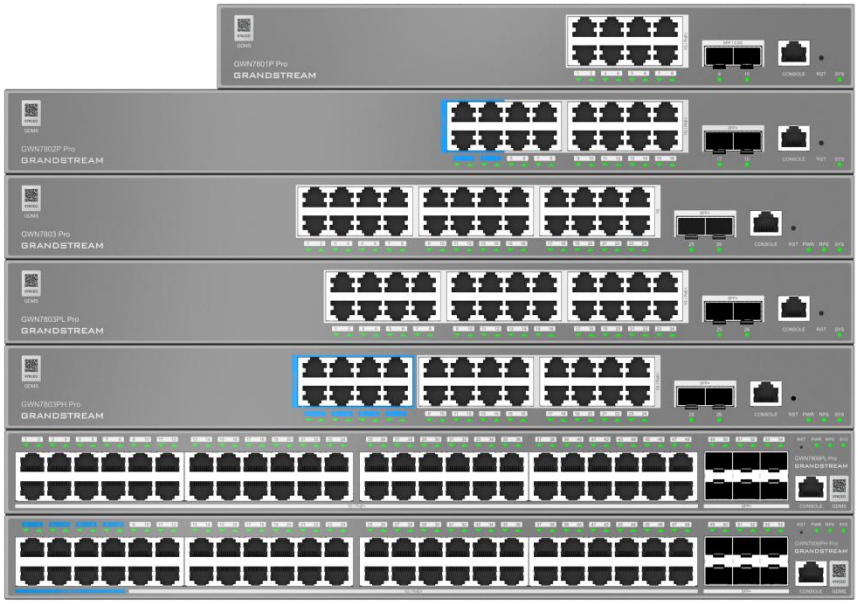
深圳市潮流网络技术有限公司

GWN7800 Pro 系列 L2++网管交换机

用户手册



技术支持

深圳市潮流网络技术有限公司为客户提供全方位的技术支持。您可以与本地代理商或服务提供商联系，也可以与公司总部直接联系。

地址：深圳市南山区科技园北区酷派大厦 C 座 14 楼

邮编：518057

网址：http://www.grandstream.cn

客服电话：0755-26014600

客服传真：0755-26014601

技术支持热线：4008755751

技术支持论坛：http://forums.grandstream.com/forums

网上问题提交系统：http://www.grandstream.com/support/submit-a-ticket

商标注明

和其他潮流网络商标均为潮流网络技术有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

图目录

表目录

更新日志

本文主要介绍了 GWN7800 Pro 系列网管交换机新老版本交替的重大更新，列出了如下新功能。本文没有记录变动或编辑小的更新。

固件版本 1.0.15.211

- 初始版本

欢迎

GWN780x Pro系列是面向中小企业的二层管理型网络交换机，适用于需要可扩展、安全且高性能网络并且管理简便的场景。

每款型号均提供高速千兆以太网连接，并配有2.5G SFP或SFP+上行端口，交换容量高达216Gbps，以满足苛刻的业务需求。

GWN780x Pro系列中所有型号都支持先进的VLAN以实现灵活和复杂的流量分段，支持先进的QoS以实现网络流量的优先级，支持IGMP/MLD Snooping以实现网络性能优化，并支持针对潜在攻击的全面安全功能。PoE型号支持提供智能动态PoE输出，为IP电话、IP摄像头、Wi-Fi接入点和其他PoE端点供电。GWN780x Pro系列可以通过多种方式进行管理，支持便捷化智能WEB管理，可视化端口配置，页面简单易操作。同时支持潮流网络GDMS Networking云管理和GWN Manager管理平台，还支持被GWN路由器管理，以及CLI命令行配置界面。GWN780x Pro系列结合了企业级性能、强大的安全性和灵活的管理功能，提供了一个完整的交换解决方案，非常适合现代商业环境。

产品概述

技术规格

下表为 GWN780x Pro 系列网管交换机的所有技术参数，包括硬件参数和软件参数。

表 1 GWN780x Pro 系列技术规格

	GWN7801P Pro	GWN7802P Pro	GWN7803 Pro	GWN7803P L Pro	GWN7803P H Pro	GWN7806P L Pro	GWN7806P H Pro
接口							
以太网端口	8	16	24			48	
2.5G SFP/SFP+端口	2x 2.5G SFP	2x SFP+				6x SFP+	
支持模块的最大数量	MM-10G：2 SM-10G：2 RJ45-10G：2					SM-10G：6 MM-10G：6 RJ45-10G：3 *注：RJ45-10G 模块需间隔插入*	
MGMT 端口	1x Console 端口						
辅助接口	1x Reset 端口						
LED 指示灯							

系统指示灯	1x 三色 LED 用于设备状态展示				
电源指示灯	/		2x 绿色电源指示灯（PWR & RPS）	/	2x 绿色电源指示灯（PWR & RPS）
数据转发指示灯	10x 绿色 LED	18x 绿色 LED	26x 绿色 LED		54x 绿色 LED
PoE 供电指示灯	8x 黄色 LED	16x 黄色 LED	/	24x 黄色 LED	48x 黄色 LED
系统					
闪存	32MB Nor Flash				8MB Nor Flash，128MB Nand Flash
RAM	128MB RAM	256MB RAM			512MB RAM
CPU	单核，MIPS interAptive 1GHz				双核，MIPS interAptive™ 1GHz
转发模式	存储转发				
总无阻塞吞吐量	13Gbps	36Gbps	44Gbps		108Gbps
交换容量	26Gbps	72Gbps	88Gbps		216Gbps

转发速率	19.344Mpps	53.568Mpps	65.472Mpps			160.704Mpps	
数据缓冲区	8.4Mb						
网络延迟	<4μs						
电源							
电源供电	100-240V~ 50/60Hz						
冗余电源	/		1+1 外置 RPS	/	1+1 外置 RPS		
外置 RPS	/		30W	/	460W		800W
最大供电功率	9.5W/145.5W(PoE 120W)	21.8W/294.4W(PoE 250W)	21.4W	27.5W/299.2W(PoE 250W)	30.5W/471.4W(PoE 400W)	65.4W/509.3W(PoE 400W)	68.0W/870.9W(PoE 800W)
最大输出功率	145.5W	294.4W	21.4W	299.2W	471.4W	609.3W	870.9W
PoE							
PoE 供电标准	IEEE 802.3af/at	IEEE 802.3af/at/bt	/	IEEE 802.3af/at	IEEE 802.3af/at/bt	IEEE 802.3af/at	IEEE 802.3af/at/bt
PoE 端口数	8	16	/	24		48	

单个 PoE 端口最大输出功率	30W	60W	/	30W	60W	30W	60W
最大供电总功率	120W	250W	/	250W	400W		800W
设备							
设备尺寸	330mm(L)*175mm(W)*44mm(H)	440mm(L)*200mm(W)*44mm(H)			440mm(L)*300mm(W)*44mm(H)		
设备重量	1.77Kg	2.9Kg	2.5Kg	3.06Kg	4.15Kg	5.05Kg	5.3Kg
安装	桌面，墙装，机架安装				桌面，机架安装		
包装清单	1x 交换机 1x 25cm 接地线缆 4x 橡胶脚垫 1x 电源线防脱扣 8x 螺丝(KM3*6) 1x 1.2m(10A)AC 电源线 1x SQIG 1x 法规折页						
	2x 加长版挂耳支架	2x 挂耳支架					
环境							

温度	操作温度：0℃-45℃ 存储温度：-10℃-60℃					
湿度	操作湿度：10%-90%RH(无冷凝) 存储湿度：5%-95%RH(无冷凝)					
MTBF	70000H					
风扇	/	2	/	2	3	4
CPU 监控	监控 CPU 使用率，CPU 使用率过高进行告警					
内存监控	监控内存使用率，内存使用率过高进行告警					
电源监控	监控电源及其状态，电源故障进行告警					
风扇监控	风扇温控调节，风扇故障进行告警					
温度监控	监控设备温度，温度过高进行告警					
浪涌保护	± 6KV CM：电源 ± 4KV CM：网络端口					
ESD	± 12KV：接触放电					
认证	FCC，CE，RCM，IC					
软件参数						

<table>
<tr><td>网络协议</td><td colspan="2">IPv4, IPv6, IEEE 802.3, IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ae, IEEE 802.3az, IEEE 802.3ad, IEEE 802.3x, IEEE 802.3af/at/bt, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, IEEE 802.1x</td></tr>
<tr><td>堆叠</td><td>/</td><td>支持，最多 8 台设备</td></tr>
<tr><td rowspan="5">以太网特性</td><td colspan="2">巨型帧（最大长度：12288）
4K VLAN，基于端口的 VLAN，IEEE 802.1Q VLAN 标记
QinQ
基于 MAC 的 VLAN
基于协议的 VLAN
语音 VLAN，包括自动语音 VLAN、tagged OUI 和 untagged OUI
GVRP(pending)
ERPS(pendig)</td></tr>
<tr><td>生成树，支持 STP/RSTP/MSTP/PVST(+)/RPVST(+)，16 个实例（MSTP/PVST(+)/RPVST(+)）</td><td>生成树，支持 STP/RSTP/MSTP/PVST(+)/RPVST(+)，64 个实例（MSTP/PVST(+)/RPVST(+)）</td></tr>
<tr><td>/</td><td>PVLAN</td></tr>
<tr><td>16K MAC 地址，包括静态 MAC 地址、动态 MAC 地址、黑洞 MAC 地址</td><td>32K MAC 地址，包括静态 MAC 地址、动态 MAC 地址、黑洞 MAC 地址</td></tr>
<tr><td>链路聚合，支持静态和 LACP
最多 8 个聚合组，每个聚合组至多 8 个成员端口</td><td>链路聚合，支持静态和 LACP
最多 32 个聚合组，每个聚合组至多 8 个成员端口</td></tr>
<tr><td>IP 服务</td><td colspan="2">DHCP 客户端，DHCP 服务器，DHCP 中继和 DHCP Snooping
DHCPv6 客户端和 DHCPv6 Snooping
ND Snooping
DNS</td></tr>
</table>

	64 ARP/NDP 邻居表项，包括静态表项和动态表项		1K ARP/NDP 邻居表项，包括静态表项和动态表项
	16 个 VLAN IP 接口，MTU 默认 9216		32 个 VLAN IP 接口，MTU 默认 9216
IP 路由	策略路由(pending)		
	32(IPv4)/32(IPv6)静态路由		1K(IPv4)/1K(IPv6)静态路由
组播	• IGMP Snooping，支持 IGMPv2 和 IGMPv3 • MLD Snooping，支持 MLDv2 和 MLDv3 • MVR		
	256 个组播组	384 个组播组	640 个组播组
QoS	• 端口优先级 • 端口映射，包括 802.1p 映射、DSCP 映射和 IP 优先级映射 • 队列调度，包括 SP、WRR、WFQ、SP-WRR、SP-WFQ • 流量整形 • 端口限速		
ACL	128 ACL，包括链路层 ACL、IPv4 ACL 和 IPv6ACL，最多 1.5K ACE		256 ACL，包括链路层 ACL、IPv4 ACL 和 IPv6ACL，最多 4K ACE
最大输出功率	• MAC ACL（基于源 MAC 地址、目标 MAC 地址、可选以太网类型和时间范围的硬件 ACL） • IPv4 ACL（基于源 IP 地址、目标 IP 地址、可选协议类型和时间范围的硬件 ACL） • IPv6 ACL（基于源 IPv6 地址、目标 IPv6 地址、可选协议类型和时间范围的硬件 ACL） • 专家级 ACL（基于 VLAN、以太网类型、MAC 地址、IP 地址、协议类型和时间范围灵活组合的硬件 ACL） • 自定义 ACL(ACL80)(TBD) • ACL 重定向 • ACL 高级设置，包括统计计数、镜像、优先级映射和限速		

	• ACL 绑定，支持端口绑定和 VLAN 绑定
安全	• 用户级管理和密码保护，HTTPS、SSH、Telnet • 身份验证管理，包括 802.1X 认证和 MAC 认证 • AAA 认证，包括 RADIUS 和 TACACS+ • 风暴控制 • 端口隔离 • 端口安全，Sticky MAC 地址，过滤无效 MAC 地址 • IP/IPv6 元防护，DoS 攻击防护、动态 ARP 检测、CPU 防护 • 环路保护，包括端口环回检测、BPDU 保护、根保护和环回保护 • 安全锁 • 固件签名
可靠性	• 电源模块 1+1 冗余模式 • 堆叠智能升级
维护	• NTP • 1588v2 TC • CPU 和内存使用率监控 • 电源和风扇的状态监测与告警 • SNMP，包括 SNMPv1、SNMPv2c 和 SNMPv3 • RMON，包括历史组、事件组、告警组和统计组 • LLDP&LLDP-MED • 备份与恢复 • 日志 • 诊断，包括 Ping、路由跟踪、Ping 看门狗、SPAN 与 RSPAN、UDLD(TBD)、线缆检测、光模块和一键调试 • sFlow(pending) • 支持通过 FTPS/TFTP/HTTP/HTTPS 升级或本地上传升级，通过 DHCP Option/TE-069(pending)/GDMS Networking/GWN Manager/GWN 路由器进行批量升级
管理平台	• 本地 Web GUI：内置控制器 • GDMS Networking：免费云管理平台，支持无限量的设备管理 • GWN Manager：私有部署的免费云管理平台 • GWN APP：内嵌 GDMS Networking 和 GWN Manager，可供管理 GWN780x Pro 系列交换机 • 管理协议：SNMP、RMON、TR-069(pending)

入门

在部署和配置 GWN780x Pro 系列网管交换机之前，设备需要正确通电并连接到网络。本节介绍了 GWN780x Pro 系列网管交换机的安装、连接方法和保修政策。

设备清单

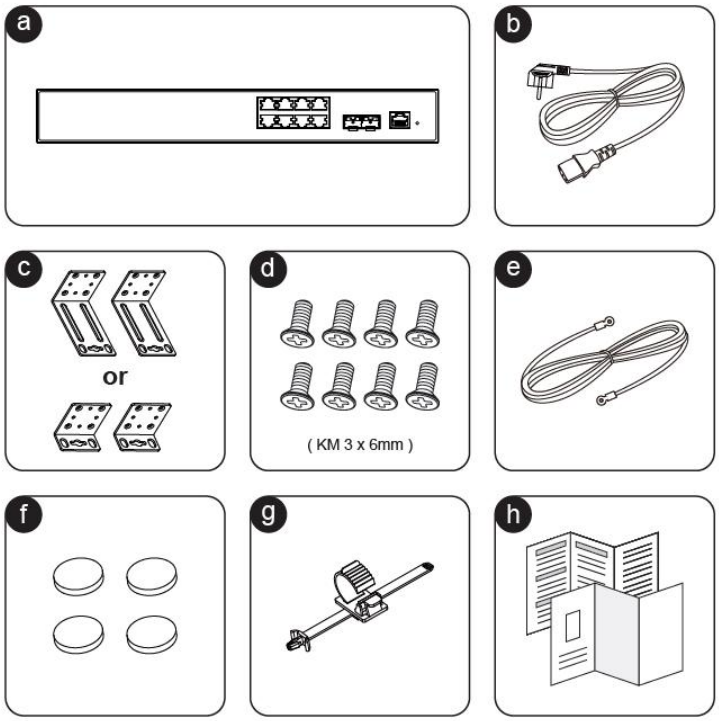


图 1 GWN780x Pro 系列包装清单

表 2 GWN780x Pro 系列包装清单

a	GWN780x Pro 系列交换机
b	1x 1.2m(10A)AC 电源线
c	2x 加长版挂耳支架或挂耳支架
d	8x 螺丝(KM3*6)
e	1x 25cm 接地线缆
f	4x 橡胶脚垫
g	1x 电源线防脱扣
h	1x SQIG 1x 法规折页

风扇降温

GWN780x Pro 系列配备了专用通风系统，旨在在设备为连接的设备提供大量电力的部署环境中保持设备冷却。这种电力供应会增加设备的工作负荷和内部温度。根据型号不同，冷却机制和风扇数量可能有所不同。

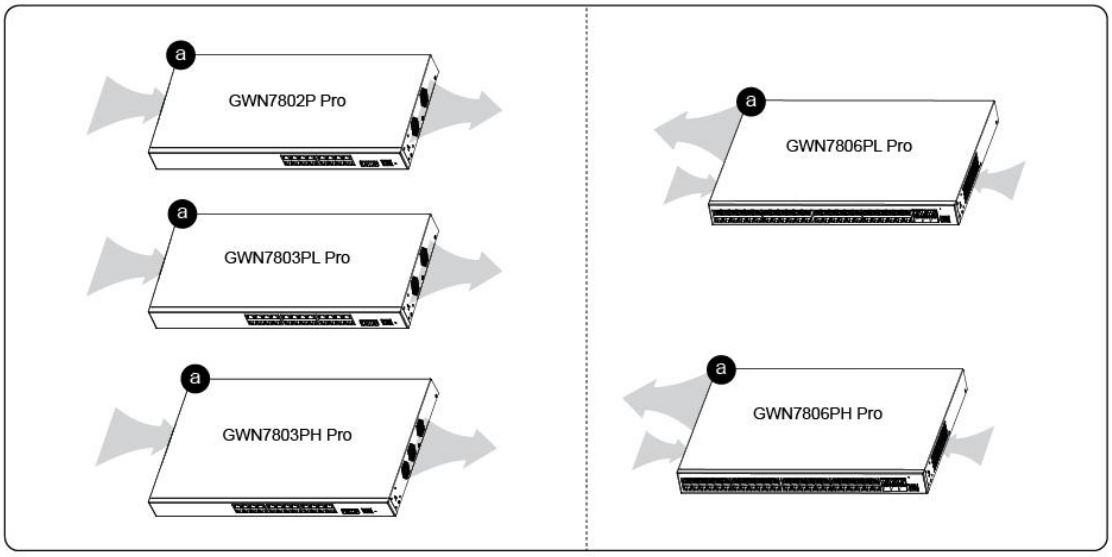


图 2 GWN780x Pro 系列风扇降温

桌面安装

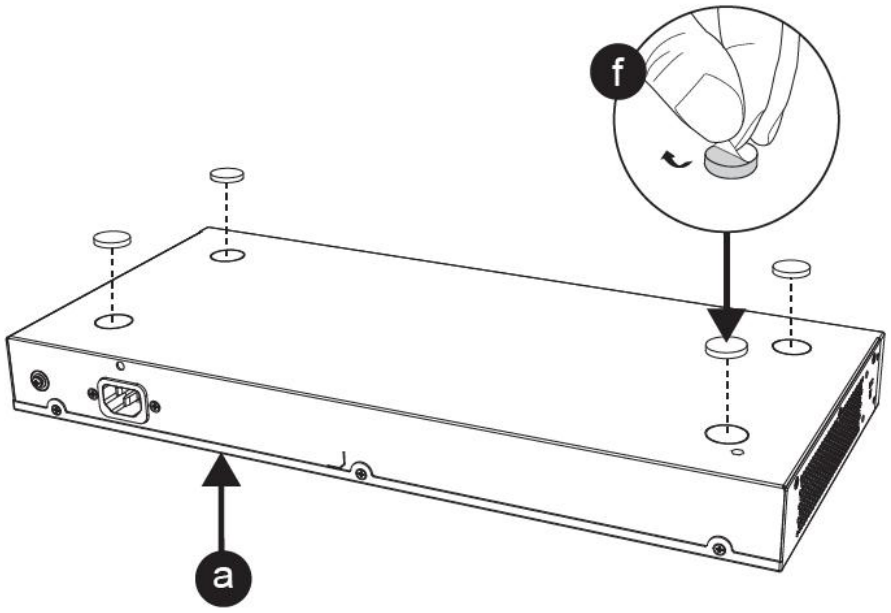


图 3 桌面安装

1. 将交换机底部朝上放在足够大且稳定的桌子上。

2. 撕开四个脚垫的橡胶保护纸，并将其粘在箱子底部四角对应的圆形凹槽中。
3. 翻转交换机，将其平稳地放在桌子上。

19 英寸机架安装（无 GWN7816P）

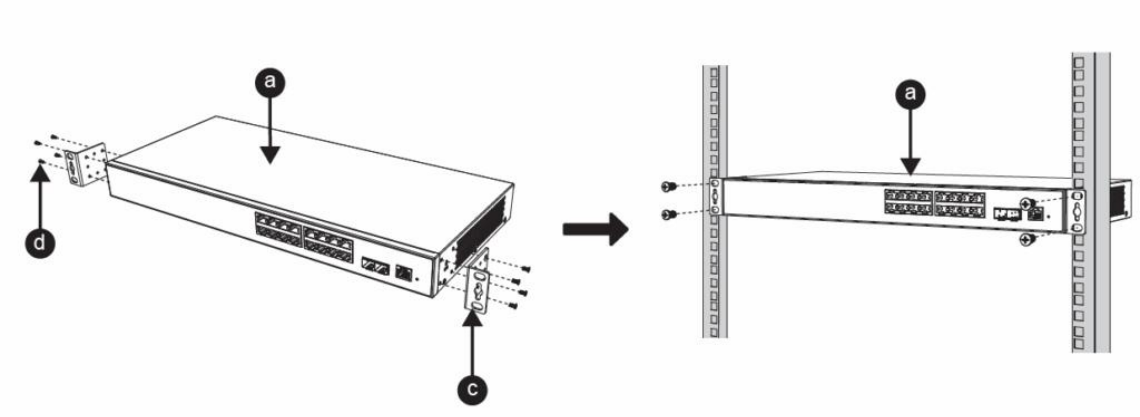


图 4 机架安装

1. 检查机架的接地和稳定性。
2. 将两个 L 形支架安装在交换机两侧的连接处，并用提供的螺钉（KM 3*6）固定。
3. 将交换机置于支架中的适当位置，并用支架支撑。
4. 用螺钉（自行准备）将 L 形支架固定在机架两端的导槽上，以确保交换机稳定水平地安装在机架上。

注意：GWN7801P Pro 需要使用加长版 L 型挂耳支架。

启动并连接 GWN780x Pro

首先将电源线连接到交换机，然后将电源线连接到设备室的电源系统。

为了防止电源意外断开，建议购买电源线防脱扣以进行安装。

1. 将固定带的光滑侧朝向电源插座，并将其插入电源插座侧的孔中。
2. 将电源线插入电源插座后，将保护器滑到剩余的带子上，直到它滑到电源线末端。
3. 将保护线的带子缠绕在电源线上，并将其锁紧。紧固束带，直到电源线牢固固定。

交换机接地，请按下述操作：

1. 从交换机背面拆下接地螺钉，将接地电缆的一端连接到交换机的接线端子。
2. 将接地螺钉放回螺孔中，并用螺丝刀拧紧。
3. 将接地电缆的另一端连接到已接地的其他设备，或直接连接到设备室内接地棒的端子。

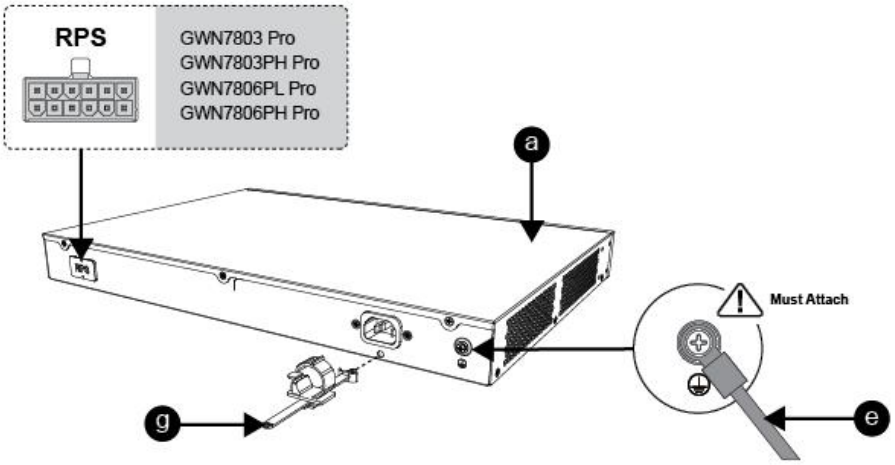


图 5 启动并连接交换机

连接 RJ45 接口

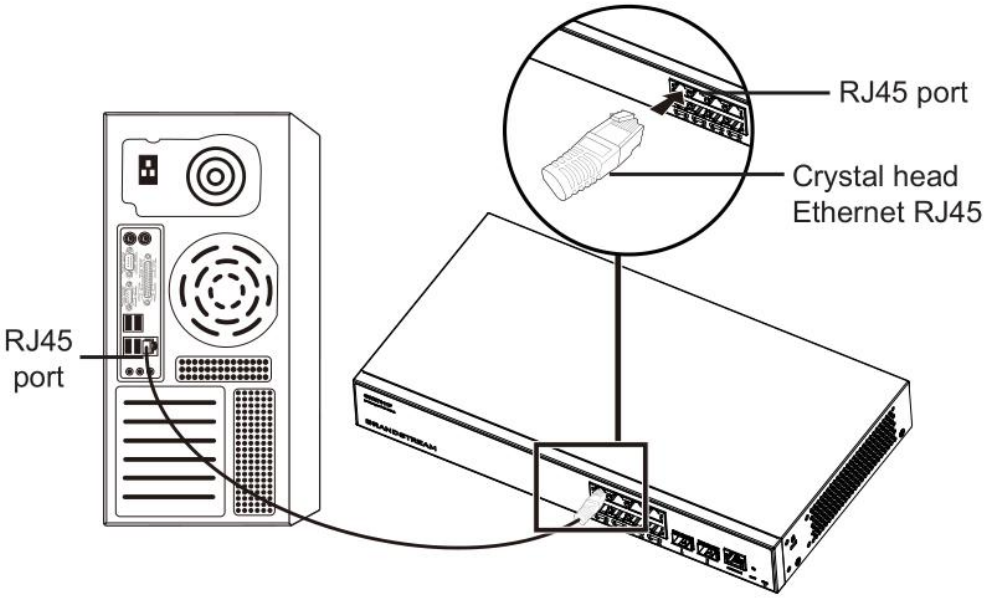


图 6 连接 RJ45 接口

1. 将网线的一端连接到交换机，另一端连接到对等设备。
2. 通电后，检查端口指示灯的状态。如果启用，则表示链路连接正常；如果关闭，则表示链路断开，请检查线缆，并检查对等设备是否已启用。

连接 SFP/SFP+接口

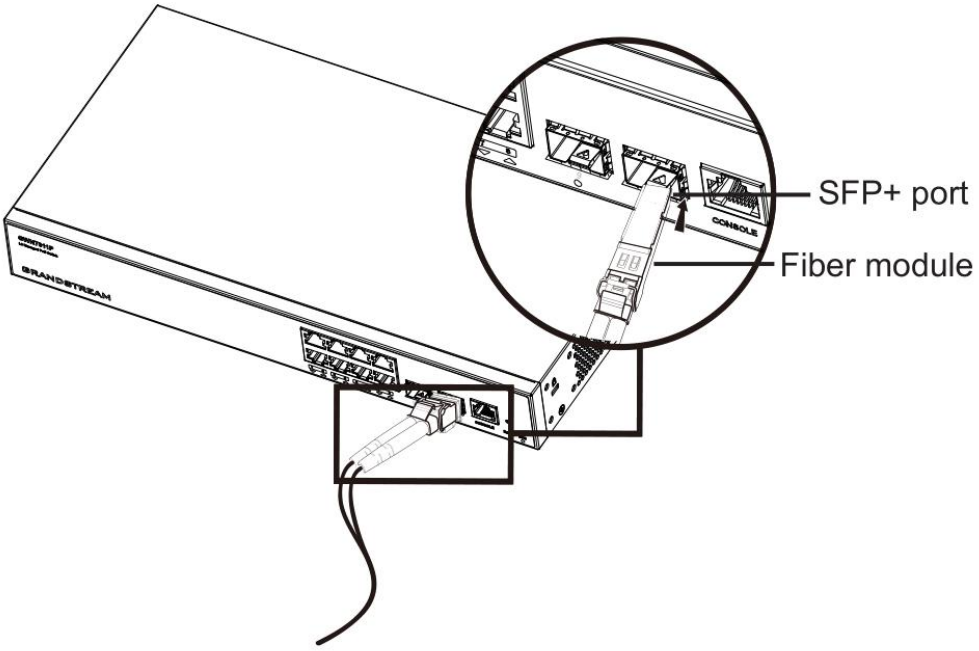


图 7 连接 SFP/SFP+接口

1. 从侧面抓住光纤模块，将其沿交换机 SFP/SFP+端口插槽顺利插入，直到模块与交换机紧密接触。
2. 连接时，注意确认 SFP/SFP+光纤模块的 Rx 和 Tx 端口。将光纤的一端插入相应的 Rx 和 Tx 端口，并将另一端连接到另一个设备。
3. 通电后，检查端口指示灯的状态。如果启用，则表示链路连接正常；如果关闭，则表示链接已断开，请检查电缆，并检查对等设备是否已启用。

注意：

- 请根据模块类型选择光纤电缆。多模模块对应多模光纤，单模模块对应单模光纤。
- 请选择相同波长的光纤电缆进行连接。
- 请根据实际组网情况选择合适的光模块，以满足不同的传输距离要求。
- 一流激光产品的激光对眼睛有害。不要直视光纤连接器。

连接 Console 口

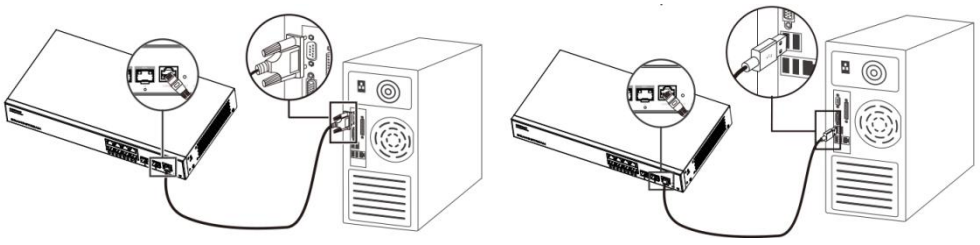


图 8 连接 Console 口

1. 将控制台电缆的 RJ45 端连接到交换机的控制台端口。
2. 将控制台电缆的另一端连接到 DB9 连接器或 PC 的 USB 端口。

安全合规性

GWN780x Pro 系列三层网管网络交换机符合 FCC/CE 和各种安全标准。GWN780x Pro 系列电源适配器符合 UL 标准。请使用 GWN780x Pro 系列包装提供的通用电源适配器。制造商的保修不包括不受支持的电源适配器对设备造成的损坏。

保修

如果 GWN780x Pro 系列三层网管交换机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 Grandstream 购买的，请在产品退回前联系我们的技术支持团队获取 RMA（退回材料授权）编号。Grandstream 保留在未事先通知的情况下对保修政策进行补修的权利。

了解 GWN780x Pro 系列网管交换机

LED 指示灯

GWN780x Pro 系列网管交换机的前面板具有指示电源和接口活动的 LED 指示灯，下表描述了 LED 指示灯的状态。

表 3 LED 指示灯

LED 指示灯	状态	描述
系统指示灯	关闭	电源关闭
	绿灯常亮	设备启动中
	绿灯闪烁	升级
	蓝灯常亮	正常使用中
	蓝灯闪烁	正在部署
	红灯常亮	升级失败
	红灯闪烁	恢复出厂
接口指示灯	关闭	• **所有接口：**接口关闭 • **SFP/SFP+接口：**接口故障
	绿灯常亮	接口已连接且没有活动
	绿灯闪烁	接口已连接，数据正在传输
	黄灯常亮	以太网接口已连接，没有活动，PoE 已通电
	黄灯闪烁	以太网接口已连接，数据正在传输，PoE 已通电

	黄绿灯交替	以太网接口故障
PWR/RPS 电源指示灯	关闭	• 未接入 • 电源故障
	绿灯常亮	• 使用中 • 已接入但未使用

注意：在启机期间，LED 指示灯会经历多种颜色状态。

访问和配置

注意：

如果没有使用 DHCP 服务器获取 IP 地址，则 GWN780x Pro 系列网管交换机默认 IP 地址为 192.168.0.254。

通过 Console 口登录

1. 使用控制台电缆连接交换机的 Console 端口和 PC 的串口。
2. 打开 PC 的终端仿真程序（如 SecureCRT），输入默认用户名和密码登录。（默认管理员用户名为“admin”，默认随机密码可在 GWN780x Pro 系列网管交换机的标签上找到）。

注意：

波特率需要设置为 115200。

通过 SSH 远程登录

1. 在 PC/开始中输入“cmd”。
2. 在 cmd 窗口中输入 ssh＜GWN780x Pro_IP＞。
3. 输入要登录的默认用户名和密码。（默认管理员用户名为“admin”，默认随机密码可在 GWN780x Pro 系列网管交换机的标签上找到）。

通过 GDMW Networking/GWN Manager 配置

输入 https://www.gdms.cloud（gwn manager 为 https://<gwn_manager_IP>），并输入云平台的账号和密码。如果您没有帐户，请先注册或要求管理员为您分配一个帐户。

通过 Web UI 登录

GWN780x Pro 系列网管交换机嵌入式 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（如 Microsoft IE、Mozilla Firefox 或 Google Chrome）配置设备。

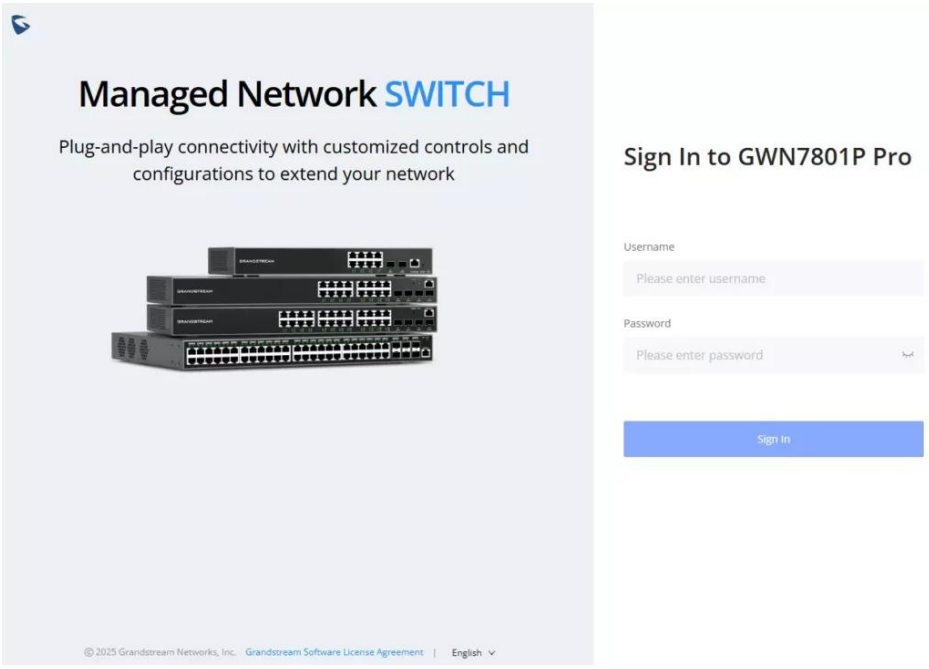


图 9 GWN780x Pro Web 登录页面（以 GWN7801P Pro 为例）

1. PC 使用网线正确连接交换机的任意 RJ45 端口。
2. 将 PC 的以太网（或本地连接）IP 地址设置为 192.168.0.x（“x”是 1-253 之间的任何值），将子网掩码设置为 255.255.255.0，以便它与交换机 IP 地址位于同一网段中。如果使用 DHCP，则可以跳过此步骤。
3. 在浏览器中输入交换机的默认管理 IP 地址 https://< GWN780x Pro_IP>，然后输入用户名和密码登录。（默认管理员用户名为“admin”，默认随机密码可在 GWN780x Pro 系列网管交换机的标签上找到）。

CLI 访问

除了基于网络的配置，GWN780x Pro 系列还可以通过命令行接口（CLI）进行配置。有关使用 CLI 的详细说明，请参阅 GWN78xx CLI 用户使用指南。

Web GUI 语言

要更改默认语言，请在登录之前或之后在 Web GUI 相应位置选择显示的语言。

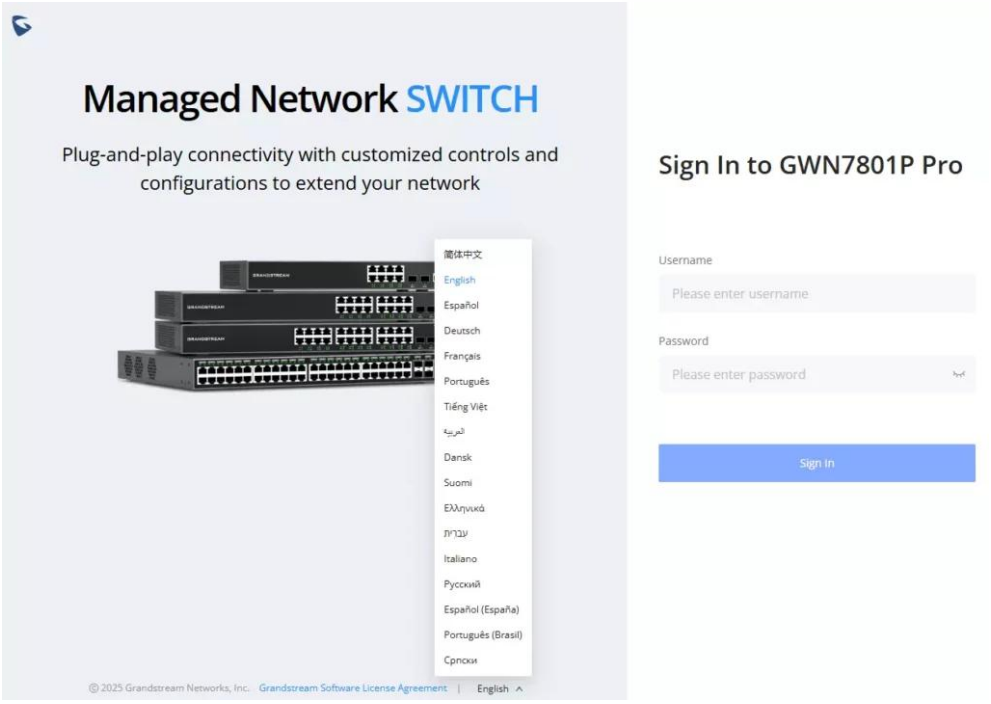


图 10 Web GUI 显示语言-登录页面（以 GWN7801P Pro 为例）

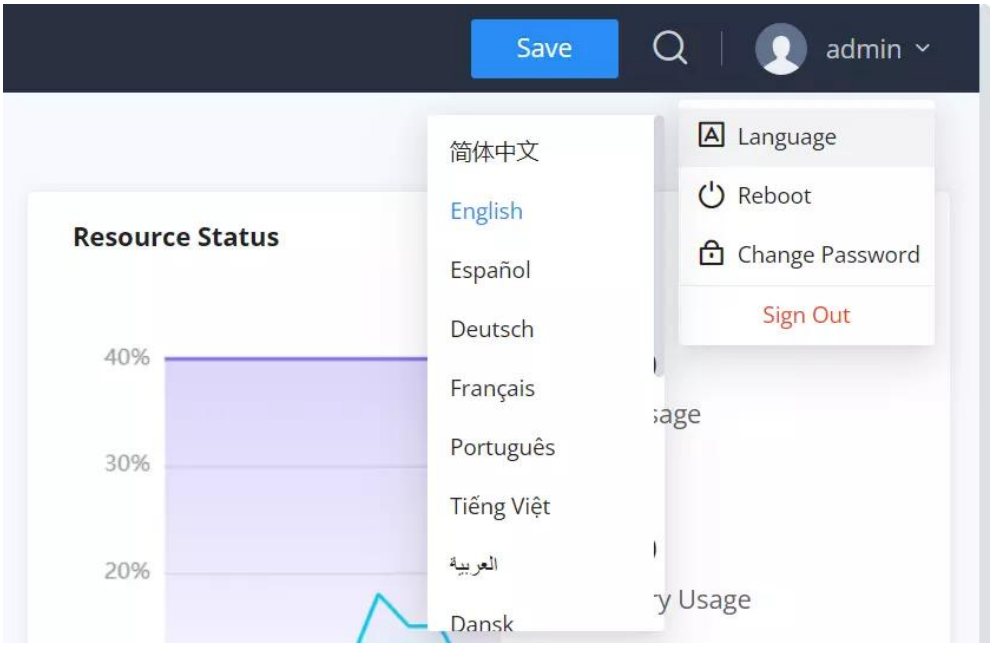


图 11 Web GUI 显示语言-开始页面（以 GWN7801P Pro 为例）

注：当从登录页面或界面内手动更改 Web GUI 语言时，所选语言将保存在设备的配置中。无论系统的区域设置或浏览器设置如何，此偏好都将在会话、重启和不同浏览器之间持续存在。

搜索

因为很难浏览每个部分，GWN780x Pro 系列网管交换机具有搜索功能，可帮助用户查找正确的配置、设置或参数等。

在页面顶部，有一个搜索图标，用户可以单击它，然后输入搜索关键字，将获得该关键字所在的所有可能位置。

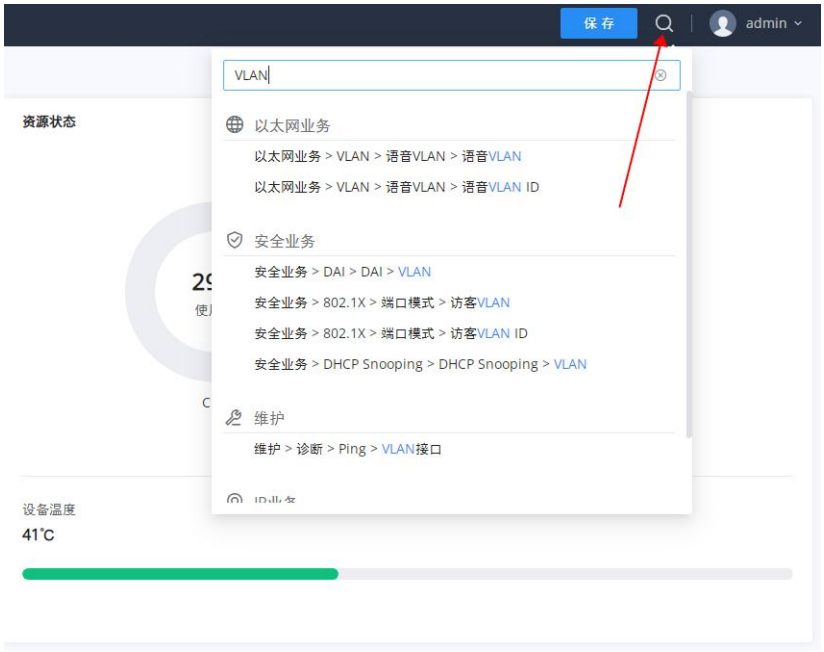


图 12 搜索

概览界面

登录后首先显示概览，“系统信息”显示系统信息，“端口信息”显示端口状态。本节为用户提供有关GWN780x Pro系列交换机系统和端口状态的一般和全局视图，以便于监控。

系统信息

系统信息是成功登录 GWN780x Pro 系列交换机 Web 界面后的第一页。它提供了 GWN780x Pro 系列交换机信息的总体视图，以仪表板样式显示，便于监控。其中包括基本信息、资源状态、温度、PoE 状态、风扇状态和系统事件。

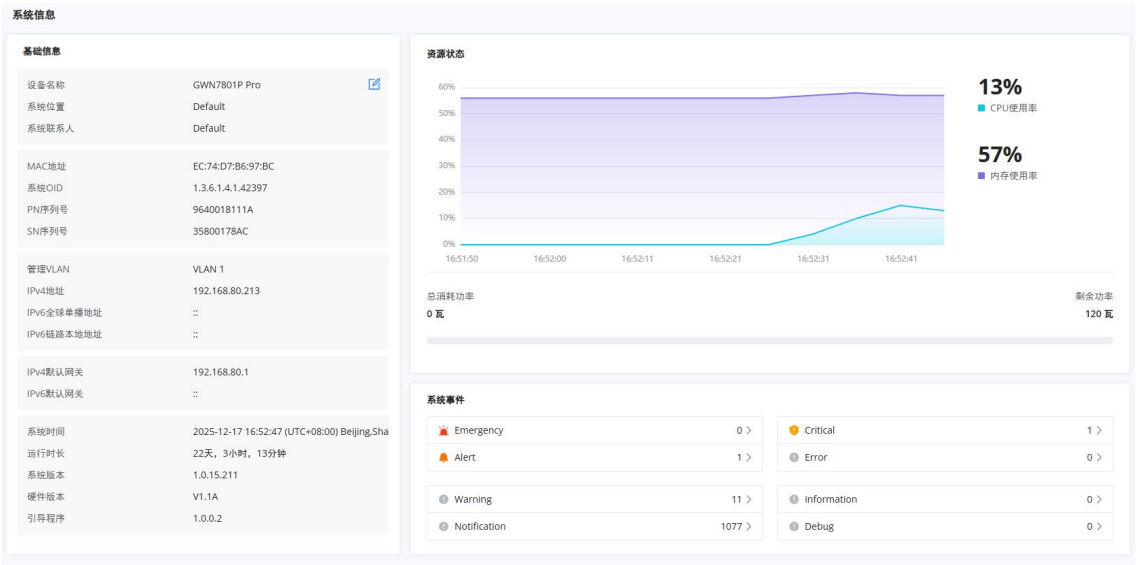


图 13 系统信息页面

要重命名设备基本信息，请单击，然后输入所需的名称、位置和联系人。

表 4 系统信息

基础信息	显示设备和系统常规信息，包括（设备名称、MAC 地址、默认网关、系统时间、系统版本等）
资源状态	实时显示 CPU 和内存的使用情况。
设备温度	显示设备当前温度。 **注意：**GWN7802P Pro、GWM7803PL/PH Pro 和 GWN7806PL/PH Pro 有设备温度。
PoE 状态	显示总功耗和剩余功率（mA）。

	注意：GWN7801P Pro、GWN7802P Pro、GWN7803PL/PH Pro 和 GWN7806PL/PH Pro 有 PoE 状态信息。
电源	显示电源信息。 **注意：**GWN7803 Pro、GWN7803PH Pro 和 GWN7806PL/PH Pro 有电源信息。
风扇	显示风扇运行状态和速度。 **注意：**GWN7802P Pro、GWN7803PL/PH Pro 和 GWN7806PL/PH Pro 有风扇信息。
系统事件	显示每个类别（紧急、警报、警告等）的事件总数。 **注意：**单击任何事件类别都会将您重定向到诊断页面以获取更多详细信息。

端口信息

此页面提供有关 GWN780x Pro 交换机的全面端口统计信息、PoE 电源供应信息以及详细的端口和邻居信息。它帮助用户高效地监控网络性能和管理连接的设备。

- 端口信息

“端口信息”部分以视觉方式显示每个端口的状态和速度，使用不同的颜色表示速度和状态。用户可以快速识别活动、非活动或有问题的端口及其 PoE 电源状态。

图 14 端口信息 1

- 基本信息和邻居信息

“基本信息”部分显示所选端口的具体细节，包括其状态和设置。“邻居信息”部分提供关于连接到端口的设备的信息，例如主机名和当前流量速率。

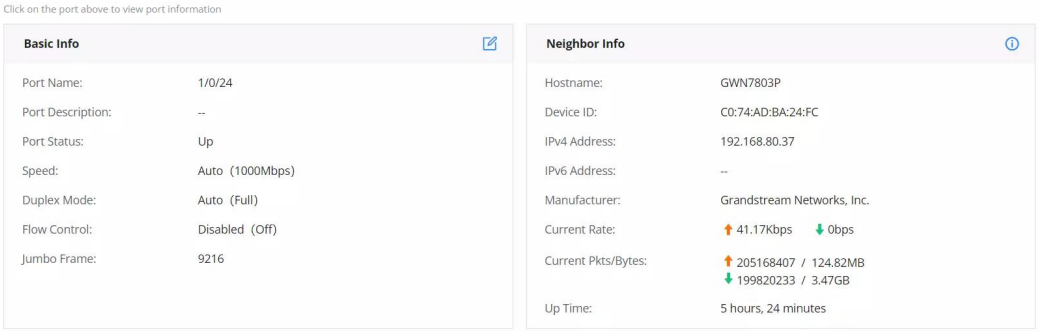


图 15 端口信息 2

- 数据统计

“统计”部分提供了通过交换机的网络流量的详细指标。它包括有关字节、数据包和丢弃的数据，这对于监控性能和故障排除至关重要。

- PoE 供电/光模块信息

如果所选端口支持 PoE，则 "PoE 供电" 部分显示电源状态和使用情况。如果端口是 SFP/SFP+，则 "光模块信息" 部分显示信号损失、温度、接收和发送功率等详细信息。

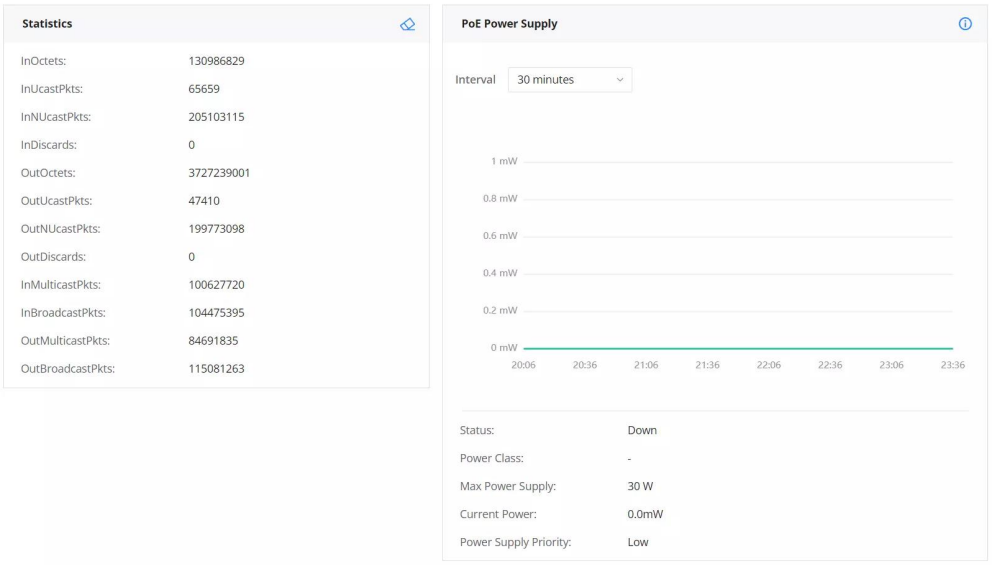


图 16 端口信息 3

下表对颜色和符号进行说明：

表 5 端口信息

1	以太网接口未连接，PoE 关闭

	以太网端口已禁用
	以太网接口已连接且速率为 1000Mbps，PoE 关闭
	以太网接口已连接且速率为 100Mbps/10Mbps，PoE 关闭
	以太网端口异常关闭
	2.5G SFP/SFP+端口速率为 1000Mbps
	2.5G SFP/SFP+端口速率 2.5Gbps 注：仅 GWN7801P Pro、GWN7802P Pro 和 GWN7803(PL/PH) Pro
	SFP+口速率 10Gbps 注：仅 GWN7802P Pro、GWN7803(PL/PH) Pro 和 GWN7806PL/PH Pro
	PoE 供电启用

注意：也可以使用 PoE 符号和颜色组合表示。例如：  在这种情况下，端口以 1000 Mbps 的速度运行，同时也在使用 PoE 供电。

图标描述：

- 基本信息：  将用户转发至端口基本设置页面，在该页面用户可以修改端口设置，如描述、速度、双工模式和流量控制，或启用/禁用端口。
- 邻居信息：  将用户转发至 LLDP/LLDP-MED 邻居信息页面。在这里，用户可以查看有关连接设备的附加信息，包括底盘 ID、端口 ID、设备名称、系统描述和生存时间。
- PoE 供电/光模块信息：  将用户转发至相应的详细页面。对于 PoE，它转发至 PoE 接口页面，显示

每个端口的 PoE 设置的详细信息。对于光纤，它转发至光纤模块页面，显示综合光纤详细信息，如信号损失、温度、接收功率（RX）和发送功率（TX）。

- 数据统计：  清除显示的统计信息。

以太网业务

以太网业务部分用于配置端口基本设置、链路聚合、VLAN、生成树等。

端口基本配置

在此页面上，您可以配置 GWN780x Pro 系列网管交换机端口的基本参数，如禁用或启用端口、添加“描述”、指定默认速率为“自动”、“双工模式”和“流量控制”。另外还会有一个过滤器用于编辑千兆以太网端口的电口或 SFP/SFP+光口或 Combo 口。

配置端口，请导航到 **Web UI → 以太网业务 → 端口基本设置**。

图 17 端口基本设置

点击操作列下的 进行端口配置。

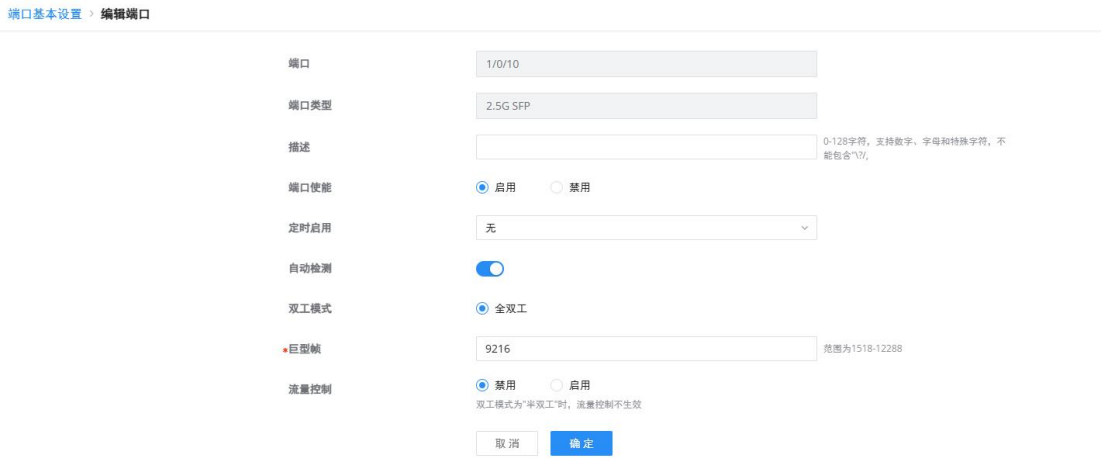


图 18 端口基本配置-编辑端口

用户可以为特定端口指定定时启用策略，这旨在实现对何时应用配置的精确控制。这些策略规定了端口设置生效的确切时间。

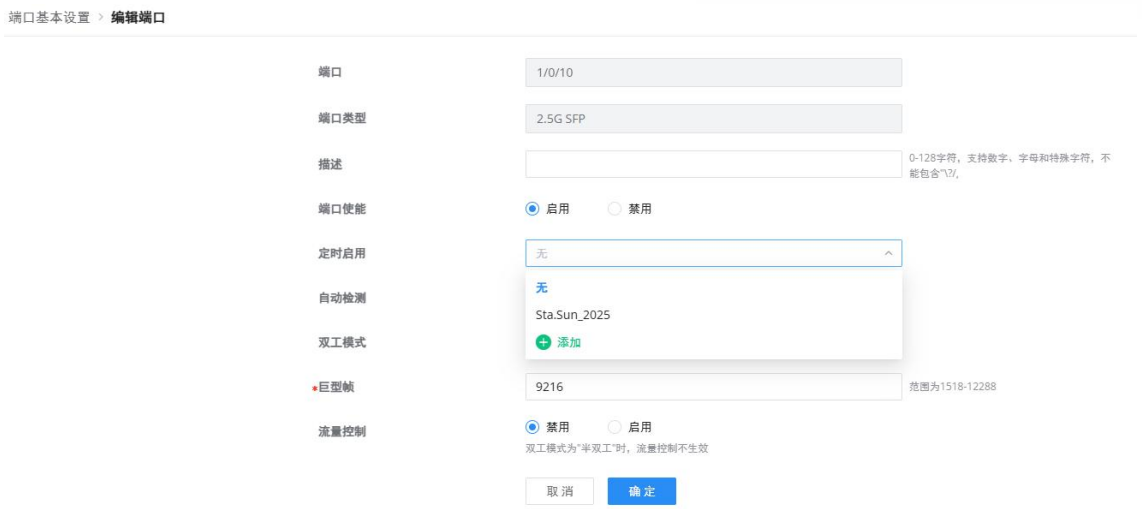


图 19 端口基本设置-定时启用

表 6 端口基本配置

端口	要配置的选定端口，可以是千兆以太网端口或 SFP/SFP+/Combo 端口。
端口类型	显示端口类型，以太网端口或 SFP+或 SFP 或 Combo
描述	用于配置此接口的信息描述，可以是使用说明等，最多 128 个字符，支持的字符具体为 ASCII 0x20~0x7E，但不包含"\?/,这 5 项
端口使能	设置是否启用接口。 默认情况下启用。
定时启用	从下拉列表中选择端口（包括物理端口和 LAG 端口）启用的时间安排。
自动检测	一旦开启，速率和 DAC 线使用将根据接入情况自动探测，不可配置速率和 DAC 线。 **注意：**仅 SFP+端口支持。
速率	设置接口速率。 **以太网端口：**选项为{自协商、10Mbps、100Mbps、1000Mbps}，默认为自协商。 **注意：**当设置为自协商时，接口的速率将在接口和对等端口之间自动协商。

	2.5G SFP 端口：选项为{100Mbps、1000Mbps、2.5Gbps}，默认 2.5Gbps。 **SFP+端口：**选项为{100Mbps、1000Mbps、2.5Gbps、10Gbps}，默认 10Gbps。 **注意：**SFP+端口 2.5Gbps 速率仅 GWN7802P Pro 和 GWN7803(PL/PH) Pro 支持
双工模式	设置接口的双工模式。以太网端口选项为｛自动协商、全双工、半双工｝。默认为自协商。 **注意：**SFP+端口仅支持全双工模式。 • **自协商：**接口的双工状态由接口和对等端口之间的自协商决定 • **全双工：**接口发送和接收数据包。 • **半双工：**接口只能发送/接收数据包。
巨型帧	最大传输有效负载或 MTU。如果用户需要特定场景的更大 MTU 长度，有效范围为 1518-12288，基于端口设置。默认 9216。
流量控制	设置流量控制，选项为｛禁用、启用、自协商｝。默认值为禁用。 在启用之后，如果本地设备拥塞，它将向对端发送消息以通知对端设备暂时停止发送数据包，在接收到消息之后，对端设备将暂时停止向本地设备发送数据包，反之亦然。因此，避免了数据包丢失的发生。 **注意：**2.5G SFP/SFP+端口不支持自协商模式。

端口组

端口组功能允许管理员将特定端口逻辑上捆绑在一个组下，并分配一个对应的组 ID，这在对交换机端口进行分类以识别每组端口的使用情况时非常有用。例如，端口 1 到 8 可以设置为组 ID 20，这些端口将用于连接安全设备。

端口组设置可以为端口组端口提供快速批量设置。

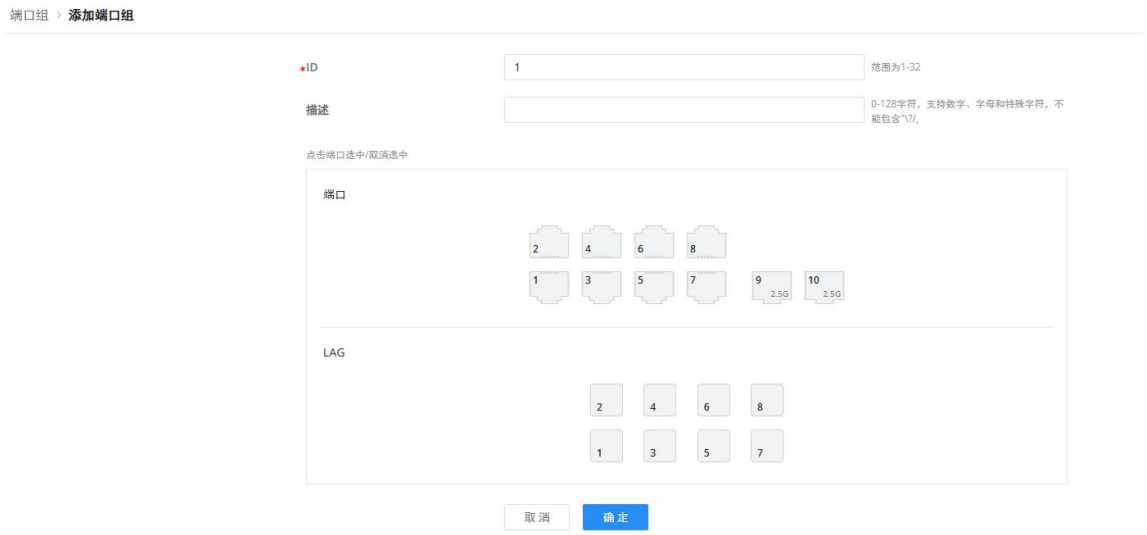


图 20 端口组

一旦创建了端口组，它可以简化单独选择和 Tag/Untag VLAN 端口的过程。在**以太网业务 → VLAN** 下，选择要用于您的 VLAN 的端口组。

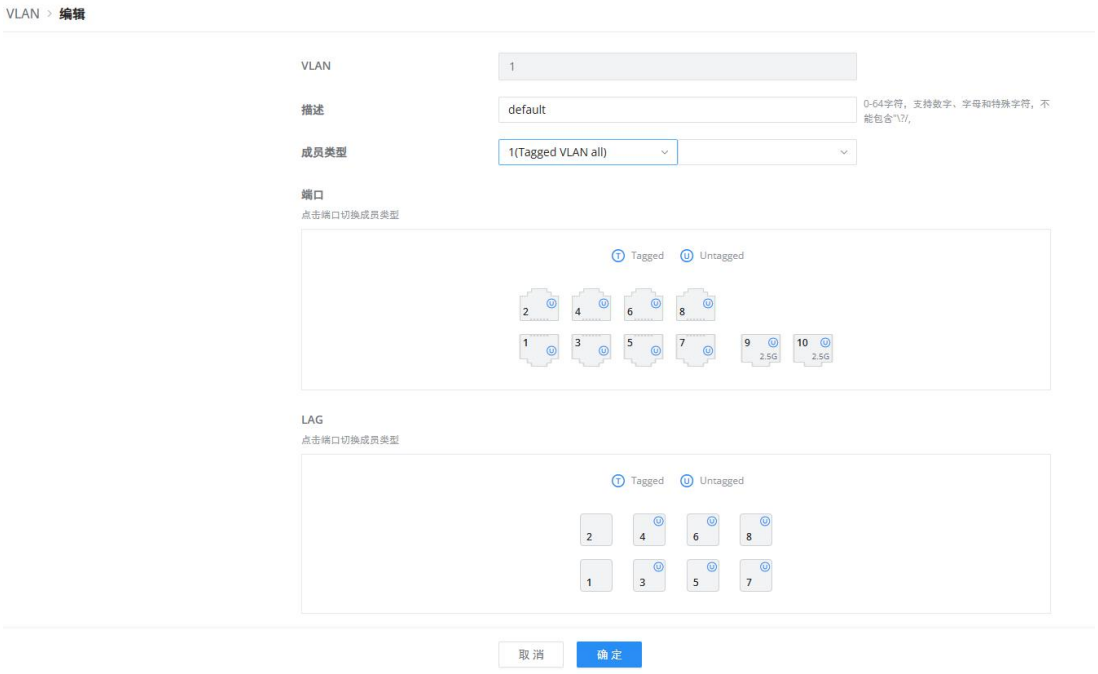


图 21 端口组选择

此外，用户可以根据创建的端口组启用/禁用特定端口，而无需单独逐个选择每个端口:

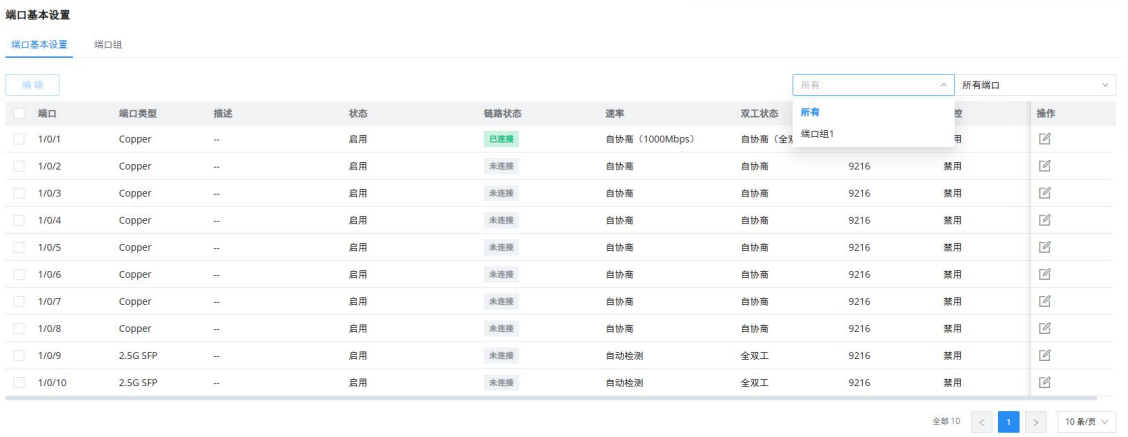


图 22 选择端口组进行端口基本设置

端口统计

为了进行监控、故障排除，端口统计信息实时显示不同类型的数据流，如接收/发送速率、接收/发送字节数、接收/发送错误报文数等。还支持清除所有统计信息或特定端口的信息。

图 23 端口统计 1

查看更详细的信息，例如 Etherlike (SNMP)、RMON 和端口私有 MIB 信息。

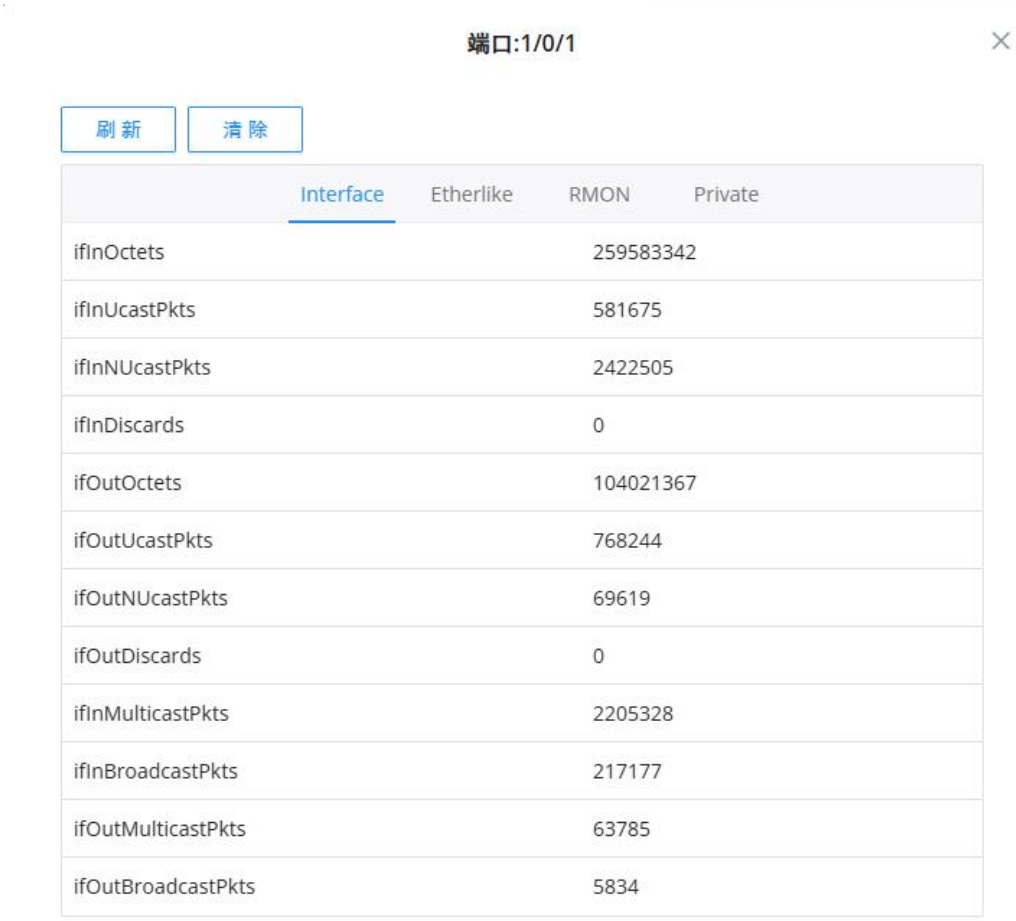


图 24 端口统计 2

环路检测

通过启用接口的环路检测功能，接口会定期发送检测数据包，以检查数据包是否返回到设备，然后判断设备中是否存在环路。如果检测到环路，端口将自动关闭，以消除环路并确保网络环境的正常运行。

注意：如果启用了 STP，因为 STP 保护会覆盖接口回环检测，导致接口回环检测无效。

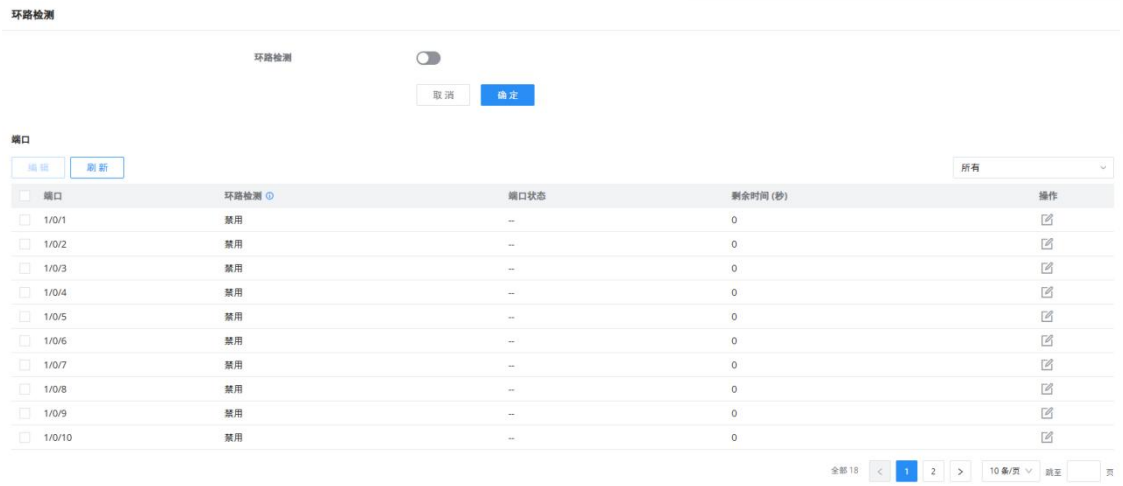


图 25 环路检测

端口自动恢复

端口自动恢复可以在用户指定的特定延迟后恢复端口。当端口的以下功能触发端口关闭时，端口会在延迟时间后自动回到启用状态：

例如：

- **ARP 报文检测：**如果 DAI 中的 ARP 速率超过设置值，则当前端口将关闭。
- **STP BPDU 保护：**在生成树中，端口启用 BPDU Guard。当触发此功能时，端口将关闭。
- **端口环路：**当端口自环且启用生成树时，端口将关闭。
- **ACL：**当 ACL 规则匹配且行为为禁用时，端口将关闭。
- **端口安全：**当端口 MAC 地址的数量超过设置的数量时，端口将关闭。

注意：

当恢复时间结束且端口恢复时，如果再次出现触发关闭的情况，则端口将再次关闭。

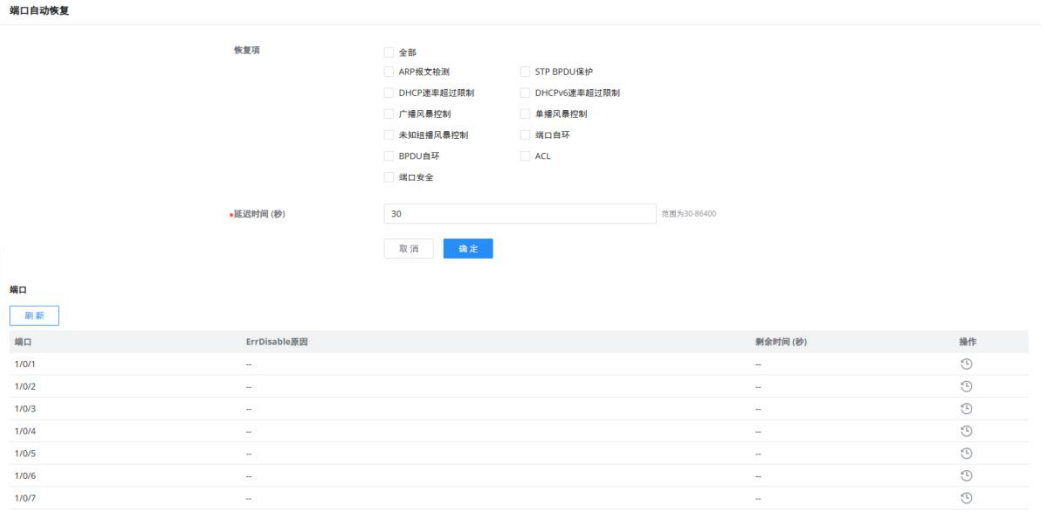


图 26 端口自动恢复

链路聚合

LAG 是指链路聚合组，它将一些物理端口组合在一起，形成一条高带宽数据链路。因此，它可以在组中的成员端口之间实现业务负载共享，以提高连接可靠性。

链路聚合组

GWN780x Pro 系列交换机上有两种负载平衡模式，基于 MAC 地址或基于 IP－MAC 地址。就 LAG 的类型而言，有静态选项或使用 LACP 或链路聚合控制协议，这两者都受支持。

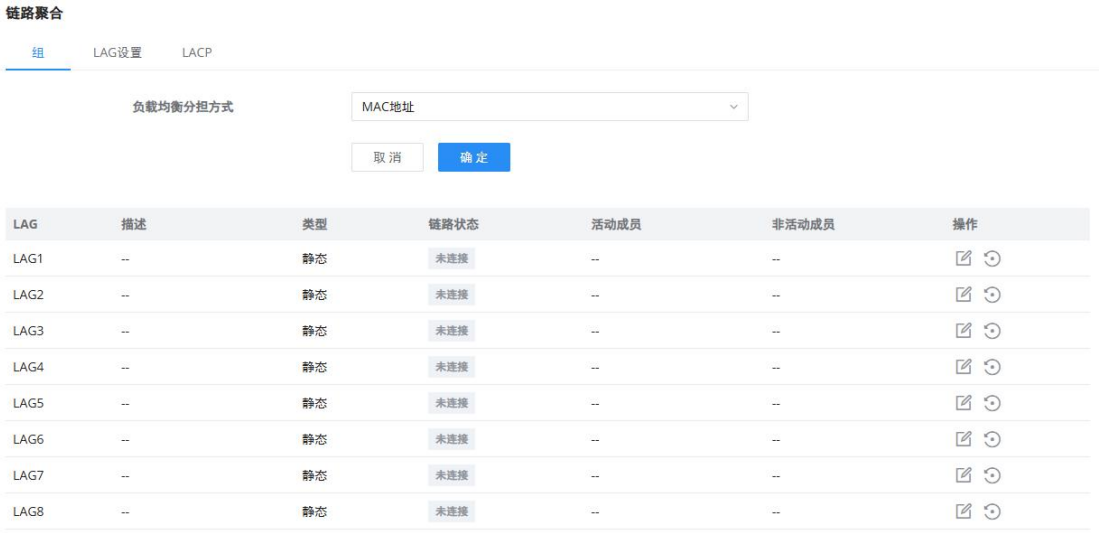


图 27 链路聚合组

表 7 链路聚合组

负载均衡分担方式	选择你的负载均衡模式 • **MAC 地址**：聚合组将根据不同的 MAC 地址平衡流量。因此，来自不同 MAC 地址的数据包将被发送到不同的链路。 • **IP-MAC 地址**：聚合组将根据 MAC 地址和 IP 地址平衡流量。因此，来自相同 MAC 地址但不同 IP 地址的数据包将被发送到不同的链路。
编辑组	**名称**：输入链路聚合组的名称 **类型**：使用下拉菜单指定 LAG 的类型。 • **静态**- 静态聚合端口通过活动成员发送数据包，而无需检测或与远程聚合端口协商。 • **LACP**- LACP 聚合端口仅在与远程聚合端口协商后才将成员置于活动状态，以获得最佳可靠性。 **GE**：单击端口以选中/取消选中哪些端口将成为此 LAG 的成员端口。

LAG 设置

在此页面中，用户可以启用链路聚合组并添加描述，以及指定 LAG 的速度和流量控制。

图 28 LAG 端口设置

表 8 端口设置

端口	要配置的选定 LAG 端口。
描述	用于配置此接口的信息描述，可以是使用说明等，最多 128 个字符，支持的字符具体为 ASCII 0x20~0x7E，但不包含"\?/,这 5 项
端口使能	设置是否启用接口。 默认情况下启用。
速率	设置接口速率，选项为｛自协商、10Mbps、100Mbps、1000Mbps、10Gbps｝。 默认为自协商。 **注意：**当设置为自协商时，接口的速率将在接口和对端端口之间自动协商。
巨型帧	最大传输有效负载或 MTU。如果用户需要特定场景的更大 MTU 长度，有效范围为 1518-12288，基于端口设置。默认 9216。
流量控制	设置流量控制，选项为｛禁用、启用、自协商｝。默认值为禁用。 在启用之后，如果本地设备拥塞，它将向对端设备发送消息以通知对端设备暂时停止发送数据包，在接收到消息之后，对端设备将暂时停止向本地设备发送数据包，反之亦然。因此，避免了数据包丢失的发生。

LACP

LACP 或链路聚合控制协议是基于优先级来控制的协议。用户可以启用系统优先级，甚至可以单独指定每个端口的优先级。

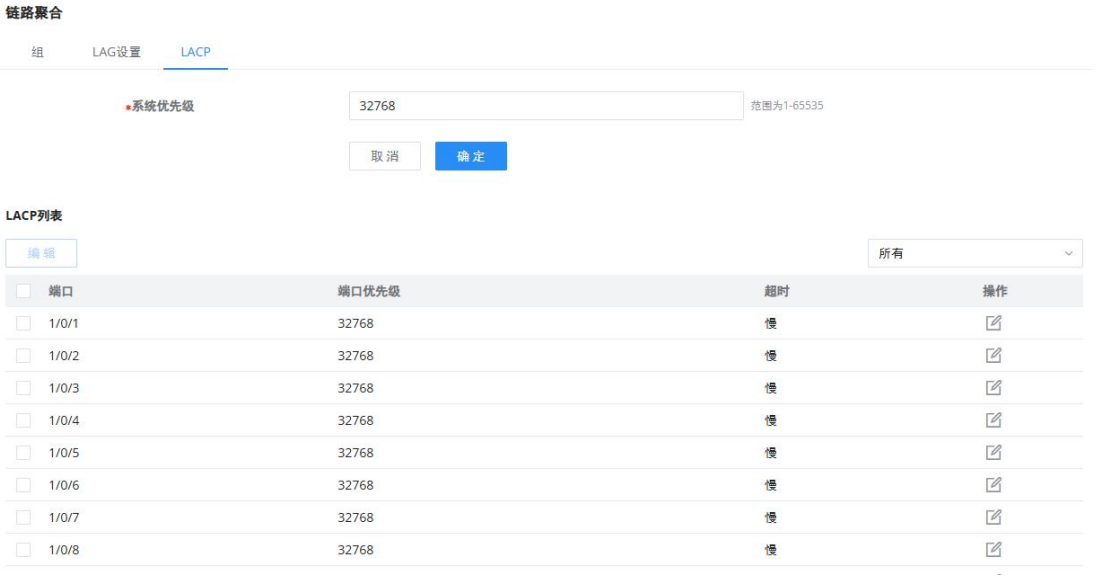


图 29 LACP

表 9 LACP

系统优先级	设置 LACP 的系统优先级，取值范围为 1-65535 之间的整数，默认值为 32768。
编辑 LACP	**端口：**选择要配置的交换机 LAG 接口 **端口优先级：**设置端口的 LACP 协议优先级，取值范围为 1 到 65535 之间的整数，默认值为 1。 **注意：***端口的优先级值越小，端口的 LACP 优先级越高。* **超时：**设置接收 LACP 数据包的超时时间，选项为｛快，慢｝，默认值为慢。 • **快模式：**接收 LACP 协议分组的默认超时周期是 3 秒。 • **慢模式：**接收 LACP 协议分组的默认超时周期是 90 秒。

MAC 地址表

MAC 地址表记录由交换机获知的其他设备的 MAC 地址与接口之间的对应关系，以及诸如接口所属的 VLAN 之类的信息。当转发数据包时，设备根据包的目的 MAC 地址查询 MAC 地址表。如果 MAC 地址表包含与包的目的 MAC 地址相对应的条目，则它通过条目中的出接口直接转发分组。如果 MAC 地址表不包含与分组的目的 MAC 地址相对应的条目，则设备将使用广播模式在其所属 VLAN 中除接收接口之外的所有接口上转发数据包。

MAC 地址表中的条目分为动态地址、静态 MAC 地址、黑洞地址和端口安全地址。

动态地址

MAC 地址表是基于自动学习设备接收的数据帧中的源 MAC 地址来建立的。如果 MAC 地址条目在 MAC 地址表中不存在，则设备将新的 MAC 地址以及与 MAC 地址相对应的接口和 VLAN 作为新条目添加到 MAC 地址表。GWN780x Pro 系列交换机将通过重置老化时间来更新条目。

老化时间：

动态 MAC 地址并不总是有效的。每个地址都有一个生命周期，达到生命周期后无法更新的条目将被删除。这个生命周期被称为老化时间。如果记录在达到生命周期之前更新，则将重新计算条目的老化时间。

注意：

- 取值范围为 0 或 60-1 000000 的整数，默认值为 300 秒。如果设置为 0，则表示动态 MAC 地址将始终有效。
- 系统重新启动后，动态表条目会丢失。

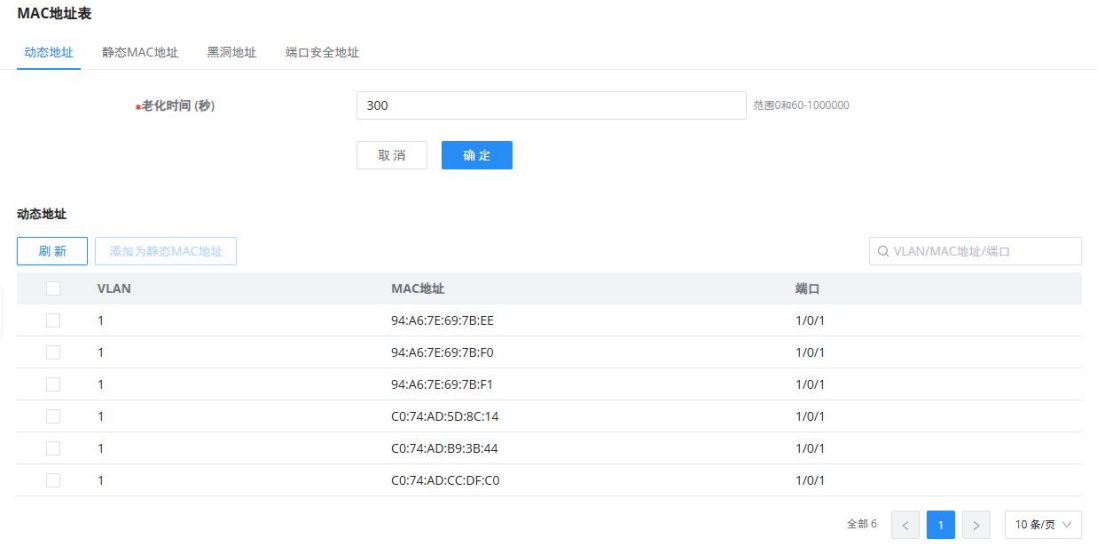


图 30 动态 MAC 地址

单击“**刷新**”按钮更新 MAC 地址表，或单击“**添加静态 MAC 地址**”按钮将条目添加到静态 MAC 地址。

静态 MAC 地址

此部分允许用户手动将 MAC 地址添加到 MAC 表中。配置结果将显示列出在页面列表中。

注意：

- 静态 MAC 地址必须为单播 MAC 地址。

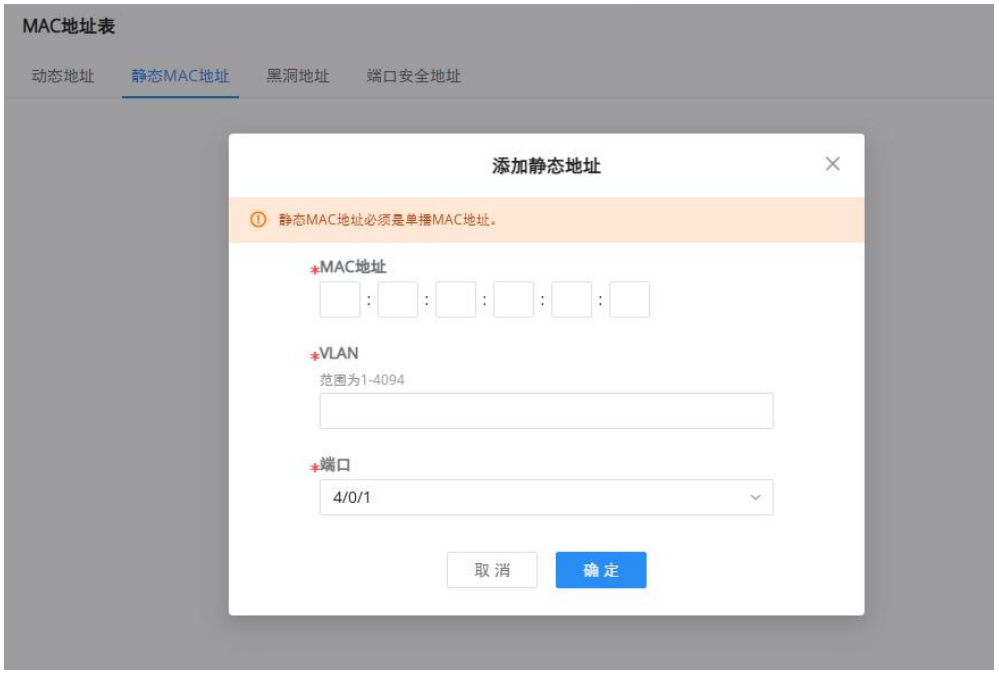


图 31 静态 MAC 地址

表 10 静态 MAC 地址

MAC 地址	输入要转发的 MAC 地址。
VLAN	MAC 地址所属的 VLAN。
端口	选择匹配目的地 MAC 地址的接收帧将转发到的端口。

黑洞 MAC 地址

如果 MAC 地址不受信任或不安全，用户可以阻止某些 MAC 地址的流量，并通过将其添加到黑洞地址表中来丢弃这些地址。

单击“**添加**”按钮，然后输入 MAC 地址和 VLAN。

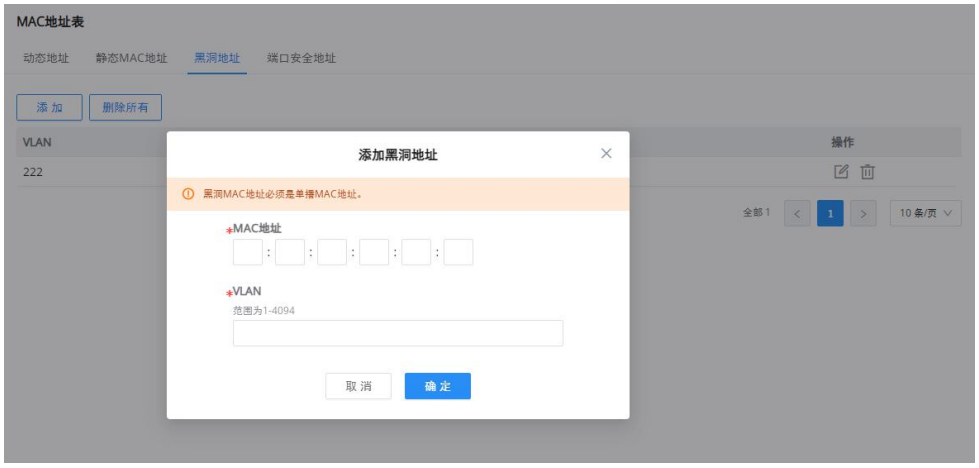


图 32 黑洞地址

端口安全地址

在**安全业务**中启用**端口安全**之后，地址将同步显示在 **MAC 地址表 → 端口安全地址**中。
该列表显示端口名称、VLAN 和 MAC 地址。

注意：

- 要编辑、删除或添加安全地址，请导航到**安全业务 → 端口安全**。

图 33 端口安全地址

VLAN

虚拟局域网，虚拟 LAN 或 VLAN，是一个具有共同请求的主机群，无论其物理位置如何，它们都像连接到同一广播域一样进行通信。VLAN 具有与物理局域网（LAN）相同的属性，但它允许将终端分在一组，即使它们位于不同网络交换机上。VLAN 成员可以通过软件配置，而不是物理重新定位设备或连接。

用户可以单击“**添加**”按钮添加新 VLAN，也可以指定范围同时创建多个 VLAN，例如（7-9）将创建 VLAN 7、8 和 9，或创建不同的单独 VLAN，例如（11,89）将创建 VLAN11 和 89。

注意：

VLAN 有效范围为 2-4094，VLAN 0、1 和 4095 为系统保留 VLAN。

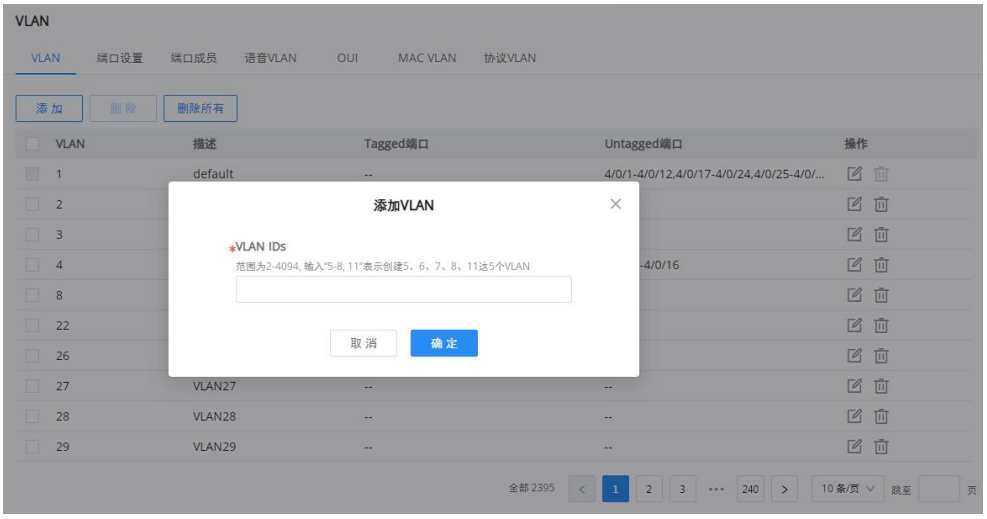


图 34 添加 VLAN

如果 VLAN 已经创建，也可以通过单击 按钮来编辑更多选项和设置，如描述、Tagged 和 Untagged 端口和 LAG。

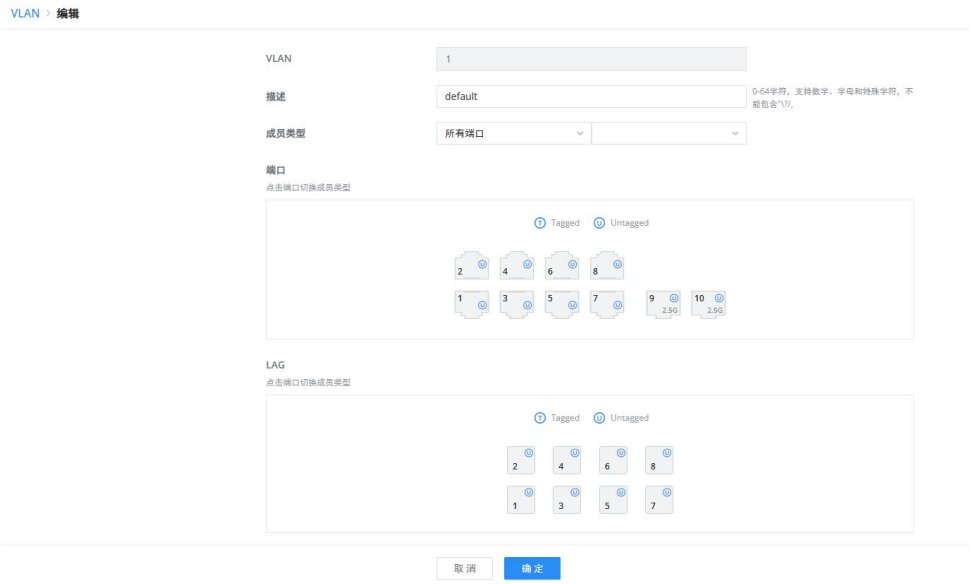


图 35 编辑 VLAN

表 11 编辑 VLAN

VLAN	指定的 VLAN ID。
描述	输入 VLAN ID 的简短描述，最长 64 字符，支持的字符具体为 ASCII 0x20~0x7E，但不包含"\?/,这 5 项

成员类型	从下拉框中选择： • **所有端口/端口组**：从所有端口中选择指定端口，从端口组中选择既定端口。 • **移除所有**：从此 VLAN 中删除所有端口 GE/LAG。 • **Tagged All**：Tag 此 VLAN 的所有端口 GE/LAG • **Untagged All**：Untag 此 VLAN 的所有端口 GE/LAG
GE	分别选择 tagged、untagged 或未选择的端口。 **注意：** • 未选择的端口将不属于 VLAN。 • tagged 端口需要标记帧（Trunk 端口），如将交换机连接到另一个交换机。 • untagged 端口需要未标记的帧（Access 端口），如将交换机连接终端设备。
LAG	分别选择 tagged、untagged 或未选择的 LAG。

有关 tagged 和 untagged 端口的详细信息，请参阅下表。

表 12 VLAN tagged 和 untagged

端口类型	**接收包**		**转发包**
	Untagged 包	**Tagged 包**	**Tagged 包**
Untagged	当接收到未标记的数据包时，端口将向数据包添加默认 VLAN 标签，即入口端口的 PVID。	如果端口允许数据包的 VID，则将接收数据包。如果端口禁止数据包的 VID，则数据包将被丢弃。	删除 VLAN 标签后，将转发数据包。
Tagged			数据包将以其当前 VLAN 标签转发。

VLAN 端口设置

端口设置页面可以通过指定链路类型（Hybrid、Access 和 Trunk）以及默认 VLAN 或 PVID 来配置每个端口和 LAG 上的 VLAN。用户还可以为所选端口启用入站过滤，选择接收的帧类型（All、Tagged Only 和 Untagged Only）。

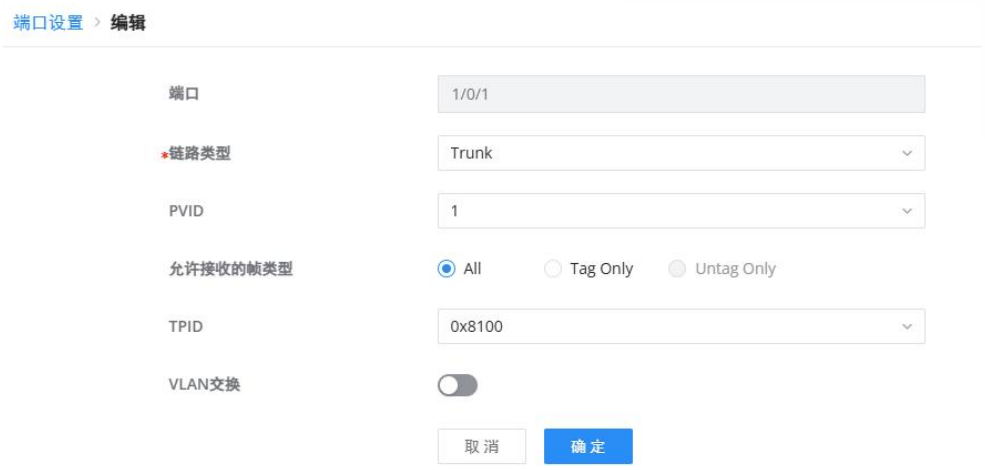


图 36 VLAN 端口设置-链路类型

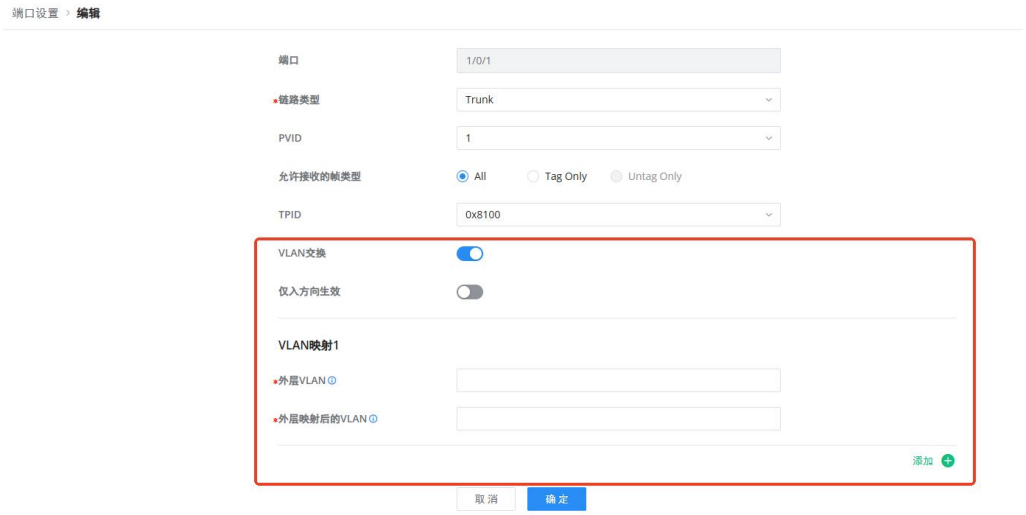


图 37 VLAN 端口设置-VLAN 交换

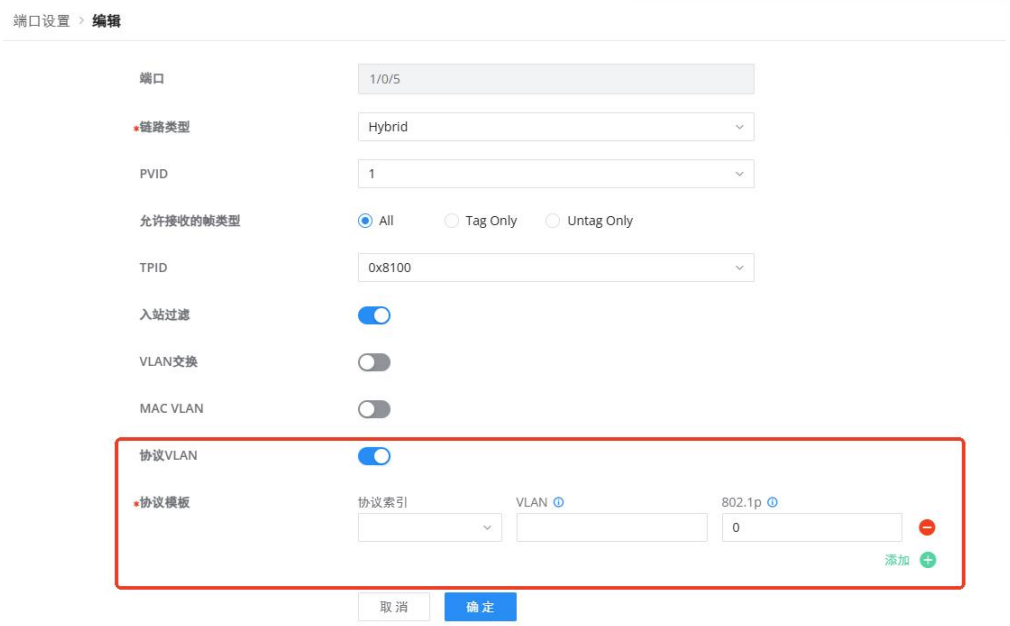


图 38 VLAN 端口设置-协议模板

表 13 VLAN 端口设置

端口	显示选择的端口
链路类型	选择链接类型： • Hybrid：用于交换机或交换机与计算机之间的连接。 • Access：用于连接交换机和用户终端。 • Trunk：用于交换机互联或交换机和路由器互联，可以承载多个不同 VLAN 的数据帧。 • QinQ：这是一种扩展的 VLAN 标记技术，在此基础上添加了额外的 VLAN 标签，也称为“双重标记”。它允许二层隧道，并且通常被服务提供商用来传输客户 VLAN。
PVID	输入默认 VLAN ID。
允许接收的帧类型	选择帧类型（Tag Only，Untag Only 或 All）。
入站过滤	设置是否启用接口的入站过滤功能。 入站过滤仅适用于 Hybrid 端口，默认情况下已启用。 **注意：**入站过滤是企业和互联网服务提供商（ISP）用来防止可疑流量进入网络的一种方法。

VLAN 交换	允许在端口级别将一个 VLAN ID 转换为另一个 VLAN ID。这在网络的不同部分使用不同的 VLAN ID 但需要相互通信的场景中非常有用。
MAC VLAN	允许交换机根据传入流量的 MAC 地址分配 VLAN。它可以用于更动态的 VLAN 分配，根据设备的 MAC 地址将其自动放置到特定的 VLAN 中。
协议 VLAN	允许根据帧中的协议类型（如 IP 或 ARP）进行 VLAN 分配。它可以将某些协议的流量分组到特定的 VLAN 中，以便更轻松地进行网络管理。

VLAN 端口成员

在此页面中，用户可以分别为每个端口定义 Tagged 和 Untagged VLAN（成员）。

注意：

- 例如：输入“5-8，11”表示关联“5，6，7，8 和 11”的 5 个 VLAN。

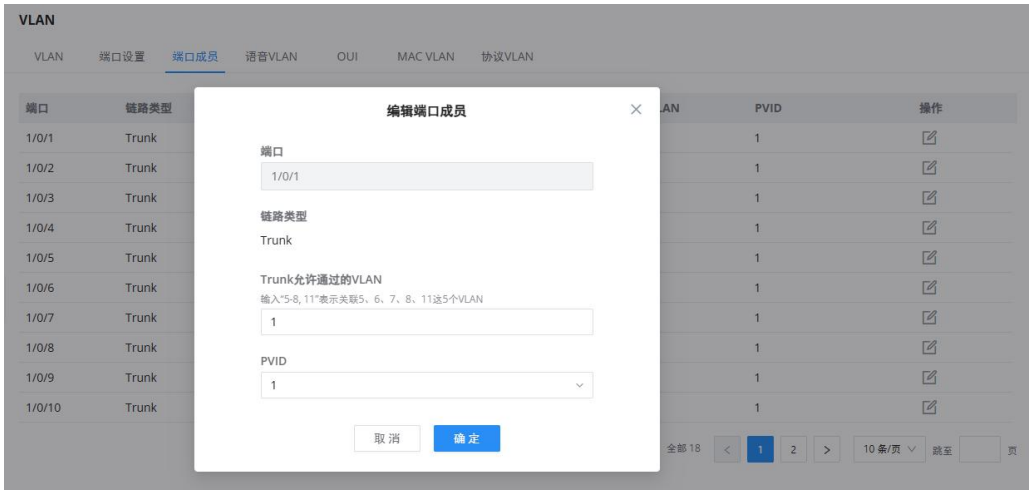


图 39 VLAN 端口成员-Trunk

Trunk 允许通过的 VLAN 可以配置在交换机上尚不存在的 VLAN，并且仅对已配置的 VLAN 有效。

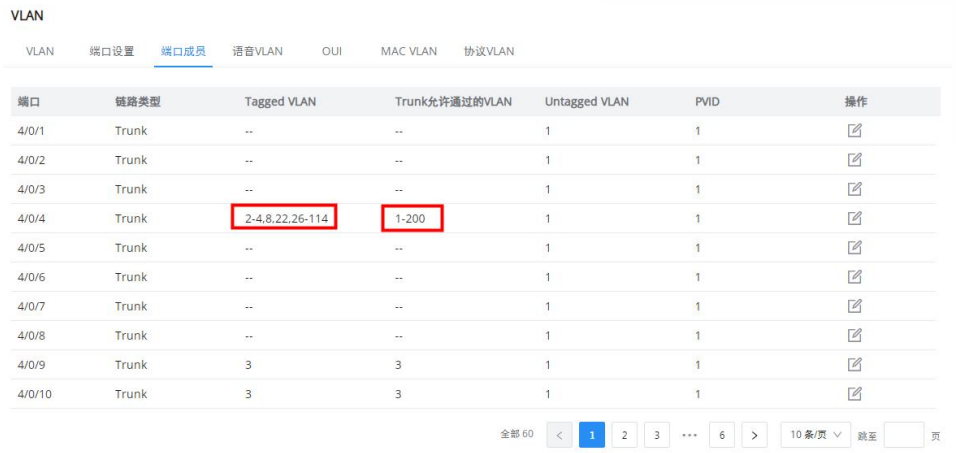


图 40 VLAN 端口成员

语音 VLAN

语音 VLAN 是专门为语音数据流配置的 VLAN。通过配置语音 VLAN 并添加语音设备到语音 VLAN 的端口，可以对语音数据执行 QoS 配置，确保语音数据流的传输优先级和语音质量。

语音 VLAN 优势：

- 改善语音质量：通过将语音流量与其他类型的网络流量隔离，语音 VLAN 有助于减少延迟和抖动，从而避免电话通话中出现卡顿或失真的音频。
- 减少拥塞：通过优先处理语音流量，语音 VLAN 有助于阻止其他类型的网络流量干扰电话通话，即使在网络使用高峰期也能保持通话质量。
- 简化网络管理：语音 VLAN 可以简化网络管理，使故障排除和解决与语音相关的问题变得更加容易。

例如，当 IP 电话连接到 GWN780x Pro 交换机端口时，交换机会优先处理语音 VLAN 中的流量，确保语音数据包在其他类型的数据包之前被转发。

用户可以选择多种方式来设置语音 VLAN：

- 通过 LLDP 自动加入语音 VLAN
- 通过 LLDP Tagged OUI
- 通过 VLAN Tag Tagged OUI
- Untagged OUI

获取更多细节，请访问此配置指导手册：GWN78xx(P)-Voice VLAN Guide。

配置语音 VLAN，请访问 **Web UI → 以太网业务 → VLAN → 语音 VLAN**。

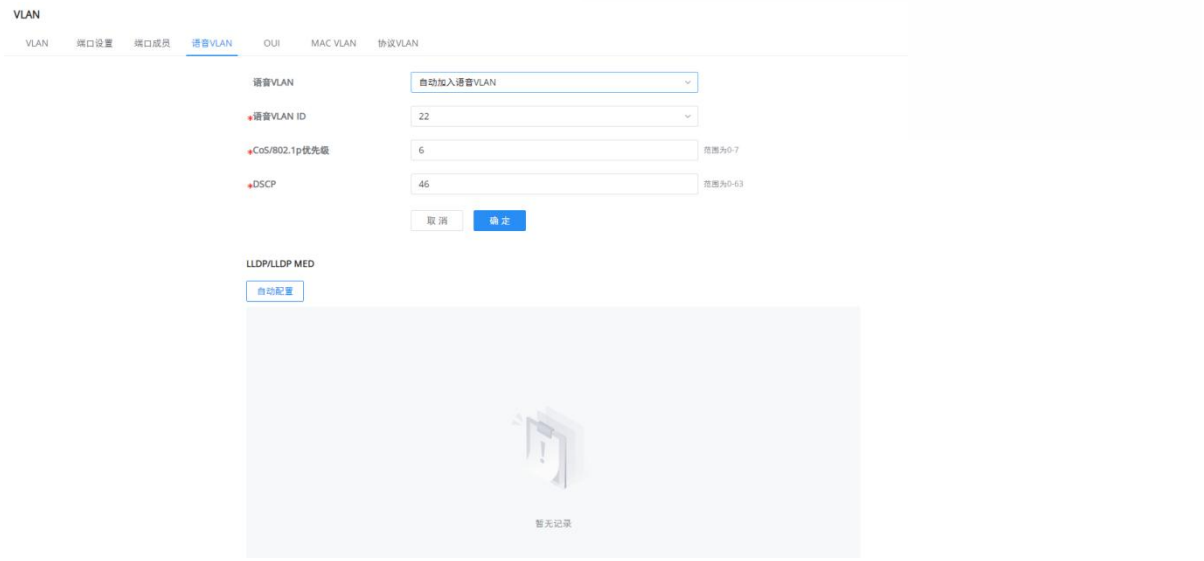


图 41 语音 VLAN

表 14 语音 VLAN

语音 VLAN	设置语音 VLAN 模式。默认禁用。 • 禁用 • 自动加入语音 VLAN • Tagged OUI • Untagged OUI
语音 VLAN ID	从 VLAN 列表中选择 VLAN 作为语音 VLAN。 **注意：**默认 VLAN 1 不能用作语音 VLAN
CoS/802.1p 优先级	设置是否启用 CoS 重标记。
如果设置自动加入语音 VLAN	
DSCP	DSCP 优先级，有效范围为 0-63，默认 46
LLDP/LLDP-MED 自动配置	如果选择自动加入语音 VLAN，则需要进入 LLDP 设置网络策略。LLDP 自动配置已添加到语音 VLAN，以便用户能够更轻松、更快速地一键配置。
如果设置 Tagged OUI 或 Untagged OUI	

CoS 重标记	指定 CoS 优先级，范围为 0 到 7。 默认值为 6。值越高，优先级越高。
老化时间 (分钟)	设置语音 VLAN 的老化时间。 范围为从 30 到 65536 的整数，默认值为 1440 分钟。
编辑端口设置	**端口：** 显示选择的端口。 **状态：** 设置是否启用端口的语音 VLAN 功能。 默认情况下禁用 **模式：** 在端口上设置语音 VLAN 的工作模式，选项为｛手动、自动｝。默认设置为手动。 **注意：** 当设置为“手动”时，必须手动将端口添加到语音 VLAN，并且需要使用 LLDP 功能；当设置为“自动”时，源 MAC 地址与数据包中的 OUI 匹配的端口将自动添加到语音 VLAN。

OUI

OUI 地址是 IEEE 分配给设备供应商的唯一标识符。它包括 MAC 地址的前 24 位。您可以根据 OUI 地址识别设备属于哪个供应商。下表显示了几个制造商的 OUI 地址。还可以根据用户需要自定义添加自定义 OUI。

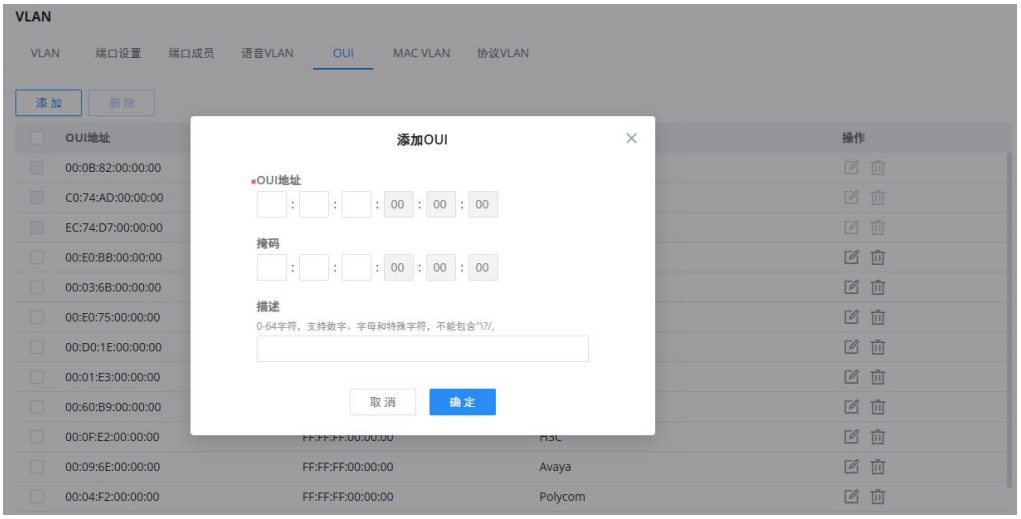


图 42 OUI

MAC VLAN

MAC VLAN 是一种网络技术，其中每个 VLAN 基于传入帧的源 MAC 地址。具有相同 MAC 地址的设备共享一个 VLAN。这种分割使得在相同 VLAN 内的设备之间可以基于 MAC 地址进行隔离通信。

VLAN 根据数据帧的源 MAC 地址进行划分。通过配置的 MAC 地址和 VLAN 映射表，当交换机接收到一个未标记的帧时，它会根据映射表将指定的 VLAN 标签添加到数据帧中。

要将 MAC 地址添加到 VLAN 映射中，请点击“**添加**”按钮，然后指定 MAC 地址、掩码长度、VLAN 和优先级（802.1p）。

注意：仅针对 Hybrid 端口生效。

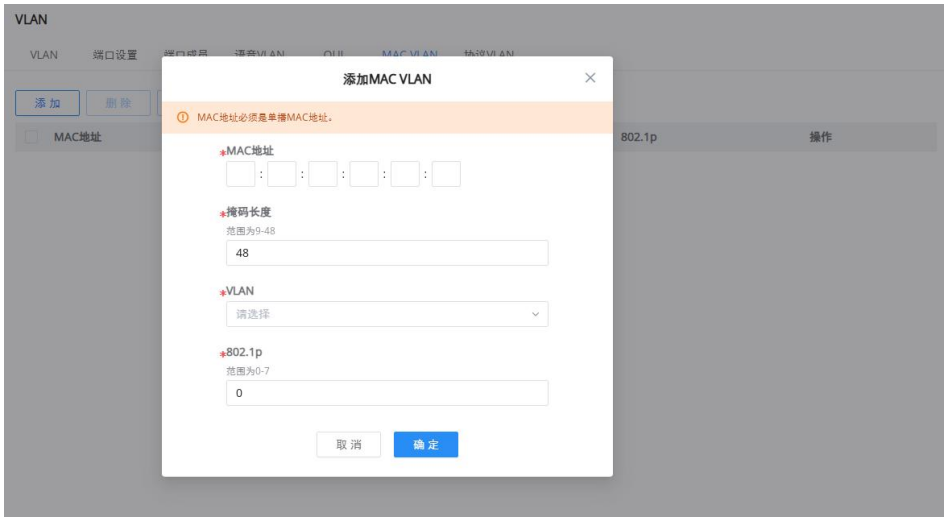


图 43 MAC VLAN

协议 VLAN

VLAN 根据协议（家族）类型和数据帧归属的封装格式进行划分。当交换机接收到一个未标记的帧时，通过配置的协议域和 VLAN 映射表，它会根据映射表添加指定的 VLAN 标签。

注意：仅针对 Hybrid 端口生效。

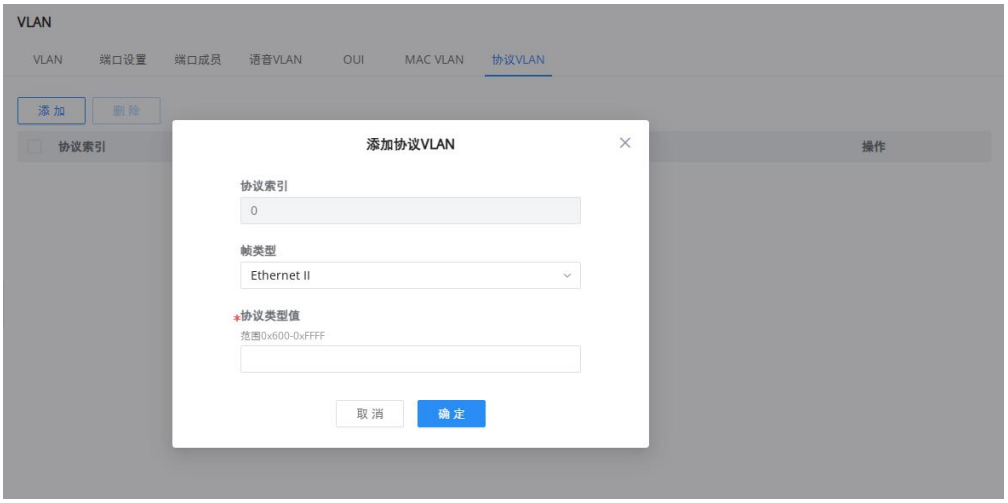


图 44 协议 VLAN

生成树

STP（生成树协议），运行 STP 的设备通过交换信息来发现网络中的环路和阻塞端口，这样环形网络可以被剥离，形成树状拓扑的无环网络，以防止数据包在网络中被重复和无休止地转发。

PVST(+)或 RPVST(+)可以在每个 VLAN 内都拥有一棵生成树，能够有效地提高链路带宽的利用率。PVST(+)或 RPVST(+)可以简单理解为在每个 VLAN 上运行一个 STP 或 RSTP，不同 VLAN 之间的生成树完全独立。

BPDU（网桥协议数据单元）是 STP、RSTP 和 MSTP 使用的协议数据。BPDU 中携带了足够的信息，以确保生成生成树。STP 通过在设备之间传输 BPDU 来确定网络的拓扑。

此页面允许用户配置生成树协议（STP）属性，包括 STP 模式（STP、RSTP、MSTP、PVST(+)或 RPVST(+)）、路径开销、桥优先级、最大跳数、联络时间和最大老化时间以及转发延迟时间。

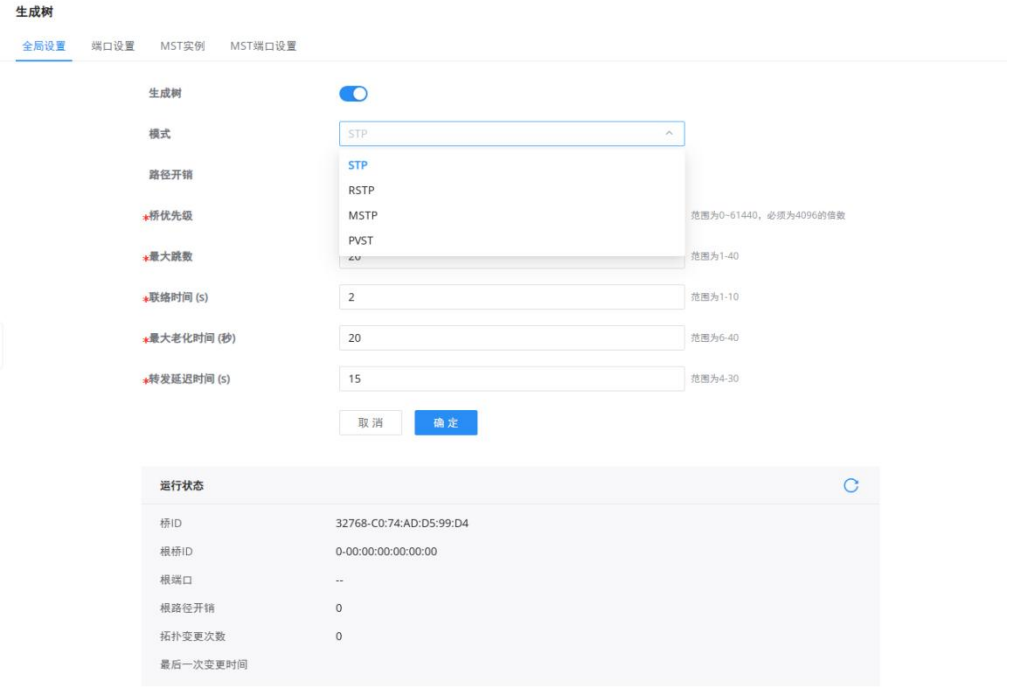


图 45 生成树-全局设置

表 15 生成树-全局设置

生成树	设置是否启用生成树
模式	设置生成树（STP）的模式。 • **STP**：启用生成树（STP） • **RSTP**：启用快速生成树（RSTP）。 • **MSTP**：启用多生成树协议（MSTP）。

	• **PVST(+)**：启用快速生成树协议（PVST(+)）。 • **RPVST(+)**：启用基于 VLAN 的快速生成树协议（RPVST(+)）。
忽略 BPDU VLAN	此功能允许交换机忽略桥接协议数据单元（BPDU）中的 VLAN 特定信息。这可以防止 VLAN 配置影响跨多个 VLAN 的生成树协议（STP）决策。
路径开销	指定路径开销方法（短、长）。默认值为短。
桥优先级	选择网桥优先级。在 STP 网络中，具有最小网桥 ID 的设备被选为根网桥。 默认值为 32768。 **注意：** • 有效范围为 0~61440，必须是 4096 的倍数。 • PVST 模式不支持配置。
最大跳数	选择最大跳数（范围为 1-40）。默认值为 20。 **注意：**PVST 模式不支持配置。
联络时间 (秒)	以秒为单位指定联络时间（范围为 1-10）。默认值为 2。 **注意：** • 运行 STP 协议的设备发送 BPDU 的时间间隔，设备使用该时间间隔来检测链路是否存在故障。 • PVST 模式不支持配置。
最大老化时间 (秒)	选择端口的 BPDU 数据包的老化时间（范围为 6-40）。默认值为 20。 **注意：**PVST 模式不支持配置。
转发延迟时间 (秒)	指定转发延迟时间（范围为 4-30）。默认值为 15。 **注意：** • 3 个时间配置时，必须满足如下关系：（联络时间+1）*2≤最大老化时间≤（转发延迟时间-1）*2 • PVST 模式不支持配置。

端口设置

要在每个端口和 LAG 上配置 STP/RSTP，请导航到 **WEB UI→生成树→端口设置**，然后单击“**编辑**”按钮。

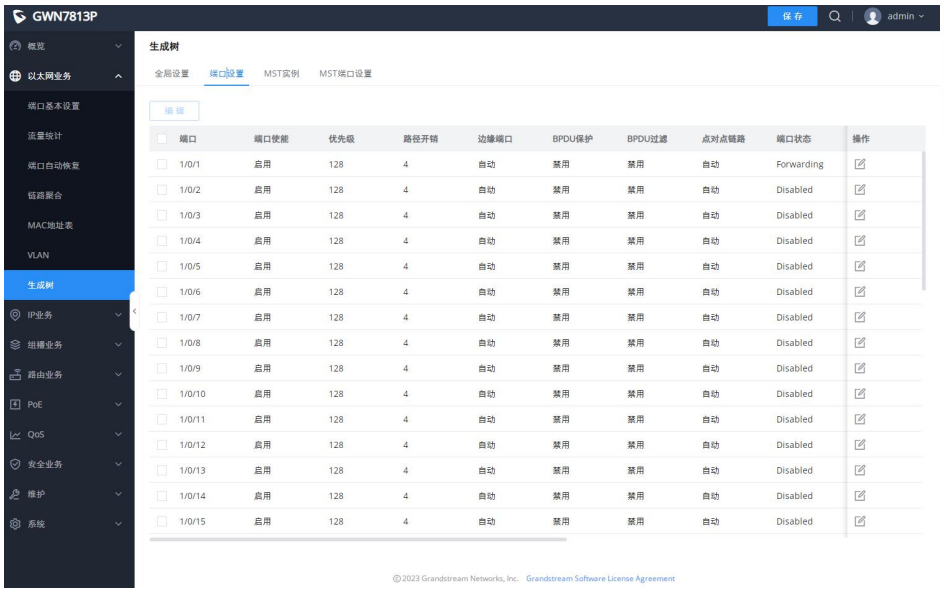


图 46 生成树-端口设置

对于每个端口或 LAG，用户可以启用 STP 并指定优先级、路径开销、边缘端口、BPDU 保护和过滤以及点对点链路。

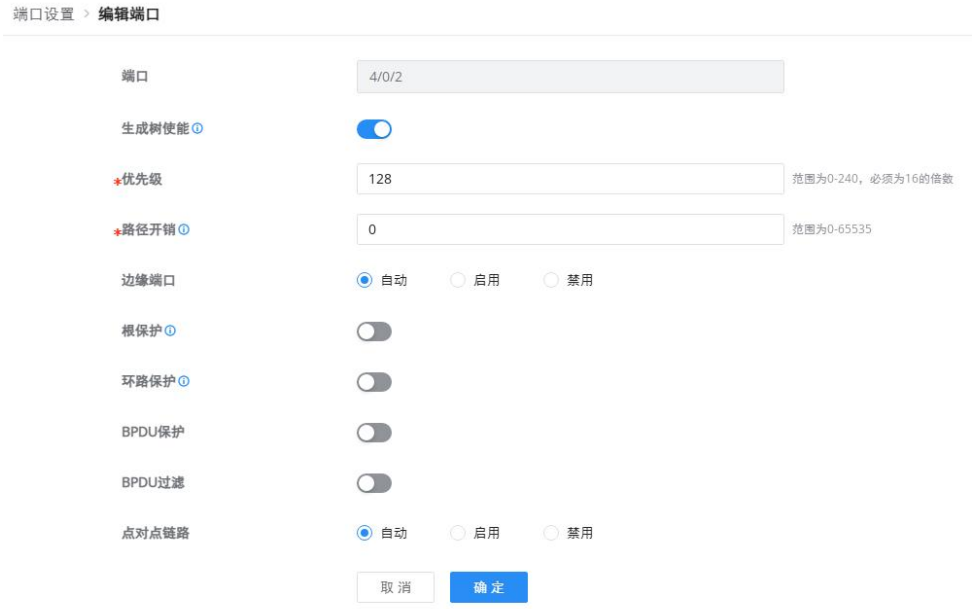


图 47 生成树-编辑端口设置

表 16 生成树-编辑端口设置

端口	显示所选的 GE/LAG 端口。
启用 STP	设置是否启用该端口的 STP。

优先级	优先级是决定端口是否被选为根端口的重要依据，在相同条件下优先级较高的端口将被选为根端口。值越小，优先级越高。取值范围为 0-240 间的整数，步长为 16，默认值为 128。
路径开销	在指定的生成树上设置端口的路径开销。默认值为 0，表示自动执行路径成本计算。 **注意：**当全局设置的“路径开销”为“长”时，有效范围为 0~200000000；当全局设置的“路径开销”为“短”时，取值范围为 0~65535。0 表示自动。
边缘端口	设置是否启用边缘端口，默认情况下为自动。 **注意：** • 当端口直接连接到用户终端或服务器，而不是任何其他交换机或共享网段时，该端口被视为边缘端口。边缘端口不会在网络拓扑更改时造成循环。 • 在边缘模式下，接口将在连接后立即进入转发状态。在自动模式下，它将检测端口是否为边缘端口。
根保护	通过防止指定端口成为根端口来保护根桥，从而保护当前根桥不被低优先级的 BPDU 取代。
环路保护	通过确保在停止接收 BPDU 的端口上处于阻塞状态，防止第二层循环，从而避免网络循环的形成。
BPDU 保护	设置是否启用 BPDU 保护。. **注意：**BPDU 保护通过将此端口设置为错误状态，并在收到 BPDU 时关闭端口来进一步保护交换机。
BPDU 过滤	设置是否启用 BPDU 过滤。 **注意:** 丢弃所有 BPDU 数据包，不会发送任何 BPDU。
点对点链路	选择点到点链路（自动、启用或禁用）。默认值为自动。 **注意：** • 如果设置为自动，则自动确定此端口的链路类型 STP。 • 当且仅当"RSTP"模式下生效。

MST 实例

MST（Multiple Spanning Tree Instance）或多生成树实例允许将不同 VLAN 的流量映射到不同的 MST 实例。GWN7801P Pro-GWN7802P Pro-GWN7803(PL/PH) Pro 交换机最多支持 16 个独立的 MST 实例（0-15），GWN7806PL/PH Pro 交换机最多支持 64 个独立的 MST 实例（0-63），每个实例可以与多个 VLAN 相关联。

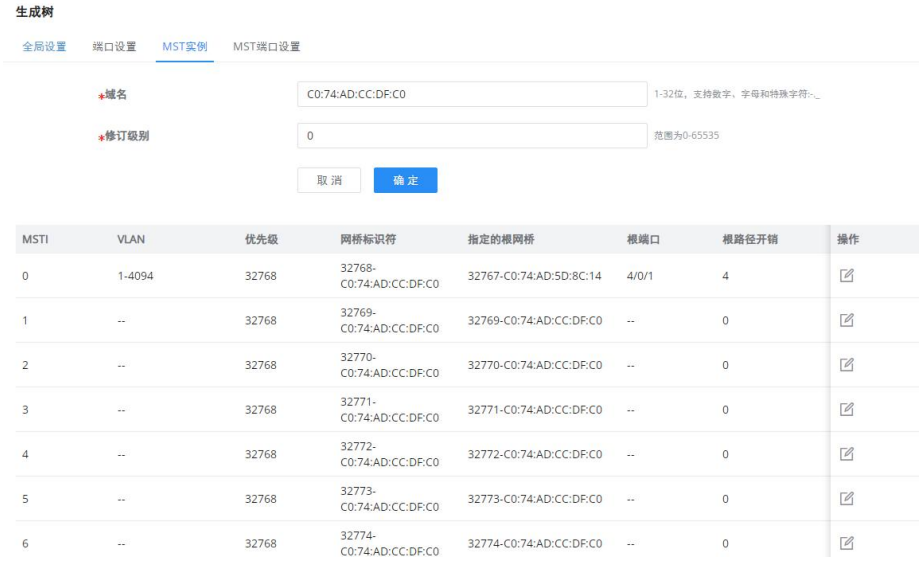


图 48 MST 实例

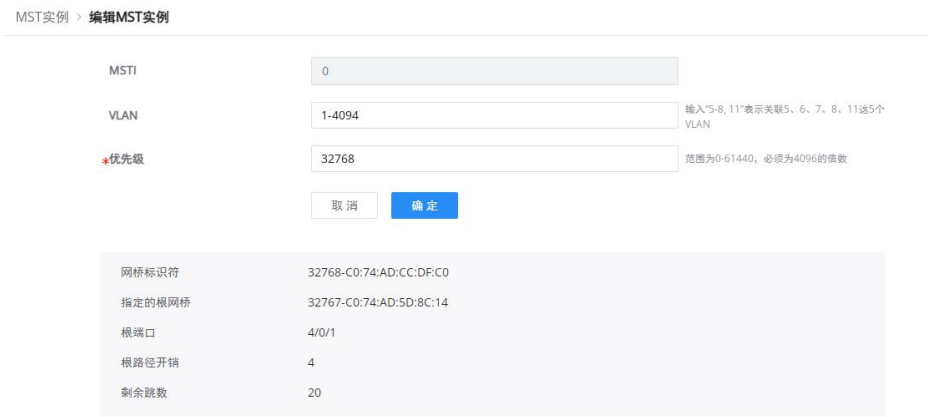


图 49 编辑 MST 实例

MST 端口设置用于配置每个 MST 实例的物理端口/LAG 组设置。该表显示了每个端口的 MST 参数。

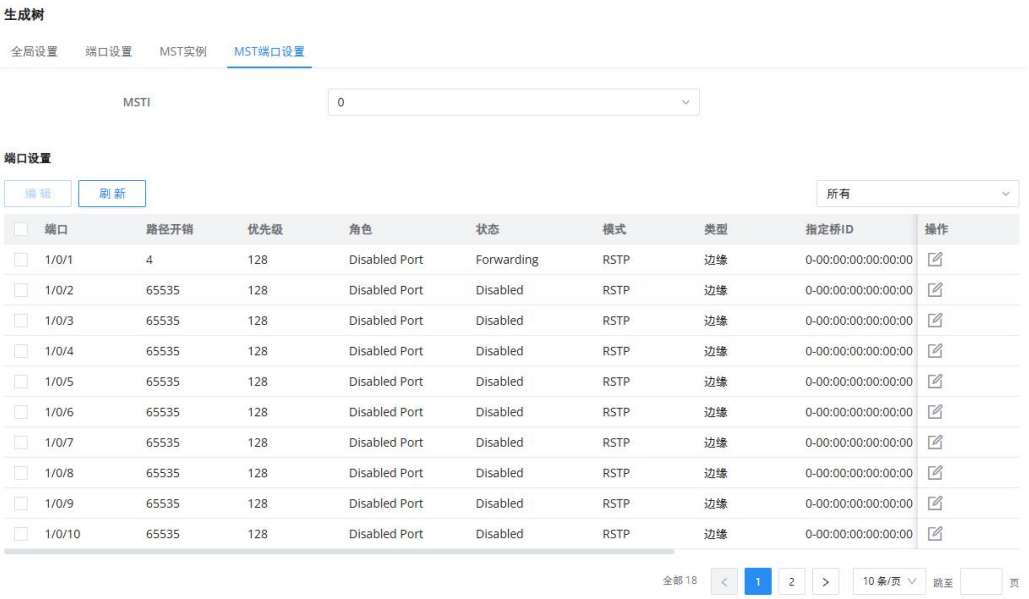


图 50 MST 端口设置

单击“**编辑**”按钮，分别编辑每个端口/LAG 的 MST 端口设置，用户还可以指定每个端口/LAG 的路径开销和优先级。

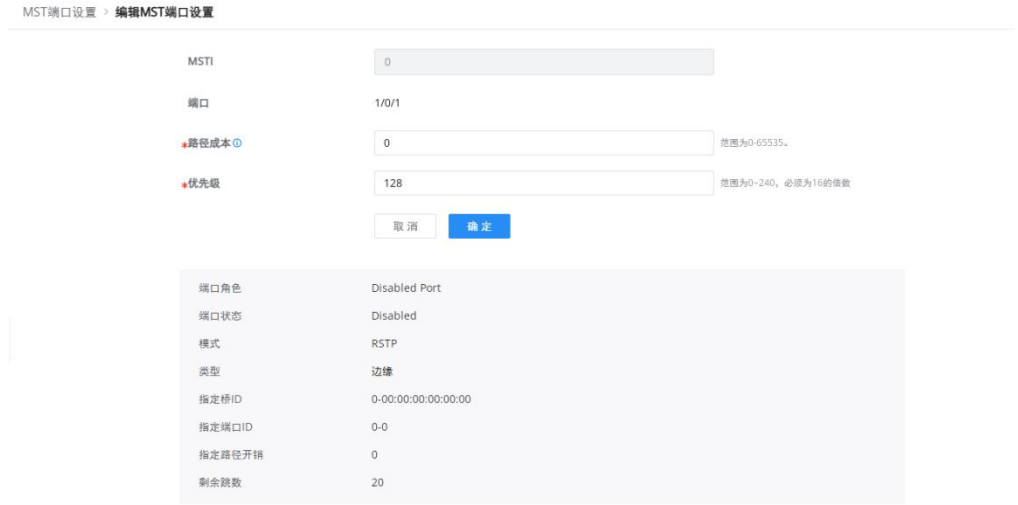


图 51 编辑 MST 端口

PVST(+)/RPVST(+) VLAN 设置

PVST(+)/RPVST(+)基于 VLAN 进行实例设置。

GWN7801P Pro-GWN7802P Pro-GWN7803(PL/PH) Pro 交换机最多支持 16 个独立的 PVST VLAN 实例，GWN7806PL/PH Pro 交换机最多 64 个独立的 PVST VLAN 实例，每个实例对应 1 个 VLAN。

图 52 VLAN 设置

表 17 VLAN 设置

VLAN	显示选择的 VLAN。
PVST(+)/RPVST(+)使能	设置是否在 VLAN 上开启 PVST(+)/RPVST(+)功能，默认仅 VLAN 1 使能，其余 VLAN 禁用，且在下方可见剩余可以使能的 VLAN 个数。
桥优先级	选择网桥优先级。在 PVST(+)/RPVST(+)网络中，具有最小网桥 ID 的设备被选为根网桥。 默认值为 32768。 **注意：**有效范围为 0~61440，必须是 4096 的倍数。
联络时间 (秒)	以秒为单位指定联络时间（范围为 1-10）。默认值为 2。 **注意：**运行 PVSt 协议的设备发送 BPDU 的时间间隔，设备使用该时间间隔来检测链路是否存在故障。
最大老化时间 (秒)	选择端口的 BPDU 数据包的老化时间（范围为 6-40）。默认值为 20。
转发延迟时间 (秒)	指定转发延迟时间（范围为 4-30）。默认值为 15。 **注意：**3 个时间配置时，必须满足如下关系：（联络时间+1）*2 ≤最大老化时间≤（转发延迟时间-1）*2

PVST(+)/RPVST(+)端口设置

PVST(+)/RPVST(+)端口设置用于为每个 VLAN 实例配置 GE 端口/LAG 组。它还显示了每个端口的角色、指定的桥接 ID、指定的端口 ID 和指定的路径成本。

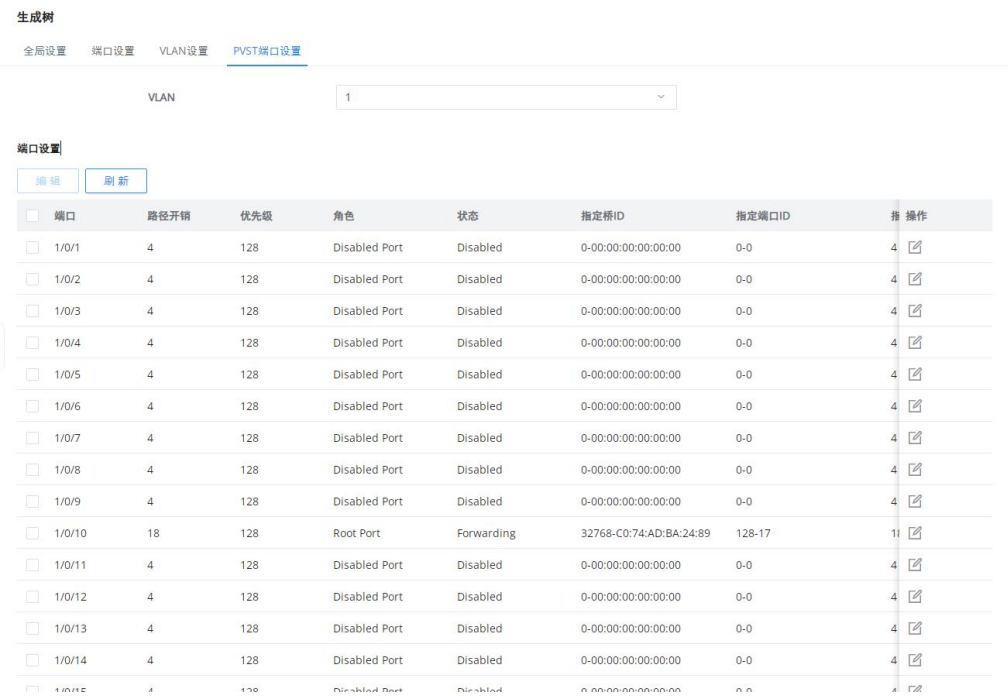


图 53 PVST(+)/RPVST(+)端口设置

单击“编辑”按钮，分别编辑每个端口/LAG 的 PVST(+)/RPVST(+)端口设置，用户还可以指定每个端口/LAG 的路径开销和优先级。

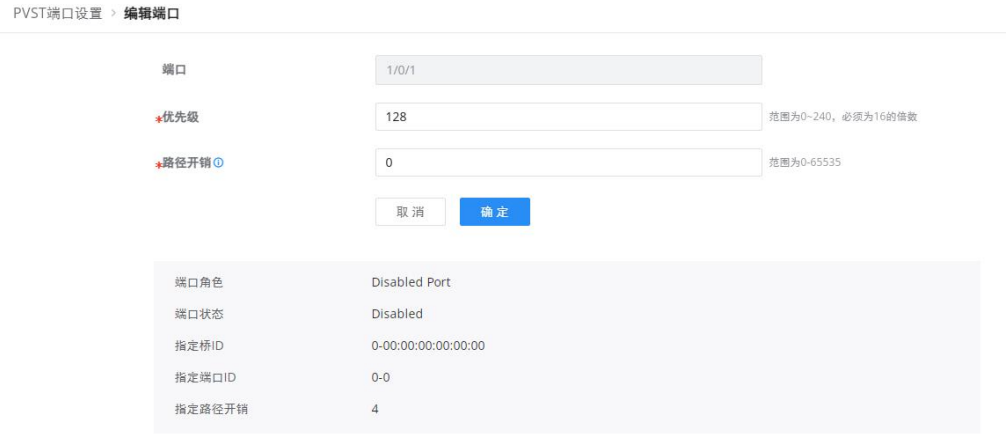


图 54 PVST(+)/RPVST(+)端口设置

表 18 PVST(+)/RPVST(+)端口设置

端口	显示选择的端口。
优先级	设置端口优先级。有效范围为 0-240，默认值为 18。 **注意：**该值必须是 16 的倍数。

路径开销	为指定的生成树配置端口上的端口路径成本。该值必须是 0-65535 之间的整数。默认值为 0，表示路径成本计算将自动执行。

IP 业务

VLAN IP 接口

不同 VLAN 中的主机无法直接通信，需要通过路由器或 3 层交换协议进行转发。

VLAN 接口是 3 层模式下的虚拟接口，主要用于实现 VLAN 之间的第三层通信，不作为物理实体存在于设备上。每个 VLAN 通过为其配置 IP 地址来对应一个接口，可以用作 VLAN 中每个端口的网关地址，以便不同 VLAN 之间的数据包可以通过 VLAN 接口在第 3 层路由上相互转发。GWN 交换机支持 IPv4 和 IPv6 接口。

配置 VLAN IP 接口，请前往 **Web GUI→IP→VLAN IP 接口**页面。

IPv4 接口

点击“**添加**”按钮增加 VLAN IPv4 接口。

图 55 添加 VLAN IPv4 接口

使用 向 DHCP 服务器请求新的 IP 地址。此操作会弹出确认对话框；点击“确定”将获取新的 IP 地址，成功获取后该地址可能会发生变化。

图 56 刷新 IP 地址

表 19 VLAN IPv4 接口

VLAN	设置添加的 VLAN IPv4 接口 ID
IPv4 地址类型	• **DHCP**：主机将会自动从 DHCP 地址池（如路由器）中获取 IP 地址。 • **静态 IP**：主机根据 DHCP 地址池（如路由器）的网段，配置相同不冲突的 IP 地址进行设置。
网关优先级	有效范围为 2-255，值越小优先级越高。
IPv4 地址	设置 VLAN 接口的 IPv4 地址，点分十进制格式。
掩码	设置 VLAN 接口的网络掩码。 • 网络掩码：设置子网掩码，点分十进制格式。 • 掩码长度：设置掩码长度，有效范围为 8-30。
MTU	设置 VLAN 接口的 MTU 值，取值范围为 1280-9216，默认 1500

注意：

网关使用优先级：

- 静态配置的网关优先级最高。
- 指定优先级的网关，优先级值越低，优先级越高。
- 如果优先级值相同，则优先使用 VLAN ID 小的网关。

IPv6 接口

点击“**添加**”按钮增加 VLAN IPv6 接口。

图 57 添加 VLAN IPv6 接口

表 20 添加 VLAN IPv6 接口

VLAN	设置添加的 VLAN 接口 ID
IPv6 使能	设置是否开启 VLAN IPv6 能力。默认关闭
链路本地地址	设置 VLAN 接口的链路本地地址。 **注意：**交换机所有 VLAN 接口共用一个链路本地地址。 • 自动生成 • 手动配置：默认 fe80://64
全球单播地址	设置 VLAN 接口的全球单播地址。 • 有状态 DHCPv6：通过 DHCPv6 服务器自动获取 IPv6 地址和前缀。 • 无状态 DHCPv6：根据路由通告获取前缀和 DNS 等，借助 RA 报文的前缀进行地址分配。 • 手动配置 • 无状态自动配置：利用 EUI-6 格式，利用 RA 报文中的前缀信息结合设备 MAC 地址自动生成。
网关优先级	有效范围为 2-255，值越小优先级越高。
MTU	设置 VLAN 接口的 MTU 值，取值范围为 1280-9216，默认 1500

IPv6 路由通告

IPv6 路由通告(RA)是路由器发送的消息，用于向网络上的设备提供信息，例如默认网关、DNS 服务器和网络前缀。这些广告帮助设备自动配置其 IP 地址和路由，而无需手动配置。在 VLAN IP 接口部分，您可以为每个 VLAN 配置 RA，以管理 IPv6 网络设置。

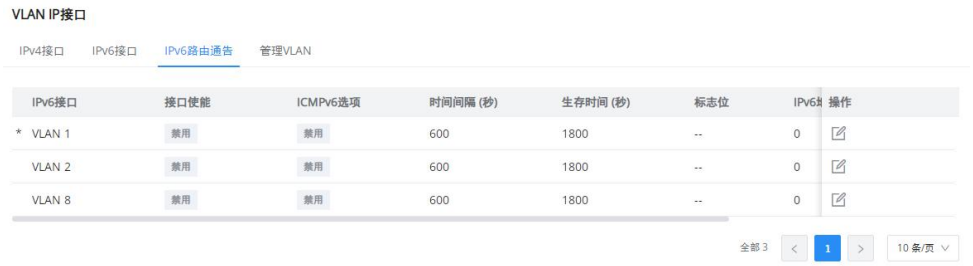


图 58 IPv6 路由通告

编辑 IPv6 路由通告页面时，您可以为特定 VLAN 自定义设置。这包括启用或禁用接口、设置路由信息，以及配置通告的超时和生命周期。您还可以定义 IPv6 地址和前缀，调整其他配置的标志，以及设置默认路由

的优先级。这允许您调整通告的行为，以满足您的网络需求。

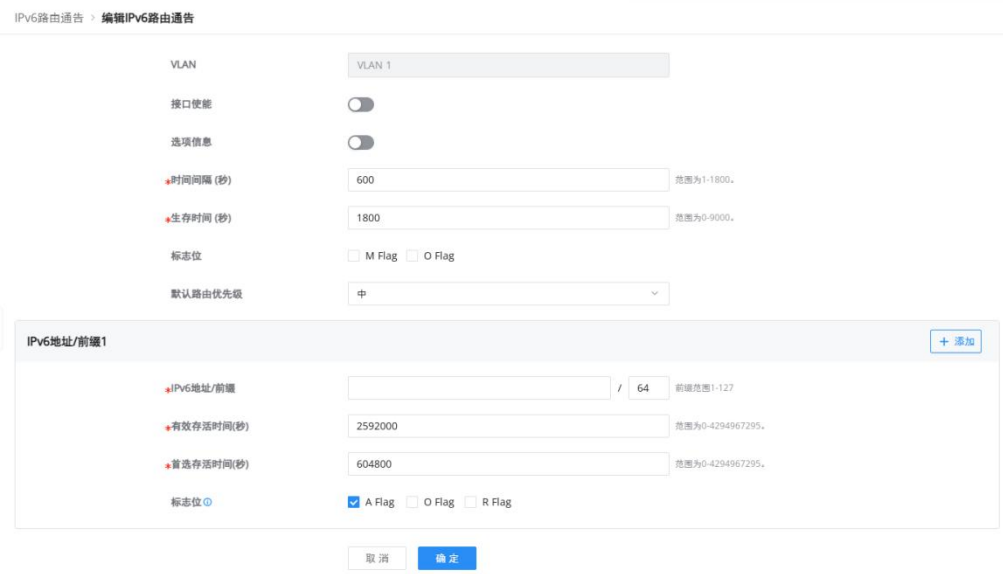


图 59 编辑 IPv6 路由通告

表 21 编辑 IPv6 路由通告

VLAN	显示所选的 VLAN 接口 ID
接口使能	设置是否使能 VLAN 接口路由通告功能。默认关闭
选项信息	设置是否在 RA 报文中添加路由选项信息。默认关闭
时间间隔 (秒)	设置发送 RA 报文的时间间隔，取值范围为 1-1800 的整数，默认 600
生存时间 (秒)	设置 RA 报文的存活时间，取值范围为 0-9000 的整数，默认 1800。设置为 0 表示下级设备不会将交换机地址更新到自己的默认路由表项中。
标志位	• M Flag：设置是否在 RA 报文中添加有状态自动配置地址的标志位，默认关闭，即下级主机通过无状态自动配置获取 IPv6 地址（通过 RA 报文向主机发布 IPv6 地址前缀信息自动生成 IPv6 地址）。若开启，则下级主机通过有状态自动配置获取 IPv6 地址。 • O Flag：设置是否在 RA 报文中添加有状态自动配置其他信息

	的标志位，默认关闭，即下级主机进行无状态自动配置（通过 RA 报文向主机发布除 IPv6 地址外的其他配置信息，包括生存时间、邻居可达时间和重传时间、链路的 MTU 值等）。若开启，下级主机可通过有状态自动配置获取除 IPv6 地址外的其他配置信息。
IPv6 地址/前缀	• IPv6 地址/前缀 • 有效存活时间 (秒)：设置前缀信息的有效存活时间，用于确定前缀的 on-link 状态。取值范围为 0-4294967295 的整数，默认 2592000 • 首选存活时间 (秒)：设置前缀信息的首选存活时间，不能大于有效存活时间。取值范围为 0-4294967295 的整数，默认 604800 • 标志位：选项有 A Flag、O Flag 和 R Flag，默认选中 A Flag。A Flag 表示配置的前缀可以用于无状态地址自动配置，A Flag 标志位是 RA 报文前缀选项中的自治地址配置标志位；O Flag 表示本链路内的主机 RA 报文中的前缀不是分配给本地链路的；R Flag 表示主机使用路由器的全局 IP 地址，而不是链路本地地址。 **注意：**支持添加多组，至多 8 组
默认路由优先级	设置 RA 报文中的默认路由优先级，选项有低、中和高，默认中。

管理 VLAN

MGMT VLAN（管理 VLAN）：顾名思义，用于管理交换机的 VLAN，例如借助管理 VLAN 来使用 Telnet、SSH、syslog 等协议进行远程定位。默认的管理 VLAN 是 VLAN 1，用户可以从下拉列表中选择其他 VLAN 来替换。

当你为管理 VLAN 接口分配 IP 地址时，系统会将此 IP 配置与设备的第 3 层 IP 接口配置中的相应 VLAN 接口同步。这确保用于管理设备的 IP 地址与 VLAN 的路由和交换配置一致。例如，如果你在 VLAN 2 上为管理 VLAN 配置一个 IP 地址 192.168.2.100，那么这个 IP 也会在 VLAN 2 的 IP 接口配置中反映，确保管理功能和路由功能保持一致。

图 60 管理 VLAN

DHCP 服务器

当使用静态 IP 创建 VLAN 接口时，可以使用此 VLAN 接口创建 DHCP 服务器，为下级设备分配 IP 地址。

点击前往 **Web UI→IP→DHCP 服务器**页面。

步骤 1. 开启 **DHCP 服务**。

图 61 DHCP-全局设置

步骤 2. 在**地址池设置**页面，点击“**添加**”按钮添加地址池。

注意：

- 全局地址池仅用于 DHCP 中继分配 IP 地址。
- 当 VLAN 配置为使用 DHCP 自动获取 IP 地址时，系统现在可以优先选择使用哪个网关（负责将流量路由到其他网络的设备）。

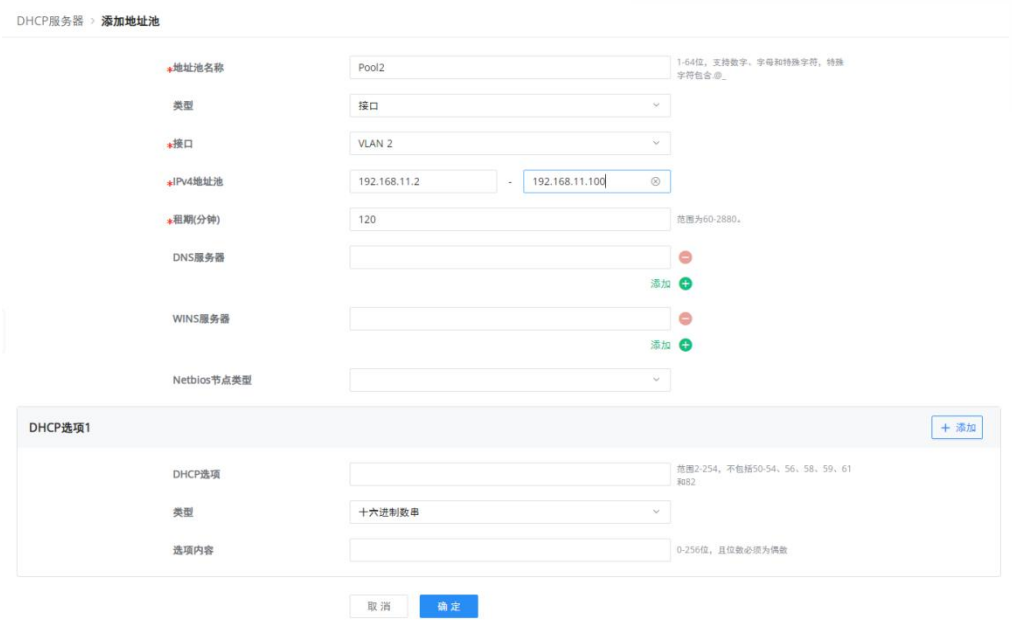


图 62 DHCP-添加地址池

步骤 3. 使用 DHCP 服务器时，地址表将显示主机设备的 MAC 地址和 IP 地址。也可以通过点击“**添加**”指定特定设备绑定固定静态 IP 地址；还可以为动态客户端绑定静态 IP 地址。

图 63 DHCP-地址表

在此页面，用户可以配 DHCP 选项，如类型、服务（选项 43）和选项内容。还可以通过点击下面所示的“**添加**”来添加更多 DHCP 选项：

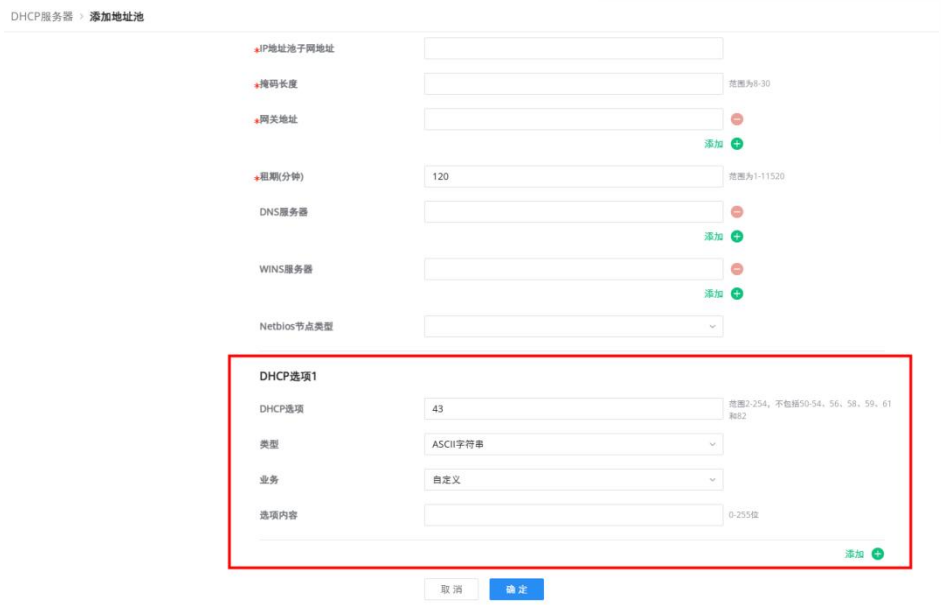


图 64 DHCP 地址池-添加地址池-DHCP 选项

DHCP 中继

GWN780x Pro 系列交换机上的 DHCP 中继帮助网络设备在完全不同网络上的客户端和服务器之间传递 DHCP 消息。当 DHCP 服务器需要为不同子网（或 VLAN）上的客户端提供服务时，DHCP 中继代理是一种可以在客户端的子网和服务器的子网之间路由的网络设备。中继代理从客户端获取广播请求并将其发送到服务器，将其自己的接口地址作为数据包中的网关地址（giaddr）字段。通过这种方式，服务器可以判断客户端所在的子网，并分配合适的 IP 地址，然后服务器将回复发送给中继代理，中继代理将其传递给客户端。

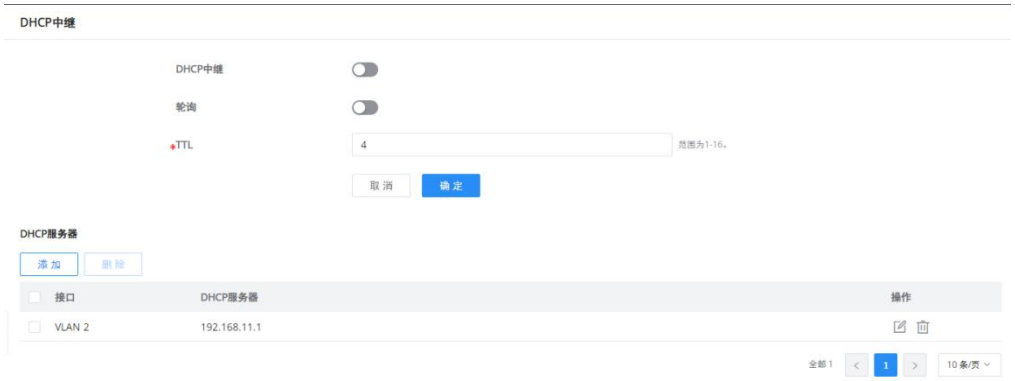


图 65 DHCP 中继

表 22 DHCP 中继

DHCP 中继	设置是否开启全局 DHCP 中继功能。默认关闭

轮询	设置是否开启 DHCP 中继的轮询功能。默认关闭
TTL	设置 DHCP 请求报文在经过 DHCP 中继三层转发之后的 TTL 值，取值范围为 1-16 的整数，默认 4
DHCP 服务器	
接口	从已有的 VLAN 接口中选择
DHCP 服务器	设置 DHCP 服务器地址。 支持添加多个，至多 10 个。 **注意：**DHCP 服务器地址不能为 DHCP 中继网关的接口 IP 地址，否则会导致 DHCP 客户端无法获取 IP 地址。

ARP 表

地址解析协议 ARP 是用来将 IP 地址解析为 MAC 地址的协议。在局域网中，当主机或其它三层网络设备有数据要发送给另一台主机或三层网络设备时，需要知道对方的网络层地址（即 IP 地址）。因为 IP 地址必须封装成帧才能通过物理网络发送，因此发送方还需要知道接收方的实际物理地址（即 MAC 地址），这就需要一个从 IP 到 MAC 地址的映射。ARP 即实现将 IP 地址解析为 MAC 地址。主机或三层网络设备上会维护一张 ARP 表，存储 IP 地址与 MAC 地址的关系。ARP 表项包括动态 ARP 表项和静态 ARP 表项。

- **动态 ARP 表项：**由 ARP 协议通过 ARP 报文自动生成和维护，可以被老化，可以被新的 ARP 报文更新，可以被静态 ARP 表项覆盖。当到达老化时间、接口 down 时，设备会立即删除响应的动态 ARP 表项。
- **静态 ARP 表项：**由网络管理员手工建立的 IP 地址和 MAC 地址之间固定的映射关系，不会被老化，不会被动态 ARP 表项覆盖，可以保证网络通信的安全性。静态 ARP 表项可以限制本端设备和指定 IP 地址的对端设备通信时只使用指定的 MAC 地址，此时攻击报文无法修改本端设备的 ARP 表中 IP 地址和 MAC 地址的映射关系，从而保护了本端设备和对端设备间的正常通信。

配置 ARP，请前往 **Web UI→IP→ARP 表**页面。

图 66 ARP 表

老化时间 (秒)：设置动态 ARP 表项的老化时间。老化时间到达后，动态 ARP 表项将会自动删除。取值范围为 15-21600 的整数，默认 1200 秒。

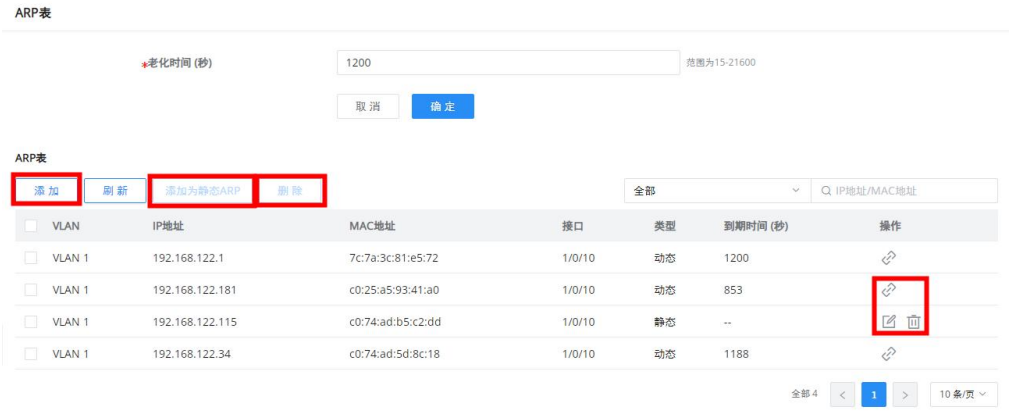


图 67 ARP 表-操作

- 点击  或“添加为静态 ARP”按钮，将动态 ARP 转变为静态 ARP。
- 点击  或“删除”按钮，将静态 ARP 表项删除。
- 点击  ，编辑静态 ARP 表项。

还可以通过点击“**添加**”按钮手动添加静态 ARP 条目，然后指定 VLAN、IP 地址和 MAC 地址的组合。

图 68 添加静态 ARP 表项

邻居发现

邻居发现协议 NDP 是 IPv6 协议体系中一个重要的基础协议，替代了 IPv4 的 ARP 和 ICMP 路由器发现，定义了使用 ICMPv6 报文实现地址解析，邻居不可达性检测、重复地址检测、路由器发现、重定向以及 ND 代理等功能。

IPv6 地址自动配置和路由发现依赖于两种 ICMPv6 消息：RS（路由请求）和 RA（路由通告）。主机发送 RS 消息，要求同一链路上的路由器立即发送 RA 消息。路由器发送 RA 消息，让主机知道位置信息，并向其提供 IPv6 前缀、下一跳、MTU 和配置标记等信息。

配置邻居发现，请前往 **Web UI→IP→邻居发现**页面。

图 69 邻居发现

老化时间 (秒)：设置动态邻居表项的老化时间。老化时间到达后，动态邻居表项将会自动删除。取值范围为 15-21600 的整数，默认 1200 秒。

注意：
老化时间仅针对动态 ARP 表项有效。

点击“**刷新**”按钮以动态加载条目，或点击“**添加**”按钮以添加静态条目。

图 70 添加静态邻居表项

域名系统

域名系统 DNS 提供域名与 IP 地址之间的转换服务。IPv4 DNS 提供域名和 IPv4 地址之间的转换，IPv6 DNS 提供域名和 IPv6 地址之间的转换。设备作为 DNS 客户端，当用户在设备上进行某些应用（如 Telnet 到一台设备或主机）时，可以直接使用便于记忆的、有意义的域名，通过域名系统将域名解析为正确的地址。

DNS 域名解析分为静态域名解析和动态域名解析，二者可以配合使用。在解析域名时，首先采用静态域名解析（查找静态域名解析表），如果静态域名解析不成功，再采用动态域名解析。由于动态域名解析可能会花费一定的时间，且需要域名服务器的配合，因而可以将一些常用的域名放入静态域名解析表中，这样可以大大提高域名解析效果。

全局设置

在此页面上，用户可将交换机指定 DNS 客户端。通过一个或多个配置的 DNS 服务器，将 DNS 域名解析为 IP 地址。默认启用。

配置 DNS，请前往 **Web UI→IP→域名系统**页面。

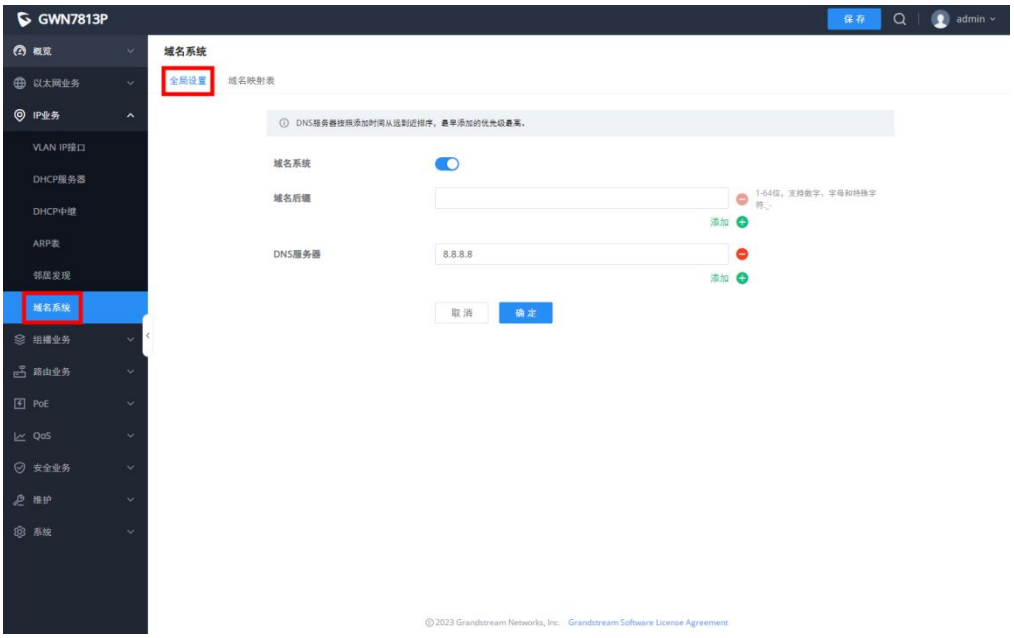


图 71 DNS-全局设置

至多添加 8 个域名后缀和 8 个 DNS 服务器。

注意：

- DNS 服务器根据添加时间从远到近排序，最早添加的 DNS 服务器优先级最高。

域名映射表

点击“**域名映射表**”，添加静态域名或查看动态域名。

图 72 DNS-域名映射表

点击“**添加**”按钮可添加静态 DNS 域名。

图 73 DNS-添加静态域名

注意：

- 可添加多个域名，至多 32 个。

点击 或“**添加为静态域名**”可将动态域名变为静态域名。

组播业务

IP 组播是一种通过网络中的 IP 基础设施进行一对多通信的技术。为了避免传入的数据广播到所有 GE/LAG 端口，IGMP 侦听或 MLD 侦听可以让组播将数据/消息传输到指定的 GE/LAG 端口。当交换机收到客户端“订阅”的消息时，它必须根据客户端（订阅成员）的位置决定将数据传输到指定的 GE/LAG 端口。

IGMP Snooping

作为 IPv4 的 2 层多播协议，IGMP Snooping 用来侦听 Internet 组管理协议（IGMP）网络流量。该功能允许网络交换机监听主机和路由器之间的 IGMP 会话。通过监听这些对话了解交换机维护哪些链路需要哪些 IP 多播流的映射。通过过滤多播，从而控制哪些端口接收特定的多播流量。

全局设置

此页面允许用户启用/禁用 IGMP Snooping 功能，选择侦听版本和启用/禁用侦听报文抑制。此外，还可以选择“组播转发模式”以及如何处理未知组播报文。

注意：

- **未知组播报文：**此选项与 MLD Snooping 的关联。这里选择的任何选项都将与 MLD Snooping 相同，反之亦然。

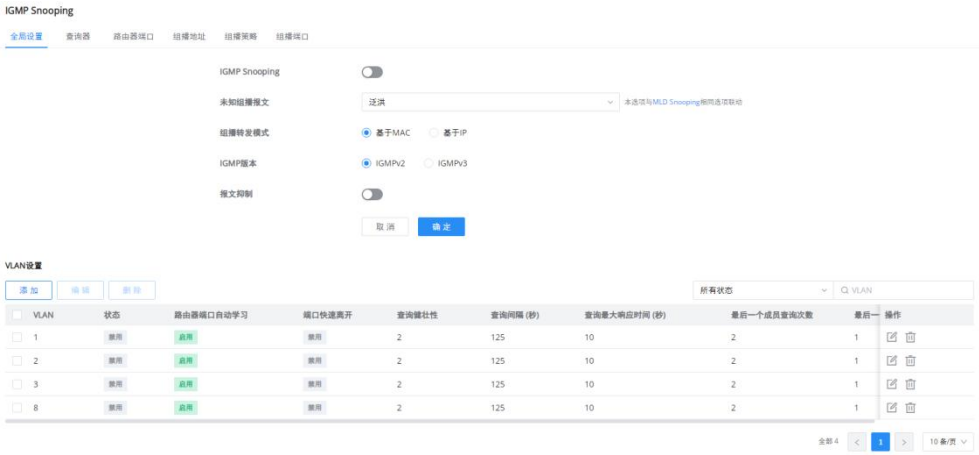


图 74 IGMP Snooping-全局设置

表 23 IGMP Snooping-全局设置

未知组播报文	选择交换机处理未知组播报文的操作。 • **丢弃：**丢弃未知的组播数据。 • **泛洪：**泛洪未知的组播数据。 • **转发至路由器端口：**将未知的组播数据转发到路由器。
IGMP Snooping	启用或禁用 IGMP Snooping。

组播转发模式	设置组播转发模式。 • **基于 MAC:** 使用 MAC 地址转发。 • **基于 IP**: 使用 IP 地址转发。
IGMP 版本	选择 IGMP 版本。
报文抑制	启用或禁用交换机以处理路由器和主机之间的 IGMP 报告，从而抑制 IGMP 使用的带宽。

用户还可以启用/禁用每个 VLAN 的 IGMP Snooping、路由器端口自动学习和端口快速离开等。

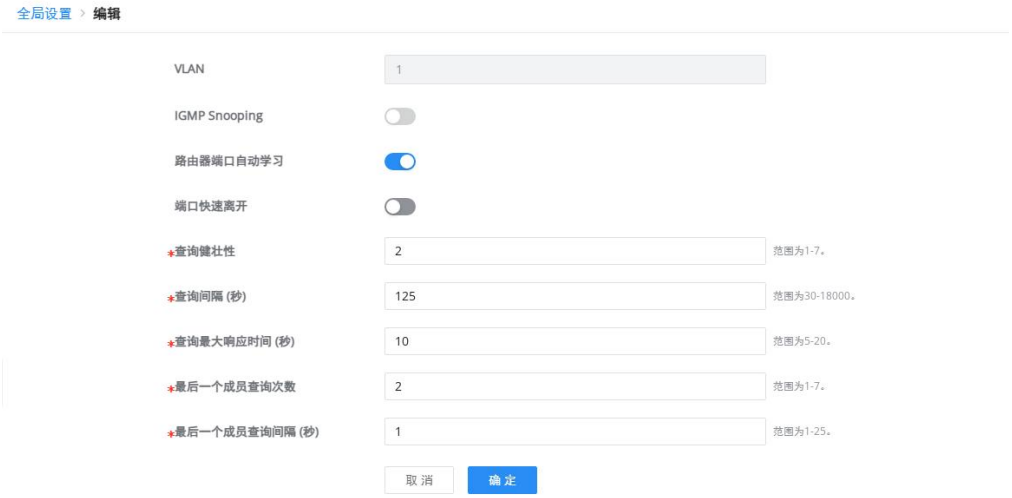


图 75 IGMP Snooping 编辑 VLAN

表 24 IGMP Snooping 编辑 VLAN

VLAN	显示选择的 VLAN
IGMP Snooping	单击切换按钮为所选 VLAN 启用 IGMP Snooping。
路由器端口自动学习	单击切换按钮以通过 IGMP 查询了解路由器端口。
端口快速离开	为所需端口启用/禁用快速离开功能。 **注意：**如果为某个端口启用了快速离开，交换机将在收到 IGMP 离开消息后立即从组播组中删除该端口。

查询健壮性	设置一个允许调整子网预期报文丢失的数字。 有效范围为 1-7。
查询间隔 (秒)	设置查询器发送常规查询的间隔。有效范围为 30-18000。
查询最大响应时间 (秒)	指定发送响应报告之前允许的最长时间。 **注意：**有效范围为 5-20。
最后一个成员查询次数	在查询指定时间后，仍然没有收到订阅成员的任何响应，GWN7810 系列交换机将停止向相关 GE 端口传输数据。 **注意：**有效范围为 1-7。
最后一个成员查询间隔 (秒)	计数没有任何订阅成员响应的每个成员查询消息之间的最大时间间隔。 **注意：**有效范围为 1-25。

IGMP Snooping 查询器

用户设置每个 VLAN 的 IGMP Snooping 查询器。

图 76 IGMP Snooping-查询器

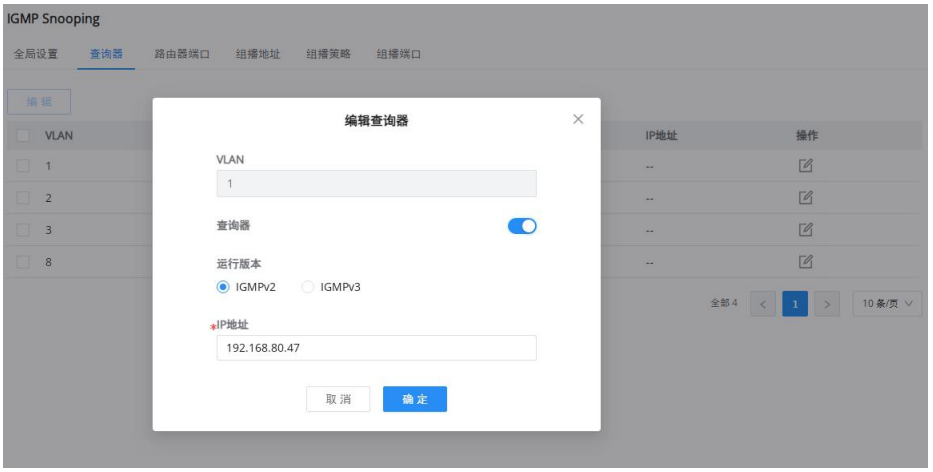


图 77 IGMP Snooping-编辑查询器

表 25 IGMP Snooping-查询器

VLAN	显示选择的 VLAN。
查询器	设置是否使能所选 VLAN 的 IGMP Snooping 查询器功能。
运行版本	选择 IGMP Snooping 查询器版本。
状态	显示查询器的运行状态。
IP 地址	默认使用 VLAN 接口 IP 地址，支持编辑

路由器端口

此页面显示此交换机已知的 IGMP Snooping 路由器端口。单击“**添加**”按钮添加端口，或单击 图标修改已创建的端口设置。

图 78 IGMP Snooping-路由器端口

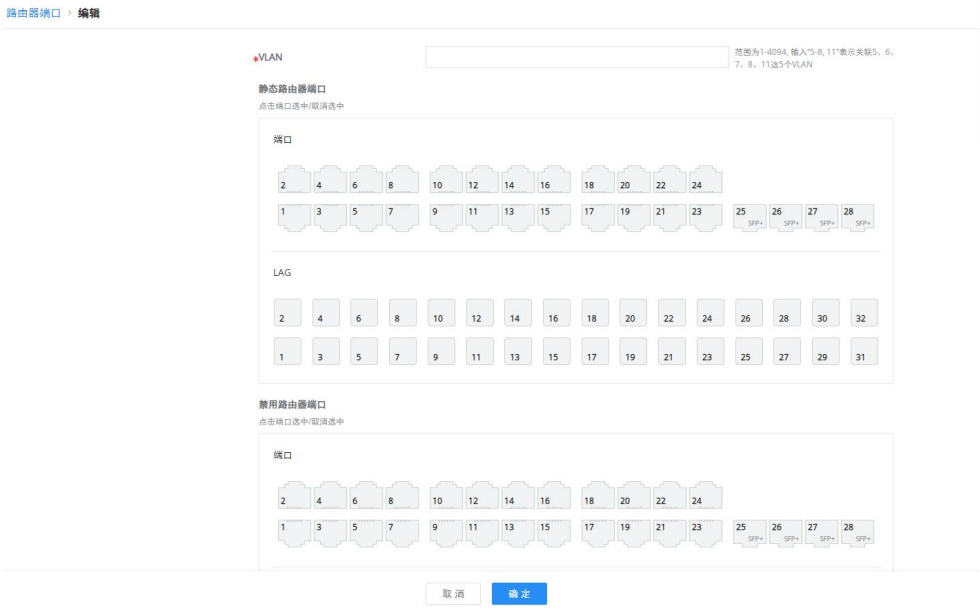


图 79 IGMP Snooping-添加/编辑路由器端口

组播地址

动态多播地址将在此处显示，用户还可以通过单击“添加”按钮或单击 图标来添加基于VLAN的静态多播地址条目。

图 80 IGMP Snooping-组播地址

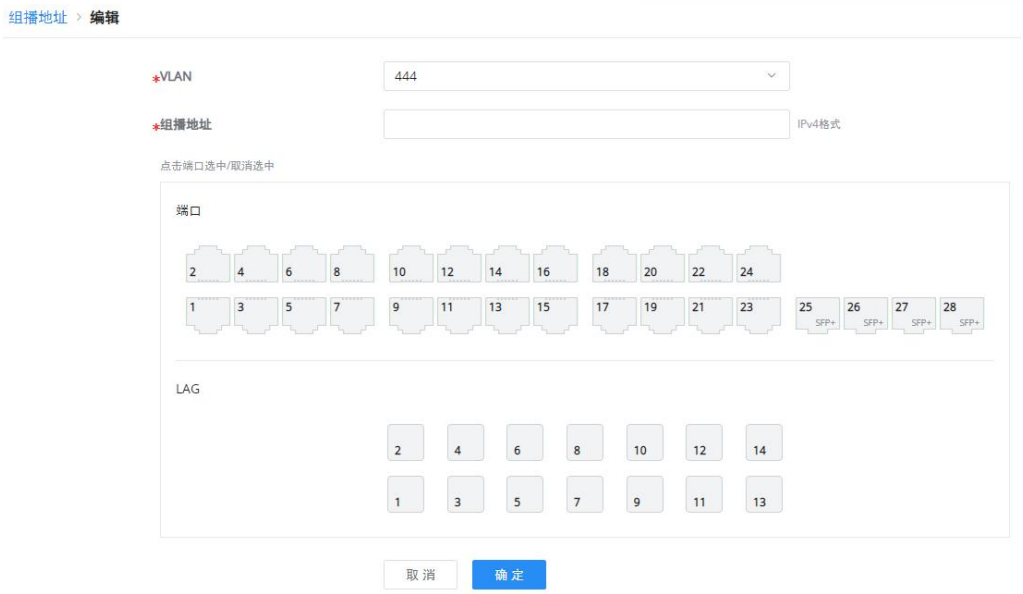


图 81 IGMP Snooping-添加组播地址

组播策略

在此页面中，用户至多可以添加最多 128 个允许/限制组播报文转发行为的组播策略。

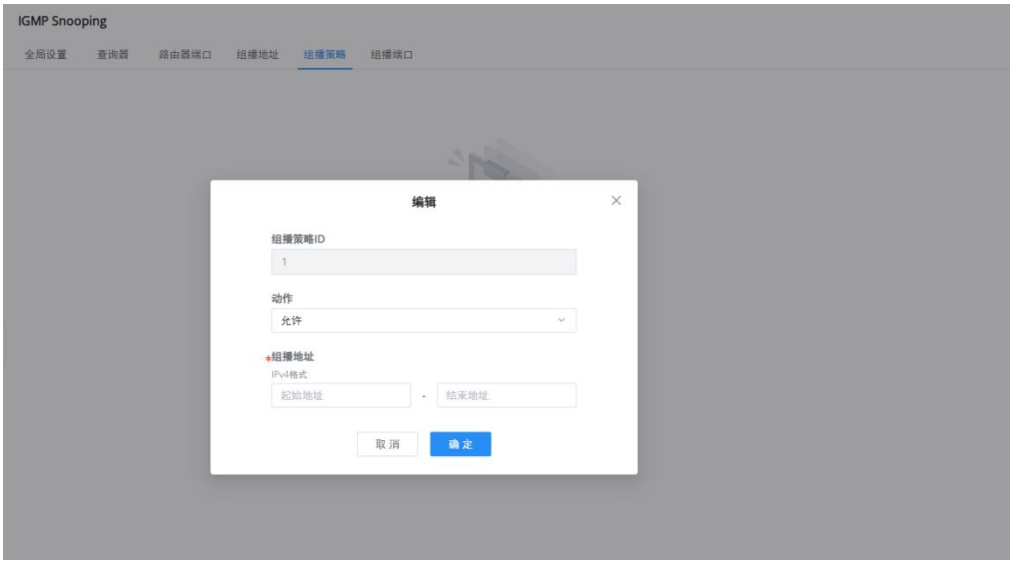


图 82 IGMP Snooping-组播策略

组播端口

创建组播策略后，用户可以在端口上应用此策略。

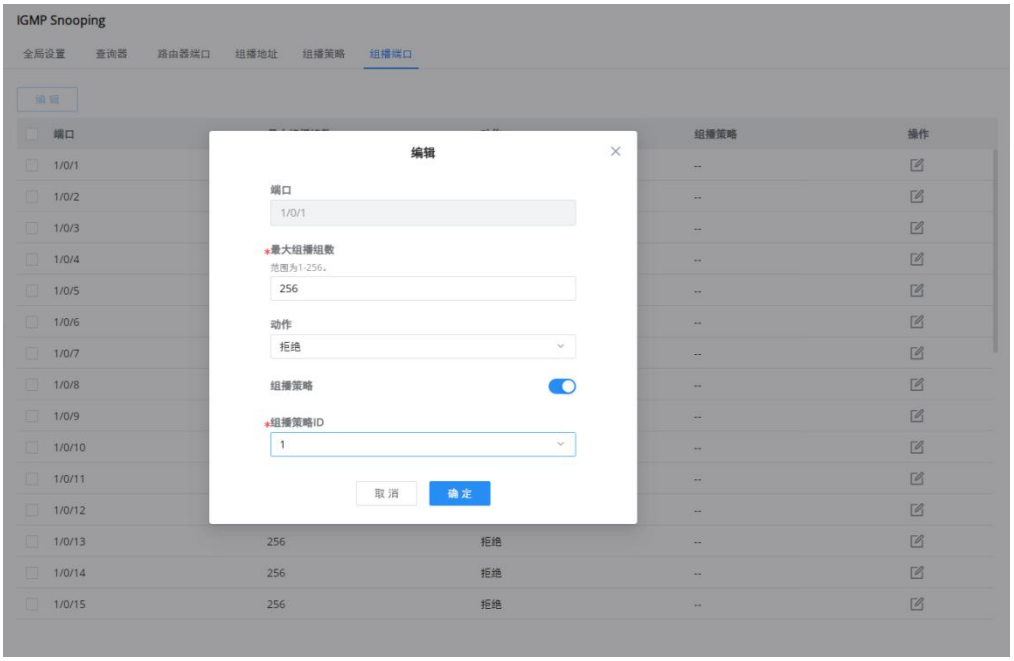


图 83 IGMP Snooping-组播端口

MLD Snooping

全局设置

作为 IPv6 的 2 层组播协议，MLD Snooping 通过监听第 3 层组播设备和用户主机之间发送的组播协议包来维护组播数据包的出端口信息，从而管理和控制组播数据，在数据链路层转发数据包。当在主机和上游第 3 层设备之间传输的 MLD 协议包通过 2 层设备时，MLD Snooping 分析包中携带的信息，基于该信息建立并维护 2 层组播转发表，并引导数据流中的组播数据。

“全局设置”页面允许用户启用 MLD Snooping 以及选择组播转发模式等。

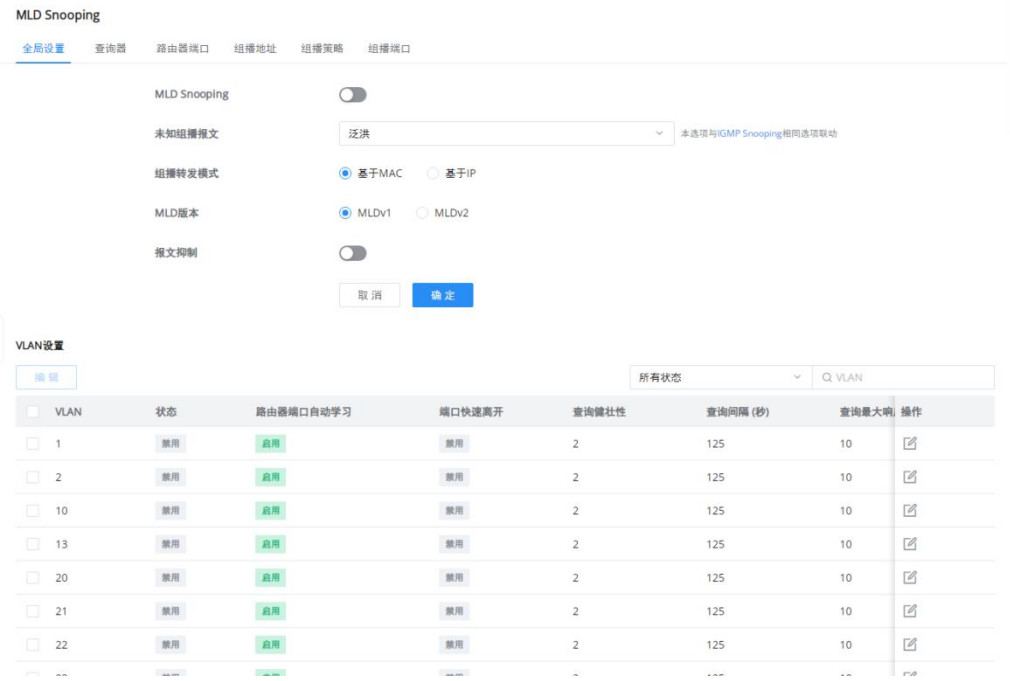


图 84 MLD Snooping-全局设置

表 26 MLD Snooping-全局设置

MLD Snooping	启用或禁用全局 MLD Snooping 。
未知组播报文	选择交换机处理未知组播报文的操作。 • **丢弃：**删除未知的组播数据。 • **泛洪：**泛洪未知的组播数据。 • **转发至路由器端口：**将未知的组播数据转发到路由器。 **注意：**此设置与 IGMP Snooping 相关联。
组播转发模式	设置组播转发模式 • **基于 MAC:** 使用 MAC 地址转发。 • **基于 IP**: 使用 IP 地址转发。
MLD 版本	选择 MLD 版本
报文抑制	启用或禁用交换机以处理路由器和主机之间的 MLD 报告，从而抑制 MLD 使用的带宽。

用户还可以启用/禁用每个 VLAN 的 MLD Snooping 等。

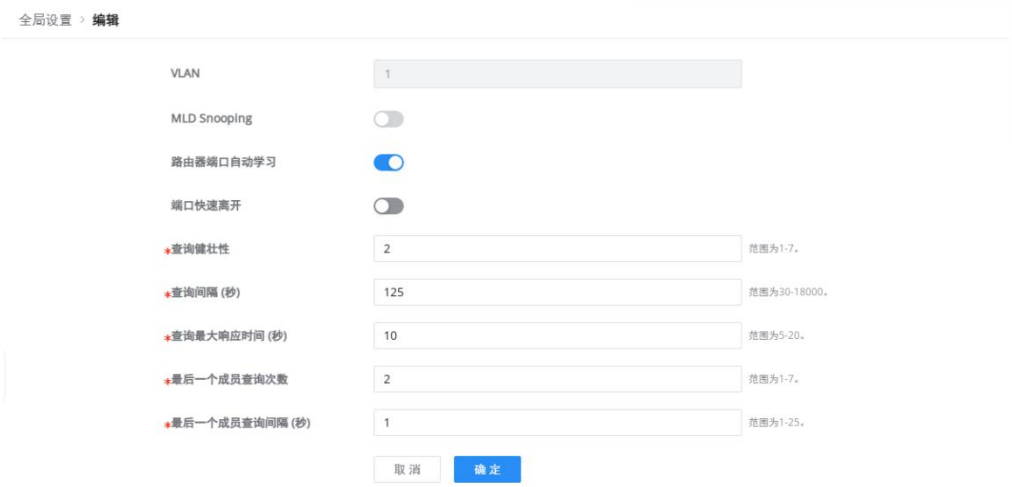


图 85 MLD Snooping-编辑 VLAN

表 27 MLD Snooping-编辑 VLAN

VLAN	显示选择的 VLAN
MLD Snooping	单击切换按钮为所选 VLAN 启用 IGMP 侦听。
路由器端口自动学习	单击切换按钮以通过 MLD 查询了解路由器端口。
端口快速离开	为所需端口启用/禁用快速离开功能。 **注意：**如果为某个端口启用了快速离开，交换机将在收到 IGMP 离开消息后立即从组播组中删除该端口。
查询健壮性	设置一个允许调整子网预期报文丢失的数字。 有效范围为 1-7。
查询间隔 (秒)	设置查询器发送常规查询的间隔。
查询最大响应时间 (秒)	指定发送响应报告之前允许的最长时间。 **注意：**有效范围为 5-20。
最后一个成员查询次数	在查询指定时间后，仍然没有收到订阅成员的任何响应，GWN7800 系列交换机将停止向相关 GE 端口传输数据。 **注意：**有效范围为 1-7。

最后一个成员查询间隔(秒)	计数没有任何订阅成员响应的每个成员查询消息之间的最大时间间隔。 **注意：**有效范围为 1-25。

MLD Snooping 查询器

用户设置每个 VLAN 的 MLD Snooping 查询器。

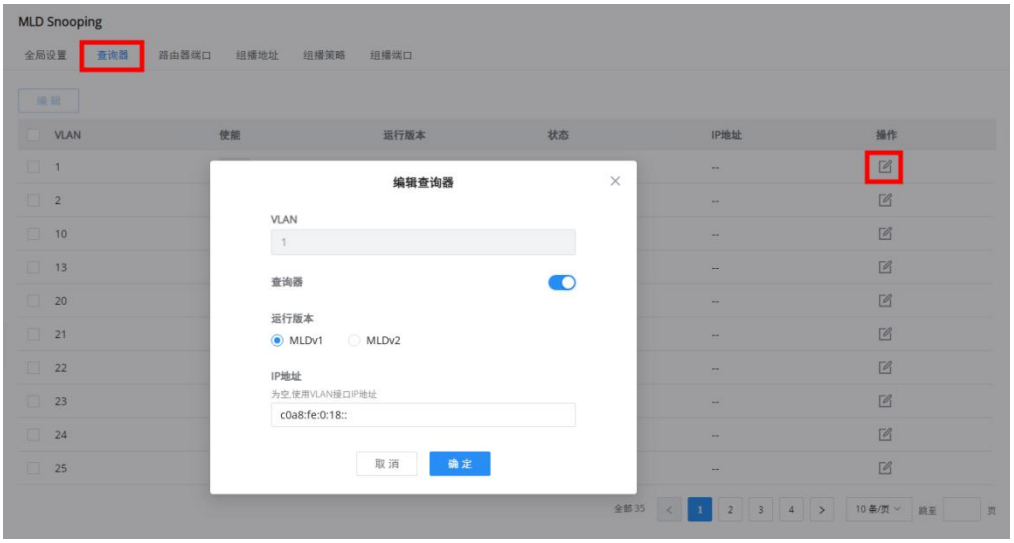


图 86 MLD Snooping-查询器

表 28 MLD Snooping-查询器

VLAN	显示选择的 VLAN。
查询器	设置是否使能所选 VLAN 的 MLD Snooping 查询器功能。
运行版本	选择 MLD Snooping 查询器版本。
状态	显示查询器的运行状态。
IP 地址	默认使用 VLAN 接口 IPv6 地址，支持编辑

路由器端口

如果路由器端口是静态配置的，Layer 2 设备也会将 MLD 报告和离开消息转发到静态路由器端口。如果配置了静态成员端口，该接口将作为转发表中的出接口添加。当 Layer 2 设备上建立 Layer 2 多播转发表项后，

当 Layer 2 设备接收到多播数据包时，它会根据数据包所属的 VLAN 和数据包的目标地址（即 IPv6 多播组地址）查找转发表。检查该项是否具有相应的“出接口”信息。如果存在，数据包将发送到所有多播组成员端口；如果不存在，数据包将被丢弃或在 VLAN 中广播。

此页面显示此交换机已知的 MLD 查询器路由器。单击“**添加**”添加端口，或单击 图标修改已创建的端口。

图 87 MLD Snooping-路由器端口

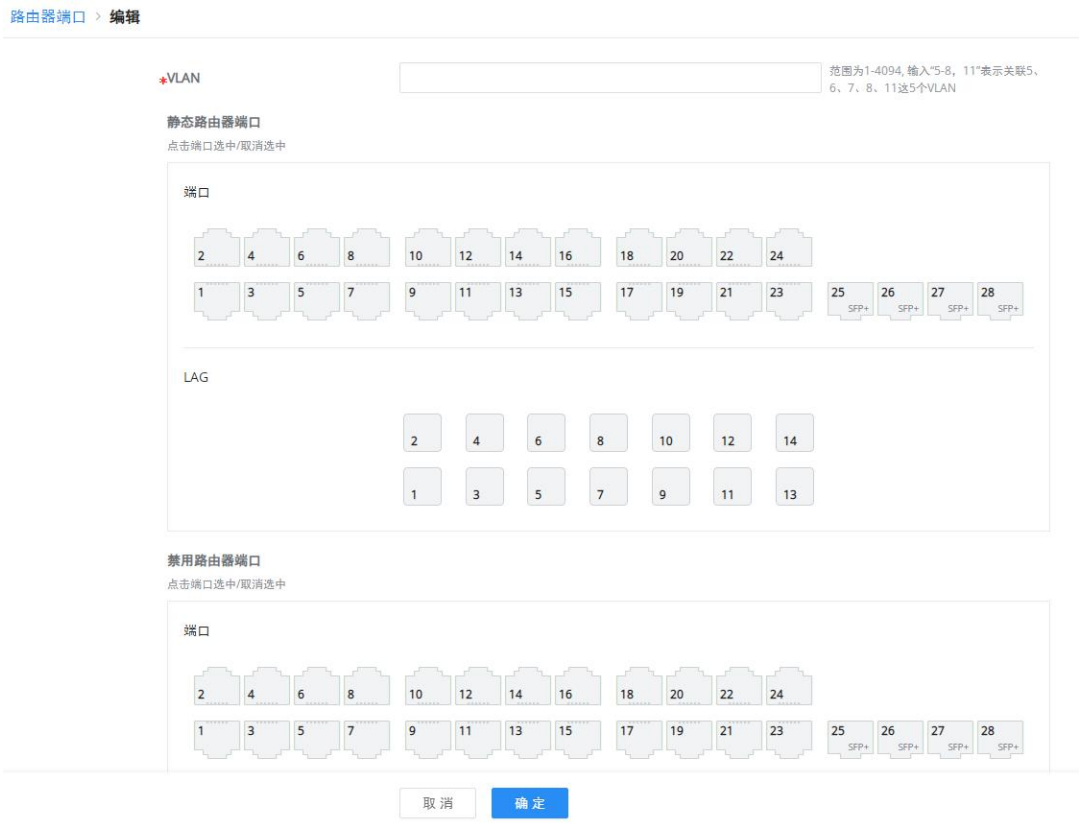


图 88 MLD Snooping-添加路由器端口

组播地址

GWN780x Pro 系列交换机还支持通过指定 VLAN 和成员端口来添加静态多播地址。

图 89 MLD Snooping-组播地址

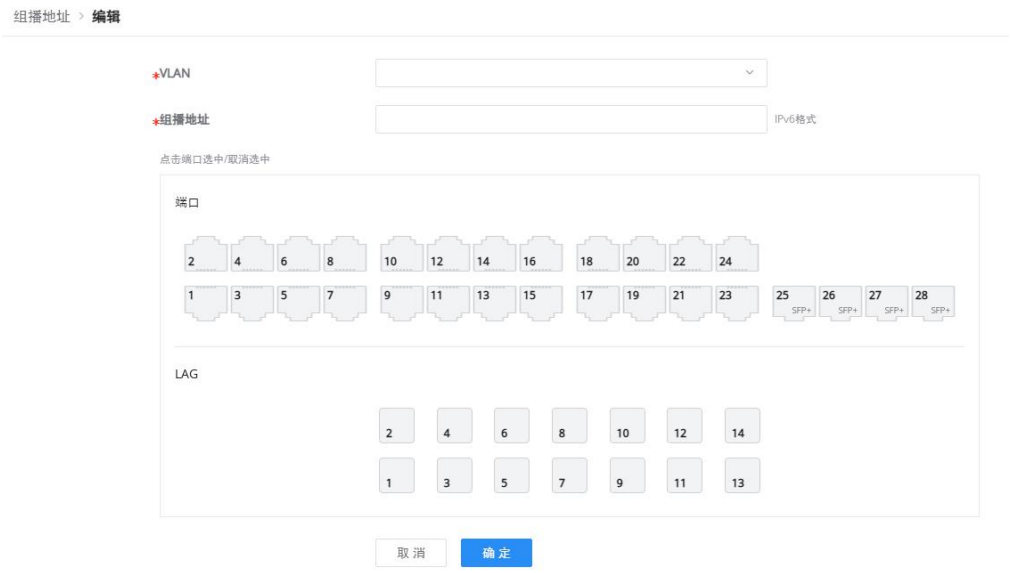


图 90 MLD Snooping-添加组播地址

组播策略

可以在此页面中创建组播策略，以允许或拒绝一系列 IPv6 组播地址。最多可创建 128 个策略。

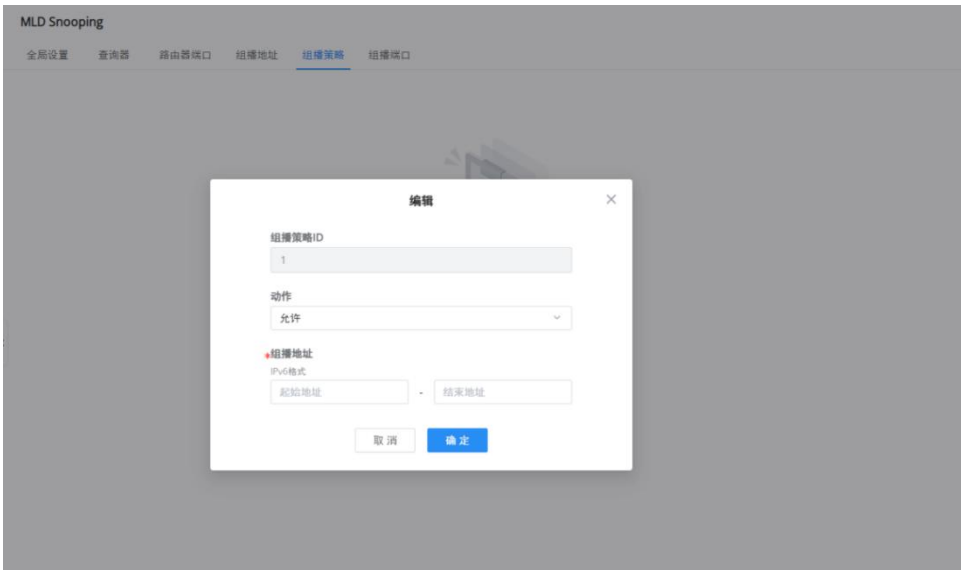


图 91 MLD Snooping-组播策略

组播端口

组播策略可以应用于千兆以太网/LAG 端口，用户还可以设置端口允许加入的组播组的最大数量，并在端口组播超过限制时设置操作，默认值为拒绝。

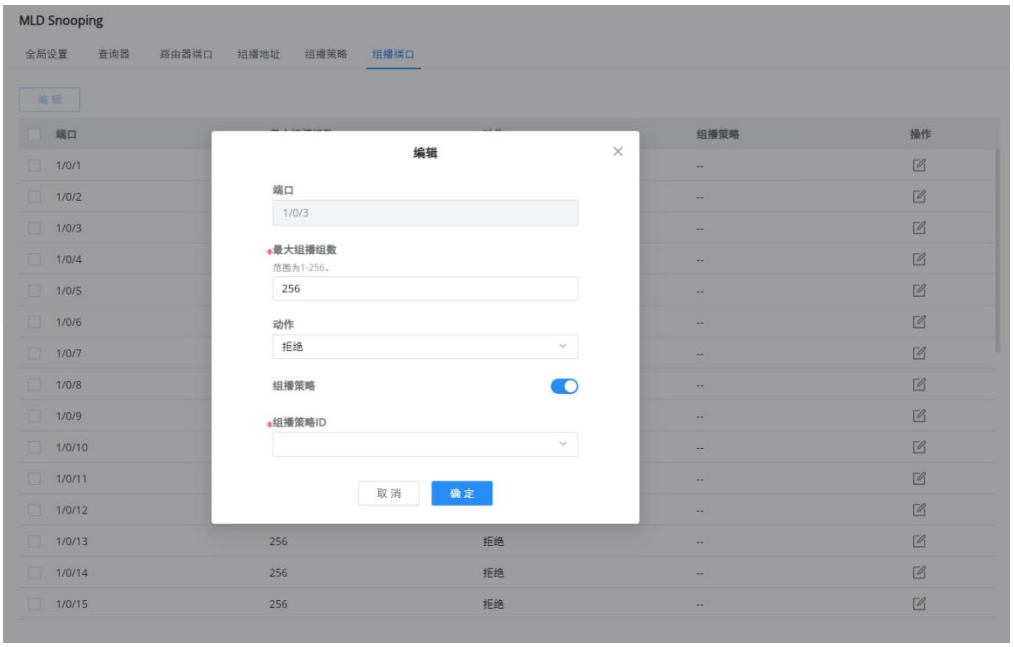


图 92 MLD Snooping-组播端口

路由业务

路由是路由器根据收到的数据包的目的地址选择最优路径，并转发到通往目标网络的下一个网络节点的过程，而此路径下的最后一个路由节点则将数据转发给目标主机。（路由器既指传统意义上的路由器，也指运行了路由协议的以太网交换机）

GWN780x Pro 系列交换机支持 IPv4 静态路由和 IPv6 静态路由。

路由表

路由表就像网络的地图，显示通往每个目的地的最佳路线。它通过存储如何到达网络上不同目的地的信息来实现。有了这个表，路由器可以决定将它从其他设备接收到的数据包转发到哪里。

您可以启用/禁用路由转发选项，这允许交换机作为一个 3 层设备，从而使其能够根据路由表条目在不同的网络或 VLAN 之间转发数据包。

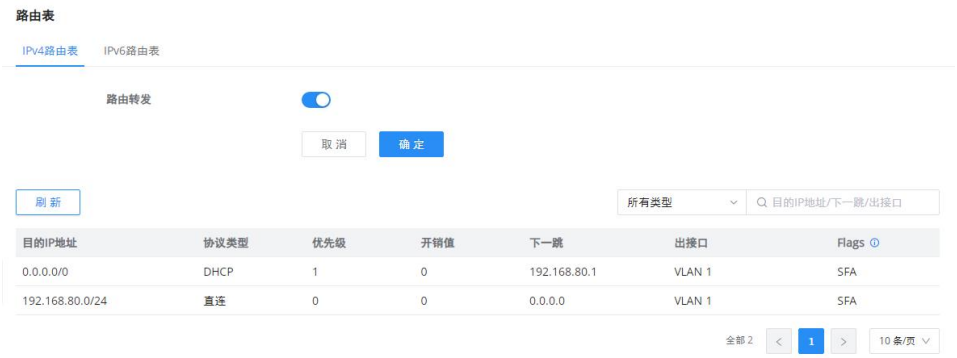


图 93 IPv4 路由表

图 94 IPv6 路由表

路由表包含每个条目的以下信息：目的地 IP 地址、掩码长度、协议类型、优先级、下一跳、输出接口和标志。

路由表随着时间的推移而被静态条目（由管理员手动配置）或直接连接的网络填充。

静态路由

静态路由是一种需要管理员手动配置的特殊路由。在不同的网络环境中具有不同的用途：

- 当网络结构相对简单时，只需配置静态路由就可以使网络正常工作。
- 在复杂的网络环境中，配置静态路由可以改进网络的性能，并可为重要的应用保证带宽。

添加静态路由，请前往 **Web UI→路由→静态路由**页面。

IPv4 静态路由

图 95 IPv4 静态路由

点击“**添加**”按钮以添加新的静态路由。然后填写目标 IP 地址及其掩码长度，然后选择下一跳或出接口（VLAN），并指定优先级。

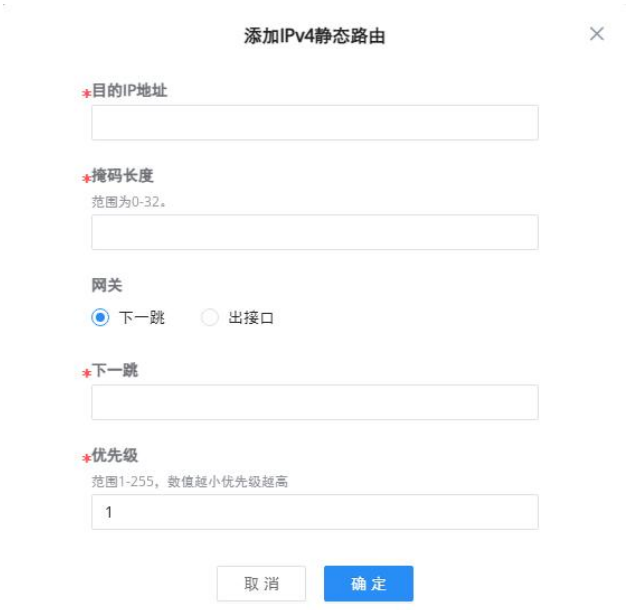


图 96 添加 IPv4 静态路由

表 29 添加 IPv4 静态路由

目的 IP 地址	设置路由到达的目的网络地址。
掩码长度	设置目标网络地址的掩码长度，取值范围为 0-32 的整数。 **注意：**当目的 IP 地址设置为 0.0.0.0，且掩码长度为 0 时，此为默认路由。
网关	• 下一跳：设置通往目的网络地址的路由路径上下一个路由节点的 IP 地址。 • 出接口：设置通往目的网络地址的路由路径的下一跳出口。
优先级	设置静态路由的优先级，数值越小优先级越高。取值范围为 1-255，默认 1

IPv6 静态路由

图 97 IPv6 静态路由

点击“**添加**”按钮添加静态路由表项。

图 98 添加 IPv6 静态路由

表 30 添加 IPv6 静态路由

目的 IPv6 地址	设置路由到达的目的网络地址。 **注意：**必须为有效单播地址。
前缀长度	设置目标网络地址的前缀长度，取值范围为 0-128 的整数，默认 64。 **注意：**当目的 IP 地址设置为全零，且掩码长度为 0 时，此为默认路由。
网关	• 下一跳：设置通往目的网络地址的路由路径上下一个路由节点的 IPv6 地址。 • 出接口：设置通往目的网络地址的路由路径的下一跳出口。 **注意：**若下一跳地址为链路本地地址，则下一跳和出接口必须同时配置。
优先级	设置静态路由的优先级，数值越小优先级越高。取值范围为 1-255，默认 1

PoE

以太网供电（PoE）是指通过以太网供电，也称为局域网供电系统 PoL 或有源以太网。

通常，接入点的终端设备需要使用直流电源，但由于布线不足，这些设备需要统一的电源管理。此时，交换机接口提供电源功能，可以解决上述问题，实现端口 PoE 电源的精确控制。

注意：
GWN780x ProP 型号支持 PoE 供电功能。

全局设置

此页面显示电源信息，如 PoE 接口数量、总供电功率、消耗功率、PoE 芯片工作状态等。

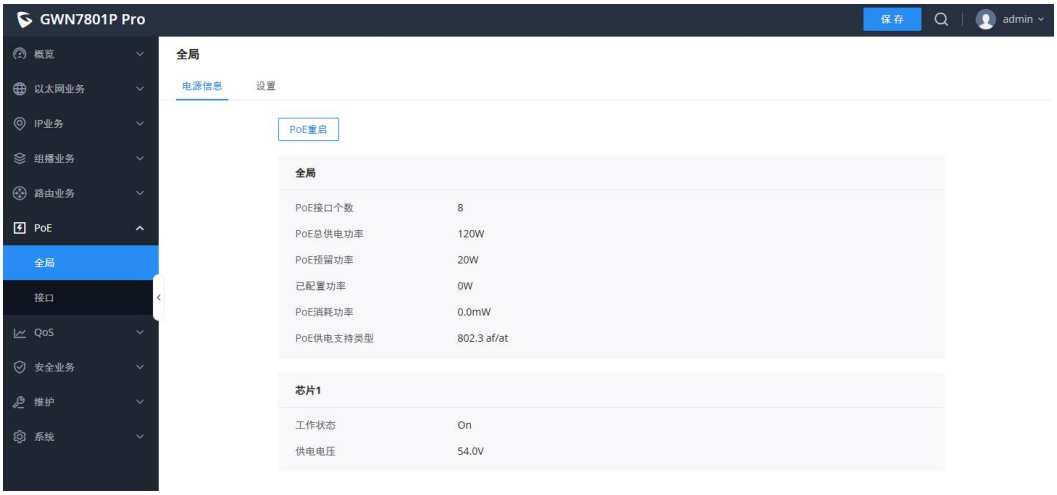


图 99 PoE-电源信息

点击 重启 按钮软重启 PoE 模块。

PoE 预留功率

- **PoE 预留功率(W)：**指定 PoE 电源的总保留功率。

图 100 PoE 预留功率

应用场景：
设备将根据每个接口实际消耗的功率动态地向每个接口分配功率。在每个 PD 设备的运行过程中，其功耗将

继续变化，系统将定期计算所有当前连接的 PD 所需的总功率，是否超过可用 PoE 功率上限，如果超过，系统将自动关闭优先级较低接口上的 PD 设备，以确保其他设备的正常运行。然而，有时会突然出现功耗激增，系统的剩余可用功率无法支持这种需求激增，并且系统还没有时间计算超过限制的总功耗来断开优先级较低的接口的电源。因此当 PoE 电源过载时，过载保护将关闭，所有 PD 设备将关闭。使用 PoE 电源预留功率合理设置系统的预留功率，在电力需求突然激增的情况下，系统的预留电力可以支持突然的需求，并确保系统有时间关闭低优先级接口上的设备供电，确保其他设备稳定运行。

接口设置

选择要配置的支持 PoE 电源的交换机接口，可以同时选择多个。

单击“**编辑**”按钮或 图标更改每个端口的配置，包括供电标准、供电模式和供电优先级等。

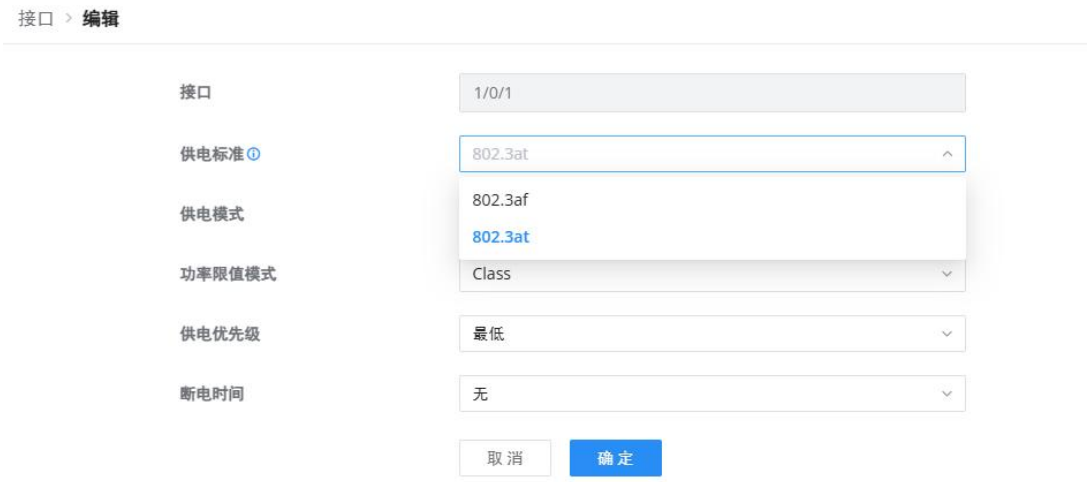


图 101 PoE-接口设置

QoS

网络的普及和业务的多样化使得互联网流量激增，从而产生网络拥塞，增加转发时延，严重时还会产生丢包，导致业务质量下降甚至不可用。所以，要在网络上开展这些实时性业务，就必须解决网络拥塞问题，最好的办法是增加网络的带宽，但从运营、维护的成本考虑，这不现实，最有效的解决方案是应用一个“有保证”的策略对网络流量进行管理。QoS 技术就是在这种背景下发展起来的。QoS 即服务质量，其目的是针对各种业务的不同需求，为其提供端到端的服务质量保证。QoS 是有效利用网络资源的工具，它允许不同的流量不平等的竞争网络资源，语音、视频和重要的数据应用在网络设备中可以优先得到服务。

端口优先级

此页面允许用户启用/禁用端口优先级，为接收的数据包配置信任模式包括 802.1p、DSCP、802.1p-DSCP 和 IP 优先级。

启用端口优先级后，用户可以单击“**编辑**”按钮进一步配置每个端口/LAG。

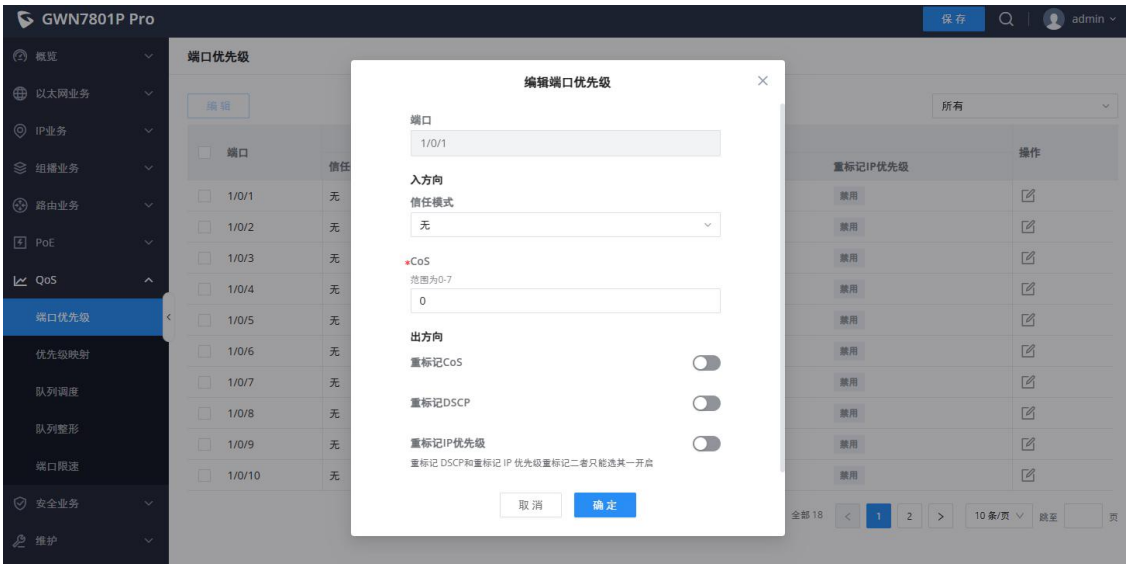


图 102 端口优先级

表 31 端口优先级

端口	显示选择的 GE/LAG 端口。
端口优先级	选择是否启用端口优先级，默认设置为禁用。
信任模式	选择 QoS 信任模式 • **802.1p**：流量基于 802.1p 映射到 CoS，可以在 **QoS→优先级映射→802.1p 映射**页面中进行配置。 • **DSCP**：所有 IP 流量都根据 IP 标头中的 DSCP 字段映射到队列。如

	果流量不是 IP 流量，则将其映射到最低优先级队列。 • **802.1p-DSCP**：所有 IP 流量都根据 IP 标头中的 DSCP 字段映射到队列。如果流量不是 IP 流量，但具有 VLAN 标签，则根据 VLAN 标签中的 CoS 值映射到队列。它可以在 **QoS→ 优先级映射→ DSCP 映射**页中配置。 • **IP 优先级**：IP 优先级是 ToS 中的一个 3 位字段，它威胁高优先级数据包比其他数据包更重要。它可以在 **QoS→优先级映射→IP 映射**页面中配置。
CoS	设置接口的 CoS 值，值范围为 0 到 7 的整数（7 是最高优先级），默认值为 0。
重标记 CoS	设置是否启用传出数据包的重标记 CoS 功能（默认情况下禁用）。
重标记 DSCP	设置是否启用传出数据包的重标记 DSCP 功能（默认情况下禁用）。
重标记 IP 优先级	设置是否启用传出数据包的重标记 IP 优先级功能（默认情况下禁用）。 **注意：**只能启用 DSCP 和 IP 优先级重标记中的一个。

优先级映射

优先级映射用来实现报文携带的 QoS 优先级与设备内部优先级（又称为本地优先级，是设备内部区分报文服务等级的优先级）之间的转换，从而设备根据内部优先级提供有差别的 QoS 服务质量。用户可以根据网络规划在不同网络中使用不同的 QoS 优先级字段。

802.1p 映射

显示 802.1p 和队列之间的映射关系。

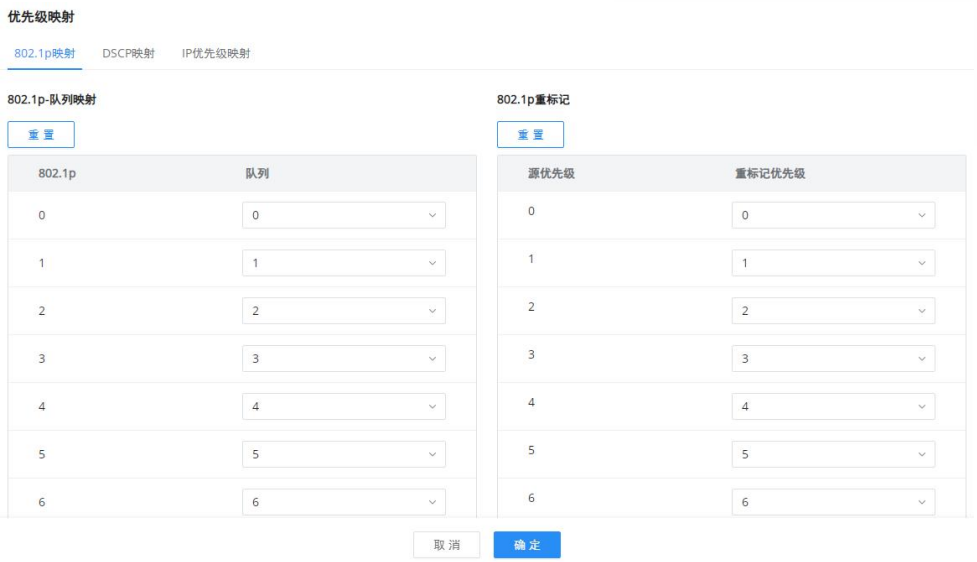


图 103 CoS 映射

DSCP 映射

显示 DSCP 和队列之间的映射关系。

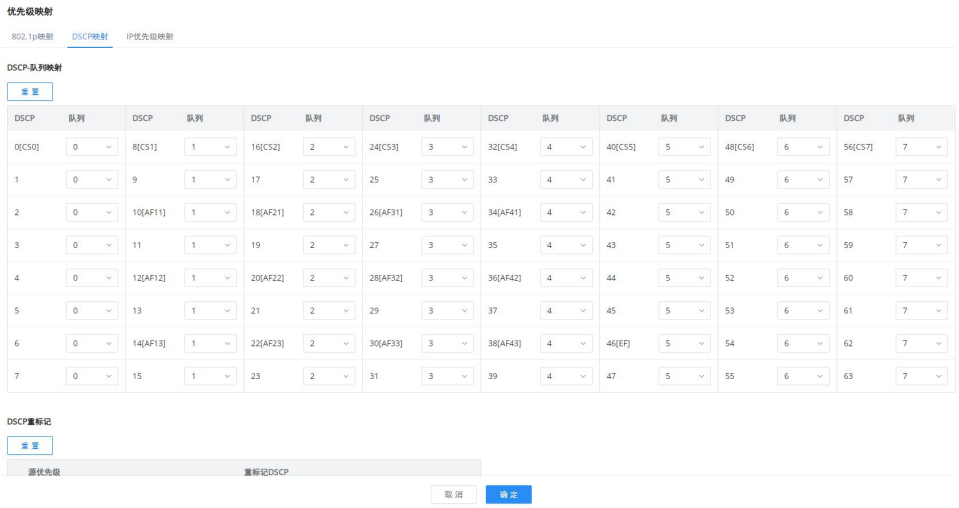


图 104 DSCP 映射

IP 优先级映射

显示 IP 优先级和队列之间的映射关系。

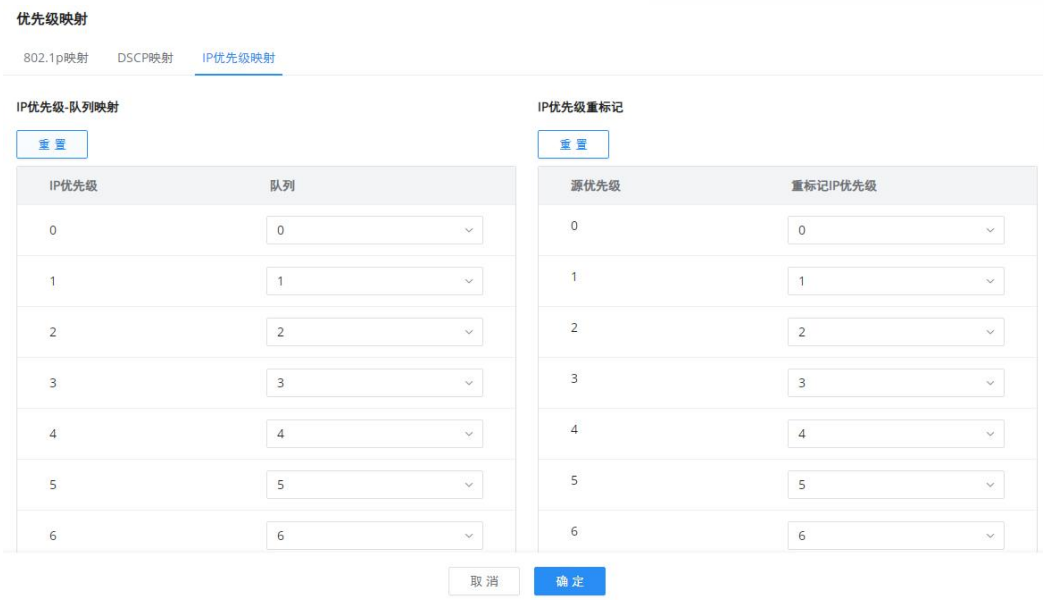


图 105 IP 优先级映射

队列调度

当网络中发生拥塞时，设备将按照指定的调度策略决定报文转发时的处理次序，以达到高优先级报文优先被调度的目的。

队列调度算法：根据交换机接口进行队列调度。

- **严格优先级（SP）调度**：优先级最高的流首先被服务，然后优先级第二高的流被服务，直到没有该优先级的流为止。交换机的每个接口支持 8 个队列（队列 0-7），队列 7 是最高优先级的队列，队列 0 是最低优先级的队列。**缺点**：当发生拥塞时，如果高优先级队列中长期存在数据包，则无法调度低优先级队列中的数据包，并且无法传输数据。
- **加权轮询（WRR）调度**：为每个优先级队列分配一定的带宽，并根据优先级从高到低为每个优先级排队提供服务。当高优先级队列用完所有分配的带宽时，它会自动切换到下一个优先级队列为其服务。
- **加权公平队列（WFQ）调度**：在尽可能保证公平（带宽、延迟）的基础上增加优先权方面的考虑，使高优先权的报文获得优先调度的机会多于低优先权的报文。WFQ 能够按流的“会话”信息（协议类型、源和目的 IP 地址、源和目的 TCP 或 UDP 端口、ToS 域中的优先级位等）自动进行流分类，并且尽可能多地提供队列，以将每个流均匀地放入不同队列中，从而在总体上均衡各个流的延迟。在出队的时候，WFQ 按流的优先级（Precedence）来分配每个流应占有出口的带宽。优先级的数值越小，所得的带宽越少；反之，所得的带宽越多。
- **SP-WRR**：交换机优先调度 SP 调度组（权重为 0）的分组，且当 SP 调度组为空时，调度 WRR 调度组中的分组。SP 调度组中的队列使用 SP 队列调度算法进行调度，WRR 调度组中的队列使用 WRR 调度算法进行调度。
- **SP-WFQ**：交换机优先调度 SP 调度组（权重为 0）的分组，且当 SP 调度组为空时，调度 WFQ 调度组中的分组。SP 调度组中的队列使用 SP 队列调度算法进行调度，WFQ 调度组中的队列使用 WFQ 调度算法进行调度。

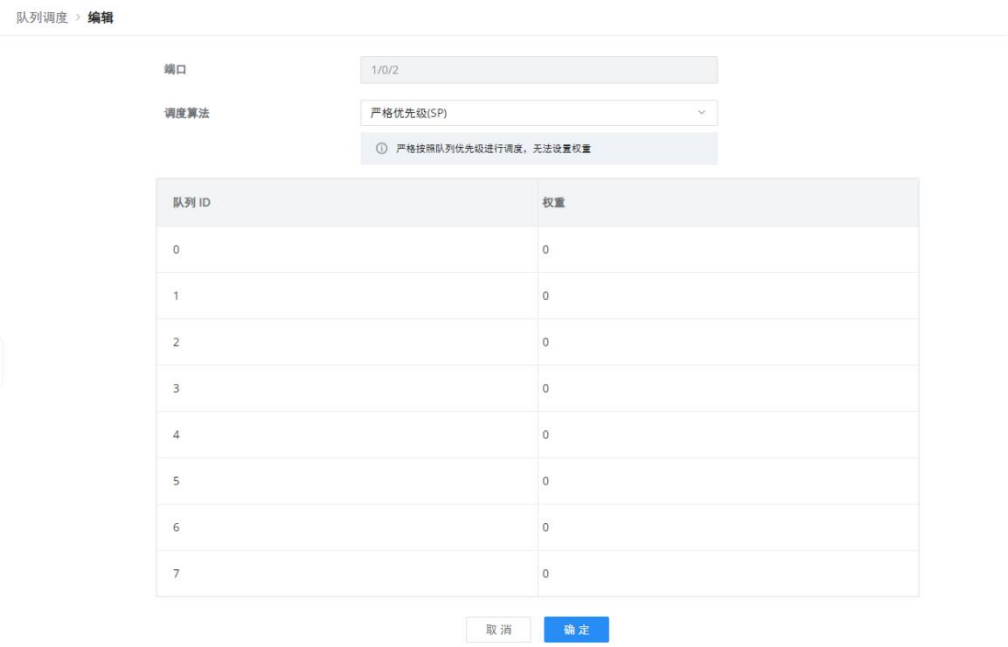


图 106 队列调度-编辑端口

队列整形

当报文的发送速率大于接收速率，或者下游设备的接口速率小于上游设备的接口速率时，可能会引起网络的拥塞。如果不限制用户发送的业务流量大小，大量用户不断突发的业务数据会使网络更加拥挤。为了使有限的网络资源更有效地为用户服务，需要对用户的业务流量加以限制。

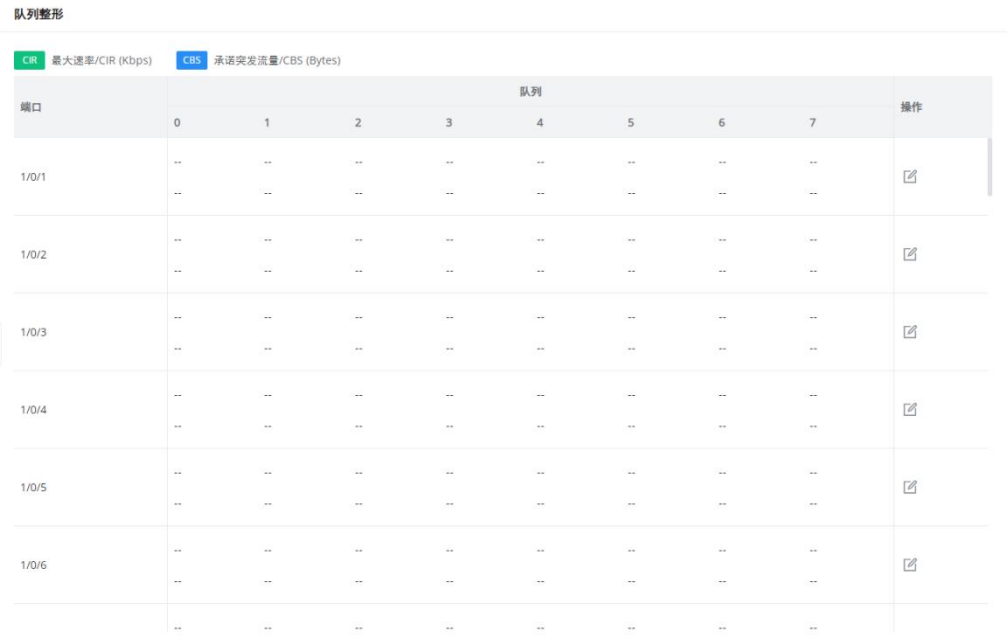


图 107 队列整形

要配置端口，单击操作栏下的“**编辑**”图标。

最大速率/CIR (Kbps)：配置整形的最大速率。该值必须是介于 16-[端口最大速率]之间的整数，并且必须是

16 的倍数。默认情况下，它是端口速率。

承诺突发流量/CBS (Bytes)：配置整形的承诺突发流量。有效范围为 678-53247 的整数。

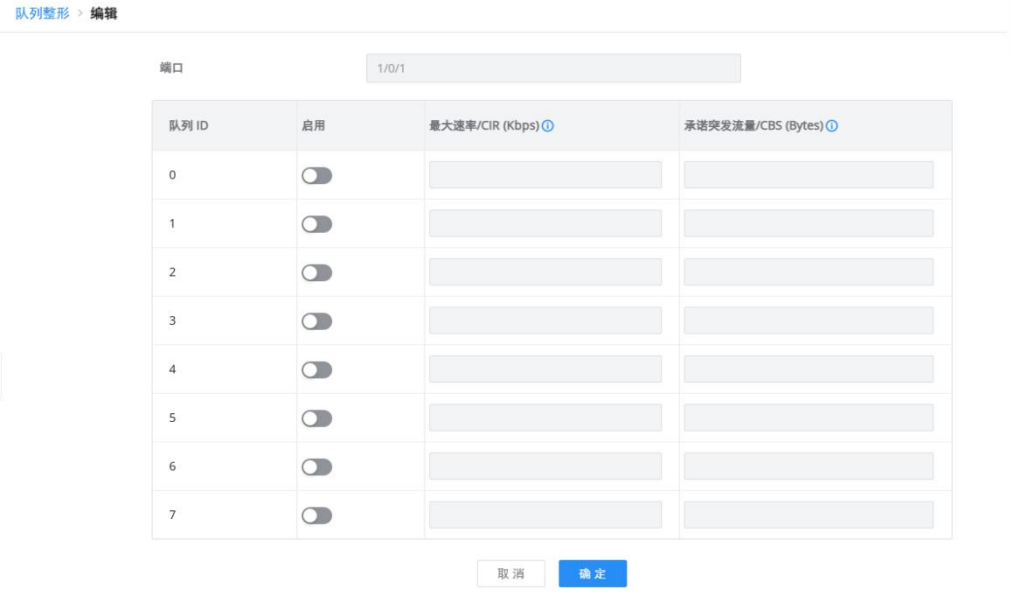


图 108 队列整形-配置 CIR/CBS

端口限速

接口限速可以对一个接口上发送或者接收全部报文的总速率进行限制。接口限速也是采用令牌桶进行流量控制。如果在设备的某个接口配置了接口限速，所有经由该接口发送的报文首先要经过接口限速的令牌桶进行处理。如果令牌桶中有足够的临牌，则报文可以发送；反之，报文将被丢弃或者被缓存。

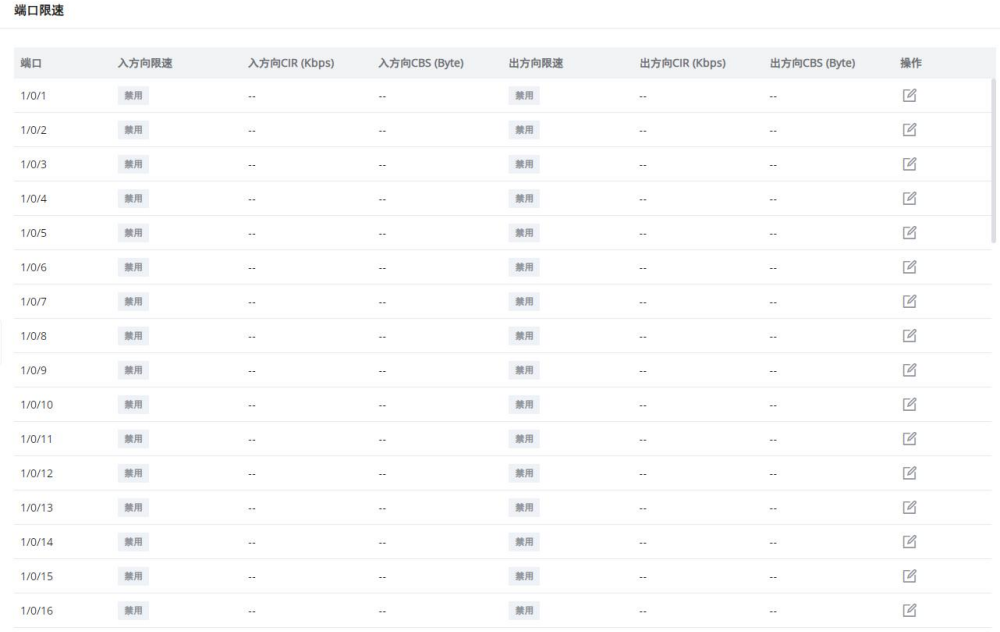


图 109 端口限速

要配置端口，请点击操作列下的“**编辑**”图标，然后设置入口和出口的 CIR 和 CBS。

CIR（承诺信息速率）：网络中保证的平均传输速率或最低保证流量。
CBS（承诺突发流量）：可以通过接口传输的平均突发流量。

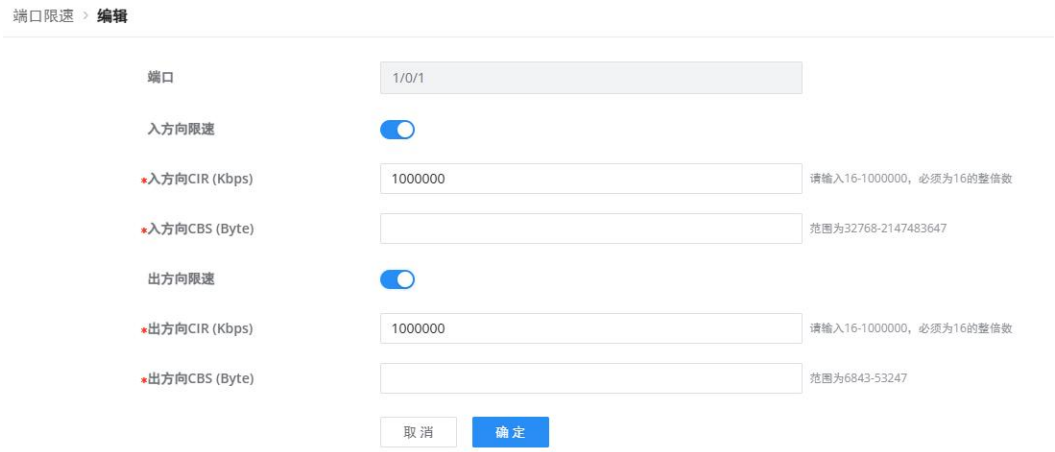


图 110 端口限速-编辑端口

安全业务

GWN780x Pro 系列交换机系列支持许多工具和功能，以增强设备的安全性，防止错误配置或攻击。

风暴控制

流量抑制可以通过配置阈值来限制广播、未知组播、未知单播、已知组播和已知单播报文的速率，防止广播、未知组播报文和未知单播报文产生广播风暴，防止已知组播报文和已知单播报文的大流量冲击。

风暴控制可以通过阻塞报文或关闭端口来阻断广播、未知组播和未知单播报文的流量。设备支持对接口下的上述三类报文分别按包速率、字节速率、百分比进行风暴控制。在一个检测时间间隔内，设备监控接口下接收的三类报文的平均速率并和配置的最大阈值相比较，当报文速率大于配置的最大阈值时，设备会对该接口进行风暴控制，执行配置好的风暴控制动作。风暴控制动作包括阻塞报文和关闭接口。

- 如果数据包被阻止，当接口上接收数据包的平均速率小于指定的最小阈值时，风暴控制将释放对接口上数据包的阻止。
- 如果操作是关闭接口，则需要手动运行命令以启动接口，或启用接口状态自动返回启用状态，也可以使用**端口自动恢复**功能自动启动界面。

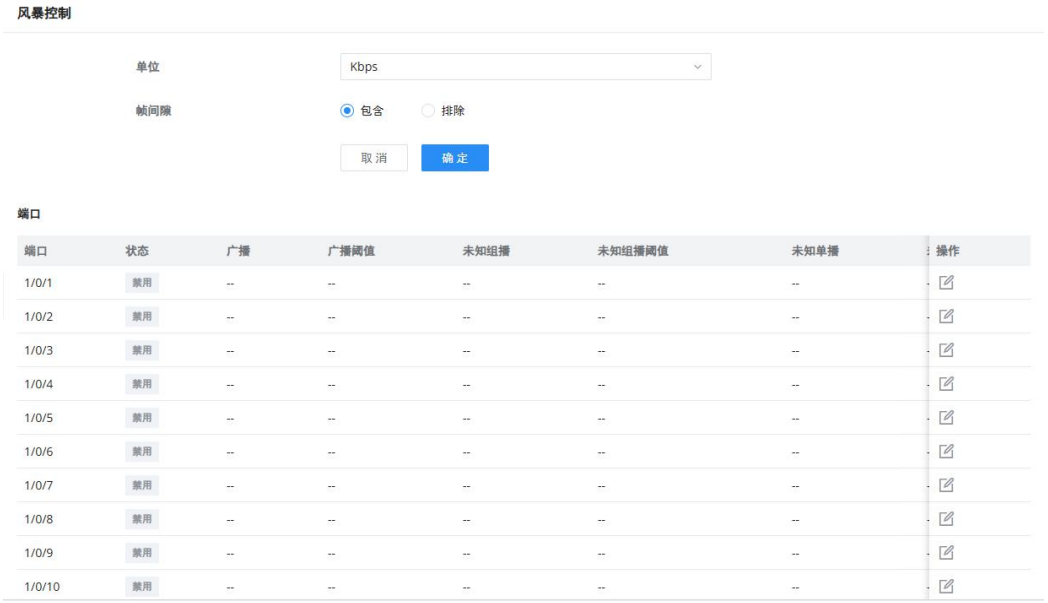


图 111 风暴控制

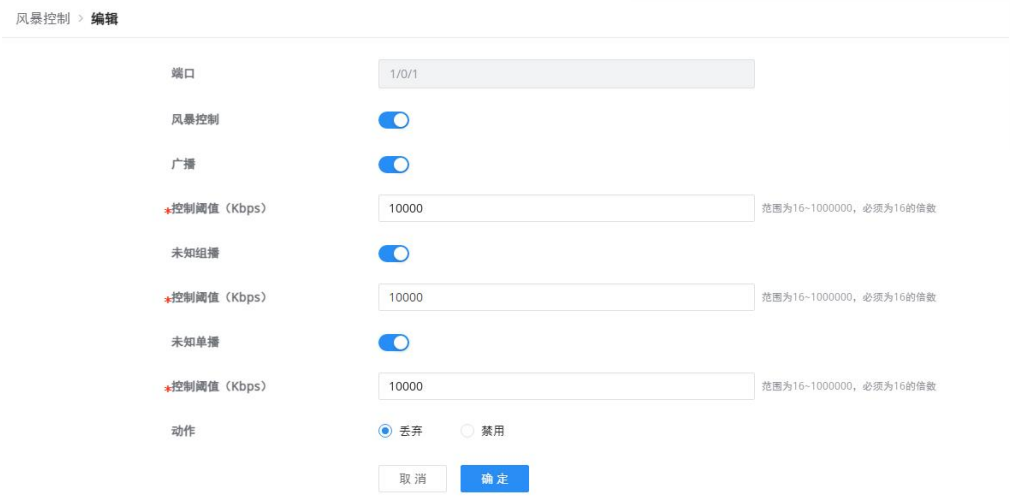


图 112 风暴控制-编辑端口

表 32 风暴控制

单位	• Kbps：风暴控制率将根据字节计算。 • pps：风暴控制率将根据数据包计算。
帧间隙	选择帧间隙。 • **包含:** 计算入口风暴控制率时，不包括 IFG。计算入口风暴控制率时包括 IFG。 • **排除:** 计算入口风暴控制率时，不包括 IFG。 默认包含。
风暴控制→编辑	
端口	显示选择的端口。
风暴控制	选择是否在所选端口上启用风暴控制。
广播	设置是否为广播数据包启用风暴阈值设置。如果已启用，请输入阈值（Kbps）。 **注意：**Kbps 的有效范围为 16 ~ [最大端口速率]，必须是 16 的倍数，默认值为 10000。pps 的有效范围为 1 ~ 16777215 的整数
未知组播	设置是否为未知组播数据包启用风暴阈值设置（如果启用）请输入阈值。 **注意：**Kbps 的有效范围为 16 ~ [最大端口速率]，必须是 16 的倍数，默认值为 10000。pps 的有效范围为 1 ~ 16777215 的整数。

未知单播	设置是否为未知单播数据包启用风暴阈值设置（如果启用）请输入阈值。 **注意：**Kbps 的有效范围为 16 ~ [最大端口速率]，必须是 16 的倍数，默认值为 10000。pps 的有效范围为 1 ~ 16777215 的整数。
动作	选择设置状态 • **丢弃：**超过风暴控制速率的数据包将被丢弃。 • **禁用：**端口超过风暴控制速率将被关闭。

端口安全

端口安全通过将接口学习到的 MAC 地址转换为安全 MAC 地址（包括安全动态 MAC 地址、安全静态 MAC 地址和 Sticky MAC），阻止非法用户通过本接口和交换机通信，从而增强设备的安全性。

安全 MAC 地址分为：安全动态 MAC、安全静态 MAC 和 Sticky MAC。

表 33 安全 MAC 地址类型

安全动态 MAC 地址	如果启用，但 Sticky MAC 功能未启用。	如果设备重新启动，条目将丢失，需要重新学习。
安全静态 MAC 地址	启用端口安全时手动配置静态 MAC 地址。	这些条目不会过期，在重新启动后也不会丢失。
Sticky MAC 地址	启用端口安全性并同时启用 Stcky MAC 功能后转换的 MAC 地址	重新启动设备后，条目不会过期，地址也不会丢失。

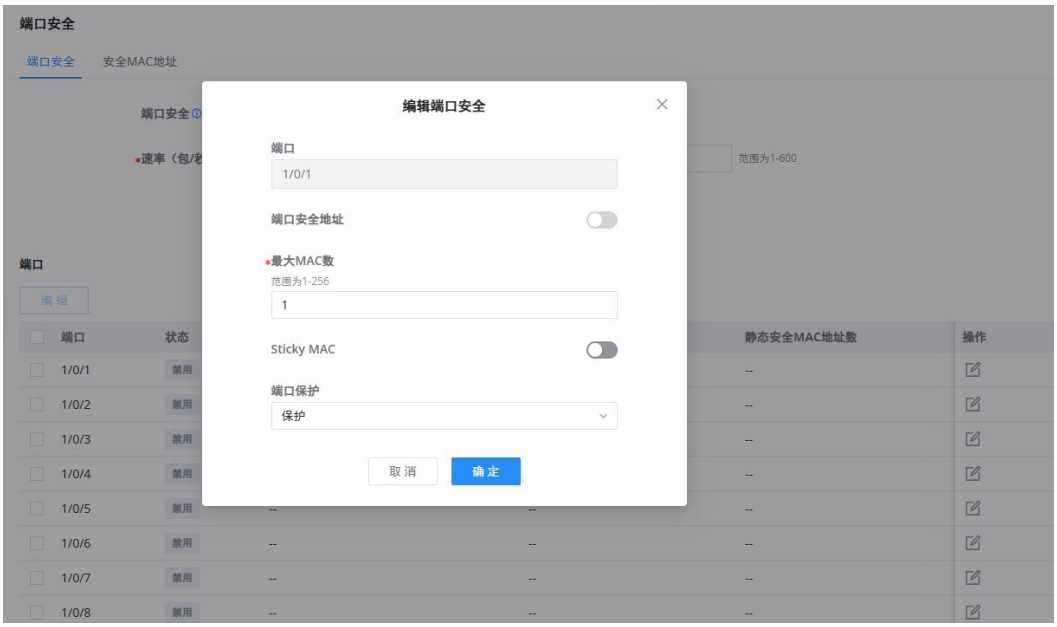


图 113 端口安全

表 34 端口安全

端口安全	设置是否启用全局端口安全功能，默认情况下禁用。
速率 (包/秒)	设置端口 MAC 地址的学习速率。取值范围为 1-600 的整数，默认值为 100。
编辑端口安全	
端口	显示选择的端口
端口安全地址	设置是否启用端口安全地址，默认情况下禁用。
最大 MAC 数	设置接口要学习的最大 MAC 地址数，值范围为 1 到 256 之间的整数，默认值为 1。达到最大数量后，如果交换机接收到源 MAC 地址不存在的数据包，无论目标 MAC 地址是否存在，交换机都认为存在非法用户的攻击，并将根据端口保护配置（保护、限制或关闭）接口。
Sticky MAC	启用端口安全时，可以启用 Sticky MAC 功能，默认情况下禁用。启用后，该接口将学习到的安全动态 MAC 地址转换为 Sticky MAC。如果已达到 MAC 地址的最大数量，则将丢弃接口获知的非 Sticky MAC 条目中的 MAC 地址，并根据接口保护模式配置报告陷阱警报。

端口保护	当接口获知的 MAC 地址数量达到最大数量或发生静态 MAC 地址摆动时，设置保护动作。 有三种模式（保护、限制或关闭），默认为保护。 • **保护：**仅丢弃源 MAC 地址不存在的数据包，并且不告警。 • **限制：**丢弃不存在源 MAC 地址的数据包并告警。 • **关闭：**接口状态设置为异常关闭，并告警。 **注意：**默认情况下，接口关闭后不会自动恢复，接口只能由网络管理员启用。如果您希望关闭的接口自动恢复，您可以启用端口自动恢复功能，将接口状态自动恢复为“启动”。

点击“**添加**”按钮可添加安全 MAC 地址。

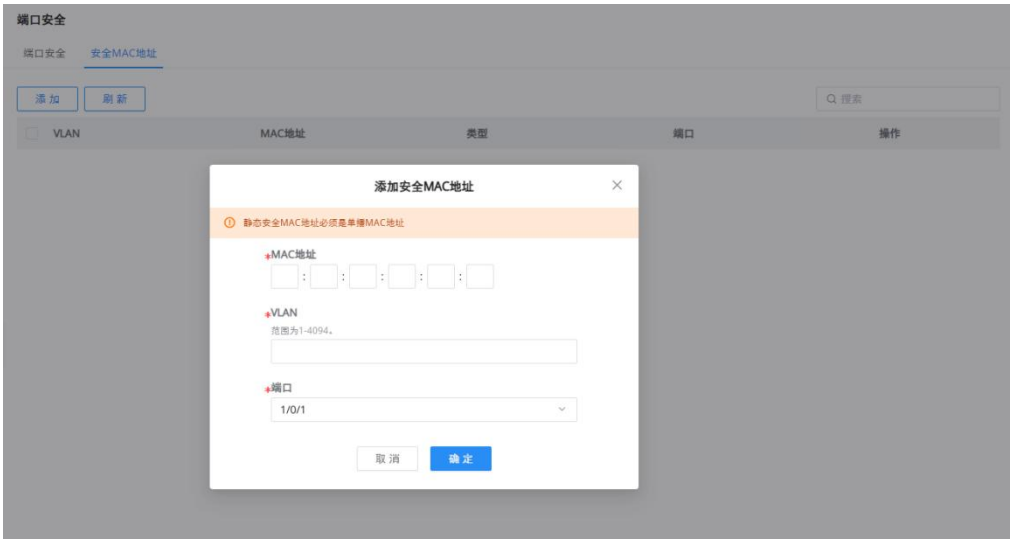


图 114 添加安全 MAC 地址

端口隔离

采用端口隔离功能，可以实现同一 VLAN 内端口之间的隔离。用户只要将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

注意：

由于软件限制，当前仅支持一个隔离组，默认情况下禁用端口隔离功能。将端口添加到默认隔离组，加入后，各端口之间执行双向隔离。

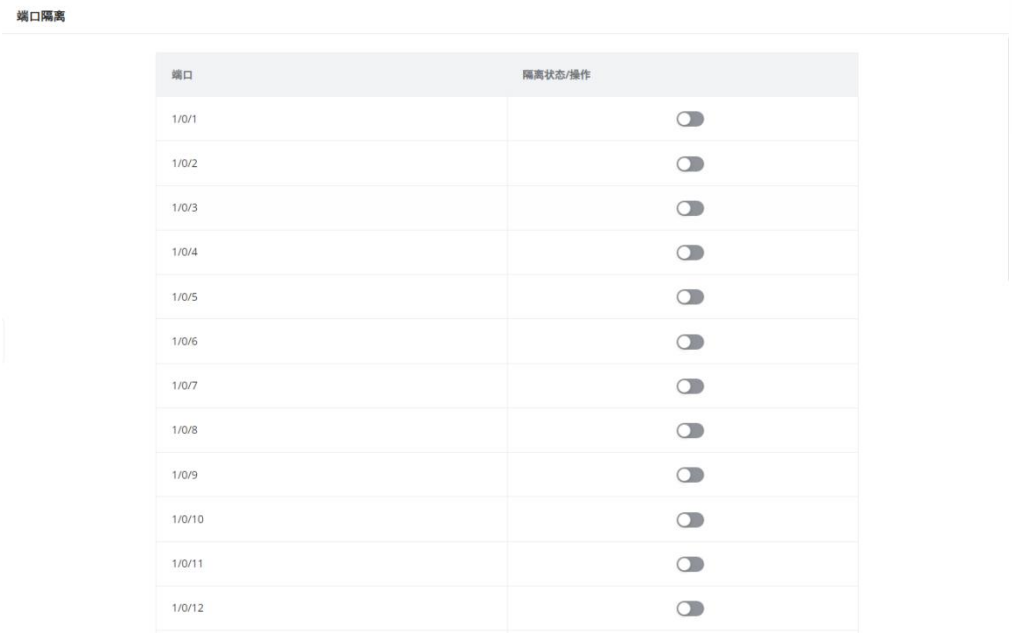


图 115 端口隔离

ACL

访问控制列表 ACL 是由一条或多条规则组成的集合。规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。ACL 本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用 ACL 的业务模块的处理策略来允许或组织该报文通过。

注意：

- 一个 ACL 支持设置多个规则。当规则设置（规则编号除外）相同时，将提示“此规则已存在”
- 如果在遍历所有规则后没有匹配项，则将直接发送拒绝消息。

IPv4 ACL

此页面显示 IPv4 ACL 列表和规则数。

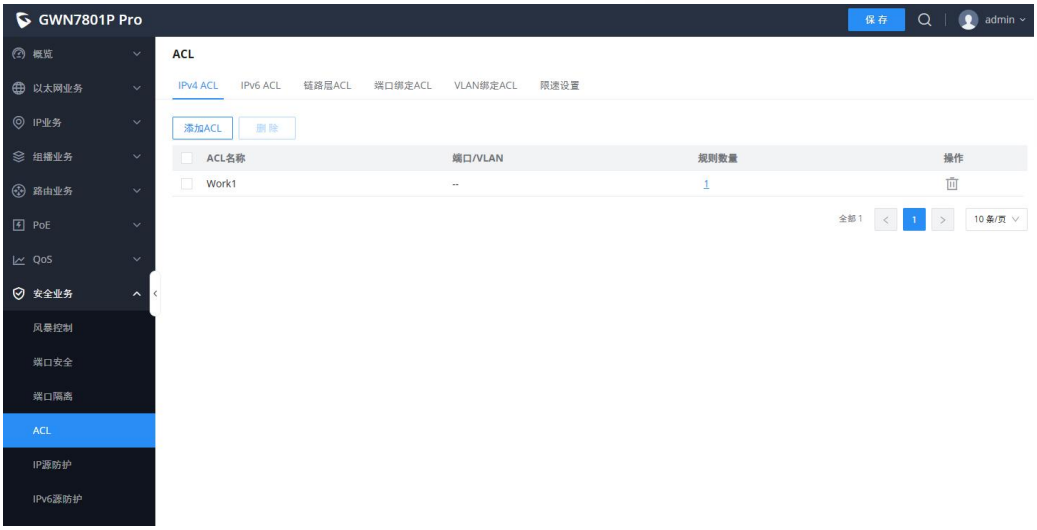


图 116 IPv4 ACL

点击“**添加 ACL**”按钮以添加基于 IPv4 的 ACL 规则。

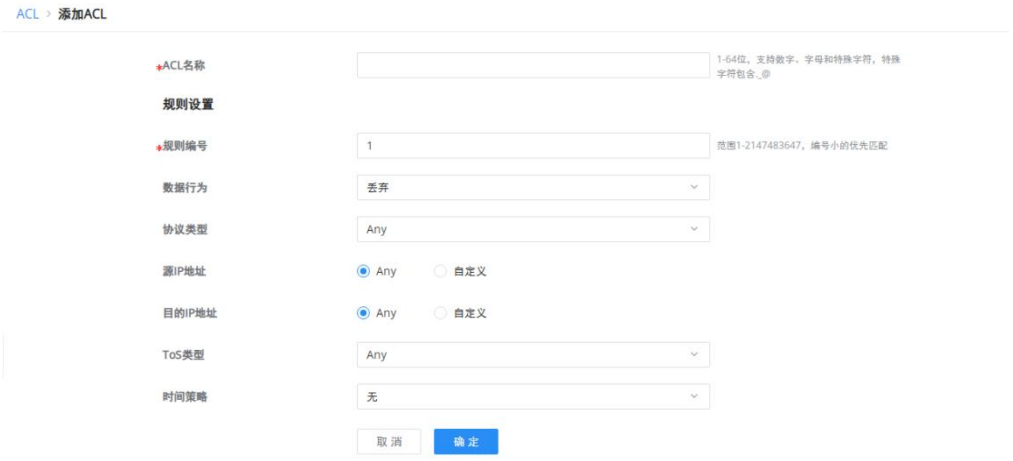


图 117 添加 IPv4 ACL

规则操作可以通过以下四种方式之一进行定义：

- 丢弃：此操作拒绝或阻止匹配指定 ACL 规则的流量，防止数据包通过网络转发。
- 放行：此操作放行匹配 ACL 规则的流量，使数据包能够通过并继续到达其目的地。
- 关闭：此操作在 ACL 规则被触发时禁用通过的接口或端口，有效地停止该接口上的所有流量。
- 重定向至接口：此操作将匹配 ACL 规则的流量转发到不同于其原本目的地的接口，通常用于流量监控、负载均衡或安全目的。

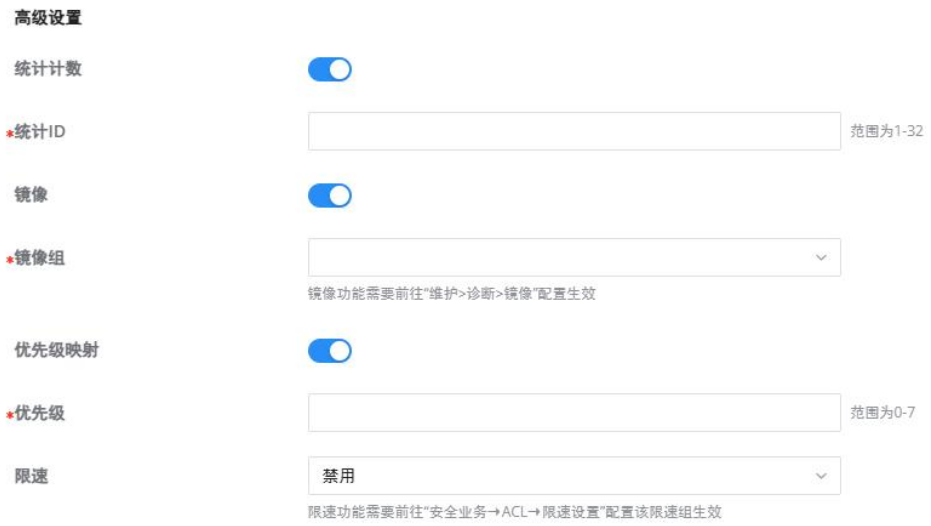


图 118 IPv4 ACL 规则-高级设置

ACL 高级设置支持如下功能：

- 统计计数：规则命中后开启报文统计，并计入对应统计 ID。
- 镜像：规则命中后加入镜像组观察。支持 SPAN 和 RSPAN，需进入“维护 → 诊断 →镜像”进行配置。
- 优先级映射：规则命中后对报文在交换机内部优先级进行映射。
- 限速：对匹配规则的报文进行限速。需进入“安全 → ACL → 限速设置”以配置速率限制组使其生效。

IPv6 ACL

此页面显示 IPv6 ACL 列表和规则数。

图 119 IPv6 ACL

点击“**添加 ACL**”按钮以添加基于 IPv6 的 ACL 规则。

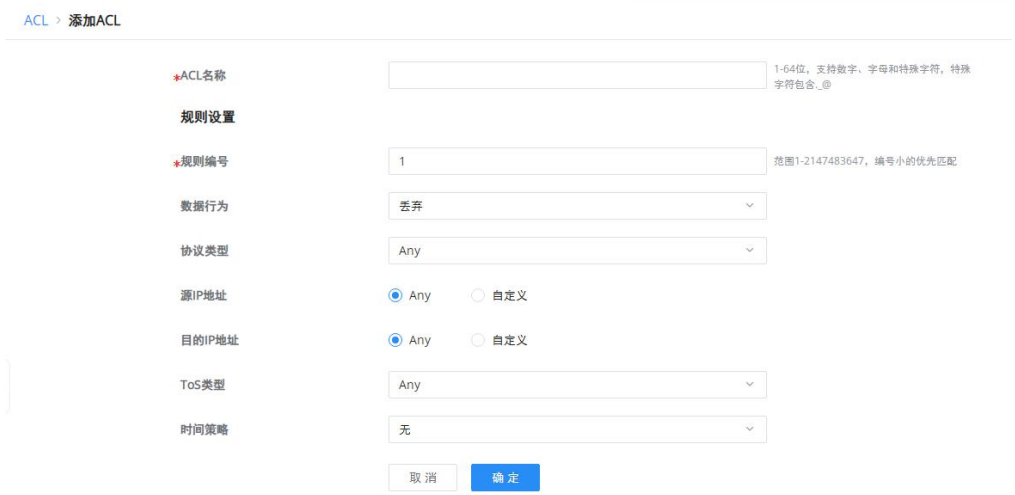


图 120 添加 IPv6 ACL

规则操作可以通过以下四种方式之一进行定义：

- 丢弃：此操作拒绝或阻止匹配指定 ACL 规则的流量，防止数据包通过网络转发。
- 放行：此操作放行匹配 ACL 规则的流量，使数据包能够通过并继续到达其目的地。
- 关闭：此操作在 ACL 规则被触发时禁用通过的接口或端口，有效地停止该接口上的所有流量。
- 重定向至接口：此操作将匹配 ACL 规则的流量转发到不同于其原本目的地的接口，通常用于流量监控、负载均衡或安全目的。

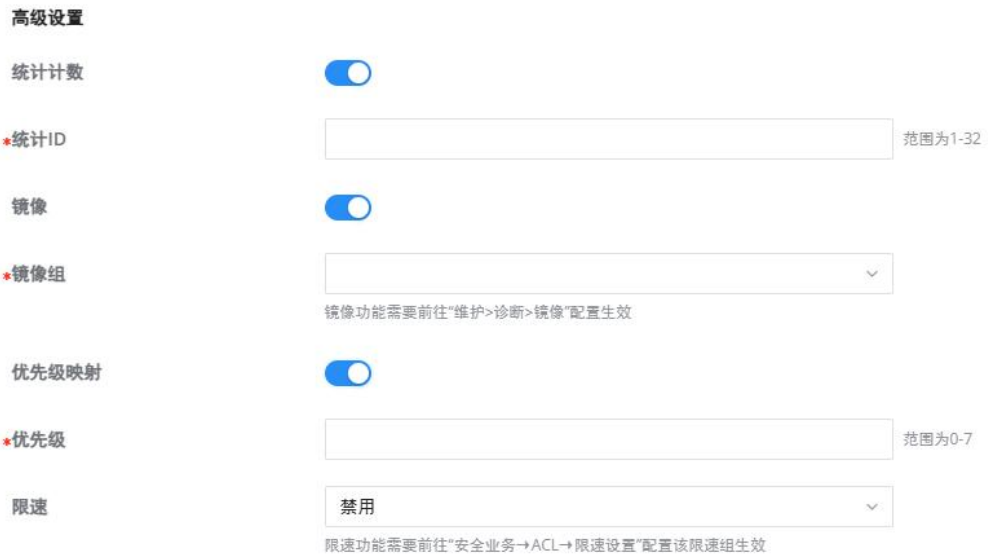


图 121 IPv6 ACL 规则-高级设置

ACL 高级设置支持如下功能：

- 统计计数：规则命中后开启报文统计，并计入对应统计 ID。
- 镜像：规则命中后加入镜像组观察。支持 SPAN 和 RSPAN，需进入“维护 → 诊断 →镜像”进行配置。
- 优先级映射：规则命中后对报文在交换机内部优先级进行映射。
- 限速：对匹配规则的报文进行限速。需进入“安全 → ACL → 限速设置”以配置速率限制组使其生效。

链路层 ACL

链路层 ACL 允许您根据其 MAC 地址允许或拒绝对单个设备的 Wi-Fi 访问。例如，如果您注意到某个顾客设备使用了太多带宽，则可以拒绝其进行 Wi-Fi 访问，而不影响其他顾客设备的使用。

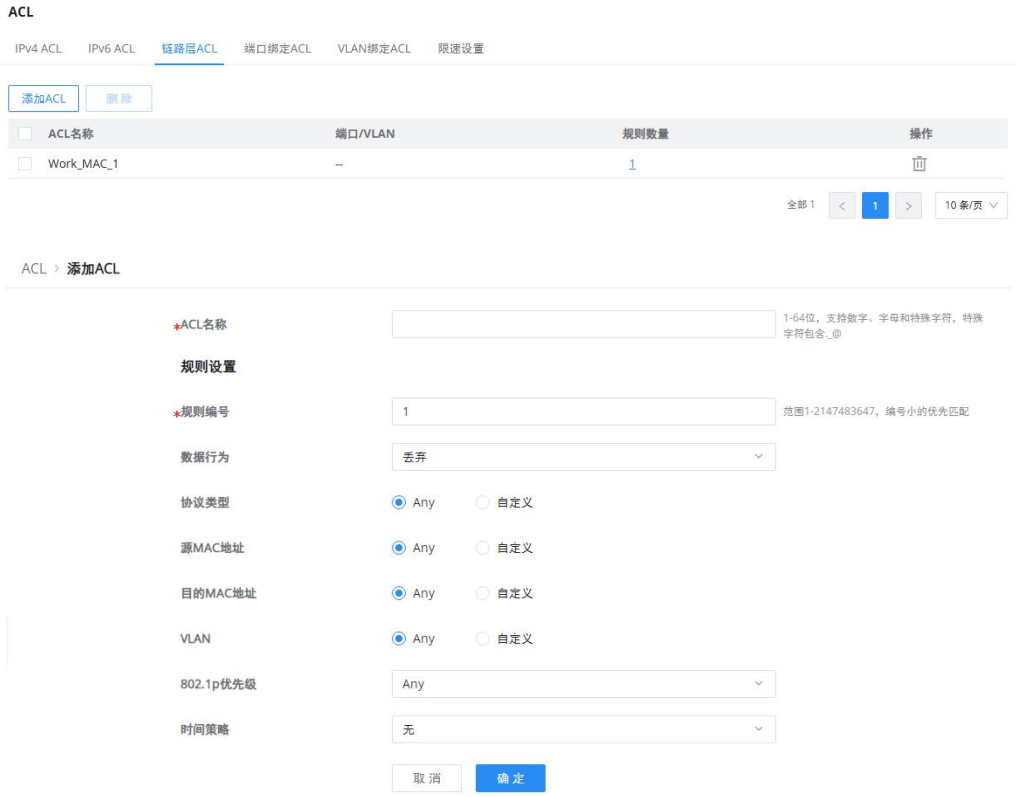


图 122 链路层 ACL

端口绑定 ACL

ACL 绑定允许用户将链路层 ACL 或 IP ACL 绑定到特定端口 GE/LAG。

要在多个端口上应用 IP/MAC ACL 规则，首先选择这些端口，然后单击“**编辑**”按钮，从下拉列表中选择 IP 和 MAC ACL 规则。

要在特定端口上应用 ACL 规则，请单击页面右侧的“**编辑**”，如下面所示：

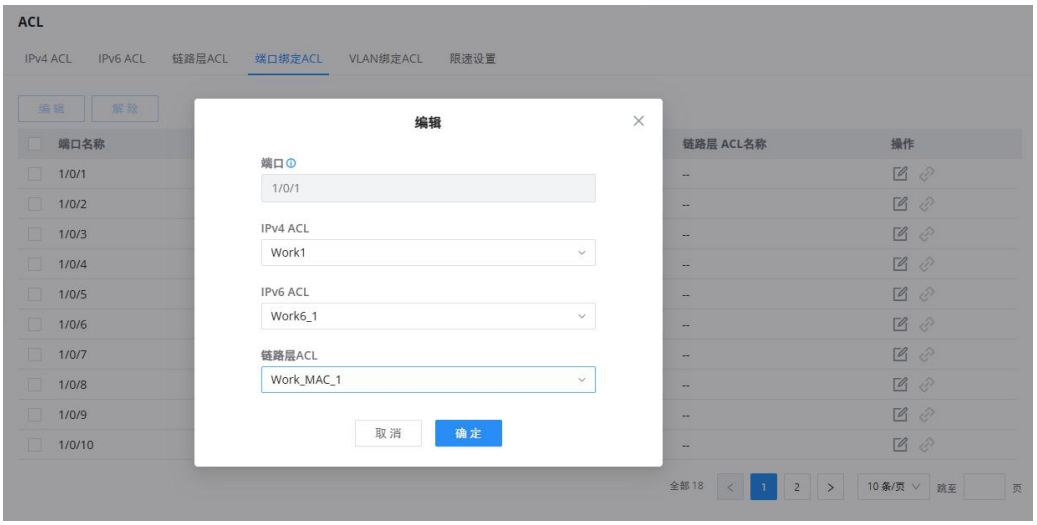


图 123 端口绑定 ACL

VLAN 绑定 ACL

在此页面上，用户可以将 IPv4/MAC ACL 规则绑定到 VLAN，以便将 ACL 规则应用于多个 VLAN，首先从列表中勾选 VLAN，然后点击“**编辑**”按钮，从 IPv4/MAC ACL 下拉列表中选择 ACL 规则。

例如：如果 IPv4/MAC ACL 规则配置了速率限制，然后绑定到 VLAN，带宽限制将适用于指定的 VLAN。

请参见下图：

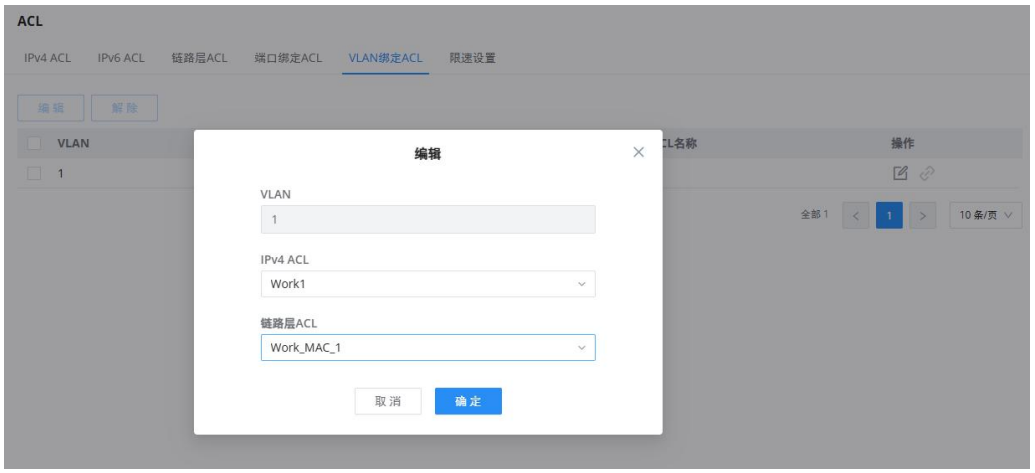


图 124 VLAN 绑定 ACL

限速设置

ACL（访问控制列表）中的速率限制设置部分允许用户为多达 128 个组配置速率限制。速率限制有助于管理和控制网络上发送或接收的流量，以防止拥塞并确保公平使用。此功能对于维护最佳网络性能和避免过载至关重要。

图 125 ACL 限速设置

用户可以通过点击操作列下的“**编辑**”来配置多达 128 个组。

- 点击操作列下的“**编辑**”以配置一个组。
- 选择速率限制类型，以确定限制是按数据包还是按字节。
- 指定突发数据包/字节，这设置允许在突发中发送的最大数据包或字节数。
- 设置速率阈值，它定义每秒允许的数据包或字节的最大速率。

图 126 ACL 限速设置-编辑限速组

IP 源防护

IP 源保护是一种基于第二层接口的源 IP 地址过滤技术。它可以防止恶意主机伪造合法主机的 IP 地址以冒充合法主机，同时确保未经授权的主机无法通过指定的 IP 地址访问网络或攻击网络。IPSG 使用绑定表（源 IP

地址、源 MAC 地址、所属 VLAN 和入接口的绑定）来匹配和检查在第二层接口上接收到的 IP 数据包。只有与绑定表匹配的数据包才被允许通过。

注意：
建议通过访问安全 → DHCP Snooping 先启用 DHCP Snooping。

要启用 IP 源保护，首先访问安全 → IP 源防护页面，然后选择端口并点击“**编辑**”以配置端口。

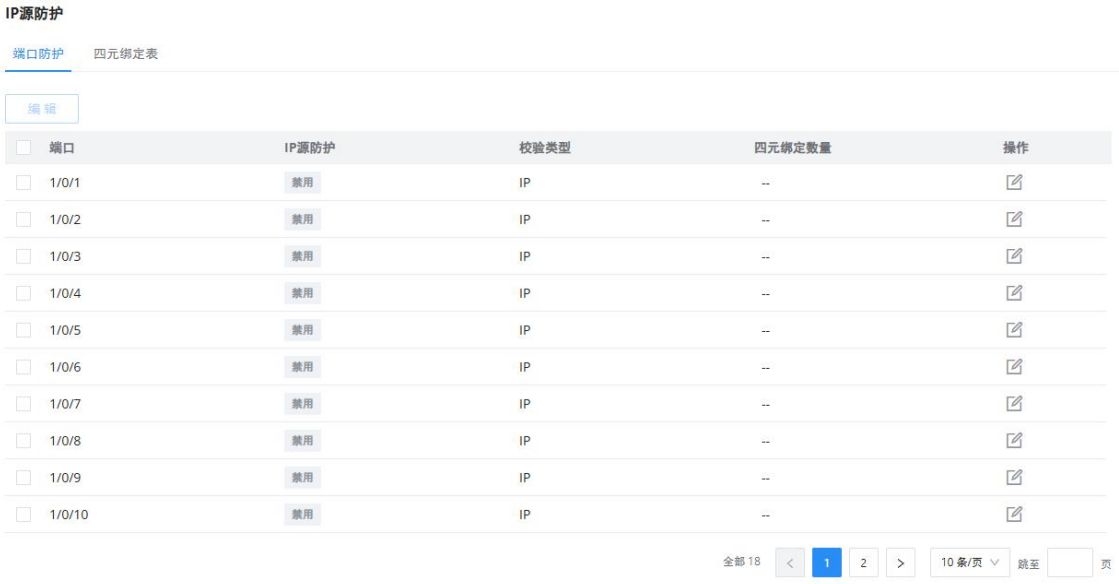


图 127 IP 源防护

然后，选择校验类型，其中校验将基于 IP 地址或 IP 和 MAC 地址均可。

图 128 IP 源防护-编辑端口防护

此页面显示在启用 DHCP Snooping 时，GWN780x Pro 交换机生成的动态绑定（端口、IP、MAC、VLAN），用户还可以通过点击下面的“**添加**”按钮来添加静态绑定。

注意：
动态表项需要开启 DHCP Snooping 功能。

要导入或导出列表，请分别点击**导入**或**导出**按钮。

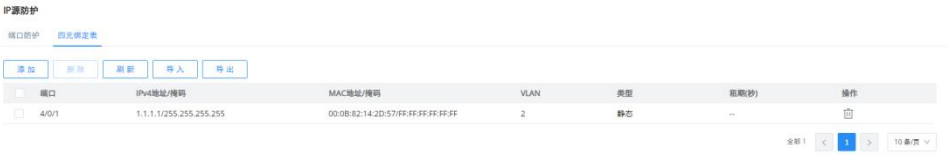


图 129 IP 源防护-导入/导出四元绑定表

绑定要求指定端口、IP 地址及其掩码、MAC 地址及其掩码，以及 VLAN ID。这些信息将用于验证流量，以确保所有流量均由合法用户生成。

图 130 IP 源防护-添加四元绑定表

IPv6 源防护

IPv6 源保护类似于 IP 源保护（基于 IPv4），唯一的区别是 IPv6 源保护过滤 IPv6 地址。

注意：

建议通过访问安全 → DHCPv6 Snooping 先启用 DHCPv6 Snooping。

要启用 IPv6 源保护，首先访问安全 → IPv6 源防护页面，然后选择端口并点击“**编辑**”以配置端口。

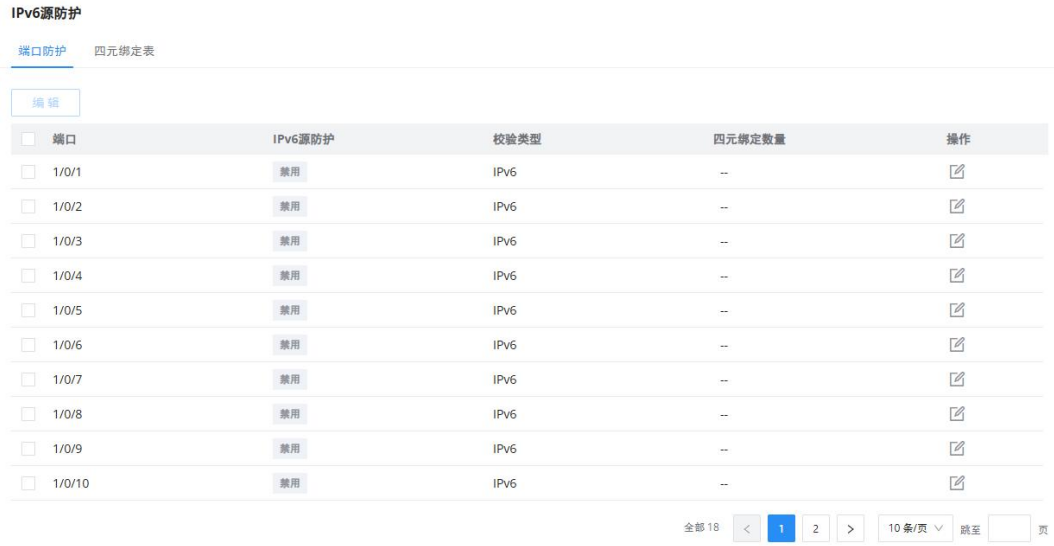


图 131 IPv6 源防护

要在端口上启用 IPv6 源保护，请选择该端口并点击操作列下的“**编辑**”按钮，然后选择校验类型。

图 132 IPv6 源防护-编辑端口防护

此页面显示在启用 DHCPv6 Snooping 时，GWN780x Pro 交换机生成的动态绑定（端口、IPv6、MAC、VLAN），用户还可以通过点击下面的“**添加**”按钮来添加静态绑定。

注意：

动态表项需要开启 DHCPv6 Snooping 功能。

要导入或导出列表，请分别点击**导入**或**导出**按钮。

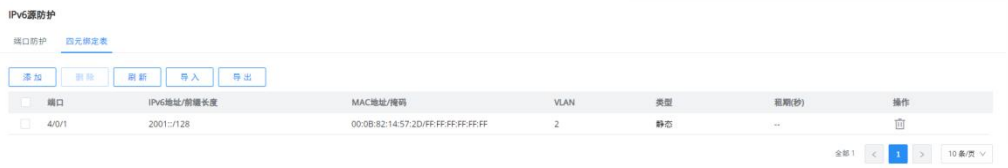


图 133 IPv6 源防护-导入/导出四元绑定表

绑定要求指定端口、IPv6 地址及其掩码、MAC 地址及其掩码，以及 VLAN ID。这些信息将用于验证流量，以确保所有流量均由合法用户生成。

图 134 IPv6 源防护-添加四元绑定表

攻击防范

在网络中，存在着大量针对 CPU 的恶意攻击报文以及需要正常上送 CPU 的各类报文。针对 CPU 的恶意攻击报文会导致 CPU 长时间繁忙的处理攻击报文，从而引发其他业务的断续甚至系统的中断；大量正常的报文也会导致 CPU 占用率过高，性能下降，从而影响正常的业务。

为了保护 CPU，保证 CPU 对正常业务的处理和响应，交换机提供了本地防攻击功能，其针对的是上送 CPU 的报文，主要用于保护设备自身安全，保证已有业务在发生攻击时的正常运转，避免设备遭受攻击时各业务

的相互影响。

攻击防范是一种重要的网络安全特性。它通过分析上送 CPU 处理的报文的内容和行为，判断报文是否具有攻击特性，并配置对具有攻击特性的报文执行一定的防范措施。防范攻击主要分为畸形报文攻击防范、分片报文攻击防范和泛洪攻击防范。

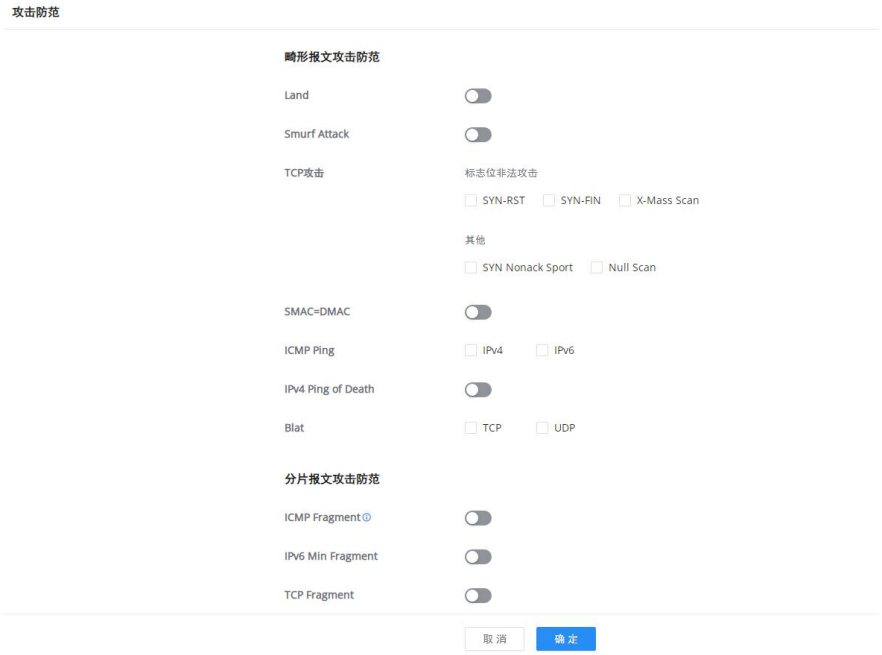


图 135 攻击防范

动态 ARP 检查（DAI）

为了防御中间人攻击，避免合法用户的数据被中间人窃取，可以执行本命令使能动态 ARP 检测功能。设备会将 ARP 报文对应的源 IP、源 MAC、接口和 VLAN 信息与绑定表中的信息进行比较，如果信息匹配，说明发送该 ARP 报文的用户是合法用户，允许此用户的 ARP 报文通过，否则就认为是攻击，丢弃该 ARP 报文。

可在接口视图或 VLAN 视图下使能动态 ARP 检测功能。在接口视图下使能时，则对该接口收到的所有 ARP 报文进行绑定表匹配检查；在 VLAN 视图下使能时。则对加入该 VLAN 的接口收到的属于该 VLAN 的 ARP 报文进行绑定表匹配检查。

当设备丢弃的不匹配绑定表的 ARP 报文数量较多时，如果希望设备能够以告警的方式提醒网络管理员，则可以使能动态 ARP 检测丢弃报文告警功能。当丢弃的 ARP 报文数超过告警阈值时，设备将产生告警。

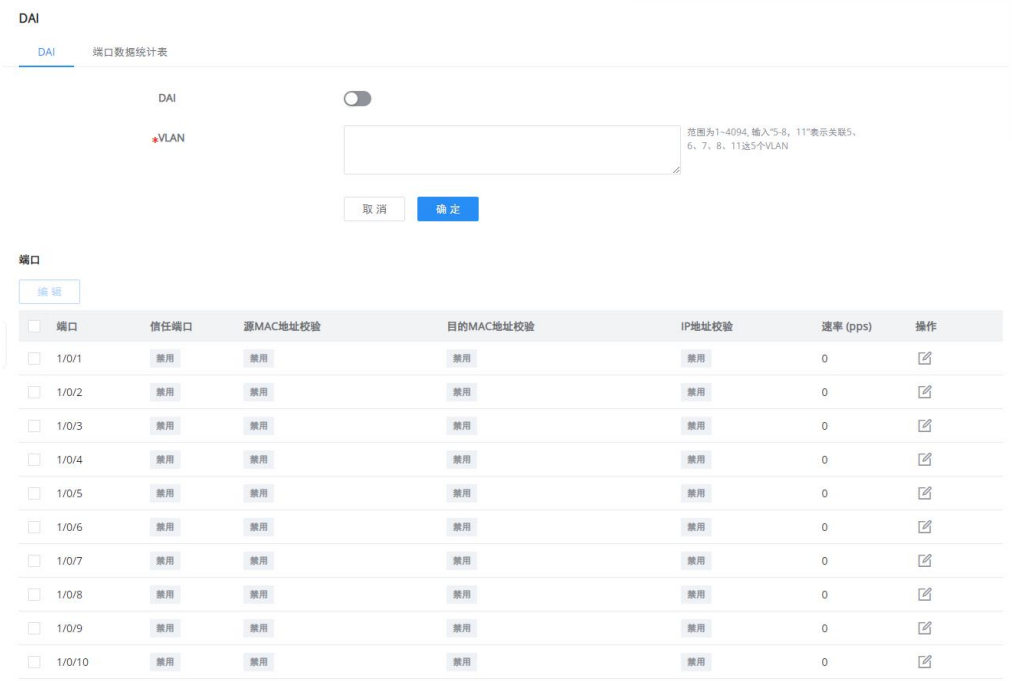


图 136 DAI

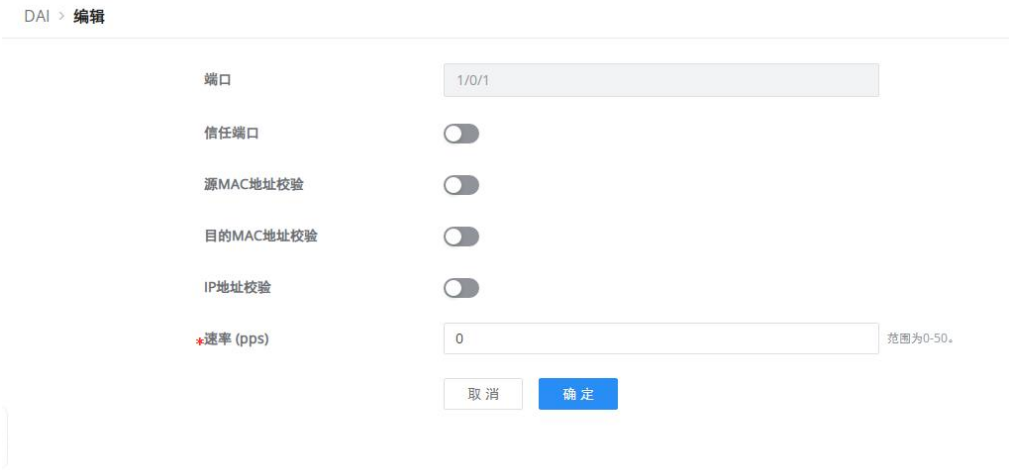


图 137 DAI-编辑端口 DAI

端口数据统计表将列出每个端口/LAG 的 DAI 活动统计信息，并提供刷新统计信息或清除指定端口数据的选项。

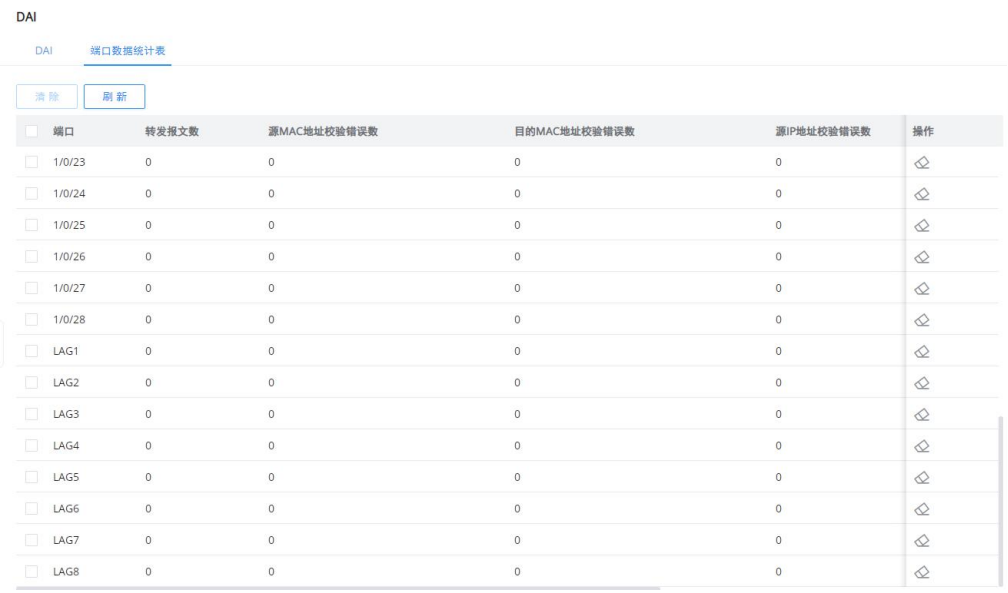


图 138 DAI-端口数据统计表

RADIUS

RADIUS 是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。该协议定义了基于 UDP 的 RADIUS 报文格式及其传输机制，并规定目的 UDP 端口 1812、1813 分别作为默认的认证、计费端口号。

RADIUS 通过认证授权来提供接入服务，通过计费来收集、记录用户对网络资源的使用。RADIUS 协议的主要特征有：（1）客户端/服务器模式；（2）安全的消息交互机制；（3）良好的扩展性。

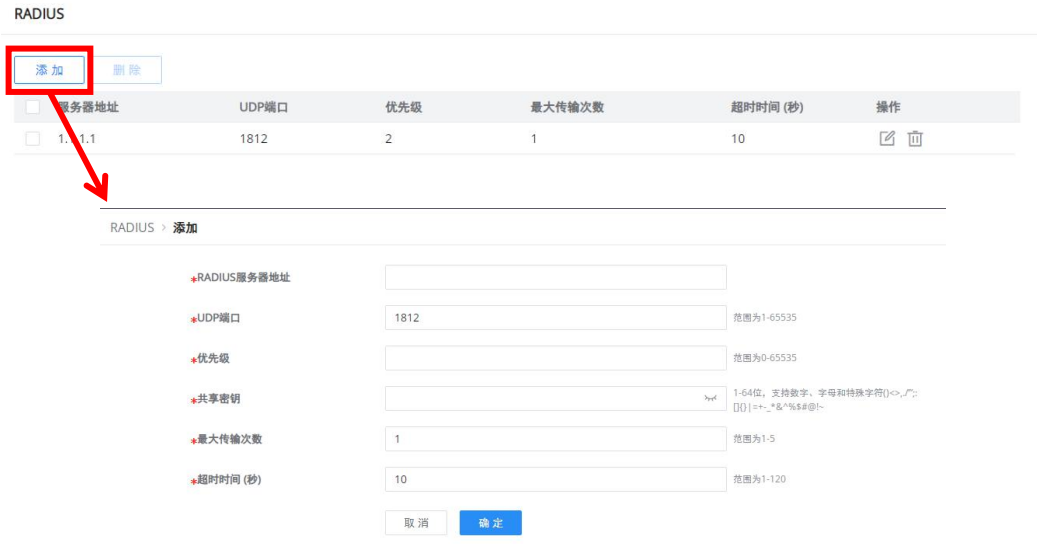


图 139 RADIUS

TACACS+

TACACS+（终端访问控制器控制系统协议）是在 TACACS 协议的基础上进行了功能增强的安全协议。该协议与 RADIUS 协议的功能类似，采用客户端/服务器模式实现 NAS 与 TACACS+服务器之间的通信。

TACACS+是一种集中式的、客户端/服务器结构的信息交互协议，使用 TCP 协议传输，TCP 端口号为 49。TACACS+提供的认证、授权和计费服务器相互独立，能够在不同的服务器上实现。其主要用于采用点对点协议 PPP 或虚拟私有拨号网络 VPDN 方式接入 Internet 的接入用户以及进行操作的管理用户的认证、授权和计费。

TACACS+与 RADIUS 协议相似：（1）结构上都采用客户端/服务器模式；（2）都使用共享密钥对传输的用户信息进行加密；（3）都有较好的灵活性和扩展性。TACACS+具有更加可靠的传输和加密特性，更适合于安全控制。

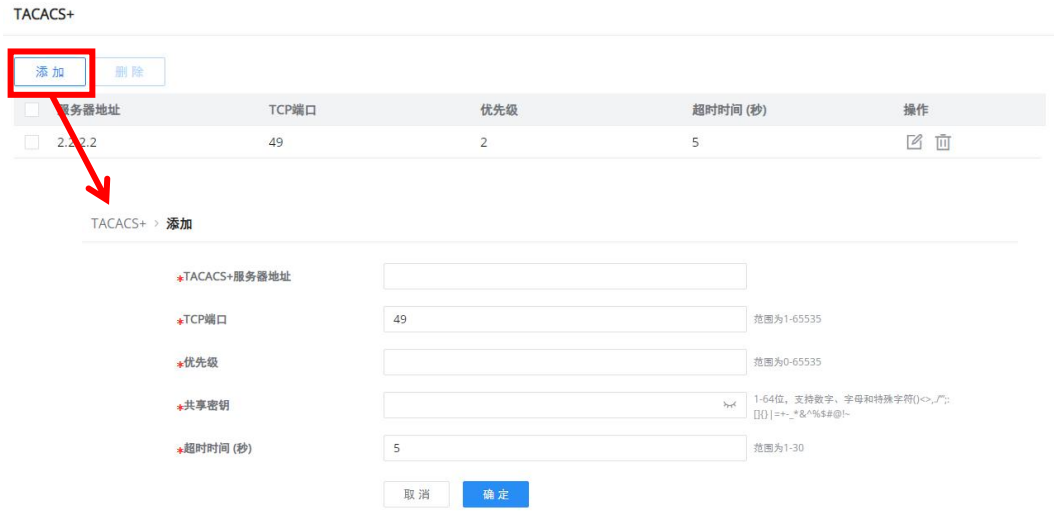


图 140 TACACS+

AAA

访问控制是用来控制哪些用户可以访问网络以及可以访问的网络资源。AAA 是 Authentication（认证）、Authorization（授权）和 Accounting（计费）的简称，提供了在 NAS（网络接入服务器）设备上配置访问控制的管理框架。

AAA 作为网络安全的一种管理机制，以模块化的方式提供服务：

- 认证，确认访问网络的用户的身份，判断访问者是否为合法的网络用户；
- 授权，对不同用户赋予不同的权限，限制用户可以使用的服务；
- 计费，记录用户使用网路服务过程中的所有操作，包括使用的服务类型、起始时间、数据流量等，用于收集和记录用户对网络资源的使用情况，并可以实现针对事件、流量的计费需求，也对网络起到监视作用。

AAA 采用客户端/服务器结构，AAA 客户端运行在接入设备上，通常被称为 NAS 设备，负责验证用户身份与管理用户接入；AAA 服务器是认证服务器、授权服务器和计费服务器的统称，负责集中管理用户信息。AAA 可以通过多种协议来实现，目前设备支持基于 RADIUS 或 TACACS+协议来实现 AAA，在实际应用中，最常使用 RADIUS 协议。

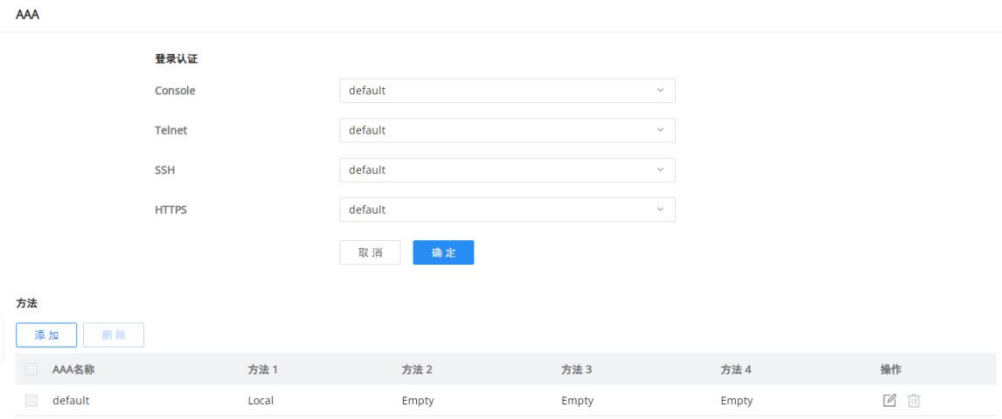


图 141 AAA

添加一个方法，请点击“**添加**”按钮；修改一个方法，请点击上面所示的“**编辑**”图标。

图 142 添加 AAA

表 35 AAA 方法

方法	描述	应用
None	不进行身份验证。用户可以在没有用户名或密码的情况下登录。由于安全风险，通常应避免此设置。	Console，Telnet，SSH，Web UI

Local	使用交换机上的本地用户数据库进行身份验证。用户凭据直接存储在交换机上。	Console，Telnet，SSH，Web UI
Enable	需要用户输入启用密码以获得提升的权限（管理员访问）。这在初始身份验证后提供了额外的安全层。注意：进入特权模式的用户模式密码必须使用 CLI 设置。	Console，Telnet，SSH，Web UI
RADIUS	利用 RADIUS 服务器进行身份验证。RADIUS（远程身份验证拨号用户服务）用于集中管理身份验证、授权和账务。	Console，Telnet，SSH
TACACS+	利用 TACACS 服务器进行身份验证。TACACS（终端访问控制器访问控制系统 Plus）提供更细颗粒度的授权控制，并用于集中式 AAA 管理。	Console，Telnet，SSH，Web UI

身份验证管理

Grandstream GWN780x Pro 交换机上的身份认证管理功能提供了一种通过 802.1X 和基于 MAC 的认证来安全网络访问的强大方法。它允许管理员配置和管理用户认证设置，确保仅授权设备可以连接到网络，从而增强整体网络安全和控制。

802.1X 协议是一种基于端口的网络接入控制协议。基于端口的网络接入控制是指在局域网接入设备的端口这一级验证用户身份并控制其访问权限。802.1X 协议为二层协议，不需要达到三层，对接入设备的整体性能要求不高，可以有效降级建网成本；认证报文和数据报文通过逻辑接口分离，提高安全性。

端口模式

要启用 802.1x 和 MAC 认证，请访问安全性 → 身份认证管理，然后开启“802.1X 认证”和“MAC 认证”，并点击“**确定**”按钮保存。

在此页面上，您还可以为基于 MAC 的用户 ID 指定格式，并启用访客 VLAN。这确保这些设备与主网络保持隔离，同时通过访客 VLAN 保持有限的网络连接。访客 VLAN ID 将未认证的用户引导到指定的网络段，提供受控和安全的访问。

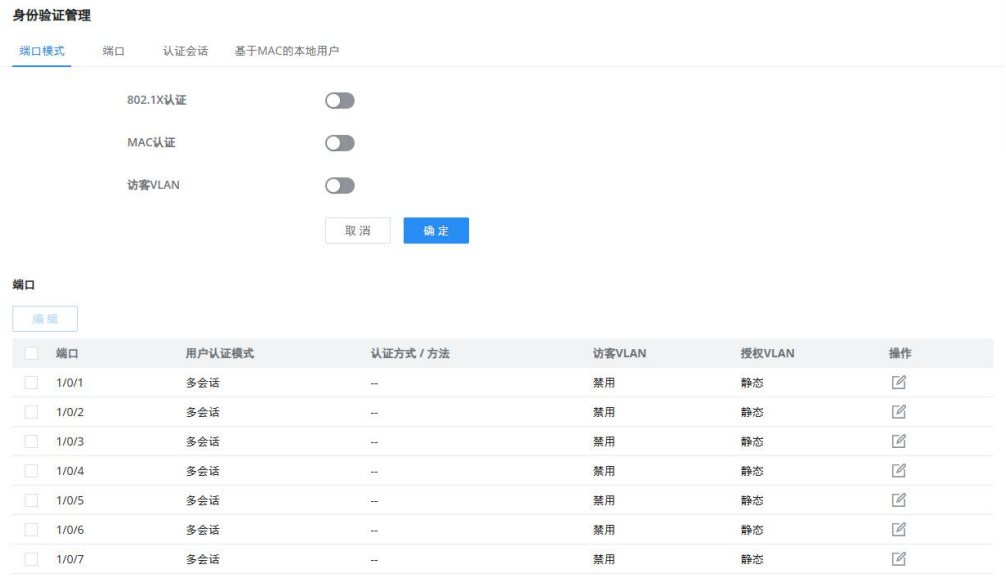


图 143 身份验证管理-端口模式

要在端口上启用，请从列表中选择端口，然后点击“**编辑**”按钮或在操作列右侧点击“**编辑**”。

注意：

必须首先在安全 → RADIUS 下添加 RADIUS 服务器。

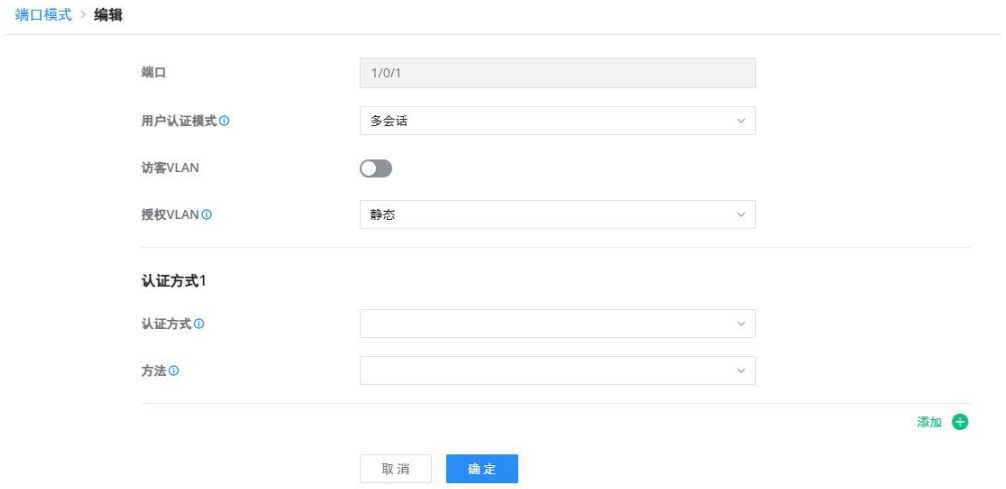


图 144 端口模式-编辑端口

表 36 端口模式-编辑端口

端口	配置的指定端口。
用户认证模式	此端口要使用的用户身份验证模式。选项包括： • **基于 MAC**：表示允许多个用户进行认证，且用户之间互不影响（基于用户 MAC 受控，即使用该 MAC 的用户认证通过了才能上网；每一个 MAC 都必须认证通过才能通信）。

	• **基于端口：**表示允许多个用户认证，且只要一个用户认证通过，其余用户免认证（只要有认证用户在端口认证通过，该端口就成为认证通过的端口，所有接在此端口下的用户都能够正常的使用网络）。 • **单用户：**表示只允许一个用户认证通过（只允许单一用户认证通过，此端口变成已认证端口，认证用户能够正常的使用网络。此时如果发现端口有其它的用户存在，则把端口下的所有用户清除，重新认证）。 默认基于 MAC。
访客 VLAN	选择是否在所选端口上启用风暴控制。
授权 VLAN	指定已认证用户将被分配到的 VLAN ID。这可确保授权设备被放置在正确的网段中。
认证方式 ***注意：****点击 添加 进行新一组认证方式的添加*	
认证方式 1	选择身份验证方法，有如下选项： • **802.1X：**将使用 802.1x 身份验证，必须先添加 RADIUS。 • **MAC 认证：**将使用本地 MAC 地址，具体方法请参见“安全”→“身份验证管理” →“基于 MAC 的本地用户”。
方法	• 如果选择 MAC 身份验证，用户可以添加两种身份验证方式：RADIUS 和 Local。 • 如果选择 802.1x，用户只能选择 RADIUS。

端口

在此选项卡上，用户可以启用身份验证将在哪些端口生效，选择端口，然后单击“**编辑**”按钮或图标来配置端口，如下所示：

图 145 身份验证管理-端口

要在端口上启用身份验证，请在端口控制（禁用、强制身份验证、强制取消身份验证、自动）下选择自动或强制身份验证，然后保存配置。

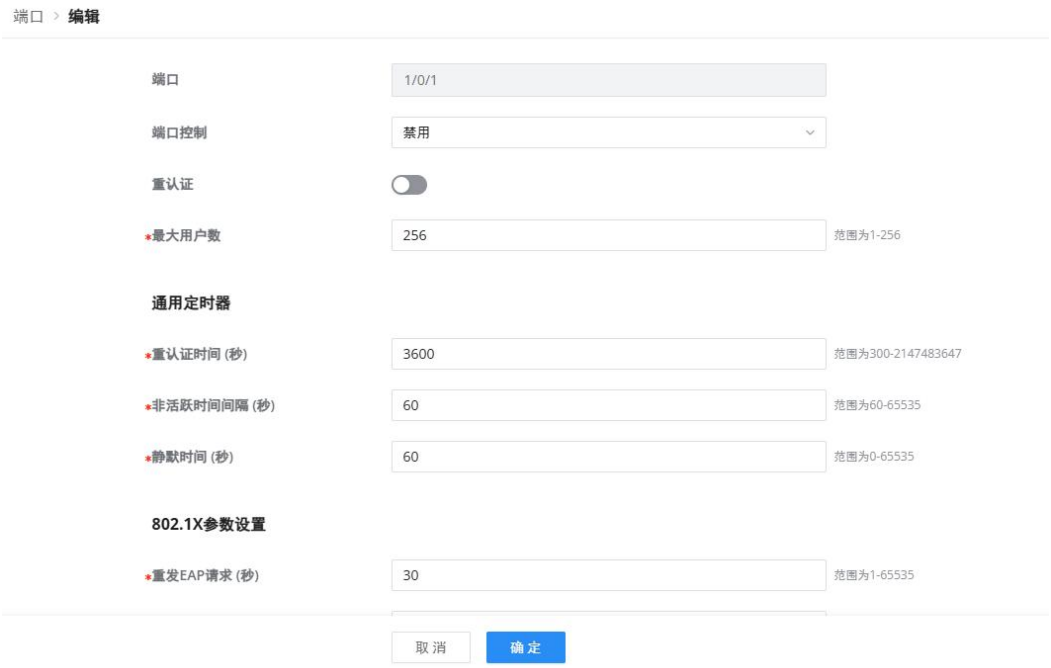


图 146 端口-编辑端口

注意：

连接到 GWN780x Pro 交换机端口的设备上也必须配置 802.1X 功能。

GXV3480 IP 视频电话上的 802.1X 配置示例。

图 147 GXV3480 配置 802.1X

认证会话

在此选项卡中，将列出已认证的设备及其详细信息。请参阅下图：

图 148 身份验证管理-认证会话

有 3 种认证状态（已授权、已锁定、访客）：

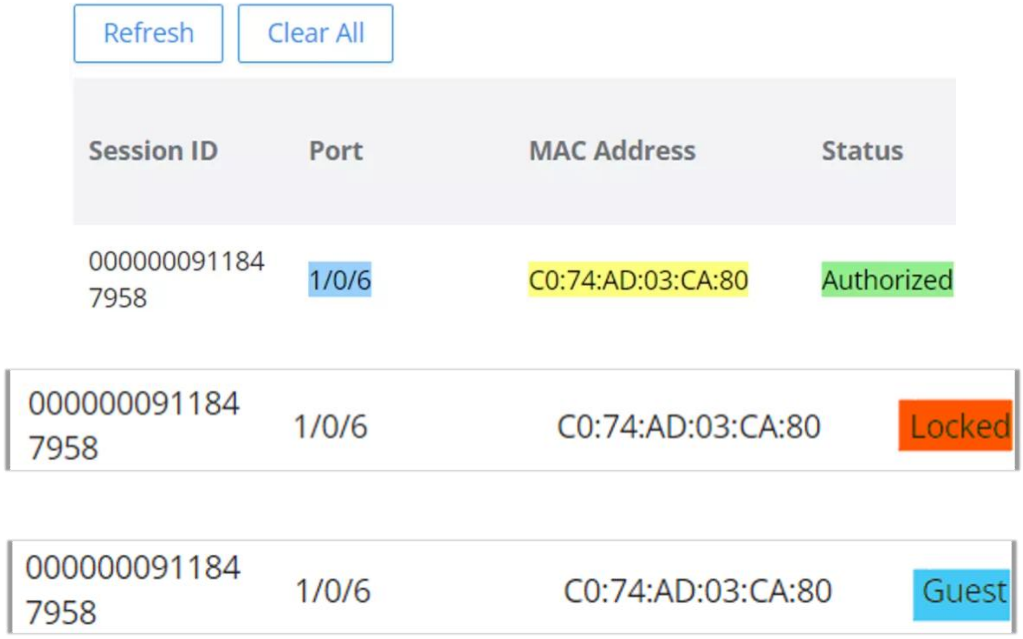


图 149 认证状态

基于 MAC 的本地用户

Grandstream GWN780x Pro 交换机中的“基于 MAC 的本地用户”功能提供了一种根据 MAC 地址添加和管理用户的方法。该功能确保只有具有指定 MAC 地址的设备才能获得网络访问权限，从而增强了对网络资源的安全性和控制力。

图 150 基于 MAC 的本地用户

图 151 添加基于 MAC 的本地用户

表 37 基于 MAC 的本地用户

MAC 地址	本地用户的 MAC 地址必须是单播地址。
端口控制	• 强制授权：强制端口授权具有指定 MAC 地址的设备，使其能够访问网络。

	• 强制拒绝授权：强制端口不授权该设备，阻止其访问网络。
VLAN	VLAN 有效范围为 1-4094。
重认证时间 (秒)	有效范围为 300-2147483647。
非活跃时间 (秒)	有效范围为 60-65535。

DHCP Snooping

DHCP Snooping 确保 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，并记录 DHCP 客户端的 IP 地址与 MAC 地址的对应关系，以防止网络上的 DHCP 攻击。

为了保障网络通信服务的安全，引入了 DHCP 侦听技术，在 DHCP 客户端和 DHCP 服务器之间建立防火墙，防御网络中各种针对 DHCP 的攻击。

设备重启后，IP 源保护的动态绑定表会自动恢复。

注意：
与 DHCPv6 Snooping 的“固化 DHCPv6 Snooping 表项条目”选项关联。

用户可以配置 DHCP Snooping 的静态表项，确保设备重启后，IP 源保护的动态绑定表会在定义的固定时间（以秒为单位）后自动恢复。请注意，这与 DHCPv6 Snooping 的“固化 DHCPv6 Snooping 表项”选项关联。

要在 GWN780x Pro 交换机上启用 DHCP Snooping 功能，请访问“安全”→“DHCP Snooping”，然后启用 DHCP Snooping。要在 VLAN 上启用 DHCP Snooping，请指定 VLAN 或 VLAN 范围，例如 VLAN 5-8 表示从 5 到 8 的 VLAN，然后单击“**确定**”按钮保存。请参考下图：

图 152 DHCP Snooping

Option 82

Option 82 被称为中继代理信息选项，在客户端发起的 DHCP 报文转发到 DHCP 服务器时由 DHCP 中继代理插入。

为了识别客户端访问的设备，用户需要设置远程 ID，支持标准格式和私有格式。

- 标准格式：通常在需要不同供应商设备之间的互操作性时使用，对于 GWN780x Pro 交换机，默认情况下将使用交换机的 MAC 地址但可以使用 1 - 63 范围内的任何其他字符。
- 私有格式：特定于供应商的生态系统 并且可能与其他供应商的设备不兼容（检查供应商特定的格式）。

Option 82 用于标识特定端口的 Curcuit ID 和远程 ID，这可用于标识 VLAN、接口和客户端所在的其他信息。要定义此信息，请访问 DHCP Snooping → Option 82，选择特定端口：

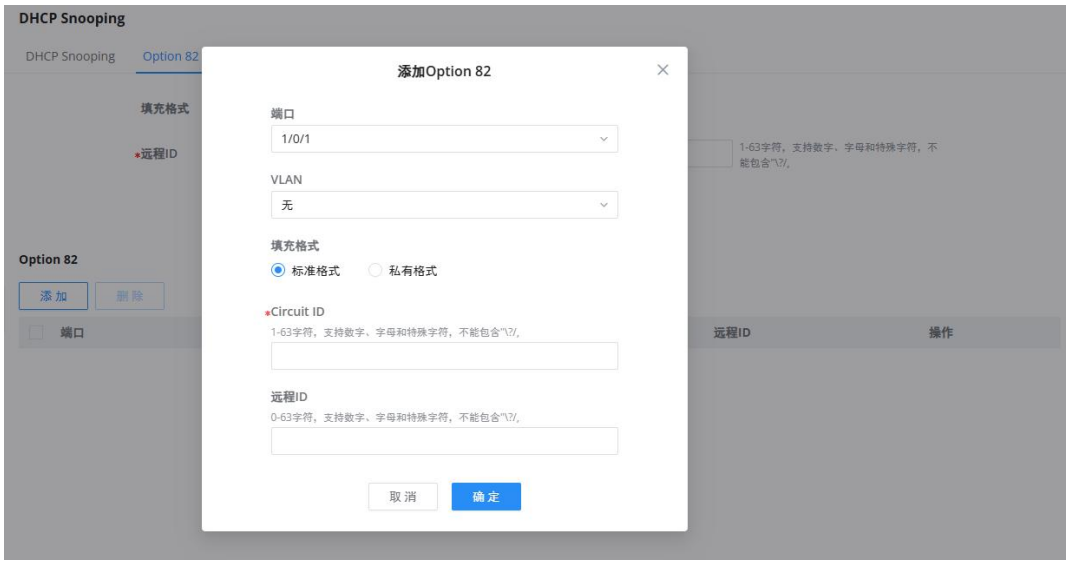


图 153 Option 82-添加 Circuit ID

注意：

每个端口的远程 ID 与交换机的全局远程 ID 不同。

端口设置

在此页面上，用户可以配置允许 DHCP 消息的受信任端口，不受信任的所有其他端口将丢弃 DHCP 消息，这样 GWN780x Pro 将保护用户免受插入不受信任端口的恶意 DHCP 服务器的攻击。

要配置端口，请选择端口并单击“**编辑**”按钮，或单击操作列下的“**编辑**”，如下所示：

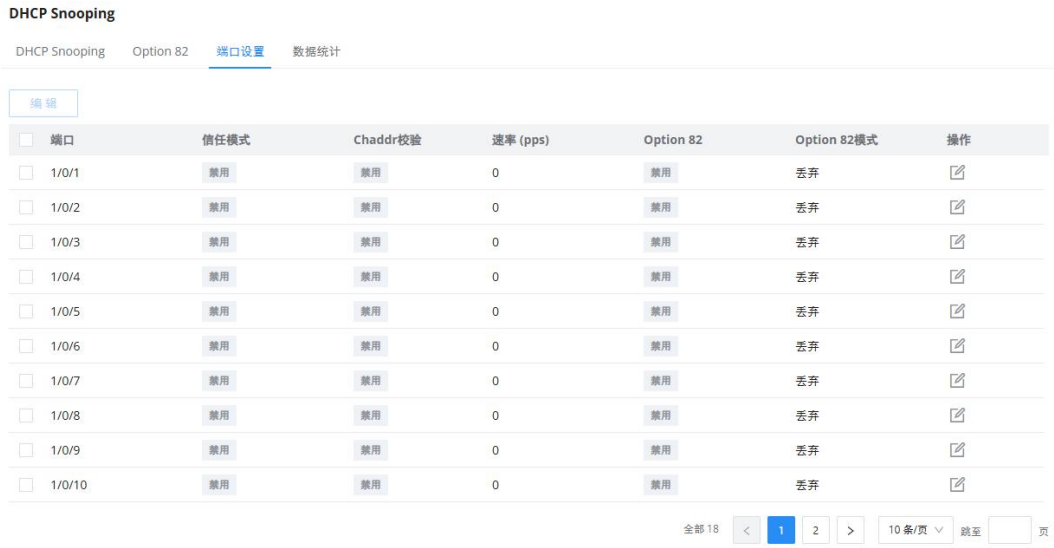


图 154 DHCPSnoping-端口设置

要使端口可信，请打开信任模式，也可以启用更多安全参数，例如 Chaddr 验证、速率（pps = 每秒数据包数）以限制 DHCP 数据包的数量，并为此端口启用 Option 82 具有三种模式（保留、丢弃、替换）。请参考下图：

图 155 DHCP Snooping-编辑端口设置

数据统计

此页面显示 DHCP Snooping 功能记录的所有统计信息。

单击端口的“清除”按钮进行端口数据信息清除，如下所示：

图 156 DHCP Snooping-数据统计

DHCPv6 Snooping

DHCPv6 Snooping 是 IPv6 网络中的一项安全功能，可防止未经授权的 DHCPv6 服务器消息并控制 IPv6 地址分配，类似于 DHCPv4 Snooping 在 IPv4 中的运行方式。

要在 GWN780x Pro 交换机上启用 DHCPv6 Snooping 功能，请访问 Web UI → 安全业务 → DHCPv6 Snooping，然后启用 DHCPv6 Snooping。在 VLAN 上启用 DHCPv6 Snooping，指定 VLAN 或 VLAN 范围，例如 VLAN 5-8 表示 VLAN 从 5 到 8，点击“**确定**”按钮。请参考下图：

图 157 DHCPv6 Snooping

Option 设置

在此页面上，用户可以配置远程 ID（Option 37），默认情况下 GWN780x Pro 交换机使用 GWN780x Pro 交换机的 MAC 地址。

DHCPv6 中继选项（包括 Option 18 和 Option 37）使 DHCPv6 中继代理能够将电路特定的远程信息作为

TLV（类型长度值）嵌入到发送到 DHCPv6 服务器的中继消息中。在这种情况下，托管设备充当 DHCPv6 中继代理。

要为端口添加 Option 18，请单击“**添加**”按钮，如下所示：

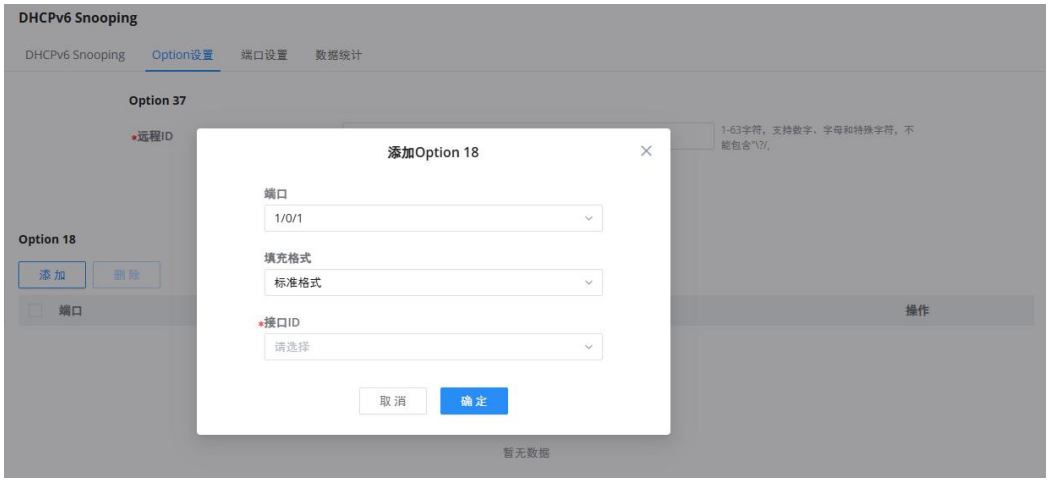


图 158 Option 设置-添加 Option 18

然后，选择端口，格式（标准格式、扩展格式），当选择标准格式时，用户可以选择 VLAN，如果选择了扩展格式，则用户可以接口 ID（3~63 个字符），点击“**确定**”保存。

端口设置

在此页面上，用户可以配置允许 DHCPv6 消息的受信任端口，不受信任的所有其他端口将丢弃 DHCPv6 消息，这样 GWN780x Pro 将保护用户免受插入不受信任端口的恶意 DHCPv6 服务器的攻击。

要配置端口，请选择端口并单击“**编辑**”按钮，或单击操作列下的“**编辑**”，如下所示：

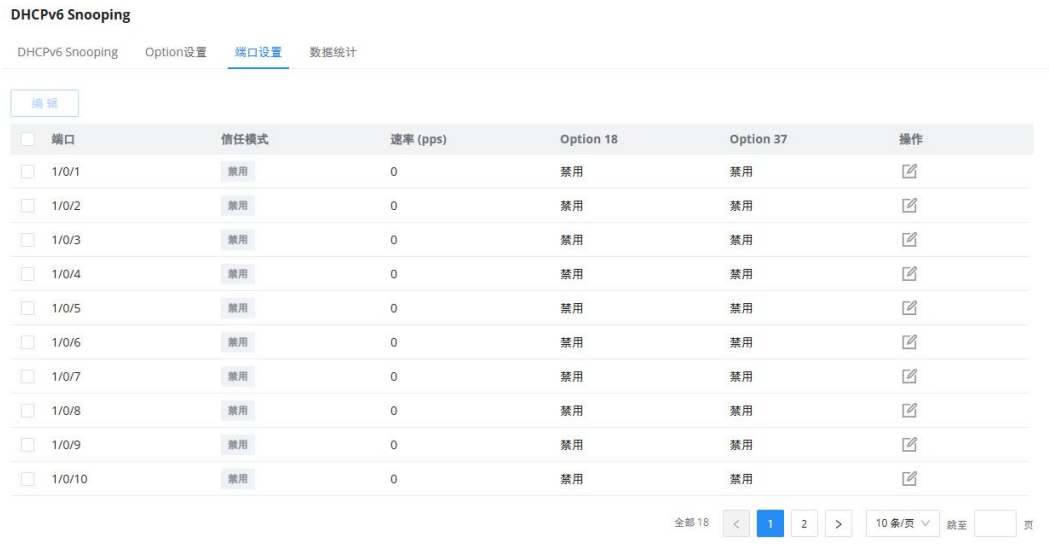


图 159 DHCPv6 Snooping-端口设置

要使端口可信，请打开信任模式，也可以启用更多安全参数，例如速率（pps = 每秒数据包数）以限制

DHCPv6 数据包的数量，并为此端口启用 Option 18 和 Option 37，具有三种模式（保留、丢弃、替换）。请参考下图：

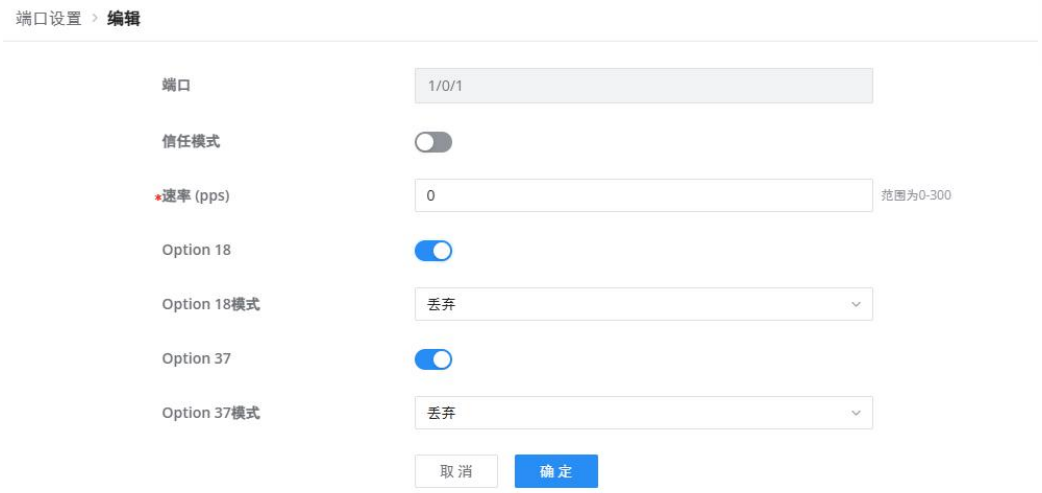


图 160 DHCPv6 Snooping-编辑端口设置

数据统计

此页面显示 DHCPv6 Snooping 功能记录的所有统计信息。

单击端口的“清除”按钮进行端口数据信息清除，如下所示：

图 161 DHCPv6 Snooping-数据统计

维护

升级

GWN780x Pro 系列交换机支持通过 BIN 文件手动上传固件升级，BIN 文件可从 Grandstream 固件页面下载：http://www.grandstream.cn/SoftwareDownloads2/index.aspx

升级方式现有 5 种：

- TFTP
- HTTP
- HTTPS
- FTP
- FTPS

设备也支持通过指定固件服务器路径（例如：Firmware.soutstream.com）升级。

注意：

- 如果 Server 需要，则必须指定用户名和密码。
- FTP 协议使用报头“ftp://”，FTPS 使用报头“ftps://”。
- 考虑到设备的内存问题，上传升级支持流式升级，升级是在上传的同时进行的。

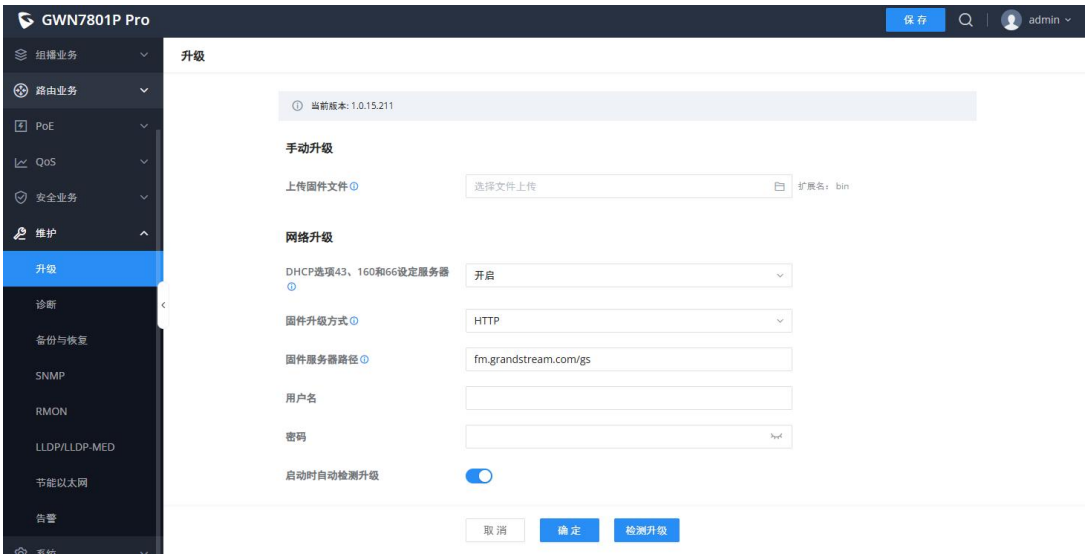


图 162 升级

诊断

GWN780x Pro 系列交换机支持许多诊断工具，可帮助用户排除故障并解决问题。这些工具包括日志、Ping、路由跟踪、镜像和光模块等。

日志

此页面列出了所有生成的日志以及其详细信息、等级和生成时间，还提供了导出列表的选项。

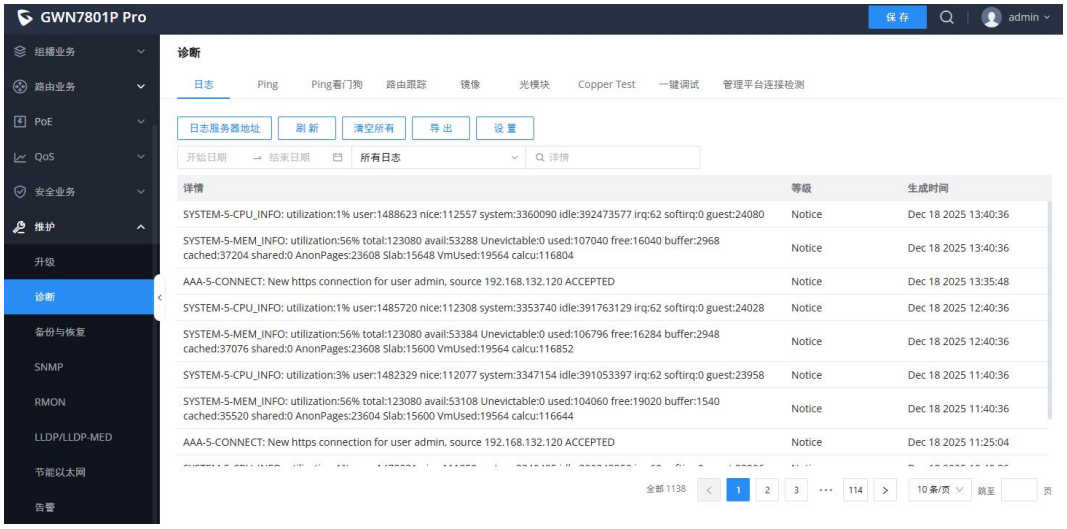


图 163 诊断-日志

GWN780x Pro 系列交换机还支持为日志添加日志服务器地址。

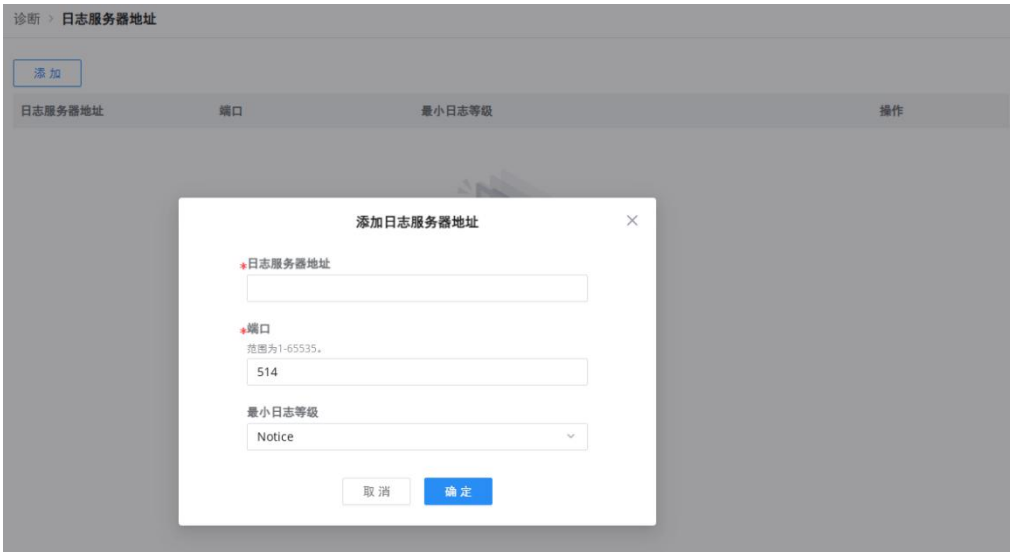


图 164 诊断-日志服务器

用户可以在日志设置中配置以下内容：

- 最小日志级别：定义将记录的事件的最低严重性。“Debug”表示将记录所有消息，包括详细的诊断信息。其他日志级别（例如，Info、Warning、Error）将过滤掉优先级较低的消息。
- 日志聚合：此选项允许您将来自各种来源或组件的多个日志合并到一个集中位置，以便于监控、分析和管理。
- 超时时间 (秒)：此设置定义日志记录作超时之前的时间（以秒为单位）。在显示的示例中，超时设置为 60 秒。有效范围为 15-3600 的整数。

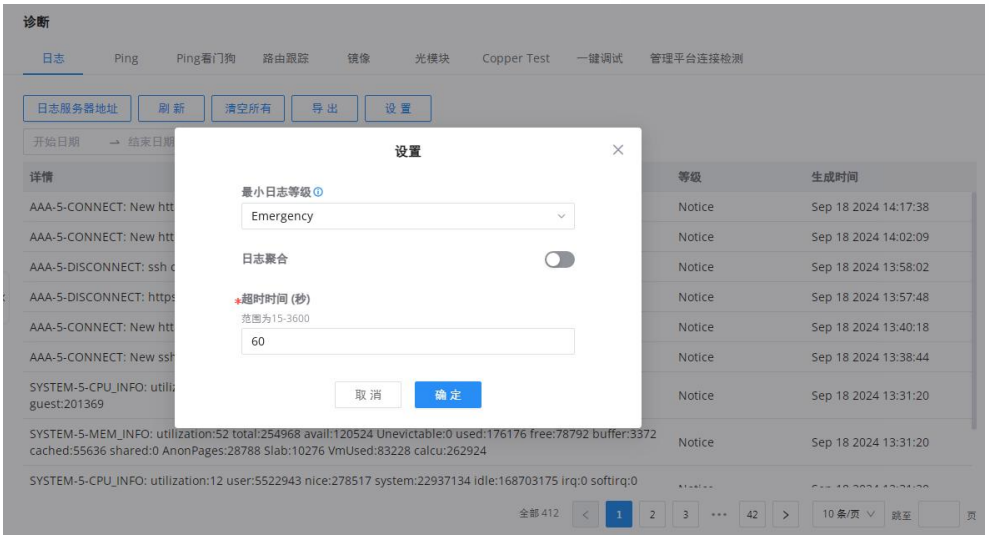


图 165 日志-设置

Ping

此页面中的用户可以输入 IP 地址或主机名，单击“开始”按钮，Ping 命令的结果将显示在下面。

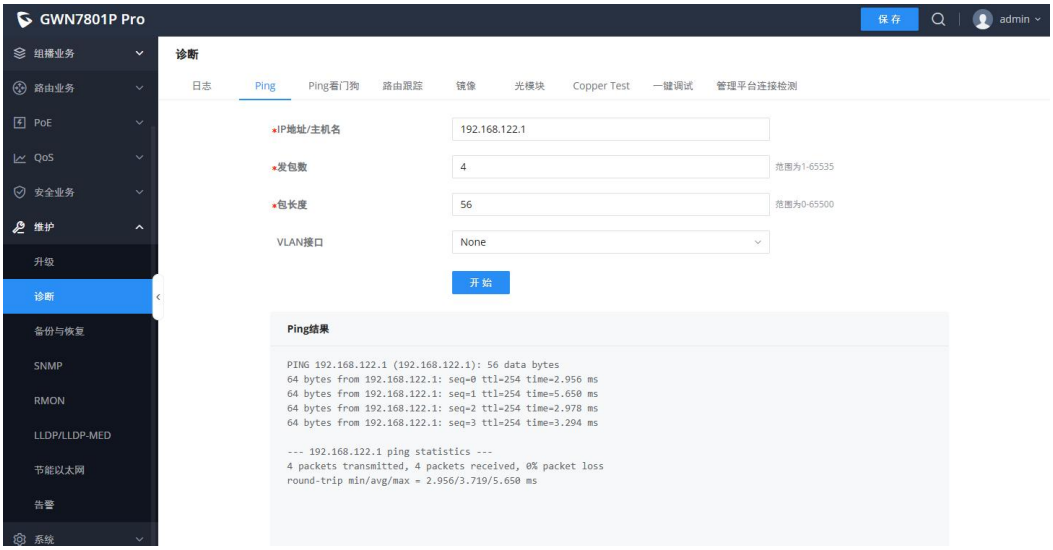


图 166 诊断-Ping

Ping 看门狗

Ping 看门狗是一项功能，旨在通过持续 ping 指定的 IP 地址来监控设备的连接。如果设备对 ping 无响应，则可以根据配置设置触发纠正措施。

- 端口：指定设备上将由 Ping 看门狗监控或管理的端口。
- 使能：打开或关闭所选端口的 Ping 看门狗功能。
- IP 地址：设备将向其发送 ping 请求的目标 IP 地址。

- 数据包发送间隔 (秒)：定义将 ping 数据包发送到指定 IP 地址的频率。
- 延迟时间 (秒)：这将设置 Ping 看门狗在启用设备后或重新启动后开始监控设备之前的延迟。
- 重试次数：指定在监视器执行作之前允许的失败 ping 尝试次数。
- 禁用间隔（秒）：在 ping 测试失败并触发关闭作后，受监控的 PoE 端口将保持关闭状态的时间。

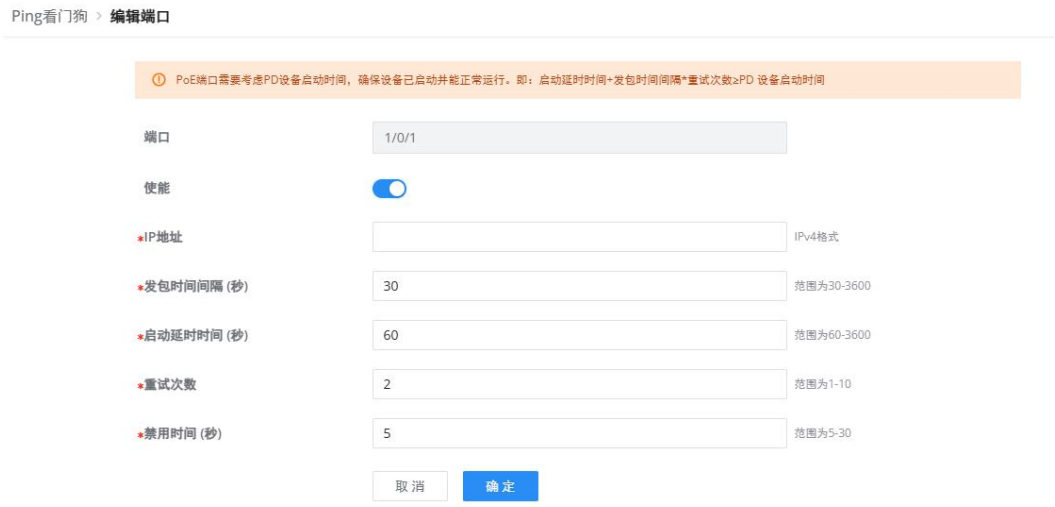


图 167 诊断-Ping 看门狗

路由跟踪

另一个工具是显示跳数的路由跟踪，GWN780x Pro 系列交换机可以让用户直接在交换机 Web UI 运行 Traceroute 命令。

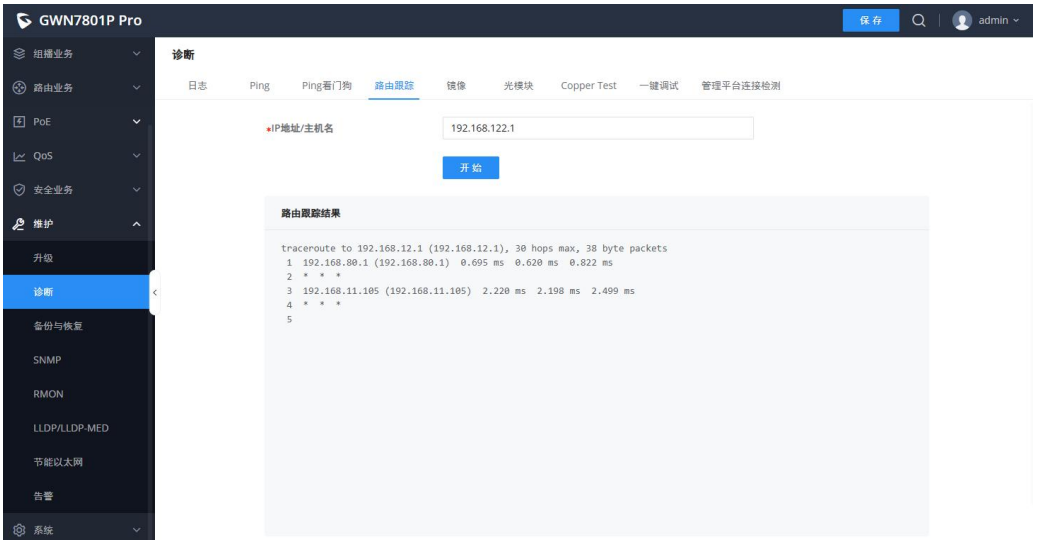


图 168 诊断-路由跟踪

镜像

镜像是指将指定源的报文复制一份到目的端口。指定源被称为镜像源，目的端口被称为观察端口，复制的报

文被称为镜像报文。

镜像可以在不影响设备对原始报文正常处理的情况下，将其复制一份，并通过观察端口发送给监控设备，从而判断网络中运行的业务是否正常。

GWN780x Pro 交换机支持两种端口镜像模式：SPAN 和 RSPAN：

- SPAN（本地）：流量在同一交换机内本地镜像。
- RSPAN（Remote）：使用远程 VLAN 通过网络远程镜像流量。

SPAN

流量镜像在同一交换机内本地进行。SPAN 允许您从一个或多个端口捕获流量，并将其副本发送到另一个端口，通常连接到网络分析器或监控工具。

- 入方向镜像：捕获源端口上的传入流量。
- 出方向镜像：捕获来自源端口的传出流量。
- 观察端口：流量监控的端口。
- 收发普通数据报文：定义在目标交换机上监控的流量类型。

图 169 诊断-镜像-SPAN

RSPAN

RSPAN（远程交换端口分析器）允许通过网络将流量从一个交换机镜像到另一个交换机。与仅限于在同一交换机内本地镜像流量的 SPAN 不同，RSPAN 使用远程 VLAN 在多个交换机之间传输镜像流量，从而实现集中监控。

源交换机角色：

- 入方向镜像：这将捕获指定源端口上的传入流量。它会在交换机处理端口接收的数据包之前对其进行镜像，并将其转发到指定的目标进行监控或分析。
- 出方向镜像：捕获来自指定源端口的传出流量。它会在交换机处理数据包后镜像离开端口的数据包，并将这些数据包转发到监控目标。
- 输出端口：这是源交换机上发送镜像流量的端口。在 SPAN 中，它通常是连接到监控设备的本地端口，但在 RSPAN 中，此流量使用远程 VLAN 通过网络转发到目标交换机。
- 远程 VLAN：这是用于在 RSPAN 配置中的源交换机和目标交换机之间传输镜像流量的 VLAN。源交换机将镜像流量转发到此 VLAN，从而允许通过网络将其发送到目标交换机进行分析。

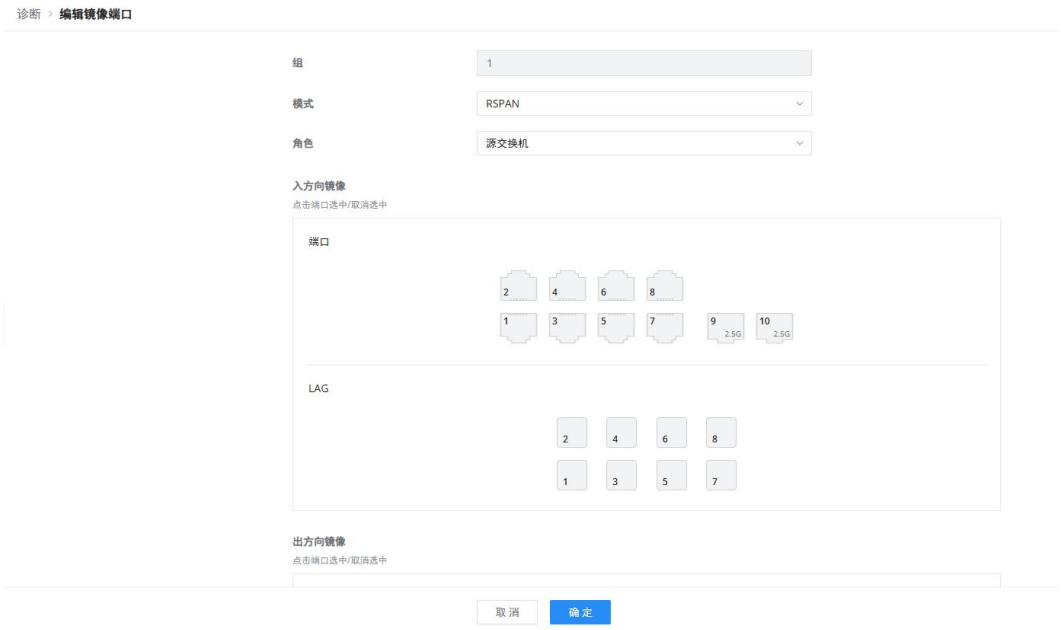


图 170 诊断-镜像-RSPAN-源交换机

目的交换机角色：

- 源端口：这是来自源交换机的镜像流量到达的远程 VLAN。目标交换机通过此 VLAN 接收镜像的数据包，并将其转发到相应的监控端口。
- 观察端口：流量监控的端口。
- 收发普通数据报文：定义在目标交换机上监控的流量类型。
- 远程 VLAN：用于从源交换机接收镜像流量的 VLAN。它与源交换机用于通过网络将镜像流量转发到目标交换机的 VLAN 相同。

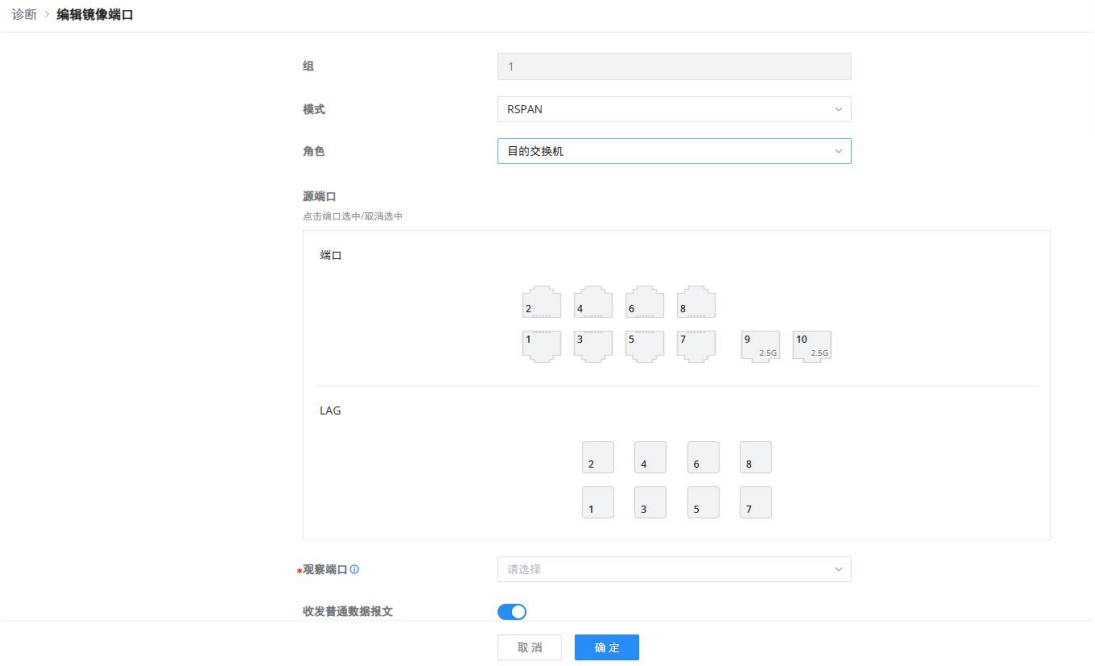


图 171 诊断-镜像-RSPAN-目的交换机

光模块

此页面为用户提供支持光纤模块的端口信息。从下拉列表中选择端口，然后单击 图标更新端口信息。

注意：每个制造商的光模块上显示的信息不同。

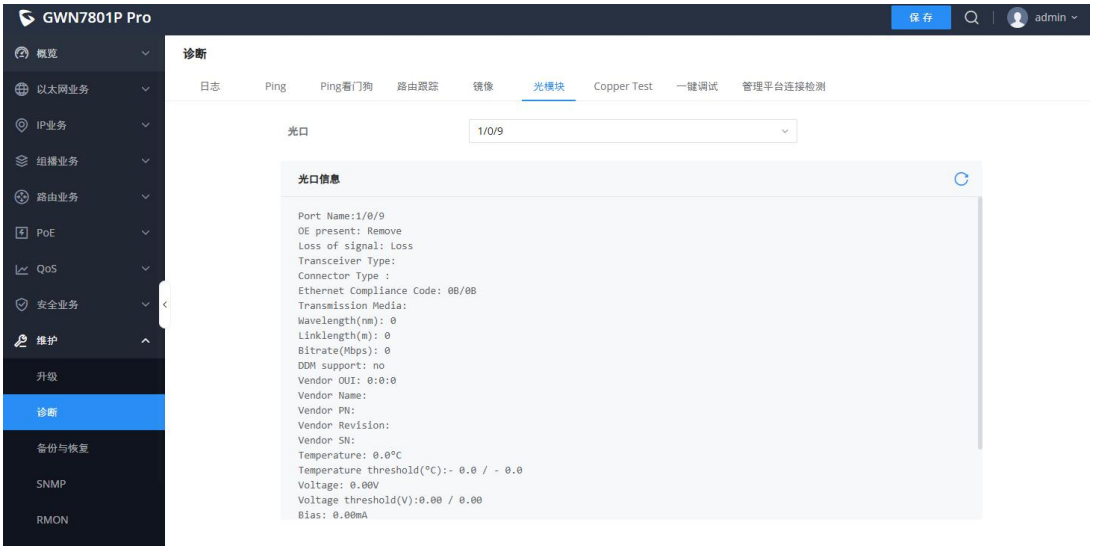


图 172 诊断-光模块

线缆检测

线缆检测能够检测与交换机相连的线缆是否有故障以及故障的位置，利用此功能可以辅助日常工程安装诊断。

注意：

- 检测的端口必须为非 UP 状态。
- 有故障时为端口到故障位置的长度；无故障时为线缆的实际长度；未接线缆时默认为 0 米。
- 诊断结果可能存在±3 米误差，仅供参考。

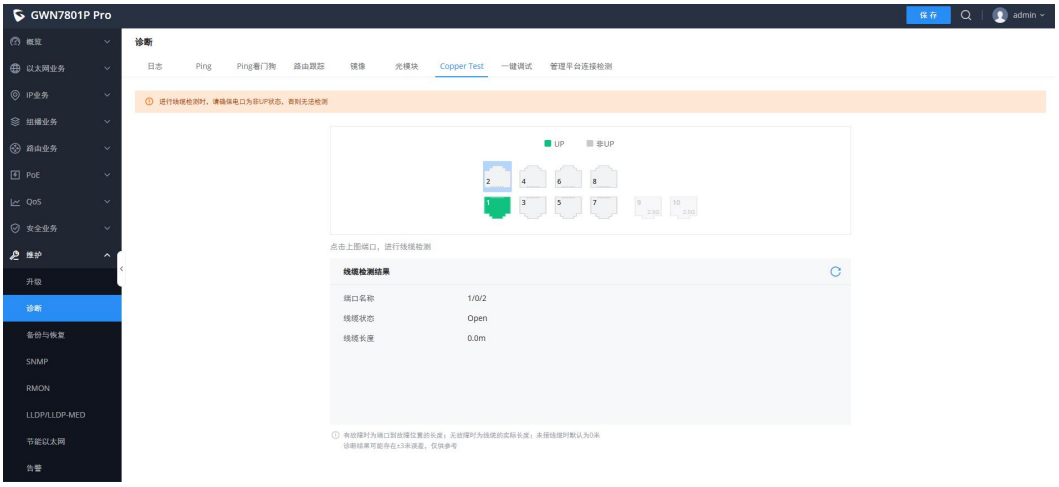


图 173 诊断-线缆检测

线缆状态：

- OK(正常)、Open(开路)、Short(短路)、Mismatch(阻抗不匹配)、LineDriver(线路驱动)、Unknown(未知)

线缆长度：

- 线缆有故障：为端口到故障线缆处的长度
- 线缆无故障：线缆真实长度

一键调试

一键调试功能可以帮助管理员或技术支持在几分钟内快速轻松地获取有关 GWN 交换机的调试信息。

调试中，不影响对设备的配置管理。若触发设备的重启等操作，自动取消调试，设备内不保留调试文件。

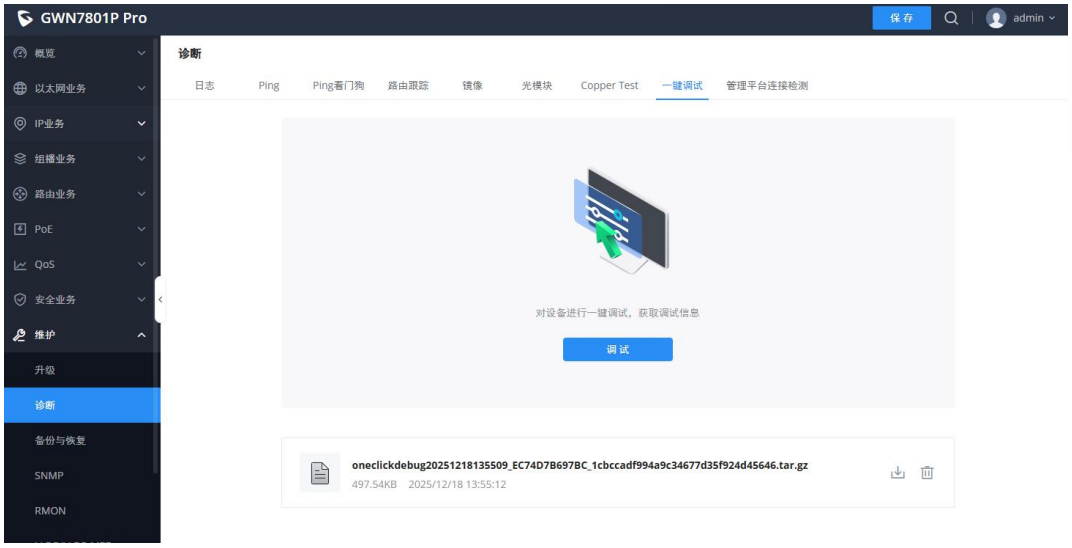


图 174 诊断-一键调试

可以删除生成的文件或在本地下载以与技术支持共享。该文件夹包含许多日志文件，还有一个技术支持文件，其中包含交换机配置等有价值的信息。

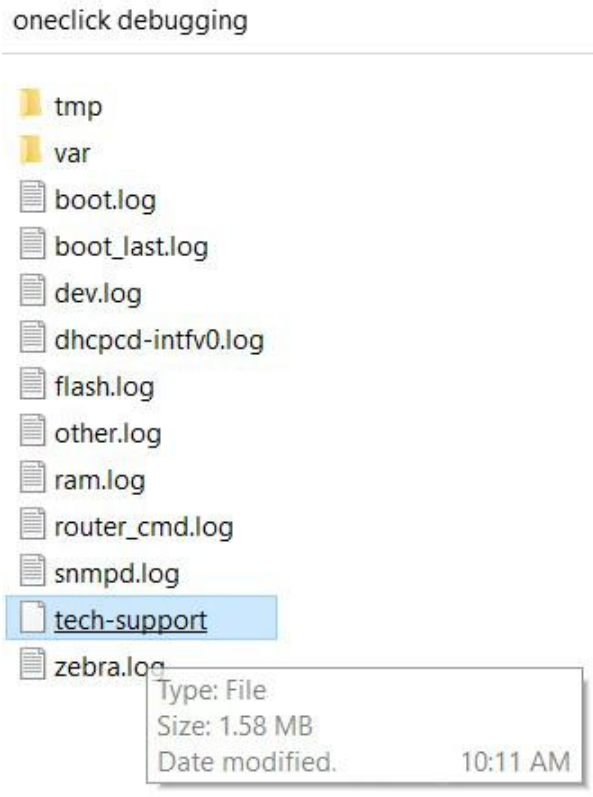


图 175 诊断-调试文件夹信息

管理平台连接检测

如果将 GWN780x Pro 交换机添加到 GDMS Networking、GWN Manager 或 GWN 路由器，它将显示一个

带有绿色复选标记的云图标（如下图所示），表示它已添加到 GDMS Networking、GWN Manager 或 GWN 路由器。

如果连接出现问题，则用户可以访问到 Web UI → 维护 → 诊断 → 管理平台连接检测，然后单击“**检测**”或“**重新检测**”按钮以查看连接在哪个阶段/步骤失败。请参考下图：

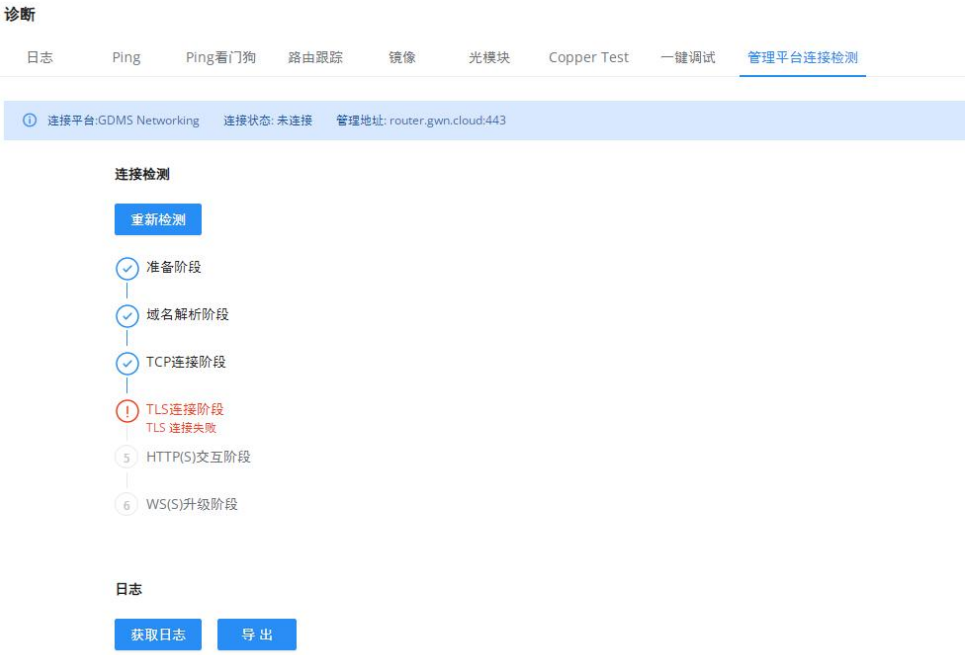


图 176 诊断-管理平台连接检测

备份和恢复

单击“恢复出厂”按钮将 GWN780x Pro 系列交换机重置为默认设置，或通过上载配置文件恢复到以前保存的备份，这些配置文件可作为备份或保存配置的方式。

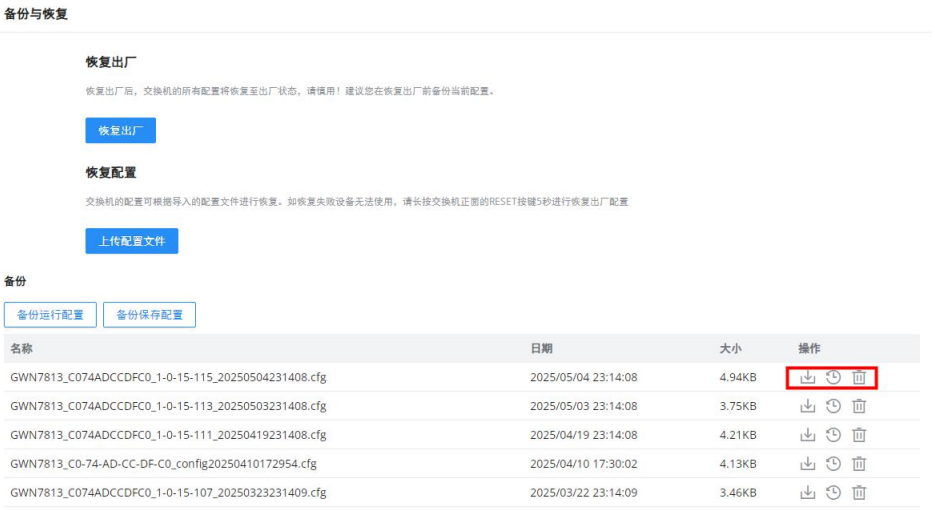


图 177 备份与恢复

SNMP

网络管理协议（SNMP）是用于管理 IP 网络上设备的 Internet 标准协议。通常支持 SNMP 的设备包括路由器、交换机、服务器、工作站、打印机、调制解调器等。SNMP 主要用于网络管理系统，用来监控网络连接设备是否存在需要管理注意的情况。SNMP 是互联网工程任务组（IETF）定义的互联网协议套件的一个组件。它由一组网络管理标准组成，包括应用层协议、数据库模式和一组数据对象。SNMP 管理的网络由三个关键组件组成：

- **受管设备**
- **代理：**在托管设备上运行的软件
- **网络管理站（NMS）：**在管理器上运行的软件

受管设备是实施 SNMP 接口的网络节点，该接口允许对节点特定信息进行单向（只读）或双向（读写）访问。受管设备与 NMS 交换节点特定信息。受管设备有时被称为网络元件，它可以是任何类型的设备，包括但不限于路由器、访问服务器、交换机、网桥、集线器、IP 电话、IP 摄像机、计算机主机和打印机。代理是驻留在受管设备上的网络管理软件模块，代理具有管理信息的本地知识，并将该信息转换为特定于 SNMP 的形式。网络管理站（NMS）执行监视和控制受管设备的应用程序。NMS 提供网络管理所需的大量处理和内存资源，管理网络上可以存在一个或多个 NMS。

全局设置页面允许用户使用本地引擎 ID 启用 SNMP 功能或添加远程引擎 ID。

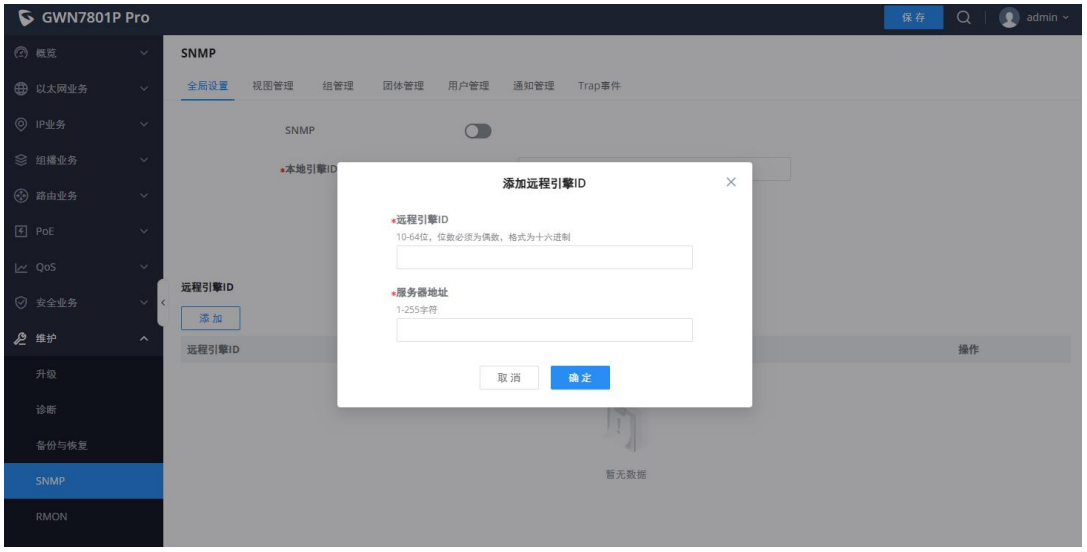


图 178 SNMP-全局设置

表 38 SNMP-全局设置

SNMP	选择是否启用 SNMP。
本地引擎 ID	设置本地 SNMP 实体的引擎 ID 或单击“重置”以恢复到初始值。

	注意: 默认值为 8000 A59Dxxxxxxxx，其中 xxxxxxxx 是默认的设备 MAC 地址，可由用户修改。它以十六进制表示，长度限制在 2 到 56 个字符之间。字符数必须是偶数。
添加/编辑远程引擎 ID	
远程引擎 ID	设置 SNMP 管理端的引擎 ID，在远程引擎下建立远程用户。输入长度限制为 10-64 个字符，以十六进制表示，字符数必须为偶数。
服务器地址	设置网管站服务器的地址，支持主机名和 IP 地址（包括 IPv4 和 IPv6），需要满足各种类型地址格式的要求，否则会提示错误消息。

视图管理

此页面允许网络管理员创建 MIB 视图（管理信息基础），在视图中包括或排除 OID（对象标识符）。

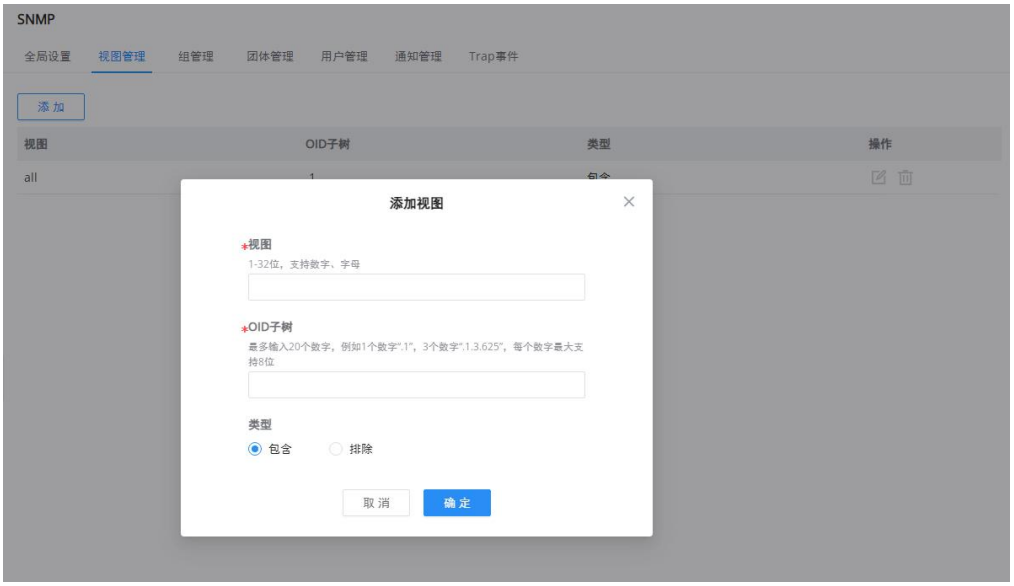


图 179 SNMP-视图管理

组管理

此页面允许网络管理员对 SNMP 用户进行分组，并分配不同的授权和访问权限。

图 180 SNMP-组管理

团体管理

此页面允许用户添加/删除多个 SNMP 团体。

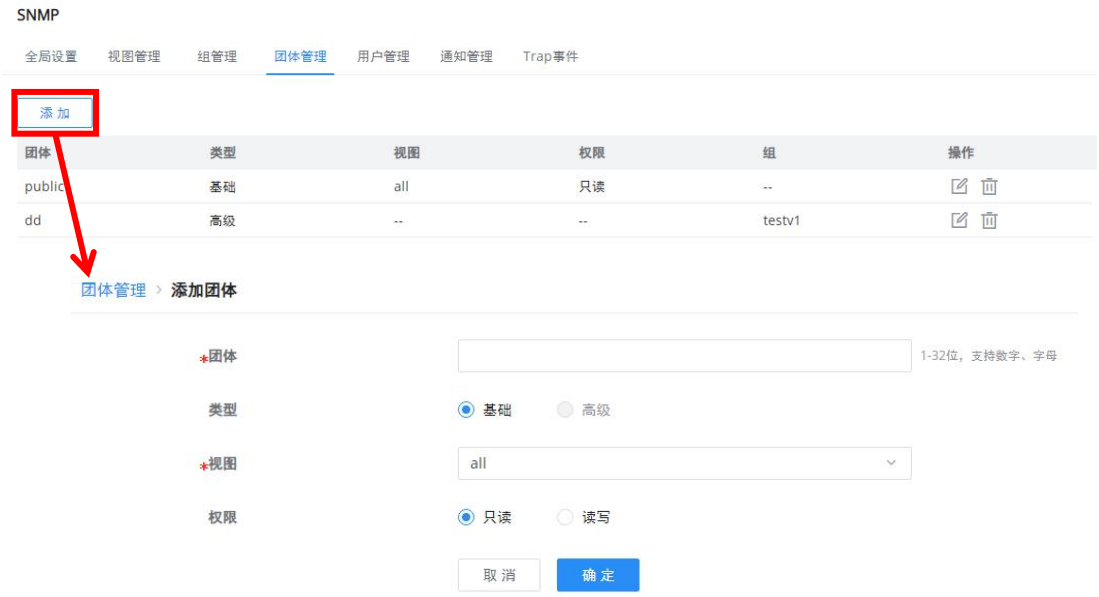


图 181 SNMP-团体管理

用户管理

此页面允许用户配置 SNMPv3 的用户配置文件。

前提：必须添加有 SNMPv3 的组。

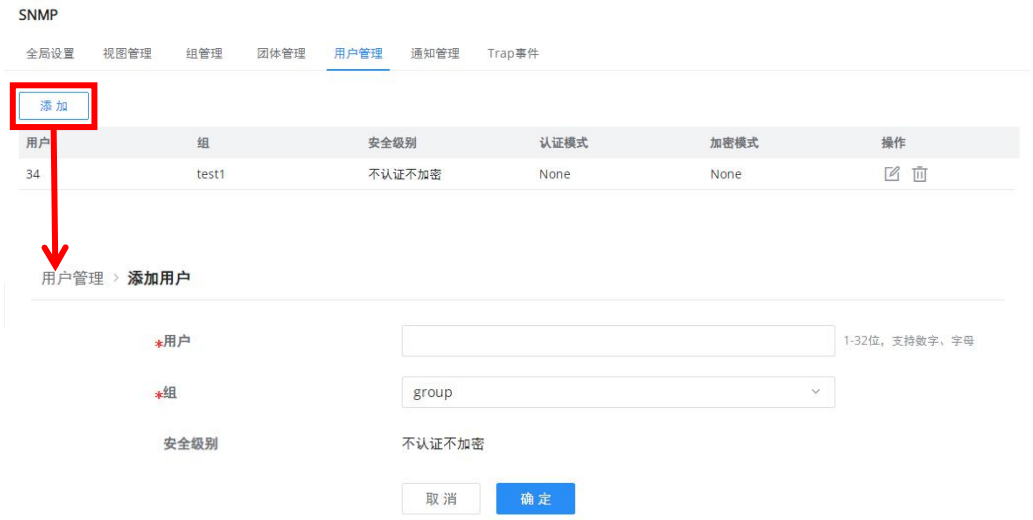


图 182 SNMP-用户管理

通知管理

此页面允许用户配置主机以接收 SNMPv1/v2/v3 通知。

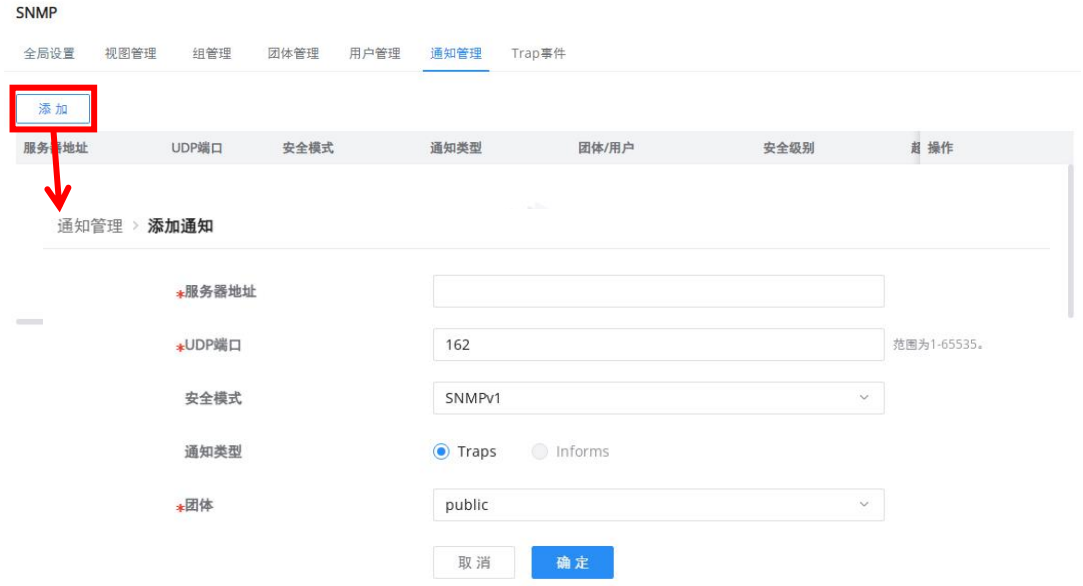


图 183 SNMP-通知管理

Trap 事件

Trap 事件是指在发生特定事件时设备或系统自动发送的警报或通知。这些事件（显示在 SNMP 配置中）是系统正在监控的各种类型的情况。启用后，设备会向 SNMP 管理器发送一个 Trap，通知其发生如下情况：

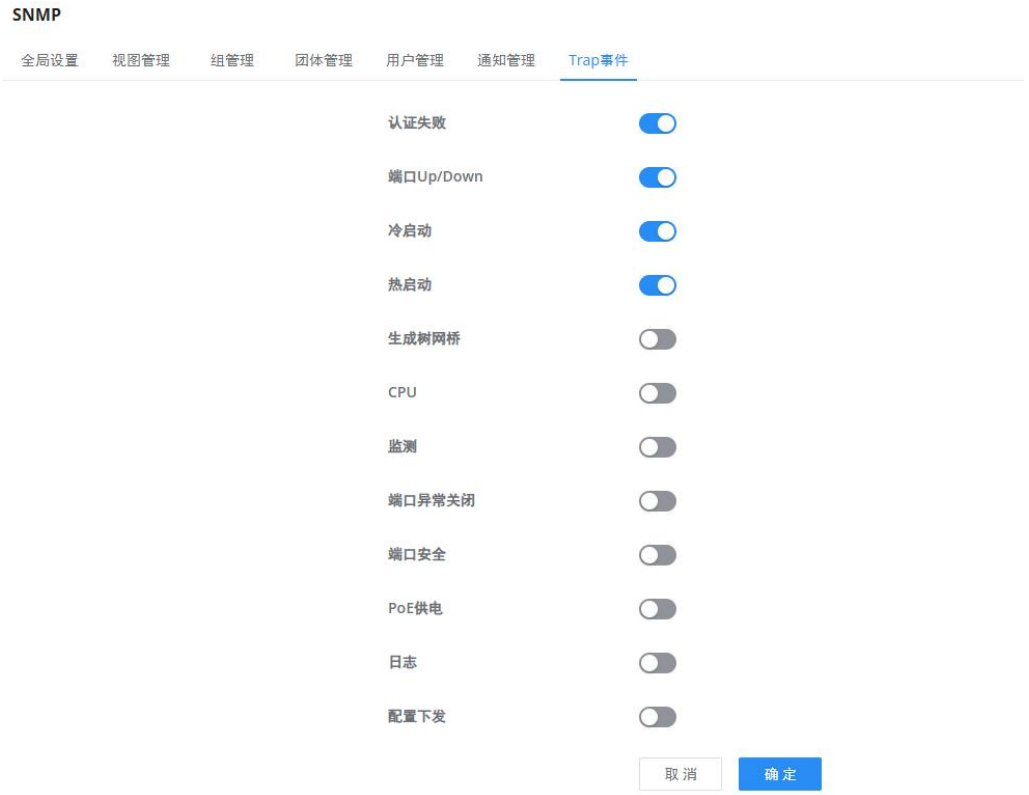


图 184 SNMP-Trap 事件

RMON

基于 SNMP（简单网络管理协议）架构的 RMON（远程监控），用于监控网络。RMON 是目前由互联网工程任务组（IETF）定义的一种常用的网络管理标准，它主要用于监控跨网段甚至整个网络的数据流量，使网络管理员能够及时采取保护措施，避免网络故障。此外，RMON MIB 定期记录网络性能和故障的网络统计信息，管理站可以根据这些信息随时有效地监控网络。RMON 有助于网络管理员管理大规模网络，因为它减少了管理站和被管理代理之间的通信流量。

注意：

- 要使用 RMON 功能，必须先开启 **SNMP→全局设置→SNMP** 开关。

RMON 统计组

以太网统计功能（对应于 RMON MIB 中的统计组）：系统统计被监控的每个网络的基本统计信息。系统将持续统计某一网段的流量和各种类型包的分布，或者各种类型的错误帧数、碰撞次数等，统计对象包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接

收报文数等。

图 185 RMON-统计组

RMON 历史组

历史统计功能（对应 RMON MIB 中的历史组）：系统定期采样收集网络状态统计信息并存储，以便后续的处理。系统将按周期定时对各种流量信息进行统计，统计数据包括带宽利用率、错误包数和总包数等。

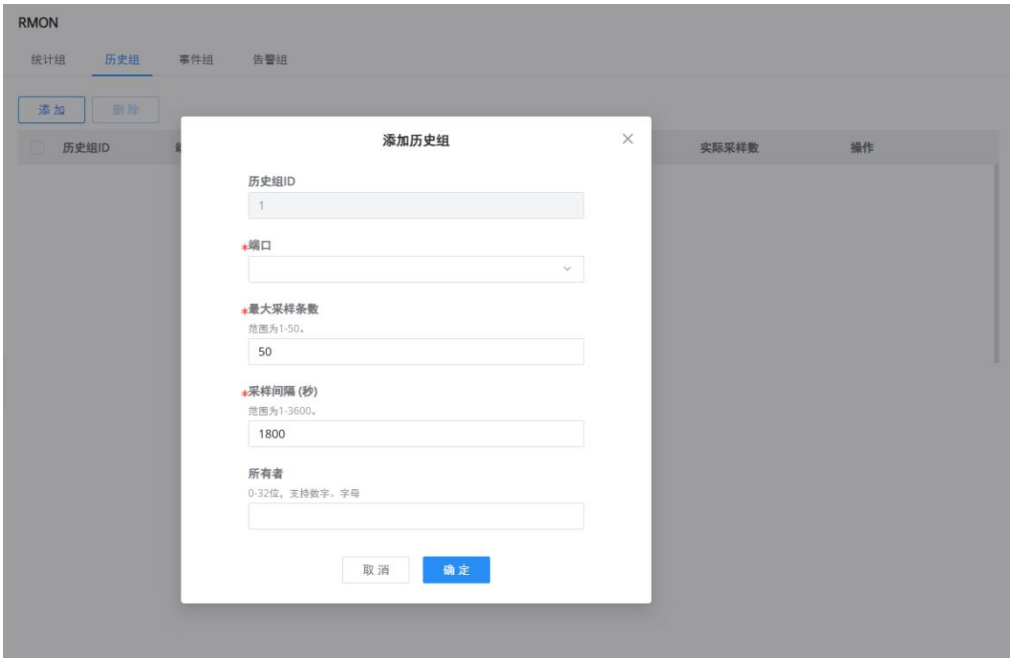


图 186 RMON-历史组

RMON 事件组

事件定义功能（对应 RMON MIB 中的事件组）：事件组控制从设备来的事件和提示，提供关于 RMON Agent

所产生的所有事件。当某事件发生时，可以记录日志或发送 Trap 到网管站。

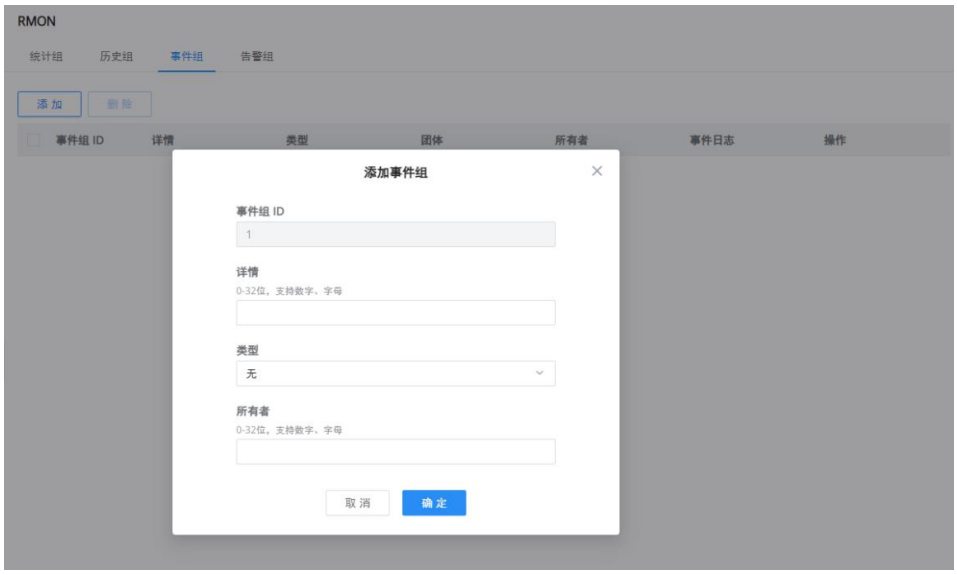


图 187 RMON-事件组

RMON 告警组

设置告警阈值功能（对应 RMON MIB 中的告警组）：系统针对指定的告警变量（任意告警对象对应的 OID）进行监控。在用于预先定义指定告警的一组阈值和采样时间后，系统会按照定义的时间周期去获取指定告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件。RMON Agent 会将上述监控到的状态记录为日志或者把 Trap 发往网管站。

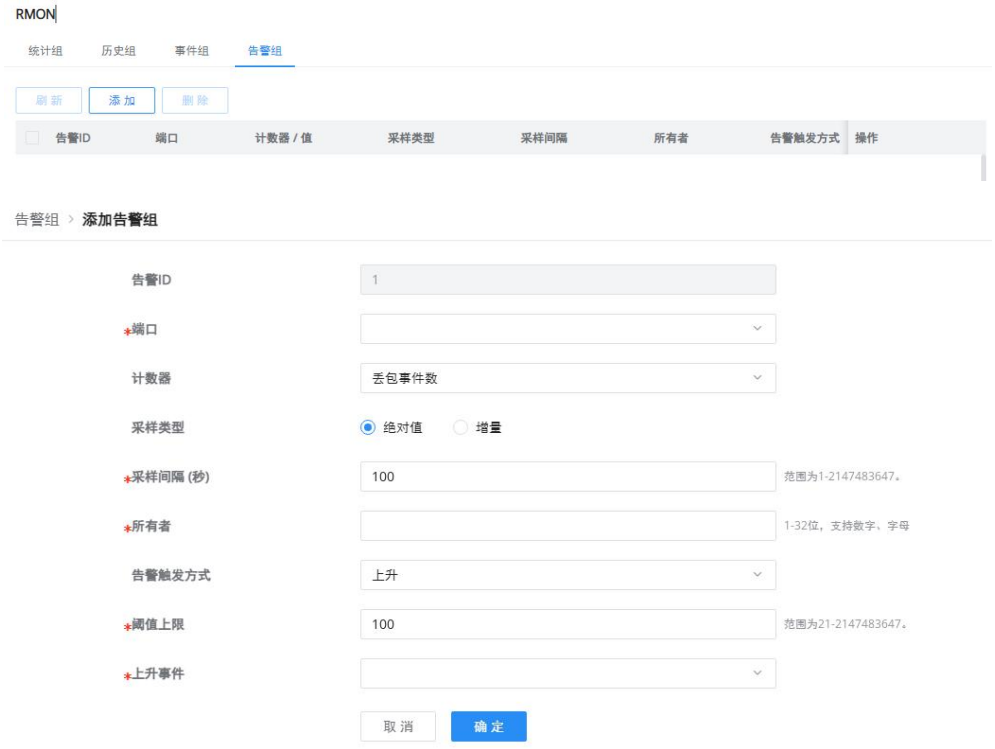


图 188 RMON-告警组

LLDP/LLDP-MED

LLDP/LLDP-MED 是一种单向协议，没有请求/响应序列。信息由施行传输功能的站通告，并由实现接收功能的站接收和处理。

LLDP MED 是 LLDP 的增强功能，提供其他功能以支持介质设备。LLDP MED 具备功能有：实现实时应用（如语音和/或视频）的网络策略通告和发现；发现设备位置以让用户创建位置数据库，对于 IP 电话（VoIP）和紧急电话服务（911），则使用 IP Phone 电话位置信息；获取设备资产清单，了解设备相关信息；获取设备 PoE/PSE 供电情况信息。

LLDP 全局设置

此页面允许用户设置 LLDP 的常规设置，包括启用 LLDP 和其他参数。

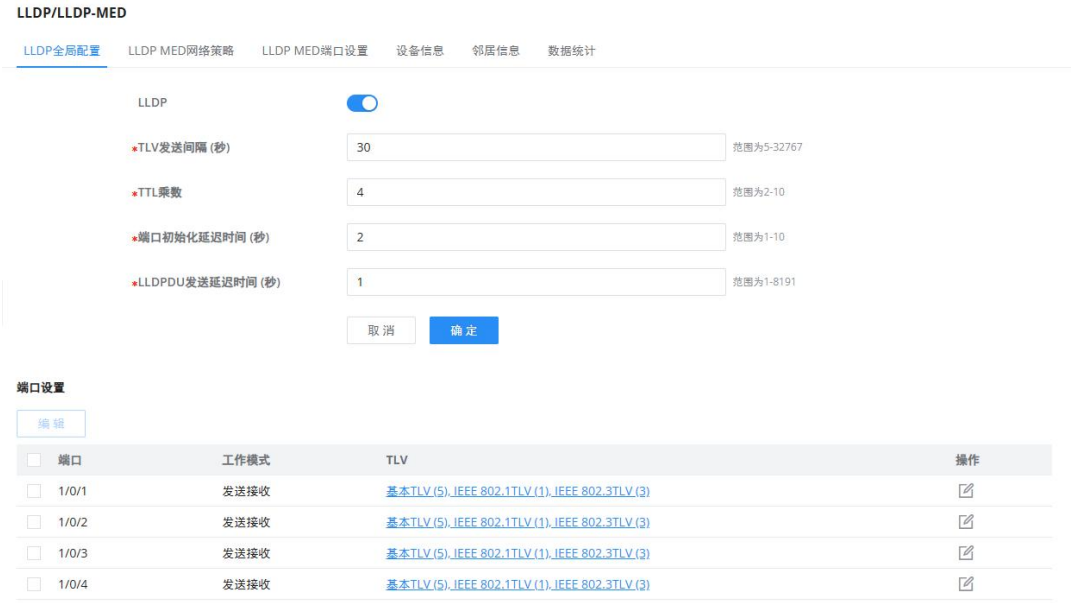


图 189 LLDP 全局设置

每个端口可以调整更多配置。

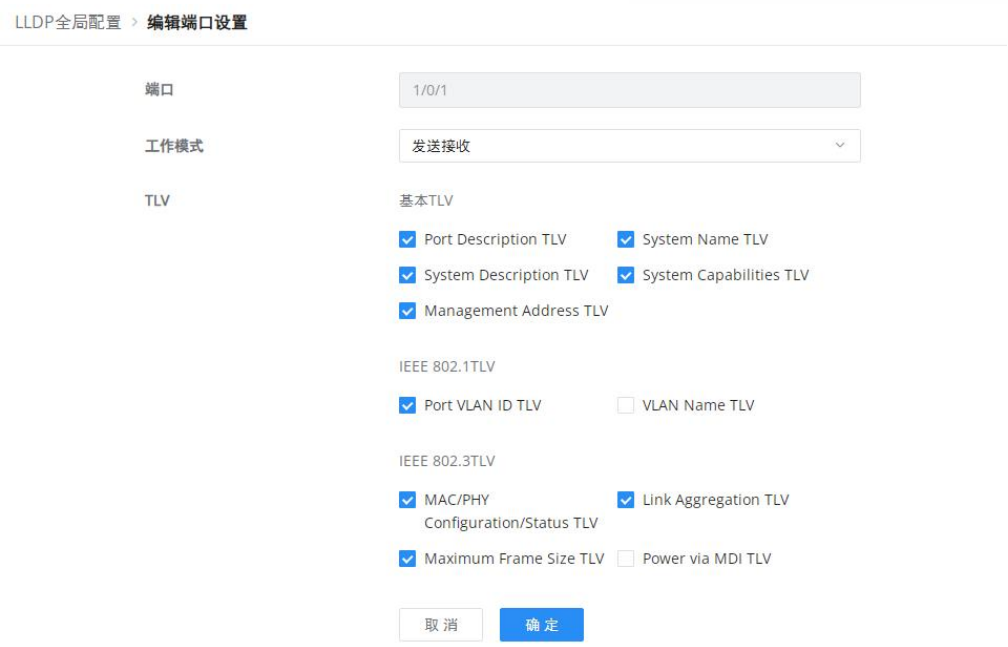


图 190 LLDP 端口设置

LLDP MED 网络策略

此页面允许网络管理员设置 MED（媒体终端发现）网络策略。单击“添加”按钮添加网络策略。
“自动语音网络策略”开启，无需手动添加应用为“语音”的网络策略，将会自动根据协商结果自动创建。

图 191 LLDP MED 网络策略

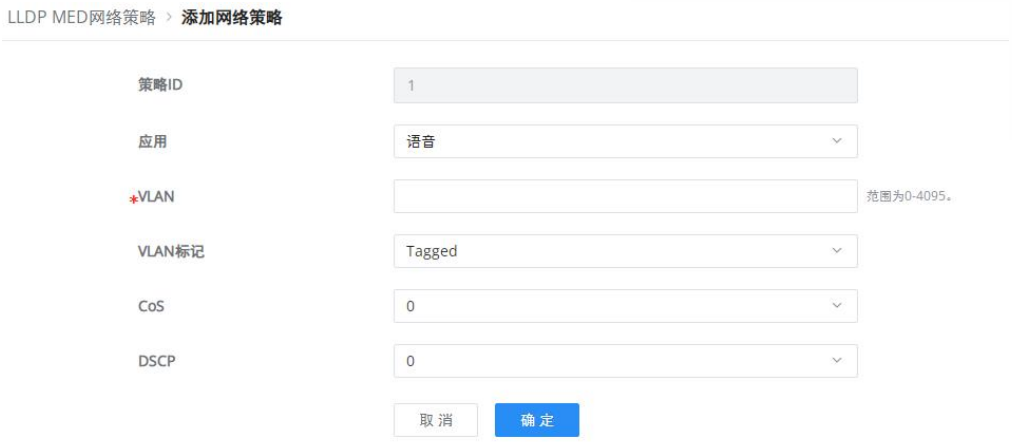


图 192 LLDP MED 网络策略-添加网络策略

LLDP MED 端口设置

用户可以在此页面中为每个端口配置 LLDP MED。

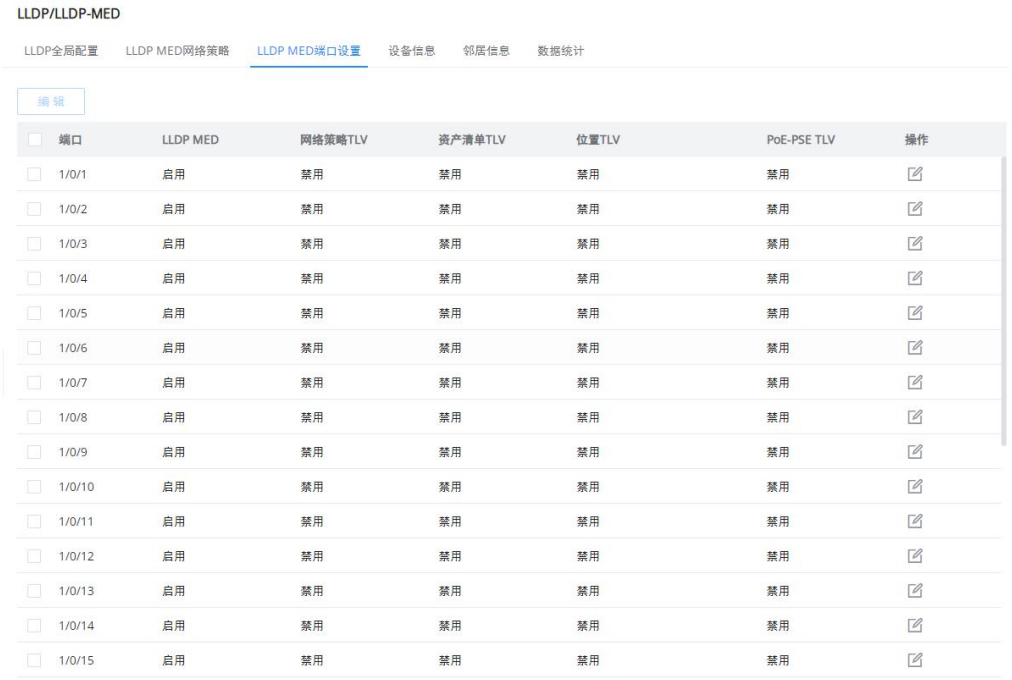


图 193 LLDP MED 端口设置

LLDP 设备信息

此页面显示连接到每个端口的 LLDP 本地设备的信息。单击该端口可查看有关该端口的相关 LLDP 信息。

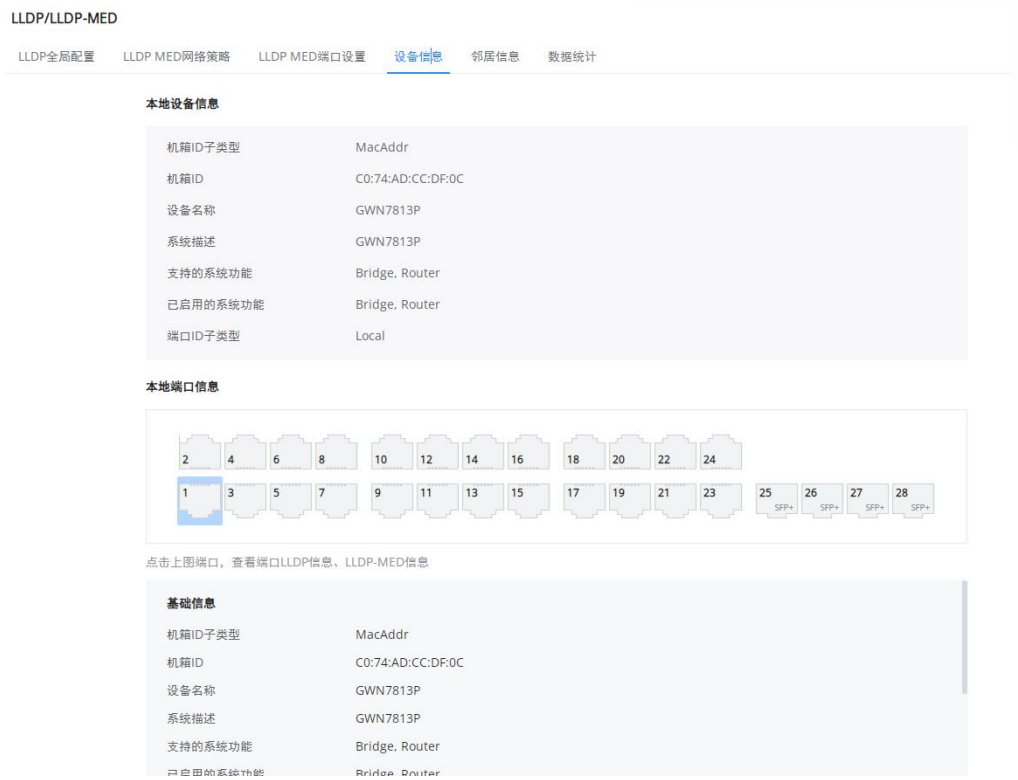


图 194 LLDP 设备信息

邻居信息

此页面列出了在交换机端口上获得的邻居。单击“刷新”按钮更新列表。

图 195 LLDP 邻居信息

图 196 邻居信息-详情

LLDP 数据统计

通过此功能查看本地设备的 LLDP 统计信息。单击“刷新”以更新列表。

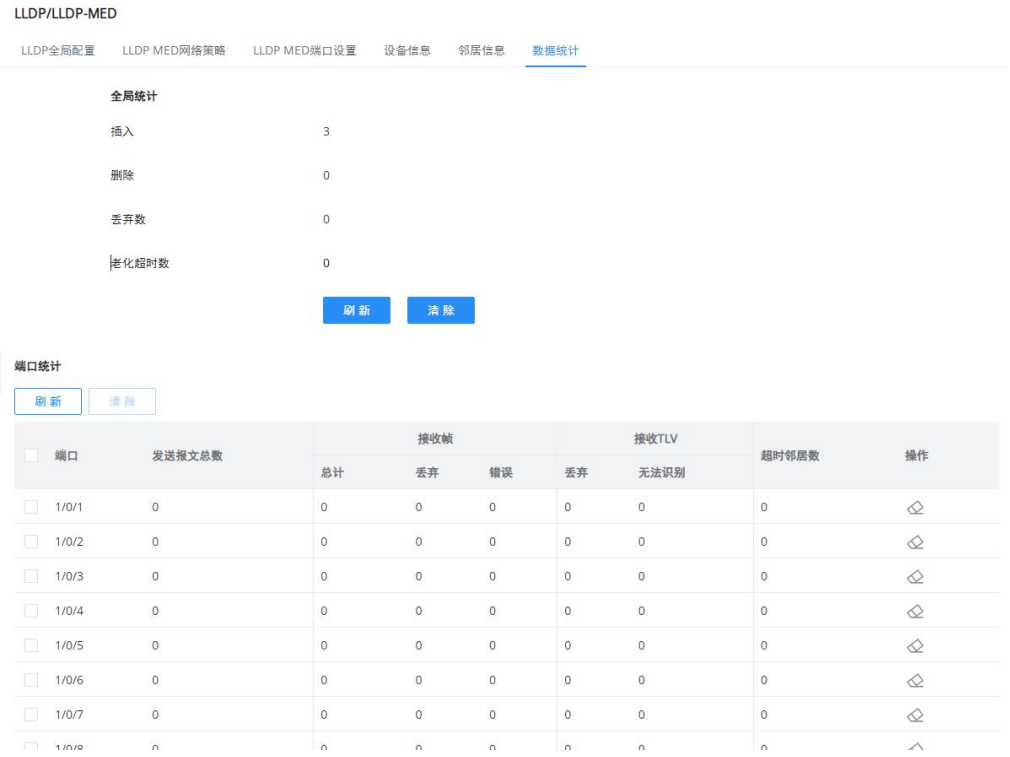


图 197 LLDP 数据统计

节能管理

节能以太网 EEE：一种根据网络流量动态调节电接口功率的节能方法。没有配置电接口的功率自调节功能时，系统以一定的功率为每个接口供电，即使接口处于业务空闲状态，也需要消耗同样的能量。配置电接口的功率自调节功能后，当接口处于业务空闲状态时，系统将会自动降低给该接口的供电，这样能够节省系统的总体能耗；当接口开始正常传输数据时，则恢复正常供电。

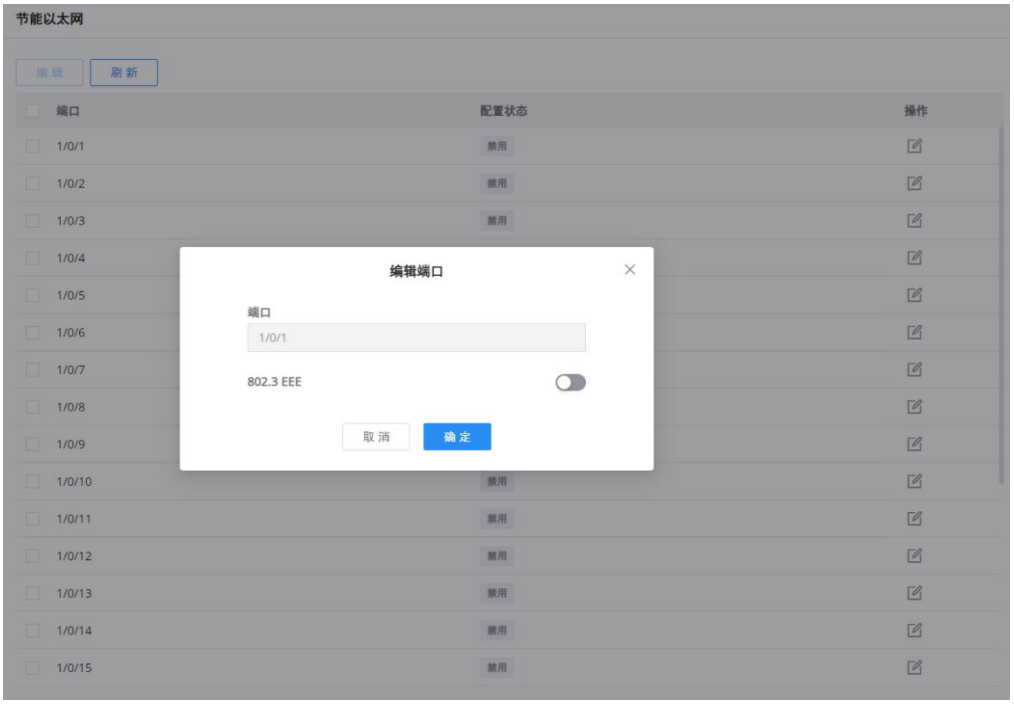


图 198 节能管理

告警

告警功能允许管理员为不同类型的事件设置告警，包括 CPU 使用率、内存使用率、PoE 功率、MAC 地址超出限制、温度、风扇故障、PoE 芯片故障等。

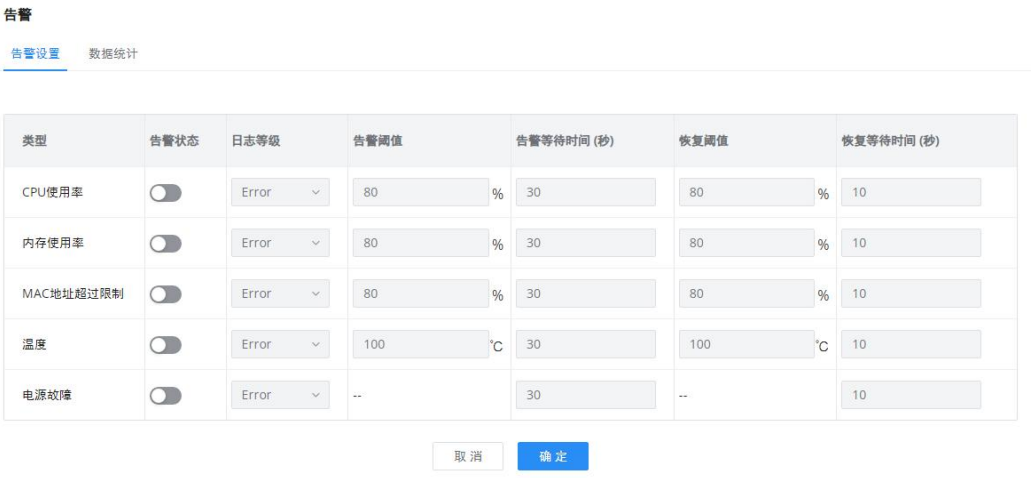


图 199 告警

数据统计

数据统计显示不同告警类型的当前状态，除了一些其他信息外，它还显示服务的上次警报时间和上次恢复时间。

图 200 告警-数据统计

系统

基础设置

基本设置页面分为三类：

- 基本信息：用户可以指定 GWN780x Pro 交换机的名称、系统位置和系统联系人。
- 时间设置：用户可以手动配置时间，也可以使用 NTP 服务器配置时间，也可以配置夏令时。
- 定时重启：用户可以通过在时间策略下添加定时重启策略来设置定时重启。

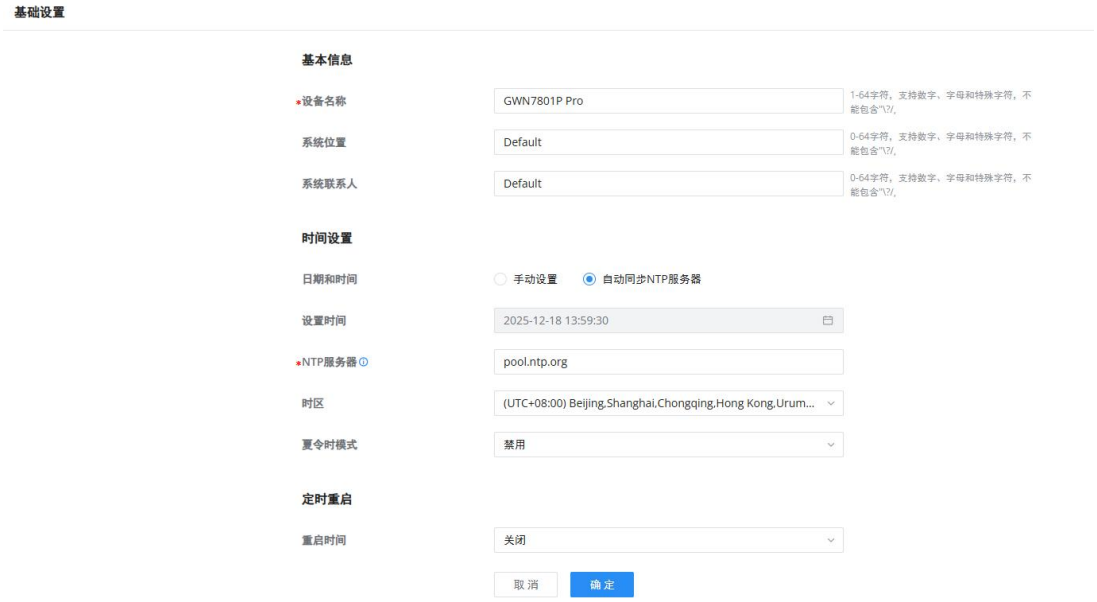


图 201 基础设置

访问控制

在访问控制上，用户可以在网页自动锁定之前指定 Web 闲置超时时间、启用 Telnet 或 SSH、SSh 远程访问、管理平台设置和管理 ACL。

Web 服务管理

用户可以配置以下内容：

- Web 闲置超时时间（分钟）：GWN780x Pro Web UI 无任何操作的自动退出登录时间，有效范围为 1-1440 的整数。
- Telnet：设置启用通过 Telnet 方式访问交换机，默认情况下是禁用的。
- SSH：设置通过 SSH 方式访问交换机，默认开启。默认端口为 22，必要时可以更改（建议保持 22）。

图 202 访问控制-Web 服务管理

注意：

VTY 会话允许通过命令行界面远程管理网络设备。GWN780x Pro 交换机现在支持多达 12 个同步 VTY 会话，为管理员提供并发 SSH 或 Telnet 访问。

SSH 远程访问

注意：

此功能专供我们的开发人员和支持工程师进行故障排除。当任何一方请求远程访问时，请输入当前用户的密码以授予访问设备的权限。

图 203 访问控制-SSH 远程访问

输入密码，然后单击“SSH 远程访问”按钮，它将在 48 小时内自动禁用。

图 204 访问控制-停止 SSH 远程访问

管理平台设置

允许用户配置 GWN Manager 或 GWN 路由器的参数（服务器地址和端口）。也可以允许 DHCP 选项 43，如果启用，则首选 DHCP 选项 43 分配的服务器地址。

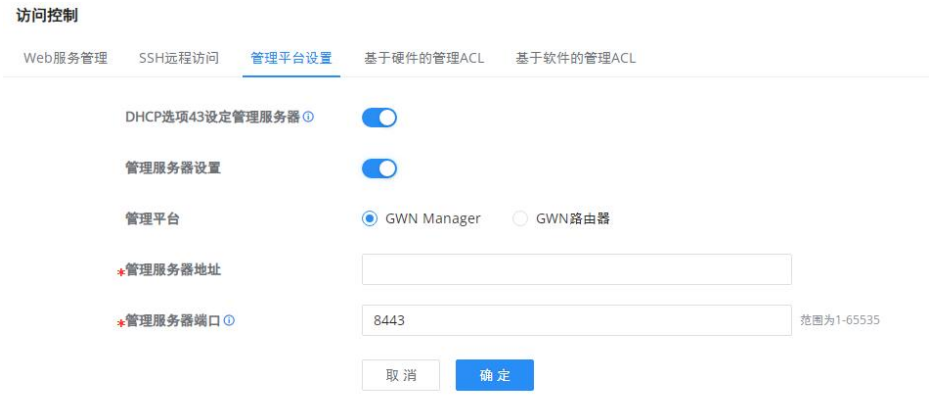


图 205 访问控制-管理平台设置

注意：

当 GWN Manager 想要接管托管交换机时，它可以通过输入交换机当前密码来强制接管。

基于硬件的管理 ACL

在 GWN780x Pro 交换机上，硬件管理访问控制列表（ACL）旨在通过在流量到达 CPU 之前直接在硬件级别过滤流量来优化资源效率。此预处理步骤可确保仅转发与定义的安全规则匹配的流量以进行进一步处理，从而有效减少不必要的 CPU 负载并提高整体性能。通过将初始流量验证卸载到交换机硬件，GWN780x Pro 提高了网络效率和安全性。

图 206 访问控制-基于硬件的管理 ACL

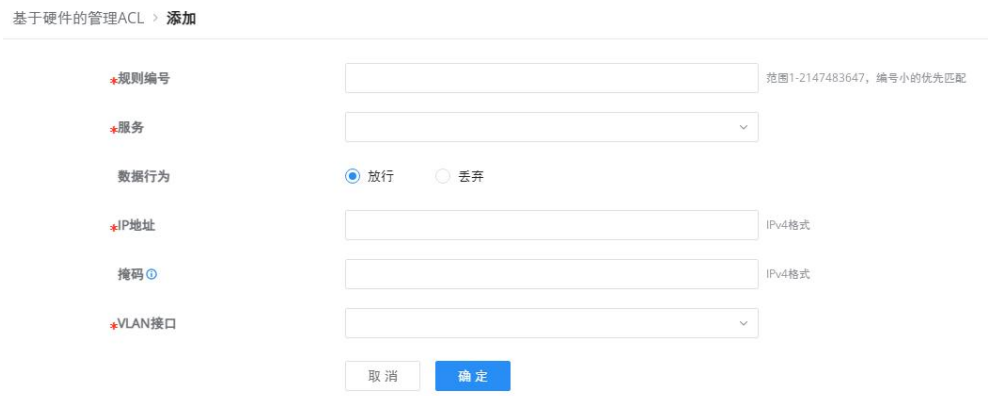


图 207 访问控制-添加基于硬件的管理 ACL

基于软件的管理 ACL

在 GWN780x Pro 交换机上，基于软件的管理 ACL 使用类似防火墙的规则来控制谁可以访问网络及其管理功能。这意味着它会设置限制以确保只有授权用户和设备才能访问交换机的重要部分，从而有助于保持网络安全和管理良好。

图 208 访问控制-基于软件的管理 ACL

用户管理

设备有三个级别的用户，即管理员、Operator 和 Monitor。管理员根据管理需要对登录交换机的用户进行身份验证和授权，每个用户都有不同的权限和密码。

管理员

- 每个设备只有一个管理员。
- 管理员拥有最高权限，可以执行任何命令。
- 用户名 admin 不能更改，只能更改密码。
- 支持添加、删除 Operator 和 Monitor。

Operator

- 由管理员添加，可以有多个账号作为 Operator。
- 拥有第二高权限，可以执行除管理员的关键操作和重要的强制命令外的所有命令，不支持恢复出厂
- 无法更改用户名，只能更改密码。
- 支持添加、删除 Monitor 用户。

Monitor

在管理员或 Operator 的许可下，可以拥有多个 Monitor。

- 最低权限，只能查看交换机状态和统计信息，没有任何执行和配置权限。
- 无法更改用户名，只能更改密码。

单击“**添加**”按钮添加新用户，然后指定用户级别和密码（Operator 或 Monitor）。

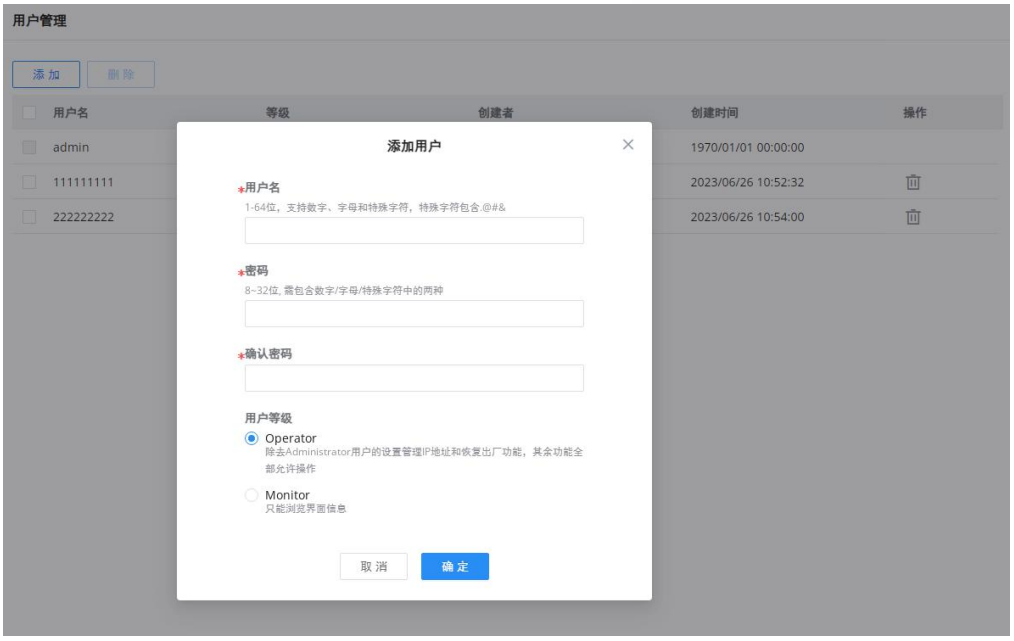


图 209 用户管理

时间策略

时间策略用于创建时间计划，例如 Office 工作时间、升级计划和重启计划等。

图 210 时间策略

注意：

- 如果在同一天同时配置周期计划和特殊计划，则只有特殊计划生效。
- 如果在特殊日期没有选择时间短，则不会执行相应日期的功能。