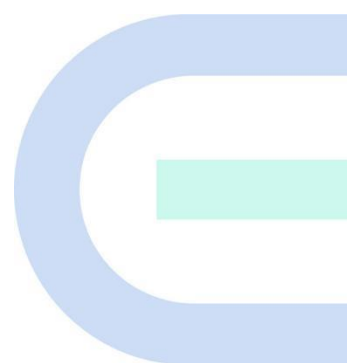


# RG-NBS7000 系列交换设备

OW3.0PJ17\_R71 WEB 管理手册



文档版本 V1.0

归档日期 2021-11-28

copyright © 2021 锐捷网络

## 版权声明

copyright © 2021 锐捷网络

保留对本文档及本声明的一切权利。

未得到锐捷网络的书面许可，任何单位和个人不得以任何方式或形式对本文档的部分或全部内容进行复制、摘录、备份、修改、传播、翻译成其他语言、将其部分或全部用于商业用途。

 **Ruijie 锐捷**、 **Ruijie**、 **Reyee** 和其他锐捷网络商标均为锐捷网络的商标。

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。

## 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](mailto:4001000078@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。

## 文档修订记录

修订日期	修订版本号	修订描述	修订人
2021-11-04	V0.5	初稿	林锦清
2021-11-5	V0.6	格式修改	黄双全
2021-11-15	V0.7	根据评审意见修改	黄双全
2021-11-30	V1.0	根据AQ评审意见修改	黄双全

# 目 录

前 言.....	1
1 概述.....	1
2 配置指南.....	2
2.1 准备配置.....	2
2.2 进入 Eweb 管理界面.....	3
2.3 Eweb 界面简介.....	5
2.3.1 整网信息区.....	6
2.3.2 头部导航栏.....	7
2.3.3 工作模式.....	8
2.3.4 菜单导航区.....	9
3 Eweb 配置 (独立模式).....	10
3.1 首页.....	10
3.2 VLAN 划分.....	11
3.2.1 VLAN 列表.....	12
3.2.2 端口列表.....	13
3.3 监控信息.....	15
3.3.1 端口信息.....	15
3.3.2 终端管理.....	16
3.4 端口管理.....	22
3.4.1 端口设置.....	23
3.4.2 聚合端口.....	25

3.4.3	端口镜像.....	27
3.4.4	端口限速.....	28
3.4.5	管理 IP.....	29
3.4.6	机箱管理 IP.....	30
3.5	二层组播.....	31
3.5.1	全局配置.....	32
3.5.2	IGMP Snooping.....	32
3.5.3	MVR 配置.....	33
3.5.4	组播组.....	33
3.5.5	端口过滤器.....	34
3.5.6	查询器.....	35
3.6	三层管理.....	36
3.6.1	三层口.....	36
3.6.2	客户端列表.....	37
3.6.3	静态地址分配.....	38
3.6.4	DHCP 选项.....	39
3.6.5	静态路由.....	40
3.6.6	ARP 列表.....	41
3.7	安全管理.....	42
3.7.1	DHCP Snooping.....	42
3.7.2	风暴控制.....	43
3.7.3	ACL.....	44

3.7.4	端口保护 .....	46
3.7.5	IP+MAC 绑定.....	47
3.7.6	IP Source Guard.....	48
3.7.7	防网关 ARP 欺骗.....	51
3.8	高级设置 .....	52
3.8.1	STP.....	52
3.8.2	LLDP.....	54
3.8.3	RLDP .....	56
3.8.4	本机 DNS .....	58
3.9	故障诊断 .....	58
3.9.1	信息中心.....	58
3.9.2	网络工具.....	59
3.9.3	故障收集.....	61
3.9.4	线缆检测.....	62
3.9.5	系统日志.....	63
3.9.6	故障告警.....	63
3.10	系统设置 .....	64
3.10.1	系统时间.....	64
3.10.2	登录管理.....	64
3.10.3	配置管理.....	66
3.10.4	系统升级.....	68
3.10.5	定时重启.....	69



3.10.6	设备重启.....	69
4	常见问题.....	71
4.1	无法登录 WEB.....	71
4.2	忘记密码和恢复出厂配置.....	71
4.3	IP 掩码.....	71

# 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。

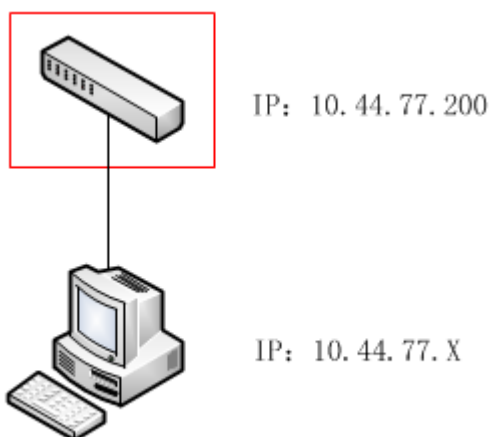
用户使用浏览器如（如 Chrome）访问 Eweb 管理系统来管理交换机设备。

## 2 配置指南

### 2.1 准备配置

#### 应用场景

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

图中红框内设备被访问的交换机设备，确保PC能够ping通该交换机设备就可以访问其Eweb管理系统。

#### 功能部属

##### 配置环境要求

客户端的要求：

- 网管使用 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。**特别注意如果您还在使用,IE6,7,8 请升级到 IE10, 11 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

**第一步：在您的浏览器地址栏中输入交换机设备的 IP 地址 10.44.77.200。您的 PC 当前 IP 地址必须与交换机设备的 IP 地址处在同一网段**



### 说明

1. 设备默认的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。
5. 设备管理IP为10.44.77.200，PC直连设备可进行管理配置。

### 第二步：快速配置

首次登录（初次配置）web 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。



点击<开始配置>

“网络名称” 标识设备所在的网络（首次使用时需要用户输入）

“管理密码” 设备 WEB 登录时的登录密码（**请勿忘记，仔细保存，若忘记可以见 [“4.2”](#)**）

“上网方式” 配置设备上网方式，分为动态 IP（DHCP，上联 DHCP 服务器分配 IP 地址）和静态 IP 方式（用户输入指定并符合格式的 IP 配置）

点击下载<完成配置>，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>，按照提示设备将跳过快速配置进入设备配置管理系统。

### 第三步：进入系统登录页面



图 2-1 登录页面

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

## 2.3 Eweb 界面简介

整网概览：



点击<配置>进入到交换机的管理界面：

名称：Ruijie      SN号：MACCMSWljq111      IP地址：172.30.71.230  
 MAC地址：00:00:11:11:22:22      软件版本：ReyeeOS 1.70.2303      硬件版本：1.00  
 DNS：172.30.44.20,192.168.5.28

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

**设备基本信息**

设备名称：Ruijie	管理IP地址：172.30.71.230	软件版本：ReyeeOS 1.70.2303
设备型号：NBS6002	MAC地址：00:00:11:11:22:22	系统时间：2021-11-03 20:41:47
联网状态：已联网	SN号：MACCMSWljq111	系统运行：6时 50分 58秒
工作模式：组网模式		

**设备工作模式**

设备温度：异常/0.0°C	电源版本：1.40	电源序列号：R253A2128142389
电源1在位信息：在位	电源功率：150W	电源状态：正常
电源类型：RG-PA150I-FS	电源版本：--	电源序列号：--
电源2在位信息：不在位	电源功率：--	电源状态：--
电源类型：--		

端口信息 查看图示说明

流量数据5分钟更新一次 刷新

### 2.3.1 整网信息区

在 Eweb 管理首页的左半部分是“整网信息区”，您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。

Ruijie | 易Rcycc

整网概览      整网设备的状态

交换管理      管理其它整网的设备

整网管理      整网管理

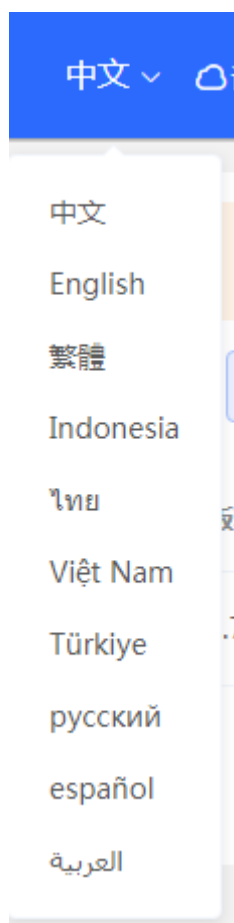
## 2.3.2 头部导航栏



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（“语言切换”、“诺客云端运维”、“下载 APP”、“快速配置”、“退出”）。

### 2.3.2.1 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。



### 2.3.2.2 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。



### 2.3.2.3 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 进行移动配置。

### 2.3.2.4 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。

### 2.3.2.5 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，Eweb 系统将在1小时内在此浏览器上免密码访问。

## 2.3.3 工作模式

设备工作模式有独立模式和组网模式两种，出厂模式下设备默认为组网模式。点击组网模式可以切换设备的工作模式。

The screenshot displays the 'Basic Information' (基本信息) section of the Eweb configuration page. It lists the following details:

- 设备名称: Ruijie
- 设备型号: NBS6002
- 联网状态: 已联网
- 工作模式: 组网模式 (highlighted with a red box)

Below this, the 'Smart Monitoring' (智能监控) section shows the device temperature as 'Abnormal/0.0°C' (异常/0.0°C).

To the right, a 'Notes' (说明) box contains the following instructions:

1. 模式切换后，设备IP可能发生改变。
2. 修改终端地址，让终端Ping通设备。
3. 浏览器输入新地址重新访问WEB系统。
4. 系统根据工作模式呈现不同的菜单项。

At the bottom of the notes box, there is a toggle switch for 'Self-network discovery' (自组网发现) which is currently turned on, and a 'Switch Mode' (切换模式) button.



说明

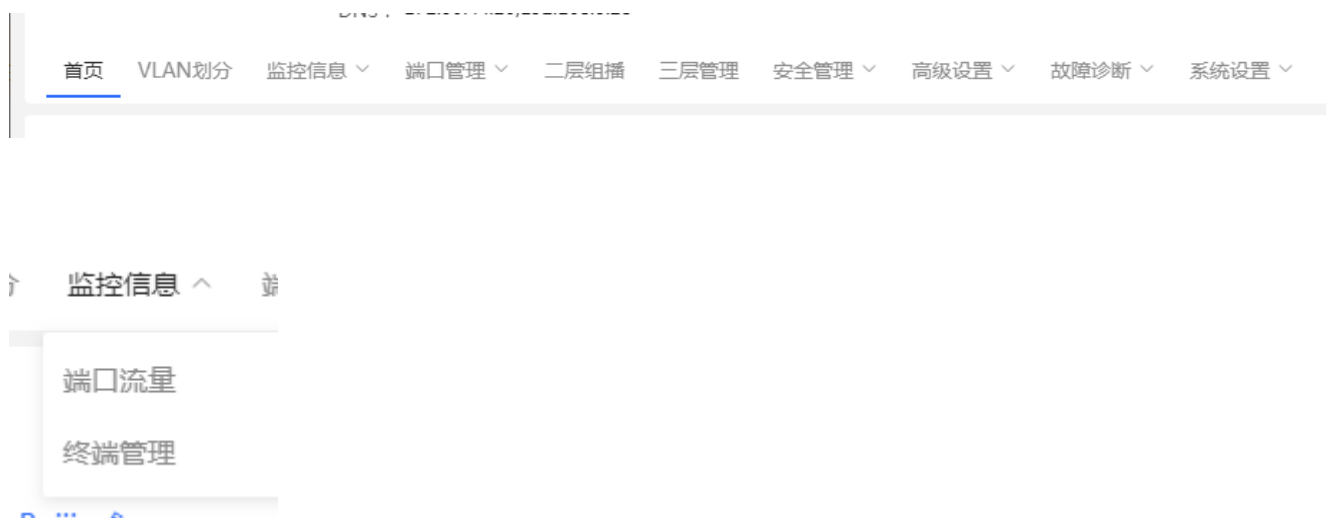
设备切换完模式，浏览器会刷新页面。

切换到独立模式下，导航栏在左侧：



## 2.3.4 菜单导航区

在 Eweb 管理页面的设有“菜单导航”区域，该区域列出了交换机的所有功能列表。当您点击相应菜单会打开详细的设置页面。菜单的组织方式可分为二级，当您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]



## 3 Eweb 配置 (独立模式)

### 3.1 首页

首页界面显示设备基本信息及交换机端口的基本信息，如下图：



“基本信息”中可以配置设备名称、管理 IP 的快捷链接及设备工作模式的切换（工作模式将在工作模式章节介绍）；

“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》，显示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, 如下:



点击端口面板上方的[刷新]可以获取最新的端口流量及状态信息。

## 3.2 VLAN 划分

VLAN 是虚拟局域网 (Virtual Local Area Network) 的简称, 它是在一个物理网络上划分出来的逻辑网络。这个网络对应于 ISO模型的第二层网络。

VLAN 有着和普通物理网络同样的属性, 除了没有物理位置的限制, 它和普通局域网一样。第二层的单播、广播和多播帧在一个 VLAN 内转发、扩散, 而不会直接进入其他的 VLAN 之中。

可以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是虚拟网络的一部分，并且整个网络可以支持多个 VLAN。当在 VLAN 中增加、删除和修改用户的时候，不必从物理上调整网络配置。VLAN 之间的通讯必须通过三层设备

WEB界面中，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。

### 3.2.1 VLAN 列表

VLAN列表 <span style="float: right;">+ 批量添加 + 添加 批量删除</span>				
最大支持配置 4094 条。(默认VLAN、管理VLAN、Native VLAN、SVI VLAN、MVR VLAN及Access VLAN不允许被删除。)				
<input type="checkbox"/>	VLAN ID	描述	端口	操作
<input checked="" type="checkbox"/>	1	VLAN0001	Gi1/1-Gi1/24,Te1/25-Te1/26,Gi2/1-Gi2/24,Te2/25-Te2/26	修改 删除
<input type="checkbox"/>	2	VLAN0002	--	修改 删除
<input type="checkbox"/>	3	VLAN0003	--	修改 删除
<input type="checkbox"/>	4	VLAN0004	--	修改 删除
<input type="checkbox"/>	5	VLAN0005	--	修改 删除

#### ➤ 添加VLAN:

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

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

#### ➤ 删除VLAN:

方法1: 在“VLAN 列表”中选择多条记录, 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>, 提示“确定”, 点击<确定>提示“删除成功”, 完成删除。

#### ➤ 编辑VLAN:

方法1: 点击“VLAN列表”最后一列操作栏下的<修改>, 在弹出框中可以修改VLAN描述, 点击<确定>提示“修改成功”, 完成编辑。

#### i 说明

1. VLAN范围为1-4094。
2. 默认vlan (vlan1)、管理vlan、native vlan及access vlan不允许被删除。
3. 批量添加的多个VLAN以‘,’英文逗号分隔, VLAN范围以‘-’中划线分隔。
4. 添加VLAN时, 没有配置描述系统将会创建对应格式的VLAN描述, 如: VLAN000XX, VLAN描述不可重复;
5. VLAN项目很多时, 进入VLAN划分页面加载时间会增加。
6. 不能被删除的vlan<删除>按钮是灰色的。

7. 若有三层的功能，vlan资源与路由口和L3AP(三层聚合)是共用用的，若vlan不足，会提示” 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，来确定这个端口能通过怎样的帧，以及这个端口可以属于多少个 VLAN。关于 VLAN 成员类型的详细说明，请看下表：

表 3-2-2 vlan 类型

端口类型	作用
Access 端口	一个 Access 端口，只能属于一个 VLAN，并且是通过手工设置指定 VLAN 的。
Trunk 端口 (802.1Q)	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， 也可以通过设置许可 VLAN 列表(Allowed-VLANs)来加以限制。

端口与 VLAN 关系的配置 (支持批量配置和单个端口配置)：

端口	端口模式	Access VLAN	Native VLAN	Permit VLAN	操作
Gi1/1	ACCESS	1	--	--	<a href="#">修改</a>
Gi1/2	ACCESS	1	--	--	<a href="#">修改</a>
Gi1/3	ACCESS	1	--	--	<a href="#">修改</a>
Gi1/4	ACCESS	1	--	--	<a href="#">修改</a>
Gi1/5	ACCESS	1	--	--	<a href="#">修改</a>
Gi1/6	ACCESS	1	--	--	<a href="#">修改</a>
Gi1/7	ACCESS	1	--	--	<a href="#">修改</a>
Gi1/8	ACCESS	1	--	--	<a href="#">修改</a>
Gi1/9	ACCESS	1	--	--	<a href="#">修改</a>
Gi1/10	ACCESS	1	--	--	<a href="#">修改</a>

#### ➤ 设置端口VLAN、修改：

方法 1：点击<批量设置>，弹出如下框，选择端口模式并选择需要配置的端口及配置 Native VLAN 或则 Access VLAN，点击<确定>提示“配置成功”完成编辑。

### 批量设置 ×

端口模式：

\* Native VLAN：

允许通过的VLAN：

\* 选择端口：

可选端口  不可选端口  聚合端口  上联口  电口  光口



注意：可按住左键拖拽选取多个端口 全选 反选 取消选择

方法 2：点击“端口列表”最后一列操作栏下选择端口的<修改>配置端口模式及 VLAN，点击<确定>提示“配置成功”完成编辑。

端口 : Gi1/1

✕

端口模式 :

\* Native VLAN :

允许通过的VLAN :

**i** 说明

1. 产品支持的 VLAN 遵循 IEEE802.1Q 标准, 最多支持 4094 个 VLAN(VLAN ID 1-4094), 其中 VLAN 1 是不可删除的默认 VLAN。
2. 许可配置的 VLAN ID 范围为 1-4094。
3. 当硬件资源不足的情况下, 系统将返回创建 VLAN 失败信息。
4. 端口VLAN配置不当(特别是上连口), 可能造成WEB访问不了, 需谨慎配置。

## 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:



端口信息

流量数据5分钟更新一次 [刷新](#)

<input type="checkbox"/>	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
<input type="checkbox"/>	Gi1/1	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi1/2	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi1/3	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi1/4	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi1/5	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi1/6	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi1/7	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi1/8	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi1/9	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi1/10	未连接	0/0	0.00/0.00	0/0	0/0	0/0	0

共 52 条  [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [>](#) 前往  页

点击<清除>、<全部清除>将清除端口流量等数据的统计信息。



说明

设备切换完模式，浏览器会刷新页面。

### 3.3.2 终端管理

#### 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

本文只涉及动态地址、静态地址与过滤地址的管理，组播地址的管理不在本文内描述，请参看《IGMP Snooping 配置指南》。

表 3-3-2 MAC 主要应用场景

端口类型	作用
动态地址学习	通过动态地址学习，实现报文的单播转发。
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、ARP 列表业务。

### 3.3.2.1 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)。

序号	MAC	VLAN ID	端口	类型
1	00:1A:A9:00:38:01	1	Gi1/23	动态
2	70:85:E8:78:B7:80	1	Gi1/23	动态
3	60:3A:7C:CE:B3:8C	1	Gi1/23	动态
4	00:D0:F8:18:92:60	1	Gi1/23	动态
5	70:85:E8:78:B6:41	1	Gi1/23	动态
6	08:00:27:66:05:F4	1	Gi1/23	动态
7	E0:05:C5:F0:47:F7	1	Gi1/23	动态
8	00:74:9C:72:70:83	1	Gi1/23	动态
9	00:D0:F8:32:20:65	1	Gi1/23	动态
10	00:74:9C:71:00:38	1	Gi1/23	动态

#### ➤ 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。

#### **i** 说明

1. MAC表项根据不同的设备具有不同的容量 (例如上面截图设备容量为32K)。
2. 搜索功能, 支持模糊搜索。

### 3.3.2.2 静态 MAC 地址

配置设备的静态MAC地址;

显示用户手工绑定网络设备的MAC地址与端口关系。

The screenshot shows the '静态MAC地址' (Static MAC Address) configuration page in the Eweb interface. The page title is 'MAC地址表' (MAC Address Table) and the sub-header is '静态MAC地址'. A note explains that static MAC addresses are used for forwarding data based on MAC addresses. The table below shows one entry:

端口	MAC地址	VLAN ID	操作
Gi1/1	00:11:22:33:44:55	1	删除

The page also includes a '+ 添加' (Add) button and a '批量删除' (Batch Delete) button. The table indicates a maximum support of 256 entries.

#### ➤ 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号, 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“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。

#### 说明

交换机在转发数据时, 需要根据MAC地址表来做出相应转发, 手工方式绑定设备下接的网络设备的MAC地址与端口关系, 如添加一个静态地址, 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。

### 3.3.2.3 动态 MAC 地址

设备学习到的动态MAC信息。

MAC地址表 静态MAC地址 动态MAC地址 过滤MAC地址 MAC基础配置 ARP列表

MAC地址表 基于MAC清除 格式: 00:11:22:33:44:55 清除 刷新

序号	MAC	VLAN ID	端口
1	00:1A:A9:00:38:01	1	Gi1/23
2	60:3A:7C:CE:B3:8C	1	Gi1/23
3	00:D0:F8:18:92:60	1	Gi1/23
4	70:B5:E8:78:B6:41	1	Gi1/23
5	08:00:27:66:05:F4	1	Gi1/23
6	E0:05:C5:F0:47:F7	1	Gi1/23
7	00:74:9C:72:70:83	1	Gi1/23
8	00:D0:F8:32:20:65	1	Gi1/23
9	00:74:9C:71:00:38	1	Gi1/23
10	00:D0:F8:20:91:11	1	Gi1/23

共 88 条 10条/页 < 1 2 3 4 5 6 ... 9 > 前往 1 页

智能小香哥，有问必答

#### 清除:

选择清除类型 (支持基于MAC、基于VLAN、基于端口的清除), 输入搜索的字符串, 点击<清除>, 设备将清除符合条件的MAC表项。

#### 刷新:

点击<刷新>重新获取最新的动态MAC表项。

### 3.3.2.4 过滤 MAC 地址

显示用户手工方式绑定设备下接的网络设备的MAC地址与端口关系, 用于过滤符合此条件的数据包。

过滤MAC地址

说明：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MAC地址时，将丢弃此报文，不进行转发。应用场景如某个用户发起ARP攻击时，可以将其配置为过滤地址，防止攻击。

MAC地址表

最大支持配置 256 条。

MAC地址	VLAN ID	操作
00:11:22:33:44:55	1	删除

共 1 条 10条/页 < 1 > 前往 1 页

#### ➤ 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。

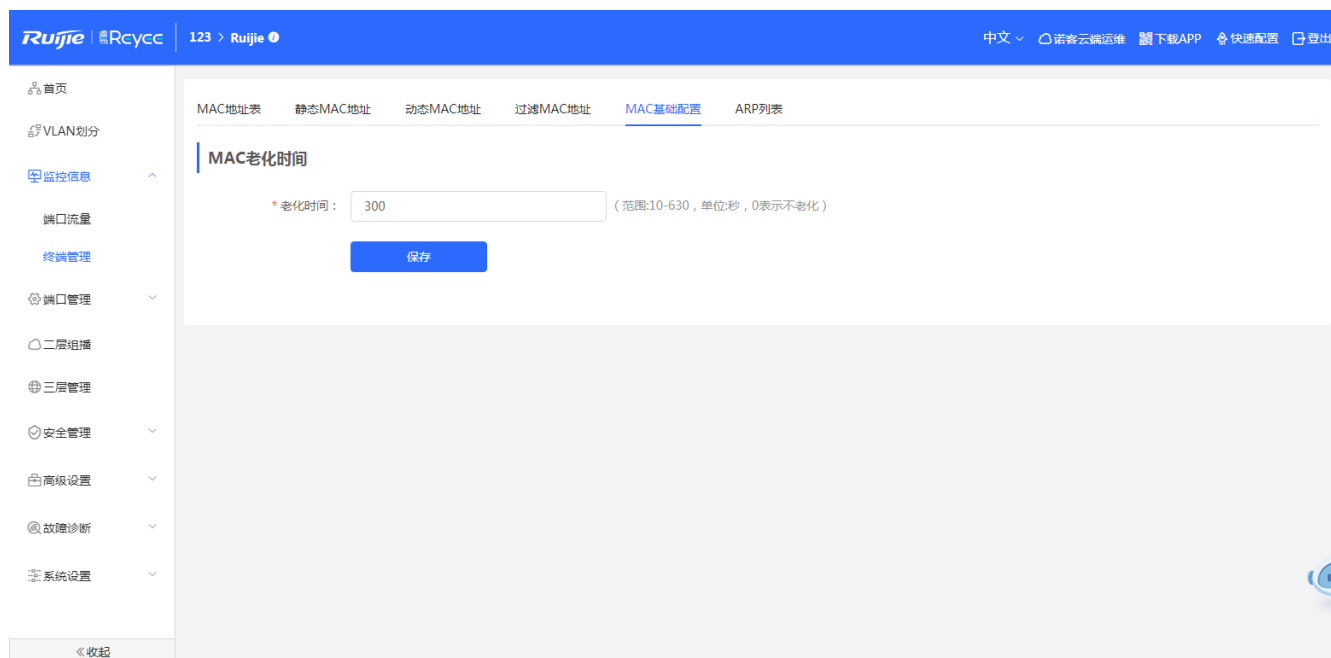
方法2：点击“MAC列表”最后一列操作栏下的<删除>，提示“确定删除选中的MAC”，点击<确定>提示“删除成功”，完成删除。

#### **i** 说明

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MAC地址时，将丢弃此报文，不进行转发。应用场景如某个用户发起ARP攻击时，可以将其配置为过滤地址，防止攻击。

### 3.3.2.5 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”配置设备MAC老化时间。

#### 说明

设备老化时间范围: 10~630, 单位:秒, 0表示不老化。

### 3.3.2.6 ARP 列表

ARP(Address Resolution Protocol, 地址解析协议)是用来绑定 MAC 地址和 IP 地址的, 以 IP 地址作为输入, ARP 能够知道其关联的 MAC 地址。一旦知道了 MAC 地址, IP 地址与 MAC 地址对应关系就会保存在设备的 ARP 缓存中。有了 MAC 地址, IP 设备就可以封装链路层的帧, 然后将数据帧发送到局域网上去。缺省配置下, 以太网上 IP 和 ARP 的封装为 Ethernet II 类型。

The screenshot shows the 'ARP列表' (ARP List) page in the Eweb configuration interface. At the top, there is a search bar labeled '查找IP地址/MAC地址' with a search icon and a '刷新' (Refresh) button. Below the search bar is a table with the following data:

序号	IP地址	MAC地址
1	172.30.71.38	c0:b8:e6:00:00:01
2	172.30.71.207	c0:b8:e6:7c:f2:7c
3	172.30.71.191	40:b0:34:3a:48:fd
4	172.30.71.198	58:69:6c:00:00:06
5	172.30.71.143	d8:9e:f3:3f:9c:22
6	172.30.71.119	00:1a:a9:00:38:01
7	172.30.71.204	00:d8:d8:d8:d8:56
8	172.30.71.142	00:d0:f8:15:08:5c
9	172.30.71.242	00:d0:f8:33:34:f9
10	172.30.71.188	50:9a:4c:42:0caa

#### ➤ 搜索:

ARP列表支持根据IP、根据MAC来搜索ARP列表。

#### ➤ 刷新:

点击<刷新>, 重新获取最新的ARP表项。

#### 说明

端口包含聚合口, 聚合口流量为成员口流量的总和。

## 3.4 端口管理

### ➤ 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)。

### ➤ 接口类型

表3-4 接口类型

操类型	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	本章介绍

	之相关的第二层协议。	
二层聚合端口	<p>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）。</p> <p>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。</p>	本章介绍
SVI 口	<p>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。创建一个交换虚拟接口很简单，用户可通过 interface vlan 接口配置命令来创建 SVI 接口，然后给交换虚拟接口分配 IP 地址来建立 VLAN 之间的路由。</p>	详见“ <a href="#">3.6 三层管理</a> ”
路由端口	<p>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。</p>	详见“ <a href="#">3.6 三层管理</a> ”
三层聚合端口	<p>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。</p>	详见“ <a href="#">3.6 三层管理</a> ”

### 3.4.1 端口设置

端口基础配置包含端口开关、双工速率、流控以及端口物理等信息配置。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。



### 3.4.1.1 基本配置

端口	端口开关	双工/速率		流控		操作
		配置状态	实际状态	配置状态	实际状态	
Gi1/1	开启	自动/自动	未知/未知	关闭	关闭	修改
Gi1/2	开启	自动/自动	未知/未知	关闭	关闭	修改
Gi1/3	开启	自动/自动	未知/未知	关闭	关闭	修改
Gi1/4	开启	自动/自动	未知/未知	关闭	关闭	修改
Gi1/5	开启	自动/自动	未知/未知	关闭	关闭	修改
Gi1/6	开启	自动/自动	未知/未知	关闭	关闭	修改
Gi1/7	开启	自动/自动	未知/未知	关闭	关闭	修改

#### ➤ 编辑端口：

方法1：点击<批量设置>，弹出配置框，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>配置。

方法2：点击列表项<修改>，弹出配置框，选择端口状态、速率、模式等，点击<确定>配置。

#### 说明

1. 同属性端口（千兆口、万兆口、光口等）可配置的项（比如速率）不一样。
2. 量配置时，可选配置项为所选端口的共有集合（及所有口公共的交集）。

### 3.4.1.2 物理配置

物理配置

配置交换机端口物理信息 (光口不支持开启EEE; 当聚合口成员为复用口时不支持光电模式切换)

端口列表

端口	EEE	模式	描述	MTU	操作
Gi1/1	关闭	fiber模式		1500	修改
Gi1/2	关闭	fiber模式		1500	修改
Gi1/3	关闭	fiber模式		1500	修改
Gi1/4	关闭	fiber模式		1500	修改
Gi1/5	关闭	fiber模式		1500	修改
Gi1/6	关闭	fiber模式		1500	修改
Gi1/7	关闭	fiber模式		1500	修改
Gi1/8	关闭	fiber模式		1500	修改

#### 端口编辑:

方法1: 点击<批量设置>, 弹出配置框, 首先选中需要配置的端口, 然后选择EEE、端口模式, 输入端口描述, 点击<确定>配置。

方法2: 点击列表项<修改>, 弹出配置框, 选择EEE、端口模式, 输入端口描述, 点击<确定>配置。

#### 说明

1. 不同端口属性配置项有所不同。
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, 不支持电口和光口同时配置。

## 3.4.2 聚合端口

### 概述

Aggregate Port (简称 AP) 是将多个物理链接捆绑在一起形成一个逻辑链接, 可以用于扩展链路带宽, 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。

比如两台设备之间, 单个端口相连最多为 1000M (假定两台设备的端口都为 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, 而端口聚合将可以解决这一问题。例如, 使用若干根网线连接这两台设备, 再将这若干个端口进行聚合绑定, 这样这些端口就逻辑捆绑形成了  $1000M * n$  的最大流量。

比如，如果两台设备是通过单个网线相连接，当这两个端口之间出现链路断开时，这条线路上承载的业务就会断掉，而如果将多个互连的端口进行聚合绑定，只要有一条链路没有出现链路断开，那么在那些端口上承载的业务就不会断掉。

### ➤ AP模式

AP 模式包含静态 AP (支持) 和动态聚合 (不支持)：

静态 AP 模式是一种利用手工配置模式直接将物理端口加入到 AP 聚合组中，在物理端口的链路状态和协议状态准备好的情况下，就能进行数据报文转发的一种聚合模式。

静态 AP 模式下的 AP 接口，称为静态 AP 口，对应的成员口称为静态 AP 成员口。

LACP 是一个关于动态链路聚合的协议，它通过协议报文 LACPDU(Link Aggregation Control Protocol Data Unit, 链路聚合控制协议数据单元)和相连的设备交互信息。

LACP 模式下的 AP 接口，称为 LACP AP 口，对应的成员口称为 LACP AP 成员口。

### ➤ 流量平衡

AP 可以根据报文的源 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。

本章包含聚合全局配置及聚合口编辑配置。

### ➤ 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操作

#### ➤ 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，会提示是否删除聚合端口的确认框，点击确认即可实现聚合端口的删除操作，删除后面板会将删除的“聚合端口”变成“可选端口”。

#### 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，不支持电口和光口同时配置。

### 3.4.3 端口镜像

#### ➤ 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，进行网络监控与故障排除。

通过 SPAN 可以监控所有进入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 上的所有报文。图 3-4-2 SPAN 配置实例

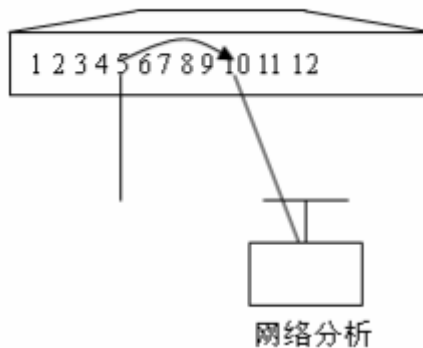


图 3-4-2 SPAN 配置实例

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。

#### ➤ 典型应用

表3-4 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。	本章介绍

RSPAN 基本应用	需要将镜像源设备的报文镜像到目的设备上监控。	本章介绍
------------	------------------------	------

配置端口镜像，最多配置4条。

The screenshot shows the '端口镜像' (Port Mirroring) configuration page. At the top, there is a blue header with the Ruijie logo and navigation options. Below the header, a sidebar menu on the left lists various configuration categories. The main content area features a '端口镜像' section with a blue information box containing a note: '说明：开启端口镜像功能，源端口上的所有报文都会被复制一份转发给目的端口，目的端口上通常连接一个报文分析器分析源端口的报文情况，可以将多个端口镜像到一个目的端口。注意：目的端口和源端口不能为同一个。' Below this is a table titled '镜像列表' (Mirror List) with the following columns: #, 镜像源端口 (Mirror Source Port), 镜像目的端口 (Mirror Destination Port), 监控报文 (Monitor Traffic), 是否接收非镜像源端口报文 (Receive Non-Mirror Source Port Traffic), and 操作 (Action). The table contains four rows, each with a '配置' (Configure) and '清空' (Clear) button in the '操作' column.

#	镜像源端口	镜像目的端口	监控报文	是否接收非镜像源端口报文	操作
1	--	--	--	--	配置 清空
2	--	--	--	--	配置 清空
3	--	--	--	--	配置 清空
4	--	--	--	--	配置 清空

#### ➤ 配置端口镜像：

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

#### ➤ 删除端口镜像：

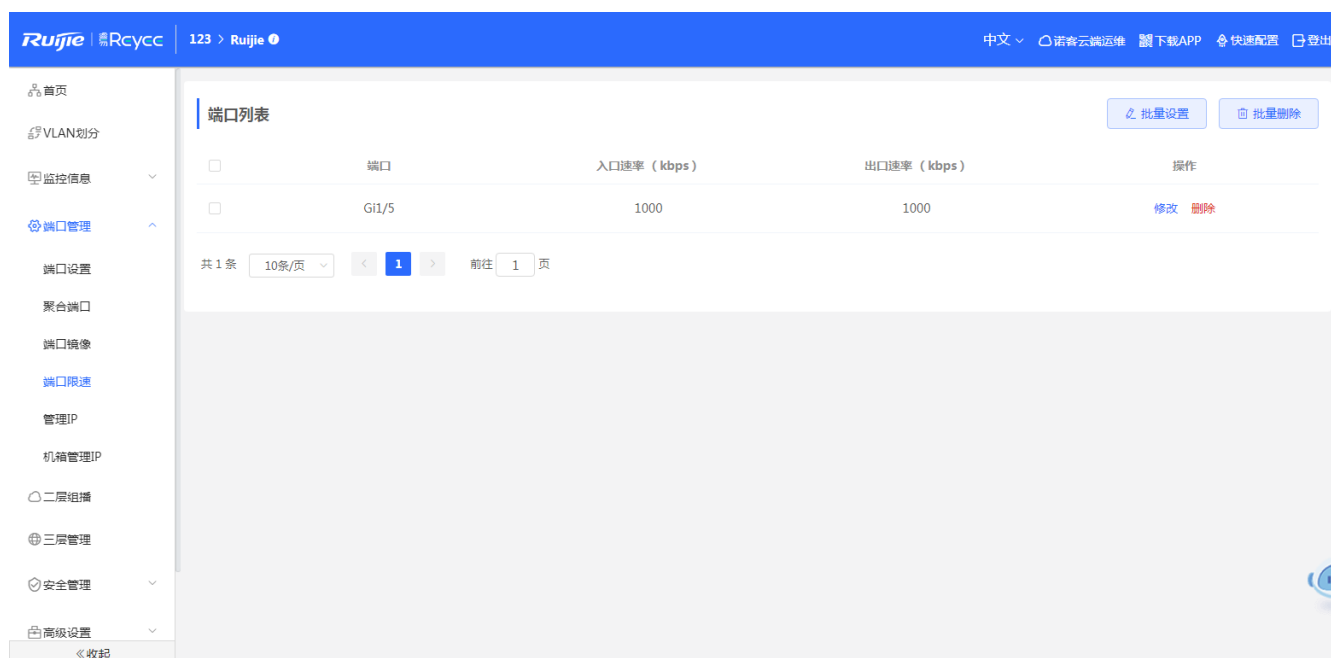
点击列表<清空>，在确认框中点击<确定>删除镜像。

#### **i** 说明

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，聚合端口不可作为目的端口。
2. 镜像最多可以配置4条，已配置过的端口不可再次配置。

### 3.4.4 端口限速

配置端口流量现值。



#### ➤ 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<修改>，在弹出框中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，会更新限速列表中的限速。

#### ➤ 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。

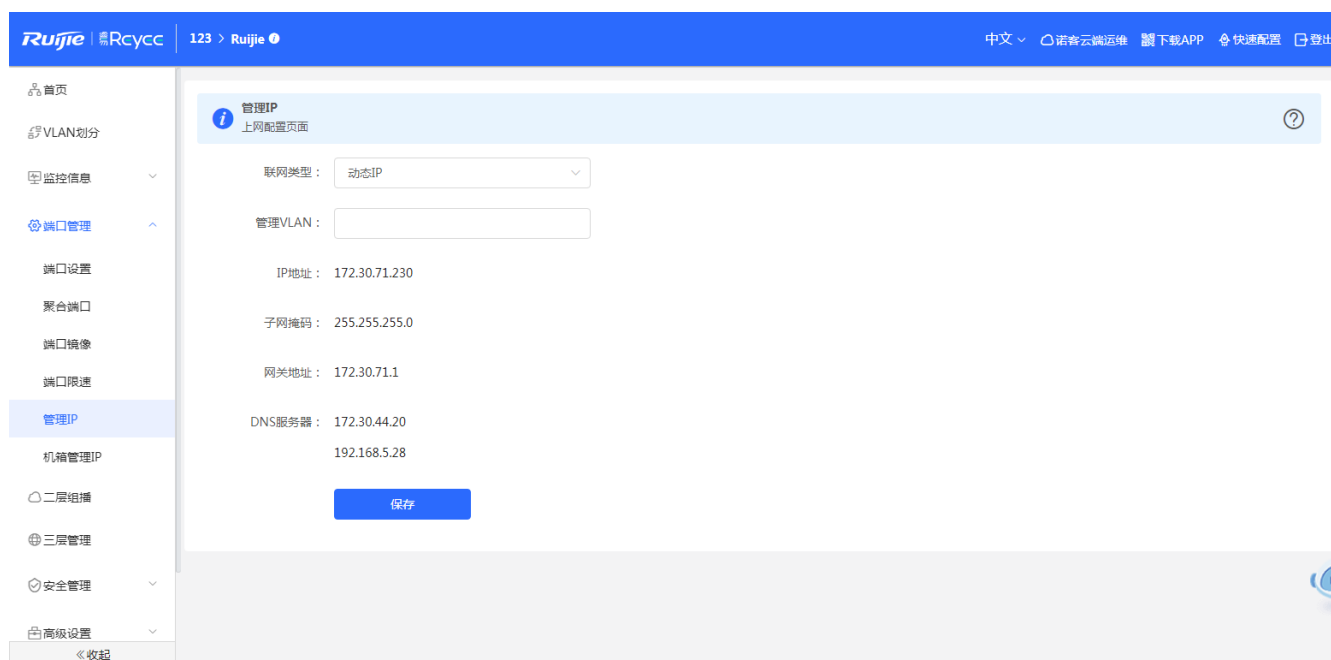
方法2：在“端口列表”中点<删除>，在确认框中点击<确定>删除数据。

#### 说明

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

### 3.4.5 管理 IP

配置设备管理IP地址。



#### 配置IP:

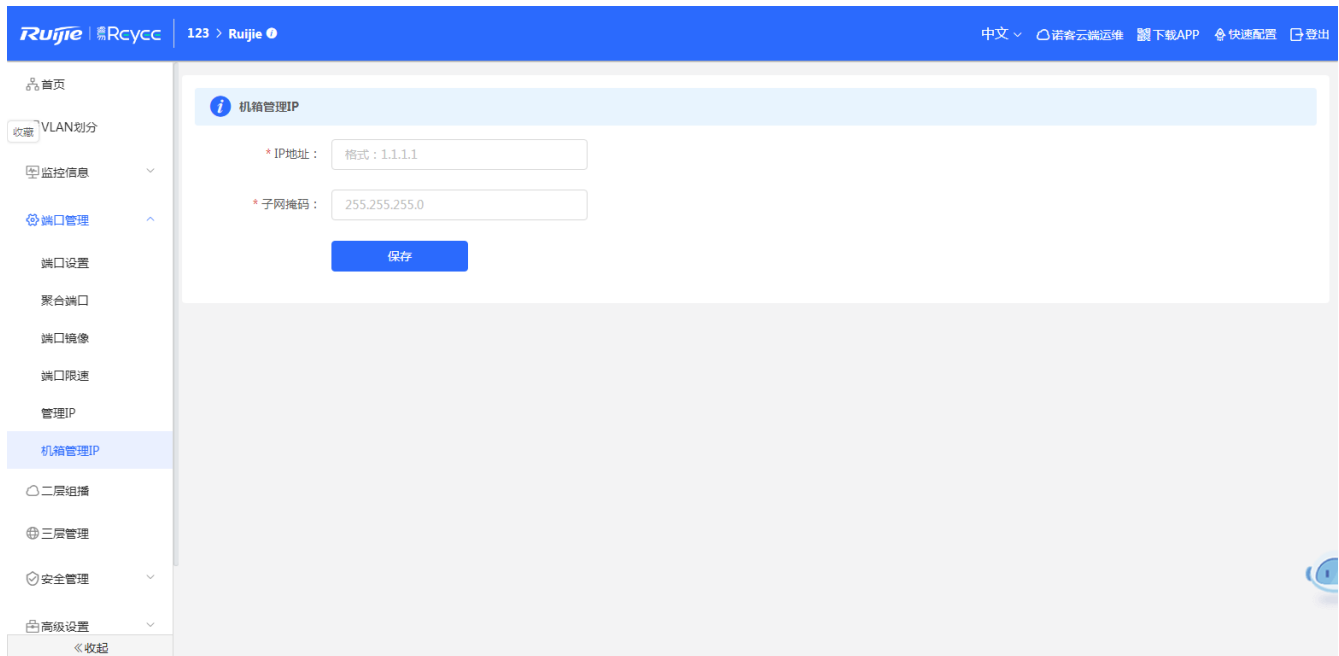
以配置上网类型, 选择动态IP, 设备会从DHCP server中获取各项参数。选择静态IP, 设备需要配置管理 VLAN、IP地址、子网掩码、默认网关及 DNS 服务器进行设置, 点击<保存>, 提示设置成功即可。

#### 说明

1. 管理VLAN为空及不填时默认生效vlan1。
2. 管理VLAN必须已创建, 未创建前往VLAN列表进行添加。
3. 配置的管理VLAN最好绑定当前上联端口, 否则可能造成WEB访问不了。

### 3.4.6 机箱管理 IP

机箱的管理 IP 是指 MGMT 口的 IP,一般只有高端的交换机才有。



#### 说明

MGMT默认是没有设置IP, IP目前只支持静态配置, 不支持动态。

## 3.5 二层组播

### ➤ 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。

### ➤ 典型应用

表3-4 二层组播应用

应用类型	说明	备注
二层组播控制	层组播精确转发, 避免组播报文在二层泛洪。	本章介绍
公共组播服务(组播 VLAN)	多个 VLAN 的用户共享同一 VLAN 的组播流	本章介绍
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。	本章介绍

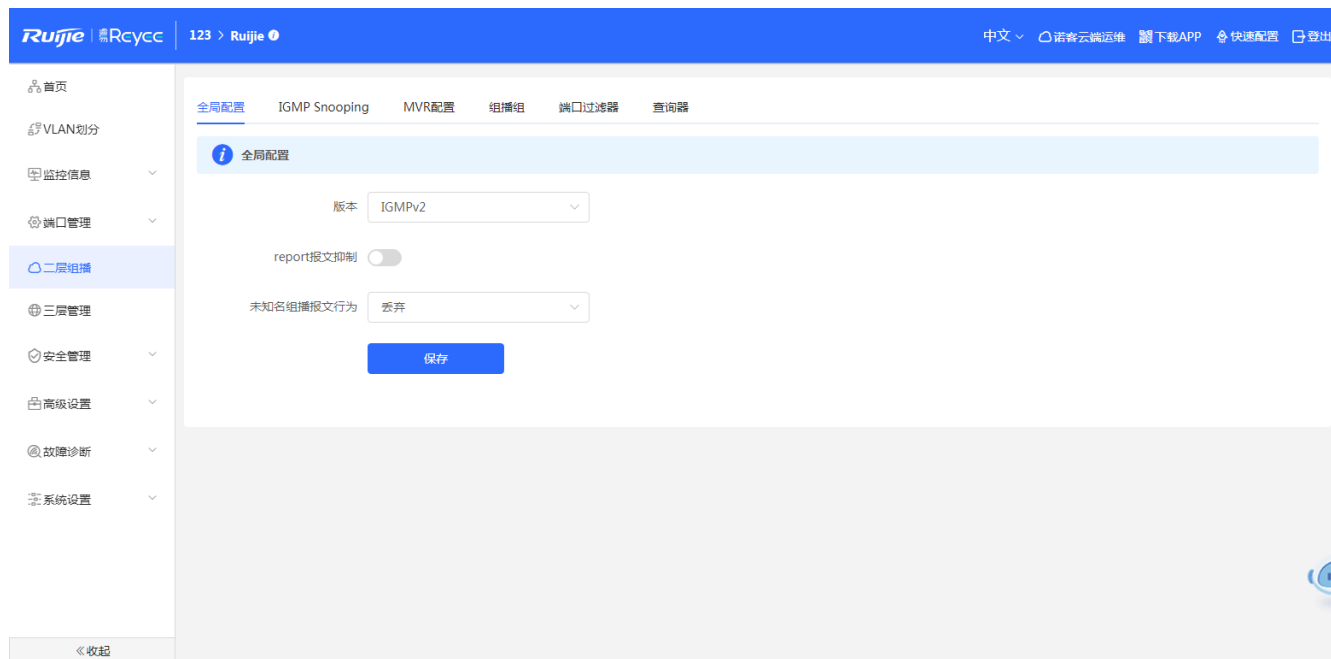
### ➤ 目前支持功能

二层组播包含全局配置、IGMP Snooping、MVR配置、组播组、端口过滤器、查询器。



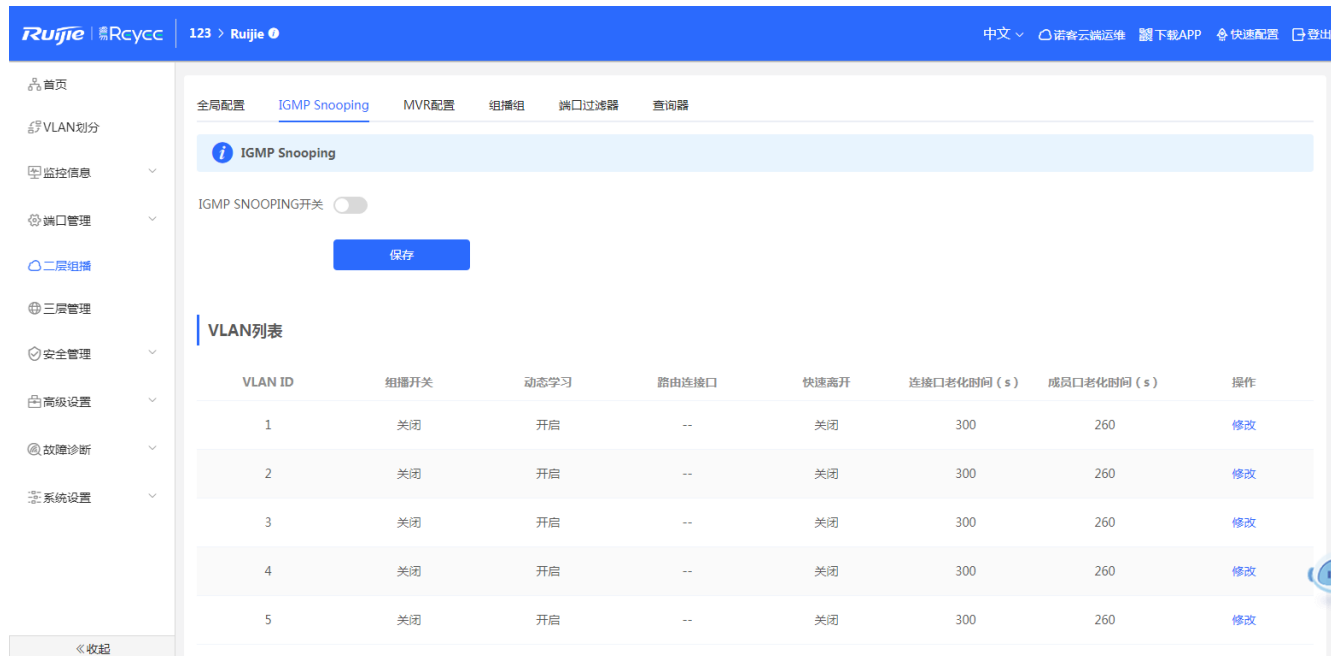
### 3.5.1 全局配置

全局配置可以选择IGMP的协议版本、是否开启report报文抑制和未知名组播的行为。



### 3.5.2 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。



#### ➤ 使能IGMP Snooping:

点击IGMP Snooping的开关按钮，可以设置开或者关，然后点击<保存>就可以使配置生效。

#### ➤ 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、路由端口、快速离开、输入连接口老化时间、输入成员口老化时间等，点击<确定>配置。

#### **i** 说明

1. 连接口老化时间范围是30-3600秒。
2. 成员口老化时间范围是30-65535秒

### 3.5.3 MVR 配置

The screenshot shows the Ruijie Eweb configuration interface for MVR settings. The interface includes a sidebar with navigation options and a main content area with the following elements:

- MVR配置** (MVR Configuration) section:
  - A blue information icon and a note: "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。快速离开功能仅在接收端口上生效。"
  - A toggle switch for **MVR开关** (MVR Switch), currently turned off.
  - A blue **保存** (Save) button.
- 端口列表** (Port List) section:
  - A blue **批量设置** (Batch Settings) button.
  - A table with the following columns: **端口** (Port), **端口角色** (Port Role), and **快速离开** (Fast Leave).
  - The table lists ports Gi1/1 through Gi1/5, all with 'NONE' as the role and '快速离开' disabled.

#### ➤ MVR开关：

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>后配置。

#### ➤ 端口配置：

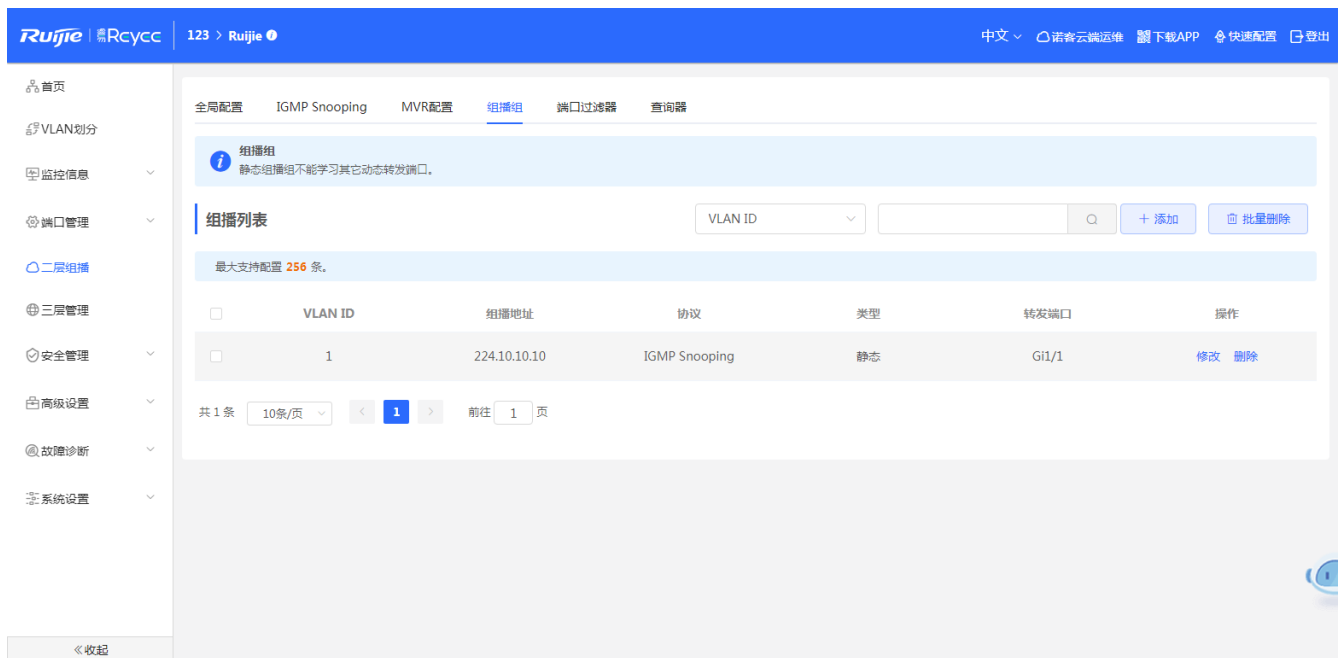
端口中可以选择NONE、RECEIVER、SOURCE三种类型之一，同时可以在端口是否开启快速离开功能。

#### **i** 说明

1. 源端口必须在mvr vlan。
2. 接收器端口不得在mvr vlan中。
3. 快速离开功能仅在接收端口上生效。

### 3.5.4 组播组

显示配置的组播列表



#### ➤ 组播搜索：

择搜索类型（支持按按VLAN ID、按组播地址查询），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：

在已经添加好的组播列表中，点击“组播列表”中<修改>，在弹出框中选择端口，点击<确定>提示“配置成功”后，会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，列表更新数据。

方法2：点击“组播列表”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。

#### 说明

最大可以配置256条组播地址。

## 3.5.5 端口过滤器

### ➤ 概述

Profile 用于定义允许或禁止用户点播的组地址范围，供其他功能引用Profile 用来定义组地址范围。

配置 SVGL 模式时，引用 profile 来定义 SVGL 组地址范围。

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

配置 VLAN 过滤器时，引用 rofile 来定义 VLAN 中允许/禁止用户点播的组地址范围。

配置预览功能时，引用 rofile 来定义提供预览的组地址范围。

The screenshot displays the Ruijie Eweb configuration interface. The main content area is titled '端口过滤器' (Port Filter). It contains two tables:

- PROFILE列表** (Profile List): This table is currently empty, displaying '暂无数据' (No data). It has columns for Profile ID, Action, Start Group IP, End Group IP, and Action. Buttons for '+ 添加' (Add) and '批量删除' (Batch Delete) are visible.
- 过滤器列表** (Filter List): This table lists four filters for ports Gi1/1, Gi1/2, Gi1/3, and Gi1/4. Each filter has a Profile ID of '--' and a maximum multicast count of 256. A '批量设置' (Batch Settings) button is located to the right of the table.

The interface also features a sidebar on the left with navigation options and a top navigation bar with tabs for '全局配置', 'IGMP Snooping', 'MVR配置', '组播组', '端口过滤器', and '查询器'.

#### **i** 说明

创建 profile，默认为 deny 所有组范围址。

## 3.5.6 查询器

### ➤ 概述

在每一条VLAN下都有设置一个查询器，所以设备有多少个VLAN，查询器就有多少个。

全局配置 IGMP Snooping MVR配置 组播组 端口过滤器 **查询器**

**查询器**  
 查询器版本不能高于全局版本, 当全局版本降低时, 查询器版本会随之相应降低。  
 查询器源IP如果没有配置, 则使用设备管理IP。

**查询器列表**

VLAN ID	查询器开关	查询器版本	查询器源IP	查询报文间隔 (s)	操作
1	关闭	IGMPv2		60	<a href="#">修改</a>
2	关闭	IGMPv2		60	<a href="#">修改</a>
3	关闭	IGMPv2		60	<a href="#">修改</a>
4	关闭	IGMPv2		60	<a href="#">修改</a>
5	关闭	IGMPv2		60	<a href="#">修改</a>

共 5 条 10条/页 < 1 > 前往 1 页

### 编辑表项:

在查询器中最后一列, 点击<修改>, 弹出配置框, 首先选择查询器开关, 然后选择查询器版本、查询器源IP、输入查询报文间隔等, 点击<确定>配置。

#### 说明

1. 查询器版本不能高于全局版本, 当全局版本降低时, 查询器版本会随之相应降低。
2. 查询器源IP如果没有配置, 则使用设备管理IP。
3. 查询间隔时间范围为: 30-18000秒

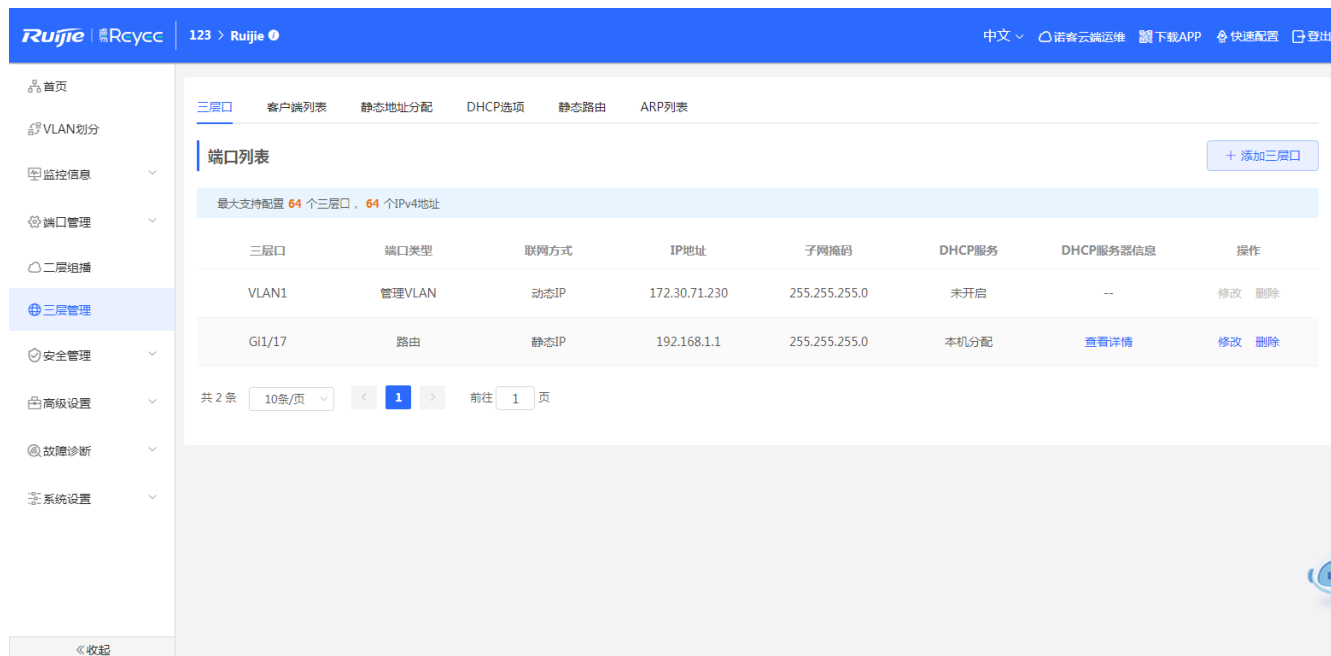
## 3.6 三层管理

### 概述

三层管理下包含三层口、地址池、dhcp relay(中继功用)、客户端列表、静态地址分配、DHCP选项、静态路由、ARP列表。

### 3.6.1 三层口

三层口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。

### ➤ 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。

#### **i** 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“3.4.5管理IP”
3. 三层口的中继和dhcp sever是互斥功能。
4. 三层聚合的成员必需是路由口类型。

## 3.6.2 客户端列表

客户端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。

123 > Ruijie

中文 语音云端运维 下载APP 快速配置 登出

三层口 客户端列表 静态地址分配 DHCP选项 静态路由 ARP列表

您可以在本页面查看DHCP的客户端相关信息。

客户端列表

查找主机名/IP地址/MAC地址 刷新 批量转换

最大支持配置 2000 条绑定。

序号	主机名	IP地址	MAC地址	剩余租期 (分)	状态
1	NBS7003-742AE6	192.168.1.2	c0:b8:e6:74:2ae8	62	添加到静态地址

1 10条/页 共 1 条

#### 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:

方法1: 在“客户端列表”中勾选需要添加的表项, 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条数据, 以产品的SPEC为主。

### 3.6.3 静态地址分配

静态表项分配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>，在弹出的框中输入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地址和出口MAC地址，点击<确定>提示“配置成功”后，会更新列表中的数据

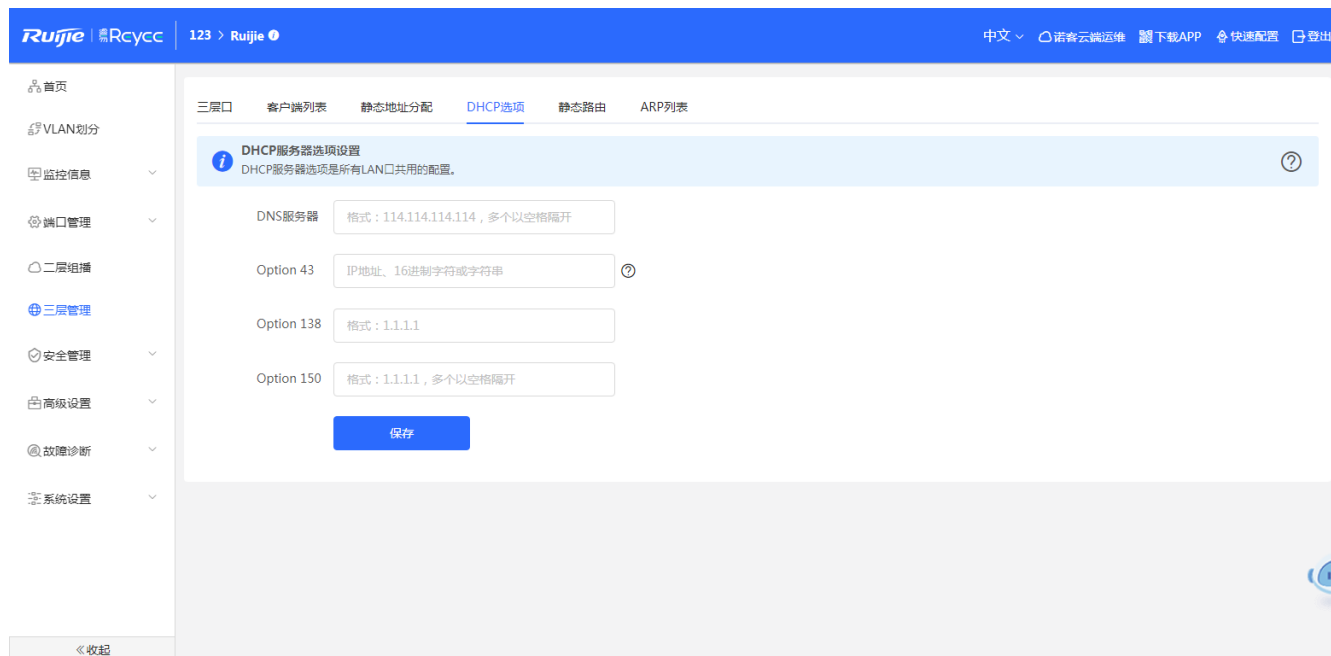
#### **i** 说明

静态地址表项最大支持2000条表项，以产品的SPEC为主。

## 3.6.4 DHCP 选项

DHCP 选项可以设置设备的三层口作为 DHCP server 时，对下列设备下发的配置。

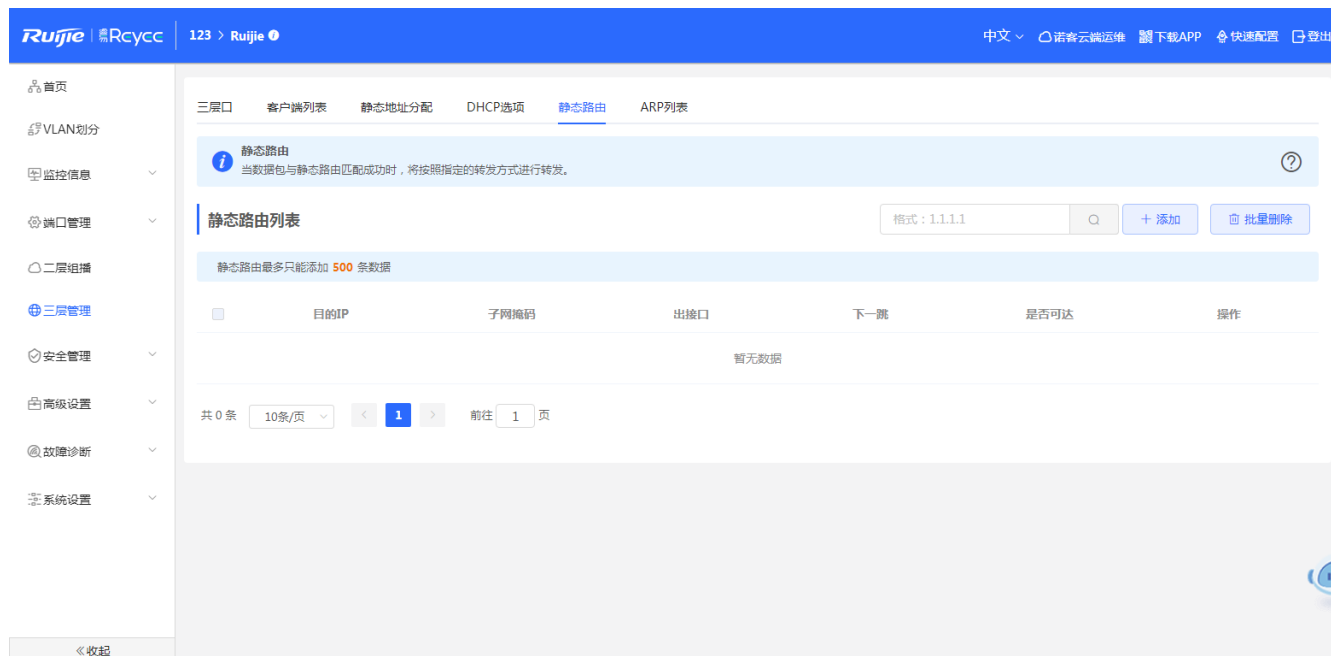




### 说明

【DHCP服务器】是全局的当三层为sever才用到，默认不用配置，下联口分配到的DNS是网关IP。

## 3.6.5 静态路由



### 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的地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

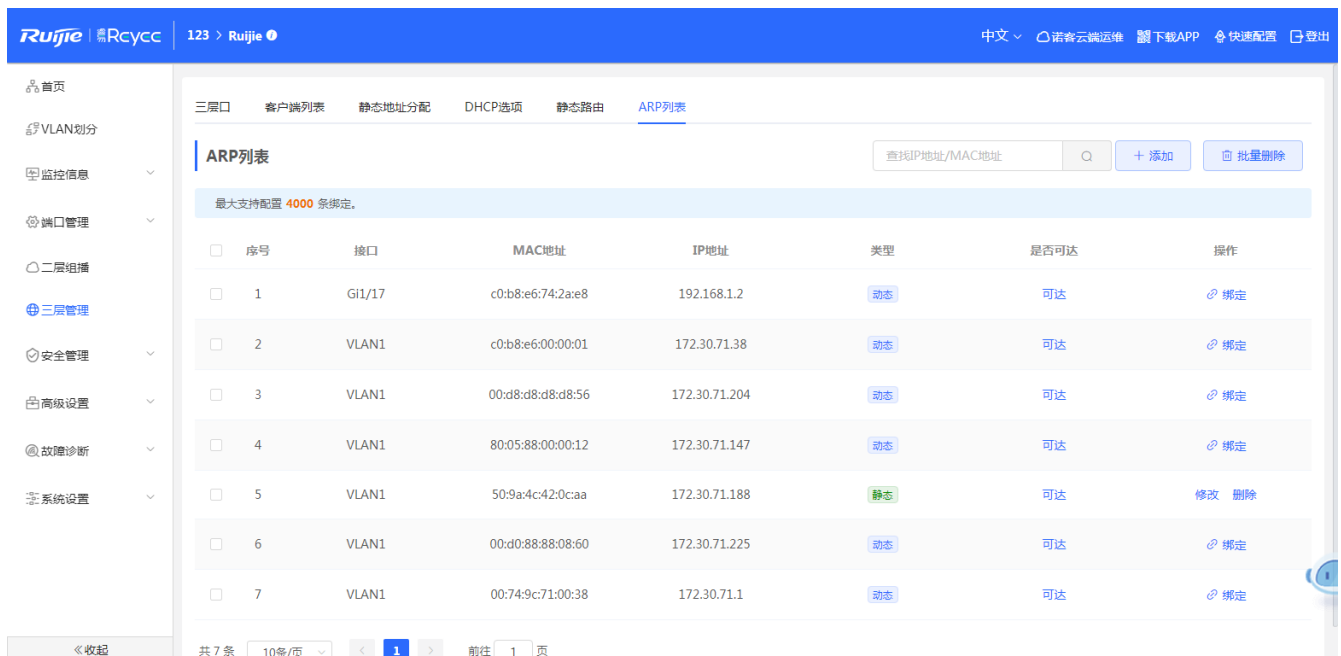
#### 说明

1. 静态路由表项最多只能添加500条数据, 以产品的SPEC为主。

## 3.6.6 ARP 列表

### ➤ 概述

ARP(Address Resolution Protocol, 地址解析协议)是用来绑定 MAC 地址和 IP 地址的, 以 IP 地址作为输入, ARP 能够知道其关联的 MAC 地址。一旦知道了 MAC 地址, IP 地址与 MAC 地址对应关系就会保存在设备的 ARP 缓存中。有了 MAC 地址, IP 设备就可以封装链路层的帧, 然后将数据帧发送到局域网上去。缺省配置下, 以太网上 IP 和 ARP 的封装为 Ethernet II 类型。



序号	接口	MAC地址	IP地址	类型	是否可达	操作
1	Gi1/17	c0:b8:e6:74:2ae8	192.168.1.2	动态	可达	绑定
2	VLAN1	c0:b8:e6:00:00:01	172.30.71.38	动态	可达	绑定
3	VLAN1	00:d8:d8:d8:d8:56	172.30.71.204	动态	可达	绑定
4	VLAN1	80:05:88:00:00:12	172.30.71.147	动态	可达	绑定
5	VLAN1	50:9a:4c:42:0c:aa	172.30.71.188	静态	可达	修改 删除
6	VLAN1	00:d0:88:88:08:60	172.30.71.225	动态	可达	绑定
7	VLAN1	00:74:9c:71:00:38	172.30.71.1	动态	可达	绑定

### ➤ 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表项拥有<修改>按钮, 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

1. ARP列表最大支持配置4000条数据, 以产品的SPEC为主。

---

## 3.7 安全管理

➤ **概述**

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。

### 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切换开关进行功能的开关。

开启后选择设置信任口，点击<保存>配置。

#### **i** 说明

1. 一般连接DHCP服务器端口设置为信任口。

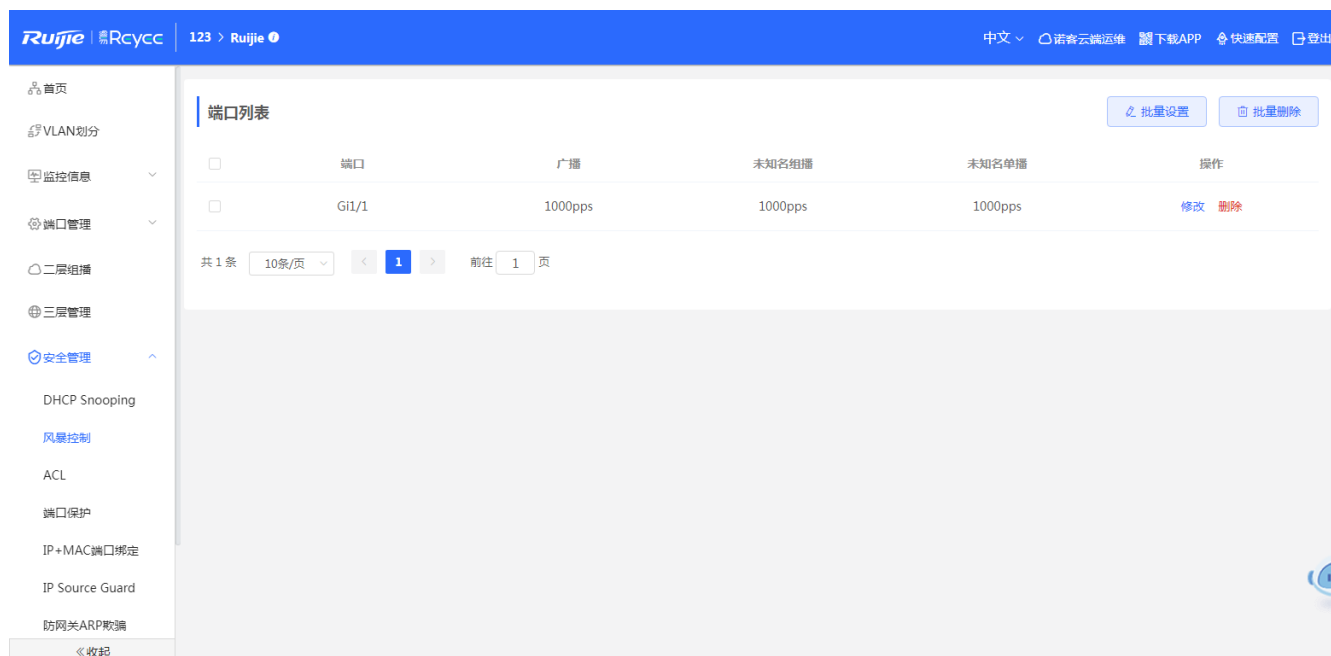
2. 开启DHCP Snooping可以起到DHCP报文过滤的功能。对于DHCP客户端请求报文，仅将其转发到信任口，对于DHCP服务器响应报文，仅转发来自信任口的响应报文

## 3.7.2 风暴控制

### ➤ 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。拓朴协议的执行错误或对网络的错误配置都有可能产生风暴。

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干比特数时，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干比特数的数据流，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。



#### ➤ 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

1. 配置端口限速时, 入口速率和出口速率必须填写一个。
2. 组播、未知名单播、未知组播为空时, 表示不限速。

### 3.7.3 ACL

#### ➤ 概述

ACLs (Access Control Lists, 接入控制列表), 也称为访问列表 (Access Lists), 俗称为防火墙, 在有的文档中还称之为包过滤。通过定义一些规则对网络设备接口上的数据报文进行控制: 允许通过、丢弃。

ACL模块包括添加ACL (两种模式: 基于MAC和基于IP), 端口绑定ACL。

### 3.7.3.1 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:

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。

#### **i** 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, deny所有报文。
5. ACL目前只支持端口的入口。

### 3.7.3.2 应用 ACL

应用ACL

设备过滤方向：入口方向（只在接收报文上做过滤）。

应用ACL

+ 批量添加    - 批量解除

<input type="checkbox"/>	端口	MAC-based ACL	IP-based ACL	操作
<input type="checkbox"/>	Gi1/1	111	--	修改 解除绑定
<input type="checkbox"/>	Gi1/2	--	222	修改 解除绑定
<input type="checkbox"/>	Gi1/3	--	--	修改 解除绑定
<input type="checkbox"/>	Gi1/4	--	--	修改 解除绑定
<input type="checkbox"/>	Gi1/5	--	--	修改 解除绑定
<input type="checkbox"/>	Gi1/6	--	--	修改 解除绑定
<input type="checkbox"/>	Gi1/7	--	--	修改 解除绑定
<input type="checkbox"/>	Gi1/8	--	--	修改 解除绑定

#### ➤ 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。

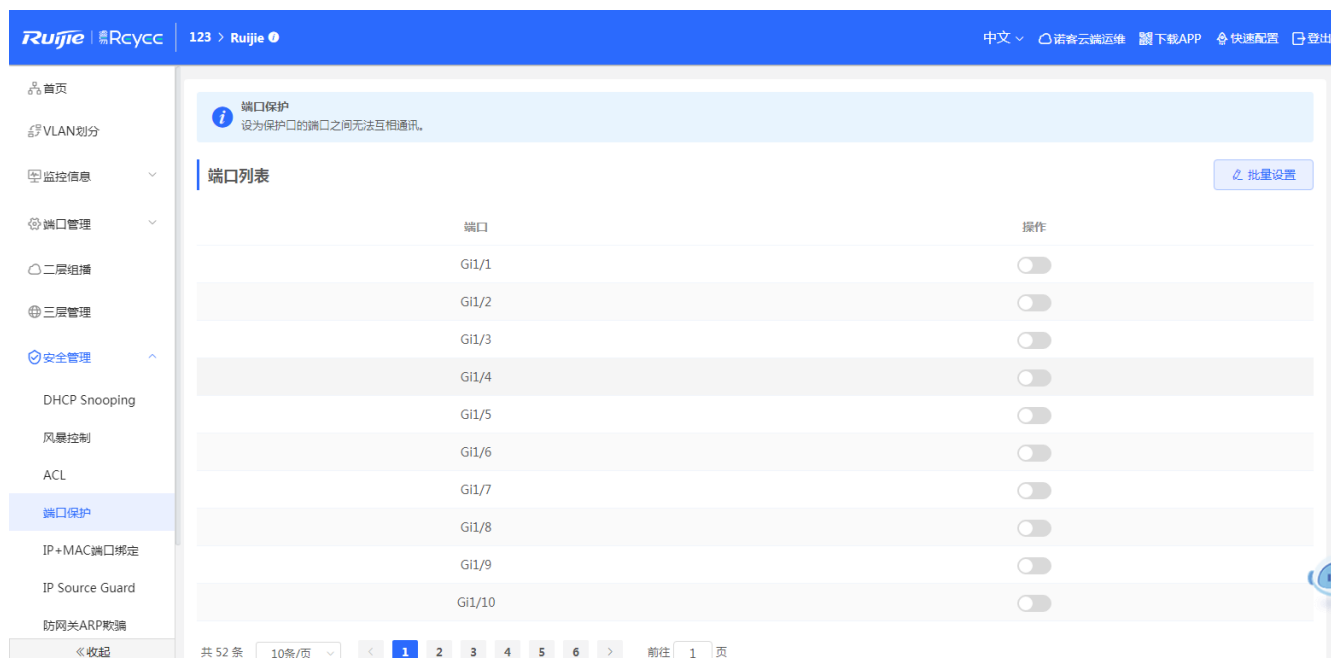
#### 说明

1. 端口绑定ACL至少选择一种类型的ACE。

### 3.7.4 端口保护

#### ➤ 概述

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。



### ➤ 切换端口保护开关

方法1: 点击<批量设置>, 在弹出框中切换开关并选择端口:

方法2: 点击“端口列表”操作栏“切换按钮”, 在确认框中点击<确定>配置端口保护。

## 3.7.5 IP+MAC 绑定

### ➤ 概述

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, 过滤掉不符合配置的IP报文, 严格控制设备输入源合法性。



**IP+MAC绑定**

说明：配置IP+MAC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，过滤掉不符合配置的IP报文，严格控制设备输入源合法性。  
注意：IP+MAC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。

根据IP查询

最大支持配置 500 条。

<input type="checkbox"/>	IP地址	MAC地址	端口	操作
<input type="checkbox"/>	192.168.1.1	00:11:22:33:44:55	Gi1/1	<a href="#">修改</a> <a href="#">删除</a>

共 1 条   前往  页

### ➤ 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

#### **i** 说明

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。

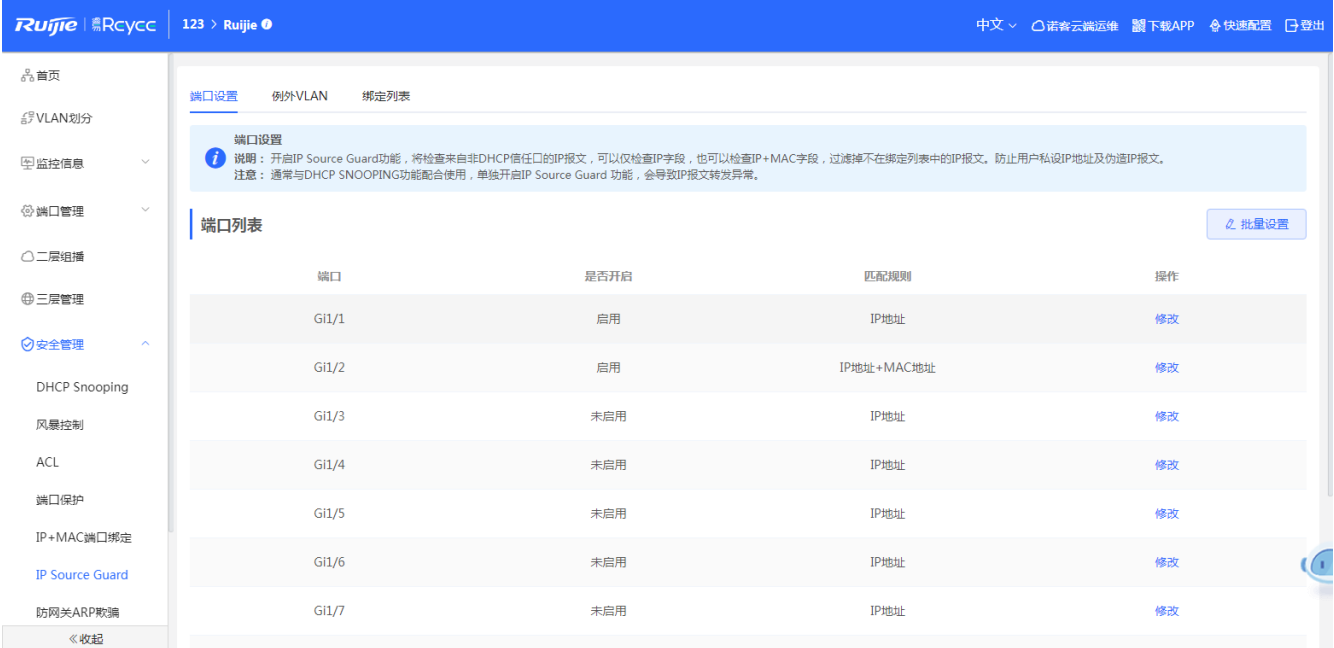
2. IP+MAC端口绑定最大支持配置500条。

## 3.7.6 IP Source Guard

IP Source Guard中有端口设置、例外VLAN、绑定列表。

### 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。



端口设置

说明：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。  
注意：通常与DHCP SNOOPING功能配合使用，单独开启IP Source Guard 功能，会导致IP报文转发异常。

批量设置

端口	是否开启	匹配规则	操作
G11/1	启用	IP地址	修改
G11/2	启用	IP地址+MAC地址	修改
G11/3	未启用	IP地址	修改
G11/4	未启用	IP地址	修改
G11/5	未启用	IP地址	修改
G11/6	未启用	IP地址	修改
G11/7	未启用	IP地址	修改

#### 使能端口：

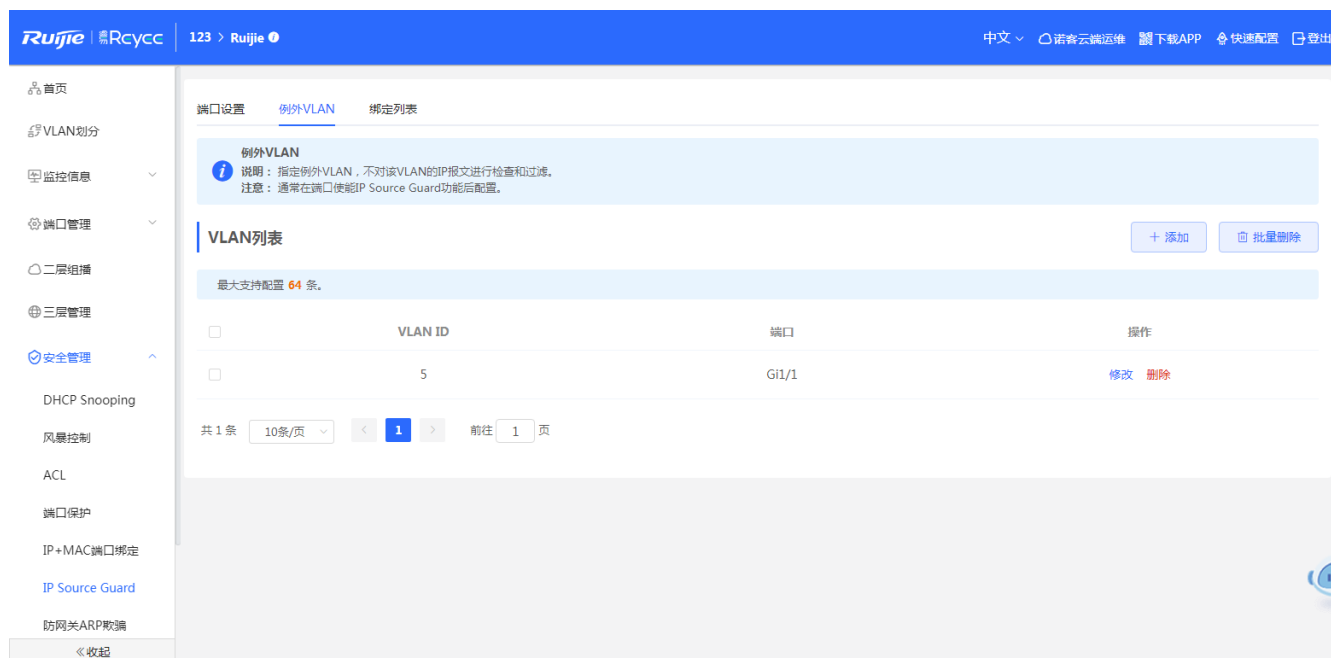
在端口列表中，点击“操作”中<修改>，在弹出框中修改该端口是否开启、匹配规则，点击<确定>提示“配置成功”后，会更新端口列表中的数据

#### 说明

1. 通常与DHCP SNOOPING功能配合使用，单独开启IP Source Guard 功能，会导致IP报文转发异常。

### 3.7.6.2 例外 VLAN

指定例外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

#### **i** 说明

1. 通常在端口使能IP Source Guard功能后配置。
2. 最大支持配置64条数据,以产品的spec为准。

### 3.7.6.3 绑定列表

#### ➤ 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。

#### **i** 说明

1. 列表内容来源于DHCP SNOOPING的动态学习。
2. 最大支持配置1000条数据，以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

#### **i** 说明

1. ARP列表最大支持配置4000条数据，以产品的SPEC为准

## 3.8 高级设置

高级设备包含STP、LLDP、RLDP、本机DNS配置。

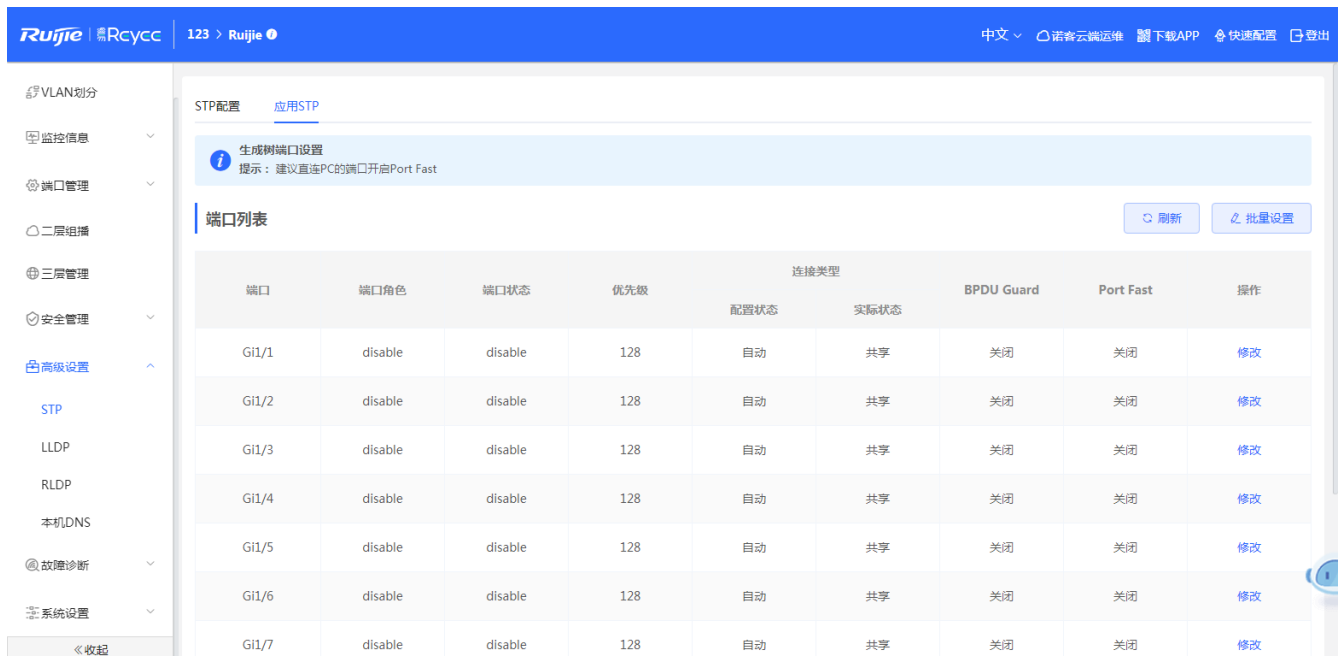
### 3.8.1 STP

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。



### ➤ 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。

#### **i** 说明

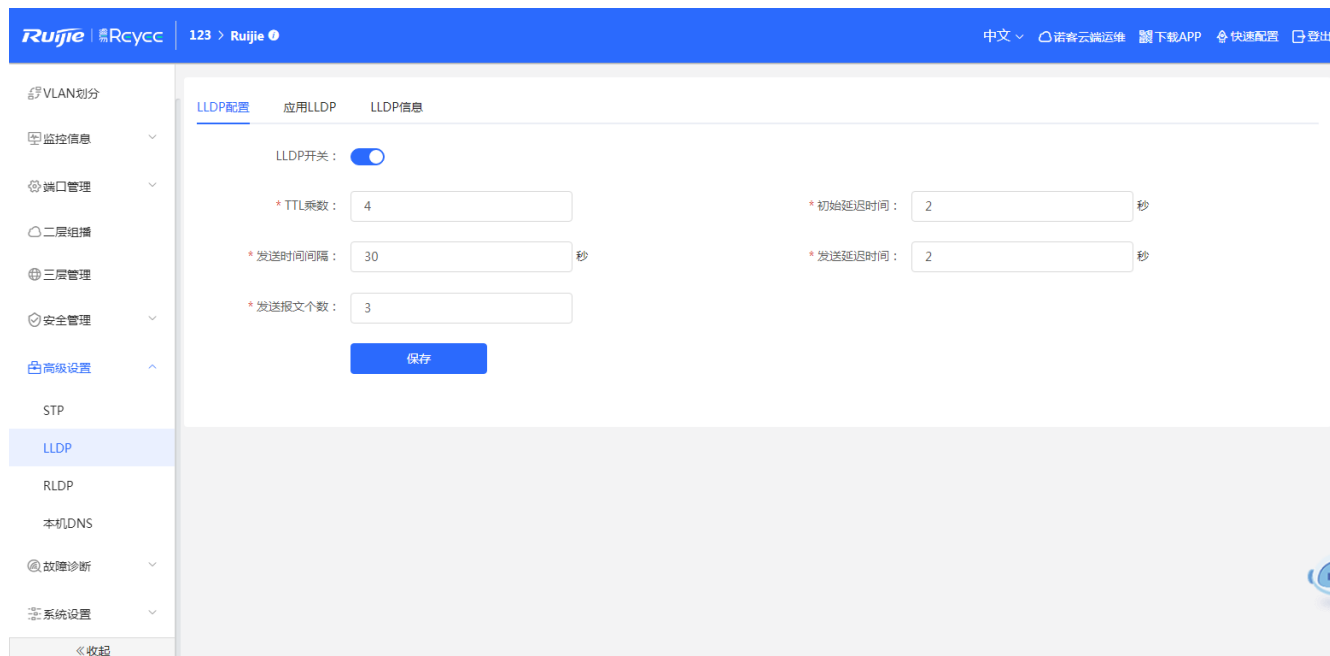
1. A开启生成树功能及改变生成树模式，浏览器将会重新连接，配置过程中请勿刷新页面。
2. 建议直连PC的端口开启Port Fast。
3. 开启STP是要30s以上端口才能变成转发，所以会出现短暂连接(不转报文)。

## 3.8.2 LLDP

### ➤ 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。

### 3.8.2.1 LLDP 配置



### ➤ LLDP配置:

开启LLDP开关并配置相关参数, 点击<保存>进行LLDP配置。

### 3.8.2.2 应用 LLDP

端口	发送LLDPDU	接收LLDPDU	媒体终端发现MED	操作
Gi1/1	开启	开启	开启	修改
Gi1/2	开启	开启	开启	修改
Gi1/3	开启	开启	开启	修改
Gi1/4	开启	开启	开启	修改
Gi1/5	开启	开启	开启	修改
Gi1/6	开启	开启	开启	修改
Gi1/7	开启	开启	开启	修改
Gi1/8	开启	开启	开启	修改
Gi1/9	开启	开启	开启	修改

#### ➤ 端口应用LLDP:

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LLDP。

### 3.8.2.3 LLDP 信息

端口	设备ID类型	设备ID	端口ID类型	端口ID	邻居系统	Time To Live(s)
Gi1/23	MAC address	00:D0:88:88:08:5F	Locally assigned	Gi39	Ruijie	113

#### ➤ 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。

**i** 说明

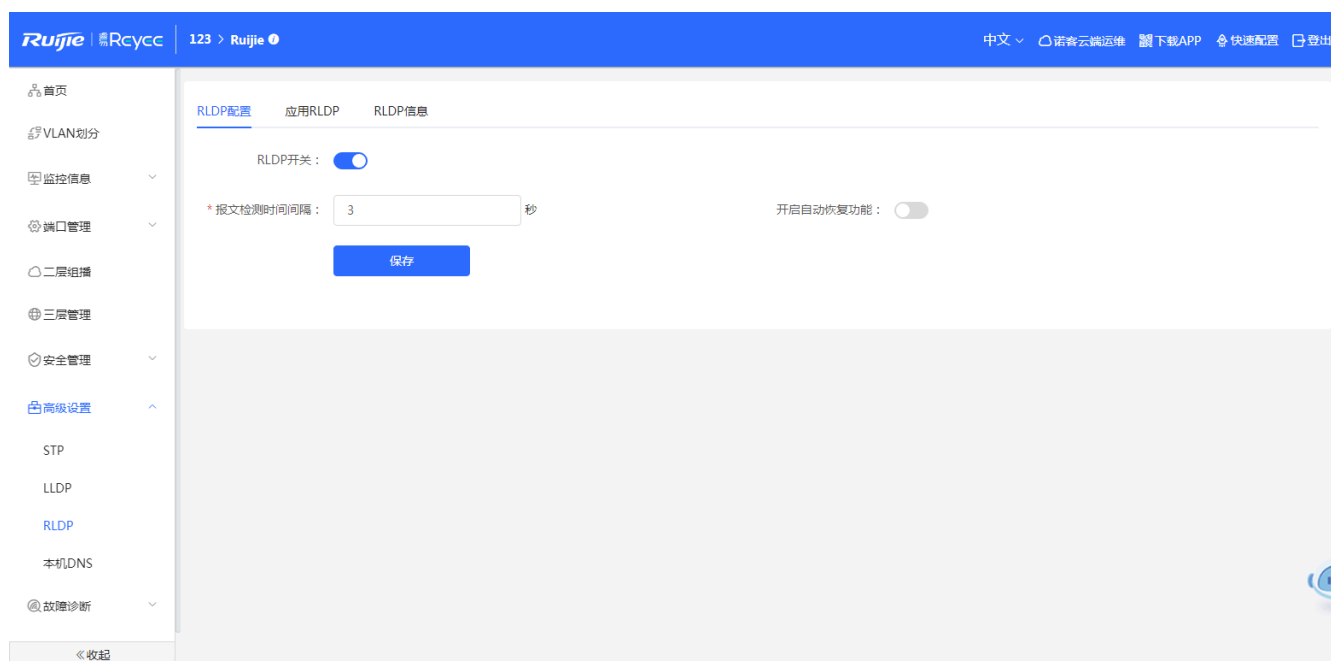
1. 可以利用LLDP查看拓扑连接情况，例如：网络拓扑中有若干交换机设备、MED 设备、NMS 设备。
2. 利用LLDP进行错误检测，例如：网络拓扑中有直连的两台交换机设备，错误配置信息将显示。

### 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



#### ➤ 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

The screenshot shows the '端口列表' (Port List) table in the '应用RLDP' (Apply RLDP) section. The table has four columns: '端口' (Port), '环路开关' (Loop Protection), '处理方式' (Action), and '操作' (Action). The data is as follows:

端口	环路开关	处理方式	操作
Gi1/1	开启	只警告 (warning)	修改
Gi1/2	开启	警告且阻塞报文转发 (block)	修改
Gi1/3	开启	警告且关闭端口 (shutdown port)	修改
Gi1/4	关闭	--	修改
Gi1/5	关闭	--	修改
Gi1/6	关闭	--	修改
Gi1/7	关闭	--	修改
Gi1/8	关闭	--	修改
Gi1/9	关闭	--	修改

#### ➤ 端口应用RLDP:

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RLDP。

### 3.8.3.3 RLDP 信息

The screenshot shows the 'RLDP信息' (RLDP Information) section. The table has four columns: '端口' (Port), '检测状态' (Detection Status), '处理方式' (Action), and '邻居端口' (Neighbor Port). The data is as follows:

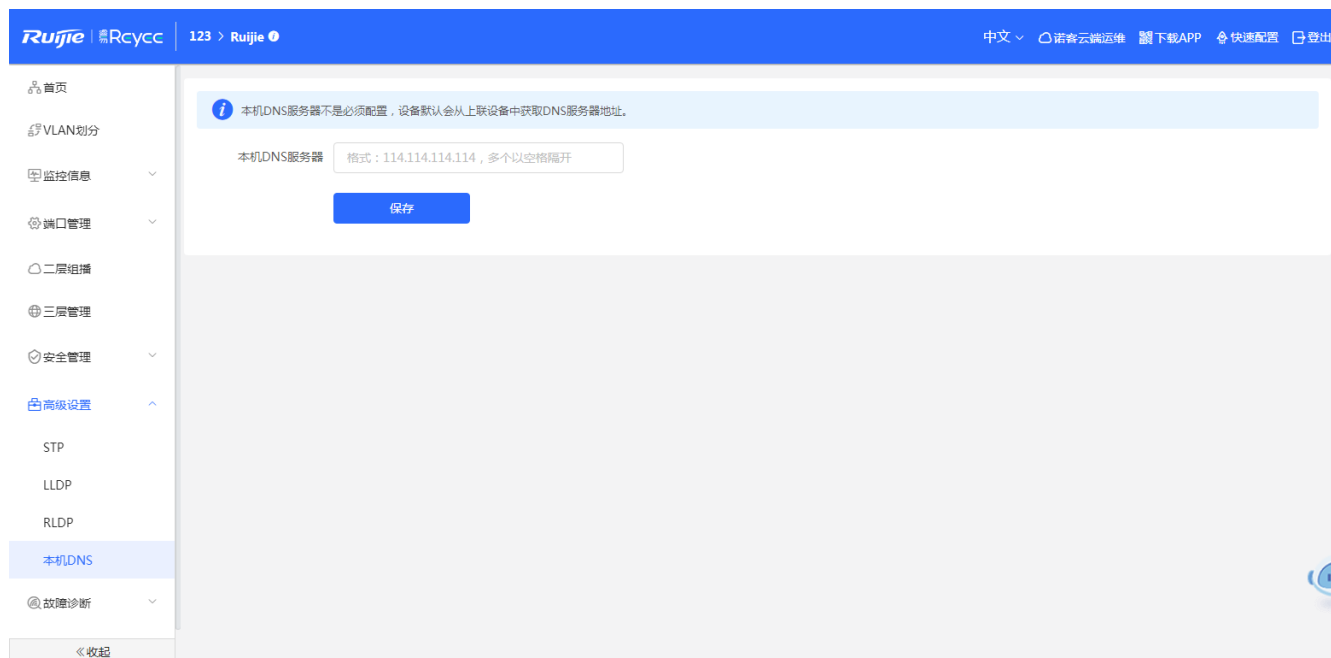
端口	检测状态	处理方式	邻居端口
Gi1/1	正常	只警告 (warning)	--
Gi1/2	正常	警告且阻塞报文转发 (block)	--
Gi1/3	正常	警告且关闭端口 (shutdown port)	--
Gi1/4	正常	--	--
Gi1/5	正常	--	--
Gi1/6	正常	--	--
Gi1/7	正常	--	--
Gi1/8	正常	--	--
Gi1/9	正常	--	--
Gi1/10	正常	--	--

共 52 条 | 10条/页 | 1 2 3 4 5 6 | 前往 1 页

### ➤ 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的IP地址, 点击<保存>配置。

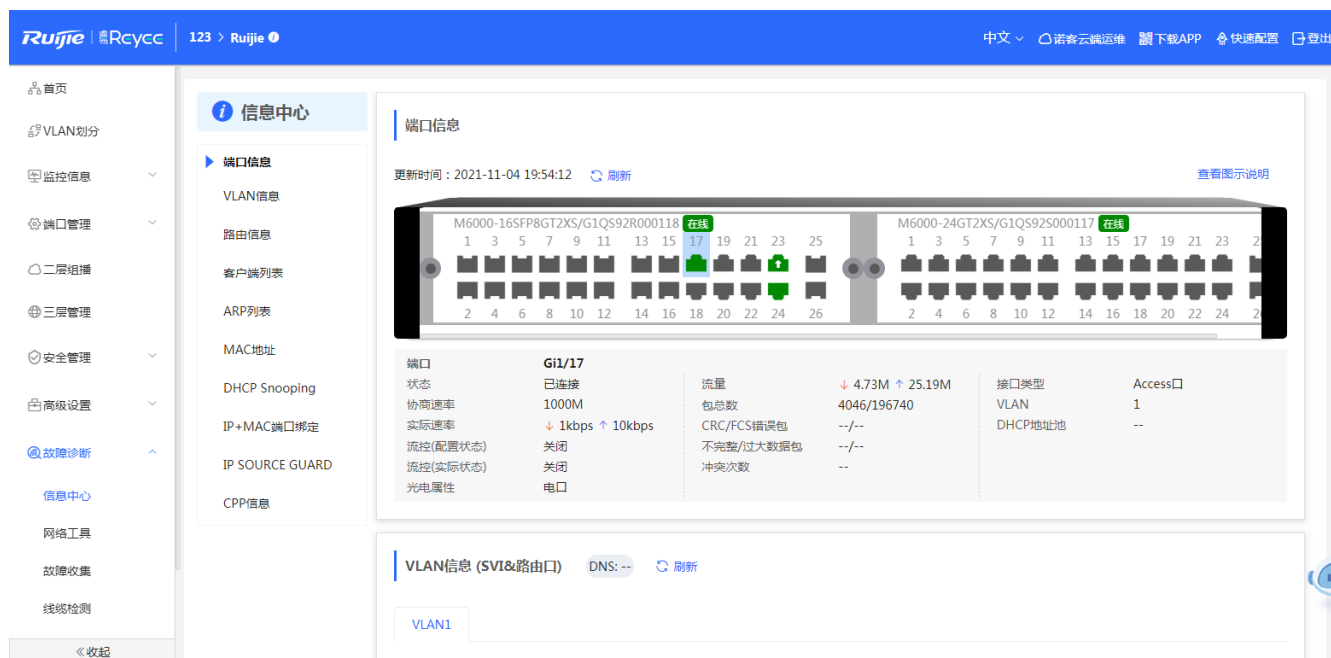
#### **i** 说明

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. 如果有配置的话, 报文优先使用管理IP的DNS, 再使用此DNS。

## 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信息。



## 3.9.2 网络工具

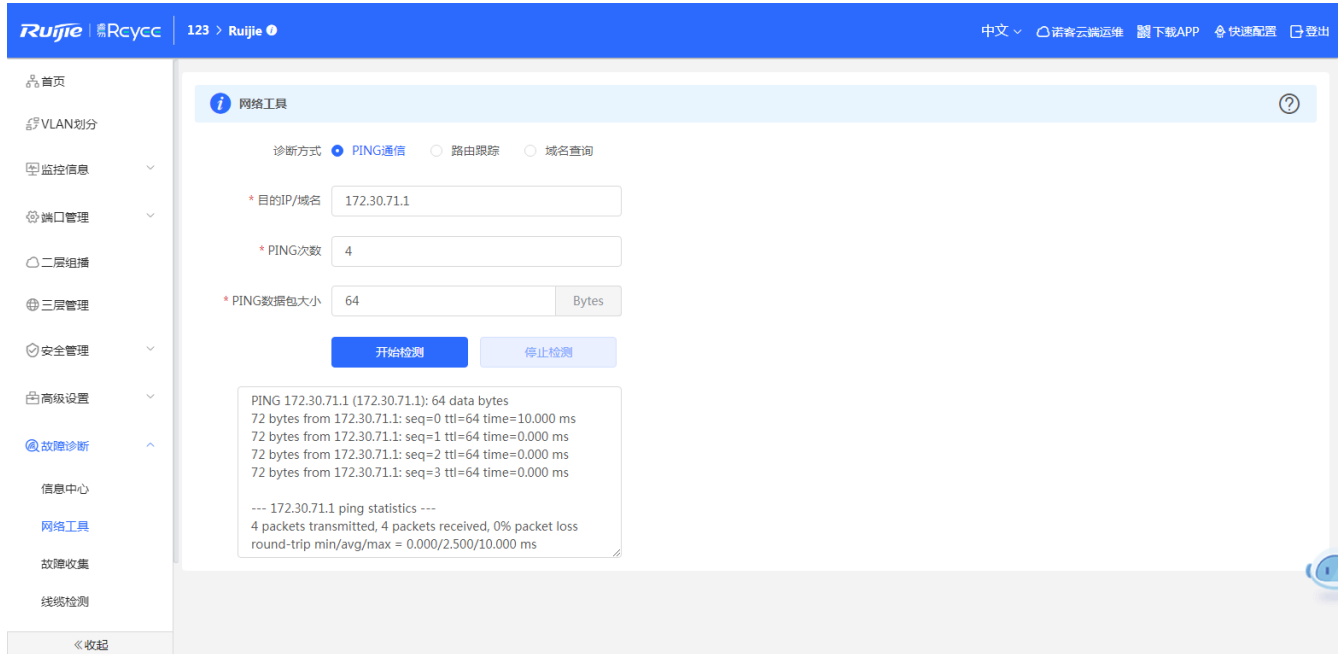
网络检测工具提供 PING 通信、路由跟踪、域名查询三种命令检查网络状态。

### 3.9.2.1 PING 通信

ping 是一种通信协议，是 TCP/IP 协议的一部分。利用“ping”命令可以检查网络是否连通。

如果要知道设备是否与其他设备连通，只要知道对方 IP 地址或者域名，可以在“PING 通信 (ping)”检测界面上输入目的 IP/域名，PING 次数及数据包大小，点击开始检测，即可进行连通性检测，如下图所示

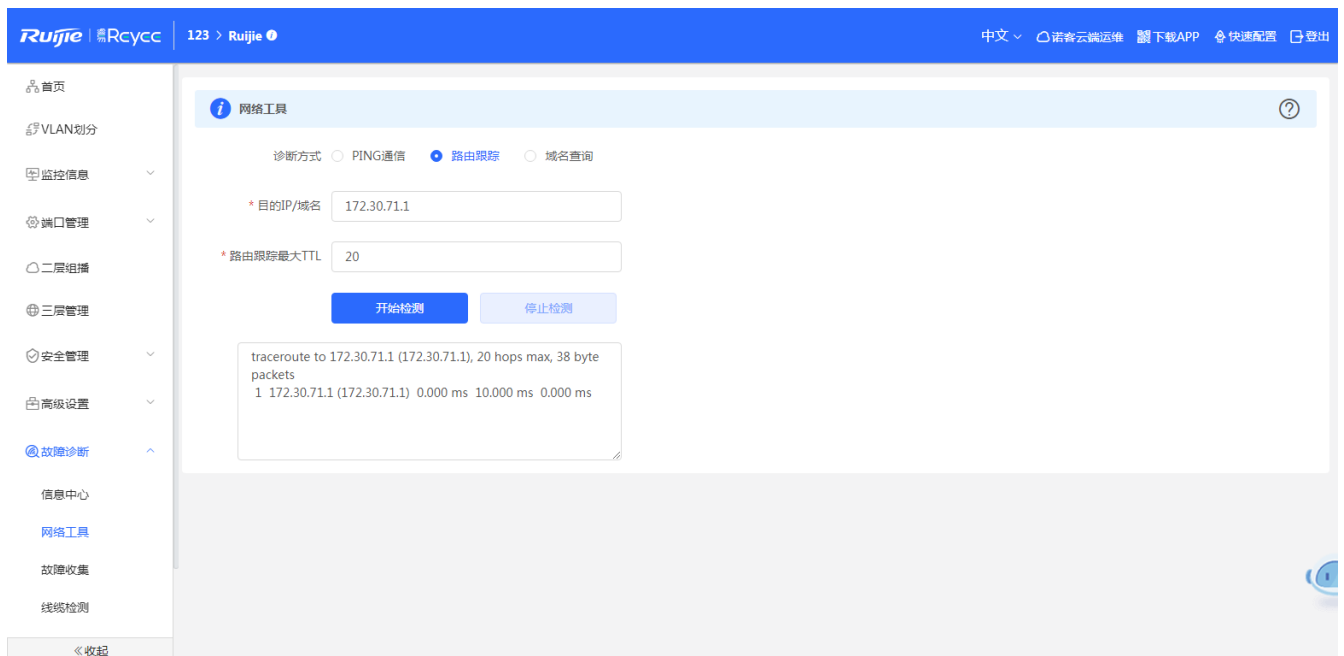
“PING 通信 (ping)”检测界面及结果：



### 3.9.2.2 路由跟踪

路由跟踪功能是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器,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器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。

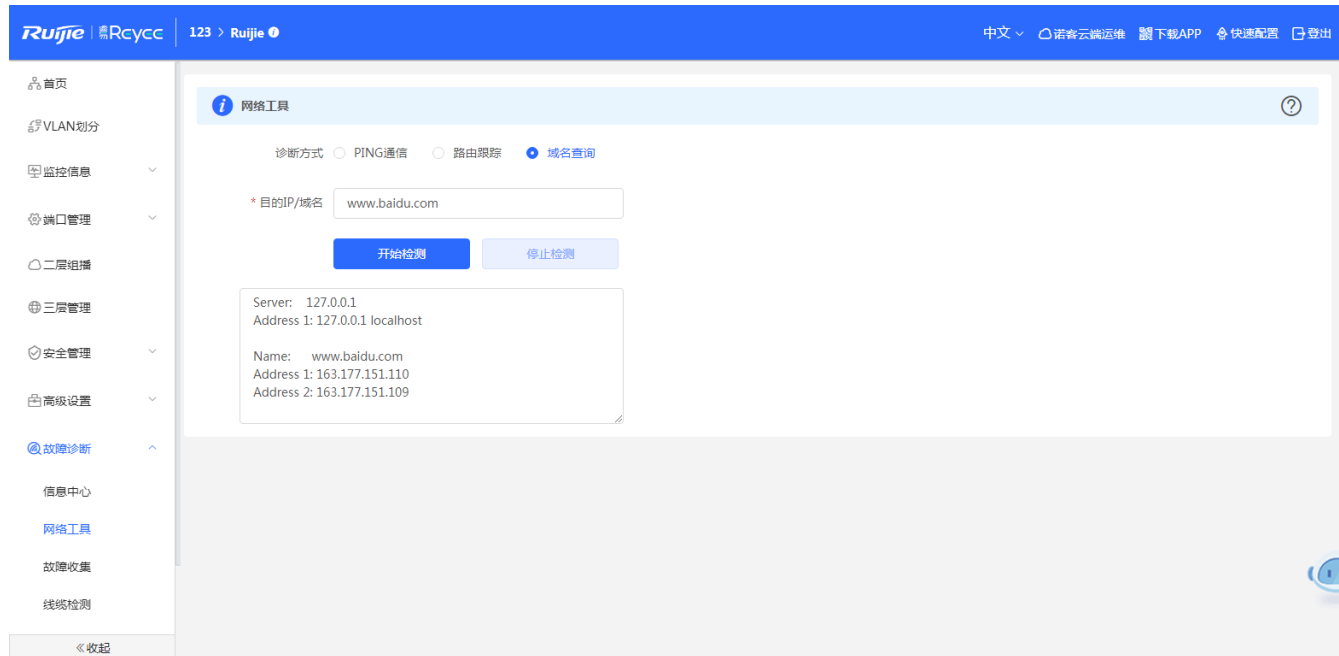
“路由跟踪 (traceroute) ” 检测界面及结果:



### 3.9.2.3 域名查询

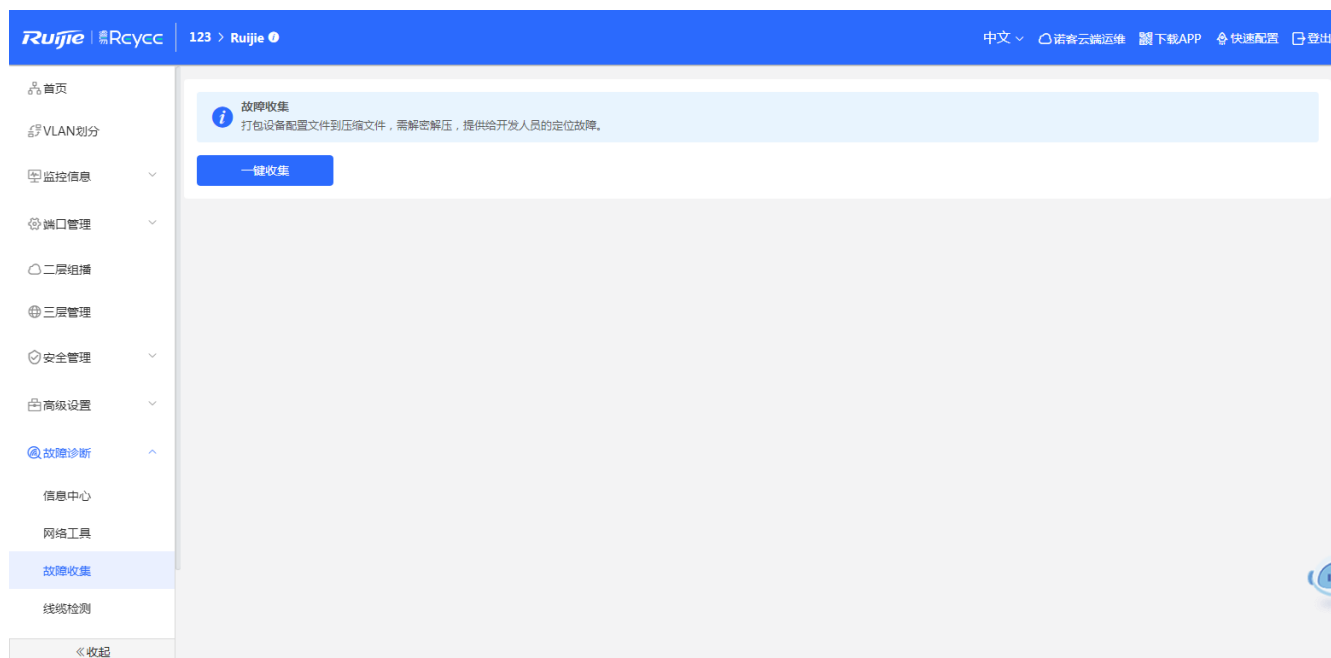
nslookup 的作用是用来查询 DNS 的记录, 查看域名解析是否正常, 在网络故障的时候用来诊断网络问题。若您的网页可以 ping 通外网的 IP 地址但浏览器无法正常打开网页, 可以尝试用 nslookup, 检测域名解析是否正常。

“域名查询 (nslookup)” 检测界面及结果:



### 3.9.3 故障收集

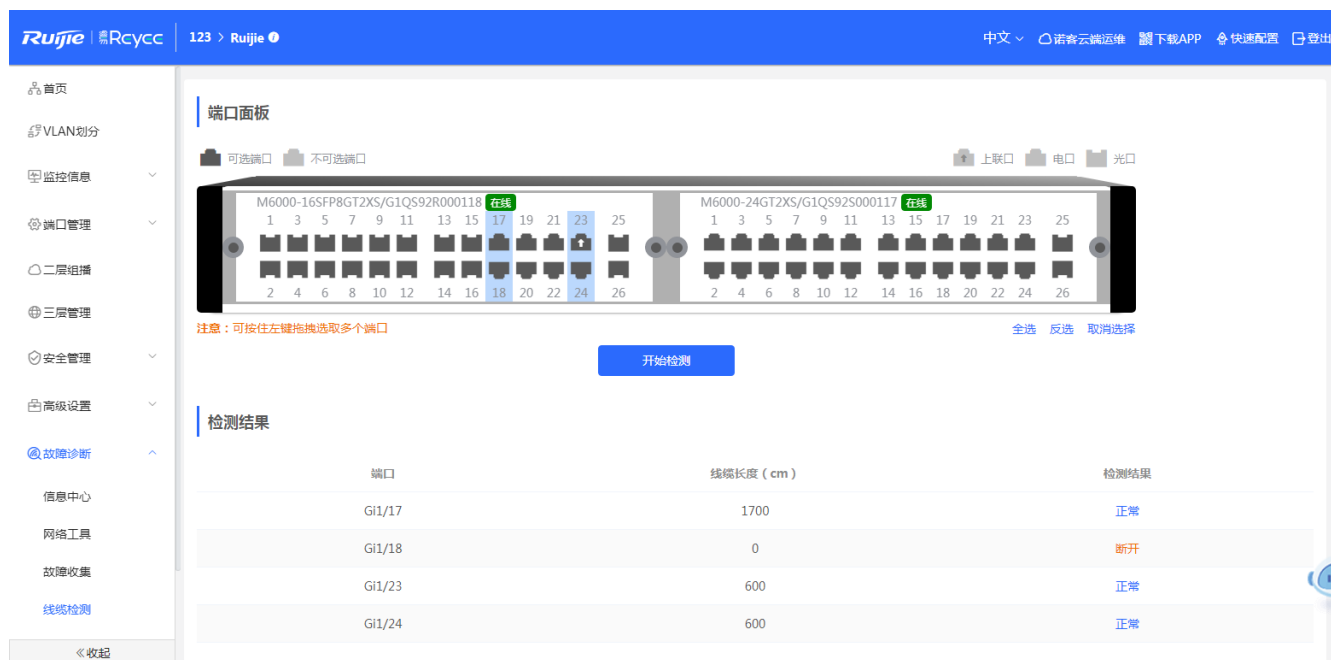
若您的设备出现未知原因的故障, 可在此页面下执行一键故障收集命令, 并下载到本地。提供给我们的开发人员分析。



点击<一键收集>即可下载故障信息。

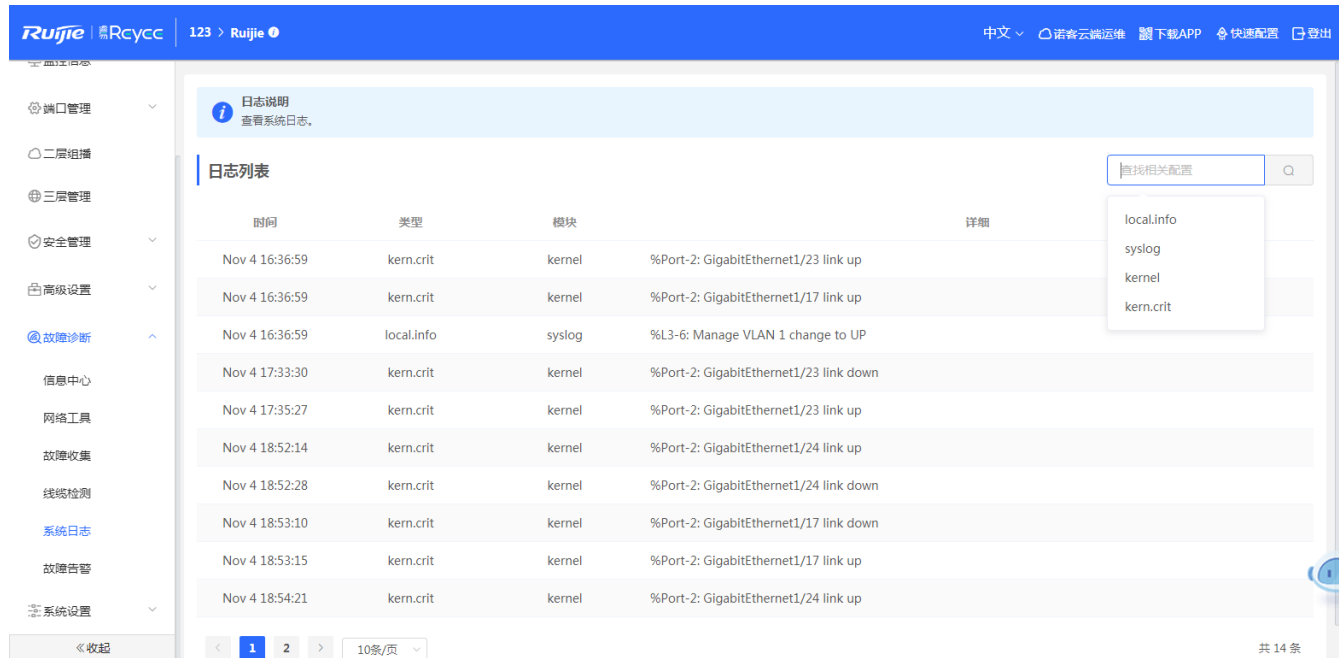
### 3.9.4 线缆检测

线缆检测可以大概检测出链接端口的线缆长度和线缆是否有故障。



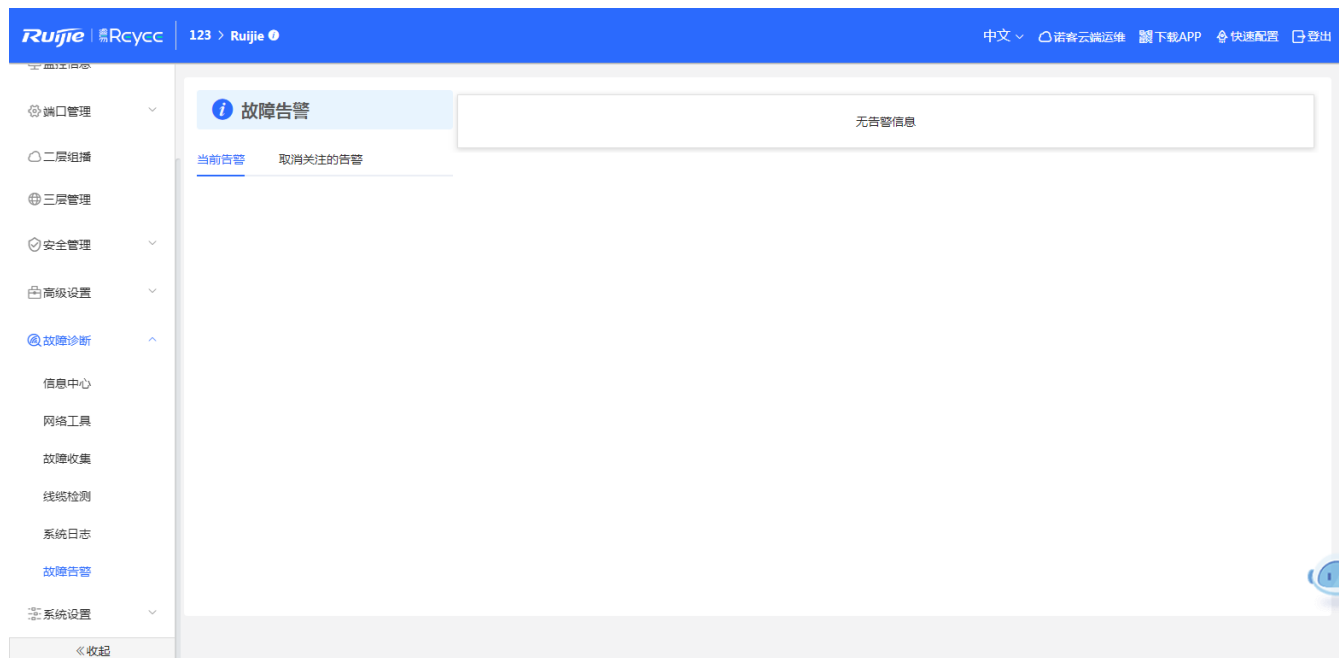
### 3.9.5 系统日志

系统日志可以清楚知道设备在什么时间、什么模块发生了什么操作。



可以按照故障类型或者故障名称来搜索指定的日志。

### 3.9.6 故障告警





## 3.10 系统设置

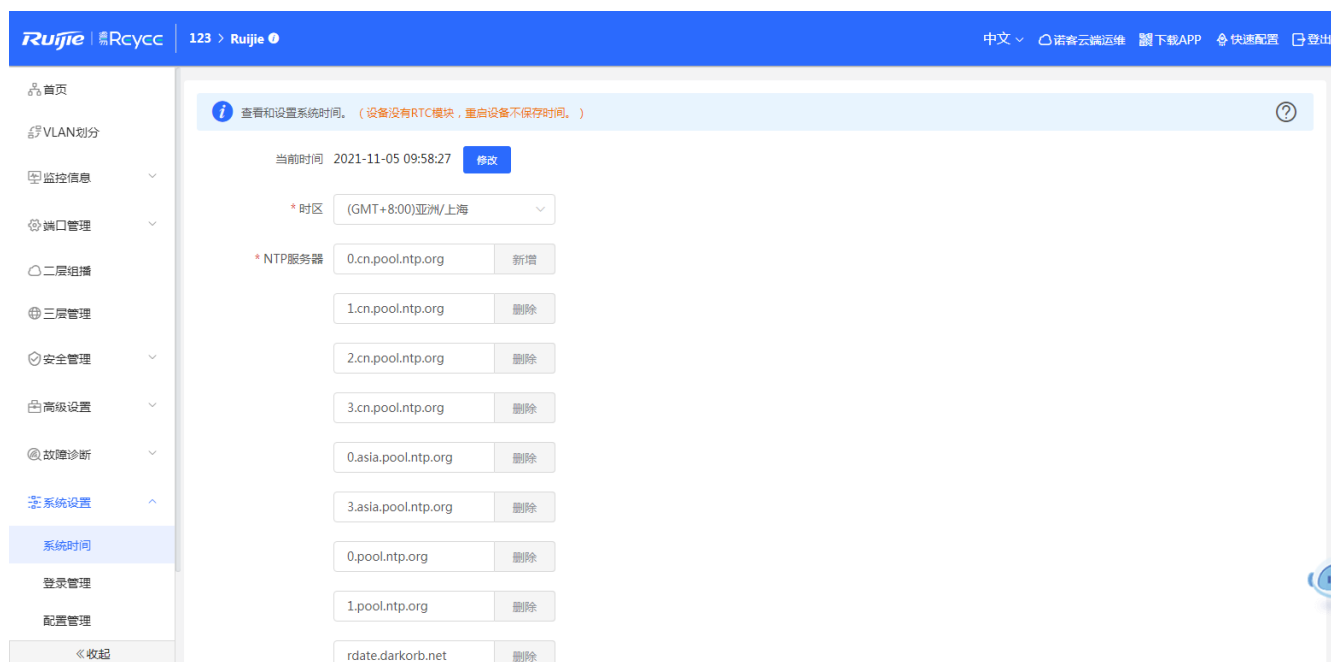
### 3.10.1 系统时间

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

#### 说明

1. 时区：由于世界各国与地区经度不同，地方时也有所不同，因此会划分为不同的时区。您可以根据地区设置时区。

2. NTP服务器：EST设备可从网络同步时间，NTP服务器是互联网上提供时区同步服务的服务器，不同地区指定的NTP服务器不同。

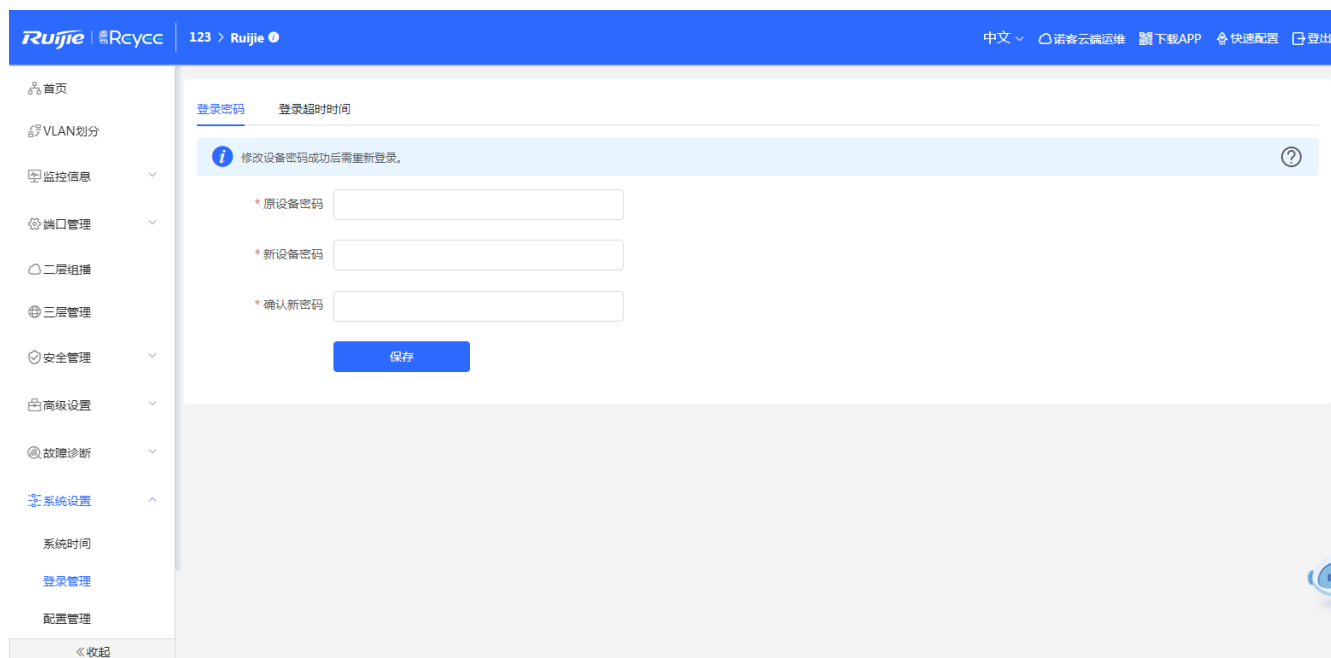


The screenshot shows the Ruijie Eweb configuration interface for system time settings. The page title is "查看和设置系统时间。(设备没有RTC模块, 重启设备不保存时间。)" (View and set system time. (Device does not have RTC module, restart device does not save time.)). The current time is displayed as 2021-11-05 09:58:27 with a "修改" (Modify) button. The time zone is set to (GMT+8:00)亚洲/上海. Below, there is a list of NTP servers with "新增" (Add) and "删除" (Delete) buttons for each.

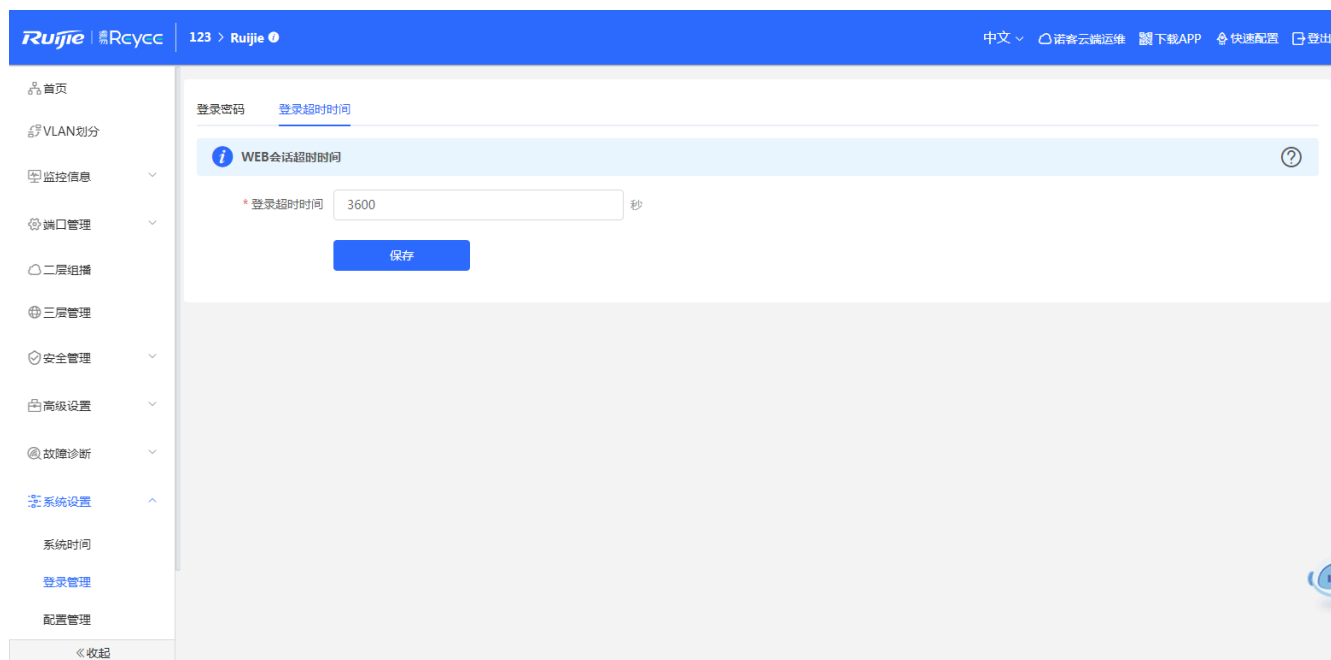
NTP Server	Action
0.cn.pool.ntp.org	新增
1.cn.pool.ntp.org	删除
2.cn.pool.ntp.org	删除
3.cn.pool.ntp.org	删除
0.asia.pool.ntp.org	删除
3.asia.pool.ntp.org	删除
0.pool.ntp.org	删除
1.pool.ntp.org	删除
rdate.darkorb.net	删除

### 3.10.2 登录管理

登录管理可以修改设备的登录密码：



在浏览器上登录设备 Eweb 后，若不退出登录，Eweb 系统将在 1 小时内在此浏览器上免密码访问。在登录超时时间下可以设置系统的免密码访问时长：



#### 说明

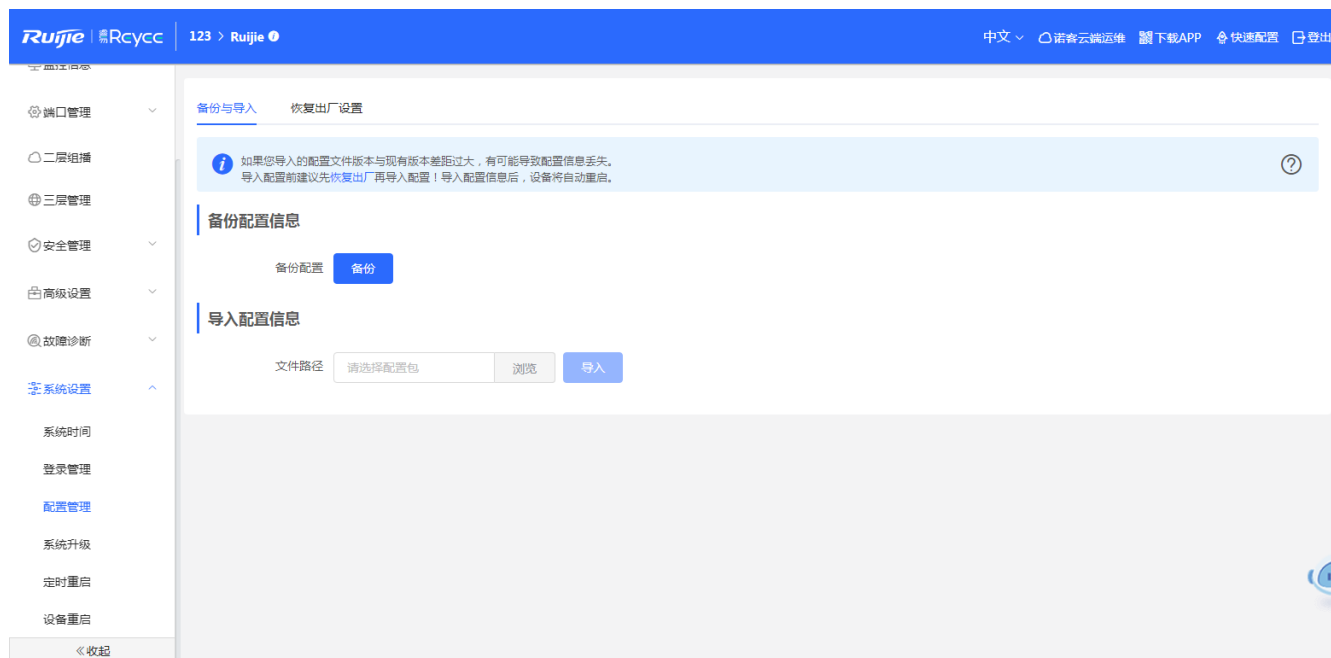
1. web访问超时时间，默认是1小时（3600秒）。建议用户及时<退出>可参考页头描述。

## 3.10.3 配置管理

### 3.10.3.1 备份和导出

当您配置完成交换机设备后，设备支持将配置文件的导出，生成备份配置并下载到本地。

当设备恢复出厂时，支持导入配置文件，然后恢复成导入的配置。

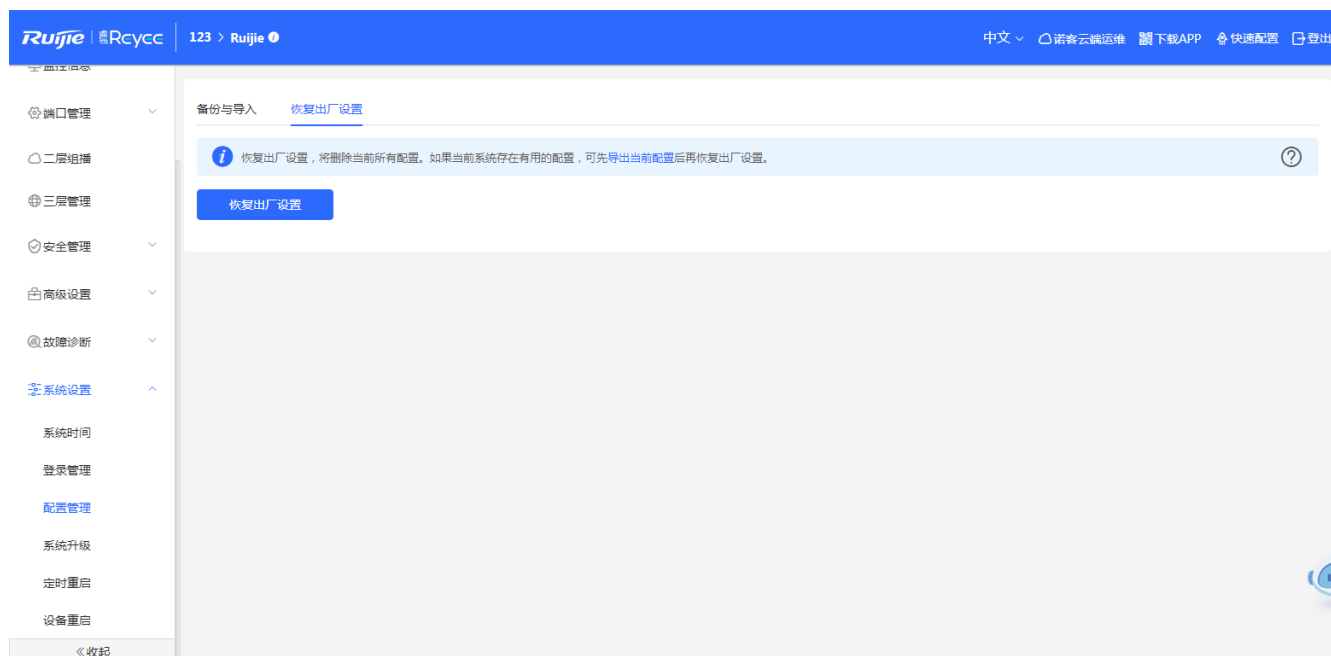


### 3.10.3.2 恢复出厂设置

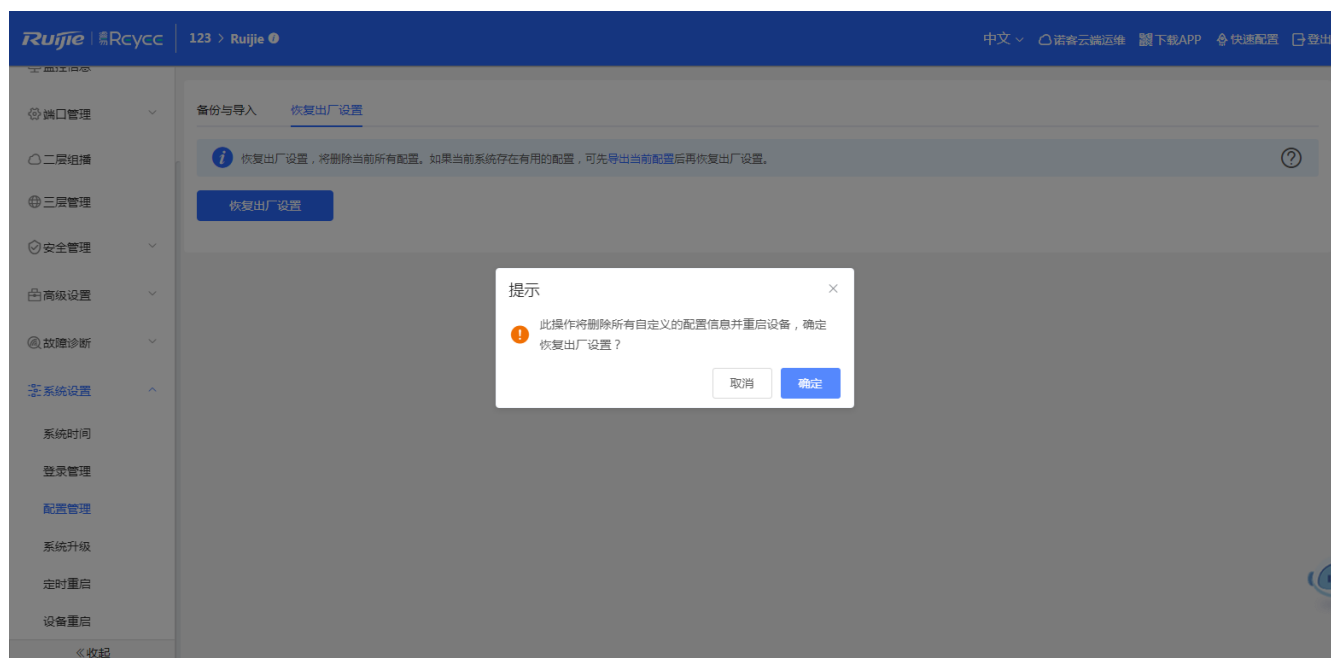
提供设备恢复出厂设置的入口。

#### **i** 说明

1. 当设备恢复出厂配置时，会恢复到出厂状态。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。



恢复出厂是比较敏感的操作，需要您点击确认后触发恢复并重启设备。如下：



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，如果网络上检测有存在可升级的“在线版本”，界面会显示可升级的版本信息，如下：



#### 在线升级

在线升级会保留当前配置，升级过程中会重启设备，请不要刷新或关闭浏览器，升级成功会自动跳转到登录页。

当前版本号

新版本号

新版本说明 1、优化抗扰算法；2、增强数据连接的稳定性。

提示 1) 若您的设备无法访问外网，请点击“[下载升级包](#)”保存到本地电脑。

2) 接着通过“[本地升级](#)”页面，选取升级包文件上传到设备进行升级。

马上升级 (推荐)

点击<直接升级>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，显示如下界面：



#### 在线升级

在线升级会保留当前配置，升级过程中会重启设备，请不要刷新或关闭浏览器，升级成功会自动跳转到登录页。

当前版本号

### 3.10.4.2 本地升级

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版本(格式：xxxx.tar.gz)。

**本地升级**

升级过程中请不要刷新页面或者关闭浏览器。



设备型号

软硬件版本

保留配置  (如果版本差异太大, 建议不保留配置升级)

安装包

请选择安装包

选取文件

上传文件

(上传系统升级包)

### 3.10.5 定时重启

开启此功能将在指定时间进行定时重启, 以获得更好的体验。建议定时重启时间在凌晨或无人使用网络的时间段执行。

The screenshot shows the Ruijie Rcycc web interface. The top navigation bar includes the Ruijie logo, the user '123', and the language '中文'. The left sidebar lists various system management options, with '系统设置' (System Settings) expanded to show '定时重启' (Scheduled Restart). The main content area displays the configuration for the scheduled restart feature. It includes an information icon and a note: '开启此功能将在指定时间进行定时重启, 以获得更好的体验。建议定时重启时间在凌晨或无人使用网络的时间段执行。' Below this is a toggle switch for '是否开启' (Enable) which is turned on. A row of checkboxes allows selecting the days for the restart, with all days (星期一至日) selected. A time selection field is set to 03:00. A blue '保存' (Save) button is located at the bottom of the configuration area.

### 3.10.6 设备重启

提供重启设备按钮, 如下:



**系统重启**

在系统重启过程中，请不要将设备断电！

重启系统

点击<重启系统>并确认后，设备将重启，重启后需要重新登录 web 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，设备起来之后，登入 Eweb，在界面中，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<>：是恢复默认密码；

选择<>：是恢复出厂配置，即密码和配置都会被清楚；

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）。