www.ip-com.com.cn

Web 配置指南

IP-COM 室外网桥

IP-COM
无线网络解决方案专家

声明

版权所有©2020 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、摘抄及翻译本文档部分或全部内容，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，本文档内容会不定期更新。除非另有约定，本文档仅作为使用指导，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，请先阅读本手册。

本配置指南适用于 IP-COM 室外网桥，具体产品图和软件截图以实物为准。文中如无特别说明，均以 CPE12V1.0 为例。

约定

本文可能用到的格式说明如下。

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

本文可能用到的标识说明如下。

标识	含义
	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。
	表示有助于节省时间或资源的方法。

缩略语

缩略语	全称
AES	高级加密标准（Advanced Encryption Standard）
AP	接入点（Access Point）
ARP	地址解析协议（Address Resolution Protocol）
CCQ	客户端链接质量（Client Connection Quality）
CPE	客户终端设备（Customer Premises Equipment）
DHCP	动态主机配置协议（Dynamic Host Configuration Protocol）
DNS	域名系统（Domain Name System）
GMT	格林威治时间（Greenwich Mean Time）
ICMP	网际控制报文协议（Internet Control Message Protocol）

缩略语	全称
IP	网际协议（Internet Protocol）
TKIP	临时密钥完整性协议（Temporal Key Integrity Protocol）
LAN	局域网（Local Area Network）
MAC	媒体接入控制（Medium Access Control）
P2MP	点到多点（Point-to-Multi-Point）
PoE	以太网供电（Power Over Ethernet）
PVID	端口的虚拟局域网 ID 号（Port-based VLAN Identifier）
RADIUS	远程用户拨号认证服务（Remote Authentication Dial In User Service）
SSID	服务集标识符（Service Set Identifier）
TCP	传输控制协议（Transmission Control Protocol）
UDP	用户数据报协议（User Datagram Protocol）
VLAN	虚拟局域网（Virtual Local Area Network）
WAN	广域网（Wide Area Network）
WEP	有线等效保密字段（Wired Equivalent Privacy）
WLAN	无线局域网（Wireless Local Area Network）
WMM	无线多媒体（Wi-Fi Multi-media）
WPA	Wi-Fi 网络安全接入（Wi-Fi Protected Access）
WPA-PSK	WPA 预共享密钥（WPA-Preshared Key）

相关资料获取方式

访问 IP-COM 官方网站：www.ip-com.com.cn，搜索对应产品型号，可获取最新的产品资料。

产品资料一览表

文档名称	描述
快速安装指南	帮助您快速设置网桥联网。包括网桥的上网设置指导、指示灯/接口/按钮说明、常见问题解答、保修条款等。
Web 配置指南	帮助您了解网桥的更多功能配置。包括网桥 Web 界面上的所有功能介绍。
产品彩页	帮助您了解网桥的基本参数。包括产品概述、产品卖点、产品规格等。

技术支持

如需了解更多信息，请通过以下方式与我们联系。

40066-50066	ip-com@ip-com.com.cn	www.ip-com.com.cn

目录

1 典型应用场景 1

1.1 小区电梯监控 1

1.1.1 方案 1

1.1.2 设置网桥 2

1.1.3 安装网桥 10

1.2 小区、学校、工厂、塔吊、果园、养殖场监控 12

1.2.1 方案 12

1.2.2 设置网桥 12

1.2.3 安装网桥 14

1.3 农业监测数据回传 16

1.3.1 方案 16

1.3.2 设置网桥 16

1.3.3 安装网桥 16

2 登录 Web 管理界面 18

2.1 登录 18

2.2 退出登录 20

3 Web 界面简介 21

3.1 页面布局 21

3.2 常用元素 22

4 快速设置 23

4.1 概述 23

4.2 AP 模式 24

4.2.1 应用场景 24
4.2.2 设置 AP 模式 24
4.3 客户端模式 26
4.3.1 应用场景 26
4.3.2 设置客户端模式 26
4.4 万能中继模式 29
4.4.1 应用场景 29
4.4.2 设置万能中继模式 29
4.5 无线 WAN 模式 32
4.5.1 应用场景 32
4.5.2 设置无线 WAN 模式 32
4.6 中继模式 36
4.6.1 应用场景 36
4.6.2 设置中继模式 36
4.7 P2MP 模式 45
4.7.1 应用场景 45
4.7.2 设置 P2MP 模式 45
4.8 路由模式 51
4.8.1 应用场景 51
4.8.2 设置路由模式 51
5 状态 54
5.1 系统状态 54
5.2 无线状态 57
5.3 统计 59
5.3.1 吞吐量 59
5.3.2 无线客户端 59
5.3.3 上级 AP 60
5.3.4 接口 61

5.3.5 ARP 表 61
5.3.6 路由表 62
6 网络设置 63
6.1 LAN 口设置 63
6.1.1 概述 63
6.1.2 修改 LAN IP 地址 64
6.2 MAC 克隆 67
6.2.1 概述 67
6.2.2 克隆 MAC 地址 67
6.3 DHCP 服务器 69
6.3.1 概述 69
6.3.2 配置 DHCP 服务器 69
6.4 DHCP 客户端列表 71
6.5 VLAN 设置 72
6.5.1 概述 72
6.5.2 配置 VLAN（以 CPE6SV1.0 为例） 72
6.5.3 VLAN 设置举例（以 CPE12V1.0 为例） 73
7 无线设置 76
7.1 基本设置 76
7.1.1 概述 76
7.1.2 修改基本设置 77
7.1.3 基本设置举例 83
7.2 高级设置 100
7.3 访问控制 103
7.3.1 概述 103
7.3.2 配置访问控制 103
7.3.3 访问控制配置举例 104
8 高级设置 106

8.1 LAN 口速率 106
8.2 网络诊断 107
8.2.1 扫描信号 107
8.2.2 Ping 108
8.2.3 Traceroute 109
8.2.4 速率测试 110
8.2.5 频谱分析 113
8.3 带宽控制 115
8.3.1 概述 115
8.3.2 带宽控制配置举例 116
8.4 端口映射 118
8.4.1 概述 118
8.4.2 端口映射配置举例 119
8.5 MAC 过滤 122
8.5.1 概述 122
8.5.2 MAC 过滤配置举例 123
8.6 网络服务 125
8.6.1 动态 DNS 125
8.6.2 远程 WEB 管理 129
8.6.3 定时重启 131
8.6.4 WEB 闲置超时时间 131
8.6.5 SNMP 代理 132
8.6.6 Ping 看门狗 135
8.6.7 DMZ 主机 136
8.6.8 Telnet 服务 139
8.6.9 UPnP 服务 139
8.6.10 硬件看门狗 140
8.6.11 STP 140
9 系统工具 141

9.1 时间与日期 141
9.1.1 网络校时 141
9.1.2 手动设置时间 142
9.2 设备维护 143
9.2.1 重启 143
9.2.2 恢复出厂设置 144
9.2.3 软件升级 145
9.2.4 备份与恢复 146
9.3 用户名与密码 150
9.3.1 管理员 150
9.3.2 访客 151
9.4 系统日志 152
附录 153

1 典型应用场景

提示

- 不同的应用场景所需要的网桥型号不同，更多信息请访问 www.ip-com.com.cn。
- 1 个网桥可以带多个摄像头，具体的摄像头个数可以通过公式计算：摄像头个数=网桥发送/接收速率 ÷ 摄像头码流

1.1 小区电梯监控

某小区为保障住户的人身和财产安全，需要在电梯内安装监控摄像头进行实时监控。

1.1.1 方案

使用无线网桥搭建监控网络，下文以 CPE12V1.0 为例。

您只需两步：设置网桥 > 安装网桥，即可轻松实现小区电梯监控。

提示

为方便您快速搭建监控网络，建议先设置网桥，再安装网桥。

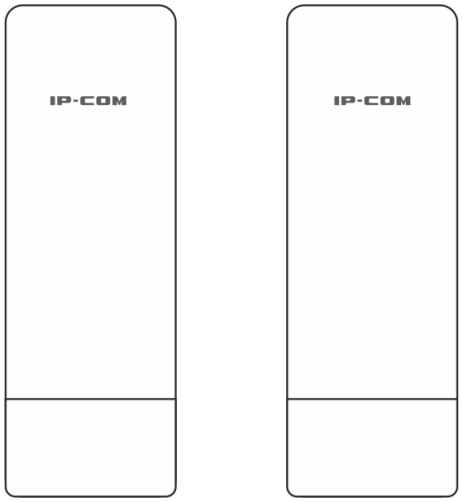
1.1.2 设置网桥

方式一：自动桥接（推荐）

注意

- 自动桥接仅对处于出厂状态的网桥生效。
- 电梯监控场景一般使用 2 个网桥进行桥接。进行 1 对 1 自动桥接时，请确保近距离内有且只有 2 台同时通电且处于出厂状态的网桥。否则会导致自动桥接失败。
- 桥接成功后，网桥的 DHCP 服务都自动关闭。工作在 AP 模式的网桥的 IP 地址不变（192.168.2.1），工作在客户端模式的网桥的 IP 地址变为 192.168.2.2。

1. 将两台网桥相邻放置，如下图所示。



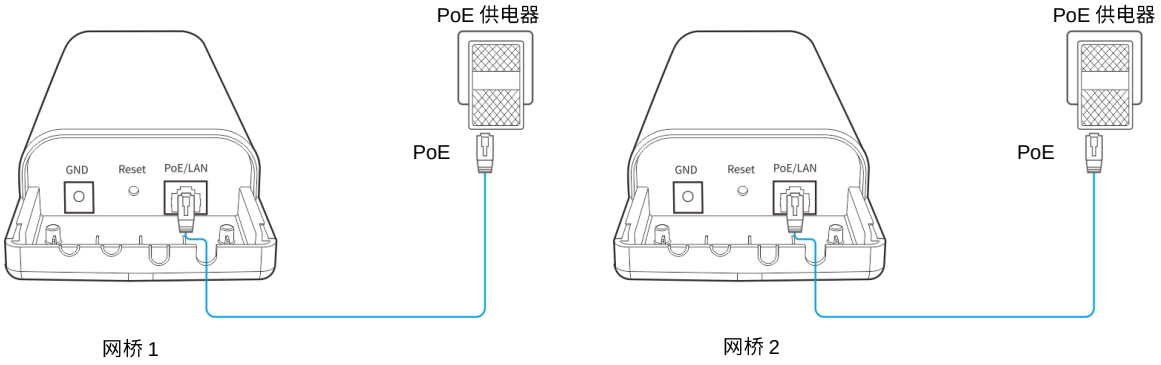
网桥 1　　网桥 2

2. 打开网桥的保护盖，用网线（推荐使用超 5 类或以上网线，网线长度≤60 米）将网桥的 PoE/LAN 口连接到 PoE 供电器的 PoE 口。

3. 将 PoE 供电器连接到电源插座。网桥的 PoE/LAN 灯亮。

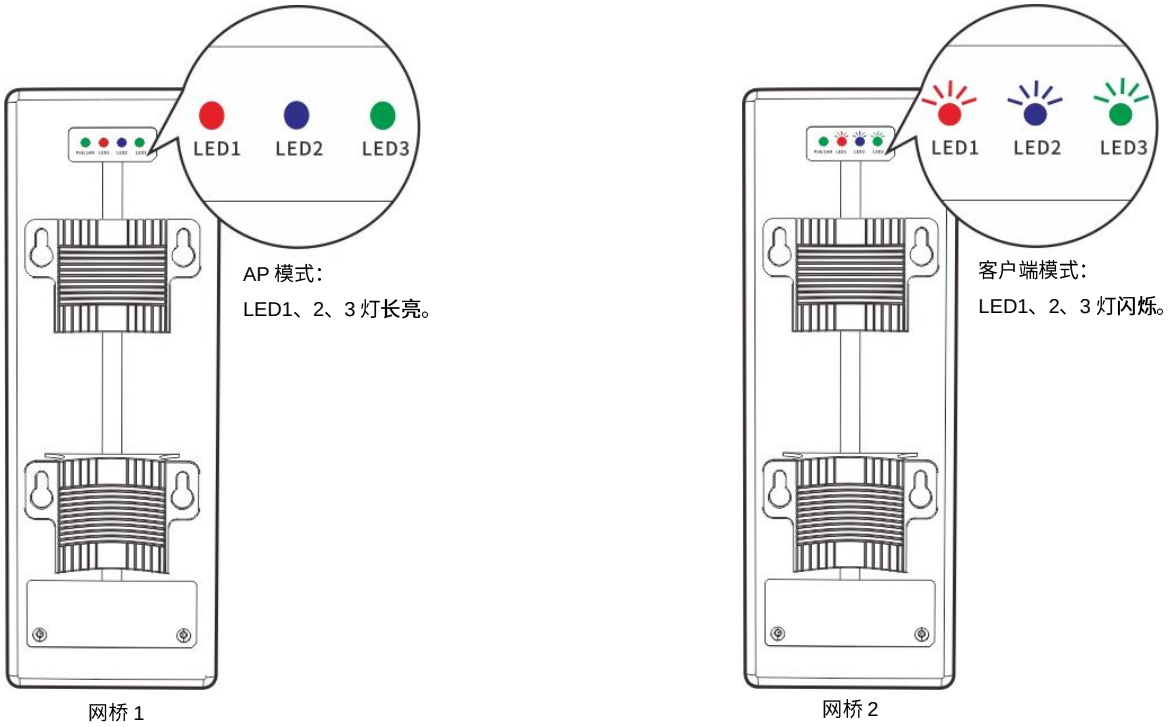
提示

- 如果网桥支持 DC 供电，使用包装盒内的电源适配器可以给网桥进行 DC 供电。
- 各网桥所支持的 PoE 供电距离以实际为准。



----完成

等待两台网桥自动进行桥接。当一台网桥的 LED1、2、3 灯呈长亮状态，另一台网桥的 LED1、2、3 灯保持闪烁状态时，1 对 1 自动桥接成功。

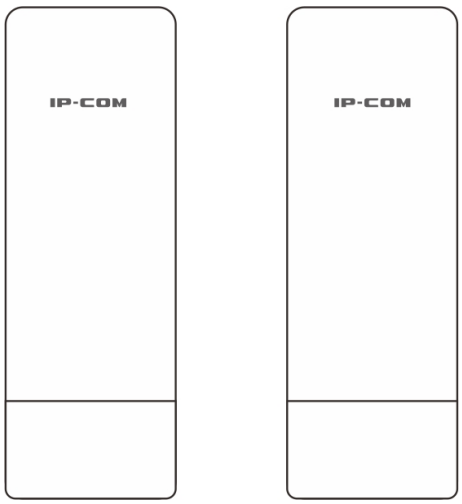


提示

如果 1 对 1 自动桥接失败，请将 2 台网桥均恢复出厂设置，然后重新尝试。恢复出厂设置方法：请在网桥正常运行时，按住 Reset 按钮 8 秒后松开，当指示灯全亮再熄灭时，网桥恢复出厂设置成功。

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 供电器供电为例）

(1) 打开网桥的保护盖。

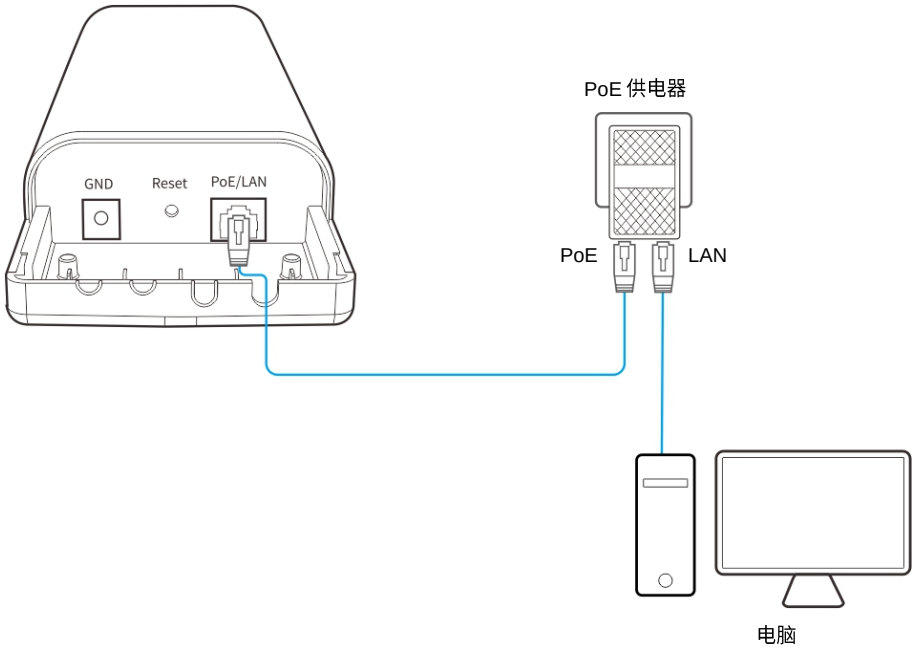
(2) 用网线（推荐使用超 5 类或以上网线，网线长度≤60 米）将网桥的 PoE/LAN 口连接到 PoE 供电器的 PoE 口。

(3) 将 PoE 供电器连接到电源插座。网桥的 PoE/LAN 灯亮。

(4) 用网线将电脑连接到 PoE 供电器的 LAN 口。

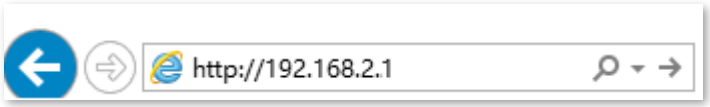
提示

各网桥所支持的 PoE 供电距离以实际为准。



3. 设置第 1 个网桥为 AP 模式。

(1) 打开电脑上的浏览器，在地址栏（非搜索栏）输入 **192.168.2.1**，按键盘上的 Enter（或 Return）键。



(2) 输入用户名和密码，点击 登录。

提示

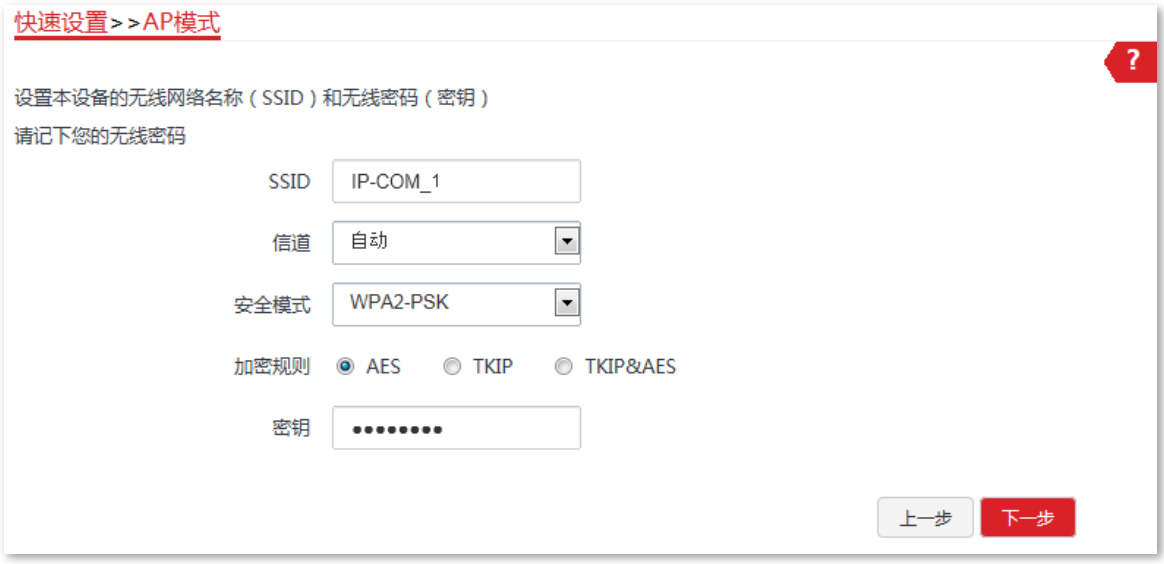
若未出现上述页面，请尝试使用以下办法解决：

- 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 2~254，且未被其他设备占用）。
- 将网桥恢复出厂设置再登录。恢复出厂设置方法：请在网桥正常运行时，按住 Reset 按钮 8 秒后松开，当指示灯全亮再熄灭时，网桥恢复出厂设置成功。

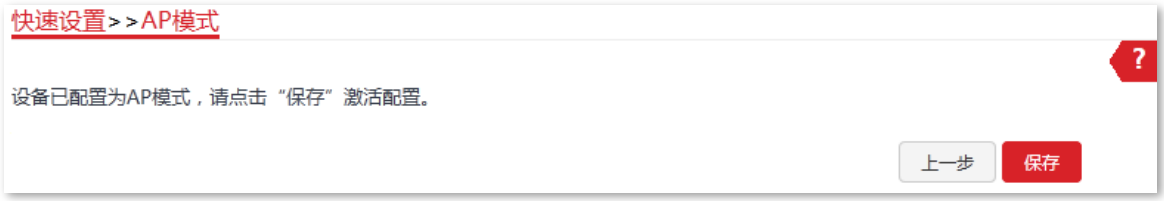
(3) 进入「快速设置」页面，选择 **AP 模式**，点击 下一步。

(4) 设置网桥的无线网络参数，然后点击 下一步 。

- 修改无线网络名称（SSID），如“IP-COM_1”。
- 选择无线工作的信道。
- 选择“安全模式”，建议为“WPA2-PSK”。
- 选择“加密规则”，建议为“AES”。
- 设置密钥（无线密码）。



(5) 点击 保存 ，等待网桥自动重启使设置生效。



4. 连接第 2 个网桥。（以 PoE 供电器供电为例）

(1) 打开网桥的保护盖。

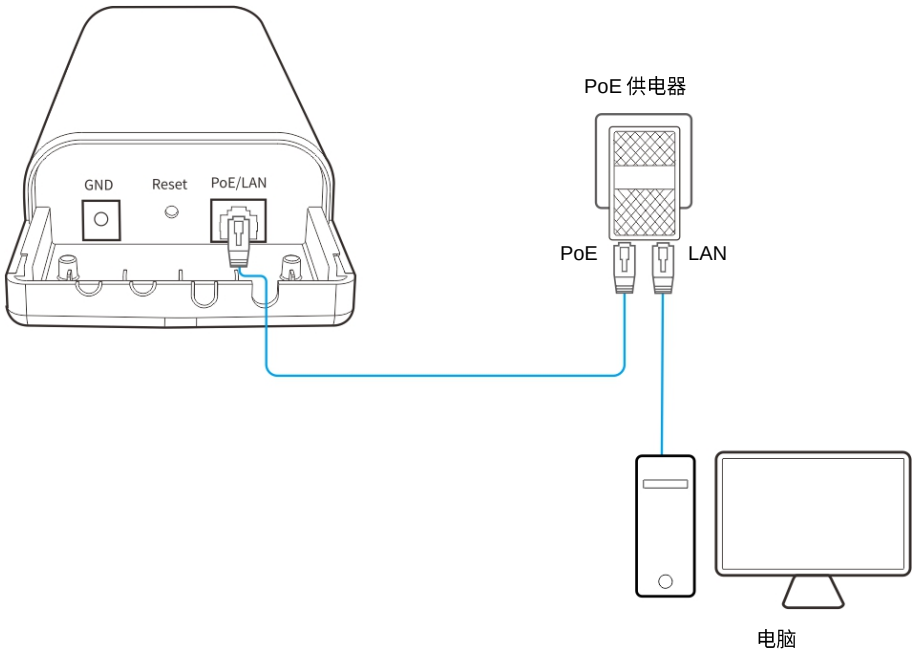
(2) 用网线（推荐使用超 5 类或以上网线，网线长度≤60 米）将网桥的 PoE/LAN 口连接到 PoE 供电器的 PoE 口。

(3) 将 PoE 供电器连接到电源插座。网桥的 PoE/LAN 灯亮。

(4) 用网线将电脑连接到 PoE 供电器的 LAN 口。

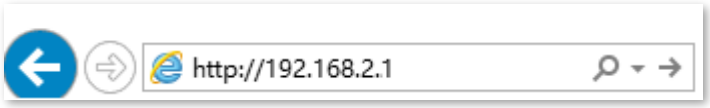
提示

各网桥所支持的 PoE 供电距离以实际为准。



5. 设置第 2 个网桥为客户端模式。

(1) 打开电脑上的浏览器，在地址栏（非搜索栏）输入 **192.168.2.1**，按键盘上的 Enter（或 Return）键。



(2) 输入用户名和密码，点击 登录 。

提示

若未出现上述页面，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 2~254，且未被其他设备占用）。
- 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，避免因 IP 地址冲突而无法登录其他网桥的管理页面。
- 将网桥恢复出厂设置再登录。恢复出厂设置方法：请在网桥正常运行时，按住 Reset 按钮 8 秒后松开，当指示灯全亮再熄灭时，网桥恢复出厂设置成功。

(3) 选择**客户端模式**，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 。

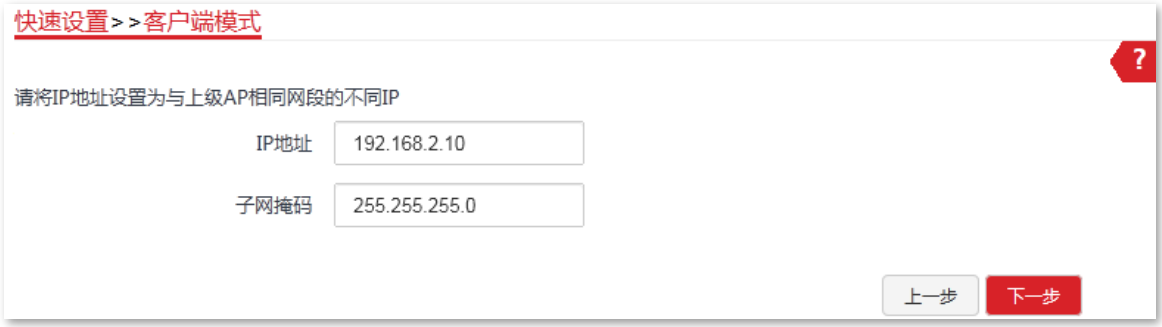
提示

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。

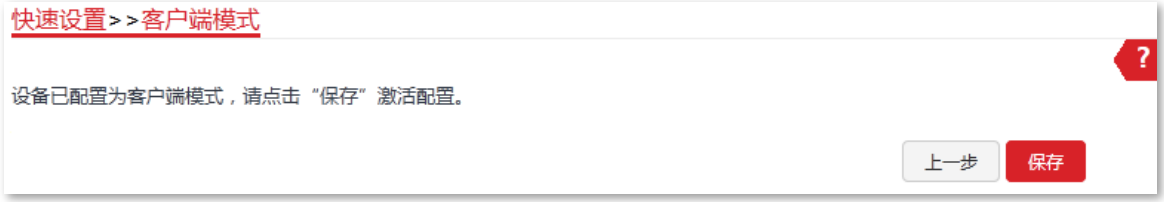
(6) 输入上级无线网络的密钥，点击 下一步 。

(7) 修改 IP 地址信息，然后点击 下一步。

- 将本网桥 IP 地址设置为与第一个网桥的 IP 地址在同一网段的其他 IP 地址，如“192.168.2.10”。
- 将“子网掩码”设置为与上级 AP 的子网掩码一致。



(8) 点击 保存，等待网桥自动重启使设置生效。



----完成

当第 1 个网桥的 LED1、LED2、LED3 长亮，第 2 个网桥的 LED1、LED2、LED3 保持闪烁状态时，桥接成功。

如果需要进行 1 对多桥接，请登录其他网桥，参考步骤 4~5，设置其工作在客户端模式桥接第 1 个网桥的无线网络，依次类推。

提示

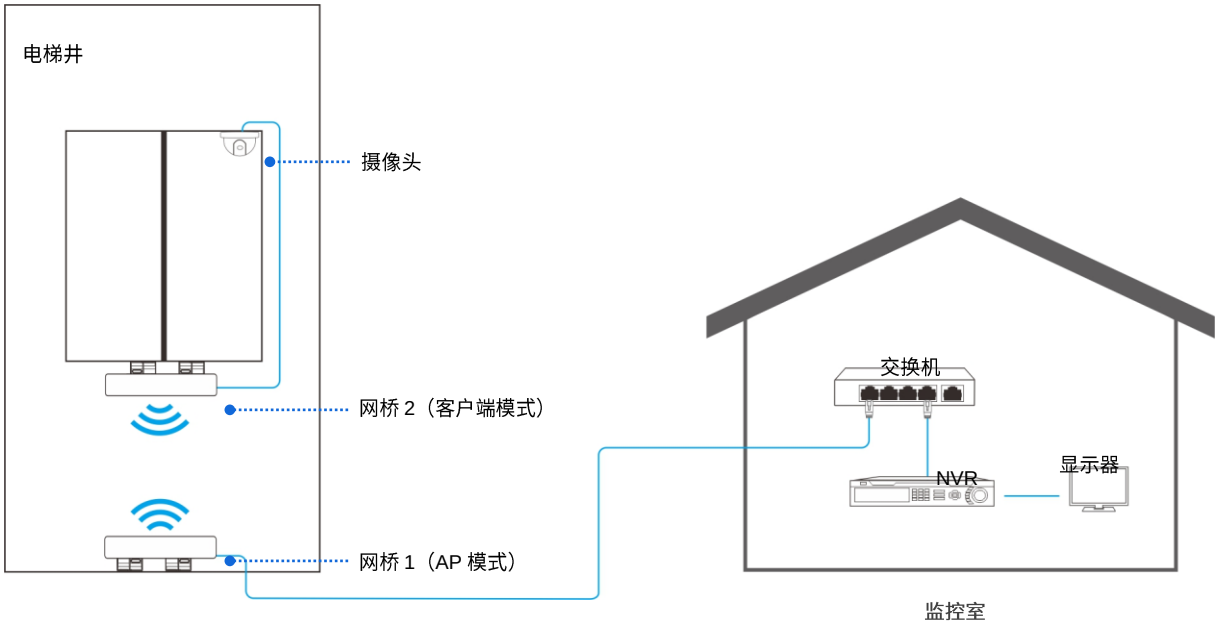
如果需要查看网桥的 SSID 和密钥，可登录到网桥管理页面，进入「无线设置」>「基本设置」页面查看。

1.1.3 安装网桥

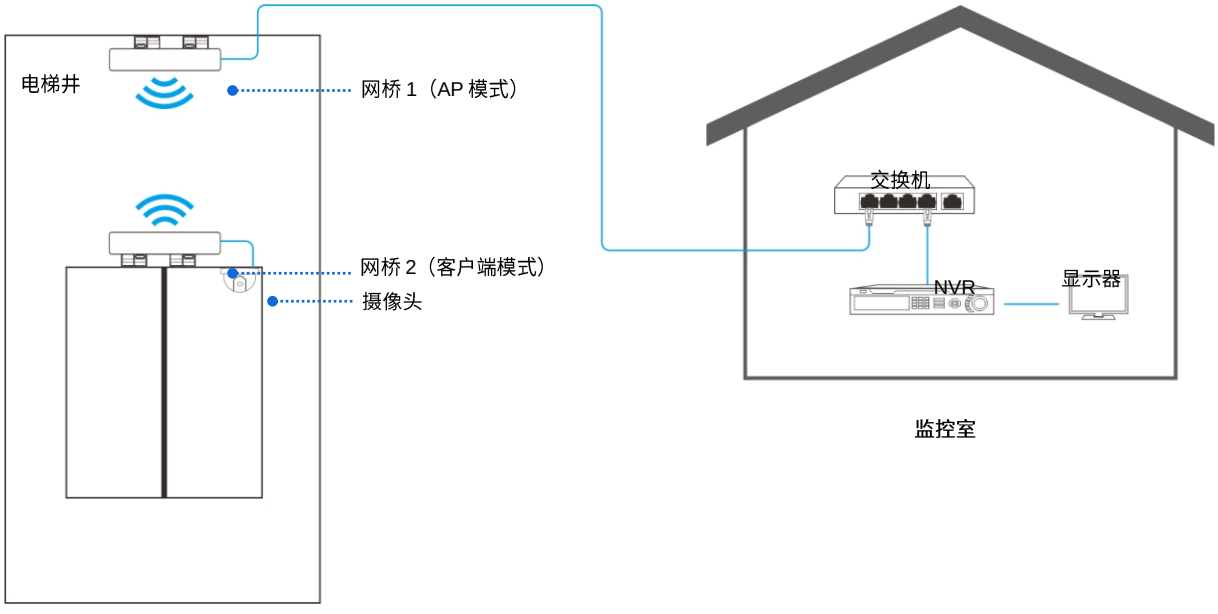
根据机房的位置选择以下任一场景将网桥安装到相应位置。

机房位置距离电梯井**底部**位置更近时，请参考场景 1 安装。

机房位置距离电梯井**顶部**位置更近时，请参考场景 2 安装。

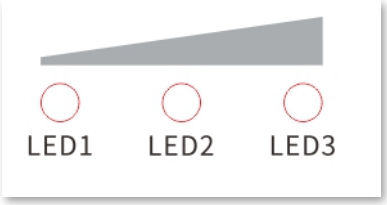


场景 1



场景 2

您可以根据指示灯检查网桥安装位置是否合适。当网桥的 LED1、LED2、LED3 灯长亮或闪烁时，桥接信号最好，安装位置最佳。

指示灯	状态	说明
LED1、LED2、LED3 （接收信号强度指示灯）	长亮/闪烁	有设备已连接到网桥。 – 长亮：网桥当前可能工作在 AP 模式、中继模式、P2MP 模式或路由模式。 – 闪烁：网桥当前可能工作在客户端模式、万能中继模式或无线 WAN 模式。 每个 LED 灯对应一个无线信号强度值，当网桥接收到的对端无线信号强度达到点亮值时，相应的 LED 灯亮起。您可以根据 LED 灯点亮情况，判断无线连接质量。默认情况下，各 LED 灯的点亮值如下。 -90dBm -80dBm -70dBm  您可以在网桥管理页面的「无线设置」>「高级设置」页面修改 LED 灯点亮值。
	熄灭	没有设备连接，或接收信号强度小于 LED 灯亮起的最小值（默认为 -90dBm）。

1.2 小区、学校、工厂、塔吊、果园、养殖场监控

此处以塔吊监控为例。

某一建筑工地为了保障人员的生命财产安全，需要对塔吊使用过程进行有效监控。

1.2.1 方案

使用无线网桥搭建监控网络，下文以 CPE12V1.0 为例。

您只需两步：设置网桥 > 安装网桥，即可轻松实现塔吊监控。

提示

为方便您快速搭建监控网络，建议先设置网桥，再安装网桥。

1.2.2 设置网桥

方式一：自动桥接（推荐）

场景一：1 对 1 自动桥接

设置步骤请参考方式一：自动桥接（推荐）。

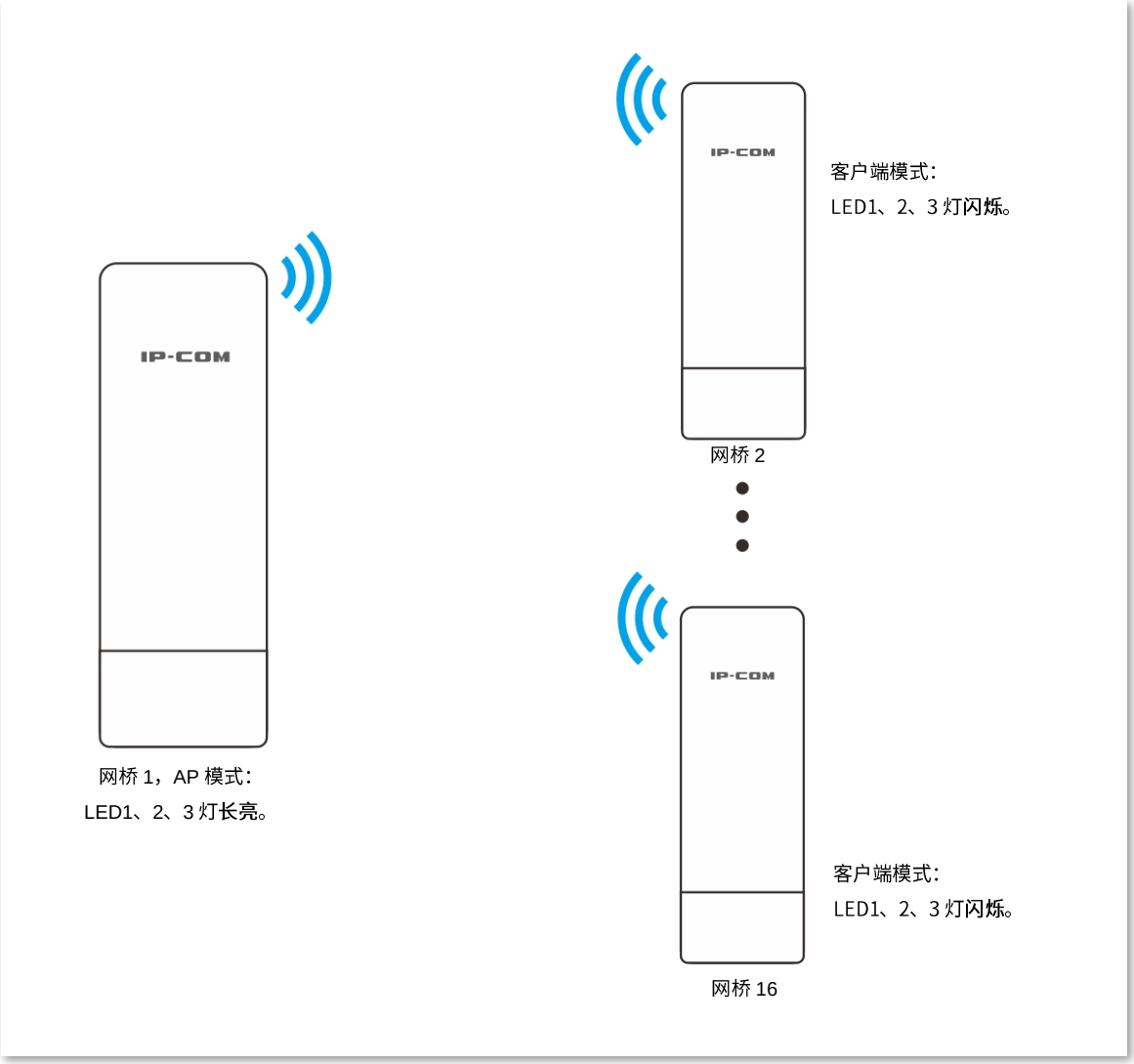
场景二：1 对多自动桥接

注意

- 自动桥接仅对处于出厂状态的网桥生效。
- 进行 1 对多自动桥接需要先将 2 台网桥进行 1 对 1 自动桥接，在桥接成功后的 30 分钟内将其他待配置网桥上电。
- 1 对多自动桥接中，1 台网桥最多能桥接 15 台网桥。
- 桥接成功后，网桥的 DHCP 服务都自动关闭。工作在 AP 模式的网桥的 IP 地址不变（192.168.2.1），工作在客户端模式的网桥的 IP 地址变为 192.168.2.2。
- 如果要批量修改网桥 IP 地址，请访问 www.ip-com.com.cn，搜索对应产品型号，在其详情页下载网桥管理软件。

1. 参考方式一：自动桥接（推荐）的设置步骤，将任意 2 台网桥进行自动桥接。
2. 在 1 对 1 桥接成功后的 **30 分钟**内，将**剩余所有**处于出厂状态的网桥放在指示灯 LED1、LED2、LED3 灯长亮的网桥附近并上电。

大约 1 分钟后，当新增网桥的 LED1、LED2、LED3 灯保持闪烁状态时，表示 1 对多自动桥接成功。



提示

- 如果新增网桥上电 1 分钟后，LED1、2、3 灯由闪烁变为熄灭，表示桥接失败，请将该网桥恢复出厂设置，等待 LED1、2、3 灯保持在闪烁状态。
- 使用 CPE6 进行一对多桥接时，1 对 1 桥接成功后，请在**3 分钟**内将**剩余所有**处于出厂状态的网桥放在指示灯 LED1、LED2、LED3 灯长亮的网桥附近并上电。
- 如果仍然桥接失败，请手动桥接，详情请参考设置客户端模式。

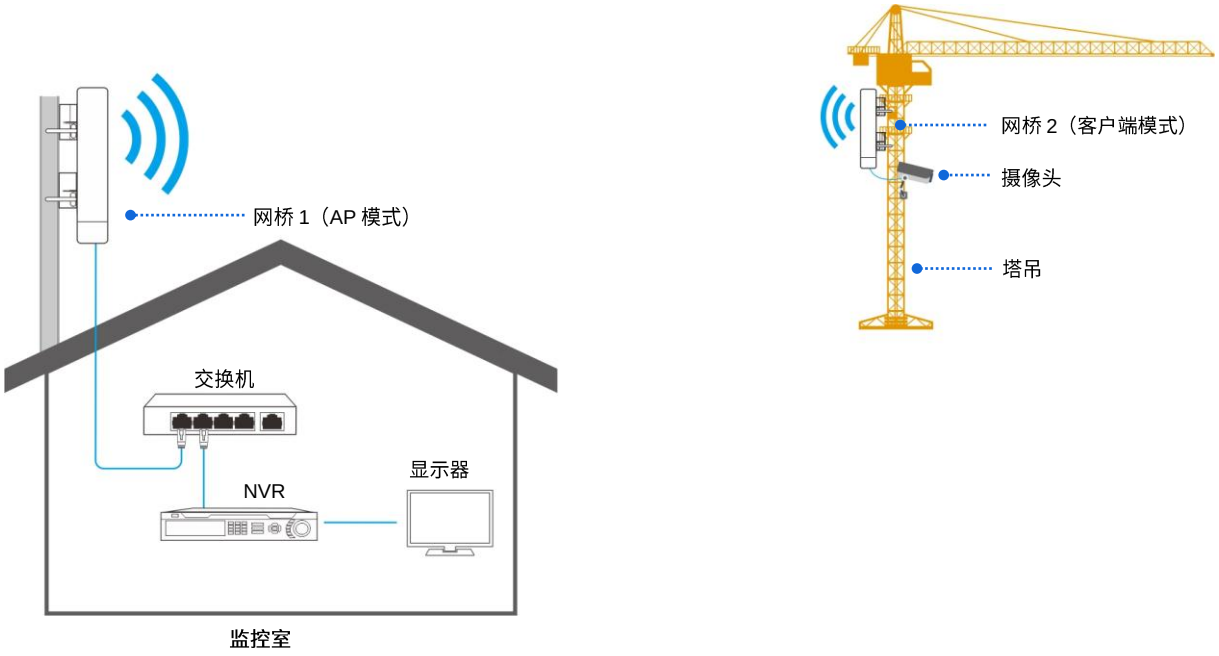
方式二：手动桥接

设置步骤请参考方式二：手动桥接。

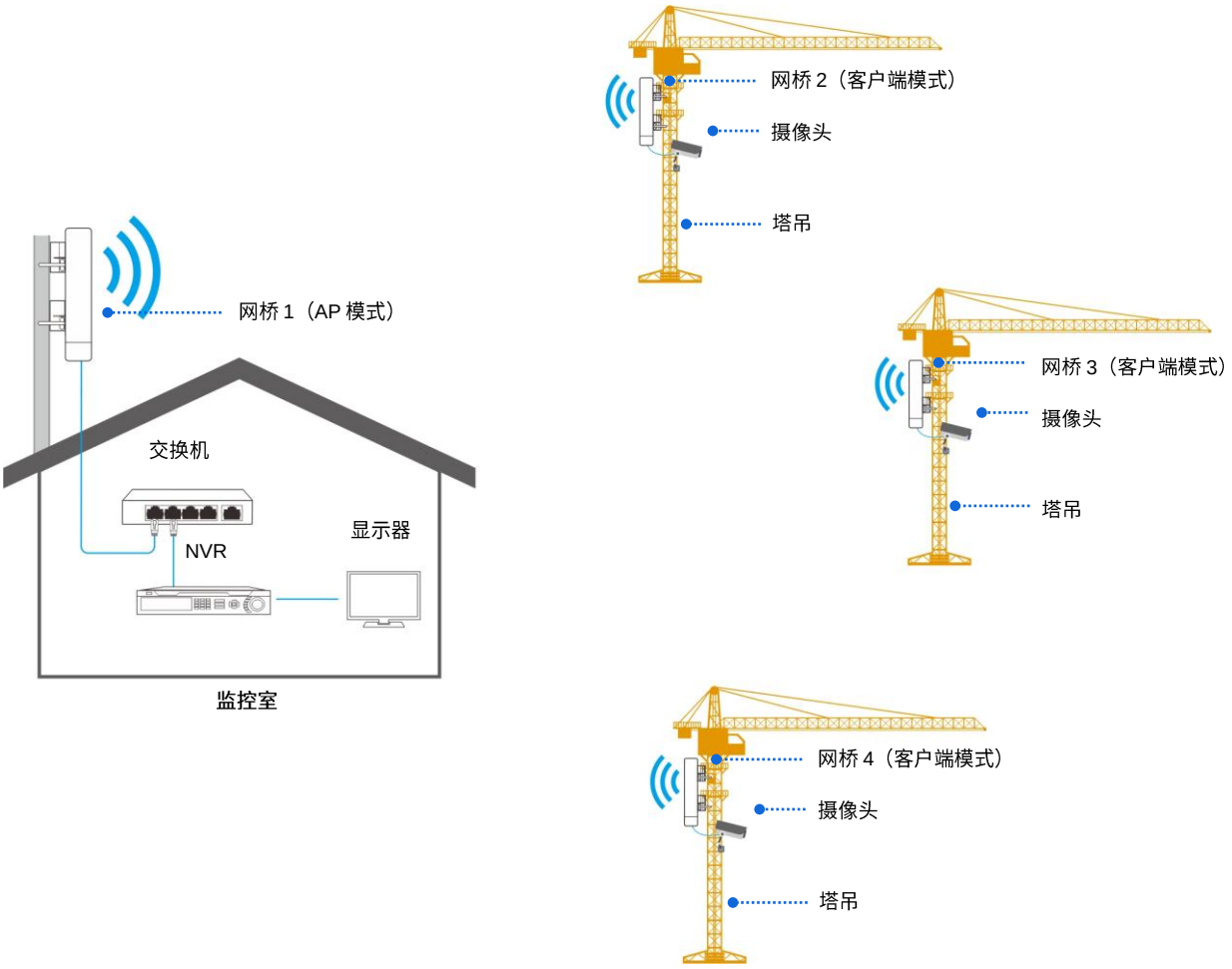
1.2.3 安装网桥

将网桥安装到相应位置。

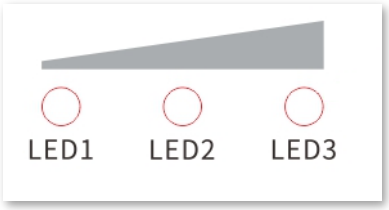
1 对 1 桥接安装场景图：



1 对多桥接安装场景图（以 1 对 3 桥接为例）：



您可以根据指示灯检查网桥安装位置是否合适。当网桥的 LED1、LED2、LED3 灯长亮或闪烁时，桥接信号最好，安装位置最佳。

指示灯	状态	说明
LED1、LED2、LED3 （接收信号强度指示灯）	长亮/闪烁	有设备已连接到网桥。 – 长亮：网桥当前可能工作在 AP 模式、中继模式、P2MP 模式或路由模式。 – 闪烁：网桥当前可能工作在客户端模式、万能中继模式或无线 WAN 模式。 每个 LED 灯对应一个无线信号强度值，当网桥接收到的对端无线信号强度达到点亮值时，相应的 LED 灯亮起。您可以根据 LED 灯点亮情况，判断无线连接质量。默认情况下，各 LED 灯的点亮值如下。 -90dBm -80dBm -70dBm  您可以在网桥管理页面的「无线设置」>「高级设置」页面修改 LED 灯点亮值。
	熄灭	没有设备连接，或接收信号强度小于 LED 灯亮起的最小值（默认为 -90dBm）。

1.3 农业监测数据回传

为实现“智能农业”和“精准农业”，促进现代农业的升级，某研究中心需要实时查看前端收集的关于农作物生长环境信息，包括气候、土壤、水质等。

1.3.1 方案

使用无线网桥搭建无线传输网络，下文以 O9V1.0 为例。

您只需两步：设置网桥、安装网桥，即可轻松实现农业监控。

提示

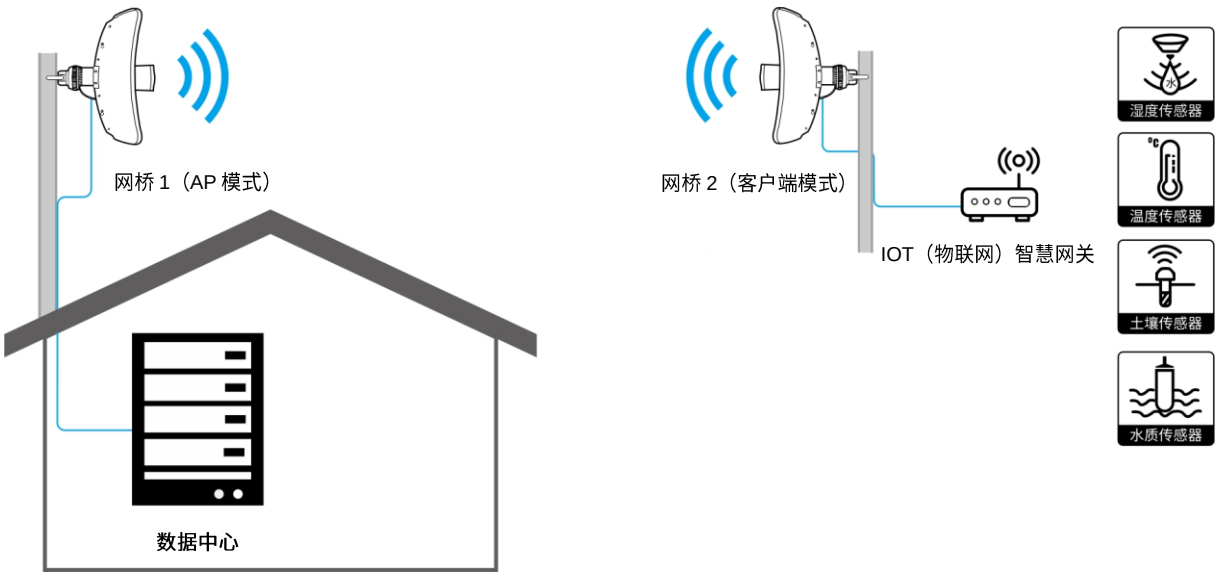
为方便您快速搭建监控网络，建议先设置网桥，再安装网桥。

1.3.2 设置网桥

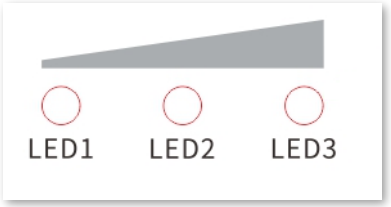
设置步骤请参考方式一：自动桥接（推荐）。

1.3.3 安装网桥

将网桥安装到相应位置，拓扑图如下。



您可以根据指示灯检查网桥安装位置是否合适。当网桥的 LED1、LED2、LED3 灯长亮或闪烁时，桥接信号最好，安装位置最佳。

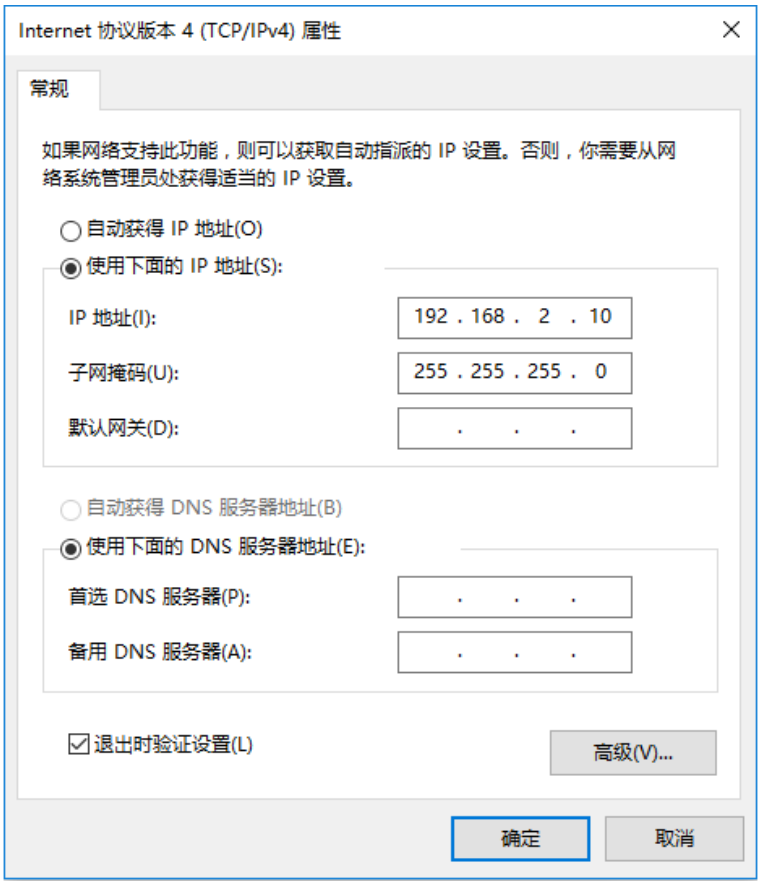
指示灯	状态	说明
LED1、LED2、LED3 （接收信号强度指示灯）	长亮/闪烁	有设备已连接到网桥。 – 长亮：网桥当前可能工作在 AP 模式、中继模式、P2MP 模式或路由模式。 – 闪烁：网桥当前可能工作在客户端模式、万能中继模式或无线 WAN 模式。 每个 LED 灯对应一个无线信号强度值，当网桥接收到的对端无线信号强度达到点亮值时，相应的 LED 灯亮起。您可以根据 LED 灯点亮情况，判断无线连接质量。默认情况下，各 LED 灯的点亮值如下。 -90dBm -80dBm -70dBm  您可以在网桥管理页面的「无线设置」>「高级设置」页面修改 LED 灯点亮值。
	熄灭	没有设备连接，或接收信号强度小于 LED 灯亮起的最小值（默认为 -90dBm）。

2 登录 Web 管理界面

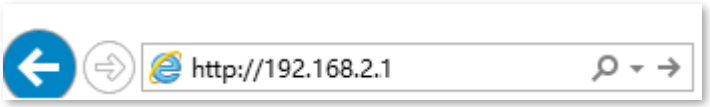
2.1 登录

1. 用网线将管理电脑连接到网桥（或已连接网桥的交换机）。
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 2~254，且未被其他设备占用），子网掩码为“255.255.255.0”。



3. 打开电脑上的浏览器，在地址栏（非搜索栏）输入网桥的管理 IP 地址，默认为 **192.168.2.1**，按键盘上的 Enter（或 Return）键。



4. 在出现的页面输入登录用户名/密码，点击 登录 。

提示

若未出现上述页面，请将网桥恢复出厂设置再登录。方法如下：

请在网桥正常运行时，按住 Reset 按钮 8 秒后松开，当指示灯全亮再熄灭时，网桥恢复出厂设置成功。

----完成

成功登录到网桥的管理页面，您可以开始配置网桥了。

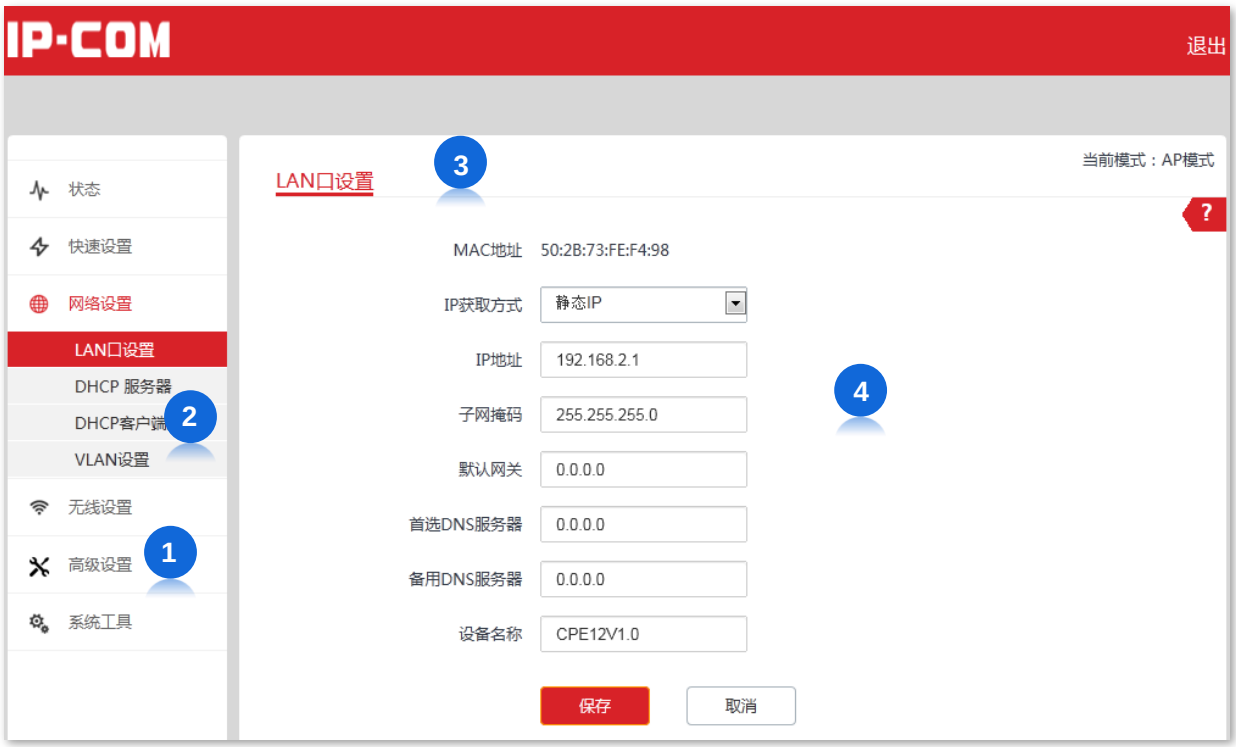
2.2 退出登录

登录到网桥的管理页面后，如果在 WEB 闲置超时时间（默认 5 分钟）内没有任何操作，系统将自动退出登录。此外，点击管理页面右上角的“退出”，也可以安全的退出管理页面。

3 Web 界面简介

3.1 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。



提示

管理页面上显示为灰色的功能或参数，表示网桥不支持或在当前配置下不可修改。

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

3.2 常用元素

网桥管理页面中常用元素的功能介绍如下表。

常用元素	说明
保存	用于保存当前页面配置，并使配置生效。
取消	用于取消当前页面未保存的配置，并恢复到修改前的配置。
刷新	用于刷新当前的页面信息。
	用于查看当前页面功能的帮助信息。

4 快速设置

4.1 概述

网桥各工作模式说明如下，请根据实际情况选择。

- AP 模式：把现有的有线网络转化为无线网络。
- 客户端模式：作为无线网卡连接其他无线网络。此时网桥不提供无线接入服务，用户需要通过网线连接到网桥。
- 万能中继模式：桥接现有无线信号，扩展无线网络覆盖范围。新无线网络的 SSID、密码以及其他无线信息与上级无线网络相同。
- 无线 WAN 模式：网桥的无线接口作为 WAN 口，用于连接宽带运营商的热点，如 CMCC、ChinaNet，也可以连接上级无线路由器，并通过 DHCP（自动获取）、静态 IP 或 PPPoE 使网桥的 WAN 口获取 IP 地址，连接到互联网。
- 中继模式：通过无线桥接将多个有线网络连通起来，并提供无线接入功能。
- P2MP 模式：通过无线桥接将多个有线网络连通起来，不提供无线接入功能。
- 路由模式：作为路由器使用，设备的“PoE/LAN”口为 WAN 口，连接到 Modem（猫），并通过 DHCP（自动获取）、静态 IP 或 PPPoE 使网桥的 WAN 口获取 IP 地址，连接到互联网。

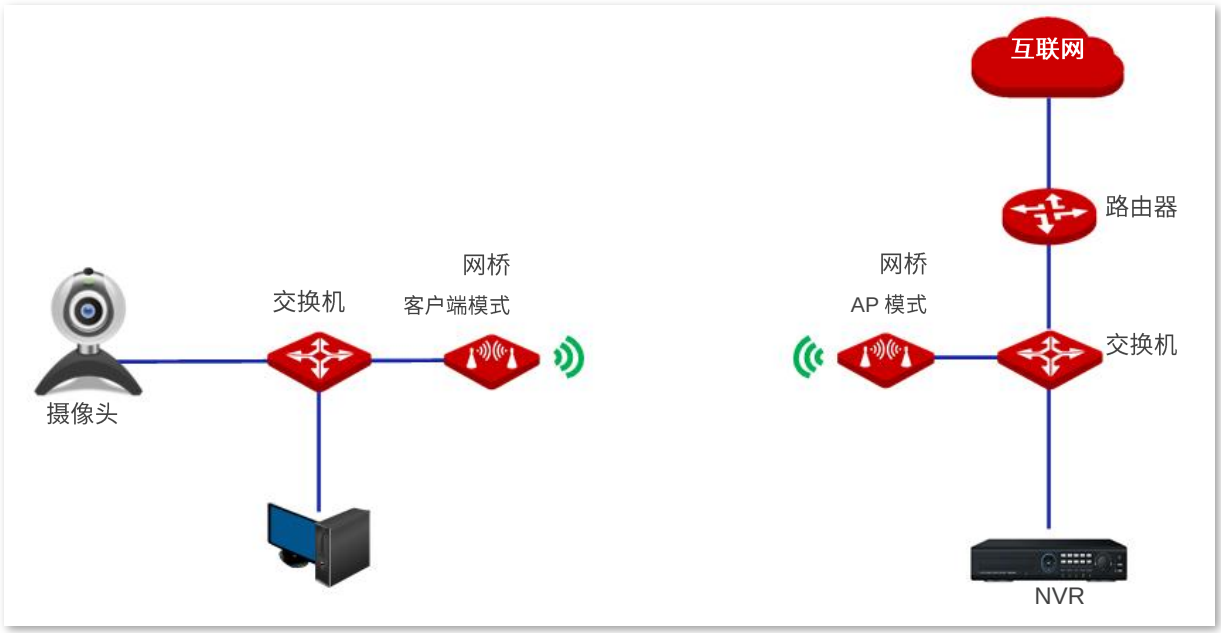
4.2 AP 模式

4.2.1 应用场景

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。

AP 模式可与客户端模式、万能中继模式搭配使用，常用于搭建视频监控网络。

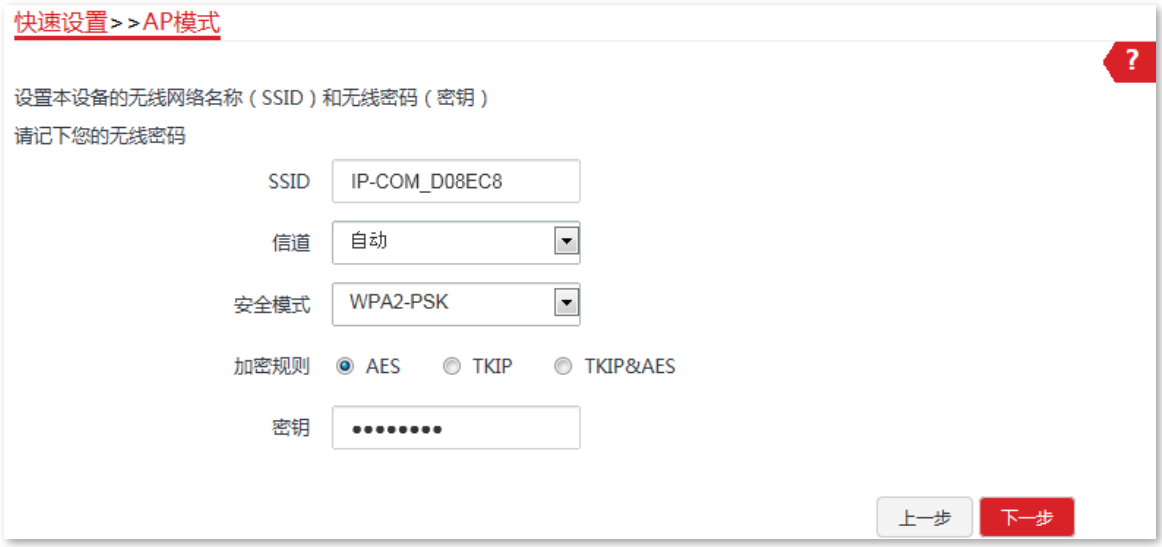
下图以 AP 模式与客户端模式搭配为例：



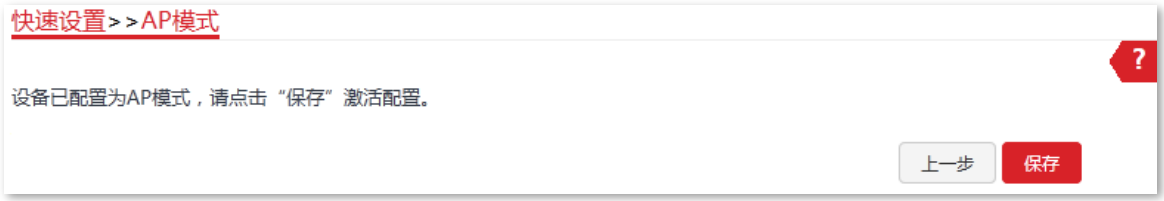
4.2.2 设置 AP 模式

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

2. 修改无线网络名称（SSID）。
3. 选择无线工作的信道。
4. 选择“安全模式”，建议为“WPA2-PSK”。
5. 选择“加密规则”，建议为“AES”。
6. 设置“密钥”，即无线密码。
7. 点击 下一步 。



8. 点击 保存 。等待网桥自动重启使配置生效。



----完成

AP 模式的参数说明

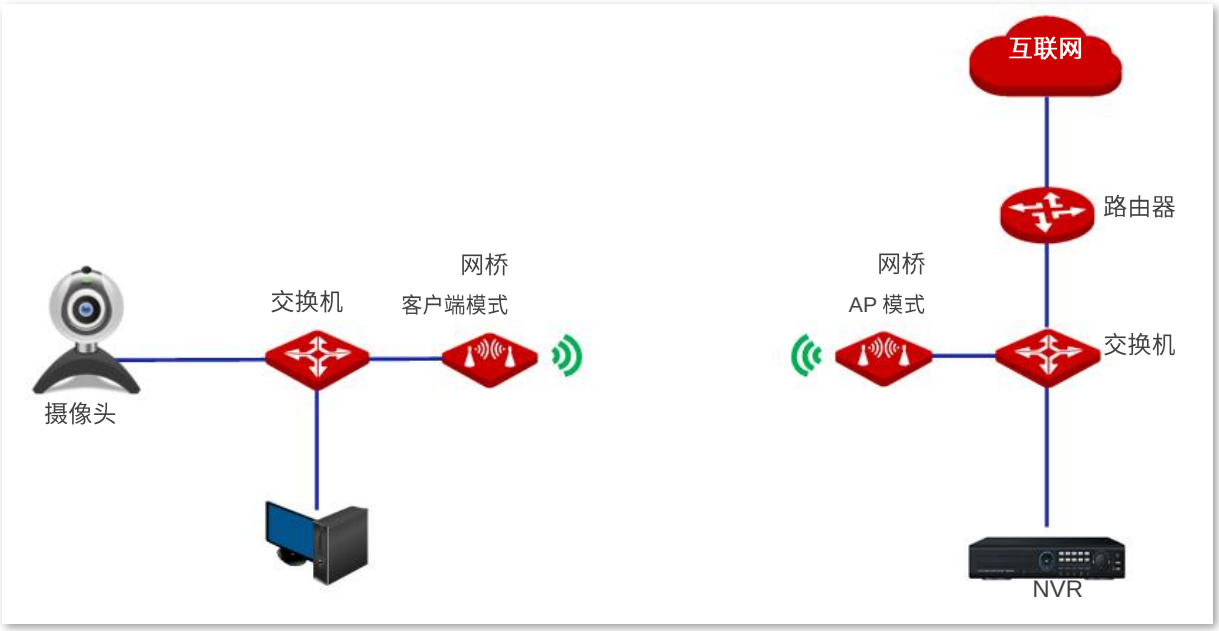
标题项	说明
SSID	点击可修改无线网络名称。
信道	选择网桥的工作信道。 尽可能选择当前区域使用比较少的信道以减少干扰。“自动”表示网桥根据周围环境情况自动调整工作信道。
安全模式	选择对应无线网络的安全模式。此处可选择：不加密、WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK。

4.3 客户端模式

4.3.1 应用场景

客户端模式下，网桥作为无线网卡连接到上级无线信号，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。

客户端模式一般与 AP 模式搭配使用，常用于搭建视频监控网络。应用拓扑图如下。



4.3.2 设置客户端模式

1. 进入网桥的「快速设置」页面，选择**客户端模式**，点击 下一步 。

2. 在出现的无线网络列表中，选择要连接的无线网络，如“IP-COM_1”，点击 下一步 。

提示

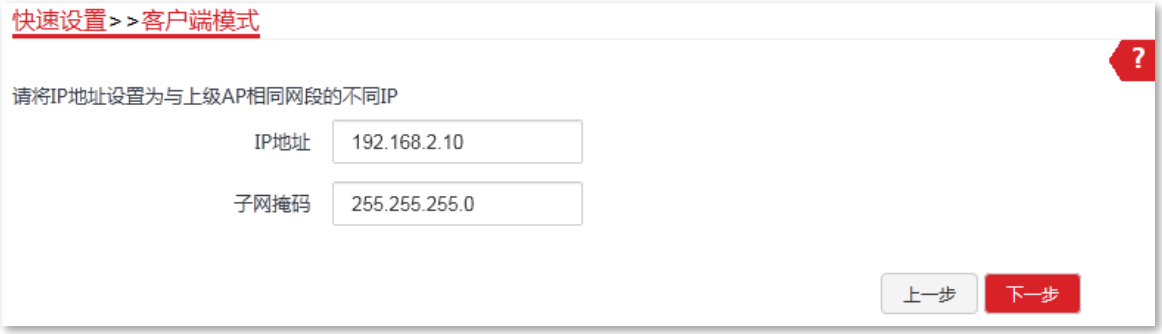
如果扫描不到无线网络，请进入「无线设置」>「基本设置」页面，确认您已开启无线，然后重新尝试。

3. 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 。

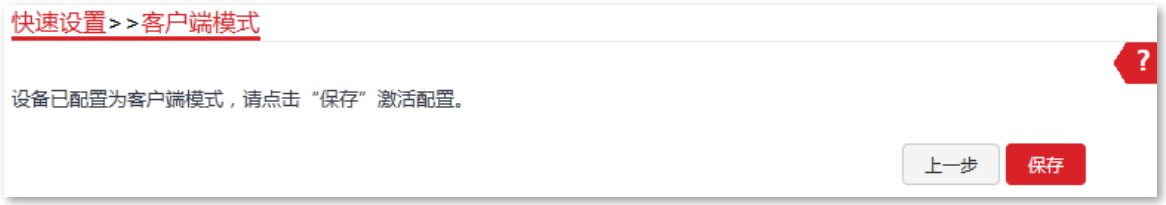
4. 设置本网桥的 IP 地址信息，然后点击 下一步 。

(1) 将本网桥 IP 地址设置为与上级 AP 的 IP 地址在同一网段的其他 IP 地址，如“192.168.2.10”。

(2) 将“子网掩码”设置为与上级 AP 的子网掩码一致。



5. 点击 保存 。等待网桥自动重启使配置生效。



----完成

提示

如果需要查看网桥的 SSID 和密钥，可登录到网桥管理页面，进入「无线设置」>「基本设置」页面查看。

客户端模式的参数说明

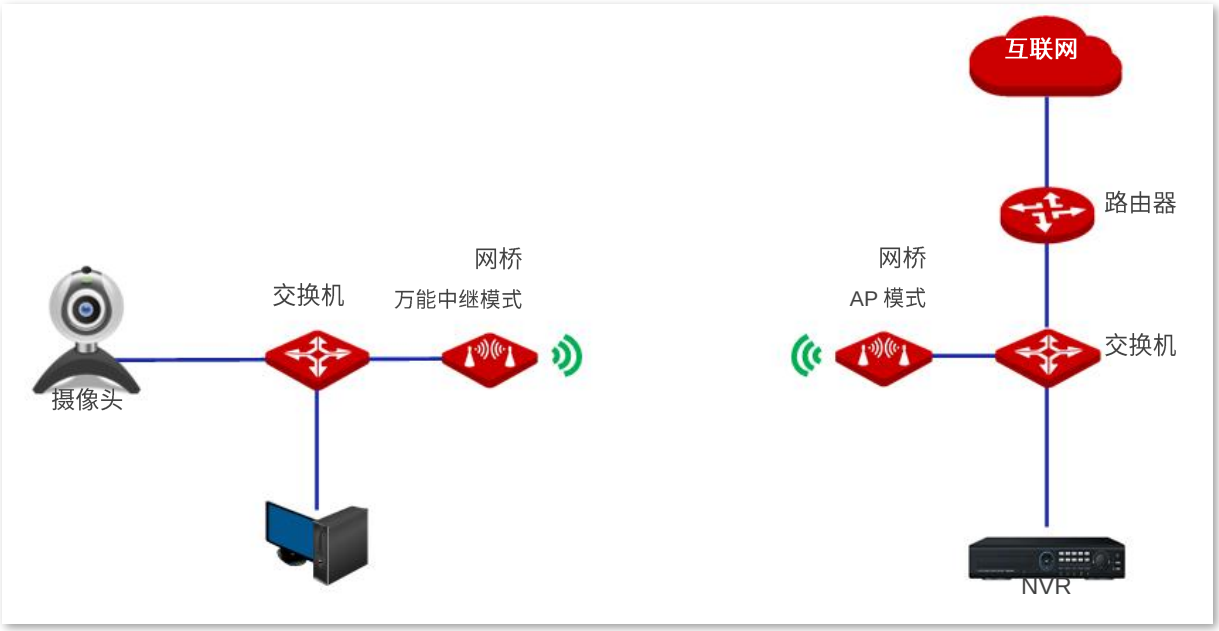
标题项	说明
上级 AP	待桥接无线网络的名称（SSID）。
信道	待桥接无线网络的工作信道。通过扫描选择时，会自动填充，无需手动设置。
安全模式	待桥接无线网络使用的安全模式。通过扫描选择时，会自动填充，无需手动设置。如果待桥接的无线网络已加密，须手动输入其密钥。

4.4 万能中继模式

4.4.1 应用场景

桥接现有无线信号，扩展无线网络覆盖范围。新无线网络的 SSID、密码以及其他无线信息与上级无线网络相同。

万能中继模式可与 AP 模式搭配使用，常用于视频监控。应用拓扑图如下。



4.4.2 设置万能中继模式

1. 进入网桥的「快速设置」页面，选择**万能中继模式**，点击 下一步 。

2. 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 。

提示

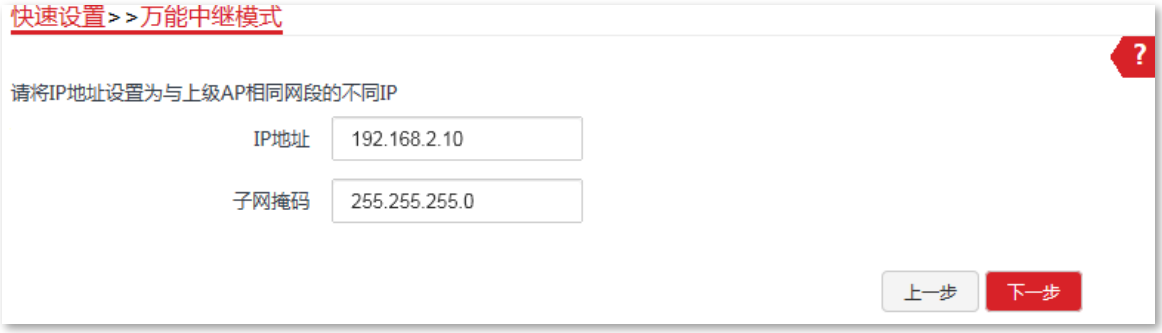
如果扫描不到无线网络，请进入「无线设置」>「基本设置」页面，确认您已开启无线，然后重新尝试。

3. 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 。

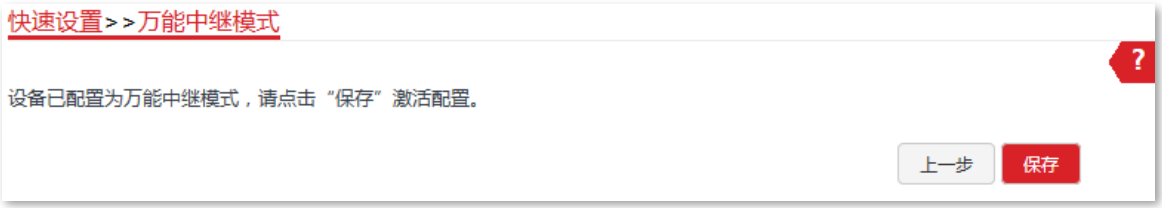
4. 设置网桥的 IP 地址信息，然后点击 下一步 。

(1) 将本网桥 IP 地址设置为与上级 AP 的 IP 地址在同一网段的其他 IP 地址，如“192.168.2.10”。

(2) 将“子网掩码”设置为与上级 AP 的子网掩码一致。



5. 点击 保存 。等待网桥自动重启使配置生效。



----完成

提示

如果需要查看网桥的 SSID 和密钥，可登录到网桥管理页面，进入「无线设置」>「基本设置」页面查看。

万能中继模式的参数说明

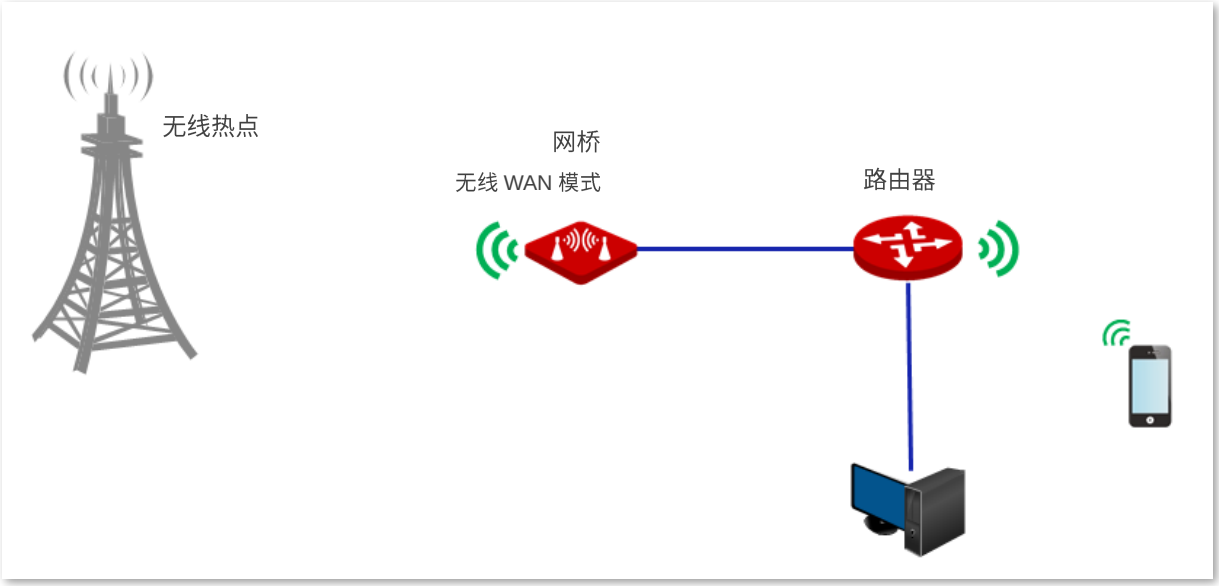
标题项	说明
上级 AP	待桥接无线网络的名称（SSID）。
信道	待桥接无线网络的工作信道。通过扫描选择时，会自动填充，无需手动设置。
安全模式	待桥接无线网络使用的安全模式。通过扫描选择时，会自动填充，无需手动设置。如果待桥接的无线网络已加密，须手动输入其密钥。

4.5 无线 WAN 模式

4.5.1 应用场景

无线 WAN 模式下，网桥可以连接宽带运营商的热点，如 CMCC，并分享网络给用户。

应用拓扑图如下。



4.5.2 设置无线 WAN 模式

1. 进入网桥的「快速设置」页面，选择**无线 WAN 模式**，点击 下一步 。

2. 在出现的无线网络列表中，选择要连接的无线网络，如“IP-COM_1”，点击 下一步 。

提示

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。

3. 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 。

4. 设置 WAN 口信息，然后点击 下一步 。

(1) 选择联网方式，如“PPPoE”。

(2) 输入运营商提供的“PPPoE 用户名”和“PPPoE 密码”。

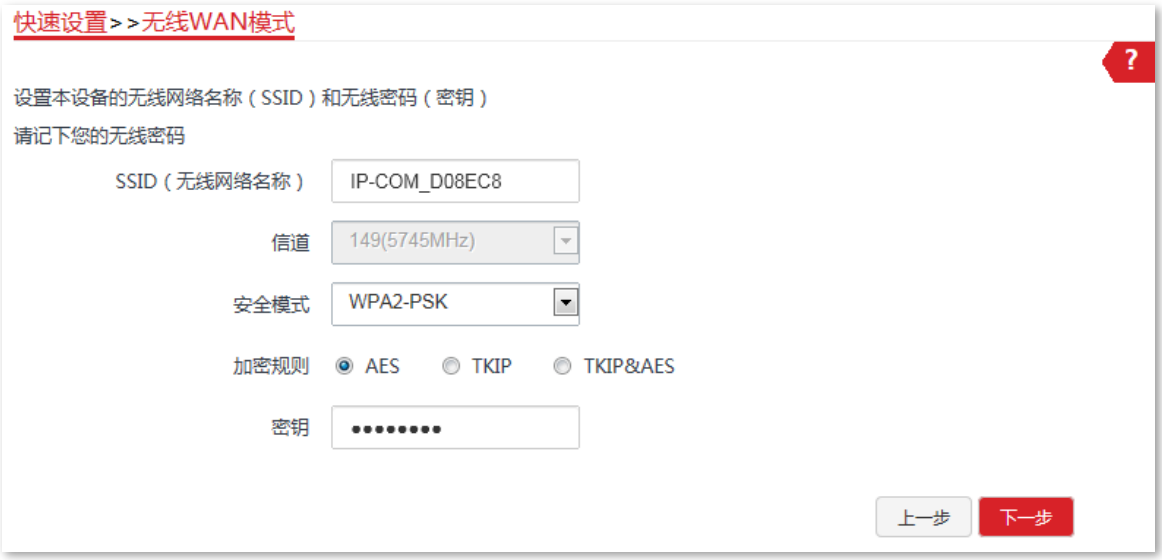
5. 设置网桥的无线基本信息，然后点击 下一步 。

(1) 修改无线网络名称。

(2) 选择“安全模式”，建议为“WPA2-PSK”。

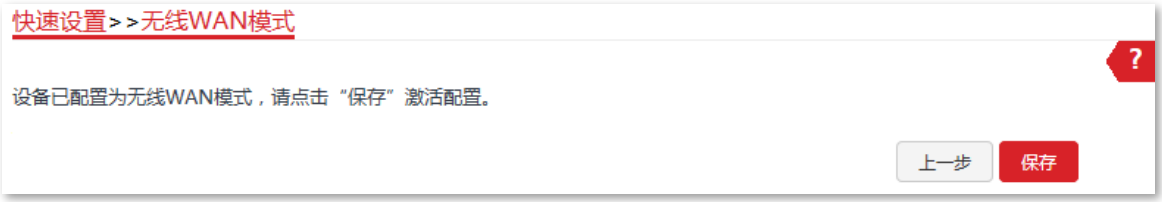
(3) 选择“加密规则”，建议为“AES”。

(4) 设置“密钥”，即无线密码。



6. 根据需要修改网桥的 LAN 口 IP 地址（默认为 192.168.2.1），点击 下一步 。

7. 点击 保存 。等待网桥自动重启使配置生效。



----完成

提示

如果需要查看网桥的 SSID 和密钥，可登录到网桥管理页面，进入「无线设置」>「基本设置」页面查看。

无线 WAN 模式的参数说明

标题项	说明
上级 AP	待连接无线网络的名称（SSID）。
信道	待连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	待连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。如果待连接的无线网络已加密，须手动输入其密钥。
联网方式	设置网桥的联网方式，支持三种联网方式，如下： - DHCP（自动获取）：网桥从上级 DHCP 服务器获取 IP 地址上网。 - 静态 IP：网桥使用固定的 IP 地址、子网掩码、默认网关、DNS 服务器信息上网。 - PPPoE：网桥使用用户名和密码拨号上网。 以上所需的上网参数均由宽带运营商提供，如不清楚，请咨询您的宽带运营商。

4.6 中继模式

4.6.1 应用场景

通过无线桥接将多个有线网络连通起来，自身提供无线接入功能。

中继模式一般搭配中继模式、P2MP 模式使用，最多支持 1 对 4 桥接，常用于实现企业在相同城市的多个办公区之间的通信。

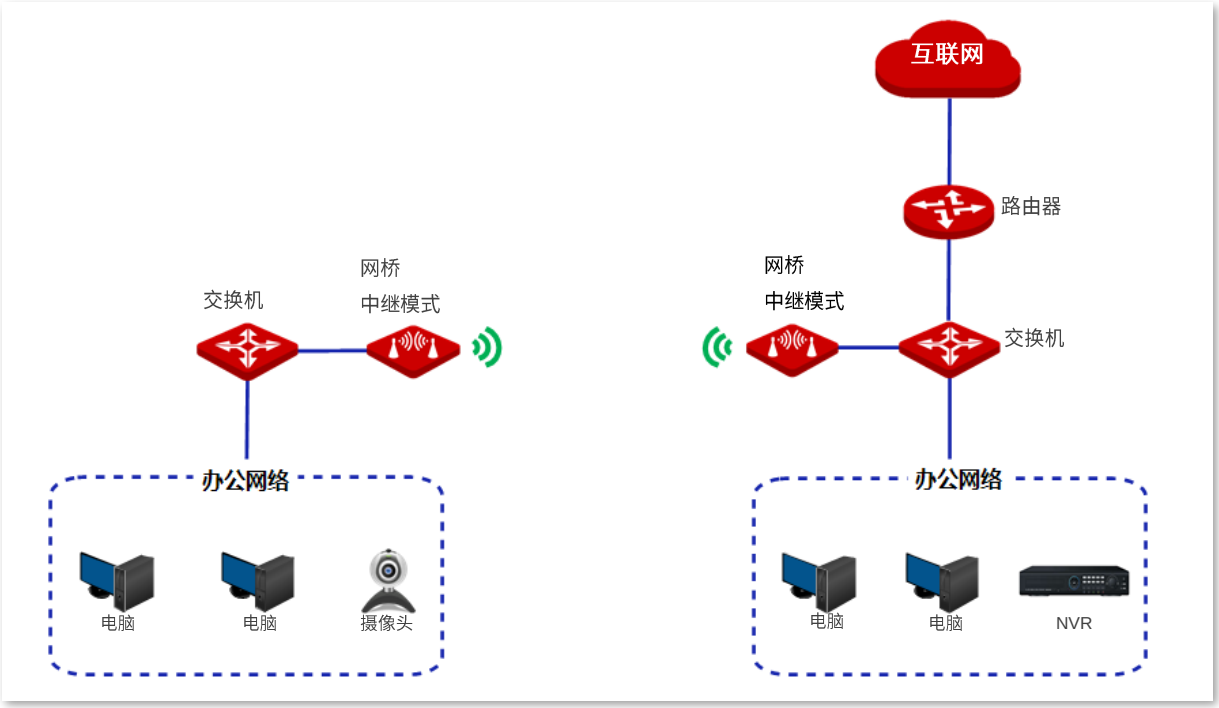
4.6.2 设置中继模式

提示

设置中继模式时，请保持所有网桥均工作在同一信道。

1 对 1 中继

假设 2 个网桥都采用中继模式，应用拓扑图如下。



设置步骤：

提示

如果需要查看网桥的 SSID 和密钥，可登录到网桥管理页面，进入「无线设置」>「基本设置」页面查看。

1. 设置第一个网桥为中继模式。

(1) 进入任意一个网桥的「快速设置」页面，选择**中继模式**，点击 下一步 。

(2) 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 。

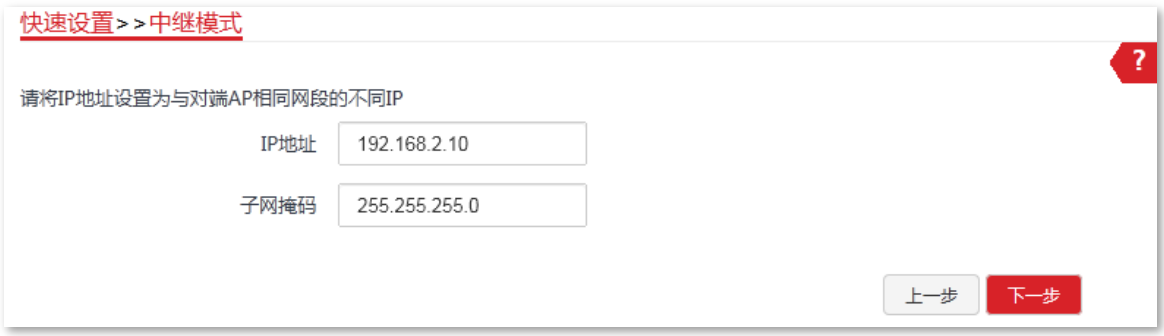
提示

- 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。
- 中继模式仅支持“不加密”和“WEP”安全模式。

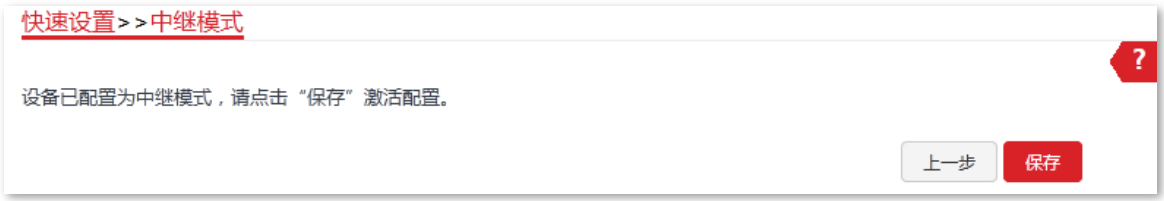
(3) 如果对端无线网络已加密，输入对端无线网络的**密钥**（无线密码），点击 下一步 。

(4) 设置网桥的 IP 地址信息，然后点击 下一步 。

- 将本网桥 IP 地址设置为与对端网桥的 IP 地址在同一网段的其他 IP 地址，如“192.168.2.10”。
- 将“子网掩码”设置为与对端网桥的子网掩码一致。



(5) 点击 保存 。等待网桥自动重启使配置生效。



2. 设置另一个网桥。

参考步骤 1，将第二个网桥也设置为中继模式，桥接第一个网桥的无线网络。

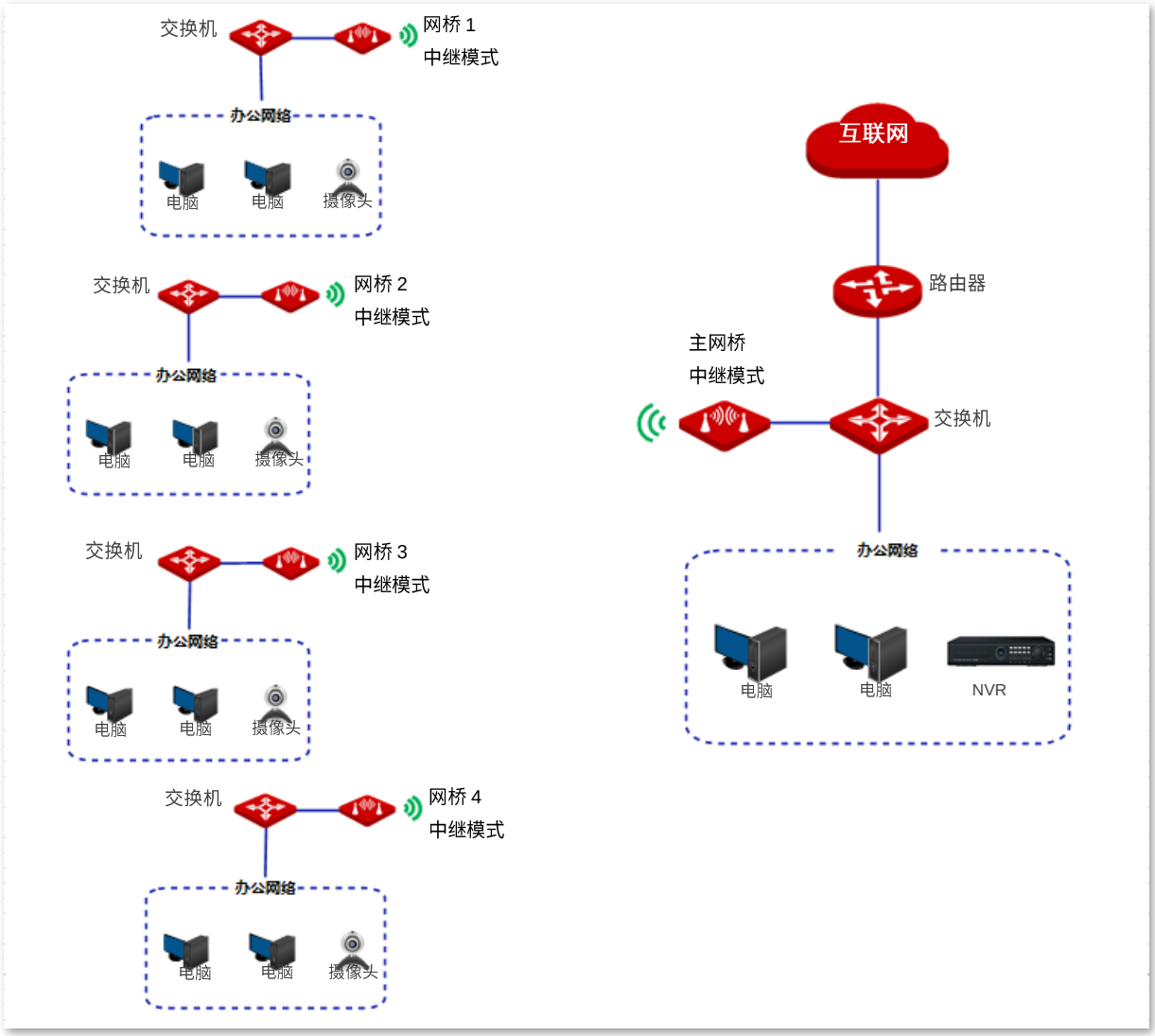
----完成

中继模式的参数说明

标题项	说明
对端 AP1	待桥接无线网络的名称（SSID）。
对端 AP1 的 MAC 地址	待桥接无线网络的 MAC 地址。
信道	待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	待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。如果待桥接的无线网络已加密，须手动输入其密钥。 提示 中继模式仅支持“不加密”和“WEP”安全模式。

1 对 4 中继

假设网桥都采用中继模式，应用拓扑图如下。



假设主网桥的基本参数如下：

- IP 地址：192.168.2.1
- 子网掩码：255.255.255.0
- SSID：IP-COM_1
- 信道：157
- 安全模式：不加密

假设网桥 1、2、3、4 的 SSID 和 MAC 地址分别如下：

网桥	SSID	MAC 地址
网桥 1	IP-COM_2	50:2B:73:FE:F6:69
网桥 2	IP-COM_3	50:2B:73:35:BA:01
网桥 3	IP-COM_4	50:2B:73:FD:8D:A1
网桥 4	IP-COM_5	50:2B:73:09:93:51

设置步骤：

1. 设置网桥 1 通过中继模式桥接主网桥。

(1) 进入网桥 1 的「快速设置」页面，选择**中继模式**，点击 下一步 。

(2) 在出现的无线网络列表中，选择要桥接的无线网络，本例为主网桥的无线网络"IP-COM_1"，点击 下一步 。

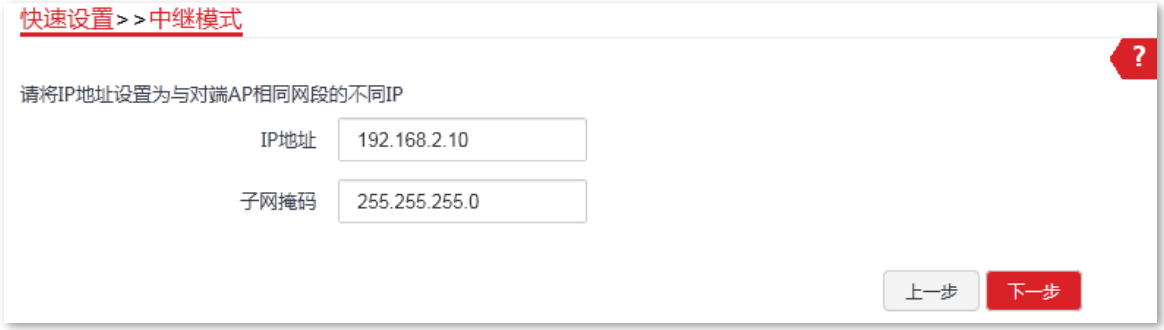
提示

- 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。
- 中继模式仅支持“不加密”和“WEP”安全模式。

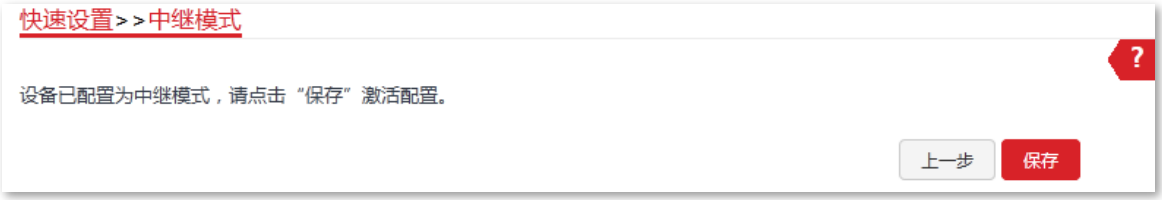
(3) 点击 下一步 。

(4) 设置网桥的 IP 地址信息，然后点击 下一步 。

- 将本网桥 IP 地址设置为与对端网桥的 IP 地址在同一网段的其他 IP 地址，如“192.168.2.10”。
- 将“子网掩码”设置为与对端网桥的子网掩码一致。



(5) 点击 保存 。等待网桥自动重启使配置生效。



2. 参考步骤 1，设置网桥 2/3/4 通过中继模式桥接主网桥。

3. 在主网桥设置无线中继，桥接网桥 1/2/3/4。

(1) 进入主网桥的「快速设置」页面，选择**中继模式**，点击 下一步 。

(2) 在出现的无线网络列表中，依次选择网桥 1/2/3/4 的无线网络，点击 下一步 。

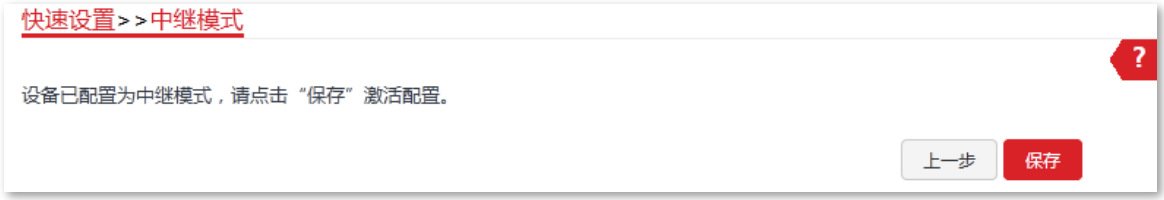
提示

- 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。
- 中继模式仅支持“不加密”和“WEP”安全模式。

(3) 点击 下一步 。

(4) 点击 下一步 。

(5) 点击 保存 。等待网桥自动重启使配置生效。



----完成

4.7 P2MP 模式

4.7.1 应用场景

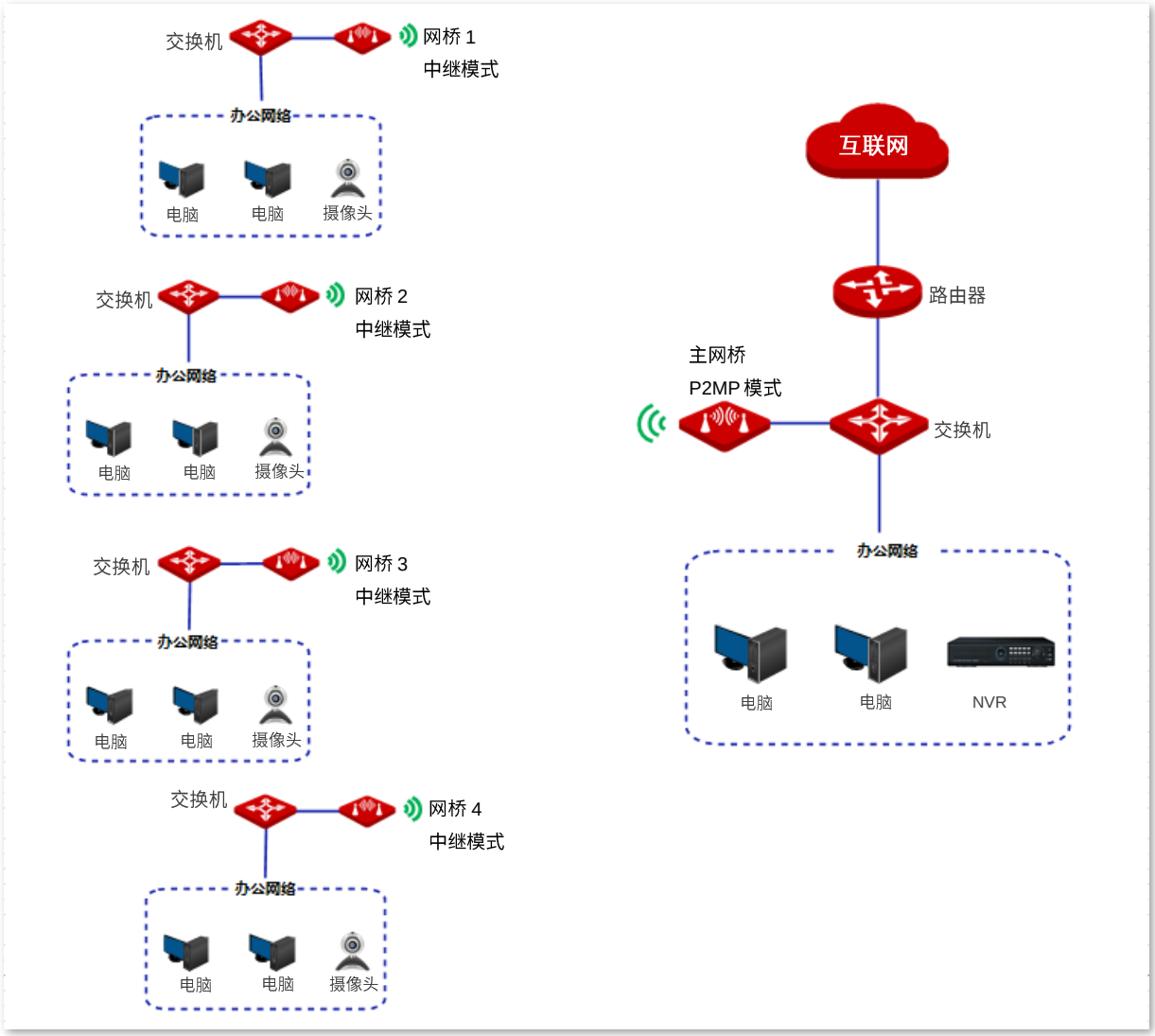
通过无线桥接将多个有线网络连通起来，自身不提供无线接入功能。

P2MP 模式一般搭配中继模式、P2MP 模式使用，最多支持 1 对 4 桥接，常用于实现企业在相同城市的多个办公区之间的通信。

4.7.2 设置 P2MP 模式

设置步骤与中继模式相似，下文以 P2MP 模式搭配中继模式进行 1 对 4 桥接为例。

应用拓扑图如下。



假设主网桥的基本参数如下：

- IP 地址：192.168.2.1
- 子网掩码：255.255.255.0
- SSID：IP-COM_1
- 信道：157
- 安全模式：不加密

假设网桥 1、2、3、4 的 SSID 和 MAC 地址分别如下：

网桥	SSID	MAC 地址
网桥 1	IP-COM_2	50:2B:73:FE:F6:69
网桥 2	IP-COM_3	50:2B:73:35:BA:01
网桥 3	IP-COM_4	50:2B:73:FD:8D:A1
网桥 4	IP-COM_5	50:2B:73:09:93:51

设置步骤：

提示

设置 P2MP 模式、中继模式时，请保持所有网桥均工作在同一信道。

1. 设置网桥 1 通过中继模式桥接主网桥。

(1) 进入网桥 1 的「快速设置」页面，选择**中继模式**，点击 下一步 。

(2) 在出现的无线网络列表中，选择要桥接的无线网络，本例为主网桥的无线网络"IP-COM_1"，点击 下一步 。

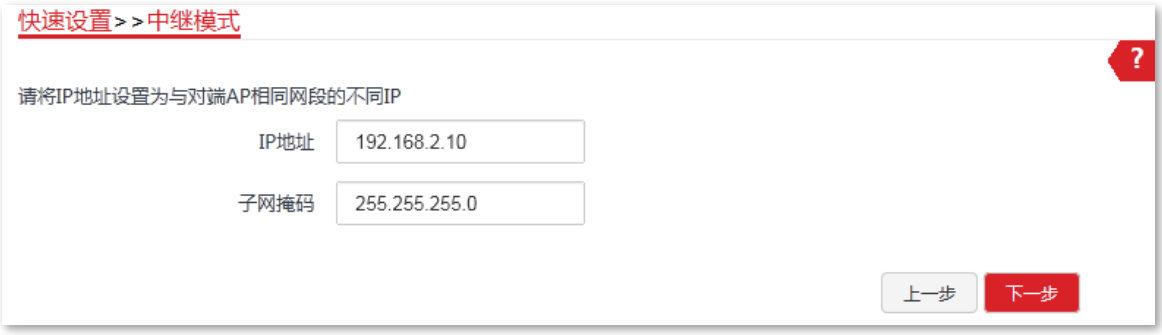
提示

- 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。
- 中继模式仅支持“不加密”和“WEP”安全模式。

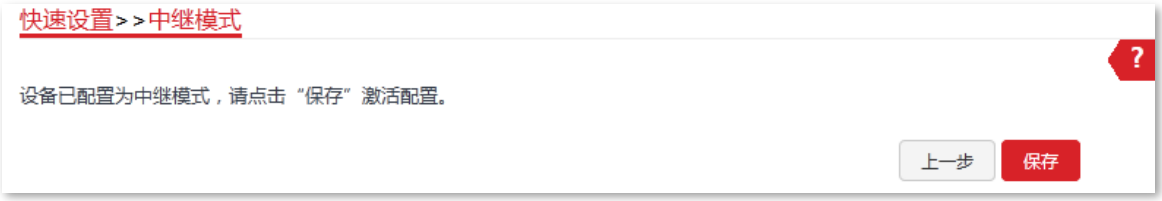
(3) 点击 下一步 。

(4) 设置网桥的 IP 地址信息，然后点击 下一步 。

- 将本网桥 IP 地址设置为与对端网桥的 IP 地址在同一网段的其他 IP 地址，如“192.168.2.10”。
- 将“子网掩码”设置为与对端网桥的子网掩码一致。



(5) 点击 保存 。等待网桥自动重启使配置生效。



2. 参考步骤 1，设置网桥 2/3/4 通过中继模式桥接主网桥。

3. 设置主网桥通过 P2MP 模式桥接网桥 1/2/3/4。

(1) 进入主网桥的「快速设置」页面，选择 **P2MP 模式**，点击 下一步 。

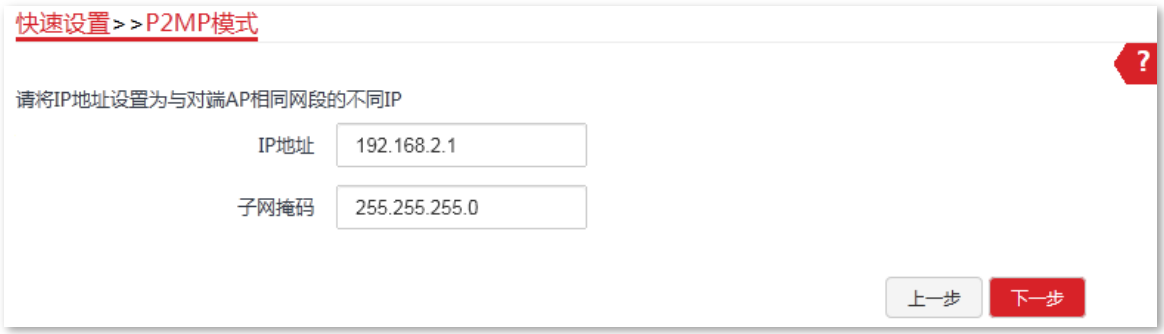
(2) 在出现的无线网络列表中，依次选择网桥 1/2/3/4 的无线网络，点击 下一步 。

提示

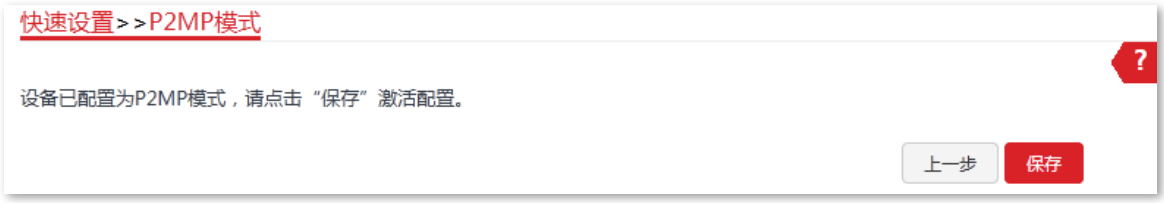
- 如果扫描不到无线网络，请进入「无线设置」>「基本设置」页面，确认您**已开启无线**，然后重新尝试。
- P2MP 模式仅支持“不加密”和“WEP”安全模式。

(3) 点击 下一步 。

(4) 点击 下一步 。



(5) 点击 保存 。等待网桥自动重启使配置生效。



----完成

P2MP 模式的参数说明

标题项	说明
对端 AP1	待桥接无线网络的名称（SSID）。
对端AP1的MAC地址	待桥接无线网络的 MAC 地址。
信道	待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	待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。如果待桥接的无线网络已加密，须手动输入其密钥。 提示 P2MP 模式仅支持“不加密”和“WEP”安全模式。

4.8 路由模式

4.8.1 应用场景

路由模式下，网桥充当路由器为用户提供无线网络。

网桥设置为路由模式后，网桥的 PoE 供电接口变为 WAN 口，用于连接上级网络设备。

应用拓扑图如下。

4.8.2 设置路由模式

提示

如果网桥只有一个网口，请先使用笔记本等无线设备连接网桥的无线网络。

1. 进入网桥的「快速设置」页面，选择**路由模式**，点击 下一步 。

2. 设置 WAN 口信息，然后点击 下一步 。

(1) 选择联网方式，如“PPPoE”。

(2) 输入运营商提供的“PPPoE 用户名”和“PPPoE 密码”。

3. 设置网桥的无线基本信息，然后点击 下一步 。

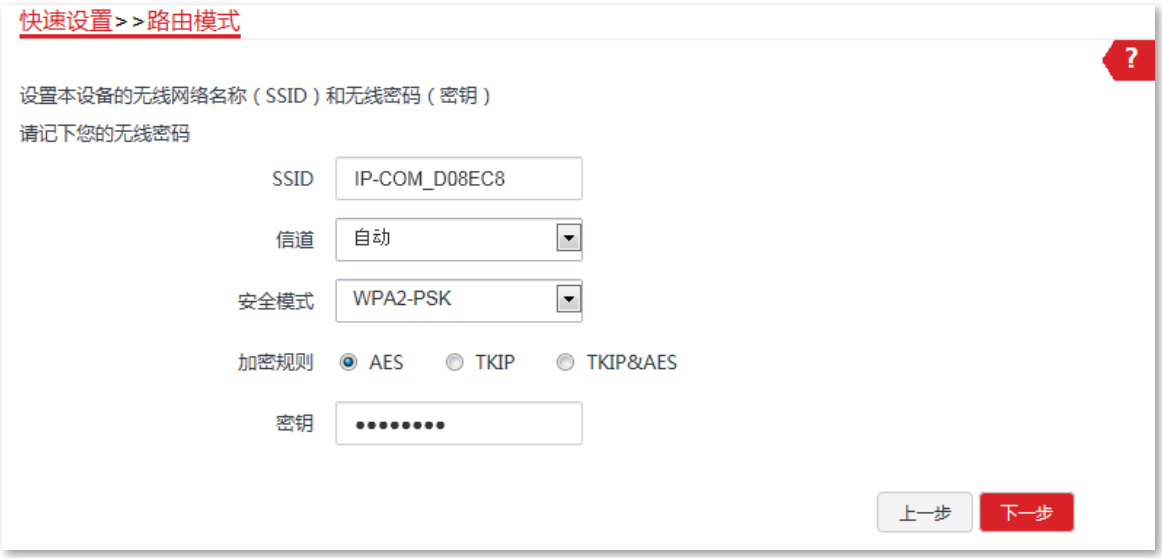
(1) 修改无线网络名称。

(2) 设置无线工作信道。

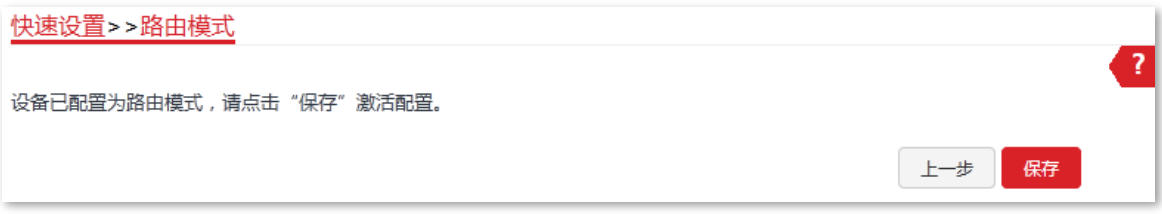
(3) 选择“安全模式”，建议为“WPA2-PSK”。

(4) 选择“加密规则”，建议为“AES”。

(5) 设置“密钥”，即无线密码。



4. 点击 保存 。等待网桥自动重启使配置生效。



----完成

路由模式的参数说明

标题项	说明
联网方式	设置网桥的联网方式，支持三种联网方式，如下： - DHCP（自动获取）：网桥从上级 DHCP 服务器获取 IP 地址上网。 - 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。 - PPPoE：网桥通过用户名和密码拨号上网。
SSID	点击可修改网桥的无线网络名称。SSID 支持中文字符（汉字）。
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。
安全模式	SSID 的安全模式。此处可选择：不加密、WEP、WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK。

5 状态

5.1 系统状态

在这里，您可以查看网桥的系统状态和接口状态。

AP 模式、客户端模式、万能中继模式、中继模式、P2MP 模式下的系统状态内容如下图示，如果网桥有多个网口，将会显示各 LAN 口当前的连接速率。下图以 CPE6SV1.0 为例。

无线 WAN 模式、路由模式下的系统状态内容如下：

提示

网桥工作在路由模式时，PoE 供电接口由 LAN 口变为 WAN 口。

参数说明

标题项	说明
设备名称	该台网桥的名称。当网络中存在多台相同型号网桥时，不同的设备名称可以帮助您区分各网桥设备。 您可以在 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。
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。
CPU	网桥的 CPU 使用率。
RAM	网桥的内存使用率。
LAN MAC	网桥以太网口（LAN 口）的物理地址。

标题项	说明
WLAN MAC	网桥无线接口的 MAC 地址。
LAN 口速率	网桥以太网口当前的连接速率。
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。
透明网桥	透明网桥的状态。
联网方式	网桥当前的联网方式。仅无线 WAN 模式、路由模式支持。 本设备支持三种联网方式，如下： – DHCP（自动获取）：网桥从上级 DHCP 服务器获取 IP 地址上网。 – 静态 IP：网桥使用固定的 IP 地址、子网掩码、默认网关、DNS 服务器信息上网。 – PPPoE：网桥使用用户名和密码拨号上网。
连接状态	网桥当前的网络连接状态。仅无线 WAN 模式、路由模式支持。
WAN IP	网桥 WAN 口获取的 IP 地址。仅无线 WAN 模式、路由模式支持。
默认网关	网桥的网关地址信息。仅无线 WAN 模式、路由模式支持。
首选 DNS 服务器	网桥的 DNS 服务器地址。仅无线 WAN 模式、路由模式支持。
备用 DNS 服务器	

5.2 无线状态

在这里，您可以查看网桥的无线状态信息，包括工作模式、SSID、安全模式等。

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。
安全模式	网桥无线网络当前的安全模式。
信道/频段	网桥当前的工作信道及频段。
信道带宽	网桥当前的信道带宽。
发射功率	网桥当前的发射功率。
无线客户端	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。 - AP、路由、中继、P2MP 模式下，显示本网桥的无线接口 MAC 地址。 - 客户端、万能中继、无线 WAN 模式下，桥接成功时，显示上级 AP 的无线接口 MAC 地址；桥接失败时，显示 N/A。
信号强度	对端设备的无线信号强度。 - AP、路由模式下，显示第一个接入设备无线网络的客户端信号强度。 - 客户端、万能中继、无线 WAN、中继、P2MP 模式下，显示设备接收到的对端 AP 的无线信号强度。
背景噪声	当前环境中干扰信号和电磁噪声的强度。绝对值越大，干扰越小。

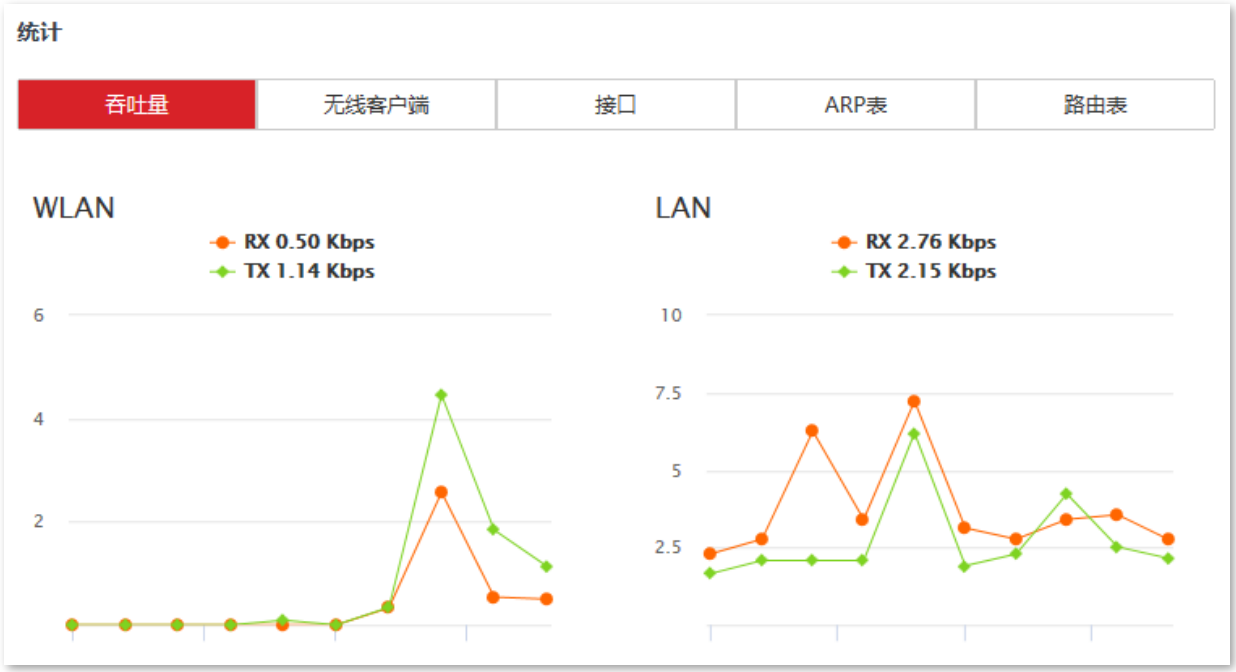
标题项	说明
TX/RX 链路	当前无线数据传输空间流数量。链路数量越多，传输流量越多。本设备为 2 收 2 发。
发送/接收速率	无线发送/接收速率。 – AP、路由模式下，显示第一个接入网桥无线网络的客户端的发送速率和接收速率。 – 客户端、万能中继、无线 WAN、中继、P2MP 模式下，显示本网桥的发送速率和接收速率。
IMAX	IMAX（时分多址技术）的状态，详细参数说明请参考 IMAX 说明。

5.3 统计

在这里，您可以查看网桥的吞吐量、无线客户端、上级 AP、接口、ARP 表、路由表。

5.3.1 吞吐量

显示网桥 WLAN 和 LAN 的吞吐量情况。



5.3.2 无线客户端

AP、中继、P2MP、路由模式下，显示当前连接到网桥的无线设备信息。

参数说明

标题项	说明
IP 地址	客户端的 IP 地址。

标题项	说明
MAC 地址	客户端的 MAC 地址。
信号/噪声	客户端的无线信号强度/当前环境中干扰信号和电磁噪声的强度。
发送/接收	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、万能中继、无线 WAN 模式下，显示网桥当前连接的上级 AP 的信息。

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/当前环境中干扰信号和电磁噪声的强度。
发送/接收	上级设备当前的发送/接收速率。
CCQ	网桥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	网桥成功桥接上级设备的时长。

5.3.4 接口

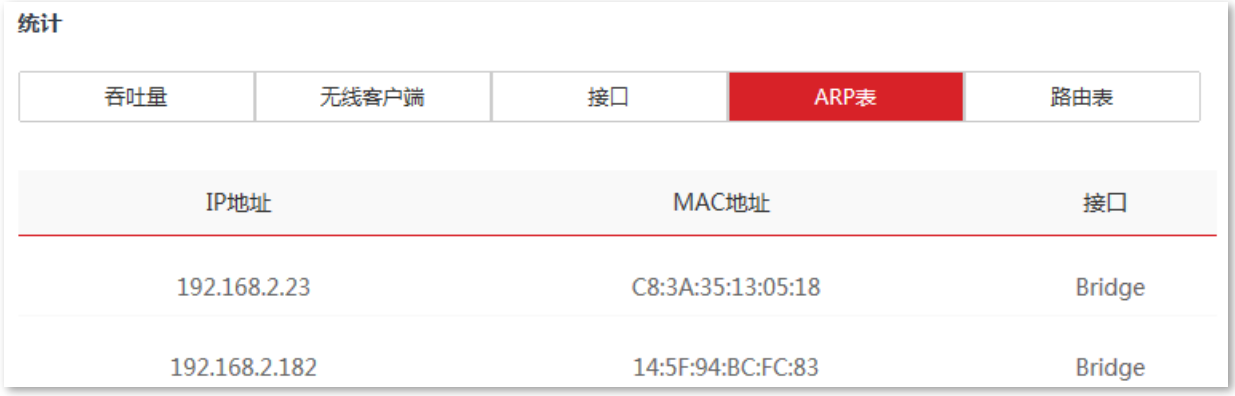
显示网桥各接口的 IP 地址、MAC 地址和数据流量信息。

参数说明

标题项	说明
接口	显示网桥各接口。
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 发送数据包	接口接收/发送的数据包情况。
接收错误 发送错误	接口接收/发送错误数据包的情况。

5.3.5 ARP 表

在这里，您可以查看网桥当前的 ARP 表。

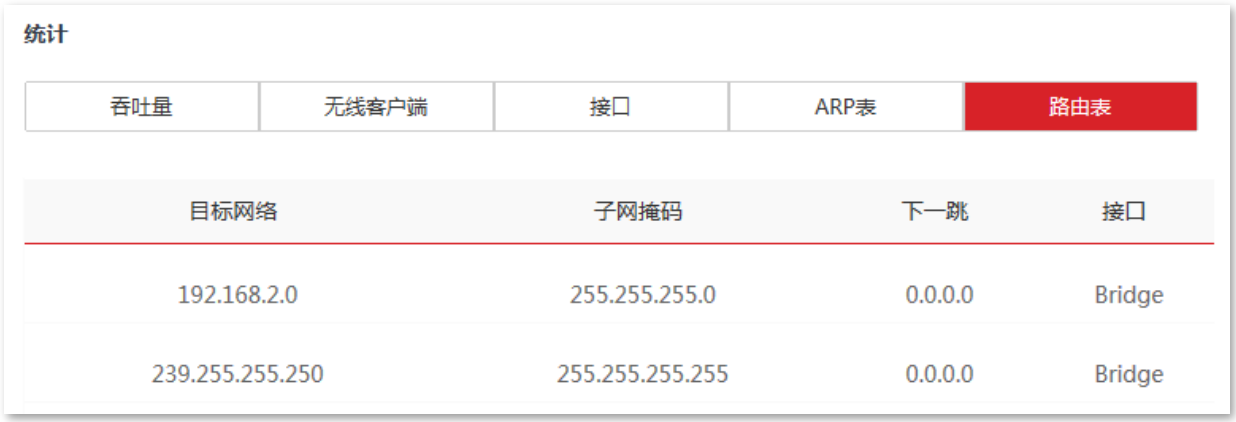


参数说明

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

在这里，您可以查看网桥当前可达的目标网络。



参数说明

标题项	说明
目标网络	IP 数据包的目的网络地址。
子网掩码	目的网络的子网掩码。
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 获取方式等相关信息。

参数说明

标题项	说明
MAC 地址	网桥的 LAN 口 MAC 地址。
IP 获取方式	网桥获取 IP 地址的方式。默认为“静态 IP”。 – 静态 IP：手动指定网桥的 IP 地址、子网掩码、默认网关、DNS 服务器。 – 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、默认网关、DNS 服务器。 提示 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，一般要设置默认网关为出口路由器的 LAN 口 IP 地址。
首选 DNS 服务器	网桥的首选 DNS 服务器地址。 如果出口路由器有 DNS 代理功能，此地址可以是出口路由器的 LAN 口 IP 地址。如果出口路由器无 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，方便在管理多台相同型号的网桥时，通过设备名称快速定位各网桥设备。

6.1.2 修改 LAN IP 地址

手动设置 IP 地址

网络管理员可指定网桥的 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几台网桥的场景。

设置步骤：

1. 点击「网络设置」>「LAN 口设置」。
2. 选择“IP 获取方式”为“静态 IP”。
3. 设置 IP 地址、子网掩码（如果需要设置网桥联网，还需设置“默认网关”、“首选/备用 DNS 服务器”）。
4. 点击 保存 。

5. 确认提示信息后，点击 确定 。

----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 地址

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

----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

6.2.1 概述

MAC 克隆功能仅在无线 WAN 模式、路由模式下可用。

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。

注意

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

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，点击「网络设置」>「MAC 克隆」。
3. 点击 克隆本地 MAC 。
4. 点击 保存 。

----完成

方法 2：

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

----完成

提示

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

6.3 DHCP 服务器

6.3.1 概述

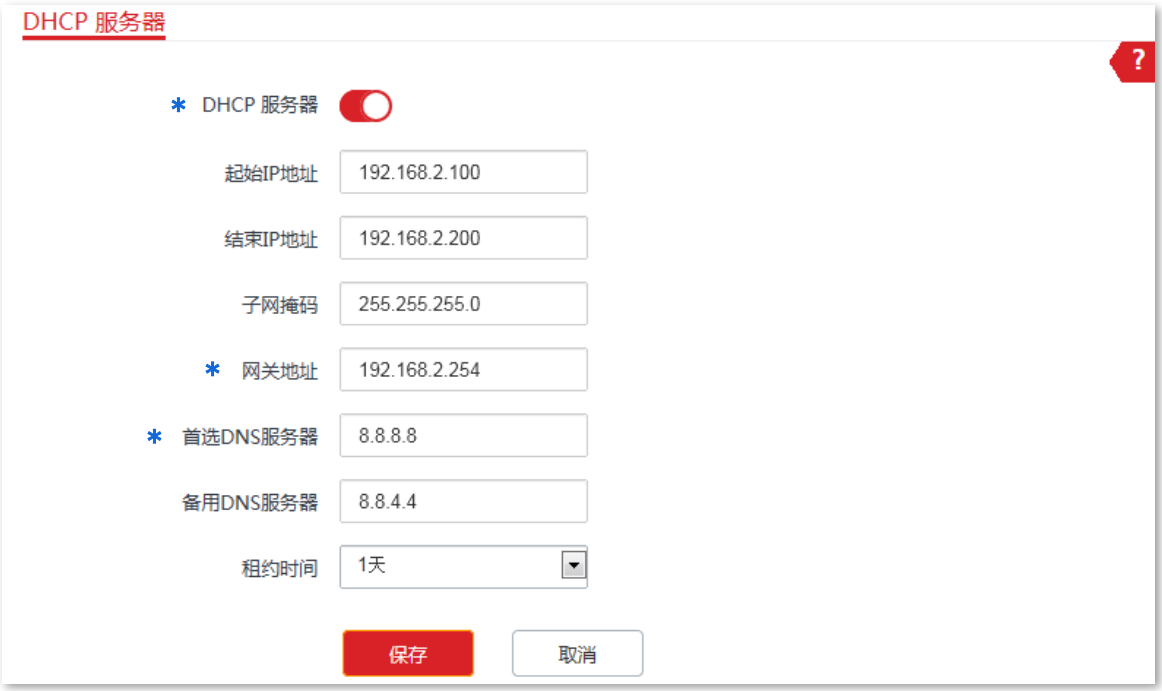
网桥提供了 DHCP 服务器，可以为局域网中的客户端自动分配 IP 地址信息。默认情况下，网桥启用了 DHCP 服务器功能。

提示

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

6.3.2 配置 DHCP 服务器

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



----完成

注意

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。

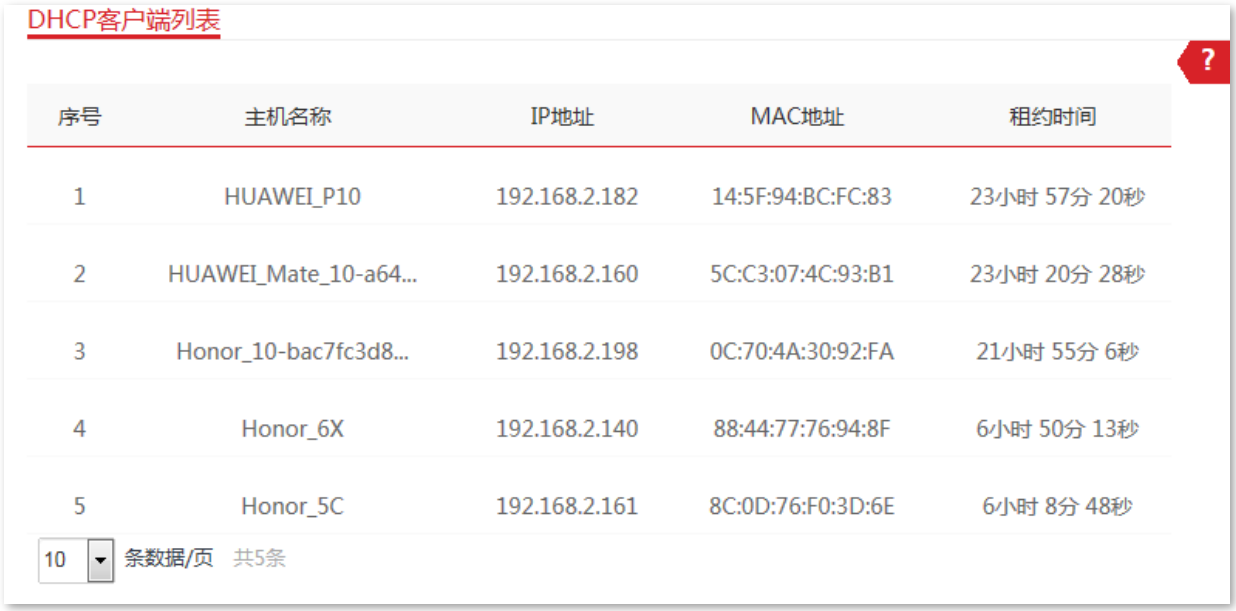
参数说明

标题项	说明
DHCP 服务器	DHCP 服务器功能开关。表示关闭， 表示开启。
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。
结束 IP 地址	DHCP 地址池的结束 IP 地址。默认为 192.168.2.200。 提示 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。 提示 客户端访问本网段以外的服务器或主机时，数据必须通过网关进行转发。
首选 DNS 服务器	DHCP 服务器分配给客户端的首选 DNS 服务器 IP 地址。默认为 8.8.8.8。 提示 为了使局域网设备能够正常上网，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

进入页面：点击「网络设置」>「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 地址的设备的主机名称、IP 地址等信息。



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。

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

各链路类型端口对数据的接收和发送处理方式详见下表：

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

6.5.2 配置 VLAN（以 CPE6SV1.0 为例）

1. 点击「网络设置」>「VLAN 设置」。
2. 点击滑块至 。
3. 根据需要修改各参数。
4. 点击 保存 。

----完成

参数说明

标题项	说明
VLAN 设置	开启/关闭网桥的 802.1Q VLAN 功能。默认关闭。开启 VLAN 后，网桥的 PoE/LAN 口为 Trunk 口。
PVID	Trunk 口默认所属的 VLAN ID，默认为“1”。开启 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，默认为 1000。开启 VLAN 后，SSID 所在的无线接口相当于一个 Access 口，其 PVID 与 VLAN ID 相同。
LAN2	设置网桥网口的 VLAN ID，默认为 1。启用 VLAN 后，网口相当于一个 Access 口，其 PVID 与 VLAN ID 相同。
LAN3	
LAN4	

6.5.3 VLAN 设置举例（以 CPE12V1.0 为例）

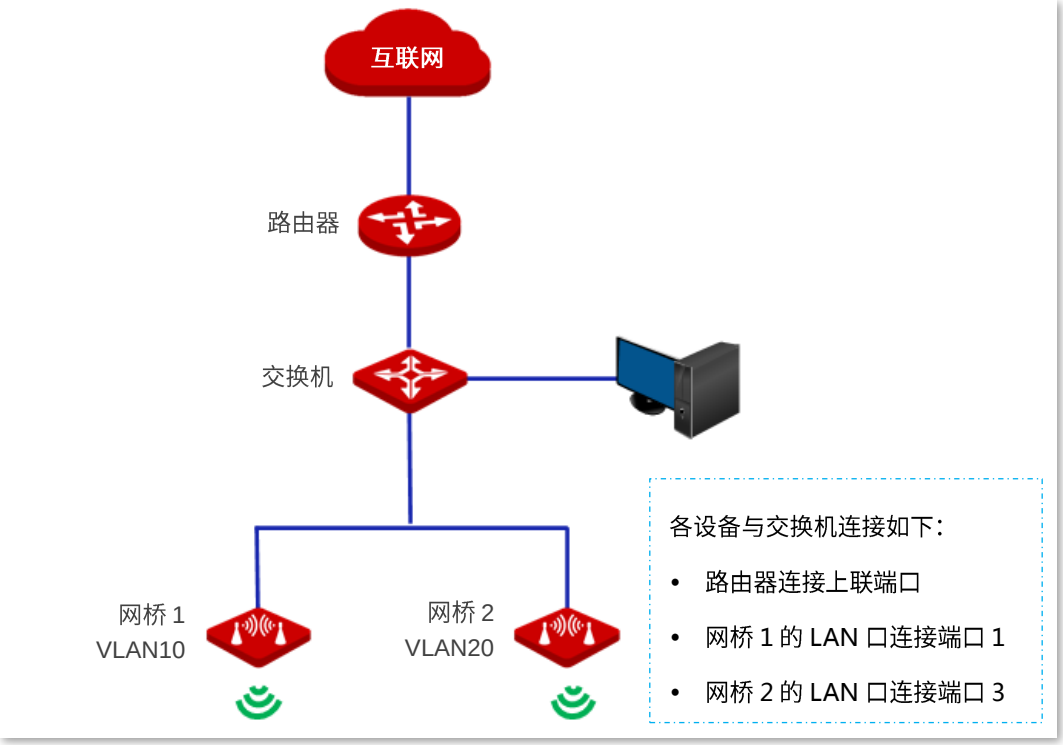
组网需求

某两个小区使用网桥部署网络，并通过同一个路由器连接到互联网。现要求，两个小区上网互不干扰。

方案设计

将第 1 个网桥划分在 VLAN10，第 2 个网桥划分在 VLAN20。

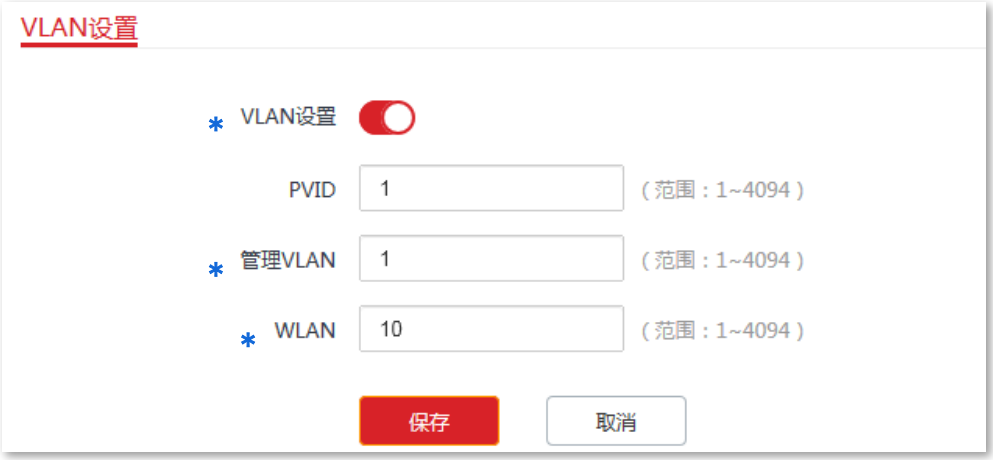
路由器需要支持并进行 QVLAN 配置，且为 VLAN10 和 VLAN20 配置不同的 DHCP，使两个 VLAN 下的客户端获取不同网段的 IP 地址上网。



配置步骤

一、配置网桥

1. 登录任意一台网桥的管理页面，点击「网络设置」>「VLAN 设置」。
2. 点击滑块至 。
3. 设置“管理 VLAN”，默认为 1，建议保持默认设置。
4. 设置“WLAN”，即无线接口 VLAN ID，本例为“10”。
5. 点击 保存 。



6. 在弹出的窗口点击 确定 。等待网桥自动重启完成即可。

7. 参考步骤 1~6 设置另一台网桥工作在 VLAN20。

二、配置交换机

在交换机上划分 IEEE 802.1Q VLAN，具体设置如下。

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

三、配置路由器

1. 在路由器上进行 QVLAN 配置，具体设置如下。

端口连接到	VLAN ID（允许通过的 VLAN）	端口属性	PVID
交换机	10,20	Trunk	1

2. 在路由器上给 VLAN10 和 VLAN20 配置不同的 DHCP 地址池。

具体配置方法请参考路由器的使用手册。

----完成

验证配置

如果路由器 VLAN10、VLAN20 均设置了 DHCP 服务器，则连接到第一个网桥的客户端会获取到路由器 VLAN10 分配的 IP 地址信息；连接到第二个网桥的客户端会获取到路由器 VLAN20 分配的 IP 地址信息。

7 无线设置

7.1 基本设置

7.1.1 概述

本模块用于配置网桥的无线基本参数，如 SSID 相关参数、网络模式、信道、发射功率等。

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：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。下图以 CPE15V1.0 为例。

1. 点击「无线设置」>「基本设置」。
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 。

----完成

参数说明

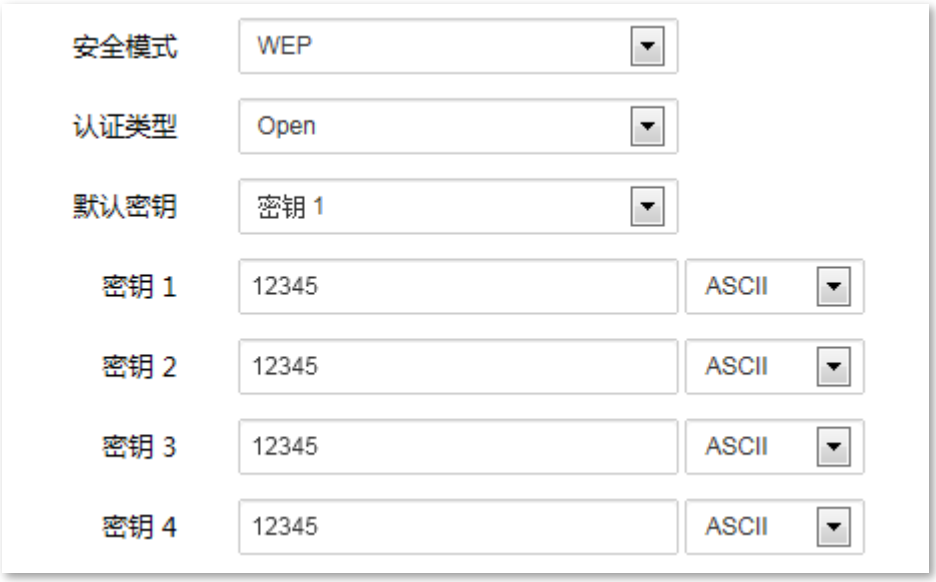
标题项	说明
开启无线	无线功能开关。 表示关闭， 表示开启。
国家或地区	选择网桥当前所在的国家或地区，以适应不同国家（或地区）对信道的管制要求。默认为“中国”。
SSID	点击此栏，可修改网桥的无线网络名称（SSID）。SSID 支持中文字符。
SSID 广播	SSID 的广播状态。 – 启用：网桥广播该 SSID，周边无线设备可以扫描到该 SSID。 – 禁用：网桥不广播该 SSID，无线设备连接网桥的 WiFi 时，需要正确输入该 SSID。
网络模式	选择无线网络模式。 网桥仅允许支持该网络模式的无线设备接入。
信道	选择网桥的工作信道。“自动”表示网桥根据周围环境情况自动调整工作信道。

标题项	说明
信道偏移	信道中心频率的偏移。启用后，信道中心频率将会在 IEEE 802.11 标准信道中心频率上偏移 5MHz，从而获得干扰更少的频谱。 注意 网桥启用“信道偏移”后，与之进行桥接的网桥也要启用该功能，否则将会导致桥接失败。
DFS 功能	DFS，Dynamic Frequency Selection，动态频率选择。启用后，网桥会主动探测雷达系统（军用雷达、气象雷达等）的频率，当侦测到同频段雷达信号时，网桥自动切换到另一个频率，以避免对雷达系统造成干扰。
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	选择网桥的无线信道带宽。 不同的网络模式所支持的信道带宽各异，请根据实际情况选择。设置为“自动”时，网桥会根据周围环境，自动调整其信道带宽。
传输速率	网桥的无线传输速率，建议选择“自动”。 不同的信道带宽和网络模式，网桥所能协商的最大速率各异，详情见 Web 管理界面。设置为“自动”时，网桥的最大传输速率可协商为当前网络模式所能协商到的最大速率。
安全模式	SSID 的安全模式。网桥支持的安全模式有：不加密、WEP、WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK、WPA、WPA2。
客户端隔离	- 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。 - 禁用：连接在该 SSID 下的设备之间能互相通信。默认为“禁用”。
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**

  网桥的无线网络不加密。为了保障网络安全，不建议选择此项。

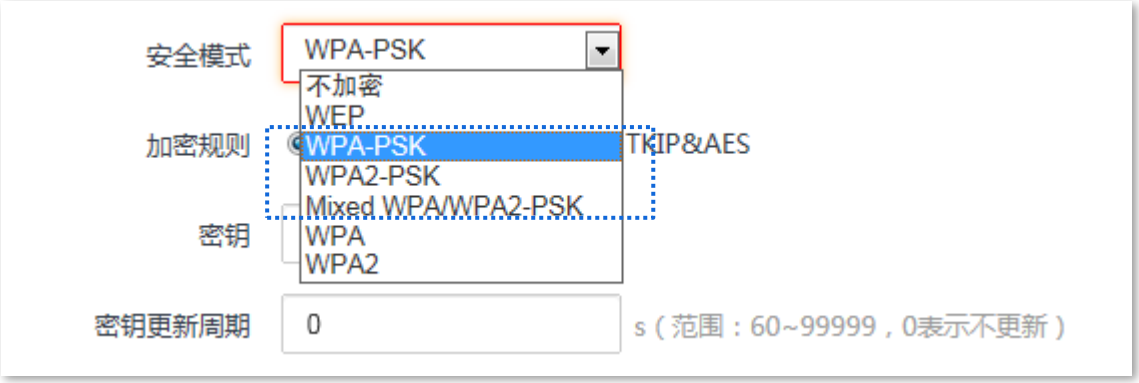
- **WEP**



参数说明

标题项	说明
认证类型	WEP 加密时使用的认证方式：Open、Shared。两者加密过程完全一致，只是认证方式不同。 – Open：采用“空认证+WEP 加密”。无线设备无需经过认证，即可与 SSID 进行关联，只对传输数据进行 WEP 加密。 – Shared：采用“共享密钥认证+WEP 加密”。无线设备与 SSID 进行关联时，需提供在网桥上指定的 WEP 密钥，只有在双方 WEP 密钥一致的情况下，才能关联成功。
默认密钥	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 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	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	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）。

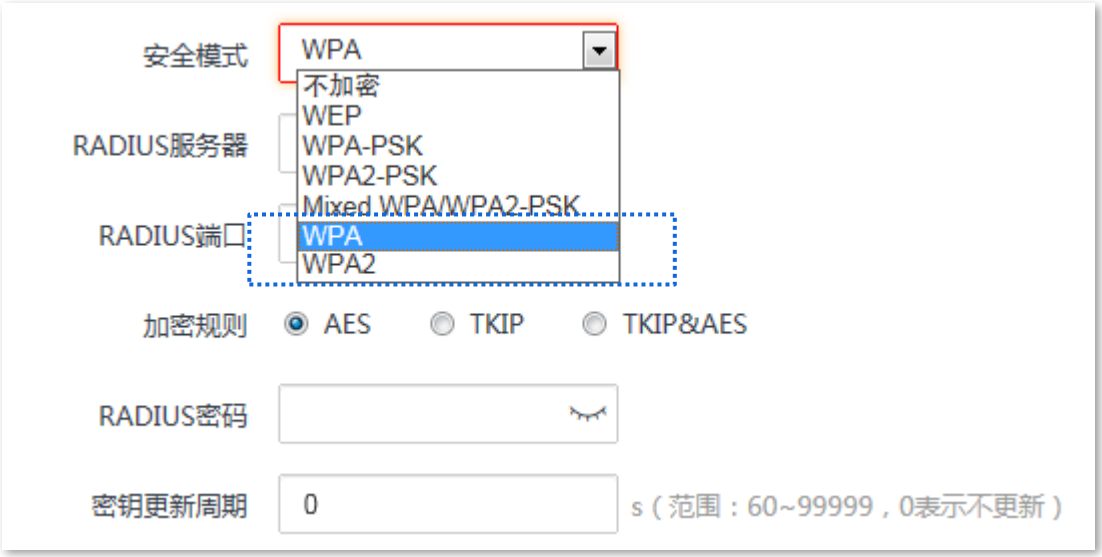
- **WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK**



参数说明

标题项	说明
安全模式	选择安全模式。 – WPA-PSK：此时，SSID 对应的无线网络采用 WPA-PSK 安全模式。 – WPA2-PSK：此时，SSID 对应的无线网络采用 WPA2-PSK 安全模式。 – Mixed WPA/WPA2-PSK：兼容 WPA-PSK 和 WPA2-PSK，此时，无线设备使用 WPA-PSK 和 WPA2-PSK 均可连接 SSID。
加密规则	WPA 加密规则，WPA-PSK 只可选择“AES”或“TKIP”；WPA2-PSK 和 Mixed WPA/WPA2-PSK 还可选择“TKIP&AES”。 – AES：高级加密标准。 – 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）。 – TKIP&AES：兼容 TKIP 和 AES，无线客户端使用 TKIP 和 AES 均可连接。
密钥	WPA 预共享密钥。
密钥更新周期	WPA 数据加密密钥自动更新周期，较短的密钥更新周期可增强 WPA 数据安全性。 为 0 表示不更新。

- **WPA、WPA2**



参数说明

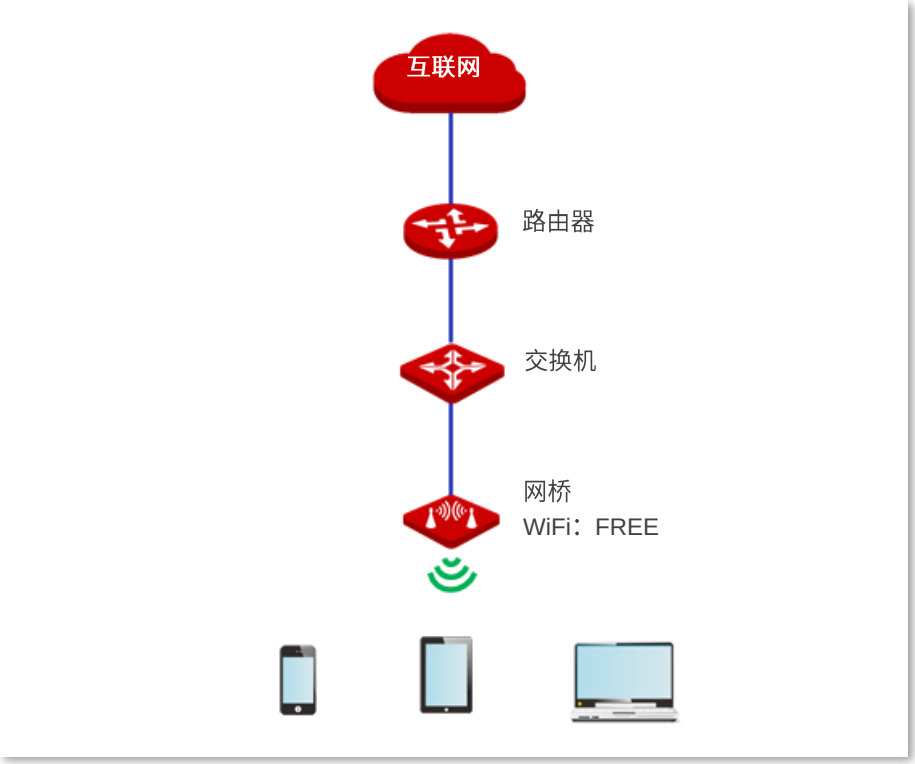
标题项	说明
安全模式	选择安全模式。 – WPA：此时，SSID 对应的无线网络采用 WPA 安全模式。 – WPA2：此时，SSID 对应的无线网络采用 WPA2 安全模式。
RADIUS 服务器	用于输入 RADIUS 服务器的 IP 地址/认证端口/共享密钥。
RADIUS 端口	
RADIUS 密码	
加密规则	选择 WPA 加密规则。 – AES：高级加密标准。 – TKIP：临时密钥完整性协议。 – TKIP&AES：兼容 TKIP 和 AES，无线客户端使用 TKIP 和 AES 均可连接。
密钥更新周期	WPA 数据加密密钥自动更新周期，较短的密钥更新周期可增强 WPA 数据安全性。 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

某小区使用网桥进行组网实现电梯监控，要求：无线网络名称为 FREE，没有无线密码。



配置步骤

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

----完成

验证配置

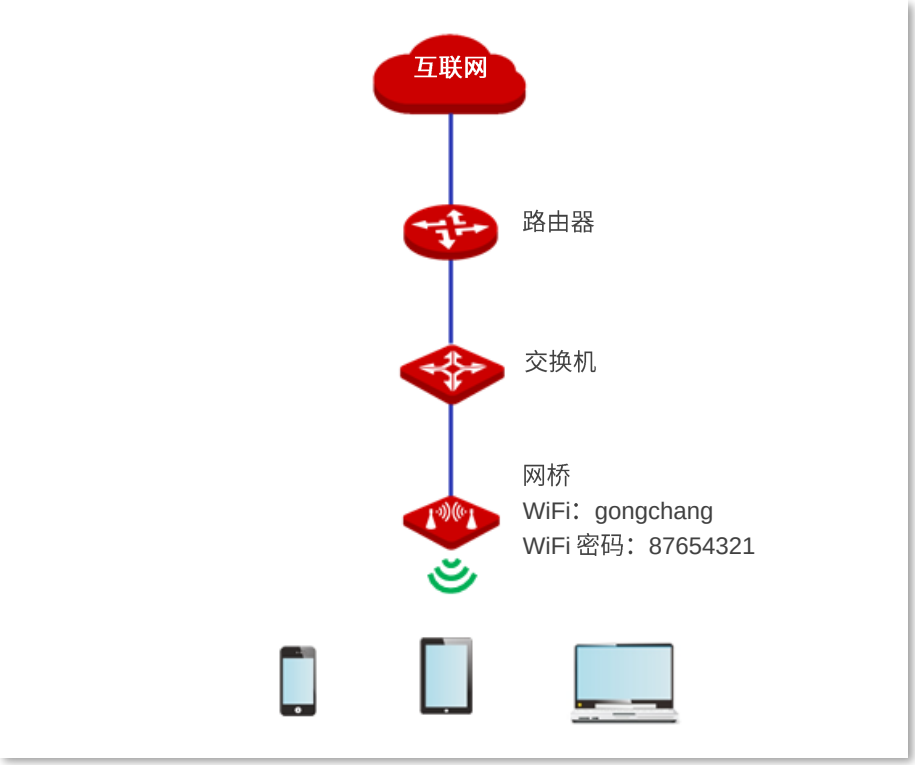
无线设备连接无线网络“FREE”时，不需要输入无线密码就可以连接成功。

WPA 个人加密无线网络配置举例

组网需求

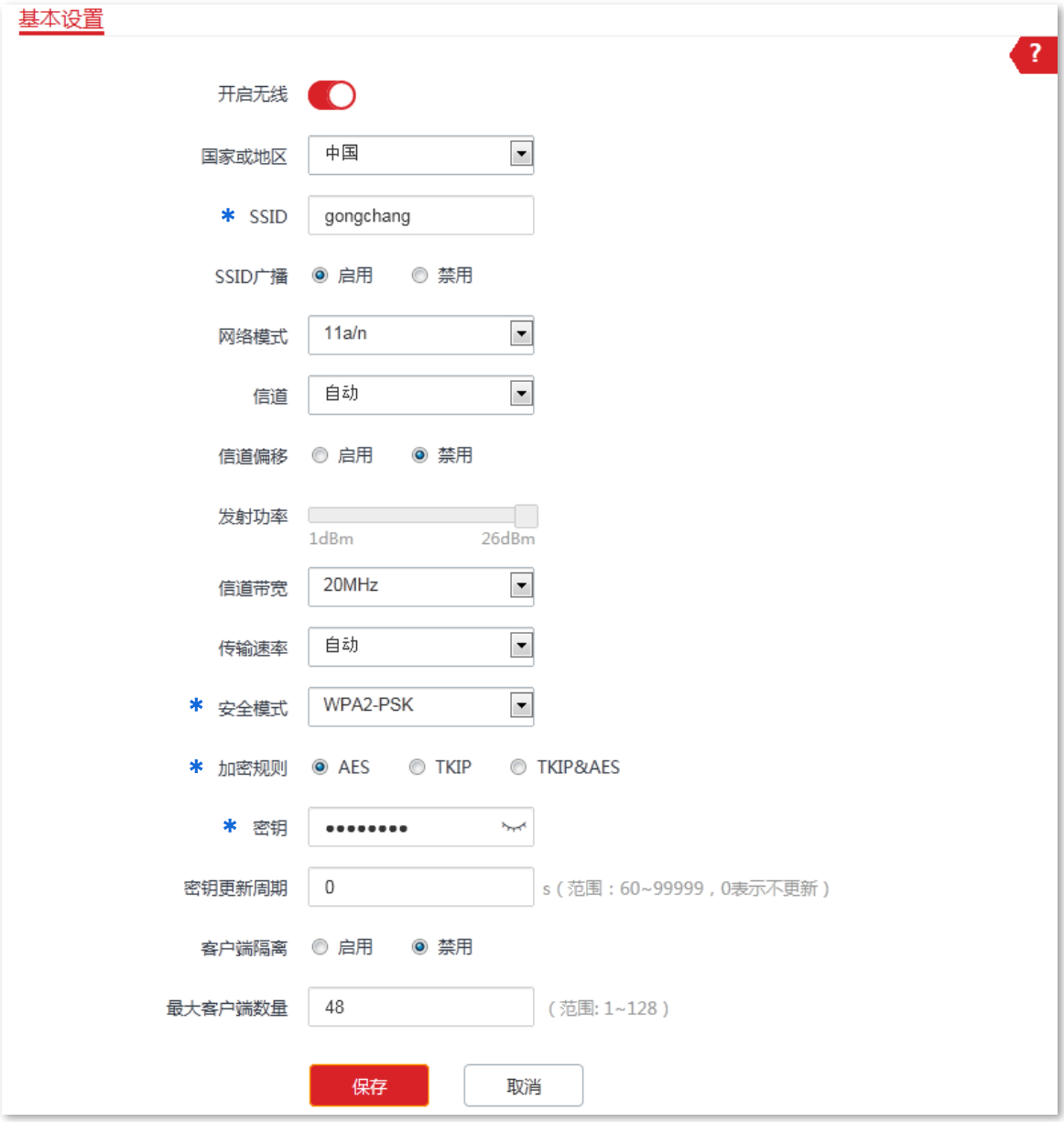
某厂区使用网桥进行组网实现厂区监控。要求：有一定安全性，且配置简单。

针对上述需求，建议采用 WPA2-PSK 安全模式。



配置步骤

1. 点击「无线设置」>「基本设置」。
2. 修改“SSID”为“gongchang”。
3. 选择“安全模式”，建议为“WPA2-PSK”。
4. 选择“加密规则”，建议为“AES”。
5. 设置“密钥”为“87654321”。
6. 点击 保存 。



----完成

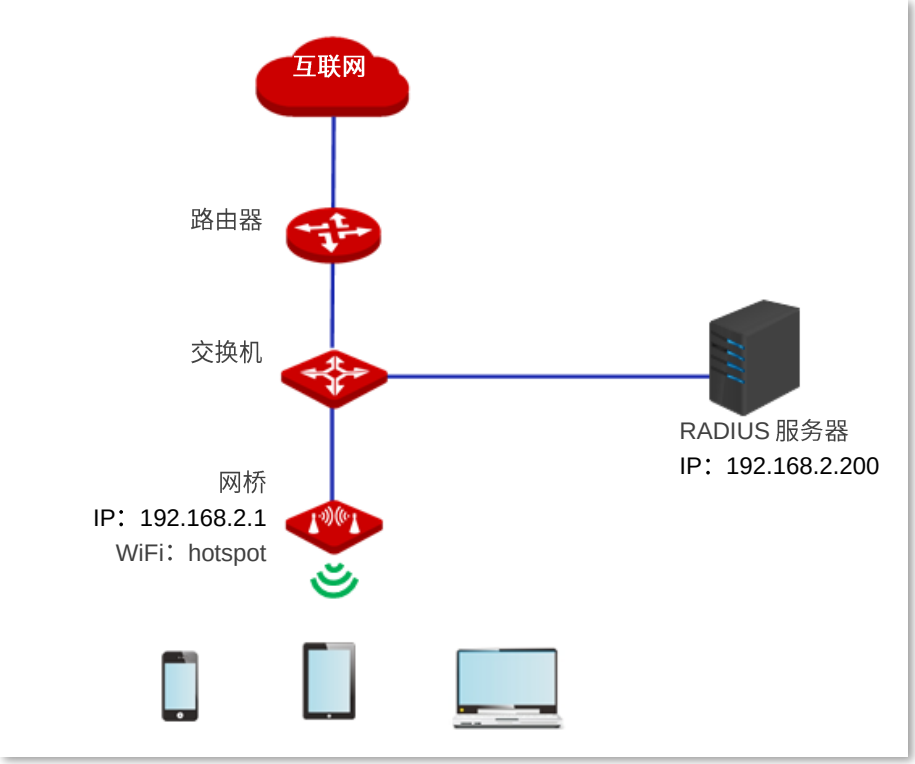
验证配置

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. 点击「无线设置」>「基本设置」。
2. 修改“SSID”，即无线网络名称，本例为“hotspot”。
3. 选择“安全模式”，建议为“WPA2”。
4. 输入 RADIUS 服务器地址，本例为“192.168.2.200”。
5. 输入“RADIUS 端口”，本例为“1812”。
6. 选择“加密规则”，建议为“AES”。
7. 设置“RADIUS 密码”为“12345678”。
8. 点击 保存 。

二、配置 RADIUS 服务器

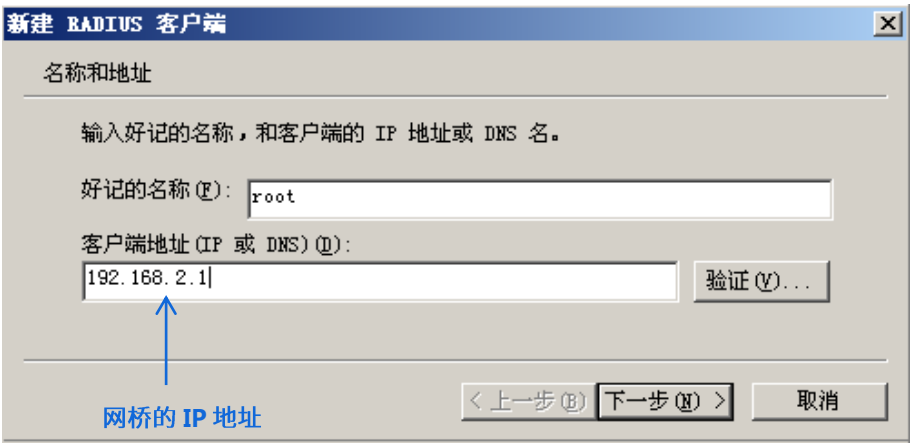
提示

以 Windows 2003 服务器上的 RADIUS 服务器为例说明。

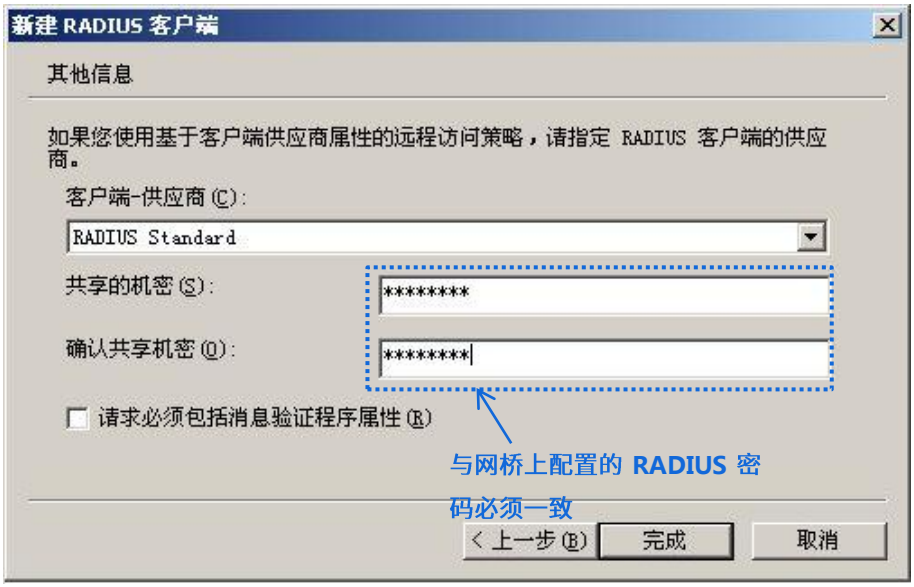
1. 配置 RADIUS 客户端。

   (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。



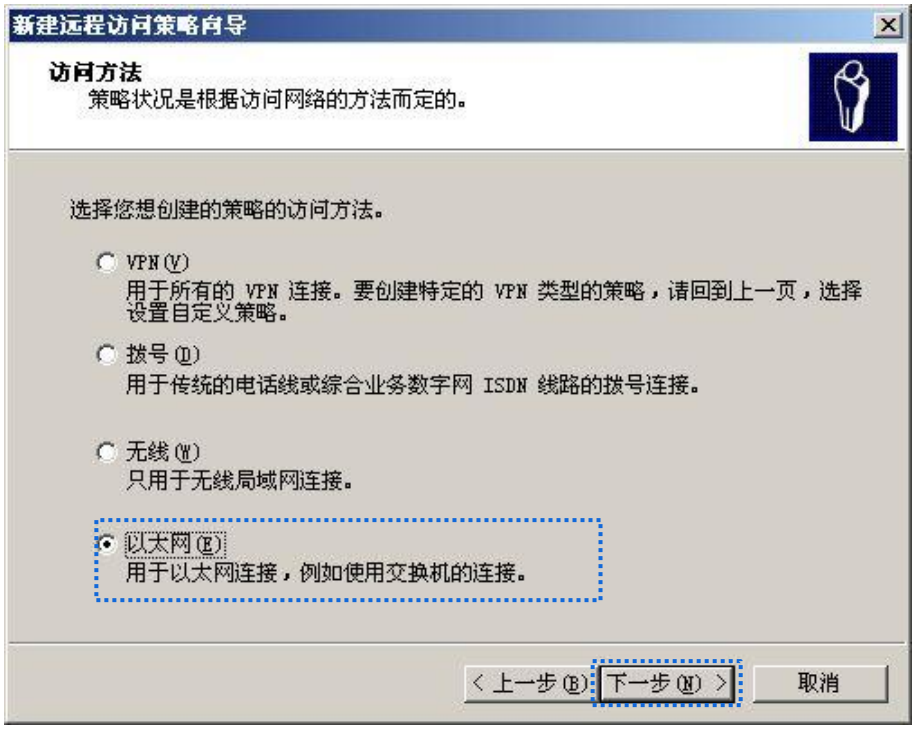
2. 配置远程访问策略。

(1) 右击“远程访问策略”，选择“新建远程访问策略”。

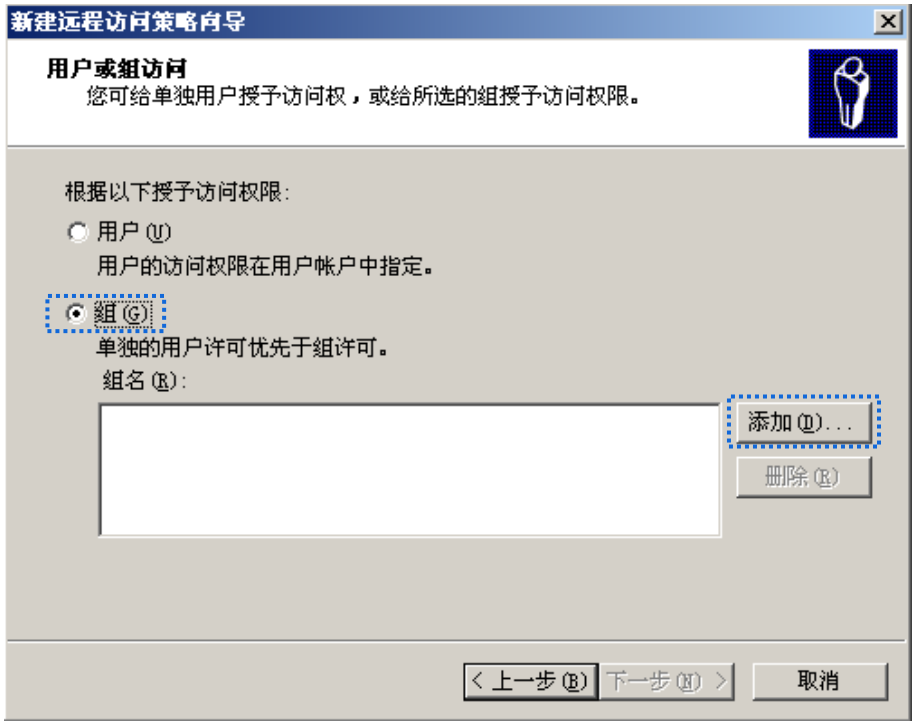
(2) 弹出新建远程访问策略向导，点击 下一步 。

(3) 设置策略名，点击 下一步 。

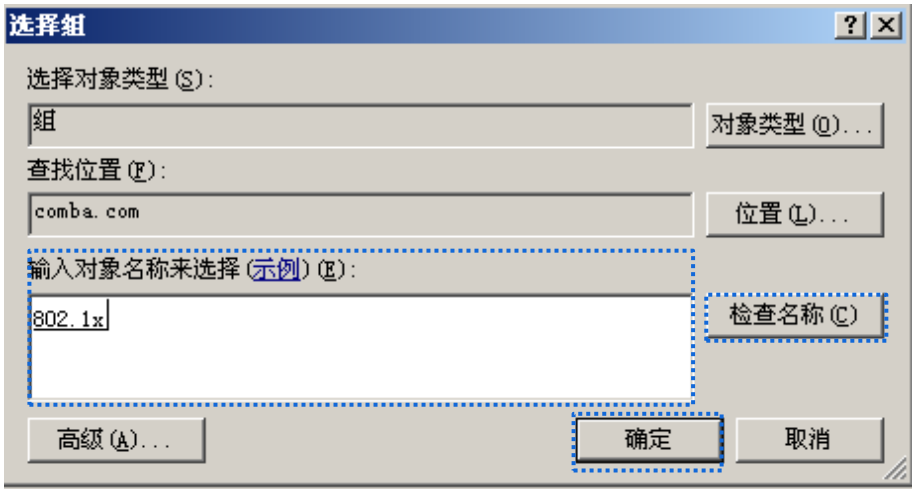
(4) 选择“以太网”，点击 下一步 。



(5) 选择“组”，点击 添加 。

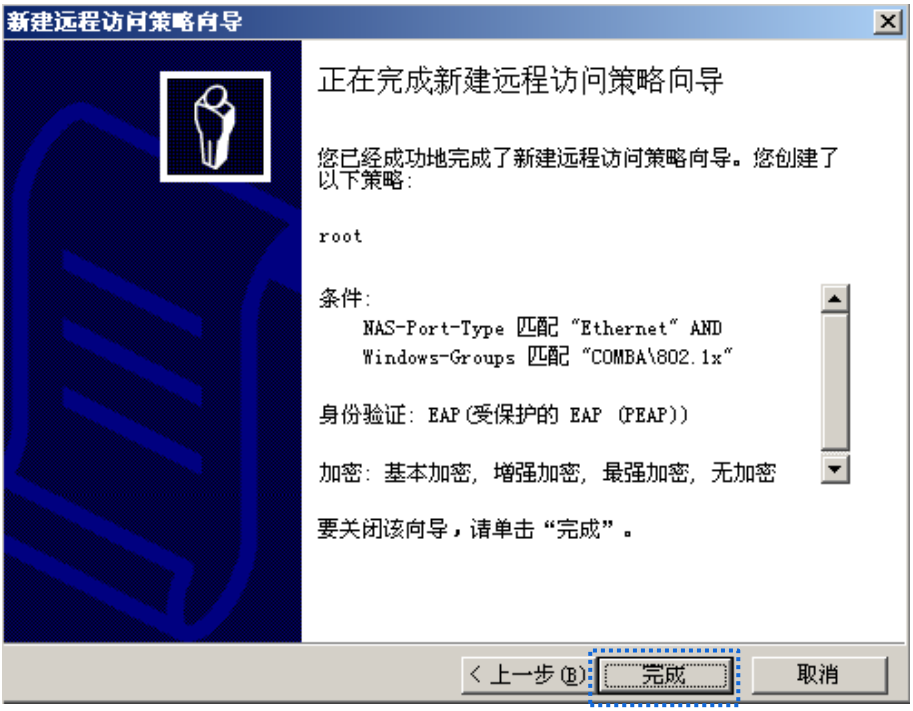


(6) 在“输入对象名称来选择”中输入 802.1x，点击 检查名称 ，点击 确定 。

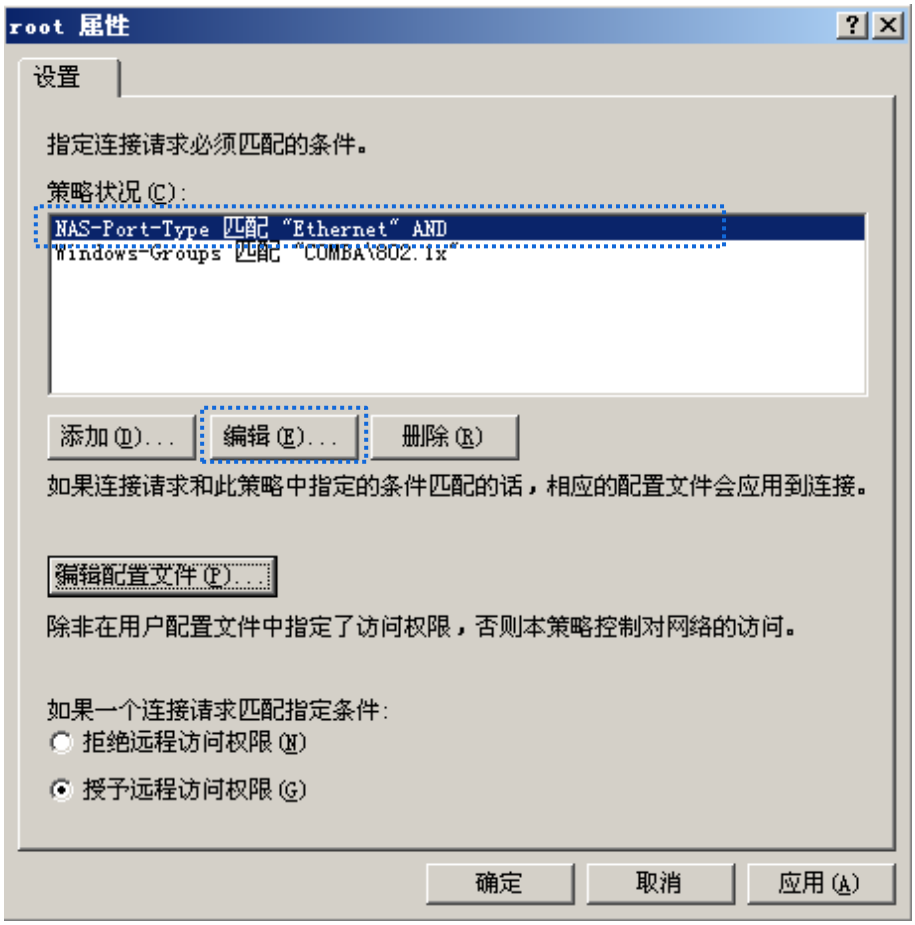


(7) 选择受保护的 EAP (PEAP)，点击 下一步 完成操作。

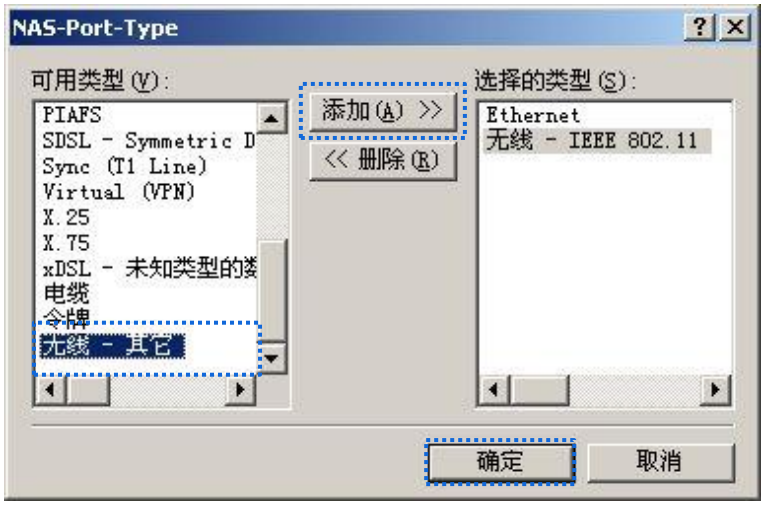
(8) 完成新建远程访问策略向导操作。



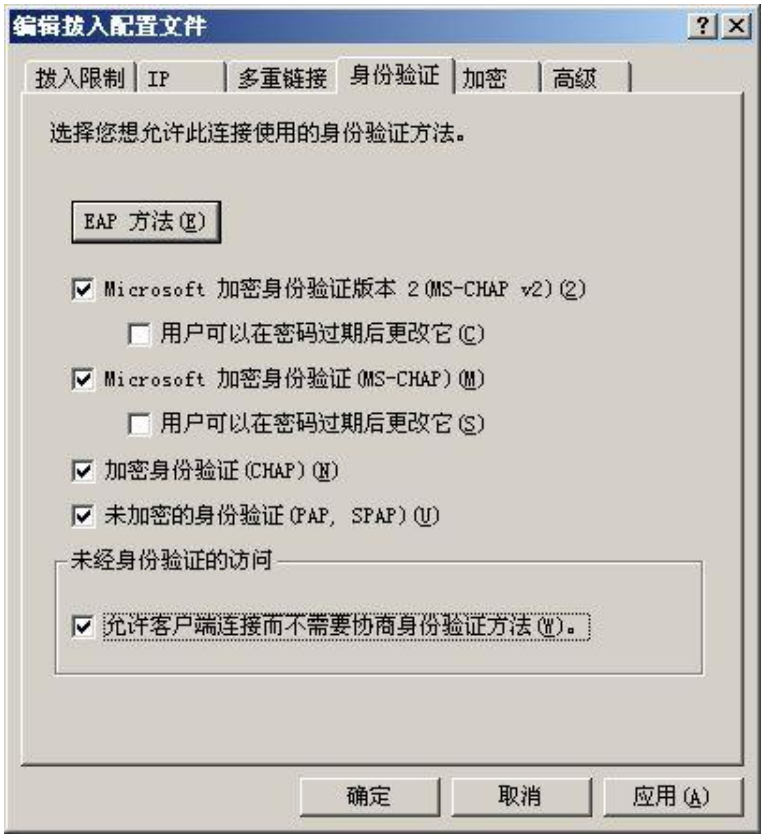
(9) 选中 root，点击右键，选择“属性”，在打开的窗口中，选择“授予远程访问权限”，然后选择“NAS-Port-Type 匹配 “Ethernet”AND”，点击 编辑 。



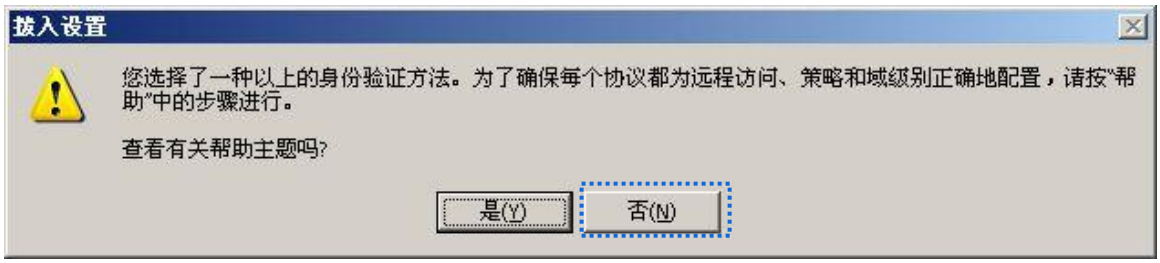
(10) 在出现的窗口选择“无线-其它”，点击 添加>> ，然后点击 确定 。



(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

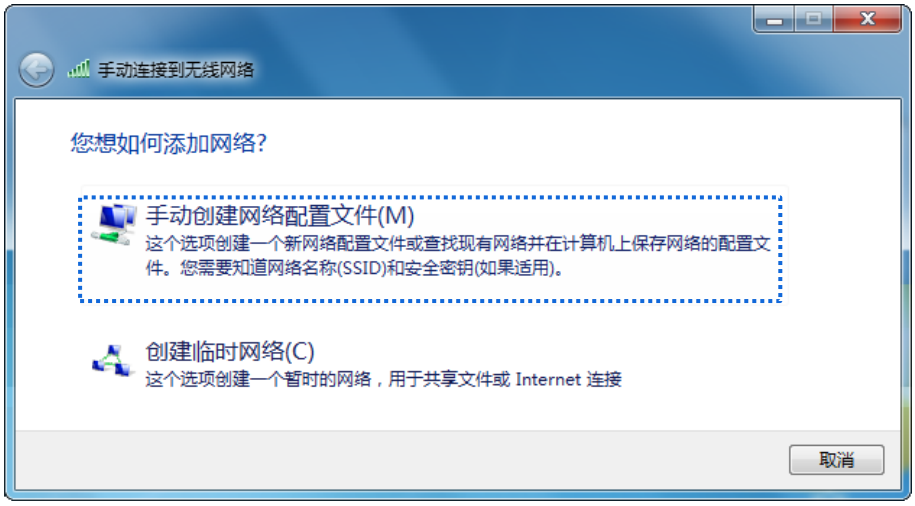
提示

本文以 Windows 7 系统为例说明。

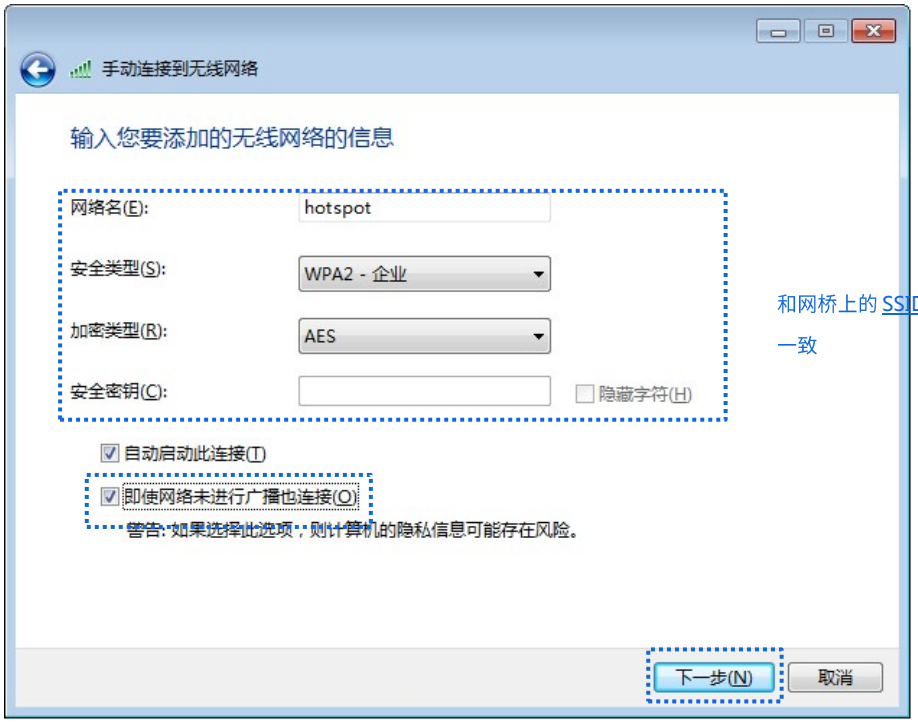
1. 在「控制面板」>「网络和 Internet」>「网络和共享中心」页面，点击“管理无线网络”。

2. 点击“添加”。

3. 选择“手动创建网络配置文件（M）”。

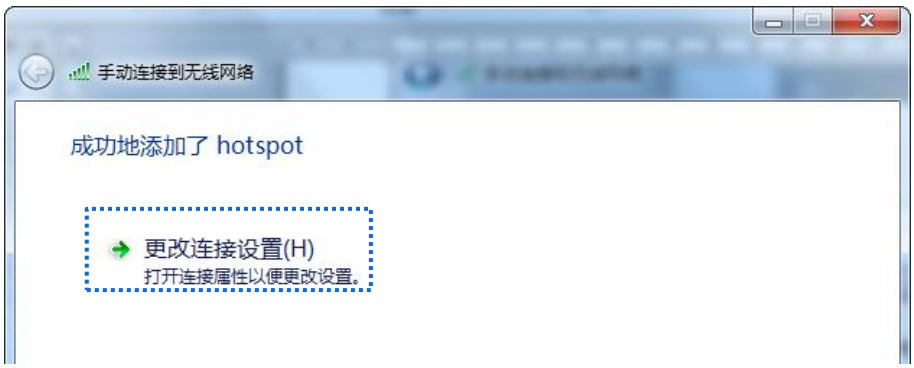


4. 如下图所示输入无线网络信息，勾选“即使网络未进行广播也连接”，然后点击 下一步 。

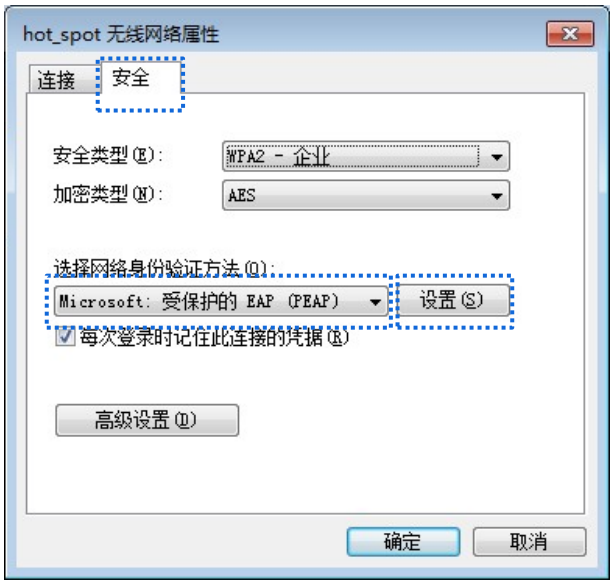


和网桥上的 SSID 安全模式设置保持一致

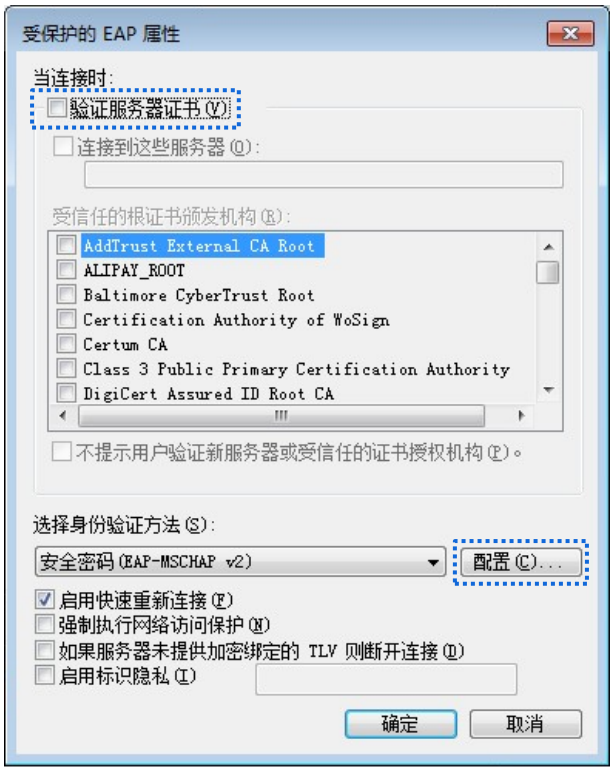
5. 点击“更改连接设置（H）”。



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

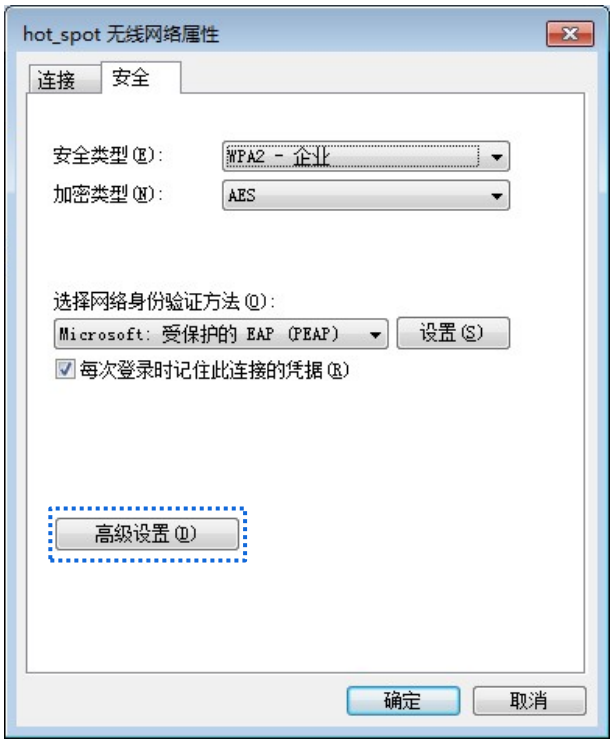


7. 取消“验证服务器证书”，然后点击 配置 。

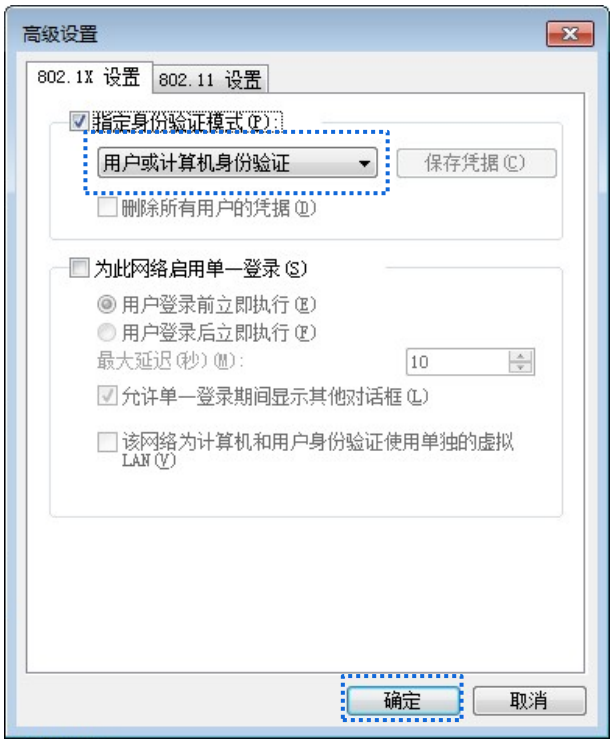


8. 取消“自动使用 windows 登录名和密码”，点击 确定 。

9. 点击 高级设置 。



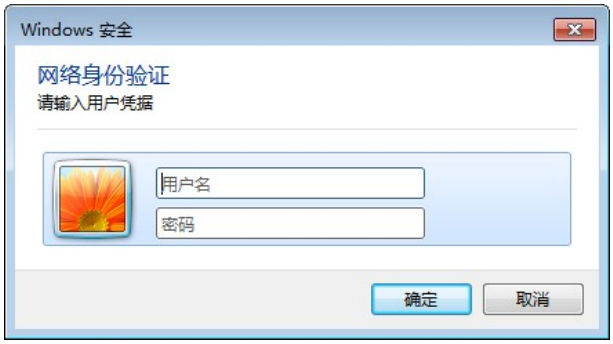
10. 指定身份验证模式为“用户或计算机身份认证”，然后点击 确定 。



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 。



----完成

验证配置

用户设备连接无线网络“hotspot”成功。

7.2 高级设置

本模块用于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。

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”能降低网桥的电能消耗。默认禁用。

标题项	说明
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。
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。 提示 仅 AP 模式、客户端模式、万能中继模式支持。
IMAX	IMAX 是 IP-COM 特有的时分多址（TDMA）技术，允许多个客户端共享同一信道接入网络。启用后，为每个客户端进行时隙分配，并将数据按时隙进行依次传送，从而完成多址连接。 启用 IMAX，可以： – 避免发生“节点隐藏”问题，即避免进行 1 对多桥接时，客户端之间不可见而导致通信失败的问题。 – 减少延时。 – 提高吞吐量和抗干扰能力。 – 提高 1 对多桥接的整体性能和带机数量。 提示 网桥启用“IMAX”后，仅接受启用“IMAX”设备的连接请求，不支持或未开启“IMAX”的 WiFi 设备（如智能手机、笔记本电脑等）将不能接入网桥的无线网络。
穿墙能力	设置网桥的穿墙能力。 – 强覆盖：当周边环境干扰小时，选择此选项可使传输距离更远。 – 高密度：当周边环境干扰大时，选择此选项可提高无线抗干扰能力。
TPC	传输功率控制。用于调节网桥的发射功率。 当两个设备距离太近时，信号饱和，可能导致协商速率降低。启用 TPC 功能后，当网桥接收到对端网桥的信号强度高于-25dBm 时，自动降低自身的发射功率，避免发生协商速率降低的情况。
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。
传输距离	网桥的无线传输距离，可根据网桥之间的安装距离进行设置。
Beacon 间隔	设置网桥发送 Beacon 帧的时间间隔。 Beacon 帧按规定的时间间隔周期性发送，以公告无线网络的存在。一般来说：间隔越小，无线客户端接入网桥的速度越快；间隔越大，无线网络数据传输效率越高。

标题项	说明
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。
LED1 信号灯阈值 LED2 信号灯阈值 LED3 信号灯阈值	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

进入页面：点击「无线设置」>「访问控制」。

在这里，您可以通过设置访问控制规则，允许或禁止指定设备连接到网桥的无线网络。访问控制功能默认关闭。

7.3.2 配置访问控制

1. 点击「无线设置」>「访问控制」。
2. 点击滑块至 。
3. 根据需要选择访问控制模式为“仅允许”或“仅禁止”。
4. 输入要进行访问控制的 MAC 地址。
5. 点击 添加 。

如果要限制的无线设备已连接网桥，可以点击 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 。

----完成

参数说明

标题项	说明
SSID	网桥的无线网络名称。
访问控制	访问控制功能开关。表示关闭， 表示开启。
模式	设置访问控制模式。 - 仅允许：仅允许访问控制列表中的无线客户端连接到网桥的无线网络。 - 仅禁止：仅禁止访问控制列表中的无线客户端连接到网桥的无线网络，其他无线客户端可以连接到网桥的无线网络。

7.3.3 访问控制配置举例

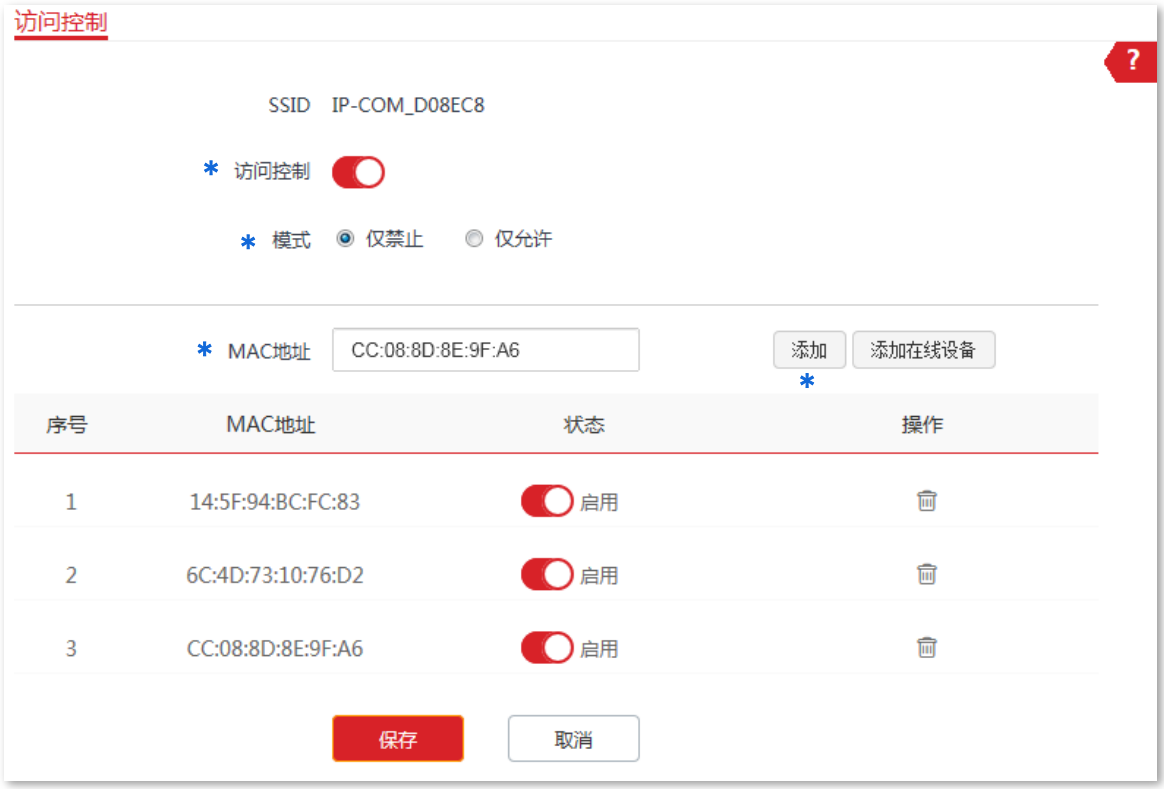
组网需求

某小区使用网桥进行无线组网，现需要禁止几个用户连接网桥的无线网络。

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：14:5F:94:BC:FC:83、6C:4D:73:10:76:D2、CC:08:8D:8E:9F:A6。

配置步骤

1. 点击「无线设置」>「访问控制」。
2. 点击滑块至 。
3. 选择“模式”为“仅禁止”。
4. 在“MAC 地址”栏输入“14:5F:94:BC:FC:83”，点击 添加 。
5. 重复步骤 4，添加 MAC“6C:4D:73:10:76:D2”、“CC:08:8D:8E:9F:A6”。
6. 点击 保存 。



----完成

验证配置

只有上述 3 台无线设备不可以连接网桥的无线网络，其他设备可以连接该网络。

8 高级设置

8.1 LAN 口速率

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和双工模式。修改时，请确保线路两端的接口的速率和双工模式要保持一致。默认为自动协商。下图以 CPE6SV1.0 为例。

修改接口的速率和双工模式后，可以在“系统状态”页面查看。

参数说明

标题项	说明
自动协商	接口的速率和双工模式由该接口和对端接口自动协商决定。
100Mbps 全双工	接口工作在 100Mbps 速率下，且接口在发送数据包的同时也可以接收数据包。
100Mbps 半双工	接口工作在 100Mbps 速率下，且接口同一时刻只能发送数据包或接收数据包。
10Mbps 全双工	接口工作在 10Mbps 速率下，且接口在发送数据包的同时也可以接收数据包。
10Mbps 半双工	接口工作在 10Mbps 速率下，且接口同一时刻只能发送数据包或接收数据包。

提示

- 如果您手动设置接口的速率和双工模式，请确保对端端口的速率和双工模式为相同的模式或为“自动协商”。
- 低速率模式可以提高接口的网线驱动距离。如果您要延长网桥的 PoE 供电距离，可以尝试修改为低速率模式，如 10Mbps 全双工，此时，请确保对端端口工作模式也为“10Mbps 全双工”或“自协商”。

8.2 网络诊断

进入页面：点击「高级设置」>「网络诊断」。

在这里，您可以扫描周围无线网络，进行 Ping/Traceroute 检测以及速率测试。

8.2.1 扫描信号

扫描周围环境中其它设备的无线信号，并显示出 SSID、MAC、信道、信号强度等信息。您可以根据扫描结果，为网桥选择干扰较小的信道（较少无线信号使用的信道），以提升无线传输效率。

扫描周围无线网络：

1. 点击「高级设置」>「网络诊断」。
2. 从“网络诊断”下拉菜单中选择“扫描信号”。

----完成

稍等片刻，扫描结果将会显示在页面下方，如下图所示。

8.2.2 Ping

Ping 可以用来检测网络的连通性和连通质量。

执行 Ping：

1. 点击高级设置」>「网络诊断」。
2. 从“网络诊断”下拉菜单中选择“Ping”。
3. 从“IP 地址”下拉菜单中选择“手动设置”。
4. 输入目标 IP 地址或域名，此处以“www.baidu.com”为例。
5. 设置 Ping 发送的数据包的个数，建议保持默认设置。
6. 设置 Ping 发送的数据包的大小，建议保持默认设置。
7. 点击 开始 。

----完成

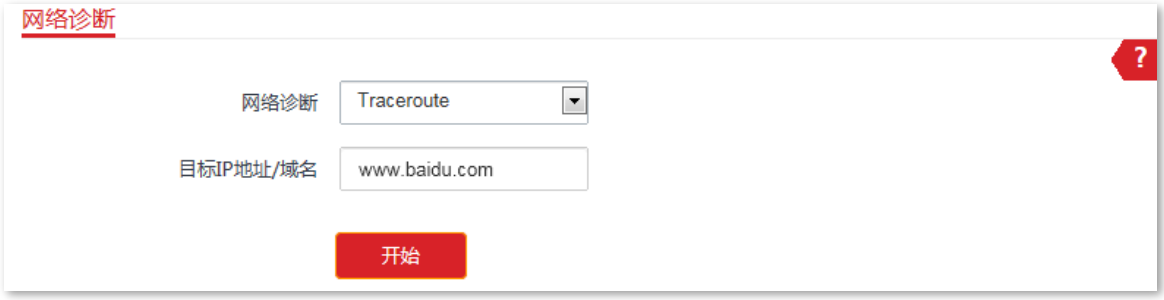
稍后，诊断结果将显示在页面下方。如下图所示。

8.2.3 Traceroute

Traceroute 可以用来检测数据包从网桥到目标主机所经过的路由。

执行 Traceroute：

1. 点击「高级设置」>「网络诊断」。
2. 从“网络诊断”下拉菜单中选择“Traceroute”。
3. 输入目标 IP 地址或域名，此处以“www.baidu.com”为例。
4. 点击 开始 。



----完成

稍后，诊断结果将显示在页面下方。如下图所示。

序号	IP地址	时间
1	172.16.200.1	0.455 ms 0.455 ms 0.358 ms
2	192.168.20.1	1.249 ms 1.426 ms 1.357 ms
3	192.168.21.254	1.311 ms 1.134 ms 0.969 ms
4	100.64.0.1	10.530 ms 6.755 ms 49.191 ms

10 条数据/页 共4条

8.2.4 速率测试

概述

速率测试可以用来检测两个进行无线桥接的网桥（双方均需支持速率测试功能）之间的连接速率，可以帮助您估量两个网桥之间的吞吐量。

在“网络诊断”下拉菜单中选择“速率测试”，将会出现如下页面：

参数说明

标题项	说明
客户端模式 服务器	此版本暂不支持。
对端 AP 的 IP 地址	对端网桥的 IP 地址。 您可以选择已存在的 IP 地址，也可以手动设置。
IP 地址	“对端 AP 的 IP 地址”选项设置为“手动设置”时，在此处输入对端设备的 LAN IP 地址。

标题项	说明
Web 服务端口号	输入对端网桥的 Web 服务端口号以建立基于 TCP/IP 的测速连接。 默认为 80，请保持默认设置。
登录用户名	输入两个网桥之间通信所需的访问凭证，即对端网桥 Web 管理页面的登录用户名及登录密码，以建立基于 TCP/IP 的测速连接。
登录密码	
组数	设置测速连接的数量。
方向	测速方向。 - 接收：仅检测本网桥接收数据的速率。 - 发送：仅检测本网桥发送数据的速率。 - 双向：同时检测本网桥接收和发送数据的速率。
时间	设置速率测试的持续时间。默认为 30 秒。
测试进度	显示测速的进度。

检测速率

假设网桥 1 工作在 AP 模式，网桥 2 工作在客户端模式且已经成功桥接网桥 1 的无线网络。现在要测试两个网桥之间的吞吐量。假设基本信息如下：

- 网桥 1 的 IP 地址：192.168.2.1
- 网桥 1 的登录用户名/密码：admin
- 网桥 2 的 IP 地址：192.168.2.2
- 网桥 2 的登录用户名/密码：admin

设置步骤：

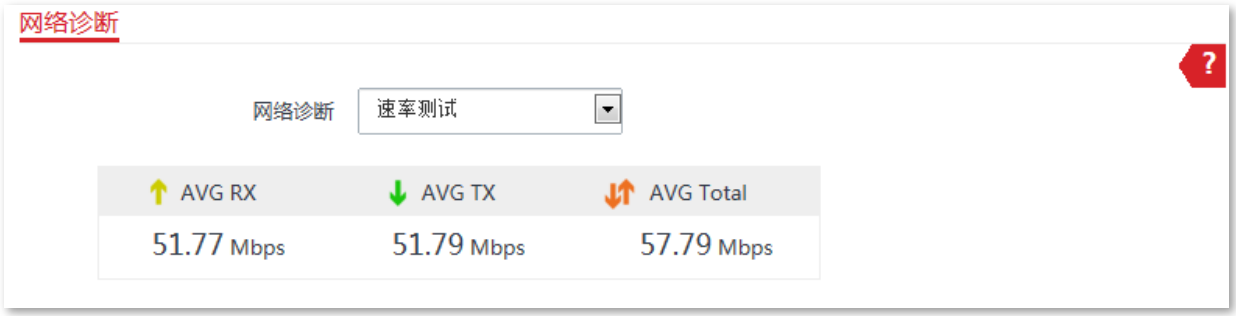
1. 登录网桥 1 或网桥 2 管理页面，此处以网桥 2 为例。
2. 点击「高级设置」>「网络诊断」。
3. 从“网络诊断”下拉菜单中选择“速率测试”。
4. 从“对端 AP 的 IP 地址”下拉菜单中选择“手动设置”。
5. 在“IP 地址”选项输入对端网桥的 LAN 口 IP 地址，本例为“192.168.2.1”。
6. 输入对端网桥 Web 管理页面的登录用户名和密码，本例为“admin”。
7. 从“方向”下拉菜单中选择“双向”。
8. 点击 开始 。

----完成

稍后，诊断结果将显示在页面下方。如下图所示。

测速结果各项参数说明：

- AVG RX：接收速率平均值。
- AVG TX：发送速率平均值。
- AVG Total：总的连接速率平均值。



8.2.5 频谱分析

通过频谱分析功能，您可以查看每个信道周围的无线噪声分布情况，然后选择噪声强度较低的频段来作为网桥的工作频段。

执行频谱分析：

1. 点击「高级设置」>「网络诊断」。
2. 从“网络诊断”下拉菜单中选择“频谱分析”。
3. 选择要检测的频段，此处以 36（5180MHz）到 165（5825MHz）为例。
4. 点击 开始 。

5. 点击 确定 。

----完成

稍后，诊断结果将显示在页面下方。如下图示例。

可根据扫描结果，选择干扰较少信道作为网桥的工作信道。如下图扫描结果，可选择 153~165 作为网桥的工作信道。

网络诊断
网络诊断
频谱分析
选择频段
36(5180MHz)
165(5825MHz)
开始
峰值
当前值
平均值
0
-25
-50
-75
-100
-125
信号强度(dBm)
36
40
44
48
149
153
157
161
165

8.3 带宽控制

8.3.1 概述

带宽控制功能仅在无线 WAN 模式、路由模式下可用。

通过带宽控制功能，网络管理员可以对用户的网速进行限制，使有限的带宽资源得到合理分配。

进入页面：点击「高级设置」>「带宽控制」。

参数说明

标题项	说明
备注	设置带宽控制规则的备注信息。
IP 地址范围	设置 IP 地址范围，以指定规则对应的用户。
最大上传速率	指定 IP 地址范围内的单用户最大上传/下载速率。
最大下载速率	
状态	规则的启用状态，可根据需要启用或禁用。
操作	点击 可以删除规则。

8.3.2 带宽控制配置举例

组网需求

某公司使用网桥组建网络，网络管理员已将网桥设置为无线 WAN 模式并接入互联网。为了保证局域网用户的上网质量，合理、公平地利用带宽，现需要进行带宽控制，使每个局域网用户都能使用 1Mbps 的带宽。

假设局域网用户电脑的 IP 地址范围为 192.168.2.100~192.168.2.200。

配置步骤

1. 点击「高级设置」>「带宽控制」。
2. 设置规则的备注信息，如“网速限制”。
3. 设置规则适用的 IP 地址范围，本例为“192.168.2.100~192.168.2.200”。
4. 设置规则中用户的最大上传速率和下载速率，本例均为“1Mbps”。
5. 点击 添加 。

----完成

添加成功，如下图所示。

验证配置

IP 地址在 192.168.2.100~192.168.2.200 范围内的每个用户，最大上传速率为 1Mbps，最大下载速率为 1Mbps。

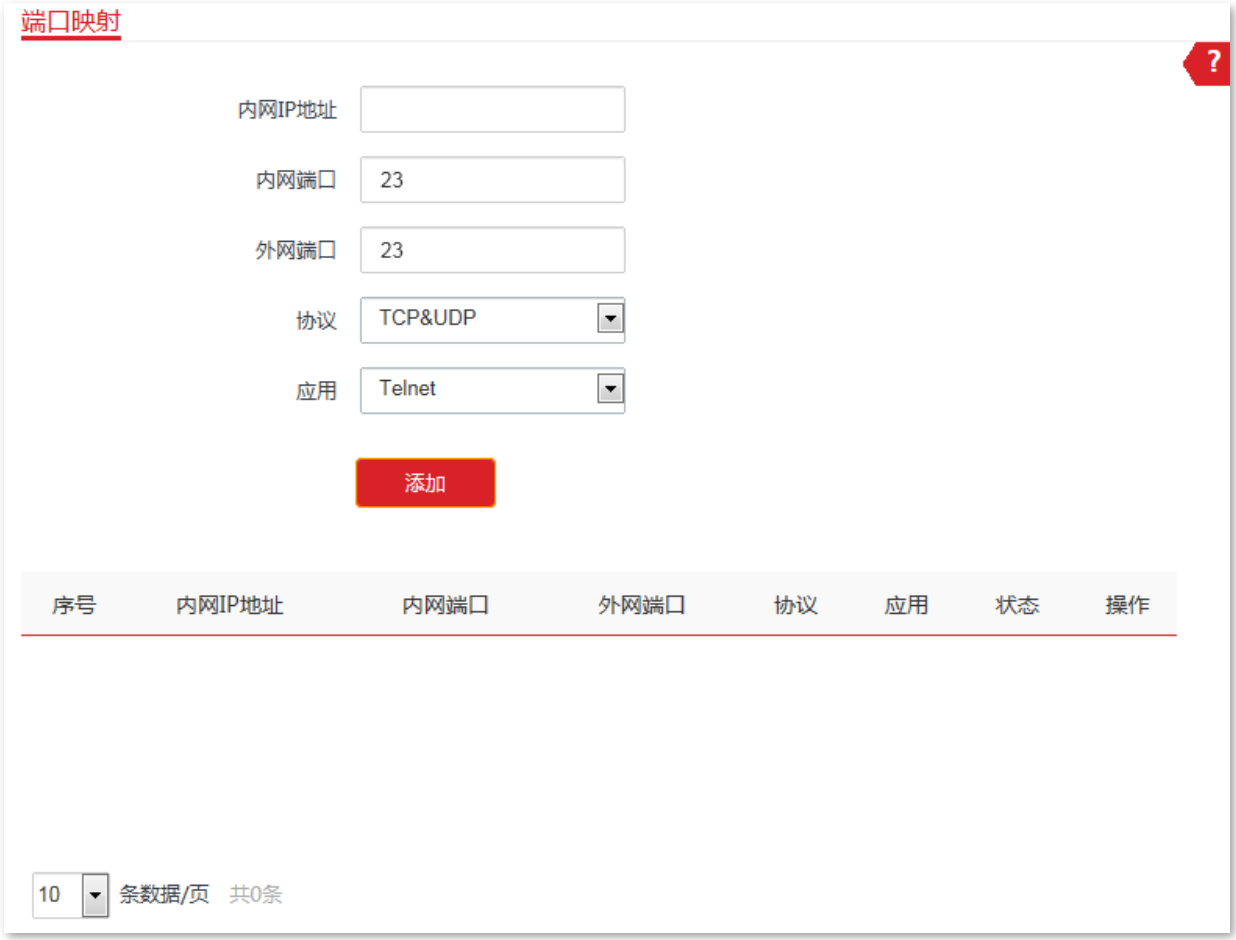
8.4 端口映射

8.4.1 概述

端口映射功能仅在无线 WAN 模式、路由模式下可用。

默认情况下，广域网中的用户不能访问局域网内的设备。端口映射开放了一个或多个服务端口，并以 IP 地址和内网端口来指定其对应的局域网服务器，之后，网桥将广域网中对此服务端口的请求定位到该局域网服务器上，这样，广域网中的用户就能够访问局域网服务器，局域网也能避免受到侵袭。

进入页面：点击「高级设置」>「端口映射」。



参数说明

标题项	说明
内网 IP 地址	内网服务器的 IP 地址。
内网端口	内网服务器的服务端口。 选择相应的“应用”后会自动填充，也可以自定义。如果您清楚内网服务端口号，可直接输入。如果不清楚，可在“应用”下拉菜单中选择相应服务，之后，系统会自动填充端口号。

标题项	说明
外网端口	网桥开放给广域网用户访问的端口。 您可以自定义此端口号。也可以在“应用”下拉菜单中选择相应服务，之后，系统会自动填充端口号。
协议	内网服务的协议类型。设置时，如果不确定服务的协议类型，可以选择“TCP&UDP”。
应用	内网服务器的服务。 设置时，选择相应的“应用”，“内网端口”和“外网端口”将会自动填充。
状态	规则的启用状态，可根据需要启用或禁用。
操作	点击 可以删除规则。

8.4.2 端口映射配置举例

组网需求

某公司使用网桥组建网络，网络管理员已将网桥设置为无线 WAN 模式并接入互联网。现需要将公司内部的 Web 服务器开放给广域网用户，使员工不在公司时也能访问企业内部网络。

方案设计

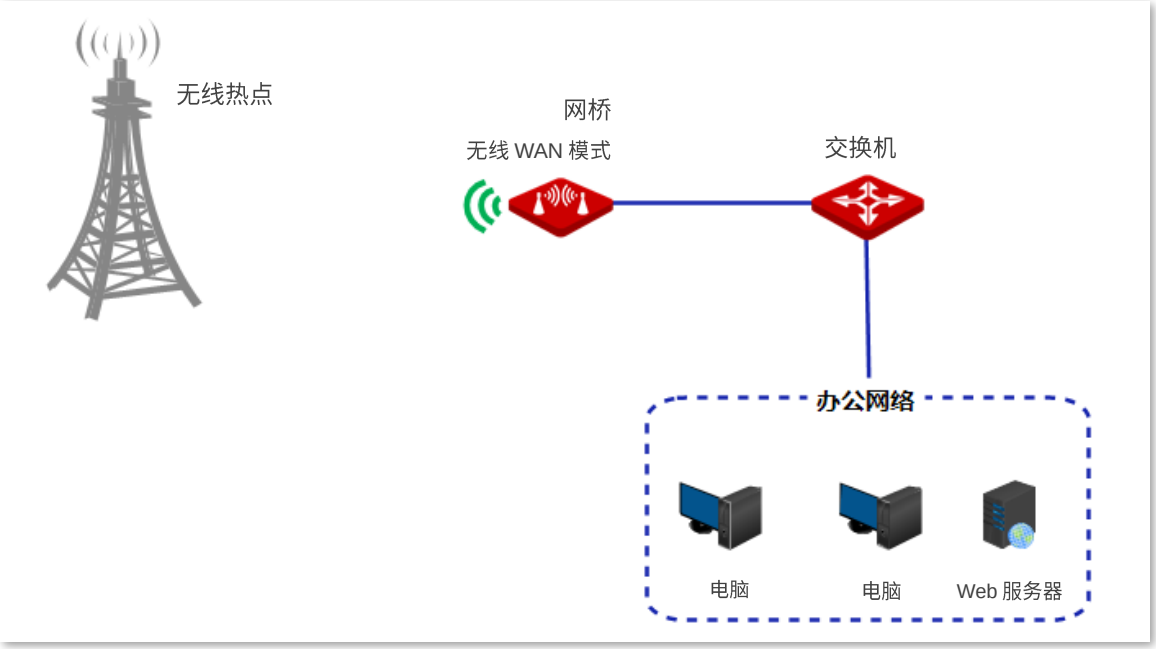
使用端口映射功能实现互联网用户访问公司内部 Web 服务器的需求。

假设：

- 网桥的 WAN 口 IP 地址：202.105.11.22
- Web 服务器地址：192.168.2.100
- Web 服务端口：9999

提示

- 配置前请确保网桥 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址，将导致功能无法实现。IPv4 常用的地址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。
- 互联网服务提供商可能不会支持未经报备的使用默认端口号 80 访问的 Web 服务。因此，在设置端口映射时，建议将外网端口设为非熟知端口（1024~65535），如 9999，以确保可以正常访问。
- 内网端口和外网端口可设置为不同的端口号。

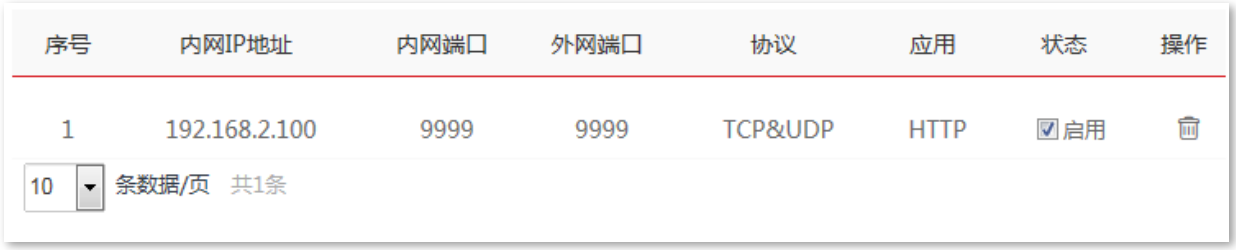


配置步骤

1. 点击「高级设置」>「端口映射」。
2. 输入内网 Web 服务器的 IP 地址，本例为“192.168.2.100”。
3. 选择内网建立的应用，本例为“HTTP”。
4. 设置内网端口，即内网 Web 服务器端口，本例为“9999”。
5. 设置外网端口，可设置为与内网端口一致。
6. 选择 Web 服务器使用的协议，如果不确定，可以选择“TCP&UDP”。
7. 点击 添加 。

----完成

添加成功，如下图所示。



验证配置

互联网上的用户使用“内网服务应用层协议名称://WAN 口当前的 IP 地址”可以成功访问内网服务器。如果设置的外网端口号不是内网服务的默认端口号，访问格式为“内网服务应用层协议名称://WAN 口当前的 IP 地址:外网端口”。

在本例中，访问地址为“http://202.105.11.22:9999”。

您可以在「系统状态」页面找到 WAN 口当前 IP 地址。

如果 WAN 口开启了动态 DNS，还可使用“内网服务应用层协议名称://WAN 口域名:外网端口”访问。

提示

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。

- 确保您填写的内网端口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的 IP 地址，避免因为 IP 地址变化而导致服务中断。

8.5 MAC 过滤

8.5.1 概述

MAC 过滤功能仅在无线 WAN 模式、路由模式下可用。

通过 MAC 过滤功能，您可以控制用户能否通过网桥访问互联网，并设置允许或禁止访问的时间段。

进入页面：点击「高级设置」>「MAC 过滤」。

MAC 过滤功能默认禁用，选择 MAC 过滤模式为“仅禁止”后，页面显示如下：

参数说明

标题项	说明
模式	MAC 过滤规则模式。 - 禁用：不启用 MAC 过滤功能。 - 仅禁止：拒绝列表中 MAC 地址对应的设备通过网桥上网，允许其他设备通过网桥上网。 - 仅允许：允许列表中 MAC 地址对应的设备通过网桥上网，拒绝其他设备通过网桥上网。
备注	MAC 过滤规则的备注信息。
MAC 地址	规则对应的用户设备的 MAC 地址。
时间	规则生效的时间段。“00:00~00:00”表示全天。

标题项	说明
日期	规则生效的具体日期。
状态	规则的启用状态，可根据需要启用或禁用。
操作	点击 可以删除规则。

8.5.2 MAC 过滤配置举例

组网需求

某公司使用网桥组建网络，网络管理员已将网桥设置为无线 WAN 模式并接入互联网。

要求：上班时间（周一到周五的 8:00~18:00），仅允许某一采购人员访问互联网，其他员工禁止访问互联网。

可以使用网桥的“MAC 过滤”功能实现上述需求。

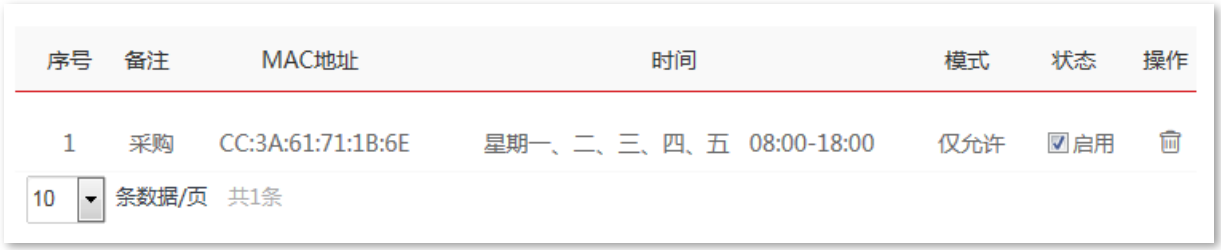
假设该采购人员电脑的物理地址为 CC:3A:61:71:1B:6E。

配置步骤

1. 点击「高级设置」>「MAC 过滤」。
2. 选择 MAC 过滤规则的模式，本例为“仅允许”。
3. 设置规则的备注，如“采购”。
4. 输入采购人员电脑的 MAC 地址，本例为“CC:3A:61:71:1B:6E”。
5. 选择规则生效的时间段，本例为“08:00~18:00”。
6. 选择规则生效的日期，本例为“星期一到星期五”。
7. 点击 添加 。

----完成

添加成功，如下图所示。



验证配置

在星期一到星期五的 8:00~18:00，局域网中，只有使用 MAC 地址为 CC:3A:61:71:1B:6E 的电脑才能访问互联网，使用其他电脑不能访问互联网。

8.6 网络服务

8.6.1 动态 DNS

概述

动态 DNS 功能仅在无线 WAN 模式、路由模式下可用。

动态 DNS，即动态域名服务。当服务运行时，网桥上的动态 DNS 客户端将其当前的 WAN 口 IP 地址传送给动态 DNS 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。

通过动态 DNS 功能，可以让网桥动态变化的 WAN 口 IP 地址（公网 IP 地址）始终被映射到一个固定的域名上。动态 DNS 功能通常与端口映射、DMZ 主机、远程 WEB 管理等功能结合使用，使外网用户可以通过域名访问网桥局域网服务器或网桥管理页面，无需再关注网桥的 WAN 口 IP 地址变化。

进入页面：点击「高级设置」>「网络服务」。

参数说明

标题项	说明
动态 DNS	动态 DNS 功能开关。 表示关闭， 表示开启。
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：Dyndns、No-ip.com、3322.org。
登录用户名	登录动态 DNS 服务的用户名/密码。
登录密码	即在动态 DNS 服务提供商网站上注册的登录用户名及对应登录密码。
域名	在动态 DNS 服务商处申请的域名信息。

动态 DNS 配置举例

组网需求

某公司使用网桥组建网络，网络管理员已将网桥设置为无线 WAN 模式并接入互联网。现需要将公司内部的 Web 服务器开放给广域网用户，使员工不在公司时也能访问企业内部服务器。

方案设计

- 使用端口映射功能实现互联网用户访问公司内部 Web 服务器的需求。
- 使用动态 DNS 功能让互联网用户可以通过固定域名访问公司内部 Web 服务器，防止因 WAN 口 IP 地址变化导致访问失败。

假设 Web 服务器信息如下：

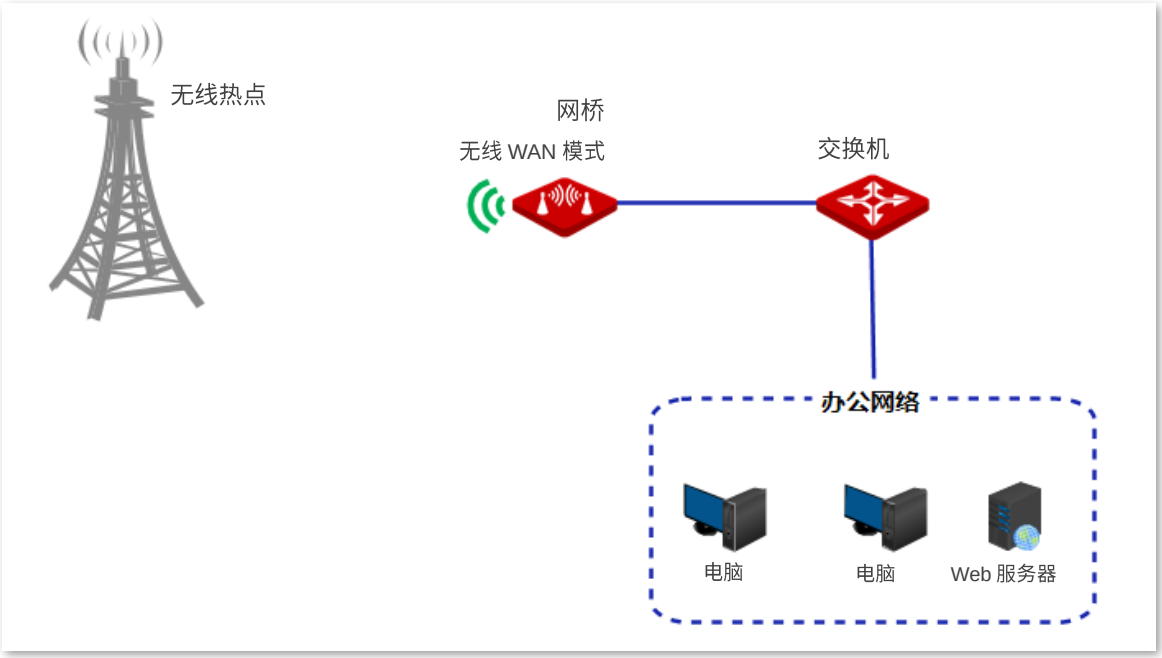
- 服务器地址：192.168.2.100
- 服务端口：9999

假设您到 Dyndns 网站注册的账户信息如下：

- 动态 DNS 登录用户名和密码均为 zhangsan
- 动态 DNS 域名为 zhangsan.dyndns.com

提示

- 配置前请确保网桥 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址，将导致功能无法实现。IPv4 常用的地址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。
- 互联网服务提供商可能不会支持未经报备的使用默认端口号 80 访问的 Web 服务。因此，在设置端口映射时，建议将外网端口设为非熟知端口（1024~65535），如 9999，以确保可以正常访问。
- 内网端口和外网端口可设置为不同的端口号。



配置步骤

1. 设置动态 DNS。

   (1) 点击「高级设置」>「网络服务」，找到“动态 DNS”模块。

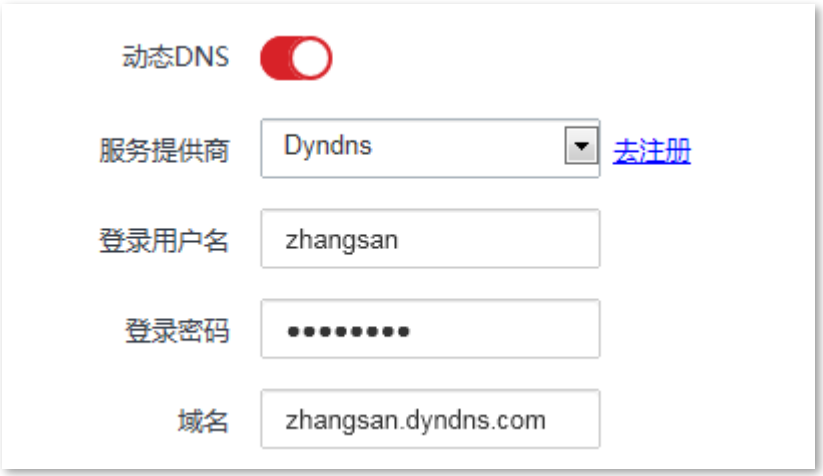
   (2) 点击动态 DNS 滑块至 。

   (3) 选择您申请域名的动态 DNS 服务提供商，本例为“Dyndns”。

   (4) 输入您在动态 DNS 服务提供商网站注册的用户名及对应登录密码，本例均为“zhangsan”。

   (5) 输入您从动态 DNS 服务提供商网站申请的域名，本例为“zhangsan.dyndns.com”。

   (6) 点击页面底端的 保存 。



2. 设置端口映射。

   (1) 点击「高级设置」>「端口映射」。

   (2) 输入 Web 服务器的 IP 地址，本例为“192.168.2.100”。

   (3) 选择内网建立的应用，本例为“HTTP”。

   (4) 设置内网端口，即内网 Web 服务器端口，本例为“9999”。

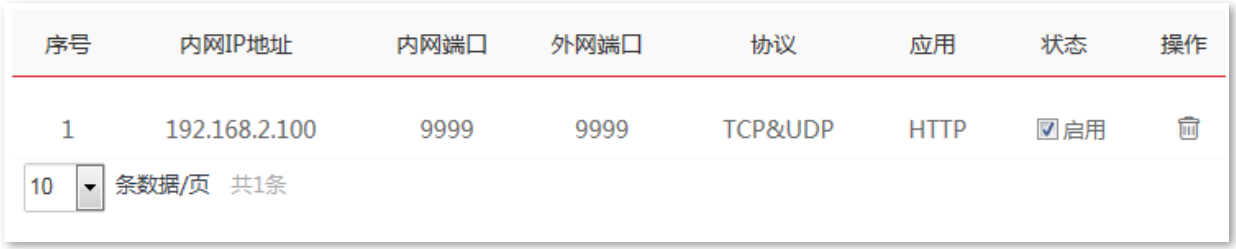
   (5) 设置外网端口，可设置为与内网端口一致。

   (6) 选择 Web 服务器使用的协议“TCP”，如果您不清楚，可以选择“TCP&UDP”。

   (7) 点击 添加 。

----完成

添加成功，如下图所示。



验证配置

互联网上的用户使用“内网服务应用层协议名称://WAN 口域名”可以成功访问内网服务器。添加端口映射规则时，如果设置的外网端口号不是内网服务的默认端口号，访问格式为“内网服务应用层协议名称://WAN 口域名:外网端口”。

在本例中，访问地址为“zhangsan.dyndns.com:9999”。

提示

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。

- 确保您填写的内网端口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的 IP 地址，避免因为 IP 地址变化而导致服务中断。

8.6.2 远程 WEB 管理

概述

远程 WEB 管理功能仅在无线 WAN 模式、路由模式下可用。

一般情况下，只有接到网桥 LAN 口或无线网络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），可以通过 WAN 口远程访问网桥的管理页面。

远程访问网桥的方式为"http://网桥的 WAN 口 IP 地址:端口号"。如果 WAN 口开启了动态 DNS 功能，还可以使用"http://网桥的 WAN 口域名:端口号"访问。

进入页面：点击「高级设置」>「网络服务」。

远程 WEB 管理默认关闭，开启后，页面显示如下：

参数说明

标题项	说明
远程 WEB 管理	远程 WEB 管理功能开关。 表示关闭， 表示开启。
IP 地址	可以远程访问网桥管理页面的电脑的 IP 地址。 – 全部：互联网上任意电脑都能访问网桥的管理页面。为了网络安全，不建议选择此项。 – 手动设置：只有指定 IP 地址的电脑能远程访问网桥的管理页面。如果该电脑在局域网，则应填入该电脑的网关的 IP 地址（公网 IP 地址）。
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 WEB 管理配置举例

组网需求

某公司使用网桥组建网络，网络管理员已将网桥设置为无线 WAN 模式并接入互联网。现在网络遇到其他问题，需要 IP-COM 技术支持远程登录到网桥分析并解决。

可以使用网桥的“远程 WEB 管理”功能实现上述需求。

假设：

- 网桥的 WAN 口 IP 地址：202.105.11.22
- 允许远程访问网桥管理页面的电脑的 IP 地址：202.105.88.77
- 远程 WEB 管理的服务端口号：8080

配置步骤

1. 点击「高级设置」>「网络服务」，找到“远程 WEB 管理”模块。
2. 点击远程 WEB 管理滑块至 。
3. 选择“IP 地址”为“手动设置”，然后输入 IP-COM 技术支持的电脑的 IP 地址，本例为“202.105.88.77”。
4. 点击页面底端的 保存 。

----完成

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:// 202.105.11.22:8080”，即可登录网桥并对其进行管理。如果 WAN 口开启了动态 DNS，还可使用“http://WAN 口域名:8080”访问。

8.6.3 定时重启

概述

进入页面：点击「高级设置」>「网络服务」。

在这里，您可以设置网桥在空闲时间周期性地定时自动重启，预防网桥长时间运行导致其出现性能下降、不稳定等现象。

设置网桥定时重启

1. 点击「高级设置」>「网络服务」，找到“定时重启”模块。
2. 点击定时重启滑块至 。
3. 设置网桥自动重启的时间点，如“3:00”。
4. 选择重启日期，如“星期一到星期五”。
5. 点击页面底端的 保存 。

----完成

如上图设置完成后，星期一到星期五的凌晨 3 点，网桥将自动重启。

8.6.4 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。

进入页面：点击「高级设置」>「网络服务」。

默认 WEB 闲置超时时间为 5 分钟，您可根据需要修改。

8.6.5 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

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。

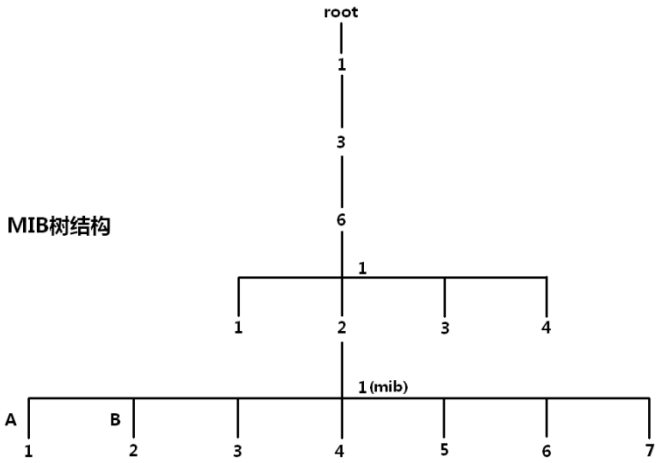
SNMP 协议版本

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）。



进入页面：点击「高级设置」>「网络服务」。

SNMP 代理默认关闭，开启后，页面显示如下：

参数说明

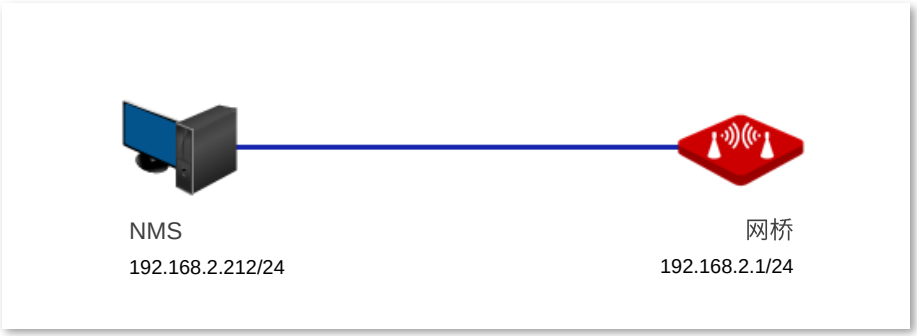
标题项	说明
SNMP 代理	SNMP 代理功能开关。 表示关闭， 表示开启。 SNMP 管理者和 SNMP 代理上的 SNMP 版本必须相同，才能成功互访。目前，网桥中的 SNMP 代理支持 SNMP v1 版本、SNMP v2c 版本。
设备名称	网桥的设备名称，默认为网桥的产品型号+版本号。 提示 建议修改设备名称，使您在使用 SNMP 管理网桥时，能快速识别出对应的网桥设备。

标题项	说明
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

1. 配置网桥。

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

   (1) 点击「高级设置」>「网络服务」，找到“SNMP 代理”模块。

   (2) 点击 SNMP 代理滑块至 。

   (3) 设置只读团体名（读 Community），本例为“zhangsan”。

   (4) 设置读/写团体名（读/写 Community），本例为“zhangsan123”。

   (5) 点击页面底端的 保存 。

2. 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。

8.6.6 Ping 看门狗

Ping 看门狗是网桥的一种“防故障”机制，致力于使用 Ping 工具持续监视网桥与远程主机的特定连接。

Ping 工具通过向目标主机发送 ICMP 回显请求数据包并侦听 ICMP 回显应答来工作。如果未收到定义的回复数量（触发重启丢包个数），则重新启动网桥。

进入页面：点击「高级设置」>「网络服务」。

配置 Ping 看门狗

1. 点击「高级设置」>「网络服务」，找到“Ping 看门狗”模块。
2. 点击 Ping 看门狗滑块至 。
3. 设置相关参数。
4. 点击页面底端的 保存 。

----完成

参数说明

标题项	说明
Ping 看门狗	Ping 看门狗功能开关。 表示关闭， 表示开启。 启用后，Ping 看门狗将周期性地 Ping 用户指定的 IP 地址（如默认网关 IP 地址），如果未收到定义的回复数量（触发重启丢包个数），将重新启动网桥。
IP 地址	指定 Ping 看门狗要监视的目标主机的 IP 地址。
Ping 间隔	指定 Ping 看门狗发送的 ICMP 回显请求报文之间的时间间隔。默认为 300 秒。
启动延迟	网桥启动到启用 Ping 看门狗功能的延迟时间。默认为 300 秒。 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。
触发重启丢包个数	触发网桥重启的最大丢包数，取值范围为 1~65535，默认值为 3。 例如触发重启丢包个数为 N，则当 Ping 看门狗连续发送 N 个 ICMP 回显请求报文至目的 IP 地址，都没有收到应答时，Ping 看门狗将重新启动网桥。

8.6.7 DMZ 主机

概述

DMZ 主机功能仅在无线 WAN 模式、路由模式下可用。

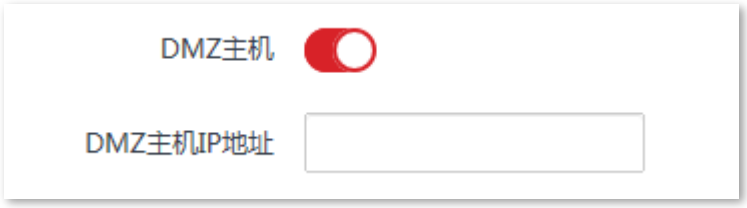
将局域网中某台设备设置为 DMZ 主机后，该设备与互联网通信时将不受限制。如某台电脑正在进行视频会议或在线游戏，可将该电脑设置为 DMZ 主机，使视频会议和在线游戏更加顺畅。

注意

- 将设备设置成 DMZ 主机后，该设备相当于完全暴露于外网，网桥的防火墙对该设备不再起作用。
- 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。

进入页面：点击「高级设置」>「网络服务」。

DMZ 主机默认关闭，开启后，页面显示如下：



参数说明

标题项	说明
DMZ 主机	DMZ 主机功能开关。 表示关闭， 表示开启。
DMZ 主机 IP 地址	要设置为 DMZ 主机的局域网设备的 IP 地址。

DMZ 主机配置举例

组网需求

某公司使用网桥组建网络，网络管理员已将网桥设置为无线 WAN 模式并接入互联网。现需要将公司内部的 Web 服务器开放给广域网用户，使员工不在公司时也能访问企业内部网络。

方案设计

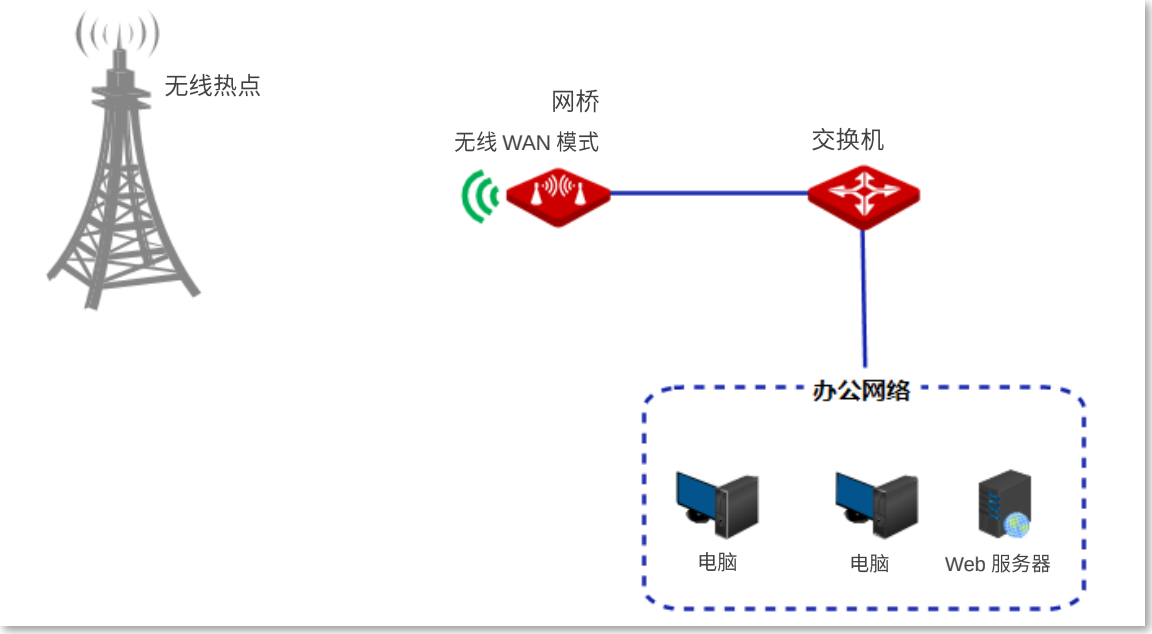
可以使用网桥的“DMZ 主机”功能实现上述需求。

假设：

- 网桥的 WAN 口 IP 地址：202.105.11.22
- 内网 Web 服务器的 IP 地址：192.168.2.100
- 服务端口：9999

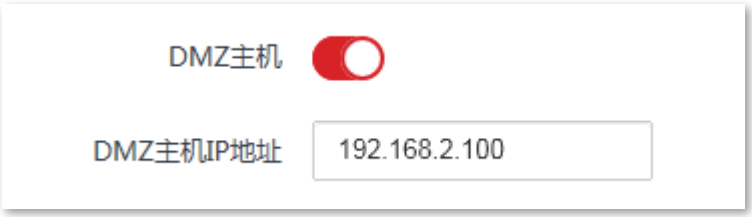
提示

- 配置前请确保网桥 WAN 口获取的是公网 IP 地址，如果是私网 IP 地址，将导致功能无法实现。IPv4 常用的地址类别包括 A 类、B 类和 C 类，A 类地址的私网地址为 10.0.0.0-10.255.255.255；B 类地址的私网地址为 172.16.0.0-172.31.255.255；C 类地址的私网地址为 192.168.0.0-192.168.255.255。
- 互联网服务提供商可能不会支持未经报备的使用默认端口号 80 访问的 Web 服务。因此，在使用 DMZ 主机功能时，建议将内网服务端口设为非熟知端口（1024~65535），如 9999，以确保可以正常访问。



配置步骤

1. 点击「高级设置」>「网络服务」，找到“DMZ 主机”模块。
2. 点击 DMZ 主机滑块至 。
3. 输入局域网内要设置为 DMZ 主机的设备的 IP 地址，本例为“192.168.2.100”。
4. 点击页面底端的 保存 。



----完成

验证配置

互联网上的用户使用“内网服务应用层协议名称://WAN 口当前的 IP 地址”可以成功访问内网服务器。如果内网服务端口不是默认端口号，访问格式为“内网服务应用层协议名称://WAN 口当前的 IP 地址:内网服务端口”。

本例中访问地址为“http://202.105.11.22:9999”。您可在「系统状态」页面找到 WAN 口当前 IP 地址。

如果该 WAN 口开启了动态 DNS，还可使用“内网服务应用层协议名称://WAN 口域名:内网服务端口”访问。

提示

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。

- 可能是 DMZ 主机上的系统防火墙、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的 IP 地址，避免因为 IP 地址变化而导致服务中断。

8.6.8 Telnet 服务

启用 Telnet 服务后，可以通过 Telnet 方式管理网桥，一般用于技术人员维护网桥。

进入页面：点击「高级设置」>「网络服务」。

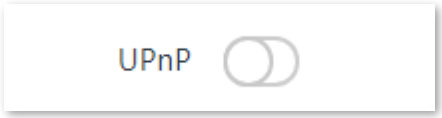
Telnet 服务默认开启。

8.6.9 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。

进入页面：点击「高级设置」>「网络服务」。

UPnP 默认关闭。



8.6.10 硬件看门狗

硬件看门狗利用了一个定时器电路来监控主程序的运行。在网桥主程序正常运行的时候，每隔一段时间会输出一个信号，给定时器清零。如果网桥主程序出现故障，不能在指定时间内提供清零信号，定时器就会溢出并产生复位信号重启网桥系统，使网桥恢复正常工作。

通过硬件看门狗功能，可以在无人干预的情况下，将一些程序潜在错误或恶劣环境干扰等因素导致的系统死机自动恢复，使网桥系统重新进入正常工作状态。

进入页面：点击「高级设置」>「网络服务」。

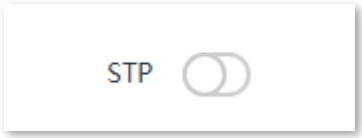
硬件看门狗默认开启。

8.6.11 STP

STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 802.1D 标准建立的，用于在局域网中消除数据链路层物理环路，并提供链路冗余备份的协议。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择地对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环，避免设备发生由于重复接收相同报文导致的报文处理能力下降问题。

进入页面：点击「高级设置」>「网络服务」。

STP 默认关闭。



9 系统工具

9.1 时间与日期

进入页面：点击「系统工具」>「时间与日期」。

在这里，您可以设置网桥的系统时间。

为了保证网桥基于时间的功能正常生效，需要确保网桥的系统时间准确。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”。

提示

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。

9.1.1 网络校时

使用此方式时，系统时间自动同步互联网上的时间服务器。只要网桥成功连接到互联网就能自动校准其系统时间，无需重新设置。网桥联网方法请参考 LAN 口设置。

设置完成后，您可以进入「状态」页面，查看网桥的系统时间是否校对准确。

参数说明

标题项	说明
时间设置	网桥系统时间的设置方式。
校时周期	网桥向互联网上的时间服务器校对系统时间的时间间隔。
时区	选择网桥当前所在地区的标准时区。

9.1.2 手动设置时间

手动设置网桥的系统时间。使用此方式时，网桥每次重启后，您都需要重新设置系统时间。选择“手动设置”时，页面展开的相关参数如下图所示。

设置完成后，您可以进入「状态」页面，查看网桥的系统时间是否校对准确。

参数说明

标题项	说明
系统时间	网桥系统时间的设置方式。
日期	可以直接在此处输入正确的时间，也可以点击 复制本地时间 ，将正在管理网桥的电脑的时间同步到网桥。
时间	

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，可以尝试重启网桥解决。

提示

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. 点击「系统工具」>「设备维护」。
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

- 恢复出厂设置后，网桥所有设置将会恢复到出厂状态，您需要重新设置网桥。请谨慎使用复位操作。
- 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. 点击「系统工具」>「设备维护」。
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

在这里，您可以对网桥进行软件升级，使网桥获得新增功能或更稳定的性能。

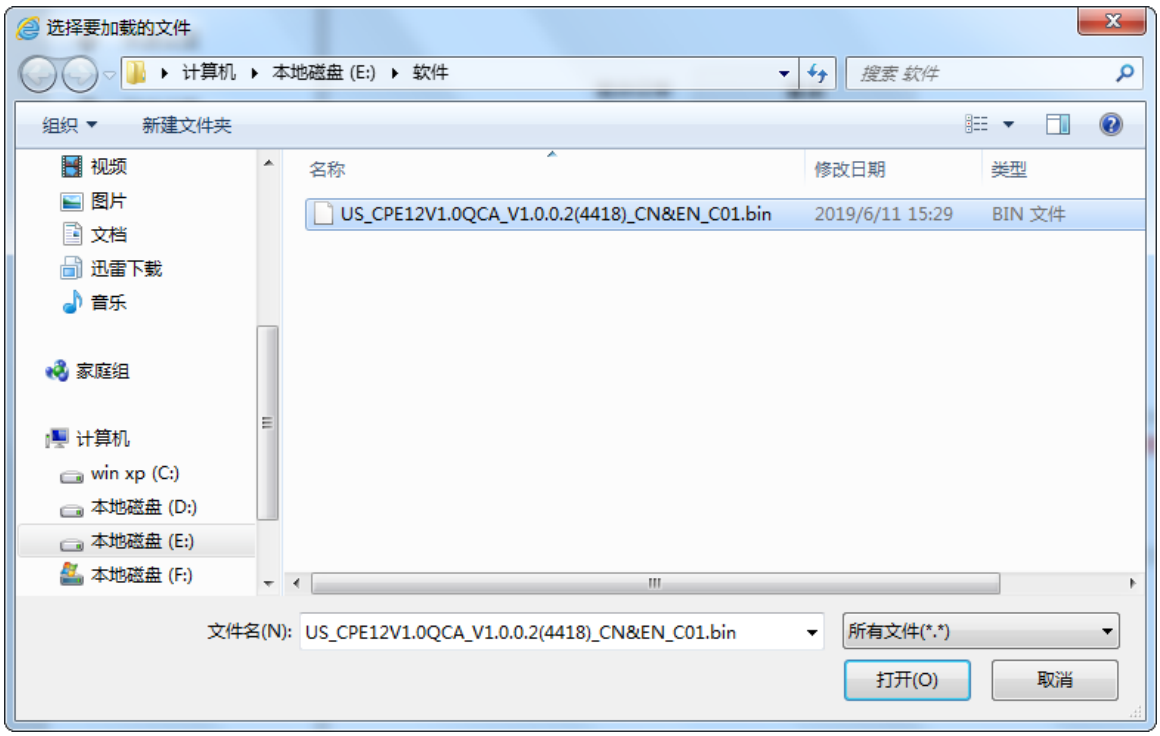
注意

- 为避免网桥损坏，请使用正确的升级文件进行升级。一般情况下，软件升级文件的文件后缀为.bin。
- 升级过程中，请勿断开网桥电源。

软件升级步骤：

1. 访问 IP-COM 官方网站 www.ip-com.com.cn，下载对应型号网桥的软件升级文件到本地电脑并解压。
2. 登录到网桥的管理页面，点击「系统工具」>「设备维护」。
3. 点击 升级 。

4. 从本地电脑选择并加载网桥的升级文件，网桥将会自动升级。



----完成

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”来确认是否升级成功。

提示

为了提高产品的稳定性，体验增值功能，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。

提示

若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. 点击「系统工具」>「设备维护」。
2. 点击 备份/恢复 。

3. 点击 备份 。

4. 确认弹出的提示信息后，点击 保存 。

----完成

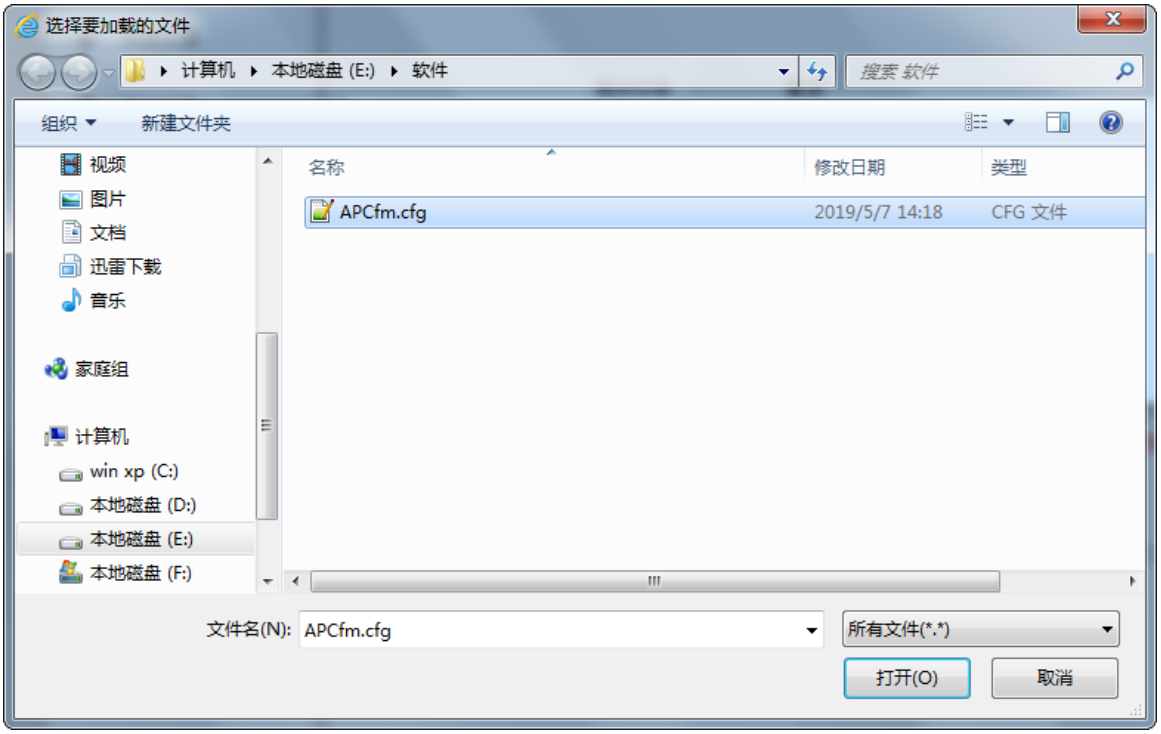
浏览器将下载文件名为 APCfm.cfg 的配置文件。

恢复

1. 点击「系统工具」>「设备维护」。
2. 点击 备份/恢复 。

3. 点击 恢复 。

4. 选择并加载之前备份的配置文件。



----完成

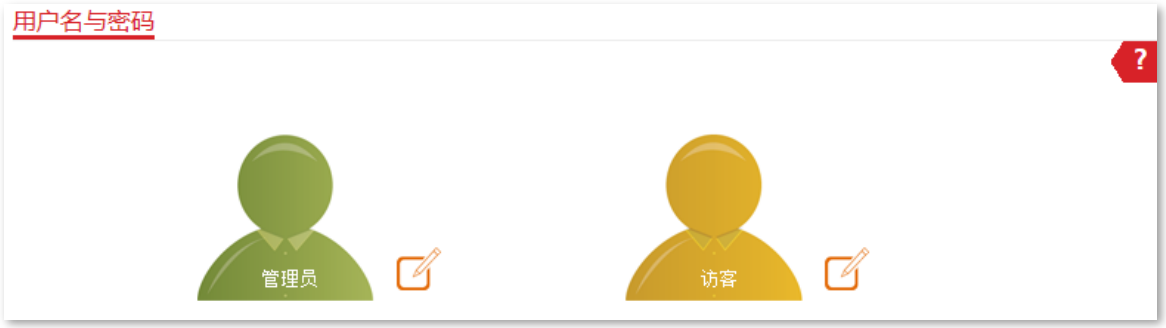
恢复配置状态将显示“正在上传···”，之后，页面会出现重启进度条，请耐心等待。进度条走完后，网桥恢复配置成功。

9.3 用户名与密码

进入页面：点击「系统工具」>「用户名与密码」。

在这里，您可以修改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。管理员账号的默认用户名和密码均为"admin"。

参数说明

标题项	说明
原用户名	当前登录用户名。
原密码	当前登录密码。
新用户名	设置新的登录用户名。
新密码	设置新的登录密码。
确认新密码	再一次输入新的登录密码。

9.3.2 访客

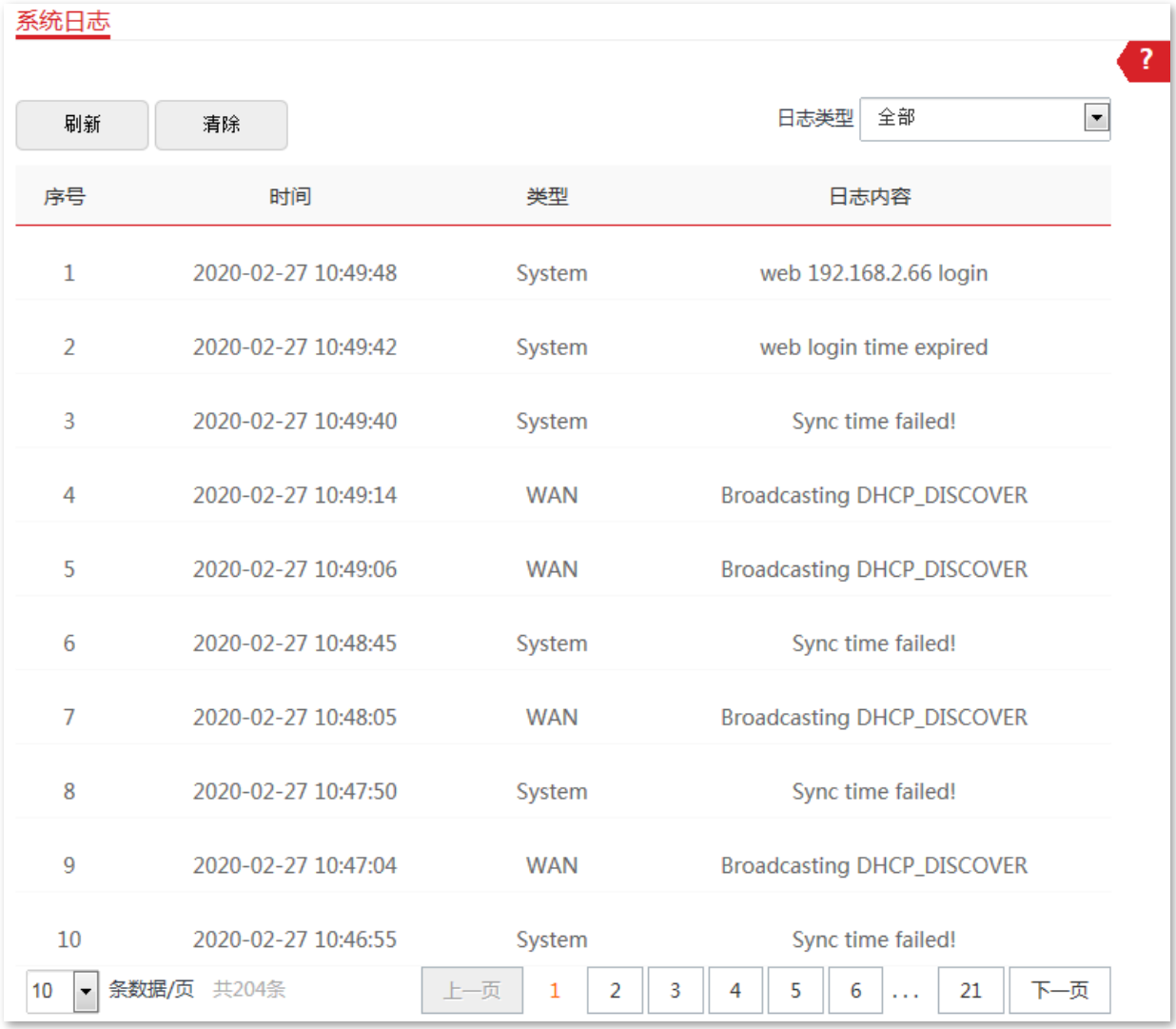
使用访客账号登录网桥后，您只能查看网桥配置信息，不能修改网桥配置。访客账号默认禁用，其默认用户名和密码均为“user”。

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。

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 。



日志记录时间以网桥的系统时间为准，为确保日志记录时间准确，请先准确设置网桥的系统时间。可以到时间与日期页面校准网桥的系统时间。

注意

- 网桥仅记录其最近一次启动后的事件信息。
- 断电后重新上电、配置 VLAN、升级软件、恢复配置、恢复出厂设置等操作都会导致网桥重启。

附录

默认参数（以 CPE12V1.0 为例）

网桥主要参数的默认设置如下表：

参数			默认设置
设备登录	管理 IP 地址		192.168.2.1
	管理员	用户名	admin
		密码	admin
	访客		禁用
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
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
	租约时间		1 天
VLAN 设置	VLAN 设置		禁用
	PVID		1
	管理 VLAN		1
	WLAN		1000

参数		默认设置
无线设置	开启无线	开启
	SSID	IP-COM_XXXXXX。XXXXXX 为网桥 LAN 口 MAC 地址的后六位
	安全模式	不加密
	透明网桥	启用
	IMAX	禁用
	TPC	启用
	LED1 信号灯阈值	-90dBm
	LED2 信号灯阈值	-80dBm
	LED3 信号灯阈值	-70dBm
	WEB 闲置超时时间	5 分钟
	Ping 看门狗	禁用
	Telnet 服务	启用
	UPnP	禁用
	硬件看门狗	启用
	STP	禁用
系统工具	时间与日期	网络校时