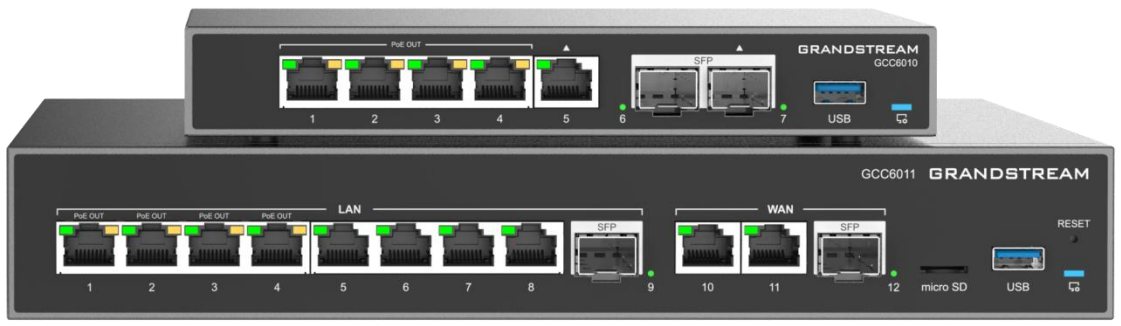
深圳市潮流网络技术有限公司

GCC6010|GCC6011|GCC601W

企业级超融合有线/无线网关

网络-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

注意

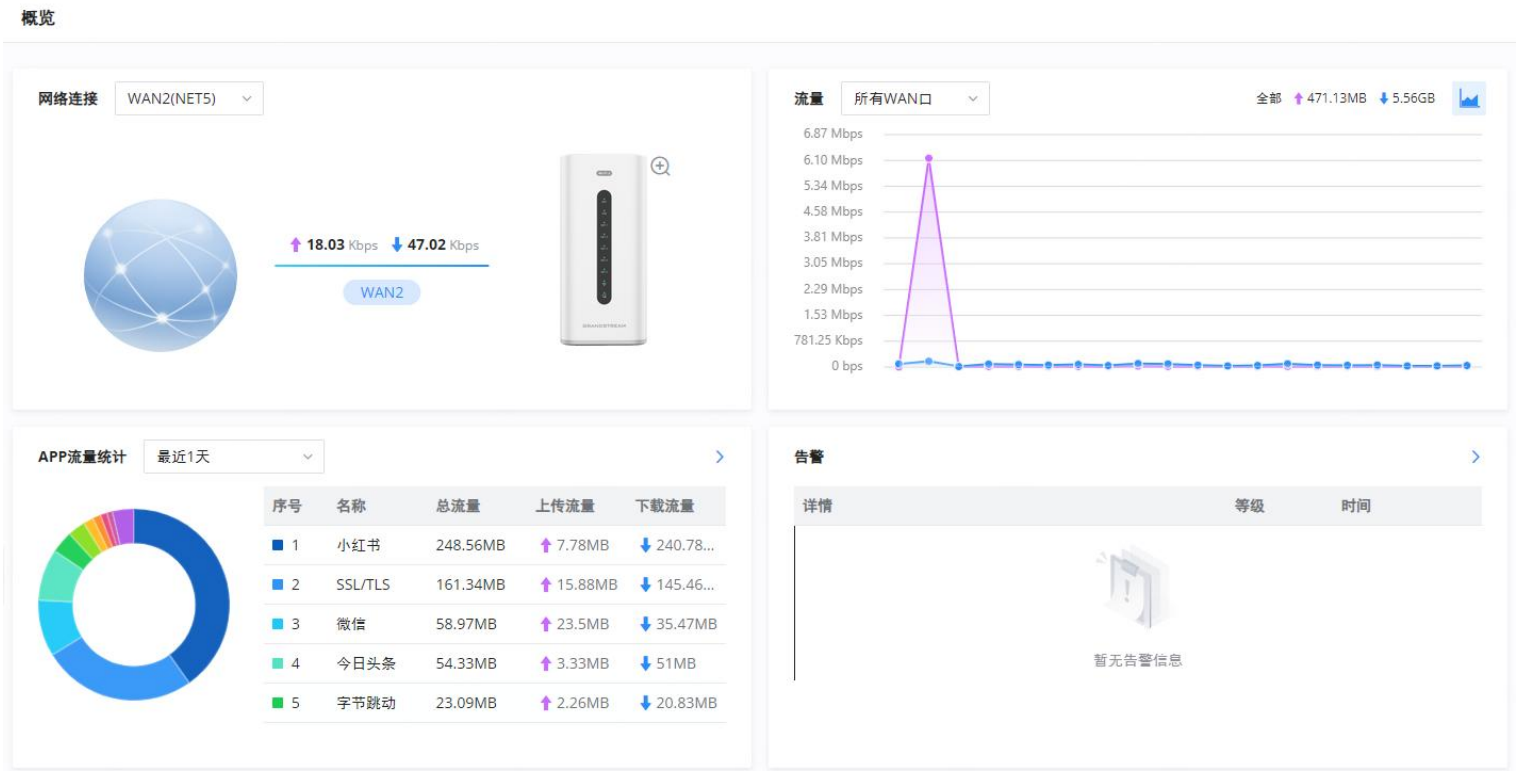
由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

在本指南中，我们将介绍GCC601X(W)网络模块的配置参数。

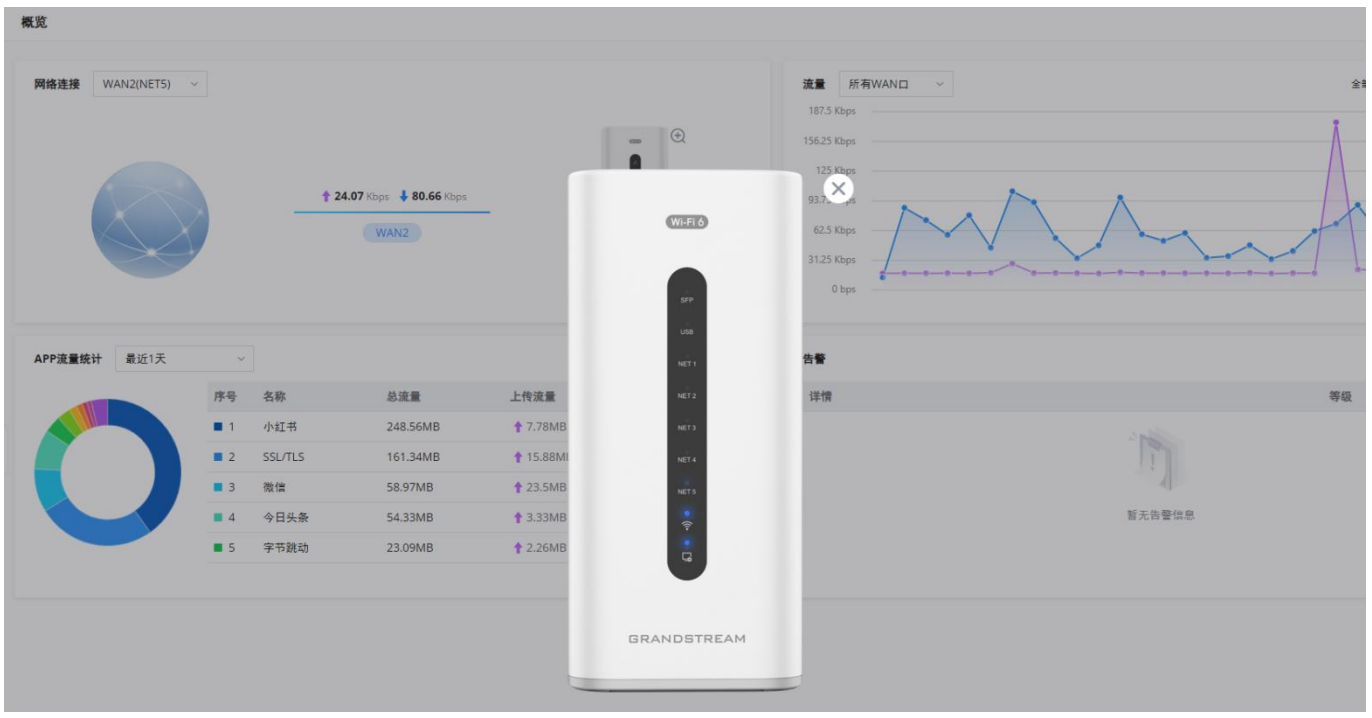
概览

概览页面以仪表板样式提供了GCC601X（W）信息的总体视图，以便于监控。请参考下图：



概览页面

- 在网络流量和应用流量统计下，用户可以将鼠标光标悬停在图表上以显示更多详细信息。
- 在网络连接下，用户可以点击“缩放图标”来显示一个带有实时LED指示灯的虚拟GCC设备。



概览页面→虚拟GCC设备

网络连接	显示所选WAN端口的网络连接的当前状态，并显示当前上传和下载速度。 *注意：用户可以从下拉列表中选择WAN端口。*
网络流量	实时显示网络流量。 *注意：用户可以从下拉列表中选择WAN端口或选择所有WAN端口。*
告警	显示带有详细信息和时间的一般、重要或紧急告警。
应用程序流量统计	显示基于应用程序使用情况的流量统计数据。

概览页面

端口信息

端口信息页面显示所有端口状态的概览，包括USB端口、千兆端口和SFP端口，以绿色表示向上的链接，以灰色表示向下的链接，此外，用户可以单击端口图标获取有关选择链接的更多信息，请参考下图：

导航至概览→端口信息：

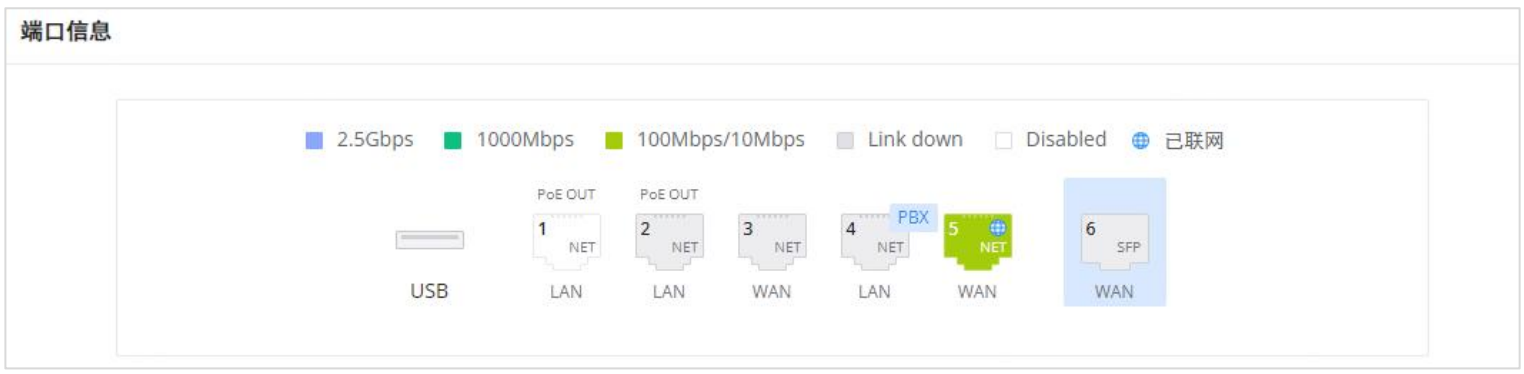
GCC6010W的端口信息

网络设置

端口配置

要访问端口配置，请访问GCC601X(W)的用户界面，然后导航到网络设置→端口配置。

- 端口状态：在顶部，您可以找到所有端口的状态。
- 紫色：端口速度为2.5 Gbps（仅适用于SFP端口和2.5 Gbps SFP模块）。
- 绿色：端口速度为1Gbps。
- 浅绿色：端口速度为100Mbps/10Mbps。
- 灰色：向下链接。
- 白色：端口禁用。
- Internet图标：连接到Internet的端口（对于WAN端口）。



端口配置-第1部分

- **端口配置**

端口配置页面允许用户配置与所有端口相关的设置；这包括千兆以太网端口和SFP端口。可以编辑的设置包括流量控制、速度和双工模式。

> **注：**
>
> - SFP端口支持2.5 G SFP模块
> - SFP端口不支持2.5 G自动协商
> - 当选择半双工模式时，流量控制不生效
> - 禁用物理端口时，所有基于端口的配置都不会生效。

端口配置-第2部分

端口	此字段指示端口号。
端口已启用	打开或关闭端口。 *注意：当设置为禁用时，此物理端口将被禁用，所有基于端口的配置都不会效果。*
端口类型	此字段指示端口类型。 ● GE：代表千兆以太网 ● SFP：小型可插拔光口
名称	指端口名称。
角色	指端口角色。 ● LAN ● WAN
速度/双工	在此设置中，用户可以配置双工*模式以及*端口速度。端口的双工设置可以设置为：半双工和全双工。 当模式设置为自动协商时，GCC设备将根据与连接的设备协商的设置进行确定。
流量控制	用户可以使用此选项启用或禁用流量控制。 *注意：当设置设置为自动协商时，GCC设备将根据与连接的设备协商的设置进行确定。*

端口配置。第2部分

- **PoE配置**

用户还可以控制GCC601X(W)的每个PoE端口上的功率限制。

端口配置-PoE配置

端口	此字段指端口号。
供电方式	此选项配置电源模式。 ● 有源PoE(802.3 af/at) ● 关闭
最大供电	配置所提供的最大功率。 注：如果供电模式为主动PoE（802.3 af/at）或48V被动PoE，请确保提供给所有端口的最大功率之和小于总功率限制。
供电优先级	根据电源指定端口的优先级。 ● 最高 ● 高 ● 中 ● 低 设置相同优先级时，供电规则如下： ①端口都接入PD设备的情况下，若功率有限。将以端口序号顺序为标准，标识小的保障优先供电。 ②部分端口接入，将优先保障已接入端口优先供电。

端口配置-PoE配置

WAN

WAN端口可以连接到DSL调制解调器或路由器。WAN端口支持还设置静态IPv4/IPv6地址并配置PPPoE。

在此页面上，用户可以修改每个WAN端口的设置，也可以删除甚至添加另一个WAN，添加一个WAN端口将减少LAN端口的数量。在存在多个WAN端口的情况下，可以在多个WAN端口之间配置负载均衡或备份（故障转移）。

WAN页面

点击 添加 添加另一个WAN端口或单击“编辑图标”编辑以前创建的端口。

添加或编辑WAN

WAN端口的网络配置参数请参考下表。

基本信息	
状态	单击以启用或禁用WAN
WAN名称	输入WAN端口的名称
端口	从下拉列表中选择要用作WAN的端口
IPv4设置	
连接类型	• 自动获取IP（DHCP）：选中后，它将充当DHCP客户端，自动从DHCP服务器获取IPv4地址。 • 手动输入IP（静态IP）：选择后，用户应设置静态IPv4地址、IPv4子网掩码、IPv4网关，并添加额外的IPv4地址，以便与Web界面、SSH或设备上运行的其他服务进行通信。 • 使用PPPoE帐户（PPPoE）访问互联网：选择后，用户应设置PPPoE帐户和密码、PPPoE保持活动间隔和密钥间超时（以秒为单位）。 *默认设置为“自动获取IP(DHCP)”。*
静态DNS	打开或关闭以启用或禁用静态DNS
首选DNS服务器	输入首选DNS服务器，例如：8.8.8.8
备用DNS服务器	输入备用DNS服务器，例如：1.1.1.1
最大传输单位(MTU)	配置WAN端口上允许的最大传输单元。 • 当使用以太网时，用户可以设置的有效范围是576-1500字节。默认值为1500。除非万不得已，请不要更改默认值。 • 使用PPPoE时，用户可以设置的有效范围是576-1492字节。默认值为1492。除非万不得已，请不要更改默认值。
跟踪IP地址1	配置跟踪WAN端口的IP地址，判断WAN端口网络是否正常。

跟踪IP地址2	添加另一个备用地址以跟踪IP地址
VLAN标记	打开或关闭以启用或禁用VLAN标记
VLAN标签ID	输入具有优先级的VLAN标记ID *注：优先级为0~7，7为最高优先级。默认值为0。*
多公网IP地址	打开或关闭以启用或禁用公网IP地址 *注意：请使用端口转发功能，以便您可以通过公共IP地址访问GCC。*
公用IP地址	输入公共IP地址 *注意：点击“加号”或“减号”图标添加或删除公共IP地址。*
VPN	打开或关闭以启用或禁用VPN
VPN连接类型	• L2TP：第二层隧道协议（L2TP）是点对点隧道协议（PPTP）的扩展，互联网服务提供商（ISP）用于支持虚拟专用网络（VPN）。 • PPTP：点对点隧道协议（PPTP）是一种网络协议，它通过在基于TCP/IP的数据网络上创建虚拟专用网络（VPN），实现从远程客户端到专用企业服务器的数据安全传输。
用户名	输入用户名以验证VPN服务器。
密码	输入密码以验证VPN服务器。
服务器地址	输入VPN服务器的IP地址或FQDN。
MPEE加密（如果选择PPTP）	当选择PPTP作为VPN连接类型时，用户可以选择打开或关闭MPEE加密。
IP类型	• 动态IP：IP将使用DHCP静态分配。 • 静态IP：IP将被静态分配。
VPN静态DNS	启用此选项以使用静态分配的DNS服务器地址。
最大传输单位(MTU)	这配置了最大发射单元的值。此值的有效范围为576-1460。默认值为1430。 *注意：除非必要，否则请不要更改此值。*
IPv6设置	
IPv6	启用此选项可在此特定WAN端口上使用IPv6。
连接类型	• 自动获取IP（DHCPv6） • 手动输入IP（静态IPv6） • 使用PPPoE帐户(PPPoE)访问互联网：必须在IPv4上启用和配置。
IPv6地址	当连接类型设置为静态IP时，用户可以在此字段中输入静态IP地址。 注意：仅当连接类型设置为静态IPv6时，此选项才会出现。
前缀长度	输入前缀长度。

	注意：仅当连接类型设置为静态IPv6时，此选项才会出现。
默认网关	输入默认网关的IP地址 注意：仅当连接类型设置为静态IPv6时，此选项才会出现。
首选DNS服务器	输入首选DNS服务器的IP地址。 注意：仅当连接类型设置为静态IPv6时，此选项才会出现。
备用DNS服务器	输入备用DNS服务器的IP地址 注意：仅当连接类型设置为静态IPv6时，此选项才会出现。
静态DNS	启用此选项以输入静态分配的DNS。 注意：仅当连接类型设置为DHCPv6时，此选项才会出现。
IPv6中继到VLAN	启用后，将IPv6地址中继到LAN端的客户端。注意：只有在VLAN上启用了“来自WAN的IPv6中继”，此功能才会生效。

WAN设置

LAN

要访问LAN配置页面，请登录GCC601x(w)WebGUI并转到网络设置→LAN。VLAN配置，如添加VLAN或设置VLAN端口，可以在此页面上找到，以及添加静态IP绑定、本地DNS记录和Bonjour网关的能力。

LAN配置

VLAN

GCC601X（W）集成了VLAN以增强安全性并添加更多功能和特性。VLAN标签可以与SSID一起使用，以将它们与其他SSID分开，用户也可以只在特定的LAN上允许这些VLAN，以实现更多的控制和隔离，它们也可以与策略路由一起使用。

添加或编辑VLAN

要添加或编辑VLAN，请导航到网络设置→LAN。点击“添加”按钮或点击“编辑”图标。

添加或编辑VLAN

VLAN ID	输入VLAN ID ***注意：****VLAN ID范围从3到4094。*
名称	输入VLAN名称
目的地	快速配置VLAN与WAN、其他VLAN和VPN的单向数据通信。默认情况下选择的选项将基于“策略路由”选项，以保持默认路由可访问。
VLAN端口IPv4地址	
IPv4地址	输入IPv4地址
子网掩码	输入子网掩码
DHCP服务器	默认为“Off”，选择“On”指定IPv4地址分配范围
IPv4地址分配范围	输入IPv4地址分配范围的开始和结束。
租期(分钟)	默认值为120，有效范围为60~2880。
DHCP选项	为每个DHCP选项选择选项、类型、服务和内容。单击“加号”或“减号”图标添加或删除条目。 ● 选项：范围为2-254，排除6、50-54、56、58、59、61、82 ● 类型：有三种可能的选项：ASCII、十六进制和IP地址 ● 服务：当选项为43，类型为ASCII字符串时，可以选择服务。 ● 内容：“十六进制字符串”，请输入XX：XX：XX格式或有效的偶数位十六进制字符串。“ASCII字符串”或“十进制”，内容限制为1-255个字符。
首选DNS服务器	输入首选DNS服务器
备用DNS服务器	输入备用DNS服务器
IPv4路由子网	一旦启用，VLAN下的客户端将被允许使用其真实IP地址访问互联网。
接口	从下拉列表中选择WAN接口
VLAN端口IPv6地址	
IPv6地址源	从下拉列表中选择WAN端口
接口ID	打开或关闭接口ID
自定义接口ID	输入接口ID
IPv6首选DNS服务器	输入IPv6首选DNS服务器
IPv6备用DNS服务器	进入IPv6备用DNS服务器
IPv6中继形式WAN	启用后，客户端将直接从WAN端获取IPv6地址。 ***注意：****只有在WAN端启用了“IPv6中继到VLAN”，此功能才会生效。*
	从下拉列表中选择IPv6地址分配

IPv6地址分配	• 禁用 • SLAAC • 无状态DHCPv6 • 有状态DHCPv6

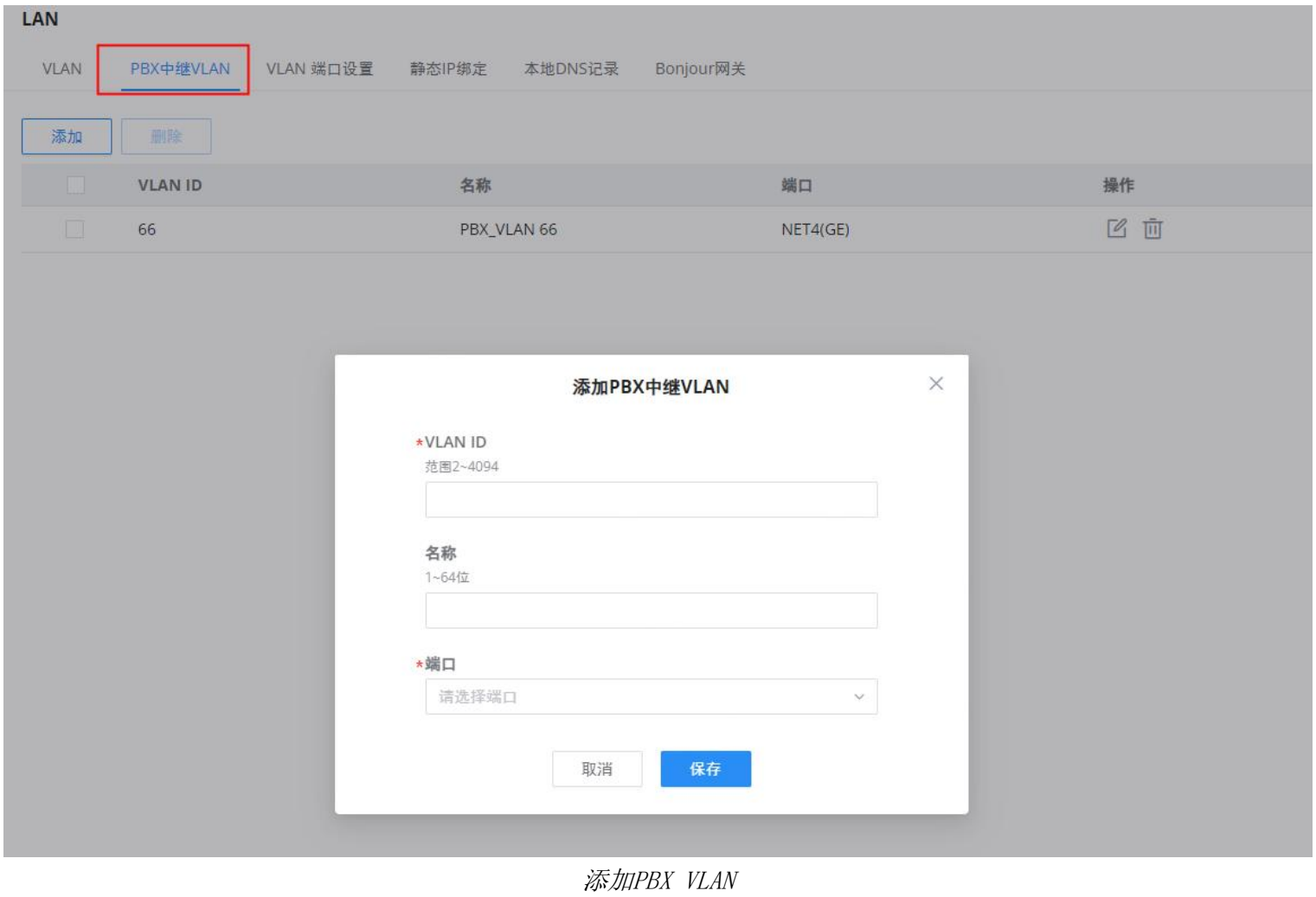
添加/编辑VLAN

PBX中继VLAN

PBX VLAN是在网络上配置以支持PBX系统（SIP中继）的特定VLAN。它是一个专用VLAN，专门用于与PBX相关的流量，出于安全性、性能和管理目的，将其与其他网络流量分开。这种隔离有助于确保来自PBX的语音业务获得必要的服务质量(QoS)，最大限度地减少来自其他网络活动的潜在干扰或拥塞。此外，它可以通过将PBX流量与其他网络流量隔离来增强安全性，从而降低未经授权的访问或窃听的风险。

在ITSP/ISP在同一网络上提供互联网和SIP中继服务的情况下，此功能非常有用。要添加PBX VLAN，请导航到网络模块→网络设置→LAN页面→PBX VLAN选项卡。点击“添加”按钮添加PBX VLAN。

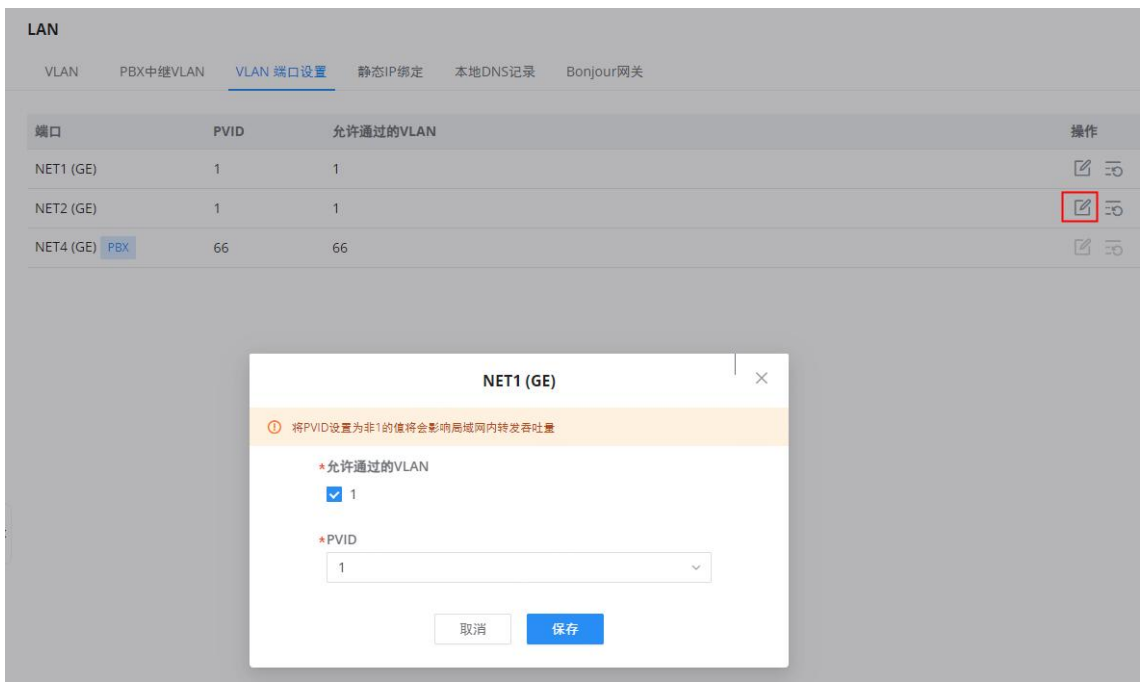
指定VLAN、名称，然后选择端口，如下所示：



添加PBX VLAN

VLAN端口设置

用户可以使用LAN端口仅允许每个LAN端口上的特定VLAN，如果有多个VLAN，则可以选择一个VLAN作为默认VLAN ID（PVID或端口VLAN标识符）。点击编辑VLAN端口设置或单击删除该配置并恢复默认设置，默认为VLAN 1。



VLAN端口

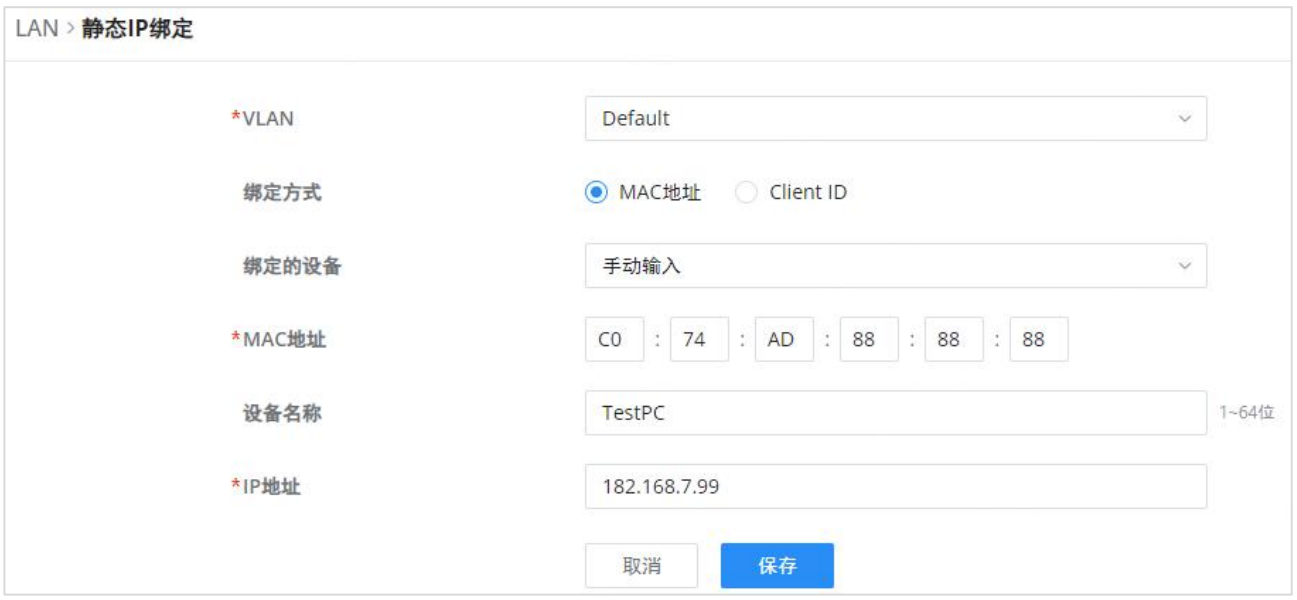
允许的VLAN	选择此端口上允许的VLAN。
PVID	选择端口VLAN标识符或默认VLAN ID

VLAN端口设置

静态IP绑定

用户可以将IP静态绑定设置到IP地址将绑定到MAC地址的设备。GCC接收到的没有相应IP地址和MAC地址组合的任何流量都不会被转发。

要配置静态IP绑定，请导航到网络设置→LAN→静态IP绑定，参考下图和表格：



静态IP绑定

VLAN	从下拉列表中选择VLAN。
绑定方式	使用客户端MAC地址或客户端ID选择绑定模式。
绑定设备	从已连接的设备列表中选择设备MAC地址。 ***注意：****只有可用的绑定模式被设置为MAC地址。*
客户端ID类型	选择客户端ID类型，基于： ● MAC地址 ● ASCII ● 十六进制 ***注意：****只有可用的绑定模式被设置为客户端ID。*
MAC地址	输入MAC地址 ***注意：****只有可用的绑定模式或客户端ID类型被设置为MAC地址*
ASCII	输入ASCII ***注意：****只有可用的客户端ID类型设置为ASCII*
十六进制	请输入XX：XX：XX：XX格式或有效的偶数十六进制数字字符串，前两位数字需要输入类型值。 ***注意：****只有可用的客户端ID类型设置为十六进制*
设备名称	输入设备的名称
IP地址	根据先前选择的VLAN输入静态IP地址。

静态IP绑定

本地DNS记录

本地DNS记录是一项功能，允许用户将DNS记录输入GCC601X（W），可用于将域名映射到IP地址。当用户需要使用域名而不是IP地址访问特定服务器时，当他们不想在公共DNS服务器中包含条目时，可以使用此功能。要添加本地DNS记录，请导航到网络设置→LAN→本地DNS记录，然后单击“添加”。

添加本地DNS记录

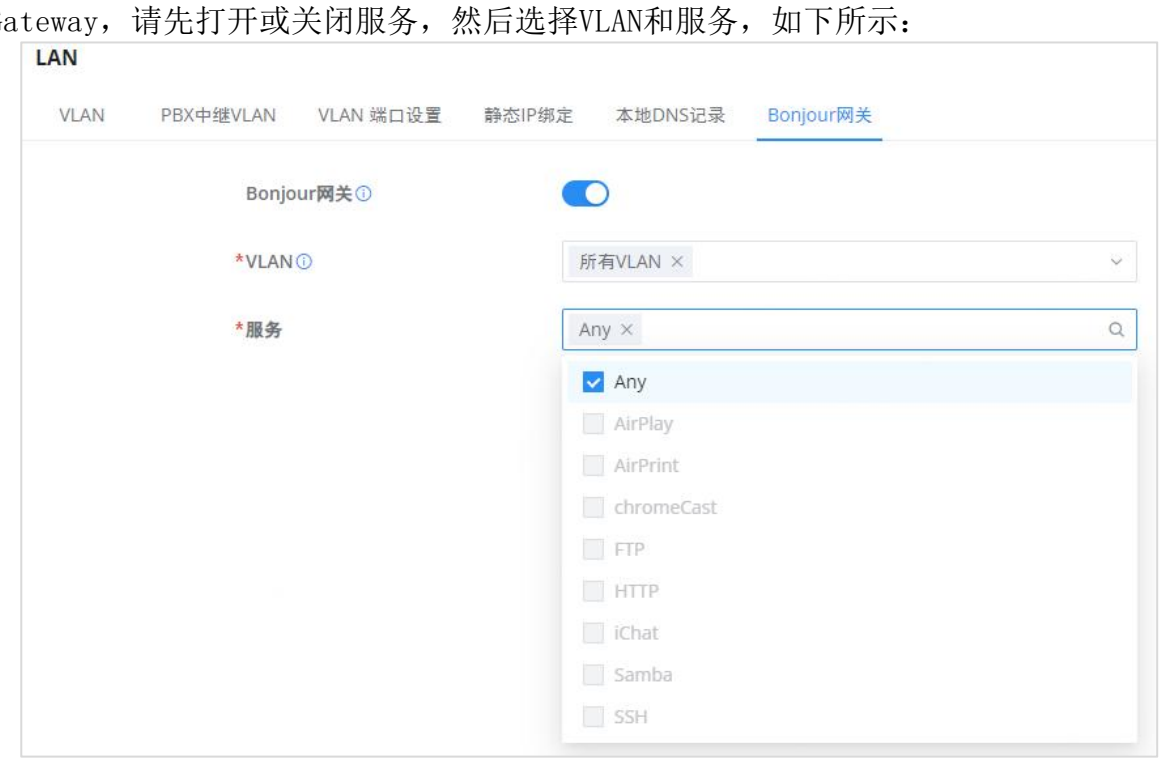
- 在“域名”中输入域名。
- 然后输入域名将映射到的IP地址。
- 打开“状态”以使映射生效。

Bonjour网关

Bonjour服务是一个零配置网络，支持自动发现本地网络上的设备和服务。例如：它可以在本地网络上使用，与Windows®和苹果®设备共享打印机。

一旦启用，Bonjour服务（如Samba）可以提供给多个VLAN下的Bonjour支持客户端。启用后，配置需要互通的VLAN和代理的服务。

要开始使用Bonjour Gateway，请先打开或关闭服务，然后选择VLAN和服务，如下所示：



Bonjour网关

IGMP

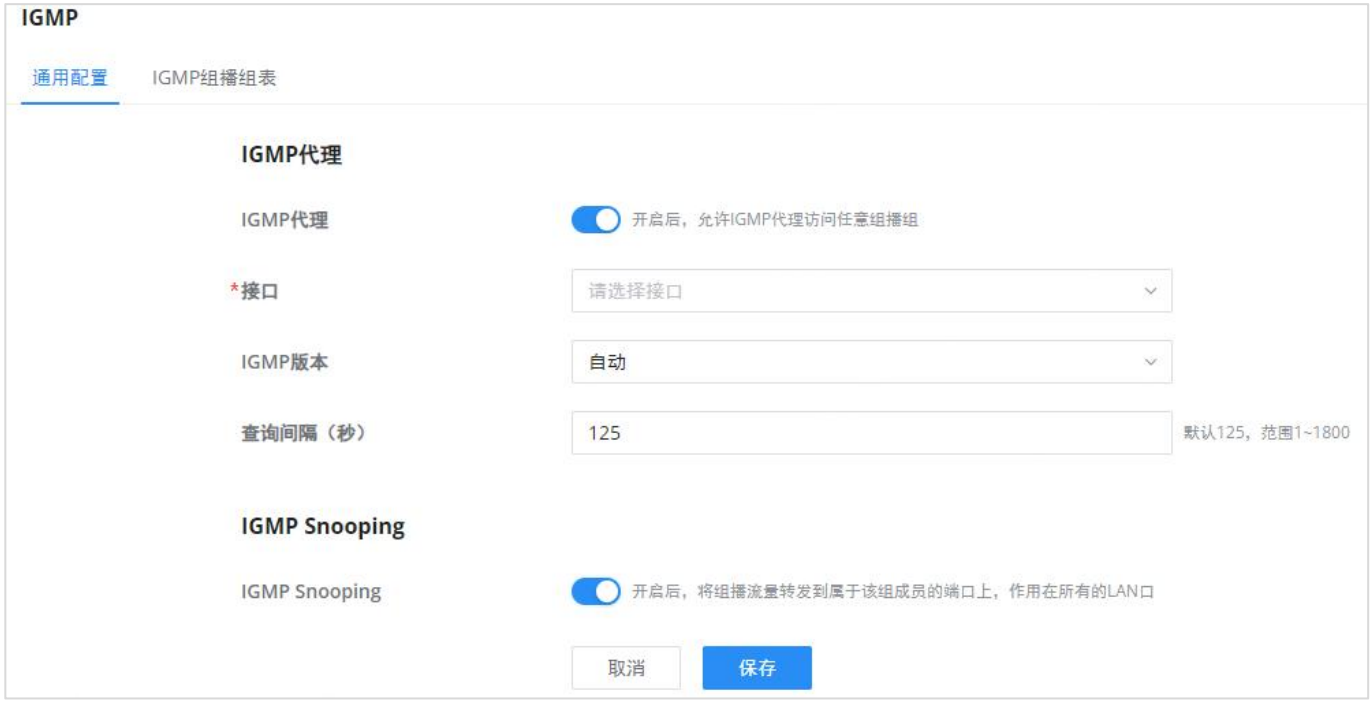
当IGMP代理被启用时，GCC可以代表其背后的客户端发出IGMP消息，那么GCC601X(W)将能够访问任何组播组。

要开始使用IGMP代理，请执行以下操作：

1. 首先打开IGMP代理。
2. 从下拉列表中选择要使用的WAN*接口（注意：无法在启用桥接模*式的WAN端口上启用IGMP代理）

3. 选择版本，默认为自动。

用户还可以启用IGMP监听。一旦启用，多播流量将被转发到属于多播组成员的端口。此配置将应用于所有LAN端口。



IGMP - 通用设置

在IGMP组播组表中，所有活动的组播组都将显示在此处。

IGMP-IGMP组播组表

网络加速

当启用硬件加速时，网络加速允许GCC601X(W)以更高的速率传输数据。这确保了高性能。

网络加速

- 硬件加速：所有网络流量将使用专用硬件加速。一旦启用，QoS、速率限制、流量统计将不会生效。
- 防火墙加速：只有防火墙授权的IDS/IPS和App流量才会使用专用硬件加速。一旦启用，QoS速率限制将不会生效。

VPN

VPN代表“虚拟专用网络”，它在使用公共网络时实时加密数据以建立受保护的网络连接。

VPN允许GCC601X(W)使用PPTP、IPSec、L2TP、OpenVPN®和WireGuard®协议连接到远程VPN服务器，或者配置OpenVPN®服务器并为客户端生成证书和密钥。

GCC601X(W)支持以下VPN功能：

- PPTP：客户端和服务器
- IPSec：站点到站点和客户端到站点（测试版）
- OpenVPN®：客户端和服务器

- L2TP：客户端
- WireGuard®：服务器

可从GCC601X(W)Web GUI→VPN访问VPN页面。

PPTP

基于点对点协议(PPP)并由Microsoft开发的用于WAN(WAN)的数据链路层协议使得网络流量能够被封装并通过不安全的公共网络(例如因特网)路由。点对点隧道协议（PPTP）允许创建虚拟专用网络（VPN），通过互联网隧道传输TCP/IP流量。

PPTP客户端

要在GCC601X(W)上配置PPTP客户端，请导航到VPN→PPTP→PPTP客户端并设置以下内容：

1.点击“添加”按钮。

PPTP页面

将弹出以下窗口：

PPTP客户端配置

名称	输入PPTP客户端的名称。
状态	打开/关闭VPN客户端帐户。
服务器地址	输入远程PPTP服务器的IP/域。

用户名	输入用户名以通过VPN服务器进行身份验证。
密码	输入密码以通过VPN服务器进行身份验证。
MPPE加密	启用/禁用MPPE进行数据加密。 *默认情况下，它是禁用的。*
接口	选择接口。 *注意：自动在防火墙中设置转发规则，允许流量从VPN转发到选定的WAN端口。如果允许远程设备访问，请在防火墙中设置相应的转发规则。*
目的地	选择允许来自VPN的流量到哪个目的组或WAN，这将生成 在“防火墙”→“传输规则”→“转发”菜单下自动设置转发规则。
IP伪装	此功能是网络地址转换(NAT)的一种形式，它允许网络外没有已知地址的内部计算机与外部通信。它允许一台机器代表其他机器。
最大传输单位(MTU)	指GCC发送的数据包的大小。除非必要，请不要更改此值。
远程子网	为VPN配置远程子网。 格式应该是“IP/Mask”，其中IP可以是IPv4或IPv6，Mask是介于1和32。 *示例：192.168.5.0/24*

PPTP客户端配置

PPTP服务器

要添加PPTP服务器，请导航到Web UI→VPN→PPTP页面→PPTP服务器选项卡，然后单击“添加”按钮。

PPTP服务器

名称	输入PPTP服务器的名称。
状态	打开或关闭以启用或禁用PPTP服务器VPN。
服务器本地地址	指定服务器本地地址
客户端起始地址	指定客户端起始IP地址
客户端结束地址	指定客户端结束IP地址
MPPE加密	启用/禁用MPPE进行数据加密。 *默认情况下，它是禁用的。*
接口	从下拉列表中选择确切的接口（WAN端口）。
目的	从下拉列表中选择目的（WAN或VLAN）。 *注意：当选择“全部”时，后续的新接口将自动包含在内。*
LCP Echo间隔（秒）	配置LCP Echo发送间隔。
LCP Echo失败阈值	设置回显传输的最大次数。如果在设置的请求帧内没有应答，PPTP服务器将认为Peer断开连接，连接将被终止。
LCP Echo自适应	● 启用后：只有在自 最后一个LCP回显请求。 ● 一旦禁用：将不检查trac，并根据 LCP Echo间隔
调试	打开/关闭以启用或禁用调试。
最大传输单元（MTU）	指GCC发送的数据包的大小。除非必要，请不要更改此值。默认为1450。
最大接收单元（MRU）	MRU指示接收到的分组的大小。默认为1450。
首选DNS服务器	指定首选DNS服务器。*例如：8.8.8.8*
备用DNS服务器	指定备用DNS服务器。*例：1.1.1.1*

PPTP服务器

创建远程用户凭据

要创建需要在客户端输入并在服务器端进行身份验证的远程用户帐户，请参考远程用户部分。

要查看连接到此服务器的客户端，请单击“客户端列表”图标，如下所示：

连接到此服务器的客户端

IPSec

IPSec或互联网协议安全性主要用于对通过网络层发送的数据包进行身份验证和加密。为实现这一点，它们使用两种安全协议—ESP（封装安全有效载荷）和AH（认证报头），前者提供认证和加密，而后者仅提供数据分组的认证。由于认证和加密两者都是同等期望的，因此大多数实现使用ESP。

IPSec支持两种不同的加密模式，它们是隧道（默认）和传输模式。隧道模式用于加密有效载荷以及IP分组的报头，这被认为更安全。传输模式用于仅加密IP数据包的有效载荷，通常用于网关或主机实现。

IPSec还涉及用于建立安全关联（SA）的IKE（Internet密钥交换）协议。安全关联在两个网络实体之间建立一组共享的安全参数，以提供安全的网络层通信。这些安全参数可以包括加密算法和模式、业务加密密钥以及用于通过连接发送的网络数据的参数。目前，有两个可用的IKE版本-IKEv1和IKEv2。IKE分两个阶段工作：

阶段1：ISAKMP操作将在两个网络实体之间建立安全通道后执行。

阶段2：将在两个网络实体之间协商安全关联。

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

• 主模式：用于在密钥交换期间建立阶段1。它在启动器和接收器之间使用三次双向交换。在第一次交换中，交换算法和散列。在第二交换中，使用Diffie-Hellman交换生成共享密钥。在最后一次交换中，验证彼此的身份。

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

• 快速模式：在使用主模式或主动模式建立安全通道后，快速模式可用于协商一般IPsec安全服务并生成新密钥的材料。它们总是在安全通道下加密，并使用用于认证数据包其余部分的哈希有效载荷。

IPSec站点到站点

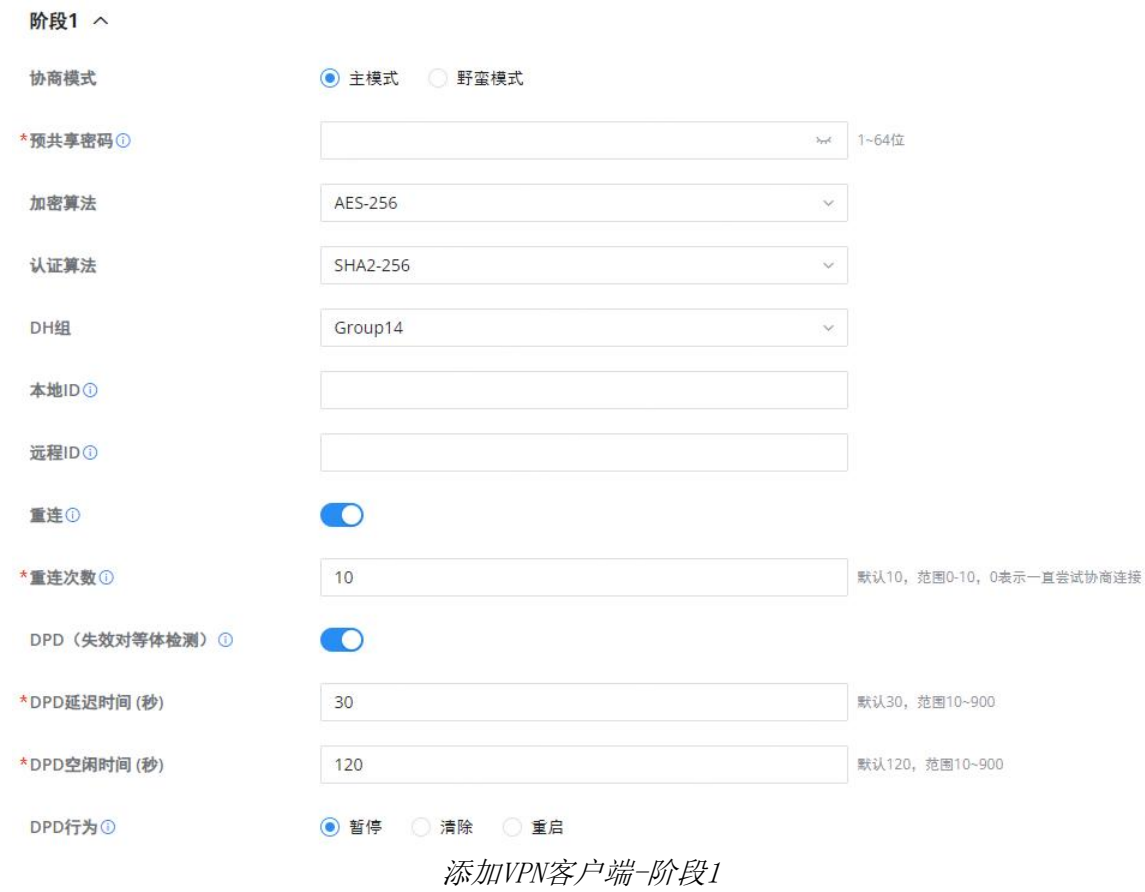
要在位于两个遥远地理位置的两个站点之间构建IPSec安全隧道，我们可以使用以下示例场景：

分支办公室路由器需要通过IPSec隧道连接到总部办公室，每一侧都有一个GCC601X（W）。用户可以如下配置这两款设备：

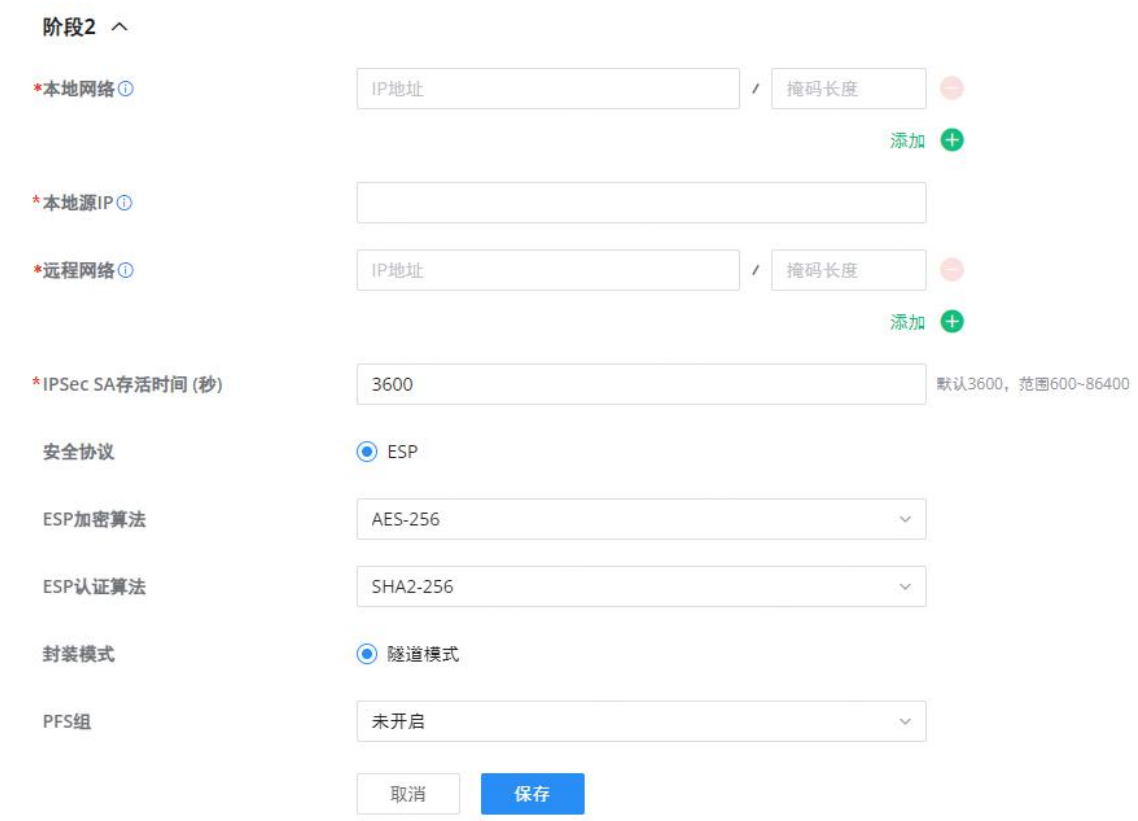
分公司路由器运行LAN子网192.168.1.0/24，总部路由器运行LAN子网192.168.3.0，分公司路由器的公网IP为1.1.1.1，总部路由器的IP为2.2.2.2。

进入VPN→IPSec→站点到站点，然后单击添加VPN客户端。

添加VPN客户端-IPSec



添加VPN客户端-阶段1



添加VPN客户端-阶段2

完成后，按“保存”并对HQ路由器执行相同的操作。这两个路由器将构建隧道和必要的路由信息，以将流量通过隧道路由回来并从分支办公室路由到总部网络。

注：

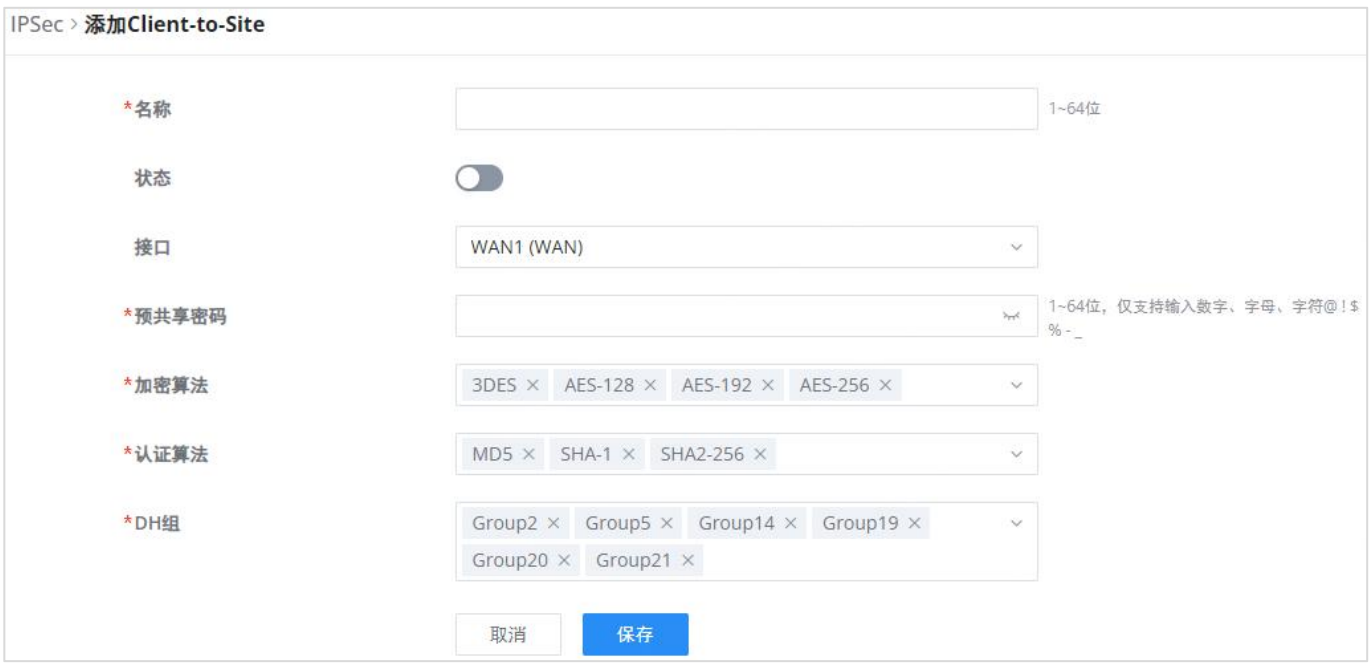
连接建立后，远程子网传入的数据包自动释放，不需要手动配置防火墙从WAN到LAN的转发规则来释放流量。

创建远程用户凭据

要创建需要在客户端输入并在服务器端进行身份验证的远程用户帐户，请参考远程用户部分。

IPSec客户端到站点

转到VPN→IPSec→客户端到站点，然后填写以下信息：



分支机构IPSec配置

OpenVPN®

OpenVPN®客户端

有两种方法可以使用GCC601X(W)作为OpenVPN®客户端：

1. 将从OpenVPN®服务器创建的客户端证书上传到GCC601X(W)。

2. 在GCC601X（W）上创建客户端/服务器证书，并将服务器证书上传到OpenVPN®服务器。转到VPN→OpenVPN®→OpenVPN®客户端并按照以下步骤操作：单击　　按钮。将弹出以下窗口。

OpenVPN®客户端

点击 保存 完成所有字段后。

名称	输入OpenVPN®客户端的名称。
状态	打开/关闭客户端帐户。
协议	指定使用的传输协议。 ● UDP ● TCP 注意：默认协议是UDP。
接口	选择OpenVPN®客户端要使用的WAN端口。
目的地	选择此OpenVPN®客户端将使用的WAN、VLAN和VPN（客户端）目的地。
本地端口	为OpenVPN®配置客户端端口。OpenVPN®客户端和客户端或客户端和服务器之间不应相同。
远程OpenVPN®服务器	配置远程OpenVPN®服务器。同时支持IP地址和域名。
OpenVPN®服务器端口	配置远程OpenVPN®服务器端口
认证模式	选择身份验证模式。 ● SSL ● 用户认证 ● SSL+用户身份验证 ● PSK
加密算法	选择加密算法。支持的加密算法有： ● 的 ● RC2-CBC ● DES-EDE-CBC ● DES-EDE3-CBC ● DESX-CBC ● BF-CBC ● RC2-40-CBC ● CAST5-CBC ● RC2-64-CBC ● AES-128-CBC ● AES-192-CBC ● AES-256-CBC ● 种子-CBC
摘要算法	选择摘要算法。支持的摘要算法有： ● MD5 ● RSA-MD5 ● SHA1 ● RSA-SHA1 ● DSA-SHA1-旧 ● DSA-SHA1 ● RSA-SHA1-2 ● DSA ● RIPEMD160 ● RSA-RIPEMD160 ● MD4 ● RSA-MD4

	• ecdsa-with-SHA1 • RSA-SHA256 • RSA-SHA384 • RSA-SHA512 • RSA-SHA224 • SHA256 • SHA384 • SHA512 • SHA224 • 漩涡
TLS身份认证	启用TLS身份认证方向。
TLS身份认证方向	选择身份认证方向。 • 服务器：在服务器端进行身份认证。 • 客户端：在客户端进行身份认证。 • 两者：双方都进行身份认证。
TLS预共享密钥	输入TLS预共享密钥。
路线	配置路由的IP地址和子网掩码，例如10.10.1.0/24。
拒绝服务器推送路由	如果启用，客户端将忽略服务器推送的路由。
IP伪装	此功能是网络地址转换(NAT)的一种形式，它允许网络外没有已知地址的内部计算机与外部通信。它允许一台机器代表其他机器。
LZO压缩	选择是否激活LZO压缩，如果设置为“自适应”，服务器将使 是否启用此选项的决定。 LZO编码提供了非常高的压缩比和良好的性能。LZO编码特别适用于存储很长字符串的CHAR和VARCHAR列。
允许对方改变IP	允许远程更改IP和/或端口，通常适用于远程IP地址频繁更改的情况。
CA认证	点击“上传”并选择CA证书 注意：这可以在系统设置→证书→CA证书中生成
客户端证书	单击“上传”并选择客户端证书 注意：这可以在系统设置→证书→证书中生成
客户端私钥密码	输入客户端私钥密码。 注意：这可以在VPN→远程用户中配置

OpenVPN®客户端

OpenVPN®服务器

要将GCC601X(W)用作OpenVPN®服务器，您需要开始创建OpenVPN®证书和远程用户。要创建新的VPN服务器，请导航到Web UI →VPN→OpenVPN®页面→OpenVPN®服务器选项卡。

创建OpenVPN®服务器

完成所有字段后单击 保存 。参考下表：

名称	输入OpenVPN®服务器的名称。
状态	打开或关闭以启用或禁用OpenVPN®服务器。
协议	从下拉列表中选择传输协议，TCP或UDP。 *默认协议是UDP。*
接口	从下拉列表中选择确切的接口(WAN)。
目的地	从下拉列表中选择目的（WAN或VLAN）。
本地端口	为OpenVPN®服务器配置监听端口。 *默认值为1194。*
服务器模式	选择OpenVPN®服务器将运行的服务器模式。有4种模式可供选择： ● SSL：仅使用证书进行身份验证（无用户/通行证身份验证）。每个用户都有一个唯一的客户端配置，其中包括他们的个人证书和密钥。如果不应提示客户机输入用户名和密码，这将非常有用，但它较少 安全，因为它只依赖于用户拥有的东西（TLS密钥和证书）。 ● 用户认证：仅使用CA、用户和密码进行认证，不 证书如果客户端不应该有单独的证书，则非常有用。不太安全 依赖于共享的TLS密钥加上用户知道的信息（用户名/密码）。 ● SSL+用户身份验证：需要证书和用户名/密码。每个用户都有一个唯一的客户端配置，其中包括他们的个人证书和密钥。 ● PSK：用于建立点对点OpenVPN®配置。VPN隧道将是 使用指定IP的服务器端点和指定IP的客户端端点创建。客户端和服务器之间的加密通信将通过UDP端口1194进行，这是默认的OpenVPN®端口。最安全，因为有多个身份验证因素（用户拥有的TLS密钥和证书，以及他们知道的用户名/密码）。
加密算法	从下拉列表中选择加密算法来加密数据，以便接收者可以使用相同的算法解密数据。
摘要算法	从下拉列表中选择摘要算法，该算法将唯一标识数据，以提供数据完整性，并确保接收者拥有原始主机发送的未修改数据。
TLS身份验证	此选项使用静态预共享密钥(PSK)，该密钥必须提前生成并在所有对方之间共享。 此功能通过要求传入数据包具有使用PSK密钥生成的有效签名，为TLS通道增加了额外的保护。
TLS身份认证方向	从下拉列表中选择TLS身份认证的方向，有三个选项可用（服务器、客户端或两者都有）。
TLS预共享密钥	如果启用了TLS身份验证，请输入TLS预共享密钥。
允许重复客户端证书	单击“打开”以允许重复的客户端证书
重定向网关	当使用重定向网关时，OpenVPN®客户端将通过VPN路由DNS查询，VPN服务器将需要处理它们。

推送路线	指定要推送到所有客户端的路由。 *示例：10.0.0.1/8*
LZO压缩算法	选择是否激活LZO压缩，如果设置为“自适应”，服务器将使 决定是否启用此选项。
允许对方更改IP	允许远程更改IP和/或端口，通常适用于远程IP地址频繁更改的情况。
CA认证	从下拉列表中选择生成的CA或添加一个。
服务器证书	从下拉列表中选择生成的服务器证书或添加一个。
IPv4隧道网络/掩码长度	输入GCC601X（W）将为OpenVPN®客户端提供服务的网络范围。 ***注意：****网络格式应为以下10.0.10.0/16。掩码应至少为16位。*

创建OpenVPN®服务器

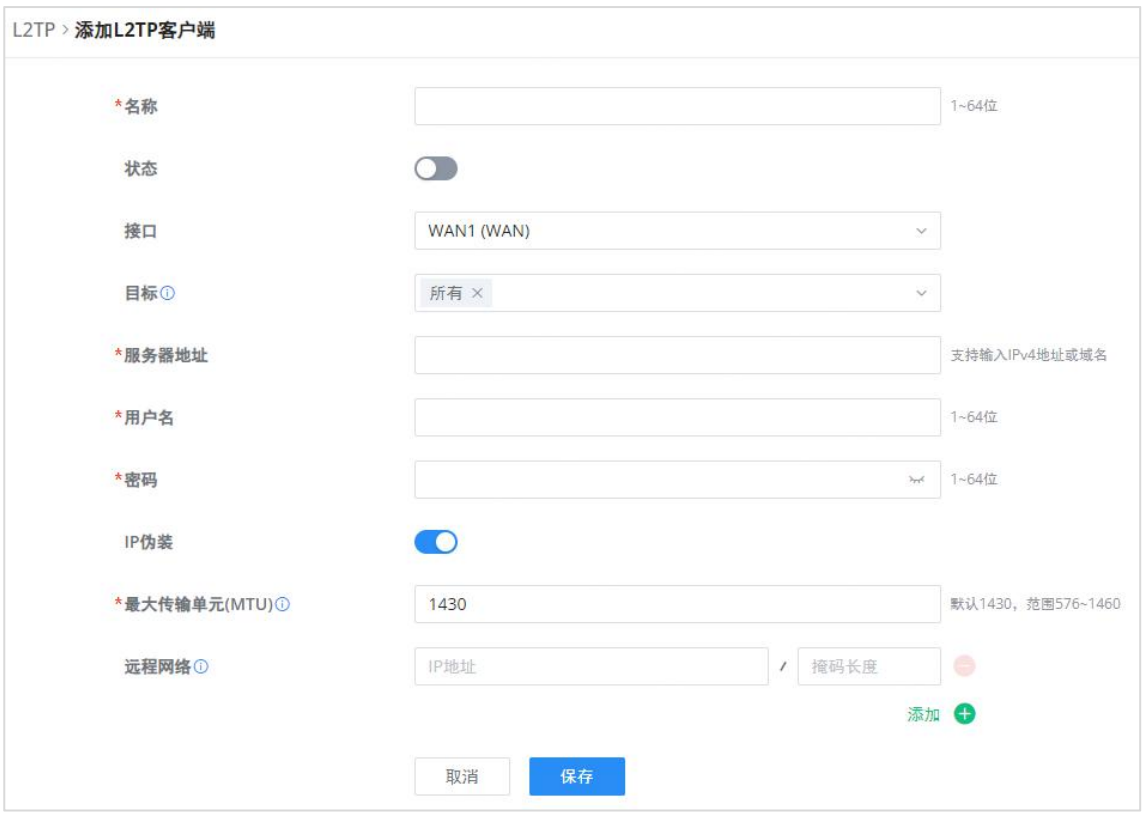
- **创建远程用户凭据**

要创建需要在客户端输入并在服务器端进行身份验证的远程用户帐户，请参考远程用户部分。

L2TP

要配置在GCC601X(W) 的L2TP客户端，请导航在 “VPN → VPN客户端” 下并且设置以下:

1.单击“添加”按钮，将弹出以下窗口。



L2TP客户端配置

名称	设置此VPN隧道的名称。
状态	打开/关闭此L2TP帐户。
接口	选择VPN使用的WAN端口。
目的	选择将使用此VPN的WAN、VLAN目的地。

服务器地址	输入VPN IP地址或FQDN。
用户名	输入已在服务器端配置的VPN用户名。
密码	输入已在服务器端配置的VPN密码。
IP伪装	此功能是网络地址转换（NAT）的一种形式，它允许网络外部没有已知地址的内部计算机与外部通信。它允许一台机器代表其他机器行动。
最大传输单原(MTU)	指由GCC发送的数据包的大小。除非必要，否则请不要更改此值。
远程子网	输入已在服务器端配置的远程子网。

L2TP客户端配置

完成所有字段后单击“保存”按钮。

L2TP客户端

WireGuard®

WireGuard®是一种免费的开源VPN解决方案，可加密虚拟专用网络，易于使用，高性能且安全。GCC601X(W) 系列支持WireGuard®具有自动生成Peer和QR码扫描功能的VPN，适用于具有相机支持的手机和设备。

开始使用WireGuard®VPN，请导航到Web UI → VPN → WireGuard®页。单击 “添加” 按钮以添加WireGuard®服务器如下所示:

WireGuard®选项卡

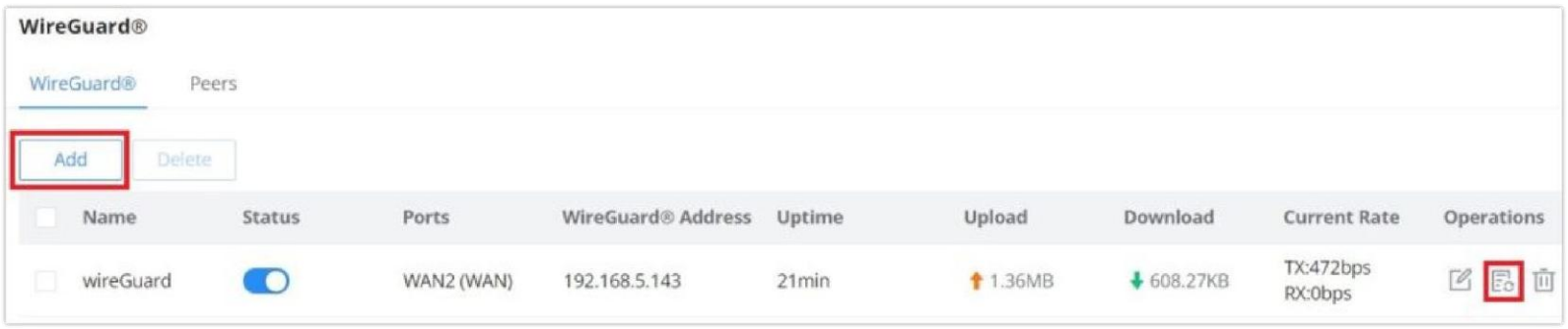
填写字段时，请参考下图和表格。

添加/编辑WireGuard®

名称	指定WireGuard®VPN的名称。
状态	打开或关闭以启用或禁用WireGuard®VPN。
接口	从下拉列表中选择WAN端口。
监控端口	建立WireGaurd时设置本地侦听端口®隧道。 *默认值：51820*
本地IP地址	指定WireGuard的网络®客户端 (Peer) 将从获取IP地址。
子网掩码	表示Peer可用的IP地址范围。
目的地	从下拉列表中选择目的地。 *注意：选择 “全部” 时，将自动包括后续的新接口。*
私钥	单击 “一键式生成” 文本以生成私钥。
公钥	公钥将根据私钥生成。单击 “复制” 文本以复制公钥。
最大传输单位 (MTU)	指由GCC发送的数据包的大小。除非必要，否则请不要更改此值。默认情况下为1450。

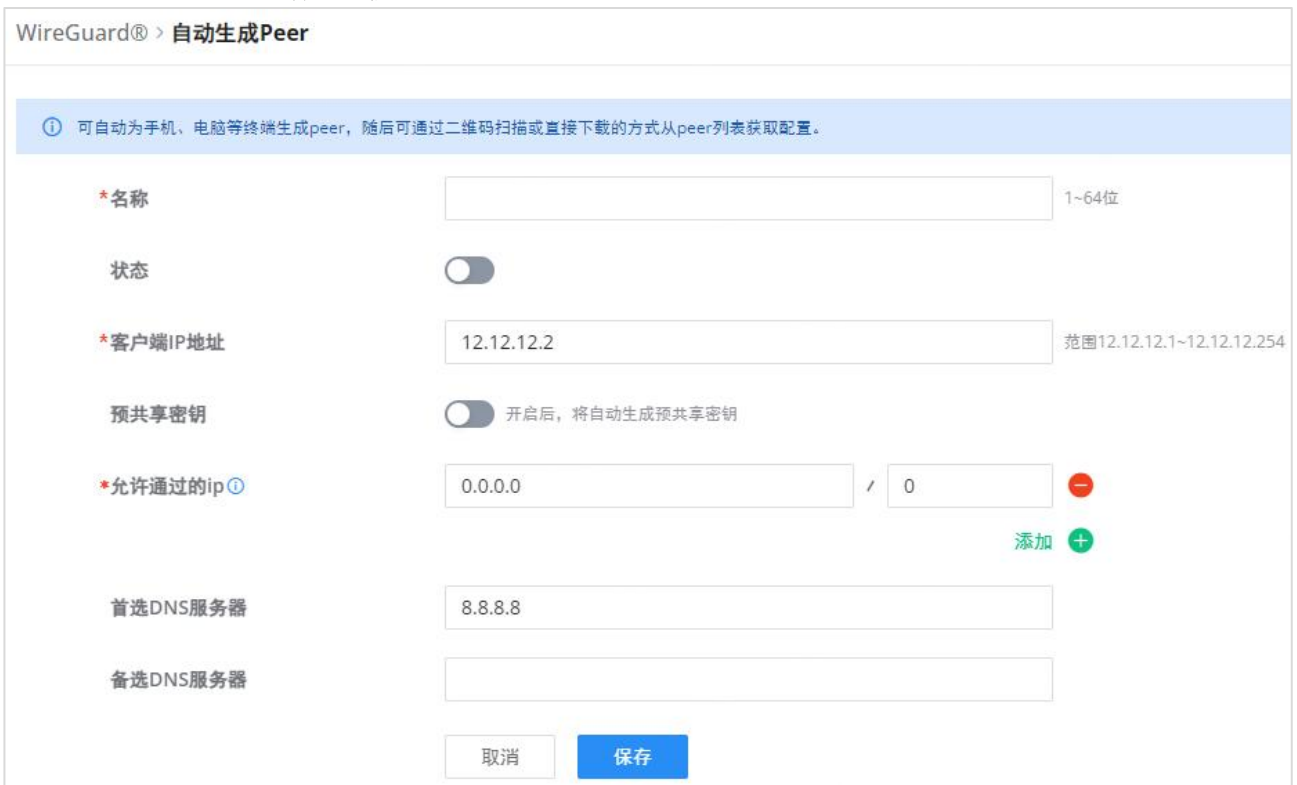
添加/编辑WireGuard®

完成配置WireGuard后®,单击 “自动生成Peer” 图标以非常快速，轻松地生成Peer，如下图所示:



WireGuard®选项卡

输入名称并切换状态，然后单击 “保存” 按钮。



WireGuard®自动生成Peer-第1部分

现在，用户可以下载配置文件并共享，或者下载QR码供手机等设备扫描。

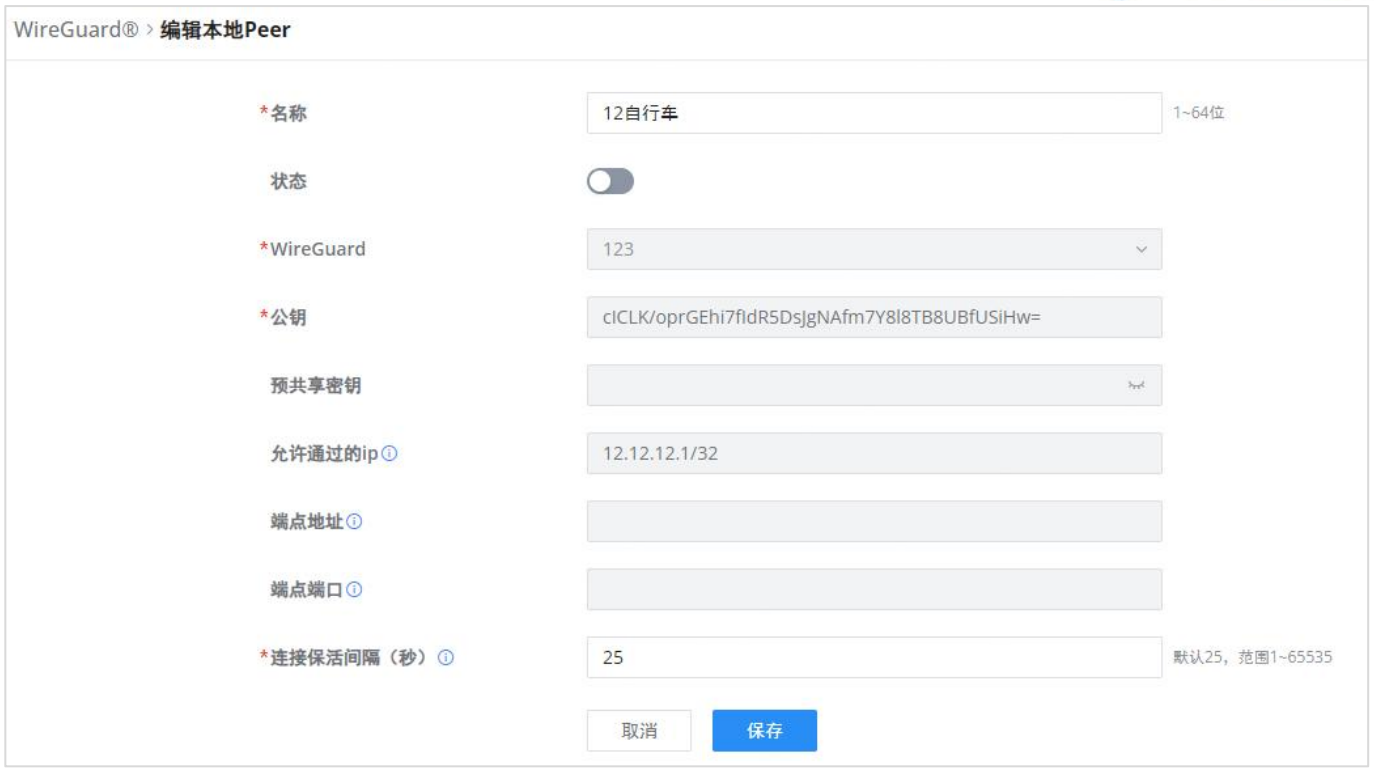
WireGuard®自动生成Peer-第2部分

Peers

在Peers选项卡上，用户可以通过点击 “添加” 按钮手动创建Peer。

WireGuard®-Peers选项卡

填写字段时，请参考下图。



WireGuard®-添加/编辑Peer

用户可以在添加Peer后下载配置文件。

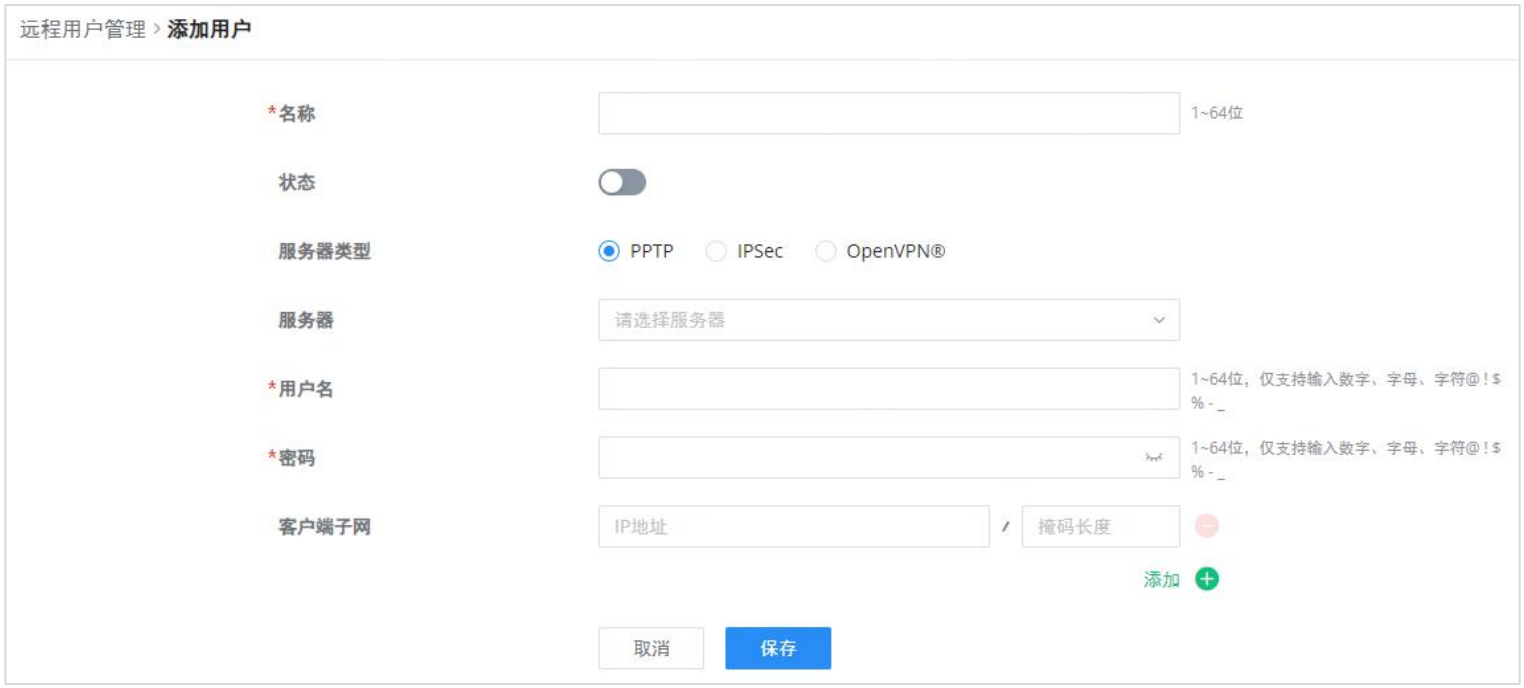
WireGuard®-下载Peer配置

或扫描具有相机支持的设备的QR码。

WireGuard®-扫描Peer配置

远程用户管理

要创建VPN用户帐户，请导航到VPN → 远程用户管理，然后单击 “添加”。配置的帐户将用于客户端向VPN服务器进行身份验证。在此部分可以创建的远程客户端用户，针对PPTP、IPSec和OpenVPN。



添加VPN远程用户

名称	输入用户的名称，此名称将不会用于登录
状态	启用或禁用此帐户
服务器类型	选择服务器的类型 ● PPTP ● IPSec ● OpenVPN
服务器名称	输入服务器的名称
用户名	输入用户名，此用户名将用于登录
密码	输入密码
客户端子网	指定客户端子网

添加VPN远程用户

要成功验证远程用户进入VPN服务器，用户名和密码与客户端证书一起使用。要创建客户端证书，请参阅证书部分。

要为每种VPN服务器类型配置VPN客户端，请参阅上面的相应VPN客户端配置。

路由

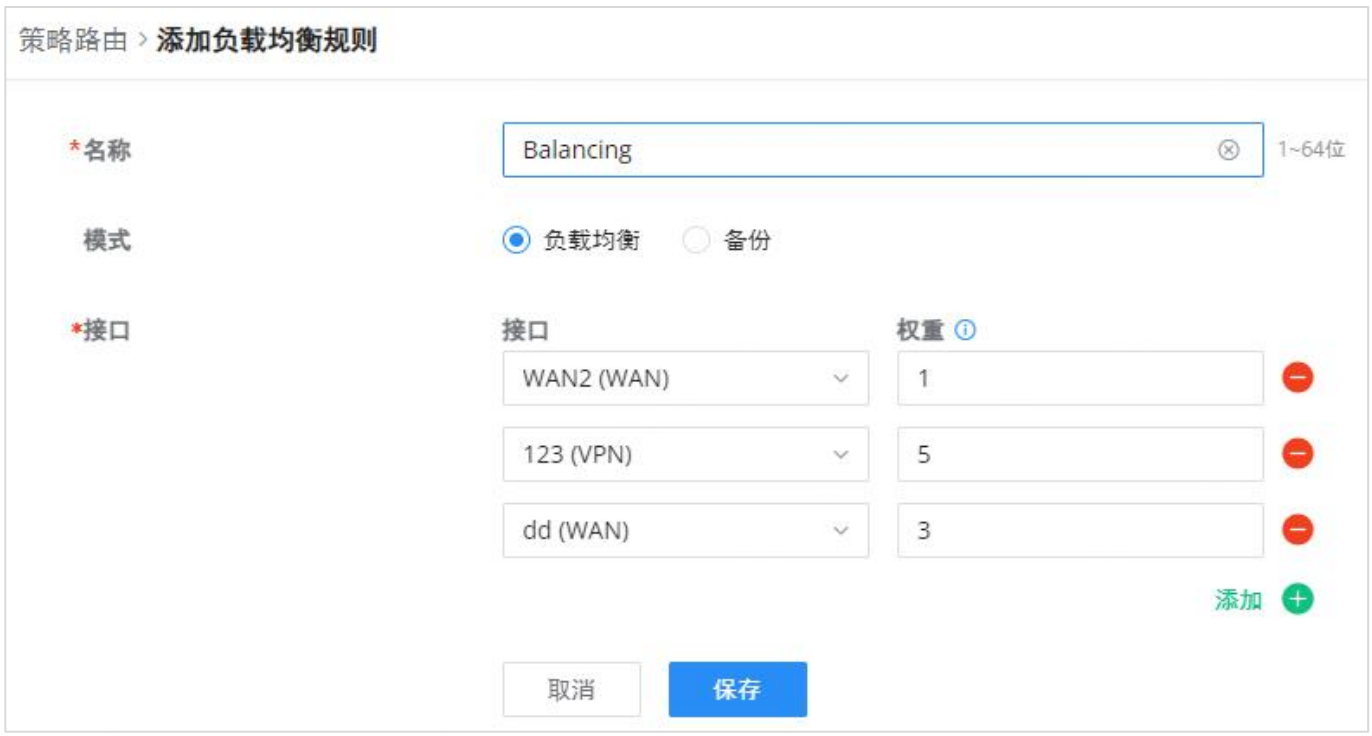
策略路由

在此部分中，用户可以创建策略路由，以在2个或更多WAN端口之间实现负载均衡或备份（故障转移）。此功能允许网络管理员为通过GCC的流量做出高级路由决策，并对指示哪些WAN端口甚至VLAN流量应使用的策略进行高粒度控制。以这种方式控制的流量可以在多个VLAN之间进行均衡。

负载均衡池

要创建负载均衡规则，请导航到路由 → 策略路由页 → 负载均衡池选项卡，单击 “添加” 按钮，然后在从下拉列表中选择WAN端口后选择模式（负载均衡或备份），并为添加的每个端口指定权重。请参考以下数字:

负载均衡池



负载均衡池-负载均衡模式

注意:

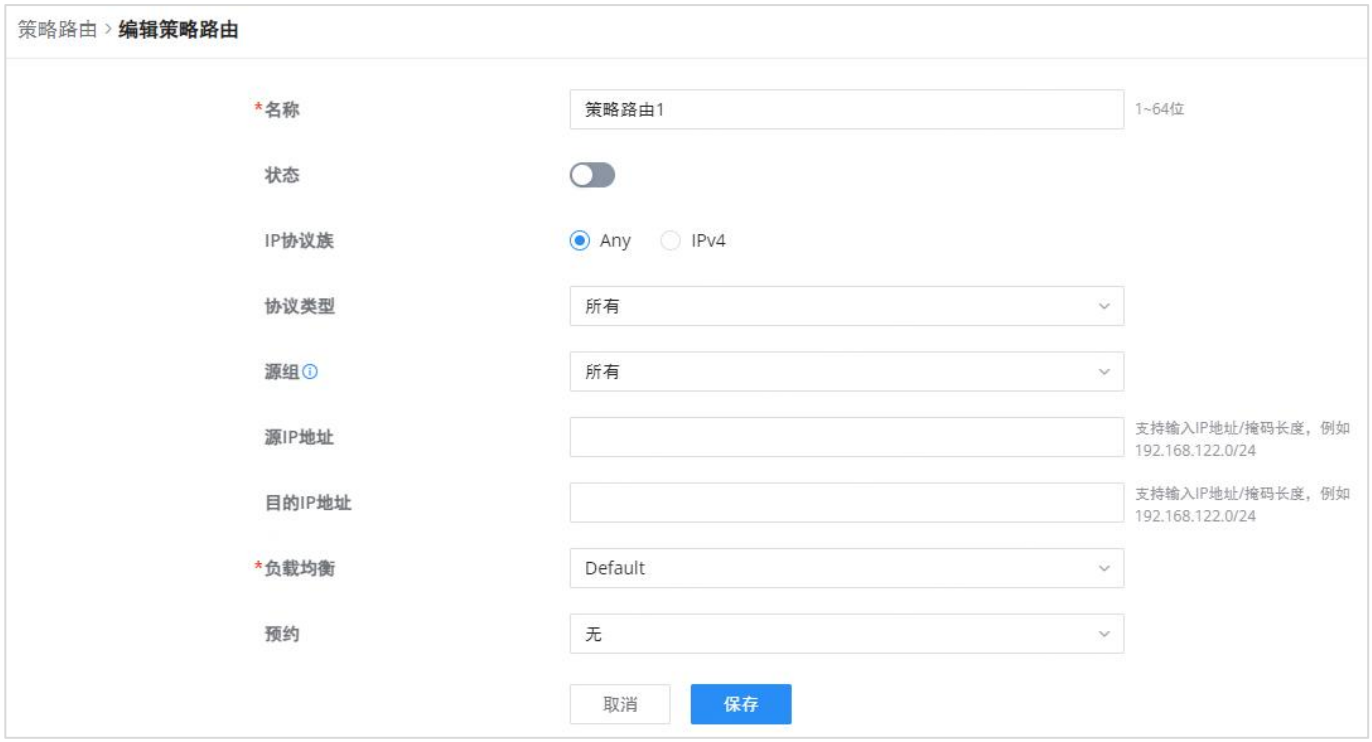
- 对于权重:默认为1，取值范围为1~10，其中10为最高权重。
- WAN端口的数量取决于GCC 设备的型号。

策略路由

在第二个选项卡（策略路由）上，用户可以指定哪个网络（VLAN）可以使用哪个负载均衡规则（必须首先创建），用户也可以指定协议类型、源和目的IP，甚至可以为其分配时间表。

要创建策略路由，请导航到路由 → 策略路由页面 → 策略路由选项卡，然后单击 “添加”。按钮如下图所示:

“策略路由” 页



添加策略路由

注意:

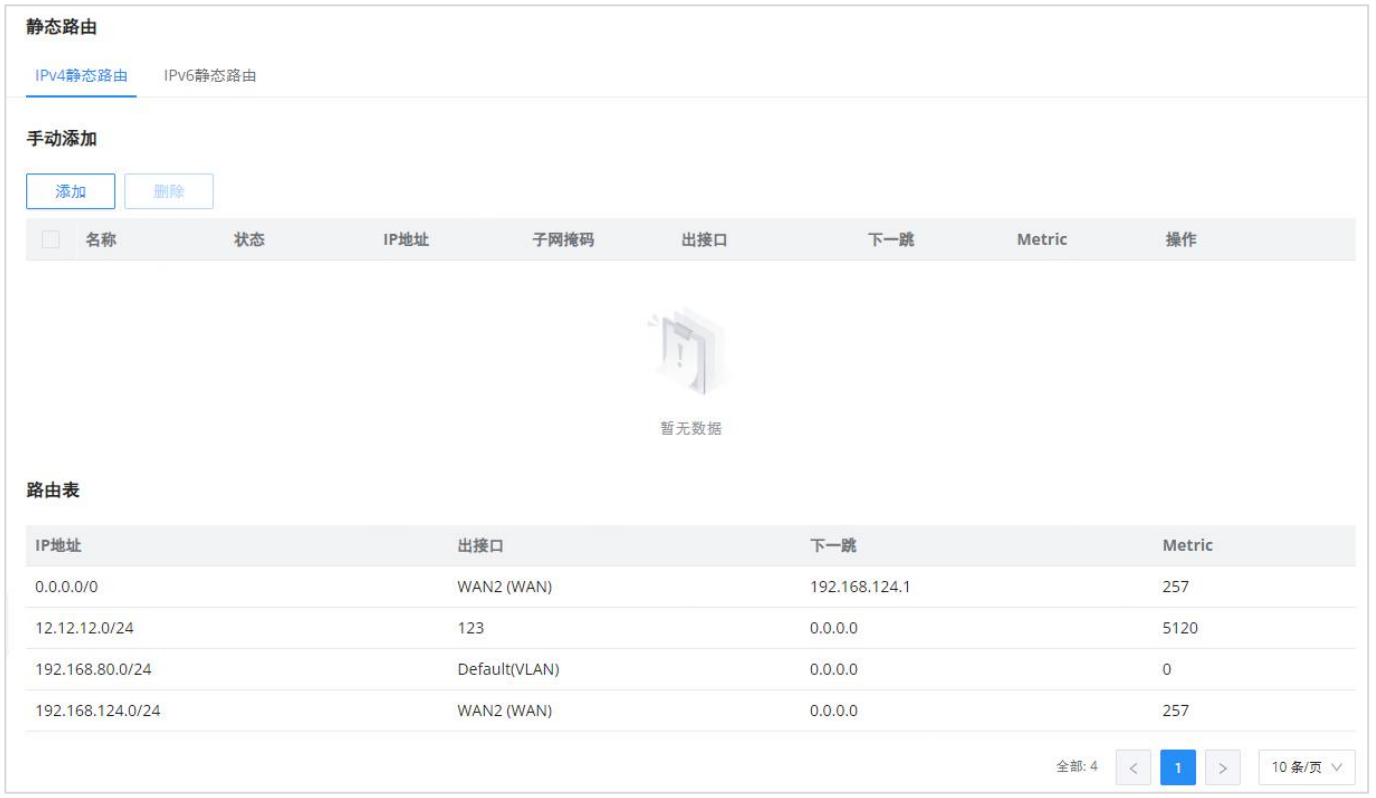
如果"源IP地址"和"目的IP地址"字段为空，则策略路由将采用任意IP地址。

静态路由

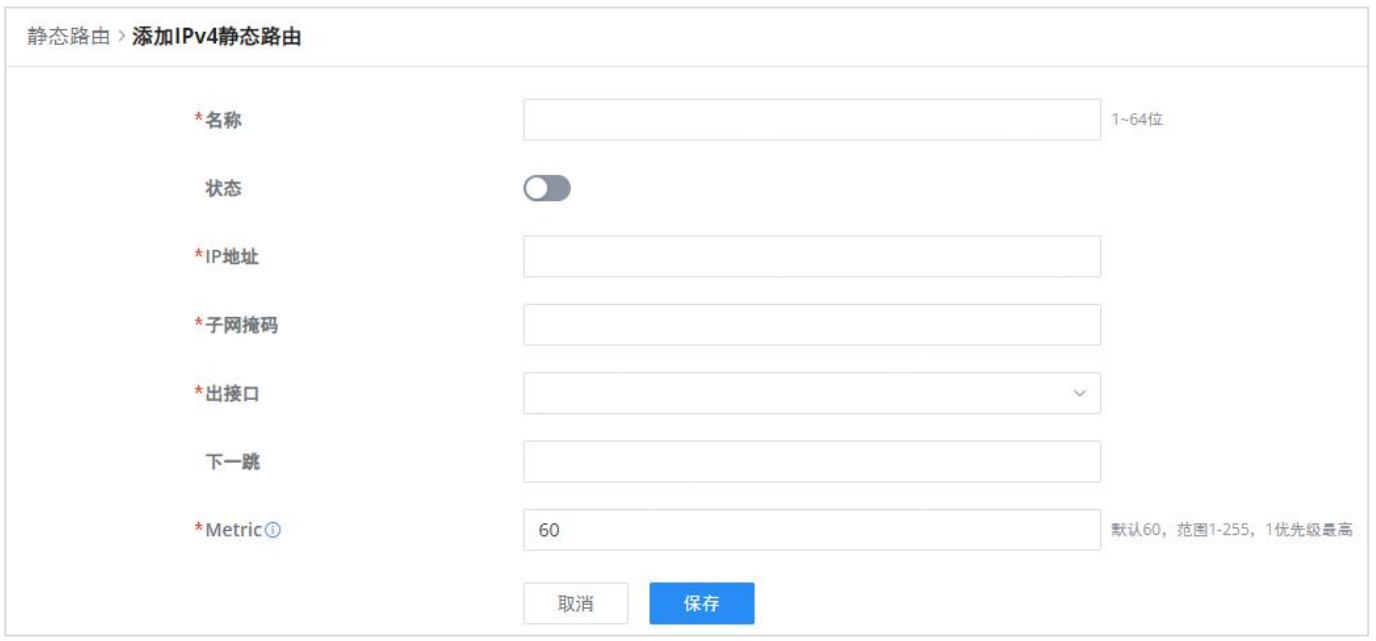
静态路由是一种通过手动配置路由项的路由形式，而不是对任何需要永不更改的静态地址的服务使用动态路由流量。

GCC601X(W) 支持手动设置IPv4或IPv6静态路由，可以从GCC601X(W)WebGUI→路由 → 静态路由访问。

要添加新的静态路由，用户需要单击“添加”按钮。



“静态路由” 页



添加IPv4静态路由

名称	指定静态路由的名称
状态	启用或禁用静态路由
IP地址	指定IP地址
子网掩码	输入子网掩码
出接口	选择接口
下一跳	指定下一个跃点
Metric	当网络中存在多个可以到达同一目的地的路由时，可以通过设置metric来调整路由规则的优先级，并且数据包将根据具有最小度量的路径进行转发。

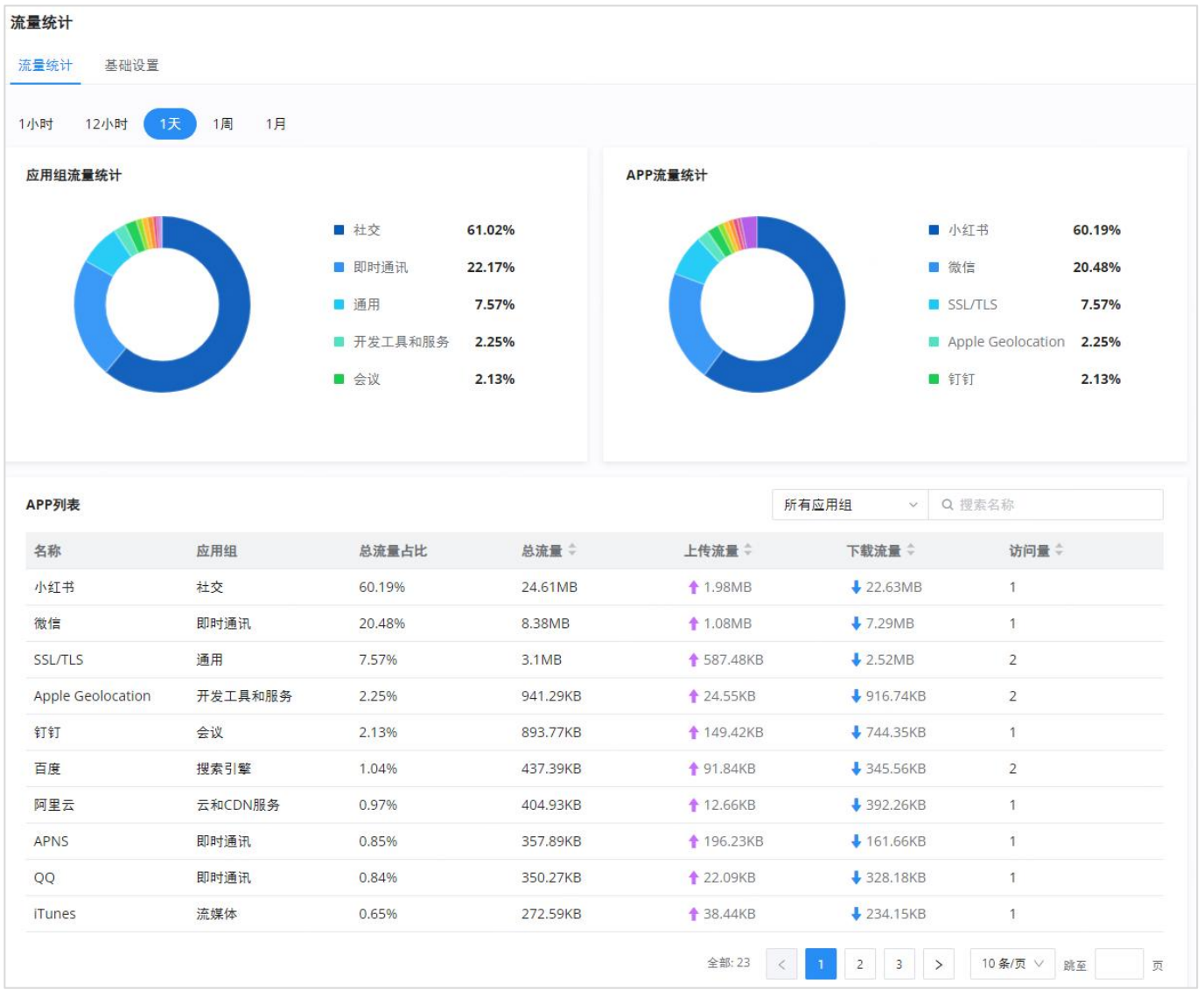
添加IPv4静态路由

流量管理

流量统计

启用流量统计后，GCC601X(W) 将开始识别流量并生成统计信息。统计数据将以图形方式表示，如下面的屏幕截图所示。该功能显示生成流量的服务的名称和类型，以便轻松识别正在使用哪些服务以及哪些客户端正在使用这些服务。

> **注意**
>
> GCC601X(W)支持最长一个月的流量统计数据。



流量统计与分析

要启用流量统计，请导航到流量管理→基础设置，然后打开 “流量统计”。

用户还可以选择启用AI识别，启用后，AI深度学习算法将用于优化应用分类的准确性和可靠性，这可能会消耗更多的CPU和内存资源。

启用流量统计

QoS

服务质量（QoS）是允许在WAN和LAN主机之间交换的延迟敏感数据流的优先级的功能。这将对有限带宽的使用提供更多控制，

并确保所有应用服务不受交换流量的影响。

通用设置

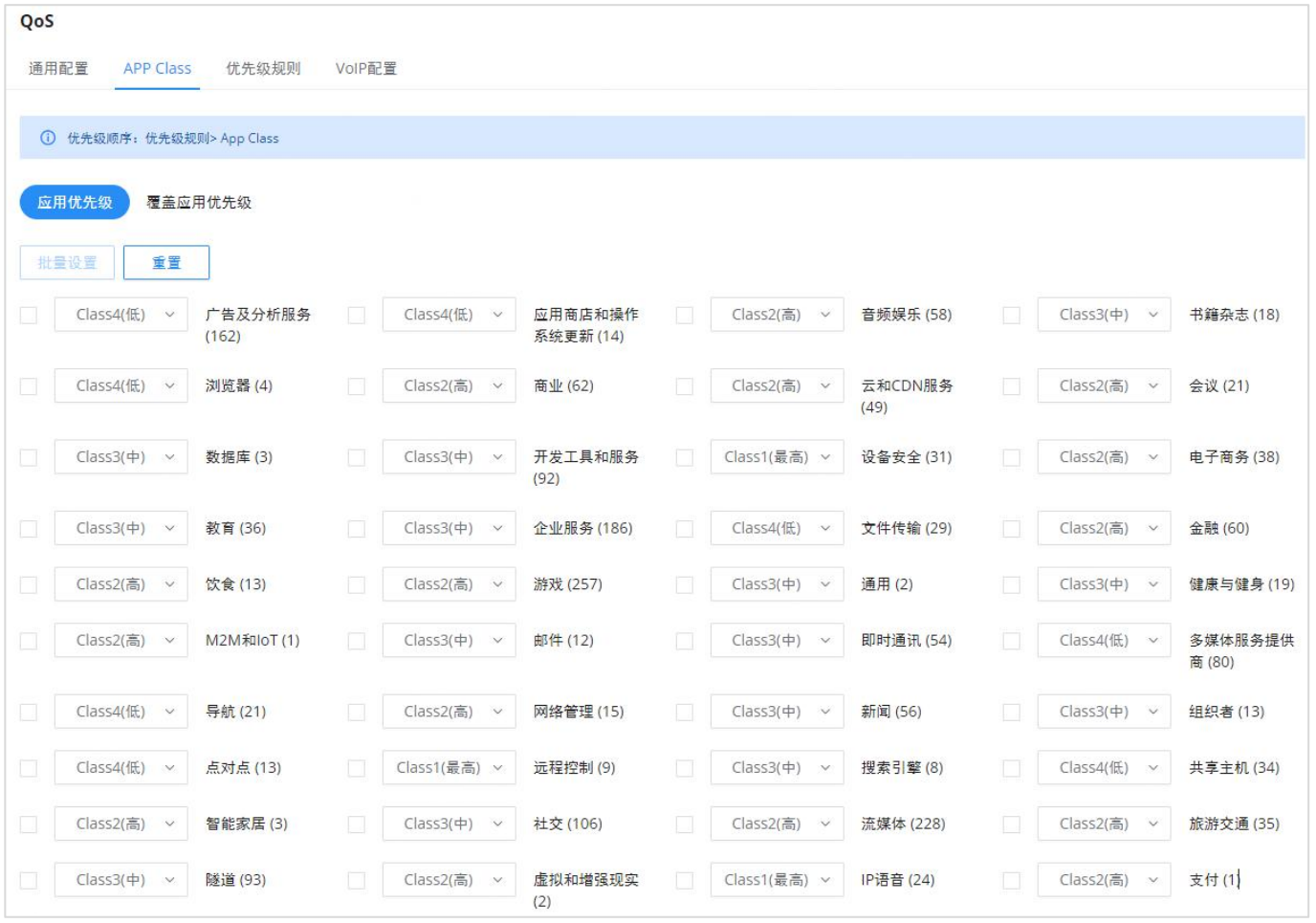
在此页面上，用户将能够将下载和上传带宽的百分比分配给4个类别。可以将这些类分配给应用程序，以确定将优先考虑哪些应用程序流量，这包括入站和出站流量。此外，还可以为每个类使用DSCP标记来标记出站流量。

App 优先级

GCC601X(W) 可以按类别或单独对应用程序的流量进行优先级排序。可以在4个类别中设置优先级，类别1具有最高优先级，而类别4具有最低优先级。要访问App类设置，请访问GCC的Web GUI，然后导航到流量管理 → QoS → App类。

- **应用程序优先级**

在应用程序优先级下，用户可以选择一个类别，然后指定优先级（最高，高，中，低或无），请看下图:



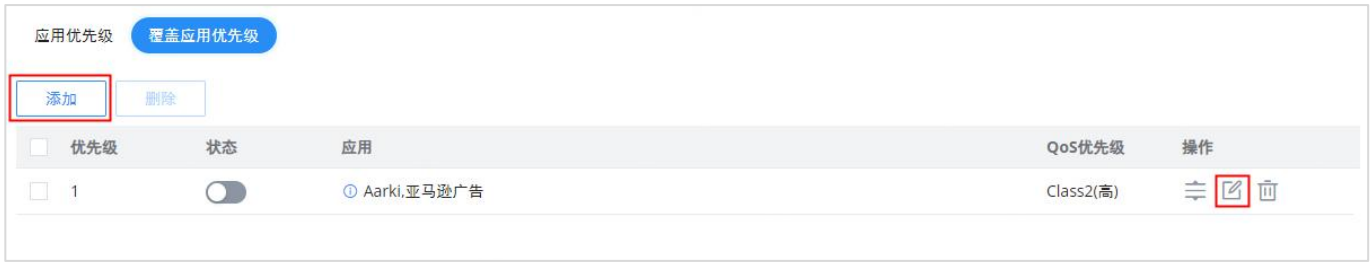
QoS-App类

也可以选择许多类别，然后单击 “批处理设置” 以一次对所有类别应用QoS优先级。

Qos-Apps类-配置类

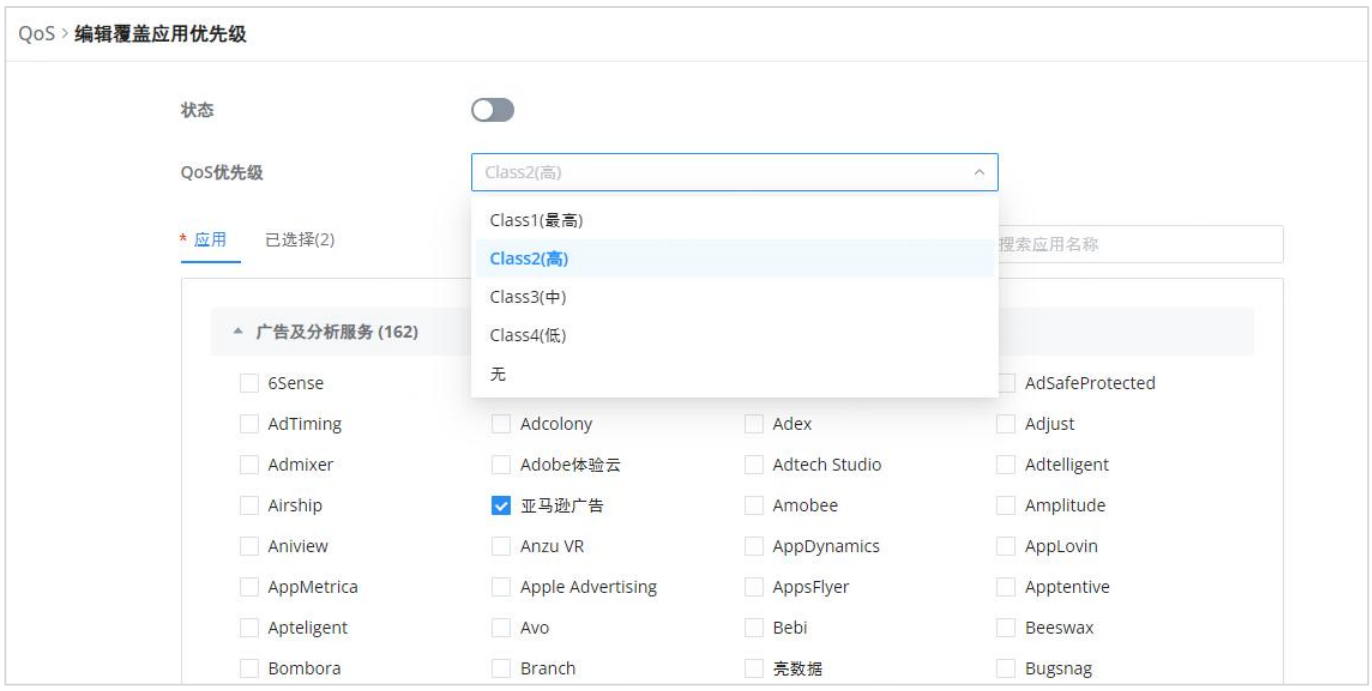
- **覆盖应用程序优先级**

上一个选项（应用程序优先级）适用于整个类别的优先级，如果用户想要进行例外或添加特定应用程序，在 “覆盖应用程序优先级” 下，单击 “添加” 按钮，如下所示:



Qos-Apps类-覆盖应用程序优先级

然后从不同的类别中选择特定的应用程序，从下拉列表中选择QoS优先级。这将覆盖在整个类别上应用的应用程序优先级。

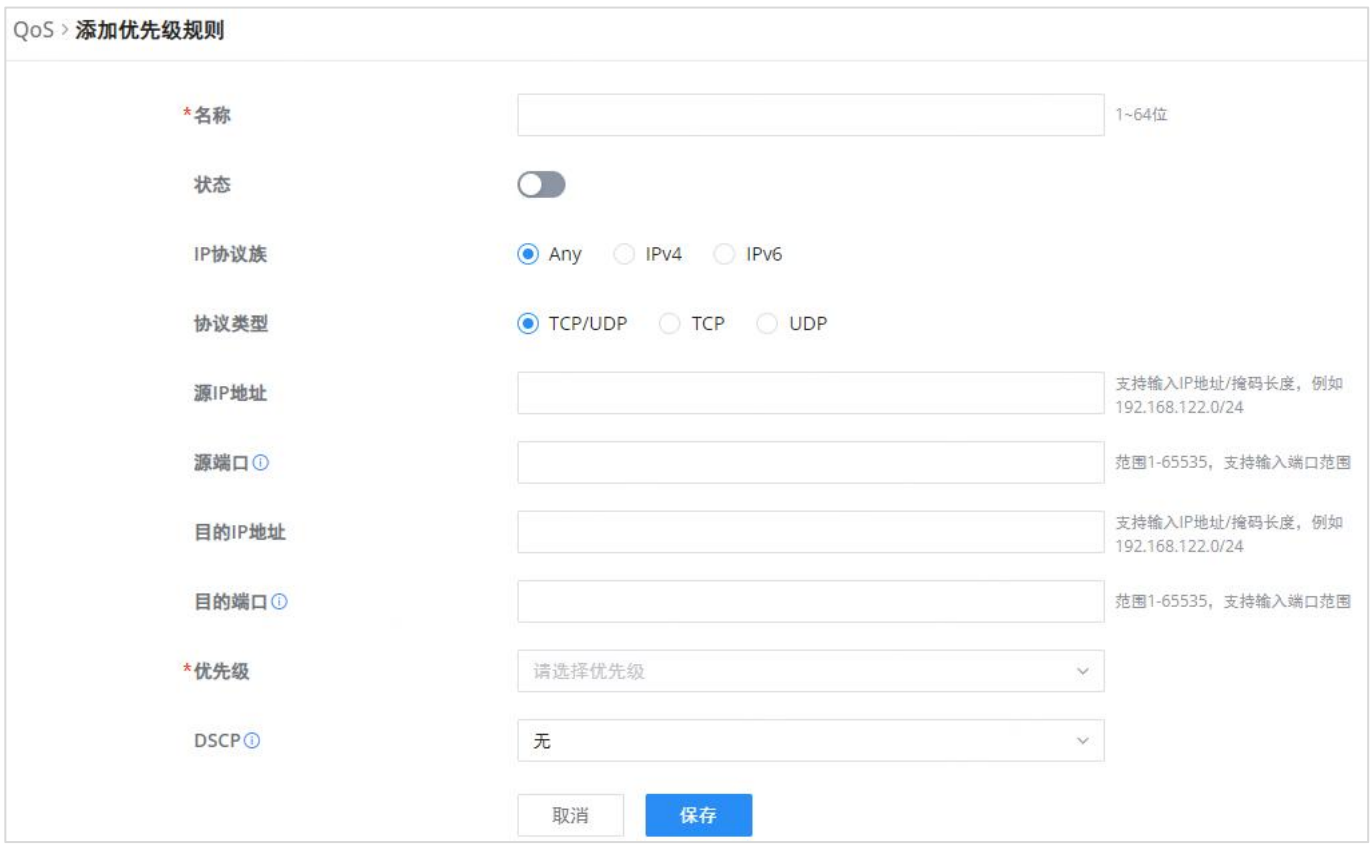


Qos-Apps类-添加/编辑覆盖应用程序优先级

> **注意**
>
> 应用App类可能需要一些时间，因为路由器需要检查足够数量的数据包来识别由应用程序生成的流量。

优先级规则

QoS优先级规则是根据源/目的IP地址以及源/目的端口设置的规则。



QoS-添加优先级规则

名称	输入类的名称。字符数限制为1-94个字符。
状态	启用或禁用类的状态。

IP协议族	选择IP协议族: ● Any: 允许的IP地址可以是IPv4或IPv6。 ● IPv4: 允许的IP地址严格为IPv4。 ● IPv6: 允许的IP地址严格为IPv6。
协议类型	选择协议类型: ● TCP/UDP: QoS类将同时应用于TCP和UDP流量。 ● TCP: QoS类将仅应用于TCP流量。 ● UDP: QoS类将仅应用于UDP流量。
源IP地址	输入源IP地址/掩码长度。例如，“192.168.122.0/24”
源端口	输入单个端口号、多个端口号或端口号范围。 示例: -要输入单个端口号，请输入端口号，如 “3074”。 要输入多个端口号，请输入端口号并在每个端口号之间加上逗号，例如 “3074, 5060, 10000”。 -要输入端口范围，请输入该范围内的第一个端口号，然后输入短划线 (-) 并输入该范围内的最后一个端口号。例如，“4,5-10” 注意: 可以输入的端口号的有效范围是1-65535。
目的IP地址	输入目的IP地址/掩码长度。例如，“192.168.122.0/24”
目的端口	输入单个端口号、多个端口号或端口号范围。 示例: -要输入单个端口号，请输入端口号，如 “3074”。 -要输入多个端口号，请输入端口号并在每个端口号之间加上逗号，例如 “3074、5060、10000”。 -要输入端口范围，请输入该范围内的第一个端口号，然后输入短划线 (-) 并输入该范围内的最后一个端口号。例如，“10000 20000” 注意: 可以输入的端口号的有效范围是1-65535。
优先级	选择优先级类别。
DSCP	选择DSCP值。针对当前优先级的DSCP标记将会覆盖出站流量标记中对应优先级的DSCP，优先生效。

QoS-添加优先级规则

VoIP设置

在QoS的VoIP设置允许用户识别和优先化由GCC601X(W) 转发的VoIP数据流。要配置此选项，请访问GCC601X(W) 的Web UI，然后导航到流量管理 → QoS → VoIP设置，然后切换 “优先保证VoIP服务”，指定SIP UDP端口，默认情况下端口号为5060。

VoIP设置

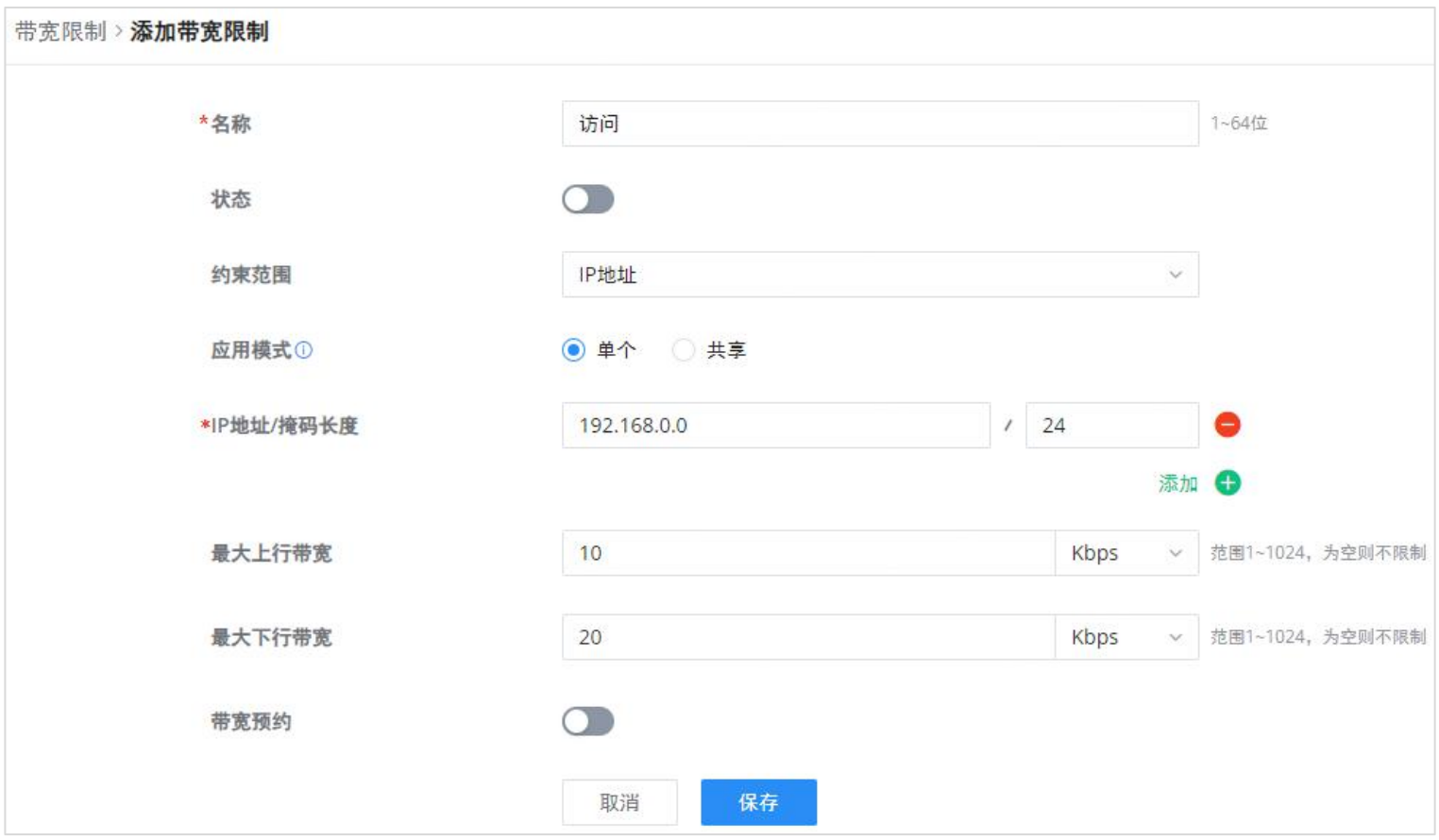
带宽限制

带宽限制功能通过指定最大上传和下载带宽来帮助限制带宽，然后可以将此限制应用于每个IP/MAC地址或应用于IP地址范围中的所有IP地址。导航至Web UI → 流量管理 → 带宽限制。

“带宽限制” 页

要添加带宽规则，请点击 “添加” 按钮或点击 “编辑” 图标，如上所示。

请参考下图:



添加/编辑带宽规则

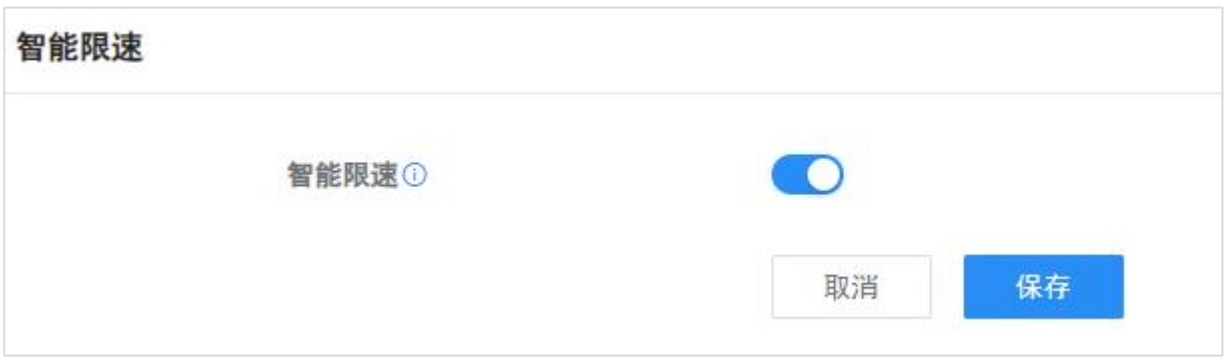
注意:

应用模式: 选择“单个”，设置每个IP地址可使用的最大上传带宽和最大下载带宽; 选择“共享”，设置IP地址段内所有IP地址可使用的最大上传带宽和最大下载带宽之和。

智能限速

启用智能速度限制后，当CPU负载高时，它会自动限制下载或上传流量的速度。

要启用智能限速，请导航至流量管理 → 智能限速，然后打开该功能。

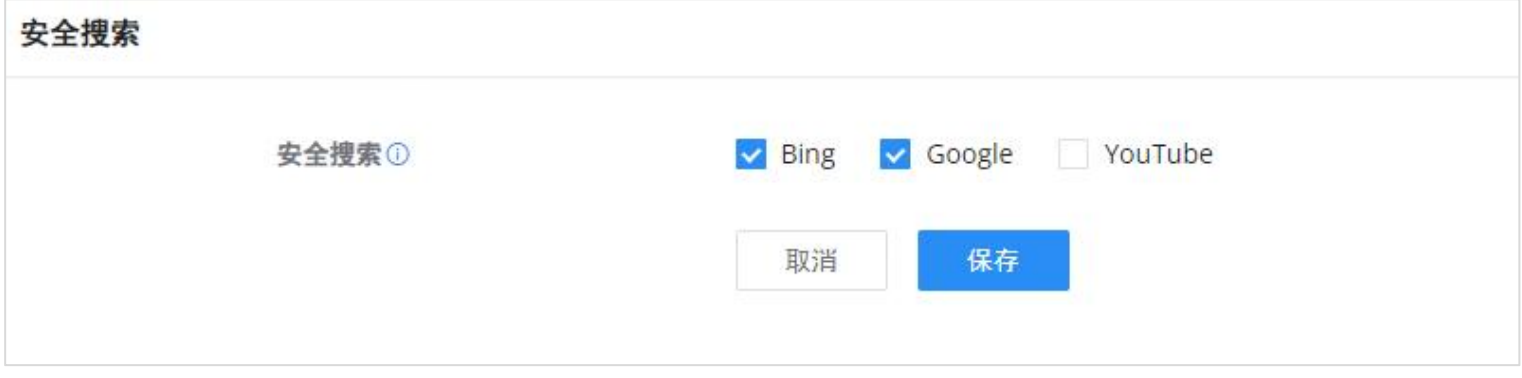


智能限速

访问控制

安全搜索

GCC601X(W) 在Bing，Google和YouTube上提供了安全搜索功能。启用此选项将隐藏任何不适当或显式的搜索结果。



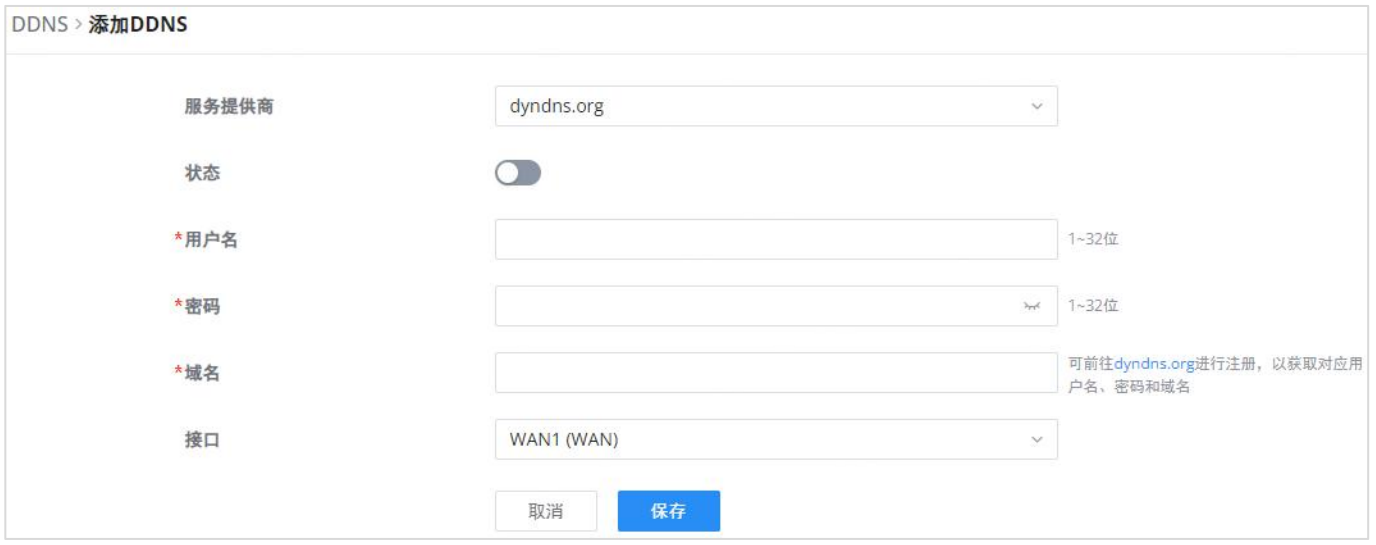
“站点控制” 页 默认情况下，从WAN侧发起的所有请求由GCC601X(W) 拒绝外部访问功能允许位于WAN侧的主机访问在GCC601X(W) 的LAN侧托管的服务。

外部访问

DDNS

访问GCC601X(W) Web GUI，导航到外部访问 → DDNS，然后单击 添加 添加服务。

1. 在 “服务提供商” 字段下填写使用DDNS提供商创建的域名。
2. 在用户名和密码字段下输入您的帐户用户名和密码。
3. 在 “域” 下指定应用DDNS帐户的域。



服务提供商

服务提供商	选择服务提供商
用户名	输入用户名
密码	输入密码
域	输入域
接口	选择接口

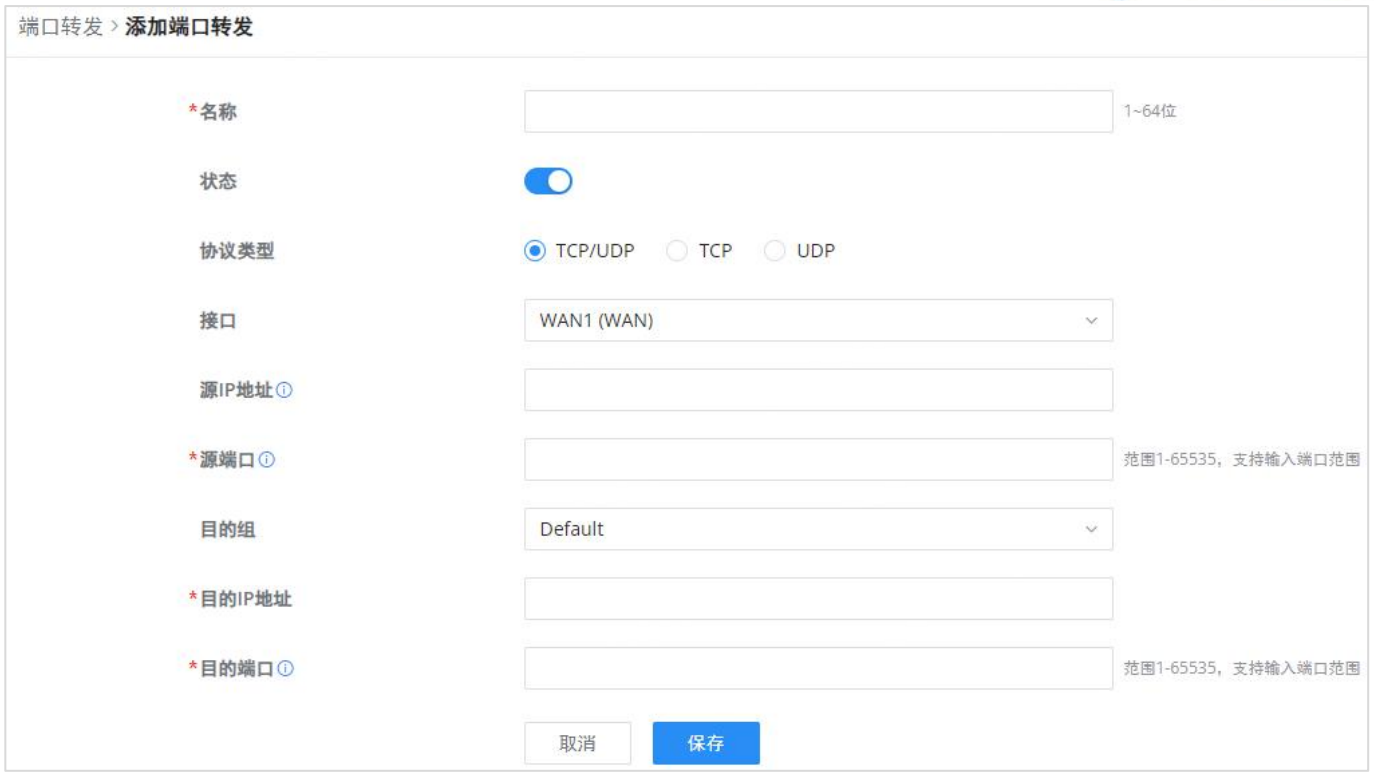
DDNS

端口转发

允许将从GCC601X(W) 的WAN侧发起的请求转发到LAN主机。

这是通过仅配置端口或端口和IP地址来完成的，以防我们要限制对该特定端口的访问到一个IP地址。一旦GCC601X(W) 接收到关于IP地址的请求，GCC601X(W) 将验证在其上发起请求的端口，并且将请求转发到主机IP地址和被配置为目的地的主机的端口。

在WAN侧的主机想要访问LAN侧的服务器的情况下，可以使用端口转发。导航到外部访问 → 端口转发:



“端口转发” 页

编辑或创建端口转发规则时，请参阅下表中的 “端口转发” 选项:

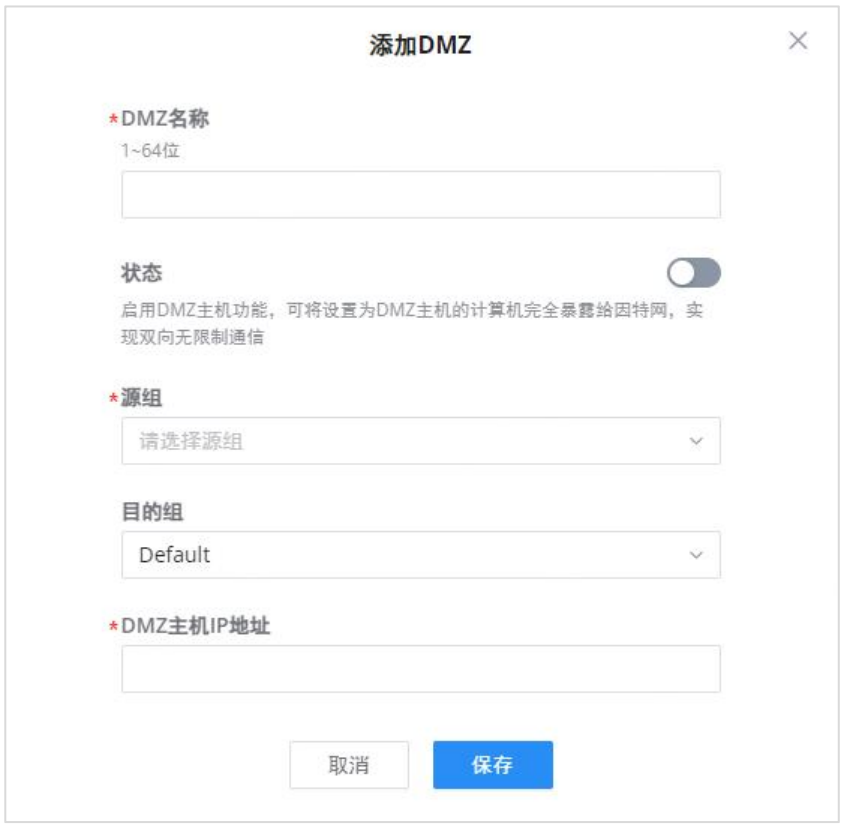
名称	输入端口转发规则的名称。
状态	打开/关闭规则状态。
协议类型	选择一个协议，用户可以选择TCP，UDP或TCP/UDP。
接口	选择WAN端口
源IP地址	设置外部用户访问此设备的IP地址。如果未设置，则可以使用相应WAN端口上的任何IP地址
源端口	设置单个或一系列端口。
目的组	选择VLAN组。
目的IP地址	设置目的IP地址。
目的端口	设置单个或一系列端口。

“端口转发” 页

DMZ

配置DMZ后，GCC601X(W) 将允许对DMZ主机的所有外部访问请求。此部分可以从Web GUI → 外部访问 → DMZ访问。

GCC601X(W) 支持DMZ，指定主机名IP地址放在DMZ是可能的。



DMZ页面

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

有关DMZ字段，请参阅下表:

DMZ名称	输入DMZ规则的名称。
状态	打开/关闭DMZ规则的状态。
源组	选择允许访问DMZ主机的接口。
目的组	选择DMZ主机所属的VLAN。
DMZ主机名IP地址	输入DMZ主机IP地址。

DMZ页面

UPnP

GCC601X(W) 支持UPnP，使主机上运行的程序能够自动配置端口转发。

UPnP允许程序使GCC601X(W) 打开必要的端口，无需用户的任何干预，无需进行任何检查。

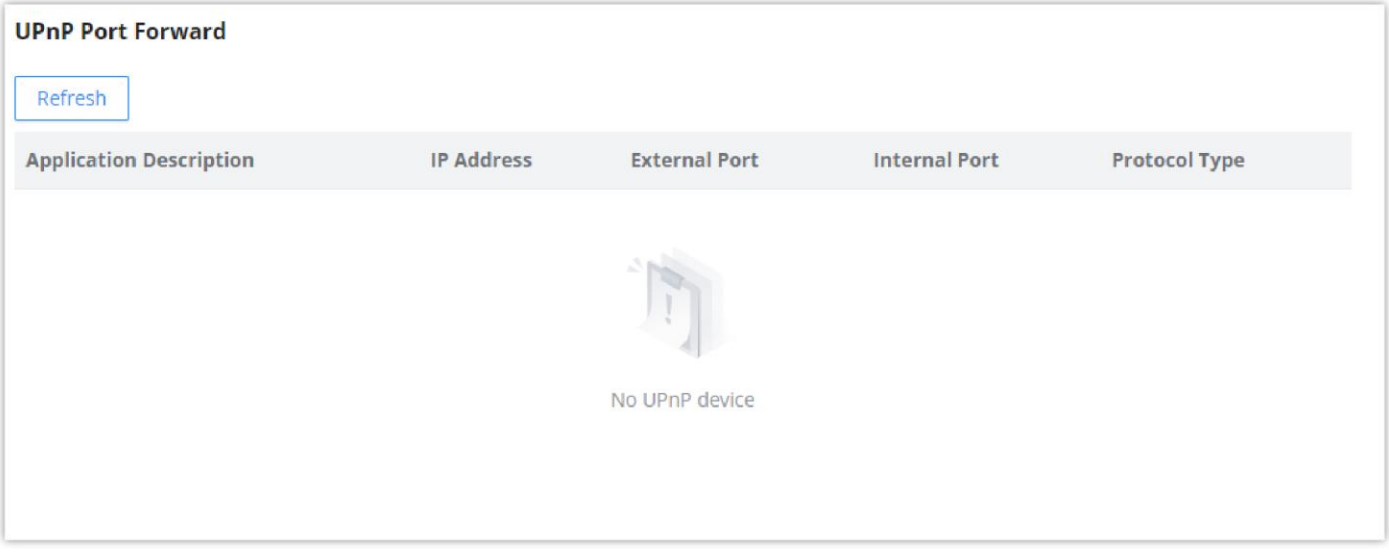
可以从GCC601X(W) Web GUI → 外部访问 → UPnP访问UPnP设置。

UPnP设置

UPnP	单击 “开关” 以启用UPnP。 注意：一旦启用UPnP（通用即插即用），LAN中的计算机可以请求GCC自动进行端口转发
接口	选择接口（WAN）
目的组	选择LAN组

UPnP设置

启用UPnP后，端口将显示在下面的部分中。显示的信息包括应用程序名称、已请求打开端口的LAN主机的IP地址、外部端口号、内部端口号以及所使用的传输协议（UDP或TCP）。



UPnP-转发端口

TURN服务

TURN代表使用NAT周围的中继进行遍历，它是一种网络服务，可帮助在NAT或防火墙后面的设备之间建立Peer连接。实时通信（如视频会议、IP语音等）受益于TURN服务，以在NAT或防火墙阻止或修改流量时在Peer之间建立连接。

导航至Web UI → 外部访问 → TURN服务。默认情况下，该服务处于关闭状态，将状态切换为打开该服务。默认的TURN服务器端口是3478，也可以通过单击 “减号” 和 “加号” 图标来添加或删除用户名和密码。

TURN服务

注意:

- TURN服务端口默认为3478。
- "转发端口": 不需要修改转发端口范围。请确保其他业务使用的端口不与TURN转发端口冲突。
- TURN业务是针对专网UC的NAT穿越解决方案，是针对Grandstream UCM和Wave的VoIP媒体流量NAT穿越网关。

维护

GCC601X(W) 为维护和调试提供了多种工具和选项，以帮助进一步排除故障和监控GCC601X(W) 资源。

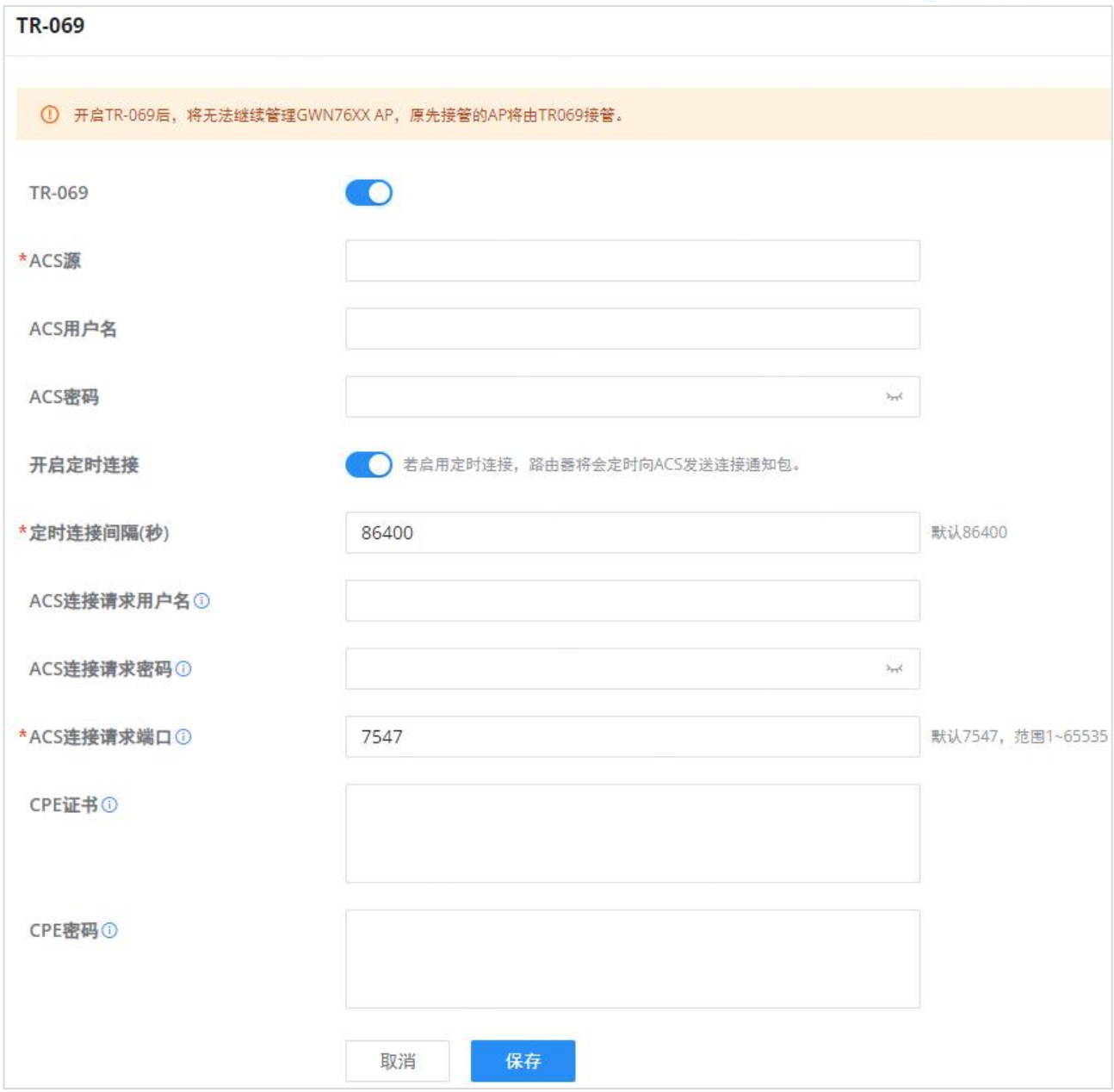
TR-069

它是用于在CPE（用户端设备）和ACS（自动配置服务器）之间的通信的协议，其提供安全的自动配置以及公共框架内的其它CPE管理功能。

TR-069代表宽带论坛定义的 “技术报告”，其中指定了CWMP “CPE WAN管理协议”。它通常使用HTTP或HTTPS作为CPE和ACS之间的通信的传输。消息交换使用SOAP（XML_RPC）来配置和管理设备。

注意

如果启用，GCC601X(W)将无法继续管理GWN设备。



TR-069页面

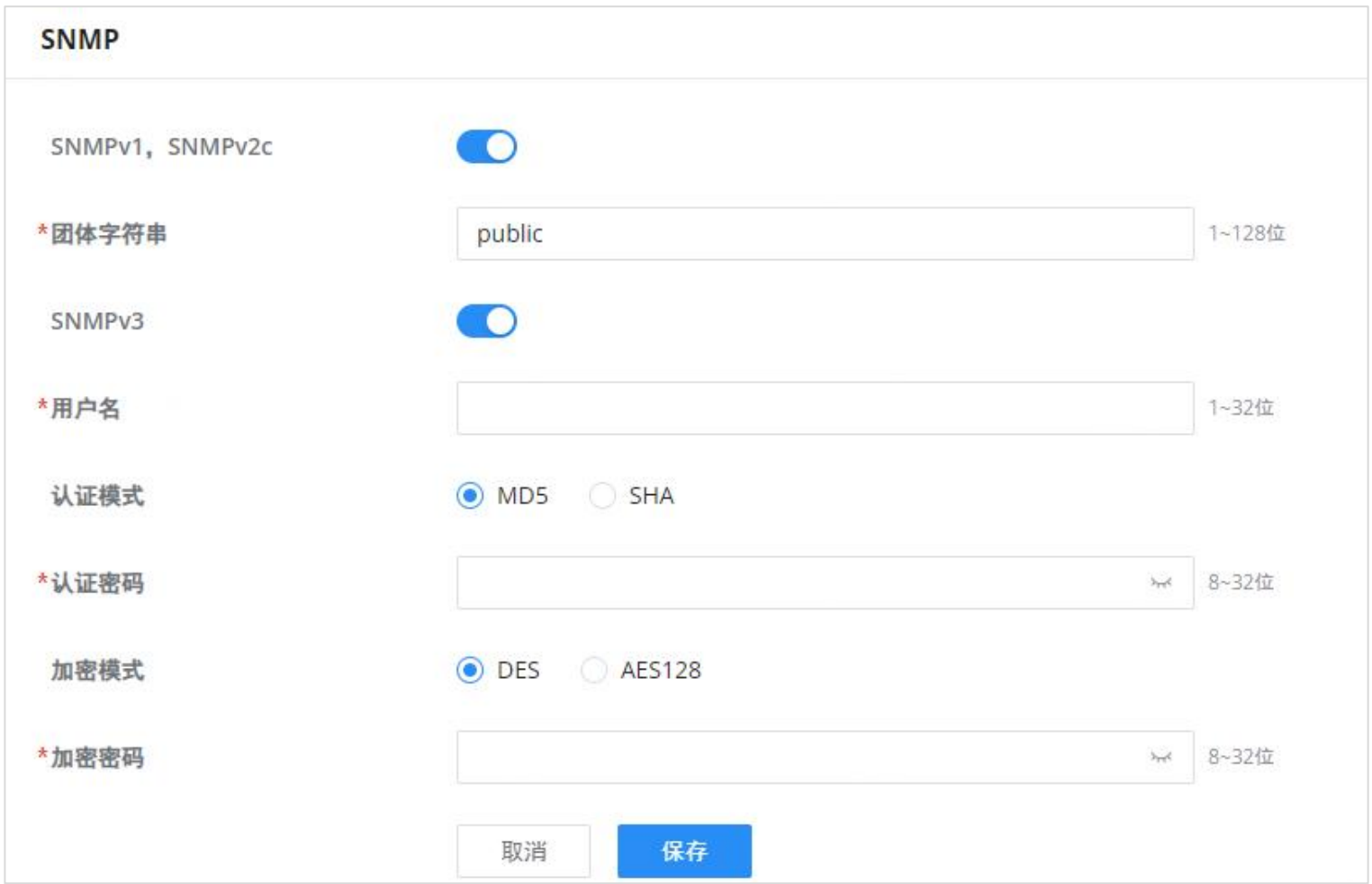
TR-069	启用/禁用TR-069。
ACS 源	输入ACS服务器的FQDN或IP地址。
ACS用户名	输入用户名。
ACS密码	输入密码。
开启定时连接	如果启用，GCC601X(W) 将定期发送连接通知数据包到ACS。
定时连接间隔（秒）	配置设备向ACS服务器发送通知的间隔时间。
ACS连接请求用户名	当ACS服务器向设备发送连接请求时， 设备身份验证ACS必须与ACS侧的配置一致。
ACS连接请求密码	设备对ACS进行身份验证的密码必须与 ACS服务器的配置。
ACS连接请求端口	ACS向GCC601X(W) 发送连接请求的端口。此端口不能被其他设备功能占用。
CPE证书	输入设备通过SSL连接到ACS时需要使用的证书
CPE密码	输入设备在通过SSL连接到ACS时需要使用的证书密钥。

TR-069页面

SNMP

GCC601X(W) 支持SNMP（简单网络管理协议），SNMP广泛用于网络管理，用于网络监视，以收集有关受监视设备的信息。

要配置SNMP设置，请转到Web GUI → 维护 → SNMP，在此页面中，用户可以启用SNMPv1、SNMPv2c或启用SNMPv3，然后输入所有必要的参数。



SNMP

要配置SNMPv1或SNMPv2，请参阅下表：

SNMPv1、SNMPv2	启用/禁用SNMPv1和SNMPv2
团体字符串	输入团体的共享密码。

SNMP-SNMPv1或SNMPv2

要配置SNMPv3，请参考下表：

SNMPv3	启用/禁用SNMPv3。
用户名	输入用户名。
身份验证模式	选择用于身份验证的算法。
身份验证密钥	选择身份验证密码。
加密模式	选择用于数据加密的加密协议。
加密密码	输入加密密码。

SNMP - SNMPv3

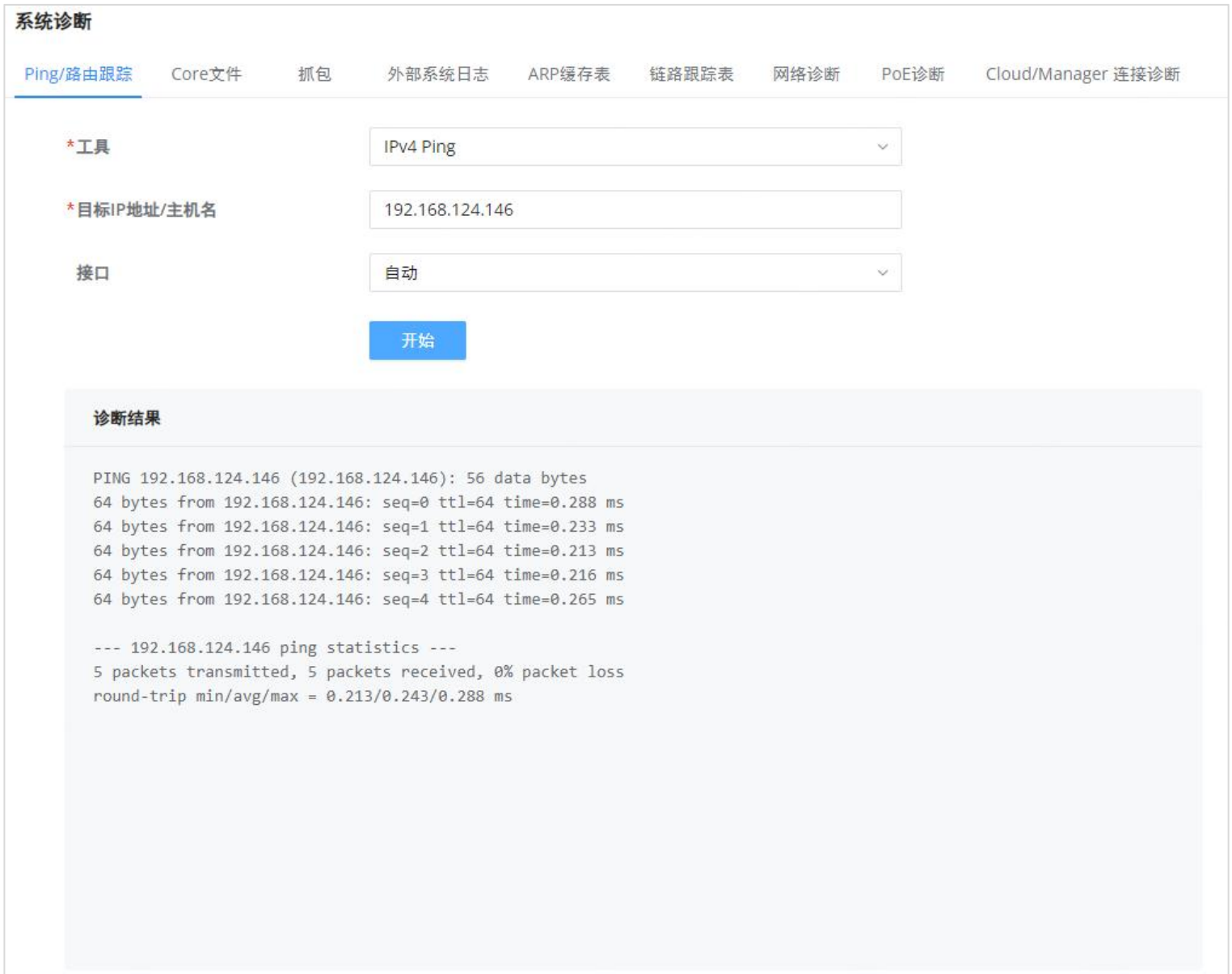
系统诊断

许多调试工具在GCC601X(W) 的Web GUI是可用的检查状态和排除故障GCC601X(W) 的服务和网络。

要访问这些工具，请导航至 “Web UI → 系统设置 → 系统诊断”。

Ping/路由跟踪

Ping和路由跟踪是有用的调试工具，用于验证与网络 (WAN或LAN) 中其他客户端的可达性。GCC601X(W) 为IPv4和IPv6协议提供Ping和路由跟踪工具。



Ping/路由跟踪

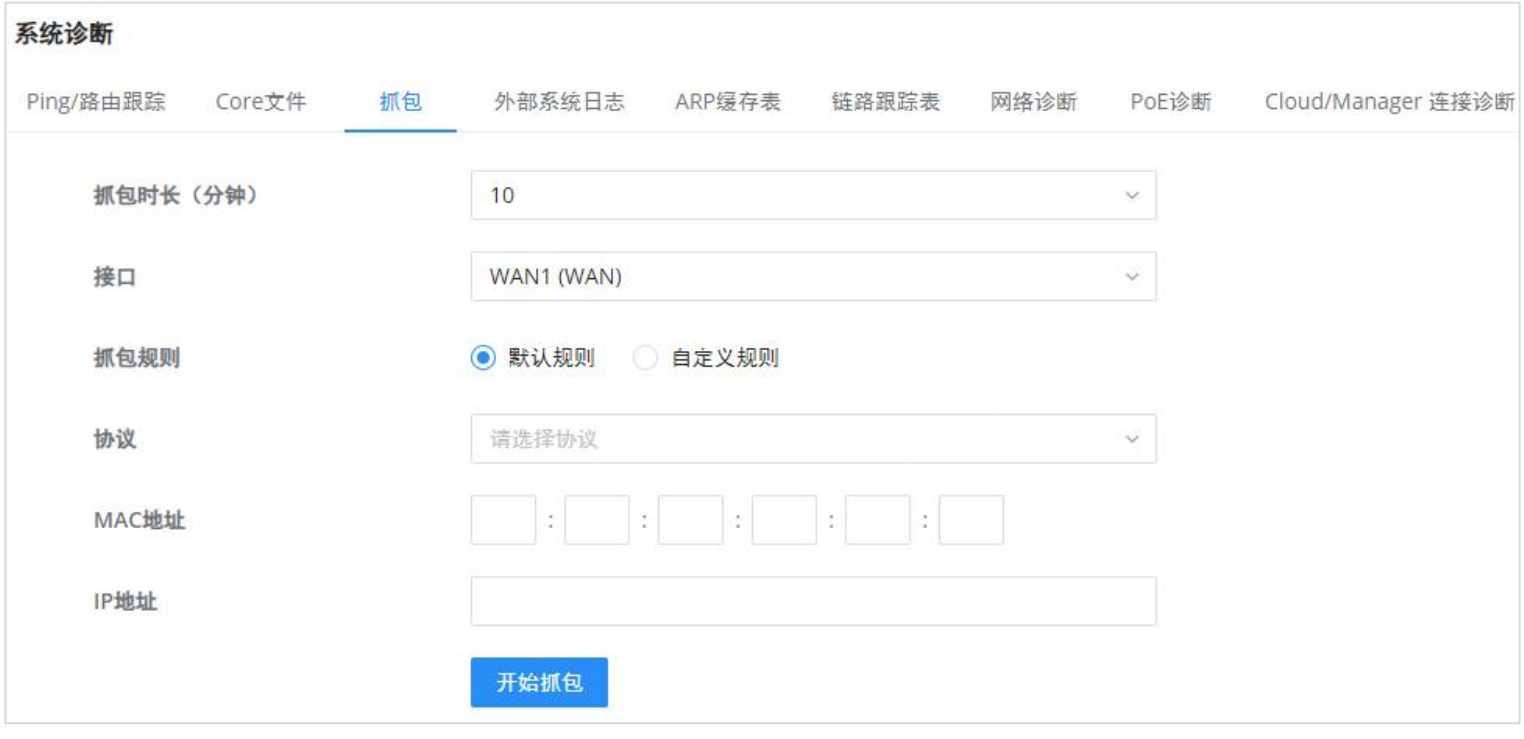
Core文件

当设备发生崩溃事件时，它会自动生成一个Core转储文件，项目团队可以将其用于调试目的。

Core文件

抓包

此部分用于从GCC601X(W) 接口（WAN端口和网络组）抓包数据包跟踪，以进行故障排除或监控。甚至可以根据MAC地址或IP地址进行抓包，一旦完成，用户可以点击 开始抓包 ，文件（CAP）将立即开始下载。



抓包

外部系统日志

GCC601X(W) 支持将系统日志信息转储到Web GUI下的远程服务器 → 系统设置 → 系统诊断 → 外部系统日志选项卡

输入系统日志服务器主机名或IP地址，并选择系统日志信息的级别。九个级别的系统日志可用：无、紧急、告警、严重、错误、警告、通知、信息和调试。

外部系统日志

ARP缓存表

GCC601X(W) 保留从GCC601X(W) 分配了一个IP地址的所有设备的ARP表记录。当设备离线时，记录将保留设备的信息。要访问ARP缓存表，请导航到系统诊断 → ARP缓存表。

ARP缓存表

链路跟踪表

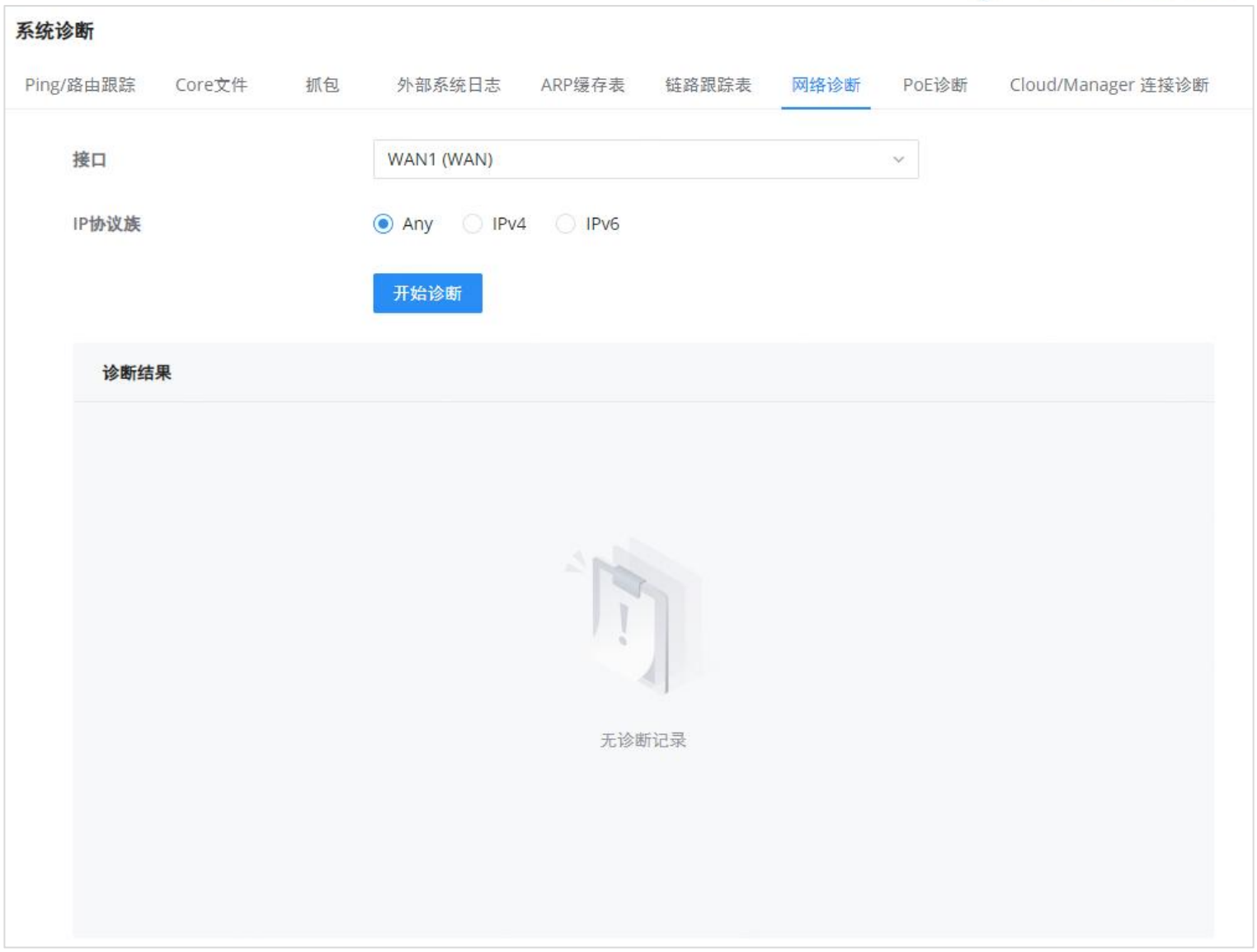
链路跟踪表通过显示源IP地址/端口（绿色）和回复IP地址/端口（蓝色）来显示流量流，还可以显示其他信息，如IP协议族、协议类型、使用期限、状态、数据包/字节等。

用户/管理员还可以删除某些IP地址/端口（源和目的）的流，或者单击“删除” 按钮以清除链接跟踪统计信息。

链路跟踪表

网络诊断

网络诊断功能允许用户快速诊断特定WAN接口上的连接链路。



网络诊断

PoE诊断

PoE诊断页面提供有关端口及其组件以及使用的功率和温度的见解。当用户遇到GCC601X(W) 的PoE功能的问题时，所提供的信息可能是有用的。

> **注意**
>
> GCC6010W不支持 PoE.

云/管理器连接诊断

将GCC601x(W) 设备添加到GDMS Networking或GWN Manager时，用户可以检查连接状态（已连接或未连接），甚至可以诊断问题。

告警和通知

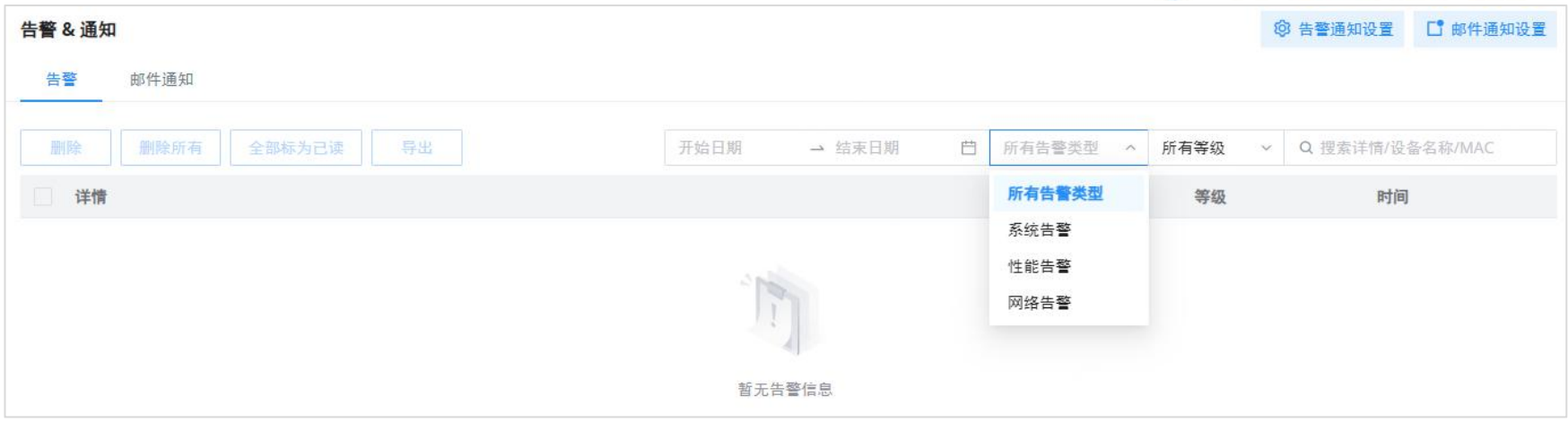
告警

告警页面显示有关网络的告警，用户可以指定仅显示某些类型，如（系统、性能、安全性或网络）或级别。要检查已生成的告警，请导航至维护 → 告警和通知 → 告警页面。

告警可以按类型或级别显示。然而，这不是显示它们的唯一方法。用户可以使用日期间隔或按MAC地址或设备名称搜索告警日志进行过滤。

告警类型

可用的类型是系统、性能、安全性和网络，或者用户可以选择显示所有类型。



告警类型

告警级别

用户可以按以下级别过滤告警级别：所有级别，紧急情况，警告或通知。

告警级别

告警通知设置

要启用告警选项卡上的通知，请单击 “告警通知设置” 按钮，如下所示：

告警通知设置

下图显示了用户可以在 “告警” 选项卡上启用的所有可能的告警通知，分为：系统告警、性能告警和网络告警。

请参考以下页面：

告警通知设置-系统告警

告警通知设置-性能告警

告警通知设置-网络告警

邮件通知

在此选项卡上，用户可以设置将接收通知的电子邮件，启用该功能后，用户可以添加多个接收者电子邮件地址。参考下图:

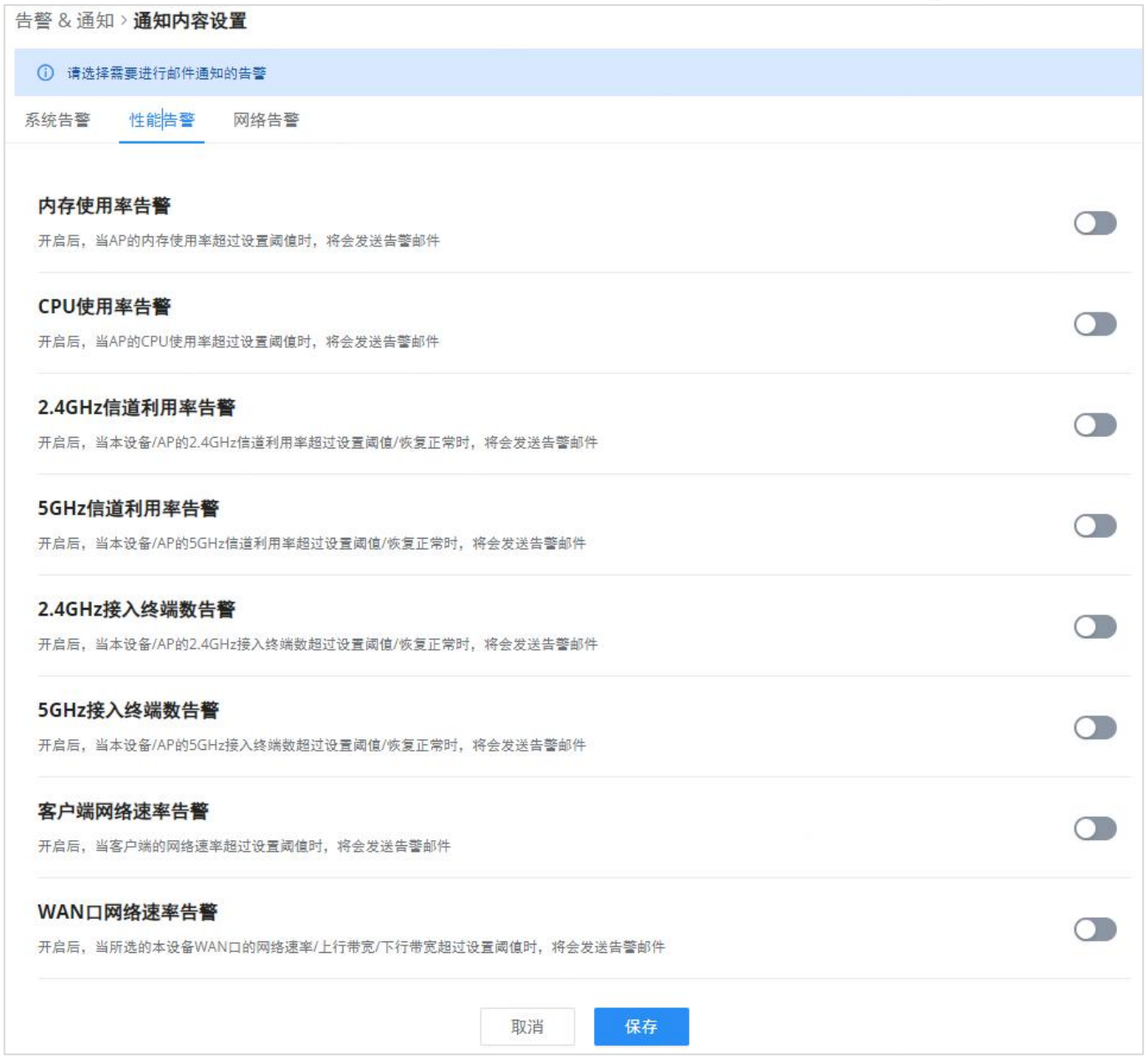
告警-电子邮件通知

- 单击 “减号” 图标以删除接收者的电子邮件地址。
- 单击 “加号” 图标以添加接收者的电子邮件地址。

邮件通知设置

下图显示了用户可以发送到预配置的接收者电子邮件地址的所有可能的电子邮件通知：

邮件通知设置-系统告警



邮件通知设置-性能告警

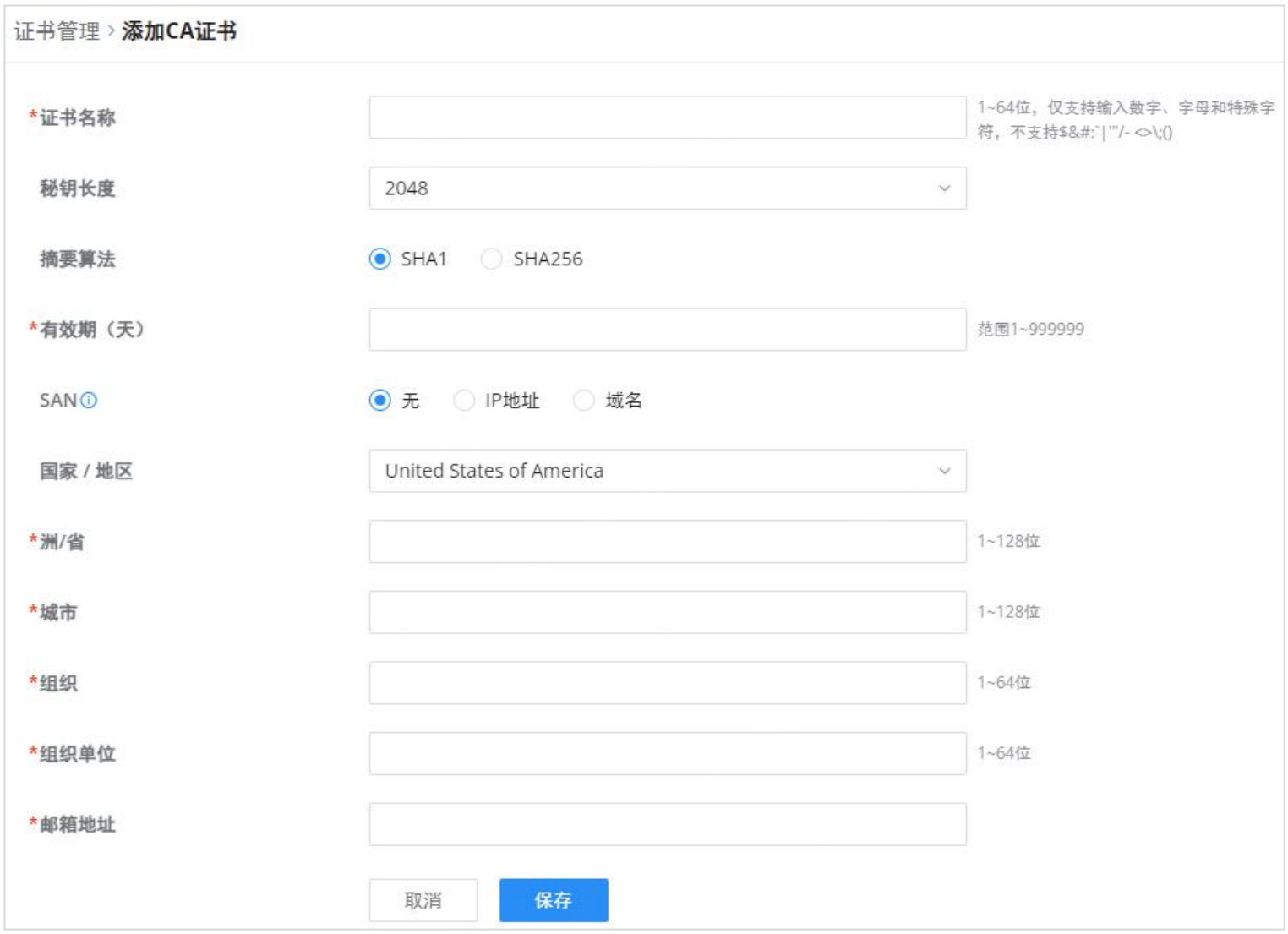
电子邮件通知设置-网络告警

系统设置

证书管理

CA证书

在此部分，用户可以创建CA证书当连接到在设备上创建的VPN服务器时，此证书将对用户进行身份验证。这种身份验证将确保没有身份被篡夺，并且交换的数据保持机密。要创建证书，请访问GCC的Web GUI并访问系统设置 → 证书 → CA证书，然后单击“添加” 并填写必要的信息。



添加CA证书

证书名称	输入CA的证书名称。 *注意：它可以是任何名称来标识此证书示例：“CATest”。*
密钥长度	选择用于生成CA 证书的密钥长度。 以下值可用： ● 512：512位密钥不安全，最好避免此选项。 ● 1024：1024位密钥不再具有足够的防攻击能力。 ● 2048：2048位密钥是一个很好的最小值。(推荐)。 ● 4096：几乎所有RSA系统都接受4096位密钥。使用4096位密钥将大大增加生成时间、TLS握手延迟和TLS操作的CPU使用率。
摘要算法	选择摘要算法： ● SHA1：这个摘要算法提供了一个基于任意长度输入的160位 fi 指纹输出。 ● SHA256：这个摘要算法生成一个几乎唯一的、固定大小的256位哈希。 *注意：哈希是一个单向函数，它不能被解密回来。*
有效期（天）	输入CA 证书的有效日期（天）。 *有效范围为1 ~ 999999。*

SAN	选择主体备用名称。选项： ● 无 ● IP地址 ● 域名
国家/地区	从下拉列表中选择国家代码。 *例如：“中国”。*
州/省	输入州名或省。 *例如：“浙江”。*
城市	输入城市名称。 *例如：“杭州”。*
组织	输入组织的名称。 *例如：“GS”。*
组织单位	此字段是提出请求的部门或组织单位的名称。 *例如：“GS销售”。*
邮箱地址	输入邮箱地址。 *示例：“EMEAregion@grandstream.com”*

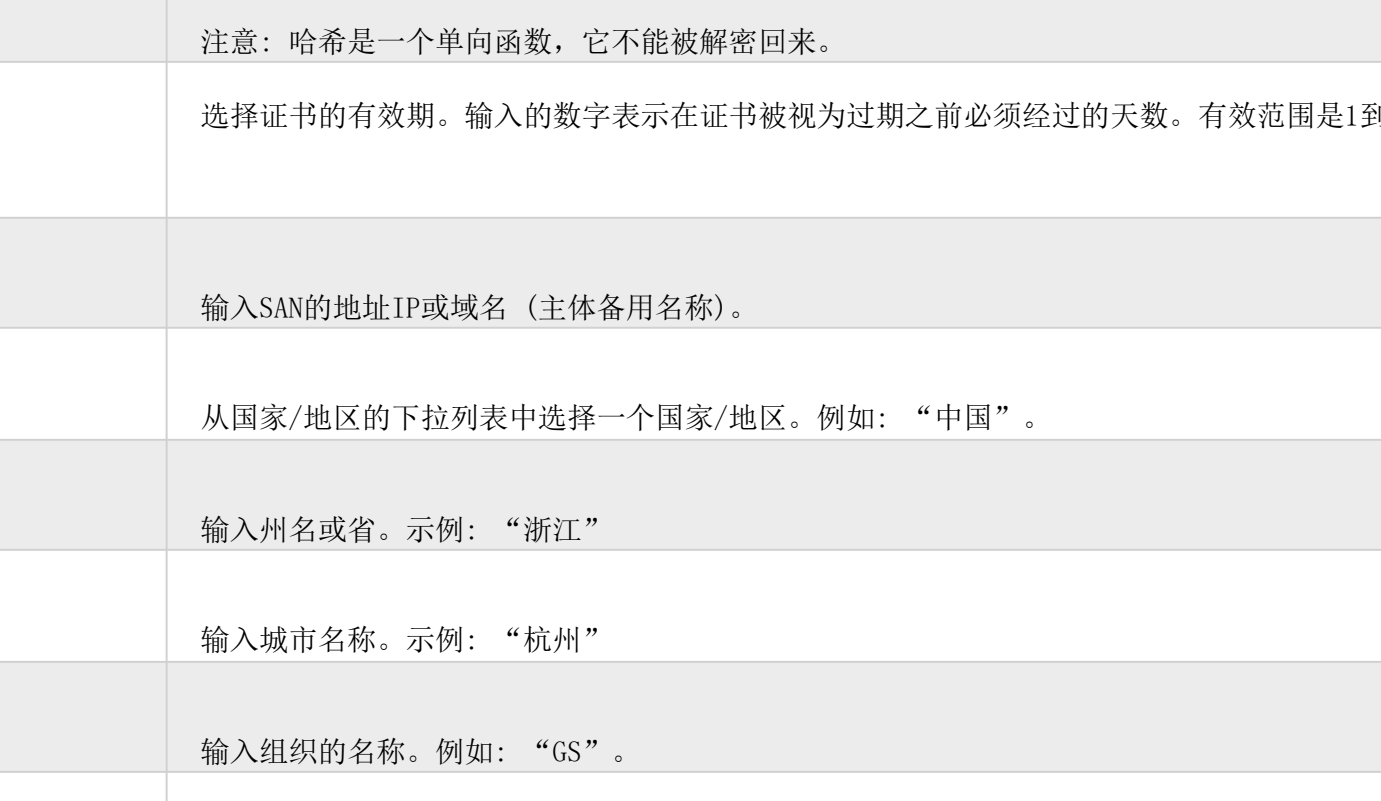
添加CA证书

证书

在此部分中，用户可以创建服务器或客户端证书要创建证书，请访问设备的Web UI，然后导航到系统设置 → 证书 → 添加证书，单击 “添加”，然后输入有关证书的必要信息。

添加证书

证书名称	输入证书的名称。
CA 证书	选择CA证书。
密钥长度	选择用于生成CA证书的密钥长度。以下值可用: ● 512：512位密钥不安全，最好避免此选项。 ● 1024：1024位密钥不再具有足够的防攻击能力。 ● 2048：2048位密钥是一个很好的最小值。(推荐)。 ● 4096：几乎所有RSA系统都接受4096位密钥。使用4096位密钥将大大增加生成时间、TLS握手延迟和TLS操作的CPU使用率。
摘要算法	选择摘要算法。 ● SHA1：这个摘要算法提供了一个基于任意长度输入的160位 fi 指纹输出。 ● SHA256：这个摘要算法生成一个几乎唯一的、固定大小的256位哈希。 注意：哈希是一个单向函数，它不能被解密回来。
有效期（天）	选择证书的有效期。输入的数字表示在证书被视为过期之前必须经过的天数。有效范围是1到999999。
SAN	输入SAN的地址IP或域名（主体备用名称)。
国家/地区	从国家/地区的下拉列表中选择一个国家/地区。例如：“中国”。
州/省	输入州名或省。示例：“浙江”
城市	输入城市名称。示例：“杭州”
组织机构	输入组织的名称。例如：“GS”。
组织单位	此字段是提出请求的部门或组织单位的名称。
邮箱地址	输入邮箱地址。 *示例：“EMEAregion@grandstream.com”*



备份证书

文件共享

文件共享

RADIUS

RADIUS是一种分布式的客户端/服务器信息交换协议，可以保护网络免受未经授权的访问。它通常用于需要高安全性并允许远程用户访问它的各种网络环境。该协议定义了基于UDP的RADIUS数据包格式及其传输机制，并将目的UDP端口1812和1813分别指定为默认的身份验证和计费端口号。

RADIUS通过认证和授权提供接入服务，并通过计费收集和记录用户对网络资源的使用情况。RADIUS协议的主要特点是客户端/服务器模式、安全的消息交换机制和良好的可扩展性。

要将RADIUS添加到GCC网络模块，请导航到网络 → 系统设置 → RADIUS，然后单击“添加” 按钮添加新的RADIUS。

注意:

可以添加多个RADIUS。

添加RADIUS

名称	定义 RADIUS服务器的名称

认证服务器	RADIUS中的“认证服务器”设置了在网络访问尝试期间负责验证用户凭据的服务器。认证服务器将按照显示的顺序(从上到下)使用，RADIUS服务器将在这些认证服务器之后使用，您可以在认证服务器中定义服务器地址、端口号和秘钥，最多可以定义两个认证服务器。
RADIUS计费服务器	RADIUS计费服务器指定负责记录和跟踪用户网络使用数据的服务器。最多可以定义两个RADIUS计费服务器
RADIUS NAS ID	配置最多48个字符的RADIUS NAS ID。支持字母数字字符，特殊字符 ″~!@ # ¥ % & * () -+ =_″ 和空格
最大重传次数	设置尝试向RADIUS服务器发送数据包的最大次数
重试超时时间（秒）	设置在重新发送RADIUS数据包之前等待RADIUS服务器响应的最长时间
计费更新时长（秒）	设置向RADIUS服务器发送计费更新的频率，单位为秒。输入数字30 ~ 604800。如果外部启动页面也配置了这个，那么其他值将具有优先级。

添加RADIUS