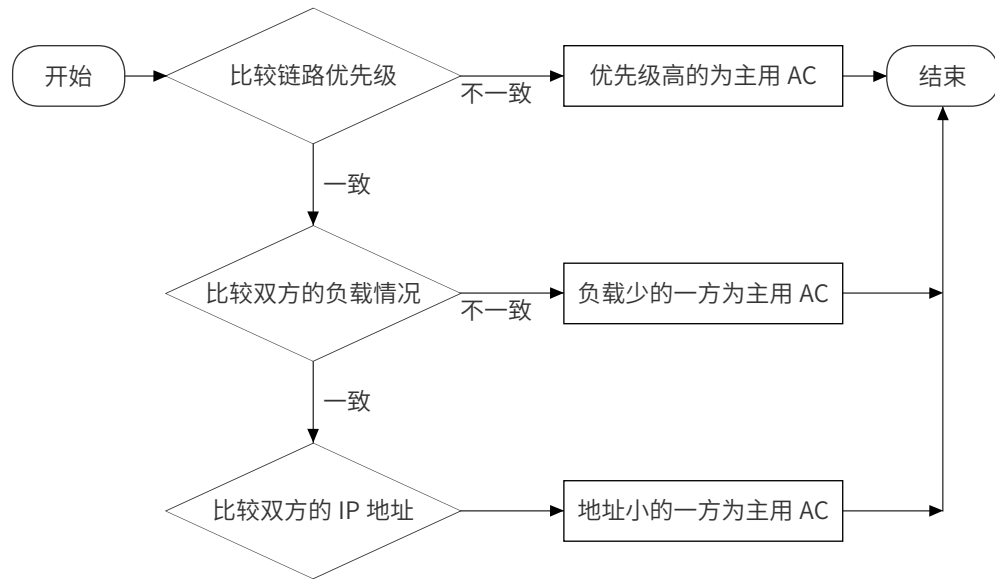
启用双链路	勾选后开启双链路功能。
链路优先级	设置 AC 的链路优先级，数值越大，AP 选择本 AC 作主用 AC 的优先度越高。
对端地址	对端 AC 的地址，通过本机配置的 DHCP 服务器的报文下发，让 AP 在通过本机提供的 DHCP 服务获取 IP 时获得对端 AC 的地址。需要开启本机的 DHCP 服务才能生效。

说明：

- 修改双链路配置将使所有处于主链路状态的 AP 重启，处于备链路状态下的 AP 断开与本机的连接。当 AP 与 AC 重新建立连接之后，会按照新的链路优先级重新选择主用 AC 和备份 AC。
- 假设备份 AC 作为 DHCP 服务器，且 AP 的地址是由备份 AC 下发，则修改备份 AC 的对端地址时，需要使备份 AC 下发地址的 AP 重启，如果不重启，AP 将无法识别新地址的 AC。
- 使用双链路备份时，用户需自行确保主、备 AC 之间配置的一致性。
- 当 AP 从主 AC 切换至备份 AC 时，已认证的无线客户端需要重新认证。

AP 选取主用 AC 规则

图 9-4 AP 选取主用 AC 规则流程图



- 1) 首先比较链路优先级，选取优先级高的为主用 AC。
- 2) 若优先级一致，则比较双方的负载情况，选取负载少的一方为主用 AC。
- 3) 若负载也一样，则比较双方的 IP 地址，选取地址小的一方为主用 AC。

10 系统工具

10.1 管理账号

10.1.1 管理账号

可以在此界面设置管理账号。

进入界面：系统工具 >> 管理账号 >> 管理账号

图 10-1 管理账号设置界面

The screenshot shows the '修改管理账号' (Modify Management Account) interface. It includes the following fields and constraints:

- 原用户名: admin (1-15个英文字母、数字或英文特殊字符)
- 原密码: (6-15个英文字母、数字或英文特殊字符)
- 新用户名: (1-15个英文字母、数字或英文特殊字符)
- 新密码: (6-15个英文字母、数字或英文特殊字符)
- 确认新密码: (6-15个英文字母、数字或英文特殊字符)

There is a '设置' (Settings) button at the bottom left of the form area.

表 10-1 管理账号设置界面项说明

原用户名	当前登录的用户名。
原密码	如果需要设置新用户名和密码，请输入原密码。
新用户名	修改后的用户名。
新密码	修改后的用户密码。
确认新密码	再次输入新密码。

10.1.2 系统管理设置

可以在此界面设置服务端口和会话超时时间。

进入界面：系统工具 >> 管理账号 >> 系统管理设置

图 10-2 系统管理设置界面

管理账号 系统管理设置

功能设置 ?

HTTP服务端口: 80 (80、1024-65535)

HTTPS服务端口: 443 (443、1024-65535)

Web会话超时时间: 6 分钟(5-60)

设置

表 10-2 系统管理设置界面项说明

HTTP 服务端口	用于 Web 管理界面的服务端口，默认为 80 端口。不能与其他的 service 端口重复。
HTTPS 服务端口	用于 Web 管理界面的 Https 服务端口，默认为 443 端口。不能与其他的 service 端口重复。
Web 会话超时时间	在会话超时时间内未进行过操作，系统将自动退出登录，以保证设备和网络的安全。默认 Web 会话的超时时间为 6 分钟。

10.2 设备管理

10.2.1 恢复出厂配置

进入界面：系统工具 >> 设备管理 >> 恢复出厂配置

图 10-3 恢复出厂配置界面

恢复出厂设置 备份与导入配置 重启设备 软件升级

恢复出厂配置 ?

点击此按钮将使设备的所有配置恢复到出厂时的默认状态。

恢复出厂配置

点击 < 恢复出厂配置 > 按键，无线控制器将会恢复所有设置的默认值。建议在网络配置错误、组网环境变更等情况时使用此功能。

恢复出厂配置后，当前的配置信息将会丢失。如果不希望丢失当前配置，请先进行配置备份，再进行此操作。备份配置可以参考[备份与导入配置](#)。

无线控制器出厂默认管理 IP 为 192.168.1.253，首次登录需自行设置登录用户名和密码。

说明：

恢复出厂配置后，设备将自动重启，此过程中请保持电源稳定，避免强行断电。

10.2.2 备份与导入配置

进入界面：系统工具 >> 设备管理 >> 备份与导入配置

图 10-4 备份与导入配置界面

恢复出厂设置 备份与导入配置 重启设备 软件升级

版本信息 ?

当前配置版本: 1.0.0

备份配置信息

您可以点击<备份>保存您当前的配置信息。我们建议在修改配置及升级软件前备份您的配置信息。

备份

导入配置信息

您可以通过导入配置文件来恢复您备份的配置。

文件路径: 浏览

导入

版本信息

显示当前无线控制器配置版本。

备份配置信息

单击 < 备份 > 按键，无线控制器会将目前所有已保存配置导出为文件。建议在修改配置或升级软件前备份当前的配置信息。

导入配置信息

单击 < 浏览 > 按键，选择已备份的配置文件；或者在文件路径输入框中填写完整的配置文件路径，然后单击 < 导入 > 按键，将无线控制器恢复到以前备份的配置状态。

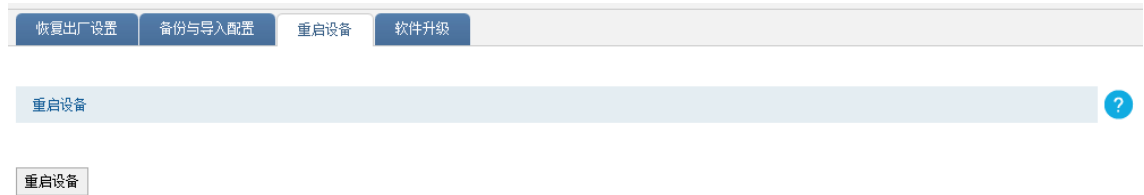
说明：

- 备份及导入文件过程中请保持电源稳定，避免强行断电。
- 导入的配置文件版本与无线控制器当前配置版本差距过大，将有可能导致无线控制器现有配置信息丢失，如果有重要的配置信息，请谨慎操作。

10.2.3 重启设备

进入界面：系统工具 >> 设备管理 >> 重启设备

图 10-5 重启设备界面



单击 < 重启设备 > 按键，无线控制器将会重新启动。重新启动不会丢失已保存的配置，在重启的过程中，网络连接将会暂时中断。

说明：

重启过程中请保持电源稳定，避免强行断电。

10.2.4 软件升级

进入界面：系统工具 >> 设备管理 >> 软件升级

图 10-6 软件升级界面



TP-LINK 服务支持网站 (<http://service.tp-link.com.cn>) 会不定期更新无线控制器的软件升级文件，可将升级文件下载保存到本地。登录无线控制器后进入软件升级界面，单击 < 浏览 > 按键，选择保存路径下的升级文件，点击 < 升级 > 按键进行软件升级。

说明：

- 升级软件可能会丢失当前未保存的配置信息，请在升级前保存配置。
- 软件升级过程中，请不要将设备断电，不要对页面进行刷新。
- 软件升级成功后，设备将自动重启，此过程中请保持电源稳定，避免强行断电。

10.3 诊断工具

可以在此界面通过 PING 通信检测或路由跟踪检测来诊断当前无线控制器的网络连接状态。

进入界面：系统工具 >> 诊断工具 >> 诊断工具

» PING 通信检测

图 10-7 诊断工具 -PING 通信检测界面



诊断工具

诊断工具

诊断工具类型: PING通信检测 路由跟踪检测

目的IP/域名:

出接口:

开始

PING次数: (1-50)

PING数据包大小: (4-1472 Bytes)

The Router is ready.

表 10-3 诊断工具 -PING 通信检测界面项说明

目的 IP/ 域名	输入需要进行 PING 通信检测的主机地址，支持 IP 地址和域名。
出接口	选择需要进行 PING 通信检测的接口。
PING 次数	设置 PING 通信检测的次数。
PING 数据包大小	设置 PING 通信检测每一次发送的数据包大小。

» 路由跟踪检测

图 10-8 诊断工具 - 路由跟踪检测界面

诊断工具

诊断工具

诊断工具类型：
 PING通信检测 路由跟踪检测

目的IP/域名：

出接口：

开始

路由跟踪最大TTL：
 (1-30)

The Router is ready.

表 10-4 诊断工具 - 路由跟踪检测界面项说明

目的 IP/ 域名	输入需要进行路由跟踪检测的主机地址，支持 IP 地址和域名。
出接口	选择需要进行路由跟踪检测的接口。
路由跟踪最大 TTL	设置路由跟踪检测的最大 TTL 值。

10.4 时间设置

时间设置界面允许对无线控制器的系统时间进行设置。若时间设置发生改变，将会影响一些与其相关的功能，如系统日志。

进入界面：系统工具 >> 时间设置 >> 时间设置

» 通过网络获取系统时间

图 10-9 时间设置 - 通过网络获取系统时间界面

时间设置

时间设置

当前时间: 01/03/1970 17:34:55

设置时间: 通过网络获取系统时间 手动设置系统时间

时区: (UTC+08:00)北京, 重庆, 乌鲁木齐, 香港特别行政区, 台北, 乌兰

首选NTP服务器: 128.138.140.44 (X.X.X.X)

备选NTP服务器: 210.72.145.44 (X.X.X.X, 可选)

设置

注意: NTP服务器只能填写IP地址。

若无线控制器可以访问互联网，可选择此项进行网络校时。选择时区后点击 < 设置 > 按键，无线控制器将在内置 NTP（Network Time Protocol，网络校时协议）服务器地址列表中搜索可用地址，并获取时间。若获取失败，请手动设置 NTP 服务器地址，由于 NTP 服务器并非固定不变，推荐搜索两个不同的地址，分别填入首选、备选 NTP 服务器输入框，NTP 服务器地址需为 IP 地址。设置完毕后点击 < 设置 > 按键，无线控制器会通过指定的 NTP 服务器获取网络时间。

» 手动设置系统时间

图 10-10 时间设置 - 手动设置系统时间界面

时间设置

时间设置

当前时间: 01/04/1970 09:39:36

设置时间: 通过网络获取系统时间 手动设置系统时间

日期: 01/04/1970 (MM/DD/YYYY)

时间: 09 : 35 : 21 (HH/MM/SS)

获取管理主机时间

设置

若无线控制器暂时不能访问互联网，可以选择对系统时间进行手动设置，或者点击 < 获取管理主机时间 > 按键，系统将自动填入当前管理主机时间信息。设置完毕后点击 < 设置 > 生效。

说明：

- 如果不能正常使用 < 获取管理主机时间 > 功能，请在主机的防火墙软件中增加一条 UDP 端口为 123 的例外条目。
- 断电重启后，断电之前设置的时间将失效，重新变为“通过网络获取时间”，如果未能连网获取时间，请手动设置系统时间。

10.5 系统日志

可以在日志界面查看无线控制器系统事件的记录信息。

进入界面：系统工具 >> 系统日志 >> 系统日志

图 10-11 系统日志界面

The screenshot shows the 'System Log' interface. At the top, there is a 'System Log' tab. Below it is a 'Log Settings' section with a help icon. The settings include:

- 选择日志等级: 所有等级
- 选择模块类别: 所有模块
- 发送系统日志
- 服务器地址: 0.0.0.0

 A '设置' (Settings) button is located below these options.

 Below the settings is a 'Backup Log Information' section with a '备份' (Backup) button.

 The main part of the interface is the 'Log List' section, which contains a table with the following columns: 序号 (Serial Number), 时间 (Time), 功能模块 (Function Module), 日志等级 (Log Level), and 日志内容 (Log Content). The table is currently empty, showing '--' in all cells.

 Above the table are several utility buttons: 清空 (Clear), 搜索 (Search), 刷新 (Refresh), and 自动刷新 (Auto Refresh).

 Below the table, there is a pagination bar showing '共0条, 每页: 10 条 | 当前: 0/0页, 0~0条 |' and navigation arrows.

日志设置

表 10-5 日志设置界面项说明

选择日志等级

选择日志等级可使日志列表中仅列出特定等级日志信息。各等级描述如下：

- 所有等级：查看所有等级的日志信息。
- 致命错误：导致系统不可用的错误。
- 紧急错误：必须对其采取紧急措施的错误。
- 严重错误：导致系统处于危险状态的错误。
- 一般错误：一般性的错误提示。
- 警告信息：系统仍然正常运行，但可能存在隐患的提示信息。
- 通知信息：正常状态下的重要提示信息。
- 信息报告：一般性的提示信息。
- 调试信息：调试过程中产生的信息。

选择模块类别

选择模块类别可使日志列表中仅列出特定模块日志信息。各模块描述如下：

- 所有模块：所有模块的日志信息。
- 系统管理：与系统管理相关的日志信息，包括管理账号、设备管理以及时间设置等。
- 接口管理：接口管理模块的日志信息。
- DHCP 服务：DHCP 服务模块的日志信息。
- AP 管理：AP 管理模块的日志信息。
- AP 升级：AP 升级模块的日志信息。
- AP 数据库：AP 数据库模块的日志信息。
- 射频管理：射频管理模块的日志信息。
- 链路备份：链路备份模块的日志信息。
- Portal 认证：Portal 认证模块的日志信息。
- MAC 认证：MAC 认证模块的日志信息。
- 用户管理：用户管理模块的日志信息。
- 无线服务：无线服务模块的日志信息。
- 无线客户端：无线客户端模块的日志信息。
- 负载均衡：负载均衡模块的日志信息。

发送系统日志

若需要在某台主机上查看无线控制器日志信息，请首先在这台主机上安装日志服务器，然后勾选无线控制器日志界面上的“发送系统日志”选项，并输入这台主机的 IP 地址。保存设置后无线控制器将向指定地址发送系统日志。

备份日志信息

点击 < 备份 > 按键，设备将以文件形式备份当前设备中所有的日志内容。

日志列表

显示系统日志信息。