深圳市潮流网络技术有限公司

GWN7OXX 系列路由器

用户手册

版权

注意

未经潮流批准擅自修改本产品，或以用户手册以外的方式使用本产品，将会导致保修无效。

警告

请不要使用与设备不匹配的电源适配器，设备可能因此损坏，导致保修失效。

目录

表目录

图目录

更新日志

本节记录了与先前版本的 GWN70XX 用户手册相比的重大变更。 此处仅列出主要的新功能或主要文档更新，未记录用于更正或编辑的小更新。

固件版本 1.0.5.3

产品名：GWN7052 / GWN7052 F/ GWN7062 / GWN7062

- .初始版本

欢迎

GWN7052/GWN7052F 是一款 Wi-Fi5 双频路由器,适用于小型办公室、家庭办公室和远程办公，它支持双频 2×2 MU-MIMO，并支持无线 MESH 网络组网，同时具备有线 LAN 口。GWN7052/GWN7052F 采用双核 880MHz 处理器，支持 100 台无线客户端接入，并提供高达 1.266 Gbps 的 Wi-Fi 速度，可提供智能办公、家庭自动化、流畅的 4K 超高清流媒体、网络会议、视频会议、在线游戏等等有线和无线网络保障。它支持 VPN，允许远程员工在家中与分支机构链接。GWN7052/GWN7052F 还提供企业级安全保障，可确保安全的 Wi-Fi 和 VPN 访问，支持唯一的安全证书和随机默认密码。为确保易于安装和管理，GWN7052/GWN7052F 采用无控制器分布式网络管理设计，内嵌 AC 控制器（嵌入 Web 用户界面中）。云 AC 与本地 AC 管理方式即将推出。通过高速无线网络、MESH 和有线 LAN 加持，同时具有高级功能的 VPN、波束形成技术以及智能 QoS，GWN7052/GWN7052F 是日益增长的家庭和商业网络的理想路由器。

GWN7062 是一款采用最新 Wi-Fi 6（802.11ax）技术的双频路由器,非常适合小型办公室。GWN7062 支持双频段 2×2 MU-MIMO，采用 DL/UL OFDMA 技术并支持无线 Mesh 网络组网，同时具备有线 LAN 口。它具有强大的 64 位 1.2GHz 四核高性能处理器，最高达 1.77 Gbps 的 Wi-Fi 速度，最多 256 个无线客户端，GWN7062 可提供智能办公、家庭自动化、流畅的 4K 超高清流媒体、网络会议、视频会议、在线游戏等等有线和无线网络保障。GWN 支持 VPN，允许远程员工在家中与分支机构链接。GWN7062 还提供企业级安全保障，可确保安全的 Wi-Fi 和 VPN 访问，支持唯一的安全证书和随机默认密码。为确保易于安装和管理，GWN7062 采用无控制器分布式网络管理设计，内嵌 AC 控制器（嵌入 Web 用户界面中）。云 AC 与本地 AC 管理方式即将推出。通过 Wi-Fi6 高速无线网络、MESH 和有线 LAN 加持，同时具有高级功能的 VPN、波束形成技术以及智能 QoS，GWN7062 是日益增长的家庭和商业网络的理想路由器。

产品概览

技术参数

表 1 GWN7052/7052F 技术参数

型号	GWN7052	GWN7052F
内存和 NAT 能力	128MB RAM 30K NAT sessions	256MB RAM 60K NAT sessions
NAT 路由和 IPSecVPN 性能	1Gbps NAT 路由 300Mbps IPSec VPN 性能	
Wi-Fi 标准	IEEE 802.11a/b/g/n/ac	
天线	4 个独立天线，每个频段 2 个 内置 2.4GHz 全向天线，增益 5dBi 内置 5GHz 全向天线，增益 5dBi	
Wi-Fi 数据速率	**5G:** IEEE 802.11ac: 6.5 Mbps - 867Mbps IEEE 802.11n: 6.5 Mbps - 300 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **2.4G:** IEEE 802.11n: 6.5 Mbps - 300Mbps IEEE 802.11b: 1, 2, 5.5, 11Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **实际吞吐量可能因许多因素而异，包括环境条件、设备之间的距离、操作环境中的无线电干扰以及网络中设备的混合。*	
频段	2.4GHz: 2400 - 2483.5 MHz 5GHz: 5150 - 5850 MHz *并非所有区域都可以使用所有频段	
信道带宽	2.4G: 20 和 40 MHz 5G: 20, 40 和 80 MHz	

Wi-Fi 和系统安全	WEP、WPA/WPA2-PSK、WPA/WPA2 企业版 (TKIP/AES)； WPA3、防黑客安全启动和通过数字签名、唯一的安全证书和每个设备的随机默认密码进行关键数据/控制锁定	
MIMO	2×2:2 2.4GHz 2×2:2 5GHz	
最大传输速率	5G: 23dBm 2.4G: 24dBm **最大功率因国家、频段和 MCS 速率而异*	
接收灵敏度	**2.4G** 802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7; **5G** 802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40: -63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9;	
SSIDs	总共支持 16 SSID，每个频段支持 8 个 (2.4GHz 和 5GHz)	
并发客户端	100	
网络接口	1 个千兆 WAN 口， 4 个千兆 LAN 口	1 个千兆 SFP WAN 口， 1 个千兆（WAN/LAN）可配置千兆口， 3 个千兆 LAN 口
辅助接口	1x Reset 复位孔,一个 USB 2.0	
安装	桌面和挂墙	
LEDs	1 个三色 LED 灯，7 个单色状态灯	
防火墙	DDNS，端口转发，DMZ，UPnP，Anti-DoS，数据规则，NAT，ALG	
网络协议	IPv4，802.1Q，802.1p，802.1x，802.11e/WMM	
QoS	802.11e/WMM，VLAN，TOS	
网络管理	内嵌 AC：GWN7052 最大支持 30 个本地 GWN AP，GWN7052F 最大支持 50 个本地 GWN AP 云 AC：免费提供，云端注册即可使用，终端数不受限 本地 AC：免费提供安装软件，最大可支持 3000 用户	

节能和绿色电源	标配电源适配器：输入 100-240VAC 50-60Hz 输出：12VDC 1A（12W）
环境	操作：0° C - 50° C 保存：-10° C - 60° C 湿度：10% - 90%非冷凝
物理尺寸	单机尺寸：205mm(L)x130(W)mmx35.5mm(H)； 单机+安装配件尺寸（天线 90° 时）：235.5mm(L)x145(W)mmx192mm(H)； 单机重量：375g 整个包装尺寸：250 mm(L)x251.5 mm(W)x56mm mm(H)；整套包装重量：740g
包装清单	GWN7052/F 路由器,电源适配器，网线，快速安装指南
认证	FCC, CE, RCM, IC, UKCA

表 2 GWN7062 技术参数

内存和 NAT 能力	512MB RAM, 120K NAT sessions
NAT 路由和 IPSecVPN 性能	2Gbps NAT 路由 850Mbps IPSec VPN 性能
Wi-Fi 标准	IEEE 802.11a/b/g/n/ac/ax
天线	4 个独立天线，每个频段 2 个 内置 2.4GHz 全向天线，增益 5dBi 内置 5GHz 全向天线，增益 5dBi

Wi-Fi 数据速率	**5G:** IEEE 802.11ax: 7.3 Mbps to 1201 Mbps IEEE 802.11ac: 6.5 Mbps - 867Mbps IEEE 802.11n: 6.5 Mbps - 300 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **2.4G:** IEEE 802.11ax: 7.3 Mbps to 573.5 Mbps IEEE 802.11n: 6.5 Mbps - 300Mbps IEEE 802.11b: 1, 2, 5.5, 11Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **实际吞吐量可能因许多因素而异，包括环境条件、设备之间的距离、操作环境中的无线电干扰以及网络中设备的混合。*
频段	2.4GHz: 2400 - 2483.5 MHz 5GHz: 5150 - 5850 MHz *并非所有区域都可以使用所有频段
信道带宽	2.4G: 20 和 40 MHz 5G: 20, 40 和 80 MHz
Wi-Fi 和系统安全	WEP、WPA/WPA2-PSK、WPA/WPA2 企业版 (TKIP/AES)； WPA3、防黑客安全启动和通过数字签名、唯一的安全证书和每个设备的随机默认密码进行关键数据/控制锁定
MIMO	2×2:2 2.4GHz 2×2:2 5GHz
覆盖范围	高达 175 米 *覆盖范围可能因环境而异
最大传输速率	5G: 26dBm 2.4G: 27dBm

接收灵敏度	2.4G 802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7; 802.11ax 20MHz: -64dBm @ MCS11; 802.11ax 40MHz: -63dBm @MCS11 5G 802.11a: -93dBm@6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm@MCS7; 802.11n 40MHz: -70dBm@MCS7 802.11ac 20MHz: -70dBm@MCS8; 802.11ac 40MHz: -66dBm@MCS9; 802.11ac 80MHz: -62dBm@MCS9; 802.11ax 20MHz: -64dBm@MCS11; 802.11ax 40MHz: -61dBm@MCS11; 802.11ax 80MHz: -58dBm @MCS11
SSIDs	总共支持 32 SSID, 每个频段支持 16 个 (2.4GHz 和 5GHz)
并发客户端	256
网络接口	1 个千兆 SFP WAN 口, 1 个千兆（WAN/LAN）可配置千兆口, 3 个千兆 LAN 口
辅助接口	1 个 Reset 复位孔,一个 USB 3.0, 1 个 SYNC 按钮
安装	桌面
LEDs	1 个三色 LED 灯，7 个单色状态灯
防火墙	DDNS, 端口转发, DMZ, UPnP, Anti-DoS, 数据规则, NAT, ALG
网络协议	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM
QoS	802.11e/WMM, VLAN, TOS
网络管理	内嵌 AC：最大支持 50 个本地 GWN AP 云 AC：免费提供，云端注册即可使用，终端数不受限 本地 AC：免费提供安装软件，最大可支持 3000 用户
节能和绿色电源	标配电源适配器：输入 100-240VAC 50-60Hz 输出：12VDC 1.5A（18W）
环境	操作: 0° C - 50° C 保存: -30° C - 60° C 湿度: 10% - 90%非冷凝

物理尺寸	单机尺寸：95mm(L)x95(W)mmx193mm(H)；单位重量：690g 整个包装尺寸：286 mm(L)x126.5 mm(W)x105mm(H)；整套包装重量：960g
包装清单	GWN7602 802.11ax 无线 AP，快速入门指南
认证	FCC, CE, RCM, IC, UKCA

安装

在部署和配置 GWN70XX 之前，设备需要正确上电并连接到网络。 本节详细介绍了 GWN70XX 的安装、连接方法和保修政策。

设备包装

GWN7052/GWN7052F

图 1 GWN7052/GWN7052F 包装清单

GWN7062

图 2 GWN7062 包装清单

GWN70xx 端口

GWN7052

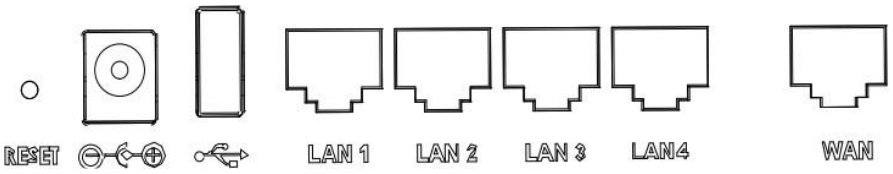


图 3 GWN7052 端口

GWN7052F

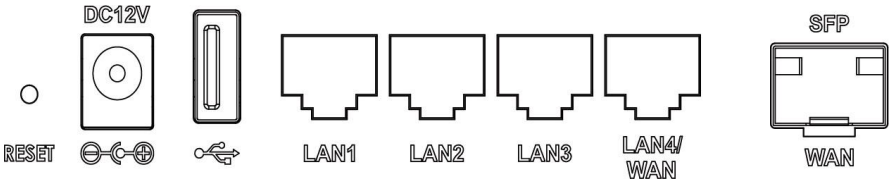


图 4 GWN7052F 端口

GWN7062

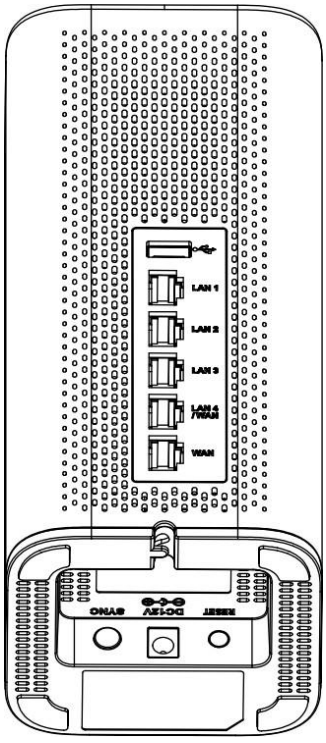


图 5 GWN7062 端口

为 GWN70XX 供电并连接

GWN7052/GWN7052F

1. 连接 GWN7052/GWN7052F 的电源

GWN7052/GWN7052F 可以在正确的 PSU（DC 12V，1A）下供电。

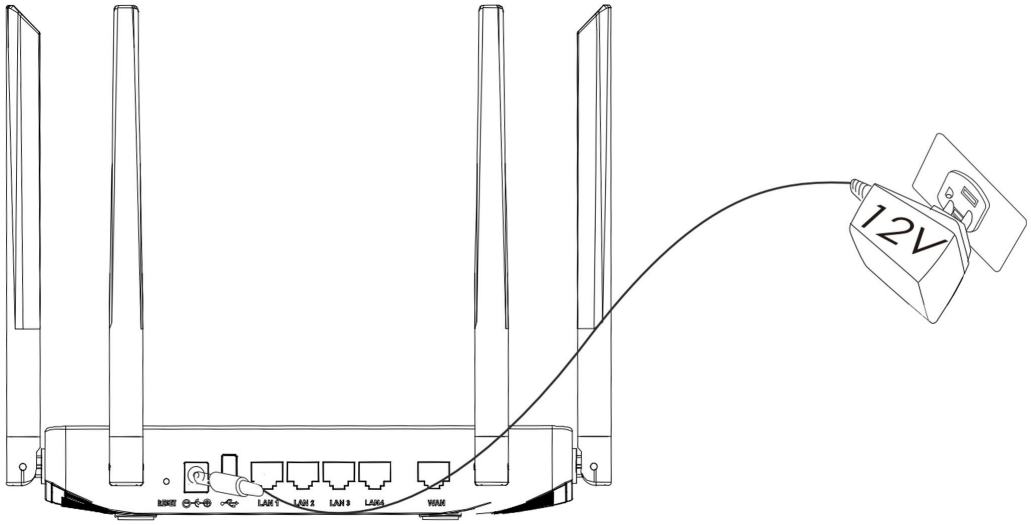


图 6 GWN7052 背部

2. 连接网络

将 WAN 端口连接到光纤宽带（通过 SFP 模块）、ADSL 宽带或社区宽带接口。

图 7 GWN7052 连接

3. 连接到网

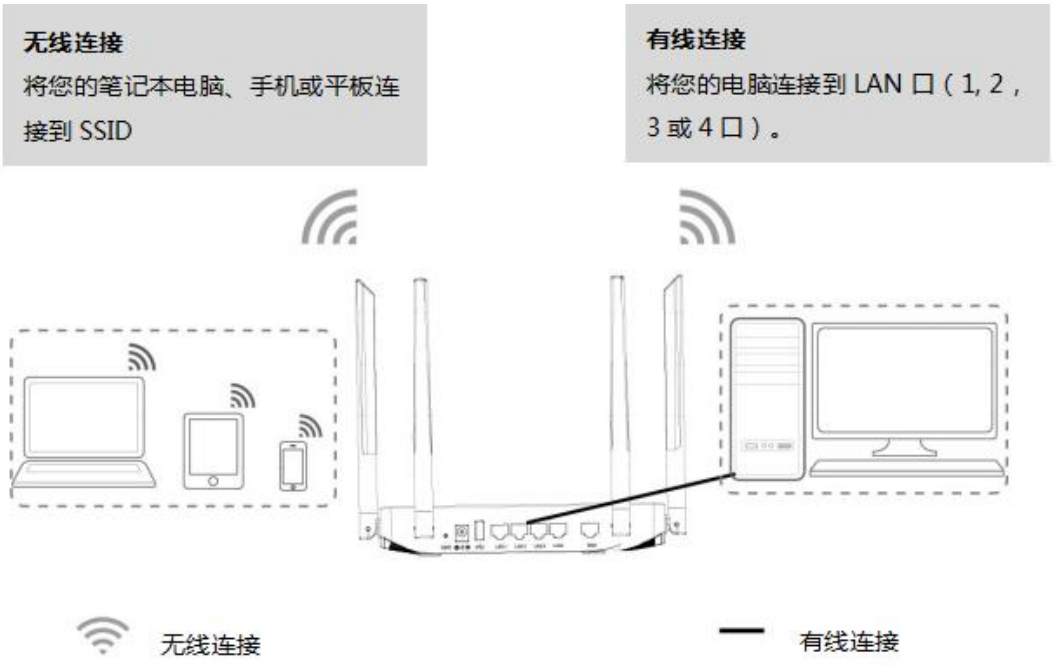


图 8 GWN7052 默认网络

GWN7062

1. 连接 GWN7062 的电源

GWN7052/GWN7052F 可以在正确的 PSU（DC 12V，1.5A）下供电。

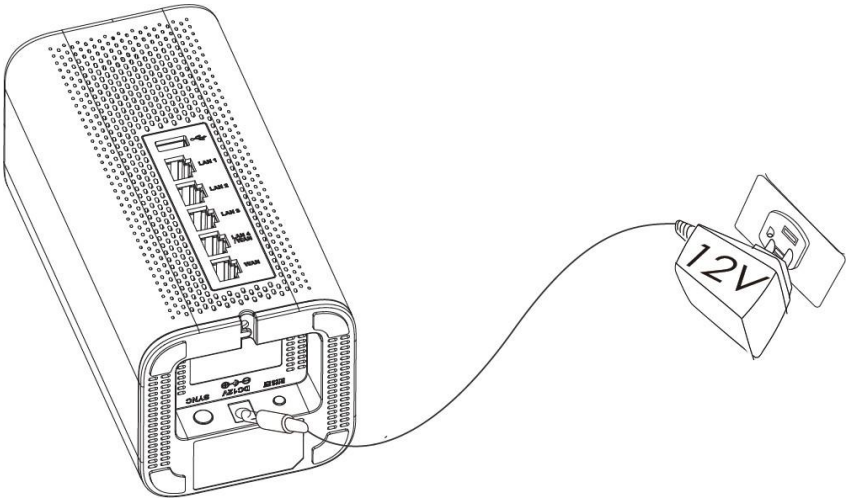


图 9 GWN7062 背部

2. 连接网络

将 WAN 端口连接到光纤宽带（通过 SFP 模块）、ADSL 宽带或社区宽带接口。

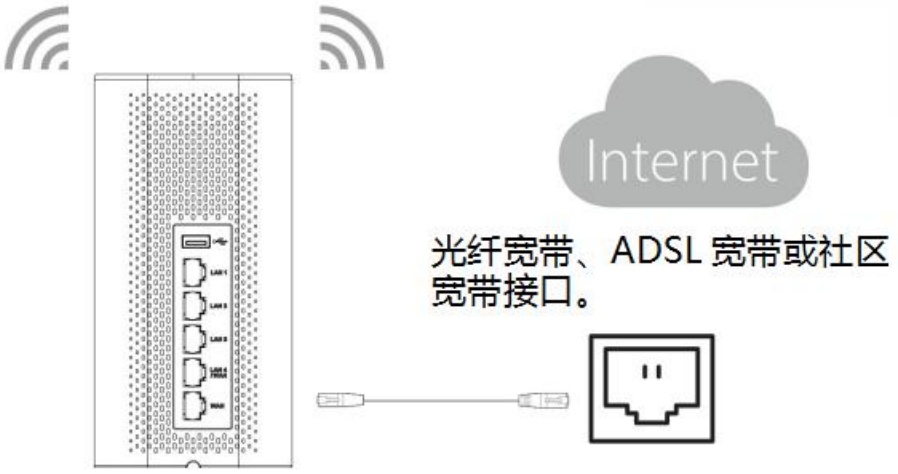


图 10 连接 GWN7062

3. 连接到默认网络

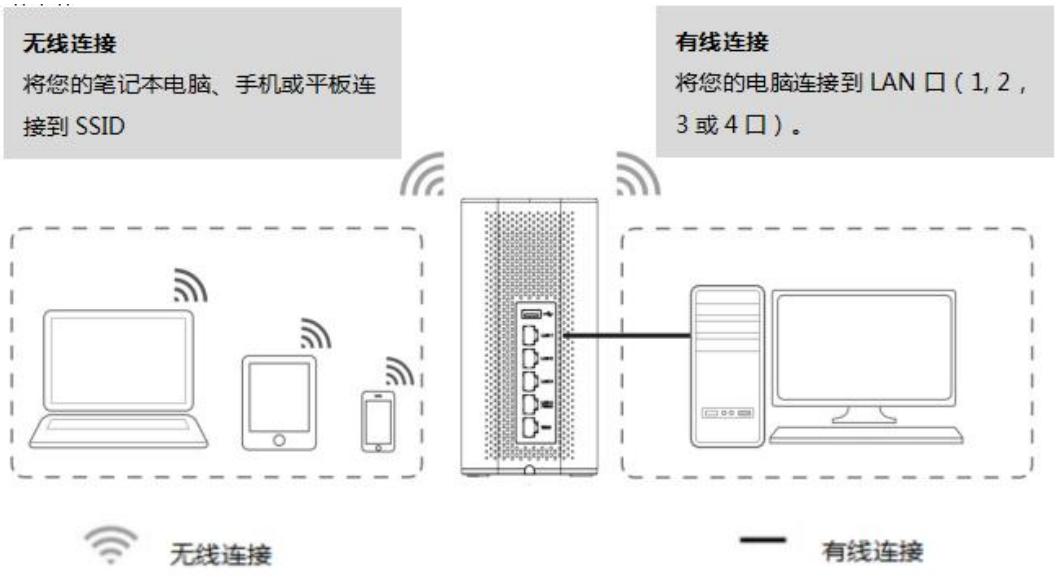


图 11 GWM7062 默认网络

SSID 的默认密码信息打印在设备底部的 MAC 标签上。

安全合规性

GWN70xx 双频 Wi-Fi 路由器符合 FCC/CE 和各种安全标准。GWN70xx 电源适配器符合 UL 标准。请使用随 GWN70xx 提供的通用电源适配器。制造商的保修不包括不支持的电源适配器对设备造成的损坏。

保修

如果 GWN7OXX 双频Wi-Fi路由器是从经销商处购买的，请联系购买设备的公司进行更换、维修或退款。如果设备是直接从潮流网络购买的，请在产品退回之前联系我们的技术支持团队获取 RMA（退货授权）编号。 潮流网络保留修改保修政策的权利，恕不另行通知。

开始使用

GWN70xx 双频 Wi-Fi 路由器提供了直观的 web GUI 配置界面，以便用户进行管理。用户可以通过 Web 页面访问 GWN70xx 的所有配置和选项。

本节对如何读取设备 LED 模式和使用 Web GUI 界面进行了说明。

LED模式

GWN70XX 的前部面板对不同的活动有不同的 LED 模式，以帮助用户读取 GWN70XX 的状态，更多详细信息请参阅下表。

表 3 LED 状态

LED	LED 状态	说明
电源/部署	红灯闪烁	重置中。
	红灯常亮	升级失败。
	粉灯	设备没有部署。
	绿灯	设备上电。
	蓝灯	正常使用。
Wi-Fi	蓝灯常亮	Wi-Fi 已启用。
	熄灭	Wi-Fi 未启用。
WAN	蓝灯闪烁	作为客户端连接到另一个网络，数据正在传输。
	熄灭	无网络，网口未连接。
LAN	蓝灯闪烁	对应的 LAN 口已连接，数据正在传输。
	熄灭	无网络，网口未连接。
USB	蓝灯闪烁	USB 设备已连接
	熄灭	未连接 USB 设备。

使用 Web GUI

用户可以通过其 WebGUI 访问 GWN70XX，以下部分介绍如何访问和使用 Web 界面。

连接 Web GUI

嵌入式 Web 服务器响应 HTTPS GET/POST 请求。 嵌入式 HTML 页面允许用户通过 Web 浏览器（例如 Microsoft IE、Mozilla Firefox、Google Chrome 等）配置设备。

图 12 登录GWN7062 的Web GUI

连接 Web GUI:

1. 将电脑连接到GWN70XX的其中给一个LAN口。
2. 确保设备已正确上电，并且Power和LAN口的LED灯为蓝色。
3. 在电脑上打开网页浏览器，使用以下格式输入IP地址：https://192.168.80.1（默认IP地址）。
4. 输入管理员的登录名和密码以访问 Web 配置菜单。 默认管理员的用户名始终为“admin”，密码是设备背面标签上的唯一默认 Wi-Fi 密码。

注意：

设备首次启动或出厂重置后，用户将被要求在访问GWN70xx web界面之前更改默认管理员和用户密码。密码字段区分大小写，最大长度为 32 个字符。出于安全目的，建议使用强密码，包含字母、数字和特殊字符。

WEB GUI 语言

目前GWN70XX系列网页界面支持英文和简体中文。

用户可以在登录前或登录后在Web GUI 下方选择显示的语言。

图 13 GWN70XX Web GUI 语言(登录页面)

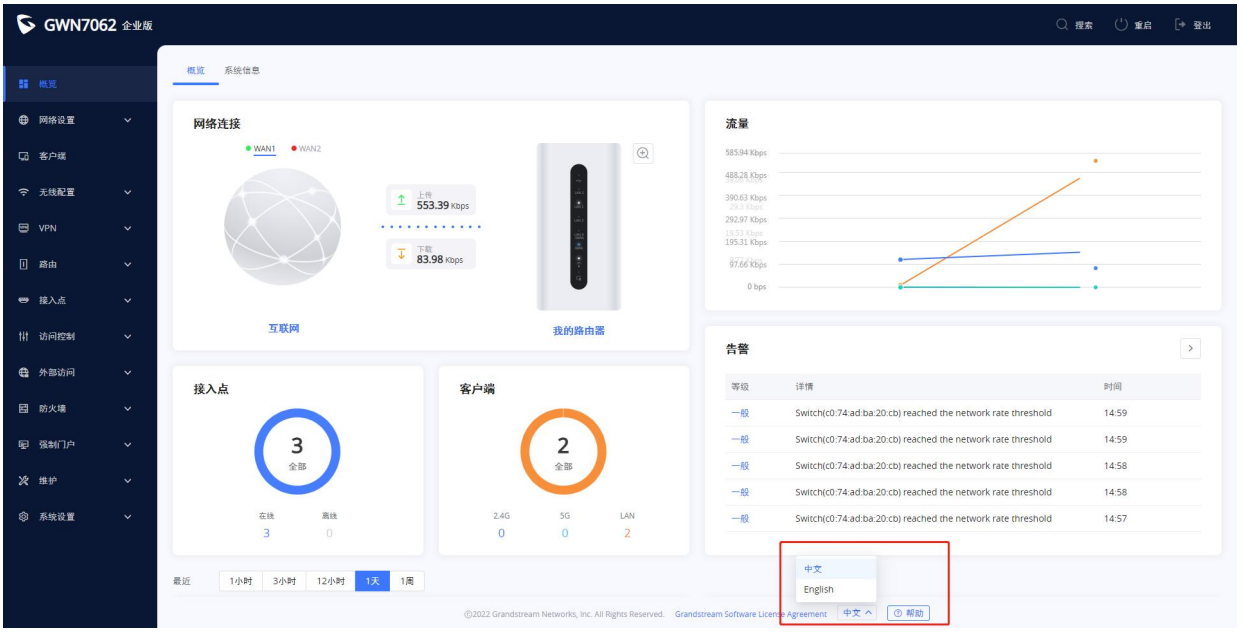


图 14 GWN70XX Web GUI 语言 (Web 界面)

Web GUI 配置

GWN70xx web GUI 包括 13 个主要部分，用于配置和管理路由器以及检查连接状态。

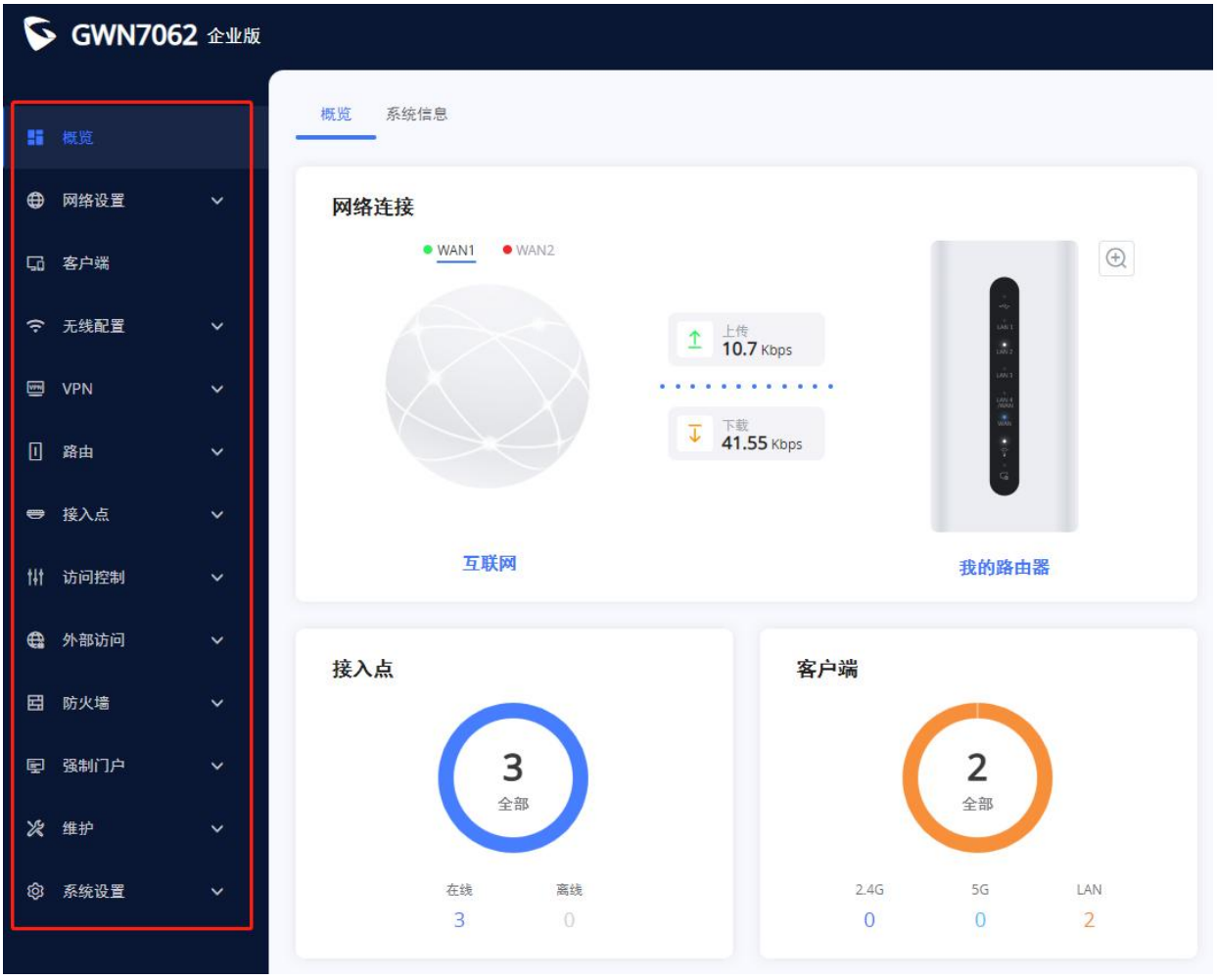


图 15 WEB GUI 配置

搜索

由于很难遍历每个部分，GWN70xx 路由器具有搜索功能，可帮助用户找到正确的配置、设置或参数等。在页面顶部，有一个搜索图标，用户可以单击该图标，然后输入搜索关键字，然后将获得该关键字的所有可能位置。

图 16 搜索功能

上网配置向导和反馈

如果用户遇到 GWN70xx 问题或有反馈。页面底部有一个帮助图标 

，用于设置路由器或发送反馈。

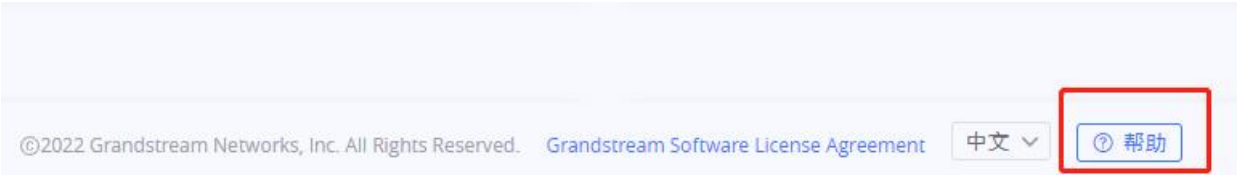


图 17 帮助

上网配置向导

如果用户在 GWN70xx 首次启动时错过了配置向导，您可以始终在页面底部访问它，它包含用户的必要设置，分为 3 个部分，分别是国家和时区、上网设置，和 SSID 设置。

点击  按钮浏览配置向导。

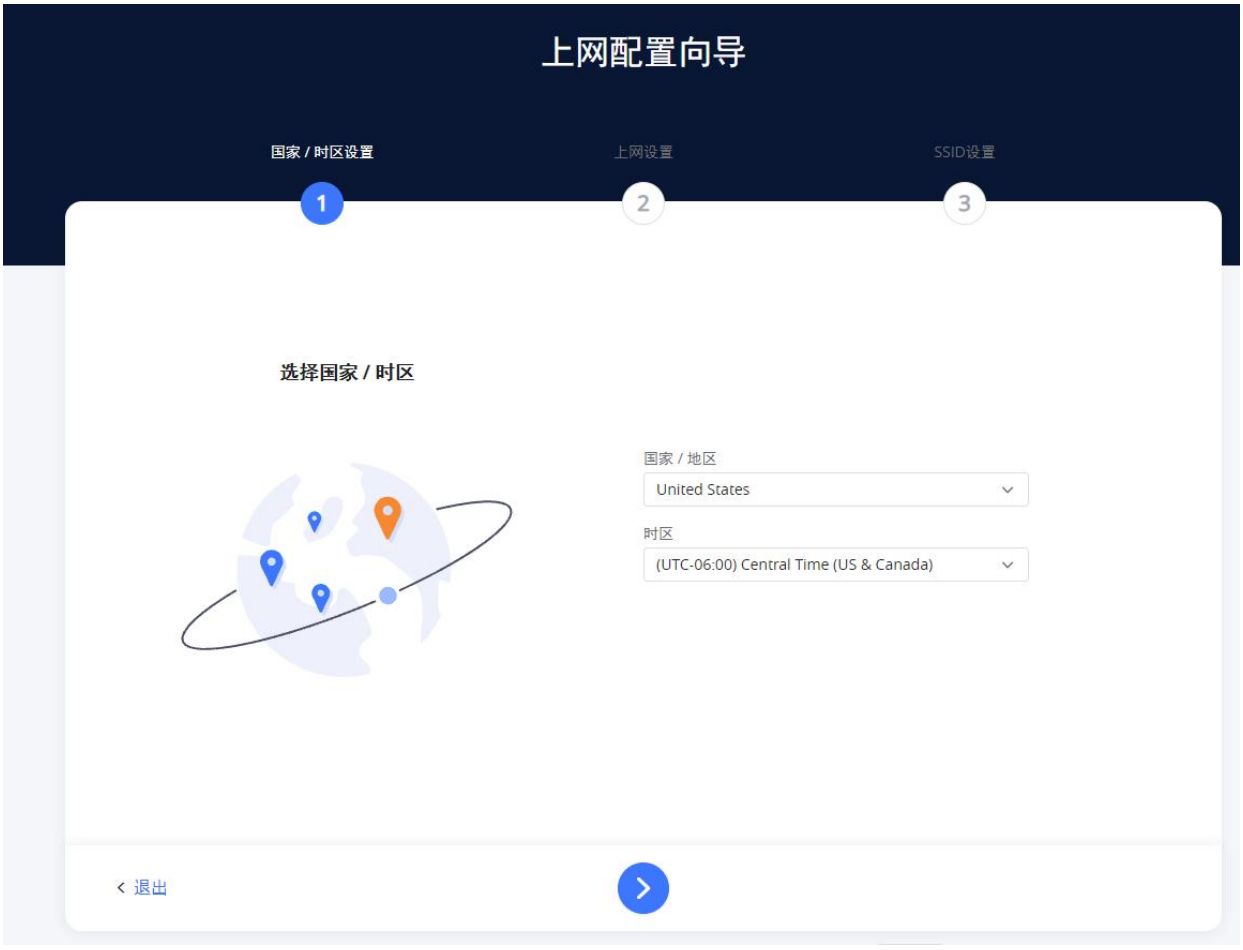


图 18 上网配置向导

反馈

如果用户有设备问题或改进产品的建议，他可以随时发送反馈，如果是设备问题，最好在反馈中包含 syslog，这有助于更快地解决问题。

图 19 反馈

概览

概述是成功登录 GWN70xx 的 Web 界面后显示的第一页。它提供了 GWN70xx 信息的总体视图，以仪表板的样式显示，便于监控设备以及显示系统信息（产品名称、系统版本、MAC 地址…）。它可以显示 GWN70xx 不同项目的状态，例如（上传和下载速度、连接的客户端数量、使用的频段、接入点、网络流量、告警、接入点排行、SSID 排行和客户端排行）。

图 20 概览界面

表 4 概览

网络连接	显示路由器的当前状态，它是否连接，以及显示当前上传和下载速度。
流量	实时显示网络流量。
接入点	显示了在线和离线的接入点总数。
客户端	显示连接到 2.4G 和 5G 以及连接到 LAN 的客户端的总数。
告警	显示 3 种警告类型：严重、重要和一般
Top Access Devices	显示接入点列表，用户可以根据每个接入点连接的客户端数量、上传和下载的数据使用情况对列表进行分类。 用户可以点击箭头进入接入点页面，了解接入点的基本和高级配置。
Top SSIDs	显示 SSID 列表，用户可以根据连接到每个 SSID 的客户端数量或结合上传和下载的数据使用情况对列表进行分类。 用户可以点击箭头进入 SSID 以获取更多选项。
Top Clients	显示客户端列表，用户可以通过上传或下载的数据来分类客户端列表。用户可以点击箭头进入客户页面以获取更多选项。

此外，用户可以单击放大镜图标 来检查路由器的 LED 状态。

图 21 LED 状态

系统信息

系统信息显示设备 GWN70xx 的 MAC 地址、PN 序列号、固件相关信息、运行时长、WAN 端口的一般信息，如 IP 地址和连接类型。


GWN7052 企业版
概览
网络设置
客户端
无线配置
VPN
路由
接入点
访问控制
外部访问
防火墙
强制门户
维护
系统设置
概览
系统信息
硬件版本
V1.1C
系统版本
1.0.5.10
MAC地址
SN序列号
PN序列号
运行时长
1天 23小时 20分钟
系统时间
2022-10-19 10:26
WAN
IPv4
连接类型
自动获取IP（DHCP）
端口速率/双工
1000M 全双工
IPv4 IP
172.16.0.136
子网掩码
255.255.254.0
默认网关
172.16.0.1
首选DNS服务器
备选DNS服务器
114.114.114.114

图 22 系统信息

路由器配置

本节包括网络 WAN 端口、LAN 端口的配置页面说明。

WAN口配置

通过连接在 LAN 端口的电脑或 GWN70xx 的 Wi-Fi SSID 连接到设备的 Web GUI，然后访问**网络设置→ WAN** 页面。

WAN 端口可以连接到 DSL 调制解调器或路由器。WAN 端口还可以设置静态 IPv4/IPv6 地址，配置 PPPoE。GWN7062 有一个端口（LAN 4/WAN），默认情况下配置为 LAN 端口。用户可以将此端口配置为 WAN 端口（WAN 2），用于 WAN 1 和 WAN 2 之间的负载平衡。

IPv4 设置

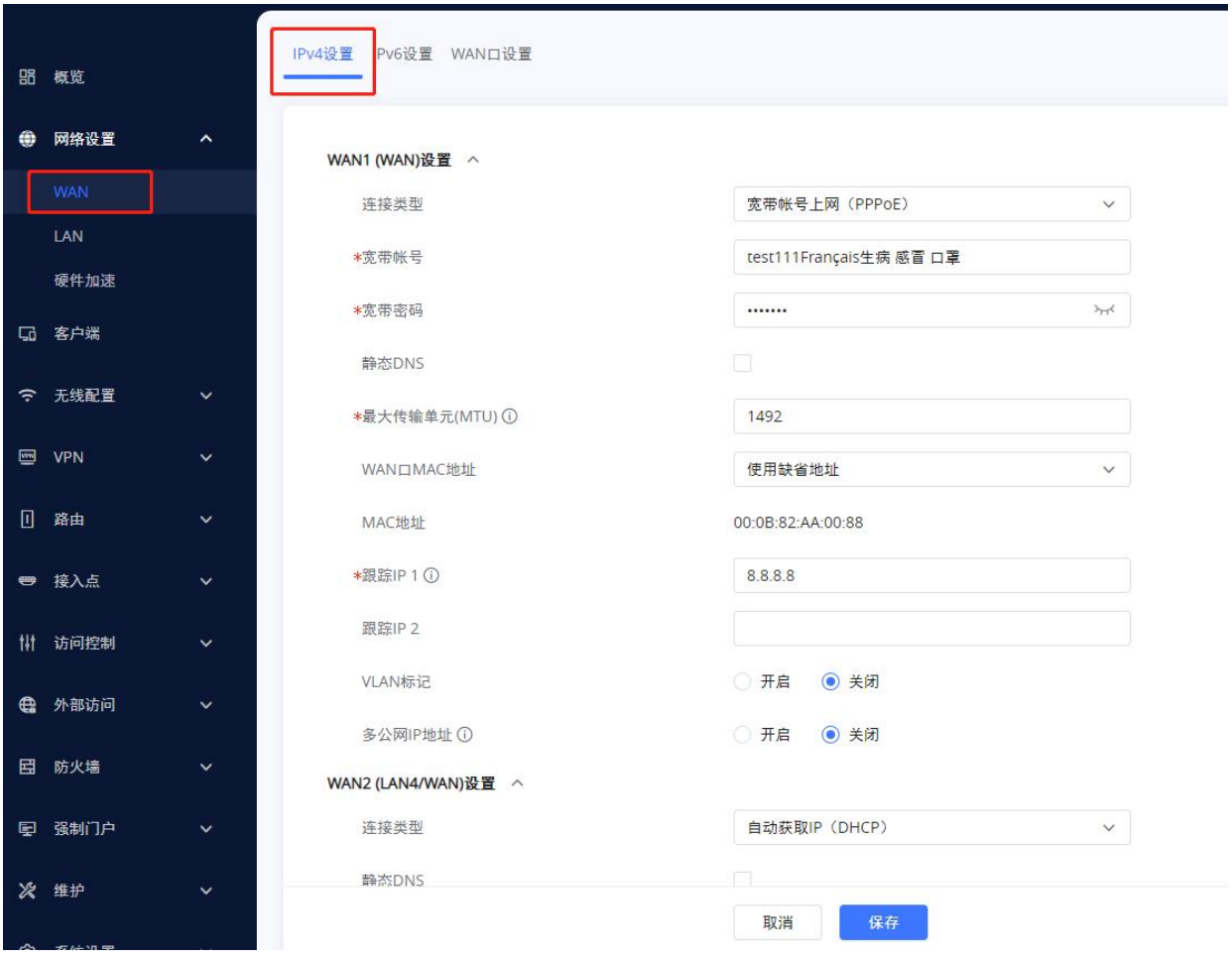


图 23 IPv4 设置

有关 GWN70xx 的 IPv4 WAN 端口上的基 本网络配置参数，请参阅下表。

表 5 IPv4 设置

连接类型	● 自动获取 IP（DHCP）：选中时，它将充当 DHCP 客户端，并自动从 DHCP 服务器获取 IPv4 地址。 ● 手动输入 IP（静态 IP）：选中时，用户应设置静态 IPv4 地址、IPv4 子网掩码、IPv4 网关，并添加其他 IPv4 地址用来访问 web 界面、SSH 或其他服务通信。 ● 宽带账号上网（PPPoE）：选中时，用户应设置 PPPoE 帐号和密码、PPPoE 保持活动间隔和密钥间超时（秒）。 ● L2TP：二层隧道协议（L2TP）是互联网服务提供商（ISP）用于启用虚拟专用网络（VPN）的点对点隧道协议（PPTP）的扩展。 ● PPTP：点对点隧道协议（PPTP）是一种网络协议，通过在基于 TCP/IP 的数据网络上创建虚拟专用网络（VPN），可以将数据从远程客户端安全传输到专用企业服务器。 默认设置为“自动获取 IP（DHCP）”。
静态 DNS	选中静态 DNS，然后输入首选 DNS 服务器和备用 DNS 服务器。
最大传输单元（MTU）	配置 WAN 端口上允许的最大传输单元。有效范围为 576-1450 字节，默认值为 1450。
WAN 口的 MAC 地址	选择使用默认 MAC 地址或使用当前管理 PC 的 MAC 地址，或使用自定义 MAC 地址。
MAC 地址	WAN 口使用的 MAC 地址。
跟踪 IP1	配置 WAN 端口的跟踪 IP 地址，以确定 WAN 端口网络是否正常。
跟踪 IP2	配置 WAN 端口的跟踪 IP 地址，以确定 WAN 端口网络是否正常。
VLAN 标记	选择是启用还是禁用 VLAN 标记。
多公网 IP 地址	请使用端口转发功能，以便您可以通过公共 IP 地址访问路由器。

IPv6 设置

GWN70XX 同时支持 IPv6。

图 24 IPv6 设置

关于 IPv6 的详细配置说明，请查阅下表。

表 6 IPv6 设置

IPv6	选择“开启”来启用 IPv6。
连接类型	● DHCPv6：选中时，它将充当 DHCP 客户端，并自动从 DHCP 服务器获取 IPv6 地址。 ● 静态 IPv6：选中后，用户应设置静态 IPv6 地址、前缀长度、默认网关和首选 DNS 服务器。 ● PPPoE（仅当启用 IPv4 PPPoE 时）：仅当 PPPoE IPv4 已启用时才能使用。 默认设置为“DHCPv6”。
静态 DNS	选中静态 DNS，然后输入首选 DNS 服务器和备用 DNS 服务器。
IPv6 中继到 VLAN	启用后，将 IPv6 地址中继到 LAN 端的客户端。 *注意：此功能仅在 VLAN 上启用“来自 WAN 的 IPv6 中继”时生效。*

WAN 口设置

GWN7062 支持双 WAN 端口设置，默认情况下，第四个 LAN 端口配置为 LAN，但用户可以启用双 WAN 口使其成为辅助 WAN 端口。

图 25 WAN 口设置

LAN

要访问 LAN 配置页面，请登录 GWN70xx WebGUI 并转至**网络设置→ LAN**。用户可以在本页进行 VLAN 配置（如添加 VLAN 或设置 VLAN 端口）和静态 IP 绑定。

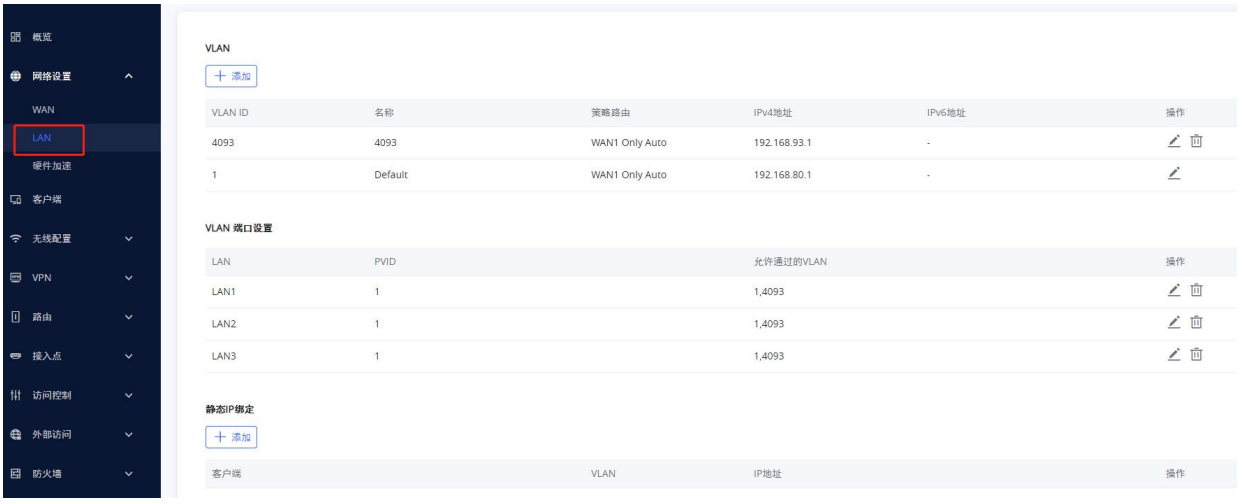


图 26 LAN 配置

VLAN

GWN70xx 路由器集成 VLAN 功能以增强安全性并添加更多功能和特性。VLAN 标记可以区分 SSID，也可以仅允许在特定 LAN 上使用这些 VLAN，以便进行更多的控制和隔离，它们还可以与策略路由一起使用。

添加或编辑 VLAN

用户可以在网络设置→LAN 下添加或编辑 VLAN。点击 

按钮添加，点击  按钮编辑 VLAN。

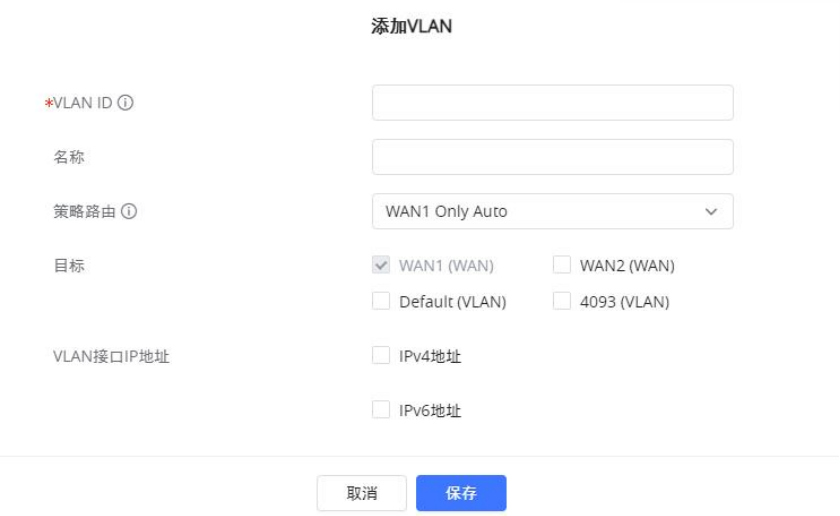


图 27 添加 VLAN

表 7 添加或编辑 VLAN

VLAN ID	输入 VLAN ID *注意：VLAN ID 范围为 3 到 4094。*
名称	输入 VLAN 名称。
策略路由	在列表中选择并添加策略路由。
目标	快速配置 VLAN 与 WAN、其他 VLAN 和 VPN 的单向数据通信。 默认选择将基于“策略路由”选项的配置，以保持默认路由的可访问性。
VLAN 接口 IP 地址	勾选来使用特定的 IP 地址。
IPv4 地址	输入 IPv4 地址。
子网掩码	输入子网掩码。
DHCP 服务	默认为关闭，选择开启来配置 IP 地址分配范围。
IPv4 地址分配范围	输入 P 地址分配范围的起始和终止地址。
租期（分钟）	默认为 120，合理范围为 60~2880。
DHCP 选项	添加 DHCP 选项。
首选 DNS 服务器	输入首选 DNS 服务器。
次选 DNS 服务器	输入次选 DNS 服务器。

VLAN 端口设置

用户可以让每个 LAN 端口仅允许特定 VLAN，如果有多个 VLAN，则可以选择一个 VLAN 作为默认 VLAN ID

（PVID 或端口 VLAN 标识符）。单击 编辑 VLAN 端口，单击 删除该配置并恢复默认设置为 VLAN 1。

图 28 VLAN 端口设置

表 8 VLAN 端口设置

允许通过的 VLAN	选择此端口上允许的 VLAN。
PVID	选择端口 VLAN 标识或默认 VLAN ID

静态 IP 绑定

用户可以使用此功能将静态 IP 绑定给某些不希望更改其 IP 地址的客户端。

请按一下步骤绑定静态 IP：

1. 进入网络设置→ LAN→ 静态 IP 绑定。
2. 单击 添加 按钮创建新条目。
3. 输入设备的 MAC 地址和 IP 地址。

图 29 静态 IP 绑定

表 9 静态 IP 绑定

VLAN	选择 VLAN 或默认 VLAN。
绑定的设备	输入设备 MAC 地址和 IP 地址进行绑定，或从客户端列表中选择。
MAC 地址	输入 MAC 地址。
IP 地址	输入给设备配置的 IP 地址。

硬件加速

启用加速模式可以实现更高的速度和减少延迟。

图 30 硬件加速

启用后，某些功能可能无法正常工作或被禁用。

1. 软件加速：禁用 QoS 和速率限制（如无线客户端速率限制）。
2. 硬件加速：禁用 QoS、NetFlow、Bonding、Suspend 和无线加速。

路由

本节介绍应用于 WAN 口或 LAN/VLAN 口的静态路由或策略路由，用户给静态路由和策略路由指定下一跳和 Metric，或给策略路由设置优先级和权重。

策略路由

功能概览

基于策略的路由功能允许网络管理员为通过路由器的流量做出高级路由决策。此功能可对指定 WAN 口和 VLAN 使用的策略进行高颗粒度控制。通过这种方式控制的流量可以在多个 VLAN 之间实现平衡。

添加/配置策略路由

要配置新的路由策略，首先用户需要在**路由→ 策略路由**创建成员。

图 31 添加策略路由

表 10 添加策略路由

名称	指定策略路由的名称。
接口	选择接口，如 WAN 口。

优先级	默认为 1，合理范围为 1~128。 *注意：优先级值越小，优先级越高。*
权重	默认为 1，合理范围为 1~10。

使用路由策略

添加 VLAN

要使用创建的路由策略，请至**“网络设置”→ LAN”**，然后添加新的 VLAN 或编辑以前创建的 VLAN。

图 32 添加 VLAN

表 11 添加 VLAN

VLAN ID	输入 VLAN ID *注意：VLAN ID 范围为 3 到 4094。*
名称	输入 VLAN 名称。
策略路由	在列表中选择并添加策略路由。
VLAN 接口 IP 地址	勾选来使用特定的 IP 地址。

静态路由

GWN70xx 支持手动设置 IPv4 静态路由，可以在 GWN70xx WebGUI **路由→ 静态路由**中配置。

用户可以点击 

按钮添加静态路由。

图 33 添加静态路由

表 12 添加静态路由

名称	指定静态路由的名称。
状态	启用或禁用静态路由。
IP 地址	设置 IP 地址。
子网掩码	输入子网掩码。
出接口	选择接口。
下一跳	第一下一跳。
Metric	当网络中存在多条路由可以达到同一目的地址时，可通过设置 Metric 来调整路由规则的优先级，数据包将按照 Metric 最小的路径转发。

WAN口负载平衡

具有双 WAN 口的路由器（如 GWN7062）可以在冗余网络连接的 WAN 端口之间进行负载平衡。它充分利用每个链路，减少了网络宕机时间。

要在多个 WAN 口之间实现负载平衡，请按照以下步骤配置：

1. 启用双 WAN 口。

首先请确认设备已经启用了双 WAN 口功能。可以在**网络设置→WAN→WAN 口**设置中打开。

图 34 双 WAN 口设置

2. 添加策略路由

在**路由→ 策略路由**中添加策略路由，然后添加成员，其中每个成员引用一个接口 WAN1 或 WAN2。每个接口的优先级范围为 1-128，优先级最高的 WAN 将被最多使用。权重范围为 1-10，表示应发送到此 WAN 的流量百分比。

优先级在相同值的情况下，才能根据权重进行负载平衡。

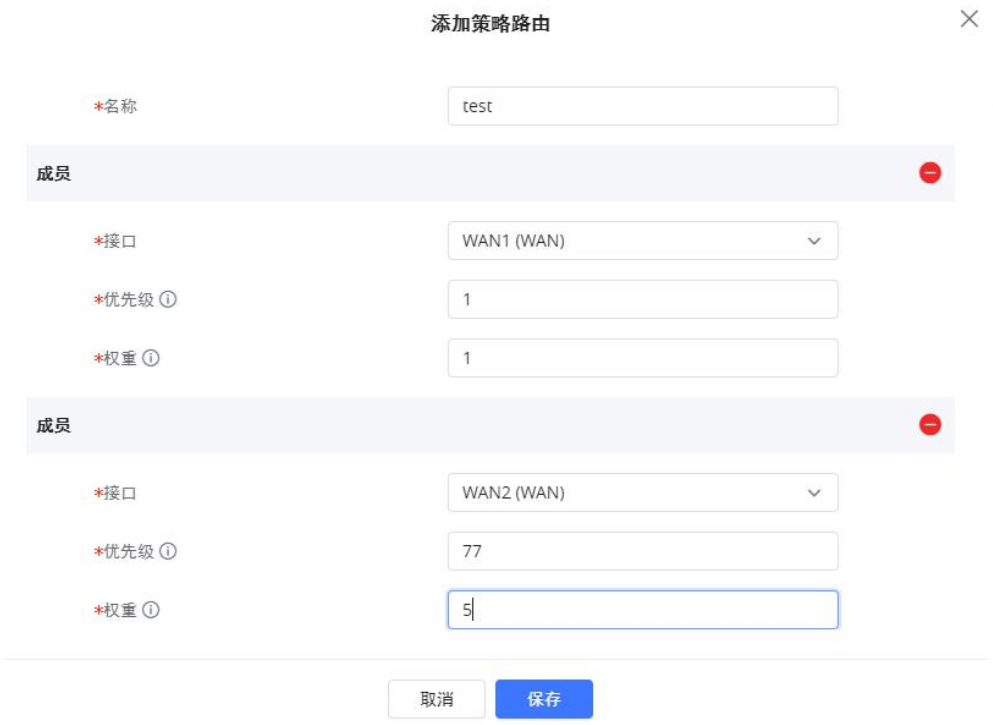


图 35 添加策略路由

3. 添加使用策略路由的 VLAN

添加 VLAN，并使用之前创建的策略路由。

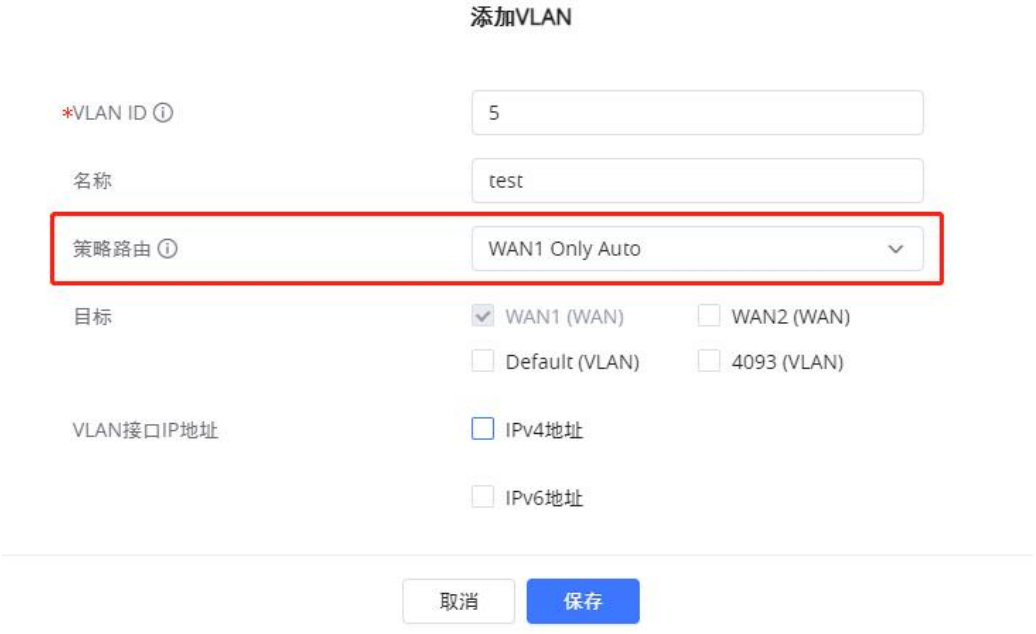


图 36 添加使用策略路由的 VLAN

4. 将 VLAN 应用到 SSID 或 LAN 口

最后，将创建好的 VLAN 应用到 SSID 或 LAN 口。

图 37：添加 SSID

类似地，用户可以将 VLAN 应用到 LAN 口，让 LAN 使用策略路由。

图 38：将 VLAN 应用到 LAN 口

配置无线网络

GWN70xx 路由器为用户提供了直接从 GWN70xx 或通过添加多个 GWN76xx 系列接入点创建无线网络的能力，用户可通过 2.4GHz&5GHz 802.11a/b/g/n/ac/ax 进行连接。GWN70xx 集成了多层安全性功能，包括 IEEE 802.1x 基于端口的身份验证协议、Wi-Fi 保护访问（WPA/WPA2、WPA2、WPA2/WPA3、WPA3 和 WPA3-192）以及防火墙和 VPN 隧道。

发现并配对其他GWN76XX 接入点

1. 在 WEB GUI 中进入**接入点→配置**。

2. 点击 

按钮发现 GWN70XX 局域网下的 AP，或点击 

按钮和与 Master AP 断开的 Slave AP 配对。

3. 检查 AP 是否在线，并点击确定。

图 39：发现并配对 AP

AP定位

GWN 支持一个方便的功能，允许用户通过闪烁的 LED 来定位其他接入点。 要使用该功能，请在**接入点→状态**页面下单击所需 AP 旁边的 图标，对应的设备将开始闪烁 LED。

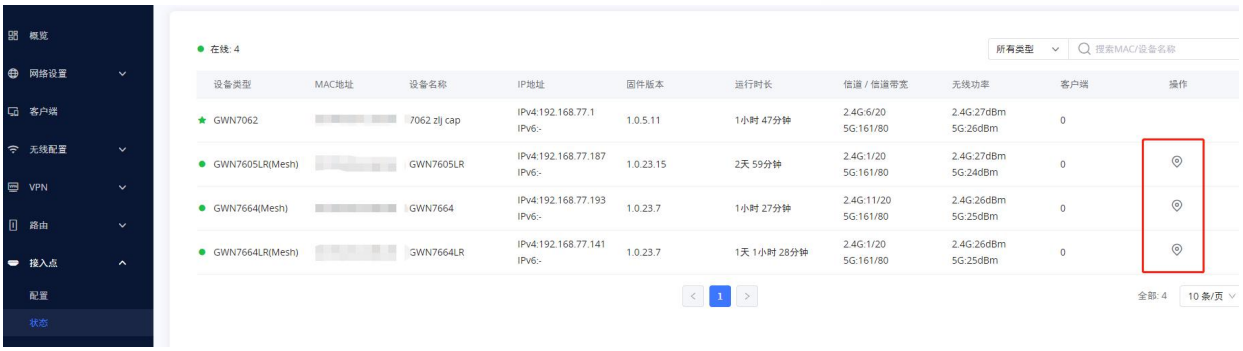


图 40：接入点-状态页面

SSIDs

当使用 GWN70XX 作为主接入点时，用户可以创建不同的 SSID 并为它们分配 GWN76XX 从接入点。

登录 GWN70XX 的 WEB GUI，进入**无线配置→SSIDs**，点击  添加新的 SSID。

图 41：添加 SSID

编辑或添加新 SSID 时，用户将配置两个选项卡：

- **Wi-Fi**：有关 Wi-Fi 选项卡选项，请参阅下表：

表：13 Wi-Fi 设置

字段	描述
Wi-Fi	点击“开启”启用 SSID。
名称	设备或修改 SSID 名称。
客户端 IP 分配方式	设置为 NAT 模式，客户端将从指定的 NAT 池中获取 IP 地址。且连接到不同 AP 的客户端是相互隔离。 *GWN7610 不支持此功能。*
频段	选择 GWN 要使用的 Wi-Fi 频段，有 3 个选项： • **Dual-Band** • **2.4GHz** • **5Ghz**
关联 VLAN	点击“开启”启用 VLAN。然后从列表中指定 VLAN 或创建 VLAN。
接入安全	设置加密的安全模式，有 6 个选项可用： • **WPA/WPA2**：使用“PSK”或“802.1x”作为 WPA 密钥模式，使用“AES”或“AES/TKIP”加密类型。 • **WPA2**：使用“PSK”或“802.1x”作为 WPA 密钥模式，使用“AES”或“GCMP-128”加密类型。 • **WPA2/WPA3**：使用“SAE-PSK”或“802.1x”作为 WPA 密钥模式，采用“AES”或“GCMP-128”加密类型。 • **WPA3**：Using “SAE” or “802.1x” as WPA Key Mode, with “AES” or “AES/TKIP” Encryption Type. • **WPA3-192**：使用“802.1x”作为 WPA 密钥模式，使用“GCMP-256”或“CCMP-256”加密类型。 • **Open**：不需要密码。 用户无需身份验证即可连接。 出于安全原因不推荐。
WEP 秘钥	输入 WEP 保护模式的密码密钥。 *此字段仅在“安全模式”设置为“WEP 64 位”或“WEP 128 位”时可用。*

WPA 秘钥模式	有两种： • **PSK**：使用预共享密钥对 Wi-Fi 进行身份验证。 • **802.1X**：使用 RADIUS 服务器对 Wi-Fi 进行身份验证。 *此字段仅在“安全模式”设置为“WPA/WPA2”、“WPA2”、“WPA2/WPA3”、“WPA3”或“WPA3-192”时可用。*
WPA 加密类型	有两种： • **AES**：此方法动态更改加密密钥，使其几乎无法绕过 • **AES/TKIP**：同时使用临时密钥完整性协议和高级加密标准进行加密，这提供了最可靠的安全性。 *此字段仅在“安全模式”设置为“WPA/WPA2”、“WPA2”、“WPA2&WPA3”、“WPA3”或“WPA3-128”时可用。*
WPA 共享秘钥	为客户端设置访问密钥，输入范围为：8-63 个 ASCII 字符或 8-64 个十六进制字符。 *此字段仅在“安全模式”设置为“WPA/WPA2”、“WPA2”、“WPA2/WPA3”或“WPA3”时可用。*
802.11w	802.11w 标准用于防止某些类型的 WLAN DoS 攻击。 802.11w 扩展了强大的加密保护，并为广播/多播鲁棒管理帧提供数据完整性和重放保护。将此选项设置为 Disabled：禁用 802.11w； Optional：支持和不支持 802.11w 的客户端都可以有网络访问权限； Required：只有支持 802.11w 的客户端才有入网权限。
RADIU 服务器地址	配置 RADIUS 认证服务器地址。 *此字段仅在“WPA 密钥模式”设置为“802.1x”时可用。*
RADIUS 服务器端口	配置 RADIUS 服务器监听端口。 默认值为：1812。 *此字段仅在“WPA 密钥模式”设置为“802.1x”时可用。*
RADIUS 服务器秘钥	输入用于与 RADIUS 服务器进行客户端身份验证的机密密码。 *此字段仅在“WPA 密钥模式”设置为“802.1x”时可用。*

备用 RADIUS 服务器	选中该框启用备用 RADIUS 服务器。 您需要指定以下三个字段： - **RADIUS 服务器地址**：配置备用 RADIUS 服务器地址。 - **RADIUS 服务器端口**：输入备用 RADIUS 服务器端口。默认端口为 1812，范围为 1-65535。 - **RADIUS 服务器秘钥**：输入用于与备用 RADIUS 服务器进行客户端身份验证的机密密码。
RADIUS 计费服务器地址	配置 RADIUS 计费服务器地址。*此字段仅在“WPA 密钥模式”设置为“802.1x”时可用。*
RADIUS 计费服务器地址端口	配置 RADIUS 计费服务器监听地址。默认为 1813. *此字段仅在“WPA 密钥模式”设置为“802.1x”时可用。*
RADIUS 计费服务器地址秘钥	输入用于与 RADIUS 计费服务器进行客户端身份验证的密码。 *此字段仅在“WPA 密钥模式”设置为“802.1x”时可用。*
备用计费服务器	选中该框启用备用 RADIUS 计费 服务器。 您需要指定以下三个字段： - **RADIUS 计费服务器地址**：配置备用 RADIUS 计费服务器地址。 - **RADIUS 计费服务器端口**：输入备用 RADIUS 计费服务器端口。默认端口为 1812，范围为 1-65535。 - **RADIUS 计费服务器秘钥**：输入用于与备用计费 RADIUS 服务器进行客户端身份验证的机密密码。
RADIUS NAS ID	启用 RADIUS NAS ID. *此字段仅在“WPA 密钥模式”设置为“802.1x”时可用。*
启用 Hotspot2.0	勾选开启 SSID 中 的 Hotspot2.0 *此字段仅在“WPA 密钥模式”设置为“802.1x”时可用。* 更多详情请参考【Hotspot2.0】
Hotspot2.0 Profile	选择要在 SSID 中使用的 Hotspot2.0 配置文件。 *此字段仅在“WPA 密钥模式”设置为“802.1x”时可用。* 更多详情请参考【Hotspot2.0】
开启强制门户	勾选启用强制门户功能。
黑名单过滤	选择黑名单/白名单以指定从连接到区域的 Wi-Fi 时排除/包含的 MAC 地址。默认为禁止。

开启动态 VLAN (beta)	启用后，将从 RADIUS 用户配置文件中配置的相应 VLAN 中为客户端分配 IP 地址。 *此字段仅在“WPA 密钥模式”设置为“802.1x”时可用。*
客户端隔离	客户端隔离功能可阻止已连接客户端与 GWN70XX 的 Wi-Fi 接入点之间的任何 TCP/IP 连接。 客户端隔离有助于提高访客网络/公共 Wi-Fi 的安全性。提供三种模式： • **无线**：无线客户端可以访问互联网服务、GWN7xxx 路由器和接入点 GWN70XX，但它们不能相互通信。 • **互联网**：无线客户端将只被允许访问互联网服务，他们无法访问路由器或接入点 GWN70XX 上的任何管理服务。 • **网关 MAC**:无线客户端扫描只与网关通信，客户端之间的通信被阻塞，无法访问 GWN70XX 接入点上的任何管理服务。
高级	
隐藏 SSID	选择隐藏 SSID。 扫描 Wi-Fi 时 SSID 将不可见，要将设备连接到隐藏的 SSID，用户需要手动指定 SSID 名称和验证密码。
DTIM 周期	配置每个 Beacon 广播的 DTIM (Delivery Traffic Indication Message) 传输频率。 客户端将在每个配置的 DTIM 周期检查 AP 的缓冲数据。 您可以为省电考虑设置一个较高的值。 • 默认值为 1，表示 AP 每个 Beacon 广播一次 DTIM。 • 如果设置为 10，AP 将每 10 个 Beacon 广播一次 DTIM。有效范围：1 - 10。
无线客户端限制	配置无线客户端的限制。 如果 LAN 上的每个无线电都有一个 SSID，则每个 SSID 将具有相同的限制。 因此，将限制设置为 50 会将每个 ssid 单独限制 50 个用户。 注意：如果设置为 0，则等于禁用限制。
客户端活动超时(秒)	如果客户端在指定的时间段内根本没有产生任何流量，AP 将删除客户端的条目。 默认情况下，客户端不活动超时设置为 300 秒。 范围为 60-3600 秒。
组播/广播抑制	当设置为“禁止”时：所有的广播和组播包将被转发到无线接口。 设置为“开启”时：丢弃除 DHCP/ARP/IGMP/ND 外的所有广播和组播包； 当设置为“开启并使用 ARP 代理”时：AP 将同时启用代理 ARP 。

IP 组播转单播	设置为“禁止”时：不转换任何组播包； 被动模式：AP 永远不会主动广播 IGMP 查询，IGMP Snooping 项在注册后会老化 300 秒，可能导致组播数据转发失败。 主动模式：AP 会主动广播 IGMP 查询，不断更新 IGMP Snooping 项。
开启预约	启用此选项可为带宽规则分配预约。
预约	在预约时间内，可以使用 SSID。
开启企业级语音	选中以启用/禁用企业级语音。 启用语音企业后，漫游时间将减少。 • 802.11k 标准通过创建优化的信道列表帮助客户端加快搜索附近可用作漫游目标的 AP。 当当前 AP 的信号强度减弱时，您的设备会从该列表中扫描目标 AP。 • 当您的客户端设备在同一网络上从一个 AP 漫游到另一个 AP 时，802.11r 使用称为快速基本服务集转换 (FT) 的功能来更快地进行身份验证。FT 适用于预共享密钥 (PSK) 和 802.1X 身份验证方法。 • 802.11v 允许客户端设备交换有关网络拓扑的信息，包括有关 RF 环境的信息，使每个客户端网络都了解，促进无线网络的整体改进。 **注意**：企业级音频功能需要 11R，11V 和 11K 是可选的。 *此字段仅在“安全模式”设置为“WPA/WPA2”或“WPA2”时可用。*
开启 802.11R	勾选开启 802.11r. *此字段仅在“安全模式”设置为“WPA/WPA2”或“WPA2”时可用。*
开启 802.11K	勾选开启 802.11k
开启 802.11V	勾选开启 802.11v
ARP 代理	此选项将使 GWN AP 能够回答其 LAN 为其连接的 Wi-Fi 客户端的 ARP 请求。这主要是为了减少 ARP 包消耗的通话时间
开启 U-APSD	此选项将允许用户启用/禁用计划外自动省电传输功能。
最大上传速度	支持 1-1000 的整数，为空则不限制。
最小上传速度	支持 1-1000 的整数，为空则不限制。

设备管理：用于向 SSID 添加或删除配对接入点。

图 42 设备管理

Mesh

在 Mesh 网络中，多个 Aps 之间可建立无线连接来传递数据流量，而不是客户端关联。 每个 AP 都会根据多个因素评估无线信道的性能，并选择一个或多个合适的 AP 来建立连接。

用户可以在系统**设置→Mesh** 中开启 Mesh 网络。

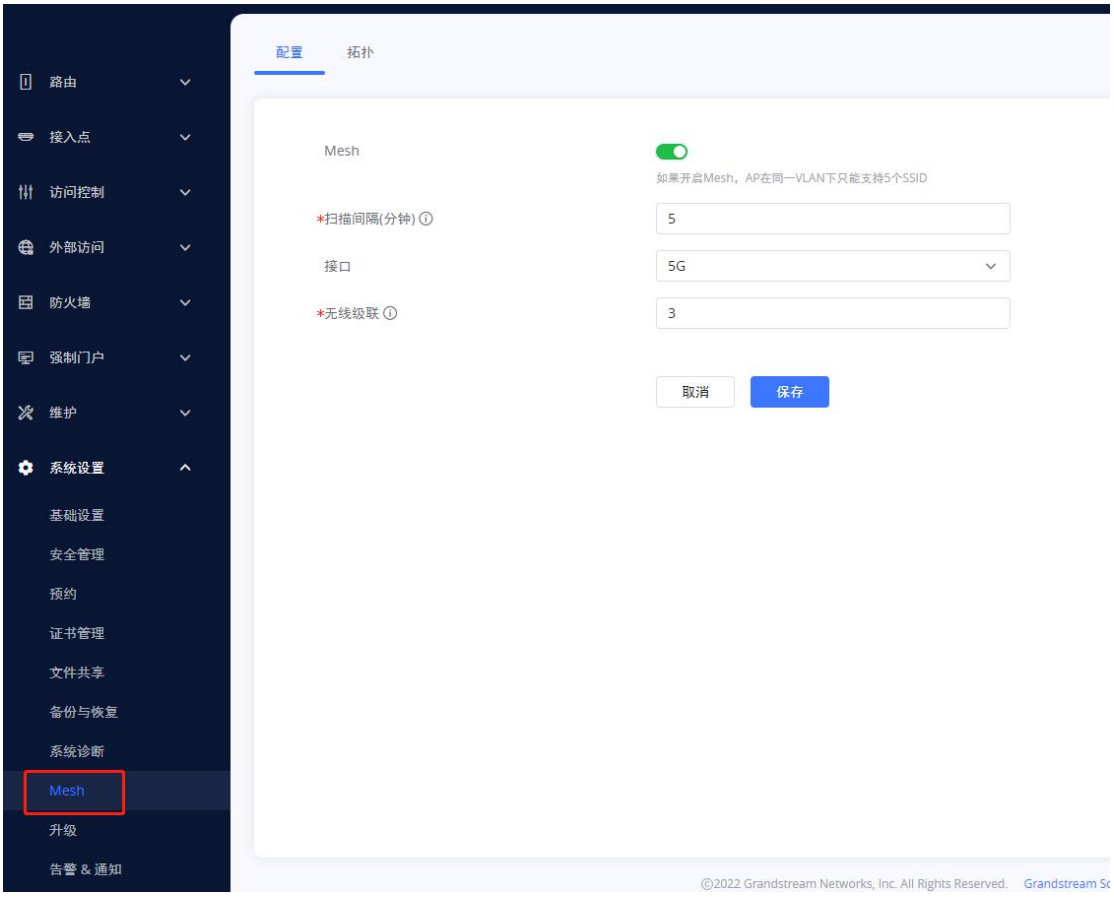


图 43 Mesh 网络

在网状网络中，接入点分为两种类型：

- **CAP （中央接入点）**：与有线网络有上行链路连接的接入点。
- **RE （范围扩展器）**：参与网状网络拓扑的接入点，具有到中央网络的无线上行链路连接。

为了部署 Mesh 接入点 (RE)，用户/安装人员可以遵循以下步骤：

1. 确保已经部署了主接入点和 CAP 接入点（有时 CAP 接入点可以是网络的主控制器）。
2. 将 RE 接入点与主设备配对。 这可以通过两种方式完成：
   A. 将所有 RE 与 master 连接到同一有线局域网，然后进行正常的发现/配对过程，AP 配对成功后即可在场地上部署。
   B. 通过 PSU 或 PoE 供电时，RE 也可以无线发现，管理员可以在发现后配置它们。 这要求 RE 必须在 Master 或 CAP Slave 的信号覆盖范围内。

下表为 Mesh 配置说明。

表 14 GWN70XX Mesh 配置

开启 Mesh	选中后，Mesh 功能将被激活。 默认为禁用。
扫描间隔（分钟）	扫描可用 Mesh 邻居的时间间隔（以分钟为单位）。 合理范围为 1-5。
接口	2.4GHzh 或 5GHz 频段。
无线级联	定义可以与 AP 无线级联的层数。 最小值为 1，最大值为 3。

关于 GWN Mesh 网络特性的更多详细信息，您可以参考以下技术文档：Mesh Network Guide.

升级接入点

如果您想升级单个或多个接入点，用户需要选择接入点，然后单击按钮启动升级过程，接入点将会使用路由器在**系统设置→ 升级**中配置的参数。

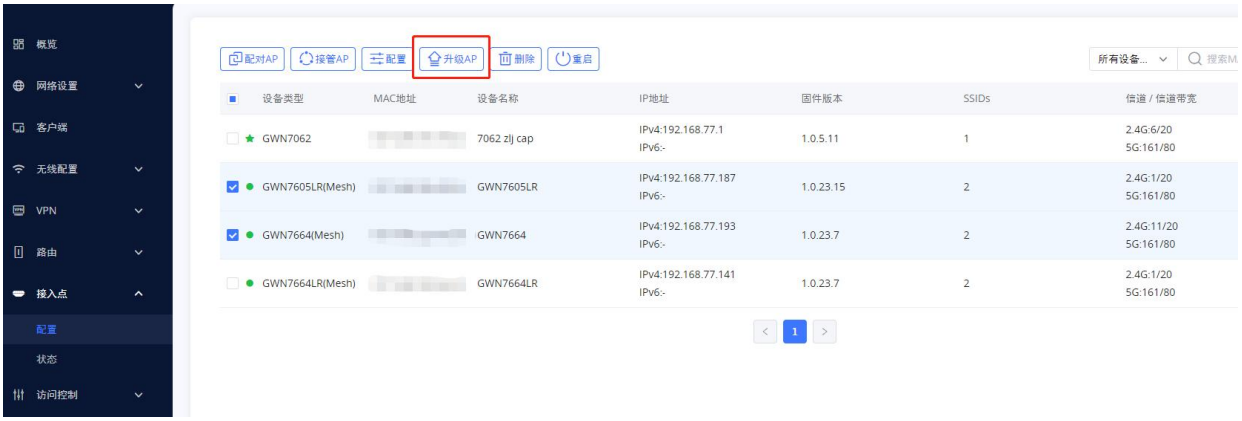


图 44 升级接入点

客户端配置

客户端

客户端页面显示当前和以前连接到不同 LAN 网的所有设备和用户，其中包含 MAC 地址、IP 地址、连接时长以及上载和下载流量等详细信息。了解客户的统计数据以及谁消耗了更多带宽是很有帮助的。用户可以在客户端页面单击  按钮编辑设备名称。

在 LAN 端口启 DHCP 服务器的 GWN70xx 将自动为连接到其 LAN 口的设备（如计算机或 GWN76xx 接入点）和连接到配对 GWN76xx 接入点的无线客户端分配 IP 地址。

用户可以从 **Web GUI→客户端**访问连接到 GWN70XX 的客户端列表，并对无线客户端执行不同的操作。

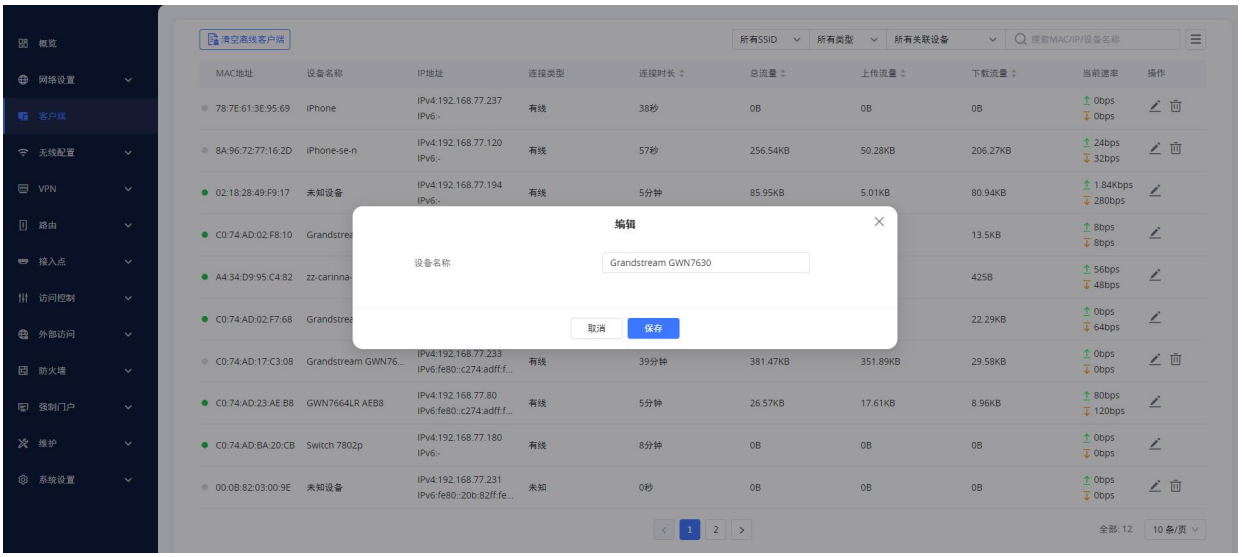


图 45 编辑客户端

VPN

概览

VPN 允许 GWN70xx 路由器使用 PPTP、IPSec、L2TP 和 OpenVPN®协议连接到远程 VPN 服务器，或者配置 OpenVPN™服务器并为客户端生成证书和密钥。用户可以从 GWN70xx Web GUI 访问 VPN 页面。

OpenVPN®配置

要将 GWN70xx 用作 OpenVPN®服务器，您需要拥有一个账号、OpenVPN™服务器证书和客户端证书。在生成服务器/客户端证书之前，需要先拥有 CA 证书，这将有助于颁发服务器/客户端的证书。

GWN70XX 证书可以在 WEB GUI 的**系统设置→证书管理**中管理。

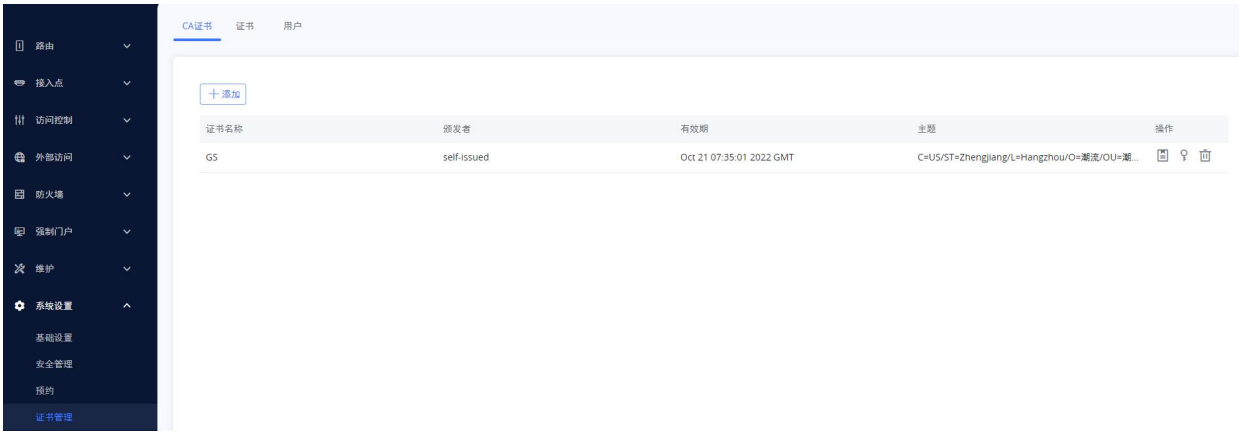


图 46 证书管理

生成自颁发证书颁发机构（CA）

证书颁发机构（CA）是一个受信任的实体，它发布在 Internet 上验证数字实体身份的电子文档。电子文档（又称数字证书）是安全通信的重要组成部分，在公钥基础设施（PKI）中发挥着重要作用。

请按照以下步骤生成 CA 证书：

1. 进入**系统设置→证书管理→CA 证书**。
2. 点击 

按钮。
3. 根据需要输入 CA 值，如证书名称、秘钥长度和摘要算法等。

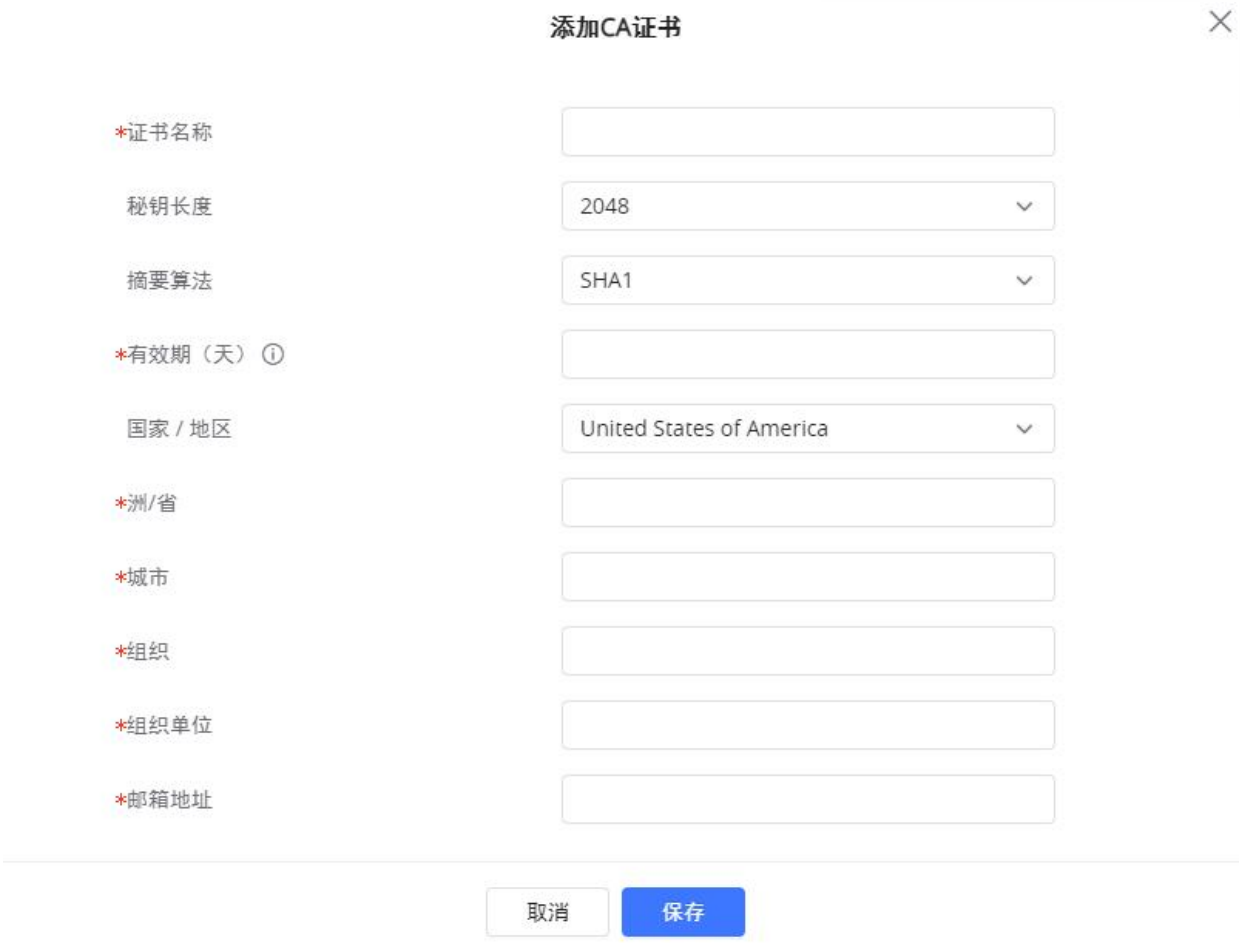


图 47 添加 CA 证书

下表对 CA 证书的配置项做了说明：

表 15 CA 证书

证书名称	输入 CA 的证书名称。 *注意：可以是任何名称来标识此证书。示例：“CATest”。*
秘钥长度	选择用于生成 CA 证书的密钥长度。以下值可用： ● 512：512 位密钥不安全，最好避免此选项。 ● 1024：1024 位密钥不足以抵御攻击。 ● 2048：2048 位密钥是一个好的最小值。（推荐）。 ● 4096：几乎所有 RSA 系统都接受 4096 位密钥。使用 4096 位密钥将显著增加生成时间、TLS 握手延迟和 TLS 操作的 CPU 使用。
摘要算法	选择摘要算法。 ● SHA1：此摘要算法提供基于任意长度的 160 位指纹输出。 ● SHA256：此摘要算法生成唯一的固定大小 256 位哈希。 *注意：哈希是一个单向函数，不能解密回来。*

有效期（天）	输入 CA 证书的有效日期（以天为单位）。
国家/地区	从下拉列表中选择国家/地区代码。
洲/省	输入洲/省的名称。
城市	输入城市名称。
组织	输入组织名称。如：Grandstream。
组织单位	输入组织单位。如：GS 市场。
邮箱地址	输入邮箱地址。

点击 保存 按钮保存证书。

点击 按钮可以导出 CA 证书至本地。CA 文件的扩展名为.crt。

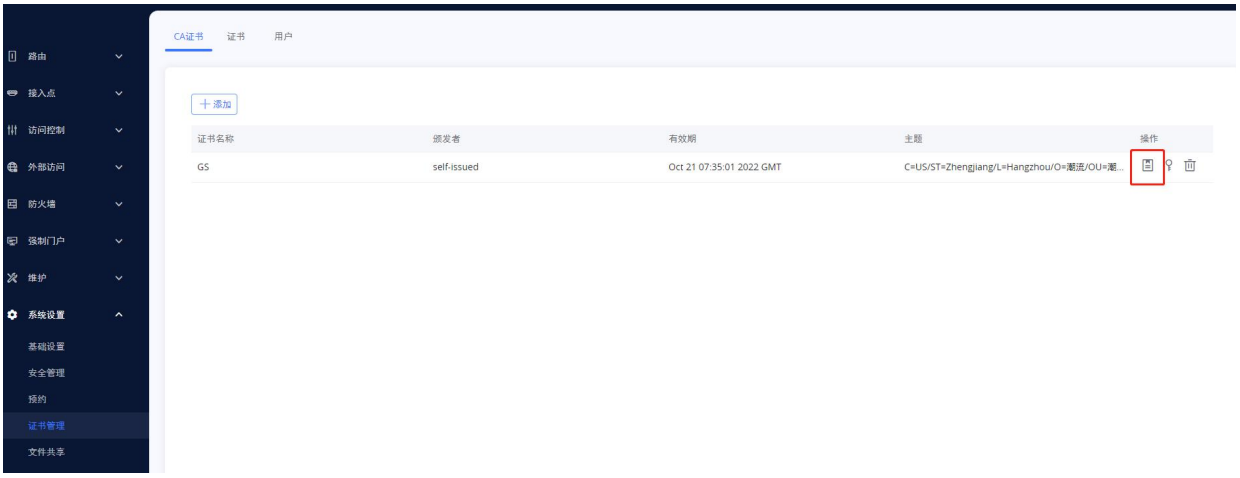


图 48 导出 CA 证书

生成服务器/客户端证书

为充当 OpenVPN®服务器的 GWN70xx 与客户端之间的加密通信创建服务器和客户端证书。

生成服务器证书

用户可以按照以下步骤生成服务器证书：

1. 进入**系统设置→证书管理→证书。**
2. 点击 添加 按钮添加证书。

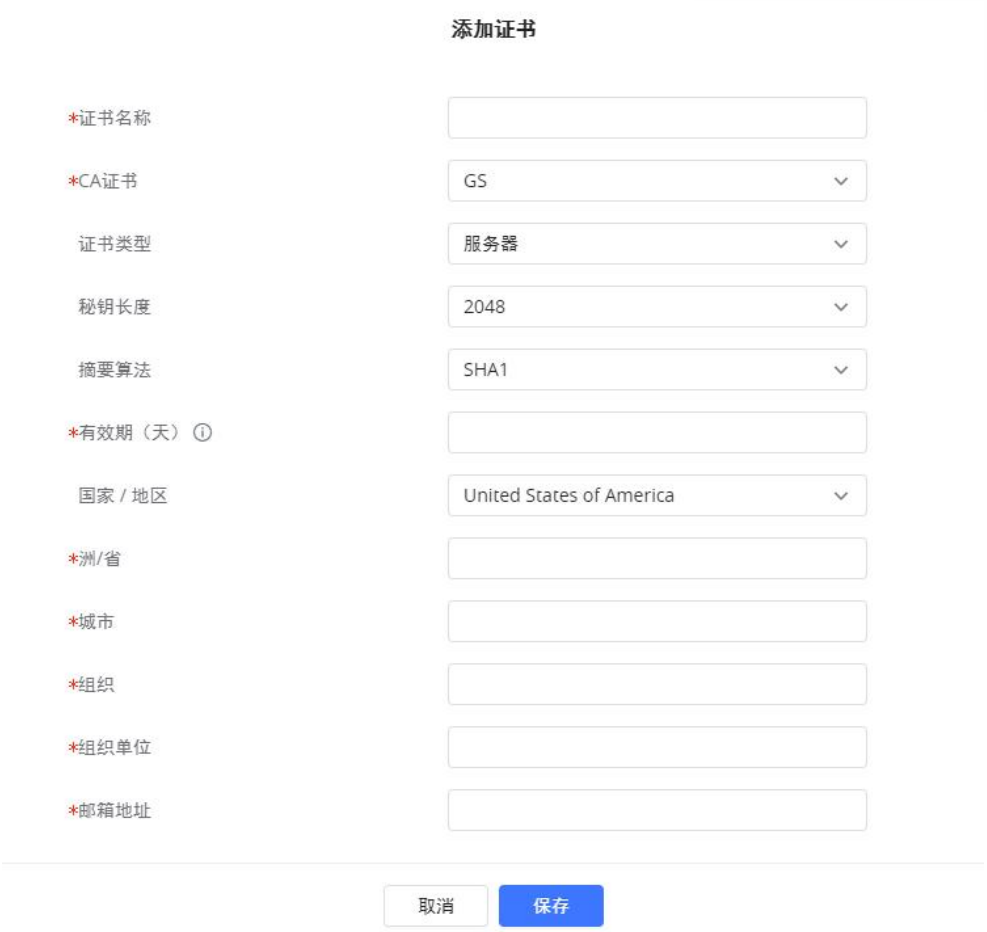


图 49 添加证书

下表对证书的配置项做了说明。

表 16 服务器证书

证书名称	输入 CA 的证书名称。 *注意：可以是任何名称来标识此证书。示例：“CATest”。*
CA 证书	在下拉框中选择先前创建的 CA 证书。
证书类型	选择证书类型，可以是服务器或客户端。选择服务器。
秘钥长度	选择用于生成 CA 证书的密钥长度。以下值可用： ● 512：512 位密钥不安全，最好避免此选项。 ● 1024：1024 位密钥不足以抵御攻击。 ● 2048：2048 位密钥是一个好的最小值。（推荐）。 ● 4096：几乎所有 RSA 系统都接受 4096 位密钥。使用 4096 位密钥将显著增加生成时间、TLS 握手延迟和 TLS 操作的 CPU 使用。

摘要算法	选择摘要算法。 ● SHA1：此摘要算法提供基于任意长度的 160 位指纹输出。 ● SHA256：此摘要算法生成唯一的固定大小 256 位哈希。 *注意：哈希是一个单向函数，不能解密回来。*
有效期（天）	输入 CA 证书的有效日期（以天为单位）。
国家/地区	从下拉列表中选择国家/地区代码。
洲/省	输入洲/省的名称。
城市	输入城市名称。
组织	输入组织名称。如：Grandstream。
组织单位	输入组织单位。如：GS 市场。
邮箱地址	输入邮箱地址。

点击 保存 按钮保存证书。

点击  按钮可以导出服务器证书至本地。CA 文件的扩展名为.crt。

点击  按钮可以导出服务器证书秘钥至本地。秘钥文件的扩展名为.key。

点击  按钮删除不再需要的服务器证书。

注意： GWN70xx 路由器在充当服务器时将使用服务器证书（.crt 和.key）。
服务器证书（.crt 和.key）可以导出并在另一个 OpenVPN®服务器上使用。

生成客户端证书

用户可以按照以下步骤生成服务器证书：

1. 创建用户

进入**系统设置→证书管理→用户。**

点击 + 添加 按钮添加用户。

图 50 添加服务器用户

下表对添加用户的配置项做了说明。

表 17 添加用户

状态	点击开启使用用户。
全称	输入用户的全称来定义用户。
用户名	输入用户名称来区分用户。
密码	输入用户的密码。
OpenVPN 子网	当 OpenVPN 客户端路由器使用用户账号建立站点对站点 VPN 时，用于指示远程设备后面的网络。

2. 创建客户端证书

1. 进入**系统设置→证书管理→证书。**
2. 点击 

按钮添加证书。

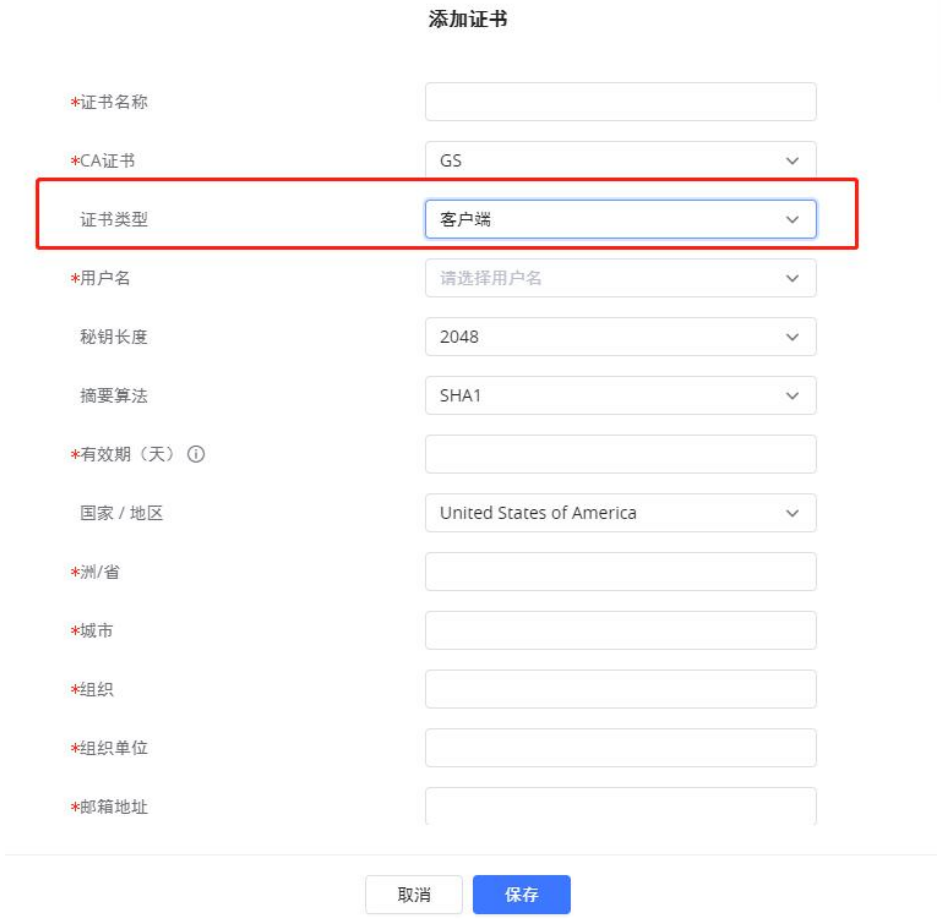


图 51 添加客户端证书

下表对证书的配置项做了说明。

表 18 客户端证书

证书名称	输入 CA 的证书名称。 *注意：可以是任何名称来标识此证书。示例：“CATest”。*
CA 证书	在下拉框中选择先前创建的 CA 证书。
证书类型	选择证书类型，可以是服务器或客户端。选择客户端。
用户名	选择用户名来生成证书。
秘钥长度	选择用于生成 CA 证书的密钥长度。以下值可用： ● 512：512 位密钥不安全，最好避免此选项。 ● 1024：1024 位密钥不足以抵御攻击。 ● 2048：2048 位密钥是一个好的最小值。（推荐）。 ● 4096：几乎所有 RSA 系统都接受 4096 位密钥。使用 4096 位密钥将显著增加生成时间、TLS 握手延迟和 TLS 操作的 CPU 使用。

摘要算法	选择摘要算法。 ● SHA1：此摘要算法提供基于任意长度的 160 位指纹输出。 ● SHA256：此摘要算法生成唯一的固定大小 256 位哈希。 *注意：哈希是一个单向函数，不能解密回来。*
有效期（天）	输入 CA 证书的有效日期（以天为单位）。
国家/地区	从下拉列表中选择国家/地区代码。
洲/省	输入洲/省的名称。
城市	输入城市名称。
组织	输入组织名称。如：Grandstream。
组织单位	输入组织单位。如：GS 市场。
邮箱地址	输入邮箱地址。

点击 保存 按钮保存证书。

点击 按钮可以导出服务器证书至本地。CA 文件的扩展名为.crt。

点击 按钮可以导出服务器证书秘钥至本地。秘钥文件的扩展名为.key。

点击 按钮删除不再需要的服务器证书。

注意：从 GWN70xx 生成的客户端证书需要上传到客户端。

为了提高安全性，每个客户端都需要有自己的用户名和证书，这样即使用户被泄露，其他用户也不会受到影响。

OpenVPN®客户端配置

用户有两种方式将 GWN70XX 设置成 OpenVPN®客户端。

1. 将从 OpenVPN®服务器创建的客户端证书上传到 GWN70xx。
2. 在 GWN70xx 上创建客户端/服务器证书，并将服务器证书上传到 OpenVPN®服务器。

在 **VPN→VPN 客户端**中按以下步骤进行操作：

点击 + 添加 按钮添加 VPN 客户端。

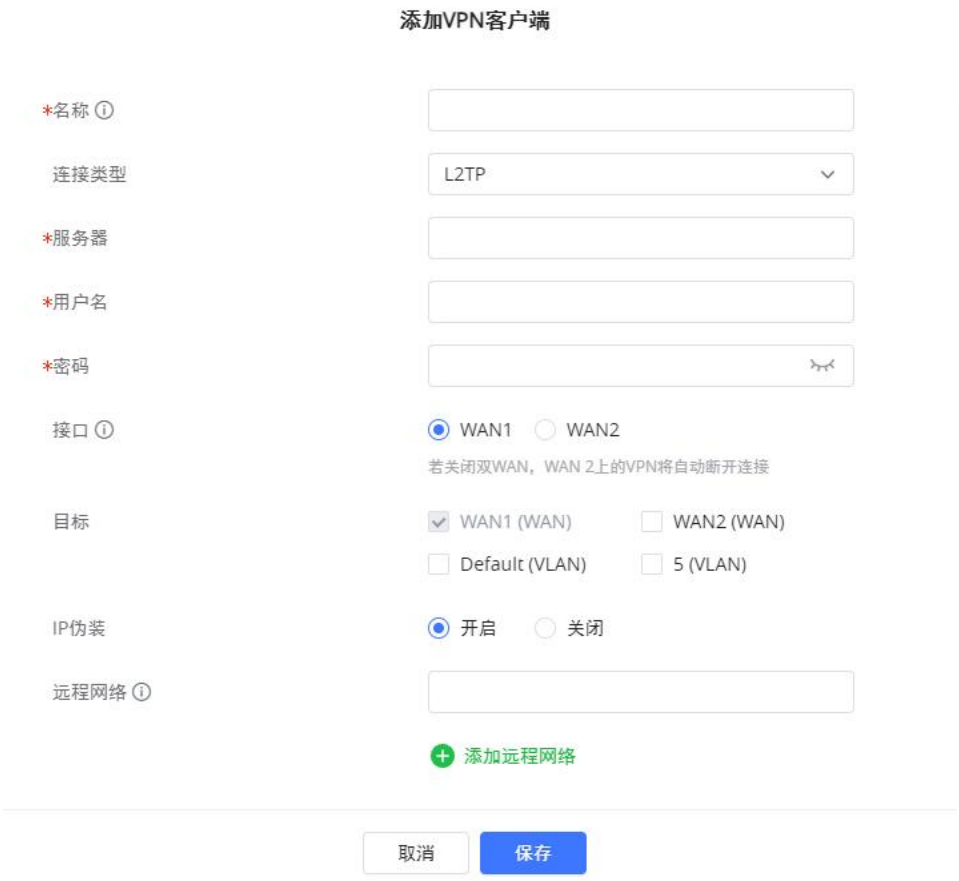


图 52 添加 VPN 客户端

点击 保存 按钮保存配置。

L2TP配置

第 2 层隧道协议（L2TP）是一种隧道协议，用于支持虚拟专用网络（VPN）或发挥 ISP 服务的部分传递作用。它本身不提供任何加密或保密。相反，它依赖于在隧道内传递的加密协议来提供隐私。

L2TP 客户端配置

用户可以在 **VPN→VPN 客户端**中对 GWN70XX 进行 L2TP 客户端配置。

1. 点击 ＋添加 按钮添加 L2TP 客户端。

图 53 添加 L2TP 客户端

点击 保存 按钮保存配置。

PPTP配置

PPTP 是由 Microsoft 开发的基于点对点协议（PPP）的数据链路层协议，用于广域网（WAN），使网络流量能够在不安全的公共网络（如因特网）上封装和路由。
点对点隧道协议（PPTP）允许创建虚拟专用网络（VPN），该虚拟专用网络通过互联网传输 TCP/IP 流量。

PPTP 客户端配置

用户可以在 **VPN→VPN 客户端**中对 GWN70XX 进行 PPTP 客户端配置。

1. 点击 + 添加 按钮添加 PPTP 客户端。

图 54 添加 PPTP 客户端

点击 保存 按钮保存配置。

IPSec VPN Tunnel

概览

互联网安全协议-IPsec 主要用于认证和加密通过网络层发送的数据包。为了实现这一点，他们使用了两种安全协议——ESP（封装安全有效载荷）和 AH（认证头域），前者既提供认证，也提供加密，而后者只提供数据包的认证。由于 ESP 可同时进行身份验证和加密，因此大多数的实施都使用 ESP。

IPsec 支持两种不同的加密模式，分别是隧道（默认）和传输模式。隧道模式用于加密有效载荷和 IP 数据包的报头，更安全。传输模式仅加密 IP 数据包的有效载荷，通常用于网关或主机部署。

IPsec 还涉及用于建立安全关联（SA）的 IKE（Internet 密钥交换）协议。安全关联在两个网络实体之间建立一组共享安全参数，以提供安全的网络层通信。这些安全参数可以包括加密算法和模式、流量加密密钥以及通过连接发送的网络数据的参数。目前，有两个 IKE 版本可用 - IKEv1 和 IKEv2。IKE 分为两个阶段：

阶段 1：ISAKMP 操作将在两个网络实体之间建立安全信道之后执行。

阶段 2：安全关联将在两个网络实体之间协商。

IKE 在三种模式下运行，用于交换密钥信息和建立安全关联，三种模式分别为：主模式、主动模式和快速模式。

主模式：用于在密钥交换期间建立阶段 1。它在发起者和接收者之间使用三个双向交换。在第一次交换中，算法和散列被交换。在第二个交换中，使用 Diffie-Hellman 交换生成共享密钥。在最后一次交换中，对彼此的身份进行验证。

主动模式：提供与主模式相同的服务，但它使用两个交换而不是三个交换。它不提供身份保护，这使得它容易受到黑客的攻击。主模式比此模式更安全。

快速模式：使用主模式或主动模式建立安全通道后，快速模式可用于协商一般 IPsec 安全服务并生成新的密钥文件。它们总是在安全信道下加密，并使用用于验证数据包其余部分的哈希有效载荷。

配置 IPSec 通道

要在位于 Internet 上不同位置的两个设备之间构建 IPSec 安全隧道，我们可以使用以下示例场景：

分支办公室路由器需要通过 IPSec 隧道连接到总部办公室，每侧都有一个 GWN70xx 路由器。用户可以按如下方式配置这两个设备：

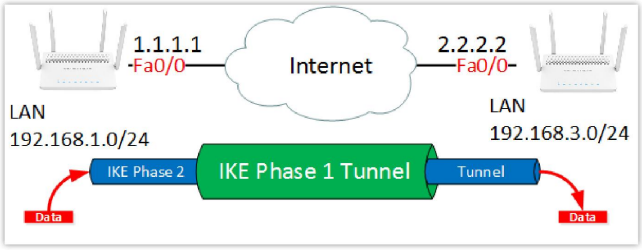


图 55 IPSec 通道

分支办公室路由器使用局域网子网 192.168.1.0/24，总部路由器使用局域网网络 192.168.3.0，分支办公室路由器的公共 IP 为 1.1.1.1，总部路由器的 IP 为 2.2.2.2。

配置分支机构的路由器

在 **VPN→VPN 客户端**中添加 VPN 客户端。

图 56 添加 IPSec VPN

阶段 1


添加VPN客户端
阶段1
协商模式
主模式
*预共享密码
加密算法
AES-256
认证算法
SHA2-256
DH组
Group14
重连
*重连次数
10
DPD（失效对等体检测）
*DPD延迟时间 (秒)
30
*DPD空闲时间 (秒)
120
DPD行为
暂停
取消
保存

图 57 阶段 1

阶段 2

图 58 阶段 2

完成后，点击“保存”并对另一台路由器执行相同操作。这两个路由器将构建通道和必要的路由信息，使流量通过隧道在分支办公室和总部网络之间传输。

配置 IPSec 服务器

用户可以在 **VPN→VPN 路由器→IPSec 服务器**配置服务器。

图 59 IPSec 服务器

点击保存。然后点击  按钮添加远程拨入用户。

图 60 添加远程拨入用户

防火墙和外部访问

GWN70xx 路由器支持防火墙功能，通过限制或拒绝特定流量来控制传入和传出流量，并防止对 GWN70xx 网络的攻击，增强安全性。像 DMZ 这样的功能允许计算机完全暴露在互联网上。

外部访问

GWN70xx 可以启用端口转发等功能使网络外部可以访问它，同时还具有 DMZ 功能暴露物理或逻辑子网络，以及通用即插即用（UPnP）功能。

.要获取有关特定接入点状态的更多详细信息，用户可以单击所需的 AP，然后将显示以下页面：

选项卡“信息”显示了所选 AP 的详细信息，例如型号、名称、固件版本、内存使用和这台 AP 正在广播的 SSID 等。

DDNS

1. 访问 GWN70xx web GUI，进入**外部访问→ DDNS**，然后单击 

添加服务。
2. 在“服务提供商”字段下填写由 DDNS 提供商创建的域名。
3. 在用户名和密码字段下输入您的账号用户名和密码。
4. 在“域名”下指定应用 DDNS 账号的域。

图 61 DDNS 服务

表 19 DDNS

服务提供商	在下拉列表中选择 DDNS 服务商。
用户名	输入用户名。
密码	输入密码。
域名	输入域名。
接口	选择接口。

端口转发

端口转发允许将通信请求从一个地址和端口号组合重定向到另一个。
用户可以在**外部访问→端口转发**中进行配置。

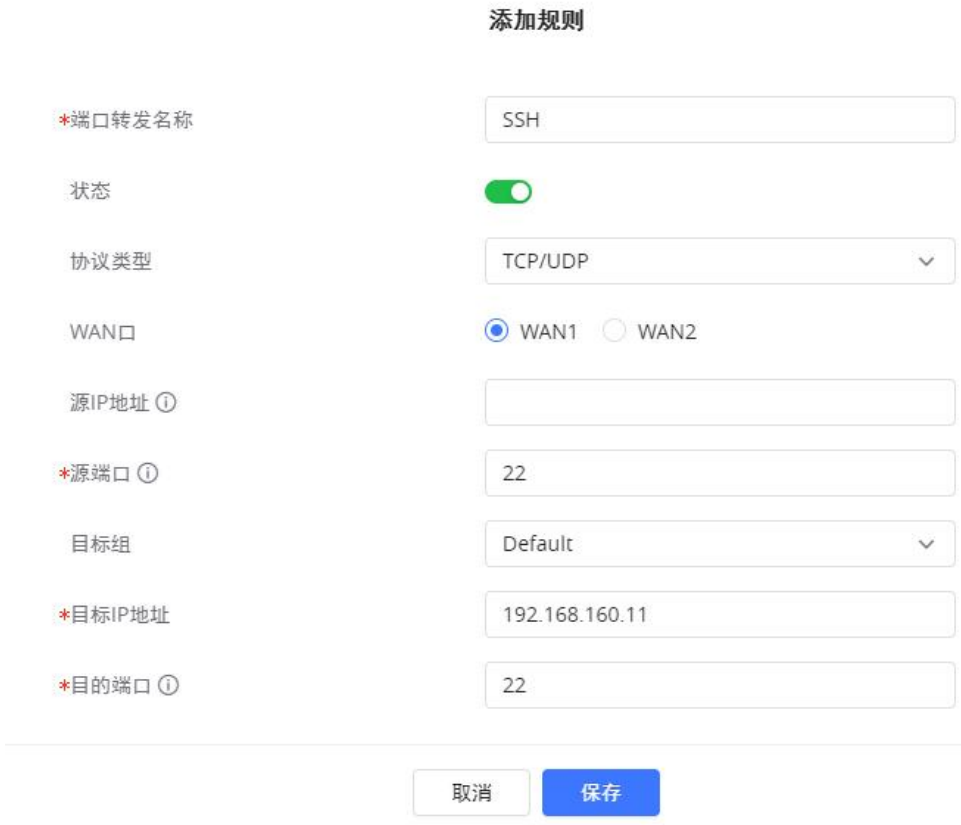


图 62 端口转发

下表对端口转发的各配置进行了解释：

表 20 端口转发

端口转发名称	设置端口转发规则的名称。

协议类型	选择协议类型。可选择 TCP、UDP 或者 TCP/UDP。
WAN 口	选择 WAN 端口。
源 IP 地址	设置外部用户访问此设备的 IP 地址。若不设置，则对应 WAN 口上的任一 IP 地址均可使用。
源端口	路由器提供给广域网的服务端口，可以输入端口号，也可以输入端口范围(如 5-23 的形式)，外部用户通过向该端口发送请求来获取服务。
目标组	选择 VLAN 组。
目标 IP 地址	选择目标 IP 地址。
目的端口	路由器提供给局域网的服务端口，即 LAN 端服务端口。当源端口设置为端口范围时，自动同步源端口范围。

DMZ

用户可以在**外部访问→DMZ** 中进行配置。

GWN70xx 支持 DMZ，在 DMZ 中可以指定要放置在 DMZ 上的主机名 IP 地址。

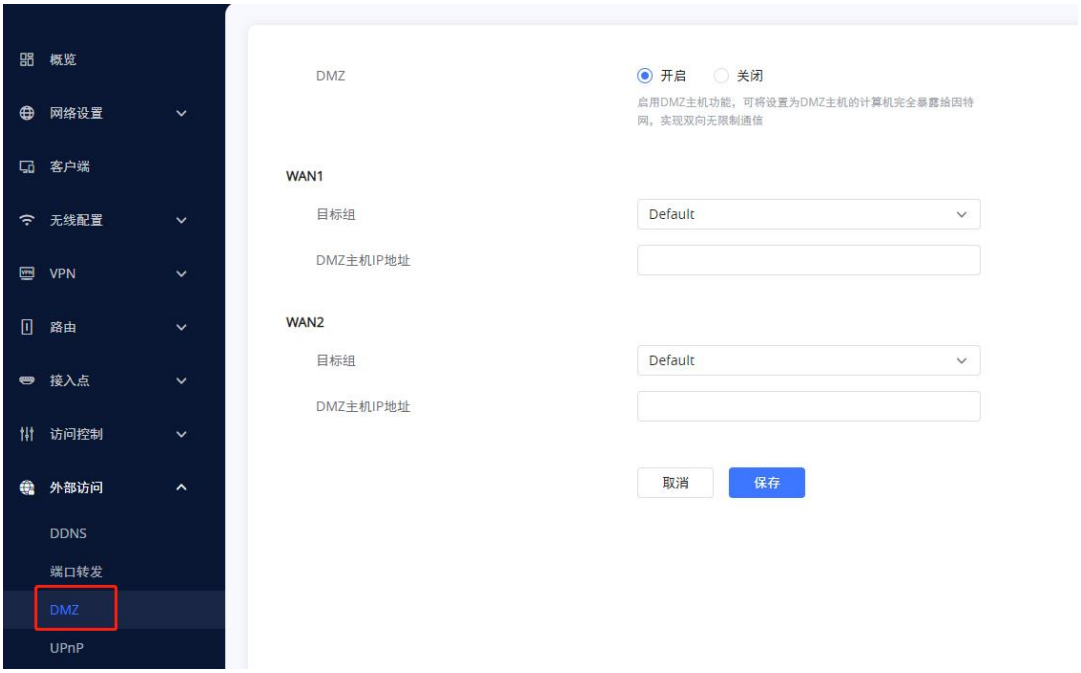


图 63 DMZ

启用 DMZ 主机功能，设置为 DMZ 主机的计算机可以完全暴露于互联网，实现双向无限制通信。

下表对 DMZ 的各配置进行了解释。

表 21 DMZ

DMZ	点击“开启”启用 DMZ。

目标组	选择 VLAN 组。
DMZ 主机 IP 地址	选择目标 IP 地址。

UPnP

GWN70xx 支持 UPnP，使运行在主机上的程序能够自动配置端口转发。
UPnP 允许程序打开 GWN70xx 必要的端口，无需用户干预，无需进行任何检查。
用户可以从 GWN70xx Web GUI→**外部访问→ UPnP** 进行 UPnP 设置。

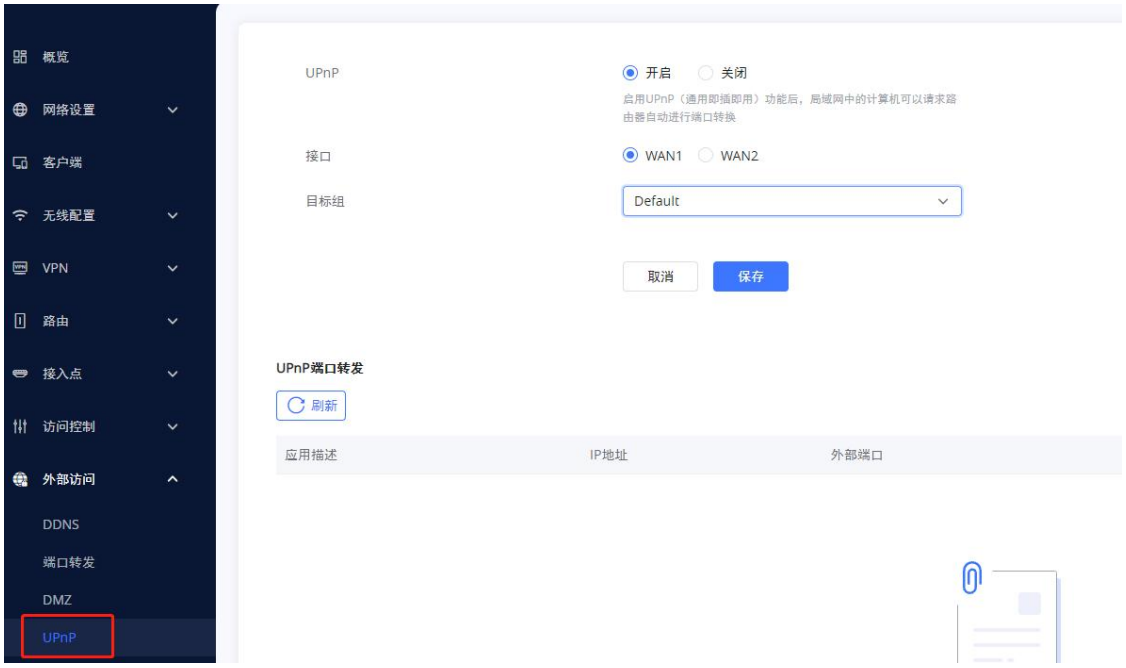


图 64 UPnP

下表对 UPnP 的各配置进行了解释。

表 22 UPnP

UPnP	点击“开启”启用 DMZ。
接口	选择接口。（WAN）
目标组	选择 VLAN 组。

防火墙

防火墙可对每个 WAN 口和 LAN 组设置入局/出局策略，并可对静态、动态 NAT 和 ALG 进行配置。

攻击防御

默认情况下，设备已启用 DoS、TCP SYN Flood、UDP Flood、ICMP Flood 防御以及死亡之 Ping。

图 65 防火墙基础设置

Flush 连接重置：启用此选项并更改防火墙配置后，先前防火墙规则允许的现有连接将被终止。这样，如果新的防火墙规则不允许以前建立的连接，连接将被终止，无法重新连接。如果禁用此选项，即使新规则不允许建立这些连接，也允许现有连接持续到超时。

流量规则

GWN70xx 能够在定制的预定时间内完全控制不同协议的传入/传出流量，并对指定规则（如接受、拒绝和丢弃）采取操作。

用户可以从 GWN70xx Web GUI **防火墙→ 流量规则**进行配置。
以下操作可为配置的协议配置输入、输出和转发规则：

点击 

添加新规则。

点击  编辑规则。

点击  删除规则。

输入规则

GWN70xx 可以过滤网络组或端口 WAN 的输入流量，并应用以下规则：
接收：允许流量通过。
拒绝：将向远端发送一个回复，说明数据包被拒绝。
丢弃：数据包将被丢弃，不会通知远端。

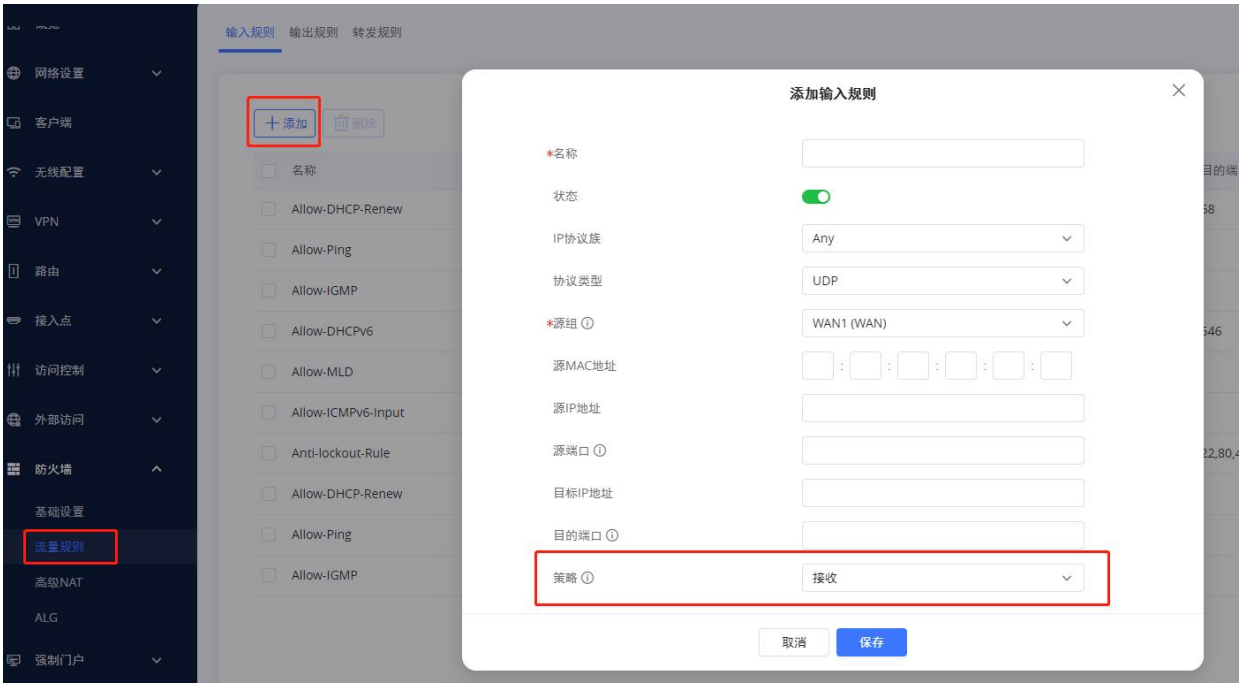


图 66 输入规则

下面的示例为拒绝向 WAN 端口输入的 ICMP 请求，这意味着无论何时 GWN70xx 在 WAN 端口上接收到输入 ICMP 请求时，目标 IP 地址都将收到一条消息，说明目标 IP 地址不可访问。
下图为配置示例：

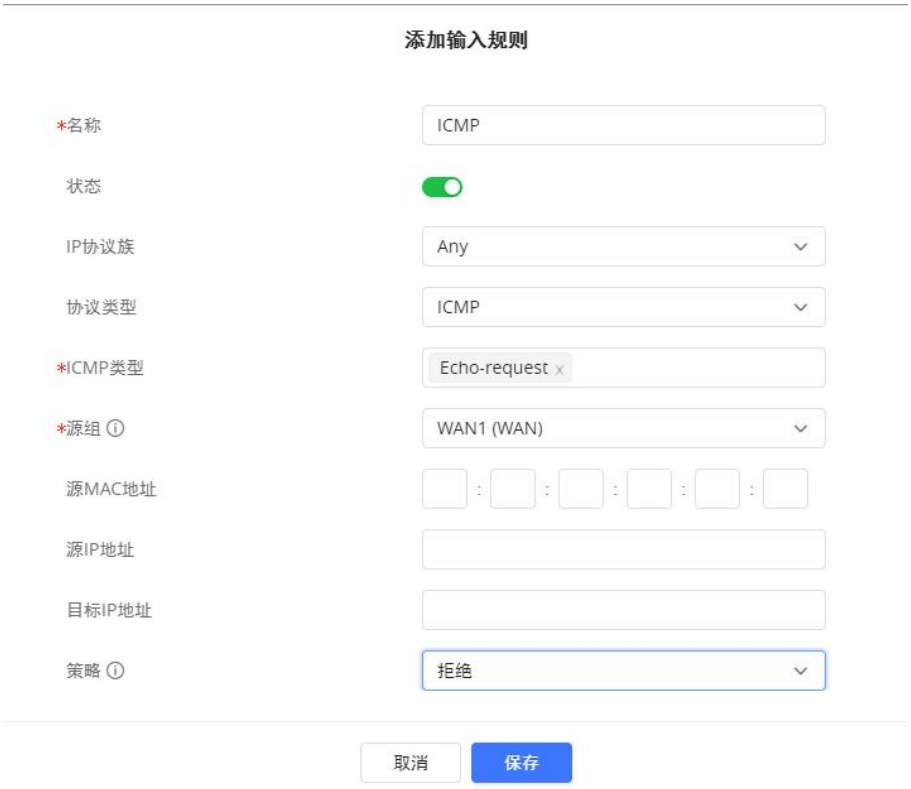


图 67 输入规则示例

输出规则

GWN70xx 可以过滤网络组或端口 WAN 的输出流量，并应用以下规则：

接收：允许流量通过。

拒绝：将向远端发送一个回复，说明数据包被拒绝。

丢弃：数据包将被丢弃，不会通知远端。

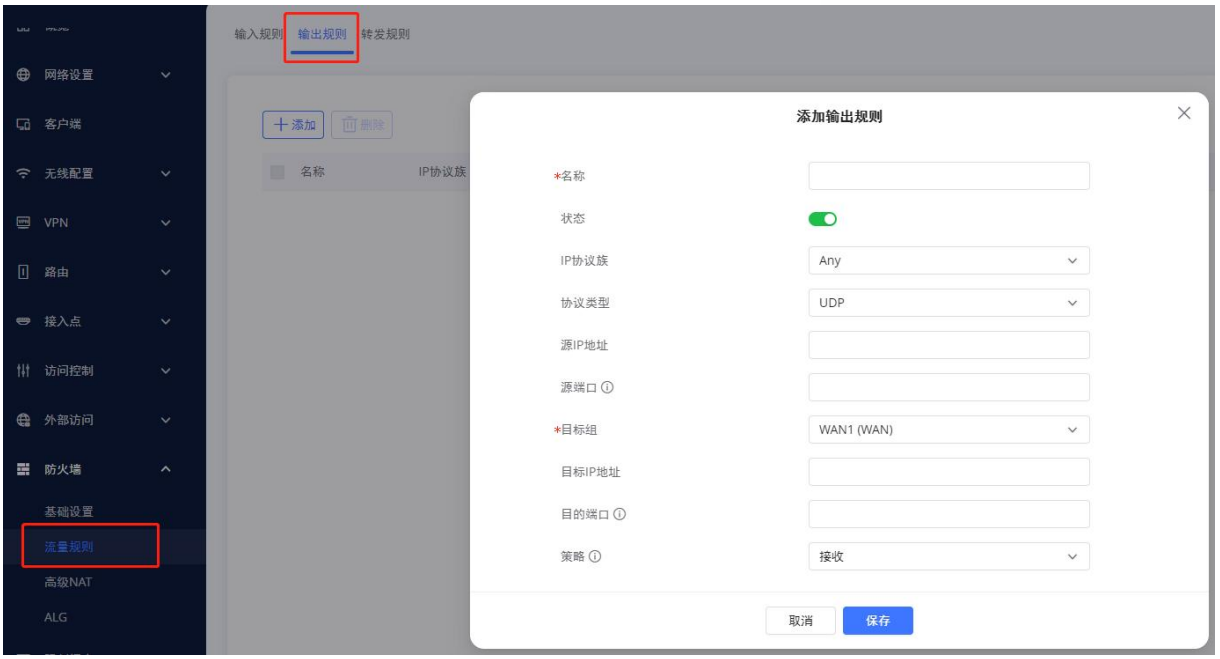


图 68 输出规则

下面的示例将拒绝从 GWN70xx 到默认（VLAN）的每个传出 ICMP 的请求，这意味着无论何时 GWN70xx 从另一个网络组接收到 ICMP“回送请求”，都将被拒绝。

下图为配置示例：

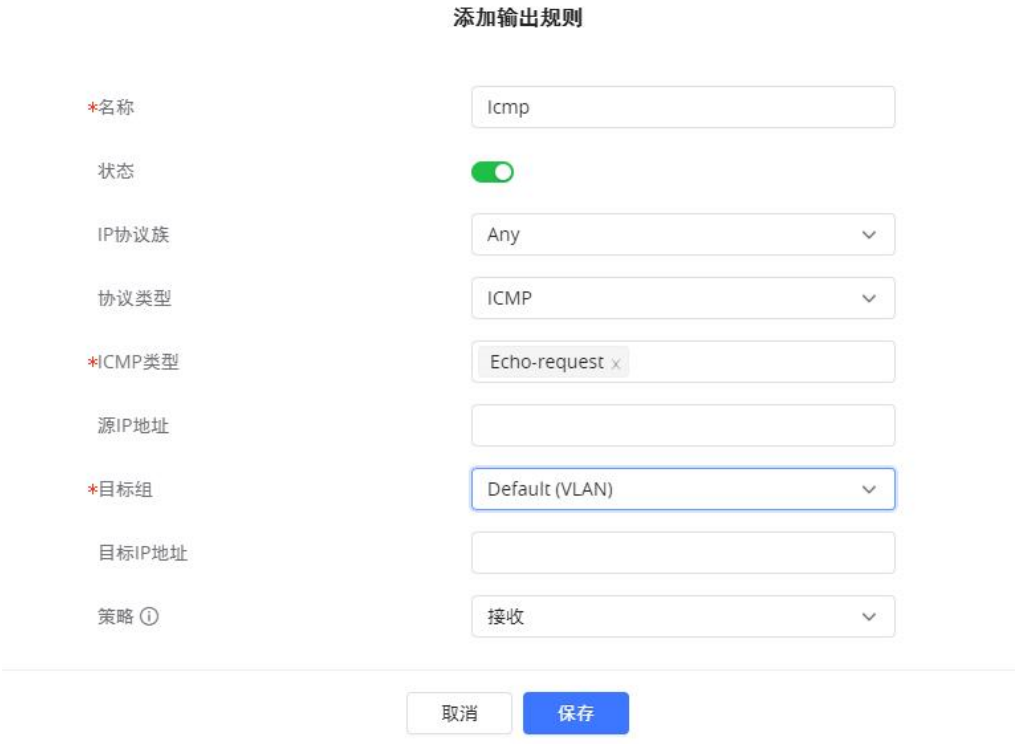


图 69 输出规则示例

转发规则

GWN70XX 可以让不同的组和接口之间进行通信。

图 70 转发规则

高级NAT

防火墙高级 NAT 页面可以配合静态和动态 NAT。

SNAT

用户可以对 SNAT 进行以下操作：

点击 

添加新 SNAT。

点击  编辑 SNAT。

点击  删除 SNAT。

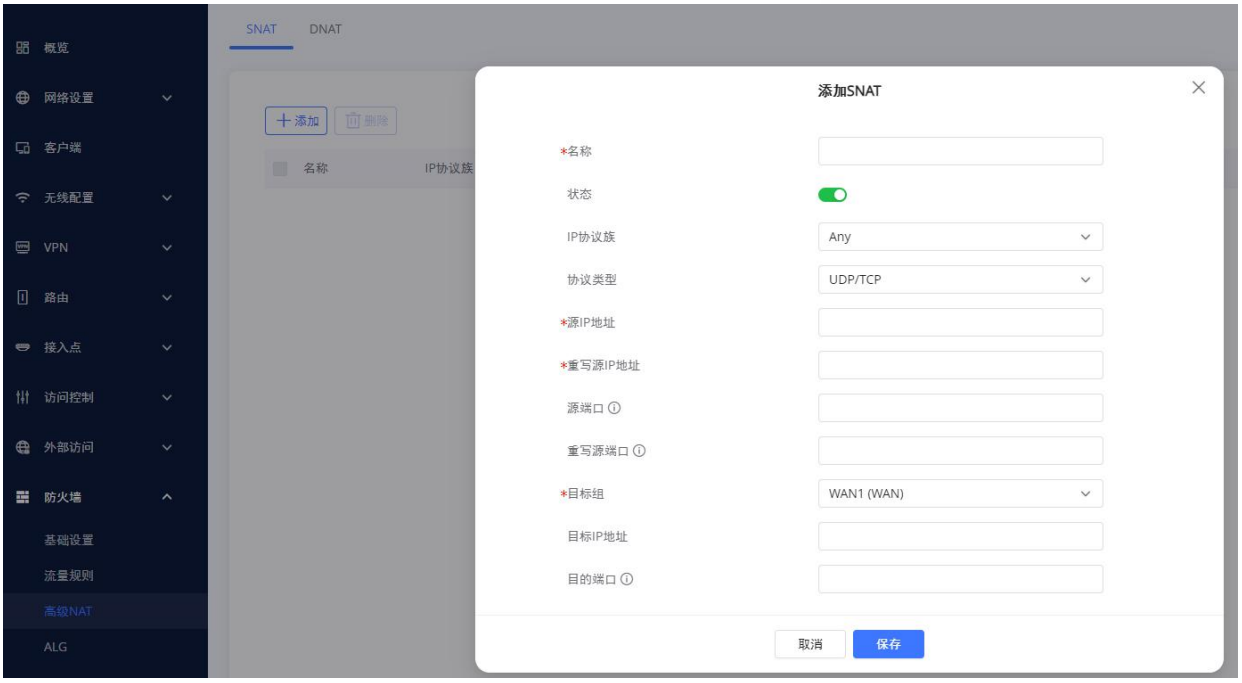


图 71 SNAT

以下对 SNAT 配置项进行了说明：

表 23 SNAT

名称	指定 SNAT 条目的名称
IP 协议族	选择 IP 版本，有连个选择项：IPv4 和 Any。
协议类型	从下拉列表中选择一个协议，可用选项包括：UDP/TCP、UDP、TCP 和所有。
源 IP 地址	设置源 IP 地址。
重写源 IP 地址	设置重写源 IP 地址。源组中数据包的源 IP 地址将更新为此配置的 IP。
源端口	合理范围为 1~65535。
重写源端口	合理范围为 1~65535。
目标组	为目标组选择 WAN 接口或 VLAN。
目标 IP 地址	设置目标 IP 地址。
目的端口	合理范围为 1~65535。

DNAT

用户可以对 DNAT 进行以下操作：

点击 

添加新 DNAT。

点击 编辑 DNAT。

点击 删除 DNAT。

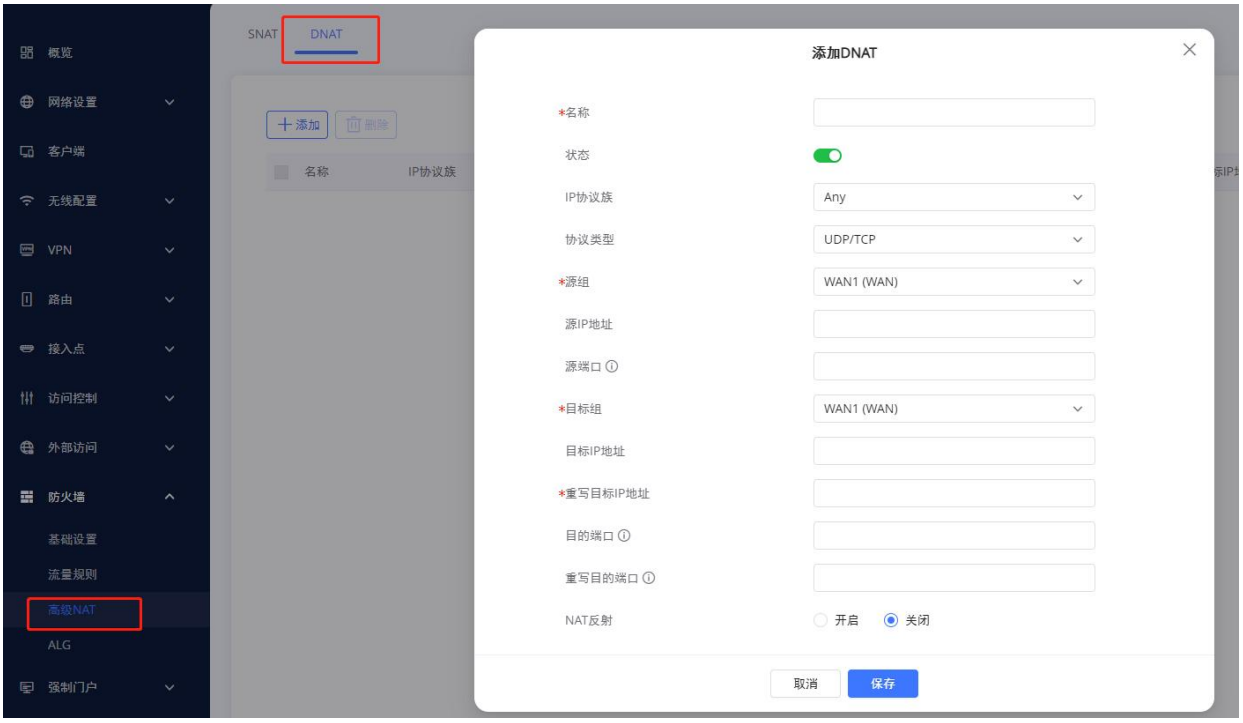


图 72 DNAT

以下对 SNAT 配置项进行了说明：

表 24 DNAT

名称	指定 DNAT 条目的名称
IP 协议族	选择 IP 版本，有连个选择项：IPv4 和 Any。
协议类型	从下拉列表中选择一个协议，可用选项包括：UDP/TCP、UDP、TCP 和所有。
源组	为“源组”选择 WAN 接口或 LAN 组，或选择“全部”。
源 IP 地址	设置源 IP 地址。
源端口	合理范围为 1~65535。
目标组	选择 WAN 接口或 LAN 组作为目标组，或选择全部。确保目标组和源组不同，以避免冲突。
目标 IP 地址	设置目标 IP 地址。
重写目标 IP 地址	设置重写目标 IP 地址。
目的端口	合理范围为 1~65535。
重写目的端口	设置重写目的端口。

NAT 反射	点击“开启”启用 NAT 反射。
NAT 反射源	选择内部或外部 NAT 反射源。

ALG

ALG 代表应用层网关。其目的是通过检查 VoIP 流量（数据包）并在必要时对其进行修改来防止路由器防火墙造成的一些问题。导航到 Web GUI→ **防火墙→ ALG** 激活 ALG。

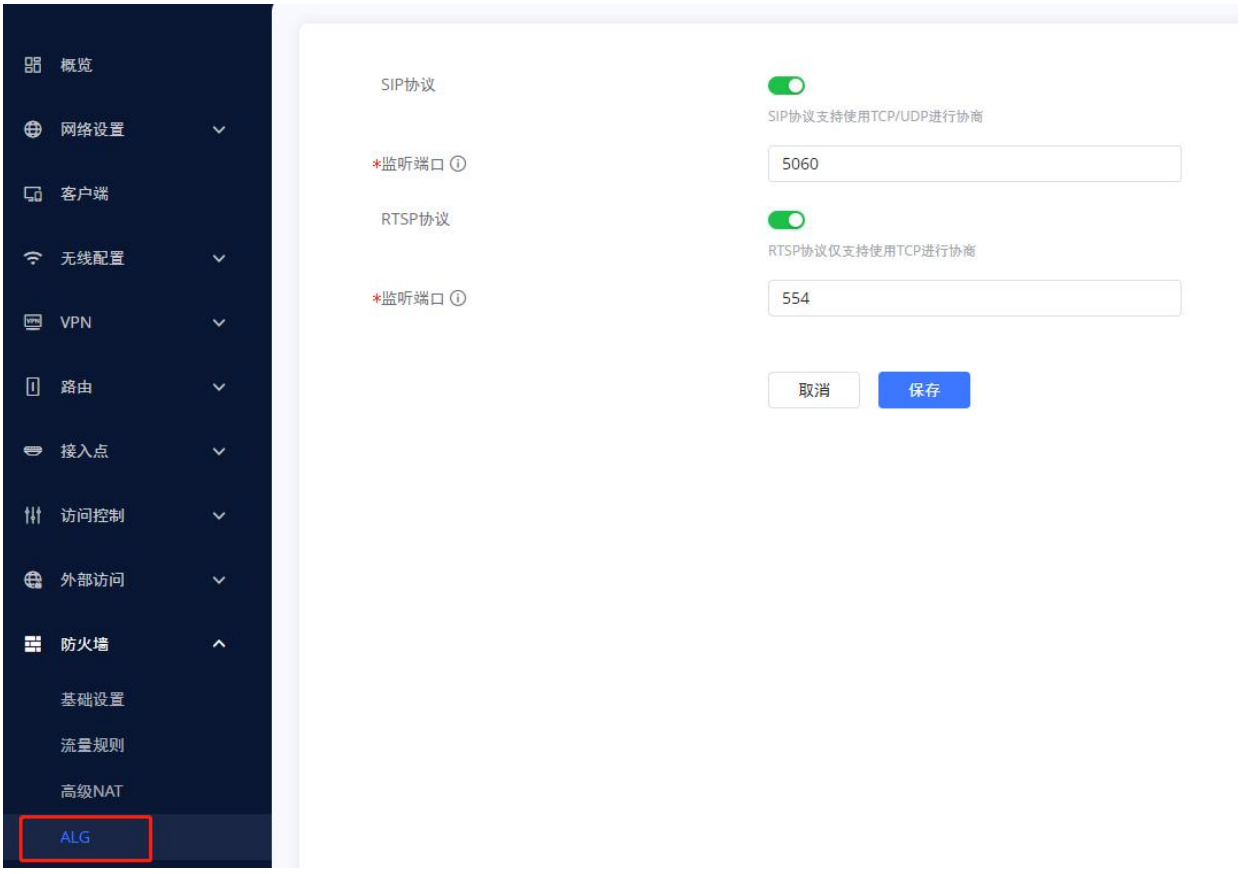


图 73 ALG

强制门户

GWN70XX 上的强制网络门户功能可以自定义登录页面（网页），当尝试访问 Internet 时，该登录页面将显示在 Wi-Fi 客户端的浏览器上。 连接到 GWN70XX AP 后，Wi-Fi 客户端将被迫查看该登录页面并与之交互，然后才能获得 Internet 访问权限。
强制网络门户功能可以在 GWN70XX 网页中的“强制门户”下配置。

策略

用户可以在此界面自定义策略列表。.

点击  添加新策略。

点击  编辑策略。

点击  删除策略。

策略配置页面允许添加多个强制门户策略，这些策略将应用于 SSID，并包含不同身份验证类型的选项，

管理员可以使用内部或外部启动页面。

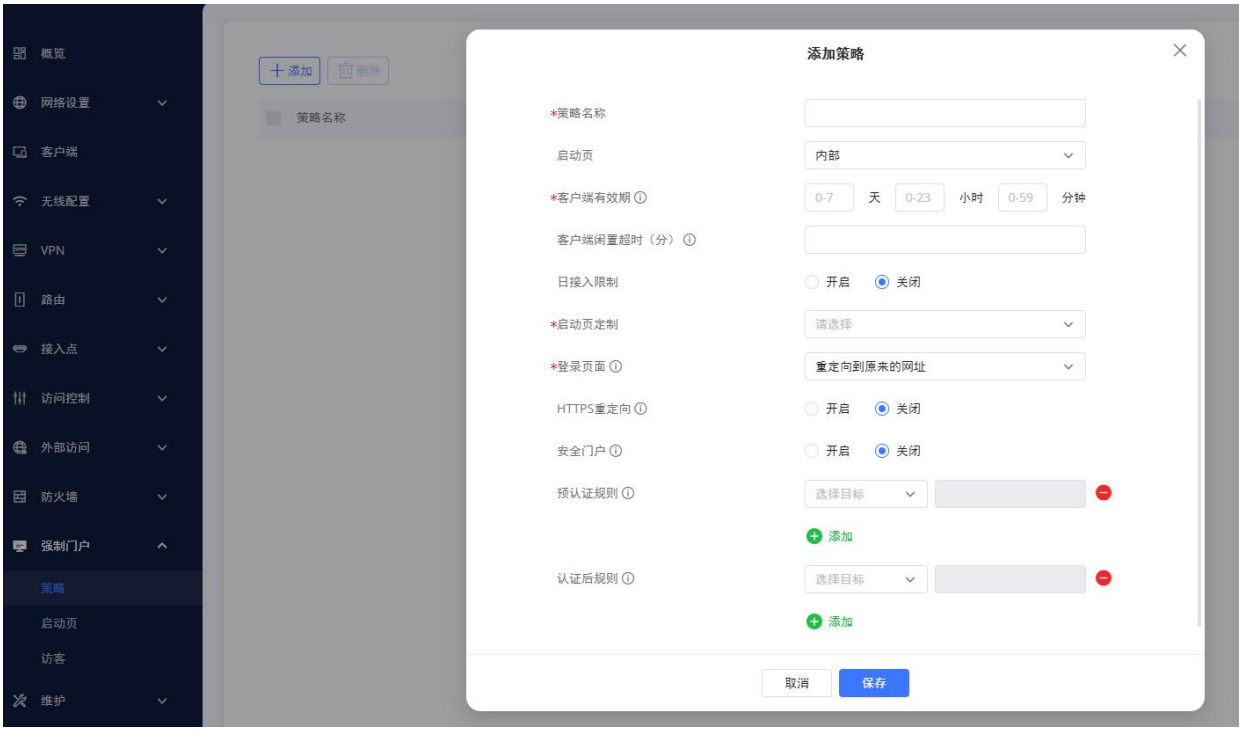


图 74 策略页面

启动页

启动页可以让用户通过易于配置的菜单生成自定义启动页面，当尝试连接到 Wi-Fi 时，该页面将显示给用户。

在此菜单上，用户可以创建多个初始页面，并将每个初始页面分配给单独的强制门户策略，以强制选择身份验证类型。

生成工具提供了一种直观的“所见即所得”方法，用户可以使用一个非常丰富的操作工具来定制强制门户。

用户可以设置以下内容：

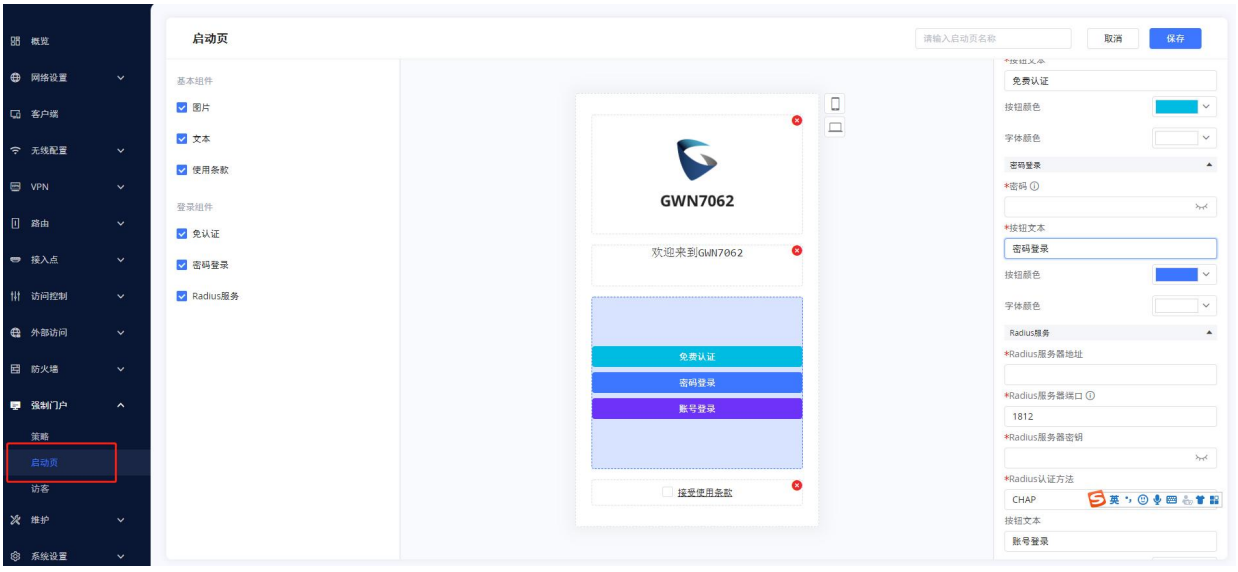
认证类型：从支持的身份验证方法（简单密码、Radius 服务器、免费）中添加一种或多种方式。

启动图片（企业 Logo）。

自定义布局和背景颜色。

自定义使用条款文本。

可视化预览移动设备和笔记本电脑界面。



访客

本部分列出了通过强制网络门户连接或尝试连接到 Wi-Fi 的客户端。

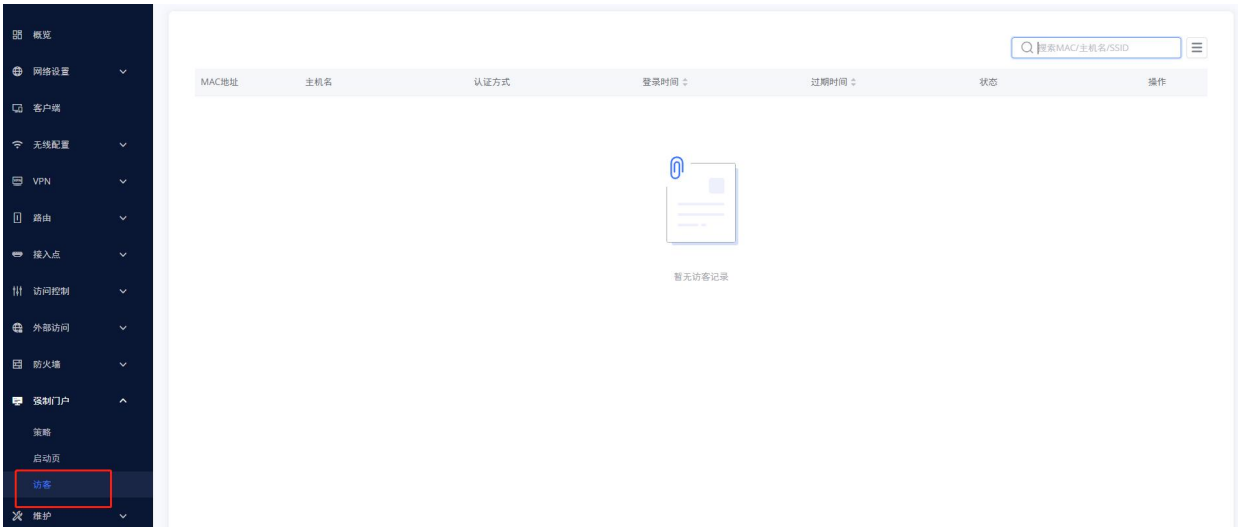


图 75 访客

点击 按钮取消认证，客户端需要重新认证才能再连接网络。

点击 按钮自定义要在页面上显示的项目。 支持以下项目：

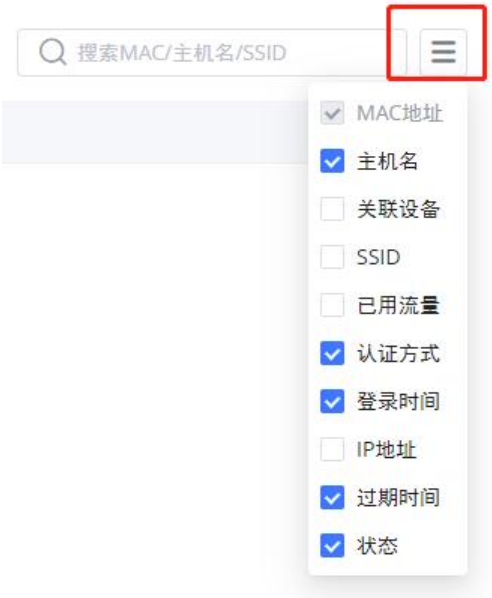


图 76 访客-选项

访问控制

GWN70XX 可以让用户启用黑名单来阻拦客户端和网站，也可以给每个 SSID 和客户端限制带宽。

黑名单

黑名单功能可以让用户从可用客户端中拦截无线客户端，也可以手动添加 MAC 地址拦截客户端。
用户可以在 WEB GUI 的**访问控制→黑名单**中配置。

图 77 黑名单

站点控制

站点控制允许系统管理员阻止设备对某些域的 DNS 查询。此功能可用于阻止广告软件网站和恶意软件网站，也可用于阻止流行的社交媒体网站（Facebook、YouTube 等）。

用户可以在 WEB GUI 的**访问控制→站点控制**中配置。

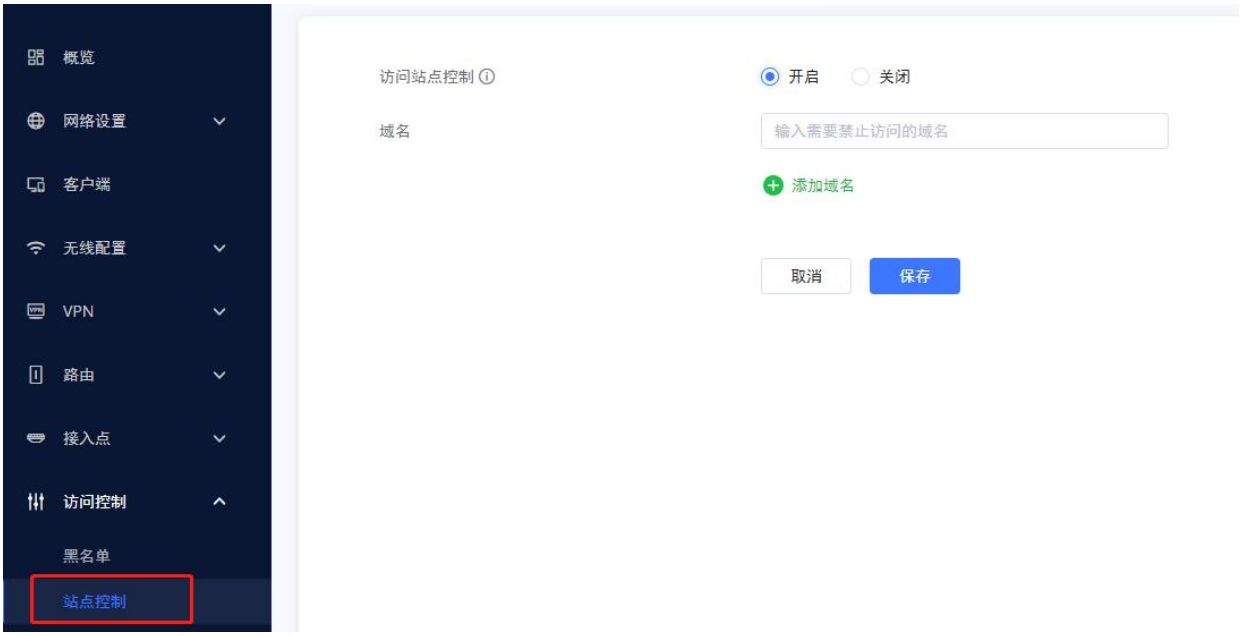


图 78 站点控制

带宽限制

带宽规则允许用户限制每个 SSID 或客户端（MAC 地址）的带宽利用率。

每个客户端

进入客户端页面，点击编辑客户端，然后给无线客户端定义名称和最大上传和下载速率。

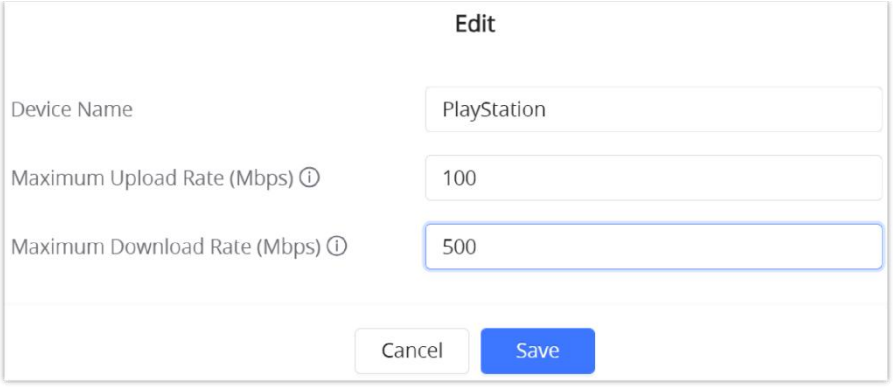


图 79 客户端带宽限制

每个 SSID

进入无线配置→SSIDs，点击编辑 SSID，在 Wi-Fi 设置标签中进入“高级”，设置 SSID 的最大上传和下载速

率。

图 80 SSID 带宽限制

维护和故障排查

GWN70xx 为维护和调试提供了多种工具和选项，来帮助排除故障并监控 GWN70xx 资源。

维护

GWN70XX 有很多工具来帮助维护设备。

基础设置

用户可以在**系统设置→基础设置**中修改国家/地区和设置设备重启时间。

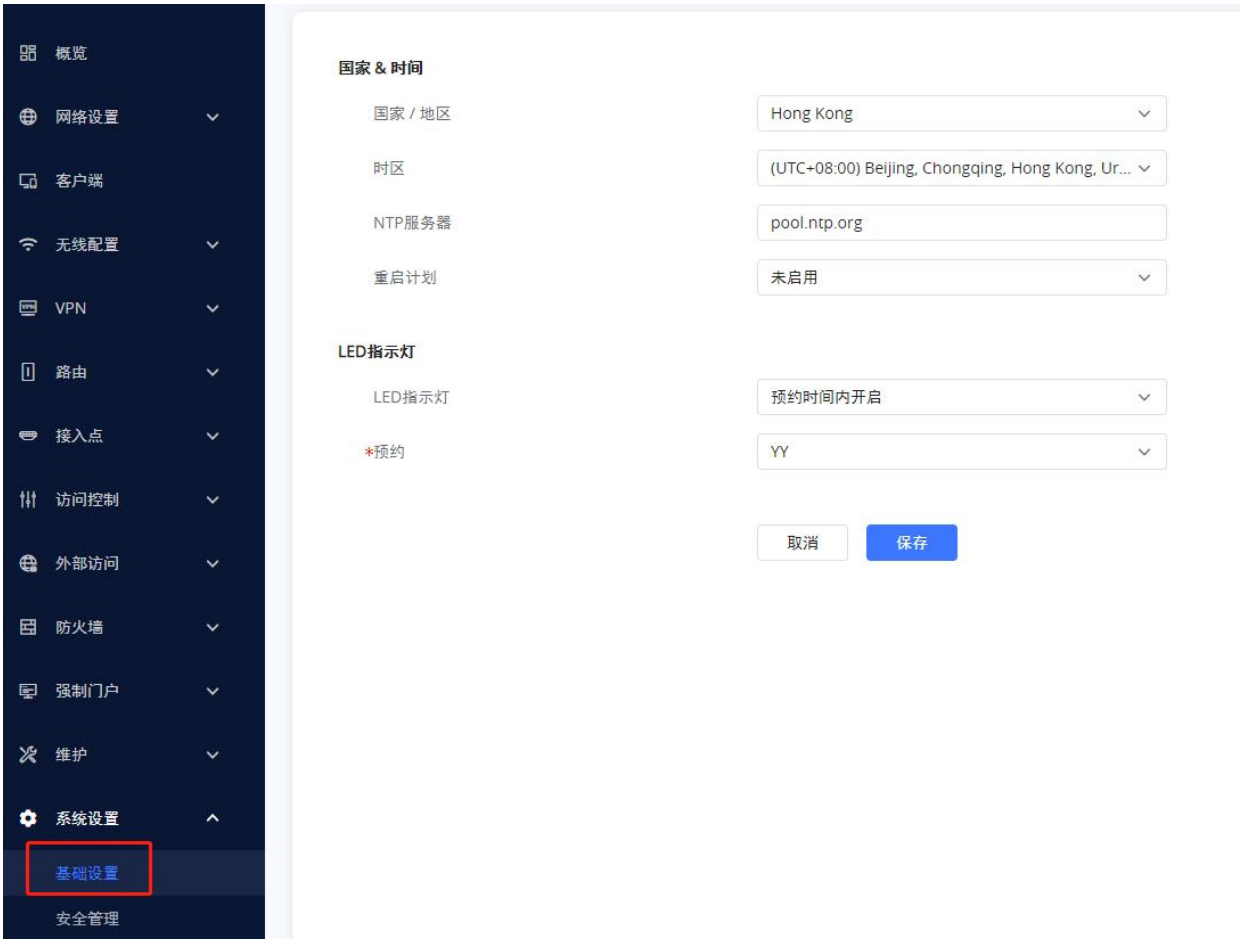


图 81 基础设置

TR-069

注意：如果启用，GWN70xx 路由器无法由 GWN Cloud 管理，也无法继续管理 GWN76xx 接入点。

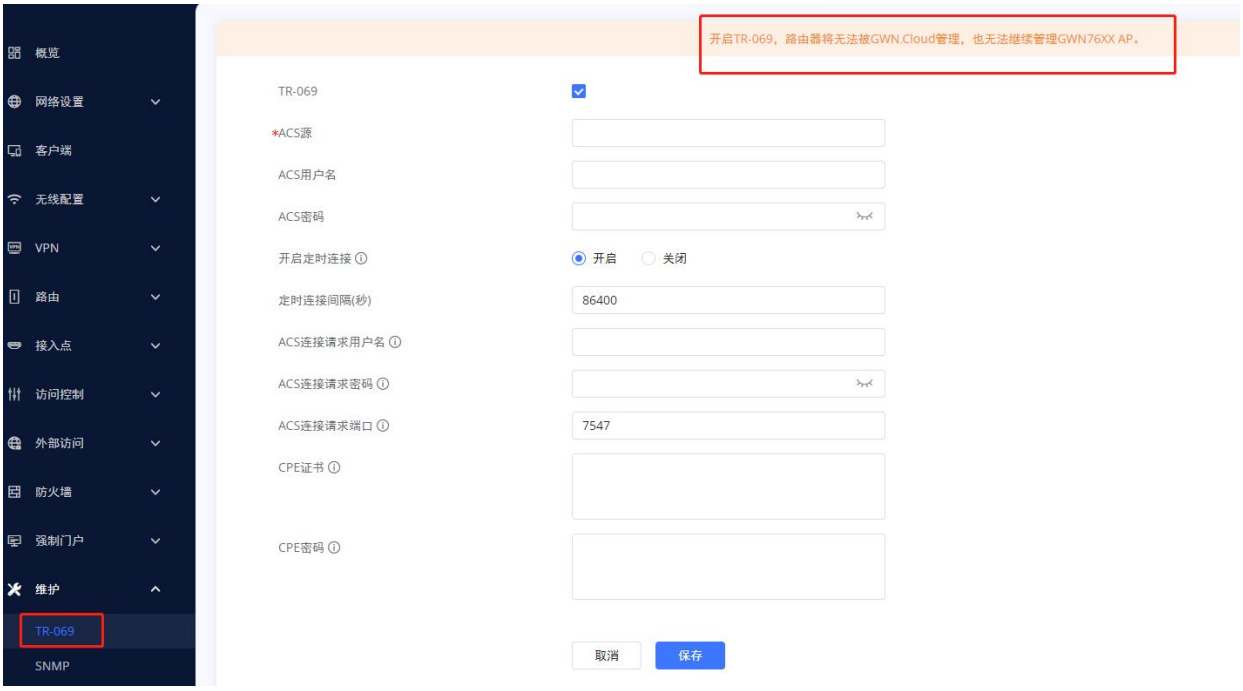


图 82 TR-069

SNMP

GWN70xx 支持 SNMP（简单网络管理协议），该协议广泛用于网络管理。

要配置 SNMP 设置，请转到 GWN70xx Web GUI→**维护→ SNMP**，在此页面中，用户可以启用 SNMPv1、SNMPv2c 或 SNMPv3，并配置所有必要的参数。

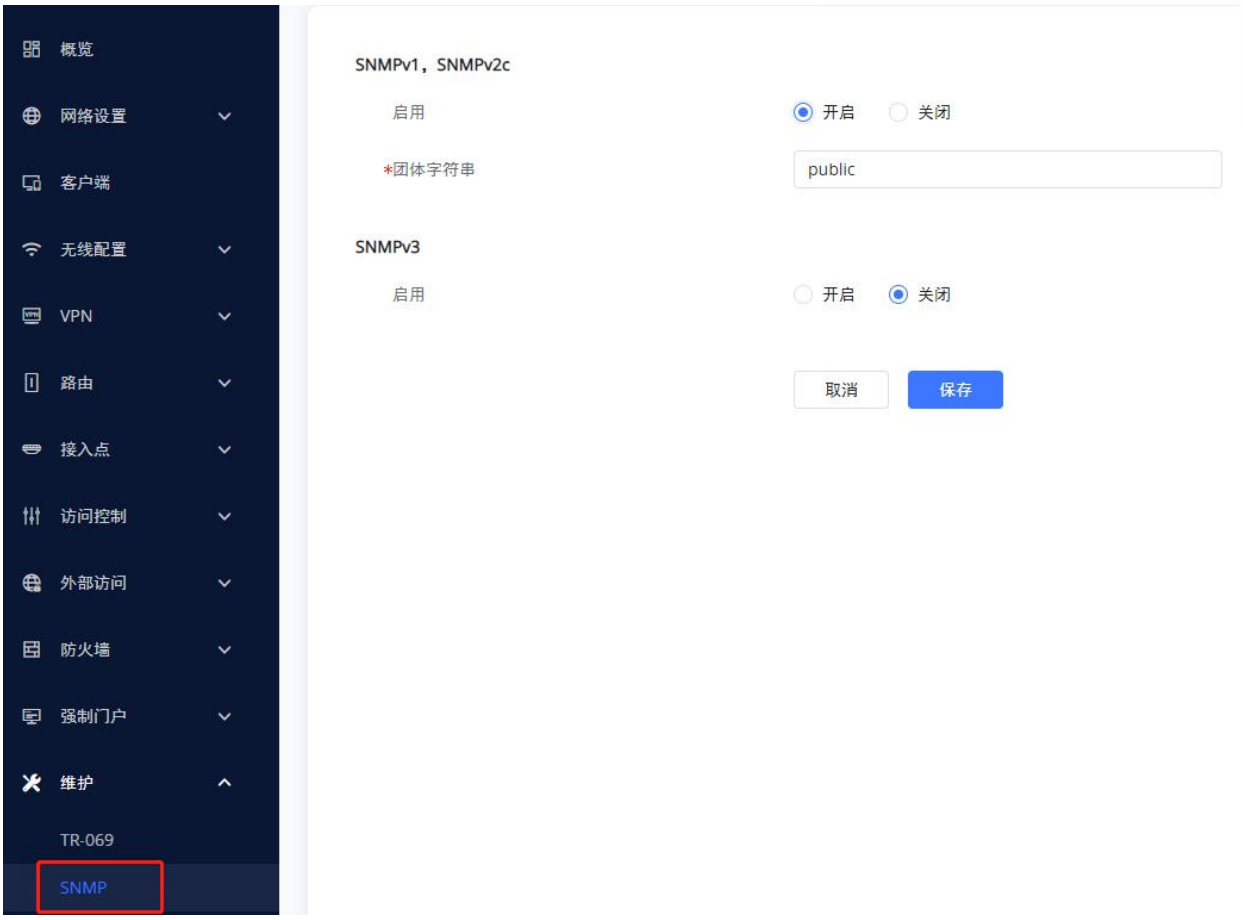


图 83 SNMP

安全管理

在 Web UI→ **系统设置→ 安全管理**下，用户可以更改登录密码并激活 web 服务，例如设置用于 web WAN 端口访问的 HTTPS 端口 443，以及启用 SSH 远程访问。

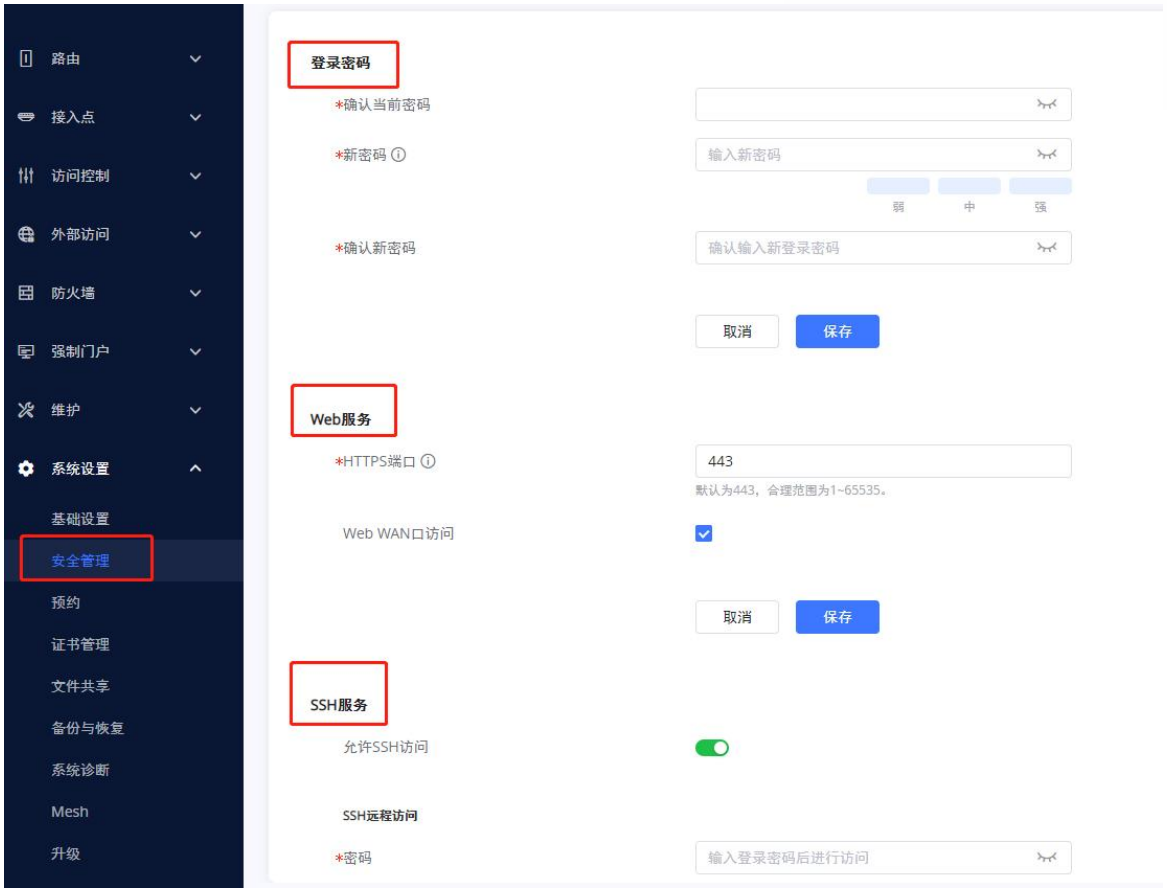


图 84 安全管理

Debug

GWN70xx 的 Web GUI 上提供了许多调试工具，用于检查 GWN70xx 的服务和网络的状态并进行故障排除。用户可以在**系统设置→系统诊断**中进行调试。

Ping/路由跟踪

Ping 和路由跟踪是一种很有用的调试工具，可用于验证网络（WAN 或 LAN）上其他客户端的可达性。GWN70xx 为 IPv4 和 IPv6 协议提供 Ping 和路由跟踪工具。

图 85 PIng/路由跟踪

core 文件

当设备发生 Crash 事件时，它将自动生成一个 core 转储文件，技术团队可以使用该文件进行调试。

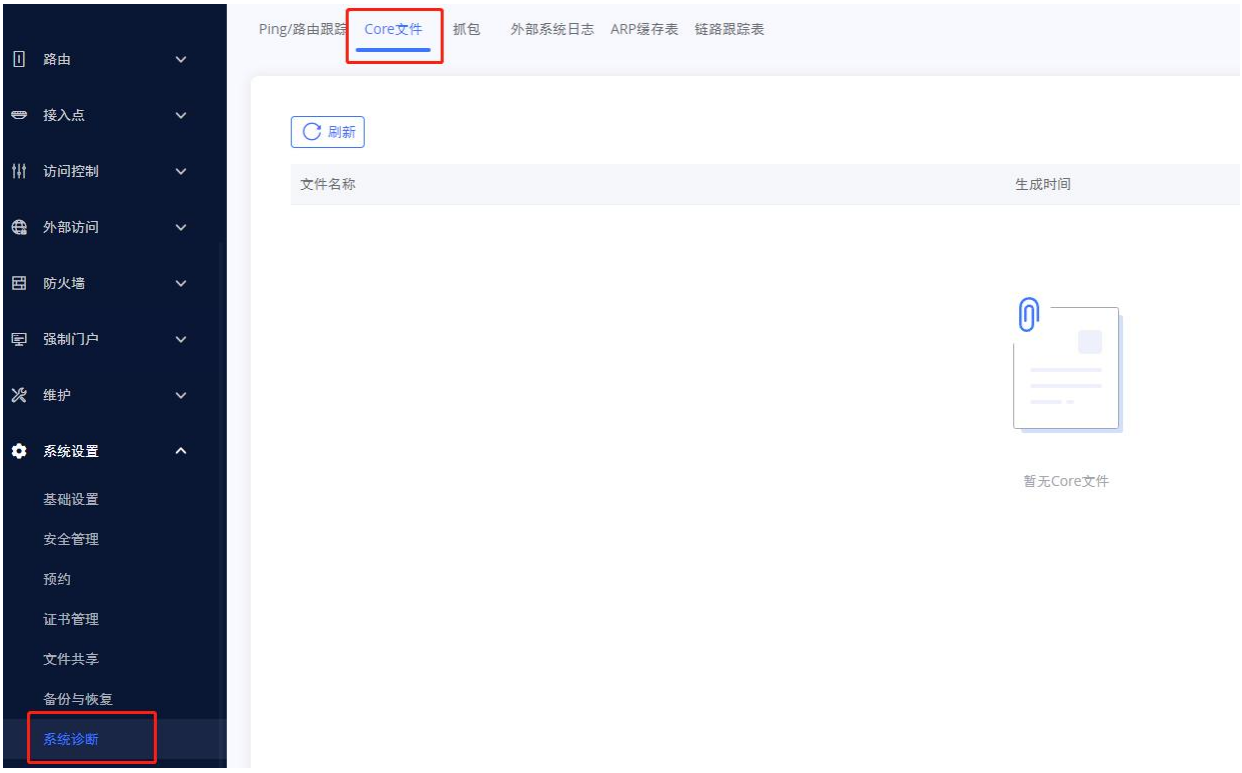


图 86 core 文件

抓包

该部分用于从 GWN70xx 接口（WAN 端口和网络组）捕获数据包跟踪，以便进行故障排除或监控。用户还可以根据 MAC 地址或 IP 地址进行捕获，用户可以单击 开始抓包 立即开始抓包并下载文件（CAP 格式）。

图 87 抓包

外部系统日志

GWN70xx 路由器支持在 Web GUI 下将 Syslog 信息转储到远程服务器 。

用户可以在**系统设置→ 系统诊断→ 外部系统日志**中进行配置。

输入 Syslog 服务器主机名或 IP 地址，并选择 Syslog 信息的级别。系统日志有九个级别： None, Emergency, Alert, Critical, Error, Warning, Notice, Information 和 Debug。

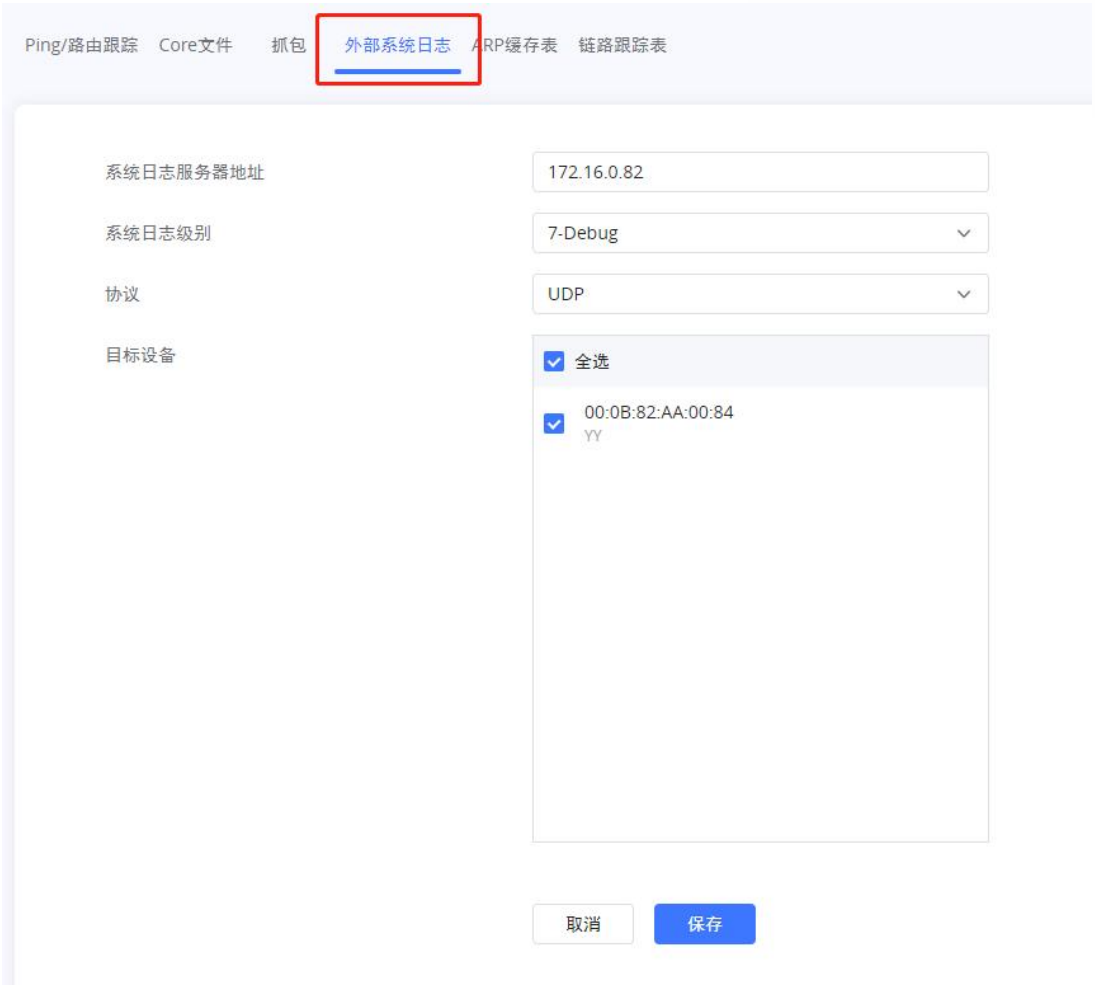


图 88 外部系统日志

预约

用户可以使用预约配置菜单来设置 GWN 功能的特定时间表，以灵活地在指定的日期和时间打开/关闭所选功能。

预约可应用于各种 AP 活动中，如 LED 灯时间表、带宽规则应用时间、黑名单应用时间等。

请按以下步骤设置预约：

1. 进入**系统-预约**界面，点击 

。
2. 选择预约的时间段，输入预约的名称（例如：office hours）。
3. 用户可选择设置周期预约或特定时间预约（以特定日期为例），如果周期预约和特殊日期在同一天同时设置，则特殊日期生效，周期预约取消。
4. 单击保存以保存预约。

创建的预约列表将如下图所示。 可以编辑或删除每个预约：

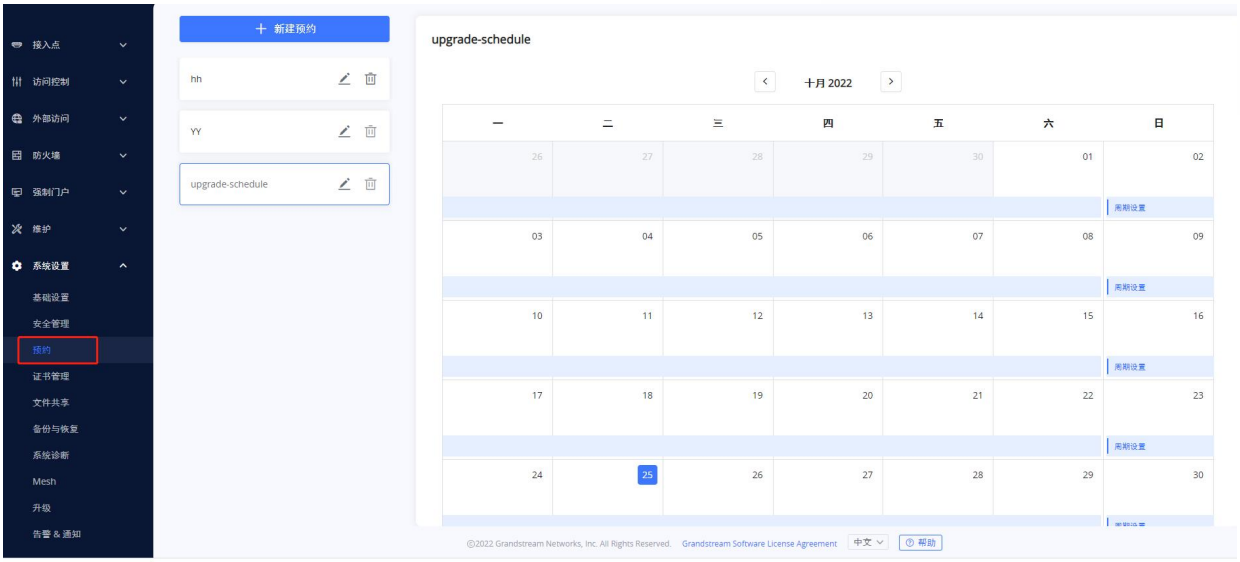


图 89 预约

LED

GWN70XX 接入点系列还支持 LED 预约功能。 此功能用于在客户方便时设置 LED 亮起和熄灭的时间。这可能很有用，例如当 LED 在一天中的某些时段让人觉得干扰时，使用 LED 预约可以设置时间，令 LED 在特定时间后如在夜间关闭，其他时间保持 Wi-Fi 服务，客户端无需关闭 AP。

用户可以在**系统设置→基础设置**用设置 LED。

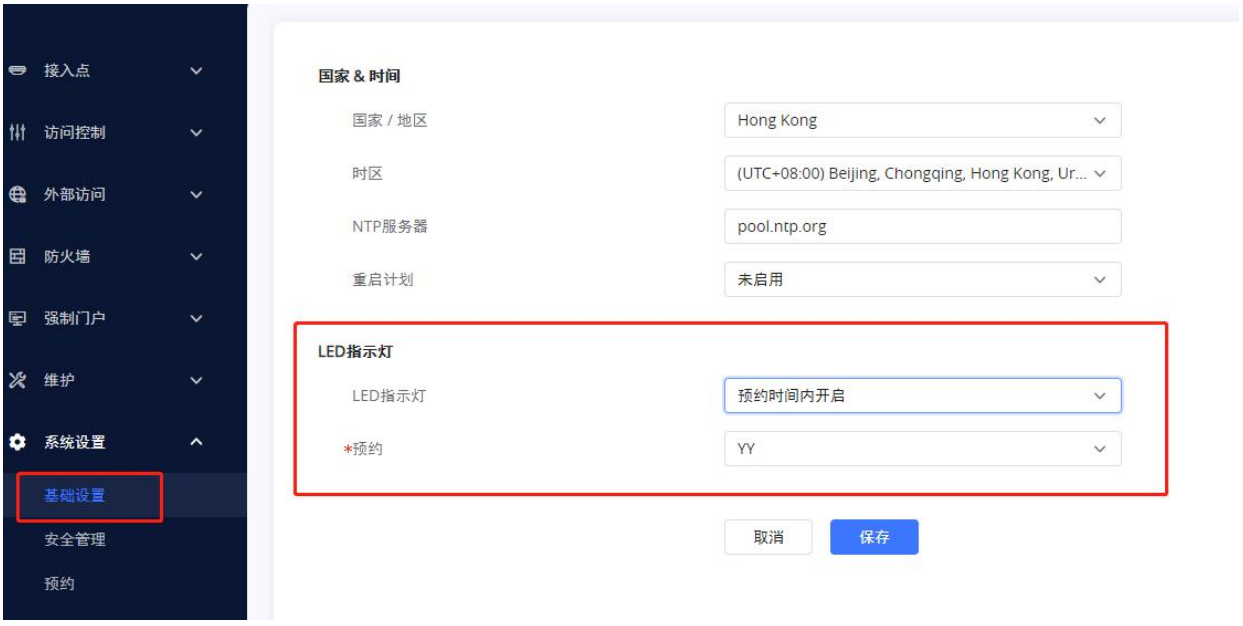


图 90 LED

文件共享

GWN70xx 有一个 USB 端口，也可用于文件共享，要启用文件共享，请转到**系统设置→ 文件共享**。

图 91 文件共享

升级和部署

升级固件

GWN70XX 可以远程或本地升级到新的固件版本。 本节介绍如何升级您的 GWN70XX。

GWN70XX 可以通过 TFTP/HTTP/HTTPS 升级，方法是配置 TFTP/HTTP/HTTPS 服务器的 URL/IP 地址并选择下载方式。 配置 TFTP、HTTP 或 HTTPS 的有效 URL； 服务器名称可以是 FQDN 或 IP 地址。

有效 URL 示例：
firmware.grandstream.com/BETA
192.168.5.87
可以通过以下方式访问升级页面：
Web GUI→系统设置→维护→升级

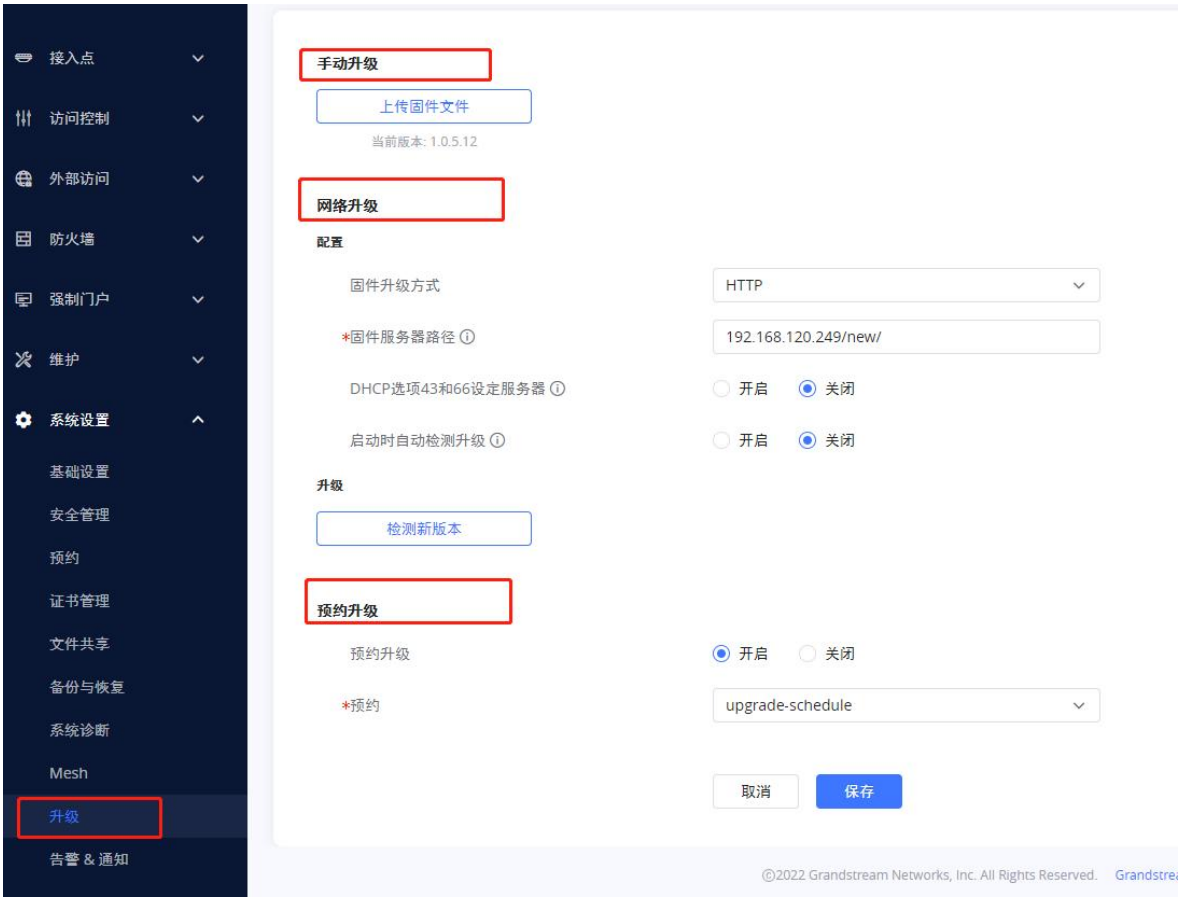


图 92 升级

配置与恢复

GWN70XX 配置可以本地备份。 备份文件将用于在必要时恢复 GWN70XX 上的配置，或恢复出厂。

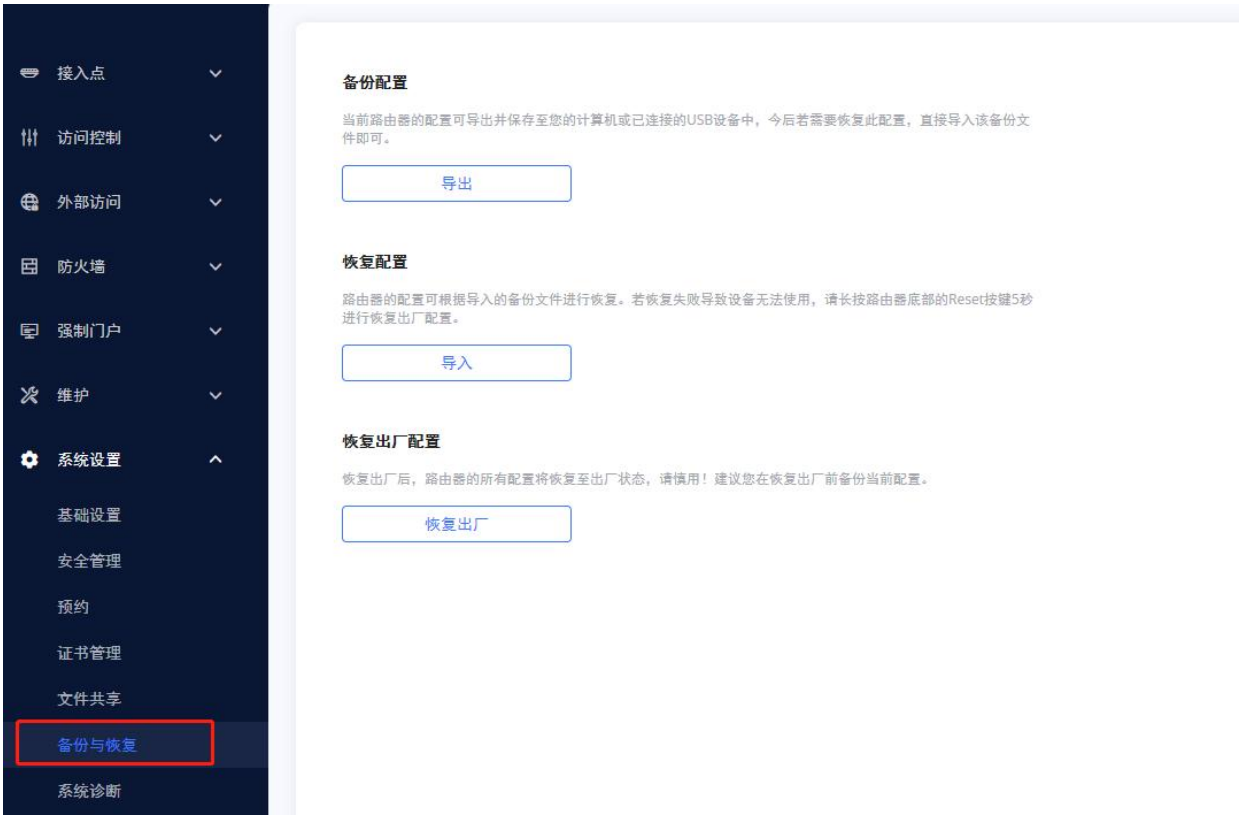


图 93 备份与恢复

重启

用户可以在 Web 页面右上角点击 

按钮重启设备。

系统日志

在 GWN70XX 上，用户可以将 syslog 信息转储到**Web GUI-系统-维护-升级**下的远程服务器。 输入系统日志服务器主机名或 IP 地址并选择系统日志信息的级别。 提供八个级别的系统日志：Emergency, Alert, Critical, Error, Warning, Notice, Information and Debug。

体验 GWN70XX Wi-Fi 接入点

请访问网页：http://www.grandstream.cn 以获取有关产品最新的固件版本、附加功能、常见问题解答、文档和新产品发布消息。

强烈推荐您通过产品相关文档、常见问题解答和论坛获取产品使用过程中常见问题的解答。如果您在潮流网络认证合作伙伴或经销商处购买了我们的产品，请直接联系他们提供直接支持。

我们的技术支持人员都是经过专业训练的，随时准备为用户回答相关问题。请联系我们的技术人员或在线提交问题反馈，获取进一步支持。

再次感谢您使用潮流 GWN70XX Wi-Fi 接入点，它一定会给您的工作和个人生活带来便利。