RG-NBS 系列交换机

ReyeeOS 1.84 版本 Web 管理手册

文档版本 V1.0

归档日期 2022-06-02

版权声明

免责声明

您所购买的产品、服务或特性等应受商业合同和条款的约束，本文档中描述的部分或全部产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，锐捷网络对本文档内容不做任何明示或默示的声明或保证。

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。锐捷网络保留在没有任何通知或者提示的情况下对文档内容进行修改的权利。

本手册仅作为使用指导。锐捷网络在编写本手册时已尽力保证其内容准确可靠，但并不确保手册内容完全没有错误或遗漏，本手册中的所有信息也不构成任何明示或暗示的担保。

前　言

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

- 锐捷睿易官方网站：https://www.ruijiery.com/
- 锐捷睿易在线客服：https://ocs.ruijie.com.cn/?p=smb
- 锐捷网络官方网站服务与支持版块：https://www.ruijie.com.cn/service.aspx
- 7天无休技术服务热线：4001-000-078
- 锐捷睿易技术论坛：http://bbs.ruijiery.com/
- 常见问题搜索：https://www.ruijie.com.cn/service/know.aspx
- 锐捷睿易技术支持与反馈信箱：4001000078@ruijie.com.cn
- 锐捷网络文档支持与反馈信箱：doc@ruijie.com.cn
- 锐捷网络服务公众号：【锐捷服务】扫码关注

本书约定

1. 图形界面格式约定

界面图标	解释	举例
<>	按钮	<确定>
[]	菜单项，弹窗名称，页面名称，标签页的名称	菜单项“系统设置”可简化[系统设置]
>>	分级页面，子菜单项	选择[系统设置]>>[系统管理员]
“”	配置项，提示信息，链接	如提示框提示“保存配置成功” 点击“开启”选项 点击“忘记密码”链接

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告

表示用户必须严格遵守的规则。如果忽视此类信息，可能导致数据丢失或设备损坏。

注意

表示用户必须了解的重要信息。如果忽视此类信息，可能导致功能失效或性能降低。

说明

用于提供补充、申明、提示等。如果忽视此类信息，不会导致严重后果。

产品/版本支持情况

用于提供产品或版本支持情况的说明。

3. 说明

本手册重在介绍产品的特点以及使用方法，指导用户对设备进行配置和试用。

目 录

1 概述

本章节说明使用 Eweb 管理系统的方法，您可以使用 Eweb 管理系统来管理您的交换机设备。

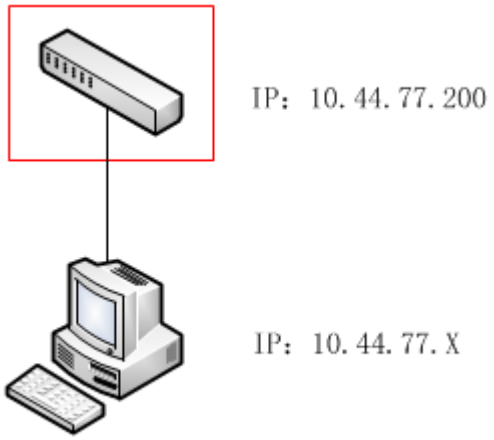
用户使用浏览器如（如 Chrome）访问 Eweb 管理系统来管理交换机设备。

2 配置指南

2.1 准备配置

2.1.1 连接设备

如下图所示，用户 PC 可通过网线连接交换机设备，通过浏览器访问设备的 Eweb 管理系统，对设备进行管理和配置



说明

图中红框内设备为被访问的交换机设备，为管理计算机配置一个与设备IP在同一网段的IP地址，确保PC能够Ping通该交换机设备就可以访问其Eweb管理系统。

2.1.2 配置环境要求

客户端的要求：

- 用户使用 Web 浏览器登录到交换机内置 Web 管理界面，对设备进行管理。客户端通常是指 PC，也可能是一些其它的移动终端设备，如笔记本电脑等。
- 浏览器：支持 Chrome（谷歌浏览器）、火狐浏览器、IE9.0、IE10.0、IE11.0、以及部分基于谷歌内核的浏览器（如 360 浏览器的极速模式）。使用其它浏览器登录 Web 管理时，可能出现乱码或格式错误等异常。如果目前使用的是 IE6、IE7、IE8 浏览器，请升级到 IE10、IE11，或使用 Chrome、FF 等更标准浏览器。
- 分辨率：建议分辨率设置为 1024*768 或以上像素。在其它分辨率下，页面字体和格式可能出现不对齐、不够美观等异常。

2.2 进入 Eweb 管理界面

在浏览器地址栏中输入交换机设备的 IP 地址（设备默认 IP 为 10.44.77.200）。PC 的当前 IP 地址必须与交换机设备的 IP 地址处在同一网段。

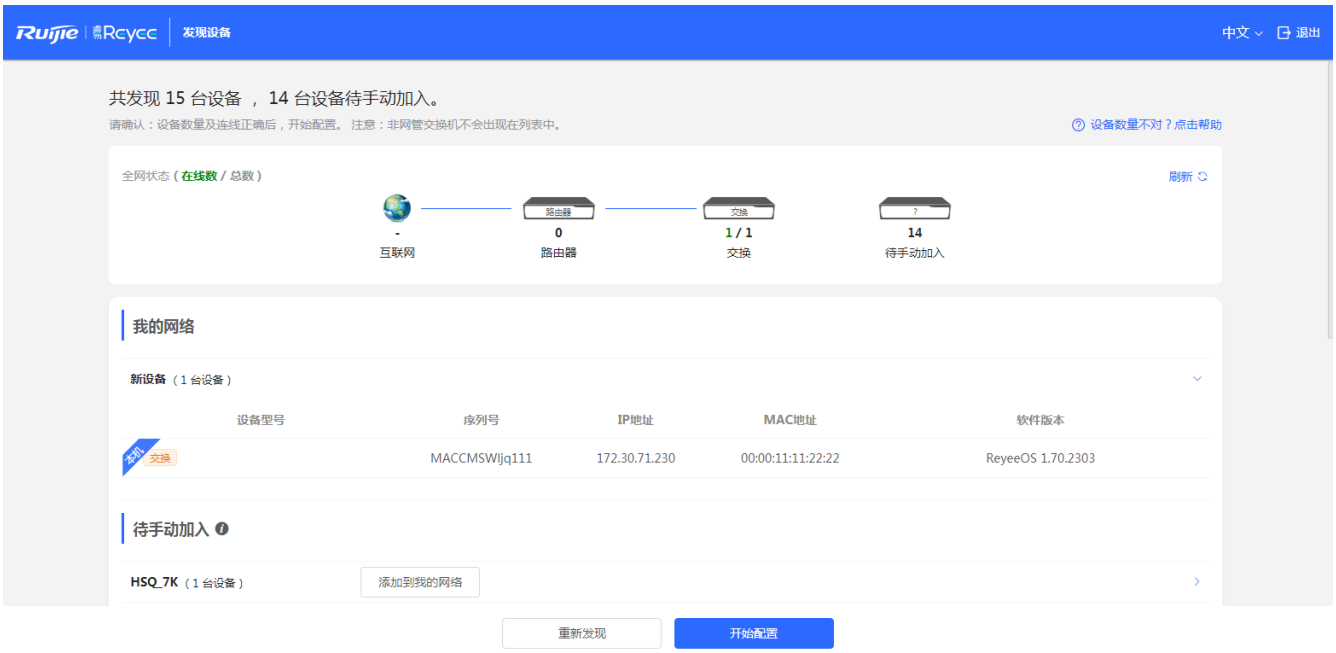
输入密码后点击<登录>按钮，进入设备管理首页。如果忘记了密码，请点击<忘记密码>，按照页面提示进行恢复出厂操作。

说明

1. 设备默认的管理IP（Eweb管理地址）为10.44.77.200。
2. 当用户设置过静态IP地址或者动态获取到新的IP地址，可以使用新的IP地址访问设备的Eweb管理系统。
3. 默认情况下，Eweb管理系统没有配置密码，用户可以直接登录设备进行配置和管理。
4. 强烈建议用户在登录Eweb管理系统后，设置管理密码，设置密码后，再次登录Eweb管理系统需要输入密码才能访问。

2.3 快速配置

首次登录（初次配置）Eweb 管理系统时，需要进行设备的快速配置（配置设备的网络名称、管理密码及管理 IP）。如果已经设置过密码，忽略这一步。



确认当前网络中的设备，点击<开始配置>。

“项目名称”标识设备所在的网络（首次使用时需要用户输入）。

“管理密码”为设备登录 Eweb 时的登录密码（请勿忘记，仔细保存，若忘记请参见 4.2 忘记密码和恢复出厂配置）。

“上网方式”配置设备的上网方式，分为动态 IP（由上联 DHCP 服务器分配 IP 地址）和静态 IP 方式（用户手动输入指定的 IP 地址、子网掩码、网关 IP 地址和 DNS 地址等）。

点击<创建项目并连通网络>，设备将自动完成设备配置的下发并初始化相关配置。

点击右上角<退出>，根据提示指引，设备将跳过快速配置进入设备配置管理系统。

2.4 Eweb 界面简介

设备工作模式分为**独立模式**和**组网模式**两种模式，出厂配置下设备默认为**组网模式**。系统根据工作模式呈现不同的菜单项。

2.4.1 组网模式下的 Eweb 页面

组网模式下，除了能够对当前登录设备进行配置和管理，还可以对网络中的其他设备进行配置与维护。

2.4.1.1 整网信息区

组网模式下，Eweb 管理首页的左半部分为“整网信息区”，可在该区域内查看整网设备的桥接状态，并修改整网配置。也可以快捷修改某台设备的配置。

2.4.1.2 交换机配置

组网模式下，在[整网概览]页面选择当前登录的设备，点击<配置>可进入到交换机的配置界面：

2.4.2 独立模式下的 Eweb 页面

独立模式下，仅支持对当前登录设备进行配置和管理。

2.4.3 切换工作模式

设备工作模式分为**独立模式**和**组网模式**两种模式，出厂配置下设备默认为**组网模式。**

1. 组网模式下，在[整网概览]页面点击<配置>进入交换机配置页面（独立模式可忽略该步骤）。
2. 在[首页]->[基本信息]处点击工作模式，选择是否开启自组网发现，并点击<切换模式>，切换设备的工作模式。

说明

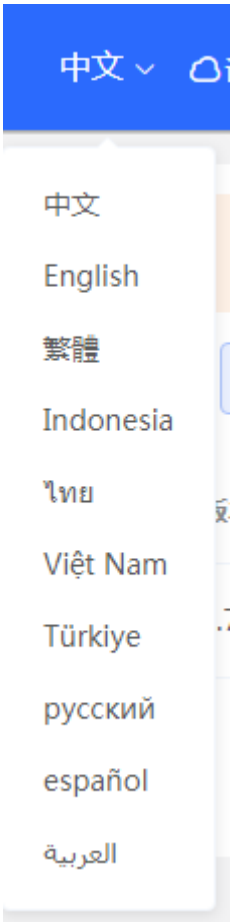
1. 设备切换完模式，浏览器会刷新页面。
2. 模式切换后，设备IP可能发生改变，需要修改终端地址，使终端Ping通设备，并在浏览器输入新地址重新访问Eweb系统。

2.4.4 头部导航栏

左侧依次为设备 LOGO、设备网络名称及设备名称，右侧显示设备快捷链接（包括“语言切换”、“诺客云端运维”、“下载 APP”、“快速配置/全网配置”、“退出”）。

2.4.4.1 语言切换

点击<中文>，选择对应语言，可以切换 Eweb 的显示语言，目前支持多种语言。



2.4.4.2 诺客云运维

鼠标移入<诺客云端运维>，下方显示诺客云 Web 链接及诺客云管理小程序二维码。

2.4.4.3 下载 APP

鼠标移入<下载 APP>，下方显示 APP 下载链接二维码，扫描二维码即可下载 APP 进行移动端配置。

2.4.4.4 全网配置

鼠标移入<全网配置>，会跳转到全网配置界面，在全网配置界面可以看到设备同一网段下的其它交换设备，可以把其它交换设备加入到你的项目网络中来集中管理。

2.4.4.5 退出

点击退出按钮，即可退出登录。如果您在公共电脑上操作，建议操作后，及时退出登录。

说明

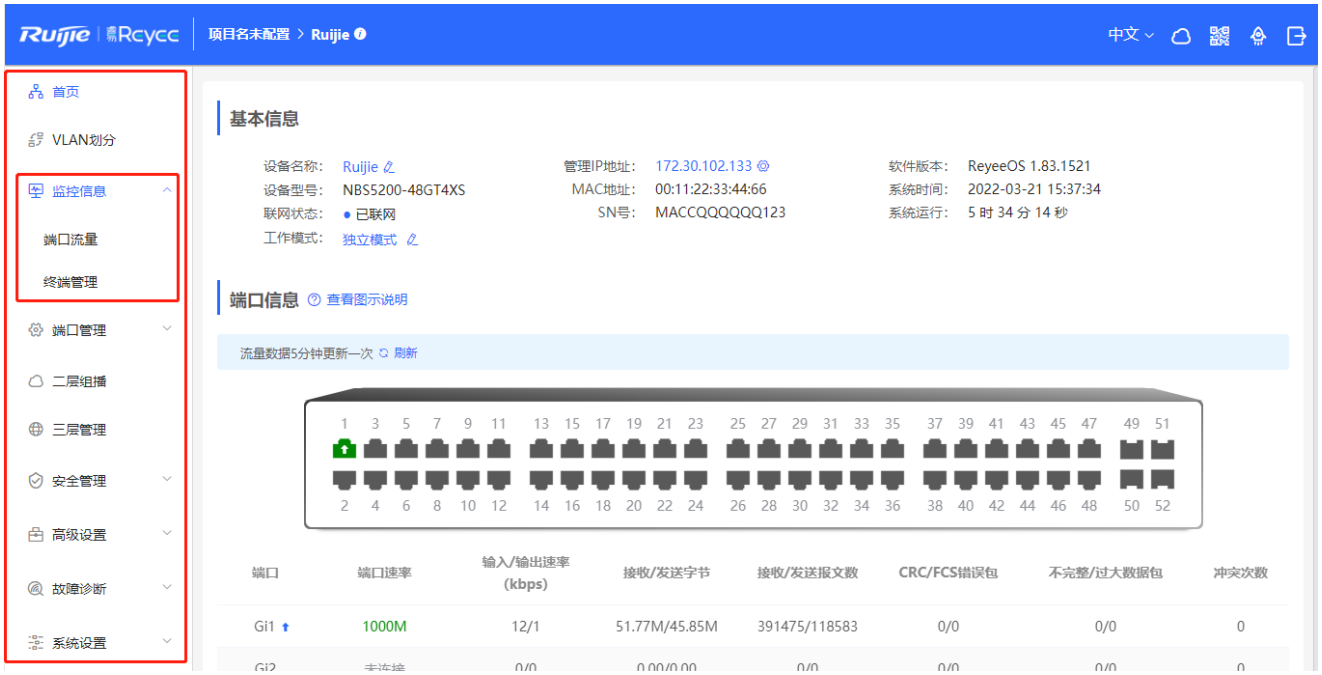
若不退出登录，用户可以在Web会话超时时间（默认为1小时）内在当前浏览器上免验证继续访问Eweb系统，直至当前会话超时后需要重新登录。Web会话超时时间的设置步骤请参见3.10.2 登录管理。

2.4.5 菜单导航区

Eweb 管理页面设有“功能菜单导航”区域（独立模式下位于 Eweb 页面左侧，组网模式下位于交换机配置页面），该区域列出了交换机的所有功能列表。点击相应菜单可打开详细的设置页面。

菜单的组织方式分为二级，当点击含有二级菜单的菜单项时，会显示出对应的二级菜单。如点击[监控信息]后将展开[端口流量]和[终端管理]子菜单项。

独立模式：


Ruijie | Rcycc
项目名未配置 > Ruijie
中文
首页
VLAN划分
监控信息
端口流量
终端管理
端口管理
二层组播
三层管理
安全管理
高级设置
故障诊断
系统设置
基本信息
设备名称： Ruijie
设备型号： NBS5200-48GT4XS
联网状态： 已联网
工作模式： 独立模式
管理IP地址： 172.30.102.133
MAC地址： 00:11:22:33:44:66
SN号： MACCQQQQQQ123
软件版本： ReyeeOS 1.83.1521
系统时间： 2022-03-21 15:37:34
系统运行： 5 时 34 分 14 秒
端口信息
查看图示说明
流量数据5分钟更新一次
刷新
端口
端口速率
输入/输出速率 (kbps)
接收/发送字节
接收/发送报文数
CRC/FCS错误包
不完整/过大数据包
冲突次数
Gi1
1000M
12/1
51.77M/45.85M
391475/118583
0/0
0/0
0

组网模式：


Ruijie | Rcycc
项目名未配置 > Ruijie [从]
中文
交换
NBS5200-48GT4XS
名称： Ruijie
MAC地址： 00:11:22:33:44:66
DNS： 192.168.5.28,172.30.44.20
SN号： MACCQQQQQQ123
软件版本： ReyeeOS 1.83.1521
IP地址： 172.30.102.133
硬件版本： 1.00
重启
首页
VLAN划分
监控信息
端口管理
二层组播
三层管理
安全管理
高级设置
故障诊断
系统设置
端口流量
终端管理
基本信息
设备名称： Ruijie
设备型号： NBS5200-48GT4XS
联网状态： 已联网
主设备地址：
工作模式： 组网模式
管理IP地址： 172.30.102.133
MAC地址： 00:11:22:33:44:66
SN号： MACCQQQQQQ123
软件版本： ReyeeOS 1.83.1521
系统时间： 2022-03-21 15:35:59
系统运行： 5 时 32 分 39 秒

3 Eweb 配置（独立模式）

3.1 首页

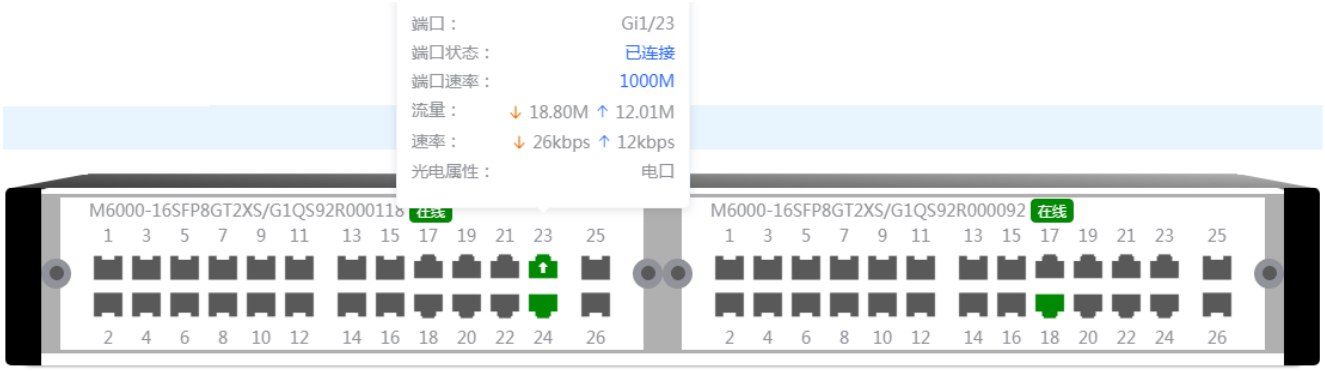
首页显示设备整机的基本信息及交换机端口的详细信息，如下图：

“基本信息”中可以配置设备名称、设备管理 IP 以及切换设备工作模式（请参见 2.4.3 切换工作模式）；

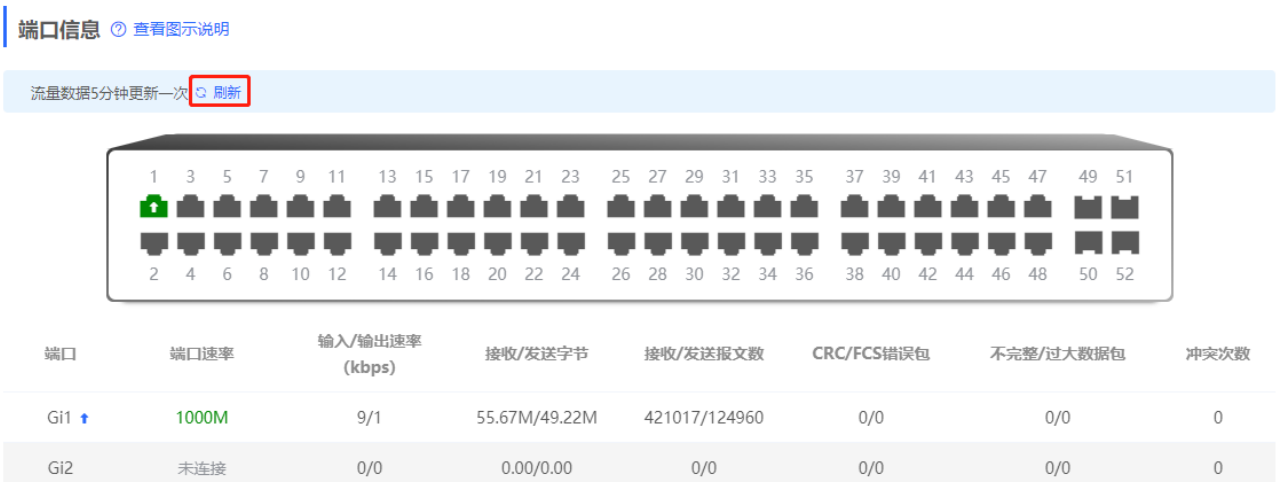
“智能监控”显示设备当前的硬件工作状态，如设备温度、电源状态等（部分设备拥有此功能）；

“端口信息”展示交换机当前所有端口的详细信息，点击<查看图示说明>，查看端口各个状态所对应的图标颜色及类别：

鼠标移入端口面板中的端口（如 Gi1/23）图标上，显示更多的端口信息，包括端口号、端口状态、端口速率、端口上下行流量与传输速率以及端口的光电属性等：



流量数据每 5 分钟自动更新一次，用户可以点击端口面板上方的<刷新]即时获取最新的端口流量及状态信息。



端口	端口速率	输入/输出速率(kbps)	接收/发送字节	接收/发送报文数	CRC/FCS错误包	不完整/过大数据包	冲突次数
Gi1	1000M	9/1	55.67M/49.22M	421017/124960	0/0	0/0	0
Gi2	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0

3.2 VLAN 划分

VLAN（Virtual Local Area Network，虚拟局域网）是在物理网络上划分出来的逻辑网络。除了无物理位置的限制，VLAN有着和普通物理网络同样的属性。每个VLAN具备独立广播域，不同VLAN之间是二层隔离的，二层的单播、广播和多播帧在一个VLAN内转发和扩散，而不会直接进入其它的VLAN之中。

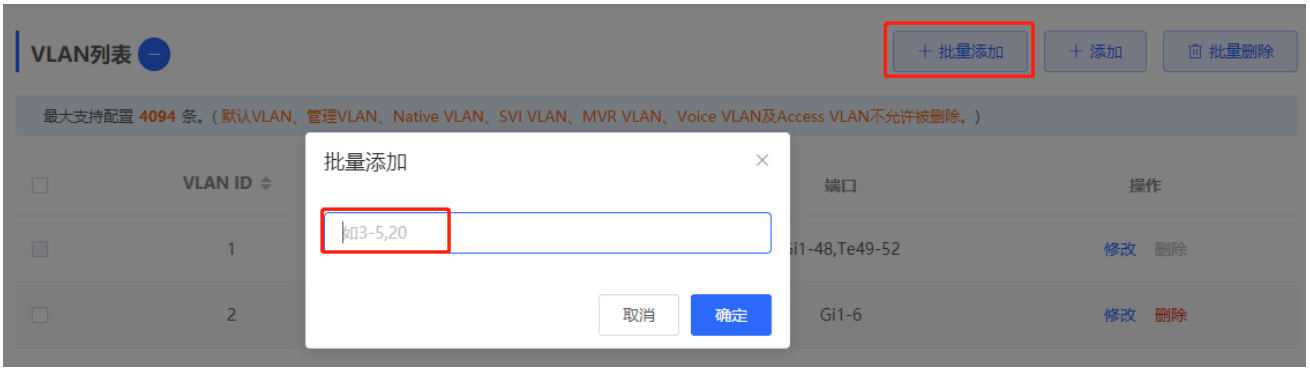
当把一个端口定义为一个VLAN的成员，所有连接到这个特定端口的终端都将是虚拟网络的一部分。整个网络支持多个VLAN。VLAN之间可以通过三层设备或三层接口实现三层通信。

Eweb系统中，VLAN划分包含VLAN列表（创建、删除、编辑VLAN）和端口列表（端口绑定VLAN）两部分功能。

3.2.1 VLAN 列表

➢ **添加VLAN：**

方法1：点击<批量添加>，在弹出框内输入单个VLAN ID或VLAN ID范围（多个VLAN ID范围以英文逗号分割），点击<确定>。VLAN添加成功后将显示在“VLAN列表”中。



方法2：点击<添加>，在弹出框内输入VLAN ID（必填）和VLAN描述，点击<确定>。VLAN添加成功后将显示在“VLAN列表”中。

➢ **删除VLAN：**

方法1：在“VLAN列表”中勾选多条记录，点击<批量删除>删除多条VLAN数据。

方法2：点击“VLAN列表”最后一列操作栏下的<删除>，在提示框中点击<确定>，提示“删除成功”表示完成删除。

➢ **编辑VLAN：**

点击“VLAN列表”最后一列操作栏下的<修改>，可以在弹出框中修改VLAN描述，点击<确定>，提示“修改成功”，完成编辑。

说明

1. VLAN ID范围为1~4094。
2. 默认VLAN（VLAN 1）、管理VLAN、Native VLAN及Access VLAN不允许被删除，<删除>按钮为灰色不可点击状态。
3. 批量添加的多个VLAN以‘,’英文逗号分隔，VLAN范围的起始ID与结束ID以‘-’中划线分隔。
4. 添加VLAN时，如果未配置描述信息，系统将会自动创建对应格式的VLAN描述，如：VLAN000XX。不同VLAN间VLAN描述不可重复。
5. VLAN项目较多时，进入VLAN划分页面的加载时间可能会增加，请耐心等待片刻。
6. 若设备支持三层功能，VLAN资源将与路由口和L3AP(三层聚合)功能共用，若VLAN不足，将提示“VLAN资源不足”。

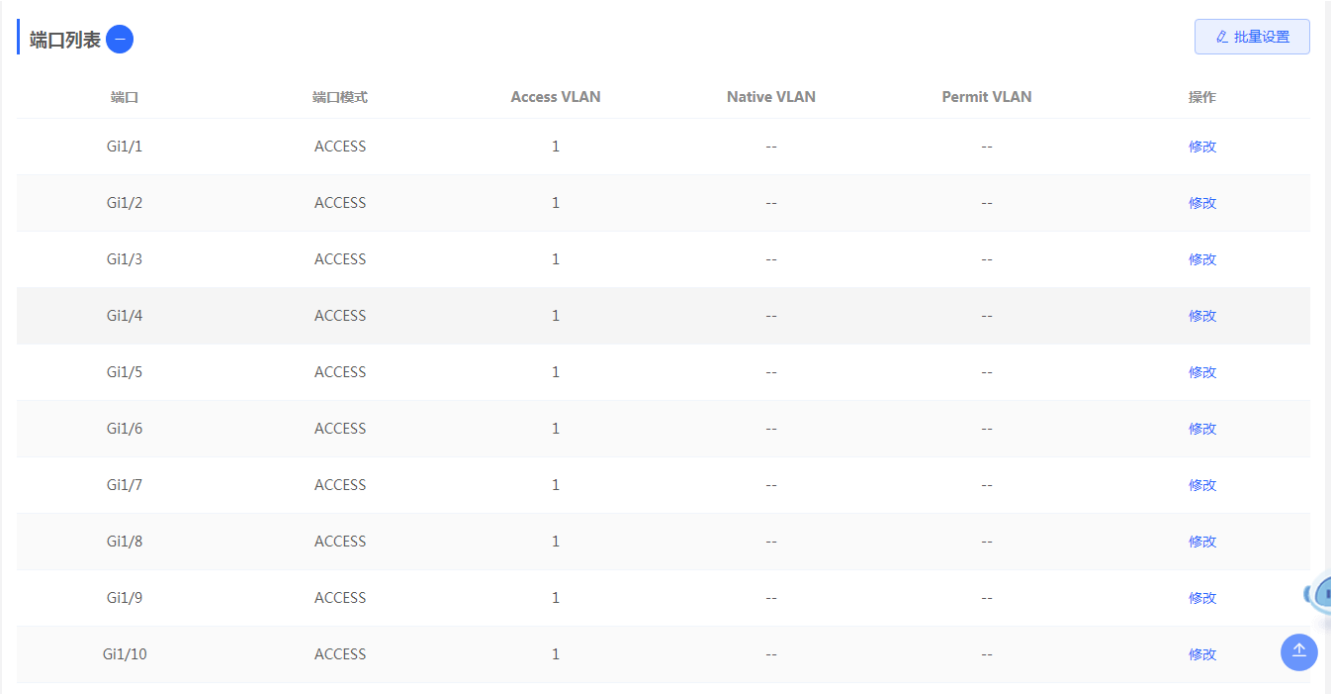
3.2.2 端口列表

可以通过配置一个端口的 VLAN 成员类型，来确定该端口允许通过的帧类型，以及该端口可以属于多少个 VLAN。VLAN 成员类型的详细说明见表 3-1 **VLAN 类型。**

表 3-1 VLAN 类型

端口类型	作用
Access 端口	一个 Access 口可以属于且仅属于一个 VLAN，只许可此 VLAN 的帧通过，此 VLAN 称为 Access VLAN
Trunk 端口（802.1Q）	一个 Trunk 口可以有一个 Native VLAN 和若干个许可 VLAN，Trunk 口转发 Native VLAN 的帧不携带 Tag，转发许可 VLAN 的帧携带 Tag 一个 Trunk 口，在缺省情况下是属于本设备所有 VLAN 的，它能够转发所有 VLAN 的帧。可以通过设置许可 VLAN 列表（Allowed-VLANs）来限制允许转发的 VLAN 帧

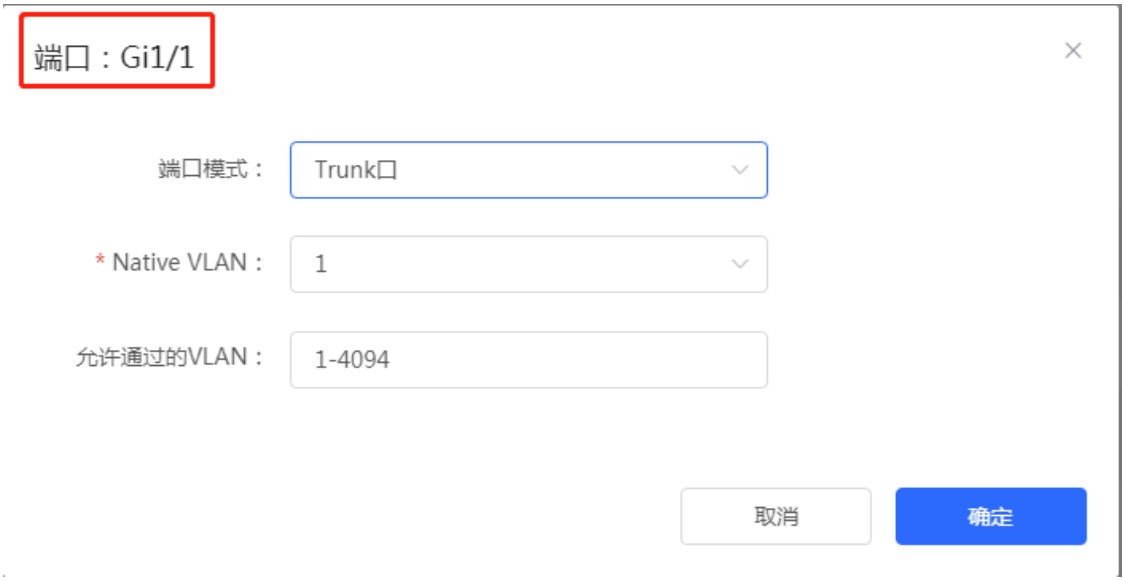
端口与 VLAN 关系的配置（支持批量配置和单个端口配置）：



- **设置和修改端口VLAN：**

方法 1：点击<批量设置>，弹出如下框。在端口图中选择需要配置的端口，并选择端口模式，若端口模式为 Access 口，设置 Access VLAN；若端口模式为 Trunk 口，设置 Native VLAN 和允许通过的 VLAN。点击<确定>，提示“配置成功”表示完成编辑。

方法 2：点击“端口列表”中指定端口最后一列操作栏下的<修改>，配置端口模式及对应 VLAN，点击<确定>。



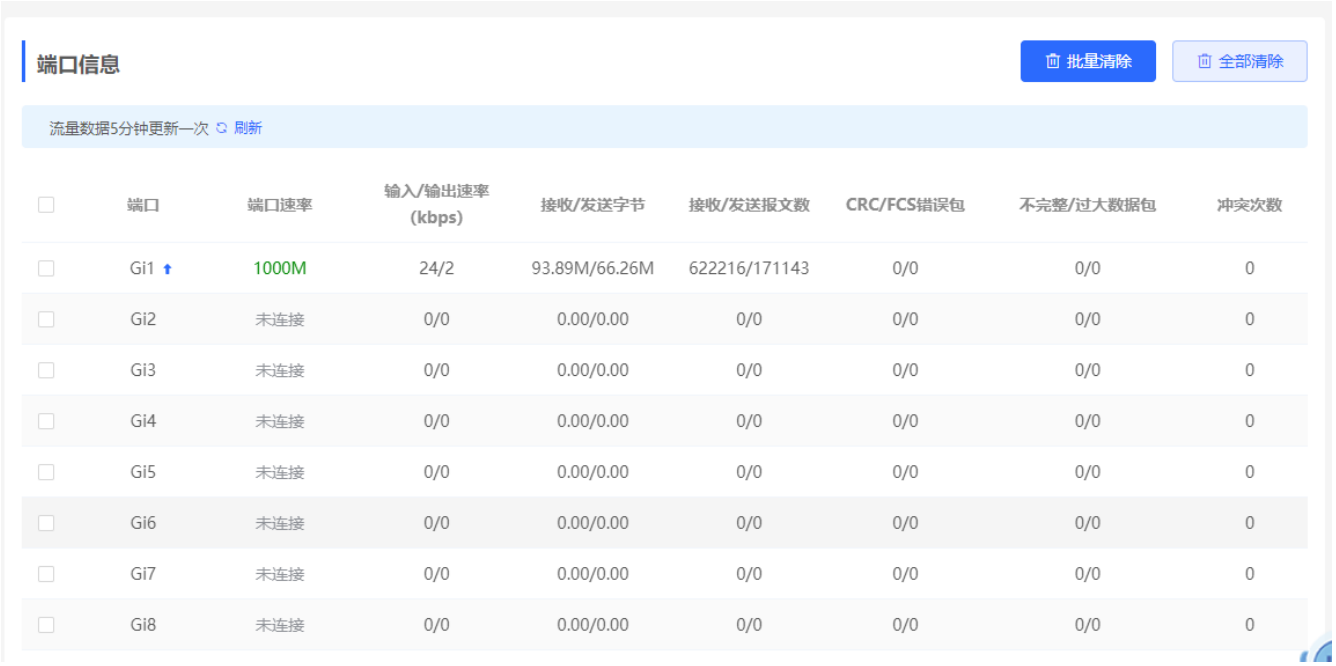
说明

1. 产品支持的VLAN遵循IEEE802.1Q标准，最多支持4094个VLAN（VLAN ID取值范围为1~4094），其中VLAN 1是不可删除的默认VLAN。
2. 许可VLAN的取值范围为1~4094。
3. 当硬件资源不足的情况下，系统将提示创建VLAN失败。
4. 端口VLAN配置不当（特别是上联口），可能造成无法访问Web，请谨慎配置。

3.3 监控信息

3.3.1 端口信息

显示设备端口的流量等数据信息：



勾选端口后点击<批量清除>或直接点击<全部清除>，可以清除当前端口流量等数据的统计信息，重新开始统计。

说明

1. “端口速率”每5秒更新一次数据，其他流量统计数据每5分钟自动更新一次数据。
2. 端口包含聚合口，聚合口流量为成员口流量的总和。

3.3.2 终端管理

3.3.2.1 功能概述

MAC 地址表记录了与该设备相连的设备的 MAC 地址、接口号以及所属的 VLAN ID。

设备在转发报文时通过报文的目的 MAC 地址以及报文所属的 VLAN ID 的信息在 MAC 地址表中查找相应的转发输出端口。根据 MAC 地址查找到转发出口后就可以采取单播、组播或广播的方式转发报文。

说明

本章节只涉及动态地址、静态地址与过滤地址的管理，组播地址的管理请参见3.5.3 IGMP Snooping。

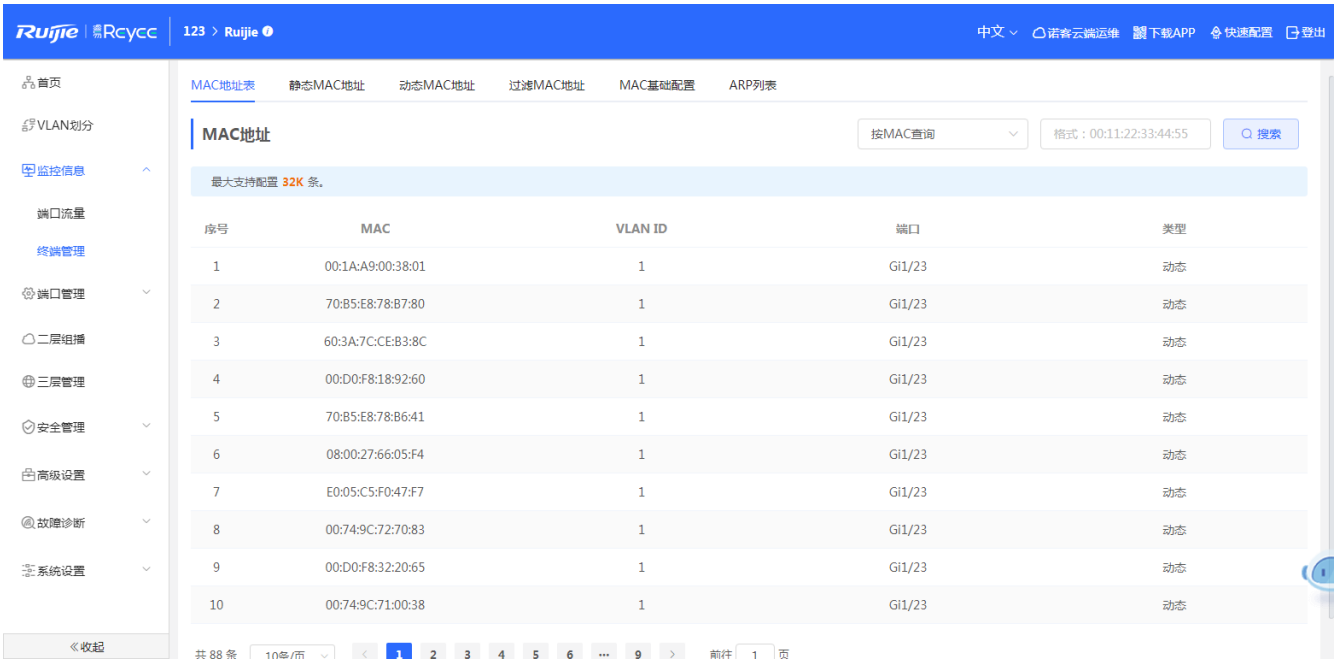
表 3-2 MAC 主要应用场景

功能	应用场景
动态地址学习	通过动态地址学习，实现报文单播转发。
MAC 地址变化通知	通过 MAC 地址添加删除通知，监控网络设备下用户变化。

终端管理包含 MAC 地址表、静态 MAC 地址、动态 MAC 地址、过滤 MAC 地址、MAC 基础配置和 ARP 列表业务。

3.3.2.2 MAC 地址表

显示设备学习到的MAC地址信息（包含静态和动态MAC信息）。



➢ **搜索：**

选择搜索类型（支持按MAC查询、按VLAN查询、按端口查询），输入搜索的字符串，点击<搜索>，列表过滤出符合搜索条件的MAC表项。

说明

1. MAC表项根据不同的设备具有不同的容量（例如示例图中设备MAC地址表容量为32K）。
2. 搜索功能支持模糊搜索。

3.3.2.3 静态 MAC 地址

交换机在转发数据时，需要根据MAC地址表来做出相应转发，用户可以通过设置静态MAC地址，手工绑定设备下接的网络设备的MAC地址与端口。添加一个静态地址后，当在VLAN中接收到目的地址为该地址的报文时，这个报文将被转发到指定的接口中。应用场景如：端口开启了802.1x认证，可以设置MAC绑定免认证。

可查看并手动配置网络设备的MAC地址与端口的关系。

➢ **添加静态地址：**

点击<添加>，在弹出的框中输入MAC地址及VLAN，选择所要转发的端口，点击<确定>。若添加成功，页面将提示“添加成功”，且列表将更新数据。

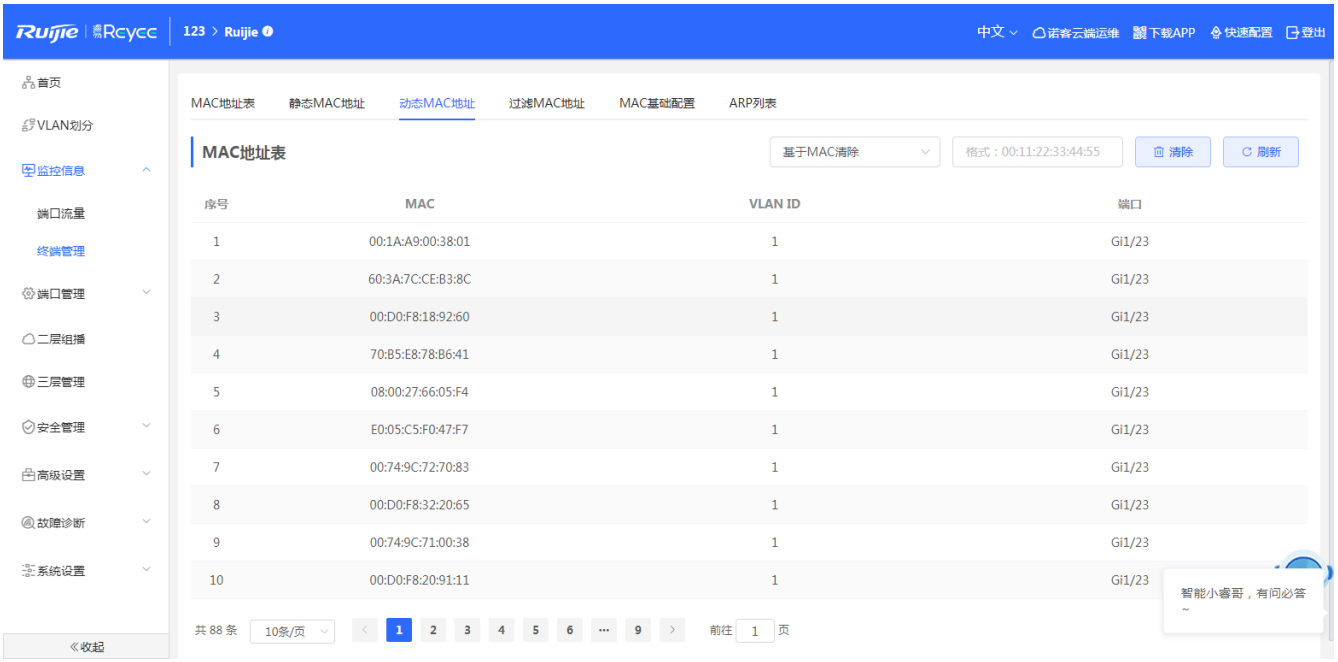
➢ **删除静态地址：**

方法1：在“MAC列表”中勾选需要删除的MAC项，点击<批量删除>，在确认框中点击<确定>。提示删除成功，列表更新数据。

方法2：点击“MAC列表”最后一列操作栏下的<删除>，提示“确定删除选中的MAC”，点击<确定>后提示“删除成功”，完成删除。

3.3.2.4 动态 MAC 地址

可查看设备学习到的动态MAC信息。



➢ **清除：**

选择清除类型（支持基于MAC、基于VLAN、基于端口的清除），输入与动态MAC地址表项进行匹配的字符串，点击<清除>，设备将清除符合条件的MAC表项。

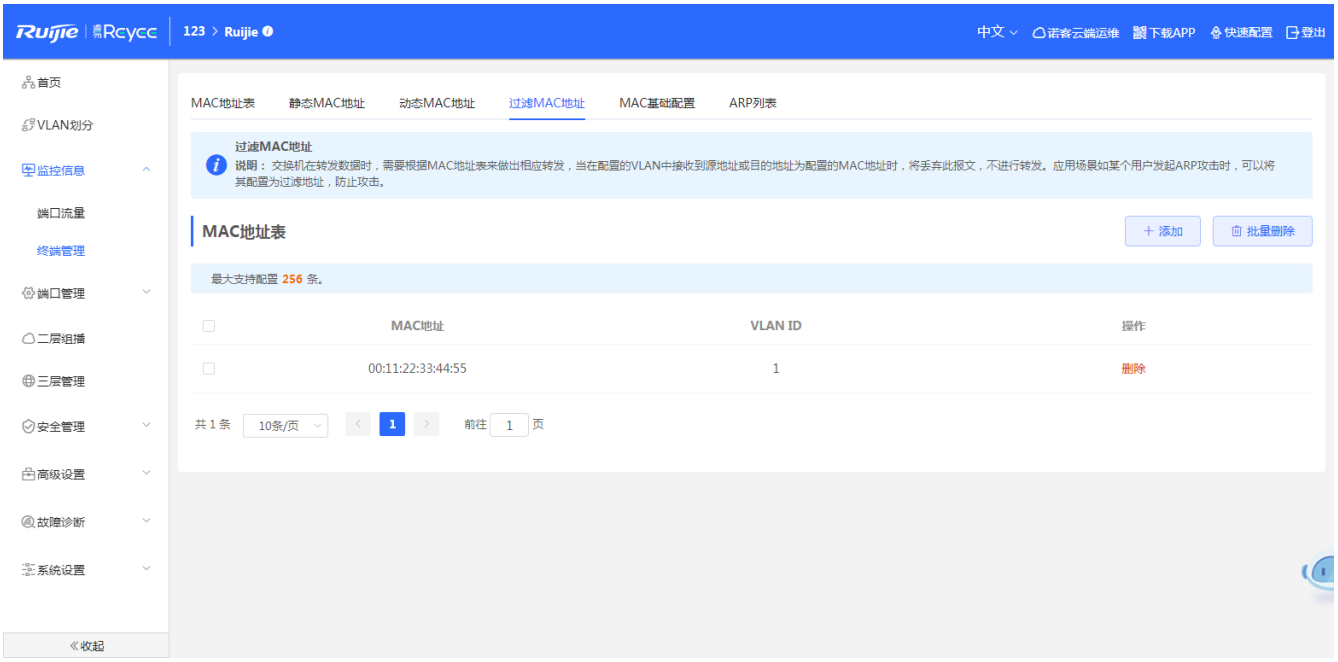
➢ **刷新：**

点击<刷新>可重新获取最新的动态MAC表项。

3.3.2.5 过滤 MAC 地址

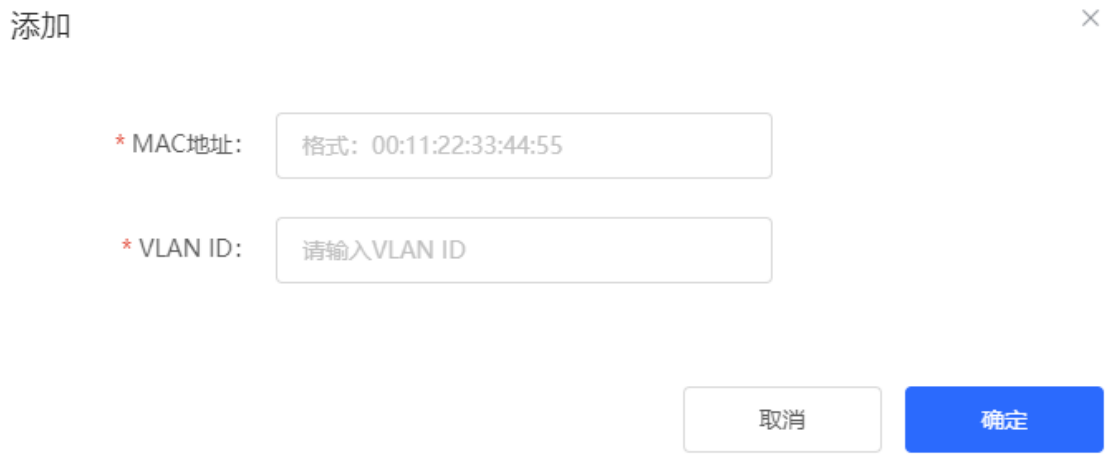
交换机在转发数据时，需要根据MAC地址表来做出相应转发，当在配置的VLAN中接收到源地址或目的地址为配置的过滤MAC地址时，将丢弃此报文，不进行转发。

用户可以手工配置设备下接的网络设备的MAC地址与设备VLAN的绑定关系，从而实现过滤符合该绑定关系的数据包。例如当某个用户发起ARP攻击时，可以将其配置为过滤地址，防止攻击。



➢ **添加过滤地址：**

点击<添加>，在弹出的框中输入MAC地址及VLAN，点击<确定>。提示“添加成功”，列表更新数据。



➢ **删除过滤地址：**

方法1：在“MAC列表”中勾选需要删除的MAC项，点击<批量删除>，在确认框中点击<确定>。提示删除成功，列表更新数据。

方法2：点击“MAC列表”最后一列操作栏下的<删除>，提示“确定删除选中的MAC”，点击<确定>。提示“删除成功”，完成删除。

3.3.2.6 MAC 基础配置

用于配置设备学习MAC表项的老化时间。

- **配置老化时间：**

  输入合法的老化时间，点击<保存>。提示“配置成功”表示成功修改设备MAC地址的老化时间。

说明

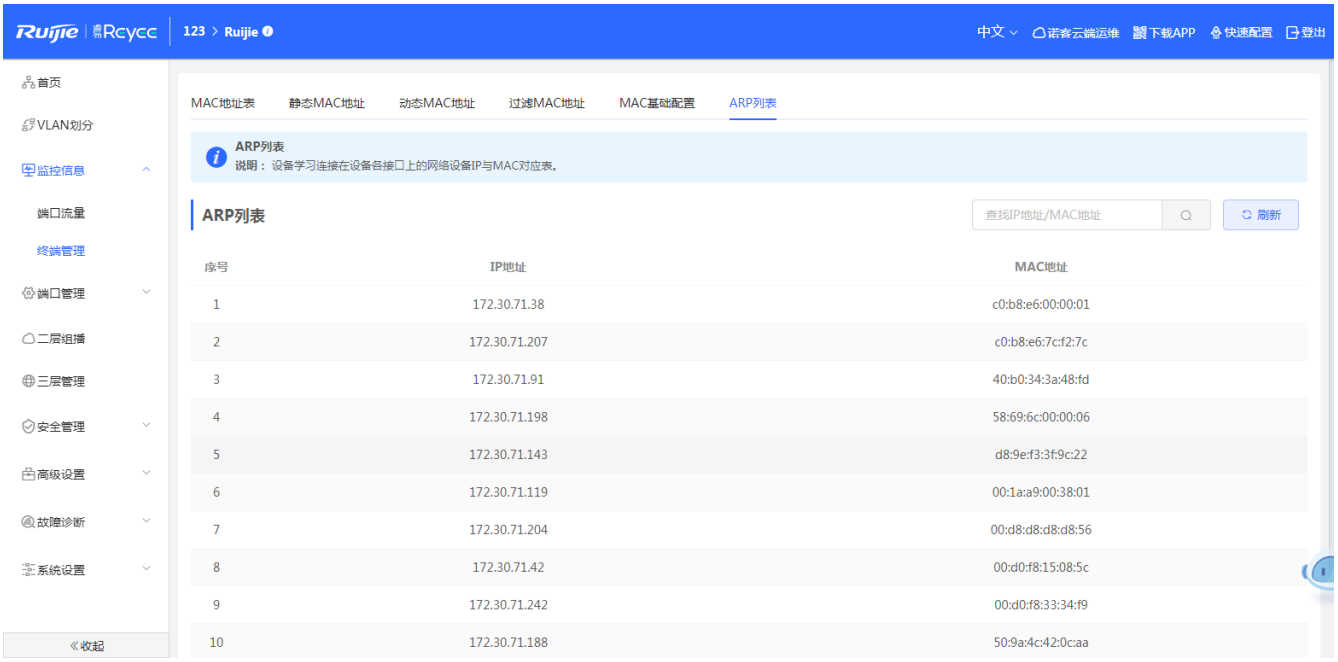
设备老化时间范围：10~630，单位为秒，0表示不老化。

3.3.2.7 ARP 列表

两台IP设备之间需要通信，发送方除了应该知道对方的IP地址，还必须知道对方的MAC地址。有了MAC地址，IP设备可以封装链路层的帧，将数据帧发送到物理网上。根据IP地址来获知MAC地址的过程称为地址解析。

ARP（Address Resolution Protocol，地址解析协议）是用来将IP地址解析为MAC地址的协议，以IP地址作为输入，ARP能够获取其关联的MAC地址。ARP协议将IP地址与MAC地址对应关系保存在设备的ARP缓存表中。缺省配置下，以太网上IP和ARP协议使用Ethernet II帧结构进行封装。

设备学习连接在设备各接口上的网络设备的IP地址与MAC地址，生成对应ARP表项。在当前页面可以查看设备学习到的ARP表项。



- **搜索：**

  ARP列表支持根据IP或MAC地址来搜索指定ARP表项。

- **刷新：**

  点击<刷新>，可重新获取最新的ARP表项。

3.4 端口管理

3.4.1 功能概述

接口（也端口）是网络设备上能够实现数据交换功能的重要部件。我司网络设备上支持两种类型的接口：物理接口和逻辑接口。物理接口意味着该接口在设备上有对应的、实际存在的硬件接口，如：百兆以太网接口、千兆以太网接口等。逻辑接口意味着该接口在路由器上没有对应的、实际存在的硬件接口，逻辑接口可以与物理接口关联，也可以独立于物理接口存在，如： Loopback 接口和 Tunnel 接口等等。实际上对于网络协议而言，无论是物理接口还是逻辑接口，都是一样对待的。

对端口进行基本设置，以及设置端口聚合、端口镜像、端口限速、管理IP、机箱管理IP（部分设备）、PoE配置（部分设备）。

3.4.2 接口类型

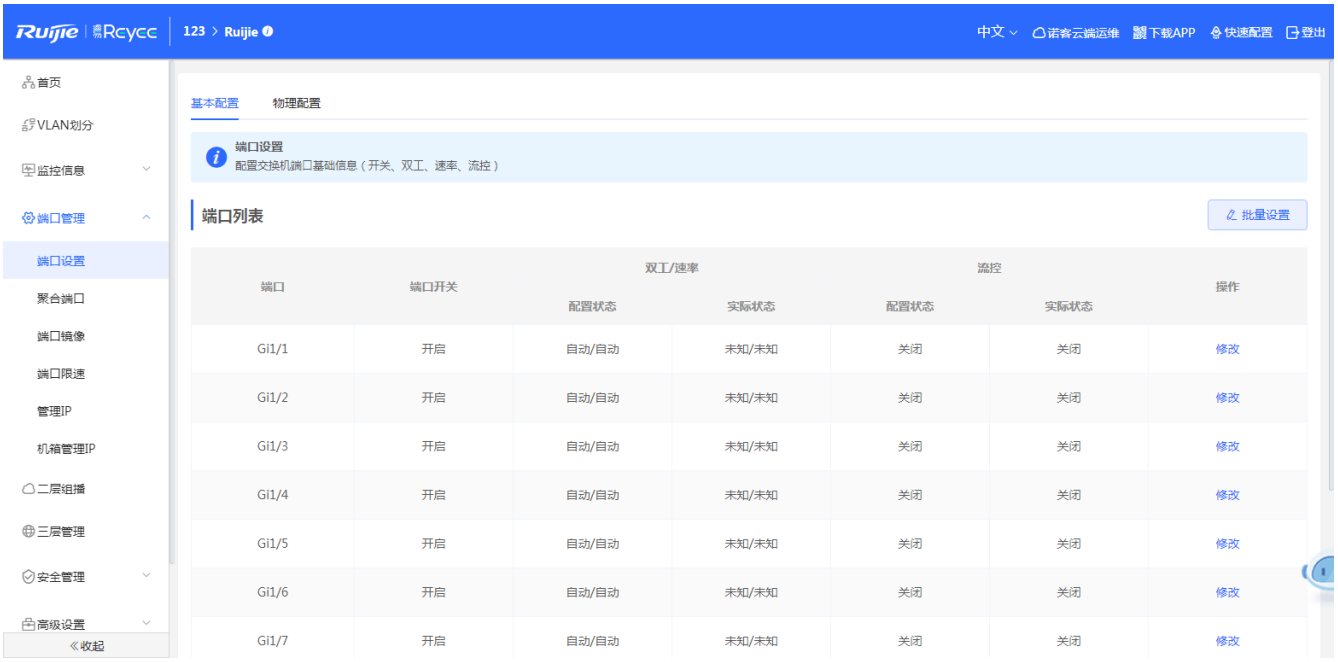
表 3-3 接口类型说明

接口类型	说明	备注
交换端口	交换端口由设备上的单个物理端口构成，只有二层交换功能。交换端口被用于管理物理接口和与之相关的第二层协议。	本章介绍
二层聚合端口	聚合端口是由多个物理成员端口聚合而成的。我们可以把多个物理链接捆绑在一起形成一个简单的逻辑链接，这个逻辑链接我 们称之为一个聚合端口（以下简称聚合端口）。 对于二层交换来说聚合端口就好像一个高带宽的交换端口，它可以把多个端口的带宽叠加起来使用，扩展了链路带宽。此外，通过二层聚合端口发送的帧还将在二层聚合端口的成员端口上进行流量平衡，如果聚合端口中的一条成员链路失效，二层聚合端口会自动将这个链路上的流量转移到其他有效的成员链路上，提高了连接的可靠性。	本章介绍
SVI 口	SVI 接口可以作为本机的管理接口，通过该管理接口管理员可管理设备。用户也可以创建 SVI 接口为一个网关接口，就相当于是对应各个 VLAN 的虚拟接口，可用于三层设备中跨 VLAN 之间的路由。	详见“3.6 三层管理”
路由端口	在三层设备上，可以把单个物理端口设置为路由端口，作为三层交换的网关接口。一个路由端口与一个特定的 VLAN 没有关系， 而是作为一个访问端口。路由端口不具备二层交换的功能。	详见“3.6 三层管理”
三层聚合端口	三层聚合端口同二层聚合端口一样，也是由多个物理成员端口汇聚构成的一个逻辑上的聚合端口组。汇聚的端口必须为同类型的三层接口。对于三层交换来说，聚合端口作为三层交换的网关接口，它相当于把同一聚合组内的多条物理链路视为一条逻辑链路，是链路带宽扩展的一个重要途径。此外，通过三层聚合端口发送的帧同样能在三层聚合端口的成员端口上进行流量平衡。 当聚合端口中的一条成员链路失效后，三层聚合端口会自动将这个链路上的流量转移到其它有效的成员链路上，提高了连接的可靠性。 三层聚合端口不具备二层交换的功能。	详见“3.6 三层管理”

3.4.3 端口设置

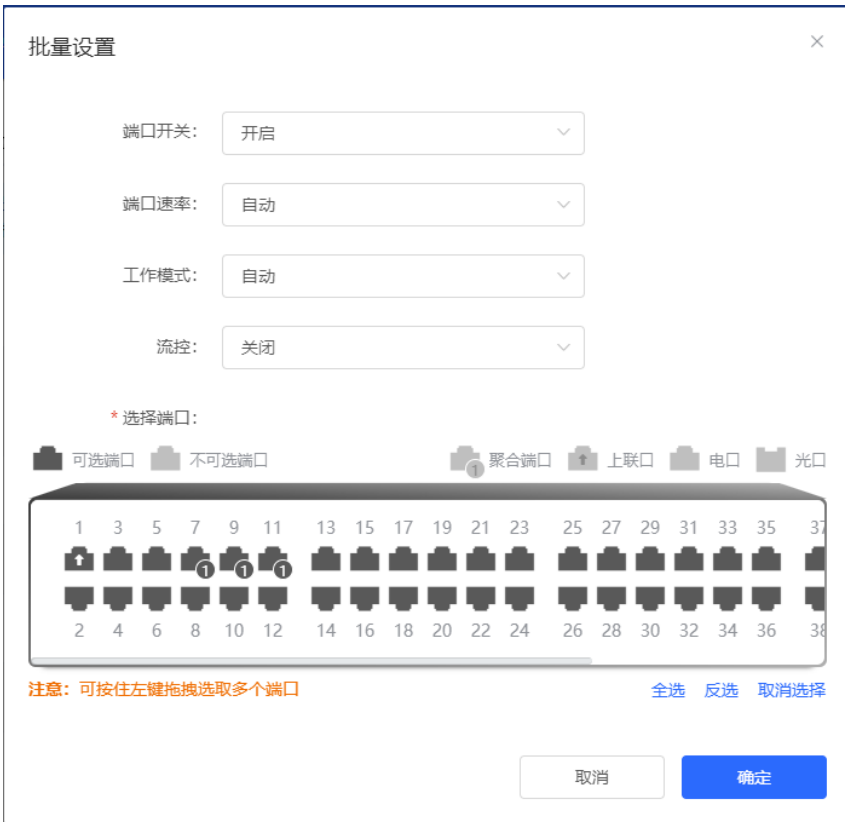
端口设置包含端口开关、双工速率、流控和端口物理信息等基础配置。用户可以调整接口的速率，双工模式、流控模式和自协商因子模式等。

3.4.3.1 基本配置

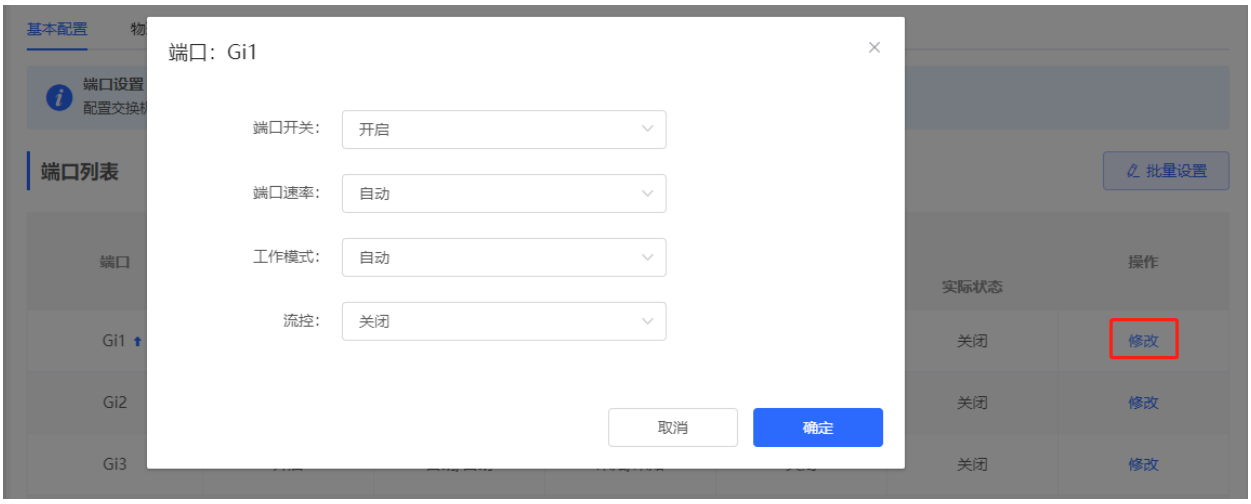


➢ **编辑端口：**

方法1：点击<批量设置>，在配置框中首先选中需要配置的端口，然后选择端口状态、速率、模式等，点击<确定>下发配置。



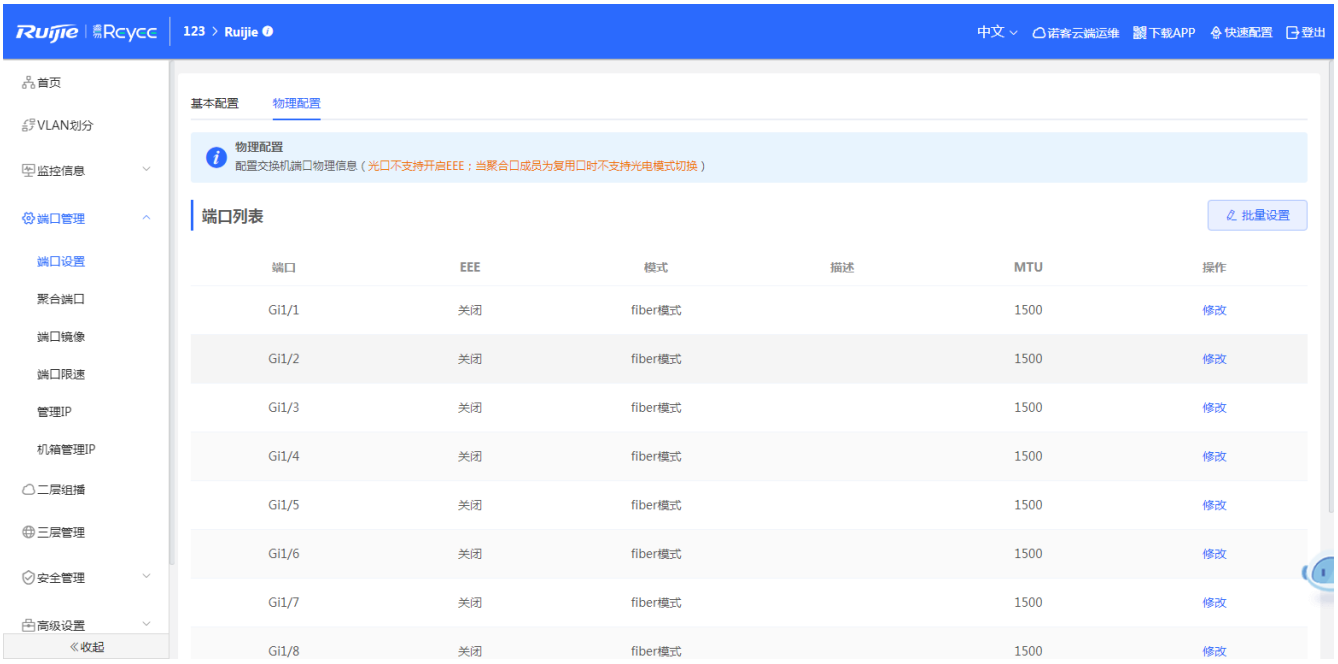
方法2：在端口列表中选择列表项，点击操作列中的<修改>，在配置框中选择端口状态、速率、模式等，点击<确定>配置。



说明

1. 千兆口支持设置端口速率为1000M/100M/自动；万兆口支持设置端口速率为10G/1000M/自动。
2. 批量配置时，可选配置项为所选端口的共有集合（即所选端口共同支持的属性）。

3.4.3.2 物理配置



➢ **设置端口物理信息：**

表 3-4 物理配置参数说明

参数	含义	默认值
EEE	全称为 Enery-Efficient-Ethernet，高效节能以太网，基于标准 IEEE 802.3az 协议。在没有数据传输的过程中通过 MAC 发送 LPI（Low Power Idle）,使 PHY 进入低功耗模式。 取值：关闭/开启	关闭
模式	端口属性，用于指明端口为电口还是光口； 电口：copper 模式(不可修改)； 光口：fiber 模式(不可修改)； 只有光/电复用口才支持修改模式	根据端口属性而定
描述	用户可以增加描述，标注端口的作用	空
MTU	最大传输单元（Maximum Transmission Unit，MTU）用来通知对方所能接受数据服务单元的最大尺寸，说明发送方能够接受的有效载荷大小	1500

方法1：点击<批量设置>，在弹出的配置框中首先选中需要配置的端口，然后选择EEE开关、端口模式并输入端口描述和MTU大小，点击<确定>。

方法2：点击列表项操作列的<修改>，弹出配置框，选择EEE开关、端口模式，并输入端口描述和MTU大小，点击<确定>。

说明

1. 不同端口支持的属性及配置项有所不同。
2. 只有支持光电复用的端口才支持端口模式切换（聚合口不支持端口模式切换）。
3. 光口不支持开启EEE配置。
4. 批量配置时，不支持同时配置电口和光口。

3.4.4 聚合端口

3.4.4.1 功能概述

AP（Aggregate Port，链路聚合口）可以将多个物理链接捆绑在一起形成一个逻辑链接，用于扩展链路带宽，提供更高的连接可靠性。

AP 支持流量平衡，可以把流量均匀地分配给各成员链路。AP 还实现了链路备份，当 AP 中的一条成员链路断开时，系统会将该成员链路的流量自动地分配到 AP 中的其它有效成员链路上。AP 中一条成员链路收到的广播或者多播报文，将不会被转发到其它成员链路上。

- 如果两台设备之间，单个接口相连最多为 1000M（假定两台设备的接口都为 1000M），当该链路上承载的业务流量超过 1000M 时，超过的部分就会被丢弃，而接口聚合将可以解决这一问题。例如，使用 n 根网线连接这两台设备，再将这些接口进行聚合绑定，这样这些接口就逻辑捆绑形成了 1000M * n 的最大流量。
- 如果两台设备是通过单个网线相连接，当这两个接口之间出现链路断开时，这条线路上承载的业务就会断掉，而如果将多千个互连的接口进行聚合绑定，只要有一条链路没有出现链路断开，那么在这些接口上承载的业务就不会断掉。

3.4.4.2 工作原理

- **静态AP模式**

静态 AP 模式是指通过手动配置物理接口加入到 AP 聚合组中，静态 AP 模式下的聚合接口，称为静态聚合接口，对应的成员接口称为静态聚合接口的成员接口。静态 AP 实现简单，用户只要将指定的物理接口通过配置命令加入到同一个聚合组 AP 中，就可以实现多条物理链路的聚合。成员接口一旦加入聚合组后，即可参与 AP 聚合组的数据收发功能，并参与聚合组的流量均衡。

- **流量平衡**

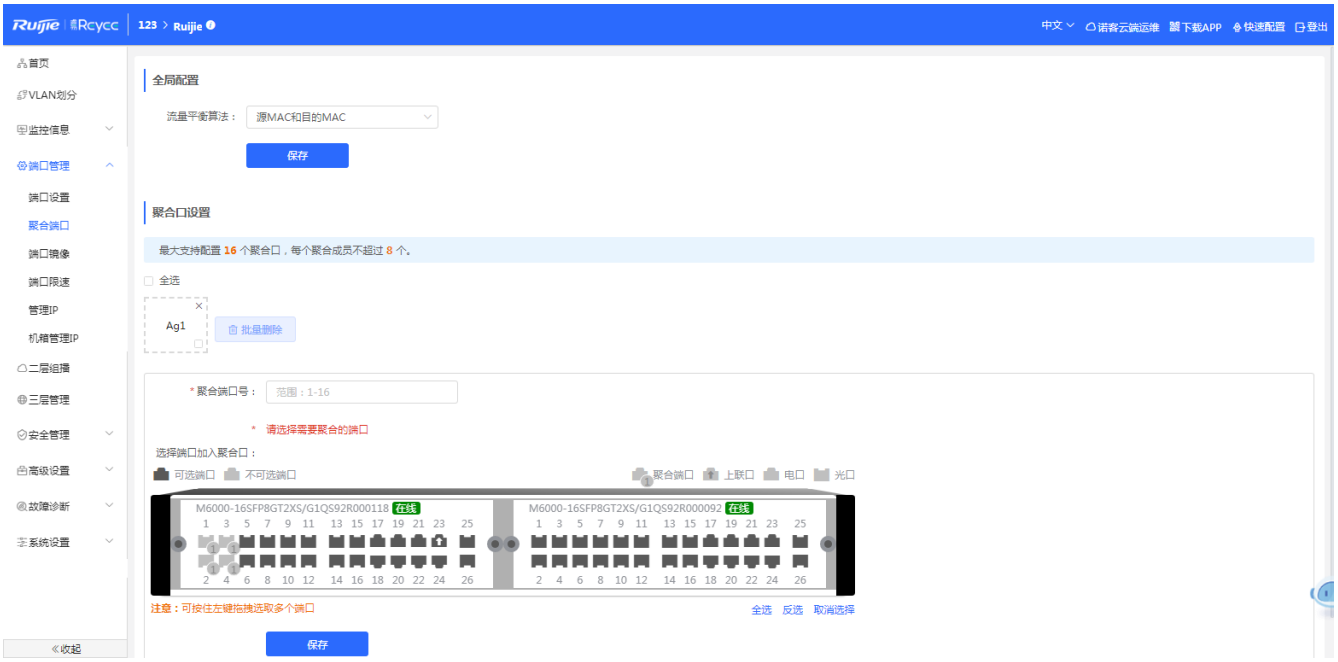
AP可以根据入接口收到的报文的源MAC地址、目的MAC地址、源IP地址、目的IP地址、L4层源端口、L4层目的端口号等报文特征信息，进行一种或几种组合模式算法对报文流进行区分，将属于同一报文流从同一条成员链路通过，不同的报文流则平均分配到各个成员链路中。例如，采用源MAC地址流量平衡模式，会根据报文的源MAC地址将报文分配到AP的各个成员链路上。不同源MAC的报文，根据源MAC地址在各成员链路间平衡分配；相同源MAC的报文，固定从同一个成员链路转发。

目前支持的AP流量平衡模式如下：

- 源 MAC 或目的 MAC 地址
- 源 MAC+目的 MAC 地址
- 源 IP 地址或目的 IP 地址
- 源 IP 地址+目的 IP 地址
- 源端口
- L4 层源端口或 L4 层目的端口
- L4 层源端口+L4 层目的端口

3.4.4.3 配置步骤

支持配置静态聚合口，并对聚合端口的全局流量平衡算法进行设置。

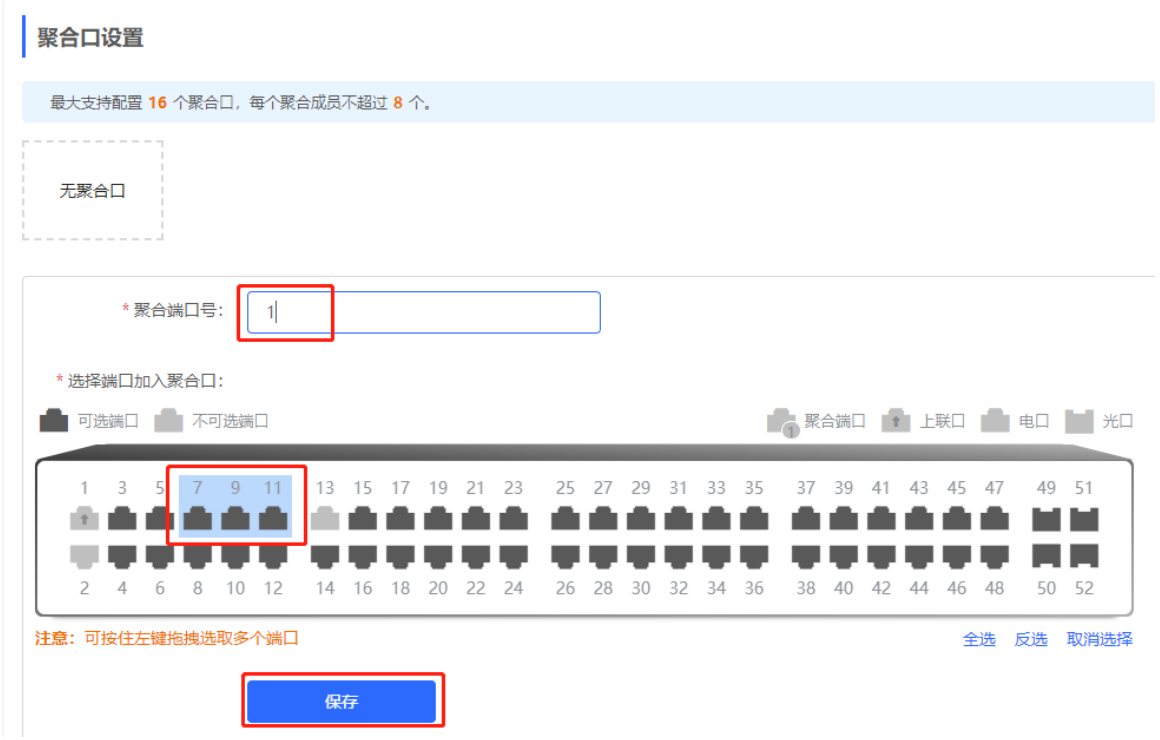


➢ **全局配置：**

选择“流量平衡算法”，点击<保存>进行配置。

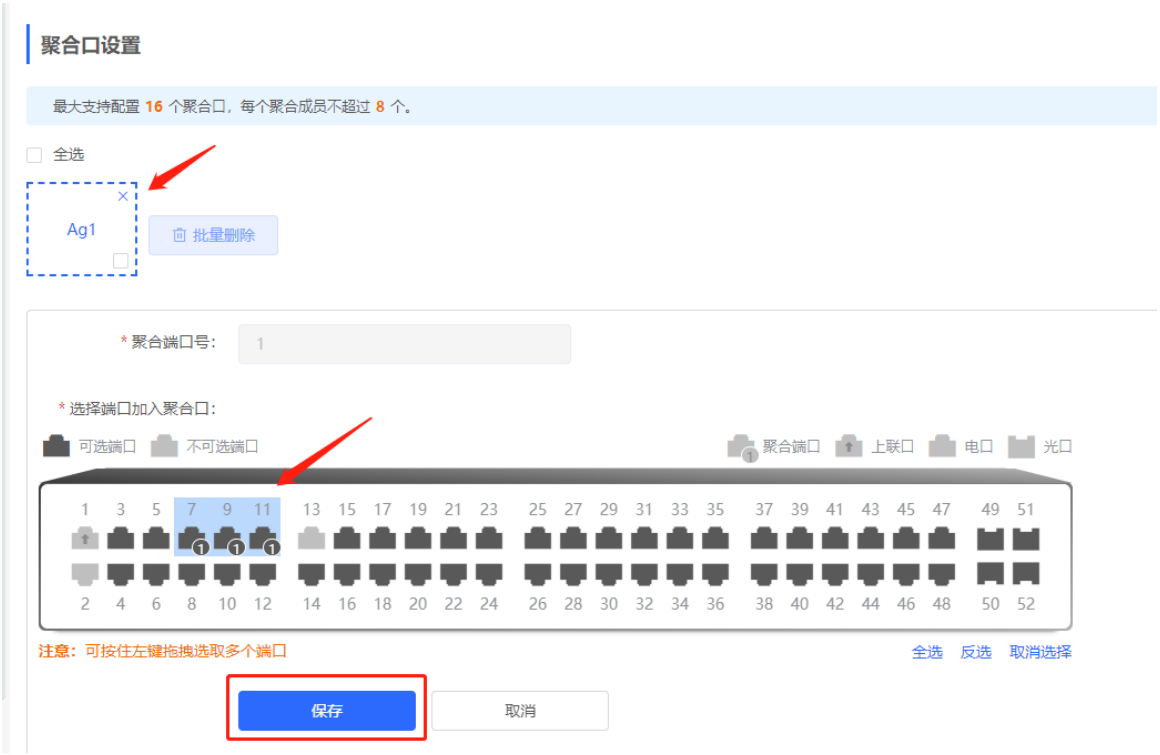
➢ **添加聚合口：**

输入聚合端口号并选择成员端口（已经添加入聚合口的端口不可选择）后点击<保存>，提示“配置成功”即完成聚合端口的添加操作。添加成功后面板会显示出添加的聚合口。



➢ **编辑聚合口：**

点击已添加的聚合口，这时该聚合口成员端口就会变成选中状态，点击端口可以取消选中，然后再点击<保存>即可以对聚合端口进行修改。



➢ **删除聚合口：**

在“端口聚合列表”中，鼠标移至聚合口上，点击<删除>图标，会弹出是否删除聚合端口的确认框，点击确认即可删除已创建的聚合端口。删除后面板中对应端口变为“可选端口”状态。

说明

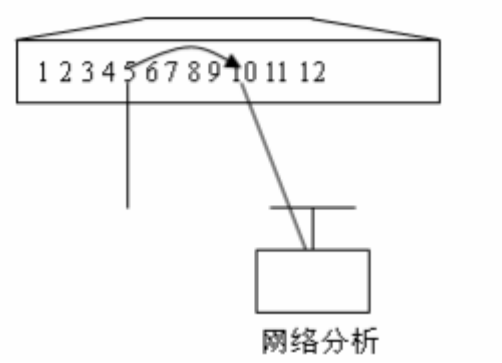
1. 已加入聚合口的端口在添加聚合口时不可被选中。
2. 当删除聚合口时，聚合口中的成员口属性将会恢复至端口出厂属性并且端口为不启用状态。
3. 一个聚合口的成员口最大个数为8。
4. 批量配置时，不支持同时配置电口和光口。

3.4.5 端口镜像

3.4.5.1 功能概述

镜像（SPAN）是将指定端口的报文复制到交换机上另一个连接有网络监测设备的端口的功能，用于网络监控与故障排除。

通过 SPAN 可以监控所有进入源端口和从源端口输出的报文。例如，在下图中，端口 5 上的所有报文都被映射到了端口 10，连接在端口 10 上的的网络分析仪虽然没有和端口 5 直接相连，但是可以接收通过端口 5 的所有报文。



镜像功能主要应用于在网络监控和故障排查两种场景中，用于对网络信息的监控和网络故障的解决。

表 3-5 镜像典型应用

应用类型	说明	备注
一对多的镜像	需要多个用户对同一端口的数据进行监控。	本节介绍
RSPAN 基本应用	需要将镜像源设备的报文镜像到目的设备上进行监控。	本节介绍

3.4.5.2 配置步骤

配置端口镜像，最多可配置4条。

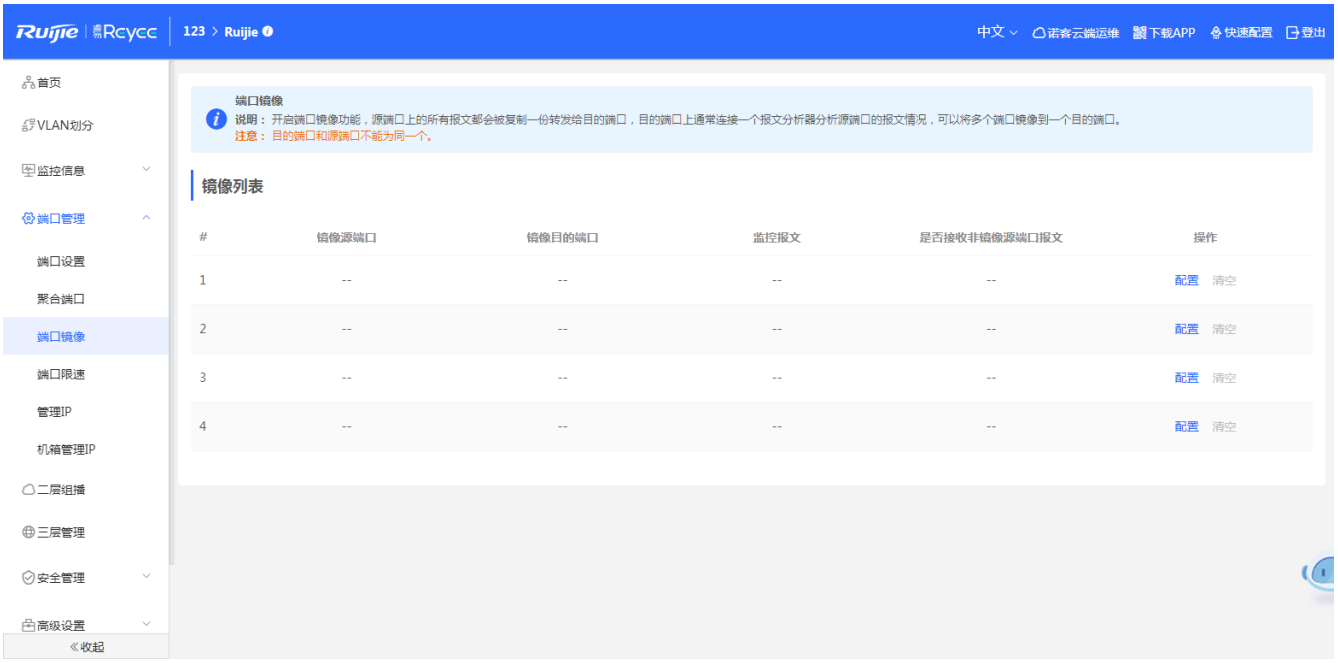


表 3-6 端口镜像参数

参数	含义	默认值
镜像源端口	源端口也被称为被监控口，在 SPAN 会话中，源端口上的数据流被监控，用于网络分析或故障排除。	无
目的端口	SPAN 会话有一个目的端口（也被称为监控口），用于接收源端口的报文拷贝。	无
监控报文	镜像源端口要监控的报文类型（数据流方向），取值：所有报文、输入报文、输出报文	所有报文
是否接收非镜像源端口报文	作用于目的端口，表示目的端口在监控报文的同时是否也转发其他报文 开启：监控报文+转发报文； 不开启：仅监控报文	开启

- **配置端口镜像：**

点击列表中的<配置>，在弹出框中配置镜像源端口、目的端口、监控报文类型等属性，点击<确定>提交完成镜像端口的配置。

➢ **删除端口镜像：**

点击列表中的<清空>，在确认框中点击<确定>删除镜像。

⚠ 注意

1. 镜像源端口可以选择多个，目的端口只能选择一个，且源端口不能包含目的端口。
2. 聚合端口不可作为目的端口。
3. 镜像最多可以配置4条，已配置过的端口不可再次配置。

3.4.6 端口限速

配置端口的流量限制，包含端口出口和入口方向的速率限制。

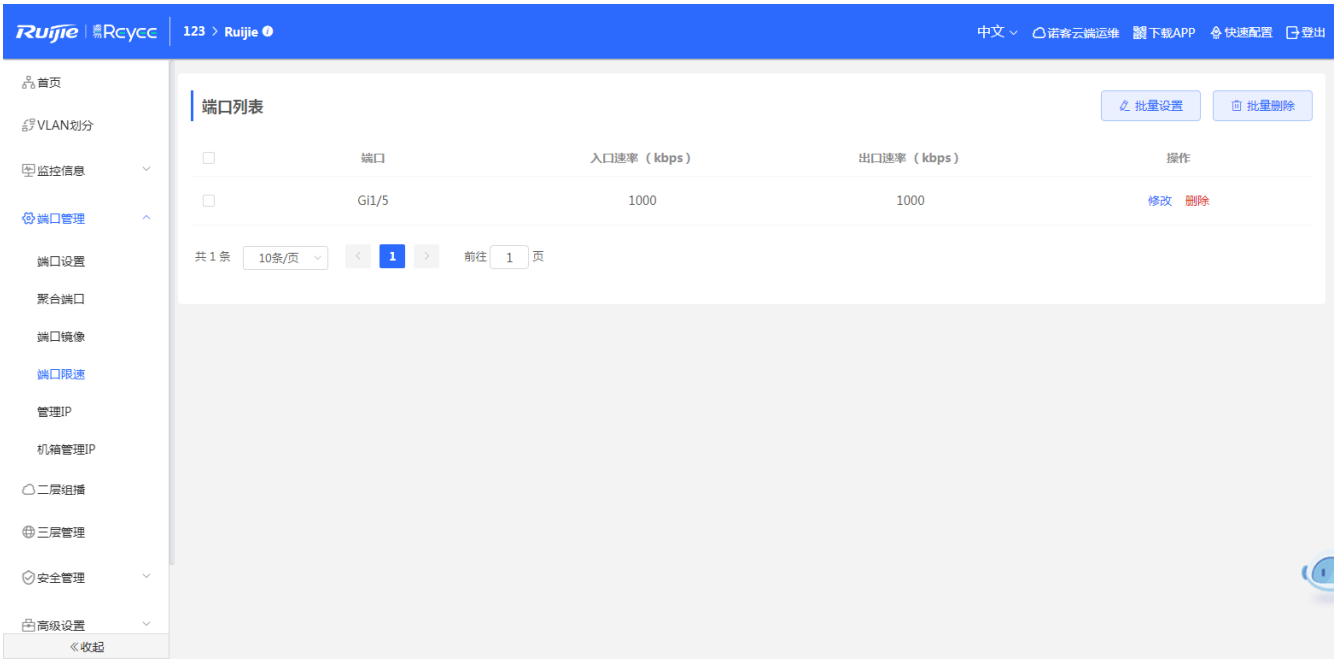


表 3-7 端口限速参数

参数	含义	默认值
入口速率	报文从端口进入交换设备的速率	不限速
出口速率	报文从端口离开交换设备的速率	不限速

➢ **添加端口限速：**

点击<批量设置>，在弹出框中选择端口，入口速率和出口速率必须填写一个；点击<确定>提示“配置成功”后，会显示在端口限速列表中。

➢ **修改单个端口限速：**

在已经添加好的端口列表中，点击“端口列表”中的<修改>，在弹出框中填写入口速率和出口速率，点击<确定>。提示“配置成功”后，会更新限速列表中的配置。

➢ **删除端口限速：**

方法1：在“端口列表”中选择多条记录，点击<批量删除>，在确认框中点击<确定>批量删除数据。

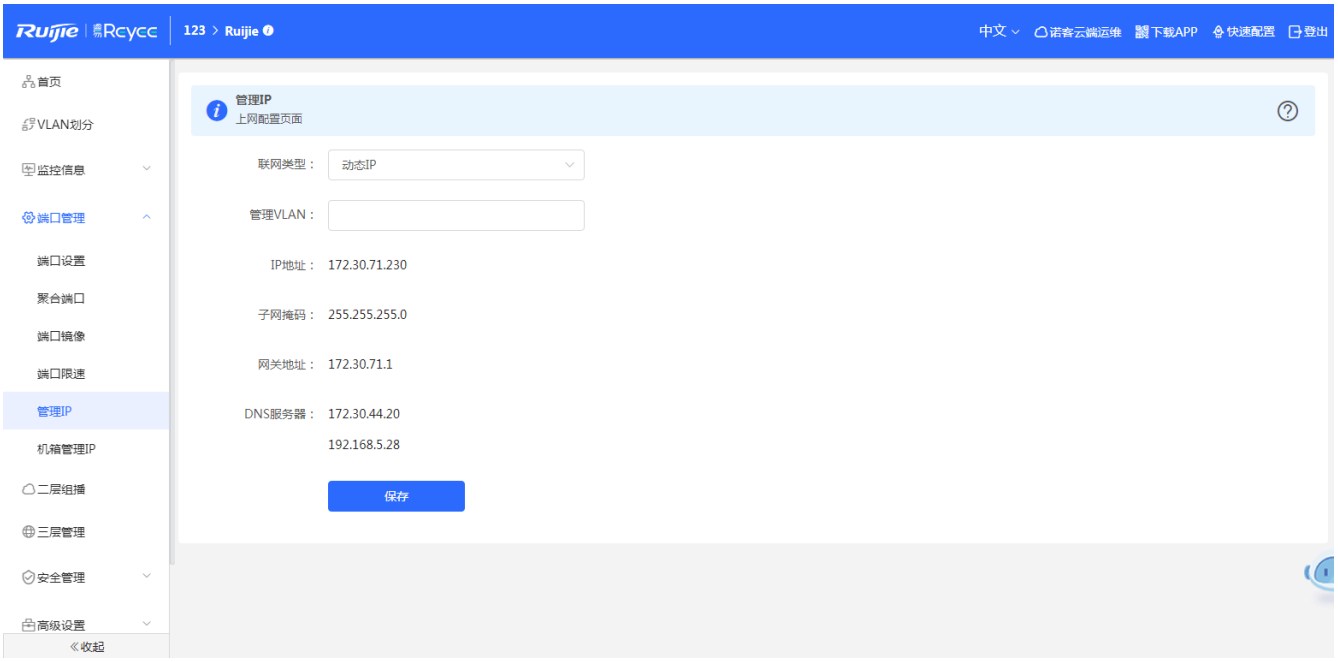
方法2：在“端口列表”中点<删除>，在确认框中点击<确定>删除数据。

说明

1. 配置端口限速时，入口速率和出口速率必须至少填写一个。
2. 入口速率或出口速率为空时，表示不限速。

3.4.7 管理 IP

配置设备管理IP地址。



联网类型有如下两种：

动态IP：使用由上游DHCP服务器动态分配的临时IP地址进行上网。

静态IP：使用固定IP进行上网。

选择动态IP方式，设备会从DHCP server中获取各项参数。选择静态IP方式，需要输入管理VLAN、IP地址、子网掩码、默认网关IP及 DNS服务器。点击<保存>，提示设置成功即可。

说明

1. 管理VLAN为空及不填时默认生效VLAN 1。
2. 管理VLAN必须从已创建的VLAN中选择，若未创建则先前往VLAN列表进行添加（参见3.2.1 VLAN列表）。
3. 建议配置的管理VLAN绑定当前上联端口，否则可能造成无法访问Web系统。

3.5 二层组播

3.5.1 功能概述

IGMP Snooping（Internet Group Management Protocol Snooping，组播侦听者发现协议窥探）是运行在 VLAN 上的 IP 组播窥探机制，用于管理和控制 IP 组播流在 VLAN 内的转发，实现二层组播功能。

表 3-8 二层组播应用

应用类型	说明
二层组播控制	层组播精确转发，避免组播报文在二层泛洪。

应用类型	说明
公共组播服务（组播 VLAN）	多个 VLAN 的用户共享同一 VLAN 的组播流
收费频道与预览	控制用户点播的组播范围，对禁止用户点播的组提供预览。

目前支持全局配置、IGMP Snooping、MVR配置、组播组、端口过滤器、查询器等功能。

3.5.2 全局配置

全局配置可以指定IGMP的协议版本、是否开启report报文抑制和设置未知名组播的行为。

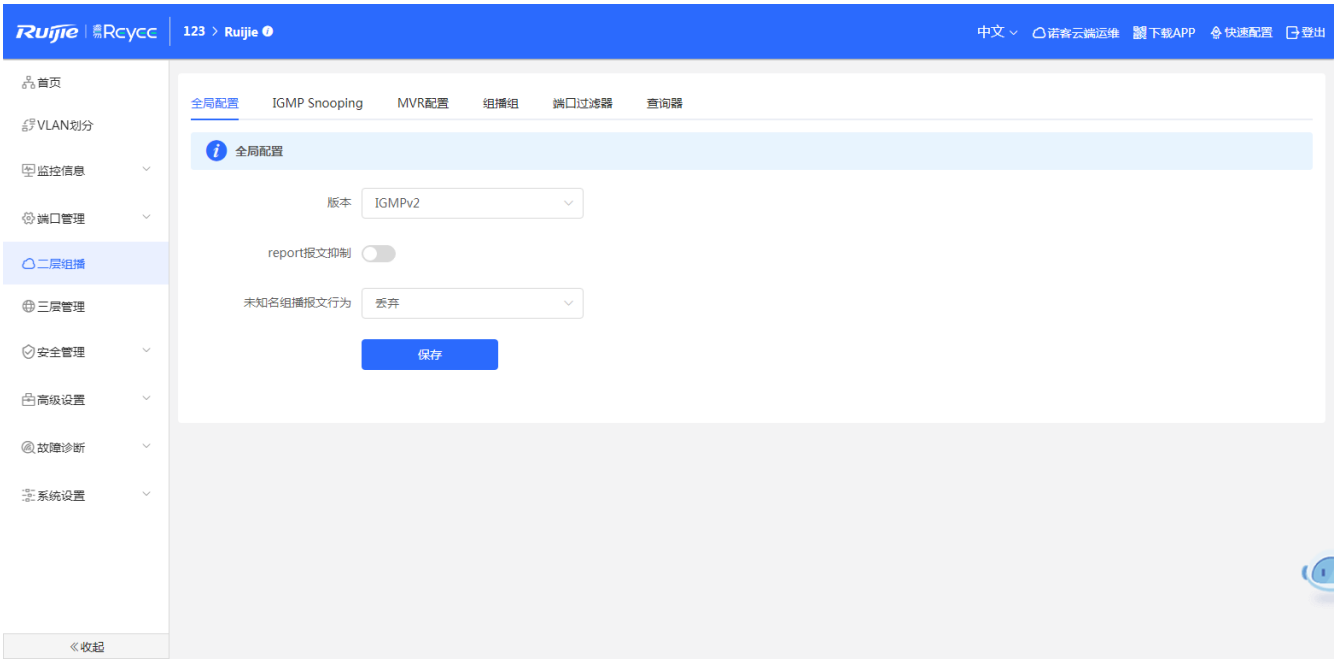
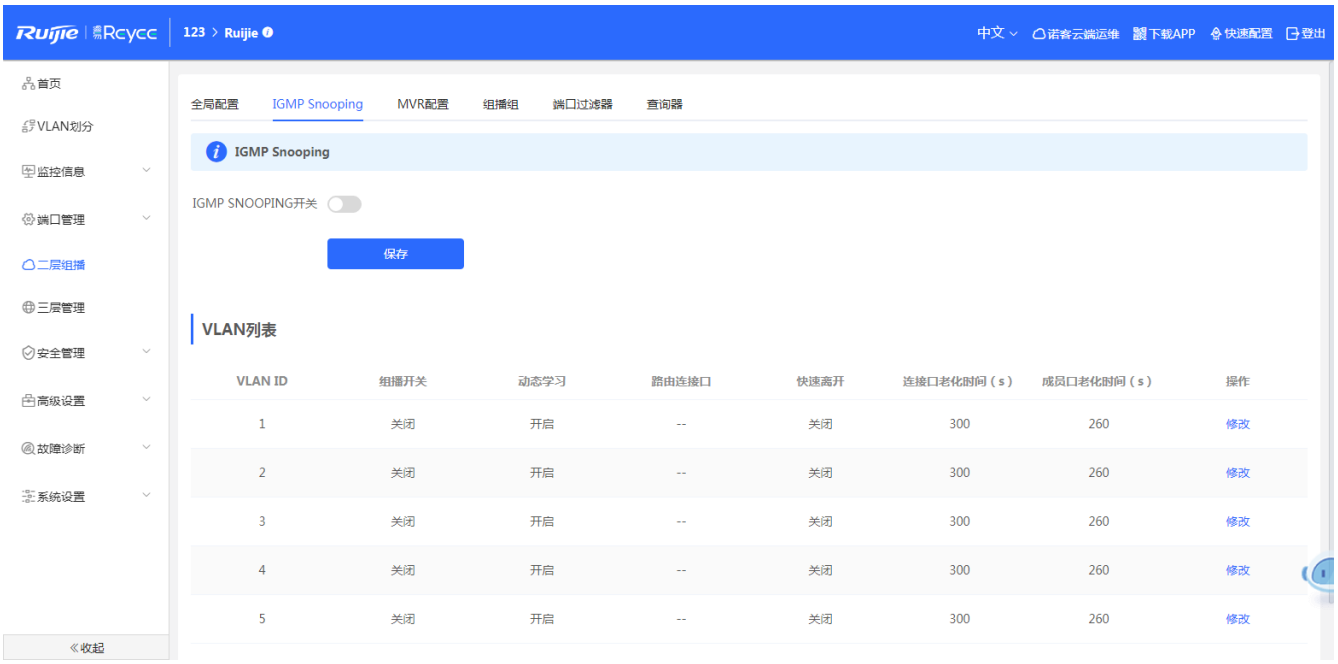


表 3-9 全局配置参数

参数	含义	默认值
版本	二层组播能处理的 IGMP 报文的最高版本。	IGMPv2
Report 报文抑制	开启的情况下，如果多个下联的终端同时发送 report 报文，点播同一个组播组，那么交换机只往组播路由器转发一份 report 报文。	关闭
未知名组播报文行为	全局和 VLAN 的组播都开启的情况下，未知名组播报文的处理方式，取值包括丢弃和泛洪。	丢弃

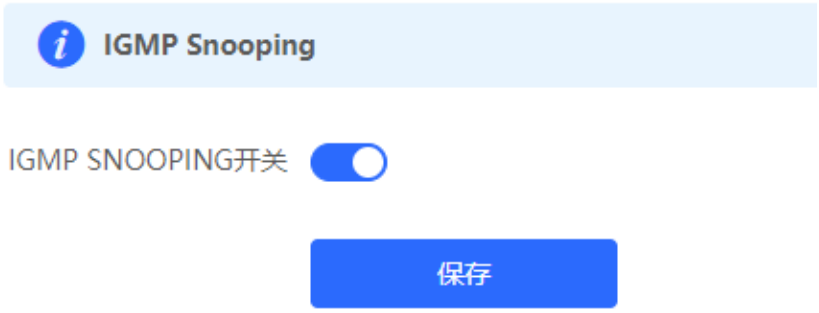
3.5.3 IGMP Snooping

IGMP Snooping在每一条VLAN下都有一个设置表项，所以设备有多少个VLAN，IGMP Snooping就有多少条表项。



- **开启IGMP Snooping：**

  点击IGMP Snooping的开关按钮，点击<保存>使配置生效。



- **编辑VLAN表项：**

  点击<修改>，弹出配置框，然后选择组播开关、动态学习功能开关、快速离开功能开关以及路由端口，并输入连接口老化时间、输入成员口老花时间等，点击<确定>。

表 3-10 IGMP Snooping VLAN 配置参数

参数	含义	默认值
组播开关	VLAN 的组播开关。只有全局 IGMP Snooping 功能和 VLAN 组播开关同时开启，VLAN 的组播功能才能生效。	关闭
动态学习	组播路由器连接口动态学习功能开关	开启
路由连接口	当前的组播路由器连接口列表，包含动态学习的和静态配置的接口	NA
快速离开	开启后，端口收到 leave 报文后，不等老化超时，立刻将端口从组播组中删除。该功能一般在与终端直连的接入交换机中开启。	关闭
连接口老化时间	动态学习的组播路由器连接口的老化时间	300s

参数	含义	默认值
成员口老化时间	动态学习的组播组成员端口的老化时间	260s
选择端口	配置静态的组播路由器连接口	NA

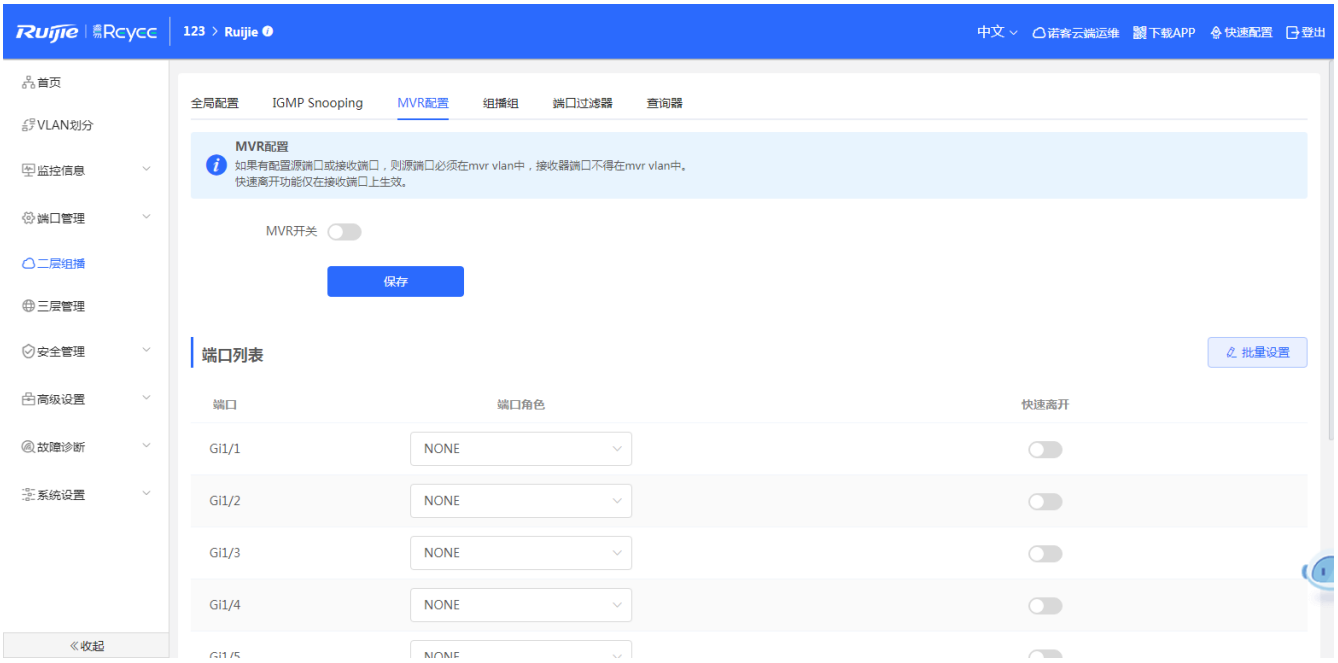
说明

1. 连接口老化时间的取值范围是30-3600秒。
2. 成员口老化时间的取值范围是30-65535秒

3.5.4 MVR 配置

IGMP Snooping只能在同一VLAN中转发组播流量，如果组播流量要转发到不同VLAN，组播源就必须发送不同VLAN的组播流量。为了节约上游带宽、减轻组播源的负担，MVR应运而生。

MVR（Multicast Vlan Register）能够将从MVR VLAN收到的组播流量复制到不同VLAN并转发出去。



➢ **MVR配置：**

开启MVR功能后，需要选择组播VLAN、输入组播起始地址、组播结束地址。点击<保存>保存配置。

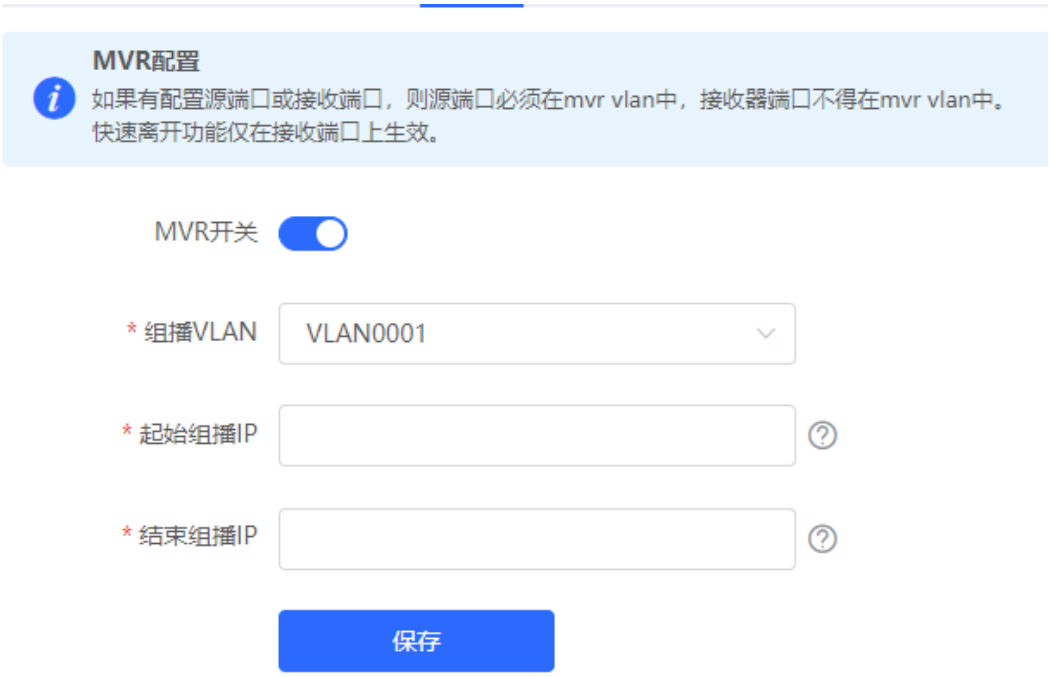


表 3-11 全局 MVR 配置参数

参数	含义	默认值
MVR 开关	全局 MVR 开关	关闭
组播 VLAN	组播源所在的 VLAN，即转换前的 VLAN	1
起始组播 IP	能够学习或者配置为 MRV 组播组的最小组播 IP 地址	NA
结束组播 IP	能够学习或者配置为 MRV 组播组的最大组播 IP 地址	NA

- **端口配置：**

  可以为端口设置NONE、RECEIVER、SOURCE三种端口角色之一，同时可以设置端口是否开启快速离开功能。

表 3-12 端口 MVR 配置参数

参数	含义	默认值
端口角色	NONE：不开启 MRV 功能 SOURCE：接收组播数据流的端口 RECIEVER：与终端相连的端口	NONE
快速离开	端口的快速离开功能	关闭

说明

1. 如果有配置源端口或接收端口，则源端口必须在MVR VLAN中，接收器端口不得在MVR VLAN中。
2. 快速离开功能仅在接收端口上生效。

3.5.5 组播组

组播组由组播报文需要发往的目的端口组成，组播报文将发送到组播组中的所有端口。

可以在当前页面查看配置的组播列表。点击<添加>可创建组播组。

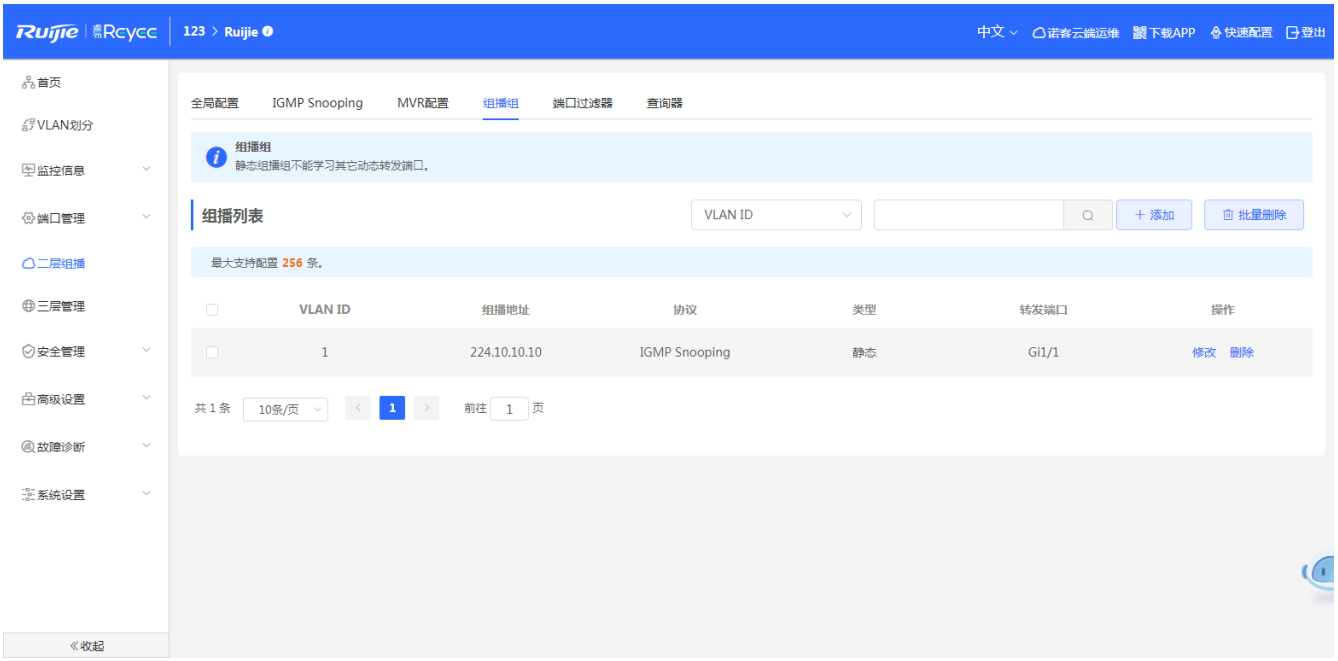


表 3-13 组播组配置参数

参数	含义	默认值
VLAN ID	接收的组播流量所在的 VLAN	NA
组播地址	点播的组播 IP 地址	NA
协议	VLAN ID 为组播 VLAN 并且组播地址在 MVR 的组播 IP 范围内，则协议为 MVR，其他情况为 IGMP Snooping	NA
类型	组播组的生成方式，静态配置或者动态学习	NA
转发端口	组播流量转发出去的端口列表	NA

- **搜索组播：**

选择搜索类型（支持根据VLAN ID或根据组播地址查询），输入搜索的字符串，点击<搜索>，列表过滤出符合搜索条件的组播地址表项。

- **修改组播端口：**

在已经添加的组播列表中，点击“组播列表”中的<修改>，在弹出框中选择端口，点击<确定>。提示“配置成功”后，将更新组播表项中的端口。

- **删除组播地址：**

方法1：在“组播列表”中勾选需要删除的组播项，点击<批量删除>，在确认框中点击<确定>。提示删除成功，列表将更新数据。

方法2：点击“组播列表”最后一列操作栏下的<删除>，在提示框中点击<确定>完成删除。

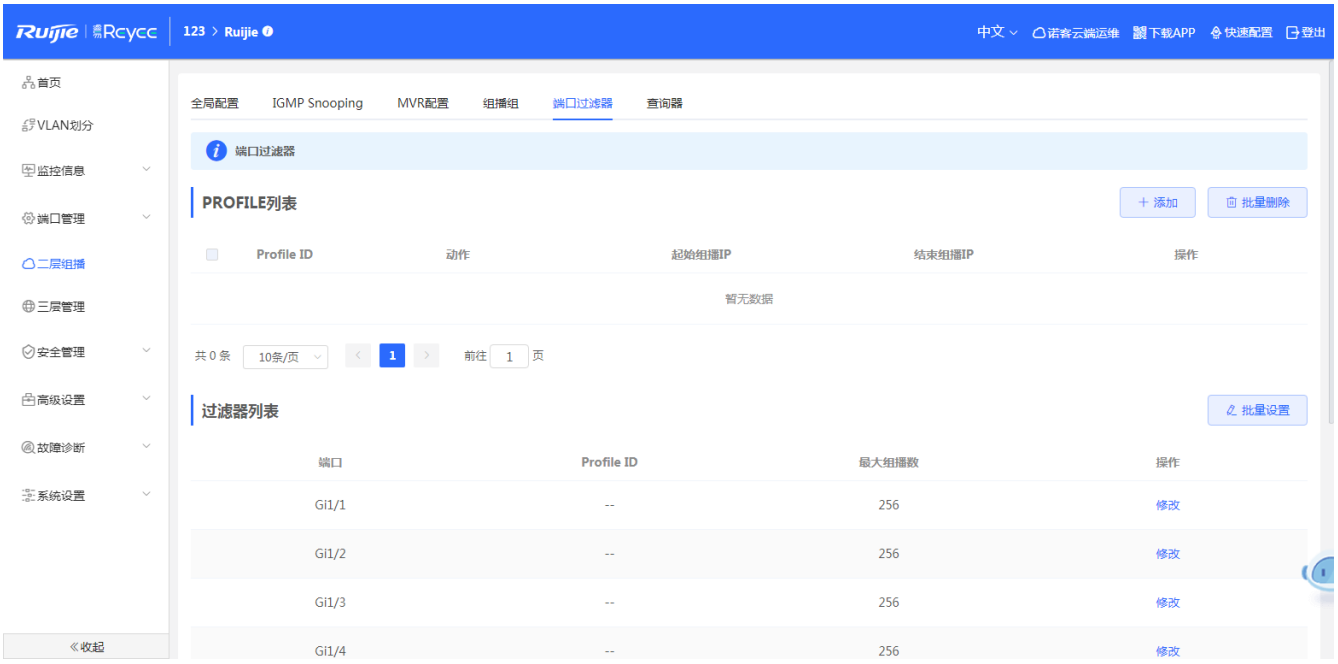
说明

最多可以配置256条组播地址。

3.5.6 端口过滤器

Profile用于定义允许或禁止用户点播的组地址范围，其他功能模块可引用Profile来定义组地址范围。

配置端口过滤器时，引用Profile来定义端口下允许/禁止用户点播的组地址范围。



- **创建Profile：**

点击“添加”，在弹出框中填写Profile ID、动作、组播地址范围。

表 3-14 Profile 配置参数

参数	含义	默认值
Profile ID	Profile 标识	NA
动作	Deny：禁止学习指定范围内的组播 IP Permit：只允许学习指定范围内的组播 IP	NA
起始组播 IP	最小组播 IP 地址	NA
结束组播 IP	最大组播 IP 地址	NA

- **配置端口过滤器：**

  点击“修改”，在弹出框中选择Profile ID，并填写端口允许的最大组播组个数。

表 3-15 端口过滤器配置参数

参数	含义	默认值
Profile ID	用来指定端口生效的 Profile，为空时表示不绑定 Profile 规则	NA
最大组播数	转发端口包含该端口的组播组的最大数目	256

说明

不支持VLAN过滤器。

3.5.7 查询器

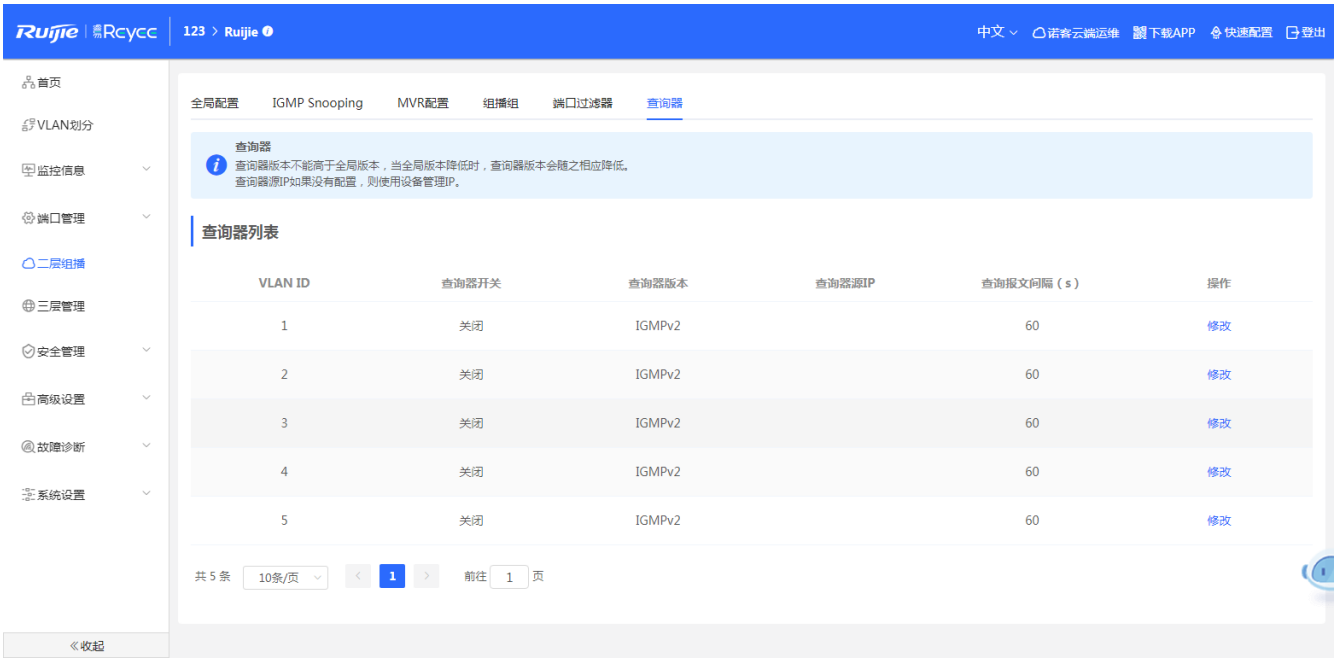
3.5.7.1 功能概述

在一个存在三层组播设备的网络中，由三层组播设备充当IGMP查询器。二层组播设备只需要监听IGMP报文，即可建立并维护转发表项，实现二层组播。

在一个没有三层组播设备的网络中，无法由三层组播设备充当IGMP查询器。为了使二层组播设备能够监听IGMP报文，必须在二层设备上配置IGMP查询器功能。二层组播设备既要充当IGMP查询器，又要监听IGMP报文，才能建立并维护转发表项，实现二层组播。

3.5.7.2 配置步骤

在每一条 VLAN 下都有设置一个查询器，查询器个数与设备 VLAN 数相同。



➢ **设置查询器：**

在查询器中最后一列，点击<修改>，弹出配置框，选择是否开启查询器，并设置查询器版本、查询器源IP、查询报文间隔等，点击<确定>。

表 3-16 查询器配置参数

参数	含义	默认值
查询器开关	VLAN 的查询开关	关闭
查询器版本	查询器发送的查询报文的 IGMP 版本，可配置为 IGMPv2 或 IGMPv3 版本	IGMPv2
查询器源 IP	查询器发送的查询报文所携带的源 IP 地址	NA
查询报文间隔	发送查询报文的时间间隔，单位为秒	60s

说明

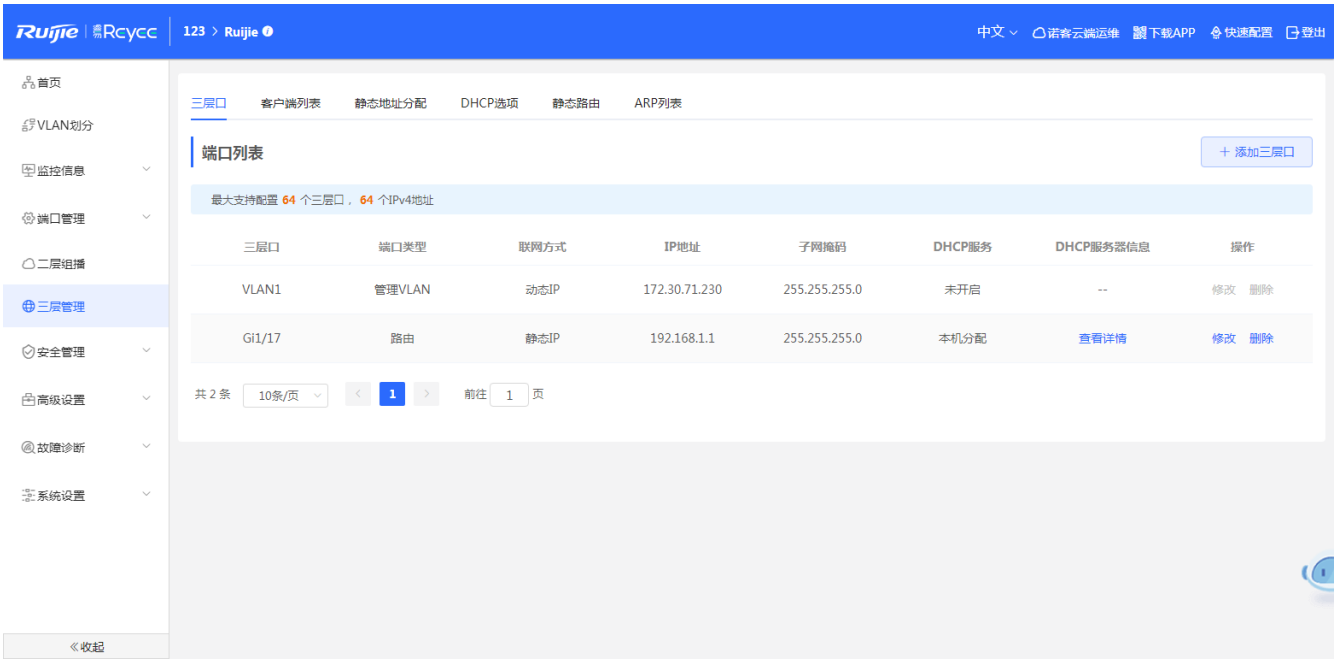
1. 查询器版本不能高于全局IGMP版本，当全局版本降低时，查询器版本会随之相应降低。
2. 若未配置查询器源IP地址，则使用设备管理IP作为查询器的源IP地址。
3. 查询间隔时间的取值范围为30~18000，单位为秒。

3.6 三层管理

三层管理下包含三层口、地址池、DHCP Relay（DHCP中继）、客户端列表、静态地址分配、DHCP选项、静态路由、ARP列表等功能。

3.6.1 三层口

端口列表下显示设备的各种类型的三层口，包括SVI口、路由口、三层聚合口。



➢ **设置三层口：**

点击<添加三层口>，在弹出框中选择要创建的三层口类型，根据三层口的类型对这个三层口进行各项属性的设置。

表 3-17 三层口配置参数

参数	含义
端口类型	创建的三层口类型，包括 SVI 口、路由口和三层 AP 口
联网方式	指定端口通过动态 DHCP 获取或静态配置方式获取接口 IP
VLAN	SVI 接口所属的 VLAN
地址/掩码	当指定联网方式为静态 IP 方式时，需要手动输入 IP 地址和子网掩码
选择端口	选择需要配置的设备端口
聚合口	当创建三层 AP 口时，指定聚合口标识，如 Ag1
DHCP 模式	选择是否在三层口上启用 DHCP 服务： 未启用：不启用 DHCP 服务。无法为接口下联终端分配 IP 地址； 本机分配：本设备作为 DHCP 服务器，为接口下联设备分配 IP 地址。需要设置地址池的开始 IP 地址、可分配 IP 数和地址租期； 外部服务器分配（DHCP Relay）：本设备作为 DHCP 中继设备，从外部服务器获取 IP 地址分配给接口下联设备。需要设置接口 IP 地址和 DHCP 服务器的 IP 地址，其中接口 IP 地址应与 DHCP 服务器地址池处于同一网段

- **修改三层口：**

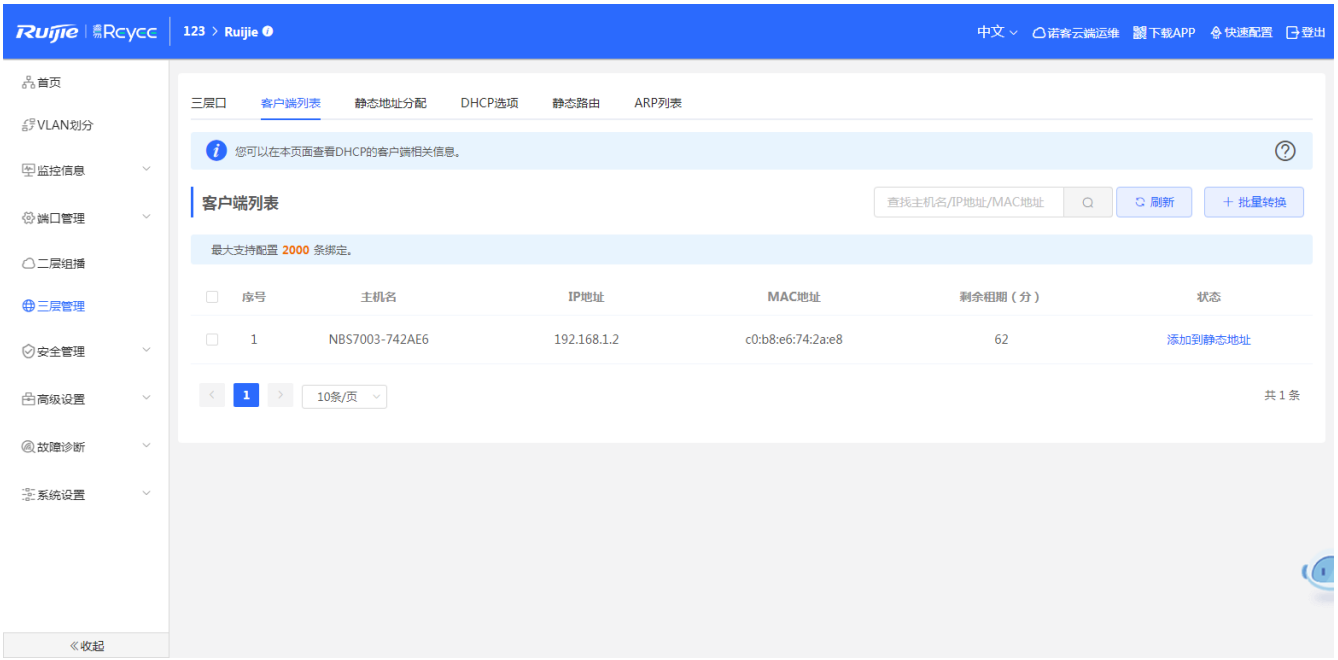
  点击<修改>，在弹出框中更改要修改的三层口的属性，点击<确定>，完成修改。

说明

1. VLAN1为设备的默认SVI口，不可更改、不可删除。
2. 管理VLAN在三层口中只做显示（不能修改），修改在[管理IP]中配置，详见“3.4.7 管理IP”。
3. 三层口的DHCP中继和DHCP服务器功能为互斥功能，不可同时配置。
4. 三层聚合的成员口必须是路由口类型。

3.6.2 客户端列表

客户端口列表下显示的设备三层口中启用DHCP Server服务后，给三层口下联设备分配的IP地址。



➢ **搜索：**

选择搜索类型（支持按MAC查询、按IP查询、按主机名查询），输入搜索的字符串(支持模糊搜索)，点击<搜索>，列表过滤出符合搜索条件的表项。

➢ **添加静态表项：**

将目前已经学习到的IP与MAC条目添加到静态地址分配列表中，实现为固定MAC地址的主机分配固定的IP地址。

方法1：在“客户端列表”中勾选需要添加的表项项，点击<批量转换>，在确认框中点击<确定>提示删除成功，列表更新静态表项数据。

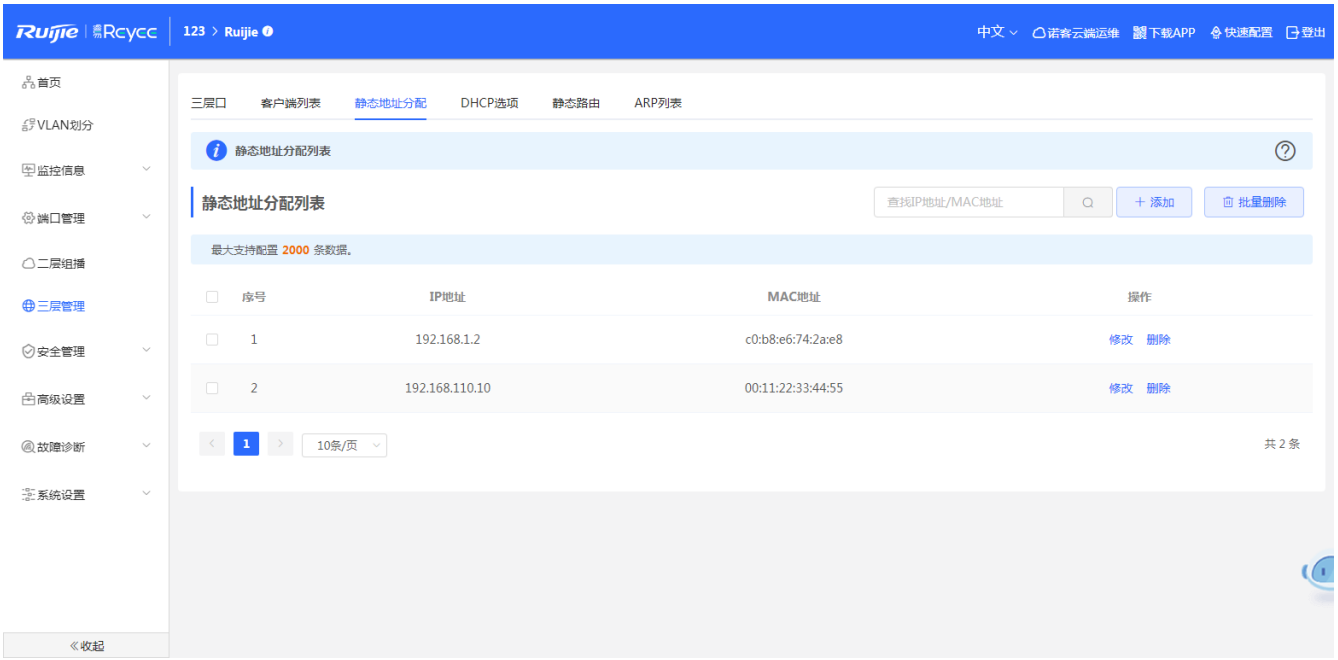
方法2：点击“客户端列表”最后一列操作栏下的<添加到静态表项>，提示“是否绑定为静态IP地址？”，点击<确定>提示“配置成功”，完成。

说明

客户端列表最大支持配置2000条静态地址表项，设备实际支持情况以产品的SPEC为准。

3.6.3 静态地址分配

静态地址分配列表显示的是从客户端列表中转换为静态地址的客户端表项和手动添加的静态表项。



- **搜索：**

选择搜索类型（支持按MAC查询、按IP查询），输入搜索的字符串（支持模糊搜索），点击<搜索>，列表过滤出符合搜索条件的静态地址表项。

- **添加静态地址：**

点击<添加>，在弹出框中输入MAC地址及IP地址，点击<确定>提示“添加成功”，列表更新数据。

- **删除静态地址：**

方法1：在“静态地址分配列表”中勾选需要删除的静态表项，点击<批量删除>，在确认框中点击<确定>提示删除成功，列表更新数据。

方法2：点击“静态地址分配列表”最后一列操作栏下的<删除>，提示“确定删除选中的MAC”，点击<确定>提示“删除成功”，完成删除。

- **修改静态地址：**

在已经添加好的静态地址列表中，点击“操作”中<修改>，在弹出框中修改该条表项的IP地址和MAC地址，点击<确定>提示“配置成功”后，会更新列表中的数据

说明

最大支持配置2000条静态地址表项，设备实际可配置表项数以产品的SPEC为准。

3.6.4 DHCP 选项

通过 DHCP 选项，设置设备的三层口作为 DHCP Server 时，对下联设备下发的配置。均为可选配置。

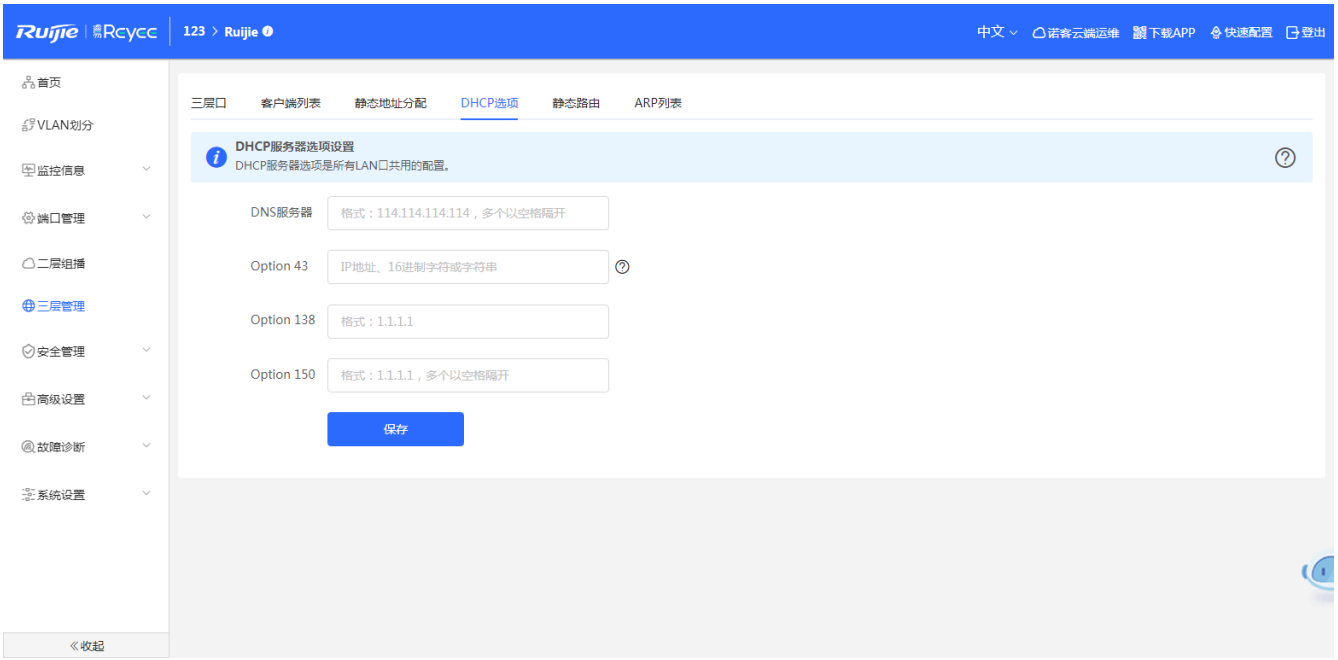


表 3-18 DHCP 服务器选项设置

参数	含义	备选
DNS 服务器	运营商提供的 DNS 服务器地址。无特殊情况无需修改	全局生效配置
Option 43	当下联 AC 与 AP 之间是三层网络时，AP 无法通过广播方式发现 AC，所以需要通过 DHCP 服务器上配置 DHCP 响应报文中携带的 Option 43 信息发现 AC	全局生效配置
Option 138	动态主机配置协议，138 项用于配置 DNS	全局生效配置
Option 150	TFTP 服务器地址选项。输入 TFTP 服务器 IP 地址，指定为客户端分配的 TFTP 服务器的地址	全局生效配置，可支持多个

说明

DHCP选项是设备作为三层DHCP服务器时的可选配置，全局生效，默认不用配置。未指定DNS服务器地址时，下联口分配到的DNS为网关IP。

3.6.5 静态路由

当数据包与静态路由匹配成功时，将按照指定的转发方式进行转发。

➢ **搜索：**

输入搜索的IP地址，点击<搜索>，列表过滤出符合搜索条件的静态路由表项。

➢ **添加静态路由：**

点击<添加>，在弹出的框中输入目地IP地址、子网掩码、下一跳、选择出接口，点击<确定>提示“添加成功”，列表更新数据。

➢ **删除静态地址：**

方法1：在“静态路由列表”中勾选需要删除的静态路由表项，点击<批量删除>，在确认框中点击<确定>提示删除成功，列表更新数据。

方法2：点击“静态路由列表”最后一列操作栏下的<删除>，提示“是否确认删除？”，点击<确定>提示“删除成功”，完成删除。

➢ **修改静态路由：**

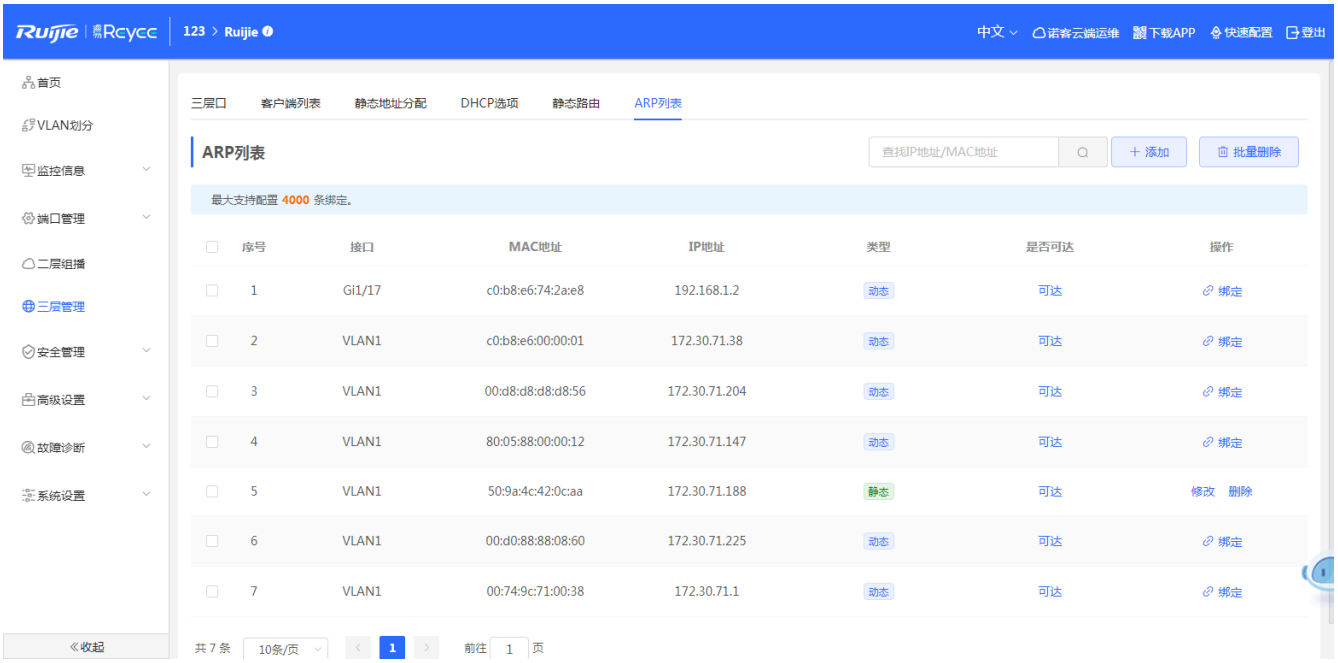
在已经添加好的静态路由列表中，点击“操作”中<修改>，在弹出框中修改该条表项的IP地址、子网掩码、下一跳、选择出接口，点击<确定>提示“配置成功”后，会更新列表中的数据

说明

最多支持添加500条静态路由表项，实际设备支持的表项数量以产品的SPEC为准。

3.6.6 ARP 列表

设备学习连接在设备各接口上的网络设备的IP地址与MAC地址，生成对应ARP表项。在当前页面可以查看设备学习到的ARP表项。



➢ **搜索：**

选择搜索类型（支持按MAC查询、按IP地址查询），输入搜索的字符串，点击<搜索>，列表过滤出符合搜索条件的ARP表项。

➢ **添加ARP表项：**

方法1：点击<添加>，在弹出的框中输入IP地址、MAC地址，点击<确定>提示“添加成功”，列表更新数据。

方法2：点击动态的ARP表项中的<绑定>，动态ARP表项就会转换为静态ARP表项。

➢ **删除ARP表项：**

方法1：在“ARP列表”中勾选需要删除的ARP表项，点击<批量删除>，在确认框中点击<确定>提示删除成功，列表更新数据。

方法2：点击“ARP列表”最后一列操作栏下的<删除>，提示“是否确认删除？”，点击<确定>提示“删除成功”，完成删除。

➢ **修改ARP表项：**

在ARP表项中，静态ARP表项支持修改。点击“操作”中<修改>，在弹出框中修改该条表项的IP地址、MAC地址，点击<确定>提示“配置成功”后，会更新列表中的数据

说明

ARP列表最大支持配置4000条ARP表项，实际可配置数量以产品的SPEC为准。

3.7 安全管理

包含DHCP Snooping、风暴控制、ACL、端口保护、IP+MAC绑定、IP Source Guard、防网关ARP欺骗等功能。

3.7.1 DHCP Snooping

DHCP Snooping意为DHCP窥探，通过对Client和服务器之间的DHCP交互报文进行窥探实现对用户IP地址使用情况的记录和监控，同时还可以过滤非法DHCP报文，包括客户端的请求报文和服务端的响应报文。DHCP Snooping记录生成的用户数据表项可以为IP Source Guard等安全应用提供服务。

- **开启、关闭DHCP Snooping：**

  点击DHCP Snooping切换开关，开启或关闭DHCP Snooping功能。开启后，选择设置为信任口的端口，点击<保存>。

说明

1. 一般将连接DHCP服务器设备的端口设置为信任口。
2. 开启DHCP Snooping可以起到DHCP报文过滤的功能。对于DHCP客户端请求报文，仅将其转发到信任口，对于DHCP服务器响应报文，仅转发来自信任口的响应报文

3.7.2 风暴控制

3.7.2.1 功能概述

当局域网中存在过量的广播、多播或未知名单播数据流时，就会导致网络变慢和报文传输超时机率大大增加。这种情况称之为局域网风暴。拓扑协议的执行错误或对网络的错误配置都有可能导致风暴的产生。

用户可以分别针对广播、多播和未知名单播数据流进行风暴控制。当设备端口接收到的广播、多播或未知名单播数据流的速率超过所设定的带宽、每秒允许通过的报文数或者每秒允许通过的千比特数时，设备将只允许通过所设定带宽、每秒允许通过的报文数或者每秒允许通过的千比特数的数据流，超出限定范围部分的数据流将被丢弃，直到数据流恢复正常，从而避免过量的泛洪数据流进入局域网中形成风暴。

3.7.2.2 配置步骤

➢ **添加端口风暴控制：**

点击<批量设置>，在弹出框中选择配置类型、端口，输入组播、未知名单播、未知名组播限制速率，点击<确定>提示“配置成功”后，会显示在风暴控制列表中。

➢ **修改单个端口风暴控制：**

点击“端口列表”中<修改>，选择配置类型、输入组播、未知名单播、未知名组播限制速率，点击<确定>提示“配置成功”后，会更新列表中的限速。

➢ **删除端口风暴控制：**

方法1：在“端口列表”中选择多条记录，点击<批量删除>，在确认框中点击<确定>批量删除数据。

方法2：在“端口列表”中点击<删除>，在确认框中点击<确定>删除数据。

说明

组播、未知名单播、未知名组播限制速率配置为空时，表示不限速。

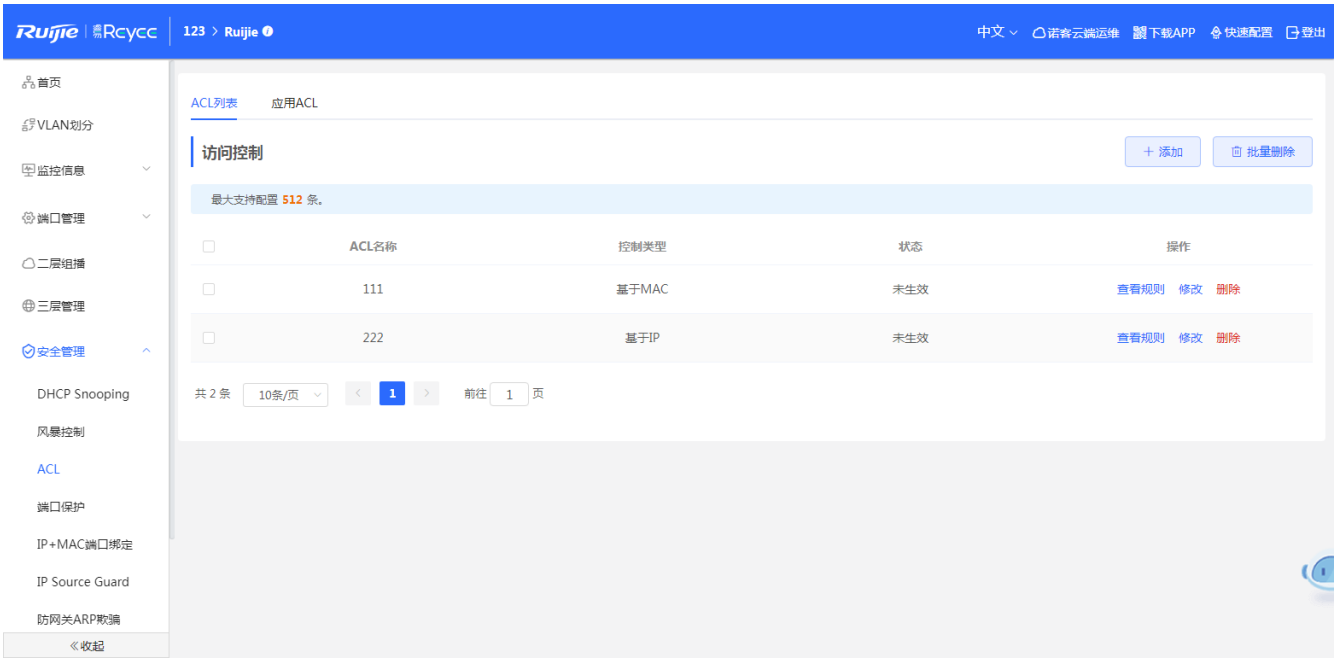
3.7.3 ACL

3.7.3.1 功能概述

ACL（Access Control List，访问控制列表）也称为访问列表，有的文档中还称之为包过滤。ACL 通过定义一系列包含“允许”或“拒绝”的规则语句，并将这些规则应用到设备接口上，对进出接口的数据包进行控制，从而提升网络设备的安全性。

支持基于MAC地址或IP地址添加ACL，并为端口绑定ACL。

3.7.3.2 ACL 列表



- **添加ACL：**

  点击<添加>，在弹出框中选择ACL控制类型，输入ACL名称，点击<确定>创建ACL。

- **删除ACL：**

  勾选“访问控制”复选框点击<批量删除>或则点击列表操作栏<删除>，在确认框中点击<确定>删除ACL。

- **修改ACL：**

  点击列表操作栏<修改>，在弹出框中修改ACL名称，点击<确定>修改ACL。

- **查看编辑ACL规则：**

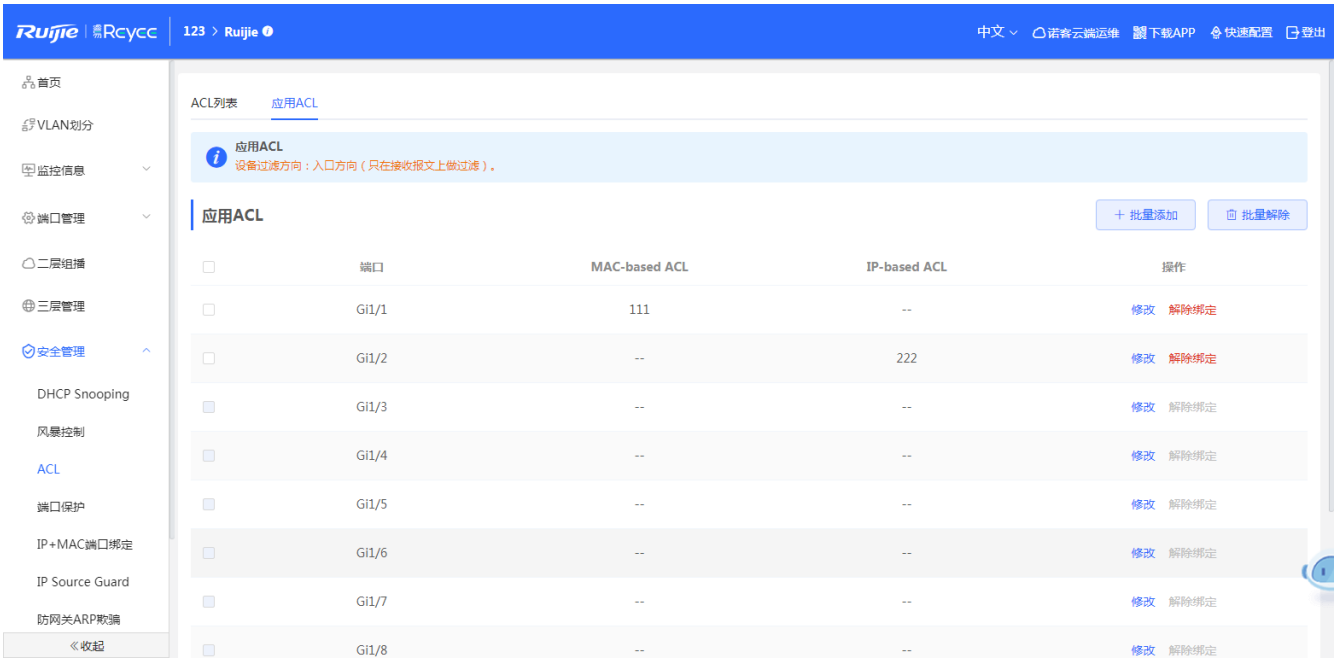
  ACE（Access Control Entry，访问控制条目）是包含“允许”或“禁止”两种动作，以及过滤规则的一条语句。ACL中ACE的顺序决定了该ACE在访问列表中的匹配优先级。网络设备在处理报文时，按ACE的序号从小到大进行规则匹配。

  点击列表操作栏<查看规则>，在弹出的侧栏中查看、增加、编辑、删除规则。

说明

1. ACL名称不可重复，ACL一旦创建只允许修改名称。
2. 被端口应用的ACL不允许修改或删除。
3. 不同控制类型对应的规则字段有所不同，规则支持增加、修改、删除、移动操作。
4. ACE表项中，隐藏最后一条默认表项，禁止所有报文。
5. ACL目前只支持应用在端口的入口方向，即对接受到的报文进行过滤。

3.7.3.3 应用 ACL



- **绑定ACL：**

  点击<批量添加>，在弹出框中选择应用的MAC ACL和IP ACL以及配置生效的端口，点击<确定>绑定端口。

- **解绑ACL：**

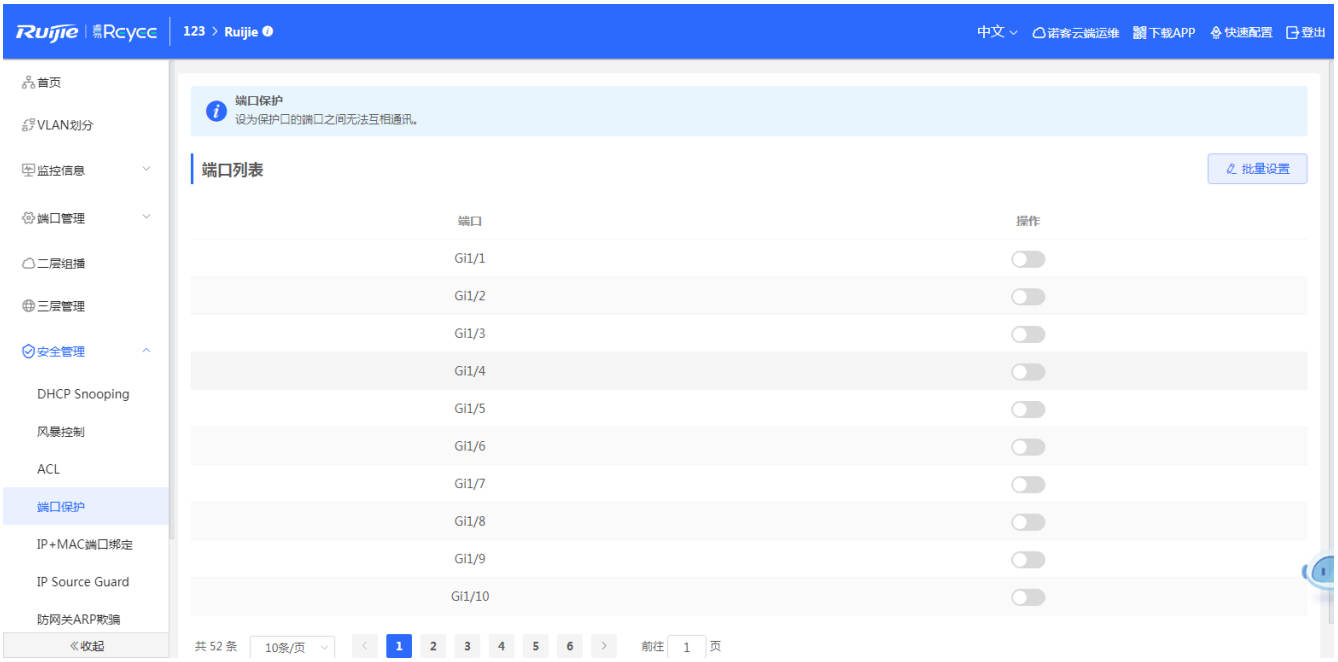
  勾选“端口列表”复选框，点击<批量删除>或点击列表操作栏<解除绑定>，在确认框中点击<确定>解除端口绑定。

说明

端口绑定ACL至少选择一种类型的ACE。

3.7.4 端口保护

设备开启端口保护的情况下，不同端口下的用户被二层隔离，设为保护口的端口之间无法通讯。



➢ **设置端口保护**

方法1：点击<批量设置>，在弹出框中切换开关并选择生效的端口；

方法2：点击“端口列表”操作栏按钮，在确认框中点击<确定>，配置端口保护。

3.7.5 IP+MAC 绑定

配置IP+MAC端口绑定功能，将在选中的端口上检查IP报文的源IP地址和源MAC地址是否为自己配置的IP地址和MAC地址，过滤不符合绑定关系的IP报文，严格控制设备输入源的合法性。

- **搜索：**

选择搜索类型（支持按MAC查询、按IP查询、按端口查询），输入搜索的字符串，点击<搜索>，列表过滤出符合搜索条件的表项。

- **添加IP+MAC端口绑定：**

点击<添加>，在弹出的框中输入MAC地址及IP地址、选择端口，点击<确定>提示“添加成功”，列表更新数据。

- **删除IP+MAC端口绑定：**

方法1：在“IP+MAC端口绑定列表”中勾选需要删除的静态表项，点击<批量删除>，在确认框中点击<确定>提示删除成功，列表更新数据。

方法2：点击“IP+MAC端口绑定列表”最后一列操作栏下的<删除>，提示“确定删除选中的MAC”，点击<确定>提示“删除成功”，完成删除。

- **修改IP+MAC端口绑定：**

在已经添加好的IP+MAC端口绑定列表中，点击“操作”中<修改>，在弹出框中修改该条表项的IP地址和MAC地址、端口，点击<确定>提示“配置成功”后，会更新列表中的数据

注意

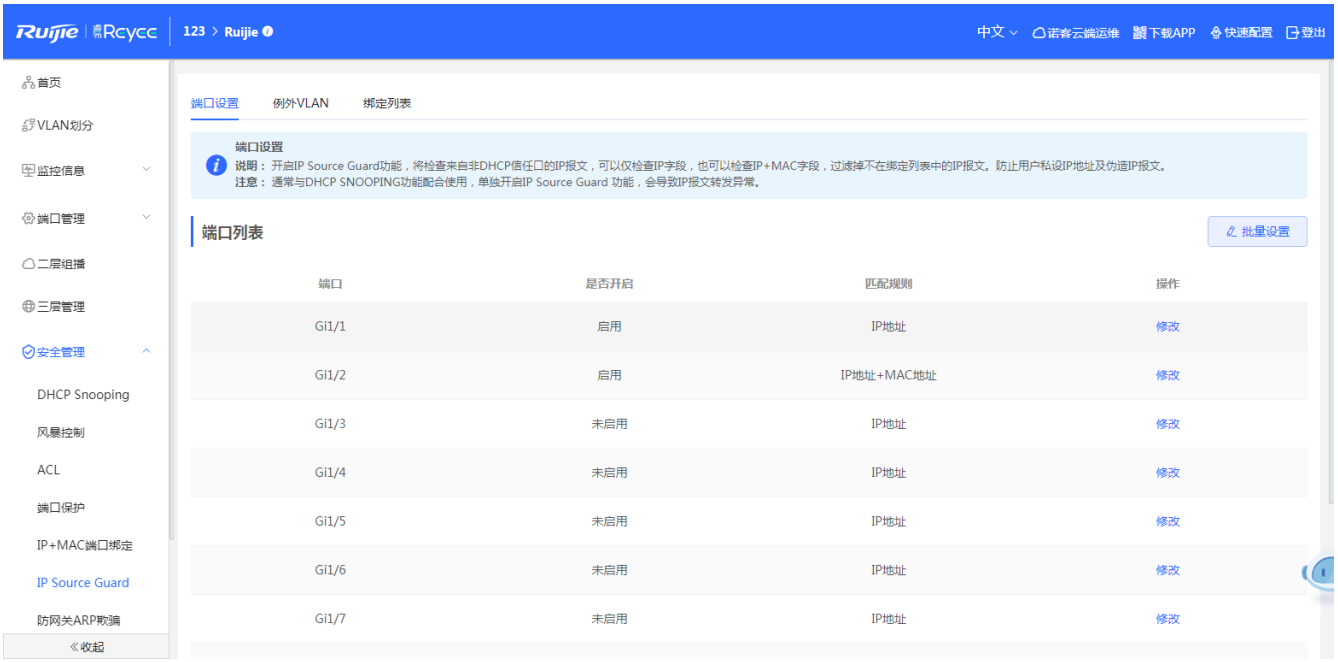
1. IP+MAC端口绑定配置后将优先于ACL生效，但与IP Source Guard功能优先级一致，只要符合其中一个功能配置，报文就会被允许通过。
2. 最多支持配置500条IP+MAC端口绑定。

3.7.6 IP Source Guard

IP Source Guard中包括端口设置、设置例外VLAN、查看绑定列表功能。

3.7.6.1 端口设置

开启IP Source Guard功能，将检查来自非DHCP信任口的IP报文，可以仅检查IP字段，也可以检查IP+MAC字段，过滤掉不在绑定列表中的IP报文。防止用户私设IP地址及伪造IP报文。



➢ **开启IP Source Guard功能：**

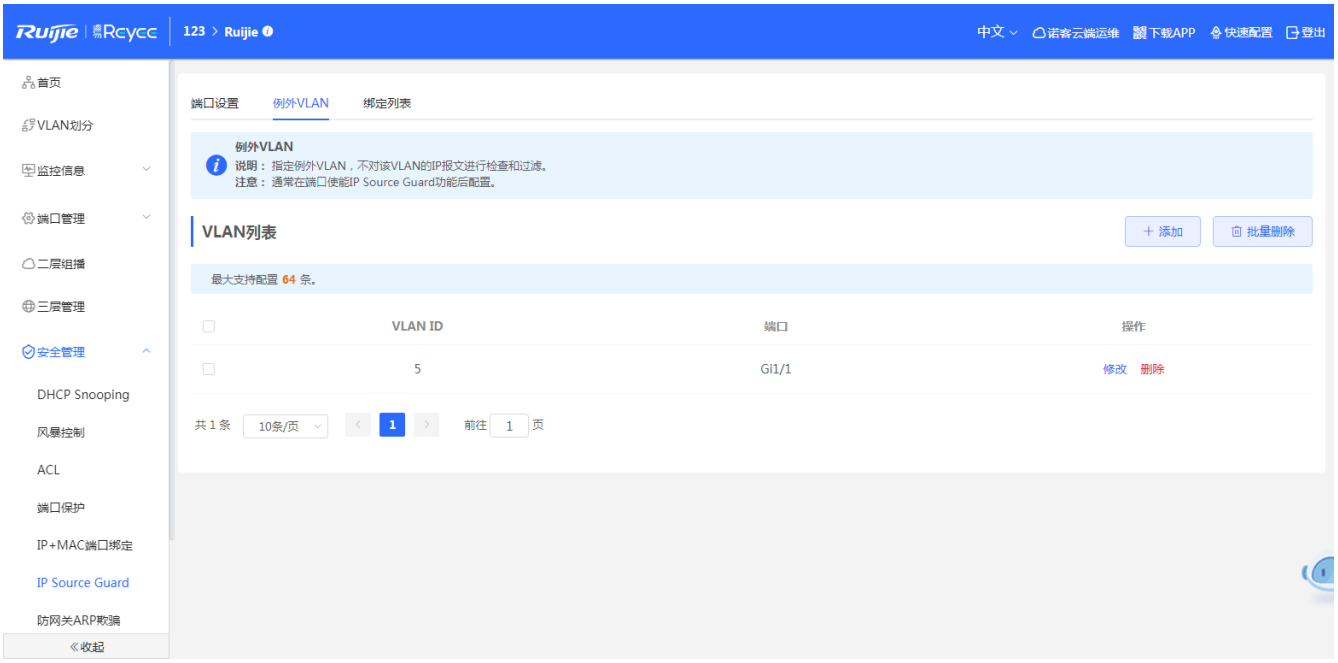
在端口列表中，点击“操作”中<修改>，在弹出框中修改该端口是否开启IP Source Guard功能、匹配规则（仅匹配IP地址或同时匹配IP+MAC地址），点击<确定>提示“配置成功”后，会更新端口列表中的数据。

注意

通常与DHCP Snooping功能配合使用（参见3.7.1 DHCP Snooping），单独开启IP Source Guard功能，会导致IP报文转发异常。请谨慎配置。

3.7.6.2 例外 VLAN

在端口开启IP Source Guard功能的基础上，设置例外VLAN，不对该VLAN的IP报文进行检查和过滤。



- **添加例外VLAN：**

  点击<添加>，在弹出的框中输入VLAN、选择端口，点击<确定>提示“添加成功”，列表更新数据。

- **删除例外VLAN：**

  方法1：在“例外VLAN列表”中勾选需要删除的例外VLAN，点击<批量删除>，在确认框中点击<确定>提示删除成功，列表更新数据。

  方法2：点击“例外VLAN列表”最后一列操作栏下的<删除>，提示“确定删除选中的VLAN ID”，点击<确定>提示“删除成功”，完成删除。

- **修改例外VLAN：**

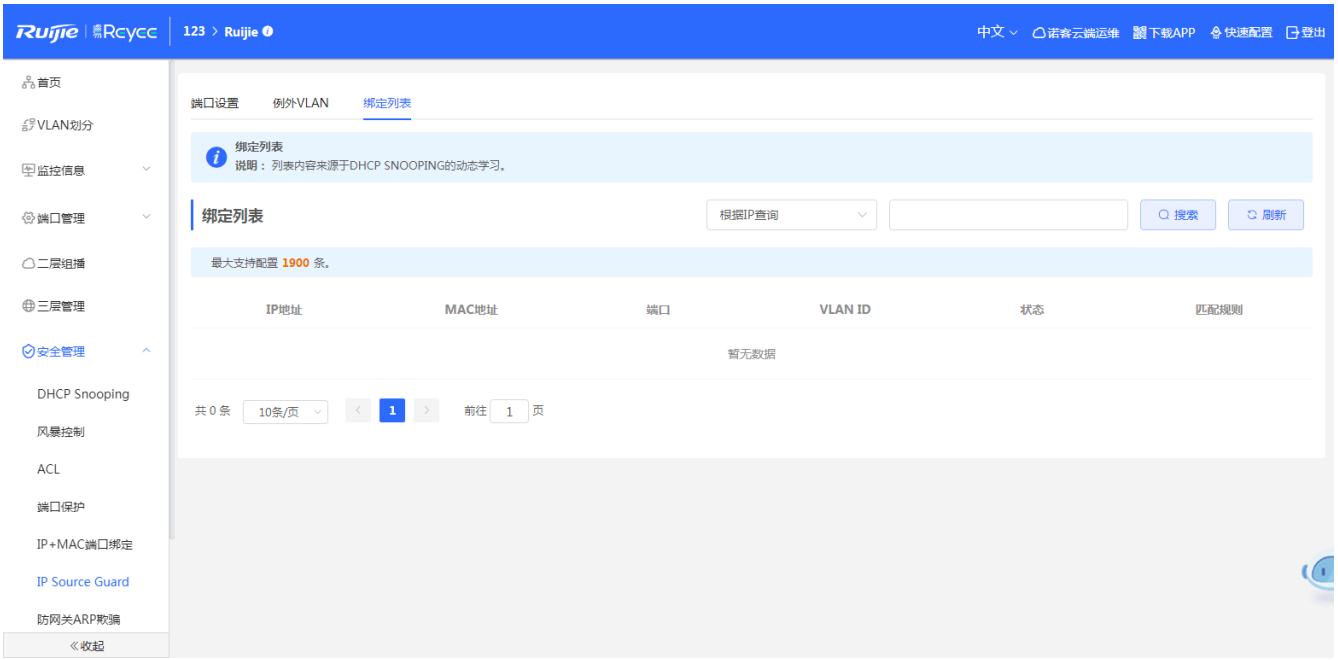
  在已经添加好例外VLAN列表中，点击“操作”中<修改>，在弹出框中修改该条表项的端口，点击<确定>提示“配置成功”后，会更新列表中的数据

说明

1. 通常在端口开启IP Source Guard功能后配置。
2. 最大支持配置64个例外VLAN，实际可配置数量以产品的SPEC为准。

3.7.6.3 绑定列表

绑定列表数据来源于 DHCP Snooping 的动态学习。IP Source Guard 功能根据绑定列表数据对 IP 报文进行过滤。



➢ **搜索：**

选择搜索类型（支持按MAC查询、按IP查询、按VLAN查询、按端口查询），输入搜索的字符串或选择端口，点击<搜索>，列表过滤出符合搜索条件的表项。

➢ **刷新：**

点击<刷新>重新获取最新的动态DHCP Snooping表项。

说明

最多支持1900条绑定数据，以产品的SPEC为准。

3.7.7 防网关 ARP 欺骗

配置防网关ARP欺骗功能，将在选中的端口上检查ARP报文的源IP地址，过滤源IP地址与配置的IP地址（网关IP地址）相同的ARP欺骗报文，能预防针对网关的ARP欺骗。

➢ **搜索：**

选择搜索类型（支持按MAC查询、按IP查询、按端口查询），输入搜索的字符串或选择端口，点击<搜索>，列表过滤出符合搜索条件的表项。

➢ **添加防网关ARP欺骗表项：**

点击<添加>，在弹出的框中输入IP、选择端口，点击<确定>提示“添加成功”，列表更新数据。

➢ **删除防网关ARP欺骗表项：**

方法1：在“防网关ARP欺骗表项列表”中勾选需要删除的表项，点击<批量删除>，在确认框中点击<确定>提示删除成功，列表更新数据。

方法2：点击“防网关ARP欺骗表项列表”最后一列操作栏下的<删除>，提示“确定删除选中的IP”，点击<确定>提示“删除成功”，完成删除。

➢ **修改防网关ARP欺骗表项：**

在已经添加好的防网关ARP欺骗表项列表中，点击“操作”中<修改>，在弹出框中修改该条表项的端口、IP，点击<确定>提示“配置成功”后，会更新列表中的数据

说明

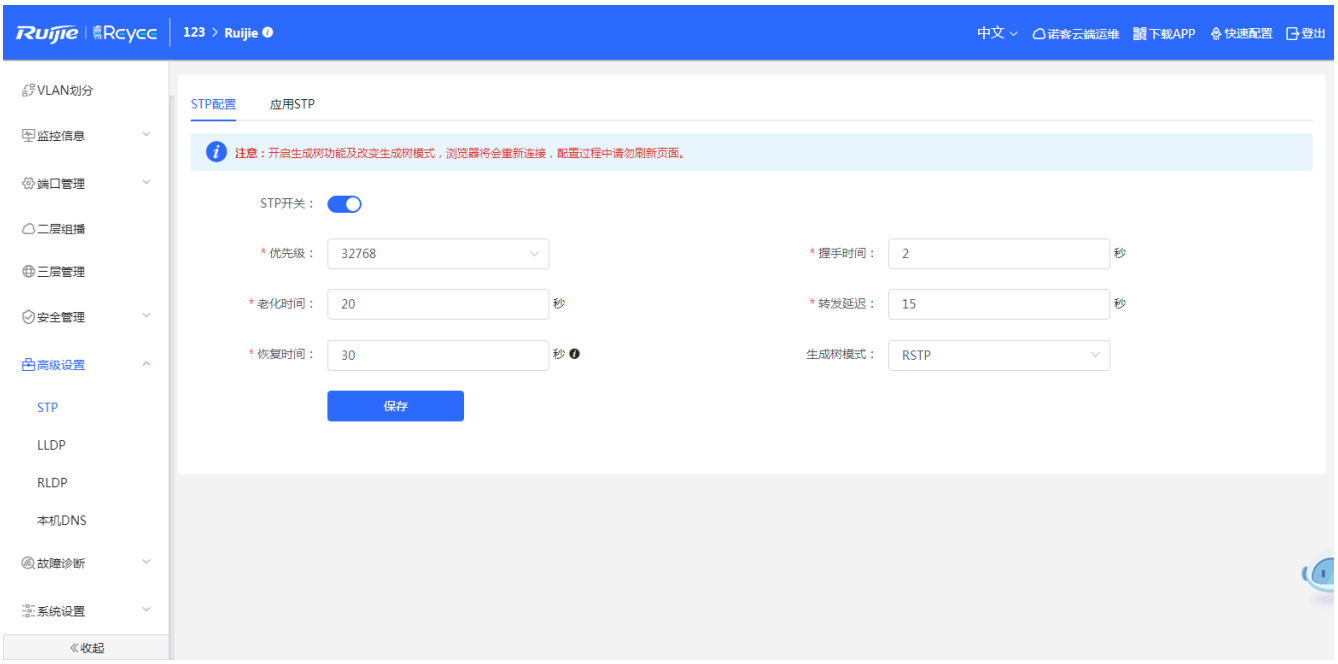
1. 防网关ARP欺骗列表最大支持配置256条数据，实际以产品的SPEC为准。
2. 一般在设备的下联口开启防网关ARP欺骗功能。

3.8 高级设置

高级设置包含STP、LLDP、RLDP、本机DNS配置。

3.8.1 STP

生成树协议是一种二层管理协议，它通过选择性地阻塞网络中的冗余链路来消除二层环路，同时还具备链路备份的功能。



➢ **全局STP配置：**

开启STP开关，配置STP全局参数，点击<保存>配置STP功能。

表 3-19 STP 参数

参数	说明	默认值
STP 开关	控制是否开启 STP 功能，全局生效，只有开启之后才能配置 STP 相关属性	关闭

参数	说明	默认值
优先级	桥优先级，在根桥选举的时候，设备会先比较桥优先级，数值越小优先级越高	32768
老化时间	表项老化时间，即网络中没有接收到新的报文，老化时间超时后表项会被删除	20 秒
恢复时间	网络中发生冗余链路时，网络恢复正常的时间	30 秒
握手时间	BPDU 的交互时间	2 秒
转发延时	BPDU 发送延时发送时间	15 秒
生成树模式	冗余链路使用的协议类型，目前支持 STP/RSTP	STP

➢ **端口应用STP：**

点击<批量设置>，选择端口并配置参数或点击“端口列表”操作栏<修改>并配置参数，然后点击<确定>完成端口应用STP。

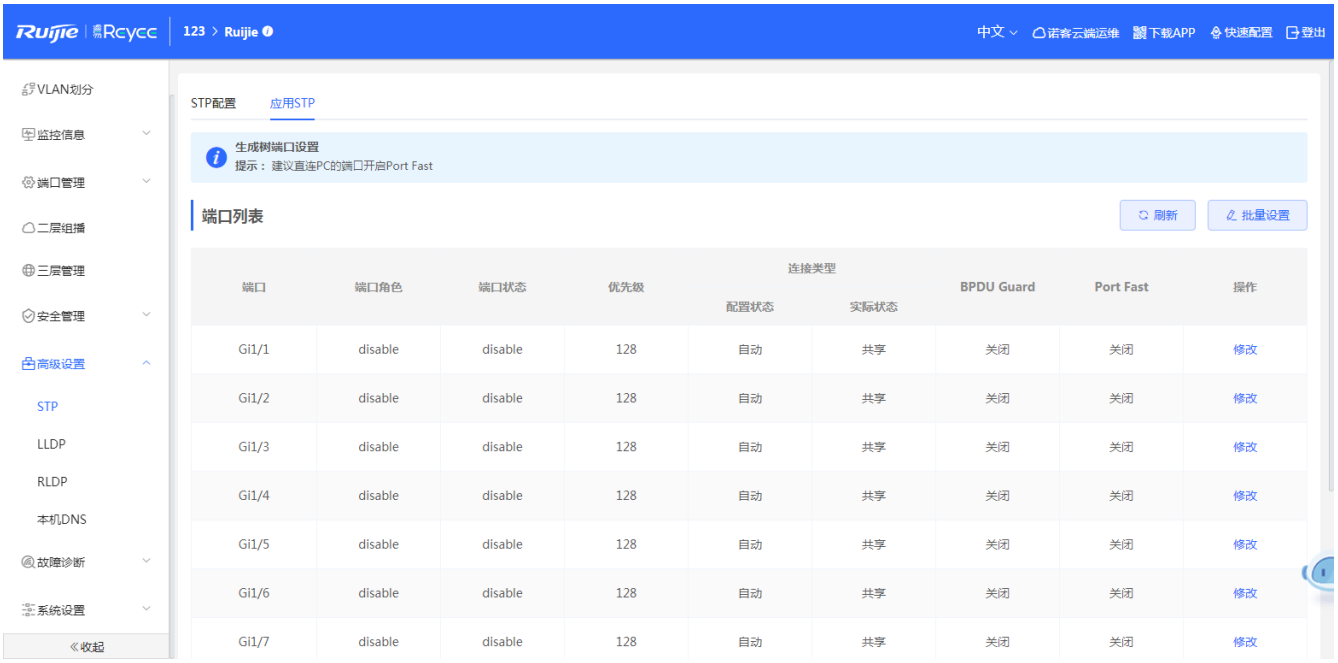


表 3-20 端口的 STP 参数

参数	说明	默认值
端口角色	根端口：存在于非根网桥上，非根交换机上距离根交换机最近的端口，根端口会将数据传送给根桥用于传输，是交换机端口去往跟桥的最佳路径。 指定端口：存在于非根网桥和根网桥上，对于根网桥来说，所有端口都为指定端口；对于非根网桥来说，指定端口根据需要与根交换机之间收发数据。	关闭

参数	说明	默认值
	备用端口：存在于非根网桥上，用来提供替代去往根网桥路径的端口，即替换当前根端口，工作在稳定拓扑中为阻塞状态。 禁用端口：存在于非根网桥和根网桥上，生成树中不起作用的端口	
端口状态	禁用(disabled) - 该端口只是相应网管消息，并且必须先转到阻塞状态。这种状态可以是由于端口的物理状（如端口物理层没有 up）态导致的，也可能是管理员手工将端口关闭。 阻塞(blocking) - 处于这个状态的端口不能够参与转发数据报文，但可以接收 BPDU 配置消息，并交给 CPU 处理。不过不能发送配置 BPDU 消息，也不能进行地址学习。 监听(listening) - 处于这个状态的端口不参与数据转发，也不进行地址学习，但可以接收并发送 BPDU 配置消息。 学习(learning) - 处于这个状态的端口不能转发数据，但是开始地址学习，并可以接收、处理和发送 BPDU 配置消息。 转发(forwarding) -一旦端口进入该状态，就可以转发任何数据，同时也进行地址学习和 BPDU 配置消息的接收、处理和发送。	关闭
优先级	端口的优先级	128
配置状态	端口是全双工时为点对点类型，端口是半双工时为共享类型，自动模式下端口根据双工模式确定接口类型	无
实际状态	共享，点对点，自动	共享
BPDU Guard	设置是否开启 BPDU 保护功能。开启后，如果某个端口开启了 Port Fast，或该端口自动识别为边缘配置口，但该端口收到了 BPDU，那么该端口就会关闭并进入 Error-disabled 状态，表示网络中可能被非法用户增加了一台网络设备，使网络拓扑发生改变	关闭
Port Fast	设置是否开启 Port Fast 功能，开启后端口将既不接收 BPDU，也不发送 BPDU，这样，直连该端口的主机就收不到 BPDU。而如果开启 Port Fast 的端口因收到 BPDU 而使 Port Fast Operational 状态 disabled，BPDU Filter 特性也就自动失效	关闭

说明

1. 开启生成树功能及改变生成树模式，浏览器将会重新连接，配置过程中请勿刷新页面。
2. 建议直连PC的端口开启Port Fast。
3. 开启STP是要30s以上端口才能变成转发，所以会出现短暂连接(不转报文)。

3.8.2 LLDP

3.8.2.1 功能概述

LLDP（Link Layer Discovery Protocol，链路层发现协议）是由 IEEE 802.1AB 定义的一种链路层发现协议。通过 LLDP 协议能够进行拓扑的发现及掌握拓扑的变化情况。通过 LLDP，网络管理系统可以掌握拓扑的连接情况，比如设备的哪些端口与其它设备相连接，链路连接两端的端口的速率、双工是否匹配等，管理员可以根据这些信息快速地定位及排查故障。

3.8.2.2 LLDP 配置

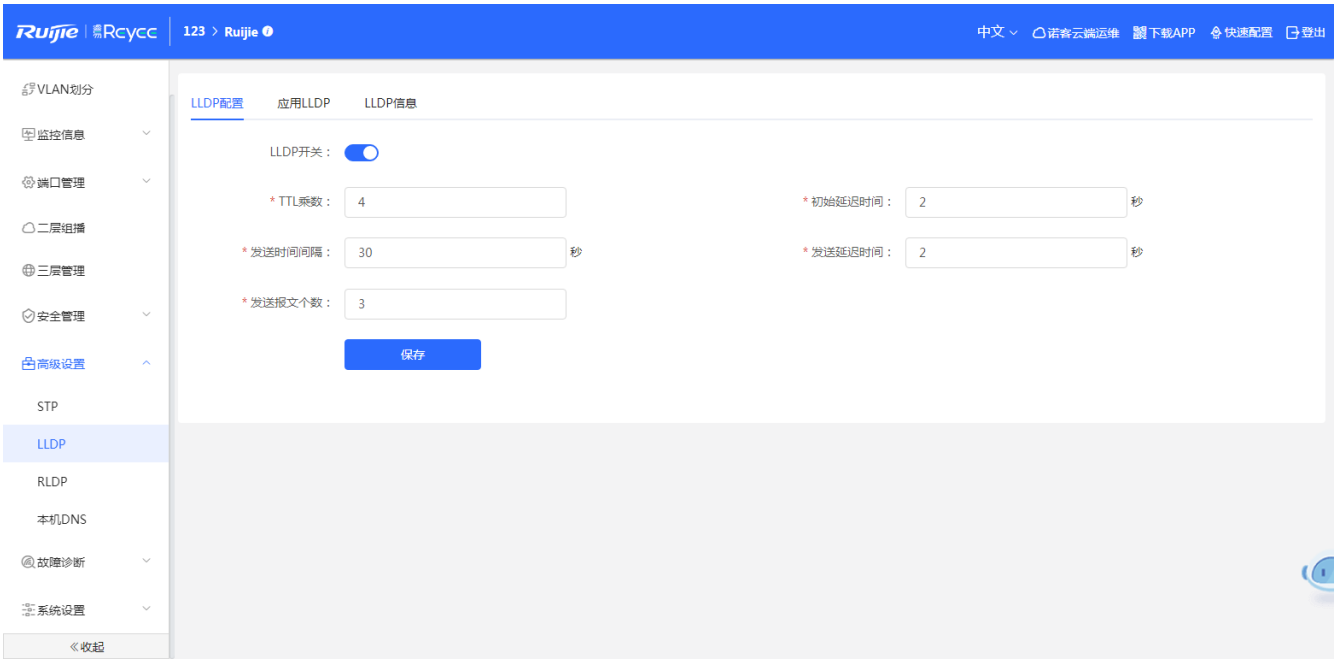


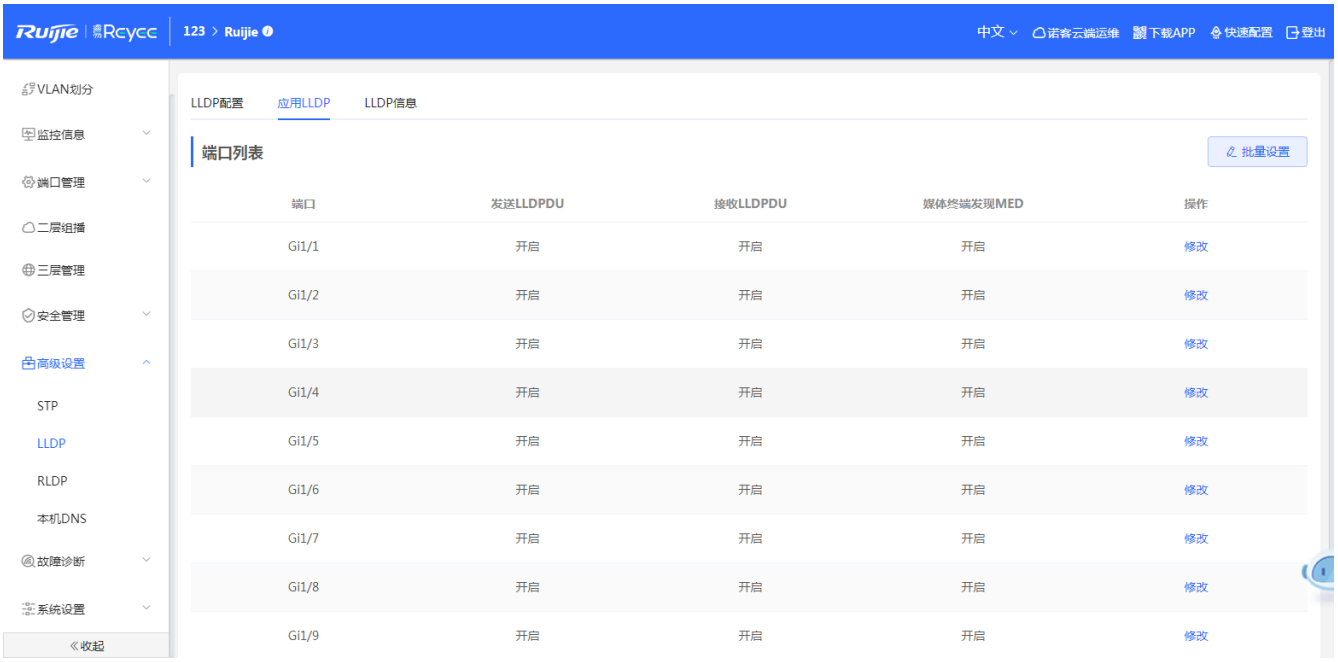
表3-21 LLDP参数

参数	说明	默认值
LLDP 开关	是否开启 LLDP	开启
TTL 乘数	LLDP 的 TTL 乘数	4
发送时间间隔	LLDP 报文发送时间间隔（单位为秒）	30
发送报文个数	发送的报文个数	3
初始延迟时间	端口初始化的延迟时间（单位为秒）	2
发送延迟时间	LLDP 报文发送延迟时间（单位为秒）	2

➢ **LLDP配置：**

开启LLDP开关并配置相关参数，点击<保存>进行LLDP配置。

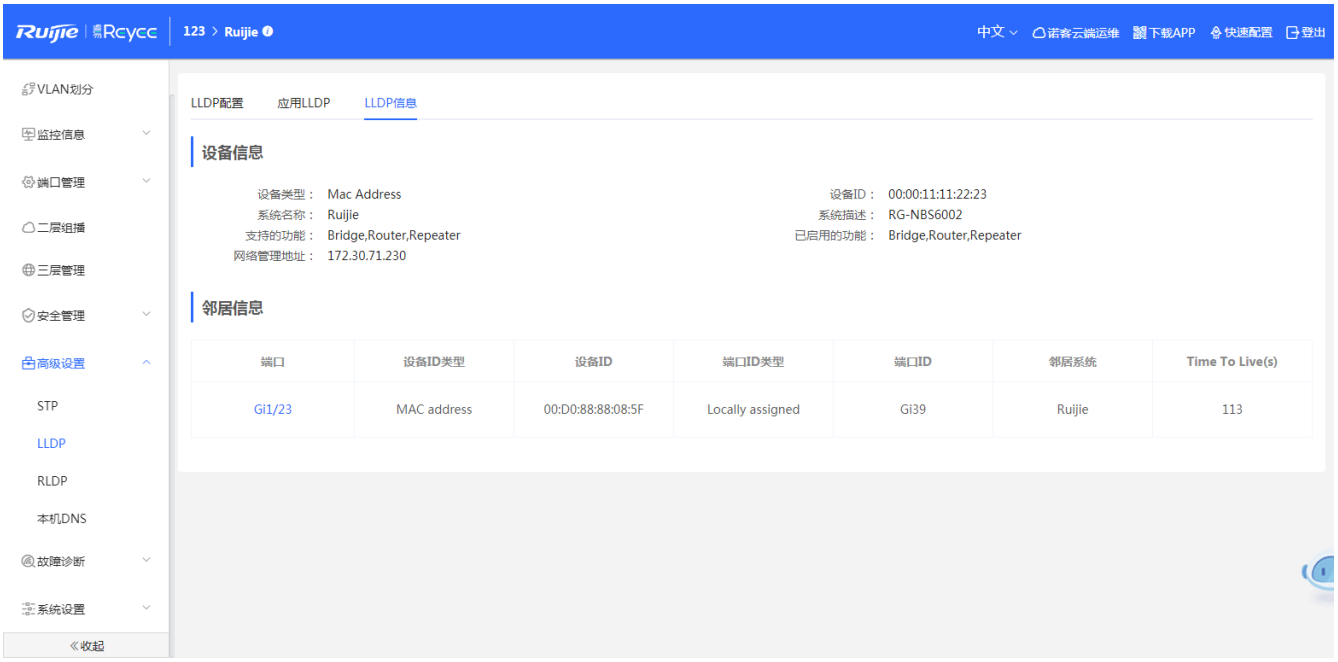
3.8.2.3 应用 LLDP



➢ **端口应用LLDP：**

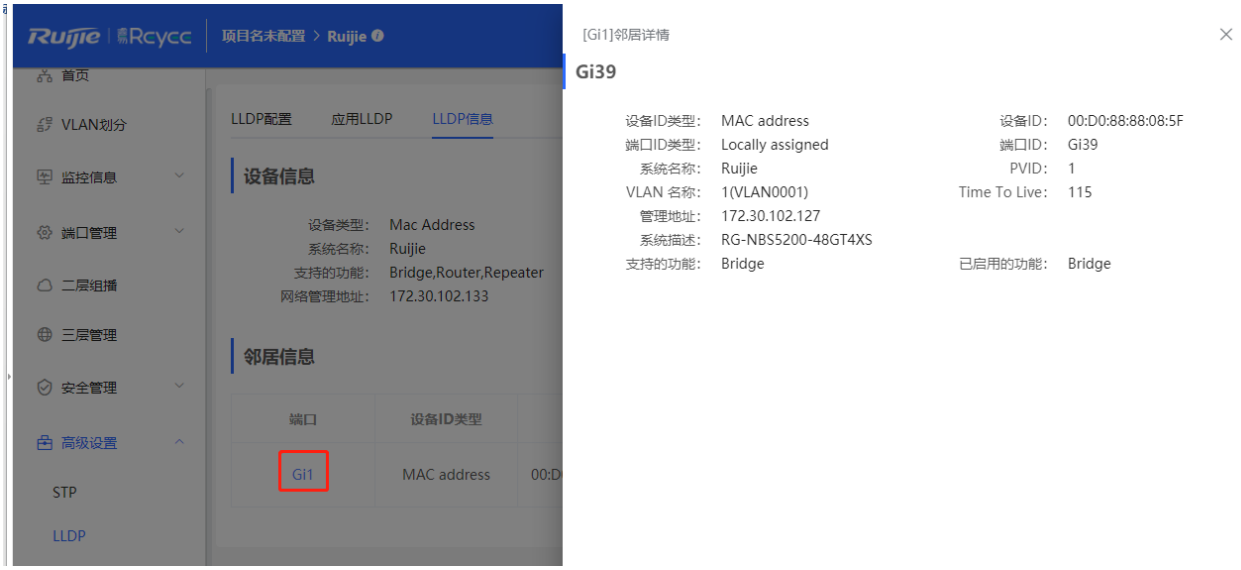
点击<批量设置>，选择端口点击“端口列表”操作栏<修改>，配置端口是否开启媒体终端发现MED功能以及是否接受或发送LLDPDU，然后点击<确定>完成端口应用LLDP。

3.8.2.4 LLDP 信息



➢ **LLDP设备信息：**

展示当前设备的信息及各个端口的邻居信息，点击<端口名称>可以查看该端口下邻居的详细信息。



说明

1. 可以利用LLDP查看拓扑连接情况，例如：网络拓扑中有若干交换机设备、MED 设备、NMS 设备。
2. 利用LLDP进行错误检测，例如：网络拓扑中有直连的两台交换机设备，错误配置信息将显示。

3.8.3 RLDP

➢ **概述**

RLDP 全称是 Rapid Link Detection Protocol，利用RLDP协议用户将可以方便快速地检测出以太网设备的链路故障，包括环路链路故障。单向链路故障、双向链路故障。

3.8.3.1 RLDP 配置

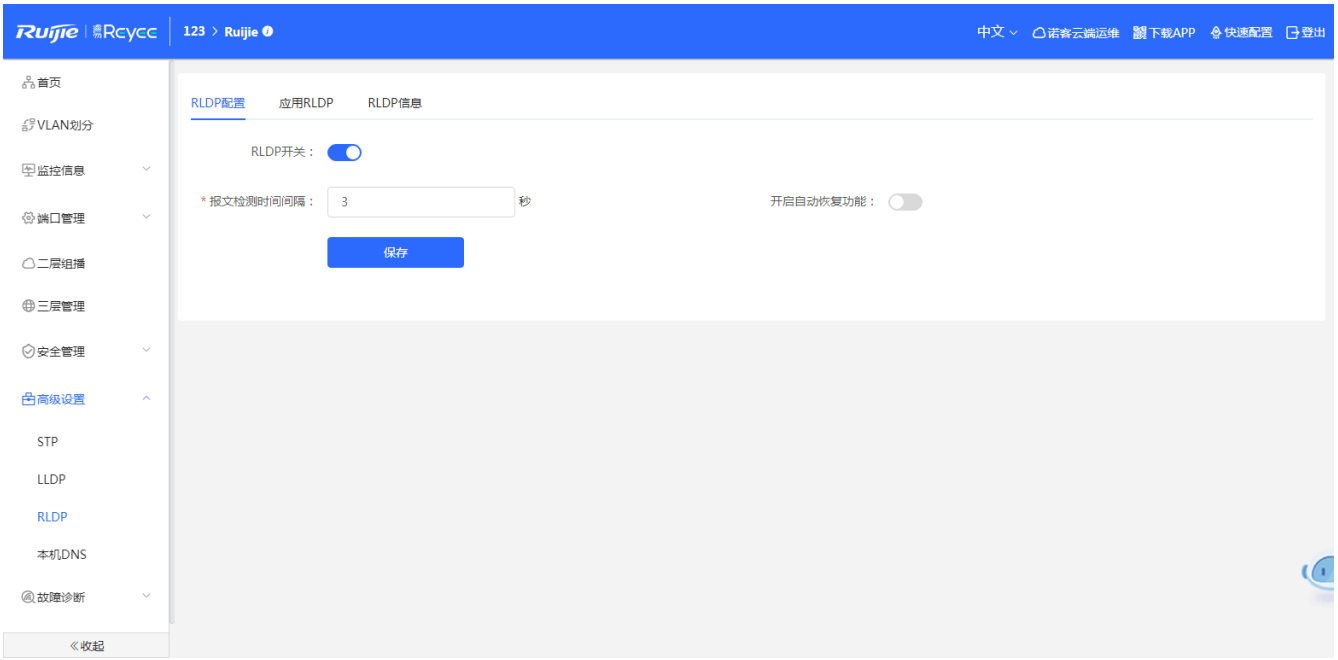


表 3-22 端口的 RLDP 参数

参数	说明	默认值
RLDP 开关	是否启用 RLDP 功能	关闭
报文检测时间间隔	RLDP 发送检测报文的时间间隔（单位为秒）	3s
开启自动恢复功能	开启后，端口发生环路后能自动恢复	关闭
定时自动恢复时间	端口发生环路之后自动恢复的响应时间（单位为秒）	30s

- **RLDP配置：**

  开启RLDP开关并配置相关参数，点击<保存>进行LLDP配置。

3.8.3.2 应用 RLDP

➢ **端口应用RLDP：**

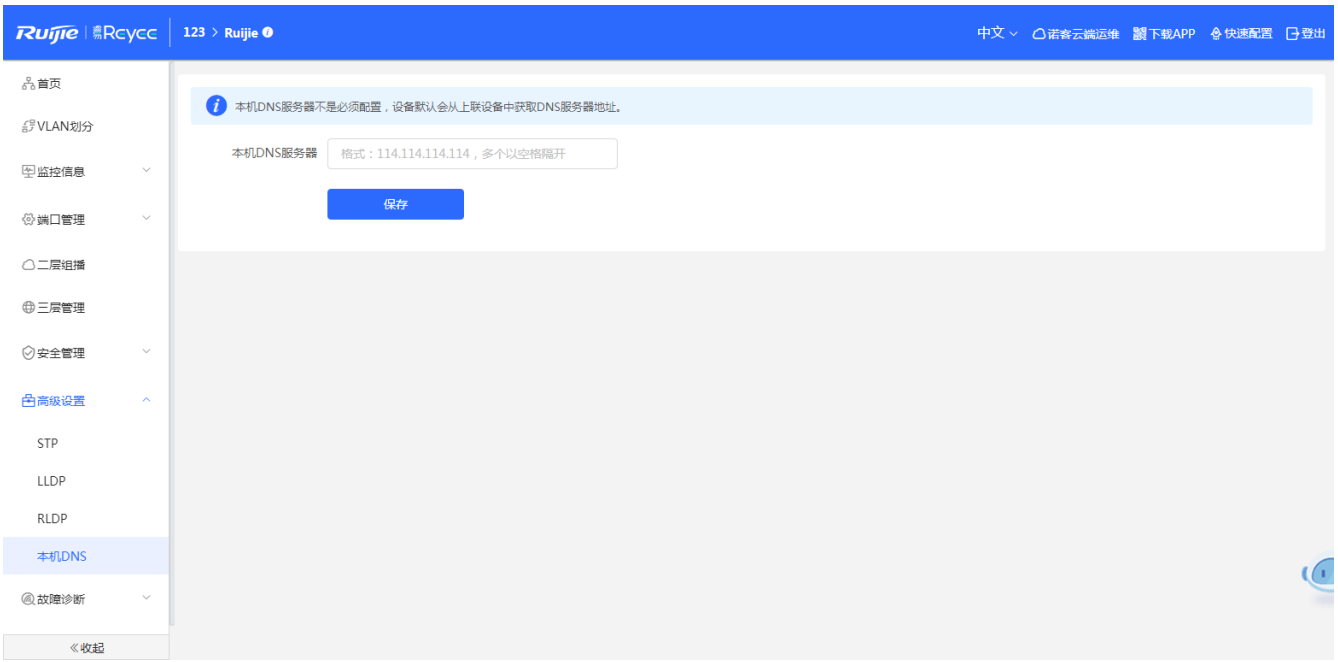
点击<批量设置>，选择端口或点击“端口列表”操作栏<修改>，配置端口是否开启环路检测和检测到链路故障后的处理方式（包括仅告警、告警并阻塞报文转发以及告警并关闭端口），然后点击<确定>完成端口应用RLDP。

3.8.3.3 RLDP 信息

➢ **RLDP信息：**

展示当前设备端口上的RLDP处理信息及各个端口的状态，点击<恢复故障端口>可以把端口触发的RLDP状态恢复为正常状态。

3.8.4 本机 DNS



➢ **配置DNS**

输入DNS服务器的IP地址，点击<保存>配置。

说明

1. 本机DNS服务器不是必须配置，设备默认会从上联设备中获取DNS服务器地址。
2. 配置后，报文优先使用管理IP的DNS，再使用此DNS。

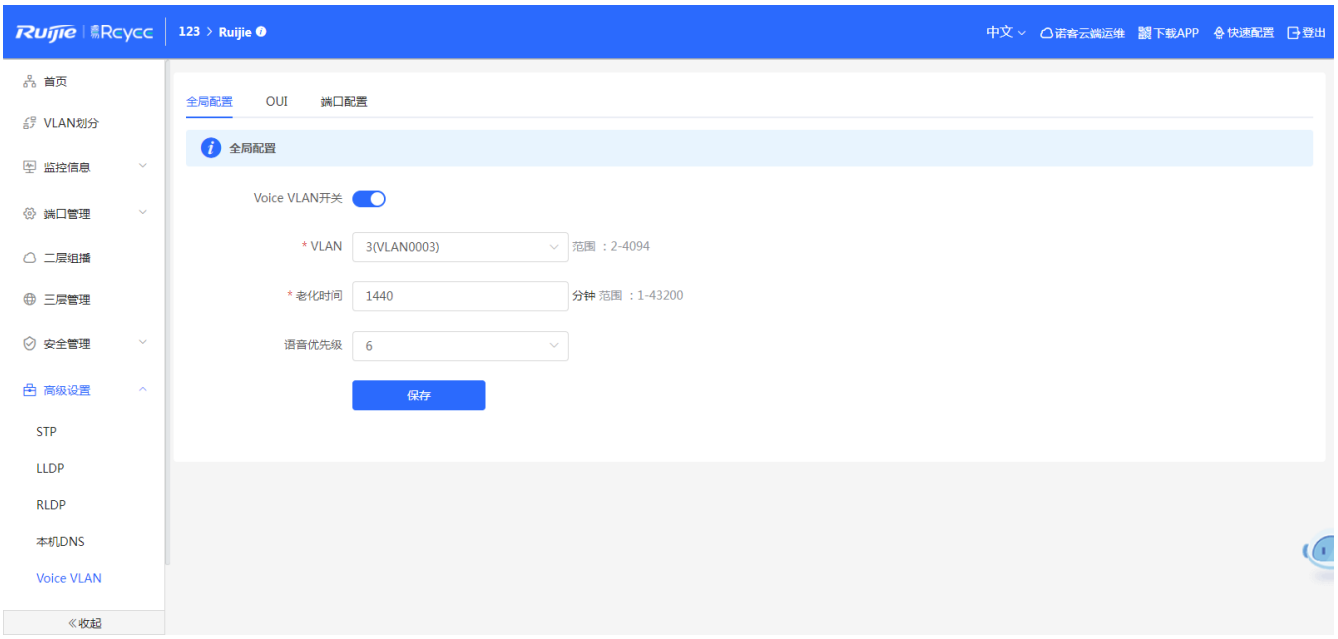
3.8.5 Voice VLAN

【页面向导】高级设置-> Voice VLAN

3.8.5.1 功能概述

Voice VLAN 是为用户的语音数据流专门划分的 VLAN。用户通过创建 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以使语音数据集中在 Voice VLAN 中进行传输，并对语音流进行有针对性的 QoS （Quality of Service，服务质量）配置，提高语音流量的传输优先级，保证通话质量。

3.8.5.2 全局配置

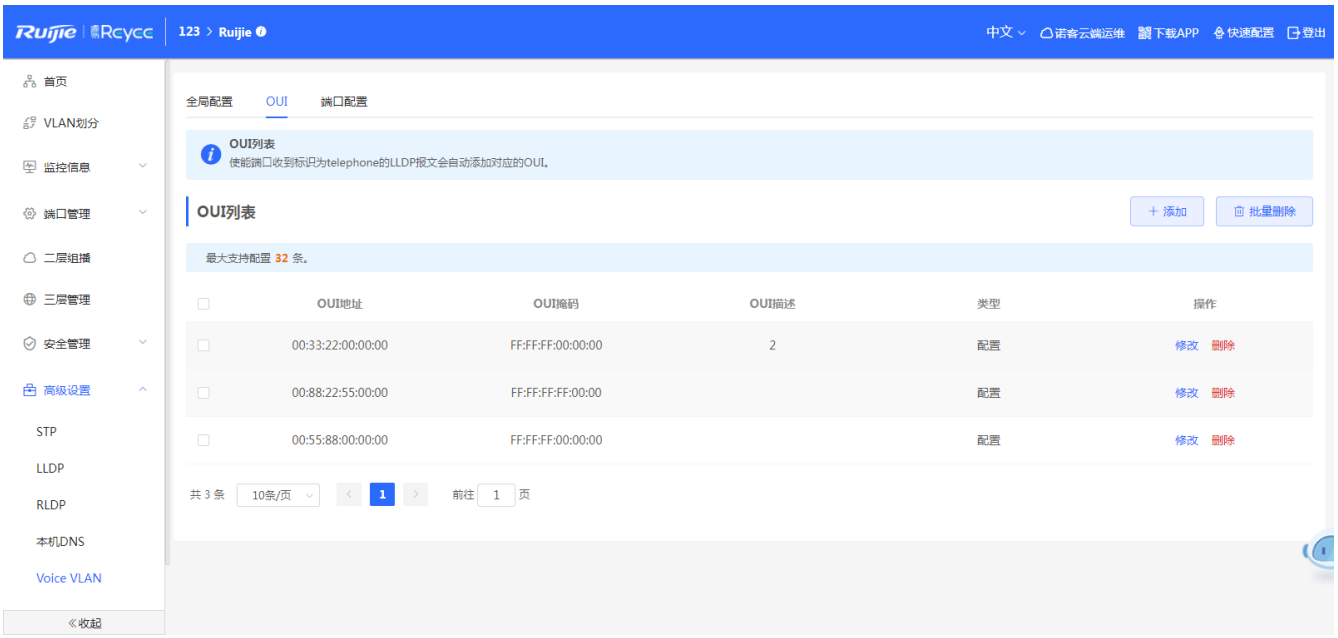


➢ **全局配置：**

开启Voice VLAN开关并配置相关参数，点击<保存>进行Voice VLAN全局配置。

3.8.5.3 OUI

语音报文的源 MAC 地址中包含了语音设备厂商的 OUI 信息，配置 Voice VLAN OUI 后，将 Voice VLAN OUI 和接收报文的源 MAC 地址进行比较，便可以识别出语音数据报文并将其划分到 Voice VLAN 中传输。



- **添加OUI：**

  点击<添加>，在弹出框中输入MAC地址，并选择MAC的掩码，点击<确定>添加一条OUI表项。

- **删除OUI：**

  勾选左边复选框点击<批量删除>或则点击列表操作栏<删除>，在确认框中点击<确定>删除OUI表项。

- **修改OUI：**

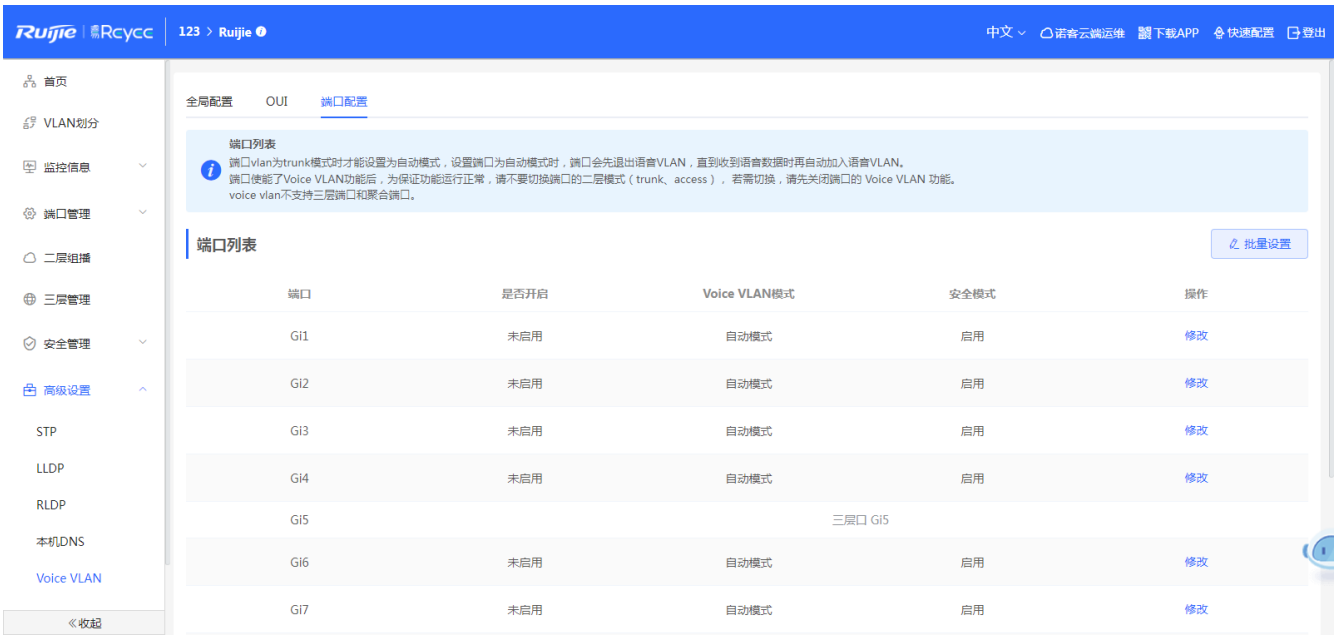
  点击列表操作栏<修改>，在弹出框中修改OUI描述，点击<确定>修改OUI。

说明

1.开启端口Voice VLAN功能后，本设备可以捕捉IP电话发出的LLDP协议报文，对协议报文中的设备能力字段进行识别，将能力为“Telephone”的设备识别为语音设备。而后将协议报文中的源MAC提取出来作为语音设备MAC进行处理，从而实现自动添加OUI。

2.支持系列：NBS3100,NBS3200,NBS5000；不支持系列：NBS6000,NBS7003,NBS7003

3.8.5.4 端口配置



➢ **开启端口Voice VLAN功能：**

点击端口右侧的<修改>或者<批量设置>，在弹出框中选择是否开启端口Voice VLAN功能和应用的Voice VLAN模式以及是否开启安全模式，点击<确定>更改端口设置。

自动模式：端口使能后检测端口的 Premit VLAN 是否包含 Voice VLAN，如果包含，就会把 Voice VLAN 从端口的 Premit VLAN 中删除掉，直到收到设定的 OUI 语音报文时，会自动把 Voice VLAN 加入到端口的 Premit VLAN 中。如果在全局设定的老化时间内，没有再次收到设定的 OUI 语音报文，端口会重新把 Voice VLAN 从端口的 Premit VLAN 中移除。

手动模式：端口的 Premit VLAN 包含 Voice VLAN 时，语音报文就可以在 Voice VLAN 中传输。

安全模式：安全模式打开时，Voice VLAN 只允许传输语音流，设备会对报文的源 MAC 地址进行检查，当报文源 MAC 地址是在 Voice VLAN OUI 表项范围内时，允许该报文在 Voice VLAN 内传输，否则将该报文丢弃。安全模式关闭时，不对报文的源 MAC 地址进行检查，所有报文均可在 Voice VLAN 内进行传输。

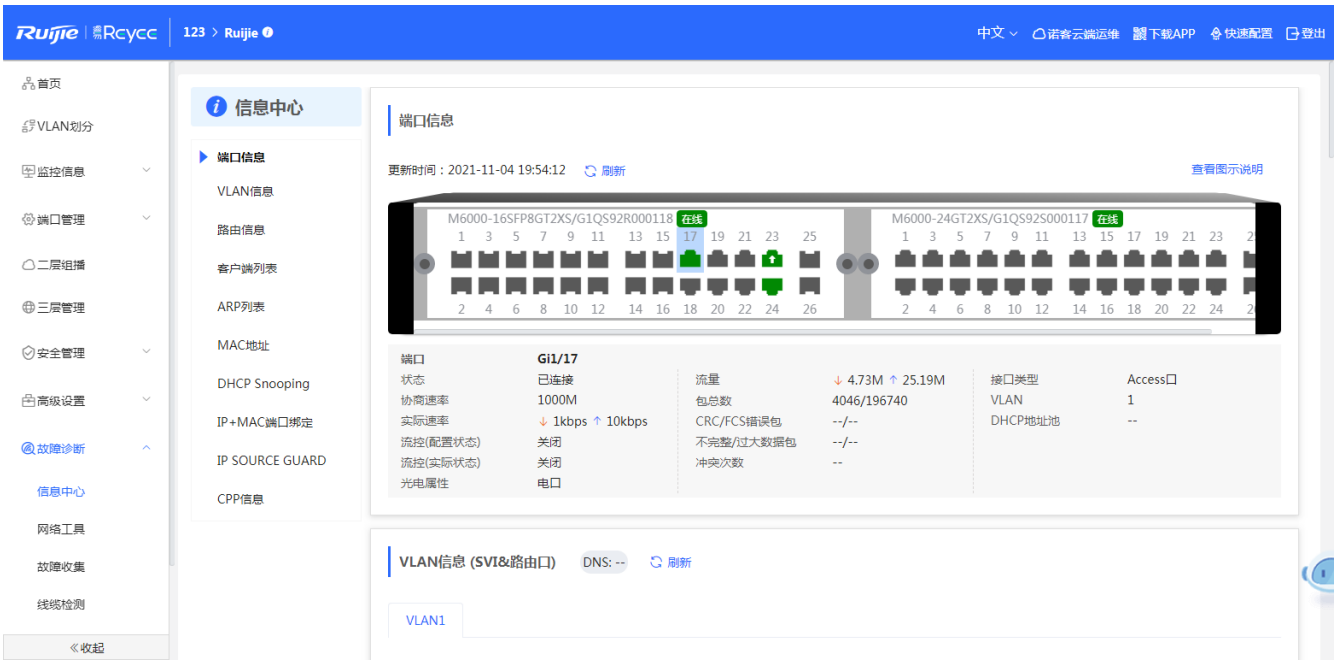
说明

1. 端口VLAN为trunk模式时才能设置为自动模式，设置端口为自动模式时，端口会先退出语音VLAN，直到收到语音数据时再自动加入语音VLAN。
2. 端口开启了Voice VLAN功能后，为保证功能运行正常，请不要切换端口的二层模式（trunk、access）， 若需切换，请先关闭端口的 Voice VLAN 功能
3. Voice VLAN不支持三层端口和聚合端口。

3.9 故障诊断

3.9.1 信息中心

信息中心可以查看到设备的端口流量、VLAN信息、路由信息、客户端列表、ARP列表、MAC地址、DHCP Snooping、IP+MAC端口绑定、IP Source Guard、CPP等状态和配置信息。



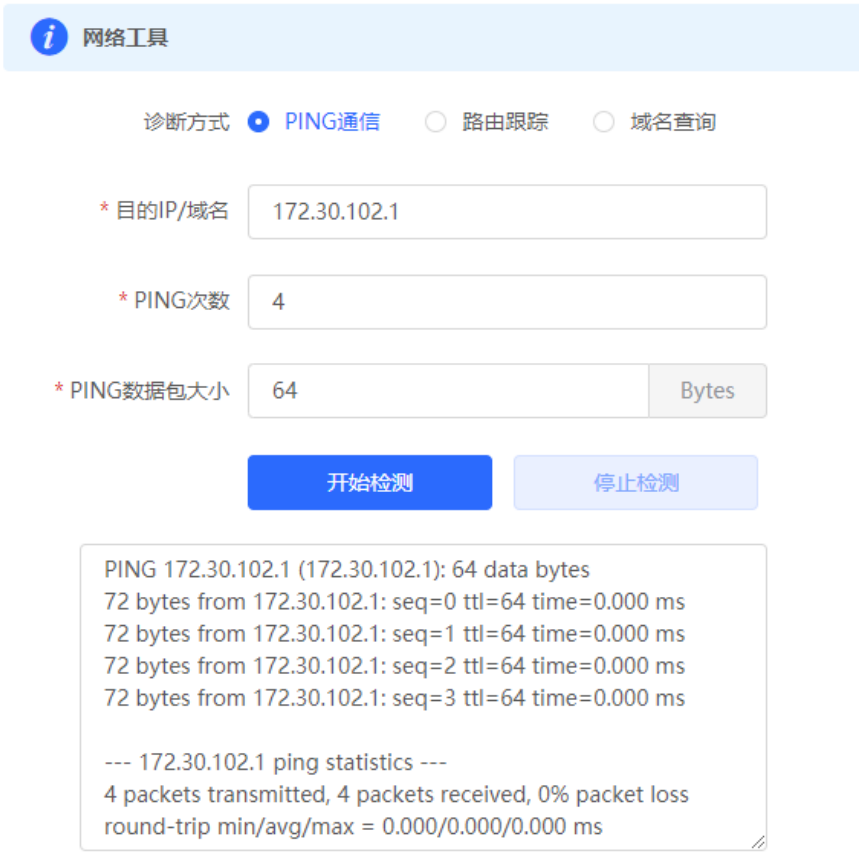
3.9.2 网络工具

网络检测工具提供 PING 通信、路由跟踪和域名查询三种命令检查网络状态。

3.9.2.1 PING 通信

“Ping”命令用于检查网络是否连通。

选择诊断方式为“PING 通信”，输入目的 IP 地址或网址、PING 次数及数据包大小，点击<开始检测>，测试设备与该 IP 或网址的网络连通性。显示“PING 通信失败”表示设备未与该 IP 或网址连通。



3.9.2.2 路由跟踪

路由跟踪功能用来识别一个设备到另一个设备的网络路径。在一个简单的网络上，这个网络路径可能只经过一个路由节点，甚至一个都不经过。但是在复杂的网络中，数据包可能要经过数十个路由节点才会到达最终目的地。在通信过程中，可以通过路由跟踪功能判断数据包传输的路径。

“路由跟踪（traceroute）”检测界面及结果：

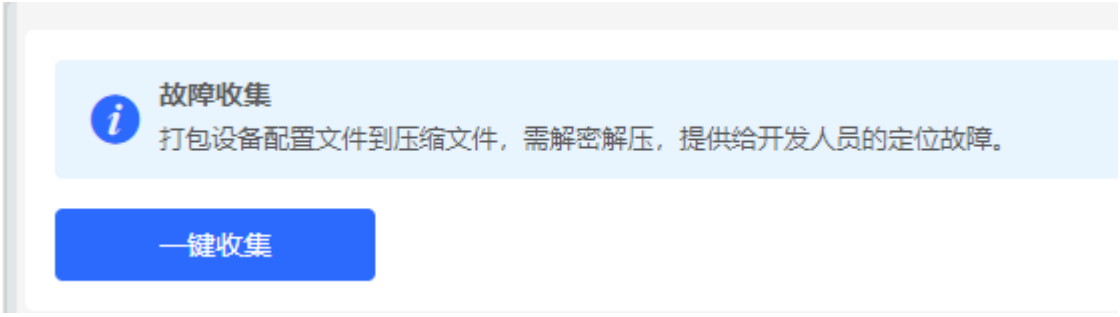
3.9.2.3 域名查询

域名查询功能用来查询 DNS 的记录，查看域名解析是否正常，在网络故障的时候用来诊断网络问题。若您的网页可以 Ping 通外网的 IP 地址但浏览器无法正常打开网页，可以尝试使用域名查询功能，检测域名解析是否正常。

“域名查询（nslookup）”检测界面及结果：

3.9.3 故障收集

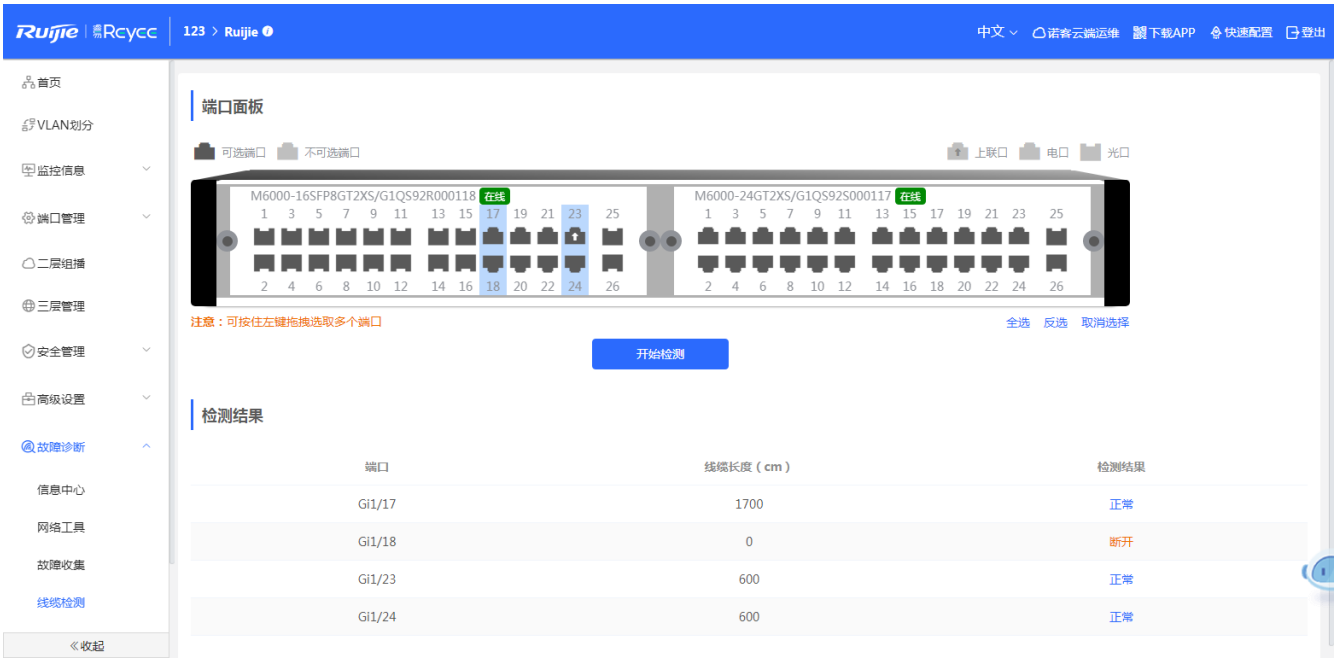
当设备出现未知原因的故障，可在此页面下执行一键故障收集命令来收集故障信息。点击<一键收集>，将会打包设备配置文件为压缩文件，下载到本地后，可提供给开发人员定位故障。



3.9.4 线缆检测

线缆检测可以检测出连接端口的线缆的大致长度以及线缆是否存在故障。

在端口面板上选择需要检测的端口，点击<开始检测>。检测结果将显示在下方。

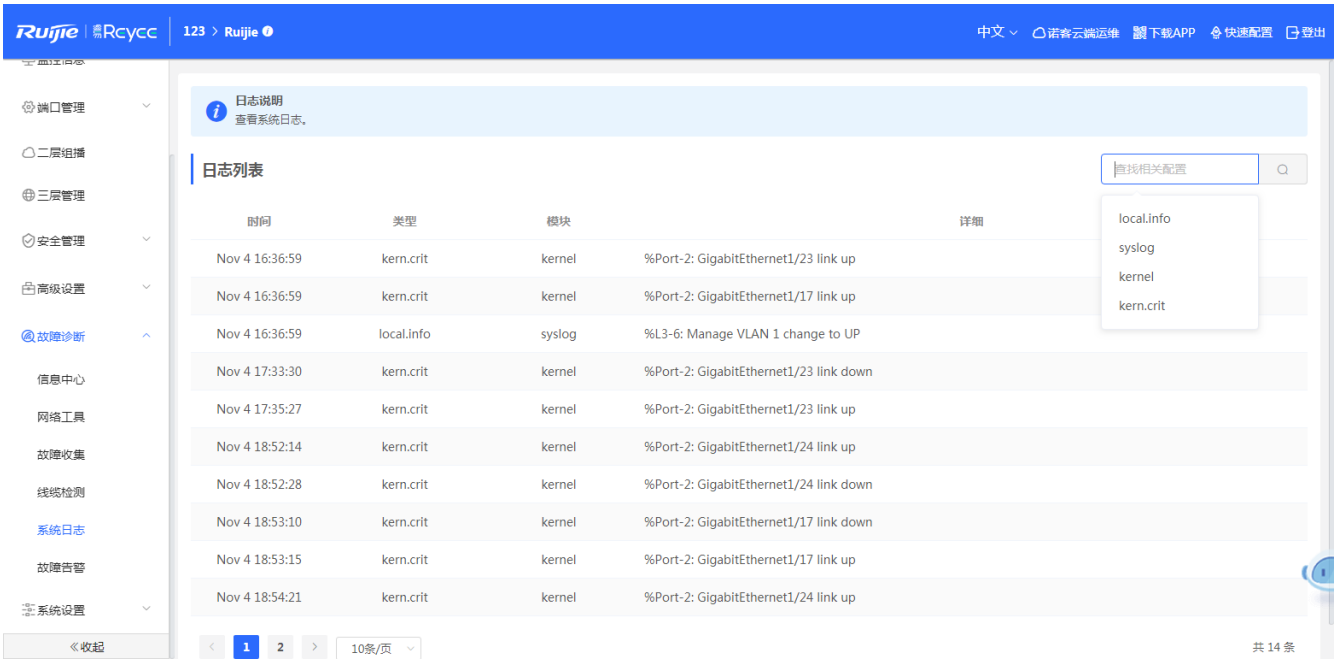


注意

若检测端口包含上联口，可能会造成网络连通闪断。请谨慎操作。

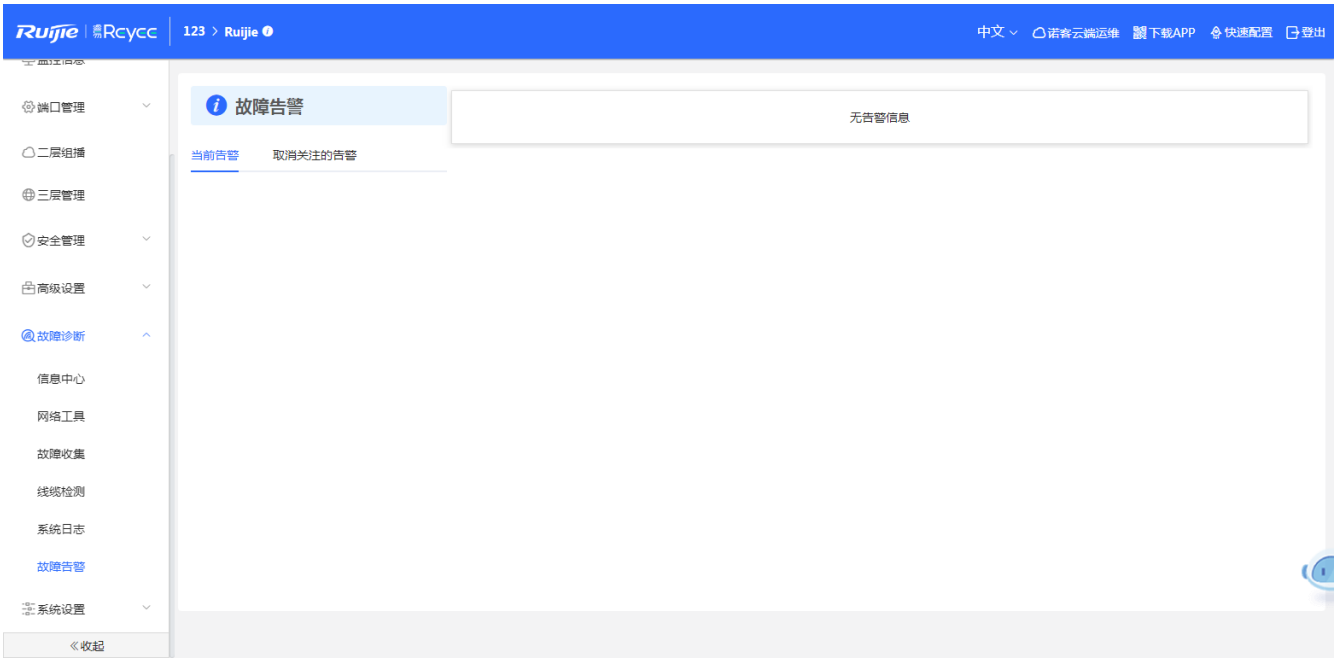
3.9.5 系统日志

系统日志清楚地记录了设备在什么时间、什么模块发生了什么操作，主要用于管理员进行监控设备运行情况、分析网络情况和定位问题。可以按照故障类型、故障模块以及故障信息中的关键字来搜索指定的日志信息。



3.9.6 故障告警

显示网络环境与设备可能存在的问题。用户可以在“当前告警”页面查看故障告警信息，并对告警信息进行删除或取消关注。



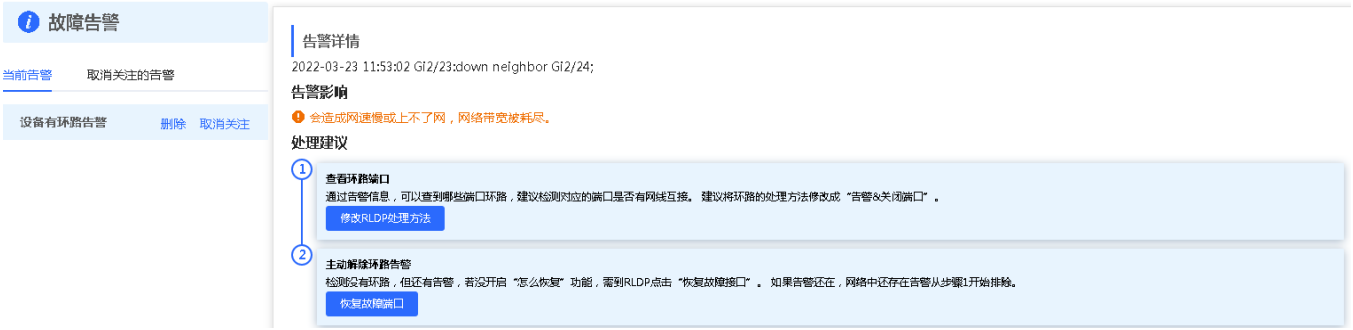
点击告警项对应操作列的<取消关注>按钮，可以取消关注此类告警，系统将不再出现该类告警信息。如需重新开启该类告警提示，可在“取消关注的告警”页面进行重新关注。

表 3-9-6 告警种类和支持产品线

告警类型	说明	支持产品	不支持产品
DHCP 地址池即将耗尽	当设备作为 DHCP Sever 时，被分配出去的地址池超过最大可分配地址数，就会产生告警提示用户	具体三层功能的产品,如：NBS5100/NBS5200/NBS6000/NBS7000	不支持三层功能的产品，如 NBS3100,NBS3200
本机与其他设备 IP 地址冲突	本机设备 IP 与当前局域网中的其它终端的 IP 地址存在冲突	全系的 NBS 产品：NBS3100,NBS3200/NBS5100/NBS5200/NBS6000/NBS7000	无
下联设备 IP 地址池冲突	连接在当前设备局域网下的设备中，有一台或一台以上的设备 IP 存在冲突	全系的 NBS 产品：NBS3100,NBS3200/NBS5100/NBS5200/NBS6000/NBS7000	无
MAC 地址表项满	二层的 MAC 地址表项超过产品的硬件容量	全系的 NBS 产品：NBS3100,NBS3200/NBS5100/NBS5200/NBS6000/NBS7000	无

告警类型	说明	支持产品	不支持产品
ARP 表项满	大网中的 ARP 表项，超过设备的 ARP 设备的容量	全系的 NBS 产品：NBS3100,NBS3200/NBS5100/NBS5200/NBS6000/NBS7000	无
PoE 进程未运行	设备 PoE 服务异常，无法供电	NBS 产品有 PoE 功能的设备(名称后面有“-P”字眼)	无
PoE 总功率过载	设备 PoE 总功率过载，无法为 PD 正常供电	NBS 产品有 PoE 功能的设备(名称后面有“-P”字眼)	无
设备有环路告警	局域网中的网络出现环路	全系的 NBS 产品：NBS3100,NBS3200/NBS5100/NBS5200/NBS6000/NBS7000	无

下面以“设备环路”为例：

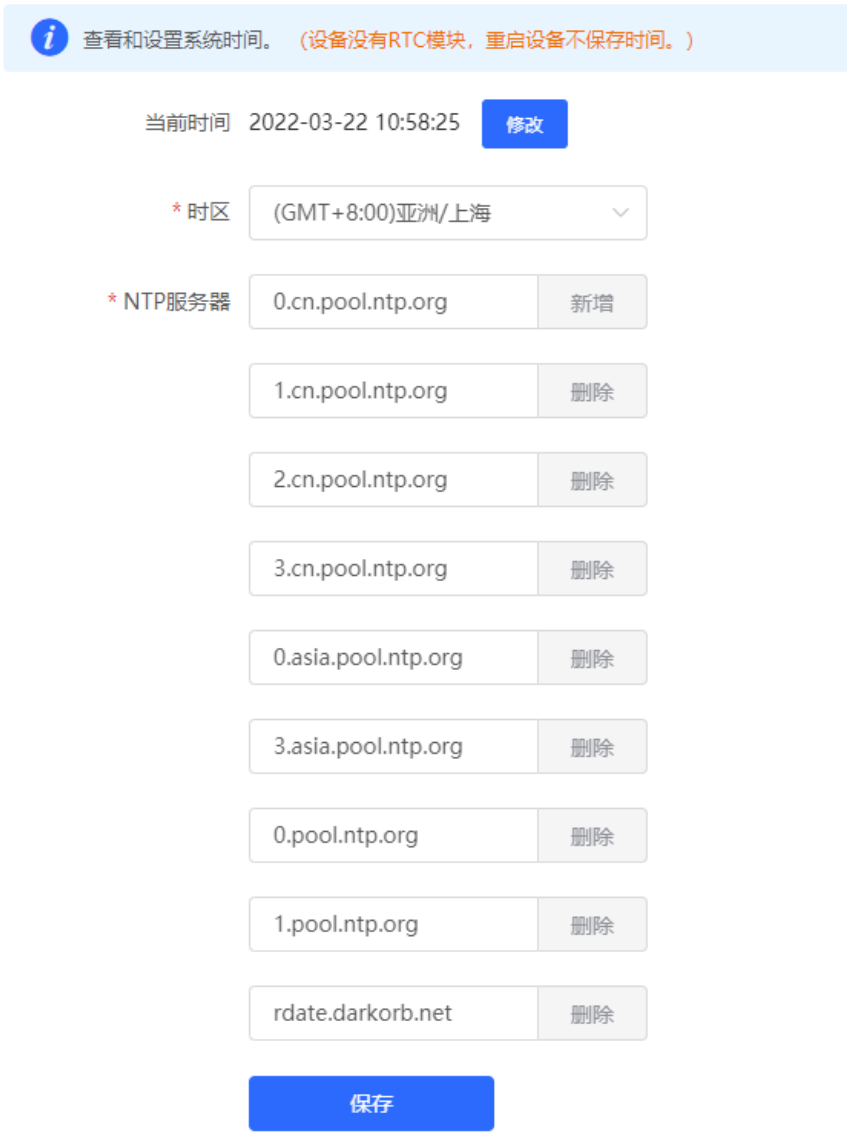


3.10 系统设置

3.10.1 系统时间

“系统时间”提供查看和设置系统时间的功能，用户可在此页面下修改系统时间，配置系统时区和 NTP 服务器。

若当前时间错误，请检查并选择当地所在的时区。若时区正确但时间仍有错误，点击<修改>可手动设置时间。同时设备支持设置 NTP 服务器（Network Time Protocol，网络时间服务器），从网络同步时间。默认多个服务器互为备份，如有本地服务器需求可根据需要增加或删除。



3.10.2 登录管理

3.10.2.1 登录密码

用户可以修改设备的登录密码。输入原设备密码和新设备密码，点击<保存>。修改设备密码成功后需要重新登录 Eweb 系统。

3.10.2.2 登录超时时间

在浏览器上登录设备 Eweb 后，若不退出登录，Eweb 系统默认允许用户在 1 小时内继续在当前浏览器上进行免验证访问，并在 1 小时后自动刷新页面并要求用户重新登录才能继续配置设备。可修改页面登录超时时间。

说明

Web访问超时时间默认为1小时（3600秒）。为保障设备安全性，建议用户在完成配置后及时登出Eweb系统。

3.10.3 配置管理

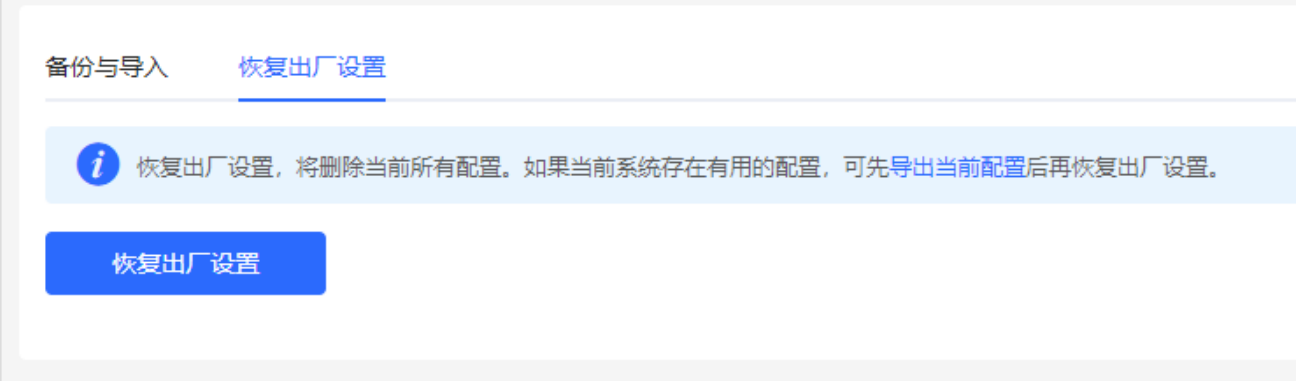
3.10.3.1 备份和导出

当完成交换机设备配置后，设备支持将配置文件导出，生成备份配置并下载到本地。

导出后的备份文件，支持在设备恢复出厂设置后进行导入，使设备恢复到导入的配置。

3.10.3.2 恢复出厂设置

点击<恢复出厂设置>按钮后确认，将恢复出厂设置。



注意

1. 建议在网络配置错误、组网环境变更等情况时使用此功能。如果发现无法访问Eweb，请参考2.1 准备配置，检查终端和设备是否已连通。
2. 当设备恢复出厂配置时，用户所有配置都会被清除，需要重新配置。云端设备会清除，需要重新添加。请谨慎操作。

点击<确认>后会恢复所有设置的默认值。建议在网络配置错误、组网环境变更等情况时使用此功能。如果发现无法访问 Web 了，可以参考准备配置里，检查终端和设备是否已联通。

3.10.4 系统升级

3.10.4.1 在线升级

本页面可以执行在线升级操作，如果联网检测到存在可升级的“在线版本”，界面会显示可升级的版本信息，如下：

点击<马上升级>按钮，设备会从网络上下载升级包，并升级版本。升级操作会保留当前设备的配置信息。您也可以选择“下载升级包”到本地，然后通过本地升级页面导入来升级版本。

如果网络上没有存在可升级的安装包，则显示如下界面：

3.10.4.2 本地升级

在本地路径下选取系统的升级包文件，点击<上传文件>按钮，设备会升级到您上传的升级包所对应的版本（升级包格式：xxxx.tar.gz）。

3.10.5 定时重启

点击<开启>，选择每周定时重启的日期和时间。点击<保存>后，下次系统时间匹配到定时时间时设备将重启。建议设置在凌晨或无人使用网络的时间段执行定时重启。

3.10.6 设备重启

提供重启设备按钮，如下：

点击<重启系统>并确认后，设备将重启。重启后需要重新登录 Eweb 管理系统。

重启过程中，请勿刷新或关闭页面，页面会检测当设备重启成功并且 Web 服务可用后，自动跳转到登录页。

4 常见问题

4.1 无法登录 Web

➢ **无法登录设备器 Web 管理界面该如何处理?**

请参考以下步骤:

1) 确认网线已正常连接到了设备的 LAN 口，对应的指示灯闪烁或者常亮。

2) 访问设置界面前，建议将计算机设置成“静态 IP 地址”，计算机的 IP 地址应设置为 10.44.77.X（X 为 2 至 254 之间任意整数），子网掩码为 255.255.255.0。

3) 使用 Ping 命令检测计算机与设备之间的连通性。

4) 若上述提示仍不能登录到设备管理界面，请将设备恢复为出厂配置。

4.2 忘记密码和恢复出厂配置

➢ **忘记设备用户名和密码怎么办？如何恢复出厂配置?**

忘记用户名密码时，可以通过设备上的 Reset 键，来恢复密码：通电状态下，长按 Reset 键 5 秒以上，待系统指示灯出现闪烁后松开 Reset，设备启动之后，登入 Eweb，在界面中，见下图，按照界面提示选择，恢复出厂配置，还是只恢复默认密码。

选择<恢复备份>：是恢复默认密码；

选择<删除备份>：是恢复出厂配置，即密码和配置都会被清除；

恢复出厂设置后，默认管理地址是 http://10.44.77.200。

4.3 IP 掩码

- **设备的某些功能设置需要填写子网掩码值划分地址范围，一般子网掩码都有哪些值?**

子网掩码是一个 32 位的二进制地址，以此来区别网络地址和主机地址。子网划分时，子网掩码不同，所得到的子网不同，每个子网能容纳的主机数目不同。

常用的子网掩码值有 8（即 A 类网络的缺省子网掩码 255.0.0.0）、16（即 B 类网络的缺省子网掩码 255.255.0.0）、24（即 C 类网络的缺省子网掩码 255.255.255.0）、32（即单个 IP 地址的缺省子网掩码 255.255.255.255）。