

**TP-LINK®**

# 无线控制器

TL-AC1000

## 用户手册

REV1.2.0  
1910040664

## 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。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

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，本手册中的所有陈述、信息等均不构成任何形式的担保。

## 目录

<b>第 1 章</b>	<b>前言</b> .....	<b>1</b>
1.1	目标读者 .....	1
1.2	本书约定 .....	1
<b>第 2 章</b>	<b>产品介绍</b> .....	<b>2</b>
2.1	产品描述 .....	2
2.2	产品特性 .....	2
2.3	产品外观 .....	3
2.3.1	前面板 .....	3
2.3.2	后面板 .....	4
<b>第 3 章</b>	<b>配置指南</b> .....	<b>5</b>
3.1	登录 WEB 界面 .....	5
3.2	WEB 界面简介 .....	6
3.2.1	界面总览 .....	6
3.2.2	界面常见按键及操作 .....	7
<b>第 4 章</b>	<b>系统维护</b> .....	<b>9</b>
4.1	系统状态 .....	9
4.2	无线状态 .....	9
4.2.1	AP 状态 .....	9
4.2.2	客户端状态 .....	10
4.3	认证状态 .....	11
4.3.1	认证状态 .....	11
4.3.2	无感知认证用户 .....	12
4.4	系统日志 .....	12
<b>第 5 章</b>	<b>基本设置</b> .....	<b>14</b>
5.1	接口设置 .....	14
5.2	DHCP 服务 .....	15

5.3	VLAN 设置 .....	18
5.3.1	VLAN 简介 .....	18
5.3.2	VLAN 设置 .....	22
5.4	交换机设置 .....	25
5.4.1	端口统计 .....	25
5.4.2	端口监控 .....	26
5.4.3	端口流量限制 .....	27
5.4.4	端口参数 .....	28
5.4.5	端口状态 .....	28
<b>第 6 章</b>	<b>认证管理 .....</b>	<b>29</b>
6.1	MAC 认证 .....	29
6.1.1	MAC 认证简介 .....	29
6.1.2	MAC 认证设置 .....	30
6.1.3	配置 MAC 认证步骤 .....	31
6.2	Portal 认证 .....	32
6.2.1	跳转页面 .....	32
6.2.2	WEB 认证 .....	38
6.2.3	微信连 WIFI .....	40
6.2.4	一键上网 .....	41
6.2.5	免认证策略 .....	42
6.2.6	配置 Portal 认证步骤 .....	44
6.3	认证服务器 .....	45
6.4	本地用户 .....	47
6.5	应用举例 .....	51
6.5.1	一键上网 .....	51
6.5.2	WEB 认证 .....	53
6.5.3	微信连 WIFI .....	56
<b>第 7 章</b>	<b>无线管理 .....</b>	<b>63</b>

7.1	无线服务.....	63
7.2	AP 管理.....	67
7.2.1	AP 设置.....	67
7.2.2	射频设置.....	70
7.2.3	AP 版本.....	73
7.2.4	AP 数据库.....	75
7.3	速率设置.....	76
7.4	负载均衡.....	78
7.5	频谱导航.....	79
<b>第 8 章</b>	<b>系统管理.....</b>	<b>82</b>
8.1	服务管理.....	82
8.1.1	服务设置.....	82
8.2	WEB 管理.....	83
8.2.1	管理信息.....	83
8.3	设备管理.....	84
8.3.1	恢复出厂配置.....	84
8.3.2	备份与导入配置.....	84
8.3.3	重启设备.....	85
8.3.4	软件升级.....	85
8.4	诊断工具.....	86
8.4.1	诊断工具.....	86
8.4.2	诊断信息.....	87
8.5	时间设置.....	87
<b>第 9 章</b>	<b>命令行简介.....</b>	<b>89</b>
9.1	搭建平台.....	89
9.2	界面模式.....	90
9.3	在线帮助.....	90
9.4	命令介绍.....	91

9.4.1	特权模式密码设置命令 .....	91
9.4.2	VLAN 配置命令 .....	91
9.4.3	系统管理 .....	92
9.4.4	历史命令管理 .....	93
9.4.5	退出 CLI .....	93
<b>附录 A</b>	<b>常见问题 .....</b>	<b>94</b>
<b>附录 B</b>	<b>规格参数 .....</b>	<b>95</b>

# 第1章 前言

本手册旨在帮助您正确使用无线控制器。内容包含对无线控制器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。

## 1.1 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。

## 1.2 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 WEB 界面的按键名称，如<确定>。
“ ”	双引号。用双引号标记的文字，表示 WEB 界面出现的除按键外名词，如“启用”。

特殊图标约定

图标	含义
 说明:	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“无线控制器”、“本产品”等名词，如无特别说明，系指 TL-AC1000 无线控制器。

## 第2章 产品介绍

### 2.1 产品描述

TL-AC1000是针对酒店、商场、企业、学校等中大型无线网络环境而推出的一款高性能无线控制器，采用基于双核网络专用处理器的硬件平台，可以统一管理TP-LINK所有的吸顶式、面板式、桌面式和室外高功率无线AP产品，支持管理的AP数目高达1000个。TL-AC1000可对整个无线网络进行精细化的统一管理，实现AP零配置接入、即插即用，提供运行状态监控、AP管理、射频管理、负载均衡、频谱导航、MAC认证、Portal认证等丰富的软件功能。

### 2.2 产品特性

#### 硬件特性

采用64位双核网络专用处理器，单核主频500MHz；

配备容量为256MB的DDRII高速内存；

提供5个10/100/1000M自适应以太网接口；

提供1个Console口；

内置高品质开关电源，无风扇静音设计；

1U钢壳，可安装于19英寸标准机架，工业级设计。

#### 功能特性

##### 无线管理

统一设置无线服务，包括SSID（支持中文）、VLAN ID、认证服务、安全选项等属性，并实现无线服务与射频的绑定，灵活适应各种网络需求。

统一管理无线网络中的所有AP，支持多AC设备链路备份功能，支持批量设置AP的射频属性，包括射频模式、带宽模式、信道、发射功率等，并可限制每个射频单元允许接入的无线客户端数目，防止单个AP过载。

设备内置DHCP服务器，可为无线网络中的所有AP分配IP地址，并可通过客户端列表查看DHCP客户端信息。

支持设置Tag VLAN，通过SSID与Tag VLAN关联，实现不同SSID之间的隔离，防止广播风暴，并可针对不同的VLAN设置不同的网络权限。

支持基于会话的负载均衡，当AP的接入终端数目同时达到设定的门限和差值门限时，启动负载均衡，使得每个AP的接入终端数趋于平均；支持多频段AP频谱导航功能，充分利用频带资源，保证2.4GHz和5GHz的频段均衡通信。



支持AP软件统一升级，只需上传最新版AP软件至设备中，设备即可将最新软件推送到无线网络中所有的AP，当有新AP接入时，设备会自动升级该AP的软件。

### 认证管理

MAC认证：启用MAC认证后，只有MAC地址经过认证的无线终端才能接入对应的SSID，确保员工网络的数据安全。

Portal认证：支持一键上网、WEB认证、微信连WIFI等认证方式，支持本地认证、远程POST认证，允许设置Radius认证计费服务器，可根据不同的需求灵活配置不同的认证策略。

### 管理维护

支持在WEB界面上查看系统资源状态、AP状态、无线客户端状态、认证状态、系统日志等信息，整个无线网络运行状态一目了然。

支持修改管理账户、恢复出厂配置、备份配置、恢复配置、软件升级、时间设置等多种管理功能，方便设备管理维护。

支持Ping检测及Tracert检测，方便快速确认网络连通状态。

## 2.3 产品外观

### 2.3.1 前面板

TL-AC1000的前面板由5个RJ45接口、1个Console接口、指示灯和Reset键组成。如图 2.1所示。

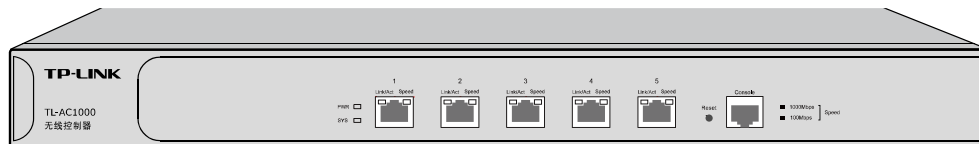


图 2.1 TL-AC1000前面板示意图

#### 5个10/100/1000Mbps自适应RJ45接口

TL-AC1000支持10Mbps/100Mbps/1000Mbps速率的连接设备。每个接口对应一组指示灯，即Link/Act和Speed指示灯。

#### 1个Console接口

Console接口位于面板最右边，使用此接口可以对无线控制器进行命令行配置，详见[命令行简介](#)。

#### Reset键

复位键。在无线控制器通电的情况下，使用尖状物按住无线控制器的Reset键，等待2-5秒后，见到系统指示灯快速闪烁1-2秒，松开按键，无线控制器将自动恢复出厂设置并重启。无线控制器出厂默认管理地址是http://192.168.1.253，需要自行设置登录用户名和密码。

## 指示灯

指示灯包括PWR电源指示灯, SYS系统指示灯, Link/Act连接状态指示灯, Speed速率指示灯。通过指示灯可以监控无线控制器的工作状态, 下表将详细说明指示灯工作状态:

指示灯	名称	状态描述
PWR	电源指示灯	常亮表示系统供电正常
		常灭表示电源关闭或电源故障
SYS	系统指示灯	系统正常工作时以每秒 1 次的频率闪烁, 其他状态表示系统异常
Link/Act	连接状态指示灯	常亮表示相应端口已正常连接
		闪烁表示相应端口正在传输数据
		常灭表示相应端口未建立连接
Speed	速率指示灯	常亮绿色表示相应端口工作在 1000Mbps 模式
		常亮黄色表示相应端口工作在 100Mbps 模式
		常灭表示相应端口工作在 10Mbps 模式或链路未建立

## 2.3.2 后面板

无线控制器后面板由电源接口和防雷接地柱组成, 如图 2.2所示:

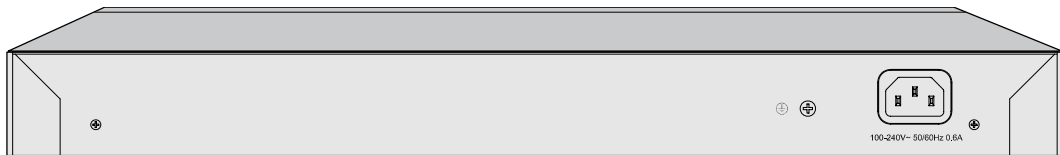


图 2.2 后面板示意图

### 电源接口

位于后面板右侧, 设备正常工作时的输入电源参数为100~240V~ 50/60Hz, 最大工作电流不超过0.6A, 为保证设备及电源设施正常工作, 请确保供电电源完全满足设备的要求。

### 防雷接地柱

请使用黄绿双色外皮的铜芯导线接地, 以防雷击, 具体请参考《设备防雷安装手册》。



#### 说明:

- 请使用原装电源线。
- 电源插座请安装在设备附近便于触及的位置, 以方便操作。

## 第3章 配置指南

### 3.1 登录 WEB 界面

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) 管理主机已正确安装有线网卡及该网卡的驱动程序。
- 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，或最新版本的FireFox、Chrome和Safari浏览器。
- 4) 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。
- 5) 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。

打开IE浏览器，在地址栏输入<http://192.168.1.253>登录无线控制器的WEB管理界面。



首次登录无线控制器需自行设置无线控制器管理账号的用户名和密码，界面如图 3.1所示。成功登录后将看到无线控制器的WEB管理界面，如图 3.2所示。

A screenshot of the TP-LINK login interface. At the top, there is a blue header with the "TP-LINK" logo in white. Below the header, the interface is light gray. It contains three input fields: "设置用户名:" followed by a text box, "设置密码:" followed by a text box, and "确认密码:" followed by a text box. Below these fields is a note in Chinese: "注意：确定提交前请记住并妥善保管用户名和密码。如遗忘，只能恢复出厂设置，重新设置设备的所有参数。" At the bottom center, there is a button labeled "确定".

图 3.1 无线控制器登录界面



图 3.2 无线控制器WEB管理界面

## 3.2 WEB 界面简介

### 3.2.1 界面总览

本无线控制器典型的WEB界面如下图所示。



图 3.3 典型WEB界面

在图 3.4典型WEB界面区域划分中可以看到，左侧为一级、二级菜单栏，右侧上方长条区域为菜单下的标签页，当一个菜单包含多个标签页时，可以通过点击标签页的标题在同级菜单下切换标签页。右侧标签页下方区域为功能设置区，此区域可分为两种类型，列表管理区和条目配置区。



图 3.4 典型WEB界面区域划分-列表管理区

### 3.2.2 界面常见按键及操作

按键	含义
	保存最终的配置。
	退出 WEB 界面。






#### 说明：

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>按键。建议在断电重启前<保存配置>，以免丢失配置信息。

#### 列表管理区常见按键：

按键	含义
	新增配置条目。
	选中当前列表中所有条目。
	启用选中的列表条目。
	禁用选中的列表条目。
	删除选中的条目，可批量操作。
	重启选中的 AP 设备，可批量操作。
	断开选中的客户端，可批量操作。
	点击后弹出搜索对话框，可以根据输入条件快速搜索条目，但仅限于搜索当前界面显示的条目。
	刷新列表。
	打开当前功能的帮助界面。

## 列表管理区常见操作：

按键	名称及含义
	编辑操作。点击后，会弹出需要编辑的条目，修改当前配置后，点击<确定>按钮保存生效。该操作不可批量进行。
	启用操作。点击后，修改当前条目状态为启用。该操作不可批量进行。
	禁用操作。点击后，修改当前条目状态为禁用。该操作不可批量进行。

## 条目配置区常见按键：

按键	含义
	提交当前的配置。
	提交当前配置条目。
	快速清空当前配置项中的所有信息。
	取消新增当前条目，返回条目列表界面。

## 第4章 系统维护

### 4.1 系统状态

进入界面：系统维护 >> 系统状态 >> 系统状态



图 4.1 系统状态界面

在初始界面中，可以在CPU利用率区域监测两个CPU的利用率。CPU利用率平均推荐值为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，部分功能可能将异常，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< + >按钮选择接口查看接口信息。

### 4.2 无线状态

#### 4.2.1 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：系统维护 >> 无线状态 >> AP状态

AP列表												
选择	序号	名称	型号	MAC地址	IP地址	2.4GHz射频		5GHz射频		SSID	链路状态	设置
						用户数	信道	用户数	信道			
<input type="checkbox"/>	1	TL-AP302I-PoE-0001	TL-AP302I-PoE	00-0A-EB-13-1A-52	192.168.1.51	0	5	---	---	详细	主用	

共1条，每页：20 条 | 当前：1/1页，1~1条 | [首页](#) [上一页](#) [下一页](#) [尾页](#)  [跳转](#)

[全选](#) [重启](#) [打开LED](#) [关闭LED](#) [刷新](#) [搜索](#) [帮助](#)

图 4.2 AP状态界面

名称	显示接入无线控制器的 AP 的名称。
型号	显示接入无线控制器的 AP 的型号。
MAC 地址	显示接入无线控制器的 AP 的 MAC 地址。
IP 地址	显示接入无线控制器的 AP 的 IP 地址。
用户数	分别显示该 AP 的 2.4GHz 射频和 5GHz 射频当前接入的用户数。
信道	分别显示该 AP 的 2.4GHz 射频和 5GHz 射频当前使用的无线信道。
SSID	点击“详细”链接，在弹出窗口显示当前 AP 绑定的无线网络，如图 4.3 所示。 如需绑定无线网络，请参考 <a href="#">无线服务</a> 。
链路状态	显示接入 AP 的链路状态是主链路还是备份链路。
设置	点击  按钮，可以重启对应 AP。当 AP 的链路状态为备份链路时，按钮不能重启 AP，只能重启 AP 与当前 AC 的连接。  点击  /  按钮来开启或关闭 AP 的 LED 指示灯。当 AP 的链路状态为备份链路时，按钮不生效。

表 4.1 AP状态界面项说明

绑定的2.4G无线服务列表					
序号	SSID	描述	VLAN ID	安全选项	状态
1	TP-LINK_AC1000	default_ssid	---	---	已启用
2	SSID中文[GBK]	中文	1	WPA-PSK/WPA2-PSK	已启用

绑定的5G无线服务列表					
序号	SSID	描述	VLAN ID	安全选项	状态
该列表为空					

图 4.3 AP状态-SSID详细界面

## 4.2.2 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：系统维护 >> 无线状态 >> 客户端状态

全局搜索									
搜索方式： <input type="text" value="MAC地址"/> 搜索内容： <input type="text"/> <input type="button" value="搜索"/>									
STA列表									
选择	序号	MAC地址	AP名称	射频单元	SSID	VLAN ID	接入时间	信号强度	设置
<input type="checkbox"/>	1	A8-A6-68-18-6A-DE	TL-AP302I-PoE-0001	2.4GHz	SSID中文[GBK]	1	2015-07-30 14:28:42	-71dBm	

共1条，每页：条 | 当前：1/1页，1~1条 | [首页](#) [上一页](#) **1** [下一页](#) [尾页](#)

图 4.4 客户端状态界面



## 全局搜索

在此可以根据客户端设备的MAC地址进行搜索。输入MAC地址，点击<搜索>按钮，列表页面将显示搜索结果。

## STA 列表

MAC 地址	客户端的 MAC 地址。
AP 名称	客户端接入 AP 的名称。
射频单元	客户端接入 AP 的射频单元。
SSID	客户端接入 AP 的 SSID。
VLAN ID	客户端接入的 VLAN ID。
接入时间	客户端接入 AP 的时间。
信号强度	客户端的信号强度。
设置	点击<-+>按键，可以断开对应客户端的连接。

表 4.2 客户端状态界面项说明

## 4.3 认证状态

### 4.3.1 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：系统维护 >> 认证状态 >> 认证状态

认证用户列表							
选择	序号	认证方式	用户名	MAC地址	VLAN ID	登录时间	设置
<input type="checkbox"/>	1	Web认证-本地认证	user1	A8-A6-68-18-6A-DE	1	2015-08-17 09:56:36	-+

共1条, 每页: 10 条 | 当前: 1/1页, 1~1条 | [首页](#) [上一页](#) [下一页](#) [尾页](#)  [跳转](#)

[刷新](#) [全选](#) [断开](#) [搜索](#) [帮助](#)

图 4.5 认证状态界面

认证方式	用户登录所使用的认证类型。
用户名	当前认证成功用户名。
MAC 地址	当前认证成功用户设备的 MAC 地址。
VLAN	当前认证成功的用户设备所属的 VLAN。
登录时间	用户登录的时间。
设置	点击<-+>按键，可以断开对应用户的连接。

表 4.3 认证状态界面项说明

## 4.3.2 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。如需启用无感知认证，请参考 [WEB 认证](#)。

无感知认证用户列表							
选择	序号	VLAN	MAC地址	用户名	密码	认证时间	设置
<input type="checkbox"/>	1	1	A8-A6-68-18-6A-DE	user1	123	2015-08-17 09:56:37	

共1条，每页：10 条 | 当前：1/1页，1~1条 | [首页](#) [上一页](#) [1](#) [下一页](#) [尾页](#)  [跳转](#)

[清空](#) [刷新](#) [全选](#) [删除](#) [搜索](#) [帮助](#)

图 4.6 无感知认证用户界面

VLAN	无感知认证用户认证时所属的 VLAN
MAC 地址	无感知认证用户认证时的 MAC 地址。
用户名	无感知认证用户认证时的用户名。
密码	无感知认证用户认证时的密码。
认证时间	无感知认证用户最后一次认证的时间。
设置	点击  按键，可以删除该无感知认证用户。

表 4.4 无感知认证用户界面项说明

## 4.4 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：[系统维护](#) >> [系统日志](#) >> [系统日志](#)

日志列表			
序号	时间	日志等级	日志内容
2	2015-08-10 09:55:48	<5> 通知信息	用户 admin (IP地址: 192.168.1.200) 登陆Web服务器成功
1	2015-08-10 09:55:46	<5> 通知信息	用户 admin 认证成功

[刷新](#) [清空日志](#)

日志设置	
<input checked="" type="checkbox"/>	启用自动刷新
选择日志等级：	<5> 通知信息
<input type="checkbox"/>	发送系统日志
服务器地址：	0.0.0.0

[设置](#) [帮助](#)

图 4.7 系统日志界面

### 日志列表

日志列表中一条日志内容可分为四个部分：

<u>2022-03-15</u>	<u>07:03:54</u>		<u>&lt;5&gt;通知信息</u>		<u>用户admin认证成功</u>
日期	时间		日志等级		系统事件

### 日志设置

在此区域可以对日志系统进行简单的配置：

- 1) 启用自动刷新后，日志列表将每隔 5 秒刷新一次。
- 2) 选择日志等级可使日志列表中列出高于或等于指定等级的日志记录。各等级描述：

<0> 致命错误	导致系统不可用的错误，红色显示。
<1> 紧急错误	必须对其采取紧急措施的错误，红色显示。
<2> 严重错误	导致系统处于危险状态的错误，红色显示。
<3> 一般错误	一般性的错误提示，橙色显示。
<4> 警告信息	系统仍然正常运行，但可能存在隐患的提示信息，橙色显示。
<5> 通知信息	正常状态下的重要提示信息。
<6> 消息报告	一般性的提示信息。
<7> 调试信息	调试过程产生的信息。

- 3) 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。

## 第5章 基本设置

### 5.1 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: 基本设置 >> 接口设置 >> 接口设置

接口列表								
选择	序号	接口名称	VLAN ID	MAC地址	IP地址	子网掩码	状态	设置
<input type="checkbox"/>	1	eth0	1	3C-46-D8-13-30-ED	192.168.1.253	255.255.255.0	已连接	

图 5.1 接口设置界面

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。

接口设置	
接口名称:	<input type="text"/> (1-15个英文字符)
VLAN ID:	<input type="text"/> ▼
IP地址:	<input type="text" value="0.0.0.0"/>
子网掩码:	<input type="text" value="255.255.255.0"/>
网关地址:	<input type="text" value="0.0.0.0"/> (可选)
MTU:	<input type="text" value="1500"/> (576-1500)
首选DNS服务器:	<input type="text" value="0.0.0.0"/> (可选)
备用DNS服务器:	<input type="text" value="0.0.0.0"/> (可选)
MAC地址:	<input type="text" value="3C-46-D8-13-30-EE"/> (XX-XX-XX-XX-XX-XX)

图 5.2 新增接口界面

接口名称	输入一个名称来标识一个接口。只支持英文、数字以及\.\_ - @六个特殊字符,最多可以输入 15 个字符。
VLAN ID	选择该接口指向的 VLAN。
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,允许留空。
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 DNS 服务器的 IP 地址,允许留空。

MAC 地址

设置接口的 MAC 地址。

表 5.1 新增接口界面条目项说明

**配置接口步骤：**

- 1) 创建 VLAN。必须操作。具体操作步骤请参考[配置 VLAN 步骤](#)。
- 2) 创建接口。必须操作。设置界面：**基本设置 >> 接口设置 >> 接口设置**，点击<新增>按钮，在显示的设置界面，输入接口名称，选择链接的VLAN，输入IP地址、MAC地址等必要信息，点击<确定>按钮完成。

## 5.2 DHCP 服务

TL-AC1000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。

DHCP服务功能配置主要分为[配置IP地址池](#)、[配置DHCP服务器](#)、[查看当前所有DHCP客户端](#)和[静态地址分配](#)四个部分。

### 1. 配置 IP 地址池

进入界面：**基本设置 >> DHCP服务 >> 地址池**

地址池列表					
选择	序号	地址池名称	地址池范围	状态	设置
<input type="checkbox"/>	1	default_dhcp	192.168.1.200-192.168.1.249	已启用	 

图 5.3 地址池界面

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地址池。点击<新增>按钮可以添加新条目，新增DHCP服务条目界面如下图所示。

地址池设置	
地址池名称：	<input type="text"/> (1-50个字符)
地址池范围：	<input type="text"/> - <input type="text"/>
启用/禁用：	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
<input type="button" value="确定"/> <input type="button" value="清除"/> <input type="button" value="取消"/> <input type="button" value="帮助"/>	

图 5.4 新增地址池界面

地址池名称	添加对本条目的说明信息。
地址池范围	输入可供分配的地址段起始地址和结束地址。
启用/禁用	选择“启用”，则使该地址池生效； 选择“禁用”，则使该地址池失效。

表 5.2 新增地址池界面条目项说明

## 2. 配置 DHCP 服务器

地址池创建完成后，需要在 DHCP 服务界面配置 DHCP 服务器参数。

进入界面：基本设置 >> DHCP服务 >> DHCP服务

图 5.5 DHCP服务界面

### 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一个DHCP服务。

点击<新增>按钮可以添加新条目，新增DHCP服务条目界面如下图所示。

图 5.6 新增DHCP服务界面

服务接口	选择需提供 DHCP 服务的接口。如需新增接口，请参考 <a href="#">接口设置</a> 。
地址池	选择已创建的地址池。如需新建地址池，请参考 <a href="#">配置 IP 地址池</a> 。 对于特殊地址，包括接口的 IP 地址、主机位为 0 的网络地址和主机位全为 1 的网络广播地址，本无线控制器不会进行分配。
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，推荐将服务接口 IP 地址配置为默认网关。
缺省域名	输入本地网域名。
首选 DNS 服务器	输入 ISP 提供的 DNS 服务器，若不清楚可以向 ISP 询问。
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。
启用/禁用服务	选择“启用”，则使该服务条目生效； 选择“禁用”，则使该服务条目失效。

表 5.3 新增DHCP服务界面条目项说明

### 3. 查看当前所有 DHCP 客户端

进入界面：基本设置 >> DHCP服务 >> 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，如下图所示。

客户端列表					
序号	主机名	服务接口	MAC地址	IP地址	剩余租期
1	android-892cf48eb5 f6758d	eth0	D4-97-0B-B2-41-68	192.168.1.241	01:36:43
2	android-813f301430 c3ca81	eth0	A8-A6-68-18-6A-DE	192.168.1.242	01:37:53
3	---	eth0	00-0A-EB-13-1A-29	192.168.1.240	01:58:52

共3条，每页： 条 | 当前：1/1页，1~3条 | [首页](#) [上一页](#) [下一页](#) [尾页](#)  [跳转](#)

[刷新](#) [搜索](#) [帮助](#)

图 5.7 DHCP服务器客户端列表界面

### 4. 静态地址分配

进入界面：基本设置 >> DHCP服务 >> 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。

静态地址							
MAC地址：	<input type="text"/>	(XX-XX-XX-XX-XX-XX)					
IP地址：	<input type="text"/>						
生效接口：	<input type="text" value="eth0"/>	▼					
备注：	<input type="text"/>	(1-50个字符，可选)					
是否生效：	<input checked="" type="radio"/> 生效	<input type="radio"/> 不生效					
<input type="button" value="新增"/> <input type="button" value="清除"/> <input type="button" value="帮助"/>							
地址列表							
选择	序号	MAC地址	IP地址	服务接口	备注	状态	设置
该列表为空							
<input type="button" value="全选"/> <input type="button" value="启用"/> <input type="button" value="禁用"/> <input type="button" value="删除"/> <input type="button" value="搜索"/>							

图 5.8 静态地址分配界面

## 静态地址

在此区域根据需要设置为特定MAC地址预留的IP地址。

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。
生效接口	设置当前静态地址条目所生效的接口。这类接口必须已经配置了 DHCP 服务器规则。
备注	设置静态地址分配条目备注，以方便管理和查找。备注最多支持 50 个字符。
是否生效	选择是否生效当前设置。

### 配置DHCP服务步骤：

- 1) 创建接口。必须操作。具体操作步骤请参考[配置接口步骤](#)。
- 2) 配置 IP 地址池。必须操作。配置界面：基本设置 >> DHCP 服务 >> 地址池，点击<新增>按键，在显示的设置界面，输入地址池名称和范围，选择“启用”，点击<确定>按键完成。
- 3) 配置DHCP服务器。必须操作。配置界面：基本设置 >> DHCP服务 >> DHCP服务，点击<新增>按键，在显示的设置界面，选择服务接口、地址池，设置地址租期等信息，选择“启用”，点击<确定>按键完成。
- 4) 配置静态地址分配。非必须操作。配置界面：基本设置 >> DHCP服务 >> 静态地址分配，输入MAC地址和要求的IP地址，选择生效接口，填写备注等信息，点击<新增>按键完成。
- 5) 查看当前所有DHCP客户端。非必须操作。查看界面：基本设置 >> DHCP服务 >> 客户端列表，在此界面可以查看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。

## 5.3 VLAN 设置

### 5.3.1 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。

#### 1. 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。

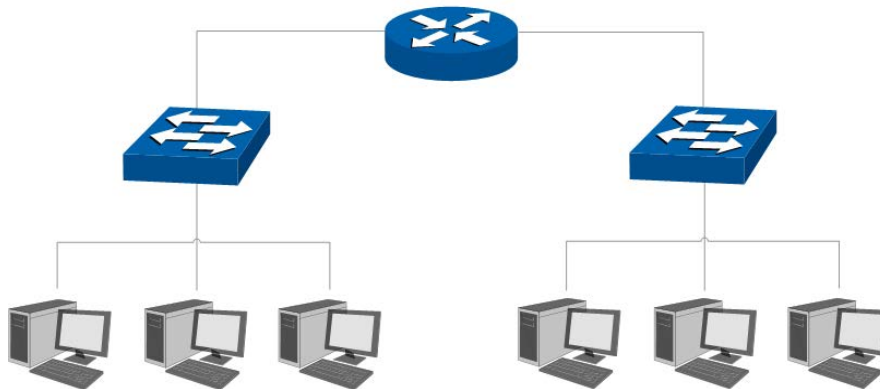


图 5.9 典型局域网拓扑

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。

## 2. 技术特点

以下是VLAN在实际网络应用中的常用基础拓扑。

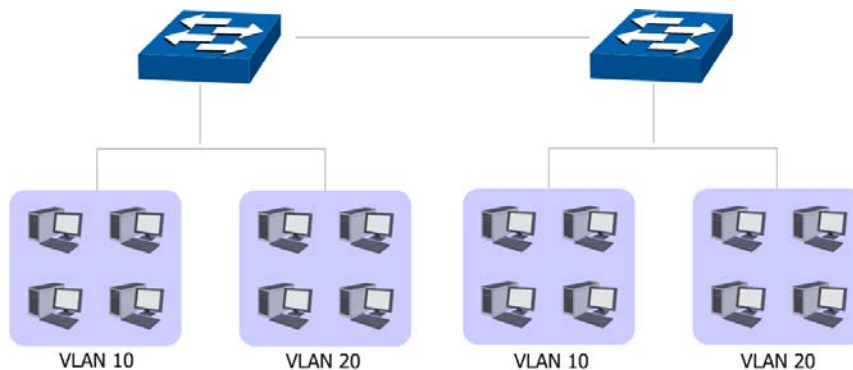


图 5.10 VLAN常用网络拓扑

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。

### 3. 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 5.10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。

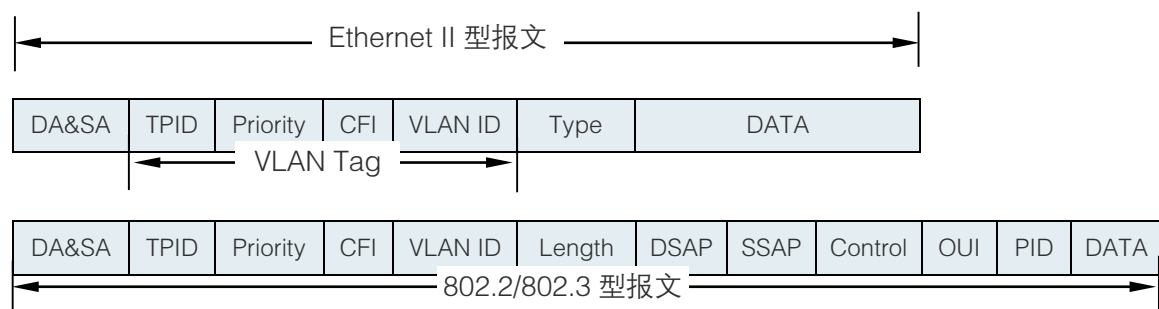


图 5.11 VLAN Tag组成字段

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。

表 5.4 Tag 字段含义

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。TL-AC1000是基于端口实现的VLAN。

#### 4. 端口的链路类型

在创建802.1Q VLAN时，需要根据端口连接的设备设置端口的链路类型。端口的链路类型有下面三种：

**Access：**端口只能属于1个VLAN，出口规则为UNTAG，即从此端口发送出去的报文不带VLAN Tag，多为连接用户终端设备的端口。如图 5.11所示，设备和普通计算机相连，计算机不能识别带VLAN Tag的报文，所以需要将设备和计算机相连端口的链路类型设置为Access。当Access类型端口加入到其它VLAN时，自动退出原有VLAN。

**Trunk：**端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，常用于网络设备之间级连。如图 5.11所示，需要将设备1和设备2相连端口的链路类型设置为Trunk。在网络中VLAN经常跨接在不同通信设备上，Trunk类型端口的出口规则为TAG，即从此端口发送出去的报文带有VLAN Tag，能够保证在转发各种VLAN的数据包时不改变其携带的VLAN信息。

**General：**端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，可以用于网络设备之间连接，也可以用于连接用户设备。如图 5.11所示，与设备2相连的某个网络环境复杂，无法判断网络中的设备是哪种类型或是该网络中有多种类型的设备时，需要将设备2和该网络相连端口的链路类型设置为General。General类型端口的出口规则可以根据该端口连接设备的实际情况灵活配置。

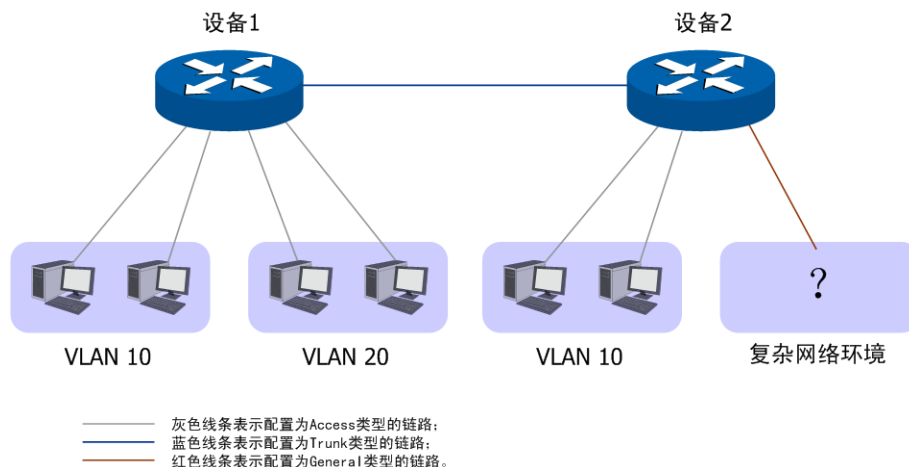


图 5.12 链路类型配置示意图

端口的链路类型本质上是通信设备接收和转发数据帧的处理方式。在实际组网中，根据不同的网络需求，可以为每个端口指定出口规则和入口规则，入口规则表示接收数据帧时的处理方式，出口规则表示转发数据帧时的处理方式。下面详细介绍端口出口规则和入口规则。

Access	<p>接收报文时： 如果报文不带 Tag，则接收报文，并为报文添加缺省的 VLAN； 如果报文带 Tag 且 VLAN ID = 端口 PVID，则接收报文； 如果报文带 Tag 而 VLAN ID ≠ 端口 PVID，则丢弃报文。</p> <p>发送报文时： 去掉 Tag 后，发送报文。</p>
Trunk	<p>接收报文时： 如果报文不带 Tag，则为报文添加缺省 VLAN 的 Tag； 如果报文带 Tag 且 VLAN ID 属于端口允许通过的 VLAN ID，则接收报文； 如果报文带 Tag 而 VLAN ID 不属于端口允许通过的 VLAN ID，则丢弃报文。</p> <p>发送报文时： 保持原有 Tag 发送报文。</p>
General	<p>接收报文时： 如果报文不带 Tag，则为报文添加缺省 VLAN 的 Tag； 如果报文带 Tag 且 VLAN ID 属于端口允许通过的 VLAN ID，则接收报文； 如果报文带 Tag 而 VLAN ID 不属于端口允许通过的 VLAN ID，则丢弃报文。</p> <p>发送报文时： 当出口规则配置为 TAG 时，保持原有 Tag 发送报文。 当出口规则配置为 UNTAG 时，去 Tag 后发送报文。</p>

表 5.5 端口出口规则与入口规则

## 5. 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。

对于不同链路类型的端口，设置PVID时会不同：若端口链路类型为Access，因为该端口只能属于一个VLAN，所以该端口的PVID不可设置。若端口链路类型为Trunk或General，因为该端口可以属于多个VLAN，所以可以设置，但所设置的PVID必须是该端口所属VLAN之一。

### 5.3.2 VLAN 设置

设置VLAN时，需要设置报文中Tag字段的VLAN ID数值，物理接口的PVID数值和VLAN成员端口的链路类型。

## 1. 设置 VLAN ID

进入界面：基本设置 >> VLAN设置 >> VLAN设置

VLAN列表						
选择	序号	VLAN ID	名称	端口设置	备注	设置
<input type="checkbox"/>	1	1	vlan1	1(UNTAG),2(UNTAG),3(UNTAG),4(UNTAG),5(UNTAG)	system vlan	

新增 全选 删除 搜索

图 5.13 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。

VLAN设置																					
VLAN ID :	<input type="text"/>	( 2-4094 )																			
名称 :	<input type="text"/>																				
端口设置 :	<table border="1"> <thead> <tr> <th><input type="checkbox"/> 端口</th> <th>链路类型</th> <th>TAG标签</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> 1</td> <td>Access</td> <td>UNTAG</td> </tr> <tr> <td><input type="checkbox"/> 2</td> <td>Access</td> <td>UNTAG</td> </tr> <tr> <td><input type="checkbox"/> 3</td> <td>Access</td> <td>UNTAG</td> </tr> <tr> <td><input type="checkbox"/> 4</td> <td>Access</td> <td>UNTAG</td> </tr> <tr> <td><input type="checkbox"/> 5</td> <td>Access</td> <td>UNTAG</td> </tr> </tbody> </table>			<input type="checkbox"/> 端口	链路类型	TAG标签	<input type="checkbox"/> 1	Access	UNTAG	<input type="checkbox"/> 2	Access	UNTAG	<input type="checkbox"/> 3	Access	UNTAG	<input type="checkbox"/> 4	Access	UNTAG	<input type="checkbox"/> 5	Access	UNTAG
<input type="checkbox"/> 端口	链路类型	TAG标签																			
<input type="checkbox"/> 1	Access	UNTAG																			
<input type="checkbox"/> 2	Access	UNTAG																			
<input type="checkbox"/> 3	Access	UNTAG																			
<input type="checkbox"/> 4	Access	UNTAG																			
<input type="checkbox"/> 5	Access	UNTAG																			
备注 :	<input type="text"/>	( 可选 )																			
<p>确定 清除 取消 帮助</p>																					

图 5.14 新增VLAN界面

VLAN ID	设置 Tag 字段的 VLAN ID 数值，可设置范围为 2-4094。
名称	输入一个名称来标识该 VLAN。
端口设置	此处勾选相应端口。端口链路类型的选择需要到端口设置界面进行，而链路类型不同，TAG 标签会有所不同。端口设置请参考 <a href="#">设置 PVID 和链路类型</a> 。
备注	添加对本条目的说明信息，非必填项。

表 5.6 新增VLAN界面条目项说明

### 说明：

- 如果新增条目的端口链路类型是Access，则该端口将会被从之前所属的VLAN中去除，添加到新设置的VLAN中。
- 如果在设置 VLAN 时，导致某个端口不属于任何一个 VLAN，则该端口将会被默认添加到系统 VLAN 中，其 PVID 为 1，TAG 标签根据链路类型来决定，Access 和 General 时为 UNTAG，Trunk 时为 TAG。

## 2. 设置 PVID 和链路类型

进入界面：基本设置 >> VLAN设置 >> 端口设置

在此界面可以选择端口链路类型或者设置端口的PVID。

端口设置		
端口	链路类型	PVID
1	access	1
2	trunk	1
3	general	1
4	access	1
5	access	1

设置 帮助

图 5.15 端口设置界面

端口	显示所有物理接口。
链路类型	选择端口链路类型，可选项有 access、trunk 和 general，详细介绍请参考 <a href="#">端口的链路类型</a> 。
PVID	设置端口的 PVID，详细介绍请参考 <a href="#">PVID</a> 。

表 5.7 端口设置界面条目项说明

**说明：**

- 每个端口的链路类型和PVID一次只能修改一项，两者不可以同时修改。
- 系统可能会根据端口的链路类型和所属VLAN的改变而自动修改端口的PVID。
- 如果端口的PVID所关联的VLAN条目被删除，则该端口将可能无法收发报文，需要用户重新为该端口设置一个合法的PVID。

### 3. 查看端口和 VLAN 的关联信息

设置完成后可以在关联表界面查看相关信息。

进入界面：基本设置 >> VLAN设置 >> 关联表

关联表		
端口	链路类型	端口所属Vlan
1	Access	1(UNTAG)
2	Trunk	1(TAG)
3	General	1(UNTAG)
4	Access	1(UNTAG)
5	Access	1(UNTAG)

帮助

图 5.16 关联表界面

#### 配置VLAN步骤：

- 1) 设置端口链路类型。必须操作。设置界面：基本设置 >> VLAN设置 >> 端口设置，在此界面根据端口连接的设备选择其链路类型，点击<设置>按键完成。
- 2) 创建VLAN。必须操作。设置界面：基本设置 >> VLAN设置 >> VLAN设置，点击<新增>按键，在显示的设置界面，设置VLAN ID，输入VLAN名称，勾选VLAN包含的端口，点击<确定>按键完成。

- 3) 设置端口的PVID。非必须操作。设置界面：基本设置 >> VLAN设置 >> 端口设置，当某个端口有多个VLAN ID时，可以在此设置其默认PVID。
- 4) 查看端口VLAN信息。非必须操作。查看界面：基本设置 >> VLAN设置 >> 关联表，在此界面可以查看每个端口对应的链路类型、PVID和出口规则。

## 5.4 交换机设置

TL-AC1000无线控制器具备一些简单的交换机端口管理功能。在此可以实时查看无线控制器各端口的数据流通状况，并进行相应的控制和管理。

### 5.4.1 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：基本设置 >> 交换机设置 >> 端口统计

统计列表						
参数	端口1	端口2	端口3	端口4	端口5	
接收	单播帧	0	6506	0	0	0
	广播帧	0	946	0	0	0
	流控帧	0	0	0	0	0
	多播帧	0	71	0	0	0
	所有帧	0	793342	0	0	0
	过小帧	0	0	0	0	0
	正常帧	0	7523	0	0	0
发送	单播帧	0	9928	0	0	0
	广播帧	0	1	0	0	0
	流控帧	0	0	0	0	0
	多播帧	0	0	0	0	0
	所有帧	0	8048356	0	0	0

刷新    清空所有    帮助

图 5.17 端口统计界面

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。
所有帧	接收/发送所有的数据帧的总字节数（包含校验和错误的帧）。
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 字节到最大帧长之间的数据帧数目（包含错误帧）。对于不带 tag 标签的帧，无线控制器支持的最大帧长为 1518 字节；对于带 tag 标签的帧，无线控制器支持的最大帧长为 1522 字节。
过大帧	收到的长度大于最大帧长的数据帧数目（包含错误帧）。

表 5.8 端口统计界面项说明

点击<清空所有>按键可以一次清空所有统计数据。

## 5.4.2 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：基本设置 >> 交换机设置 >> 端口监控

**功能设置**

启用端口监控

监控模式：

**监控列表**

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

图 5.18 端口监控界面

### 功能设置

启用端口监控	勾选即启用端口监控。推荐勾选，方便及时了解无线控制器端口报文信息。
监控模式	选择对数据包进行“输出监控”、“输入监控”或“输入输出监控”。

表 5.9 端口监控-功能设置界面项说明

### 监控列表

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。

表 5.10 端口监控-监控列表界面项说明

## 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，如图 5.18所示。设置完成后，点击<设置>按键。

功能设置

启用端口监控

监控模式： ▼

监控列表

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

图 5.19 端口监控应用举例界面

### 5.4.3 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：基本设置 >> 交换机设置 >> 端口流量限制

功能设置

端口	入口限制状态	入口限制模式	入口限制速率(Mbps)	出口限制状态	出口限制速率(Mbps)
1	<input checked="" type="checkbox"/> 启用	所有帧 ▼	<input type="text" value="1"/>	<input type="checkbox"/> 启用	<input type="text" value="1"/>
2	<input type="checkbox"/> 启用	所有帧 ▼	<input type="text" value="1"/>	<input type="checkbox"/> 启用	<input type="text" value="1"/>
3	<input checked="" type="checkbox"/> 启用	所有帧 ▼	<input type="text" value="1"/>	<input type="checkbox"/> 启用	<input type="text" value="1"/>
4	<input type="checkbox"/> 启用	所有帧 ▼	<input type="text" value="1"/>	<input type="checkbox"/> 启用	<input type="text" value="1"/>
5	<input type="checkbox"/> 启用	所有帧 ▼	<input type="text" value="1"/>	<input type="checkbox"/> 启用	<input type="text" value="1"/>

图 5.20 端口流量限制界面

端口	显示所有物理端口，需要对某个端口进行流量限制时，在其对应行设置即可。
入口限制状态	勾选“启用”后，后续设置的入口限制模式和速率才会生效。
入口限制模式	有“所有帧”、“广播和多播”和“广播”三种模式，选择其一。
入口限制速率	设置入口限制速率。
出口限制状态	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。

表 5.11 端口流量限制界面项说明

## 5.4.4 端口参数

可以在此启用各物理端口及其流量限制，并根据需要设定其协商模式。

进入界面：基本设置 >> 交换机设置 >> 端口参数

功能设置			
端口	端口状态	流量控制	协商模式
1	<input checked="" type="checkbox"/> 启用	<input checked="" type="checkbox"/> 启用	100M 半双工
2	<input checked="" type="checkbox"/> 启用	<input checked="" type="checkbox"/> 启用	自协商
3	<input checked="" type="checkbox"/> 启用	<input checked="" type="checkbox"/> 启用	10M 全双工
4	<input checked="" type="checkbox"/> 启用	<input checked="" type="checkbox"/> 启用	自协商
5	<input checked="" type="checkbox"/> 启用	<input checked="" type="checkbox"/> 启用	自协商
所有端口	--	--	--

图 5.21 端口参数界面

端口状态	只有勾选了“启用”该端口才会有数据包的传输，即物理意义上的开启。
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。
所有端口	这一栏可对以上所有端口进行统一设置，比如同时启用或禁用。

表 5.12 端口参数界面项说明

## 5.4.5 端口状态

可以在此查看各个端口的基本状态。

进入界面：基本设置 >> 交换机设置 >> 端口状态

状态列表				
端口	端口状态	连接速率(Mbps)	双工模式(Mbps)	流量控制
1	未连接	---	---	---
2	已连接	100	全双工	禁用
3	未连接	---	---	---
4	未连接	---	---	---
5	未连接	---	---	---

图 5.22 端口状态界面

## 第6章 认证管理

网络管理员可以预先对网络资源进行划分：一部分直接提供给接入网络的用户使用；一部分需要用户进行认证后才可以访问，并且可以根据需求对访问网络资源的用户进行不同认证。

TL-AC1000 提供 MAC 认证、WEB 认证、微信连 WIFI 等多种认证方式，同时提供本地认证服务器对需要访问网络资源的用户进行认证，保证了网络的安全。

### 6.1 MAC 认证

#### 6.1.1 MAC 认证简介

MAC认证是一种基于端口和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，用户也不需要任何操作。

TL-AC1000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 6.1 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”中的用户才可以通过认证，其他用户将被拒绝接入该网络。

## 6.1.2 MAC 认证设置

设置MAC认证时，需先设置允许通过认证的客户端的MAC地址，再对这些MAC地址进行分组设置。

### 1. 设置 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

MAC地址列表			
选择	序号	名称	MAC地址
<input type="checkbox"/>	1	mac1	A8-A6-68-18-6A-DE

共1条, 每页: 10 条 | 当前: 1/1页, 1~1条 | [首页](#) [上一页](#) [下一页](#) [尾页](#)  [跳转](#)

[新增](#) [全选](#) [删除](#) [导入](#) [导出](#) [搜索](#)

图 6.2 MAC地址界面

在此界面，可以对已有条目进行操作。下面介绍对MAC地址进行“导入”和“导出”的操作。

**导入：**先将需要设置的 MAC 地址条目存为一份 utf-8 编码格式的 txt 文件，再点击<导入>按钮导入该文件，从而一次性添加多个 MAC 地址条目。该 txt 文件的每一行必须代表一条 MAC 地址条目，每条条目由名称和 MAC 地址组成，且必须用“#” 隔开和结尾。例如“Jame#00-11-22-33-44-55#”。可以通过<导出>按钮获得一份符合导入规则的 txt 文件，进一步了解以上规则。

**导出：**点击<导出>按钮导出所有的 MAC 地址条目到一份 utf-8 编码格式的 txt 文件中作为备份。

点击<新增>按钮可以添加新条目，新增MAC地址条目界面如下图所示。

MAC地址设置	
名称：	<input type="text"/> ( 1-50个字符 )
MAC地址：	<input type="text"/> ( XX-XX-XX-XX-XX-XX )
<input type="button" value="确定"/> <input type="button" value="清除"/> <input type="button" value="取消"/> <input type="button" value="帮助"/>	

图 6.3 新增MAC地址界面

名称	设置客户端的名称。
MAC地址	设置客户端的 MAC 地址。

表 6.1 新增MAC地址界面项说明

## 2. 设置 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

MAC认证列表						
选择	序号	MAC认证名称	备注	VLAN ID	状态	设置
<input type="checkbox"/>	1	mac1	地址1	1	已启用	

图 6.4 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。

MAC认证设置	
MAC认证名称：	<input type="text" value="mac1"/> (1-50个字符)
VLAN ID：	<input type="text" value="1"/> ▼
MAC地址	<input type="button" value="全选"/> <input type="button" value="反选"/> <input checked="" type="checkbox"/> mac1
备注：	<input type="text" value="地址1"/> (1-50个字符，可选)
启用/禁用：	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
<input type="button" value="确定"/> <input type="button" value="清除"/> <input type="button" value="取消"/> <input type="button" value="帮助"/>	

图 6.5 新增MAC认证界面

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。
VLAN ID	选择需要进行 MAC 认证的无线 VLAN。
MAC地址	选择或者移除该 MAC 认证组内的 MAC 地址对象。如需新建 MAC 地址对象，请参考 <a href="#">设置 MAC 地址</a> 。
备注	设置该条目的备注，以方便管理和查找。
启用/禁用	选择“启用”，则使该策略生效； 选择“禁用”，则使该策略失效。

表 6.2 新增MAC认证界面项说明

### 6.1.3 配置 MAC 认证步骤

- 1) 设置使用 MAC 认证规则的 VLAN。必须操作。具体操作步骤请参考[配置 VLAN 步骤](#)。

- 2) 设置允许通过认证的客户端的 MAC 地址。必须操作。设置界面：认证管理 >> MAC 认证 >> MAC 地址，在此界面设置客户端的名称和 MAC 地址，点击<确定>按键完成。
- 3) 创建应用 MAC 认证的认证服务。必须操作。设置界面：认证管理 >> MAC 认证 >> MAC 认证，点击<新增>按键，在显示的设置界面，设置认证服务的名称，选择 VLAN ID，选择允许接入的 MAC 地址，选择“启用”，点击<确定>按键完成。

## 6.2 Portal 认证

无线控制器提供 Portal 认证服务，包括 WEB 认证、微信连 WIFI、一键上网等认证方式和跳转页面设置、免认证策略等相关功能。

### 6.2.1 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

跳转页面列表						
选择	序号	跳转页面名称	认证页面类型	页面内容	备注	设置
<input type="checkbox"/>	1	1024	微信连WIFI	<input type="button" value="预览"/>	---	<input type="button" value="设置"/>

图 6.6 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，需要设置跳转页面名称（仅限英文字符），选择跳转页面类型。根据不同的类型，显示不同的设置内容：

- 1 WEB 认证：设置界面如下图所示。

跳转页面名称： (1-50个英文字符)  
 认证页面类型：

**认证页面设置**

页面标题： (1-50个字符)  
 背景图片：    
 (可选，图片大小不能超过200KB，上传图片分辨率建议使用1080\*411)  
 欢迎信息： (1-26个字符)  
 版权声明： (1-50个字符)  
 备注： (1-50个字符，可选)

图 6.7 新增跳转页面-Web认证

跳转页面名称	设置跳转页面的名称。
认证页面类型	设置认证页面模板的类型，当前类型为 WEB 认证。
页面标题	设置跳转页面模板的标题内容。
背景图片	上传跳转页面模板的背景图片。
欢迎信息	设置跳转页面模板的欢迎信息。
版权声明	设置跳转页面模板的版权信息。
备注	设置条目的备注信息，以方便管理和查找。

表 6.3 新增跳转页面-WEB认证界面项说明

## 2 一键上网：设置界面如下图所示。

跳转页面名称： (1-50个英文字符)

认证页面类型：

**认证页面设置**

页面标题： (1-50个字符)

背景图片：    
(可选，图片大小不能超过200KB，上传图片分辨率建议使用1080\*411)

欢迎信息： (1-26个字符)

版权声明： (1-50个字符)

备注： (1-50个字符，可选)

图 6.8 新增跳转页面-一键上网

认证页面设置部分与WEB认证相同，设置时请参考WEB认证的条目设置介绍。

## 3 远程 portal：设置页面如下图所示。

跳转页面名称： (1-50个英文字符)

认证页面类型：

**认证页面设置**

自动跳转URL： (1~120个英文字符)

备注： (1-50个字符,可选)

图 6.9 新增跳转页面-远程portal

跳转页面名称	设置跳转页面的名称。
认证页面类型	设置认证页面模板的类型，当前类型为远程 portal。

自动跳转 URL	<p>当选择了远程 portal 模板时，设置外部 portal 服务器的 URL 地址。</p> <p>配置远程 portal 的认证条目，要为 portal 服务器配置免认证策略，详细内容请参考<a href="#">免认证策略</a>。</p> <p>若远程 portal 条目已经被引用，则不能再修改自动跳转 URL。</p>
备注	设置条目的备注信息，以方便管理和查找。

表 6.4 新增跳转页面-远程portal界面项说明

外部WEB服务器需要提供认证登录页面，为确保认证客户端能够正确提交用户名和密码，该页面必须按下面的要求完成：

- 认证登录页面Form的action必须设为：<http://AC IP:Port/portal/auth>，AC IP为当前无线控制器的IP地址，Port为Portal服务端口（Portal服务端口的设置参见[服务设置](#)）；
- 认证登录页面以Get方式提交Form表单；
- 认证登录页面必须包含以下参数：

username	用户名
password	密码
apIp	客户端链接的 AP 设备的 IP 地址
apMac	客户端链接的 AP 设备的 MAC 地址
staIp	客户端的 IP 地址
staMac	客户端的 MAC 地址
vlan	客户端所属的 VLAN

认证登录页面设计代码示例如下：

//页面表单提交内容

```
<form id="form1" name="form1" method="get" action=" http://AC IP:Port/portal/auth
" onsubmit="return doSubmit();">
  <p>
    <label id="t_user_name" class="">用户名: </label>
    <span id="span_usr_name">
      <input id="txt_user_name" name="username" type="text"
fieldtype="username" tabindex="1">
    </span>
  </p>

  <p>
    <label id="t_password" class="">密码: </label>
    <input id="txt_password" name="password" type="password" value=""
fieldtype="password" tabindex="2">
  </p>
```



```
<input type="submit" name="Submit" value="登录">
<input type="hidden" name="apIp" id="apIp" value="">
<input type="hidden" name="apMac" id="apMac" value="">
<input type="hidden" name="staIp" id="staIp" value="">
<input type="hidden" name="staMac" id="staMac" value="">
<input type="hidden" name="vlan" id="vlan" value="">
```

```
</form>
```

//获取页面URL中的相关信息，并按页面的要求提交表单

```
<script>
function setExtArgs()
{
    var idx = 0;
    var locSearch = window.location.search;
    var argsStr = locSearch.slice(1,locSearch.length);
    var argv = argsStr.split('&');
    var nameVal;

    for (idx = 0; idx < argv.length; idx ++)
    {
        nameVal = argv[idx].split('=');
        if (nameVal.length == 2 && null != document.getElementById(nameVal[0]))
        {
            document.getElementById(nameVal[0]).value = nameVal[1];
        }
    }
    return;
}

function doSubmit()
{
    setExtArgs();
    document.forms['form1'].submit();
}
</script>
```

## 4 微信连 WIFI：设置页面如下图所示。

**跳转页面**

跳转页面名称:  (1-50个英文字符)

认证页面类型: 微信连WIFI

**微信公众号信息设置**

ShopID:  (1-32个字符)

AppID:  (1-32个字符)

SecretKey:  (1-32个字符)

[微信公众号信息设置方法](#)

**认证页面设置**

Logo图片:  浏览... 上传  
(可选, 图片大小不能超过100KB, 上传图片分辨率建议使用128\*128)

背景图片:  浏览... 上传  
(可选, 图片大小不能超过200KB, 上传图片分辨率建议使用1024\*760)

Logo信息:  (1-25个字符, 可选)

欢迎信息:  (1-50个字符)

登录按钮提示文字:  (1-15个字符)

版权信息:  (1-25个字符, 可选)

备注:  (1-50个字符, 可选)

设置
清除
取消
预览
帮助



- 背景图片
- Logo图片
- Logo信息
- 欢迎信息
- 登录按钮提示文字
- 版权信息

图 6.10 新增跳转页面-微信连WIFI

跳转页面名称	设置跳转页面的名称。
认证页面类型	设置认证页面的类型, 当前类型为微信连 WIFI。
ShopID	设置微信连 WIFI 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 WIFI 密钥, 可登陆微信公众号官网获取。
Logo 图片	上传认证页面的 Logo 图片。
背景图片	上传认证页面的背景图片。
Logo 信息	设置认证页面的 Logo 信息。
欢迎信息	设置认证页面的欢迎信息。
登录按钮提示文字	设置认证页面的登录按钮提示文字。
版权声明	设置认证页面的版权信息。
备注	设置条目的备注信息, 以方便管理和查找。

表 6.5 新增跳转页面-微信连WIFI界面项说明

## 5 WEB 认证+微信连 WIFI：设置页面如下图所示。

**跳转页面**

跳转页面名称:  (1-50个英文字符)

认证页面类型: WEB认证+微信连WIFI

**微信公众号信息设置**

ShopID:  (1-32个字符)

AppID:  (1-32个字符)

SecretKey:  (1-32个字符)

[微信公众号信息设置方法](#)

**认证页面设置**

Logo图片:  浏览... 上传  
(可选, 图片大小不能超过100KB, 上传图片分辨率建议使用128\*128)

背景图片:  浏览... 上传  
(可选, 图片大小不能超过200KB, 上传图片分辨率建议使用1024\*760)

Logo信息:  (1-25个字符, 可选)

欢迎信息:  (1-50个字符)

登录按钮提示文字:  (1-15个字符)

版权信息:  (1-25个字符, 可选)

备注:  (1-50个字符, 可选)

设置
清除
取消
预览
帮助



图 6.11 新增跳转页面-WEB认证+微信连WIFI

微信公众号信息设置和认证页面设置部分与微信连WIFI相同，设置时请参考微信连WIFI的条目设置介绍。

## 6.2.2 WEB 认证

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/HTTPS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。

### 1. WEB 认证系统

WEB 认证系统一般网络拓扑如下图所示：

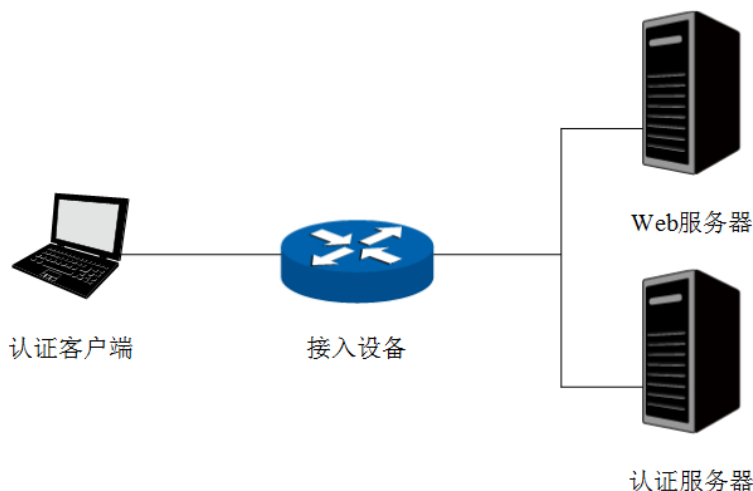


图 6.12 WEB认证系统拓扑图

#### 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。

## 2. WEB 认证过程

WEB 认证过程如下图所示：

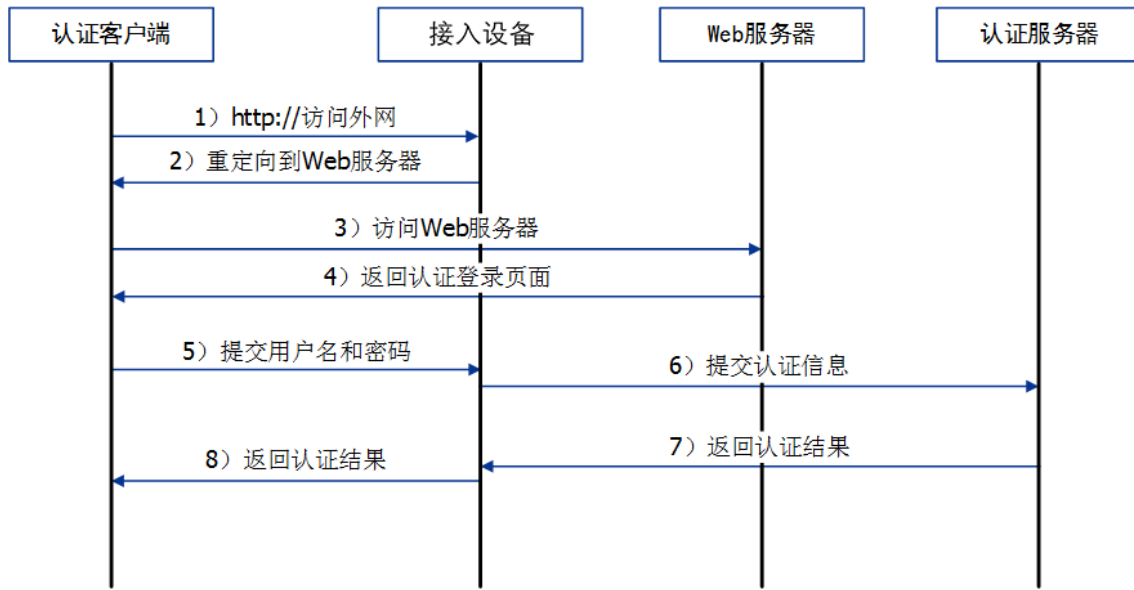


图 6.13 WEB认证过程示意图

- 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；

接入设备向认证客户端返回该认证结果。

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**

Web认证列表								
选择	序号	跳转页面名称	VLAN ID	服务器类型	Web无感知认证	备注	状态	设置
<input type="checkbox"/>	1	Web1	1	本地服务器	已启用	酒店认证	已启用	 

图 6.14 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认证条目需要选择跳转页面、生效VLAN等必要信息，详细设置如图 6.15所示。

功能设置

启用Web认证

跳转页面名称:

VLAN ID:

认证服务器类型:

认证成功后跳转链接:  (1-120个英文字符, 可选)

认证失败后跳转链接:  (1-120个英文字符, 可选)

Web无感知认证:  开启  关闭

备注:  (1-50个字符, 可选)

图 6.15 新增WEB认证界面

启用 WEB 认证	选择是否启用该 WEB 认证条目。
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	选择需要进行 WEB 认证的无线 VLAN。
认证服务器类型	选择进行 WEB 认证的服务器类型, 可选项有本地服务器(无线控制器的认证服务器功能)和远程服务器(外部独立设置的认证服务器)。 如果需要设置远程认证服务器, 请参考 <a href="#">认证服务器</a> 的相关介绍。
免费上网时长	当认证服务器类型选择“远程服务器”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。
认证服务器组	当认证服务器类型选择“远程服务器”时, 需要选择提供认证的服务器组, 相关服务器组的设置内容, 请参考 <a href="#">认证服务器</a> 。
认证成功后跳转链接	设置认证成功后跳转的 URL 地址。
认证失败后跳转链接	设置认证失败后跳转的 URL 地址。
WEB 无感知认证	选择该 WEB 认证条目是否启用 WEB 无感知认证功能, 无感知认证用户再次接入 WLAN 时会自动进行认证。
备注	设置 WEB 认证条目的备注信息, 以方便管理和查找。

表 6.6 新增WEB认证界面项说明

### 6.2.3 微信连 WIFI

无线控制器提供微信连 WIFI 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 WIFI 推广微信公众号并推送广告。

## 进入界面：认证管理 &gt;&gt; Portal 认证 &gt;&gt; 微信连 WIFI

微信连WIFI列表						
选择	序号	跳转页面名称	VLAN ID	备注	状态	设置
<input type="checkbox"/>	1	1024	---	---	已启用	 

图 6.16 微信连WIFI界面

在此界面，可以对已有条目进行操作，点击<新增>按钮可以添加新条目。

新增微信连WIFI条目需要选择跳转页面、生效VLAN等必要信息，详细设置如图 6.17所示。

微信连WIFI设置	
<input type="checkbox"/>	启用微信连WIFI
跳转页面名称:	<input type="text" value="---"/>
VLAN ID:	<input type="text" value="1"/>
免费上网时长:	<input type="text" value="30"/> 分钟 (1-1440)
备注:	<input type="text"/> (1-50个字符, 可选)
<input type="button" value="设置"/> <input type="button" value="清除"/> <input type="button" value="取消"/> <input type="button" value="帮助"/>	

图 6.17 新增微信连WIFI界面

启用微信连 WIFI	选择是否启用该微信连 WIFI 条目。
跳转页面名称	选择已经设置完成的微信连 WIFI 的跳转页面模板。
VLAN ID	选择需要进行微信连 WIFI 的无线 VLAN。
免费上网时长	选择微信连 WIFI 用户可以免费上网的时长。
备注	设置微信连 WIFI 条目的备注信息，以方便管理和查找。

表 6.7 新增微信连WIFI界面项说明

## 6.2.4 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 &gt;&gt; Portal 认证 &gt;&gt; 一键上网

一键上网列表						
选择	序号	跳转页面名称	VLAN ID	备注	状态	设置
<input type="checkbox"/>	1	Click	1	酒店一键上网	已启用	 

图 6.18 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>按钮可以添加新条目。

新增一键上网条目需要选择跳转页面、生效VLAN等必要信息，详细设置如图 6.19所示。

**一键上网设置**

启用一键上网

跳转页面名称:

VLAN ID:

免费上网时长:  分钟 (1-1440)

备注:  (1-50个字符, 可选)

图 6.19 新增一键上网界面

启用一键上网	选择是否启用该一键上网条目。
跳转页面名称	选择已经设置完成的一键上网的跳转页面模板。
VLAN ID	选择需要进行一键上网认证的无线 VLAN。
免费上网时长	选择一键上网认证用户可以免费上网的时长。
备注	设置一键上网条目的备注信息，以方便管理和查找。

表 6.8 新增一键上网界面项说明

## 6.2.5 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](#)

免认证策略列表												
选择	序号	策略名称	源IP地址范围	目的IP地址范围	源MAC地址	源VLAN	源端口	目的端口	服务协议	备注	状态	设置
<input type="checkbox"/>	1	dhcp client	---	---	---	---	68-68	67-67	UDP	---	已启用	---
<input type="checkbox"/>	2	dhcp server	---	---	---	---	67-67	68-68	UDP	---	已启用	---
<input type="checkbox"/>	3	dns client	---	---	---	---	---	53-53	UDP	---	已启用	---
<input type="checkbox"/>	4	dns server	---	---	---	---	53-53	---	UDP	---	已启用	---

图 6.20 免认证策略界面

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。

### 免认证策略设置

无线控制器支持两种**免认证方式**：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。



## 免认证策略设置

策略名称： (1-50个字符)

匹配方式： ▾

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)

源端口： -  (1-65535, 可选)

目的IP地址范围： /  (可选)

目的端口： -  (1-65535, 可选)

服务协议： ▾

备注： (1-50个字符, 可选)

启用/禁用： 启用  禁用

图 6.21 免认证策略设置-五元组方式界面

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。
备注	设置条目的备注，以方便管理和查找。
启用/禁用	选择“启用”，则使该策略生效； 选择“禁用”，则使该策略失效。

表 6.9 新增五元组免认证策略界面项说明

URL 方式：主要依据 URL 设置策略，当已知 URL 时，推荐使用 URL 方式。

**免认证策略设置**

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)

启用/禁用： 启用  禁用

图 6.22 免认证策略设置-URL方式界面

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。
启用/禁用	选择“启用”，则使该策略生效； 选择“禁用”，则使该策略失效。

表 6.10 新增URL免认证策略界面项说明

## 6.2.6 配置 Portal 认证步骤



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。

- 1) 设置使用 Portal 认证规则的 VLAN。必须操作。具体操作步骤请参考[配置 VLAN 步骤](#)。
- 2) 设置 Portal 认证服务器。必须操作。具体操作步骤请参考[认证服务器](#)。
- 3) 设置 Portal 认证的免认证策略。非必须操作。当认证服务器类型为远程服务器时，必须添加远程服务器的地址信息等为免认证策略。设置界面：认证管理 >> Portal 认证 >> 免认证策略，点击<新增>按键，在显示的设置界面，设置启用免认证策略规则的设备 IP 地址等信息和允许访问的资源信息，点击<确定>按键完成。

- 4) 创建应用 Portal 认证的认证服务。必须操作。根据认证方式选择相应的标签页，以下以 WEB 认证为例。设置界面：认证管理 >> Portal 认证 >> WEB 认证，点击<新增>按键，在显示的设置界面，选择启用 WEB 认证，设置认证服务的跳转页面，选择适用策略的 VLAN ID、认证服务器类型等信息，点击<设置>按键完成。
- 5) 当选择本地认证时，需要在本地用户页面添加允许接入的用户的登录信息。必须操作。具体操作步骤请参考[本地用户](#)。

## 6.3 认证服务器

TL-AC1000 提供本地认证服务器的功能，还提供指定外部 Radius 服务器进行认证的功能。

本地认证服务器，即无线控制器添加允许接入的用户身份信息，当用户接入时，无线控制器对身份信息进行认证。如需要添加用户身份信息，请参考[本地用户](#)。

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。

本地认证服务器为系统预定义的服务器组，不可操作。下面介绍外部 Radius 认证服务器设置过程。

### 1. 设置 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

Radius服务器列表							
选择	序号	名称	地址	认证端口	计费端口	认证方式	设置
<input type="checkbox"/>	1	radius1	116.10.20.116	1812	1813	PAP	

图 6.23 Radius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Radius条目界面如下图所示。

Radius服务器	
服务器名称：	<input type="text"/> (1-50个字符)
服务器地址：	<input type="text"/> (IP地址或域名, 1-250个英文字符)
认证端口：	<input type="text" value="1812"/> (1024-65535)
计费端口：	<input type="text" value="1813"/>
共享密钥：	<input type="text"/> (1-120个字符)
重复发送次数：	<input type="text" value="3"/> (0-10次)
超时时间：	<input type="text" value="3"/> (1-60秒)
认证方式：	<input type="text" value="PAP"/> ▼
<input type="button" value="确定"/> <input type="button" value="清除"/> <input type="button" value="取消"/> <input type="button" value="帮助"/>	

图 6.24 新增Radius界面

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。
认证方式	选择使用的认证方式, 有PAP、CHAP、MSCHAP和MSCHAPv2。

表 6.11 新增Radius界面项说明

## 2. 设置服务器组

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 >> 服务器组


服务器组列表						
选择	序号	组名称	协议类型	恢复时间	备注	设置
<input type="checkbox"/>	1	LOCAL	Local	---	---	---
<input type="checkbox"/>	2	外部认证	Radius	30	---	

图 6.25 服务器组界面

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服务器组, 不可操作。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。

**服务器组设置**

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 (30-1440分钟)

备注： (1-50个字符, 可选)

图 6.26 新增服务器组界面

组名称	自定义的认证服务器组名称，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。
备份服务器	备份服务器在主服务器发生故障时启用，备份服务器为可选项。
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。

表 6.12 新增服务器组界面项说明

## 6.4 本地用户

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 >> 本地用户 >> 本地用户

**功能设置**

用户新增：

用户数据备份：

用户导入： 浏览...

**用户列表**

选择	序号	账户类型	用户名	账户有效期	免费时长	MAC地址	备注	设置
<input type="checkbox"/>	1	正式用户	user1	2015-08-05	---	---	---	<input type="button" value="编辑"/> <input type="button" value="禁用"/> <input type="button" value="删除"/>

共1条，每页： 10 条 | 当前：1/1页，1~1条 | [首页](#) [上一页](#) [下一页](#) [尾页](#)  1

图 6.27 本地用户界面

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，**用户类型**分为正式用户和免费用户。

- 正式用户：给用户连续自然天的上网服务，当账户有效期到期后，该账户无效。

**用户设置**

用户类型： (v)

用户名： (1-100个英文字符)

密码： (1-100个英文字符)

账户有效期： (格式: xxxx-xx-xx)

允许认证时间段： :  -  :

MAC地址绑定方式： (v)

同时登录用户数： (1-2048)

姓名： (1-50个字符，可选)

电话： (1-50个字符，可选)

备注： (1-50个字符，可选)

启用/禁用： 启用  禁用

图 6.28 新增本地用户-正式用户界面

用户名	自定义的用户名，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。
账户有效期	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、动态绑定和静态绑定。 不绑定：不绑定认证客户端MAC地址。 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。 静态绑定：手动输入认证客户端MAC地址，绑定对应用户名。
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。
启用/禁用	选择“启用”，则该用户可以通过认证； 选择“禁用”，则该用户不可以通过认证。

表 6.13 新增本地用户-正式用户界面项说明

- 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。

**用户设置**

用户类型： ▾

用户名： (1-100个英文字符)

密码： (1-100个英文字符)

允许认证时间段： :  -  :

免费时长： 分钟 (1-1440)

同时登录用户数： (1-2048)

备注： (1-50个字符，可选)

启用/禁用： 启用  禁用

图 6.29 新增本地用户-免费用户界面

用户名	自定义的用户名，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。
启用/禁用	选择“启用”，则该用户可以通过认证； 选择“禁用”，则该用户不可以通过认证。

表 6.14 新增本地用户-正式用户界面项说明

点击<备份>按键，可以备份路由器中存储的用户信息，备份文件为ANSI编码格式的CSV文件。也可以导入ANSI编码格式的CSV文件到路由器中。CSV文件内容格式参考如下（可以通过“备份”一份有用户信息的文件参考）：

A	B	C	D	E	F	G	H	I	J	K	L	M
用户类型	用户名	密码	启用	账户有效期	允许认证时间段	免费时长	同时登录用户数	MAC地址绑定方式	MAC地址	姓名	电话	备注
正式用户	user1	123	启用	2015/8/5	00:00-24:00	0	1	不绑定	00-00-00-00-00-00			
免费用户	user2	123456	启用	---	00:00-24:00	30	1	不绑定	00-00-00-00-00-00			

图 6.30 csv格式文件存储用户信息示意图

A	用户类型
B	用户名
C	密码
D	启用/禁用状态

E	账户有效期。仅正式用户可设，格式：xxxx-xx-xx；免费用户为“---”。
F	允许认证时间段
G	免费时长。仅免费用户可设，正式用户为“0”。
H	同时登录用户数
I	MAC 地址绑定方式。仅正式用户可设，免费用户为“不绑定”。
J	MAC 地址
K	姓名
L	电话
M	备注

表 6.15 csv格式文件存储用户信息说明

**说明：**

导入的CSV文件内容必须按照上面顺序编排各项，且确保每一项的格式正确。



## 6.5 应用举例

### 6.5.1 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。为减少网络设备，可使用内置的 WEB 服务器提供认证页面。

#### 网络拓扑

酒店网络拓扑如下图所示：

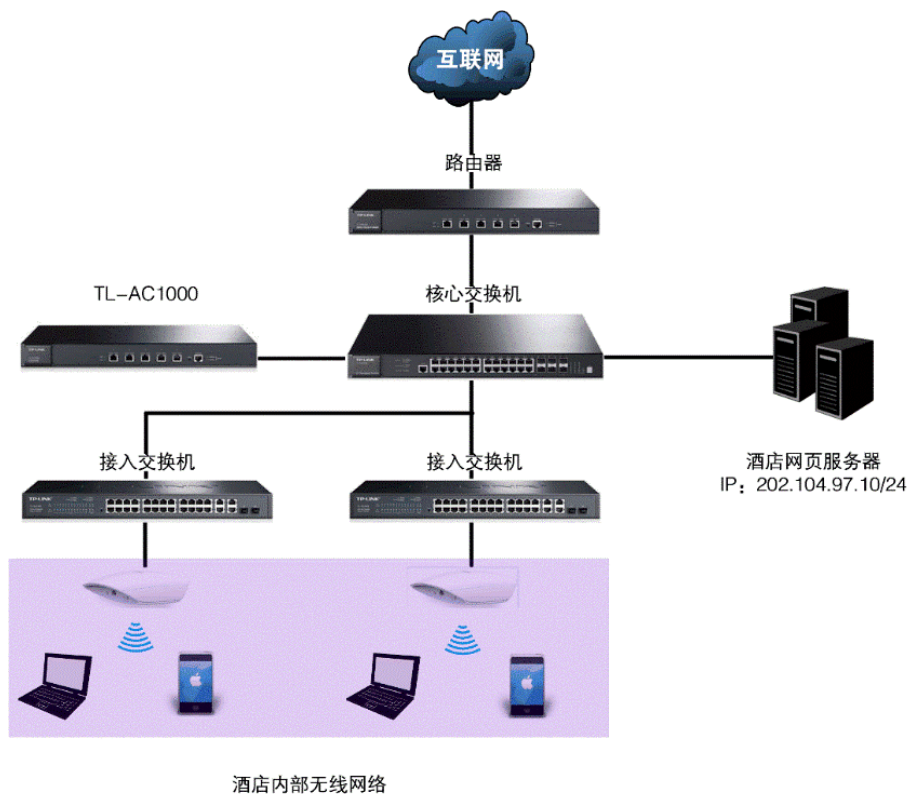


图 6.31 酒店无线网络应用拓扑

#### 配置方法

##### 1 设置一键上网跳转页面

在设置之前，需要做如下准备工作：设计一张酒店宣传图片，假设设计的广告图片为：酒店图片.png。

进入页面：认证管理 >> Portal 认证 >> 跳转页面，点击<新增>按钮，在新增跳转页面设置页面中选择“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图片上传到无线控制器上。

跳转页面名称： (1-50个英文字符)  
 认证页面类型： ▾

## 认证页面设置

页面标题： (1-50个字符)  
 背景图片：    
 (可选，图片大小不能超过200KB，上传图片分辨率建议使用1080\*411)  
 欢迎信息： (1-26个字符)  
 版权声明： (1-50个字符)  
 备注： (1-50个字符，可选)

图 6.32 一键上网跳转页面设置

设置完成后，点击<预览>按键，可以预览自定义的认证跳转页面，如下图所示。

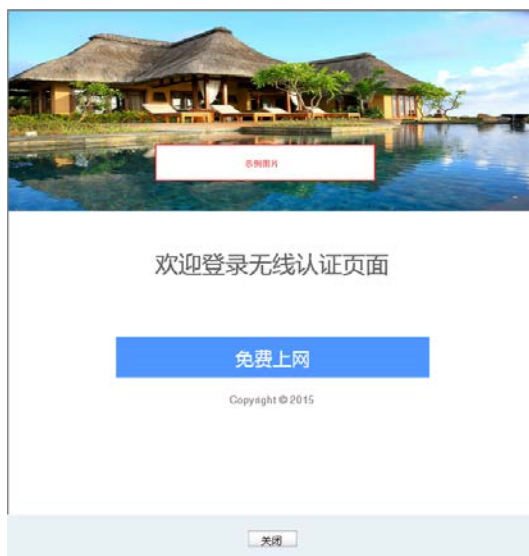


图 6.33 预览一键上网跳转页面

## 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。

## 一键上网设置

启用一键上网  
 跳转页面名称： ▾  
 VLAN ID： ▾  
 免费上网时长： 分钟 (1-1440)  
 备注： (1-50个字符，可选)

图 6.34 一键上网设置

## 6.5.2 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 TL-AC1000 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

酒店网络拓扑如下图所示：

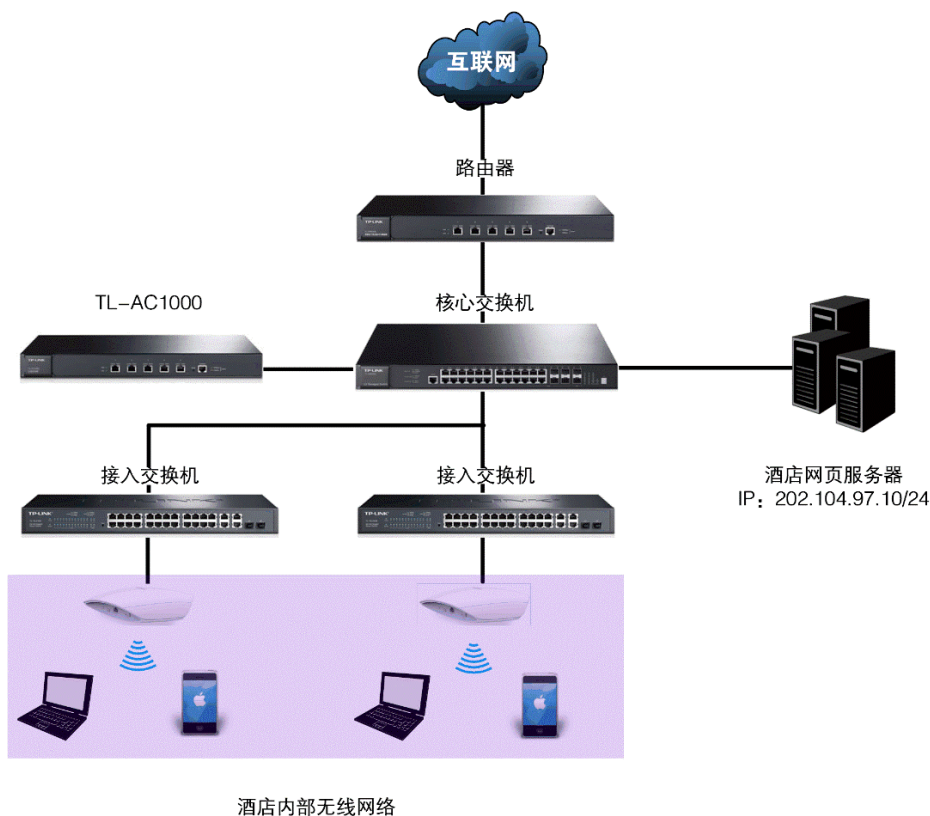


图 6.35 酒店无线网络应用拓扑

### 配置方法

#### 1 设置 WEB 认证跳转页面

在设置之前，需要做如下准备工作：设计一张酒店宣传图片，假设设计的广告图片为：酒店图片.png。

进入页面：认证管理 >> Portal 认证 >> 跳转页面，点击<新增>按钮，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图片上传到无线控制器上。

跳转页面名称： (1-50个英文字符)

认证页面类型： ▼

**认证页面设置**

页面标题： (1-50个字符)

背景图片：

(可选，图片大小不能超过200KB，上传图片分辨率建议使用1080\*411)

欢迎信息： (1-26个字符)

版权声明： (1-50个字符)

备注： (1-50个字符，可选)

图 6.36 WEB认证跳转页面设置

设置完成后，点击<预览>按钮，可以预览自定义的认证跳转页面，如下图所示。

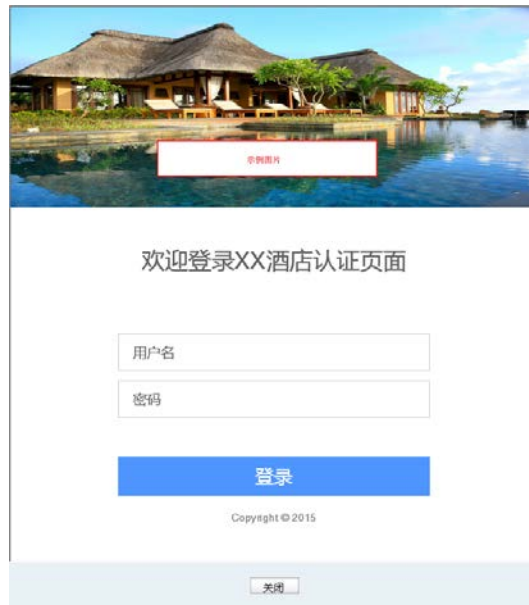


图 6.37 预览WEB认证跳转页面

## 2 设置 WEB 认证

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

**功能设置**

启用Web认证

跳转页面名称：

VLAN ID：

认证服务器类型：

认证成功跳转链接： (1-120个英文字符, 可选)

认证失败跳转链接： (1-120个英文字符, 可选)

Web无感知认证： 开启  关闭

备注： (1-50个字符, 可选)

图 6.38 WEB认证设置

### 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>> 本地用户 >> 本地用户，点击<新增>按钮，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。

**用户设置**

用户类型：

用户名： (1-100个英文字符)

密码： (1-100个英文字符)

允许认证时间段： :  -  :

免费时长： 分钟 (1-1440)

同时登录用户数： (1-2048)

备注： (1-50个字符, 可选)

启用/禁用： 启用  禁用

图 6.39 添加免费用户账户

### 6.5.3 微信连 WIFI

#### 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 WIFI 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 WIFI 功能实现需求。

#### 网络拓扑

酒店网络拓扑如下图所示：

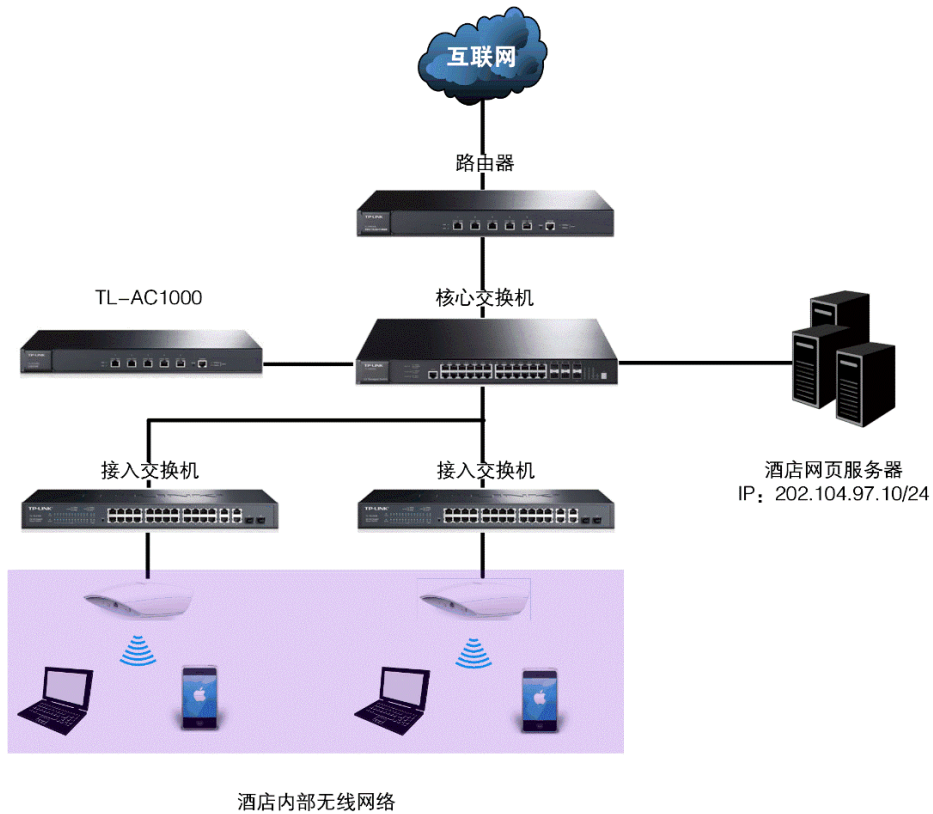


图 6.40 微信连WIFI应用拓扑图

## 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。

微信·公众平台 Beta



图 6.41 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。

微信·公众平台 Beta



图 6.42 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 6.43 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 WIFI 跳转页面时会用到。



图 6.44 添加设备2

## 2 设置微信连 WIFI 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 WIFI，可参考如下参数设置。



**跳转页面**

跳转页面名称:  (1-50个英文字符)

认证页面类型:

**微信公众号信息设置**

ShopID:  (1-32个字符)

AppID:  (1-32个字符)

SecretKey:  (1-32个字符)

[微信公众号信息设置方法](#)

**认证页面设置**

Logo图片:

(可选, 图片大小不能超过100KB, 上传图片分辨率建议使用128\*128)

背景图片:

(可选, 图片大小不能超过200KB, 上传图片分辨率建议使用1024\*760)

Logo信息:  (1-25个字符, 可选)

欢迎信息:  (1-50个字符)

登录按钮提示文字:  (1-15个字符)

版权信息:  (1-25个字符, 可选)

备注:  (1-50个字符, 可选)

图 6.45 微信连WIFI跳转页面设置

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



图 6.46 预览微信连WIFI跳转页面

### 3 设置微信连 WIFI

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

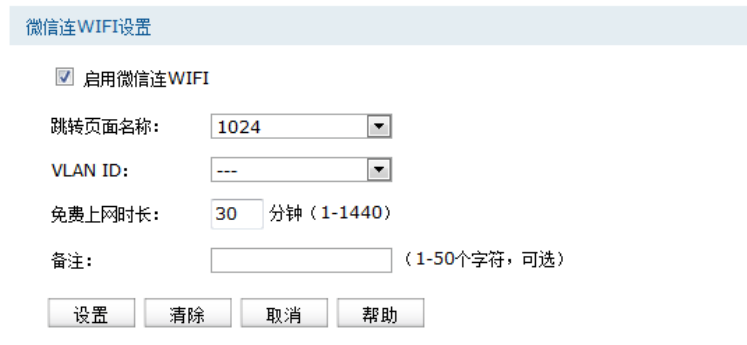


图 6.47 微信连WIFI设置

### 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。



欢迎使用微信连Wi-Fi

登录

图 6.48 跳转到认证页面

2) 点击<登录>, 进入微信连 Wi-Fi 页面, 如下图所示。



图 6.49 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 6.50 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。

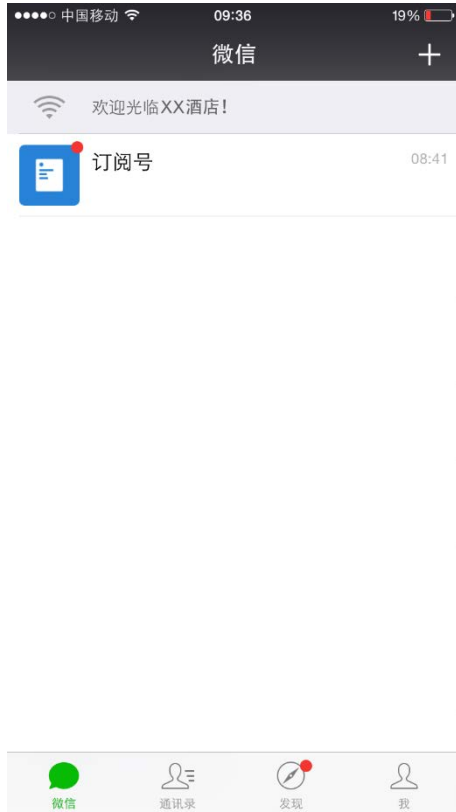


图 6.51 微信页面

## 第7章 无线管理

TL-AC1000可对整个无线网络进行统一管理，本章介绍TL-AC1000的无线管理功能。

### 7.1 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。

进入界面：无线管理 >> 无线服务 >> 无线服务

无线服务列表								
选择	序号	SSID	描述	VLAN ID	安全选项	状态	射频绑定	设置
<input type="checkbox"/>	1	TP-LINK_AC1000	default_ssid	---	---	已启用		
<input type="checkbox"/>	2	SSID中文[GBK]	1	1	---	已启用		

新增 全选 启用 禁用 删除 搜索

图 7.1 无线服务界面

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SSID。点击<新增>按钮可以添加新条目，点击按钮会进入[射频绑定列表](#)界面。

#### 1. 新增无线服务条目

新增无线服务条目界面如下图所示。

无线服务设置	
SSID :	<input type="text" value="中文"/> UTF-8编码 <input type="button" value="v"/> (1-32个字符)
描述 :	<input type="text"/> (1-50个字符, 可选)
VLAN ID :	<input type="text" value="---"/> <input type="button" value="v"/>
安全选项 :	<input type="text" value="关闭安全选项"/> <input type="button" value="v"/>
无线网络内部隔离 :	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
启用/禁用 :	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
<input type="button" value="确定"/> <input type="button" value="清除"/> <input type="button" value="取消"/> <input type="button" value="帮助"/>	

图 7.2 新增无线服务界面

SSID	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。  本产品SSID设置支持中文字符, 当输入的SSID包含中文时, 可以在右侧出现的下拉菜单中选择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。  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。
描述	设置该条目的描述信息, 以方便管理和查找。
VLAN ID	选择无线服务关联的VLAN。如需新建VLAN, 请参考 <a href="#">VLAN设置</a> 。

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>
无线网络内部隔离	<p>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。</p>
启用/禁用	<p>选择“启用”，则使该无线服务条目生效；</p> <p>选择“禁用”，则使该无线服务条目失效。</p>

表 7.1 新增无线服务界面项说明

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。

安全选项：

认证类型：

加密算法：

PSK密码： (8-63个ASCII码字符或8-64个十六进制字符)

组密钥更新周期： (30-604800秒，不更新则为0)

认证类型	<p>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。</p>
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>
PSK密码	<p>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。</p>
组密钥更新周期	<p>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。</p>

## 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。

安全选项： ▼

认证类型： ▼

加密算法： ▼

Radius服务器IP：

Radius端口： ( 1024-65535 )

Radius密码： ( 1-64个英文字符 )

组密钥更新周期： ( 30-604800秒，不更新则为0 )

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>
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。
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。

**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。

## 2. 射频绑定列表

射频绑定列表界面如下图所示。

SSID :

射频绑定列表					
选择	序号	AP名称	射频单元	射频模式	绑定状态
<input type="checkbox"/>	1	TL-AP450I-PoE-0001	2.4G	802.11b/g/n	绑定

共1条, 每页:  条 | 当前: 1/1页, 1~1条 | [首页](#) [上一页](#) [下一页](#) [尾页](#)  [跳转](#)

[全选](#) [绑定](#) [取消绑定](#) [返回](#) [搜索](#) [帮助](#)

图 7.3 射频绑定列表界面

### SSID

显示当前执行射频绑定操作的无线网络名称。

### 射频绑定列表

在此区域，勾选相应条目，点击<绑定>按键可以把对应无线服务绑定到 AP 的射频上，点击<取消绑定>按键可以从 AP 射频上取消无线服务的绑定关系，点击<返回>按键将返回到**无线服务**界面。

**说明：**

未固化的AP，不允许执行绑定操作。固化操作请参考[AP设置](#)。



## 7.2 AP 管理

### 7.2.1 AP 设置

可以在此界面进行AP设置。

进入界面：无线管理 >> AP管理 >> AP设置

AP设置

自动AP固化： 开启  关闭

定时AP重启： 开启  关闭 每天  时  分自动重启所有AP

链路优先级： (1-255)

备份AC的IP地址： (不填或填全零IP表示不存在备份链路)

AP列表

选择	序号	AP名称	型号	硬件版本	软件版本	MAC地址	状态	设置
<input type="checkbox"/>	1	TL-AP302I-PoE-0001	TL-AP302I-PoE	1.0	1.0.0	00-0A-EB-13-1A-52	运行	
<input type="checkbox"/>	2	TL-AP301C-0001	TL-AP301C	2.0	1.0.3	00-0A-EB-13-77-13	运行	
<input type="checkbox"/>	3	TL-AP1200C-PoE-0001	TL-AP1200C-PoE	1.0	1.0.3	88-25-93-1B-6F-C2	运行	

共3条，每页： 条 | 当前：1/1页，1~3条 | [首页](#) [上一页](#) [下一页](#) [尾页](#)

图 7.4 AP设置界面

#### AP 设置

自动AP固化	若开启该功能，则一旦AP连接到无线控制器上，系统将自动为该AP生成条目，并写入配置文件中。
定时AP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。
链路优先级	设置AC的链路优先级，数值越大优先级越高，AP选择本AC的优先度越大。如果修改链路优先级将会导致所有主链路的AP重连。 相关使用场景介绍请参考 <a href="#">举例介绍</a> 。
备份AC的IP地址	配置之后，AC会在回应AP的DHCP请求时携带本机和备份AC的IP地址，使AP能够向两台AC发起连接。当主链路的AC断开连接后，AP将自动接受备用AC的管理。此功能需要DHCP服务的配合。如果修改备份AC的IP地址将会导致所有主链路的AP重启。 相关使用场景介绍请参考 <a href="#">举例介绍</a> 。

表 7.2 AP设置-AP设置界面项说明

点击<设置>按键，保存以上设置。



#### 说明：

- 修改链路优先级或者备份AC的IP地址，备链路AP需要重启之后才能生效。为保证主备链路AP设置的一致性，请修改设置后立即重启所有备链路AP。
- 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 列表

可以在此查看 AP 列表，还可以对已有条目进行操作。下面介绍此界面的“批量编辑”和“固化”操作。

### 1) 批量编辑

选择多台 AP 设备，点击<批量编辑>按键，进入相应条目的编辑界面，如下图所示。

图 7.5 批量编辑AP界面

AP名称	批量编辑时无法设置AP的名称。
AP保活时间	设置AP与AC之间保活请求的时间间隔。 在AP和AC之间使用保活机制来确认控制信道是否正常工作。为了保持控制信道处于激活状态，AP周期性地发送回声请求（echo request）给AC；AC收到该请求，发送回声应答（echo response），这种保活机制主要是为了使AC感知AP下线。
客户端保活时间	设置客户端保活时间间隔。 正常情况下，客户端下线时会发送离线报文通知AC，AC收到该报文后会删除该客户端。但是，若客户端由于电源故障、系统崩溃等原因离线，客户端便无法通知AC，这样AC的用户列表中就会一直保存该客户端信息。为了防止这种情况发生，可以在AC上开启客户端保活机制，这样AC周期性的对客户端进行扫描，若AC没有收到客户端的扫描应答报文，AC就认为该客户端已经离线，并从用户列表中删除该客户端。
客户端空闲时间	设置AP和客户端之间连接允许的最大空闲时间。 如果用户空闲的时间超过了指定时间，即AP在指定的时间内没有收到从客户端传来的数据，那么客户端将被删除。
有线端口VLAN ID	设置AP额外有线端口的VLAN ID，0表示不设置。只有具备额外有线端口的机型(如TL-AP300I-POE)才能设置该项。
AP离线自管理	启用AP离线自管理，则该AP在断开与AC的连接之后可以接受新客户端的接入请求，但是该AP上配置的所有认证条目将会失效。
controller管理用户名	设置AP controller管理软件的用户名。 在AP与AC关联以后，如果AP接受管理软件管理，需要使用此用户名作为登录用户名或者管理用户名。
controller管理密码	设置AP controller管理软件的密码。 在AP与AC关联以后，如果AP接受管理软件管理，需要使用此密码作为登录密码或者管理密码。

表 7.3 编辑AP设置界面项说明

## 2) 固化

当“自动 AP 固化”功能未启用时，系统自动识别出来的 AP 条目，初始状态为“未固化”，“未固化”的 AP 条目，不能绑定无线服务，不能修改参数，而且当系统复位后，对应的条目也会消失。可以点击< 固化 >按键，将“未固化”的 AP 条目写入到系统的配置文件中，对 AP 条目进行固化，“固化”之后的条目才能进行相关参数的设置。

### 举例介绍

链路优先级和备份 AC 均适用于两台 AC 设备共同管理无线网络的使用场景，在此场景中，推荐用户使用外部 DHCP 服务器，便于网络维护和管理。

应用场景拓扑如下图所示：

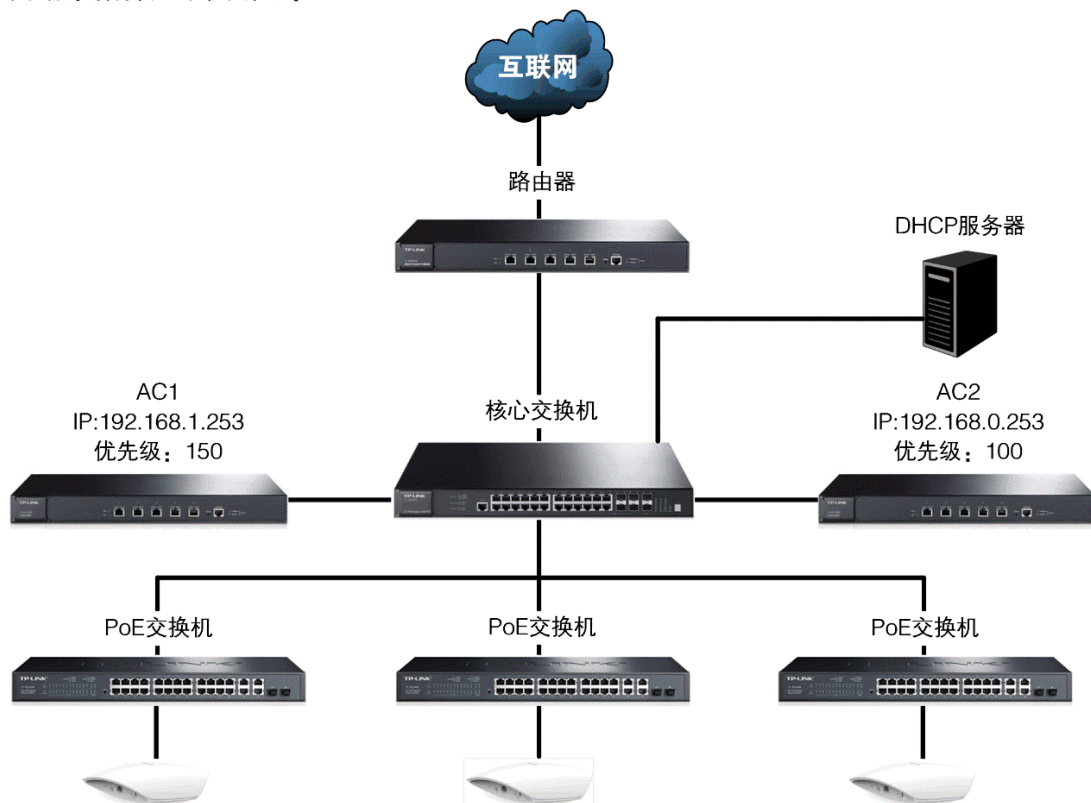


图 7.6 应用举例

### 1) 配置外部DHCP服务器

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](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。

## 2) 配置链路优先级

当网络中有多台 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，可以将这台 AC 的**链路优先级**设置为高。这样，所有新接入或者重新关联的 AP 设备都会与此台 AC 关联以接受管理。当优先级数值越大，该设备的优先级别越高，AP 设备将会优先与其关联。

在图 7.6 中，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。这样，AC1 就作为管理 AP 的主 AC 设备，所有的 AP 将会与 AC1 进行关联。此时，AC2 作为备份链路，起到备份 AC 的作用。

## 3) 配置备份AC（使用AC的DHCP服务）

当网络中有多台 AC 设备并且均可以正常管理所有的 AP，如果希望当某台 AC 设备出现故障无法管理时，其关联的 AP 将自动接收其他 AC 设备的管理，可以将另一台备份 AC 的 IP 设置在**备份 AC 的 IP 地址**。这样，主链路的 AC 在分配 AP 设备 IP 地址时，同时会将备份 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 失效后，备份链路自动转变为主链路，对原有 AP 进行管理，如下图所示。

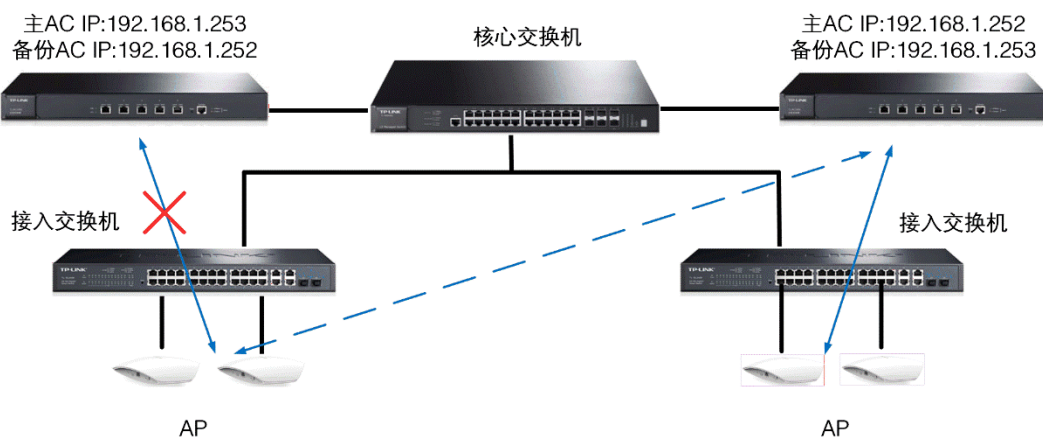


图 7.8 备份AC



### 说明：

在设置备份 AC 时，需配合链路优先级进行设置，将主 AC 的优先级设置为高。

## 7.2.2 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：无线管理 >> AP管理 >> 射频设置

射频列表										
选择	序号	AP名称	射频单元	射频模式	信道	频段带宽	功率等级	客户端限制	状态	设置
<input type="checkbox"/>	1	TL-AP450I-PoE-0001	2.4GHz	802.11b/g/n	自动	自动	Lv8	50	开启	


共1条，每页：20 条 | 当前：1/1页，1~1条 | [首页](#) [上一页](#) [下一页](#) [尾页](#)  [跳转](#)

[全选](#) [批量编辑](#) [开启](#) [关闭](#) [搜索](#) [帮助](#)

图 7.9 射频设置界面

AP名称	显示当前AP名称。
射频单元	显示当前AP射频单元。
射频模式	显示AP射频单元的工作模式。
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。
频率带宽	当射频模式支持 11n 或者 11ac 时，设置频段带宽。 2.4G：802.11n 和 802.11b/g/n 模式可以选择“自动”、“20MHz”、“40MHz”。 5G：802.11n 和 802.11a/n 模式可以选择“自动”、“20MHz”、“40MHz”；802.11a/n/ac 模式可以选择“自动”、“20MHz”、“40MHz”、“80MHz”。
功率等级	显示AP射频单元的发射功率的大小。
客户端限制	显示可以接入该AP射频单元的客户端的最大数目。
状态	显示当前AP射频单元的工作状态。

表 7.4 射频设置界面项说明

在此界面，可以在下拉菜单中修改相关参数，然后点击<  >生效设置内容，也可以勾选条目，然后点击<批量编辑>、<开启>或<关闭>按键对条目进行相应操作。

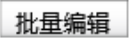
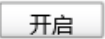
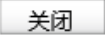
按键	含义
	无线控制器支持同型号 AP 批量编辑的功能，点击该按键进行批量编辑设置。
	点击该按键，可以开启射频单元，使其处于工作状态。
	点击该按键，可以关闭射频单元，使其停止无线信号的发射和接收。 当 AP 的所有射频单元都关闭时，此 AP 将不工作。

表 7.5 射频设置界面项说明-按键

编辑射频设置条目界面如下图所示。

**射频设置**

AP名称： (1-50个字符)

射频单元：

射频模式： ▼

频段带宽： ▼

信道： ▼

发射功率： ▼

关联最大用户数： (1-50个用户)

**- 高级设置**

天线： ▼

分片门限： (必须是偶数, 256-2346字节)

beacon间隔： (40-1000TU)

RTS门限： (1-2347字节)

DTIM周期： (1-255)

WMM： 启用  禁用

响应广播探测： 启用  禁用

Short GI： 启用  禁用

弱信号限制： 启用  禁用 禁止信号强度低于  dBm的客户端接入 (-95 - 0)

弱信号踢除： 启用  禁用 踢除信号强度低于  dBm的客户端 (-95 - 0)

图 7.10 编辑射频设置界面

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。
频段带宽	当射频模式支持11n或者11b/g/n时，设置带宽。
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。
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。
高级设置	点击“高级设置”，将展开高级参数设置项。
天线	设置AP射频单元的天线模式。
分片门限	当射频模式支持11b、11g或者11b/g时设置无线帧数据包的分片门限。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	<p>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。</p> <p>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。</p>
RTS门限	<p>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。</p>
DTIM周期	<p>设置信标的 DTIM 周期 ( Delivery Traffic Indication Message, 数据待传指示信息 )。</p>
WMM	<p>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。</p>
响应广播探测	<p>选择“启用”响应广播探测，AP 会响应客户端的广播探测请求。</p>
Short GI	<p>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。</p>
弱信号限制	<p>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。</p>
弱信号踢除	<p>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。</p>

表 7.6 编辑射频设置界面项说明

**说明：**

射频模式变化后，“高级设置”中的一些参数也会联动变化。

### 7.2.3 AP 版本

可以在此界面升级指定型号的 AP 软件版本。

进入界面：无线管理 >> AP 管理 >> AP 版本

版本升级设置

升级开关： 开启  关闭

[设置](#) [帮助](#)

AP版本列表

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	软件管理
1	TL-AP300I-DC	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
2	TL-AP300I-PoE	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
3	TL-AP300I-PoE	3.0/3.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
4	TL-AP300P	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
5	TL-AP300C-PoE	1.0/2.0/1.1/2.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
6	TL-AP300C-PoE	3.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
7	TL-AP300D	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
8	TL-AP301C	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
9	TL-AP301C	2.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
10	TL-AP302I-DC	1.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
11	TL-AP302I-PoE	1.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
12	TL-AP302C-PoE	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
13	TL-AP302C-PoE	2.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
14	TL-AP303I-PoE	1.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
15	TL-AP306I-PoE	1.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
16	TL-AP450I-DC	1.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
17	TL-AP450I-PoE	1.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
18	TL-AP450C-PoE	1.0/2.0/1.1/2.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
19	TL-AP450C-PoE	3.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
20	TL-AP450D	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
21	TL-AP451C	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
22	TL-AP451C	2.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
23	TL-AP452C-PoE	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
24	TL-AP452C-PoE	2.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
25	TL-AP453C-PoE	1.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
26	TL-AP600C-PoE	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
27	TL-AP900C-PoE	1.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
28	TL-AP902C-PoE	1.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
29	TL-AP1200C-PoE	1.0	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>
30	TL-AP1750C-PoE	1.0/1.1	---	---	---	---	<a href="#">导入</a> <a href="#">删除</a>

[搜索](#) [帮助](#)

图 7.11 AP版本界面

## 版本升级设置

选择“启用”升级开关，并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；关闭该开关，还未开始升级的AP将会停止升级。

## AP 版本列表

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	显示当前系统中保存的该型号AP的软件版本。
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>按钮生效设置。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表示当前检测到有Y台AP需要升级，其中已经升级成功X台。
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。



## 软件管理

可以进行如下操作：

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。

表 7.7 AP版本界面项说明



## 说明：

- 同一时刻最多只能给相同型号的一款AP进行升级。
- 在AC重启或者全部AP定时重启之后的10分钟之内不会执行升级。
- “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。

## 7.2.4 AP 数据库

可以通过本页面导入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：无线管理 >> AP管理 >> AP数据库

### 导入AP数据库

请选择数据库文件，然后点击<导入数据库>按钮进行导入。

文件路径：

浏览...

导入数据库

帮助

[下载新版AP数据库](#)

图 7.12 导入AP数据库界面

点击[下载新版AP数据库](http://service.tp-link.com.cn/list_download_software_1_0.html)的链接，进入TP-LINK服务支持官网的下载中心（[http://service.tp-link.com.cn/list\\_download\\_software\\_1\\_0.html](http://service.tp-link.com.cn/list_download_software_1_0.html)），我司官网会不定期更新无线控制器的AP数据库文件。搜索无线控制器的最新AP数据库，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，点击<导入数据库>按键进行数据库文件导入。

## 7.3 速率设置

可以在此界面设置无线速率。

进入界面：无线管理 >> 速率设置 >> 速率设置

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：

图 7.13 速率设置界面

### 802.11a

#### 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	<p><b>强制速率：</b> 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。</p> <p><b>支持速率：</b> 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。</p> <p><b>组播速率：</b> 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。</p>
802.11g	<p><b>强制速率：</b> 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。</p> <p><b>支持速率：</b> 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。</p> <p><b>组播速率：</b> 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。</p>
802.11n	<p><b>基本MCS索引：</b> 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。</p> <p><b>支持MCS索引：</b> 扩展MCS索引，该值不能小于“基本MCS索引”。</p>
802.11ac	<p><b>基本MCS集合：</b> 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。</p> <p><b>支持MCS集合：</b> 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。</p>

表 7.8 速率设置界面项说明

**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。

## 7.4 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：

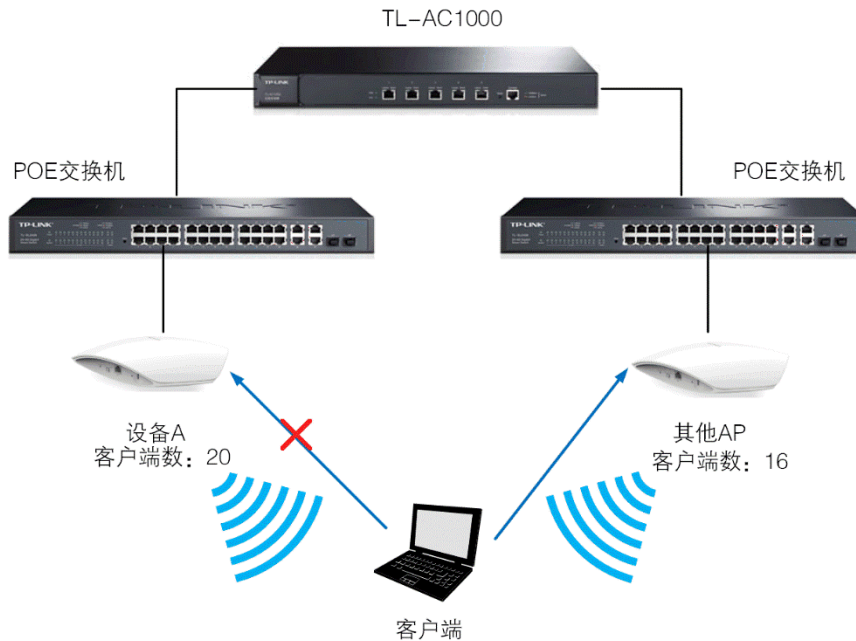


图 7.14 负载均衡应用场景

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（Received Signal Strength Indication，接收的信号强度指示）**门限**，此弱信号客户端将不会参与负载均衡的计算。

进入界面：无线管理 >> 负载均衡 >> 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： ▾

门限： 用户数(2 - 40)

差值门限： 用户数(1 - 8, 缺省值 = 4)

最大失败次数： (0 - 100)

RSSI门限： (-95 - 0,缺省值-75)

图 7.15 负载均衡界面

### 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>按钮，此时**负载均衡设置**区域内的设置生效。

### 负载均衡设置

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。

表 7.9 负载均衡界面项说明

## 7.5 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 7.16 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：无线管理 >> 频谱导航 >> 频谱导航

启用频谱导航功能

频谱导航功能：  启用  禁用

频谱导航设置

5G频段连接门限：  用户数 ( 2-40 )

差值门限：  用户数 ( 1-8 )

最大失败次数：  ( 0-100 )

图 7.17 频谱导航界面

### 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

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。

表 7.10 频谱导航界面项说明

# 第8章 系统管理

## 8.1 服务管理

### 8.1.1 服务设置

可以通过本界面对HTTP、Telnet、HTTPS和Portal服务的基本参数进行设置。

进入界面：系统管理 >> 服务管理 >> 服务设置

The screenshot shows a web-based configuration interface for service settings. It is organized into four distinct sections, each with a light blue header:

- HTTP服务设置**: Contains a '服务端口' (Service Port) field with the value '80' and a note '(80或1024-65535)'.
- Telnet服务设置**: Contains a '服务端口' (Service Port) field with the value '23' and a note '(23或1024-65535)'.
- HTTPS服务设置**: Contains a '开启/关闭服务' (Enable/Disable Service) section with radio buttons for '开启' (selected) and '关闭', and a '服务端口' (Service Port) field with the value '443' and a note '(443或1024-65535)'.
- Portal服务设置**: Contains a '服务端口' (Service Port) field with the value '8080' and a note '(1024-65535)'.

At the bottom of the interface, there are two buttons: '设置' (Settings) and '帮助' (Help).

图 8.1 服务设置界面

#### HTTP 服务设置

服务端口	设置 HTTP 服务的端口，默认为 80。
------	-----------------------

表 8.1 服务设置-HTTP服务设置界面项说明

#### Telnet 服务设置

服务端口	设置 Telnet 服务的端口，默认为 23。
------	-------------------------

表 8.2 服务设置-Telnet服务设置界面项说明

#### HTTPS 服务设置

开启/关闭服务	开启或关闭设备的 HTTPS 服务。
服务端口	设置 HTTPS 服务的端口，默认为 443。

表 8.3 服务设置-HTTPS服务设置界面项说明



## Portal 服务设置

服务端口	<p>设置内嵌 Portal 服务器的服务端口，默认为 8080。</p> <p>修改此参数，将会影响到远程 portal 页面提交和微信连 WIFI 跳转链接等设置内容。请在修改服务端口后，修改相应的设置。</p>
------	--

表 8.4 服务设置-Portal服务设置界面项说明

## 8.2 WEB 管理

## 8.2.1 管理信息

可以通过本界面设置管理账号。

进入界面：系统管理 >> WEB管理 >> 管理信息

The screenshot shows the 'Management Information' interface. It is divided into two main sections: 'Management Account' and 'Session Timeout Time'.  
 In the 'Management Account' section, there are five input fields: 'Original Username' (containing 'admin'), 'Original Password', 'New Username', 'New Password', and 'Confirm New Password'.  
 In the 'Session Timeout Time' section, there is one input field for 'Session Timeout Time' (containing '10') with a note '(5-60 minutes)'. Below this field are two buttons: 'Settings' and 'Help'.

图 8.2 管理信息界面

## 管理账号

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，不输入表示不修改。
新密码	修改后的用户密码。
确认新密码	再次输入新密码。

表 8.5 管理信息-管理账号界面项说明

## 会话超时时间

会话超时时间	在指定的会话时间内，客户端与服务器之间若没有数据交互，将触发会话超时。会话超时后，用户需要重新登录无线控制器才能继续进行操作。
--------	---

表 8.6 管理信息-会话超时时间界面项说明

## 8.3 设备管理

### 8.3.1 恢复出厂配置

进入界面：系统管理 >> 设备管理 >> 恢复出厂配置

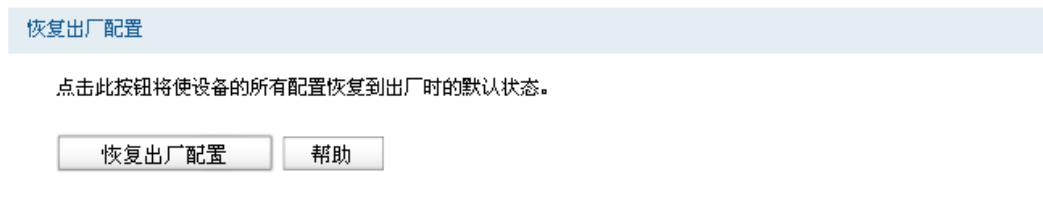


图 8.3 恢复出厂配置界面

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IP地址为192.168.1.253，需要自行设置登录用户名和密码。

### 8.3.2 备份与导入配置

进入界面：系统管理 >> 设备管理 >> 备份与导入配置



图 8.4 备份与导入配置界面

#### 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<备份配置信息>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<导入配置文件>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。

## 8.3.3 重启设备

进入界面：系统管理 >> 设备管理 >> 重启设备

### 重启设备

点击此按钮将使设备重新启动。

重启设备

帮助

图 8.5 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。

## 8.3.4 软件升级

进入界面：系统工具 >> 设备管理 >> 软件升级

### 软件升级

当前软件版本： 1.2.0 Build 20150907 Rel.69489

当前硬件版本： TL-AC1000 v1.0

升级文件路径： 浏览...

升级

帮助

图 8.6 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TL-AC1000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，单击<升级>按键进行软件升级。



### 说明：

- 软件升级成功后无线控制器将会自动重启，在无线控制器重启完成前请保证电源稳定，避免强行断电。
- 软件升级后由于新旧版本软件的差异可能会恢复出厂默认配置，如有重要配置信息，请在升级前备份。

## 8.4 诊断工具

### 8.4.1 诊断工具

可在诊断工具界面通过ping命令或tracert命令来诊断当前无线控制器的网络连接状态。

进入界面：系统管理 >> 诊断工具 >> 诊断工具

PING通信检测

目的IP/域名：

正在检测[192.168.1.200]是否可达，发送的请求包大小为64bytes:

1. 接收到 192.168.1.200 的应答包：大小：64bytes 时延：1ms 生存时间(TTL)：64.
2. 接收到 192.168.1.200 的应答包：大小：64bytes 时延：1ms 生存时间(TTL)：64.
3. 接收到 192.168.1.200 的应答包：大小：64bytes 时延：1ms 生存时间(TTL)：64.
4. 接收到 192.168.1.200 的应答包：大小：64bytes 时延：1ms 生存时间(TTL)：64.

< 检测完成 >

检测[192.168.1.200]的结果统计：

数据包数目：发送包个数：4， 接收包个数：4， 丢失包个数：0， (0% 丢包率).

时延统计：

最短时延：1ms， 最长时延：1ms， 平均时延：1ms.

路由跟踪检测

目的IP/域名：

正在跟踪[192.168.1.200]，最大跳数为 30 跳：

1.            1ms            1ms            1ms            192.168.1.200

< 跟踪完成 >

图 8.7 诊断工具界面

#### PING通信检测

##### 目的 IP/域名

输入目的地址，可以是一个合法 IP 地址，也可以是一个合法域名，如果输入地址无效将提示重新输入。在下拉菜单中选择目的地址所属接口。点击<开始>按钮后，无线控制器将发送 ping 包检测目的地址是否可以到达，并将检测结果显示在下面的方框中。

表 8.7 诊断工具-PING通信检测界面项说明

## 路由跟踪检测

目的 IP/域名	输入目的地址，可以是一个合法 IP 地址，也可以是一个合法域名，如果输入地址无效将提示重新输入。在下拉菜单中选择目的地址所属接口。点击<开始>按钮后，无线控制器将发送 tracert 包检测经过哪些路由到达目的地址，并将检测结果显示在下面的方框中。
----------	--

表 8.8 诊断工具-路由跟踪检测界面项说明

## 8.4.2 诊断信息

可在诊断信息界面将当前诊断工具页面中的诊断结果以bin文件形式导出。

进入界面：系统管理 >> 诊断工具 >> 诊断信息

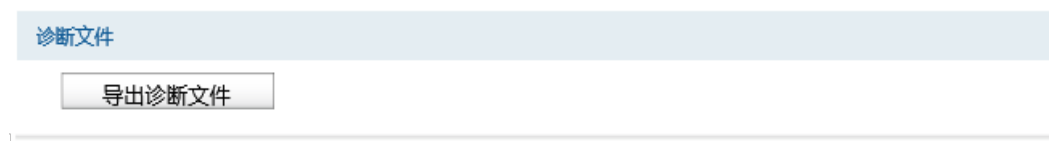


图 8.8 诊断信息界面

## 8.5 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：系统管理 >> 时间设置 >> 时间设置



图 8.9 时间设置界面

## 当前时间

此处将显示目前系统时间及时间获取方式信息。如果想对时间进行更改，可以在下方**时间设置**区域进行改动。

## 时间设置

通过网络获取系统时间	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、备用 NTP 服务器输入框，NTP 服务器地址可以为 IP 地址也可以为域名。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。
手工设置系统时间	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。

表 8.9 时间设置界面项说明



### 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。

## 第9章 命令行简介

CLI ( Command Line Interface, 命令行接口 ) 即命令行, TL-AC1000无线控制器提供了一个用于CLI配置的Console口。可以通过控制台 ( 比如超级终端 ) 和在局域网内通过Telnet进入命令行界面进行设置。

以下介绍通过超级终端访问CLI的具体步骤和一些常用的CLI命令。

### 9.1 搭建平台

请按照以下步骤通过 Console 口登录无线控制器：

1. 使用提供的 Console 线连接无线控制器和计算机的 Console 口。
2. 在 PC 上启动终端仿真程序 ( 例如超级终端 ) 。
3. 在终端仿真程序中指定连接端口。
4. 配置终端仿真程序, 按照以下设置:
  - 每秒位数: 115200
  - 数据位: 8
  - 奇偶校验: 无
  - 停止位: 1
  - 数据流控制: 无
5. 在终端仿真程序主窗口中按下回车键, 如果出现如所示的命令提示符“TP-LINK>”, 说明可以使用 CLI 命令管理无线控制器。

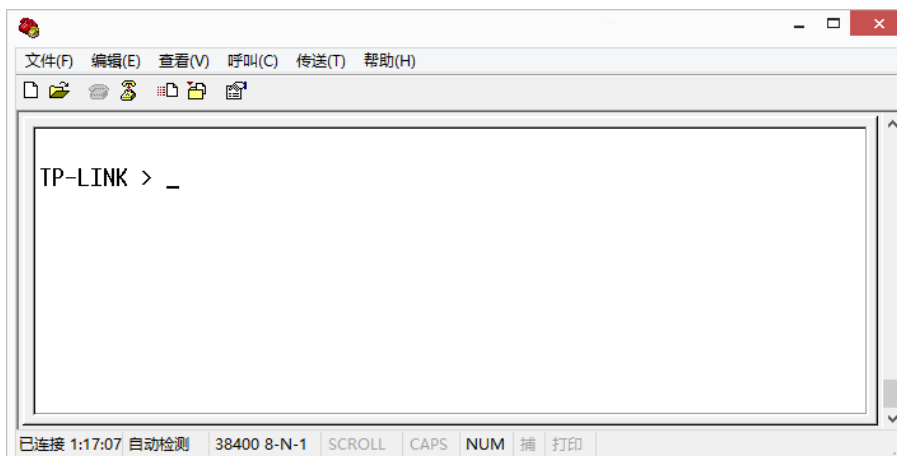


图 9.1 登录无线控制器

## 9.2 界面模式

TL-AC1000的CLI提供了两个界面模式：用户模式和特权模式。用户模式下只具有基本的权限，比如查看系统的信息等。特权模式下则拥有管理无线控制器的权限，可以进行各种配置操作等。这样就可以对不同的用户进行适当的权限管理。

**用户模式：**Telnet登录时，需输入无线控制器的用户名和密码，与webserver管理账号共用同一个用户名和密码；Console连接登录时不需要密码。登录后，用户处于用户模式下，拥有的权限为参观级。可以进行简单的查询操作，不能修改无线控制器的各种配置信息。

**特权模式：**用户在用户模式下进行密码验证，验证通过就可以进入特权模式。拥有管理级的权限，可以对无线控制器进行各种配置操作。

默认情况下，CLI用户处于用户模式下。用户可以自由的在用户模式和特权模式之间进行切换，方式如下：

模式	访问方法	提示符	离开或访问下一模式
用户模式	与无线控制器建立连接即进入该模式。	TP-LINK >	输入 exit 命令断开与无线控制器的连接。 ( Console 连接时无法断开) 要进入特权模式，输入 enable 命令。
特权模式	在用户模式下，使用 enable 命令进入该模式，初始密码 admin。	TP-LINK #	输入 exit 命令断开与无线控制器连接 ( Console 连接时无法断开) 要返回到用户模式，输入 disable 命令。

## 9.3 在线帮助

TL-AC1000提供了命令行在线帮助：

- 1) 在任一模式下，键入“?”获取该视图下所有的命令及其简单描述。例如在用户模式下直接键入问号“?”，可以获得下面提示内容：

disable	Exit the privileged mode
enable	Enter the privileged mode
exit	Exit the CLI ( only for telnet )
history	Show command history
port	Configure port
sys	System manager
vlan	Specify vlan setting

- 2) 键入一命令，后接以空格分隔的“?”，如果该命令行位置有关键字，则列出全部关键字及其简单描述。例如在tp-link > history 命令后键入问号“?”，将会弹出“clear”命令关键字提示。



- 3) 键入一字符串，其后紧接“?”，将列出以该字符串开头的命令。例如在tp-link > dis命令后键入问号“?”，将会弹出完整的命令提示disable。
- 4) 键入命令的某个关键字的前几个字母，按下<Tab>键，如果以输入字母开头的关键字唯一，则可以显示出完整的关键字。例如在tp-link > dis命令后按下<Tab>键，将会补全命令为tp-link > disable。
- 5) 命令的输入完成之后，后接以空格分隔的“?”，会显示出一个回车符<cr>，表示此时命令已正确无误，可以执行。

## 9.4 命令介绍

TL-AC1000提供了一些CLI命令，通过这些命令可以管理无线控制器和用户信息。为便于您理解，每条命令后面会注释该条命令的含义。

### 9.4.1 特权模式密码设置命令

通过super命令可以查看和修改特权模式的密码。

TP-LINK # super password get	查看特权模式的密码。密码采用 MD5 加密，查看的密码为 MD5 值。
TP-LINK # super password set Enter old password: Enter new password: Confirm new password:	修改特权模式的密码。

### 9.4.2 VLAN 配置命令

通过VLAN相关配置命令可以配置VLAN相关功能。

TP-LINK # port config portId:[ 1-5 ] 1 opType:[ 0:linktype;1:pvid ] 0 Linktype:[ 0:access;1:trunk;2:general ] 0	设置端口的链路类型或者 PVID。
TP-LINK # port show all	显示所有端口的链路类型和 PVID。
TP-LINK # port show id 1	显示指定端口的链路类型和 PVID。
TP-LINK # port vlan show	显示端口和 VLAN 之间的关联表。
TP-LINK # vlan config add 3 vlan3 portlist 4	添加 vlan 条目，指定相关的端口。
TP-LINK # vlan config delete id 2	删除指定 vlanId 的条目。
TP-LINK # vlan config show all	显示所有 vlan 条目。
TP-LINK # vlan config show id 5	显示指定 VLAN ID 的条目。

### 9.4.3 系统管理

sys命令。可以使用该命令进行相关的系统管理操作，包括配置文件的导入导出、恢复出厂配置、重启系统和升级软件等。

<pre>TP-LINK # sys save config</pre>	<p>保存系统配置。</p> <p>配置完成后，请使用保存配置命令，当重启设备时可以保证当前所有配置持续生效。</p>
<pre>TP-LINK # sys reboot This command will reboot system, Continue?[Y/N]</pre>	<p>重启系统。Y 即 YES，表确认；N 即 NO，表取消。</p>
<pre>TP-LINK # sys restore This command will restore system, Continue?[Y/N]</pre>	<p>恢复出厂配置。Y 即 YES，表确认；N 即 NO，表取消。</p>
<pre>TP-LINK # sys export config Server address: [192.168.1.101]192.168.1.100 Username: [admin]ftp Password: [admin]ftp File name: [config.bin] Try to save the configuration file &lt; config.bin &gt; ... Save configuration file &lt; config bin &gt; succeed, file size is 7104 bytes.</pre>	<p>配置文件导出。</p> <p>举例：现有一台 IP 地址为 192.168.1.100 的 FTP 服务器，服务的用户名/密码是 ftp/ftp，如需将当前配置文件以默认文件名 config.bin 保存到该 FTP 服务器上，设置如左。</p>
<pre>TP-LINK # sys import config Server address: [192.168.1.101] Username: [admin] Password: [admin] File name: [config.bin] Try to get the configuration file &lt; config.bin &gt; ... Get configuration file &lt; config bin &gt; succeed, file size is 7104 bytes.</pre>	<p>配置文件导入。说明同上。</p>
<pre>TP-LINK &gt; sys show CPU1 Used Rate: 2% CPU2 Used Rate: 1%</pre>	<p>查看系统信息。该命令将会显示当前系统的 CPU 利用率。</p>
<pre>TP-LINK # sys update Server address: [192.168.1.101] Username: [admin] Password: [admin] File name: [update.bin] Try to get the update file &lt; update.bin &gt; ... Get update file &lt; update bin &gt; succeed, file size is 2298608 bytes.</pre>	<p>系统软件升级。</p>

**说明:**

- 配置文件的导出、导入、系统升级都需要使用FTP服务。在需设置的参数中，Server address是提供FTP服务的主机IP地址，Username/Password是该FTP服务的登录名/密码，File name是配置文件名（如果已存在同名的配置文件，请更改文件名）。
- 中括号内是默认设置，可在其后输入实际参数，如果无需改动直接回车确认即可。
- 本无线控制器默认连接到使用21端口的FTP服务器。
- 由于导出、导入、系统升级等功能需要在FTP服务器上进行读写操作，因此特别需要注意您指定的账号必须具有相应权限。

## 9.4.4 历史命令管理

history命令。可以使用该命令查看或清除系统中的历史命令。

<pre>TP-LINK &gt; history 1. history 2. sys show 3. history</pre>	查看历史命令。
<pre>TP-LINK &gt; history clear 1. history 2. sys show 3. history 4. history clear</pre>	清除历史命令。

## 9.4.5 退出 CLI

exit命令。可以使用该命令退出系统。但仅限于Telnet环境，Console环境下不会退出。

<pre>TP-LINK &gt; exit</pre>	退出系统。
------------------------------	-------

## 附录A 常见问题

### 问题1：无法登录无线控制器WEB管理界面该如何处理？

- 1) 观察指示灯的状态，检查相应端口线缆是否正常连接，同时确认端口没有被禁用，可以换另外一个物理端口登录无线控制器；
- 2) 如果是通过本地计算机管理无线控制器，请确保计算机IP地址与无线控制器IP地址处于同一网段；
- 3) 通过Ping命令检查网络连接。通过“开始”→“运行”输入“cmd”命令，点击“确定”后，可以打开命令窗口。输入ping 127.0.0.1检查计算机的TCP/IP协议是否安装；输入ping 192.168.1.253（无线控制器管理接口的IP地址，如果无线控制器设有多个管理接口，也可以ping其它管理接口的IP地址）检查计算机与无线控制器的连接是否正常；
- 4) 如果确认物理连接正常，但是还是无法管理，建议通过console口管理无线控制器，检查无线控制器VLAN和管理IP相关配置信息，console口登录方法详见[命令行简介](#)；
- 5) 如果修改过无线控制器的管理端口，则注意下次登录时需要以“http://管理IP:XX”的方式登录，XX为修改后的端口号，如http://192.168.1.253:12345；
- 6) 如果恢复出厂配置后仍然无法登录或开始一段时间能登录，但过一段时间后又不能登录，则可能是遭受了ARP欺骗，建议查找欺骗源、查杀病毒或将其其他所有网络设备移除，电脑单机接无线控制器尝试。

### 问题2：忘记无线控制器用户名和密码怎么办？

忘记用户名、密码时可以将TL-AC1000通过Reset键恢复至出厂配置。需要注意的是：恢复出厂配置时无线控制器原有配置信息将丢失。

恢复出厂配置操作方法：在无线控制器通电的情况下，使用尖状物按住无线控制器的Reset键，等待2-5秒后，见到系统指示灯快速闪烁1-2秒，松开按键，无线控制器将自动恢复出厂设置并重启。无线控制器出厂默认管理地址是http://192.168.1.253，需要自行设置登录用户名和密码。

### 问题3：忘记无线控制器管理IP或管理端口怎么办？

出于对无线控制器管理安全的考虑，在用户不知道无线控制器管理IP或者端口的情况下，需要对无线控制器进行管理，建议使用Reset键将无线控制器恢复出厂设置。

## 附录B 规格参数

参数项	参数内容
支持的标准和协议	IEEE 802.3、IEEE 802.3i、IEEE 802.3u、IEEE 802.3ab
端口	RJ45 口：5 个 10/100/1000M 自适应 RJ45 端口（Auto MDI/MDIX）
	Console 口：1 个 Console 端口（RJ45）
网络介质	10BASE-T：3 类或以上 UTP/STP（≤100m）
	100BASE-TX：5 类或以上 UTP/STP（≤100m）
	1000BASE-T：超 5 类或以上 UTP/STP（≤100m）
LED 指示	PWR 电源指示灯、SYS 系统指示灯、Link/Act 指示灯、Speed 速率指示灯
尺寸（L x W x H）	440mm x 227mm x 44mm
电源输入	100-240V~ 50/60Hz 0.6A
工作温度	0° C ~ 40° C
存储温度	-40° C ~ 70° C
工作湿度	10% ~ 90%RH 不凝结
存储湿度	5% ~ 90%RH 不凝结