

[www.ip-com.com.cn](http://www.ip-com.com.cn)

# 使用说明书

500 米监控专用网桥 · CPE3

**IP-COM**  
World Wide Wireless

## 声明

**版权所有©2018 深圳市和为顺网络技术有限公司。保留一切权利。**

未经本公司书面许可，任何单位或个人不得擅自复制、摘抄及翻译本档部分或全部内容，且不得以任何形式传播。

**IP-COM** 是深圳市和为顺网络技术有限公司在中国和(或)其它国家与地区的注册商标。其它品牌和产品名称均为其相应持有人的商标或注册商标。

由于产品版本升级或其它原因，本档内容会不定期更新。除非另有约定，本档仅作为使用指导，文中的所有陈述、信息和建议均不构成任何形式的担保。

## 前言

感谢选择 IP-COM 产品。开始使用本产品前，请先阅读本说明书。

## 约定

本文可能用到的格式说明如下。

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

本文可能用到的标识说明如下。

标识	含义
 注意	表示重要信息或需要特别关注的信息。若忽略此等信息，可能导致配置失效、数据丢失或设备故障。
 提示	表示有助于节省时间或资源的方法。

## 缩略语

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

## 更多信息

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

## 技术支持

如需技术支持，请通过以下方式与我们联系。

---



40066-50066



[ip-com@ip-com.com.cn](mailto:ip-com@ip-com.com.cn)



<http://www.ip-com.com.cn>

---

# 目录

<b>1 产品介绍</b> .....	<b>1</b>
1.1 简介.....	1
1.2 外观.....	1
1.2.1 指示灯.....	1
1.2.2 按钮&接口.....	2
1.2.3 贴纸.....	3
<b>2 应用场景</b> .....	<b>4</b>
2.1 小区电梯监控.....	4
2.1.1 方案.....	4
2.1.2 设置网桥.....	4
2.1.3 组网图.....	12
2.2 塔吊监控.....	13
2.2.1 方案.....	13
2.2.2 设置网桥.....	13
2.2.3 组网图.....	13
<b>3 设备登录</b> .....	<b>14</b>
3.1 登录网桥的管理页面.....	14
3.2 退出登录.....	15
3.3 页面布局.....	16
3.4 常用按钮.....	16
<b>4 快速设置</b> .....	<b>17</b>
4.1 AP 模式.....	17

4.1.1 概述.....	17
4.1.2 设置 AP 模式.....	18
4.2 客户端模式.....	20
4.2.1 概述.....	20
4.2.2 设置客户端模式.....	20
4.3 无线 WAN 模式.....	24
4.3.1 概述.....	24
4.3.2 设置无线 WAN 模式.....	24
<b>5 系统状态.....</b>	<b>29</b>
5.1 系统状态.....	29
5.1.1 AP/客户端模式下系统状态.....	29
5.1.2 无线 WAN 模式下系统状态.....	30
5.2 无线状态.....	32
5.3 统计.....	33
5.3.1 吞吐量.....	33
5.3.2 无线客户端.....	34
5.3.3 上级 AP.....	34
5.3.4 接口.....	35
5.3.5 ARP 表.....	36
5.3.6 路由表.....	36
<b>6 网络设置.....</b>	<b>38</b>
6.1 LAN 口设置.....	38
6.1.1 概述.....	38
6.1.2 修改 LAN IP.....	39
6.2 MAC 克隆（仅无线 WAN 模式有效）.....	42
6.2.1 概述.....	42
6.2.2 克隆 MAC 地址.....	42

6.3 DHCP 服务器 .....	44
6.3.1 概述 .....	44
6.3.2 配置 DHCP 服务器 .....	44
6.4 DHCP 客户端列表 .....	46
6.5 VLAN 设置 .....	46
6.5.1 概述 .....	46
6.5.2 配置 VLAN .....	46
6.5.3 VLAN 设置举例 .....	47
<b>7 无线设置 .....</b>	<b>50</b>
7.1 基本设置 .....	50
7.1.1 概述 .....	50
7.1.2 修改基本设置 .....	52
7.1.3 基本设置举例 .....	57
7.2 高级设置 .....	75
7.2.1 概述 .....	75
7.2.2 修改高级参数 .....	75
7.3 访问控制 .....	78
7.3.1 概述 .....	78
7.3.2 配置访问控制 .....	78
7.3.3 访问控制配置举例 .....	79
<b>8 高级设置 .....</b>	<b>81</b>
8.1 LAN 口速率 .....	81
8.1.1 概述 .....	81
8.1.2 修改 LAN 口速率 .....	81
8.2 网络诊断 .....	83
8.2.1 概述 .....	83
8.2.2 扫描信号 .....	83

8.2.3 执行 Ping .....	84
8.2.4 执行 Traceroute .....	86
8.3 网络服务 .....	87
8.3.1 动态 DNS (仅无线 WAN 模式有效) .....	87
8.3.2 远程 WEB 管理 (仅无线 WAN 模式有效) .....	91
8.3.3 定时重启 .....	93
8.3.4 WEB 闲置超时时间 .....	94
8.3.5 SNMP 代理 .....	94
8.3.6 Ping 看门狗 .....	98
8.3.7 DMZ 主机 (仅无线 WAN 模式有效) .....	99
8.3.8 Telnet 服务 .....	101
8.3.9 UPnP 服务 .....	101
<b>9 系统工具 .....</b>	<b>102</b>
9.1 时间与日期 .....	102
9.2 设备维护 .....	104
9.2.1 重启 .....	104
9.2.2 恢复出厂设置 .....	105
9.2.3 软件升级 .....	106
9.2.4 备份与恢复 .....	108
9.3 管理员 .....	111
9.3.1 管理员 .....	111
9.3.2 访客 .....	112
9.4 系统日志 .....	113
<b>附录 .....</b>	<b>114</b>

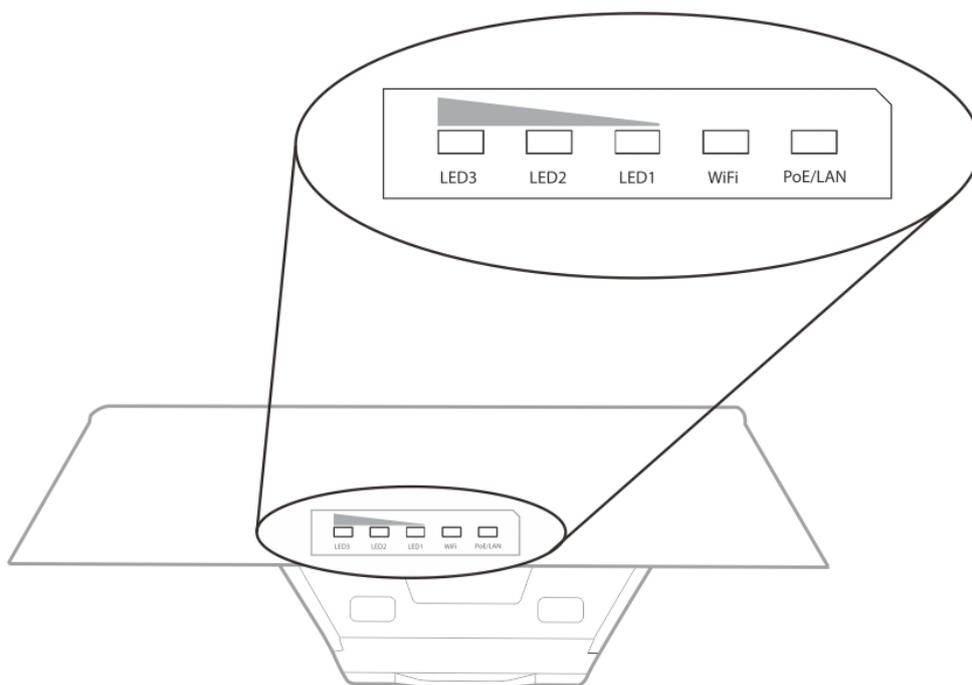
# 1 产品介绍

## 1.1 简介

CPE3 是 IP-COM 专为电梯，塔吊，小区，工厂，果园，景区等场景视频监控而设计的室外无线网桥；设备工作在 2.4GHz 频段，采用 11n 技术，最高可提供 300Mbps 的无线数据传输速率；内置 8dBi 高增益定向天线，信号穿透力更强，室外点对点桥接距离可达 500 米；基于抱杆式设计，可直接安装在墙壁和柱状物品上，美观大方；采用工业级高等防水防尘塑胶壳，可工作在风，雨，雪等各种户外环境。

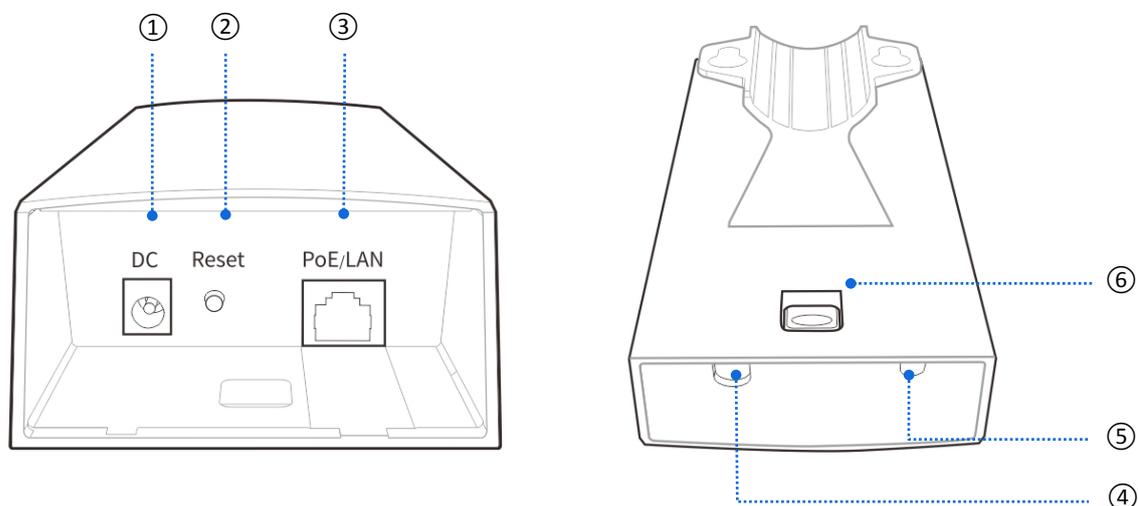
## 1.2 外观

### 1.2.1 指示灯



指示灯	状态	说明
PoE/LAN	长亮	供电正常且接口没有数据传输。
	闪烁	接口正在传输数据。
	熄灭	供电异常。
WiFi	长亮	无线功能已开启，且没有数据传输。
	闪烁	正在通过无线传输数据。
	熄灭	无线功能已关闭。
LED1、LED2、LED3	长亮	已桥接成功，网桥工作在 AP 模式。 <ul style="list-style-type: none"> <li>- LED1、LED2、LED3 均长亮：信号强</li> <li>- LED1、LED2 长亮，LED3 熄灭：信号一般</li> <li>- LED1 长亮，LED2、LED3 熄灭：信号差，请调整两个网桥的方向或位置。</li> </ul>
	闪烁	已桥接成功，网桥工作在客户端模式。
	熄灭	未桥接。

## 1.2.2 按钮&接口

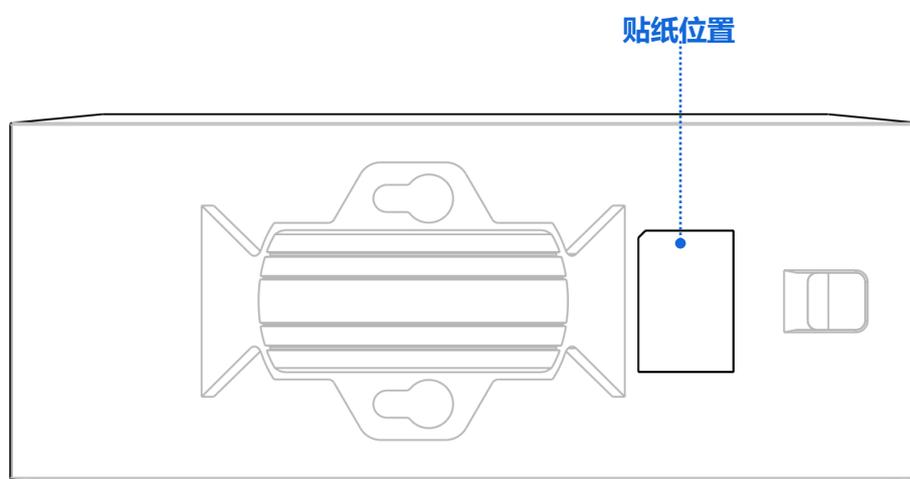


序号	丝印	说明
①	DC	电源接口。 可使用包装盒内的电源适配器给网桥供电。
②	Reset	复位按钮。 网桥通电 1 分钟后，按住 7 秒后松开，指示灯全亮时，网桥已经恢复到出厂状态。

序号	丝印	说明
③	PoE/LAN	PoE 电源输入、数据传输复用接口。 <ul style="list-style-type: none"><li>- 使用 PoE 供电时，可连接配套的 PoE 注入器给网桥通电。</li><li>- 使用 DC 供电时，可连接交换机。</li></ul>
④	/	网线卡槽。
⑤	/	电源线卡槽，使用 DC 供电时，可以剪开。
⑥	/	开盖按钮。

## 1.2.3 贴纸

贴纸位于网桥的背面，具体位置如下图所示。



您可以在该贴纸上找到它的默认登录 IP 地址、用户名和密码等信息。



## 2 应用场景

### 2.1 小区电梯监控

某小区日常进出人员流动频繁，为了保障小区业主的人身和财产安全，需要在电梯内安装监控摄像头实行监控。

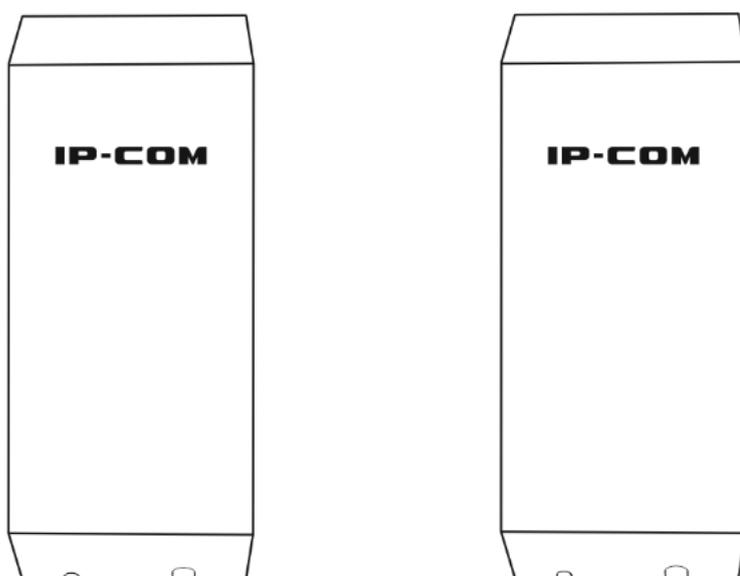
#### 2.1.1 方案

使用无线网桥进行组网。

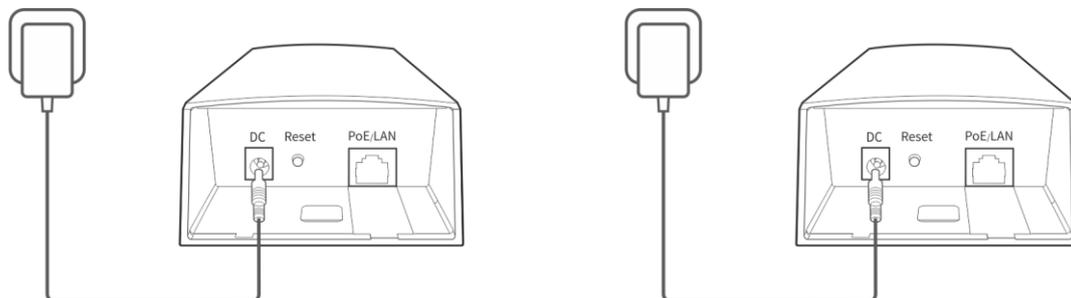
#### 2.1.2 设置网桥

##### 方式一：自动桥接（推荐）

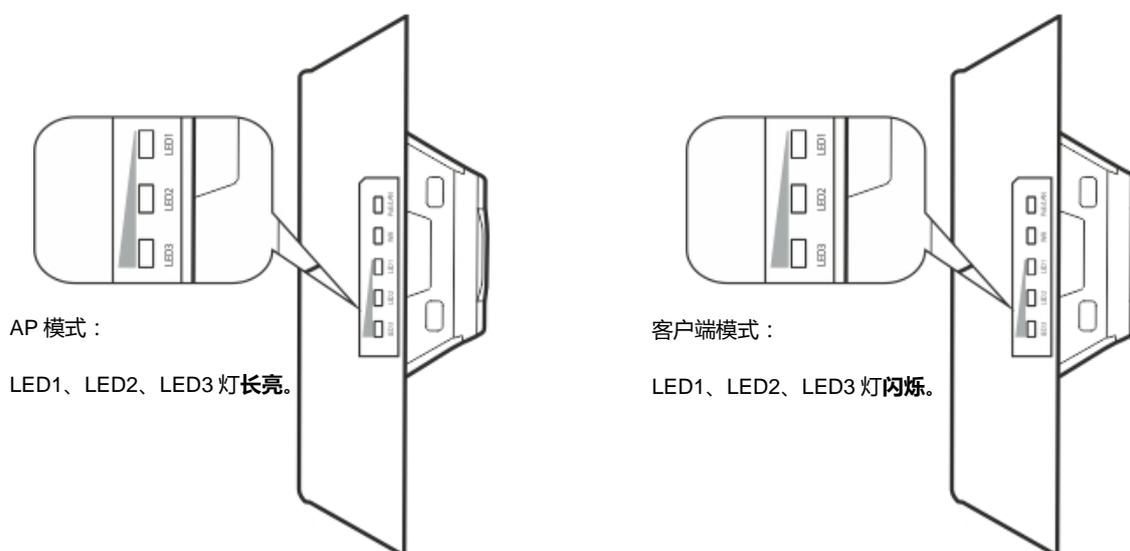
1. 将两台网桥相邻放置，如下图示。



- 按下并推动网桥背面的按钮，打开网桥的保护盖，使用电源适配器分别给两台网桥通电。系统启动完成后，网桥的 WiFi 灯亮。



- 两台网桥会自动进行桥接，请稍等。桥接成功状态如下图示。

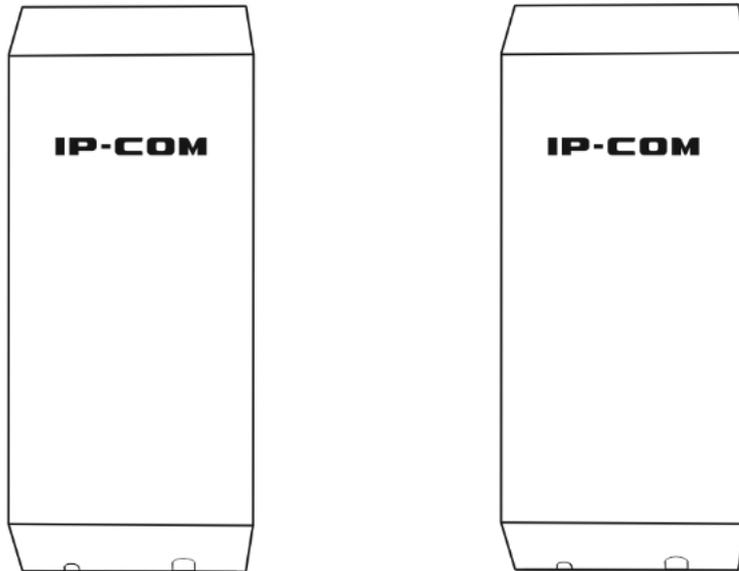


### 注意

- 自动桥接仅对处于出厂设置状态的网桥生效，且在上电后 1 分钟内生效。
- 自动桥接仅适用于 1 对 1 桥接，近距离内如果有 3 台及以上已经通电的网桥，会导致自动桥接失败。如果您需要 1 对多桥接，请使用[手动桥接](#)方式。
- 桥接成功后，两台网桥的 DHCP 服务器将自动关闭；工作在客户端模式的网桥的 IP 地址变为 192.168.2.2。

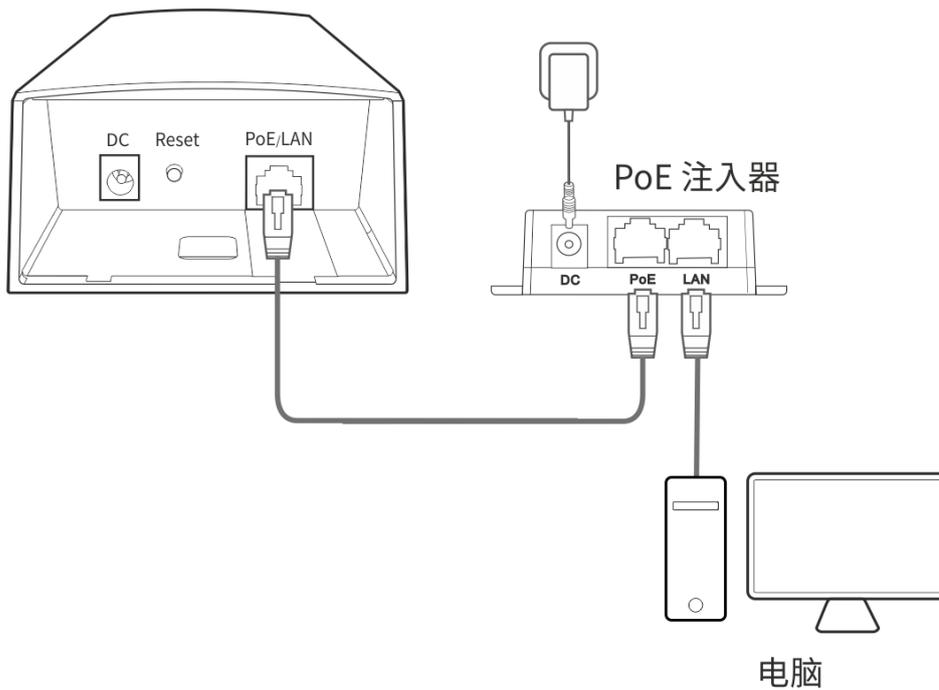
## 方式二：手动桥接

1. 将两个网桥相邻放置。



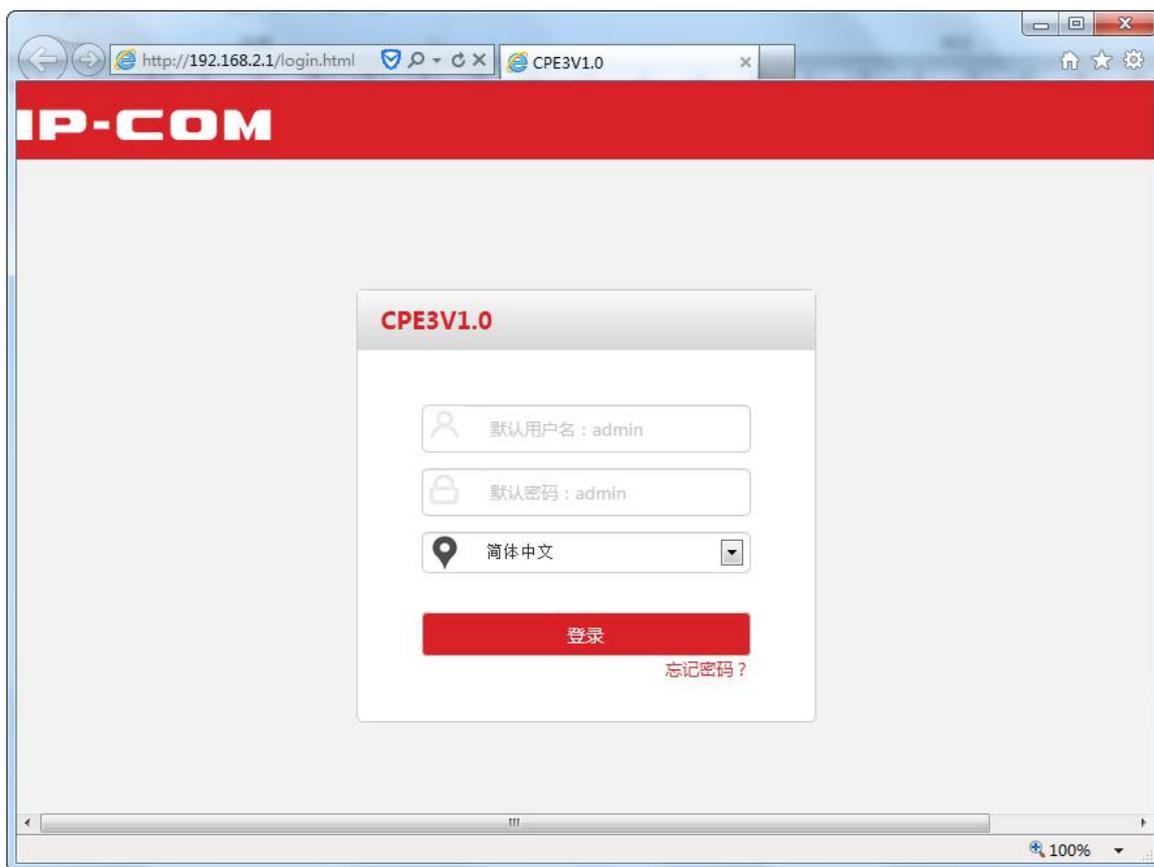
2. 连接第 1 个网桥。（以 PoE 供电为例）

- (1) 按下并推动网桥背面的按钮，打开网桥的保护盖。
- (2) 用网线连接网桥的 PoE/LAN 口和 PoE 注入器的 PoE 口。
- (3) 用包装盒内的电源适配器将 PoE 注入器连接到电源插座，网桥的 PoE/LAN 灯亮。
- (4) 用网线将电脑连接到 PoE 注入器的 LAN 口。



### 3. 设置第 1 个网桥为 AP 模式。

(1) 打开电脑上的浏览器，访问 **192.168.2.1**。输入用户名和密码，点击**登录**。



若未出现上述页面，请查看常见问题解答的[问 2](#)。

(2) 进入「快速设置」页面，选择 **AP 模式**，点击 **下一步**。



(3) SSID (无线网络名称)：点击输入框，修改无线网络的无线名称，如 IP-COM\_1。

(4) 信道：选择无线工作的信道。

(5) 安全模式：选择无线网络安全模式，设置其展开的参数( 建议选择“WPA2-PSK” > “AES” )。

(6) 点击 **下一步**。

快速设置 >> AP模式 当前模式：AP模式

设置本设备的无线网络名称（SSID）和无线密码（密钥），  
请记住您的无线密码

SSID（无线网络名称）	<input type="text" value="IP-COM_1"/>
信道	<input type="text" value="11 (2462MHz)"/>
安全模式	<input type="text" value="WPA2-PSK"/>
加密规则	<input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> TKIP&AES
密钥	<input type="text" value="12345678"/>

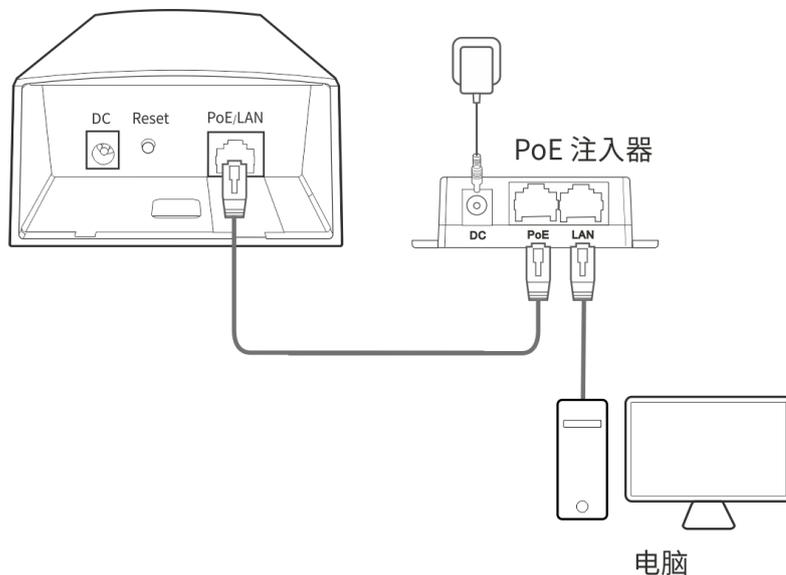
(7) 点击 **保存**，等待网桥自动重启使设置生效。

快速设置 >> AP模式 当前模式：AP模式

设备已配置为AP模式，请点击“保存”激活配置

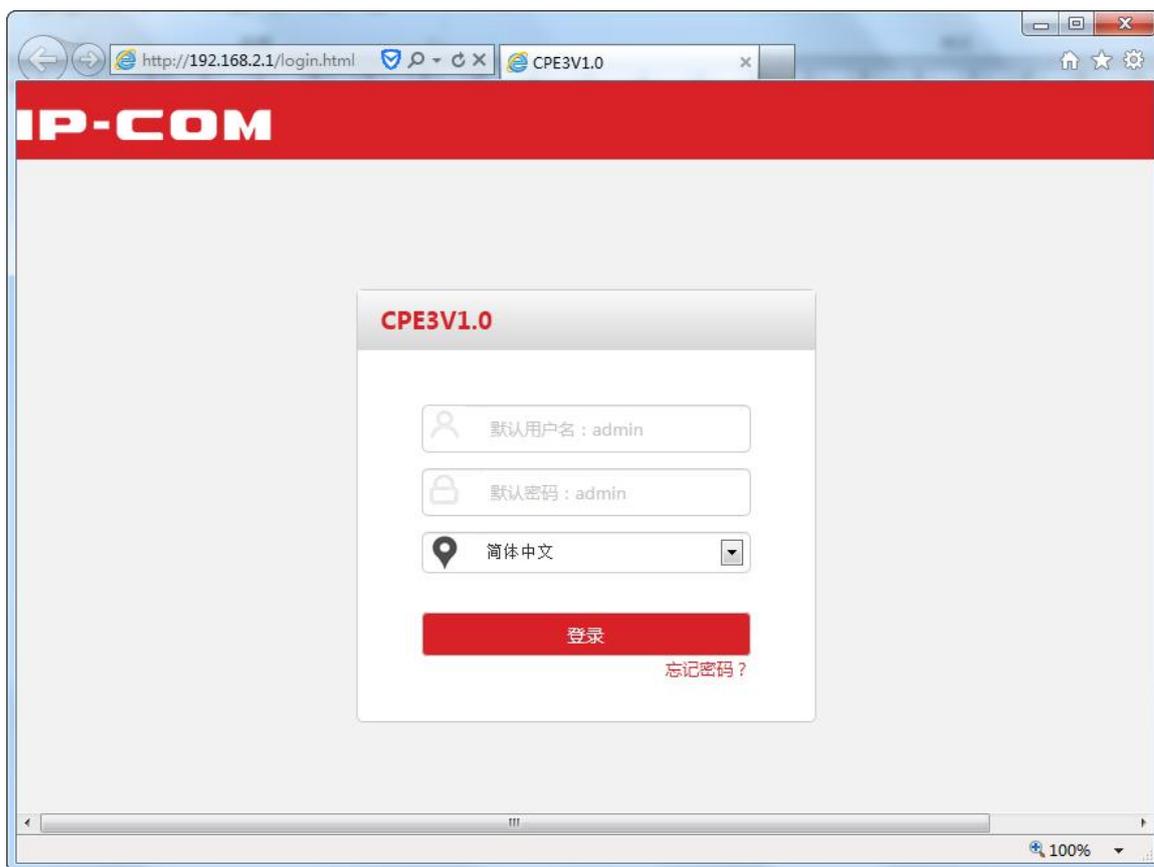
#### 4. 连接第 2 个网桥。（以 PoE 供电为例）

- (1) 按下并推动网桥背面的按钮，打开网桥的保护盖。
- (2) 用网线连接网桥的 PoE/LAN 口和 PoE 注入器的 PoE 口。
- (3) 用包装盒内的电源适配器将 PoE 注入器连接到电源插座，网桥的 PoE/LAN 灯亮。
- (4) 用网线将电脑连接到 PoE 注入器的 LAN 口。



5. 设置第2个网桥为客户端模式。

(1) 打开电脑上的浏览器，访问 **192.168.2.1**。输入用户名和密码，点击**登录**。



提示

若未出现上述页面，请查看常见问题解答的[问2](#)。

(2) 选择**客户端模式**，点击 **下一步**。



(3) 在出现的无线网络列表中，选择要桥接的无线网络，如 IP-COM\_1。

(4) 点击 **下一步**。



如果扫描不到无线网络，请进入「无线设置」>「基本设置」页面，确认您**已开启无线**，然后重新尝试。

当前模式：AP模式

**快速设置 >> 客户端模式**

点击“扫描”，选择您想要连接的无线网络，  
然后点击“下一步”

扫描  [重新扫描](#)

上级AP

透明网桥

选择	SSID	信道	MAC地址	安全模式	信号强度
	IP-COM_1	11	50:2B:73:09:94:51	WPA2-PSK,AES	

(5) 输入上级无线网络的密钥，点击 **下一步**。

当前模式：AP模式

**快速设置 >> 客户端模式**

请保持信道、安全模式、加密规则与上级AP一致，  
然后输入上级AP的密钥，点击“下一步”

上级AP

上级AP的MAC地址

信道

安全模式

加密规则  AES  TKIP  TKIP&AES

密钥

6. 修改 IP 地址信息。

- (1) IP 地址：将本网桥 IP 地址改为与第一个网桥 IP 地址不同但在同一网段，如 192.168.2.10。
- (2) 子网掩码：设置 IP 地址的子网掩码，如 255.255.255.0。
- (3) 默认网关：输入网关地址，一般为网络中已联网路由器的 LAN 口 IP 地址。
- (4) 首选 DNS 服务器：输入 DNS 信息。

7. 点击 **下一步**。

当前模式：AP模式

**快速设置 >> 客户端模式**

请将IP地址设置为与上级AP相同网段的不同IP

IP地址	<input type="text" value="192.168.2.10"/>
子网掩码	<input type="text" value="255.255.255.0"/>
默认网关	<input type="text"/>
首选DNS服务器	<input type="text"/>
备用DNS服务器	<input type="text" value="8.8.4.4"/>

8. 点击 **保存**，等待网桥自动重启使设置生效。

当前模式：AP模式

**快速设置 >> 客户端模式**

设备已配置为客户端模式，请点击“保存”激活配置

#### ----完成

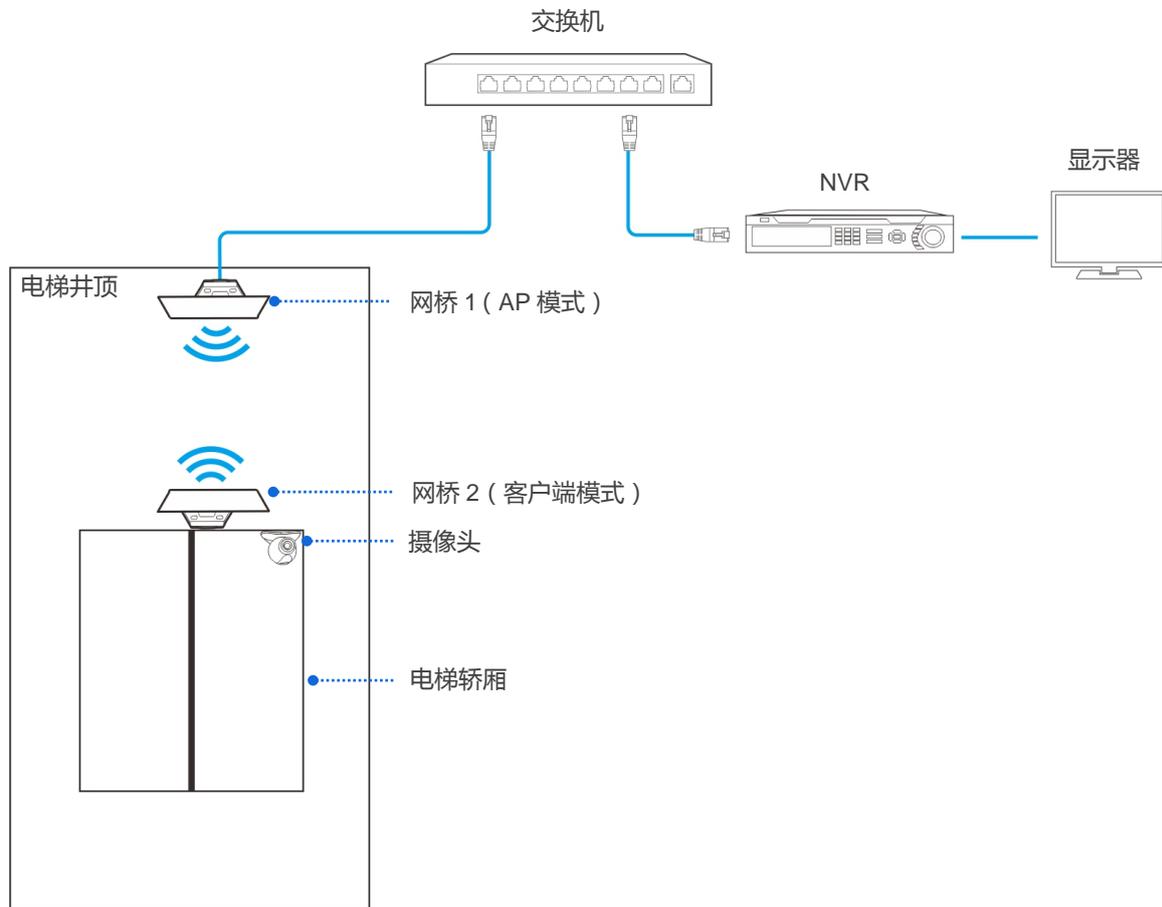
当第一个网桥的 LED1、LED2、LED3 长亮，第二个网桥的 LED1、LED2、LED3 闪烁时，桥接成功。



登录到网桥管理页面后，进入「无线设置」>「基本设置」页面，可查看网桥的 SSID 和密钥。

## 2.1.3 组网图

将网桥安装到相应位置，拓扑图如下。



## 2.2 塔吊监控

某一建筑工地进行工程施工，为了保障人员的生命财产安全，现在需要对塔吊使用过程进行有效监控。

### 2.2.1 方案

使用无线网桥进行组网。

### 2.2.2 设置网桥

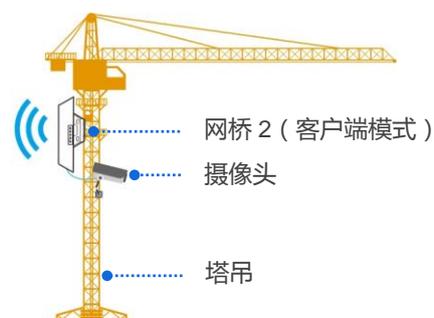
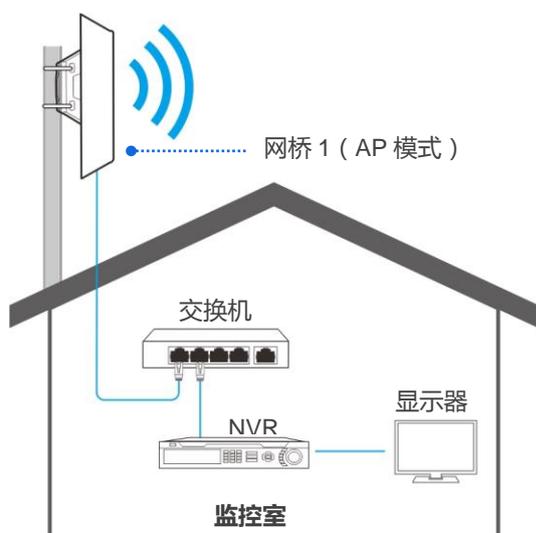
设置步骤请参考 2.1.2 [设置网桥](#)。



如果需要设置一对多桥接，请采用手动桥接。

### 2.2.3 组网图

将网桥安装到相应位置，拓扑图如下。

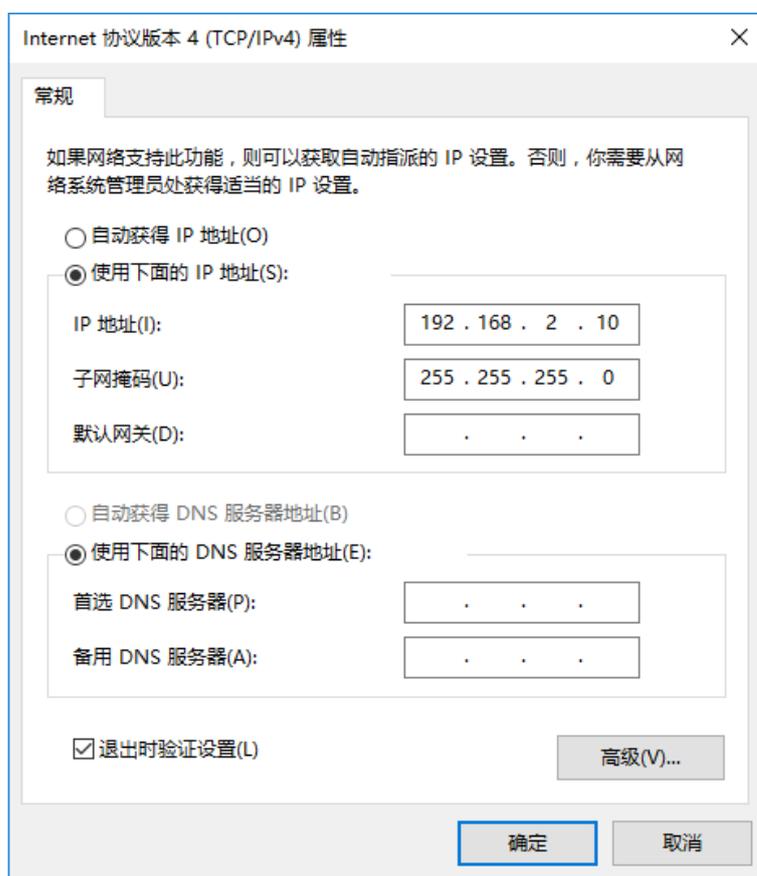


# 3 设备登录

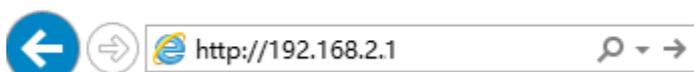
## 3.1 登录网桥的管理页面

1. 用网线将管理电脑接到网桥（或网桥连接的交换机）。
2. 设置电脑的本地连接 IP 地址，使其与网桥的 IP 地址在同一网段。

如，网桥的 IP 地址为 192.168.2.1，则电脑的 IP 地址可以设为“192.168.2.X”（X 为 2~253），子网掩码为“255.255.255.0”。



3. 在电脑上打开浏览器，访问网桥的管理 IP 地址（默认为“192.168.2.1”）。



4. 在出现的页面输入登录用户名/密码，点击 **登录**。



The image shows the login interface for CPE3V1.0. It features a header with the text 'CPE3V1.0'. Below the header, there are three input fields: the first is for the username with the label '默认用户名: admin', the second is for the password with the label '默认密码: admin', and the third is a dropdown menu for language selection, currently set to '简体中文'. At the bottom, there is a large red button labeled '登录' and a link labeled '忘记密码?'.



若未出现上述页面，请查看常见问题解答的[问2](#)。

成功登录到网桥的管理页面，您可以开始配置网桥了。



## 3.2 退出登录

登录到网桥的管理页面后，如果在 [WEB 闲置超时时间](#)内没有任何操作，系统将自动退出登录。

## 3.3 页面布局

网桥的管理页面共分为：一级导航栏、二级导航栏、页签和配置区四部分。如下图所示。



序号	名称	说明
①	一级导航栏	
②	二级导航栏	以导航树、页签的形式组织网桥的功能菜单。用户可以根据需要选择功能菜单，选择结果显示在配置区。
③	页签	
④	配置区	用户进行配置或查看配置的区域。

## 3.4 常用按钮

网桥管理页面中常用按钮的功能介绍如下表。

常用按钮	说明
	用于刷新当前页面内容。
	用于保存当前页面配置，并使配置生效。
	用于取消当前页面未保存的配置，并恢复到修改前的配置。
	点击可查看对应页面的设置帮助信息。

# 4 快速设置

通过「快速设置」模块，您可以快速设置网桥，组建无线网络。

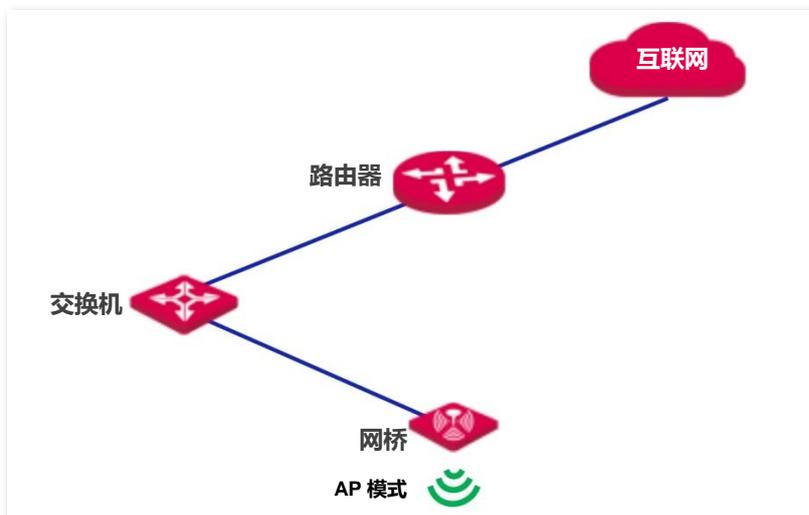
网桥支持以下工作模式：[AP 模式](#)、[客户端模式](#)、[无线 WAN 模式](#)。

## 4.1 AP 模式

### 4.1.1 概述

网桥默认工作在 AP 模式。此模式下，网桥通过网线接入互联网，将有线信号转变为无线信号。

应用拓扑图如下。



## 4.1.2 设置 AP 模式

1. 进入网桥的「快速设置」页面，选 **AP 模式**，点击 **下一步**。

快速设置 当前模式：AP模式

请选择工作模式：

- AP模式 把现有的有线网络转化为无线网络
- 客户端模式 作为无线网卡，连接到上级无线网络
- 无线WAN模式 无线连接到ISP热点，并分享网络

**下一步**

2. SSID（无线网络名称）：点击输入框，修改无线网络名称，如 zhangsan。
3. 信道：选择无线工作的信道。
4. 安全模式：选择无线网络安全模式，并设置其展开的参数（建议选择“WPA2-PSK” > “AES”）。
5. 点击 **下一步**。

快速设置 >> AP模式 当前模式：AP模式

设置本设备的无线网络名称（SSID）和无线密码（密钥），  
请记住您的无线密码

SSID（无线网络名称）

信道

安全模式

加密规则  AES  TKIP  TKIP&AES

密钥

上一步 **下一步**

6. 点击 **保存**。

快速设置 >> AP模式 当前模式：AP模式

设备已配置为AP模式，请点击“保存”激活配置

上一步 **保存**

----完成

## AP 模式的参数说明

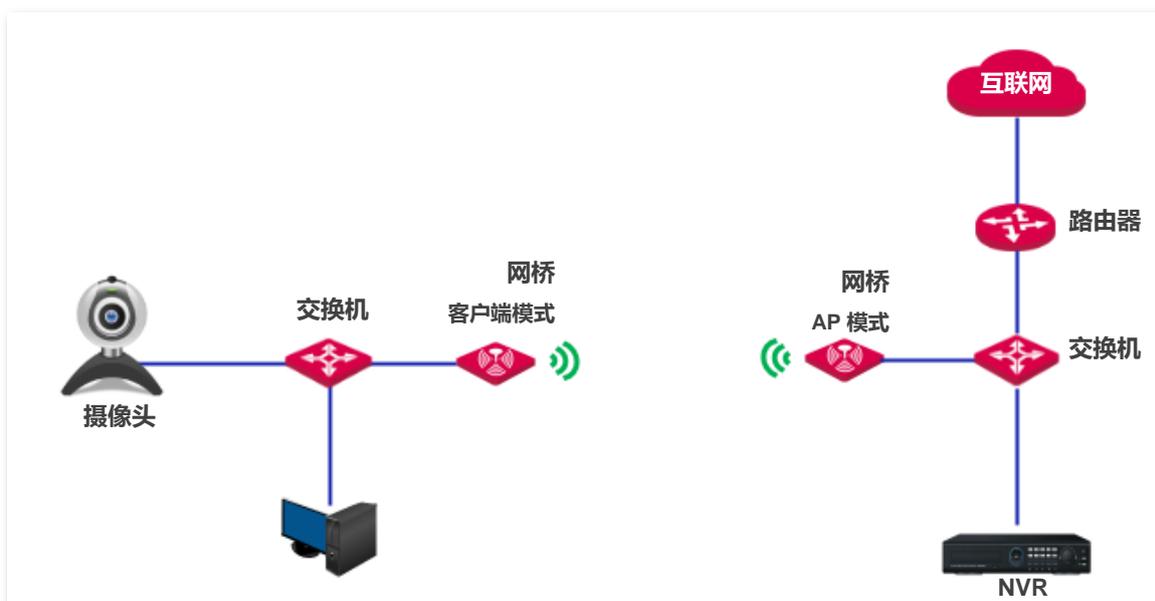
标题项	说明
工作模式	<p>选择网桥的工作模式。</p> <ul style="list-style-type: none"><li>AP 模式：把现有的有线网络转化为无线网络。</li><li>客户端模式：作为无线网卡连接其他无线网络，此时网桥不提供无线接入服务，客户端需要通过网线连接到网桥。</li><li>无线 WAN 模式：一般用于桥接宽带运营商的热点，如 CMCC、ChinaNet。也可以桥接上级无线路由器，并通过 DHCP（自动获取）、静态 IP 或 PPPoE 使网桥的 WAN 口获取 IP 地址，并连接到互联网。</li></ul>
SSID（无线网络名称）	<p>点击可修改无线网络名称。</p>
信道	<p>选择网桥的工作信道。</p> <p>尽可能选择当前区域使用比较少的信道以减少干扰。“自动”表示网桥根据周围环境情况自动调整工作信道。</p>
安全模式	<p>选择对应无线网络的安全模式。支持：<a href="#">不加密</a>、<a href="#">WPA-PSK</a>、<a href="#">WPA2-PSK</a>、<a href="#">Mixed WPA/WPA2-PSK</a>。</p> <p>点击超链接可以了解对应安全模式的详细说明。</p>

## 4.2 客户端模式

### 4.2.1 概述

客户端模式下，网桥作为无线网卡桥接上级无线信号，此时网桥不能提供无线接入服务，客户端只能有线连接网桥。一般与 AP 模式的网桥搭配使用。

应用拓扑图如下。



### 4.2.2 设置客户端模式

1. 进入网桥的「快速设置」页面。
2. 工作模式：选择**客户端模式**。
3. 点击 **下一步**。



- 在出现的无线网络列表中，选择要桥接的无线网络，如 IP-COM\_1。
- 点击 **下一步**。



如果扫描不到无线网络，请进入「无线设置」>「基本设置」页面，确认您**已开启无线**，然后重新尝试。

快速设置 >> 客户端模式 当前模式：AP模式

点击“扫描”，选择您想要连接的无线网络，  
然后点击“下一步”

扫描  [重新扫描](#)

上级AP

透明网桥

选择	SSID	信道	MAC地址	安全模式	信号强度
	IP-COM_1	11	50:2B:73:09:94:51	WPA2-PSK,AES	

- 如果上级无线网络已加密，请输入对应的**密钥**（无线密码）。
- 点击 **下一步**。

快速设置 >> 客户端模式 当前模式：AP模式

请保持信道、安全模式、加密规则与上级AP一致，  
然后输入上级AP的密钥，点击“下一步”

上级AP

上级AP的MAC地址

信道

安全模式

加密规则  AES  TKIP  TKIP&AES

密钥

- 设置本网桥的 IP 地址信息。
  - IP 地址：将本网桥 IP 地址修改为与上级设备 IP 地址不同但在同一网段，如 192.168.2.10。
  - 子网掩码：设置 IP 地址的子网掩码，如 255.255.255.0。
  - 默认网关：输入网关地址，一般为网络中已联网路由器的 LAN 口 IP 地址。
  - 首选 DNS 服务器：输入 DNS 信息。

9. 点击 **下一步**。

当前模式：AP模式

**快速设置 >> 客户端模式**

请将IP地址设置为与上级AP相同网段的不同IP

IP地址	<input type="text" value="192.168.2.10"/>
子网掩码	<input type="text" value="255.255.255.0"/>
默认网关	<input type="text"/>
首选DNS服务器	<input type="text"/>
备用DNS服务器	<input type="text" value="8.8.4.4"/>

10. 点击 **保存**。

当前模式：AP模式

**快速设置 >> 客户端模式**

设备已配置为客户端模式，请点击“保存”激活配置

----完成



提示

登录到网桥管理页面后，进入「无线设置」>「基本设置」页面，可查看网桥的 SSID 和密钥。

### 客户端模式的参数说明

标题项	说明
工作模式	<p>选择网桥的工作模式。</p> <ul style="list-style-type: none"><li>- AP 模式：把现有的有线网络转化为无线网络。</li><li>- 客户端模式：作为无线网卡连接其他无线网络，此时网桥不提供无线接入服务，客户端需要通过网线连接到网桥。</li><li>- 无线 WAN 模式：一般用于桥接宽带运营商的热点，如 CMCC、ChinaNet。也可以桥接上级无线路由器，并通过 DHCP（自动获取）、静态 IP 或 PPPoE 使网桥的 WAN 口获取 IP 地址，并连接到互联网。</li></ul>
透明网桥	启用后，网桥间可以实现双向透传，解决了 NVR 不能发现摄像头的问题。
上级 AP	要桥接的网络的无线名称（SSID）。

标题项	说明
信道	被桥接无线网络的工作信道。通过扫描选择时，会自动填充，无需手动设置。
安全模式	被桥接无线网络使用的安全模式。通过扫描选择时，会自动填充，无需手动设置。如被桥接的无线网络已加密，须手动输入其密钥。

---

## 4.3 无线 WAN 模式

### 4.3.1 概述

无线 WAN 模式下，网桥可以连接宽带运营商的热点，如 CMCC，并分享网络给客户端。应用拓扑图如下。



### 4.3.2 设置无线 WAN 模式

1. 进入网桥的「快速设置」页面。
2. 工作模式：选择**无线 WAN 模式**。
3. 点击 **下一步**。



4. 在出现的无线网络列表中，选择要桥接的无线网络，如 IP-COM\_1。
5. 点击 **下一步**。



如果扫描不到无线网络，请进入「无线设置」>「基本设置」页面，确认您**已开启无线**，然后重新尝试。



6. 如果上级无线网络已加密，请输入对应的**密钥**（无线密码）。

7. 点击 **下一步**。



8. 设置 WAN 口信息。

(1) 上网类型：选择联网方式，如“PPPoE”。

(2) PPPoE 用户名：输入运营商提供的用户名。

(3) PPPoE 密码：输入运营商提供的密码。

9. 点击 **下一步**。

当前模式：AP模式

**快速设置 >> 无线WAN模式**

请选择上网类型，并输入ISP提供的上网信息，  
然后点击“下一步”

上网类型     DHCP (自动获取)     静态IP     PPPoE

PPPoE用户名   

PPPoE密码   

10. 设置网桥的无线基本信息。

- (1) SSID (无线网络名称)：修改无线网络名称，如“zhangsan”。
- (2) 安全模式，加密规则：建议选择“WPA2-PSK > AES”。
- (3) 密钥：设置无线密码，如“87654321”。

11. 点击 **下一步**。

当前模式：AP模式

**快速设置 >> 无线WAN模式**

设置本设备的无线网络名称 (SSID) 和无线密码 (密钥)，  
请记下您的无线密码

SSID (无线网络名称)   

信道   

安全模式   

加密规则     AES     TKIP     TKIP&AES

密钥   

12. 点击 **下一步**。

当前模式：AP模式

**快速设置 >> 无线WAN模式**

请设置IP地址使其与ISP热点 (上级AP) 的IP地址在不同网段

IP地址   

子网掩码

13. 点击 **保存**。



----完成



登录到网桥的管理页面，进入「无线设置」>「基本设置」页面，可查看网桥的 SSID 和密钥。

---

## 无线 WAN 模式的参数说明

标题项	说明
工作模式	<p>选择网桥的工作模式。</p> <ul style="list-style-type: none"><li>- AP 模式：把现有的有线网络转化为无线网络。</li><li>- 客户端模式：作为无线网卡连接其他无线网络，此时网桥不提供无线接入服务，客户端需要通过网线连接到网桥。</li><li>- 无线 WAN 模式：一般用于桥接宽带运营商的热点，如 CMCC、ChinaNet。也可以桥接上级无线路由器，并通过 DHCP（自动获取）、静态 IP 或 PPPoE 使网桥的 WAN 口获取 IP 地址，并连接到互联网。</li></ul>
上级 AP	要桥接的网络的无线名称（SSID）。
信道	被桥接无线网络的工作信道。通过扫描选择时，会自动填充，无需手动设置。
安全模式	被桥接无线网络使用的安全模式。通过扫描选择时，会自动填充，无需手动设置。如被桥接的无线网络已加密，须手动输入其密钥。

# 5 系统状态

在「系统状态」模块，您可以查看网桥的系统信息及无线网络情况，包括：[系统状态](#)、[无线状态](#)、[统计](#)。

## 5.1 系统状态

进入页面：点击「系统状态」。

在这里，您可以查看网桥的系统状态和接口状态。

### 5.1.1 AP/客户端模式下系统状态

AP 模式、客户端模式下的系统状态内容如下：

系统状态			
设备名称	CPE3V1.0	LAN MAC	C8:3A:35:83:F0:60
运行时间	1天 3时 2分 52秒	WLAN MAC	C8:3A:35:83:F0:61
系统时间	2018-03-23 17:28:08	LAN口速率	100Mbps全双工
软件版本	V1.0.0.3(1930)	LAN IP	192.168.2.1
硬件版本	V1.0		

#### 参数说明

标题项	说明
设备名称	该台网桥的名称。当网络中存在多台网桥时，不同的设备名称可以帮助您区分各网桥设备。您可以在「网络设置」>「LAN 口设置」页面修改设备名称。
运行时间	网桥最近一次启动后连续运行的时长。
系统时间	网桥当前的系统时间。

标题项	说明
软件版本	网桥系统软件的版本号。
硬件版本	网桥硬件的版本号。
LAN MAC	网桥以太网口（LAN 口）的物理地址。当您用网线连接网桥和其他设备时，网桥使用本 MAC 地址和其他设备进行通信。
WLAN MAC	网桥无线接口的 MAC 地址。
LAN 口速率	网桥有线接口当前的连接速率。
LAN IP	网桥的 IP 地址，也是网桥的管理 IP 地址。 局域网用户访问此 IP 地址，可以登录到网桥的管理页面。您可以在「网络设置」>「LAN 口设置」页面修改此 IP 地址。

## 5.1.2 无线 WAN 模式下系统状态

无线 WAN 模式下的系统状态内容如下：

系统状态		当前模式：无线WAN模式	
设备名称	CPE3V1.0	LAN MAC	C8:3A:35:83:F0:60
运行时间	1分 51秒	WLAN MAC	C8:3A:35:83:F0:61
系统时间	2018-03-28 14:33:04	LAN口速率	100Mbps全双工
软件版本	V1.0.0.3(1930)	LAN IP	192.168.2.1
硬件版本	V1.0	WAN IP	192.168.0.195
连接状态	已连接	默认网关	192.168.0.252
上网类型	DHCP (自动获取)	首选DNS服务器	192.168.0.252

### 参数说明

标题项	说明
连接状态	网桥当前的网络连接状态。
上网类型	网桥当前的联网方式，本设备支持三种联网方式，如下： <ul style="list-style-type: none"><li>- DHCP（自动获取）：网桥从上级 DHCP 服务器获取 IP 地址上网。</li><li>- 静态 IP：网桥通过固定的 IP 地址、子网掩码、默认网关、DNS 服务器信息上网。</li></ul>

标题项	说明
	<ul style="list-style-type: none"><li>- PPPoE：网桥通过用户名和密码拨号上网。</li></ul>
WAN IP	网桥 WAN 口获取的 IP 地址。
默认网关	网桥的网关地址信息。客户端访问外网时，数据包必须通过网关进行转发。
首选 DNS 服务器	网桥的 DNS 服务器地址。

---

## 5.2 无线状态

进入页面：点击「系统状态」。

在这里，您可以查看网桥工作模式及无线连接状态。

无线状态			
工作模式	AP模式	上级AP的MAC地址	无上级AP
SSID	IP-COM_83F060	信号强度	N/A
安全模式	不加密	背景噪声	N/A
信道/频段	9/2452	TX/RX链路	2X2
无线客户端个数	0	发送/接收速率	N/A

### 参数说明

标题项	说明
工作模式	网桥当前的工作模式。
SSID	网桥的无线网络名称。
信道/频段	网桥当前的工作信道及频段。
无线客户端个数	当前接入到网桥无线网络的设备数量。
上级 AP 的 MAC 地址	上级设备的 MAC 地址。 网桥进行无线桥接后，显示对端设备的无线 MAC 地址。网桥工作在 AP 模式时，显示为“无上级 AP”。
信号强度	对端设备的无线信号强度。 网桥进行无线桥接后，显示对端设备的无线信号强度。网桥工作在 AP 模式时，显示第一个连接网桥 WiFi 的客户端信号强度。
背景噪声	当前环境的各种电磁干扰的信号强度，绝对值越大，干扰越小。
TX/RX 链路	当前无线数据传输空间流数量，链路数量越多，传输流量越多。本网桥为 2 收 2 发。
发送/接收	无线发送/接收速率。 AP 模式下，显示第一个连接网桥无线网络的客户端的发送速率和接收速率。 客户端、无线 WAN 模式下，显示网桥的发送速率和接收速率。

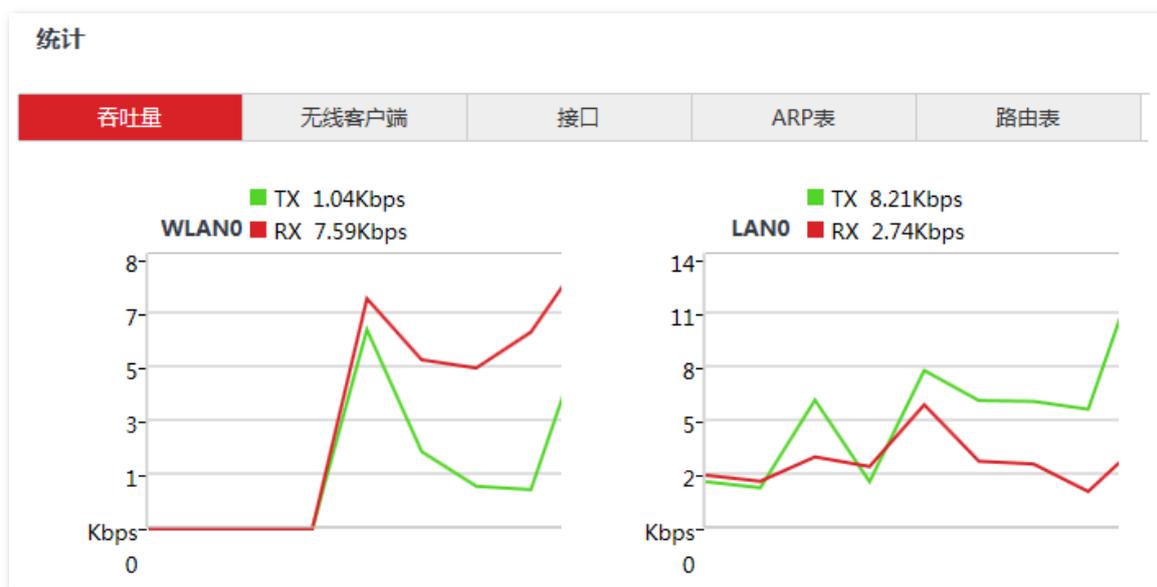
## 5.3 统计

进入页面：点击「系统状态」。

在这里，您可以查看网桥各报文统计信息，包括吞吐量、无线客户端、接口等。

### 5.3.1 吞吐量

显示无线接口和 LAN 口的吞吐量情况。



## 5.3.2 无线客户端

AP 模式有效。

统计					
吞吐量	无线客户端	接口	ARP表	路由表	
IP地址	MAC地址	信号/噪声	发送/接收速率	CCQ	连接时间
192.168.2.251	14:5F:94:BC:FC:83	-28dBm/-91d...	144.5Mbps/2..	100%	20秒

### 参数说明

标题项	说明
IP 地址	客户端的 IP 地址。
MAC 地址	客户端的 MAC 地址。
信号/噪声	客户端的无线信号强度/客户端当前环境的各种电磁干扰的信号强度。
发送/接收速率	客户端当前的发送/接收速率。
CCQ	客户端链接质量，百分比越高，网络传输质量越好。
连接时间	客户端接入网桥无线网络的时长。

## 5.3.3 上级 AP

客户端模式、无线 WAN 模式有效。可以查看上级设备的基本信息。

统计					
吞吐量	上级AP	接口	ARP表	路由表	
IP地址	MAC地址	信号/噪声	发送/接收速率	CCQ	连接时间
192.168.0.252	C8:3A:35:18:68:41	-11dBm/-91d...	144.5Mbps/1..	100%	2分 22秒

## 参数说明

标题项	说明
IP 地址	上级设备的 IP 地址。
MAC 地址	上级设备的 MAC 地址。
信号/噪声	上级设备的无线信号强度/上级设备当前环境的各种电磁干扰的信号强度。
发送/接收速率	上级设备当前的发送/接收速率。
CCQ	与上级设备的连接质量，百分比越高，网络传输质量越好。
连接时间	成功桥接上级设备的时长。

## 5.3.4 接口

显示网桥接口的 IP 地址、MAC 地址和数据流量信息。

统计						
吞吐量	无线客户端	接口	ARP表	路由表		
接口	IP地址	MAC地址	接收数据包	接收错误	发送数据包	发送错误
eth0	0.0.0.0	C8:3A:35:83:...	67566	0	92402	0
Bridge	192.168.2.1	C8:3A:35:83:...	18721	0	91781	0

## 参数说明

标题项	说明
接口	显示网桥的接口。
IP 地址	网桥接口的 IP 地址。
MAC 地址	网桥接口的 MAC 地址。
接收数据包	接口接收/发送的数据包情况。
发送数据包	
接收错误	接口接收/发送错误数据包的情况。
发送错误	

## 5.3.5 ARP 表

显示网桥当前的 ARP 表。

统计				
吞吐量	无线客户端	接口	ARP表	路由表
IP地址	MAC地址	接口		
192.168.2.23	c8:3a:35:12:12:12	Bridge		

### 参数说明

标题项	说明
IP 地址	APR 表中主机的 IP 地址。
MAC 地址	主机 IP 地址对应的 MAC 地址。
接口	用于和主机通信的接口。

## 5.3.6 路由表

显示网桥当前可达的目标网络。

统计				
吞吐量	无线客户端	接口	ARP表	路由表
目标网络	子网掩码	下一跳	接口	
0.0.0.0	0.0.0.0	192.168.2.254	Bridge	
192.168.2.0	255.255.255.0	0.0.0.0	Bridge	

### 参数说明

标题项	说明
目标网络	目的网络地址，即数据包到达的 IP 地址。

标题项	说明
子网掩码	目的网络地址的子网掩码。
下一跳	数据包从网桥的接口出去后，下一跳路由的入口 IP 地址。
接口	数据从网桥出去的接口。

# 6 网络设置

## 6.1 LAN 口设置

### 6.1.1 概述

进入页面：点击「网络设置」。在这里，您可以查看网桥的 LAN 口 MAC 地址，设置网桥的名称、IP 获取方式及相关信息。

当前模式：AP模式

### LAN口设置

MAC地址 C8:3A:35:83:F0:60

IP获取方式

IP地址

子网掩码

默认网关

首选DNS服务器

备用DNS服务器

设备名称

#### 参数说明

标题项	说明
MAC 地址	网桥的 LAN 口 MAC 地址。 网桥的 SSID 默认为 IP-COM_XXXXXX，其中，XXXXXX 为此 MAC 后六位。
IP 获取方式	网桥获取 IP 地址的方式。默认为“静态 IP”。 <ul style="list-style-type: none"><li>静态 IP：手动指定网桥的 IP 地址、子网掩码、网关地址、DNS 服务器。</li><li>DHCP（自动获取）：网桥从网络中的 DHCP 服务器自动获取其 IP 地址、子网掩码、网关地址、DNS 服务器。</li></ul>

标题项	说明
	 <b>提示</b> 设置 IP 获取方式为“DHCP（自动获取）”后，下次登录网桥的管理页面前，您必须到网络中的 DHCP 服务器的客户端列表中查看网桥获得的 IP 地址，再用该 IP 地址进行登录。
IP 地址	网桥的 IP 地址，也是网桥的管理 IP 地址，局域网用户可使用该 IP 地址登录到网桥的管理页面。默认为“192.168.2.1”。 如果要让网桥联网，一般要设置此 IP 地址，使其与出口路由器的 LAN 口 IP 地址在同一网段。
子网掩码	网桥 IP 地址的子网掩码，默认为“255.255.255.0”。
默认网关	网桥的默认网关。 如果要让网桥联网，一般要设置网关地址为出口路由器的 LAN 口 IP 地址。
首选 DNS 服务器	网桥的首选 DNS 服务器地址。 若出口路由器有 DNS 代理功能，此地址可以是出口路由器的 LAN 口 IP 地址。若出口路由器无 DNS 代理功能，请填入正确的 DNS 服务器的 IP 地址。
备用 DNS 服务器	网桥的备用 DNS 服务器地址，该选项可选填。 若有两个 DNS 服务器 IP 地址，可将另一个 IP 地址填在此处。
设备名称	该台网桥的名称，默认为网桥的产品型号+版本号。 建议修改设备名称为该台网桥的安装位置描述，方便在管理多台网桥时，通过设备名称快速定位各网桥设备。

## 6.1.2 修改 LAN IP

### 手动设置 IP

由网络管理员手动指定网桥的 IP 地址、子网掩码、默认网关、首选/备用 DNS 服务器，适用于网络中只需部署一台或几台网桥的场合。

#### 设置步骤：

1. 进入「网络设置」>「LAN 口设置」页面。
2. IP 获取方式：选择“静态 IP”。
3. 设置 IP 地址、子网掩码、默认网关、首选/备用 DNS 服务器（一般仅需修改“IP 地址”、“默认网关”、“首选 DNS 服务器”）。
4. 点击 **保存**。

当前模式：AP模式

### LAN口设置

MAC地址 C8:3A:35:83:F0:60

\* IP获取方式 静态IP

\* IP地址 192.168.2.10

子网掩码 255.255.255.0

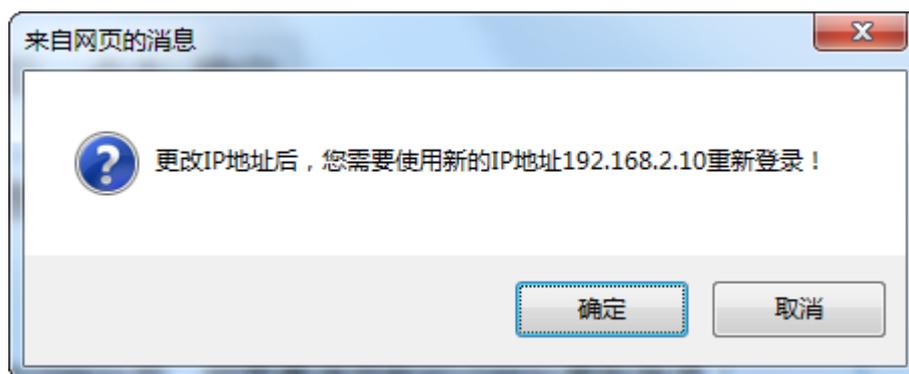
\* 默认网关 192.168.2.254

\* 首选DNS服务器 8.8.8.8

备用DNS服务器 8.8.4.4

设备名称 CPE3V1.0

5. 确认提示信息后，点击 。



#### ---完成

如果您还要继续设置网桥，请参考以下说明进行操作：

- 如果修改的 IP 地址与原 IP 地址在同一网段，稍等片刻，将会自动跳转到登录页面。
- 如果修改的 IP 地址与原 IP 地址**不在**同一网段，请先更改[管理电脑](#)的 IP 地址，使其与网桥新的 IP 地址在相同网段，然后再使用新的 IP 地址重新登录网桥的管理页面。

## 自动获取 IP

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

设置步骤：

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



The screenshot shows the 'LAN口设置' (LAN Port Settings) configuration page. The interface includes a title bar with 'LAN口设置' and '当前模式：AP模式'. A red question mark icon is in the top right corner. The configuration fields are as follows:

MAC地址	C8:3A:35:83:F0:60
* IP获取方式	DHCP (自动获取)
IP地址	192.168.2.10
子网掩码	255.255.255.0
默认网关	192.168.2.254
首选DNS服务器	8.8.8.8
备用DNS服务器	8.8.4.4
设备名称	CPE3V1.0

At the bottom, there are two buttons: a red '保存' (Save) button and a grey '取消' (Cancel) button.

----完成

如果需要重新登录网桥的管理页面，请先到 DHCP 服务器的客户端列表中查看网桥的 IP 地址，再修改[管理电脑](#)的 IP 地址 使其和网桥新的 IP 地址在相同网段 之后访问网桥新的 IP 地址进行登录。

## 6.2 MAC 克隆 (仅无线 WAN 模式有效)

### 6.2.1 概述

当上网设置完毕后，如果网桥还是无法联网，有可能是 ISP 将上网账号信息与某一 MAC 地址（物理地址）绑定了。此时，您可以尝试通过 MAC 地址克隆解决该问题。



请克隆之前能正常上网的电脑 MAC 地址或能正常上网的路由器的 WAN 口 MAC 地址。

MAC克隆

MAC地址 C8 : 3A : 35 : 83 : F0 : 61

克隆本地MAC 恢复默认MAC

保存 取消

### 6.2.2 克隆 MAC 地址

方法 1：

1. 使用之前能正常上网的电脑连接网桥。
2. 登录网桥管理页面，进入「网络设置」>「MAC 克隆」页面。
3. 点击 **克隆本地 MAC**。
4. 点击 **保存**。

MAC克隆

MAC地址 C8 : 3A : 35 : 12 : 12 : 12

克隆本地MAC 恢复默认MAC

保存 取消

----完成

稍后，进入「系统状态」页面，网桥的 WLAN MAC 地址变得和之前能上网的电脑的 MAC 地址一样，MAC 地址克隆成功。

系统状态			
设备名称	CPE3V1.0	LAN MAC	C8:3A:35:83:F0:60
运行时间	6分 36秒	WLAN MAC	C8:3A:35:12:12:12
系统时间	2018-03-28 14:43:44	LAN口速率	100Mbps全双工
软件版本	V1.0.0.3(1930)	LAN IP	192.168.2.1
硬件版本	V1.0	WAN IP	192.168.0.179
连接状态	已连接	默认网关	192.168.0.252
上网类型	DHCP (自动获取)	首选DNS服务器	192.168.0.252

## 方法 2：

1. 记录正确的 MAC 地址。
2. 登录网桥管理页面，进入「网络设置」>「MAC 克隆」页面，
3. 在 MAC 地址后的输入框里填入正确的 MAC 地址。
4. 点击 **保存**。

### MAC克隆

MAC地址

----完成



如果需要将 MAC 地址恢复为出厂 MAC，请点击「网络设置」>「MAC 克隆」，点击 **恢复默认 MAC**，点击 **保存**。

## 6.3 DHCP 服务器

### 6.3.1 概述

本网桥提供了 DHCP 服务器，可以为局域网中的计算机自动分配 IP 地址信息。默认情况下，网桥启用了 DHCP 服务器功能。



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

### 6.3.2 配置 DHCP 服务器

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

当前模式：AP模式

#### DHCP服务器

DHCP服务器  启用

起始IP地址

结束IP地址

子网掩码

\* 网关地址

\* 首选DNS服务器

备用DNS服务器

租约时间

**保存** 取消

----完成



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

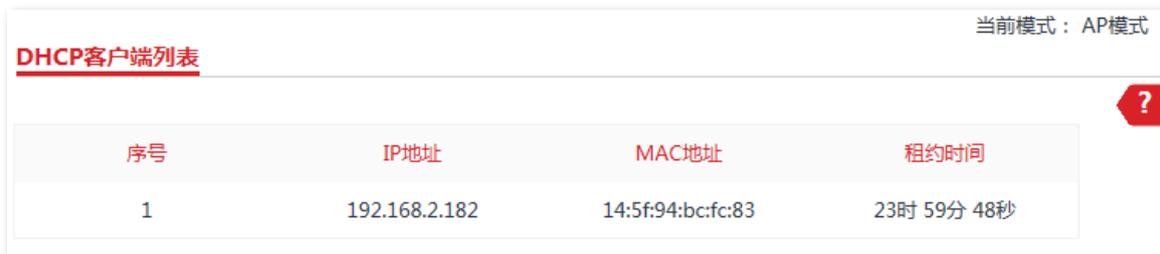
## 参数说明

标题项	说明
DHCP 服务器	启用/禁用网桥的 DHCP 服务器功能。默认禁用。
起始 IP 地址	DHCP 地址池(即 DHCP 服务器可分配的 IP 地址范围)的开始 IP 地址。默认为 192.168.2.100。 DHCP 地址池的结束 IP 地址。默认为 192.168.2.200。
结束 IP 地址	 起始 IP 地址和结束 IP 地址必须与网桥的 IP 地址在同一网段。
子网掩码	DHCP 服务器分配给客户端的子网掩码，默认为 255.255.255.0。
网关地址	 DHCP 服务器分配给客户端的默认网关 IP 地址，一般为网络中路由器的 LAN 口 IP 地址。默认为 192.168.2.254。 客户端访问本网段以外的服务器或主机时，数据必须通过网关进行转发。
首选 DNS 服务器	 DHCP 服务器分配给客户端的首选 DNS 服务器 IP 地址。默认为 8.8.8.8。 为了使局域网计算机能够正常上网，请务必确保首选 DNS 是正确的 DNS 服务器或 DNS 代理的 IP 地址。
备用 DNS 服务器	DHCP 服务器分配给客户端的备用 DNS 服务器地址。此项可不填，表示 DHCP 服务器不分配此项。
租约时间	DHCP 服务器所分配给客户端的 IP 地址的有效时间。 当租约到达一半时，客户端会向 DHCP 服务器发送一个 DHCP Request，请求更新自己的租约。如果续约成功，则在续约申请的时间基础上续租；如果续约失败，则到了租期的 7/8 时，再重复一次续约过程。如果成功，则在续约申请的时间基础上续租，如果仍然失败，则租约到期后，客户端需要重新申请 IP 地址信息。 如无特殊需要，建议保持默认设置“1 天”。

## 6.4 DHCP 客户端列表

启用网桥的 DHCP 服务器后，通过 DHCP 客户端列表，您可以查看局域网中从本 DHCP 服务器获取 IP 地址的计算机的 IP 地址、MAC 地址、剩余租约时间。

进入页面：点击「网络设置」>「DHCP 客户端列表」。



序号	IP地址	MAC地址	租约时间
1	192.168.2.182	14:5f:94:bc:fc:83	23时 59分 48秒

## 6.5 VLAN 设置

### 6.5.1 概述

网桥支持 IEEE 802.1Q VLAN，可以在划分了 QVLAN 的网络环境使用。默认情况下，网桥关闭了 QVLAN 功能。

### 6.5.2 配置 VLAN

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



VLAN设置  启用

管理VLAN

WLAN

**保存**

----完成

## 参数说明

标题项	说明
VLAN 设置	启用/禁用网桥的 802.1Q VLAN 功能。默认禁用。启用 VLAN 后，网桥的 PoE/LAN 口为 Trunk 口。
管理 VLAN	网桥的管理 VLAN ID。默认为“1”。 更改管理 VLAN 后，管理电脑需要重新连接到新的管理 VLAN，才能管理网桥。
WLAN	设置无线接口的 VLAN ID，默认均为 1000，设置范围为 1~4094。 启用 VLAN 后，SSID 所在的无线接口相当于一个 Access 口，其 PVID 与 VLAN ID 相同。

配置了 802.1Q VLAN 后，对于进入端口的 Tag 数据，按数据中的 VID 转发到相应 VLAN 的其他端口；对于进入端口的 Untag 数据，按该端口的 PVID 转发到相应 VLAN 的其他端口。

各链路类型端口对数据的接收和发送处理方式详见下表：

端口链路类型	接收数据处理		发送数据处理
	接收 Tag 数据	接收 Untag 数据	
Access			去掉报文的 Tag 再发送。
Trunk	按 Tag 中的 VID 转发到相应 VLAN 的其他端口。	按该端口的 PVID 转发到相应 VLAN 的其他端口。	VID = 端口 PVID，去掉 Tag 发送。 VID ≠ 端口 PVID，保留 Tag 发送。

## 6.5.3 VLAN 设置举例

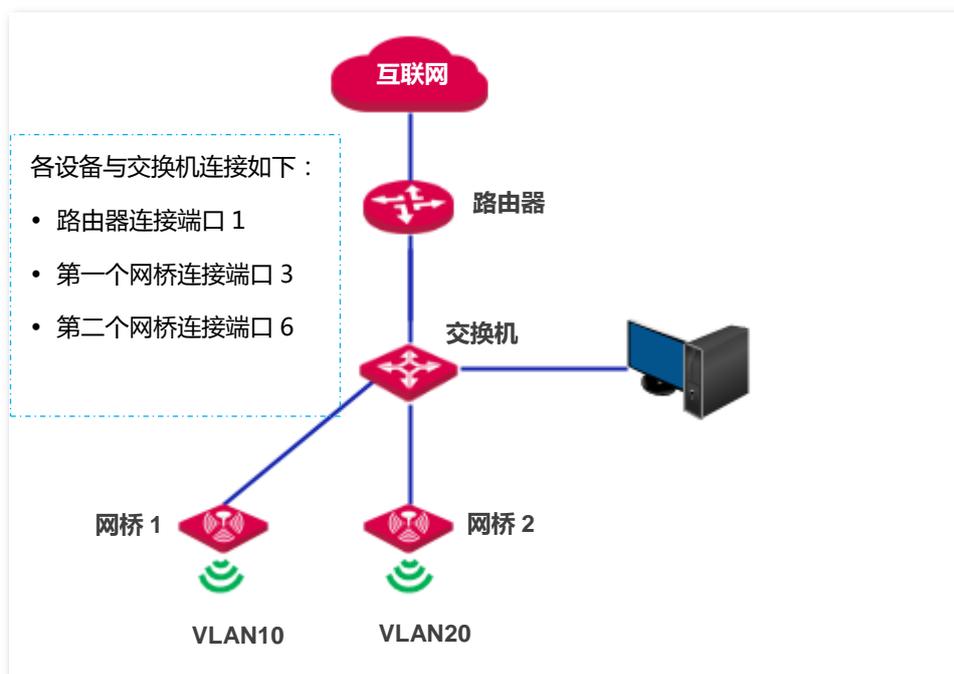
### 组网需求

要求网络中接在交换机下的网桥工作在不同的 VLAN，确保网桥互不干扰。

### 组网假设

设置 VLAN 功能，假设第一个网桥工作在 VLAN10，第二个网桥工作在 VLAN20。

## 网络拓扑



## 配置步骤

### 一、配置网桥（下文以第一个网桥为例，第二个网桥类似）

1. 登录网桥的管理页面，转到「网络设置」>「VLAN 设置」页面。
2. VLAN 设置：勾选复选框。
3. 管理 VLAN：设置管理 VLAN，默认为 1，建议保持默认设置。
4. WLAN：设置无线接口 VLAN ID，本例为 10。
5. 点击 **保存**。

The screenshot shows the 'VLAN设置' (VLAN Settings) configuration page. The current mode is 'AP模式' (AP Mode). The 'VLAN设置' (VLAN Settings) section has a checked '启用' (Enable) checkbox. The '管理VLAN' (Management VLAN) field is set to 1, and the 'WLAN' field is set to 10. There are '保存' (Save) and '取消' (Cancel) buttons at the bottom.

6. 在弹出的窗口点击 **确定**。等待网桥自动重启完成即可。

## 二、配置交换机

在交换机上划分 IEEE 802.1Q VLAN，具体如下。

交换机端口	VLAN ID (允许通过的 VLAN)	端口属性	PVID
端口 1 (连接路由器)	1,10,20	Trunk	1
端口 3 (连接第一个网桥)	1,10	Trunk	1
端口 6 (连接第二个网桥)	1,20	Trunk	1

其他未提到的端口保持默认设置即可。具体配置方法请参考交换机的使用说明书。

## 验证配置

客户端连接网桥的无线信号，即可访问互联网。且连接不同网桥的客户端相互隔离。

# 7 无线设置

## 7.1 基本设置

### 7.1.1 概述

网桥的「基本设置」模块用于配置网桥的 SSID 相关参数。

#### SSID 广播

启用 SSID 广播后，周边的无线设备可以扫描到对应 SSID。禁用 SSID 广播后，网桥不广播该 SSID，周边的无线设备不能扫描到对应 SSID，此时，如果要连接到该 SSID 的无线网络，用户必须手动在无线设备上输入该 SSID，这在一定程度上增强了无线网络的安全性。

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

#### 客户端隔离

类似于有线网络的 VLAN，将连接到同一 SSID 的所有无线用户完全隔离，使其只能访问网桥连接的有线网络。适用于酒店、机场等公共热点的架设，让接入的无线用户保持隔离，提高网络安全性。

#### 最大客户端数量

最大客户端数量参数用于限制接入 SSID 对应无线网络的用户数量，当连上该 SSID 的无线用户数达到此值后，该 SSID 不再接受新的无线连接请求。

设置最大客户端数量可以避免网桥 SSID 负载过大导致用户体验不佳。

## 安全模式

无线网络采用具有空中开放特性的无线电波作为数据传输介质，在没有采取必要措施的情况下，任何用户均可接入无线网络、使用网络资源或者窥探未经保护的数据。因此，在 WLAN 应用中必须对传输链路采取适当的加密保护手段，以确保通信安全。

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

### ■ 不加密

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

### ■ WEP

WEP(有线等效加密)使用一个静态的密钥来加密所有通信，只能提供和有线 LAN 同级的安全性。WEP 加密容易被破解，且无线速率最大只能达到 54Mbps，不建议用户使用此加密方式。

### ■ WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK

Mixed WPA/WPA2-PSK 表示网桥同时兼容 WPA-PSK、WPA2-PSK。

上述 3 种安全模式都采用预共享密钥认证，其设置的密钥只用来验证身份，数据加密密钥由网桥自动生成，解决了 WEP 静态密钥的漏洞，适合一般家庭用户用于保证无线安全。但由于其用户认证和加密的共享密码(原始密钥)为人为设定，且所有接入同一网桥的无线用户的密钥完全相同，因此，其密钥难以管理并容易泄漏，不适合在安全要求非常严格的场合应用。

### ■ WPA、WPA2

为了改善 PSK 安全模式在密钥管理方面的不足，Wi-Fi 联盟提供了 WPA 企业版本(即 WPA、WPA2)，它使用 802.1x 来进行用户认证并生成用于加密数据的根密钥，而不再使用手工设定的预共享密钥，但加密过程则没有区别。

由于采用了 802.1x 进行用户身份认证，每个用户的登录信息都由其自身进行管理，有效减少信息泄漏的可能性。并且用户每次接入无线网络时的数据加密密钥都是通过 RADIUS 服务器动态分配的，攻击者难以获取加密密钥。因此，WPA、WPA2 极大地提高了网络的安全性，并成为高安全无线网络的首选接入方式。

## 7.1.2 修改基本设置

如果要修改 SSID 的相关设置，请按如下步骤操作：

1. 进入「无线设置」>「基本设置」页面。
2. 根据需要修改各参数（一般只需修改“SSID”、“信道”以及“安全模式”相关设置）。
3. 点击 **保存**。

当前模式：AP模式

### 基本设置

开启无线

国家或地区

\* SSID

SSID广播  启用  禁用

网络模式

\* 信道

发射功率 8dBm

信道带宽  20MHz  40MHz  自动

传输速率

\* 安全模式

客户端隔离  启用  禁用

最大客户端数量  (范围：1~128)

**保存**

----完成

### 参数说明

标题项	说明
开启无线	启用/禁用网桥的无线功能。
国家或地区	选择网桥当前所在的国家或地区，以适应不同国家（或地区）对信道的管制要求。默认为“中国”。
SSID	点击此栏，可修改网桥的无线网络名称。SSID 支持中文字符（汉字）。
SSID 广播	SSID 的广播状态。 <ul style="list-style-type: none"><li>- 启用：网桥广播该 SSID，周边无线设备可以扫描到该 SSID。</li><li>- 禁用：网桥不广播该 SSID，无线设备连接网桥的 WiFi 时，需要正确输入该 SSID。</li></ul>

标题项	说明
	 <b>提示</b> 网桥支持“自动隐藏 SSID”。即，如果当前接入 SSID 的无线设备数量达到了设置的最大客户端数量，网桥将不广播 SSID。
网络模式	选择无线网络模式。 <ul style="list-style-type: none"><li>- 11b：此模式下，仅允许 802.11b 无线设备接入网桥的无线网络。</li><li>- 11g：此模式下，仅允许 802.11g 无线设备接入网桥的无线网络。</li><li>- 11b/g：此模式下，允许 802.11b、802.11g 无线设备接入网桥的无线网络。</li><li>- 11b/g/n：此模式下，允许 802.11b、802.11g 以及工作在 2.4 GHz 的 802.11n 无线设备接入网桥的无线网络。</li></ul>
信道	选择网桥的工作信道。“自动”表示网桥根据周围环境情况自动调整工作信道。
发射功率	设置网桥的无线发射功率。 发射功率越大，无线覆盖范围更广。但适当的减少发射功率更有助于提高无线网络的性能和安全性。
信道带宽	网桥工作在 11b/g/n 模式可以设置，用于选择无线信道带宽。 <ul style="list-style-type: none"><li>- 20MHz：限制网桥只能使用 20MHz 的信道带宽。</li><li>- 40MHz：限制网桥只能使用 40MHz 的信道带宽。</li><li>- 自动：网桥根据周围环境，自动调整其信道带宽为 20MHz 或 40MHz。</li></ul>
扩展信道	信道带宽为“40MHz”或“自动”的情况下可以设置，用于确定网桥工作的频率段。
传输速率	网桥的无线传输速率，可以设置 MCS0-MCS15 之间的无线速率，建议选择“自动”，此时速率传输情况如下： <ul style="list-style-type: none"><li>- “信道带宽”选择 20MHZ 时，速率会自动降低，最大速率只能为 144Mbps。</li><li>- “信道带宽”选择 40MHZ 时，最大速率能达到 300Mbps。</li><li>- “信道带宽”选择自动时，最大速率能达到 300Mbps。</li></ul>
安全模式	SSID 的安全模式。网桥支持的安全模式有： <a href="#">不加密</a> 、 <a href="#">WEP</a> 、 <a href="#">WPA-PSK</a> 、 <a href="#">WPA2-PSK</a> 、 <a href="#">Mixed WPA/WPA2-PSK</a> 、 <a href="#">WPA</a> 、 <a href="#">WPA2</a> 。点击超链接可以了解对应安全模式的详细说明。
客户端隔离	<ul style="list-style-type: none"><li>- 启用：连接在该 SSID 下的设备之间不能互相通信，可增强无线网络的安全性。</li><li>- 禁用：连接在该 SSID 下的设备之间能互相通信。默认为“禁用”。</li></ul>
最大客户端数量	SSID 最多允许接入的无线设备数量。 若接入该 SSID 的无线设备达到此值，除非某些设备断开连接，否则新的无线设备不能接入此 SSID。

## ■ 不加密

表示允许任意无线客户端接入。为了保障网络安全，不建议选择此项。

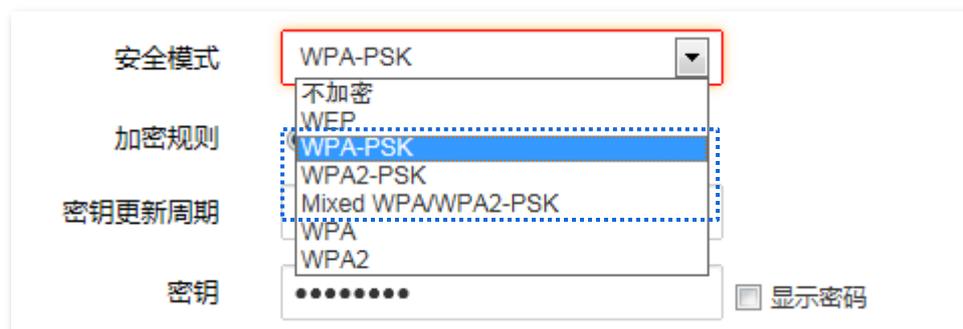
## ■ WEP

安全模式	WEP	▼
认证类型	Open	▼
默认密钥	密钥 1	▼
密钥 1	12345	ASCII ▼
密钥 2	12345	ASCII ▼
密钥 3	12345	ASCII ▼
密钥 4	12345	ASCII ▼

### 参数说明

标题项	说明
	WEP 加密时使用的认证方式 :Open、Shared 或 802.1x。三者加密过程完全一致,认证方式不同。 <ul style="list-style-type: none"><li>- Open :采用“空认证+WEP 加密”。无线设备无需经过认证,即可与 SSID 进行关联,只对传输数据进行 WEP 加密。</li></ul>
认证类型	<ul style="list-style-type: none"><li>- Shared :采用“共享密钥认证+WEP 加密”。无线设备与 SSID 进行关联时,需提供在网桥上指定的 WEP 密钥,只有在双方 WEP 密钥一致的情况下,才能关联成功。</li><li>- 802.1x :采用“802.1x 身份认证+WEP 加密”。802.1x 协议仅仅关注端口的打开与关闭,合法用户接入时,打开端口;非法用户接入或没有用户接入时,端口处于关闭状态。</li></ul>
默认密钥	Open 或 Shared 认证时,用于指定 SSID 当前使用的 WEP 密钥。 如:默认密钥为“密钥 2”,则无线设备需要使用“密钥 2”设置的无线密码连接对应 SSID。
密钥 1/2/3/4	输入 WEP 密钥。可以同时输入 4 个,但是只有“默认密钥”指定的密钥生效。
ASCII	Open 或 Shared 认证时,可选择的密钥字符类型之一。此时,密钥可以输入 5 或 13 个 ASCII 码字符。
Hex	Open 或 Shared 认证时,可选择的密钥字符类型之一。 此时,密钥可以输入 10 或 26 位十六进制数(0-9, a-f, A-F)。
RADIUS 服务器	802.1x 认证时设置。
RADIUS 端口	用于输入 RADIUS 服务器的 IP 地址/认证端口/共享密钥。
RADIUS 密码	

## ■ WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK



### 参数说明

标题项	说明
安全模式	<p>选择安全模式。</p> <ul style="list-style-type: none"><li>- WPA-PSK：此时，SSID 对应的无线网络采用 WPA-PSK 安全模式。</li><li>- WPA2-PSK：此时，SSID 对应的无线网络采用 WPA2-PSK 安全模式。</li><li>- Mixed WPA/WPA2-PSK：兼容 WPA-PSK 和 WPA2-PSK，此时，无线设备使用 WPA-PSK 和 WPA2-PSK 均可连接 SSID。</li></ul>
加密规则	<p>WPA 加密规则，WPA-PSK 只可选择“AES”或“TKIP”；WPA2-PSK 和 Mixed WPA/WPA2-PSK 还可选择“TKIP&amp;AES”。</p> <ul style="list-style-type: none"><li>- AES：高级加密标准。</li><li>- TKIP：临时密钥完整性协议。相较于 AES，采用 TKIP 时，网桥只能使用较低的无线速率（最大 54Mbps）。</li><li>- TKIP&amp;AES：兼容 TKIP 和 AES，无线客户端使用 TKIP 和 AES 均可连接。</li></ul>
密钥	WPA 预共享密钥。
密钥更新周期	WPA 数据加密密钥自动更新周期，较短的密钥更新周期可增强 WPA 数据安全性。 为 0 表示不更新。

## ■ WPA、WPA2

安全模式: WPA

RADIUS服务器: [ ]

RADIUS端口: [ ]

RADIUS密码: [ ]  显示密码

加密规则:  AES  TKIP  TKIP&AES

密钥更新周期: 0

### 参数说明

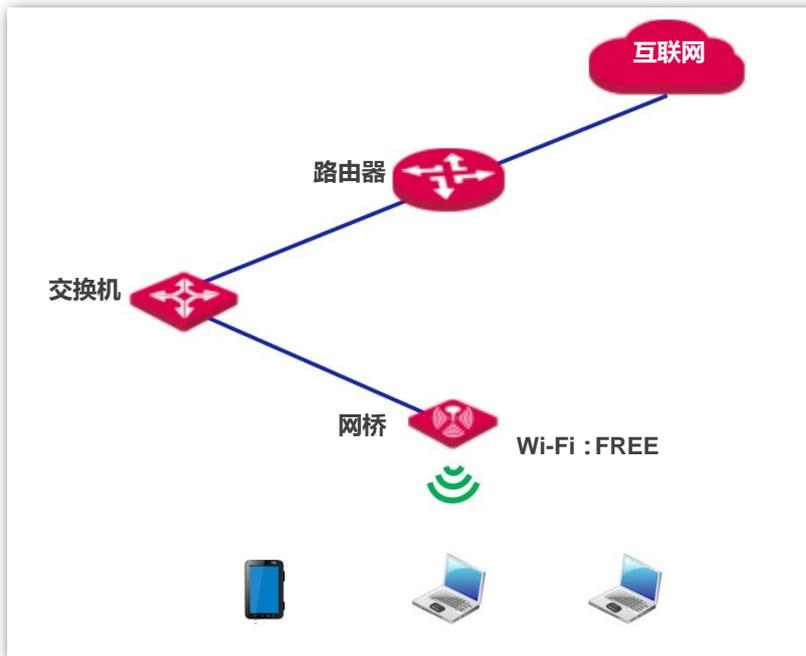
标题项	说明
安全模式	选择安全模式。 <ul style="list-style-type: none"><li>- WPA：此时，SSID 对应的无线网络采用 WPA 安全模式。</li><li>- WPA2：此时，SSID 对应的无线网络采用 WPA2 安全模式。</li></ul>
RADIUS 服务器	
RADIUS 端口	用于输入 RADIUS 服务器的 IP 地址/认证端口/共享密钥。
RADIUS 密码	
加密规则	选择 WPA 加密规则。 <ul style="list-style-type: none"><li>- AES：高级加密标准。</li><li>- TKIP：临时密钥完整性协议。</li><li>- TKIP&amp;AES：兼容 TKIP 和 AES，无线客户端使用 TKIP 和 AES 均可连接。</li></ul>
密钥更新周期	WPA 数据加密密钥自动更新周期，较短的密钥更新周期可增强 WPA 数据安全性。 为 0 表示不更新。

## 7.1.3 基本设置举例

### 不加密无线网络配置举例

#### 组网需求

某小区进行无线组网，要求：用户连接 WiFi 即可上网，不需要无线密码。



#### 配置步骤

1. 进入「无线设置」>「基本设置」页面。
2. SSID：修改为“FREE”。
3. 安全模式：选择“不加密”。
4. 点击 **保存**。

当前模式：AP模式

**基本设置**

开启无线

国家或地区

\* SSID

SSID广播  启用  禁用

网络模式

信道

发射功率 8dBm

信道带宽  20MHz  40MHz  自动

传输速率

\* 安全模式

客户端隔离  启用  禁用

最大客户端数量  (范围：1~128)

----完成

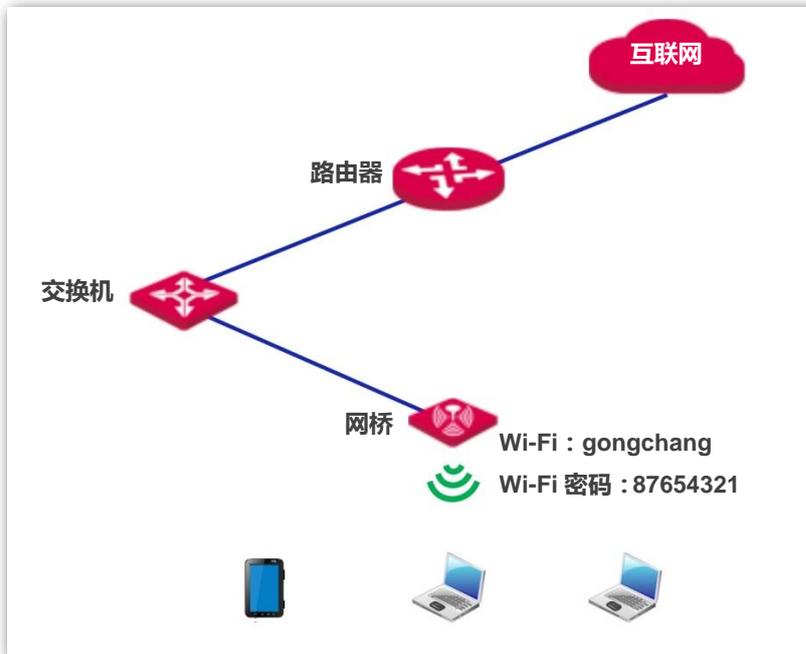
## 验证配置

无线设备连接无线网络“FREE”，不需要输入无线密码就可以连接成功。

## WPA 个人加密无线网络配置举例

### 组网需求

厂区的无线网络，要求有一定安全性，且配置简单。针对上述需求，建议采用 PSK 安全模式。



### 配置步骤

1. 进入「无线设置」>「SSID 设置」页面。
2. SSID：修改为“gongchang”。
3. 安全模式：建议选择“WPA2-PSK”>“AES”。
4. 密钥：修改为“87654321”。
5. 点击 **保存**。

当前模式：AP模式

### 基本设置

开启无线

国家或地区

\* SSID

SSID广播  启用  禁用

网络模式

信道

发射功率 8dBm

信道带宽  20MHz  40MHz  自动

传输速率

\* 安全模式

\* 加密规则  AES  TKIP  TKIP&AES

密钥更新周期

\* 密钥   显示密码

客户端隔离  启用  禁用

最大客户端数量  (范围：1~128)

----完成

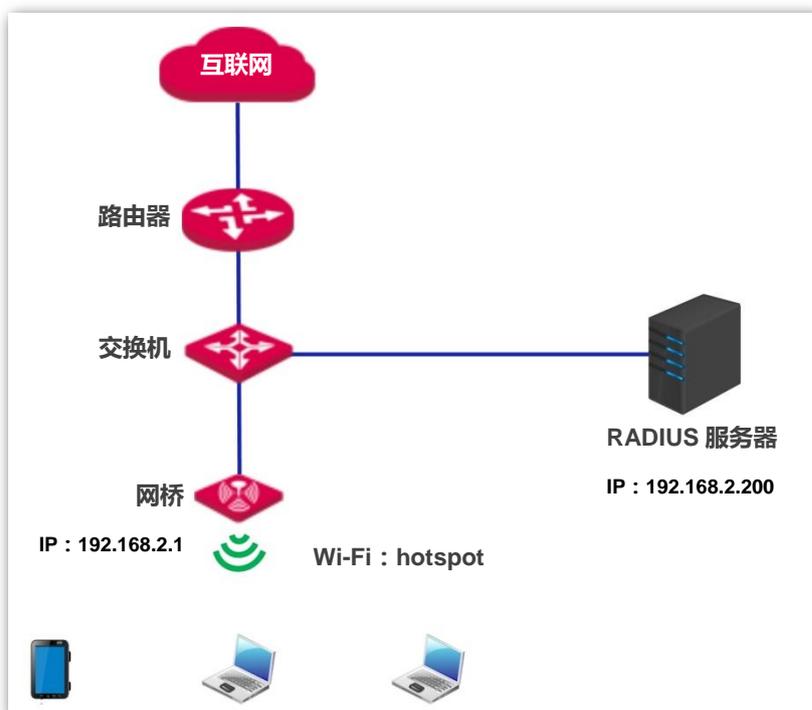
## 验证配置

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

## WPA 企业加密无线网络配置举例

### 组网需求

要求无线网络具有极高的安全性，且网络中已架设专用的 RADIUS 服务器。针对上述需求，建议采用 WPA 或 WPA2 安全模式。



### 配置步骤

#### 一、配置网桥

假设 RADIUS 服务器 IP 地址为 192.168.2.200，认证密钥为 12345678，认证端口为 1812。

1. 进入「无线设置」>「SSID 设置」页面。
2. SSID：修改，如“hotspot”。
3. 安全模式：建议选择“WPA2”。
4. RADIUS 服务器/端口/密码：分别输入“192.168.2.200”、“1812”、“12345678”。
5. 加密规则：建议选择“AES”。
6. 点击 **保存**。

当前模式：AP模式

### 基本设置

开启无线

国家或地区

SSID

\* SSID广播  启用  禁用

网络模式

信道

发射功率 8dBm

信道带宽  20MHz  40MHz  自动

传输速率

安全模式

\* RADIUS服务器

\* RADIUS端口

\* RADIUS密码   显示密码

\* 加密规则  AES  TKIP  TKIP&AES

\* 密钥更新周期

## 二、配置 RADIUS 服务器



提示

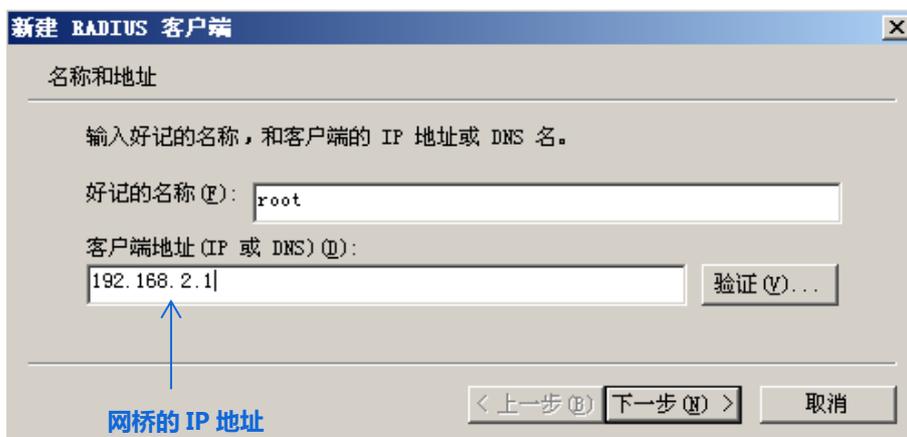
以 Windows 2003 服务器上的 RADIUS 服务器为例说明。

### 1. 配置 RADIUS 客户端。

- (1) 在 Windows 2003 服务器操作系统的管理工具，双击“Internet 验证服务”，右键单击“RADIUS 客户端”，选择“新建 RADIUS 客户端”。



(2) 设置 RADIUS 客户端名称( 可以是网桥的设备名称 ),输入网桥的 IP 地址 ,点击 **下一步** 。

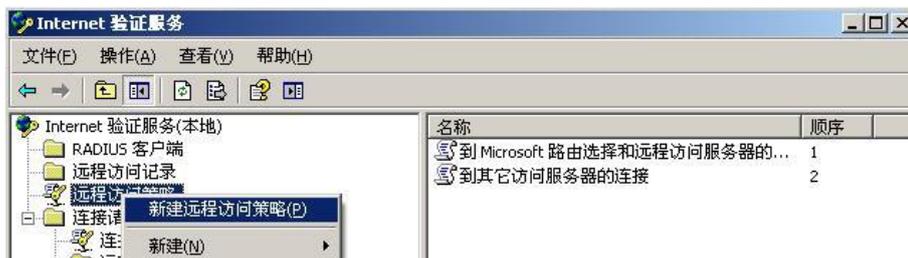


(3) 在“共享的机密”和“确认共享机密”栏均输入：12345678，点击 **完成** 返回。

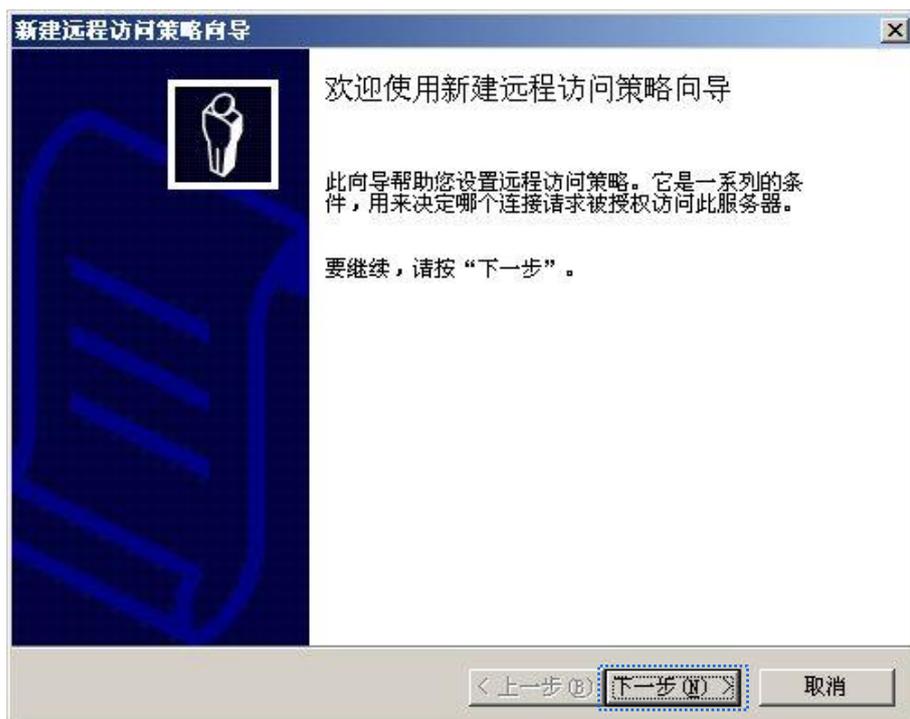


## 2. 配置远程访问策略。

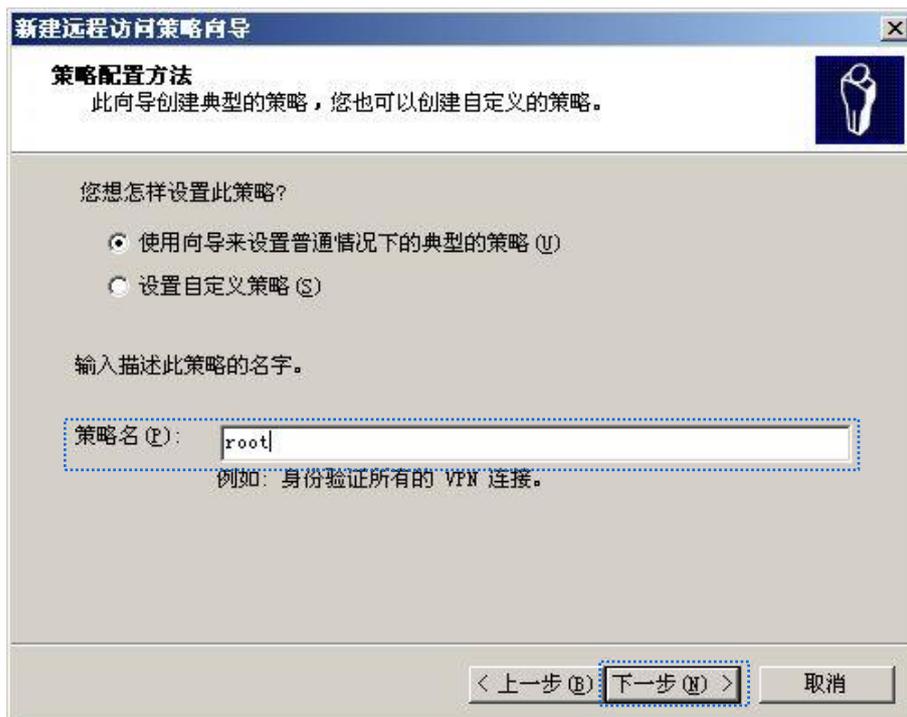
(1) 右键单击“远程访问策略”，选择“新建远程访问策略”。



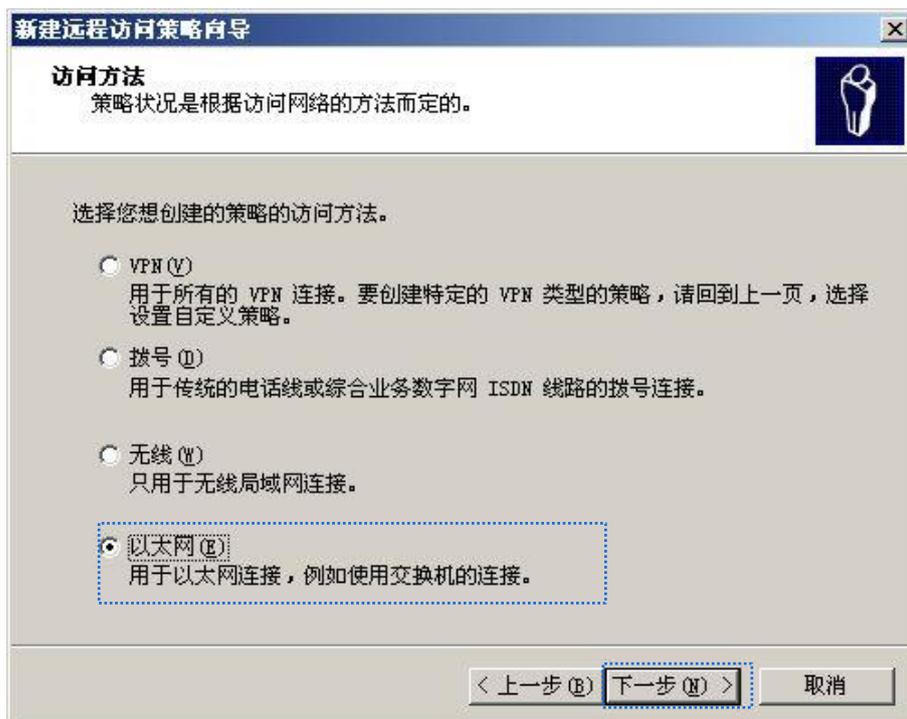
(2) 弹出新建远程访问策略向导，点击“下一步”。



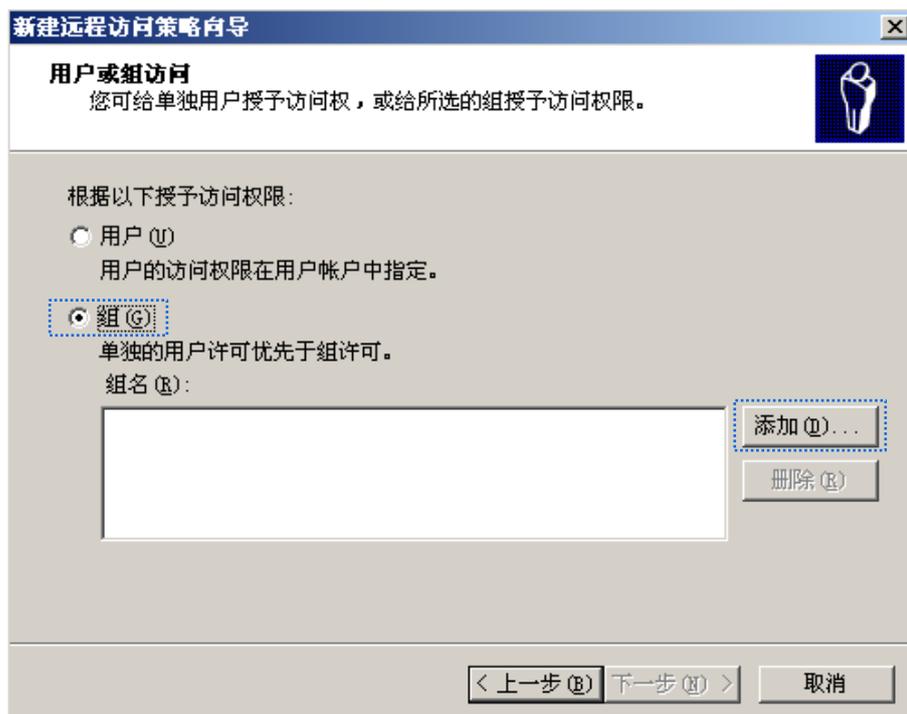
(3) 设置策略名，点击 **下一步**。



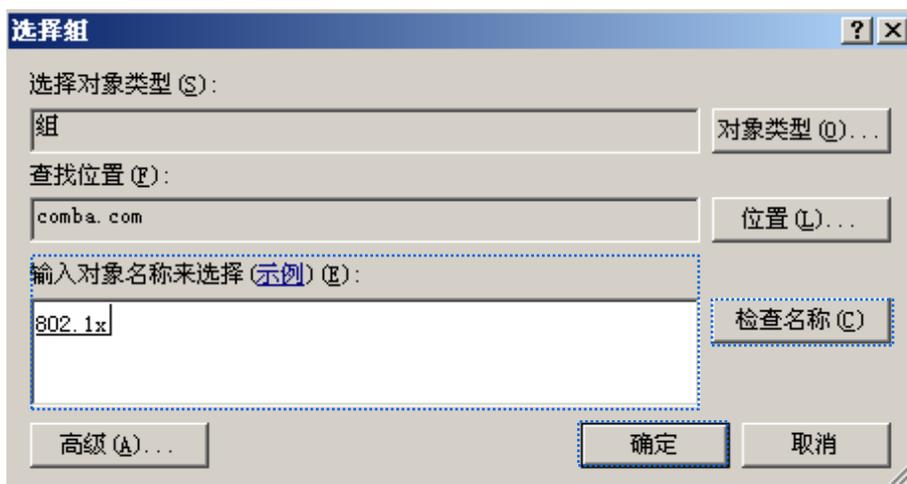
(4) 选择“以太网”，点击 **下一步**。



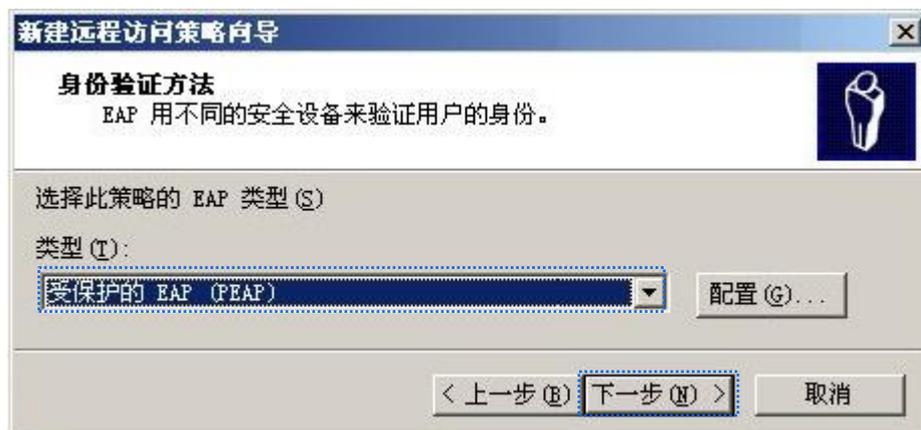
(5) 选择“组”，点击 **添加**。



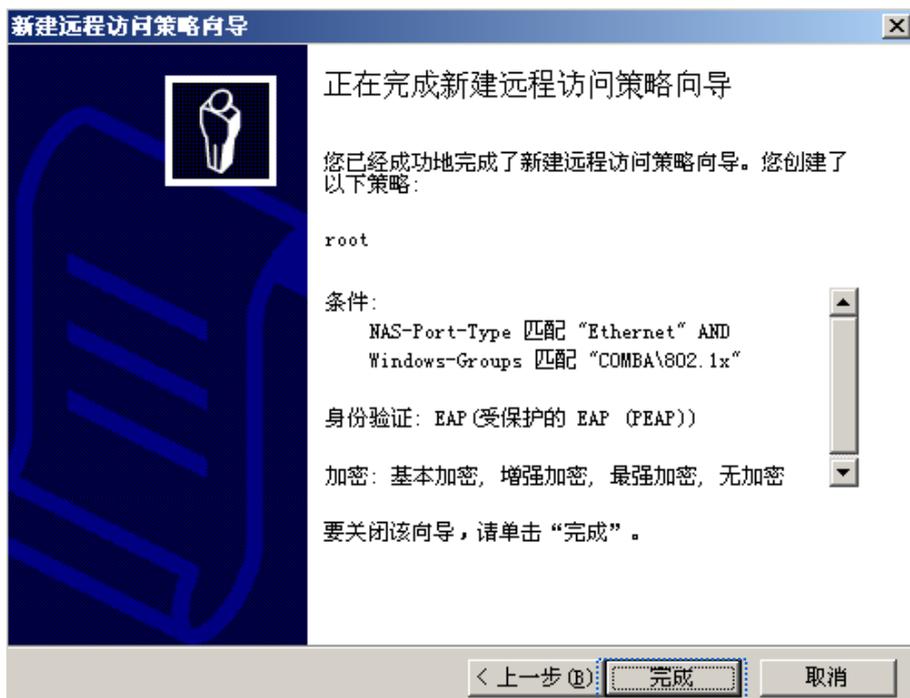
(6) 在“输入对象名称来选择”中输入 802.1x，点击 **检查名称**，点击 **确定**。



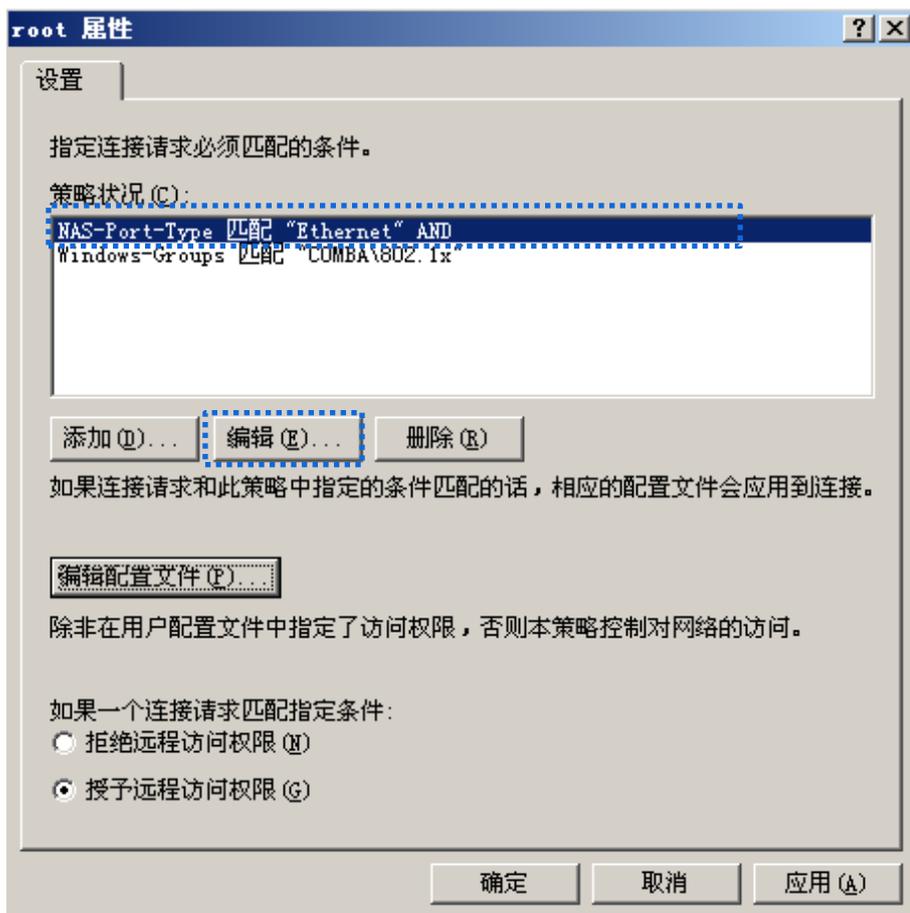
(7) 选择受保护的 EAP (PEAP)，点击 **下一步** 完成操作。



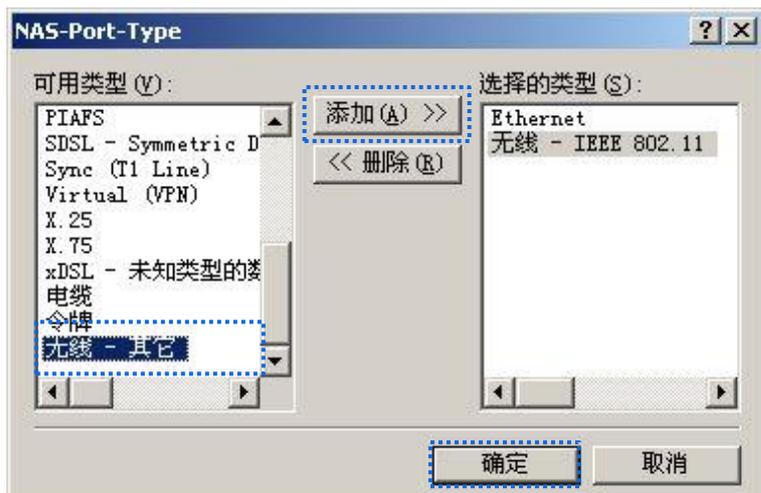
(8) 完成新建远程访问策略向导操作。



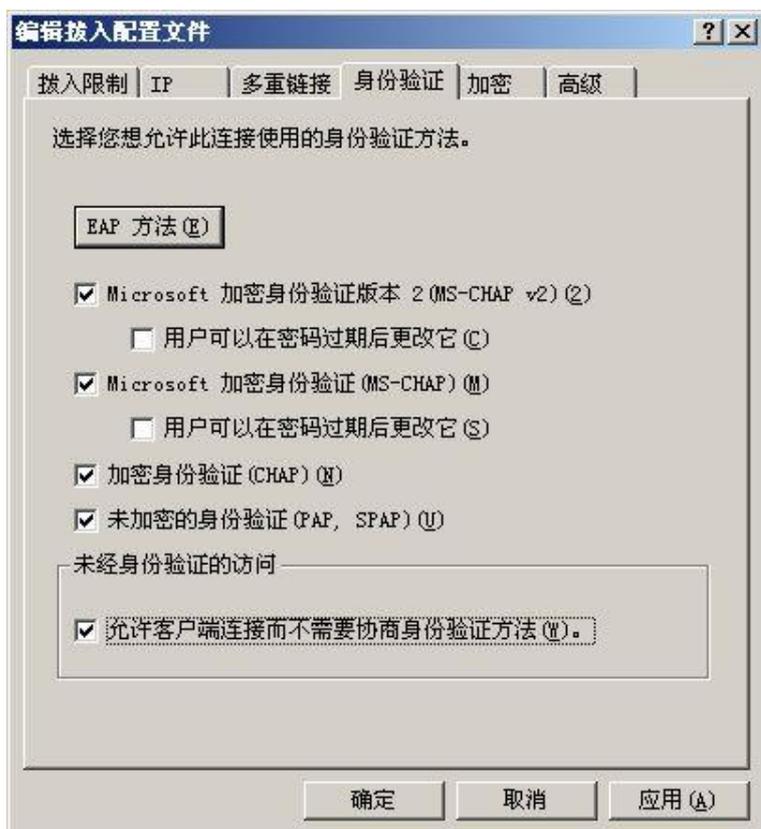
(9) 选中 root，点击右键，选择“属性”，在打开的窗口中，选择“授予远程访问权限”，然后选择“NAS-Port-Type 匹配“Ethernet”AND”，点击 编辑。



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



(11) 在返回的页面点击 **编辑配置文件**，在身份验证页面，进行下图所示配置，点击 **确定** 退出。



(12) 在弹出的提示框，点击 **否**，确认返回。



### 3. 配置用户信息。

新建用户，并将用户添加到组 802.1x。

## 三、配置用户设备



本文以 Windows 7 系统为例说明。

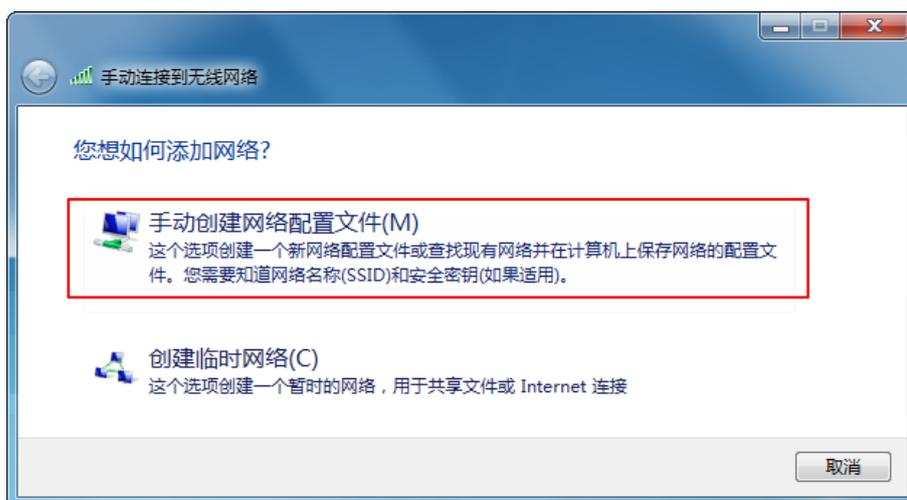
1. 在「控制面板」>「网络和 Internet」>「网络和共享中心」页面，点击“管理无线网络”。



2. 点击“添加”。



3. 选择“手动创建网络配置文件(M)”。



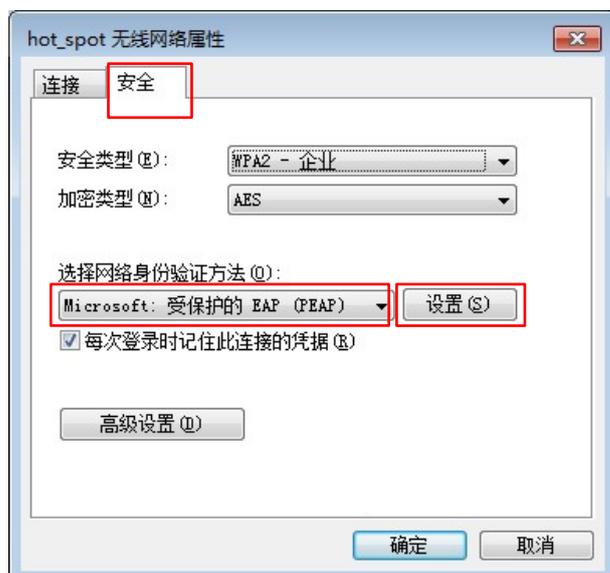
4. 如下图所示输入无线网络信息，勾选“即使网络未进行广播也连接”，然后点击 **下一步**。



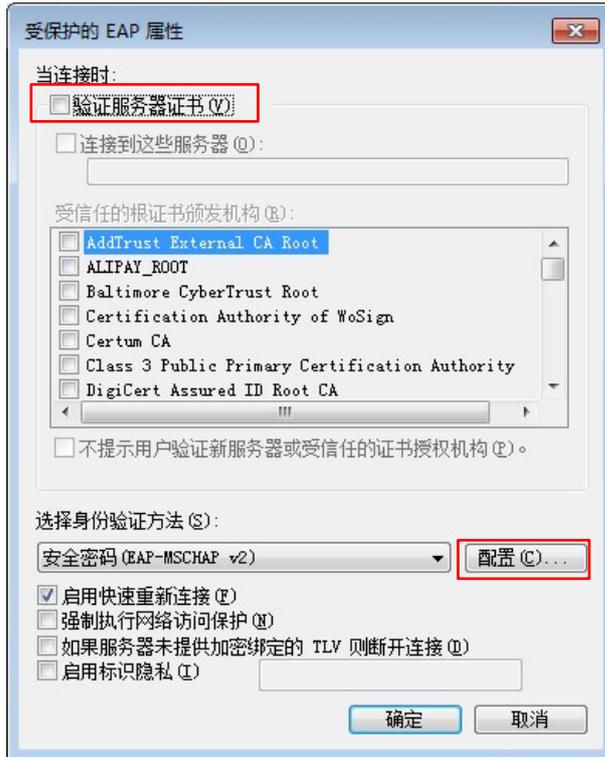
5. 点击“更改连接设置 (H)”。



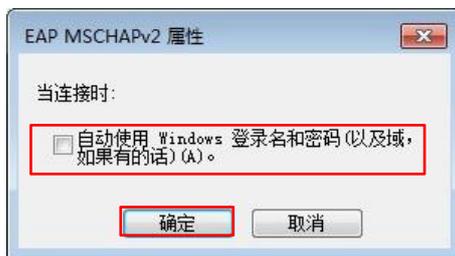
6. 选择“安全”页签，身份验证方法选择“Microsoft：受保护的 EAP (PEAP)”，再点击 **设置**。



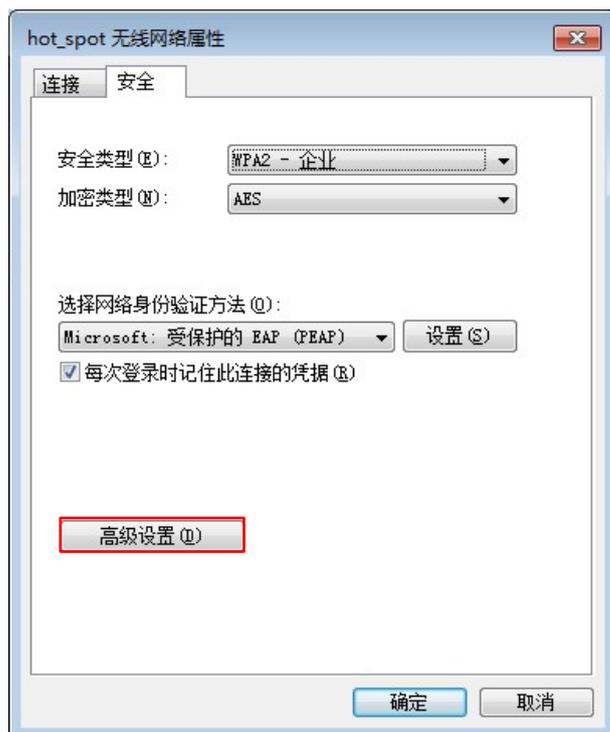
7. 取消“验证服务器证书”，然后点击 **配置**。



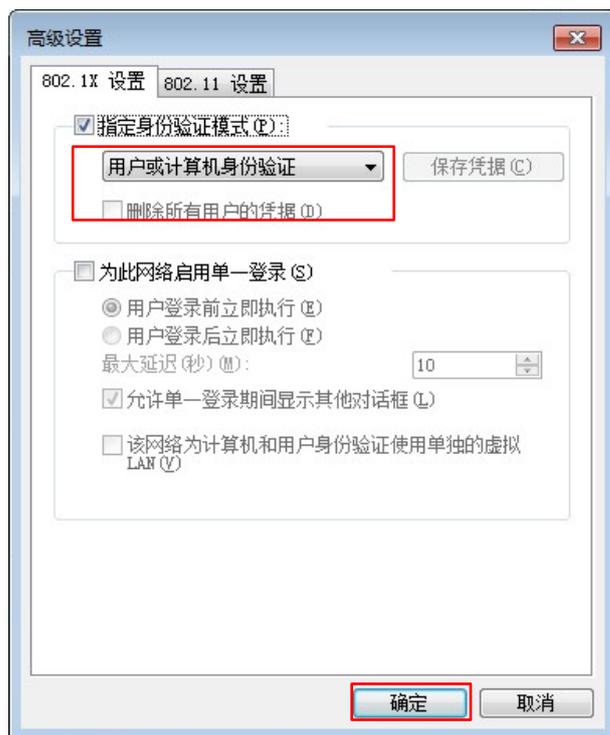
8. 取消“自动使用 windows 登录名和密码”，点击 **确定**。



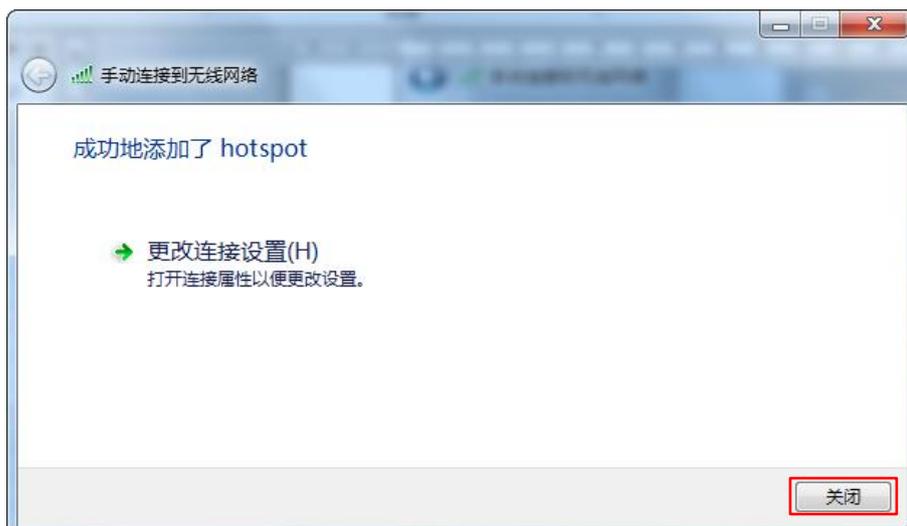
9. 点击 **高级设置**。



10. 指定身份验证模式为“用户或计算机身份认证”，然后点击 **确定**。



11. 点击 **关闭**。



12. 在电脑桌面右下角连接网桥的无线网络，本例为“hotspot”。



13. 当弹出用户名/密码输入框时，输入 RADIUS 服务器上添加的[用户名/密码](#)，然后点击 **确定**。



## 验证配置

用户设备连接无线网络“hotspot”成功。

## 7.2 高级设置

### 7.2.1 概述

本页面可以调试网桥的无线性能，如果没有专业人士指导，建议保持默认设置。

### 7.2.2 修改高级参数

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

当前模式：AP模式

### 高级设置

WMM  启用  禁用

APSD  启用  禁用

接入信号强度限制  禁用  启用

无线前导码  短导码  长导码

信号接收能力

Beacon间隔  ms (范围：100~999，默认：100)

Fragment阈值  (范围：256~2346，默认：2346)

RTS门限  (范围：1~2347，默认：2347)

DTIM间隔  (范围：1~255，默认：1)

LED1指示灯信号强度  dBm (范围：-90~0)

LED2指示灯信号强度  dBm (范围：-90~0)

LED3指示灯信号强度  dBm (范围：-90~0)

----完成

## 参数说明

标题项	说明
WMM	WMM 是一种无线 QoS 协议，用于保证高优先级的报文有优先的发送权利，从而保证语音、视频等应用在无线网络中有更好的服务质量。建议保持开启状态。
APSD	Automatic Power Save Delivery，自动省电模式。是 Wi-Fi 联盟的 WMM 省电认证协议。启用 WMM 后，开启“APSD”可降低网桥的电能消耗。默认禁用。
接入信号强度限制	禁用/启用接入信号强度限制功能。 启用后，需要设置网桥可接受的无线设备信号强度，信号强度低于此值的设备将无法接入网桥。当环境中存在多个网桥时，正确设置接入信号强度限制可以确保无线设备主动连接到信号比较强的网桥。
无线前导码	无线前导码是位于数据包起始处的一组 bit 位，接收者可以据此同步并准备接收实际的数据。默认为长前导码，可以兼容网络中一些比较老的客户端网卡。如果要使网络同步性能更好，可以选择短前导码。
信号接收能力	用于调节网桥的信号接收能力，级别越高，网桥的信号接收能力越强，扫描到的无线信号越多。
Beacon 间隔	设置网桥发送 Beacon 帧的时间间隔。 Beacon 帧按规定的间隔周期性发送，以公告无线网络的存在。一般来说：间隔越小，无线客户端接入网桥的速度越快；间隔越大，无线网络数据传输效率越高。
Fragment 阈值	设置帧的分片门限值。 分片的基本原理是将一个大的帧分成更小的分片，每个分片独立地传输和确认。当帧的实际大小超过指定的分片门限值时，该帧被分片传输。 在误码率较高的环境下，可以把分片阈值适当降低，这样，如果传输失败，只有未成功发送的部分需要重新发送，从而提高帧传输的吞吐量。 在无干扰环境下，适当提高分片阈值，可以减少确认帧的次数，以提高帧传输的吞吐量。
RTS 门限	启用冲突避免 ( RTS/CTS ) 机制所要求的帧的长度门限值。单位：字节。当帧的长度超过这个门限时，使用 RTS/CTS 机制，降低发生冲突的可能性。 RTS 门限需要进行权衡后合理设置：如果设得较小，则会增加 RTS 帧的发送频率，消耗更多的带宽；但 RTS 帧发送得越频繁，无线网络从冲突中恢复得就越快。在高密度无线网络环境可以降低此门限值，以减少冲突发生的概率。 使用冲突避免机制会占用一定的网络带宽，所以只在传输高于 RTS 门限的数据帧时才使用，对于小于 RTS 门限的数据帧不启动该机制。
DTIM 间隔	DTIM ( Delivery Traffic Indication Message ) 帧的发送间隔。单位：Beacon。 DTIM 会由此值倒数至 0，当 DTIM 计数达到 0 时，网桥才会发送缓存中的多播帧或广播帧。 例如：DTIM 间隔=1，表示每隔一个 Beacon 的时间间隔，网桥将发送所有暂时缓存的数据包。
接入信号强度阈值	设置网桥可接受的无线设备信号强度，信号强度低于此值的设备将无法接入网桥。

标题项	说明
LED1/LED2/LED3 指示灯信号强度	当环境中存在多个网桥时，正确设置接入信号强度限制可以确保无线设备主动连接到信号比较强的网桥。  用于修改网桥 LED1/LED2/LED3 指示灯的点亮值。 当网桥接收到的无线信号强度达到所设定的值时，相应的 LED 灯将亮起。

## 7.3 访问控制

### 7.3.1 概述

访问控制，即通过设置 MAC 地址过滤规则，允许或禁止指定设备接入网桥的无线网络。

网桥支持以下 MAC 过滤模式：

- 仅允许：允许指定 MAC 地址的无线设备接入网桥的无线网络，拒绝其他无线设备接入。
- 仅禁止：拒绝指定 MAC 地址的无线设备接入网桥的无线网络，允许其他无线设备接入。

### 7.3.2 配置访问控制

1. 进入「无线设置」>「访问控制」页面。
2. 访问控制：勾选“启用”选框。
3. 模式：根据需要选择“仅允许”或“仅禁止”。
4. MAC 地址：输入 MAC 地址。
5. 点击 **添加**。



如果要限制的无线设备已连接上网桥，还可以直接点击 **添加在线设备**，快速添加该无线设备的 MAC 地址到访问控制列表。

---

6. 点击 **保存**。

当前模式：AP模式

### 访问控制

SSID IP-COM\_83F060

访问控制  启用

模式  仅禁止  仅允许

MAC地址  :  :  :  :  :

序号	MAC地址	系统状态	操作
1	12:12:12:12:12:12	<input checked="" type="checkbox"/> 启用	✕

[访问控制列表](#)

---完成

### 参数说明

标题项	说明
SSID	要限制无线设备连接的 SSID。
访问控制	启用/禁用访问控制功能。
模式	设置访问控制模式。 <ul style="list-style-type: none"><li>仅允许：仅允许访问控制列表中的无线设备接入该 SSID。</li><li>仅禁止：仅禁止访问控制列表中的无线设备接入该 SSID，允许其他无线设备接入该 SSID。</li></ul>

## 7.3.3 访问控制配置举例

### 组网需求

某小区进行无线组网，现需要配置网桥，让该 SSID 仅禁止几个用户接入。

可以使用网桥的访问控制功能实现上述需求。假设要禁止的设备的 MAC 分别为 C8:3A:35:00:00:01、C8:3A:35:00:00:02、C8:3A:35:00:00:03。

## 配置步骤

1. 进入「无线设置」>「访问控制」页面。
2. 访问控制：勾选“启用”。
3. 模式：选择“仅禁止”。
4. MAC地址：输入“C8:3A:35:00:00:01”，点击 **添加**。
5. 重复步骤4，添加MAC“C8:3A:35:00:00:02”、“C8:3A:35:00:00:03”。
6. 点击 **保存**。

当前模式：AP模式

### 访问控制

SSID IP-COM\_83F060

访问控制  启用

模式  仅禁止  仅允许

MAC地址 C8 : 3A : 35 : 00 : 00 : 03

序号	MAC地址	系统状态	操作
1	C8:3A:35:00:00:01	<input checked="" type="checkbox"/> 启用	<input type="button" value="✕"/>
2	C8:3A:35:00:00:02	<input checked="" type="checkbox"/> 启用	<input type="button" value="✕"/>
3	C8:3A:35:00:00:03	<input checked="" type="checkbox"/> 启用	<input type="button" value="✕"/>

----完成

## 验证配置

只有上述3台无线设备不可以接入网桥的无线网络，其他设备可以接入该网络。

# 8 高级设置

## 8.1 LAN 口速率

### 8.1.1 概述

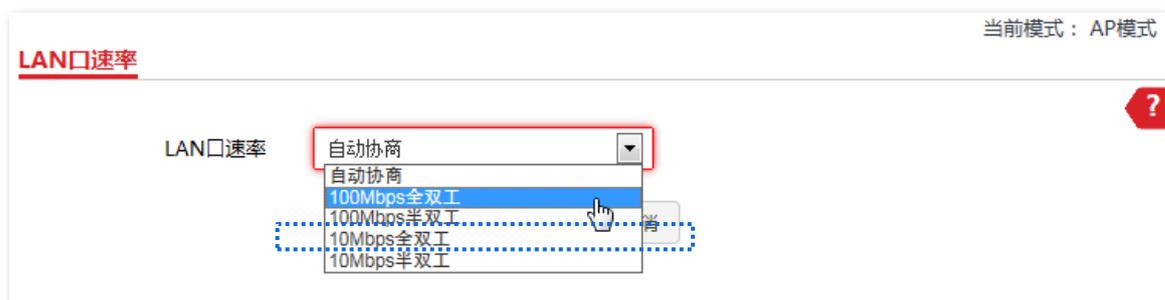
进入页面：点击「高级设置」>「LAN 口速率」。

在这里，您可以修改网桥接口的速率。修改时，请确保进行数据传输的设备之间的接口速率模式要保持一致。默认为自动。



### 8.1.2 修改 LAN 口速率

1. 进入「高级设置」>「LAN 口速率」页面。
2. 点击下拉菜单，选择相应的速率和双工模式，假设要修改为 **100Mbps 全双工**。
3. 点击 **保存**。



----完成

设置完成后，可以在“系统状态”页面查看，如下图示：

当前模式：AP模式

**系统状态**

系统状态

设备名称	CPE3V1.0	LAN MAC	C8:3A:35:83:F0:60
运行时间	1时 2分 20秒	WLAN MAC	C8:3A:35:83:F0:61
系统时间	2018-03-28 11:16:05	LAN口速率	100Mbps全双工
软件版本	V1.0.0.3(1930)	LAN IP	192.168.2.1
硬件版本	V1.0		

## 8.2 网络诊断

### 8.2.1 概述

进入页面：点击「高级设置」>「网络诊断」。

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

#### 扫描信号

用于扫描网桥当前所在区域周围的无线网络情况。

#### Ping

用于检测网络的连通性和连通质量。

#### Traceroute

用于检测数据包从网桥到目标主机所经过的路由。

### 8.2.2 扫描信号

假设要检测网桥周围的无线网络情况。

1. 进入「高级设置」>「网络诊断」页面。
2. 网络诊断：选择“扫描信号”。

**----完成**

稍等片刻，扫描结果将会显示在页面下方，如下图示。

当前模式：AP模式

**网络诊断**

网络诊断 扫描信号

序号	SSID	信道	MAC地址	安全模式	信号强度
1	FEF5A8	1	50:2B:73:FE:F5:A9	不加密	
2	IP-COM_112277	1	50:2B:73:FE:F5:AA	不加密	
3	FEF5A1	11	C8:3A:35:13:05:08	Mixed WPA/WPA..	
4	IP-COM_11F5B0	1	D8:38:0D:33:F4:01	WPA2-PSK,AES	
5	FEF5B0	1	50:2B:73:FE:F5:B1	Mixed WPA/WPA..	
6	1s	13	50:2B:73:FE:F5:9A	Mixed WPA/WPA..	
7	1111	11	C8:3A:35:83:FA:AB	Mixed WPA/WPA..	
8	IP-COM_1	11	C8:3A:50:E2:38:D1	Mixed WPA/WPA..	
9	CYL_AC9	6	D8:32:14:4C:CB:71	Mixed WPA/WPA..	
10	NOVA_2BC0	6	50:2B:73:FF:2B:C1	Mixed WPA/WPA..	

根据扫描列表，可以为网桥选择干扰较小的信道（其他无线信号较少使用的信道），以提升无线传输效率。

## 8.2.3 执行 Ping

假设要检测访问百度链路是否畅通。

1. 进入「高级设置」>「网络诊断」页面。
2. 网络诊断：选择“Ping”。
3. IP 地址：选择“手动设置”。
4. 目标 IP 地址/域名：输入要检测的 IP 地址或域名，本例为“www.baidu.com”。
5. ping 包个数：设置 ping 发送的数据包的个数。
6. 数据包大小：设置 ping 发送的数据包的大小。
7. 点击 **开始**。

当前模式：AP模式

### 网络诊断

网络诊断

IP地址

目标IP地址/域名

ping包个数  (范围：1~1000)

数据包大小  字节 (范围：1~60000)

---完成

稍后，诊断结果将显示在页面下方。如下图示。

### 网络诊断

网络诊断

IP地址

目标IP地址/域名

ping包个数  (范围：1~1000)

数据包大小  字节 (范围：1~60000)

IP地址	时间	TTL
14.215.177.38	40.000ms	50
14.215.177.38	20.000ms	50
14.215.177.38	20.000ms	50
14.215.177.38	30.000ms	50
14.215.177.38	30.000ms	50

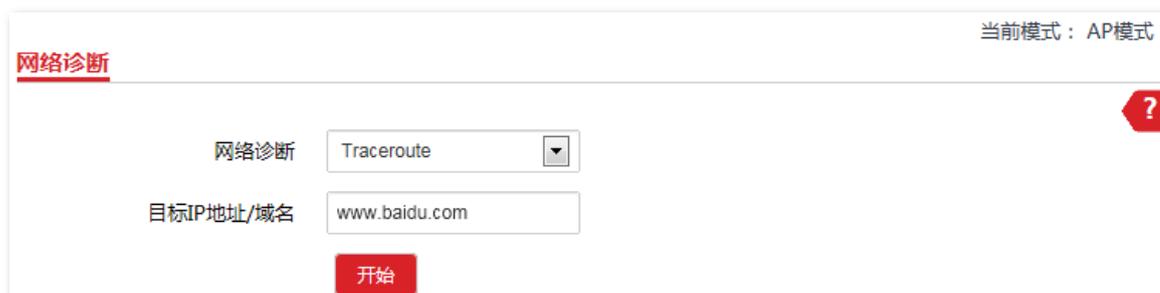
收到5个数据包，发送5个数据包，丢包率0.00%

最小20ms                      平均28ms                      最大40ms

## 8.2.4 执行 Traceroute

假设要检测网桥到百度的路径。

1. 进入「高级设置」>「网络诊断」页面。
2. 网络诊断：选择“Traceroute”。
3. IP地址或域名：输入要检测的IP地址或域名，本例为“www.baidu.com”。
4. 点击 **开始**。



网络诊断

当前模式：AP模式

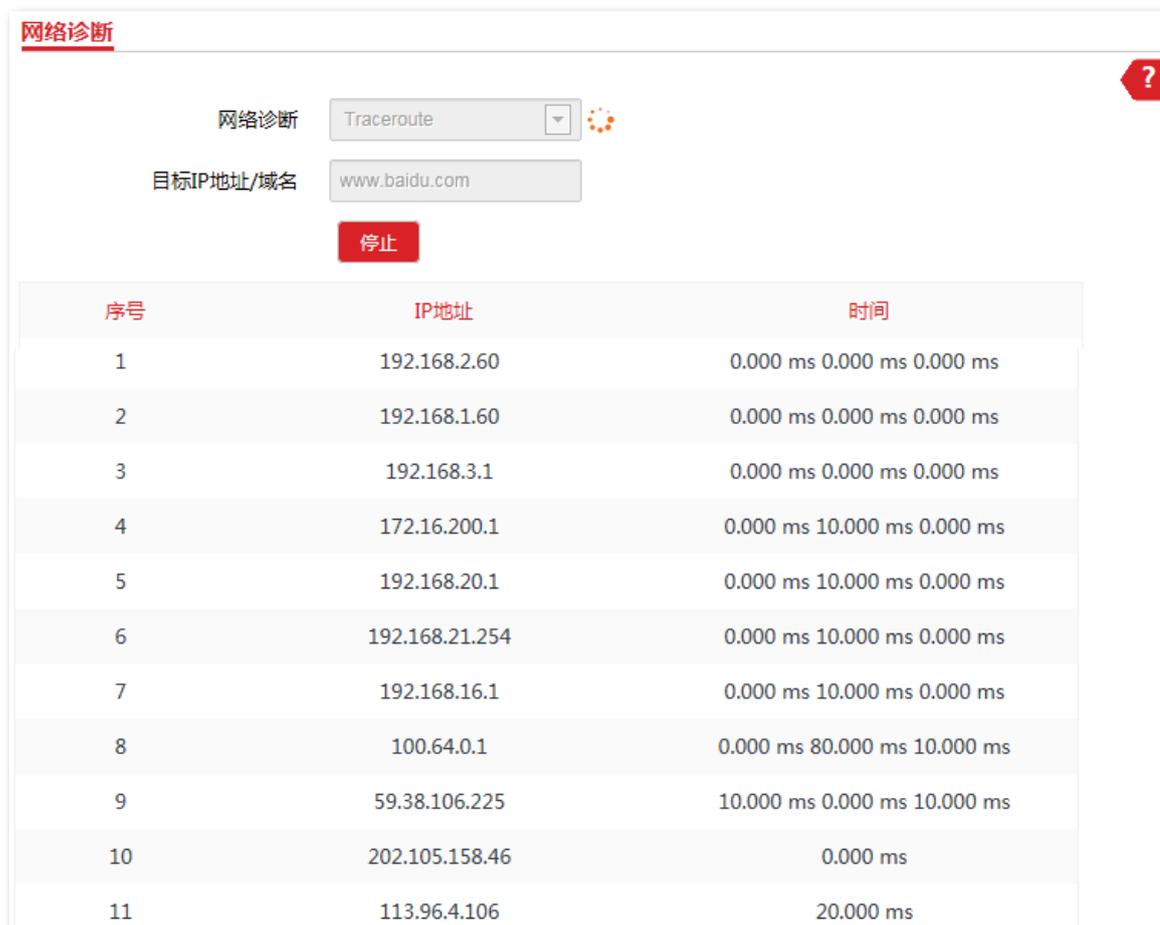
网络诊断 Traceroute

目标IP地址/域名 www.baidu.com

开始

----完成

稍后，诊断结果将显示在页面下方。如下图示例。



网络诊断

网络诊断 Traceroute

目标IP地址/域名 www.baidu.com

停止

序号	IP地址	时间
1	192.168.2.60	0.000 ms 0.000 ms 0.000 ms
2	192.168.1.60	0.000 ms 0.000 ms 0.000 ms
3	192.168.3.1	0.000 ms 0.000 ms 0.000 ms
4	172.16.200.1	0.000 ms 10.000 ms 0.000 ms
5	192.168.20.1	0.000 ms 10.000 ms 0.000 ms
6	192.168.21.254	0.000 ms 10.000 ms 0.000 ms
7	192.168.16.1	0.000 ms 10.000 ms 0.000 ms
8	100.64.0.1	0.000 ms 80.000 ms 10.000 ms
9	59.38.106.225	10.000 ms 0.000 ms 10.000 ms
10	202.105.158.46	0.000 ms
11	113.96.4.106	20.000 ms

## 8.3 网络服务

### 8.3.1 动态 DNS (仅无线 WAN 模式有效)

#### 概述

动态 DNS，即动态域名服务。当服务运行时，网桥上的 DDNS 客户端将其当前的 WAN 口 IP 地址传送给 DDNS 服务器，服务器再更新数据库中域名与 IP 地址的映射关系，实现动态域名解析。

使用 DDNS 功能，可以让网桥动态变化的 WAN 口 IP 地址（公网 IP）始终被映射到一个固定的域名上。DDNS 功能一般与其他功能如端口映射、DMZ 主机、远端 WEB 管理等结合使用，这样，用户在进行诸如远程访问局域网服务器、远程访问网桥管理页面等应用时，无需再关注网桥的 WAN 口 IP 变化，直接使用对应的域名即可，更加方便易用。

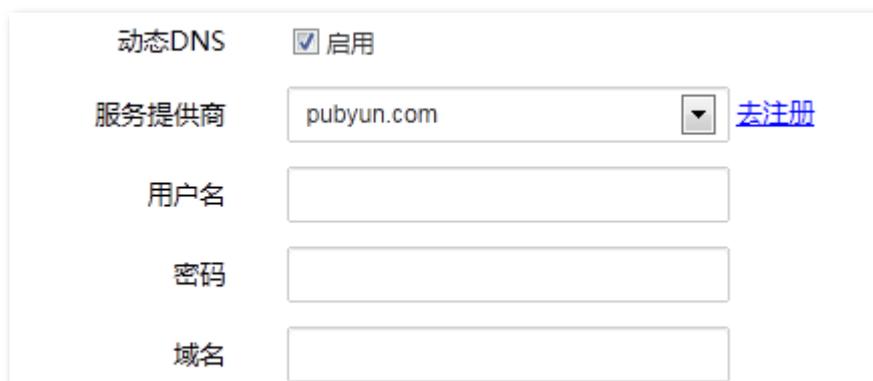
进入页面：点击「高级设置」>「网络服务」。



动态DNS	<input checked="" type="checkbox"/> 启用
服务提供商	pubyun.com <a href="#">去注册</a>
用户名	<input type="text"/>
密码	<input type="password"/>
域名	<input type="text"/>

#### 配置动态 DNS

1. 点击「高级设置」>「网络服务」。
2. 动态 DNS：勾选“启用”。
3. 设置各参数。
4. 点击 **保存**。



动态DNS  启用

服务提供商 pubyun.com [去注册](#)

用户名

密码

域名

----完成

## 参数说明

标题项	说明
动态 DNS	启用/禁用动态 DNS 功能。
服务提供商	动态 DNS 的服务提供商。网桥支持的动态 DNS 服务提供商有：no-ip.com、pubyun.com、dyndns.com。
用户名	登录动态 DNS 服务的用户名，即在“服务提供商”网站上注册的登录用户名。
密码	登录动态 DNS 服务的密码，即在“服务提供商”网站上注册的登录用户名对应的登录密码。
域名	从动态 DNS 服务器获取的域名信息，需要手动输入在其网站上申请的域名。

## 动态 DNS 示例

### 组网需求

某小区使用网桥进行网络组建，网桥工作在无线 WAN 模式并接入互联网，WAN IP 动态变化。管理员出差时需访问内网电脑上的资源，可通过动态 DNS 功能实现。首先在内网电脑上建立并开启 Web 服务器，并在服务器上存放要访问的资源，然后在网桥上设置动态 DNS 功能、DMZ 功能。

### 组网假设

内网 Web 服务器信息如下：

- IP 地址：192.168.2.100
- 端口：80

已注册的域名信息如下：

- 服务提供商：dyndns.com
- 用户名、密码：zhangsan
- 域名：zhangsan.dyndns.com

## 配置步骤

### 一、设置动态 DNS

1. 登录到网桥的管理页面，转到「高级设置」>「网络服务」页面。
2. 动态 DNS：勾选复选框。
3. 服务供应商：选择您申请域名的动态 DNS 供应商，本例为“dyndns.com”。
4. 用户名：输入您在服务供应商网站注册的用户名，本例为“zhangsan”。
5. 密码：输入您在服务供应商网站注册的用户名对应的密码，本例为“zhangsan”。
6. 域名：输入您从服务供应商网站申请的域名，本例为“zhangsan.dyndns.com”。
7. 点击 **保存**。



动态DNS	<input checked="" type="checkbox"/> 启用
服务提供商	dyndns.com <a href="#">去注册</a>
用户名	zhangsan
密码	zhangsan
域名	zhangsan.dyndns.com

### 二、设置 DMZ

1. 登录到网桥的管理页面，转到「高级设置」>「网络服务」页面。
2. 在 DMZ 主机模块，勾选“启用”复选框。
3. 在输入框中填入 Web 服务器 IP 地址，本例为“192.168.2.100”。
4. 点击 **保存**。



DMZ主机	<input checked="" type="checkbox"/> 启用	192.168.2.100
-------	--	---------------

## 验证配置

广域网用户使用“内网服务应用层协议名称://WAN 口域名:外网端口”可以成功访问内部 Web 服务器。在本例中，访问地址为“http://zhangsan.dyndns.com:80”。

---



配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，请依次尝试以下方法解决。

- 确保网桥 WAN 口获取的是公网 IP 地址，您填写的内网端口段是正确的相应服务端口。
  - 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。
  - 手动配置局域网服务器 IP，避免因为 IP 的自动变化而导致服务中断。
-

## 8.3.2 远程 WEB 管理 (仅无线 WAN 模式有效)

### 概述

一般情况下，只有接到网桥 LAN 口下的设备才能登录网桥的管理页面。

通过远程 WEB 管理功能，使您在有特殊需要时（如远程技术支持），也可以通过 WAN 口远程访问网桥的管理页面。

### 配置远程 WEB 管理

1. 登录到网桥的管理页面，转到「高级设置」>「网络服务」页面。
2. 远程 WEB 管理：勾选“启用”复选框。
3. IP 地址：输入允许远程访问网桥管理页面的用户电脑的 IP 地址。
4. 端口号：设置远程管理网桥时使用的端口号，建议保持默认。
5. 点击 **保存**。



远程WEB管理	<input checked="" type="checkbox"/> 启用
IP地址	<input type="text" value="0.0.0.0"/>
端口	<input type="text" value="8080"/>

----完成

### 参数说明

标题项	说明
远程 WEB 管理	开启/关闭远程 WEB 管理功能。
IP 地址	设置允许远程访问网桥管理页面的电脑 IP 地址。如果该管理电脑在局域网，则应填入电脑的网关的 IP 地址（公网 IP）。 0.0.0.0 表示互联网上所有电脑都能访问网桥的管理页面。为了网络安全，不建议设置为此值。
端口	远程管理网桥时使用的端口号。默认为 8080，可根据需要修改。 1~1024 端口已被熟知服务占用，为避免端口冲突，强烈建议修改该端口为 1025~65535 范围内的端口。 远程访问网桥的方式为“http://WAN 口 IP:端口号”。如果 WAN 口开启了动态 DNS 功能，还可以使用“http://WAN 口域名:端口号”访问。

## 远端 WEB 管理配置举例

### 组网需求

某小区使用网桥进行网络组建，网桥工作在无线 WAN 模式并接入互联网。网络管理员出差时可能要维护网络，需要远程登录设备管理页面。可以通过远程 WEB 访问功能实现。

### 组网假设

- 网桥的 WAN IP 地址：202.105.106.55
- 允许远程访问网桥的电脑的 IP 地址：202.105.88.77
- 端口：8080

### 配置步骤

1. 登录到网桥的管理页面，转到「高级设置」>「网络服务」页面。
2. 远程 WEB 管理：勾选复选框。
3. IP 地址：输入要远程访问网桥的电脑的 IP 地址，本例为“202.105.88.77”。
4. 端口：建议保持默认值“8080”。
5. 点击 **保存**。

远程WEB管理	<input checked="" type="checkbox"/> 启用
IP地址	<input type="text" value="202.105.88.77"/>
端口	<input type="text" value="8080"/>

### 验证配置

在 IP 地址为 202.105.88.77 的电脑上，打开浏览器，访问“http://202.105.106.55:8080”，即可登录网桥并对其进行管理。

## 8.3.3 定时重启

### 概述

通过定时重启功能，可以设置网桥定时自动重启，预防网桥长时间运行导致 WLAN 出现性能降低、不稳定等现象。设置后，网桥在每周指定的日期和时间自动重启。

### 设置网桥定时重启

1. 进入「高级设置」>「网络服务」页面。
2. 定时重启：勾选复选框。
3. 时间：设置定时重启的时间点，如“3:00”。
4. 日期：选择定时重启的日期，如“星期一 ~ 星期五”。
5. 点击 **保存**。

定时重启	<input checked="" type="checkbox"/> 启用
时间	<input type="text" value="3:00"/>
日期	<input checked="" type="checkbox"/> 星期一 <input checked="" type="checkbox"/> 星期二 <input checked="" type="checkbox"/> 星期三 <input checked="" type="checkbox"/> 星期四 <input checked="" type="checkbox"/> 星期五 <input type="checkbox"/> 星期六 <input type="checkbox"/> 星期日 <input type="checkbox"/> 每天

----完成

## 8.3.4 WEB 闲置超时时间

为了保障网络安全，当您登录到网桥的管理页面后，如果在所设置的“WEB 闲置超时时间”内没有任何操作，系统将自动退出登录。

默认 WEB 闲置超时时间为 5 分钟，您可根据需要修改。点击「高级设置」>「网络服务」进入设置页面。

WEB闲置超时时间	<input type="text" value="5"/>	分钟 (范围: 1~60, 默认: 5)
-----------	--------------------------------	----------------------

## 8.3.5 SNMP 代理

### 概述

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

SNMP 能够屏蔽不同设备的物理差异 , 实现对不同厂商设备的自动化管理。

### SNMP 的管理框架

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

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

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

## SNMP 基本操作

本网桥中，SNMP 提供以下两种基本操作来实现 SNMP 管理者和 SNMP 代理的交互：

- Get 操作：SNMP 管理者使用该操作查询 SNMP 代理的一个或多个对象的值。
- Set 操作：SNMP 管理者使用该操作重新设置 MIB 库中的一个或多个对象的值。

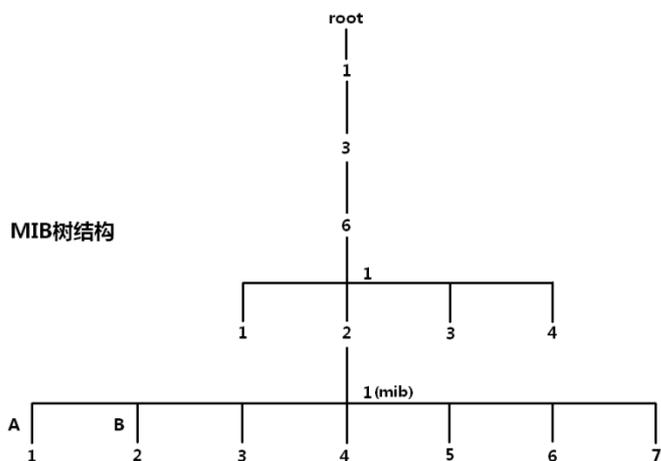
## SNMP 协议版本

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

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

## MIB 库简介

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



## 配置 SNMP

1. 进入「高级设置」>「网络服务」页面，找到 SNMP 模块，勾选“启用”SNMP 代理。
2. 设置 SNMP 相关参数。
3. 点击 **保存**。

SNMP代理	<input checked="" type="checkbox"/> 启用
设备名称	<input type="text" value="CPE3V1.0"/>
读 Community	<input type="text" value="public"/>
读/写 Community	<input type="text" value="private"/>
位置	<input type="text" value="ShenZhen"/>

----完成

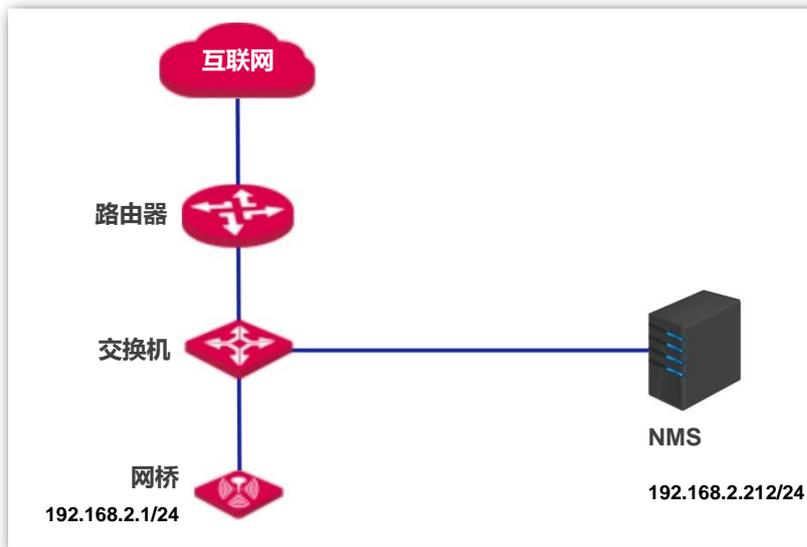
## 参数说明

标题项	说明
SNMP 代理	禁用/启用网桥的 SNMP 代理功能。默认为禁用。 SNMP 管理者和 SNMP 代理上的 SNMP 版本必须相同,才能成功互访。目前,网桥中的 SNMP 代理支持 SNMP v1 版本、SNMP v2c 版本。
设备名称	网桥的设备名称,默认为网桥的产品型号+版本号。  <b>提示</b> 建议修改设备名称,使您在使用 SNMP 管理网桥时,能快速识别出对应的网桥设备。
读 Community	只读团体名,是 SNMP 管理者和 SNMP 代理之间的读操作口令。默认为“public”。 本 SNMP 代理允许 SNMP 管理者用“读 Community”对网桥 MIB 中的变量进行读操作。
读/写 Community	读/写团体名,是 SNMP 管理者和 SNMP 代理之间的读写操作口令。默认为“private”。 本 SNMP 代理允许 SNMP 管理者用“读/写 Community”对网桥 MIB 中的变量进行读和写操作。
位置	网桥的安装位置,默认为“ShenZhen”。可根据实际情况修改。

## SNMP 配置举例

### 组网需求

- 网桥与 NMS 通过以太网相连，网桥的 IP 地址为 192.168.2.1/24，NMS 的 IP 地址为 192.168.2.212/24。
- NMS 通过 SNMP v1 或者 SNMP v2c 对网桥进行监控管理。



### 配置步骤

#### 一、配置网桥

假设读 Community 为 “zhangsan”，读/写 Community 为 “zhangsan123”。

1. 登录网桥的管理页面，转到「高级设置」>「网络服务」。
2. SNMP 代理：勾选“启用”。
3. 设置 SNMP 相关参数：设备名称、读 Community、读/写 Community、位置。
4. 点击 **保存**。

SNMP代理	<input checked="" type="checkbox"/> 启用
设备名称	<input type="text" value="CPE3V1.0"/>
读 Community	<input type="text" value="zhangsan"/>
读/写 Community	<input type="text" value="zhangsan123"/>
位置	<input type="text" value="ShenZhen"/>

## 二、配置 NMS

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

----完成

### 验证配置

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

## 8.3.6 Ping 看门狗

启用 Ping 看门狗后，网桥将周期性地向目标 IP 发送 ping 包，如果正常收到回复，则说明网络通畅，  
如果回复丢包数量超过了设置的“触发重启丢包个数”，网桥会自动重启，重启后继续检测，直到网  
络恢复正常。

### 配置 Ping 看门狗

1. 进入「高级设置」>「网络服务」页面，找到 Ping 看门狗模块，勾选“启用”Ping 看门狗。
2. 设置相关参数。
3. 点击 **保存**。

Ping看门狗	<input checked="" type="checkbox"/> 启用
IP地址	<input type="text" value="127.0.0.1"/>
Ping间隔	<input type="text" value="300"/> s (范围：20~86400)
启动延迟	<input type="text" value="300"/> s (范围：180~86400)
触发重启丢包个数	<input type="text" value="3"/>

----完成

### 参数说明

标题项	说明
Ping 看门狗	禁用/启用 Ping 看门狗功能。 启用后可以周期性地发送 Ping 包检测本设备与目的 IP 地址的网络连通性，从而判断链路是 否出现故障。如果判断为故障，网桥将自动重启，从而保证网络处于良好状态。

标题项	说明
IP 地址	网桥发送 Ping 包的目的 IP 地址，即要检测与网桥连通性的主机 IP 地址。
Ping 间隔	网桥发送 Ping 包的时间间隔。
启动延迟	网桥启动到启用 Ping 看门狗功能的延迟时间。 合理设置此参数可以避免系统启动过程中触发了 Ping 看门狗功能，而用户又无法登录网桥管理页面修改配置，导致网桥不停地重启。
触发最大丢包数	触发网桥重启的最大丢包数，取值范围为 1~65535，默认值为 3。 例如最大丢包数为 N，则当网桥连续发送 N 个 Ping 包至目的 IP 地址，都没有收到应答时，网桥将自动重启。

### 8.3.7 DMZ 主机 (仅无线 WAN 模式有效)

#### 概述

将局域网中某台计算机设置为 DMZ 主机后，该计算机与互联网通信时将不受限制。如某些视频会议和在线游戏，可将正在进行这些应用的计算机设置为 DMZ 主机，使视频会议和在线游戏更加顺畅。



- 当把计算机设置成 DMZ 主机后，该计算机相当于完全暴露于外网，网桥的防火墙对该计算机不再起作用。
- 黑客可能会利用 DMZ 主机对本地网络进行攻击，请不要轻易使用 DMZ 主机功能。

#### 配置 DMZ 主机

1. 进入「高级设置」>「网络服务」页面。
2. 在 DMZ 主机模块，勾选“启用”复选框。
3. 在输入框中填入局域网内需要设置为 DMZ 主机的电脑的 IP 地址。
4. 点击 **保存**。

DMZ主机  启用 192.168.2.100

----完成

## DMZ 主机配置举例

### 组网需求

某小区使用网桥进行网络组建，网桥工作在无线 WAN 模式并接入互联网。管理员出差时需访问内网电脑上的 Web 服务器资源。首先在内网电脑上建立并开启 Web 服务器，并在服务器上存放要访问的资源，然后在网桥上设置 DMZ 主机功能。

### 组网假设

网桥的 WAN IP 地址：202.105.106.55

内网 Web 服务器信息如下：

- IP 地址：192.168.2.100
- 端口：80

### 配置步骤

1. 进入「高级设置」>「网络服务」页面。
2. 在 DMZ 主机模块，勾选“启用”复选框。
3. 在输入框中填入局域网中 Web 服务器的 IP 地址，本例为 192.168.2.100。
4. 点击 **保存**。



DMZ主机  启用 192.168.2.100

### 验证配置

互联网用户使用“内网服务应用层协议名称://WAN 口 IP:端口号”可以成功访问内部 Web 服务器。在本例中，访问地址为“http://202.105.106.55:80”。

如果开启了[动态 DNS](#)，还可使用“内网服务应用层协议名称://WAN 口域名:端口号”访问。



配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，请依次尝试以下方法解决。

- 确保网桥 WAN 口获取的是公网 IP 地址。
  - 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。
  - 手动配置局域网服务器 IP，避免因 IP 的自动变化而导致服务中断。
-

## 8.3.8 Telnet 服务

启用 Telnet 服务后，可以通过 Telnet 方式查看网桥信息。

点击「高级设置」>「网络服务」进入设置页面，本功能默认禁用。



## 8.3.9 UPnP 服务

UPnP , Universal Plug and Play , 通用即插即用。启用 UPnP 功能后，网桥可以为内网中支持 UPnP 的程序（如迅雷等）自动打开端口，使应用更加顺畅。

点击「高级设置」>「网络服务」进入设置页面，UPnP 功能默认启用。



# 9 系统工具

## 9.1 时间与日期

在「时间与日期」模块，您可以设置网桥的系统时间。

为了保证网桥的日志记录、自定义重启等功能执行时间准确，建议校准网桥的系统时间。

进入页面：点击「系统工具」>「时间与日期」。



时间与日期 当前模式：AP模式

时间设置  网络校时  手动设置

校时周期 30分钟

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

保存 取消

网桥支持“网络校时”和“手动设置”两种时间设置方式，默认为“网络校时”。



无论采用哪种时间设置方式，当您登录到网桥管理页面时，网桥都会自动同步当前管理主机的时间。

### 网络校时

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

网桥联网方法请参考 [LAN 口设置](#)。

#### 设置步骤：

1. 进入「系统工具」>「时间与日期」页面。
2. 时间设置：选择“网络校时”。

3. 校时周期：选择网桥校对系统时间的时间间隔，建议保持默认“30 分钟”。
4. 时区：选择网桥当前所在地区的 GMT 标准时区，如中国需选择“(GMT+08:00) 北京，重庆，乌鲁木齐，香港特别行政区，台北”。
5. 点击 **保存**。

当前模式：AP模式

**时间与日期**

时间设置  网络校时  手动设置

校时周期 30分钟

时区 (GMT+08:00) 北京，重庆，乌鲁木齐，香港特别行政区，台北

**保存** 取消

----完成

## 手动设置时间

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

**设置步骤：**

1. 进入「系统工具」>「时间与日期」页面。
2. 时间设置：选择“手动设置”。
3. 时间与日期：输入正确的日期时间，或点击 **复制本地时间** 将当前正在管理网桥的电脑的时间同步到网桥（需确保该电脑的时间正确）。
4. 点击 **保存**。

当前模式：AP模式

**时间与日期**

时间设置  网络校时  手动设置

时间与日期 2018 年 03 月 28 天 13 时 50 分 37 秒

复制本地时间

**保存** 取消

----完成

## 9.2 设备维护

### 9.2.1 重启

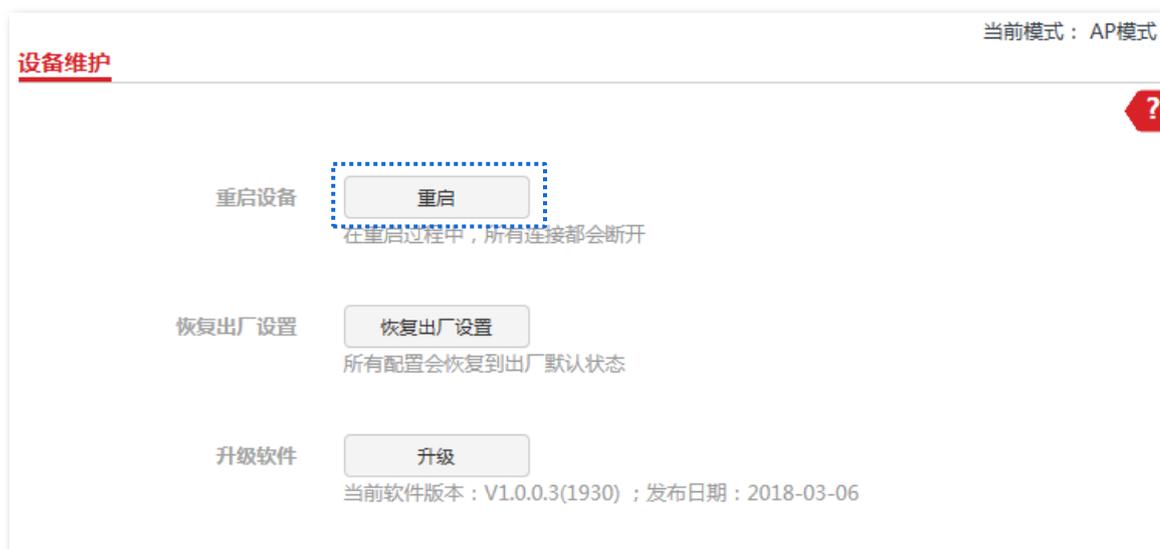
当您设置的某项参数不能正常生效或网桥不能正常使用时，可以尝试手动重启网桥解决。



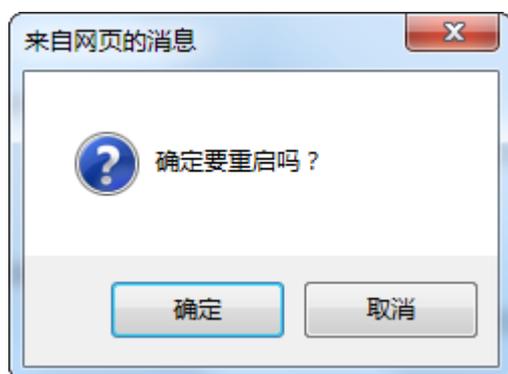
网桥重启时，会断开当前所有连接。请在网络相对空闲的时候进行重启操作。

**设置步骤：**

1. 进入「系统工具」>「设备维护」页面。
2. 点击 **重启**。



3. 确认提示信息后，点击 **确定**。



---完成

页面会出现重启进度条，耐心等待即可。

## 9.2.2 恢复出厂设置

当网桥出现无法定位的问题或您要登录网桥的管理页面却忘记登录密码时，可以将网桥恢复出厂设置后重新配置。

### 注意

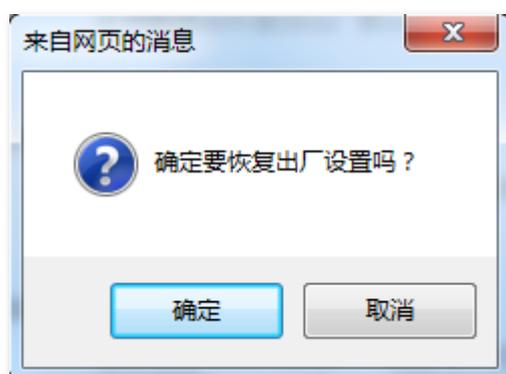
- 恢复出厂设置意味着网桥的所有设置将会丢失，您需要重新设置网桥。若非万不得已，不建议将网桥恢复出厂设置。
- 为避免损坏网桥，恢复出厂设置过程中，请确保网桥供电正常。
- 恢复出厂设置后，网桥的登录 IP 地址为 192.168.2.1，登录用户名/密码均为 “admin”。

### 设置步骤：

1. 进入「系统工具」>「设备维护」页面。
2. 点击 **恢复出厂设置**。



3. 确认提示信息后，点击 **确定**。



### ----完成

页面会出现恢复出厂设置进度条，耐心等待即可。

## 9.2.3 软件升级

通过软件升级，可以使网桥获得新增功能或更稳定的性能。

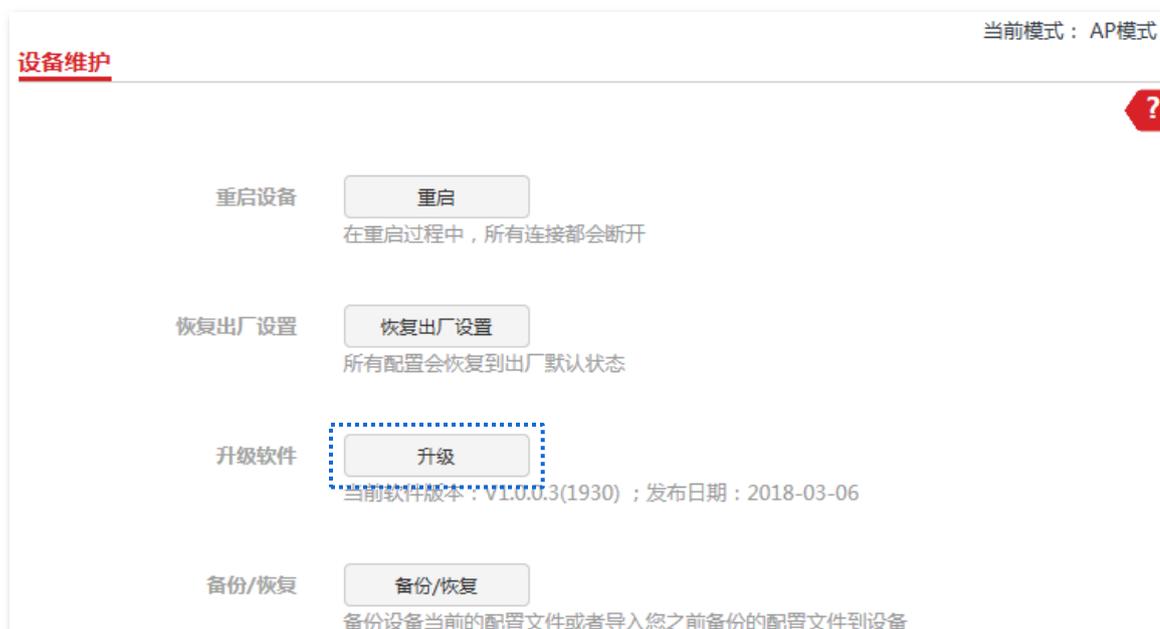


注意

为确保升级正确，避免网桥损坏，请在升级之前，务必确认新的软件适用于此网桥；升级过程中，请勿断开网桥电源。

### 软件升级步骤：

1. 登陆官方网站 [www.ip-com.com.cn](http://www.ip-com.com.cn)，下载更高版本的升级文件到本地电脑并解压。
2. 登录到网桥的管理页面，转到「系统工具」>「设备维护」页面。
3. 点击 **升级**。



4. 点击 **浏览...**，从本地电脑选择并加载网桥的升级文件。
5. 点击 **升级**。



#### ---完成

页面会出现升级及重启进度条，请耐心等待。待进度条走完后，重新登录到网桥的管理页面，然后进入「状态」页面查看网桥的“软件版本”，确认与您刚才升级的软件版本相同。



提示

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

---

## 9.2.4 备份与恢复

使用备份功能，可以将网桥当前的配置信息保存到本地电脑；使用恢复功能，可以将网桥配置还原到之前备份的配置。

如，当您对网桥进行了大量的配置，使其在运行时拥有较好的状态/性能，或更符合对应环境的需求，此时建议对该配置进行备份；当您对网桥进行了升级、恢复出厂设置等操作后，可以恢复备份的网桥配置。



如果您需要设置大量网桥，且这些网桥的配置全部一致或大部分一致，也可以使用备份与恢复功能：先配置好 1 台网桥并备份该网桥的配置信息，之后将备份的配置信息导入（恢复）到其他网桥，从而节省配置时间，提高效率。

### 备份

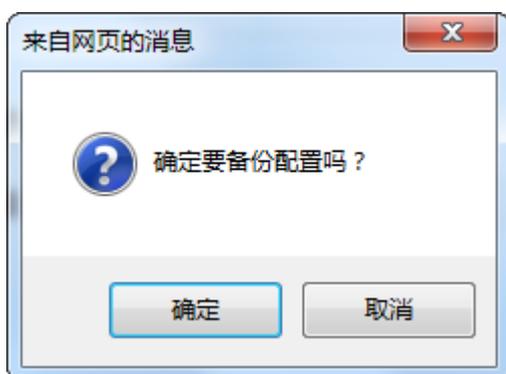
1. 进入「系统工具」>「设备维护」页面。
2. 点击 **备份/恢复**。



3. 点击 **备份**。



4. 确认提示信息后，点击 **确定**。

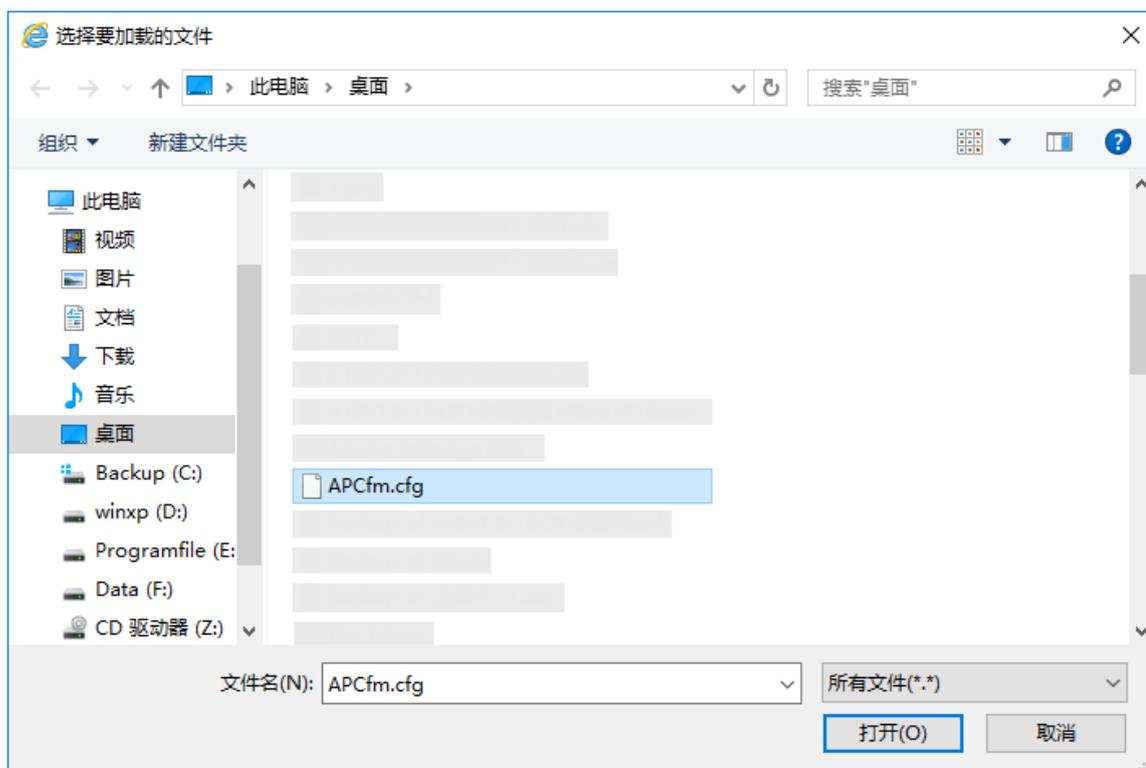


----完成

浏览器将下载文件名为 APCfm.cfg 的配置文件。

## 恢复

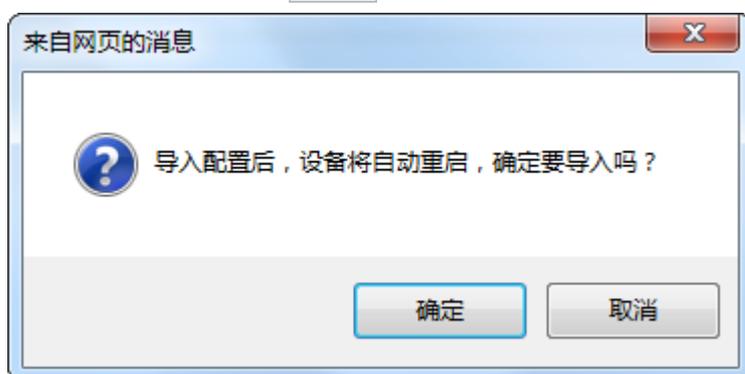
1. 进入「系统工具」>「设备维护」页面。
2. 点击 **浏览...**，选择并加载之前备份的配置文件。



3. 点击 **恢复**。



4. 确认提示信息后，点击 **确定**。



----完成

页面会出现重启进度条，请耐心等待。进度条走完后，网桥恢复配置成功。

## 9.3 管理员

进入页面：点击「系统工具」>「管理员」。

在这里，您可以修改网桥管理页面的登录账号信息，以防止非授权用户进入网桥的管理页面更改设置，影响无线网络正常使用。

点击  可以修改账号信息。



### 9.3.1 管理员

使用管理员账号登录到网桥后，可以查看、修改网桥的配置。

原用户名	<input type="text" value="admin"/>
原密码	<input type="password"/>
新用户名	<input type="text"/>
新密码	<input type="password"/>
确认新密码	<input type="password"/>

## 9.3.2 访客

使用访客账号登录网桥后，您只能查看网桥配置信息，不能修改网桥配置。

**访客** ✕

原用户名

原密码

新用户名

新密码

确认新密码

### 参数说明

标题项	说明
原用户名	当前登录用户名。 默认情况下，网桥有一个管理员账号，一个普通用户账号。其中，管理员的用户名和密码均为“admin”，普通用户的用户名和密码均为“user”。
原密码	当前登录用户名。
新用户名	设置新的登录用户名。
新密码	设置新的登录用密码。
确认新密码	再一次输入新密码。

## 9.4 系统日志

进入页面：点击「系统工具」>「系统日志」。

网桥的系统日志记录了系统启动后出现的各种情况及用户对网桥的操作记录，若遇网络故障，可以利用网桥的系统日志信息进行问题排查。



The screenshot shows the 'System Log' (系统日志) interface. At the top right, it indicates 'Current Mode: AP Mode' (当前模式: AP模式). Below the title, there are 'Refresh' (刷新) and 'Clear' (清除) buttons, and a 'Log Type' (日志类型) dropdown menu set to 'All' (全部). A red question mark icon is visible in the top right corner. The main content is a table with the following data:

序号	时间	类型	日志内容
1	2018-03-28 13:50:31	system	web 192.168.2.23 login
2	2018-03-28 13:50:23	system	web login time expired
3	2018-03-28 11:13:25	system	2.4GHz WiFi(wlan0) up
4	2018-03-28 11:13:19	system	2.4GHz WiFi(wlan0) down

日志记录时间以网桥的系统时间为准，请确保网桥的系统时间准确。您可以到「系统工具」>「时间与日期」页面校准网桥的系统时间。

如果要查看网桥最新的日志信息，请点击 **刷新**；如果要清空页面显示的日志信息，请点击 **清除**。

### 注意

- 网桥重启后，重启之前的日志信息将丢失。
- 断电后重新上电、配置 VLAN、软件升级、恢复配置、恢复出厂设置等操作都会导致网桥重启。

# 附录

## 常见问题解答

### 问 1：网桥的指示灯不亮，怎么办？

请尝试使用以下办法解决：

- 确认网桥的 PoE/LAN 口与 PoE 注入器的 PoE 口连接正常。
- 确认用来连接网桥 PoE/LAN 口和 PoE 注入器的 PoE 口的网线是八芯网线。
- 如果是通过 DC 供电，请确保电源适配器接触良好。

### 问 2：无法登录到网桥的管理页面，怎么办？

请尝试使用以下办法解决：

- 确认电脑的 IP 地址与网桥的 IP 地址在同一网段。如：网桥的 IP 地址为 192.168.2.1，则电脑的 IP 地址可设为 192.168.2.X ( X 为 2~253 )。
- 确认已在浏览器地址栏（非搜索栏）输入网桥的 IP 地址（默认为 192.168.2.1）。
- 若网络中接了多台网桥，请务必在配置每一台时都修改它的 IP 地址，避免 IP 地址冲突导致无法登录另外的网桥的管理页面。
- 将网桥恢复出厂设置再登录。

### 问 3：连接网桥后，电脑出现“IP 地址与网络上的其他系统有冲突”提示信息，怎么办？

请尝试使用以下办法解决：

- 确认局域网内的电脑没有占用网桥的 IP 地址，网桥出厂默认的 IP 地址是 192.168.2.1。
- 确认局域网内为电脑静态设置的 IP 地址没有被其它电脑使用。

### 问 4：不能登录网桥管理页面的情况下，怎么将网桥恢复出厂设置？

请在网桥正常运行时，按住 Reset 按钮 7 秒后松开，指示灯全亮时，网桥已经恢复到出厂状态。

## 默认参数

出厂时，网桥的各项参数默认设置如下表。

参数		默认设置	
设备登录	管理 IP	192.168.2.1	
	用户名 密码	管理员	admin admin
		访客	user user
快速设置	工作模式	AP 模式	
LAN 口设置	IP 获取方式	静态 IP	
	IP 地址	192.168.2.1	
	子网掩码	255.255.255.0	
	默认网关	192.168.2.254	
	首选 DNS 服务器	8.8.8.8	
	备用 DNS 服务器	8.8.4.4	
	设备名称	CPE3V1.0	
DHCP 服务器	DHCP 服务器	启用	
	起始 IP 地址	192.168.2.100	
	结束 IP 地址	192.168.2.200	
	子网掩码	255.255.255.0	
	网关地址	192.168.2.254	
	首选 DNS 服务器	8.8.8.8	
	备用 DNS 服务器	8.8.4.4	
VLAN 设置	租约时间	1 天	
	VLAN 设置	禁用	
	管理 VLAN	1	
无线—基本设置	WLAN	1000	
	无线状态	开启	
	国家或地区	中国	
	SSID	IP-COM_XXXXXX。XXXXXX 为网桥 LAN 口 MAC 后六位	
	SSID 广播	启用	
	网络模式	11b/g/n	

参数		默认设置
	信道	自动
	发射功率	20dBm
	信道带宽	20MHz
	传输速率	自动
	安全模式	不加密
	客户端隔离	禁用
	最大客户端数量	16
无线设置—高级设置	WMM	启用
	APSD	禁用
	接入信号强度限制	禁用
	无线前导码	长导码
	信号接收能力	级别 4
	Beacon 间隔	100ms
	Fragment 阈值	2346
	RTS 门限	2347
	DTIM 间隔	1
	LED1 指示灯信号强度	-90dBm
LED2 指示灯信号强度	-80dBm	
LED3 指示灯信号强度	-70dBm	
无线设置—访问控制		禁用
LAN 口速率		自动协商
网络诊断		禁用
网络服务	定时重启	禁用
	WEB 闲置超时时间	5 分钟
	SNMP 代理	禁用
	Ping 看门狗	禁用
	Telnet 服务	禁用
	UPnP	启用
系统工具	时间与日期	网络校时

参数	默认设置
	时区：( GMT+08:00 ) 北京，重庆，乌鲁木齐，香港特别行政区，台北 校时周期：30 分钟