



室外点对点网桥

使用说明书

声明

版权所有©2018 深圳市吉祥腾达科技有限公司。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。

Tenda 是深圳市吉祥腾达科技有限公司在中国和（或）其它国家与地区的注册商标。文中提及的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，本文档仅作为产品使用指导，文中的所有陈述、信息和建议均不构成任何形式的担保。

本文档对设备的使用步骤和功能设置步骤提供详细描述，对于页面直接提示信息和简单的信息查看不作详述。

前言

感谢选择腾达产品。开始使用本产品前，请先阅读本说明书。

约定

本说明书适用于腾达所有型号的室外点对点网桥。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 O3 为例。

本文可能用到的格式说明如下。

项目	格式	举例
菜单项	「」	选择「状态」菜单。
按钮	边框+底纹	点击 确定 。

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
AP	Access Point
SSID	Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
VLAN	Virtual Local Area Network
PoE	Power Over Ethernet
WEP	Wired Equivalent Privacy
AES	Advanced Encryption Standard
TKIP	Temporal Key Integrity Protocol

相关资料获取方式

访问 Tenda 官方网站 <http://www.tenda.com.cn>，在右上角搜索栏搜索对应产品型号，可获取最新的产品资料。

技术支持

如需了解更多信息，请通过以下方式与我们联系。

腾达官网：<http://www.tenda.com.cn>



热线：400-6622-666



邮箱：tenda@tenda.com.cn



腾达微信公众号



腾达官方微博

目录

1 产品介绍	1
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
2 应用场景	4
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
3 设备登录	14
3.1 登录网桥的管理页面	14
3.2 退出登录	16
3.3 页面布局	17
3.4 常用按钮	18
4 快速设置	19
4.1 AP 模式	19
4.1.1 概述.....	19
4.1.2 设置 AP 模式.....	19
4.2 客户端模式	22
4.2.1 概述.....	22
4.2.2 设置客户端模式.....	22
4.3 万能中继模式	26
4.3.1 概述.....	26

4.3.2 设置万能中继模式	26
4.4 无线 WAN 模式	30
4.4.1 概述	30
4.4.2 设置无线 WAN 模式	30
4.5 中继模式	34
4.5.1 概述	34
4.5.2 设置中继模式	34
4.6 P2MP 模式	44
4.6.1 概述	44
4.6.2 设置 P2MP 模式	44
4.7 路由模式	51
4.7.1 概述	51
4.7.2 设置路由模式	51
5 状态	54
5.1 系统状态	54
5.2 无线状态	56
5.3 统计	57
5.3.1 吞吐量	57
5.3.2 无线客户端	57
5.3.3 上级 AP	58
5.3.4 接口	58
5.3.5 ARP 表	59
5.3.6 路由表	60
6 网络设置	61
6.1 LAN 口设置	61
6.1.1 概述	61
6.1.2 修改 LAN IP	62
6.2 MAC 克隆	65
6.2.1 概述	65
6.2.2 克隆 MAC 地址	65
6.3 DHCP 服务器	68
6.3.1 概述	68
6.3.2 配置 DHCP 服务器	68

6.4 DHCP 客户端列表	70
6.5 VLAN 设置	71
6.5.1 概述	71
6.5.2 配置 VLAN	71
6.5.3 VLAN 设置举例	72
7 无线设置	75
7.1 基本设置	75
7.1.1 概述	75
7.1.2 修改基本设置	76
7.1.3 基本设置举例	81
7.2 高级设置	98
7.2.1 概述	98
7.2.2 修改高级参数	98
7.3 访问控制	101
7.3.1 概述	101
7.3.2 配置访问控制	101
7.3.3 访问控制配置举例	102
8 高级设置	104
8.1 LAN 口速率	104
8.1.1 概述	104
8.1.2 修改 LAN 口速率	104
8.2 网络诊断	106
8.2.1 扫描信号	106
8.2.2 Ping	107
8.2.3 Traceroute	108
8.2.4 速率测试	109
8.3 带宽控制	114
8.3.1 概述	114
8.3.2 配置带宽控制	114
8.3.3 带宽控制示例	115
8.4 端口映射	117
8.4.1 概述	117
8.4.2 配置端口映射	117

8.4.3 端口映射示例	119
8.5 MAC 过滤	121
8.5.1 概述	121
8.5.2 配置 MAC 过滤	121
8.5.3 MAC 过滤示例	122
8.6 网络服务	124
8.6.1 动态 DNS	124
8.6.2 远程 WEB 管理	128
8.6.3 定时重启	130
8.6.4 WEB 闲置超时时间	131
8.6.5 SNMP 代理	131
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	139
9 系统工具	140
9.1 时间与日期	140
9.2 设备维护	142
9.2.1 重启	142
9.2.2 恢复出厂设置	143
9.2.3 软件升级	144
9.2.4 备份与恢复	145
9.3 用户名与密码	149
9.3.1 管理员	149
9.3.2 访客	150
9.4 系统日志	151
附录	152
A 常见问题解答	152
B 默认参数	153

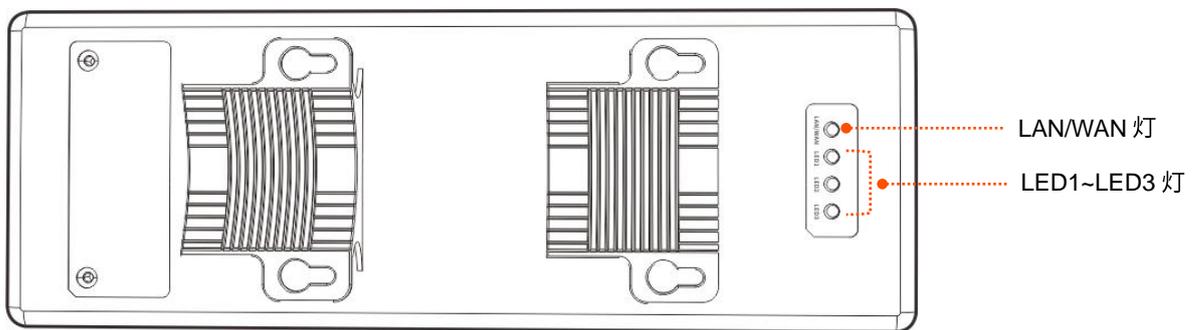
1 产品介绍

1.1 简介

Tenda 室外点对点网桥系列产品适用于电梯、塔吊、小区、工厂、果园、景区等视频监控场景，它内置高增益定向天线，信号穿透力更强；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，可以在户外风、雨、雪等恶劣环境下正常工作。

1.2 外观

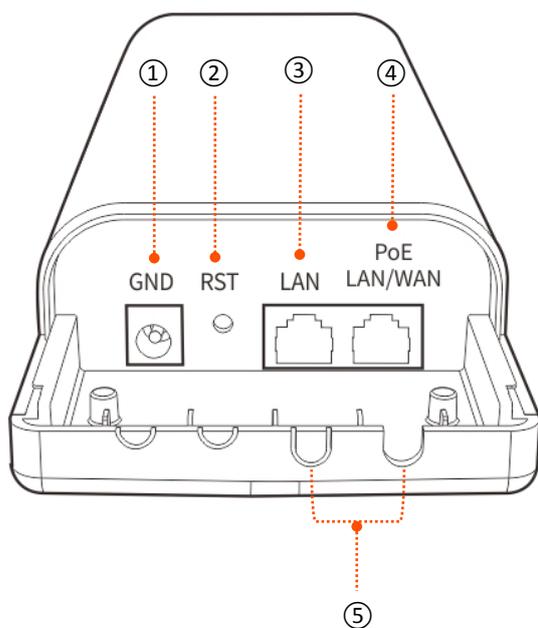
1.2.1 指示灯



指示灯	状态	说明
	长亮	供电正常且接口没有数据传输。
LAN/WAN	闪烁	接口正在传输数据。
	熄灭	供电异常。
LED1、LED2、LED3 (接收信号强度指示灯)	长亮	已有客户端连接网桥。此时，网桥工作在 AP、中继、P2MP 或路由中的一种模式。若是自动桥接，则表明网桥已设置为 AP 模式。 - LED1、LED2、LED3 均长亮：信号强 - LED1、LED2 长亮，LED3 熄灭：信号一般 - LED1 长亮，LED2、LED3 熄灭：信号差，请调整两个网桥的方向或位置。

指示灯	状态	说明
	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

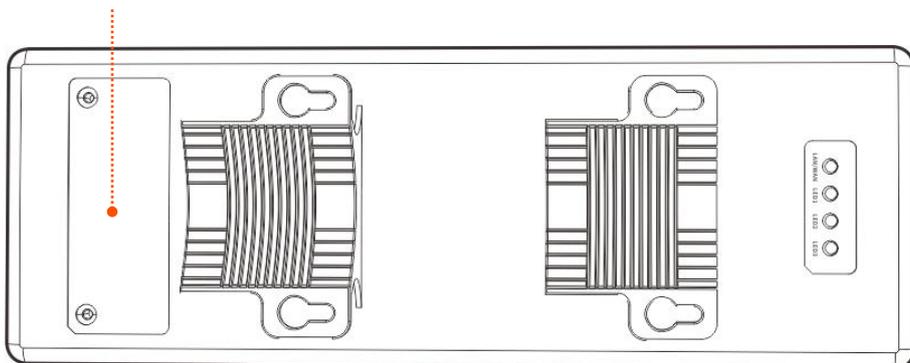


序号	丝印	说明
①	GND	防雷接地柱。 用接地线和配套的接地螺钉将网桥的防雷接地柱与建筑物的接地端相连,以防静电和雷击对设备造成损坏。
②	RST	复位按钮。 网桥通电 1 分钟后,按住 8 秒后松开,指示灯全亮时,网桥已经恢复到出厂状态。
③	LAN	10/100Mbps 自适应 RJ45 口。 可连接交换机、电脑等设备。
④	PoE LAN/WAN	PoE 电源输入、数据传输复用接口。网桥工作在路由模式时为 WAN 口,其他模式下为 LAN 口。 可连接配套的 PoE 注入器给网桥通电。
⑤	/	网线卡槽。

1.2.3 贴纸

贴纸位于网桥的背面，具体位置如下图所示。

贴纸位置



您可以在该贴纸上找到网桥的默认登录 IP 地址、用户名和密码等信息。

Tenda 腾达

深圳市吉祥腾达科技有限公司
技术支持电话: 400-6622-666

5公里室外点对点网桥

型 号 : 03

版 本 : V2.0

IP地址 : 192.168.2.1

输 入 : 12V $\overline{\text{=}}$ 1A

用户名 : admin

密 码 : admin



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。

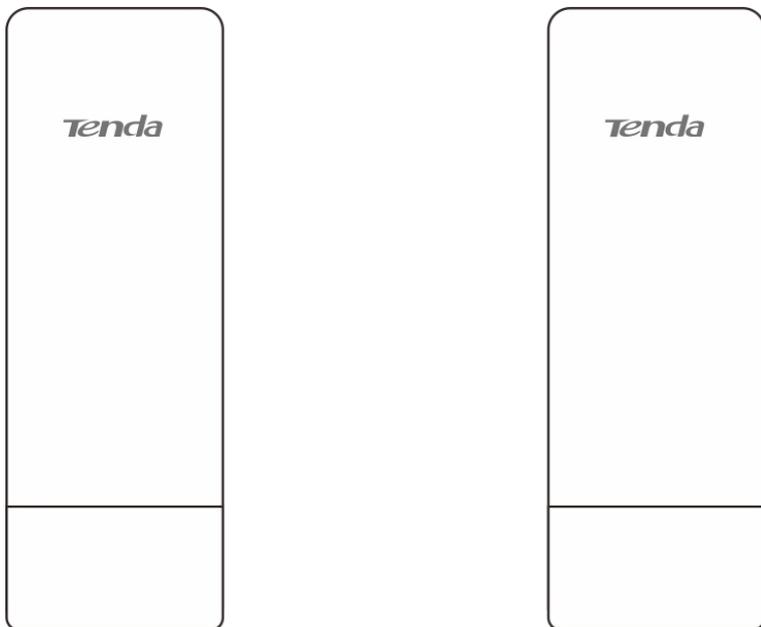
2.1.1 方案

使用无线网桥进行组网。

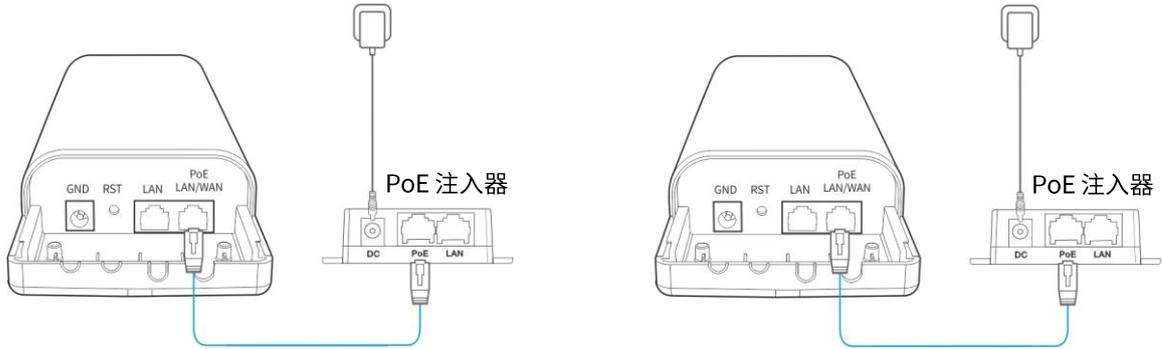
2.1.2 设置网桥

方式一：自动桥接（推荐）

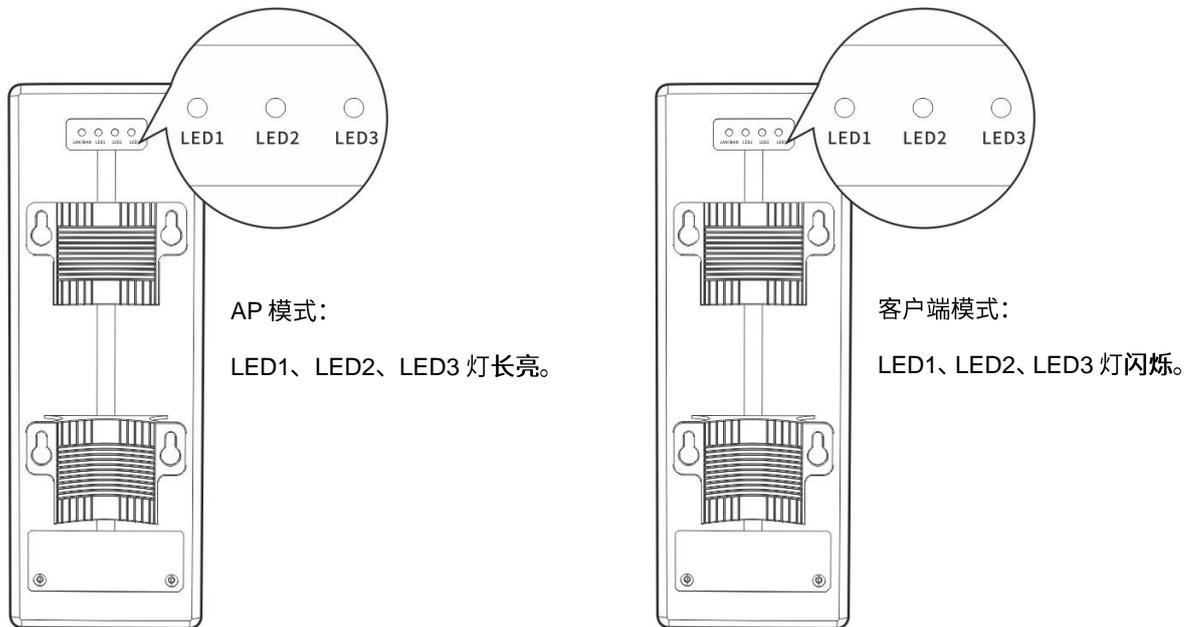
步骤 1 将两台网桥相邻放置，如下图示。



步骤 2 打开网桥的保护盖，使用 PoE 注入器分别给两台网桥通电。系统启动完成后，网桥的 LAN/WAN 灯亮。



步骤 3 两台网桥会自动进行桥接，请注意查看网桥指示灯变化。桥接成功状态如下图示。

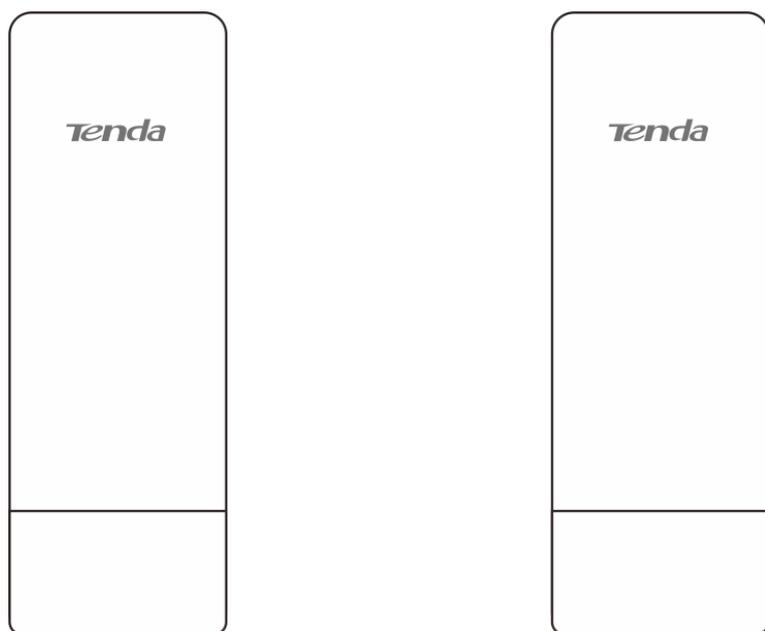


 **注意**

- 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。

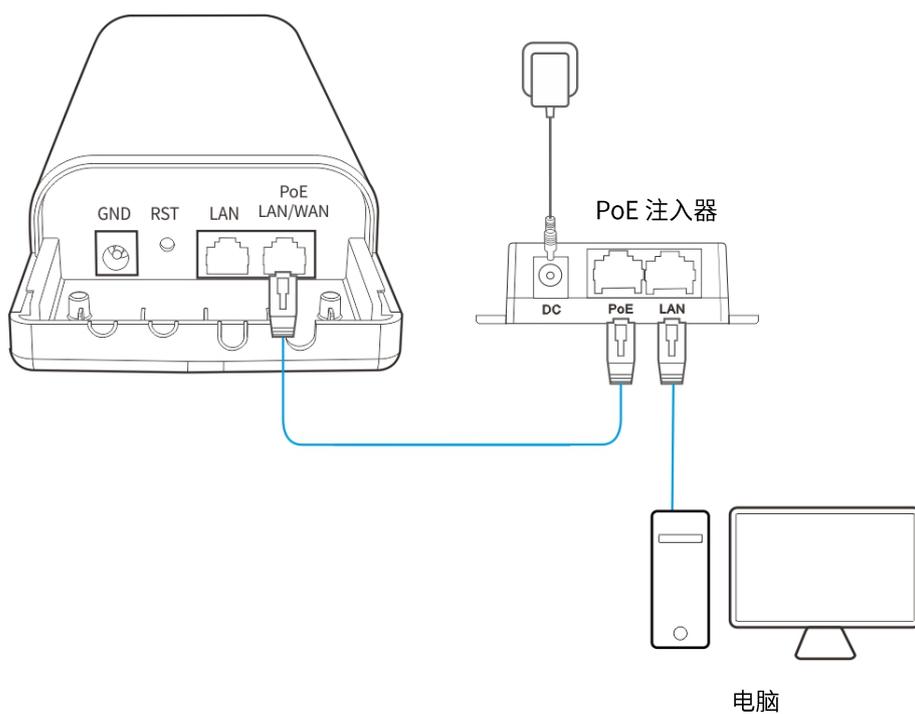
方式二：手动桥接

步骤 1 将两个网桥相邻放置。



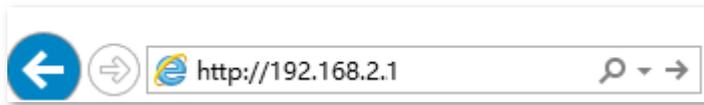
步骤 2 连接第 1 个网桥。

1. 打开网桥的保护盖。
2. 用网线连接网桥的 PoE LAN/WAN 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 LAN/WAN 灯亮。
4. 用网线将电脑连接到 PoE 注入器的 LAN 口。



步骤 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**。



2. 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](#)。

3. 进入「快速设置」页面，选择 **AP 模式**，点击 **下一步**。



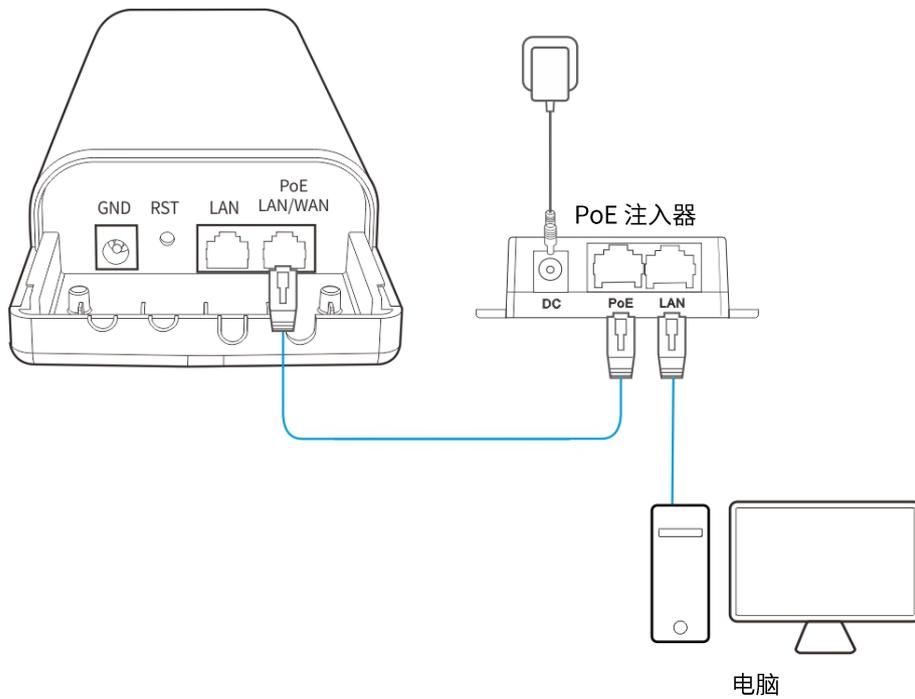
4. SSID：点击输入框，修改无线网络的名称，如 Tenda_1。
5. 信道：选择无线工作的信道。

- 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”)。
- 点击 **下一步**。

- 点击 **保存**, 等待网桥自动重启使设置生效。

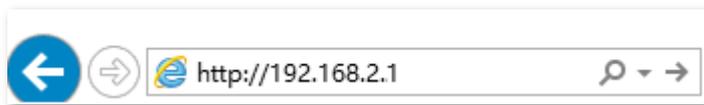
步骤 4 连接第 2 个网桥。

- 打开网桥的保护盖。
- 用网线连接网桥的 PoE LAN/WAN 口和 PoE 注入器的 PoE 口。
- 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 LAN/WAN 灯亮。
- 用网线将电脑连接到 PoE 注入器的 LAN 口。



步骤 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**。



2. 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](#)。

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 Tenda_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**。

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 Tenda_1

上级AP的MAC 50:2B:73:09:94:51

信道 7(2442)

安全模式 WPA2-PSK

加密规则 AES TKIP TKIP&AES

* 密钥 请输入上级无线网络密码

上一步 下一步

7. 修改 IP 地址信息。

- (1) IP 地址：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。
- (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。

8. 点击 **下一步**。

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 192.168.2.10

* 子网掩码 255.255.255.0

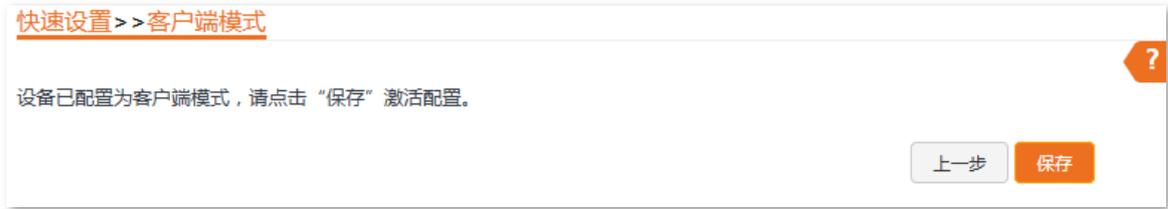
* 默认网关

* 首选DNS服务器

备用DNS服务器 8.8.4.4

上一步 下一步

9. 点击 **保存**，等待网桥自动重启使设置生效。



---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。

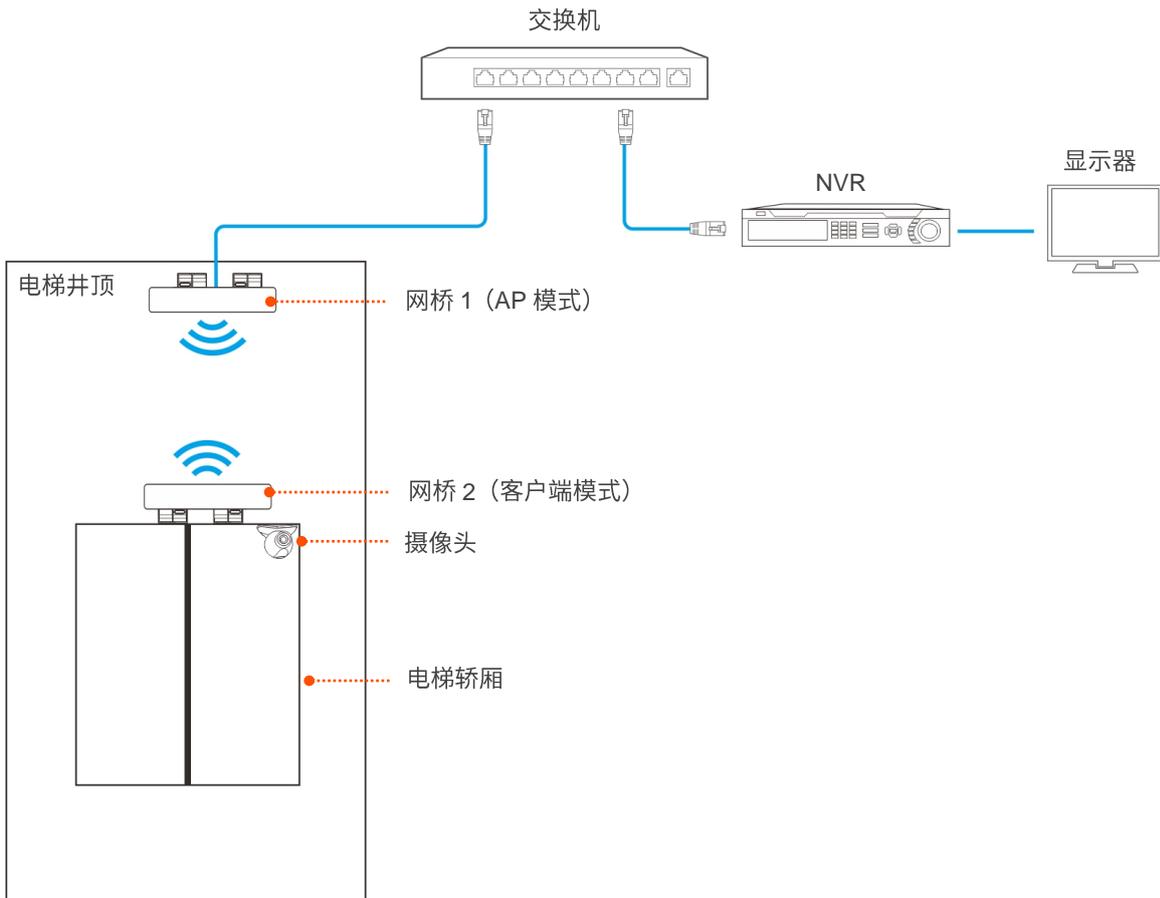


提示

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。

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

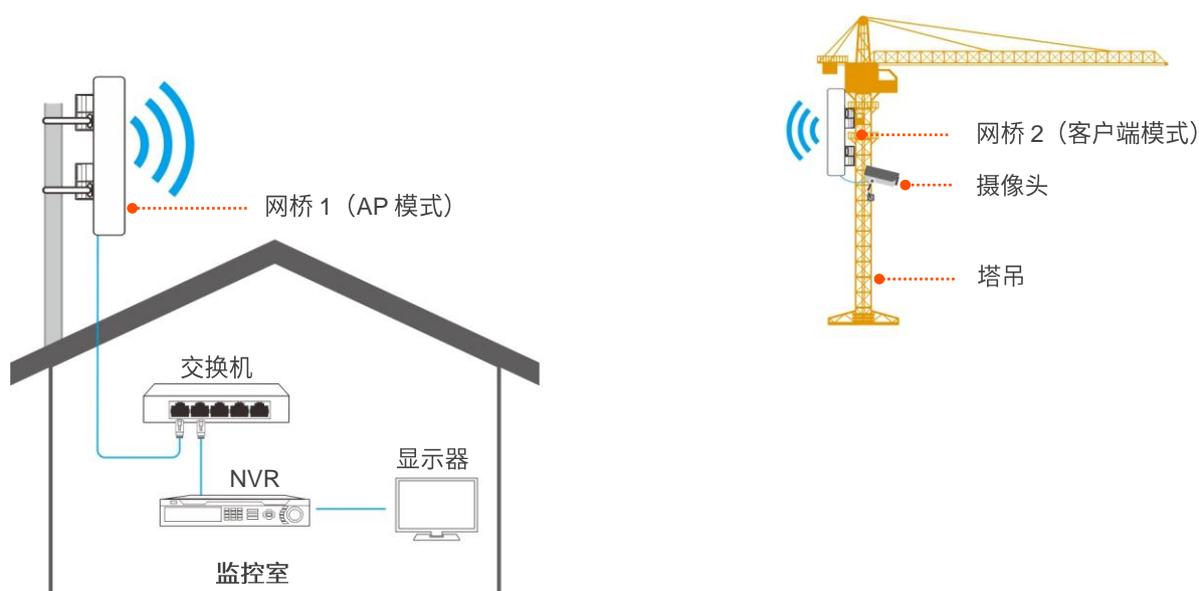
设置步骤请参考 2.1.2 [设置网桥](#)。



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。



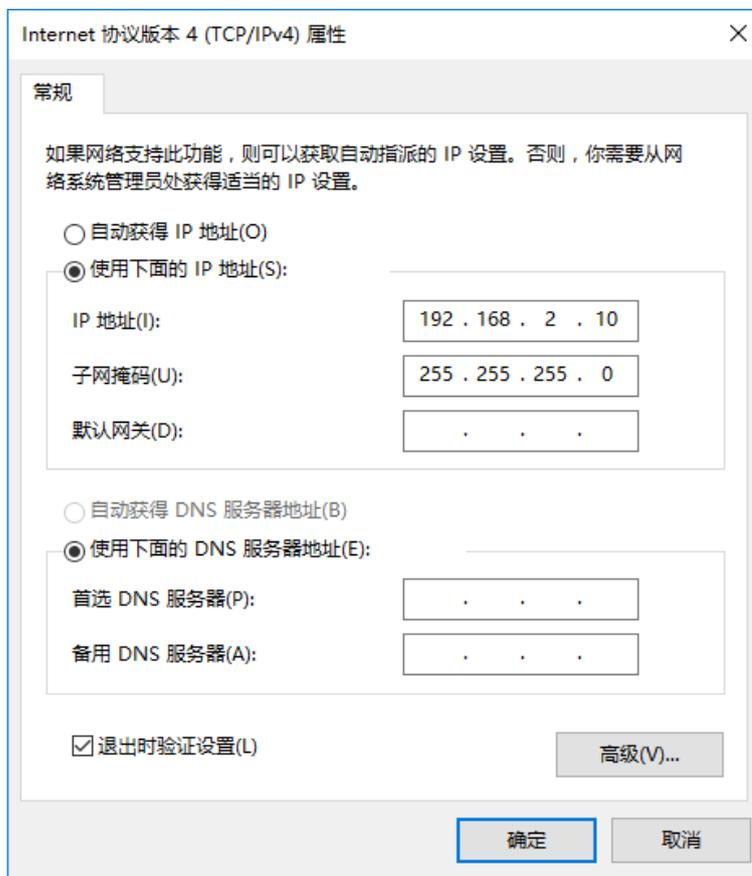
3 设备登录

3.1 登录网桥的管理页面

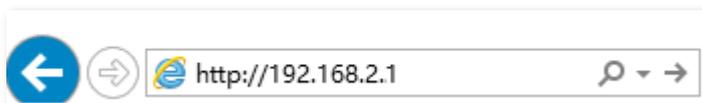
步骤 1 用网线将管理电脑接到网桥（或网桥连接的交换机）。

步骤 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”。



步骤 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”）。



步骤 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 page for O3V2.0. It features a grey header with the text "O3V2.0". Below the header, there are three input fields: the first contains the text "默认用户名为admin" (Default username is admin), the second contains "默认密码为admin" (Default password is admin) and has a small eye icon to toggle visibility, and the third contains "简体中文" (Simplified Chinese) with a dropdown arrow. At the bottom, there is a large orange button labeled "登录" (Login) and a smaller orange link labeled "忘记密码?" (Forgot password?).



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。



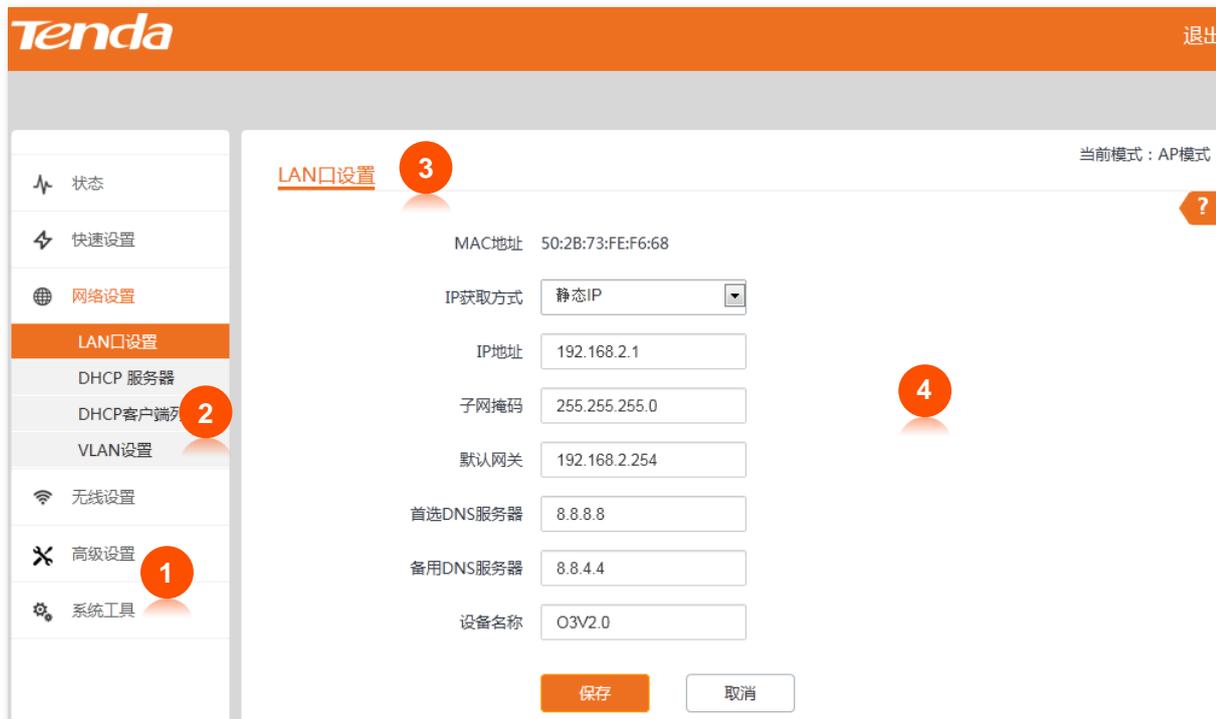
The image shows the Tenda management page. The top header is orange with the "Tenda" logo on the left and "退出" (Logout) on the right. A left sidebar contains navigation options: "状态" (Status), "快速设置" (Quick Setup), "网络设置" (Network Settings), "无线设置" (Wireless Settings), "高级设置" (Advanced Settings), and "系统工具" (System Tools). The main content area is titled "快速设置" (Quick Setup) and shows "当前模式：AP模式" (Current mode: AP mode). Under "请选择工作模式：" (Please select a working mode:), there are seven radio button options: "AP模式" (selected), "客户端模式" (Client mode), "万能中继模式" (Universal relay mode), "无线WAN模式" (Wireless WAN mode), "中继模式" (Relay mode), "P2MP模式" (P2MP mode), and "路由模式" (Router mode). A "下一步" (Next step) button is at the bottom right.

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。

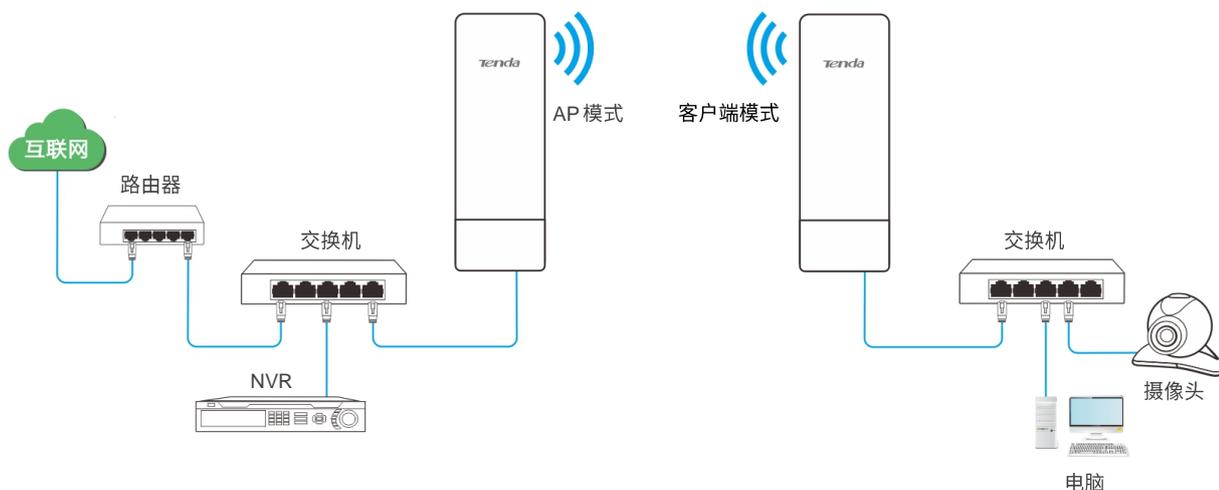
网桥支持以下工作模式：[AP 模式](#)、[客户端模式](#)、[万能中继模式](#)、[无线 WAN 模式](#)、[中继模式](#)、[P2MP 模式](#)、[路由模式](#)。

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。

AP 模式可与客户端模式、万能中继模式搭配使用。下图以 AP 模式与客户端模式搭配为例：



4.1.2 设置 AP 模式

步骤 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

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
- 万能中继模式** 中继现有无线信号，扩大无线网络覆盖范围
- 无线WAN模式** 无线连接到ISP热点，并分享网络
- 中继模式** 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
- P2MP模式** 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
- 路由模式** 有线连接到Modem（猫），并分享网络

下一步

步骤 2 SSID（无线网络名称）：点击输入框，修改无线网络名称，如“zhangsan”。

步骤 3 信道：选择无线工作的信道。

步骤 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”）。

步骤 5 点击 **下一步**。

快速设置 >> 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**

步骤 6 点击 **保存**。

快速设置 >> 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

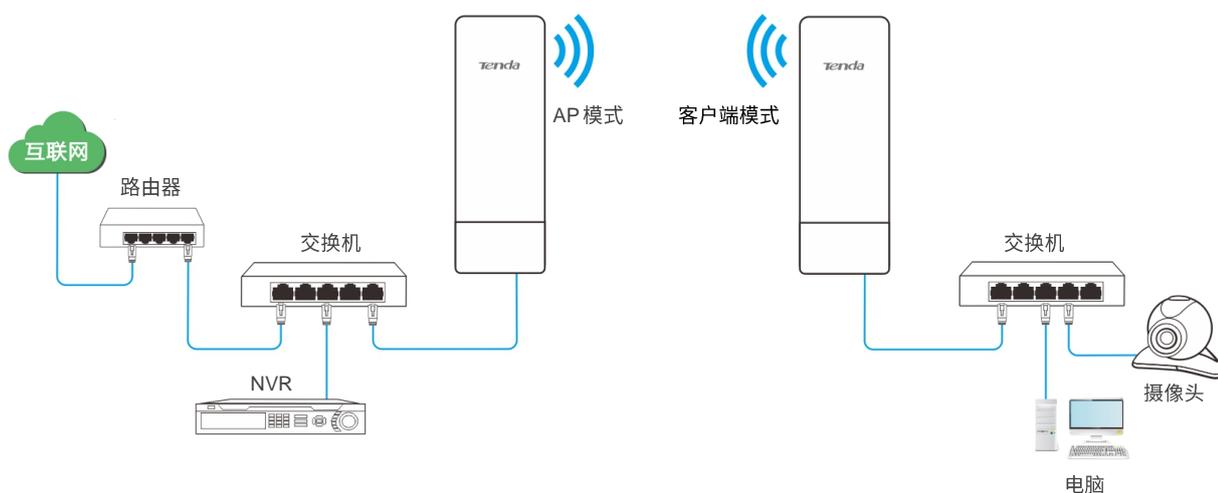
标题项	说明
工作模式	<p>选择网桥的工作模式。</p> <ul style="list-style-type: none">- AP 模式：把现有的有线网络转化为无线网络。- 客户端模式：作为无线网卡连接其他无线网络，此时网桥不提供无线接入服务，客户端需要通过网线连接到网桥。- 万能中继模式：中继现有无线信号，并自动创建一个与上级无线网络相同的无线网络，扩展无线网络覆盖范围。- 无线 WAN 模式：一般用于桥接宽带运营商的热点，如 CMCC、ChinaNet。也可以桥接上级无线路由器，并通过 DHCP（自动获取）、静态 IP 或 PPPoE 使网桥的 WAN 口获取 IP 地址，并连接到互联网。- 中继模式：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。- P2MP 模式：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。- 路由模式：作为路由器使用，设备的“PoE LAN/WAN”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，并连接到互联网。
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。此处可选择：不加密、WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK。</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。

客户端模式一般与 AP 模式搭配使用。应用拓扑图如下。



4.2.2 设置客户端模式

步骤 1 进入网桥的「快速设置」页面，选择客户端模式。

步骤 2 点击 **下一步**。



步骤 3 在出现的无线网络列表中，选择要桥接的无线网络，如 Tenda_1。

步骤 4 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。

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
	Tenda_1	11	50:2B:73:09:94:51	WPA2-PSK,AES	-27dBm

步骤 5 如果上级无线网络已加密，请输入对应的密钥（无线密码）。

步骤 6 点击 **下一步**。

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 Tenda_1

上级AP的MAC 50:2B:73:09:94:51

信道

安全模式

加密规则 AES TKIP TKIP&AES

* 密钥

步骤 7 设置本网桥的 IP 地址信息。

1. IP地址: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. 子网掩码:与上级AP的子网掩码保持一致即可。
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。

步骤 8 点击 **下一步**。

[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

* 子网掩码

* 默认网关

* 首选DNS服务器

备用DNS服务器

步骤 9 点击 **保存**。

[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



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
	<p>选择网桥的工作模式。</p> <ul style="list-style-type: none"> - 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，客户端需要通过网线连接到网桥。 - 万能中继模式：中继现有无线信号，并自动创建一个与上级无线网络相同的无线网络，扩展无线网络覆盖范围。
工作模式	<ul style="list-style-type: none"> - 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。 - 中继模式：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。 - P2MP 模式：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。 - 路由模式：作为路由器使用，设备的“PoE LAN/WAN”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，并连接到互联网。

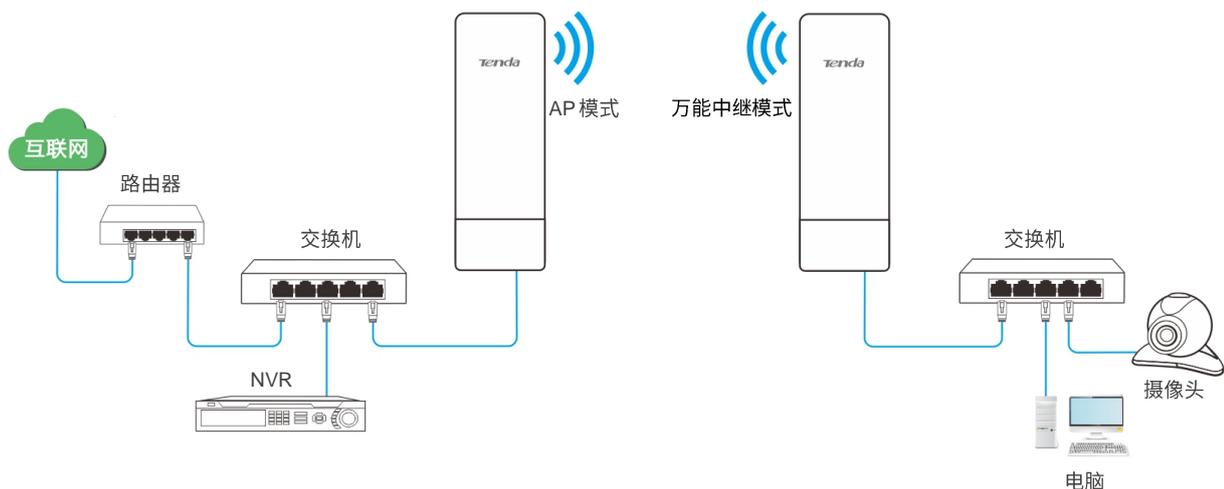
标题项	说明
透明网桥	启用后，网桥间可以实现双向透传，解决了 NVR 不能发现摄像头的问题。
上级 AP	要桥接的网络的无线名称（SSID）。
信道	被桥接无线网络的工作信道。通过扫描选择时，会自动填充，无需手动设置。
安全模式	被桥接无线网络使用的安全模式。通过扫描选择时，会自动填充，无需手动设置。如被桥接的无线网络已加密，须手动输入其密钥。

4.3 万能中继模式

4.3.1 概述

桥接现有无线信号，并自动创建一个与上级无线网络相同的无线网络，扩展无线网络覆盖范围。

应用拓扑图如下。



4.3.2 设置万能中继模式

步骤 1 进入网桥的「快速设置」页面，选择万能中继模式。

步骤 2 点击 **下一步**。



步骤 3 在出现的无线网络列表中，选择要桥接的无线网络，如 Tenda_1。

步骤 4 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。

快速设置 >> 万能中继模式

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
	Tenda_1	11	50:2B:73:09:94:51	WPA2-PSK,AES	-37dBm

步骤 5 如果上级无线网络已加密，请输入对应的密钥（无线密码）。

步骤 6 点击 **下一步**。

快速设置 >> 万能中继模式

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 Tenda_1

上级AP的MAC 50:2B:73:09:94:51

信道

安全模式

加密规则 AES TKIP TKIP&AES

* 密钥

[上一步](#) [下一步](#)

步骤 7 设置网桥的 IP 地址信息。

1. IP地址: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. 子网掩码:与上级AP的子网掩码保持一致即可。
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。

步骤 8 点击 **下一步**。

[快速设置](#) >> [万能中继模式](#)

请将IP地址设置为与上级AP相同网段的不同IP

* IP地址

* 子网掩码

* 默认网关

* 首选DNS服务器

备用DNS服务器

步骤 9 点击 **保存**。

[快速设置](#) >> [万能中继模式](#)

设备已配置为万能中继模式，请点击“保存”激活配置。

---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。

万能中继模式的参数说明

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"> - 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，客户端需要通过网线连接到网桥。 - 万能中继模式：中继现有无线信号，并自动创建一个与上级无线网络相同的无线网络，扩展无线网络覆盖范围。 - 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。 - 中继模式：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。 - P2MP 模式：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。 - 路由模式：作为路由器使用，设备的“PoE LAN/WAN”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，并连接到互联网。

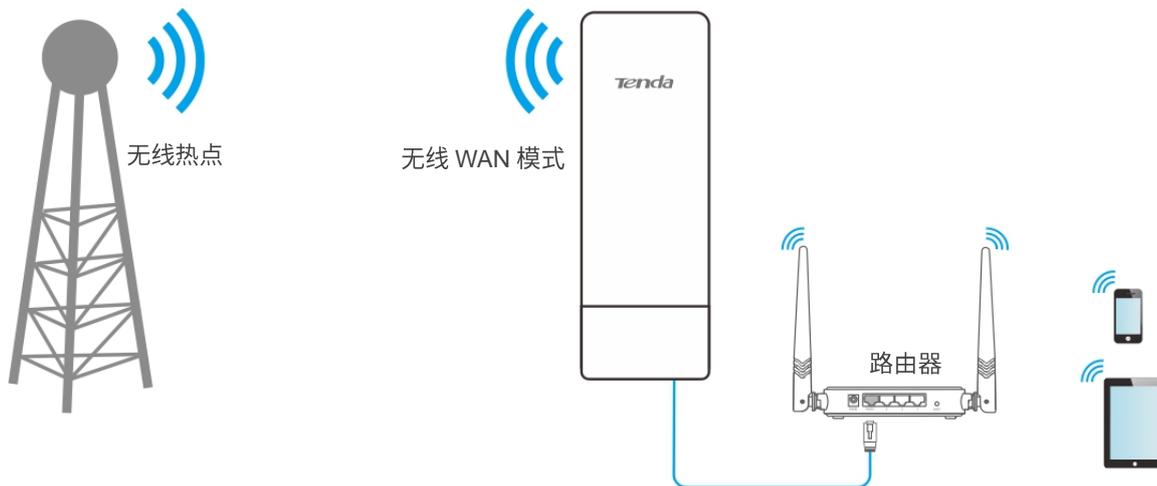
标题项	说明
透明网桥	启用后，网桥间可以实现双向透传，解决了 NVR 不能发现摄像头的问题。
上级 AP	要桥接的网络的无线名称（SSID）。
信道	被桥接无线网络的工作信道。通过扫描选择时，会自动填充，无需手动设置。
安全模式	被桥接无线网络使用的安全模式。通过扫描选择时，会自动填充，无需手动设置。如被桥接的无线网络已加密，须手动输入其密钥。

4.4 无线 WAN 模式

4.4.1 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。



4.4.2 设置无线 WAN 模式

步骤 1 进入网桥的「快速设置」页面，选择无线 WAN 模式。

步骤 2 点击 **下一步**。

快速设置

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
- 万能中继模式 中继现有无线信号，扩大无线网络覆盖范围
- 无线WAN模式 无线连接到SP热点，并分享网络
- 中继模式 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
- P2MP模式 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
- 路由模式 有线连接到Modem（猫），并分享网络

下一步

步骤 3 在出现的无线网络列表中，选择要桥接的无线网络，如 Tenda_1。

步骤 4 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。

快速设置 >> 无线WAN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

选择	SSID	信道	MAC地址	安全模式	信号强度
	Tenda_1	11	50:2B:73:09:94:51	WPA2-PSK,AES	-36dBm

步骤 5 如果上级无线网络已加密，请输入对应的密钥（无线密码）。

步骤 6 点击 **下一步**。

快速设置 >> 无线WAN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 Tenda_1

上级AP的MAC 50:2B:73:09:94:51

信道

安全模式

加密规则 AES TKIP TKIP&AES

* 密钥

步骤 7 设置 WAN 口信息。

1. 联网方式：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。

步骤 8 点击 **下一步**。

快速设置 >> 无线WAN模式

请选择联网方式，并输入ISP提供的联网信息，
然后点击“下一步”

* 联网方式 DHCP(自动获取) 静态IP PPPoE

* PPPoE用户名

* PPPoE密码

步骤 9 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。

步骤 10 点击 **下一步**。

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

步骤 11 点击 **下一步**。

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

步骤 12 点击 **保存**。



---完成



提示

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">- 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，客户端需要通过网线连接到网桥。- 万能中继模式：中继现有无线信号，并自动创建一个与上级无线网络相同的无线网络，扩展无线网络覆盖范围。- 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。- 中继模式：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。- P2MP 模式：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。- 路由模式：作为路由器使用，设备的“PoE LAN/WAN”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，并连接到互联网。
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。
联网方式	<p>设置网桥的联网方式，支持三种联网方式，如下：</p> <ul style="list-style-type: none">- 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。

4.5 中继模式

4.5.1 概述

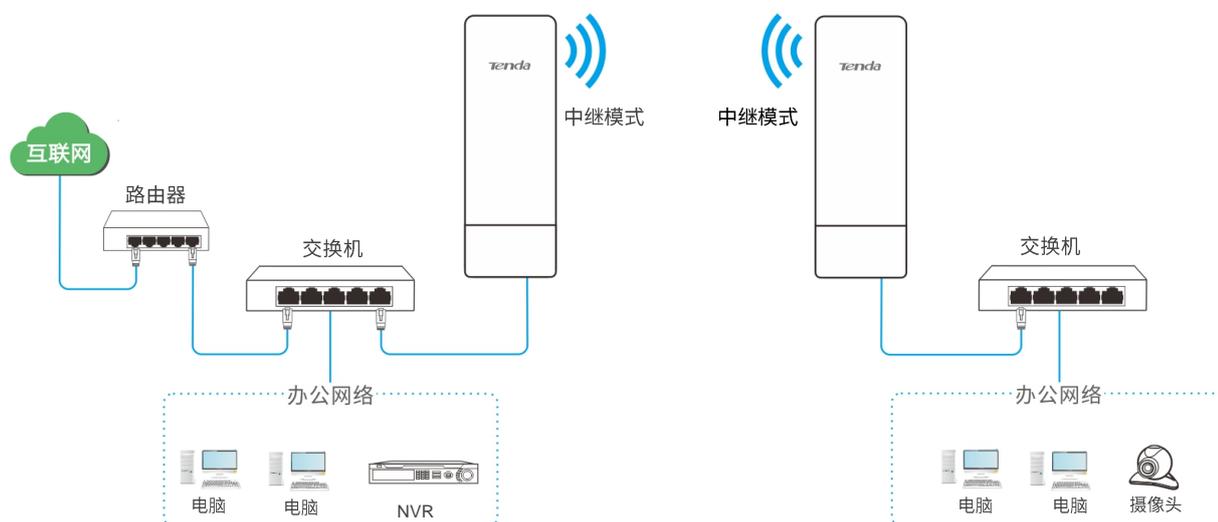
通过无线桥接将多个有线网络连通起来，自身提供无线接入功能。中继模式可以用于实现企业在相同城市的多个办公地点之间的通信。

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。

4.5.2 设置中继模式

1 对 1 中继

假设网桥两端都采用中继模式，应用拓扑图如下。



设置步骤：

步骤 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**。
2. 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 Tenda_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。



5. 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）。

6. 点击 **下一步**。

[快速设置](#) >> [中继模式](#)

请保持信道、安全模式、加密规则与对端AP一致，
然后输入对端AP1的密钥，点击“下一步”

对端AP1 Tenda_1

对端AP1的MAC地址 50:2B:73:09:94:51

信道

安全模式

7. 设置网桥的 IP 地址信息。

- (1) IP 地址：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。
- (2) 子网掩码：与对端网桥的子网掩码保持一致即可。
- (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。

8. 点击 **下一步**。

[快速设置](#) >> [中继模式](#)

请将IP地址设置为与对端AP相同网段的不同IP

* IP地址

* 子网掩码

* 默认网关

* 首选DNS服务器

备用DNS服务器

9. 点击 **保存**。

[快速设置](#) >> [中继模式](#)

设备已配置为中继模式，请点击“保存”激活配置。

步骤 2 设置另一个网桥。

参考步骤 1，设置无线桥接到第一个网桥。

---完成



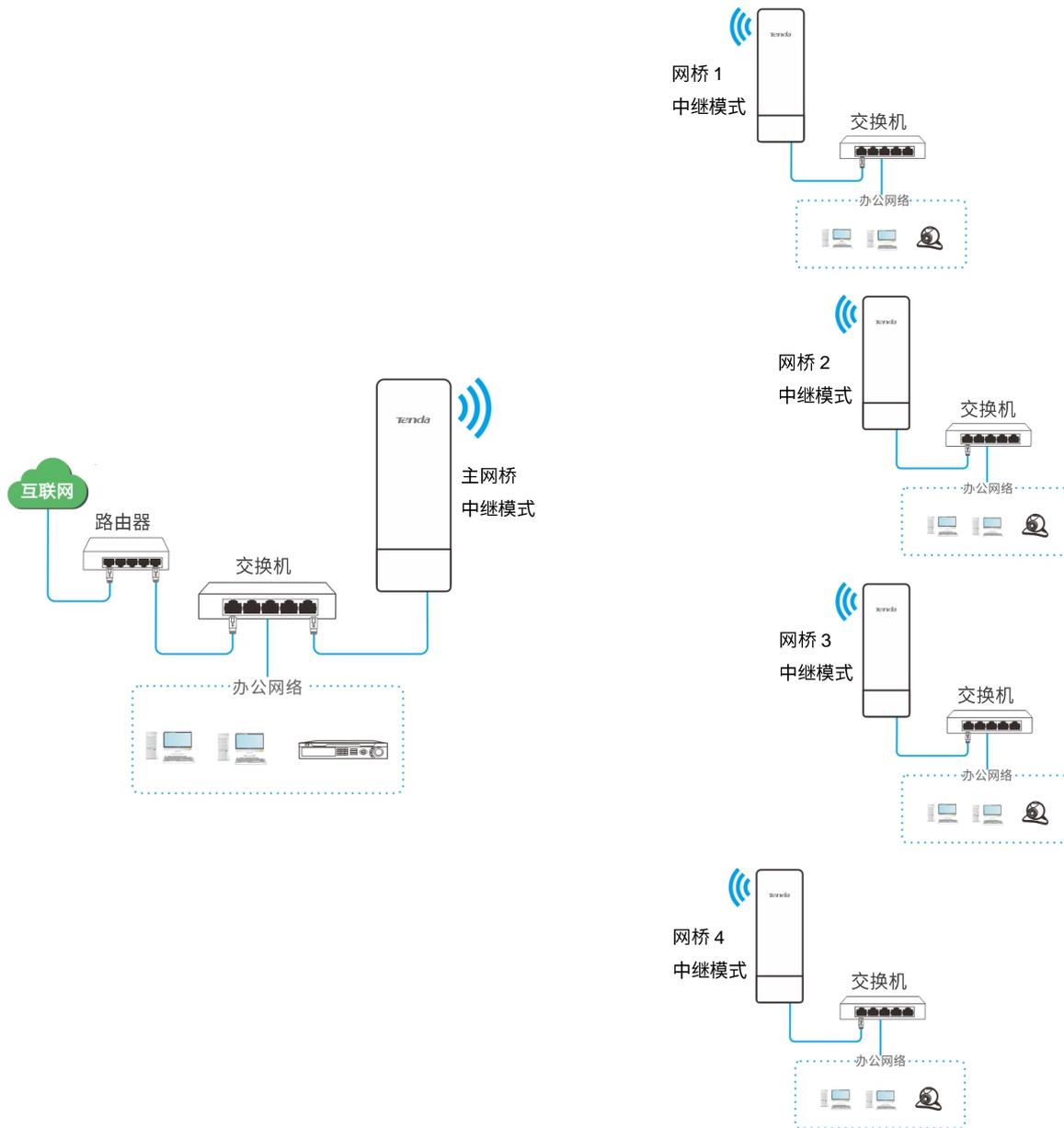
登录到网桥的管理页面，进入「无线设置」>「基本设置」页面，可查看网桥的 SSID 和密钥。

中继模式的参数说明

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">- 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，客户端需要通过网线连接到网桥。- 万能中继模式：中继现有无线信号，并自动创建一个与上级无线网络相同的无线网络，扩展无线网络覆盖范围。- 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。- 中继模式：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。- P2MP 模式：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。- 路由模式：作为路由器使用，设备的“PoE LAN/WAN”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，并连接到互联网。
对端 AP	要桥接的网络的无线网络的无线 MAC 地址。
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	<p>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。</p> <p> 提示</p> <p>中继模式仅支持“不加密”和“WEP”安全模式。</p>

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: Tenda_1
- 信道：11
- 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：

	SSID	MAC 地址
网桥 1	Tenda_2	50:2B:73:FE:F6:69
网桥 2	Tenda_3	50:2B:73:35:BA:01
网桥 3	Tenda_4	50:2B:73:FD:8D:A1
网桥 4	Tenda_5	50:2B:73:09:93:51

设置步骤：

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。
2. 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，本例为主网桥的无线网络“Tenda_1”。
4. 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。

快速设置 >> 中继模式

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](#)

对端AP1

对端AP2

对端AP3

对端AP4

选择	SSID	信道	MAC地址	安全模式	信号强度
	Tenda_1	11	50:2B:73:09:94:51	不加密	-42dBm

5. 点击 **下一步**。

快速设置 >> 中继模式

请保持信道、安全模式、加密规则与对端AP一致，
然后输入对端AP1的密钥，点击“下一步”

对端AP1 Tenda_1

对端AP1的MAC地址 50:2B:73:09:94:51

信道

安全模式

6. 设置网桥的 IP 地址信息。

- (1) IP 地址：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。
- (2) 子网掩码：与对端网桥的子网掩码保持一致即可。
- (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**。

快速设置 >> 中继模式

请将IP地址设置为与对端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**。

快速设置 >> 中继模式

设备已配置为中继模式，请点击“保存”激活配置。

步骤 2 参考**步骤 1**，设置网桥 2/3/4 通过中继模式桥接主网桥。

步骤 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**。
2. 点击 **下一步**。

快速设置

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
- 万能中继模式 中继现有无线信号，扩大无线网络覆盖范围
- 无线WAN模式 无线连接到ISP热点，并分享网络
- 中继模式 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
- P2MP模式 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
- 路由模式 有线连接到Modem（猫），并分享网络

3. 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。

4. 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。

快速设置 >> 中继模式

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](#)

对端AP1

对端AP2

对端AP3

对端AP4

选择	SSID	信道	MAC地址	安全模式	信号强度
<input checked="" type="checkbox"/>	Tenda_2	11	50:2B:73:FE:F6:69	不加密	
<input checked="" type="checkbox"/>	Tenda_3	11	50:2B:73:35:BA:01	不加密	
<input checked="" type="checkbox"/>	Tenda_4	11	50:2B:73:FD:8D:A1	不加密	
<input checked="" type="checkbox"/>	Tenda_5	11	50:2B:73:09:93:51	不加密	

5. 点击 **下一步**。

快速设置 >> 中继模式

请保持信道、安全模式、加密规则与对端AP一致，
然后输入对端AP1的密钥，点击“下一步”

对端AP1 Tenda_2

对端AP1的MAC地址 50:2B:73:FE:F6:69

信道

安全模式

6. 点击 **下一步**。

快速设置 > > 中继模式

请将IP地址设置为与对端AP相同网段的不同IP

IP地址	<input type="text" value="192.168.2.1"/>
子网掩码	<input type="text" value="255.255.255.0"/>
默认网关	<input type="text" value="192.168.2.254"/>
首选DNS服务器	<input type="text" value="8.8.8.8"/>
备用DNS服务器	<input type="text" value="8.8.4.4"/>

7. 点击 **保存**。

快速设置 > > 中继模式

设备已配置为中继模式，请点击“保存”激活配置。

---完成

4.6 P2MP 模式

4.6.1 概述

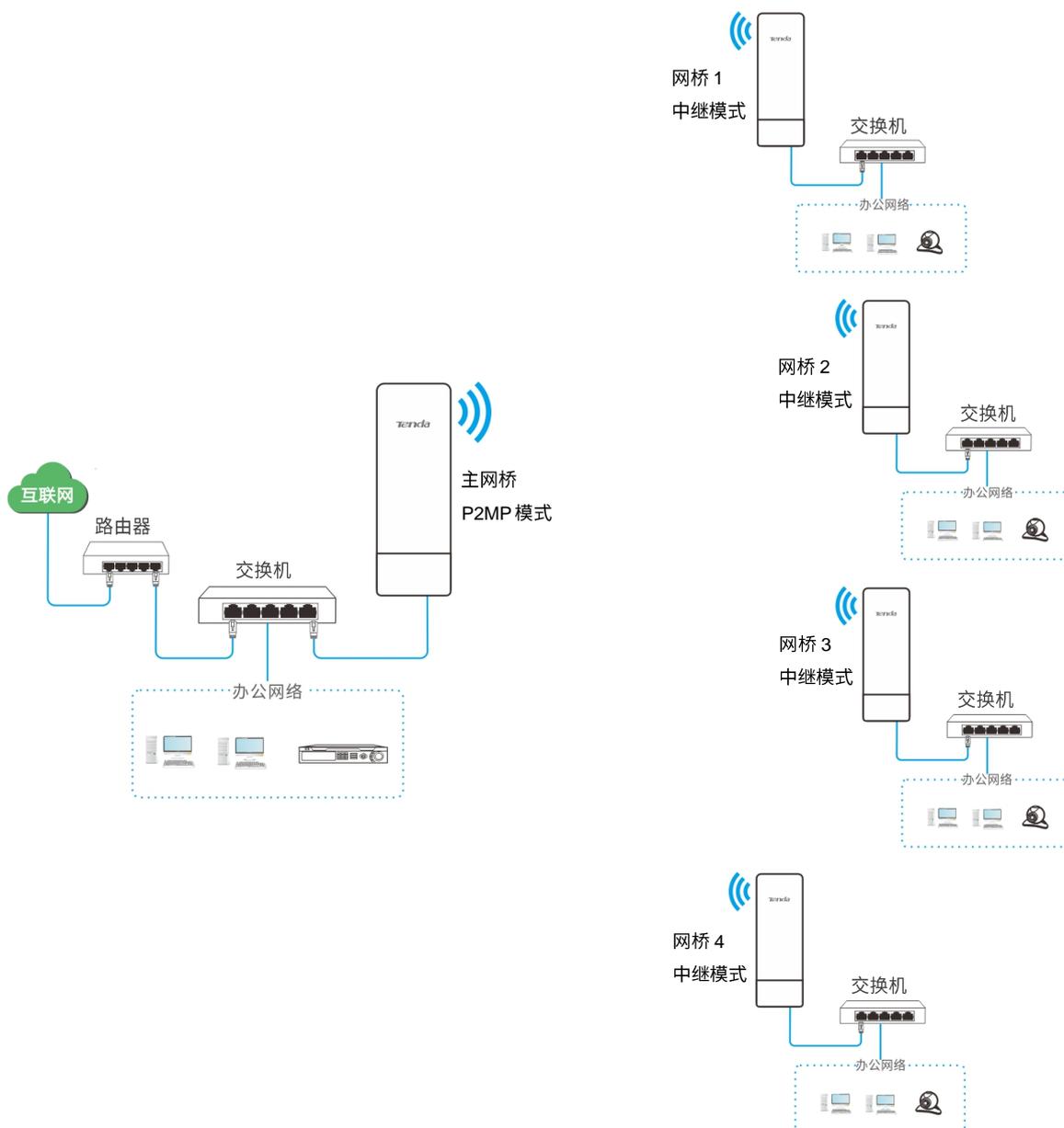
通过无线桥接将多个有线网络连通起来，自身不提供无线接入功能。P2MP 模式可以用于实现企业在相同城市的多个办公地点之间的通信。

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。

4.6.2 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：Tenda_1
- 信道：11
- 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：

	SSID	MAC 地址
网桥 1	Tenda_2	50:2B:73:FE:F6:69
网桥 2	Tenda_3	50:2B:73:35:BA:01
网桥 3	Tenda_4	50:2B:73:FD:8D:A1
网桥 4	Tenda_5	50:2B:73:09:93:51

设置步骤：

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。
2. 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，本例为主网桥的无线网络“Tenda_1”。
4. 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。



5. 点击 **下一步**。



6. 设置网桥的 IP 地址信息。

- (1) IP 地址：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。
- (2) 子网掩码：与对端网桥的子网掩码保持一致即可。
- (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**。

[快速设置](#) >> [中继模式](#)

请将IP地址设置为与对端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**。

[快速设置](#) >> [中继模式](#)

设备已配置为中继模式，请点击“保存”激活配置。

步骤 2 参考**步骤 1**，设置网桥 2/3/4 通过中继模式桥接主网桥。

步骤 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。
2. 点击 **下一步**。

[快速设置](#)

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
- 万能中继模式** 中继现有无线信号，扩大无线网络覆盖范围
- 无线WAN模式** 无线连接到ISP热点，并分享网络
- 中继模式** 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
- P2MP模式** 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
- 路由模式** 有线连接到Modem（猫），并分享网络

3. 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。
4. 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。

快速设置 >> P2MP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

对端AP1 50:2B:73:FE:F6:69
对端AP2 50:2B:73:35:BA:01
对端AP3 50:2B:73:FD:8D:A1
对端AP4 50:2B:73:09:93:51

选择	SSID	信道	MAC地址	安全模式	信号强度
<input checked="" type="checkbox"/>	Tenda_2	11	50:2B:73:FE:F6:69	不加密	
<input checked="" type="checkbox"/>	Tenda_3	11	50:2B:73:35:BA:01	不加密	
<input checked="" type="checkbox"/>	Tenda_4	11	50:2B:73:FD:8D:A1	不加密	
<input checked="" type="checkbox"/>	Tenda_5	11	50:2B:73:09:93:51	不加密	

5. 点击 **下一步**。

快速设置 >> P2MP模式

请保持信道、安全模式、加密规则与对端AP一致，
然后输入对端AP1的密钥，点击“下一步”

对端AP1 Tenda_2

对端AP1的MAC地址 50:2B:73:FE:F6:69

信道 11(2462)

安全模式 不加密

上一步

下一步

6. 点击 **下一步**。

快速设置 >> P2MP模式

请将IP地址设置为与对端AP相同网段的不同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

上一步 下一步

7. 点击 **保存**。

快速设置 >> P2MP模式

设备已配置为P2MP模式，请点击“保存”激活配置。

上一步 保存

----完成

P2MP 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">- 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，客户端需要通过网线连接到网桥。- 万能中继模式：中继现有无线信号，并自动创建一个与上级无线网络相同的无线网络，扩展无线网络覆盖范围。- 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。- 中继模式：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。- P2MP 模式：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。- 路由模式：作为路由器使用，设备的“PoE LAN/WAN”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，并连接到互联网。

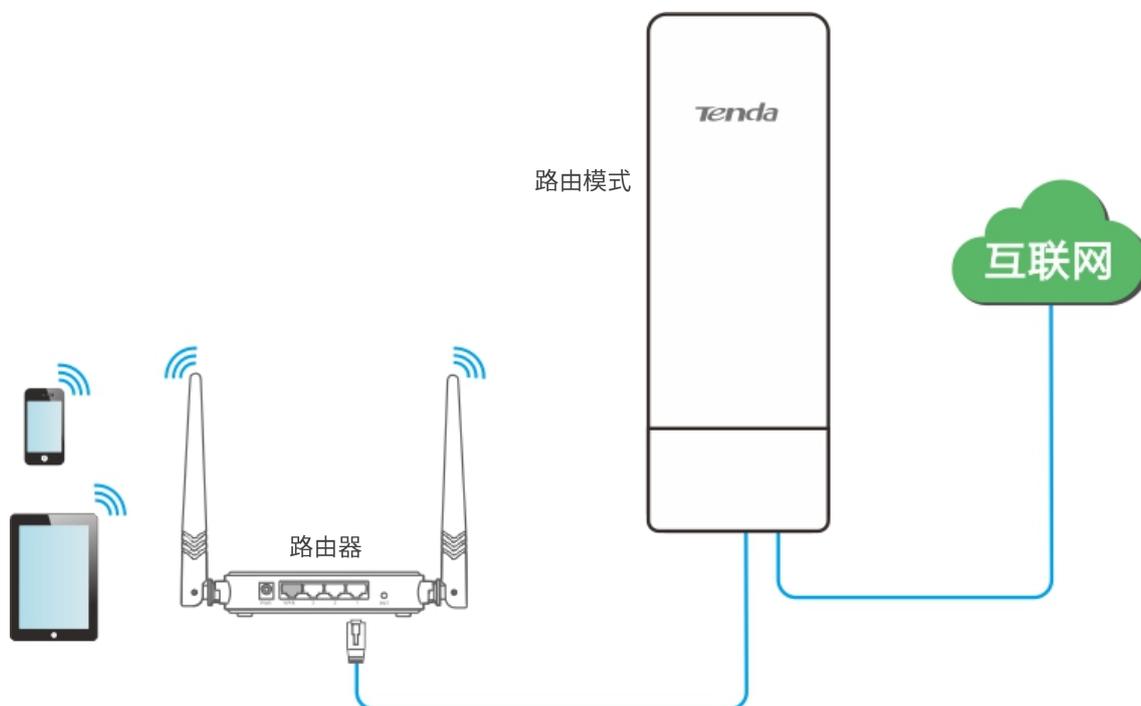
标题项	说明
对端 AP	要桥接的网络的无线网络的无线 MAC 地址。
信道	被桥接无线网络的工作信道。通过扫描选择时，会自动填充，无需手动设置。
安全模式	<p>被桥接无线网络使用的安全模式。通过扫描选择时，会自动填充，无需手动设置。如被桥接的无线网络已加密，须手动输入其密钥。</p> <p> 提示</p> <p>P2MP 模式仅支持“不加密”和“WEP”安全模式。</p>

4.7 路由模式

4.7.1 概述

路由模式下，网桥充当路由器为客户端提供网络，用户可在网桥下接一个路由器进行网络扩展。

应用拓扑图如下。



4.7.2 设置路由模式

步骤 1 进入网桥的「快速设置」页面，选择路由模式。

步骤 2 点击 **下一步**。



步骤 3 设置 WAN 口信息（以 PPPoE 为例）。

1. 联网方式：选择 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。

步骤 4 点击 **下一步**。

快速设置 >> 路由模式

请选择联网方式，并输入ISP提供的联网信息，
然后点击“下一步”

* 联网方式 DHCP(自动获取) 静态IP PPPoE

* PPPoE用户名

* PPPoE密码

上一步 下一步

步骤 5 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 FREE。
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。

步骤 6 点击 **下一步**。

快速设置 >> 路由模式

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

* 信道

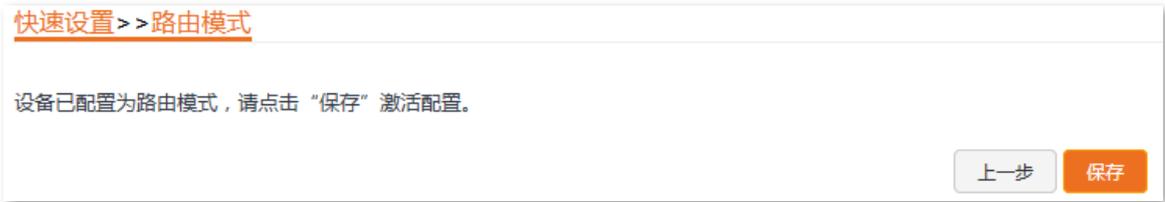
* 安全模式

* 加密规则 AES TKIP TKIP&AES

* 密钥

上一步 下一步

步骤 7 点击 **保存**。



----完成

路由模式的参数说明

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">- 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，客户端需要通过网线连接到网桥。- 万能中继模式：中继现有无线信号，并自动创建一个与上级无线网络相同的无线网络，扩展无线网络覆盖范围。- 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。- 中继模式：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。- P2MP 模式：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。- 路由模式：作为路由器使用，设备的“PoE LAN/WAN”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，并连接到互联网。
联网方式	<p>设置网桥的联网方式，支持三种联网方式，如下：</p> <ul style="list-style-type: none">- 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	点击此栏，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 。 点击超链接可以了解对应安全模式的详细说明。

5 状态

在「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

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：

系统状态			
设备名称	O3V2.0	LAN MAC	50:2B:73:FE:F6:68
运行时间	18小时9分49秒	WLAN MAC	50:2B:73:FE:F6:69
系统时间	2018-04-17 10:29:04	PoE LAN/LAN口速率	未连接/100Mbps全双工
软件版本	V1.0.0.5(2182)	LAN IP	192.168.2.1
硬件版本	V2.0		

无线 WAN 模式、路由模式下的系统状态内容如下：

系统状态			
设备名称	O3V2.0	LAN MAC	50:2B:73:FE:F6:68
运行时间	2分47秒	WLAN MAC	50:2B:73:FE:F6:69
系统时间	2018-04-17 11:28:45	PoE LAN/LAN口速率	未连接/100Mbps全双工
软件版本	V1.0.0.5(2182)	LAN IP	192.168.2.1
硬件版本	V2.0	WAN IP	172.20.20.2
连接状态	已连接	首选DNS服务器	192.168.0.60
上网类型	PPPoE	备用DNS服务器	223.5.5.5
默认网关	172.20.20.1		

参数说明

标题项	说明
设备名称	<p>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。</p> <p>您可以在「网络设置」>「LAN 口设置」页面修改设备名称。</p>
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。
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。
PoE LAN/LAN 口速率	网桥 PoE LAN/WAN 口、LAN 口当前的连接速率。
LAN IP	<p>网桥的 IP 地址，也是网桥的管理 IP 地址。</p> <p>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。</p>
连接状态	网桥当前的网络连接状态。仅适用于无线 WAN 和路由模式。
上网类型	<p>网桥当前的联网方式。仅适用于无线 WAN 和路由模式。</p> <p>本设备支持三种联网方式，如下：</p> <ul style="list-style-type: none">- 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。
WAN IP	网桥 WAN 口获取的 IP 地址。仅适用于无线 WAN 和路由模式。
默认网关	<p>网桥的网关地址信息。仅适用于无线 WAN 和路由模式。</p> <p>网桥访问外网时，数据包必须通过网关进行转发。</p>
首选 DNS 服务器	网桥的 DNS 服务器地址。仅适用于无线 WAN 和路由模式。
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。

无线状态			
工作模式	AP模式	上级AP的MAC地址	50:2B:73:FE:F6:69
SSID	Tenda_FEF668	信号强度	N/A
安全模式	不加密	背景噪声	 -95dBm
信道/频段	6/2437	TX/RX链路	1X1
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。
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。
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。 <ul style="list-style-type: none">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。 <ul style="list-style-type: none">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。
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 1 收 1 发。
发送/接收速率	无线发送/接收速率。 <ul style="list-style-type: none">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。

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。

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	CCQ	连接时间
192.168.50.182	14:5F:94:BC:FC:83	-67/-88dBm	58/24Mbps	92%	49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/当前环境中干扰信号和电磁噪声的强度。

标题项	说明
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。

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	CCQ	连接时间
172.20.20.1	C8:3A:35:18:68:41	-48/-88dBm	58/1Mbps	100%	1分40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/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	本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	本网桥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
LAN	0.0.0.0	50:2B:73:FE:F6:68	0	0	0	0
Bridge	192.168.2.1	50:2B:73:FE:F6:68	2252	0	2223	0
WLAN	0.0.0.0	50:2B:73:FE:F6:69	274	0	497	0

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	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:35:12:12:14	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。

标题项	说明
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	IP 数据包的目的网络地址。
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。

LAN口设置

MAC地址 50:2B:73:FE:F6:68

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 Tenda_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">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。

标题项	说明
	<p> 提示</p> <p>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。</p>
IP 地址	<p>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”。</p> <p>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。</p>
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	<p>网桥的默认网关。</p> <p>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。</p>
首选 DNS 服务器	<p>网桥的首选 DNS 服务器地址。</p> <p>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。</p>
备用 DNS 服务器	<p>网桥的备用 DNS 服务器地址，该选项可选填。</p> <p>若有两个 DNS 服务器 IP 地址，可将另一个 IP 地址填在此处。</p>
设备名称	<p>该台网桥的名称，默认为网桥的型号+版本号。</p> <p>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。</p>

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几台网桥的场合。

设置步骤：

步骤 1 进入「网络设置」>「LAN 口设置」页面。

步骤 2 IP 获取方式：选择“静态 IP”。

步骤 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”）。

步骤 4 点击 **保存**。

LAN口设置

MAC地址 50:2B:73:FE:F6:68

* 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 O3V2.0

保存 取消

步骤 5 确认提示信息后，点击 **确定**。

提示 ×

确认修改LAN IP,请点击确定
更改IP地址后，您需要使用新的IP地址192.168.2.10重新登录！

确定 取消

---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：

步骤 1 进入「网络设置」>「LAN 口设置」页面。

步骤 2 IP 获取方式：选择“DHCP（自动获取）”。

步骤 3 点击 **保存**。



The screenshot shows the 'LAN口设置' (LAN Port Settings) configuration page. The MAC address is 50:2B:73:FE:F6:68. The IP acquisition method is set to 'DHCP (自动获取)'. The IP address is 192.168.2.1, the subnet mask is 255.255.255.0, the default gateway is 192.168.2.254, the preferred DNS server is 8.8.8.8, and the backup DNS server is 8.8.4.4. The device name is O3V2.0. There are '保存' (Save) and '取消' (Cancel) buttons at the bottom.

MAC地址	50:2B:73:FE:F6:68
* IP获取方式	DHCP (自动获取)
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	O3V2.0

---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

仅适用于无线 WAN 模式、路由模式。

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的 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 50 : 2B : 73 : FE : F6 : 69

克隆本地MAC 恢复默认MAC

6.2.2 克隆 MAC 地址

方法 1:

步骤 1 使用之前能正常上网的电脑连接网桥。

步骤 2 登录网桥管理页面，进入「网络设置」>「MAC 克隆」页面。

步骤 3 点击 **克隆本地 MAC**。

步骤 4 点击 **保存**。

MAC克隆

MAC地址 C8 : 3A : 35 : D5 : 75 : A6

克隆本地MAC 恢复默认MAC

步骤 5 点击 **确定**。



----完成

登录网桥管理页面，进入「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	O3V2.0	LAN MAC	50:2B:73:FE:F6:68
运行时间	2分47秒	WLAN MAC	C8:3A:35:D5:75:A6
系统时间	2018-04-17 11:28:45	PoE LAN/LAN口速率	未连接/100Mbps全双工
软件版本	V1.0.0.5(2182)	LAN IP	192.168.2.1
硬件版本	V2.0	WAN IP	172.20.20.2
连接状态	已连接	首选DNS服务器	192.168.0.60
上网类型	PPPoE	备用DNS服务器	223.5.5.5
默认网关	172.20.20.1		

方法 2:

步骤 1 记录正确的 MAC 地址。

步骤 2 登录网桥管理页面，进入「网络设置」>「MAC 克隆」页面。

步骤 3 在 MAC 地址后的输入框里填入正确的 MAC 地址。

步骤 4 点击 **保存**。

MAC克隆 ?

MAC地址 C8 : 3A : 35 : D5 : 75 : A6

克隆本地MAC 恢复默认MAC

保存 取消

---完成



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

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

步骤 1 进入「网络设置」>「DHCP 服务器」页面。

步骤 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”）。

步骤 3 点击 **保存**。

DHCP 服务器

* DHCP 服务器

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

---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。默认启用。
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。
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	主机名称	IP地址	MAC地址	租约时间
1	HUAWEI_P10	192.168.2.182	14:5F:94:BC:FC:83	23小时 59分 58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

步骤 1 进入「网络设置」>「VLAN 设置」页面。

步骤 2 根据需要修改各参数（一般仅需修改“VLAN 设置”、“WLAN”、“LAN”）。

步骤 3 点击 **保存**。

VLAN设置

* VLAN设置

PVID (范围: 1~4094)

管理VLAN (范围: 1~4094)

* WLAN (范围: 1~4094)

* LAN (范围: 1~4094)

保存 **取消**

----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/WAN 口为 Trunk 口。
PVID	Trunk 口默认所属的 VLAN ID，默认为“1”。启用 VLAN 后，网桥的 PoE LAN/WAN 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。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。
LAN	设置 LAN 口的 VLAN ID，默认为 1。启用 VLAN 后，LAN 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：

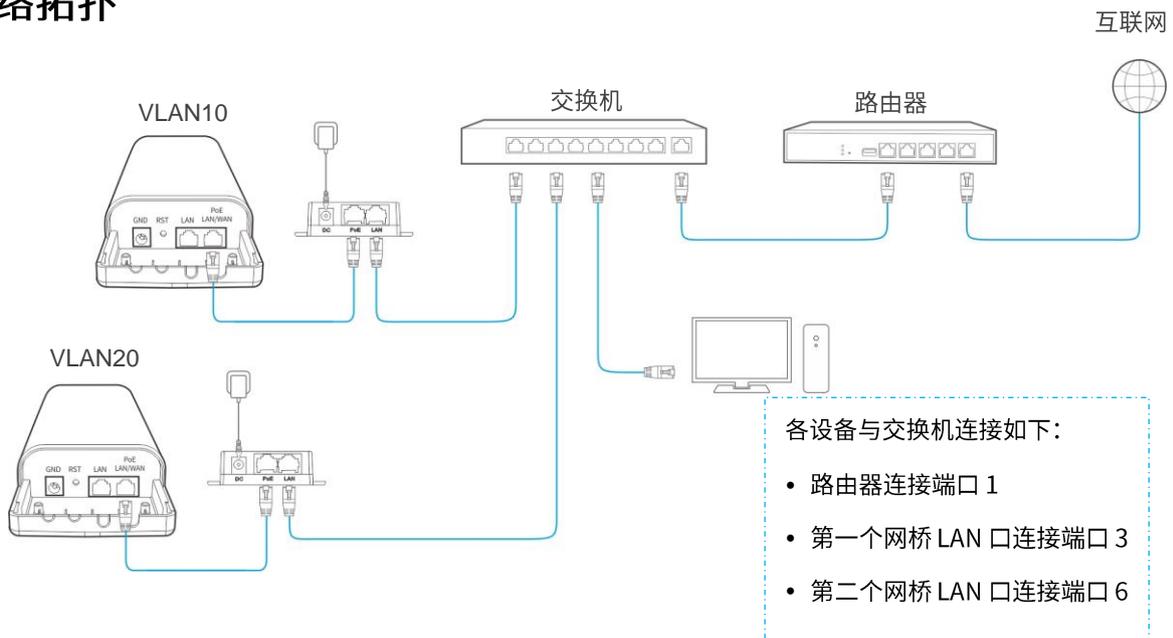
端口链路类型	接收数据处理		发送数据处理
	接收 Tag 数据	接收 Untag 数据	
Access			去掉报文的 Tag 再发送。
Trunk	按 Tag 中的 VID 转发到相应 VLAN 的其他端口。	按该端口的 PVID 转发到相应 VLAN 的其他端口。	VID = 端口 PVID，去掉 Tag 发送。 VID ≠ 端口 PVID，保留 Tag 发送。

6.5.3 VLAN 设置举例

组网需求

将第一个网桥划分在 VLAN10，第二个网桥划分在 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）

步骤 1 登录网桥的管理页面，转到「网络设置」>「VLAN 设置」页面。

步骤 2 VLAN 设置：点击滑块至 。

步骤 3 管理 VLAN：设置管理 VLAN，默认为 1，建议保持默认设置。

步骤 4 WLAN：设置无线接口 VLAN ID，本例为“10”。

步骤 5 LAN: 设置 LAN 口 VLAN ID, 本例为 “10”。

步骤 6 点击 **保存**。



步骤 7 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。

三、配置路由器

为保证接入到网桥的客户端能正常上网, 路由器需要支持并进行 QVLAN 配置。路由器具体设置如下。

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

具体配置方法请参考路由器的使用说明书。

----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 相关设置、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：

步骤 1 进入「无线设置」>「基本设置」页面。

步骤 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）。

步骤 3 点击 **保存**。

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

信道带宽

扩展信道

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

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">- 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。 <ul style="list-style-type: none">- 11b：此模式下，仅允许 802.11b 无线设备接入网桥的无线网络。- 11g：此模式下，仅允许 802.11g 无线设备接入网桥的无线网络。

标题项	说明
	<ul style="list-style-type: none"> - 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。 - 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。
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	<p>设置网桥的无线发射功率。</p> <p>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。</p>
信道带宽	<p>网桥工作在 11b/g/n 模式可以设置, 用于选择无线信道带宽。</p> <ul style="list-style-type: none"> - 20MHz: 限制网桥只能使用 20MHz 的信道带宽。 - 40MHz: 限制网桥只能使用 40MHz 的信道带宽。 - 自动: 网桥根据周围环境, 自动调整其信道带宽为 20MHz 或 40MHz。
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。
传输速率	<p>网桥的无线传输速率, 可以设置 MCS0-MCS7 之间的无线速率, 建议选择“自动”, 此时速率传输情况如下:</p> <ul style="list-style-type: none"> - 选择 20MHz 信道带宽时, 速率会自动降低, 最大速率只能为 65Mbps。 - 选择 40MHz 信道带宽时, 最大速率能达到 135Mbps。 - 选择自动时, 最大速率能达到 135Mbps。
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 。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"> - 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	<p>SSID 最多允许接入的无线设备数量。</p> <p>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。</p>

■ 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
认证类型	<p>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。</p> <ul style="list-style-type: none"> - 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	<p>用于指定 SSID 当前使用的 WEP 密钥。</p> <p>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。</p>
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	<p>可选择的密钥字符类型之一。</p> <p>此时，密钥可以输入 5 或 13 个 ASCII 码字符。</p>
Hex	<p>可选择的密钥字符类型之一。</p> <p>此时，密钥可以输入 10 或 26 位十六进制数（0-9，a-f，A-F）。</p>

■ WPA-PSK、WPA2-PSK、Mixed WPA/WPA2-PSK

安全模式	WPA-PSK	
加密规则	<div style="border: 1px solid black; padding: 5px;"> 不加密 WEP WPA-PSK WPA2-PSK Mixed WPA/WPA2-PSK </div>	TKIP&AES
密钥	<div style="border: 1px solid black; padding: 5px;"> WPA WPA2 </div>	
密钥更新周期	0	s (范围：60~99999，0表示不更新)

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">- 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	<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&AES”。</p> <ul style="list-style-type: none">- 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

The screenshot shows a configuration window for WPA/WPA2. The '安全模式' (Security Mode) dropdown menu is open, displaying the following options: 'WPA', '不加密' (No Encryption), 'WEP', 'WPA-PSK', 'WPA2-PSK', and 'Mixed WPA/WPA2-PSK'. The 'WPA' option is currently selected and highlighted in blue. Below the dropdown, the '加密规则' (Encryption Rule) section has radio buttons for 'AES' (selected), 'TKIP', and 'TKIP&AES'. The 'RADIUS密码' (RADIUS Password) field is empty with a toggle for visibility. The '密钥更新周期' (Key Update Cycle) is set to '0' seconds, with a note indicating the range is 60~99999 seconds, where 0 means no update.

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">- 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。

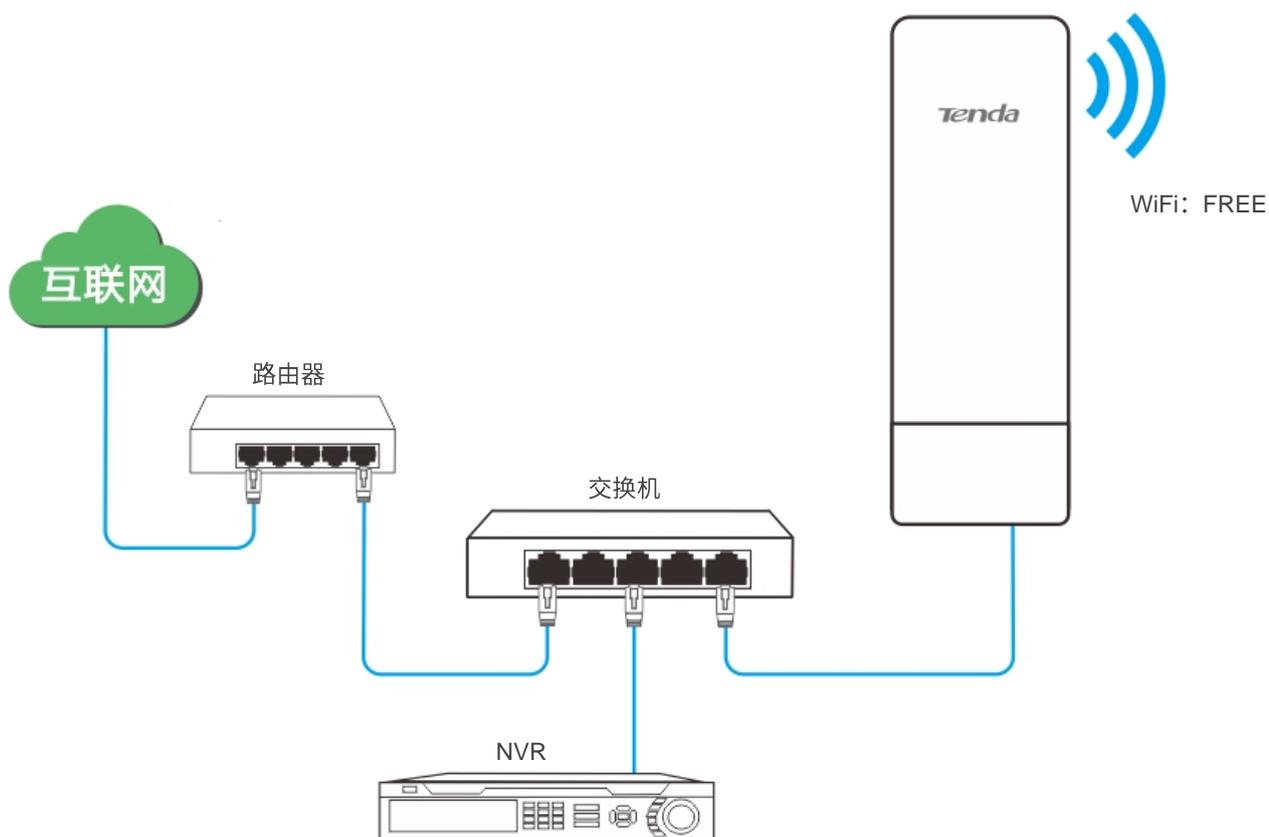
标题项	说明
RADIUS 服务器	
RADIUS 端口	用于输入 RADIUS 服务器的 IP 地址/认证端口/共享密钥。
RADIUS 密码	
加密规则	<p>选择 WPA 加密规则。</p> <ul style="list-style-type: none"> - AES: 高级加密标准。 - TKIP: 临时密钥完整性协议。 - TKIP&AES: 兼容 TKIP 和 AES, 无线客户端使用 TKIP 和 AES 均可连接。
密钥更新周期	WPA 数据加密密钥自动更新周期, 较短的密钥更新周期可增强 WPA 数据安全性。 为 0 表示不更新。

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

步骤 1 进入「无线设置」>「基本设置」页面。

步骤 2 SSID: 修改为“FREE”。

步骤 3 安全模式: 选择“不加密”。

步骤 4 点击 **保存**。

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

信道带宽

扩展信道

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

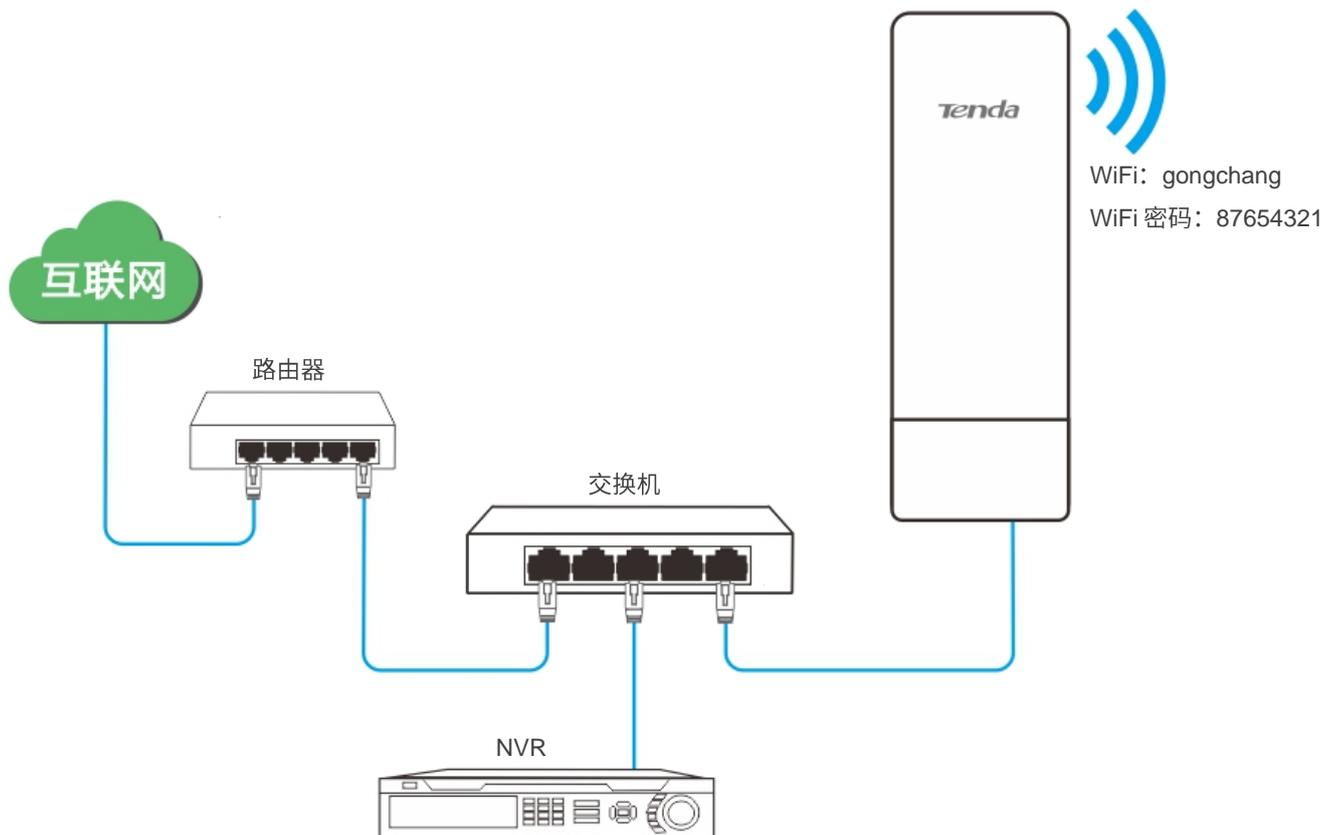
无线设备连接无线网络“FREE”时，不需要输入无线密码就可以连接成功。

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 PSK 安全模式。



配置步骤

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

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 1dBm 29dBm

信道带宽

扩展信道

传输速率

* 安全模式

* 加密规则 AES TKIP TKIP&AES

* 密钥

密钥更新周期 s (范围: 60~99999, 0表示不更新)

----完成

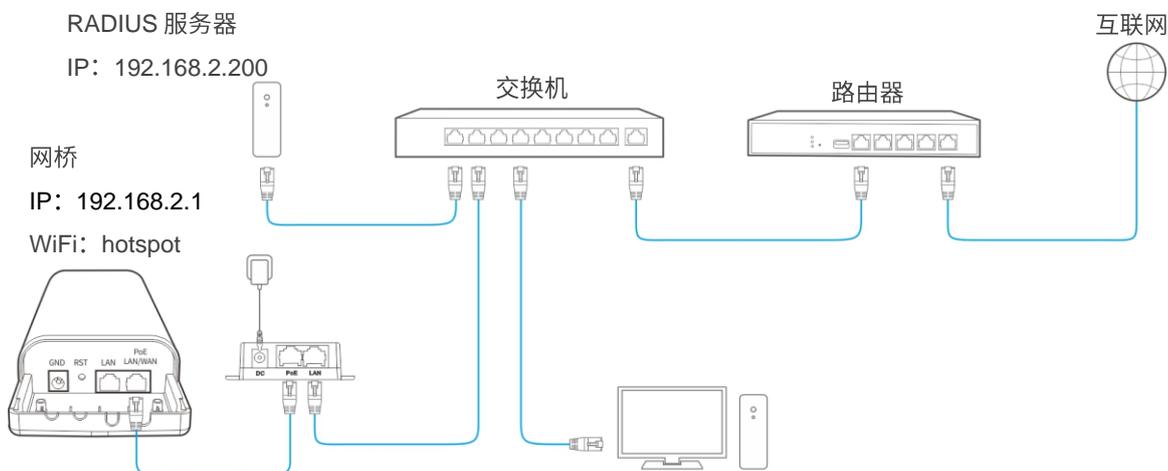
验证配置

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。

步骤 1 进入「无线设置」>「基本设置」页面。

步骤 2 SSID: 修改，如 hotspot。

步骤 3 安全模式: 建议选择“WPA2”。

步骤 4 RADIUS 服务器/端口: 分别输入“192.168.2.200”、“1812”。

步骤 5 加密规则: 建议选择“AES”。

步骤 6 RADIUS 密码: 输入“12345678”。

步骤 7 点击 **保存**。

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 29dBm

信道带宽

扩展信道

传输速率

* 安全模式

* RADIUS服务器

* RADIUS端口

* 加密规则 AES TKIP TKIP&AES

* RADIUS密码

密钥更新周期 s (范围: 60~99999, 0表示不更新)

二、配置 RADIUS 服务器



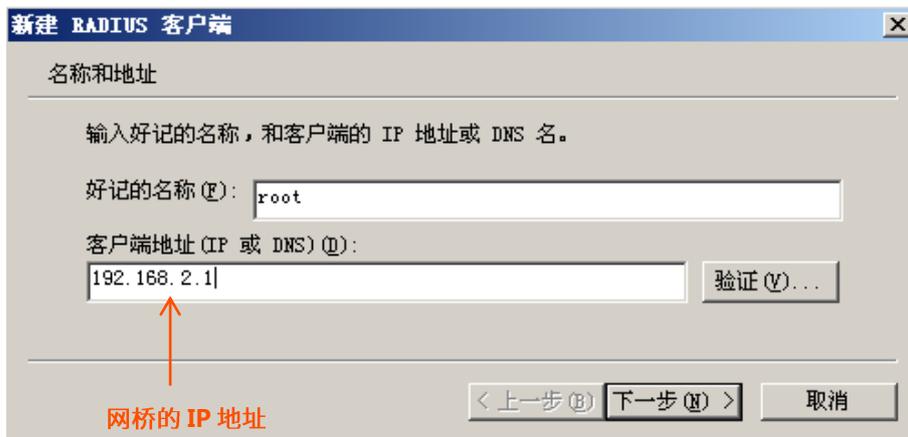
以 Windows 2003 服务器上的 RADIUS 服务器为例说明。

步骤 1 配置 RADIUS 客户端。

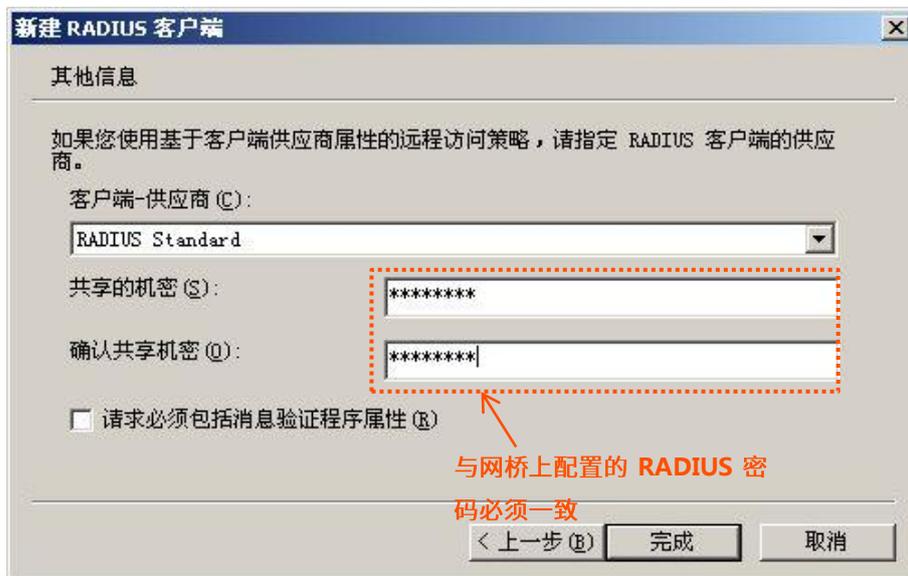
1. 在 Windows 2003 服务器操作系统的管理工具，双击“Internet 验证服务”，右键单击“RADIUS 客户端”，选择“新建 RADIUS 客户端”。



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**。

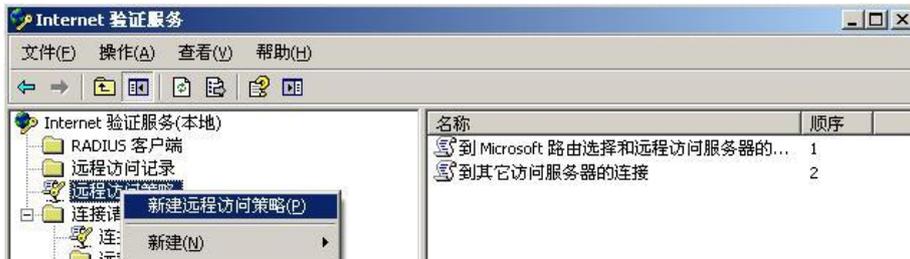


3. 在“共享的机密”和“确认共享机密”栏均输入：12345678，点击 **完成** 返回。

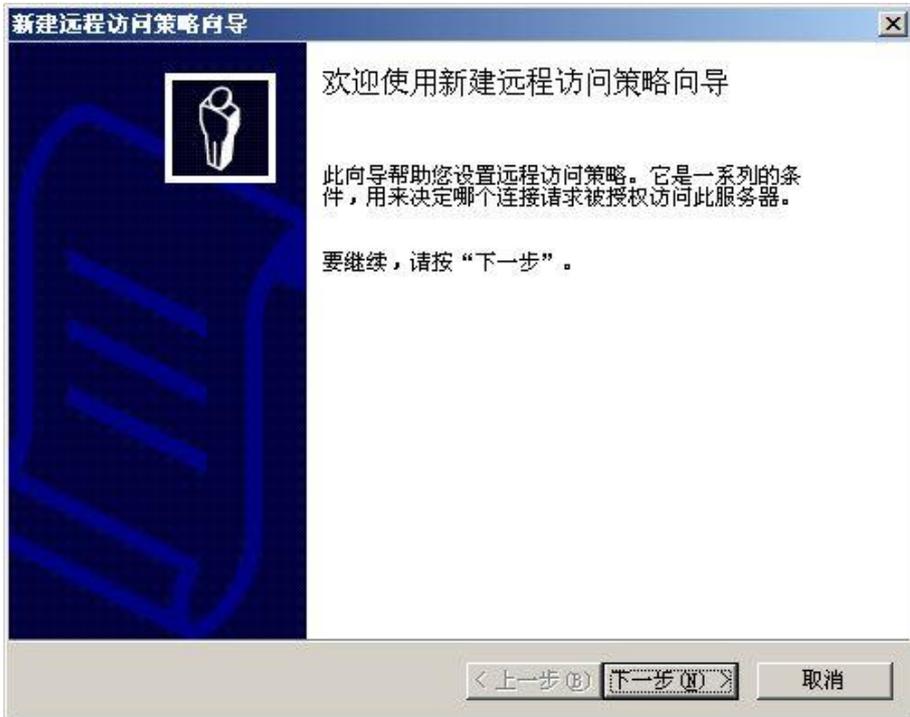


步骤 2 配置远程访问策略。

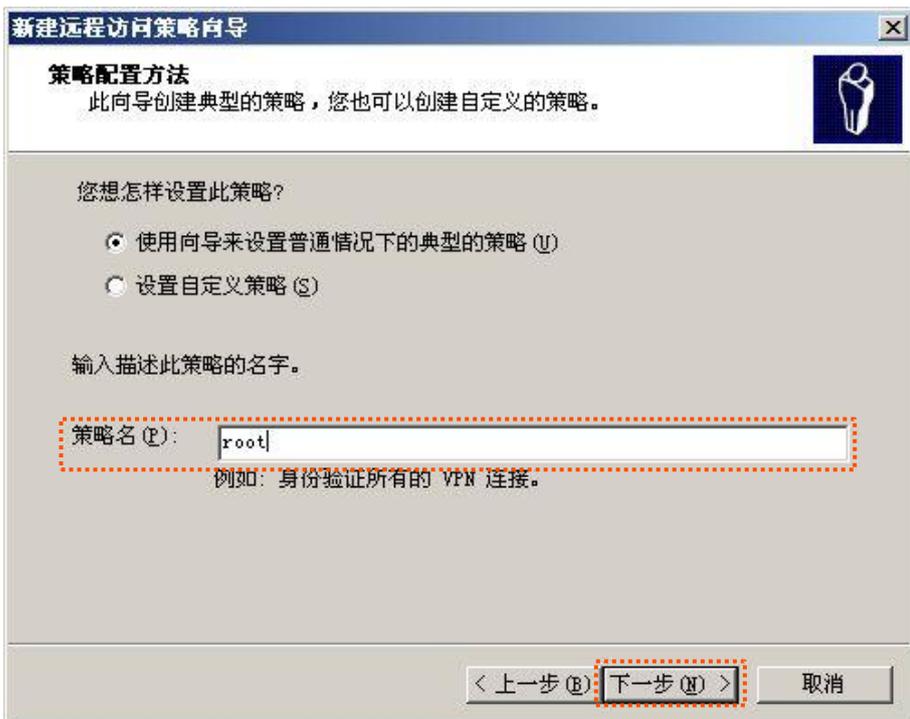
1. 右键单击“远程访问策略”，选择“新建远程访问策略”。



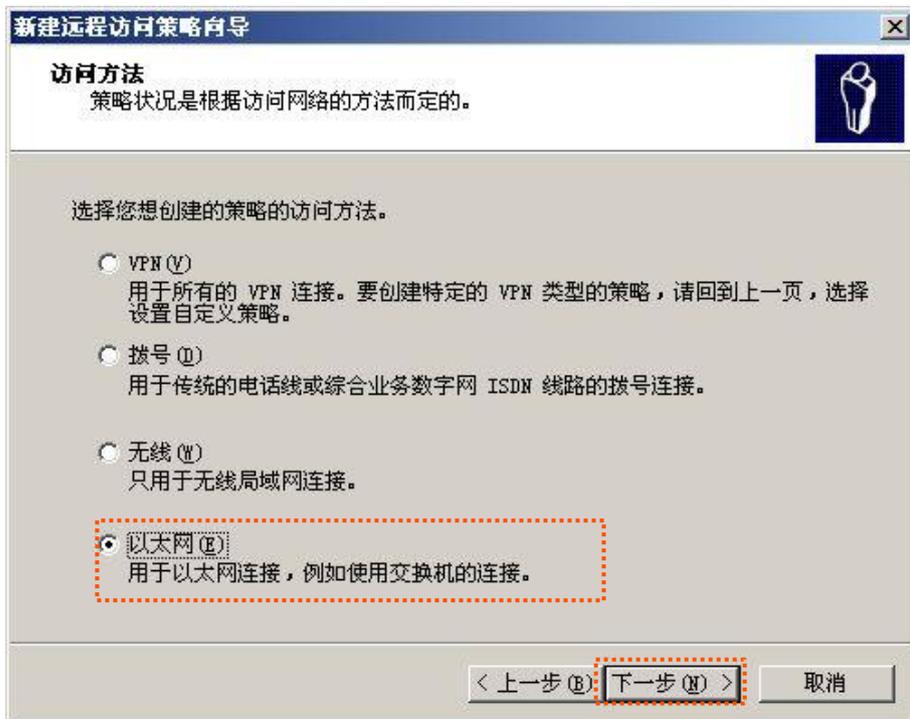
2. 弹出新建远程访问策略向导，点击 **下一步**。



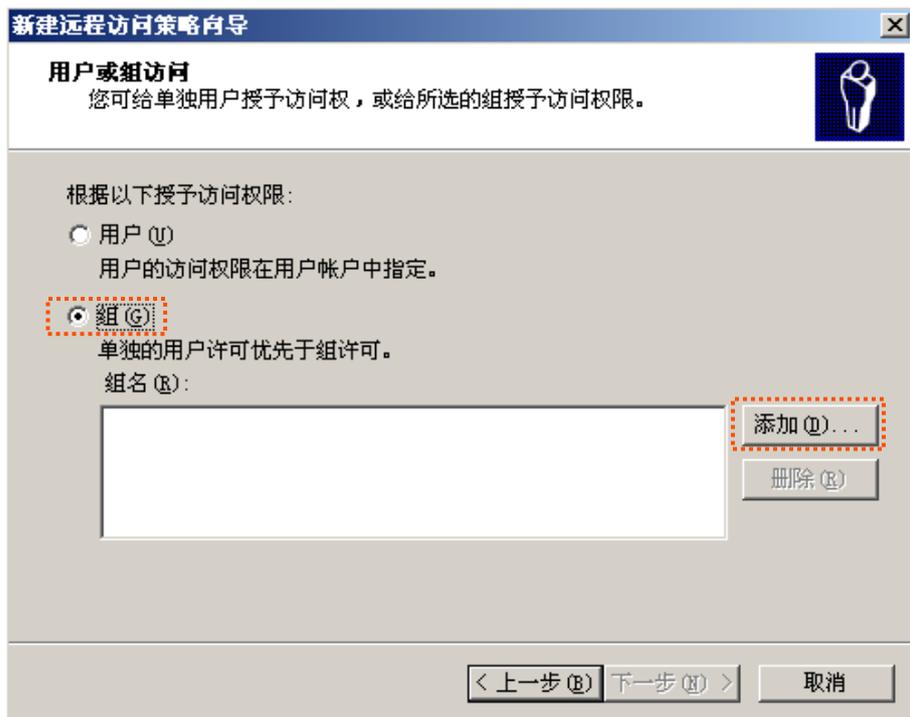
3. 设置策略名，点击 **下一步**。



4. 选择“以太网”，点击 **下一步**。



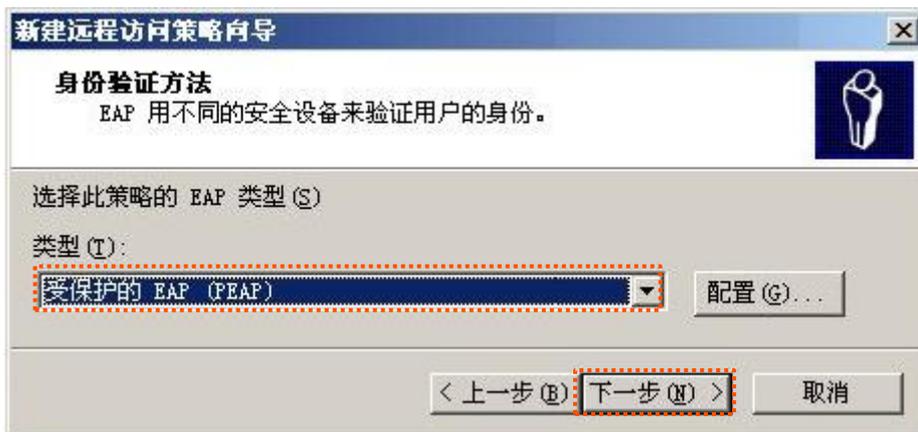
5. 选择“组”，点击 **添加**。



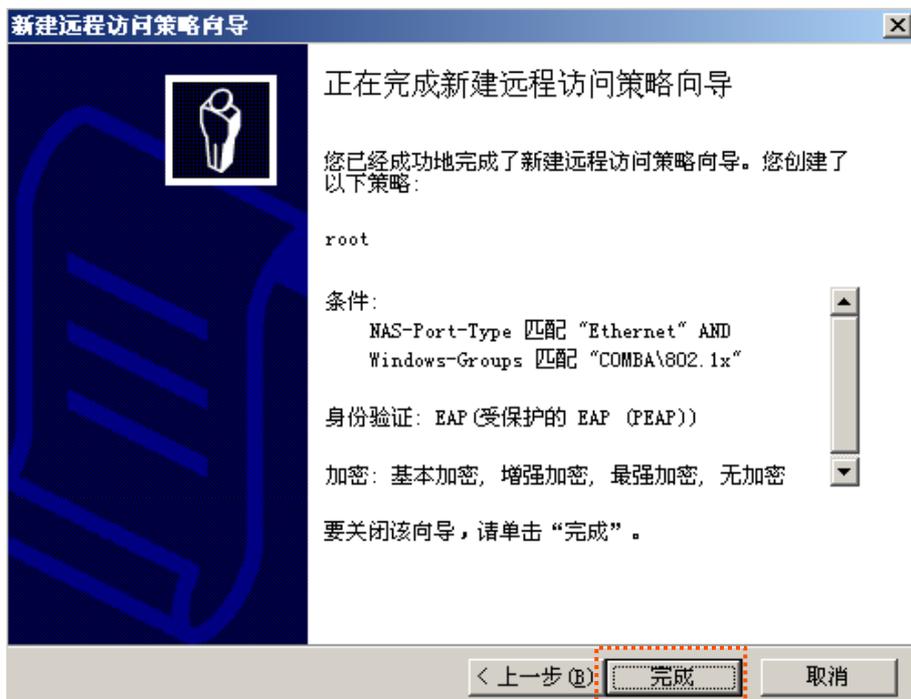
6. 在“输入对象名称来选择”中输入 802.1x，点击 **检查名称**，点击 **确定**。



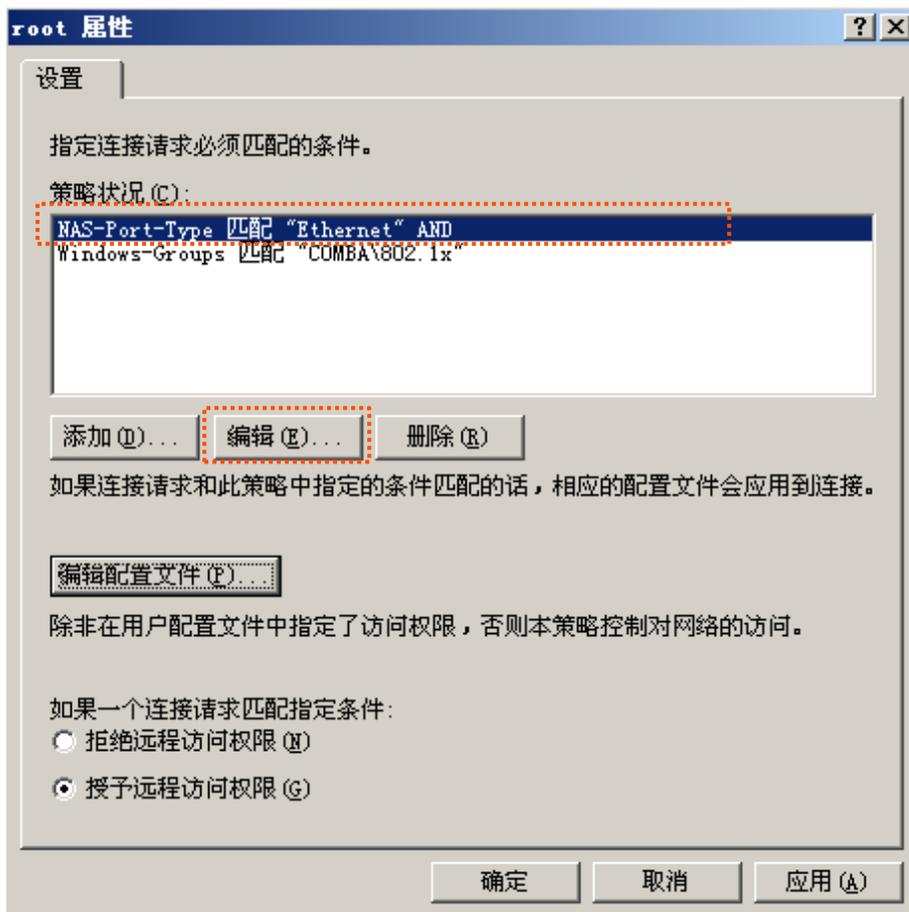
7. 选择受保护的 EAP (PEAP)，点击 **下一步** 完成操作。



8. 完成新建远程访问策略向导操作。



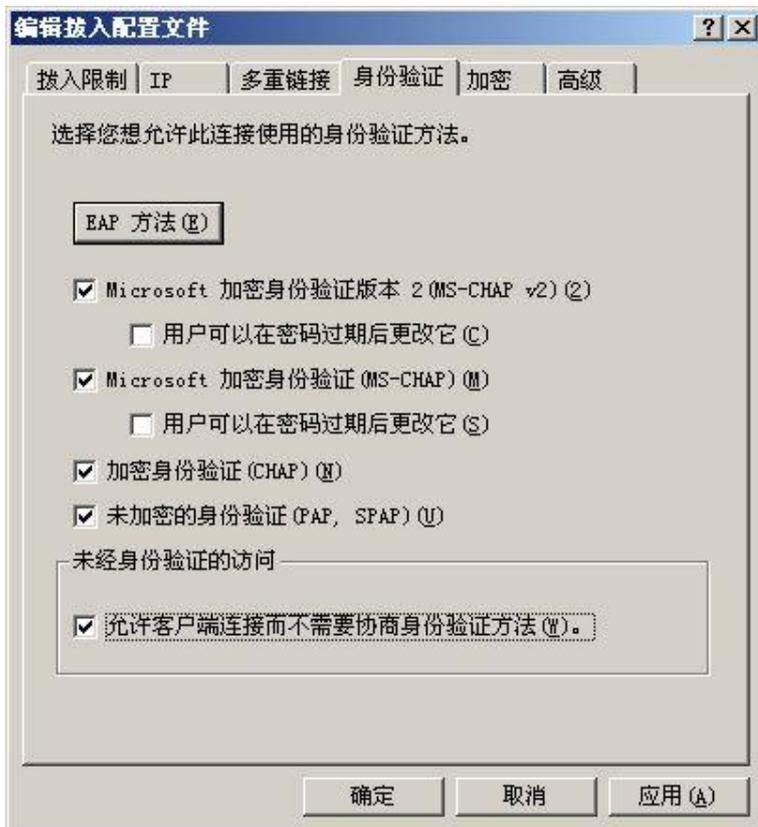
9. 选中 root，点击右键，选择“属性”，在打开的窗口中，选择“授予远程访问权限”，然后选择“NAS-Port-Type 匹配 “Ethernet”AND”，点击 **编辑**。



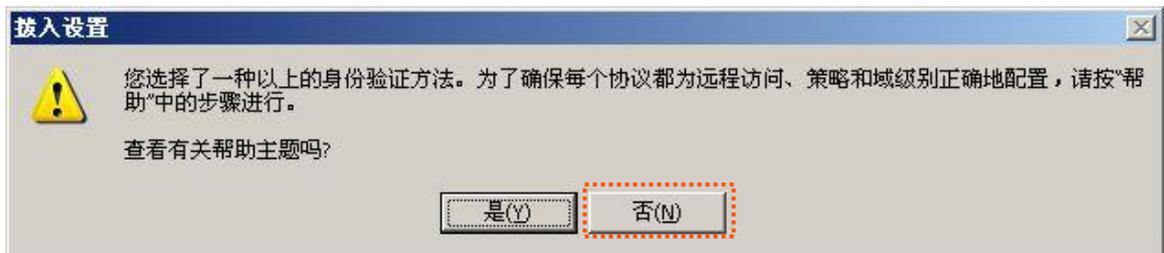
10. 在出现的窗口选择“无线-其它”，点击 **添加>>**，然后点击 **确定**。



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。



步骤 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



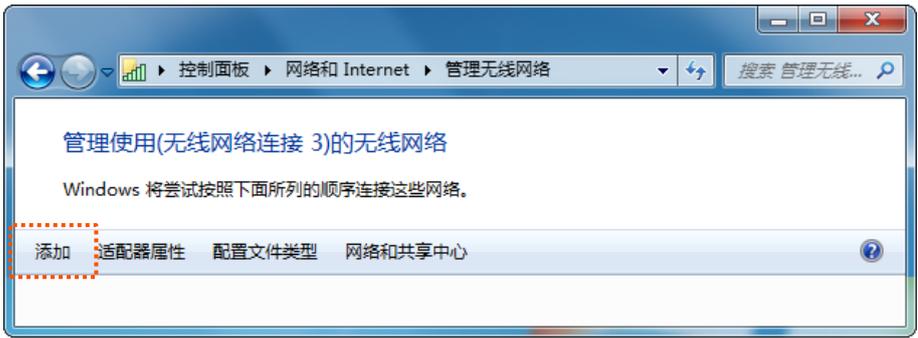
提示

本文以 Windows 7 系统为例说明。

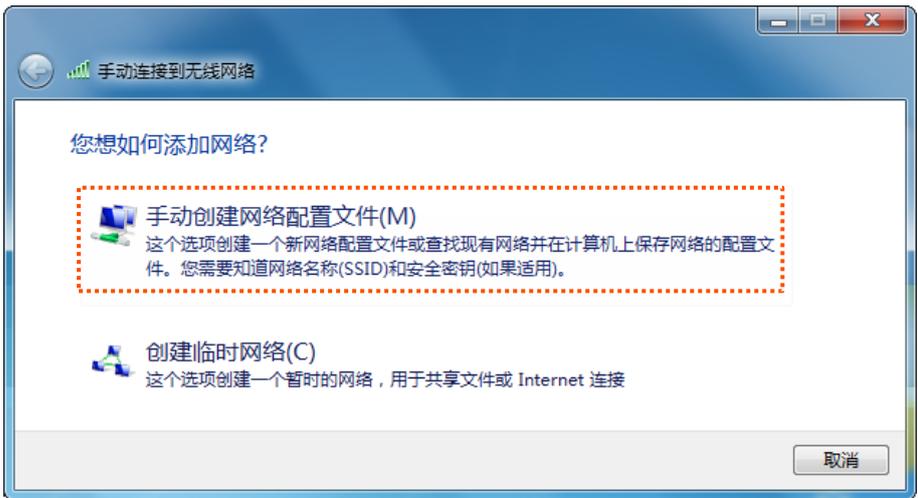
步骤 1 在「控制面板」>「网络和 Internet」>「网络和共享中心」页面，点击“管理无线网络”。



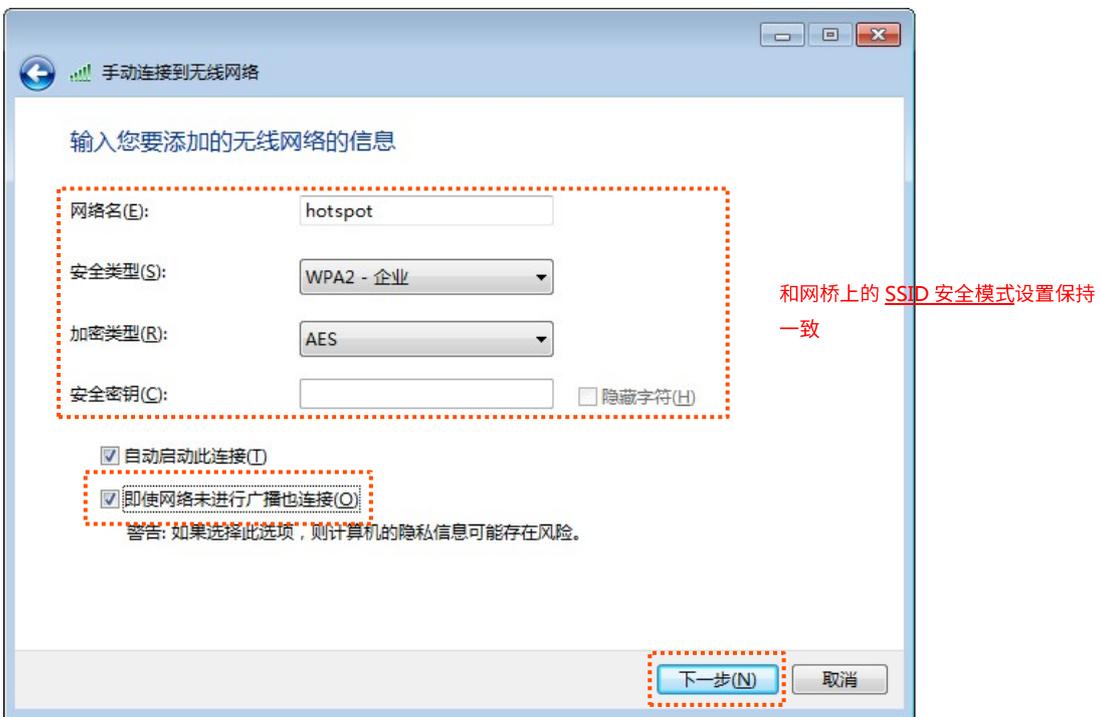
步骤 2 点击“添加”。



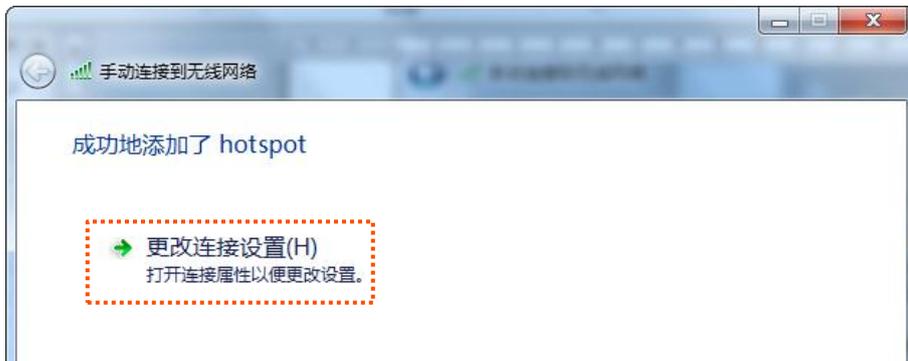
步骤 3 选择“手动创建网络配置文件 (M)”。



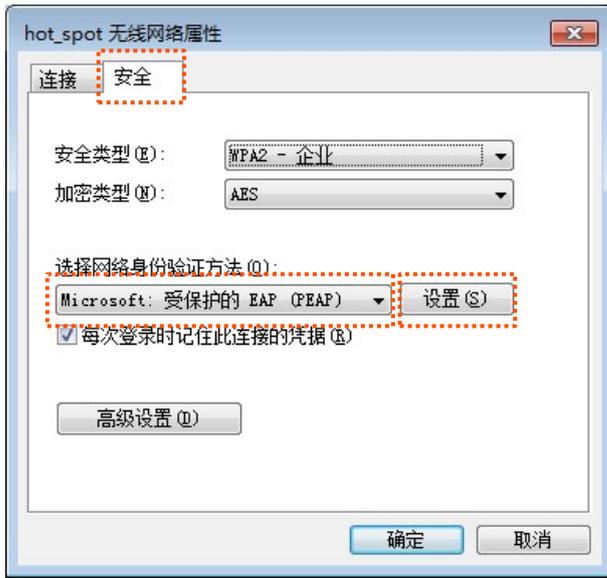
步骤 4 如下图所示输入无线网络信息，勾选“即使网络未进行广播也连接”，然后点击 下一步。



步骤 5 点击“更改连接设置 (H)”。



步骤 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**。



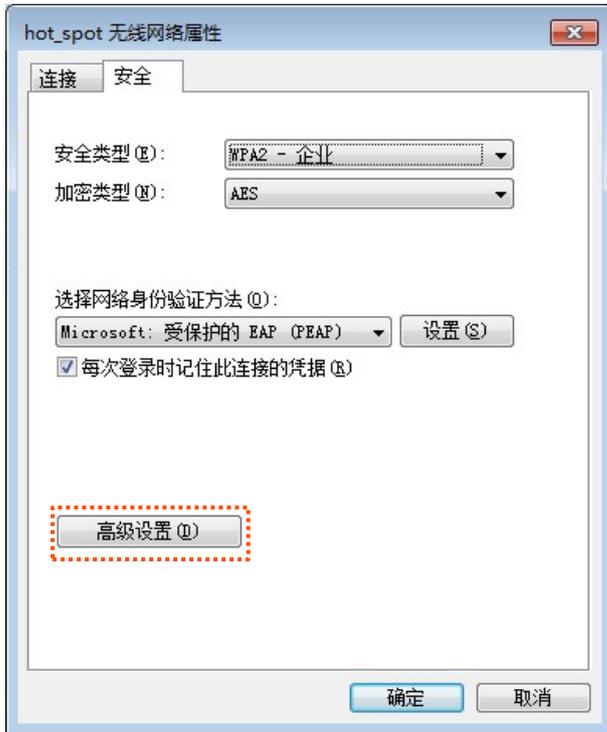
步骤 7 取消“验证服务器证书”，然后点击 **配置**。



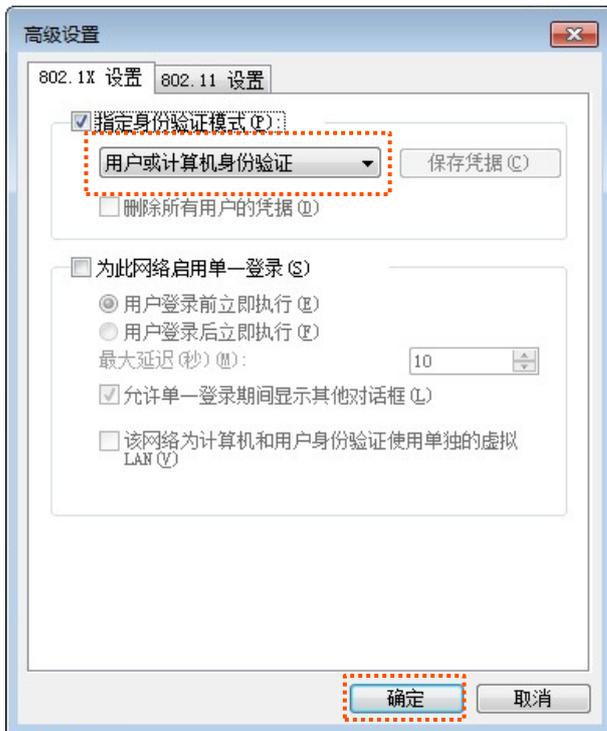
步骤 8 取消“自动使用 windows 登录名和密码”，点击 **确定**。



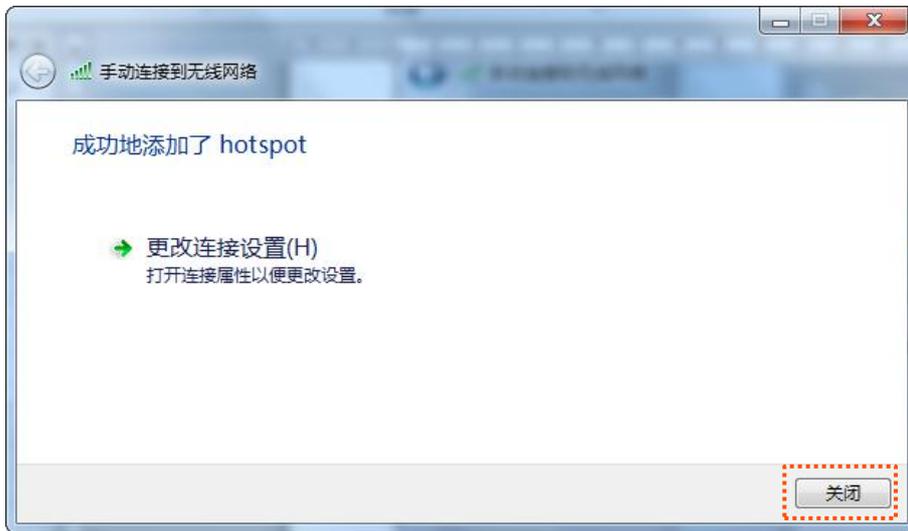
步骤 9 点击 高级设置。



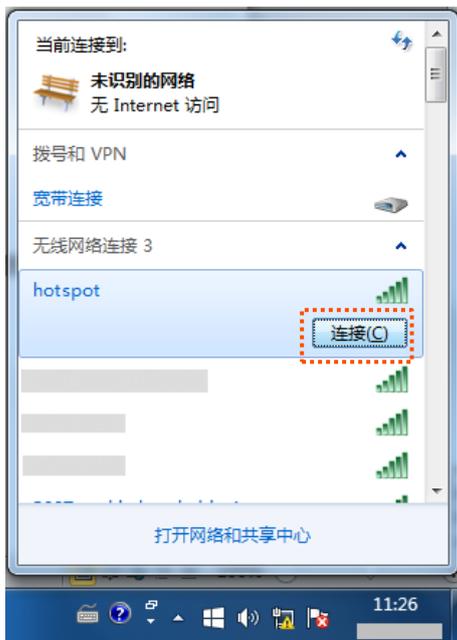
步骤 10 指定身份验证模式为“用户或计算机身份认证”，然后点击 确定。



步骤 11 点击 关闭。



步骤 12 在电脑桌面右下角连接网桥的无线网络，本例为“hotspot”。



步骤 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

7.2.1 概述

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。

7.2.2 修改高级参数

步骤 1 进入「无线设置」>「高级设置」页面。

步骤 2 根据需要修改各参数。

步骤 3 点击 **保存**。

高级设置

WMM	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
APSD	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
接入信号强度限制	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
无线前导码	<input type="radio"/> 短前导码	<input checked="" type="radio"/> 长前导码
穿墙能力	<input checked="" type="radio"/> 强覆盖	<input type="radio"/> 高密度
信号接收能力	<input type="text" value="自动"/>	
传输距离	<input type="text" value="3"/>	km (范围: 0.1~20, 默认: 3)
Beacon间隔	<input type="text" value="100"/>	ms (范围: 40~999, 默认: 100)
Fragment阈值	<input type="text" value="2346"/>	(范围: 256~2346, 默认: 2346)
RTS门限	<input type="text" value="2347"/>	(范围: 1~2347, 默认: 2347)
DTIM间隔	<input type="text" value="1"/>	(范围: 1~255, 默认: 1)
LED1信号灯阈值	<input type="text" value="-90"/>	dBm (范围: -99~0, 默认: -90)
LED2信号灯阈值	<input type="text" value="-80"/>	dBm (范围: -99~0, 默认: -80)
LED3信号灯阈值	<input type="text" value="-70"/>	dBm (范围: -99~0, 默认: -70)

----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”能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。
穿墙能力	设置网桥的穿墙能力。 <ul style="list-style-type: none">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。
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。
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。

标题项	说明
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/LED2/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

通过访问控制功能，可以允许或禁止指定设备接入网桥的无线网络。网桥支持以下访问控制模式：

- 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

步骤 1 进入「无线设置」>「访问控制」页面。

步骤 2 访问控制：点击滑块至 。

步骤 3 模式：根据需要选择“仅允许”或“仅禁止”。

步骤 4 MAC 地址：输入 MAC 地址。

步骤 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。

步骤 6 点击 **保存**。

访问控制

SSID Tenda_FEF668

访问控制

模式 仅禁止 仅允许

MAC地址 : : : : :

序号	MAC地址	状态	操作
1	12:12:12:12:12:12	<input checked="" type="checkbox"/> 启用	<input type="button" value="删除"/>

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">仅允许：仅允许访问控制列表中的无线设备接入该 SSID。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。

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 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

步骤 1 进入「无线设置」>「访问控制」页面。

步骤 2 访问控制：点击滑块至 。

步骤 3 模式：选择“仅禁止”。

步骤 4 MAC 地址：输入“C8:3A:35:00:00:01”，点击 **添加**。

步骤 5 重复**步骤 4**，添加 MAC “C8:3A:35:00:00:02”、“C8:3A:35:00:00:03”。

步骤 6 点击 **保存**。

访问控制

SSID Tenda_FEF668

* 访问控制

* 模式 仅禁止 仅允许

* MAC地址 : : : : : *

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

----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，您可以修改网桥各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。



LAN口速率

PoE/LAN口速率 自动协商

LAN口速率 自动协商

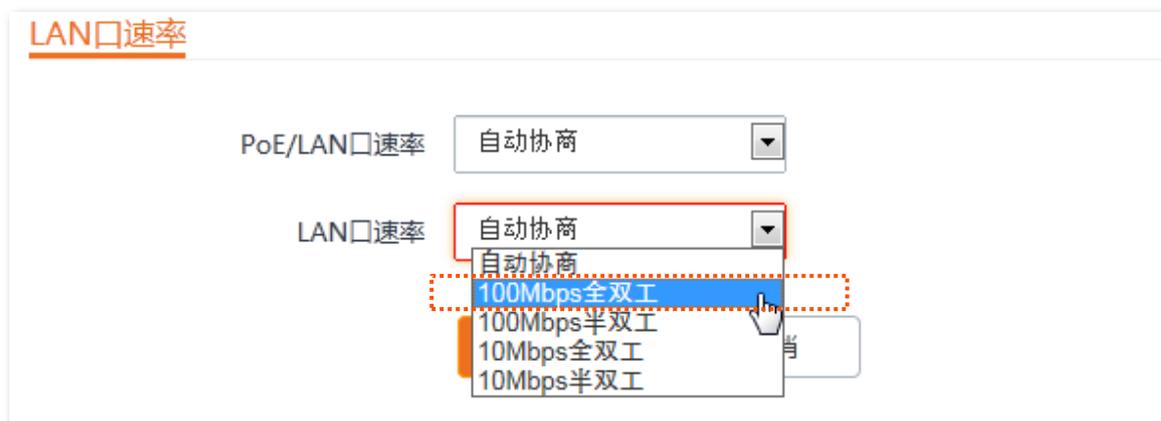
保存 取消

8.1.2 修改 LAN 口速率

步骤 1 进入「高级设置」>「LAN 口速率」页面。

步骤 2 LAN 口速率：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”。

步骤 3 点击 **保存**。



LAN口速率

PoE/LAN口速率 自动协商

LAN口速率

自动协商
自动协商
100Mbps全双工
100Mbps半双工
10Mbps全双工
10Mbps半双工

----完成

设置完成后，可以在“系统状态”页面查看，如下图所示：

系统状态			
设备名称	O3V2.0	LAN MAC	50:2B:73:FE:F6:68
运行时间	2小时16分16秒	WLAN MAC	50:2B:73:FE:F6:69
系统时间	2018-04-17 16:09:29	PoE LAN/LAN口速率	未连接/100Mbps全双工
软件版本	V1.0.0.5(2182)	LAN IP	192.168.2.1
硬件版本	V2.0		

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

概述

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，供管理员分析参考。

扫描周围无线网络

假设要检测网桥周围的无线网络情况。

步骤 1 进入「高级设置」>「网络诊断」页面。

步骤 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。



The screenshot shows the 'Network Diagnosis' page with a dropdown menu set to 'Scan Signal'. Below the menu is a table with 8 rows of detected wireless networks. Each row contains: Serial Number, SSID, MAC Address, Channel, Security Mode, and Signal Strength (represented by a bar chart icon).

序号	SSID	MAC地址	信道	安全模式	信号强度
1	Tenda_1	50:2B:73:09:94:51	11	不加密	
2	Tenda_FEF460	C8:3A:35:18:68:41	1	不加密	
3	Tenda_8BBCFF	C8:3A:35:13:05:08	11	Mixed WPA/WPA2-PSK...	
4	Tenda_AC9	D8:32:14:4C:CB:71	10	Mixed WPA/WPA2-PSK...	
5	Tenda_9AA9BB	B0:E1:7E:92:7F:80	6	WPA2-PSK,AES	
6	Tenda_843338	C8:3A:35:1E:B6:C1	9	Mixed WPA/WPA2-PSK...	
7	Tenda_661180	00:02:03:04:05:06	5	不加密	
8	Tenda_FD11E0	50:2B:73:09:93:F1	5	WPA2-PSK,AES	

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。

8.2.2 Ping

概述

用于检测网络的连通性和连通质量。

执行 Ping

假设要检测到百度服务器的链路是否畅通。

步骤 1 进入「高级设置」>「网络诊断」页面。

步骤 2 网络诊断：选择“Ping”。

步骤 3 IP 地址：选择“手动设置”。

步骤 4 目标 IP 地址/域名：输入目的 IP 地址或域名，本例为“www.baidu.com”。

步骤 5 Ping 包个数：设置 ping 发送的数据包的个数，建议保持默认设置。

步骤 6 数据包大小：设置 ping 发送的数据包的大小，建议保持默认设置。

步骤 7 点击 **开始**。

网络诊断

* 网络诊断 Ping

* IP地址 手动设置

* 目标IP地址/域名 www.baidu.com

* Ping包个数 4 (范围：1~10000)

* 数据包大小 32 字节 (范围：1~60000)

开始

----完成

稍后，诊断结果将显示在页面下方。如下图所示。

网络诊断

网络诊断

IP地址

目标IP地址/域名

Ping包个数 (范围: 1~10000)

数据包大小 字节 (范围: 1~60000)

IP地址	时间	TTL
58.217.200.112	32.685ms	48
14.215.177.38	11.772ms	50
14.215.177.38	9.648ms	50
58.217.200.112	56.315ms	48

10 条数据/页 共4条

收到4个数据包, 发送4个数据包, 丢包率0.00%

最小9.648ms 平均27.61ms 最大56.315ms

8.2.3 Traceroute

概述

用于检测数据包从网桥到目标主机所经过的路由。

执行 Traceroute

假设要检测网桥到百度服务器所经过的路由。

步骤 1 进入「高级设置」>「网络诊断」页面。

步骤 2 网络诊断：选择“Traceroute”。

步骤 3 目标 IP 地址/域名：输入目的 IP 地址或域名，本例为“www.baidu.com”。

步骤 4 点击 。

网络诊断

* 网络诊断

* 目标IP地址/域名

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

目标IP地址/域名

停止

序号	IP地址	时间
1	172.21.20.1	5.440 ms 0.718 ms 0.637 ms
2	192.168.1.60	4.471 ms 1.072 ms 11.307 ms
3	192.168.3.1	3.586 ms 1.349 ms 6.694 ms
4	172.16.200.1	2.314 ms 5.041 ms 11.049 ms
5	192.168.20.1	3.926 ms 5.113 ms 4.709 ms
6	192.168.21.254	4.093 ms 11.104 ms 7.041 ms
7	192.168.16.1	9.995 ms 2.617 ms 5.147 ms
8	100.64.0.1	94.150 ms 8.034 ms 22.698 ms

8.2.4 速率测试

概述

用于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：

网络诊断

网络诊断 速率测试

↑ AVG RX	↓ AVG TX	↕ AVG Total
0 Mbps	0 Mbps	0 Mbps

客户端模式 服务器

对端AP的IP地址 手动设置

IP地址

Web服务端口号

登录用户名

登录密码

组数 (范围: 1~20)

方向 双向

时间 s (范围: 1~60)

参数说明

标题项	说明
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。
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。

标题项	说明
	<ul style="list-style-type: none"> - 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。
	显示测速的结果。
测试结果	<ul style="list-style-type: none"> - 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。

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，并已经成功桥接网桥 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

设置步骤如下。

步骤 1 登录网桥 1 或网桥 2 管理页面，此处以网桥 2 为例。

步骤 2 进入「高级设置」>「网络诊断」页面。

步骤 3 网络诊断：选择“速率测试”。

步骤 4 对端 AP 的 IP 地址：点击下拉框，选择“手动设置”。

步骤 5 IP 地址：输入对端网桥的 LAN 口 IP 地址，本例为“192.168.2.1”。

步骤 6 登录用户名/密码：输入对端网桥 Web 管理页面的登录用户名/密码，本例为“admin”。

步骤 7 方向：点击下拉框，选择“双向”。

步骤 8 点击 **开始**。

网络诊断

* 网络诊断

↑ AVG RX	↓ AVG TX	↕ AVG Total
0 Mbps	0 Mbps	0 Mbps

客户端模式 服务器

* 对端AP的IP地址

* IP地址

Web服务端口号

* 登录用户名

* 登录密码

组数 (范围: 1~20)

* 方向

时间 s (范围: 1~60)

----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

速率测试

↑ AVG RX

50.24 Mbps

↓ AVG TX

51.45 Mbps

↕ AVG Total

55.65 Mbps

客户端模式

服务器

对端AP的IP地址

手动设置

IP地址

192.168.2.1

Web服务端口号

80

登录用户名

admin

登录密码

admin

组数

10

(范围: 1~20)

方向

双向

时间

30

s (范围: 1~60)

开始

8.3 带宽控制

8.3.1 概述

仅适用于无线 WAN 模式、路由模式。

外网带宽总是有限的，因此，网络管理员需要对用户进行网速控制，使有限的带宽资源得到合理分配，以有效利用外网资源。

进入页面：点击「高级设置」>「带宽控制」。

带宽控制

备注

IP地址范围 192.168.2. ~ 192.168.2.

最大上传速率 Mbps

最大下载速率 Mbps

序号	备注	IP地址范围	最大上传速率	最大下载速率	状态	操作
----	----	--------	--------	--------	----	----

8.3.2 配置带宽控制

步骤 1 点击「高级设置」>「带宽控制」。

步骤 2 设置各参数。

步骤 3 点击 **添加**。

带宽控制

备注

IP地址范围 192.168.2. ~ 192.168.2.

最大上传速率 Mbps ▼

最大下载速率 Mbps ▼

添加

序号	备注	IP地址范围	最大上传速率	最大下载速率	状态	操作

----完成

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。
操作	点击 可以删除规则。

8.3.3 带宽控制示例

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路由模式并接入互联网。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

步骤 1 点击「高级设置」>「带宽控制」。

步骤 2 备注：设置规则的备注信息，如网速限制。

步骤 3 IP 地址范围：设置规则适用的 IP 地址范围，本例为“92.168.2.100~192.168.2.200”。

步骤 4 最大上传速率：设置规则中用户的最大上传速率，本例为“1Mbps”。

步骤 5 最大下载速率：设置规则中用户的最大下载速率，本例为“1Mbps”。

步骤 6 点击 **添加**。

带宽控制

* 备注

* IP地址范围 192.168.2. ~ 192.168.2.

* 最大上传速率 Mbps

* 最大下载速率 Mbps

---完成

添加成功，如下图示：

序号	备注	IP地址范围	最大上传速率	最大下载速率	状态	操作
1	网速限制	192.168.2.100~192.168.2.200	1Mbps	1Mbps	<input checked="" type="checkbox"/> 启用	<input type="button" value="v"/>

10 条数据/页 共1条

验证配置

IP 地址为 192.168.2.100~192.168.2.200 的用户，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

仅适用于无线 WAN 模式、路由模式。

默认情况下，广域网中的用户不能主动访问局域网内的计算机。端口映射开放了一个服务端口，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计算机，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」。

端口映射

内网IP地址

内网端口

外网端口

协议

应用

序号	内网IP地址	内网端口	外网端口	协议	应用	状态	操作
----	--------	------	------	----	----	----	----

8.4.2 配置端口映射

步骤 1 点击「高级设置」>「端口映射」。

步骤 2 设置各参数。

步骤 3 点击 **添加**。

端口映射

内网IP地址

内网端口

外网端口

协议

应用

添加

序号	内网IP地址	内网端口	外网端口	协议	应用	状态	操作
----	--------	------	------	----	----	----	----

---完成

参数说明

标题项	说明
内网 IP 地址	局域网内建立服务器的计算机的 IP 地址。
内网端口	局域网内服务器的服务端口。
外网端口	网桥开放给广域网用户访问的端口。
协议	相应服务的协议类型。 设置时，如果不确定服务的协议类型，可以选择“TCP&UDP”。
应用	局域网建立的应用服务。 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。
操作	点击  可以删除规则。

8.4.3 端口映射示例

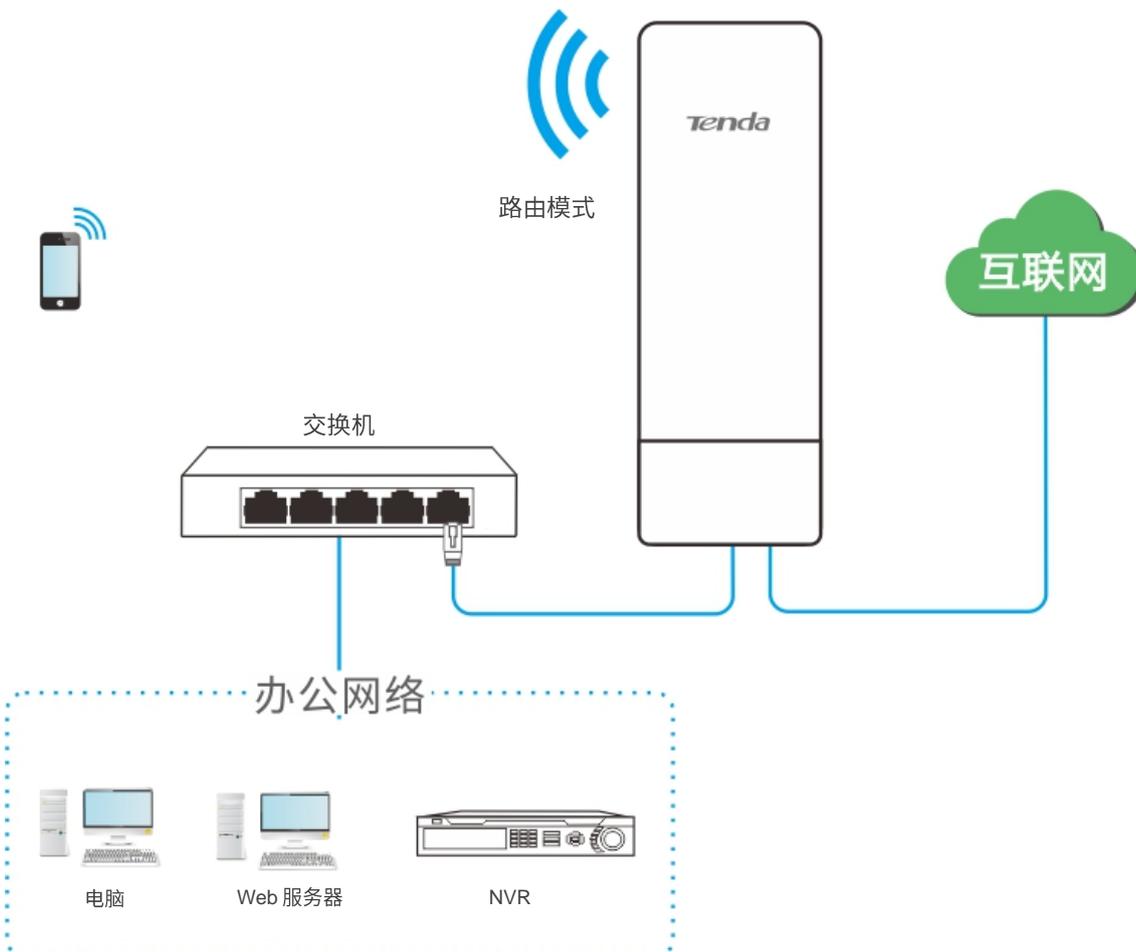
组网需求

某公司使用网桥组建网络，网络管理员已将网桥设置为路由模式并接入互联网。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。

可以使用网桥的端口映射功能实现上述需求。假设：

- 网桥开放给广域网用户访问内网 Web 服务器的端口为 80。
- 网桥的 WAN 口 IP 地址为 202.105.11.22。
- 内网 Web 服务器的 IP 地址为 192.168.2.100。
- 内网 Web 服务器的服务端口为 80。

网络拓扑



配置步骤

步骤 1 点击「高级设置」>「端口映射」。

步骤 2 内网 IP 地址：输入内网 Web 服务器的 IP 地址，本例为“192.168.2.100”。

步骤 3 应用：选择内网建立的应用，本例为“HTTP”。

步骤 4 协议：选择 Web 服务器使用的协议，如果不确定，可以选择“TCP&UDP”。

步骤 5 点击 **添加**。

端口映射

* 内网IP地址

内网端口

外网端口

* 协议

* 应用

添加

----完成

添加成功，如下图示：

序号	内网IP地址	内网端口	外网端口	协议	应用	状态	操作
1	192.168.2.100	80	80	TCP&UDP	HTTP	<input checked="" type="checkbox"/> 启用	

10 条数据/页 共1条

验证配置

广域网用户使用“内网服务应用层协议名称://网桥 WAN 口 IP 地址:外网端口”可以成功访问该公司内部 Web 服务器。在本例中，访问地址为“http://202.105.11.22:80”。



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

仅适用于无线 WAN 模式、路由模式。通过 MAC 过滤功能，您可以限定哪些用户可以通过本网桥上网。

进入页面：点击「高级设置」>「MAC 过滤」。

MAC 过滤功能默认禁用。



The screenshot shows the 'MAC过滤' (MAC Filter) configuration page. At the top, the title 'MAC过滤' is underlined. Below it, there is a '模式' (Mode) dropdown menu currently set to '禁用' (Disabled). A blue '保存' (Save) button is located at the bottom center of the form.

8.5.2 配置 MAC 过滤

步骤 1 点击「高级设置」>「MAC 过滤」。

步骤 2 设置各参数。

步骤 3 点击 **添加**。



The screenshot shows the 'MAC过滤' (MAC Filter) configuration page with the '模式' (Mode) dropdown set to '仅禁止' (Only Block). Below the mode dropdown are input fields for '备注' (Remarks) and 'MAC地址' (MAC Address). The '时间' (Time) field is set to '00:00 ~ 00:00'. The '日期' (Date) field has checkboxes for '星期一' (Monday), '星期二' (Tuesday), '星期三' (Wednesday), '星期四' (Thursday), '星期五' (Friday), '星期六' (Saturday), '星期日' (Sunday), and '每天' (Every Day). A blue '添加' (Add) button is located at the bottom center of the form. Below the form is a table header with columns: '序号' (Serial Number), '备注' (Remarks), 'MAC地址' (MAC Address), '时间' (Time), '模式' (Mode), '状态' (Status), and '操作' (Action).

----完成

参数说明

标题项	说明
模式	MAC 过滤规则模式。 <ul style="list-style-type: none">- 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本网桥上网，允许其他设备通过本网桥上网。- 仅允许：允许列表中 MAC 地址对应的设备通过本网桥上网，拒绝其他设备通过本网桥上网。
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。
日期	规则生效的具体日期。
状态	规则的启用状态。
操作	点击  可以删除规则。

8.5.3 MAC 过滤示例

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路由模式并接入互联网。

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

步骤 1 进入「高级设置」>「MAC 过滤」页面。

步骤 2 模式：选择 MAC 过滤规则的模式，本例为“仅允许”。

步骤 3 备注：设置规则的备注，如采购。

步骤 4 MAC 地址：输入采购人员电脑的物理地址，本例为“CC:3A:61:71:1B:6E”。

步骤 5 时间：选择规则生效的时间段，本例为“08:00~18:00”。

步骤 6 日期：选择规则生效的日期，本例为“星期一~星期五”。

步骤 7 点击 **添加**。

MAC过滤

* 模式

* 备注

* MAC地址

* 时间 08:00 ~ 18:00

* 日期 星期一 星期二 星期三
 星期四 星期五 星期六
 星期日 每天

---完成

添加成功，如下图示：

序号	备注	MAC地址	时间	模式	状态	操作
1	采购	CC:3A:61:71:1B:6E	星期一、二、三、四、五 08:00-18:00	仅允许	<input checked="" type="checkbox"/> 启用	<input type="button" value="删除"/>

10 条数据/页 共1条

验证配置

在星期一~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

仅适用于无线 WAN 模式、路由模式。

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（通常需要是公网 IP 地址）始终被映射到一个固定的域名上。动态 DNS 功能一般与其他功能如端口映射、DMZ 主机、远程 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 地址变化，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

服务提供商 3322.org [去注册](#)

登录用户名

登录密码

域名

配置动态 DNS

步骤 1 点击「高级设置」>「网络服务」。

步骤 2 动态 DNS：点击滑块至 。

步骤 3 设置各参数。

步骤 4 点击 **保存**。

动态DNS

服务提供商 [去注册](#)

登录用户名

登录密码

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：Dyndns、No-ip.com、3322.org。
登录用户名	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。
登录密码	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	在动态 DNS 服务提供商网站上申请的域名。

动态 DNS 示例

组网需求

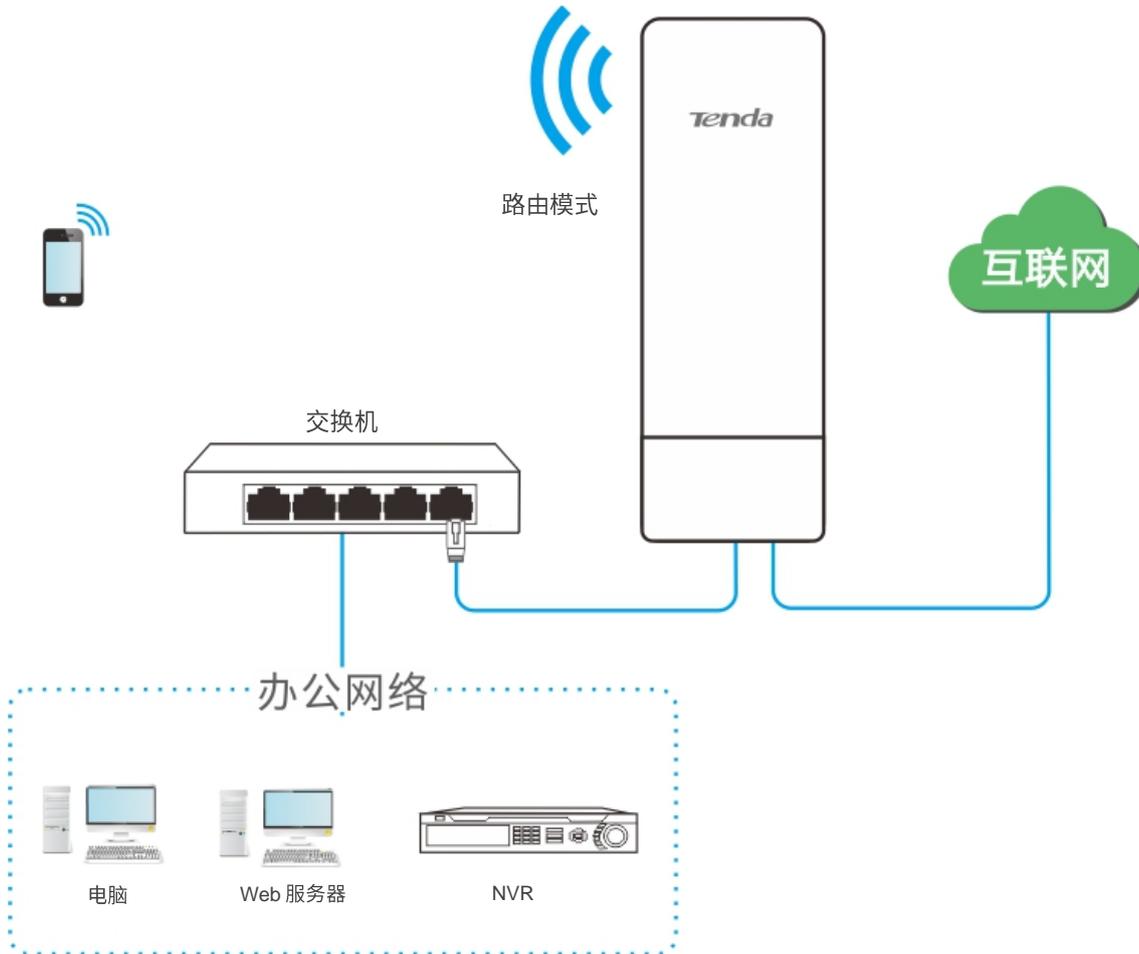
某公司使用网桥组建网络，网络管理员已将网桥设置为路由模式并接入互联网。现需要将公司内部的 Web 服务器开放给广域网用户，使员工不在公司时也能访问企业内部网络。

可以使用网桥的“动态 DNS+端口映射”功能实现上述需求。

假设：

- 网桥开放给广域网用户访问内网 Web 服务器的端口为 80。
- 内网 Web 服务器的 IP 地址为 192.168.2.100。
- 内网 Web 服务器的服务端口为 80。
- 动态 DNS 服务提供商为 Dyndns.com。
- 动态 DNS 登录用户名和密码均为 tenda。
- 动态 DNS 域名为 tenda.dyndns.com。

网络拓扑



配置步骤

一、设置动态 DNS

步骤 1 进入「高级设置」>「网络服务」页面。

步骤 2 动态 DNS：点击滑块至 。

步骤 3 服务提供商：选择您申请域名的动态 DNS 供应商，本例为“Dyndns.com”。

步骤 4 登录用户名：输入您在服务提供商网站注册的用户名，本例为“tenda”。

步骤 5 登录密码：输入您在服务提供商网站注册的用户名对应的密码，本例为“tenda”。

步骤 6 域名：输入您从服务提供商网站申请的域名，本例为“tenda.dyndns.com”。

步骤 7 点击 **保存**。



A configuration form for Dynamic DNS. It includes a toggle switch for '动态DNS' (Dynamic DNS) which is turned on. Below it are fields for '服务提供商' (Service Provider) set to 'Dyndns' with a '去注册' (Go Register) link, '登录用户名' (Login Username) set to 'tenda', '登录密码' (Login Password) masked with dots, and '域名' (Domain Name) set to 'tenda.dyndns.com'.

二、设置端口映射

步骤 1 点击「高级设置」>「端口映射」。

步骤 2 内网 IP 地址：输入 Web 服务器的 IP 地址，本例为“192.168.2.100”。

步骤 3 应用：选择内网建立的应用，本例为“HTTP”。

步骤 4 协议：选择 Web 服务器使用的协议，如果不确定，可以选择“TCP&UDP”。

步骤 5 点击 **添加**。



A '端口映射' (Port Mapping) configuration form. It contains fields for '内网IP地址' (Internal IP Address) set to '192.168.2.100', '内网端口' (Internal Port) set to '80', '外网端口' (External Port) set to '80', '协议' (Protocol) set to 'TCP&UDP', and '应用' (Application) set to 'HTTP'. An orange '添加' (Add) button is at the bottom.

---完成

添加成功，如下图示：

序号	内网IP地址	内网端口	外网端口	协议	应用	状态	操作
1	192.168.2.100	80	80	TCP&UDP	HTTP	<input checked="" type="checkbox"/> 启用	

10 条数据/页 共1条

验证配置

广域网用户使用“内网服务应用层协议名称://网桥的 WAN 口域名:外网端口”可以成功访问该公司内部 Web 服务器。在本例中，访问地址为“http://tenda.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 IP 地址变化而导致服务中断。

8.6.2 远程 WEB 管理

概述

仅适用于无线 WAN 模式、路由模式。

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

步骤 1 进入「高级设置」>「网络服务」页面。

步骤 2 远程 WEB 管理：点击滑块至

步骤 3 设置各参数。

步骤 4 点击 **保存**。



----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	可以远程访问网桥的电脑的 IP 地址。 <ul style="list-style-type: none">- 全部：互联网上任意电脑都能访问路由器的管理页面。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路由器的管理页面。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。

远程 WEB 管理配置举例

组网需求

某公司使用网桥组建网络，网络管理员在设置网络时遇到问题，需要 Tenda 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 地址为 202.105.106.55。
- 允许远程访问网桥管理页面的电脑的 IP 地址为 202.105.88.77。
- 远程 WEB 管理的服务端口号为 8080。

配置步骤

步骤 1 进入「高级设置」>「网络服务」页面。

步骤 2 远程 WEB 管理：点击滑块至 。

步骤 3 IP 地址：选择“手动设置”。

步骤 4 输入 IP 地址：输入要远程访问网桥管理页面的电脑的 IP 地址，本例为“202.105.88.77”。

步骤 5 端口：本例为“8080”。

步骤 6 点击 **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://202.105.106.55:8080”，即可登录网桥并对其进行管理。

8.6.3 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。启用定时重启功能后，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

步骤 1 进入「高级设置」>「网络服务」页面。

步骤 2 定时重启：点击滑块至 。

步骤 3 时间：设置定时重启的时间点，如“3:00”。

步骤 4 日期：选择定时重启的日期，如“星期一 ~ 星期五”。

步骤 5 点击 **保存**。

* 定时重启

* 时间

* 日期 星期一 星期二 星期三
 星期四 星期五 星期六
 星期日 每天

----完成

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。

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 分钟 (范围: 1~60, 默认: 5)

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

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。

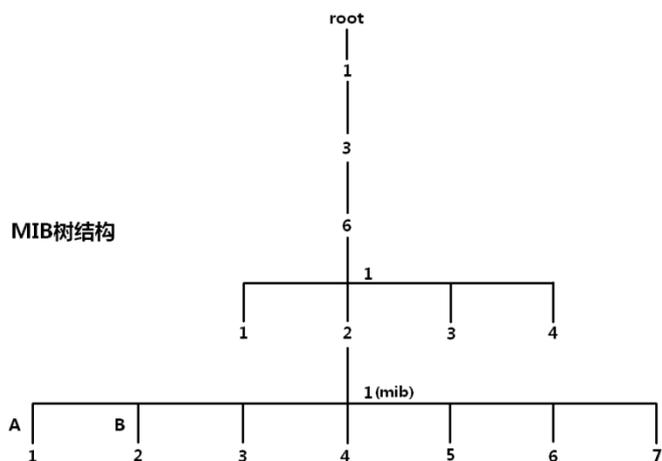
SNMP 协议版本

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

步骤 1 进入「高级设置」>「网络服务」页面。

步骤 2 SNMP 代理：点击滑块至 。

步骤 3 设置 SNMP 相关参数。

步骤 4 点击 **保存**。



The image shows a configuration window for SNMP. At the top, there is a toggle switch for 'SNMP代理' (SNMP Agent) which is turned on. Below this are four input fields: '设备名称' (Device Name) with the value 'O3V2.0', '读Community' (Read Community) with the value 'public', '读/写Community' (Read/Write Community) with the value 'private', and '位置' (Location) with the value 'ShenZhen'.

----完成

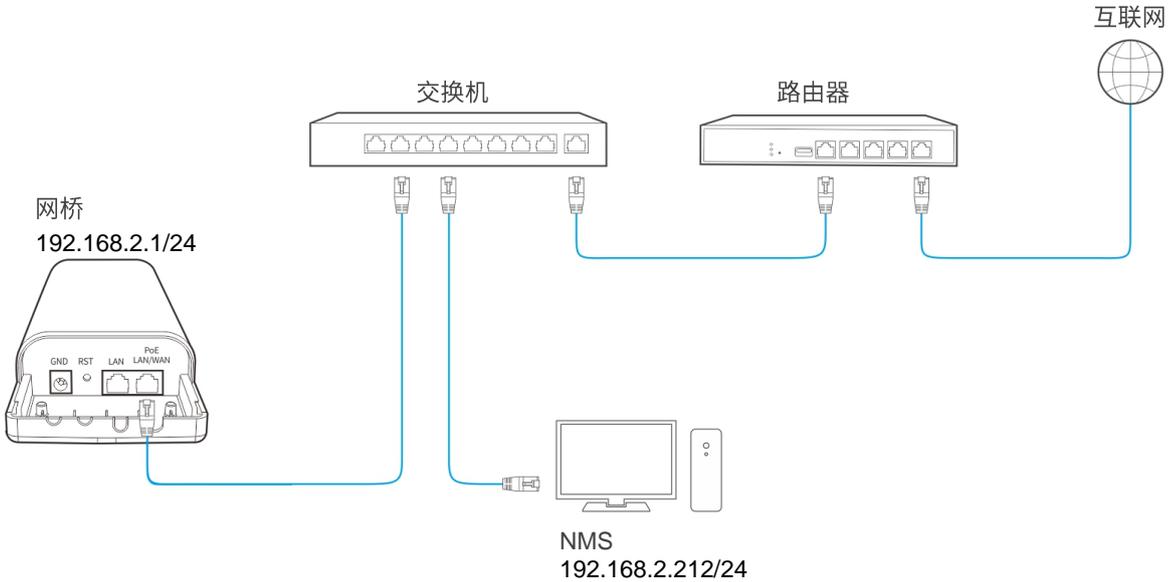
参数说明

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。  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。
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”。

步骤 1 登录网桥的管理页面，转到「高级设置」>「网络服务」。

步骤 2 SNMP 代理：点击滑块至 。

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

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

步骤 5 点击 **保存**。

* SNMP代理

设备名称

* 读Community

* 读/写Community

位置

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。

8.6.6 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显数量（触发重启丢包个数），则重新启动网桥。

配置 Ping 看门狗

步骤 1 进入「高级设置」>「网络服务」页面。

步骤 2 Ping 看门狗：点击滑块至 。

步骤 3 设置相关参数。

步骤 4 点击 **保存**。

Ping看门狗

IP地址

Ping间隔 s (范围: 20~86400)

启动延迟 s (范围: 180~86400)

触发重启丢包个数

----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, 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。 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

仅适用于无线 WAN 模式、路由模式。

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。

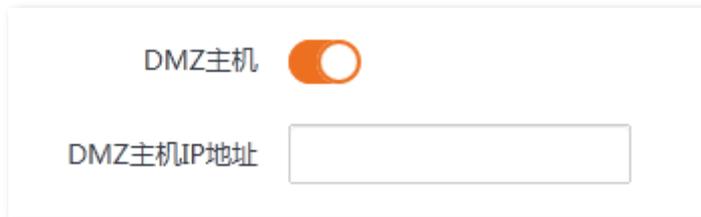
配置 DMZ 主机

步骤 1 进入「高级设置」>「网络服务」页面。

步骤 2 DMZ 主机：点击滑块至 。

步骤 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。

步骤 4 点击 **保存**。



The image shows a configuration panel for DMZ host. It contains a toggle switch labeled "DMZ主机" which is turned on, and a text input field labeled "DMZ主机IP地址" which is currently empty.

----完成

DMZ 主机配置举例

组网需求

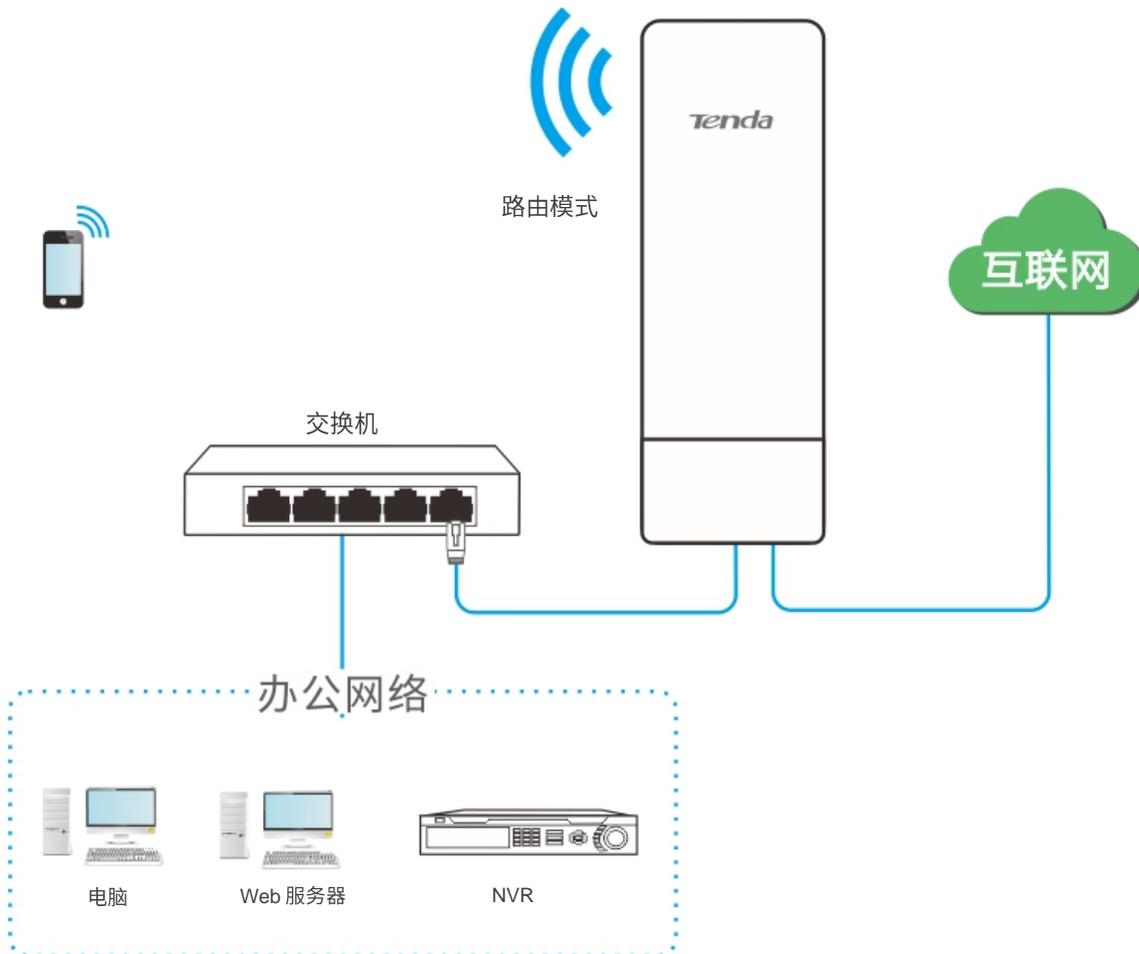
某公司使用网桥组建网络，网络管理员已将网桥设置为路由模式并接入互联网。现需要将公司内部的 Web 服务器开放给广域网用户，使员工不在公司时也能访问企业内部网络。

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 地址为 202.105.106.55。
- 内网 Web 服务器的 IP 地址为 192.168.2.100。
- 内网 Web 服务器的服务端口为 80。

网络拓扑



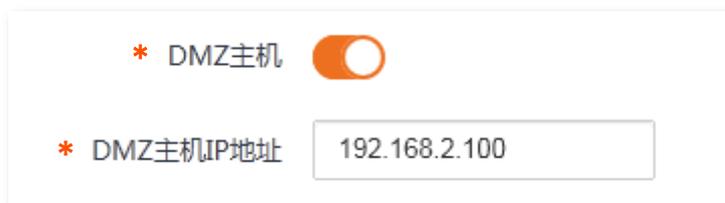
配置步骤

步骤 1 进入「高级设置」>「网络服务」页面。

步骤 2 DMZ 主机：点击滑块至 。

步骤 3 DMZ 主机 IP 地址：填入局域网中 Web 服务器的 IP 地址，本例为“192.168.2.100”。

步骤 4 点击 **保存**。



---完成

验证配置

互联网用户使用“内网服务应用层协议名称://网桥的 WAN 口 IP 地址:端口号”可以成功访问该公司内部 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://网桥的 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。



8.6.9 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。

点击「高级设置」>「网络服务」进入设置页面。UPnP 功能默认启用。



8.6.10 硬件看门狗

硬件看门狗利用了一个定时器电路。在网桥主程序正常运行时，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。

点击「高级设置」>「网络服务」进入设置页面。硬件看门狗功能默认启用。



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、定时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」。

日期与时间

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

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。

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：

步骤 1 进入「系统工具」>「时间与日期」页面。

步骤 2 时间设置：选择“网络校时”。

步骤 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”。

步骤 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”。

步骤 5 点击 **保存**。

The screenshot shows the 'Date and Time' configuration interface. At the top, there is a title '日期与时间'. Below it, there are three radio buttons for '时间设置': '网络校时' (selected), '手动设置', and '手动设置'. Underneath, there are three fields: '校时周期' (set to '30分钟'), '时区' (set to '(GMT+08:00) 北京, 重庆, 乌鲁木齐, 香港特别行政区, 台北'), and a '保存' button.

----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：

步骤 1 进入「系统工具」>「时间与日期」页面。

步骤 2 时间设置：选择“手动设置”。

步骤 3 日期与时间：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）。

步骤 4 点击 **保存**。

The screenshot shows the 'Date and Time' configuration interface with '手动设置' selected. The '日期与时间' field is set to '2018 年 04 月 18 日 16 小时 11 分 01 秒'. There is a '复制本地时间' button below the time field.

----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：

步骤 1 进入「系统工具」>「设备维护」页面。

步骤 2 点击 **重启**。



步骤 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。



- 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。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：

步骤 1 进入「系统工具」>「设备维护」页面。

步骤 2 点击 **恢复出厂设置**。



步骤 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。



为了避免损坏网桥，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：

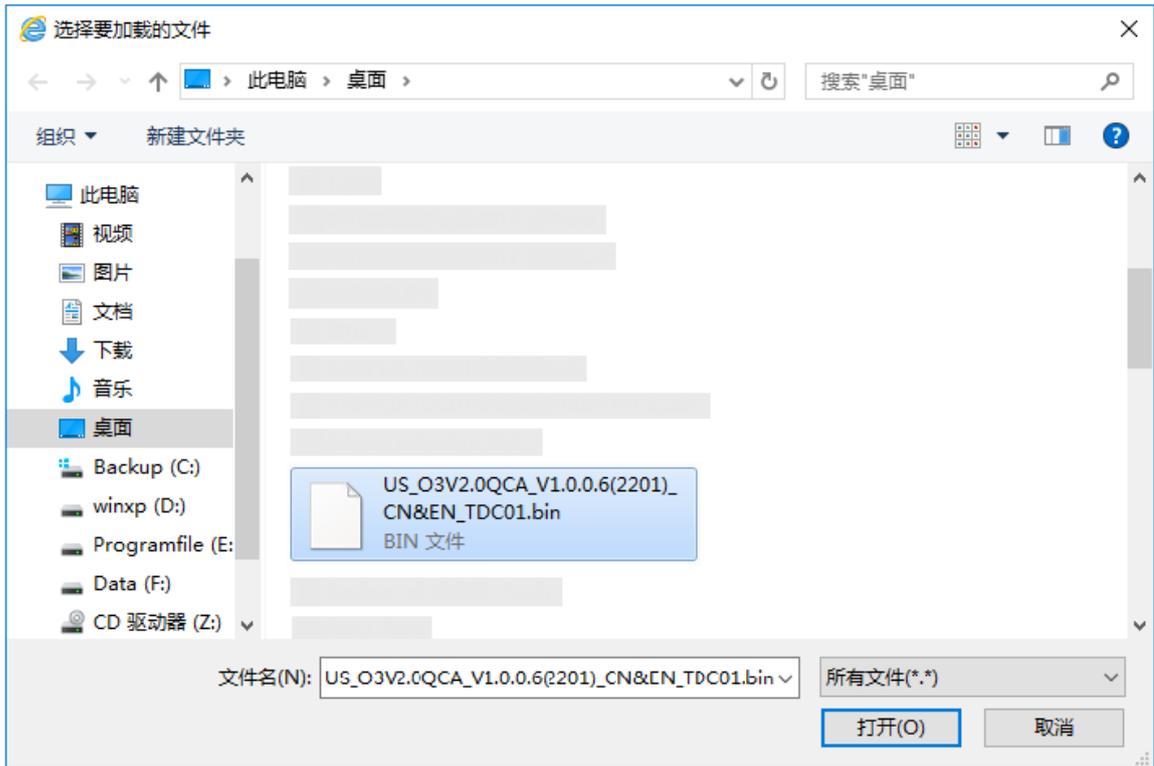
步骤 1 登陆 Tenda 官方网站 www.tenda.com.cn，下载更高版本的升级文件到本地电脑并解压。

步骤 2 登录到网桥的管理页面，转到「系统工具」>「设备维护」页面。

步骤 3 点击 **升级**。



步骤 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

页面会出现进度条，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。



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。



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

步骤 1 进入「系统工具」>「设备维护」页面。

步骤 2 点击 **备份/恢复**。



步骤 3 点击 **备份**。



步骤 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

步骤 1 进入「系统工具」>「设备维护」页面。

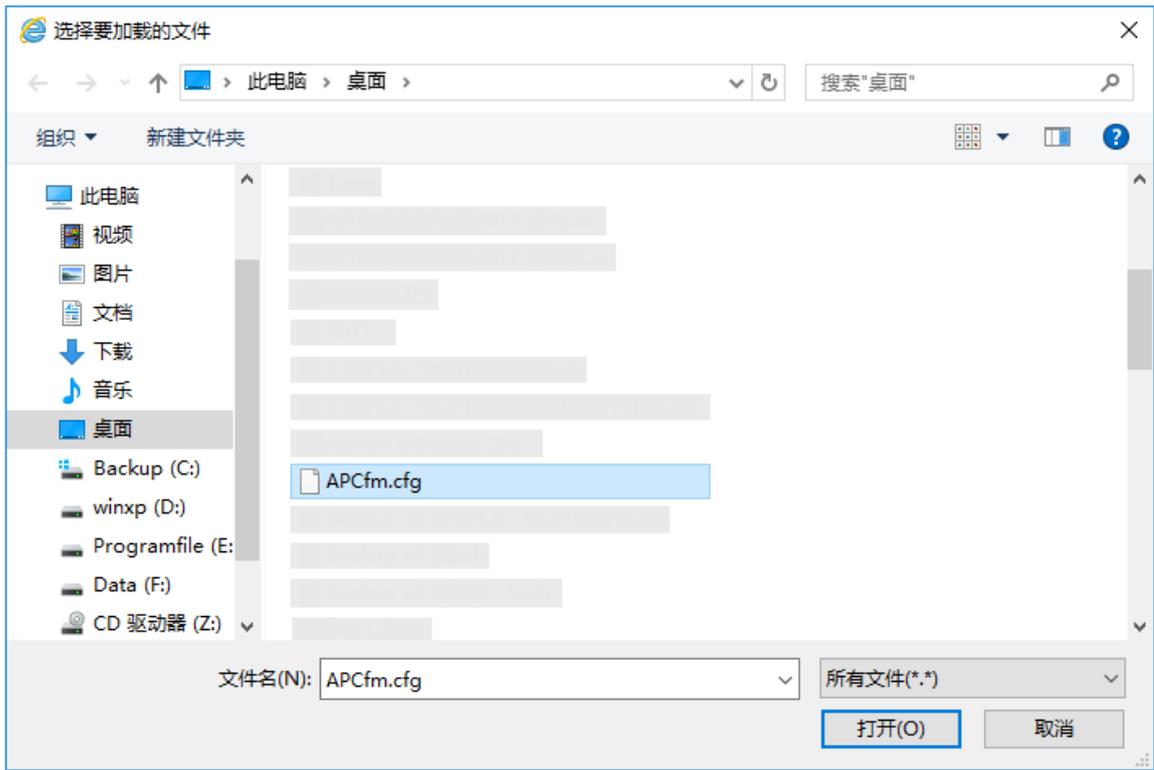
步骤 2 点击 **备份/恢复**。



步骤 3 点击 。



步骤 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。

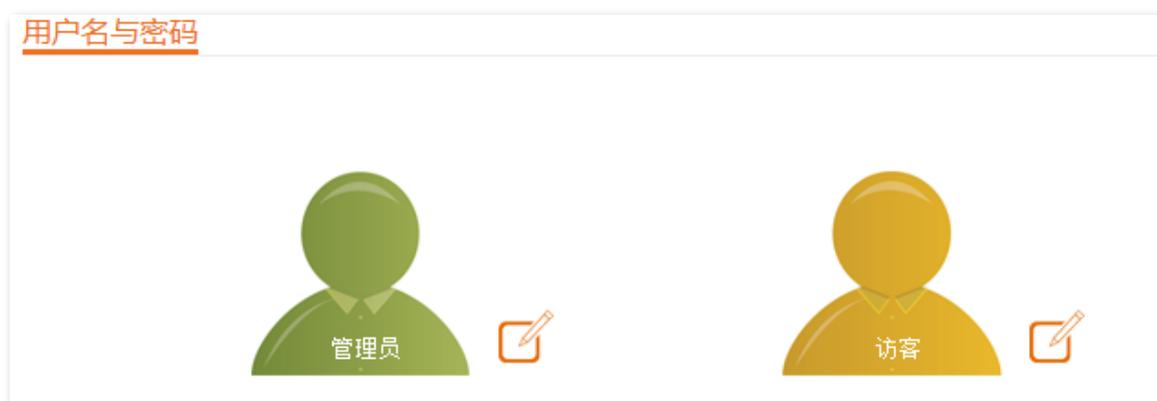


9.3 用户名与密码

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。

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。

访客账户

启用

原用户名

原密码

新用户名

新密码

确认新密码

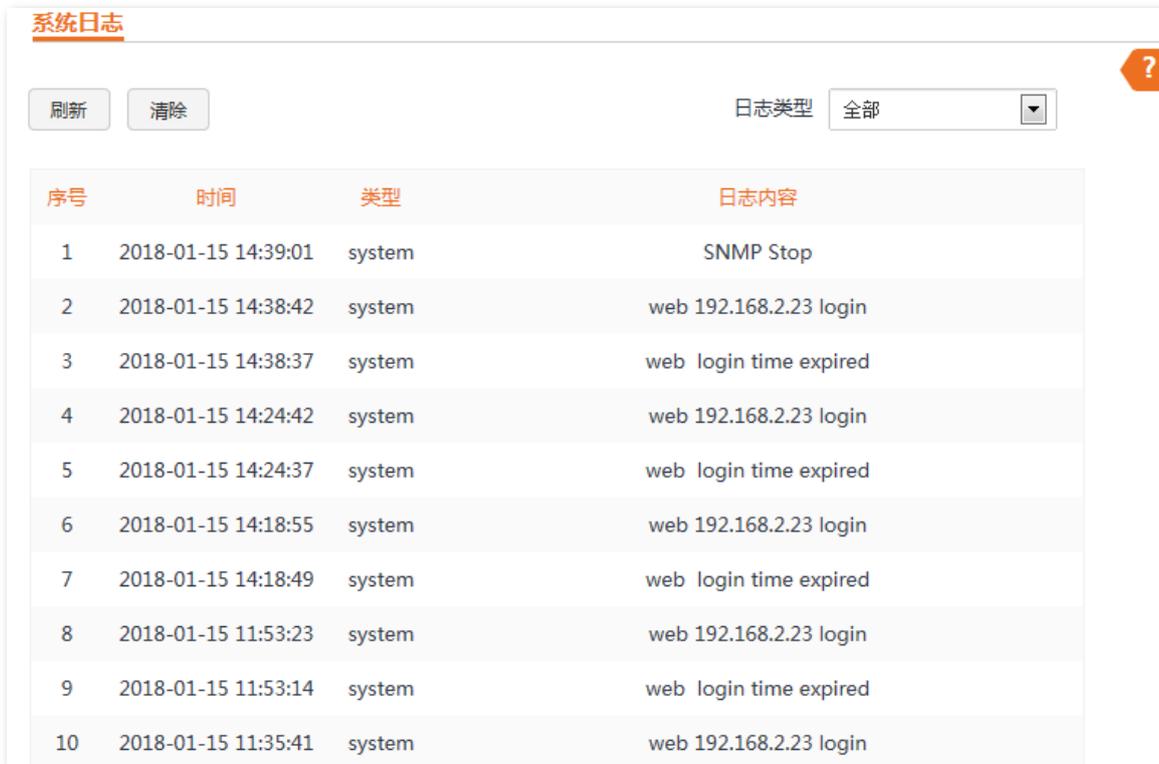
参数说明

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, there are buttons for 'Refresh' (刷新) and 'Clear' (清除), and a dropdown menu for 'Log Type' (日志类型) set to 'All' (全部). The main content is a table with the following data:

序号	时间	类型	日志内容
1	2018-01-15 14:39:01	system	SNMP Stop
2	2018-01-15 14:38:42	system	web 192.168.2.23 login
3	2018-01-15 14:38:37	system	web login time expired
4	2018-01-15 14:24:42	system	web 192.168.2.23 login
5	2018-01-15 14:24:37	system	web login time expired
6	2018-01-15 14:18:55	system	web 192.168.2.23 login
7	2018-01-15 14:18:49	system	web login time expired
8	2018-01-15 11:53:23	system	web 192.168.2.23 login
9	2018-01-15 11:53:14	system	web login time expired
10	2018-01-15 11:35:41	system	web 192.168.2.23 login

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

A 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/WAN 口与 PoE 注入器的 PoE 口连接正常。
- 确认用来连接网桥 PoE LAN/WAN 口和 PoE 注入器的 PoE 口的网线是八芯网线。

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 RST 按钮 8 秒后松开。

B 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 默认禁用
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
	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	O3V2.0
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
	租约时间	1 天
VLAN 设置	VLAN 设置	禁用
	PVID	1
	管理 VLAN	1
	WLAN	1000
	LAN	1

参数		默认设置
无线设置—基本设置	开启无线	开启
	国家或地区	中国
	SSID	Tenda_XXXXXX。XXXXXX 为网桥 LAN 口 MAC 后六位
	SSID 广播	启用
	网络模式	11b/g/n
	信道	自动
	发射功率	29dBm
	信道带宽	自动
	扩展信道	自动
	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	48
	无线设置—高级设置	WMM
APSD		禁用
接入信号强度限制		禁用
无线前导码		长前导码
穿墙能力		强覆盖
信号接收能力		自动
传输距离		3km
Beacon 间隔		100ms
Fragment 阈值		2346
RTS 门限		2347
DTIM 间隔		1
LED1 信号灯阈值		-90dBm
LED2 信号灯阈值		-80dBm
LED3 信号灯阈值	-70dBm	
无线设置—访问控制	禁用	
PoE/LAN 口速率	自动协商	

参数		默认设置
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
	硬件看门狗	启用
系统工具	时间与日期	网络校时 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