RG-NBS 系列交换机

ReyessOS 1.214 Web 管理手册

文档版本 V1.0

归档日期 2023-05-17

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
- 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

本手册中展示的部分信息（如产品型号、描述、端口类型、软件界面等）仅供参考，具体信息请以实际使用的产品版本为准。

1 登录设备

1.1 配置环境要求

- 浏览器：支持Google chrome、IE9.0、IE10.0、IE11.0以及部分基于谷歌/IE内核的浏览器（如360安全浏览器，推荐使用极速模式）。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。
- 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。

1.2 登录 Web

1.2.1 连接设备

使用网线将交换机端口与PC的网口相连，为PC配置一个与设备默认IP在同一网段的IP地址，确保PC能够Ping通交换机设备。如设置PC的IP地址为10.44.77.100。

表1-1 默认配置

功能特性	缺省值
设备IP	10.44.77.200
密码	首次登录时无需密码，可直接开始配置

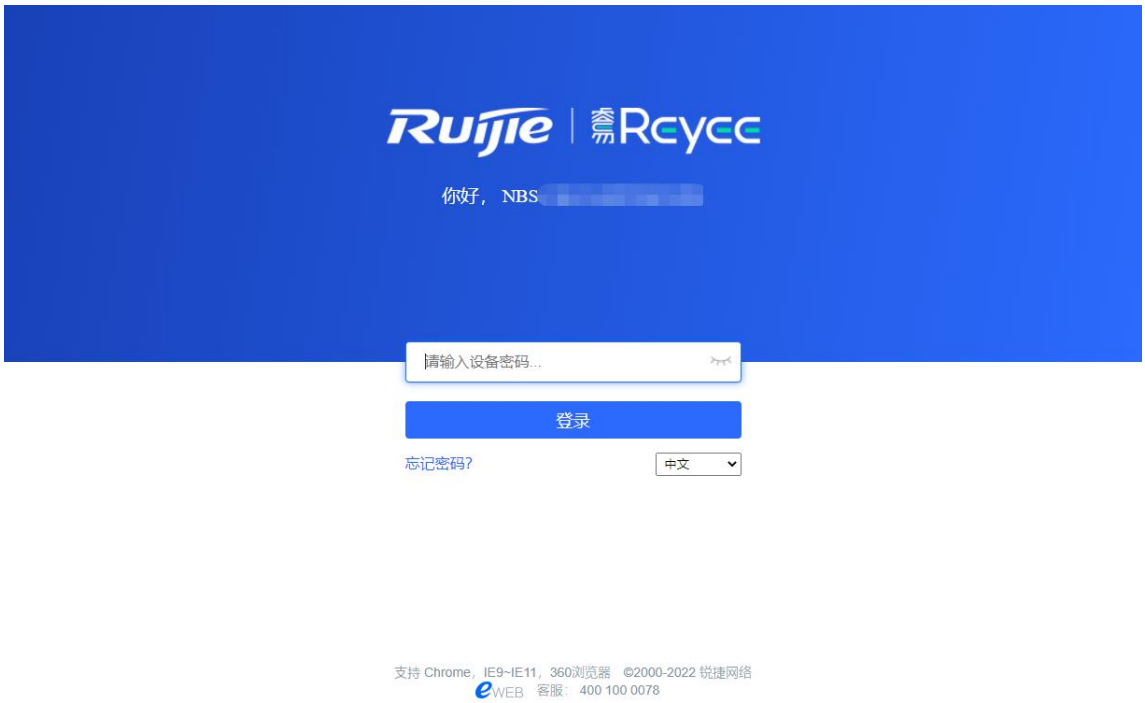
1.2.2 登录 Web

(1) 在浏览器地址栏中输入设备的IP地址（默认为10.44.77.200），进入登录页面。

说明

若用户修改了设备的静态IP地址，或者设备动态获取到了新的IP地址，只要保证PC和设备处于同一局域网，且IP地址处于同一网段，就可以使用新的IP地址访问设备的Web管理系统。

(2) 输入密码后点击<登录>，进入Web管理系统首页。



首次登录无需输入密码，可直接开始配置。

为了保障设备安全，建议在首次登录Web管理系统后及时设置管理密码。设置管理密码后，再次登录Web管理系统时需要输入密码。

若忘记设备IP或密码，可在设备接通电源的情况下长按设备面板上的reset键5秒以上使设备恢复出厂设置，恢复后即可使用默认IP和密码登录。

注意

恢复出厂设置将清空设备的全部配置，请谨慎操作。

1.3 快速配置

1.3.1 配置前的准备

设备连接电源，用网线将设备端口与上级设备连接。

1.3.2 配置步骤

1. 添加设备至网络

出厂配置下，用户可以对组网中所有设备进行批量设置和集中管理，因此在开始配置前，需要查看并确认全网在线设备的数量和网络状态。

说明

一般情况下，多台新设备上电接入会自动互联成一个网络，用户只需要确认设备数量无误即可。

若网络中存在未加入当前网络的其他设备，可以点击<添加到我的网络>并输入所添加设备的管理密码，将对应设备手动添加至设备所在网络中，再开始全网配置。

2. 创建网络项目

点击<开始配置>，设置设备的联网方式和管理密码等。

(1) **项目名称**：用于标识设备所在的网络。

(2) **上网方式**：选择设备的联网方式。

- **动态IP**：由上联DHCP服务器为设备分配IP地址。设备默认检测能否动态获取到IP地址，若成功获取，则无需手动设置IP。
- **静态IP**：用户手动输入指定的IP地址、子网掩码、网关IP地址和DNS服务器地址。

(3) **管理密码**：设置登录管理页面的密码。

(4) **国家码**：请选择实际所在的国家或地区。

(5) **时区**：设置系统时间，默认开启网络时间服务器提供时间服务。请选择实际所在的时区。

点击<创建项目并连通网络>，设备将下发初始化相关配置，并检测网络。完成快速配置后，新设备已联网，可继续将设备绑定云端账号，进行远程管理，具体操作请参考页面指引登录诺客云平台进行配置。

说明

- 点击右上角<退出>，可根据提示指引，跳过快速配置进入Web配置页面。退出或完成快速配置后如需再次配置，请点击Web页面顶部导航栏中的  标志。
- 修改管理密码后需要重新访问设备管理地址，使用新密码登录设备。

1.4 工作模式介绍

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。修改工作模式请参考3.1.1　2. 切换工作模式。

组网模式：开启自组网发现功能，设备能够在网络中被发现和发现网络中其他设备，设备间根据设备状态进行自组网并同步全局配置。登录设备的Web管理页面，可以查看到整网设备的管理信息。开启自组网发现后能够帮助用户更高效地对当前网络进行运维和管理，建议保持开启。

当设备处于组网模式时，Web页面分为两种配置模式：整网管理模式和本机管理模式。详见1.5　切换管理模式。

独立模式：关闭自组网发现功能，设备在网络中将不被发现。登录Web后只能对当前登录设备进行配置和管理。若仅配置单台设备，或不希望设备被同步全局配置，可关闭自组网发现功能。

1.5 切换管理模式

独立模式下，只能对当前登录设备进行配置和管理，无自组网功能，页面如图1-1；

组网模式下，Web页面分为整网管理模式与本机管理模式。点击导航栏中当前管理模式，在下拉框中选择模式可进行切换。

- 整网管理模式：查看网络中所有设备的管理信息，基于整网视角对当前网络中的所有设备进行配置，页面如图1-2；
- 本机管理模式：仅对当前登录设备进行配置，页面如图1-3。

图1-1 独立模式下 Web 页面

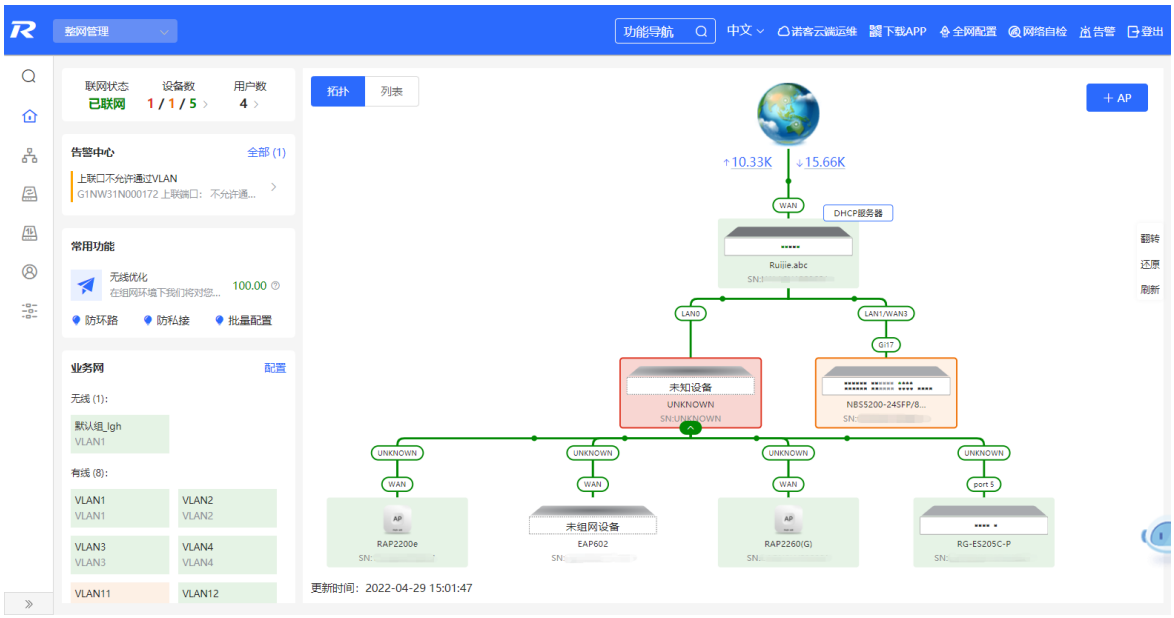
图1-2 组网模式下整网管理模式 Web 页面

图1-3 组网模式下本机管理模式 Web 页面

2 整网管理

2.1 整网信息概览

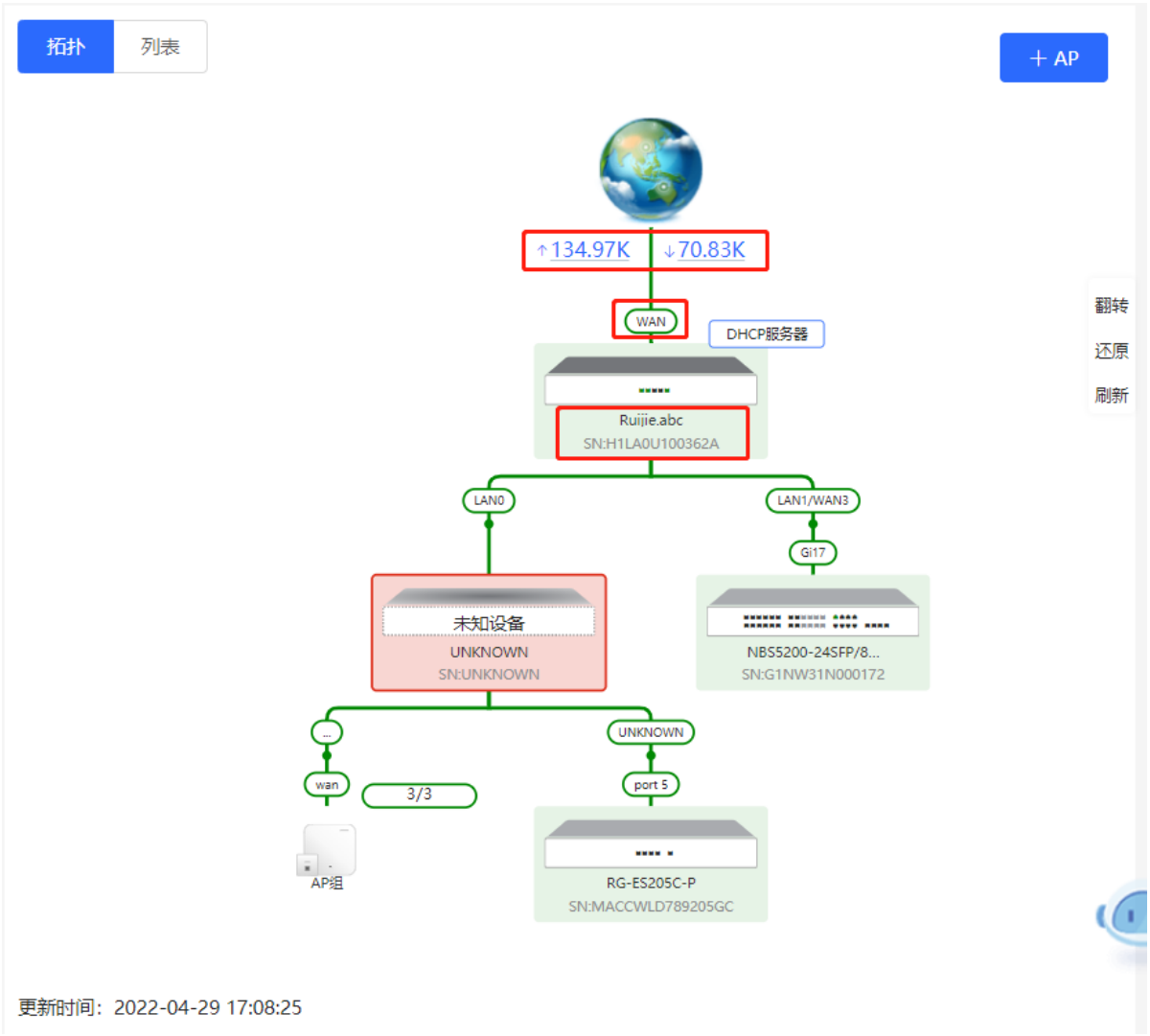
整网管理模式下，[整网概览]页面可视化地展现了当前网络的拓扑结构、上下行实时流量、联网状态、用户数等信息，并提供了网络与设备的快捷设置入口。用户可以在该页面对整网的网络状态进行监控和管理。



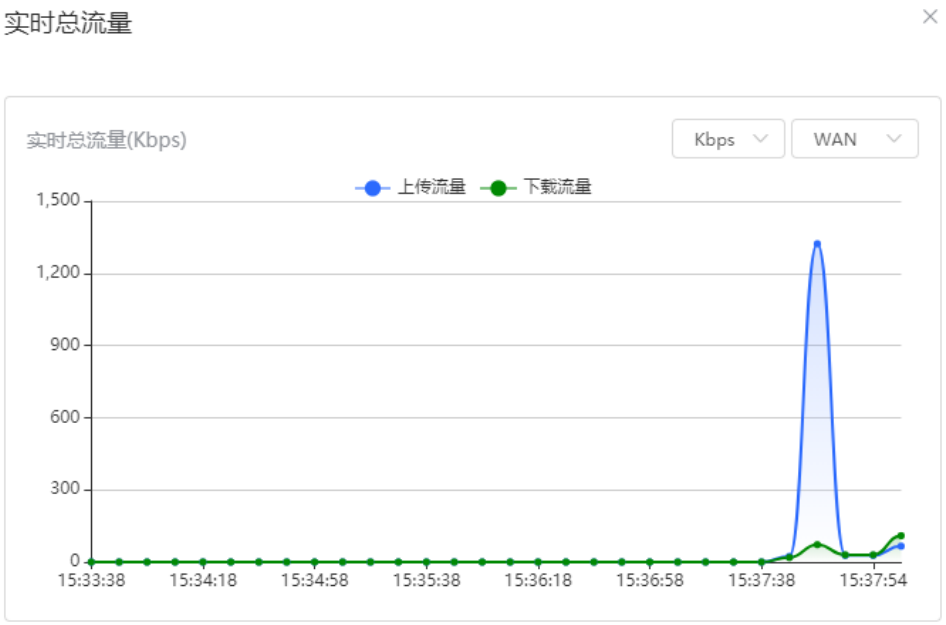
2.2 查看组网信息

【整网管理-页面向导】整网概览

组网拓扑图包含了在线设备、连接端口号、设备SN号和上下行实时流量等信息。

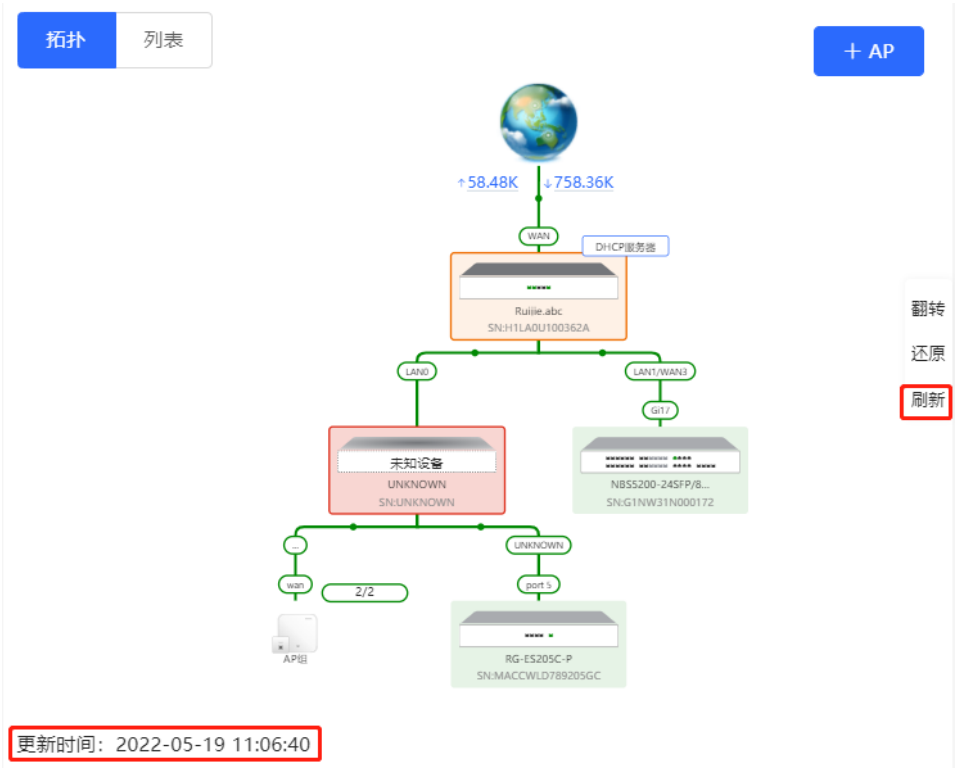


- 点击流量数据，可查看实时总流量信息。



- 点击拓扑中的设备，可查看设备的运行状态和配置信息，并对设备功能进行配置。设备名称默认为产品型号，点击 可将设备名称修改为便于区分的描述信息。

- 拓扑图左下角为该拓扑的更新时间。点击“刷新”可更新拓扑图为最新状态。更新拓扑数据需要一定时间，请耐心等待。

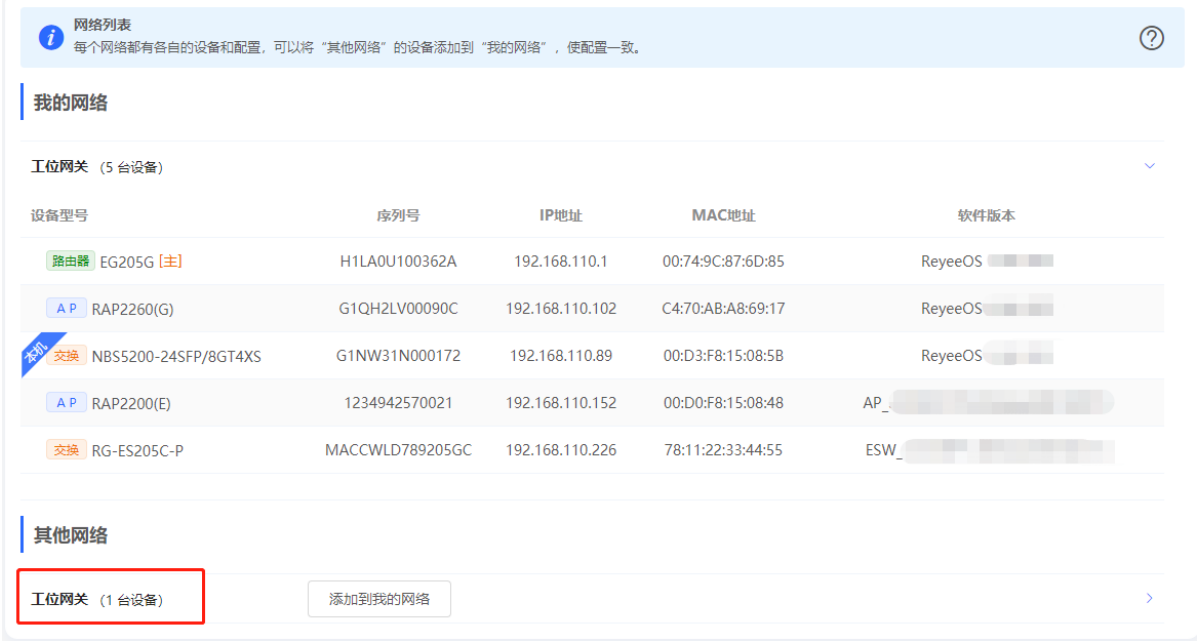


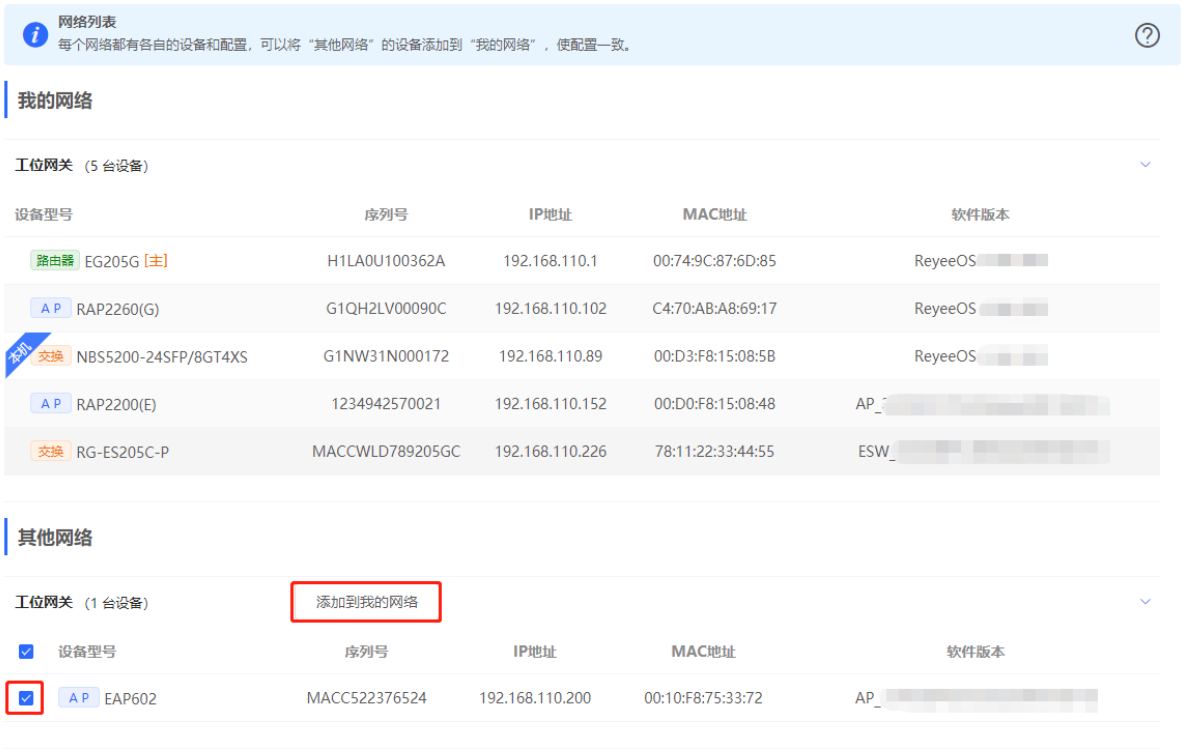
2.3 添加组网设备

2.3.1 有线连接

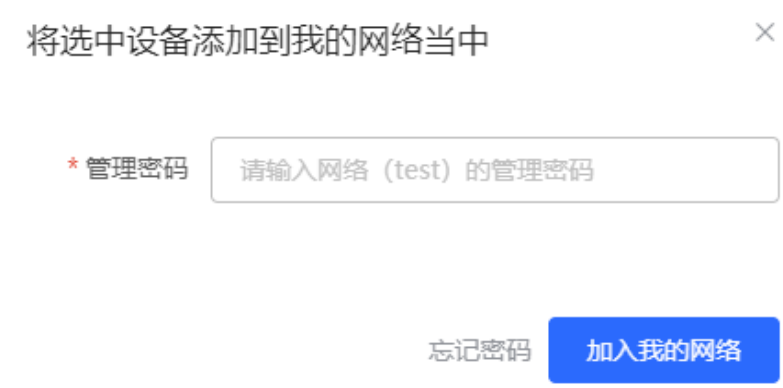
(1) 新设备通过有线方式连接网络中的设备时，系统将弹出提示信息，提示网络中出现未组网的其他网络设备，并在[整网概览]页面左上角“设备数”中显示（橙色数字表示发现的未组网设备数量），点击“点击去处理”可设置加入当前网络。

(2) 跳转到网络列表页面后，点击展开“其他网络”中的信息，勾选待添加的设备，点击<添加到我的网络>。





(3) 添加出厂新设备不需要输入密码，而添加有密码的设备需要输入该设备的配置密码。密码错误将添加失败。



2.3.2 AP Mesh

对于支持AP Mesh易联功能的AP，上电后无需连线，可直接通过易联方式添加到当前组网中，与其他无线设备进行Mesh组网，并自动同步Wi-Fi配置。

注意

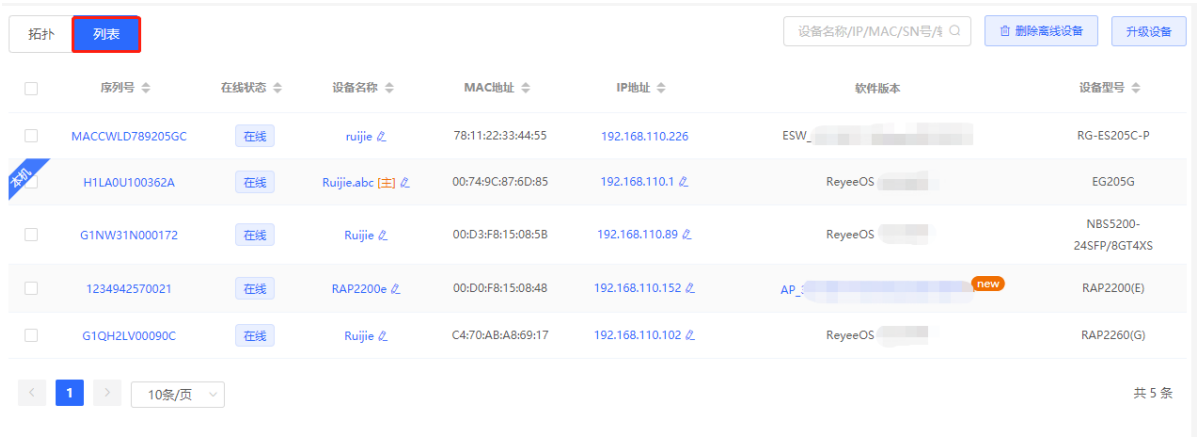
当前网络需开启易联功能（参考11.9 ）才可以扫描到AP，AP需在附近上电，距离太远或有障碍物遮挡将导致AP无法被扫描到。

(1) 新AP上电后放置在已有AP附近（能够接收到AP的Wi-Fi信号），登录组网中的设备，在[整网概览]页面点击拓扑右上角的<+AP>，扫描周围不属于当前网络且未接网线的AP。

(2) 选择需要添加的AP，添加至当前网络。添加新设备不需要输入密码，添加有密码的设备需要输入该设备的管理密码。

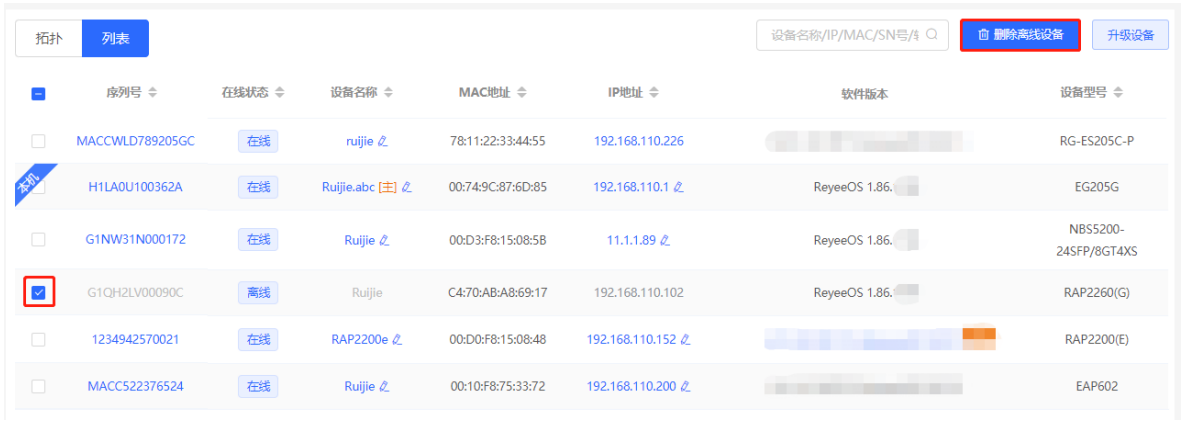
2.4 管理组网设备

在[整网概览]页面点击拓扑左上角的“列表”或点击菜单栏的“设备管理”，可切换至设备列表视图，查看当前组网中的所有设备信息。用户只需登录组网中的一台设备，便可以对整网设备进行配置和管理。



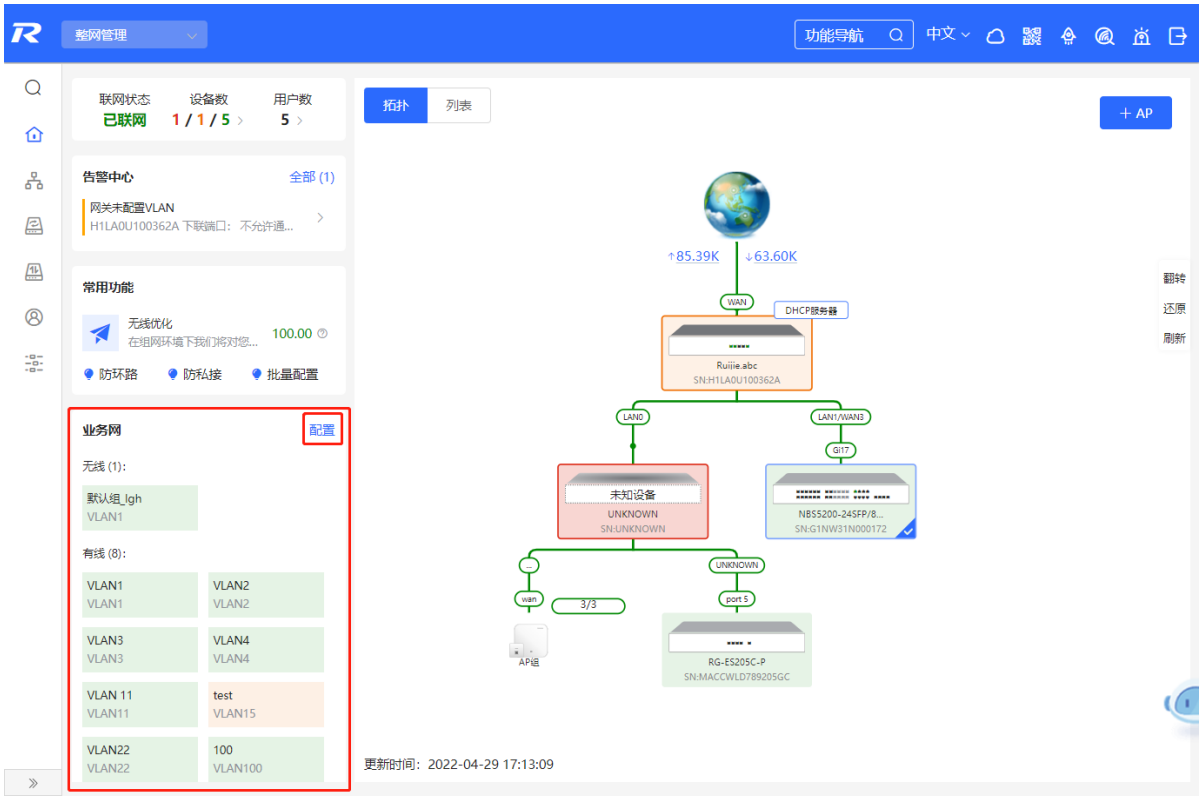
- 点击设备序列号，可对指定设备进行单独配置。

- 勾选已离线的设备，点击<删除离线设备>，可以将设备从列表和组网拓扑中移除。



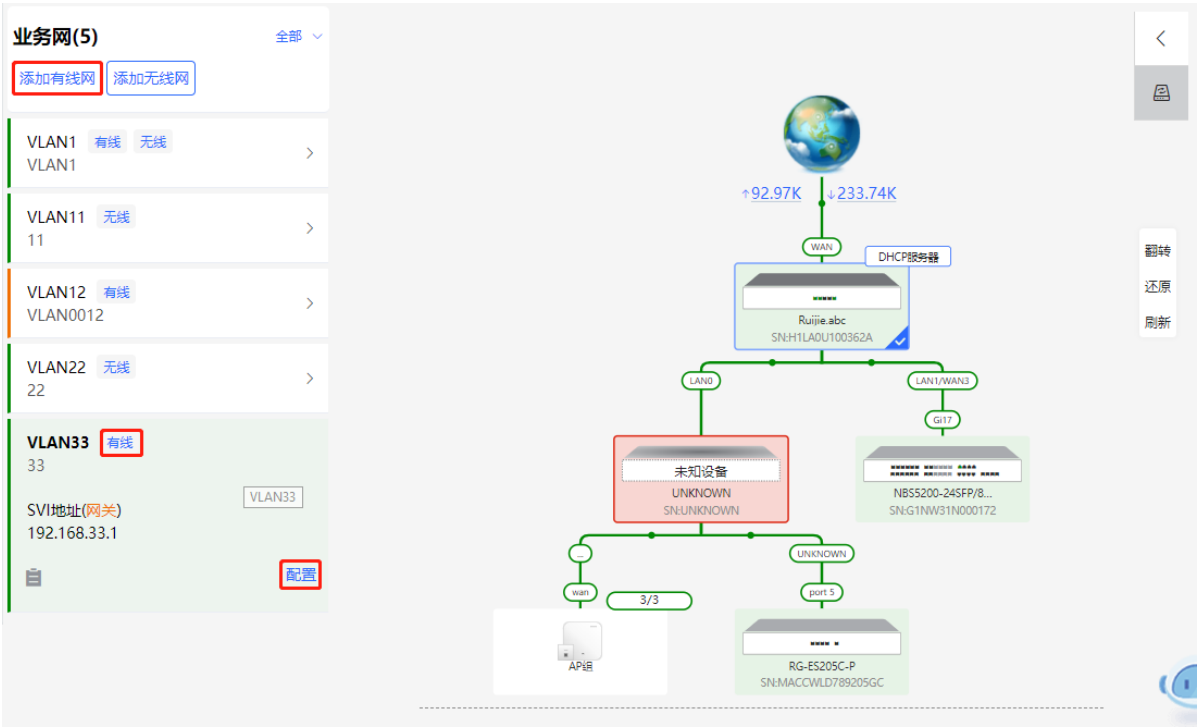
2.5 设置业务网

[整网概览]页面左下方显示当前网络中的无线网络和有线网络配置。点击“配置”可跳转至业务网配置页面（或点击[整网管理]>>[业务网]）。

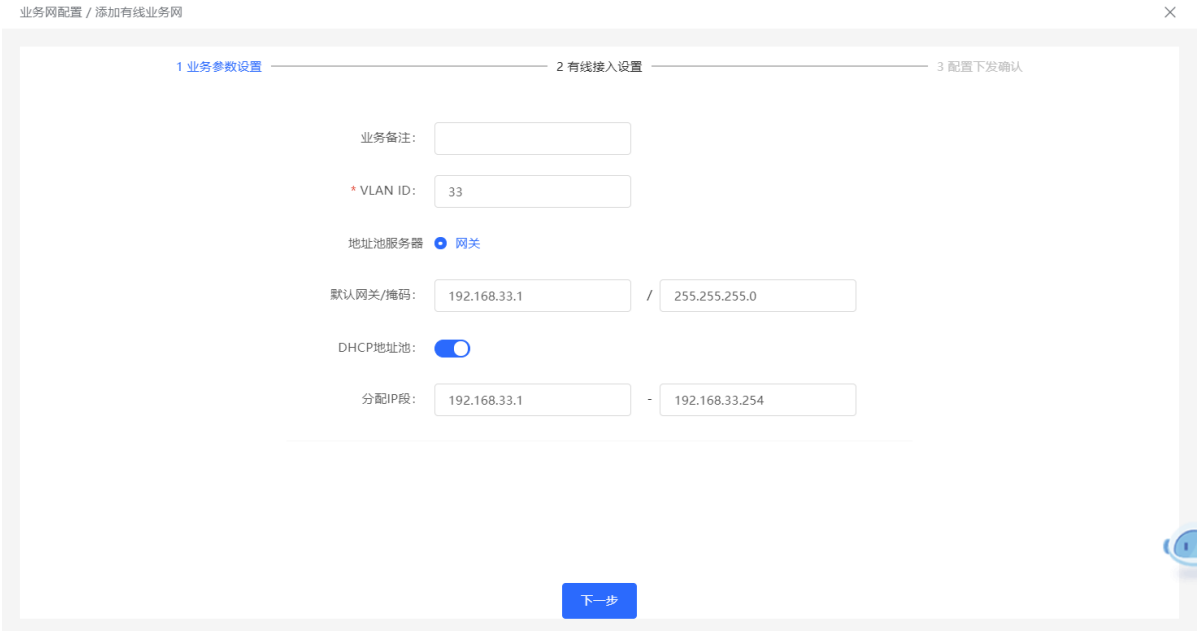


2.5.1 设置有线网

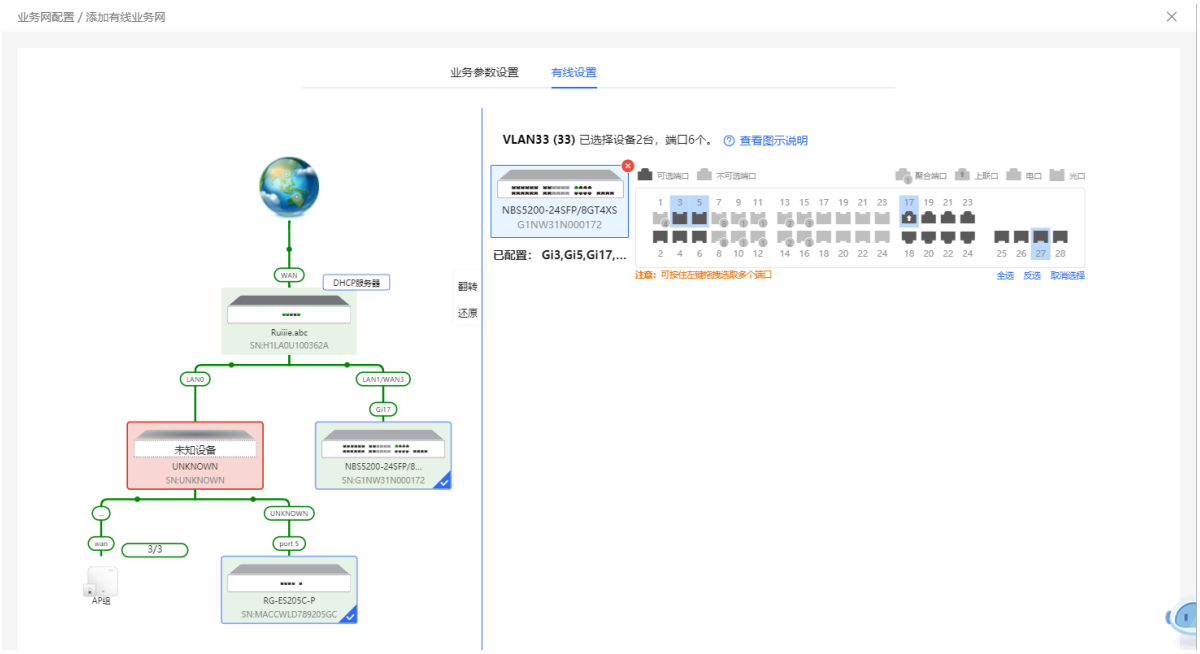
(1) 点击“添加有线网”为当前网络添加有线网络配置，或选择已创建的有线网络VLAN，点击“配置”进行修改。



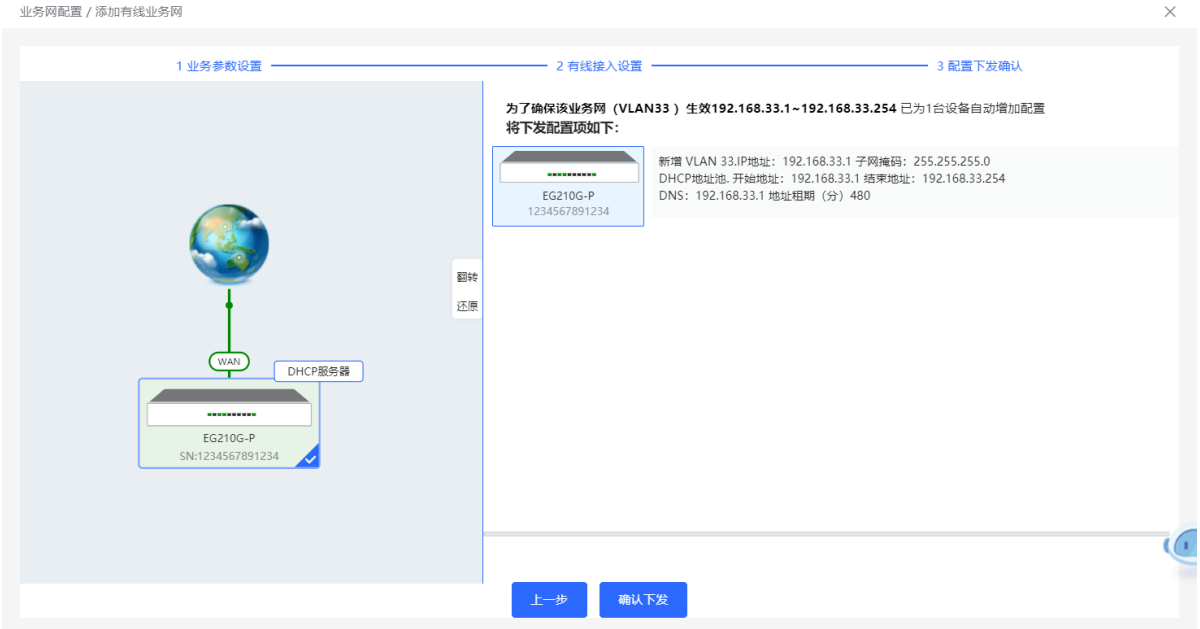
(2) 设置用于有线接入的VLAN、该VLAN下接入终端的地址池服务器以及是否创建新的DHCP地址池。可选择交换机或网关设备作为地址池服务器。完成业务参数设置后，点击<下一步>。



(3) 在拓扑中选择需要配置的交换机，并选择VLAN所包含的交换机端口，点击<下一步>。

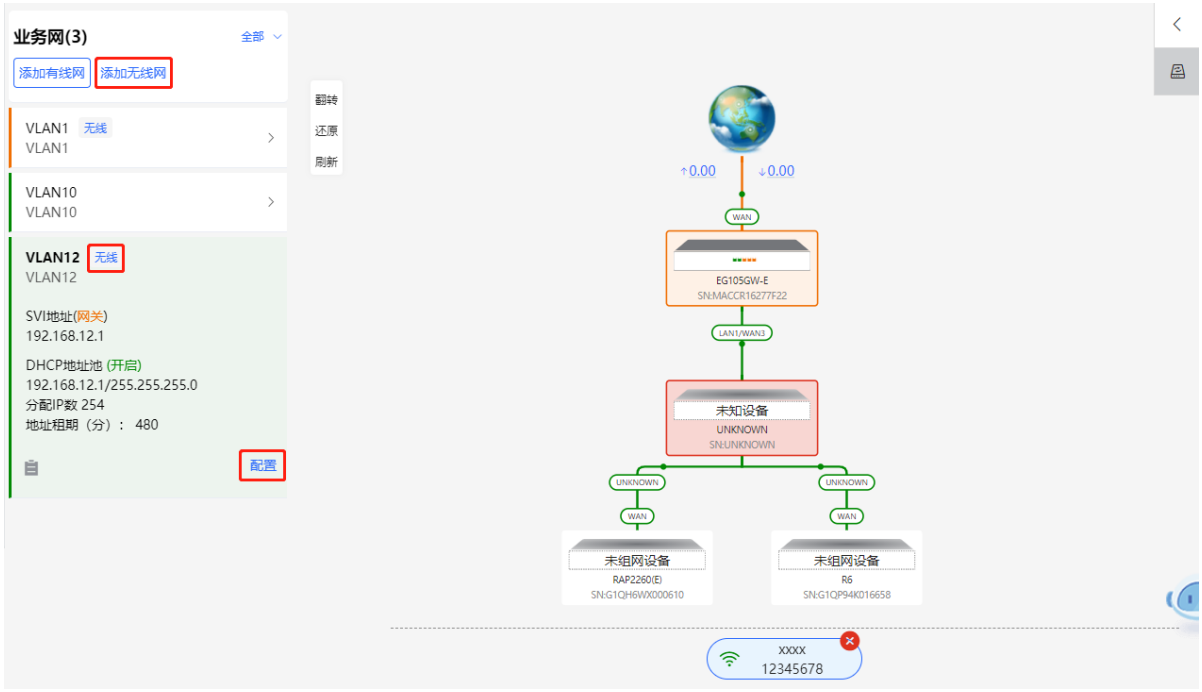


(4) 请确认将下发的配置项是否正确，确认无误后点击<确认下发>，稍等片刻等待配置生效。

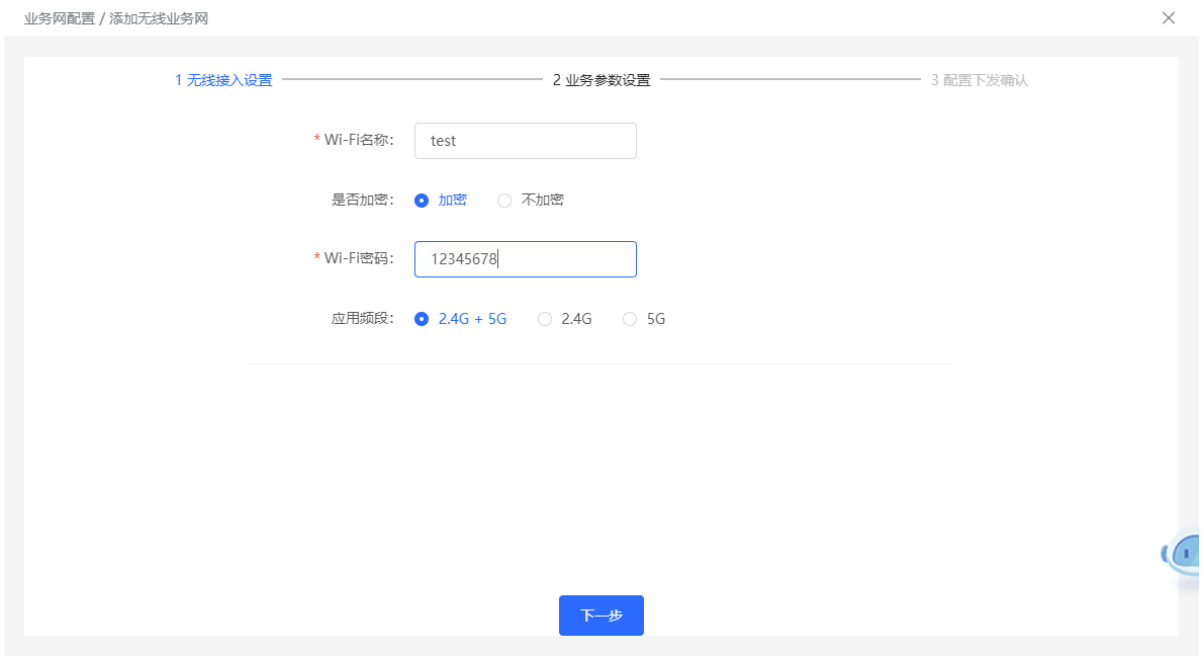


2.5.2 设置无线网

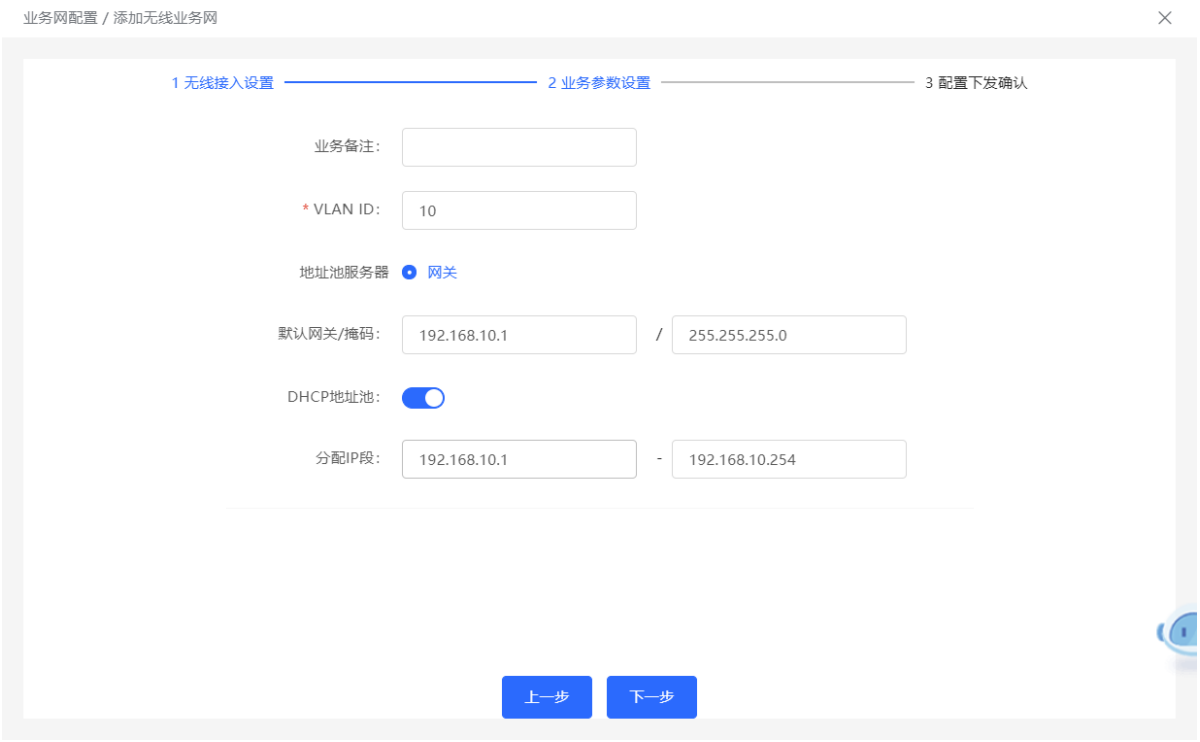
(1) 点击“添加无线网”为当前网络添加无线网络配置，或选择已创建的无线网络VLAN，点击“配置”进行修改。



(2) 设置Wi-Fi名称、Wi-Fi密码和应用频段。点击<下一步>。



(3) 设置用于无线接入的VLAN、该VLAN下接入终端的地址池服务器以及是否创建新的DHCP地址池。可选择交换机或网关设备作为地址池服务器。完成业务参数设置后，点击<下一步>。



(4) 请确认将下发的配置项是否正确，确认无误后点击<确认下发>，稍等片刻等待配置生效。

2.6 告警信息处理

【整网管理-页面向导】整网概览

当网络存在异常，整网概览页面将对异常信息进行告警提示，并给出相应解决方案。点击“告警中心”的告警提示，可查看故障设备、问题详情及解决方案，请参考解决方案进行故障排查与处理。

2.7 查看在线用户

[整网概览]页面左上角的“用户数”显示了当前网络中的在线终端用户总数；鼠标移至用户数量处，将分别显示当前有线用户、2.4GHz频段的无线用户以及5GHz频段的无线用户的数量。

点击可跳转至在线用户详情页面（或点击[终端管理]>>[在线用户]）。

表2-1 在线用户信息说明

字段	说明
名称/接入类型	终端用户名称以及接入方式，分为有线接入和无线接入
接入位置	用户接入的设备的SN号，有线接入时点击可查看接入端口
IP地址/MAC地址	用户的IP地址和MAC地址
当前速率	用户上传和下载的数据传输速率
无线信息	无线用户所关联的无线网络信息，包含信道、信号强度、在线时间、协商速率等

2.8 智能设备网

注意

本功能的支持情况在不同产品间存在差异，目前支持本功能的产品有：RG-NBS6002系列、RG-NBS7003系列和RG-NBS7006系列设备。

2.8.1 功能简介

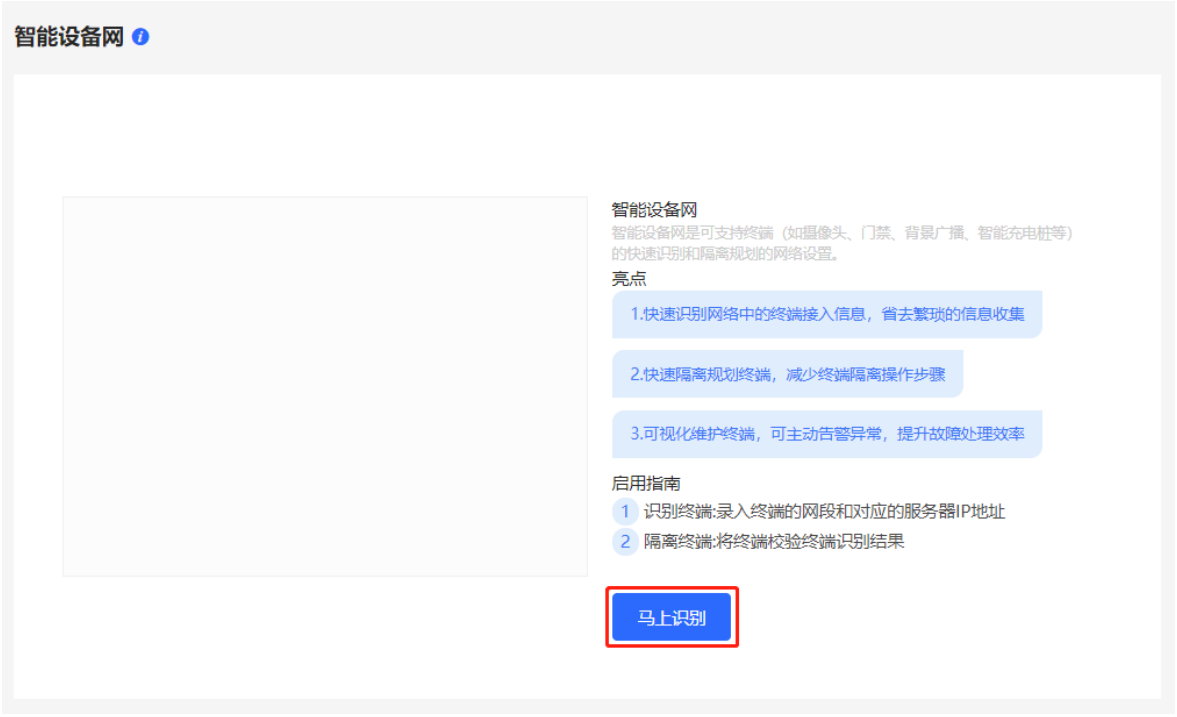
智能设备网用于快速为智能终端规划和设置隔离网络，使终端网络与正常业务网络以及其他类型的终端间相互隔离，提高网络的稳定性。智能设备网支持快速识别多种类型的终端（如摄像头、门禁、背景广播、智能充电桩等）和在终端上批量执行隔离规划，与传统的终端网络规划及部署步骤相比，免去了繁琐的信息收集并简化了设置终端隔离的步骤。

设置智能设备网后，页面可视化地展现终端信息，并主动告警异常，能够有效提升故障处理效率。

2.8.2 配置步骤

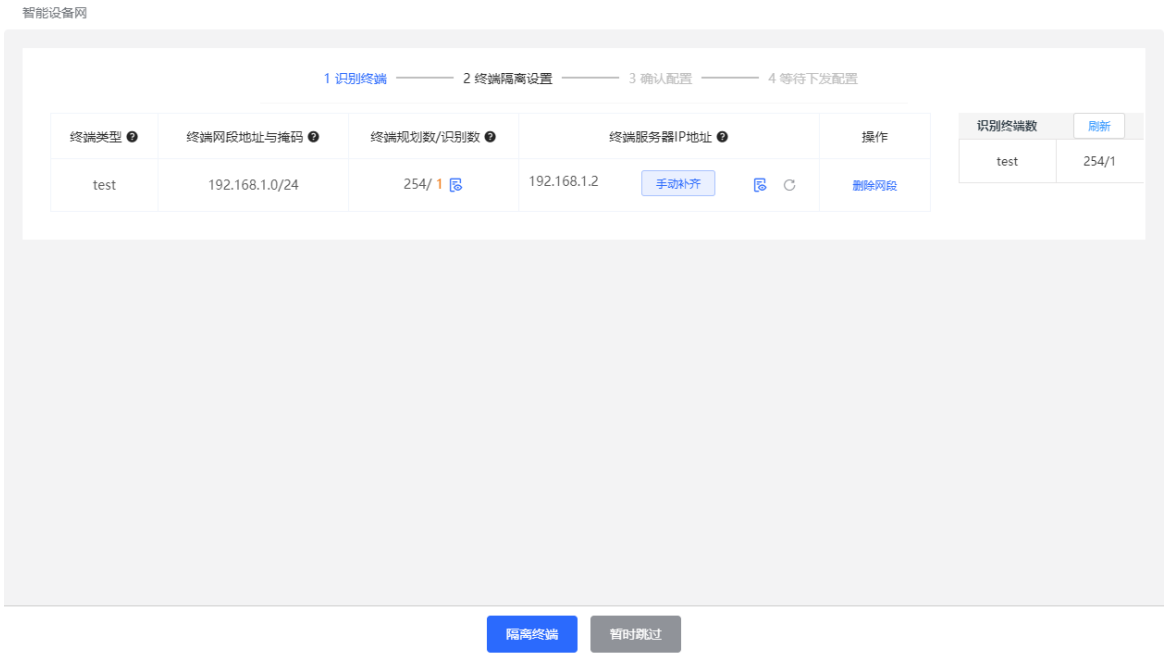
【整网管理-页面向导】终端管理>>智能设备网

(1) 点击<马上识别>。



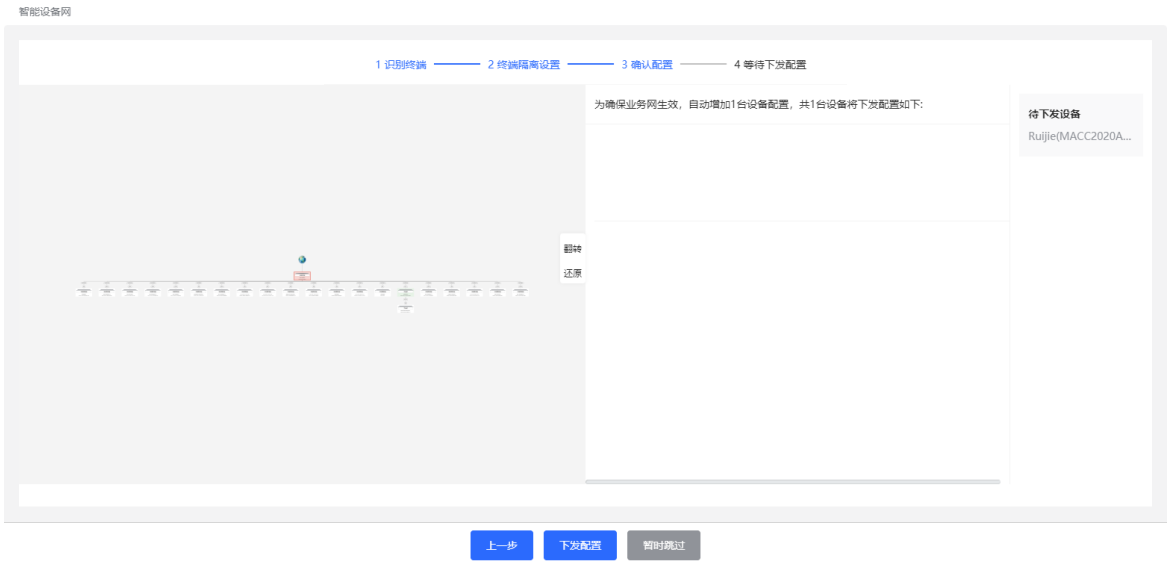
(2) 点击<+终端设备>，输入终端类型（可从下拉框中选择或自定义）、终端的网段、规划数量和对应的服务器IP地址，用于识别终端。可设置多类终端的网段。填写完成后点击<马上识别>。

(3) 显示识别到的终端和终端服务器信息，包括IP地址、MAC地址、所连接交换机的SN号以及连接端口，点击 可查看详细信息。如果未识别到终端服务器的连接信息，需要点击<手动补齐>，手动填写相关信息。确认终端设备信息正确后，点击<隔离终端>。

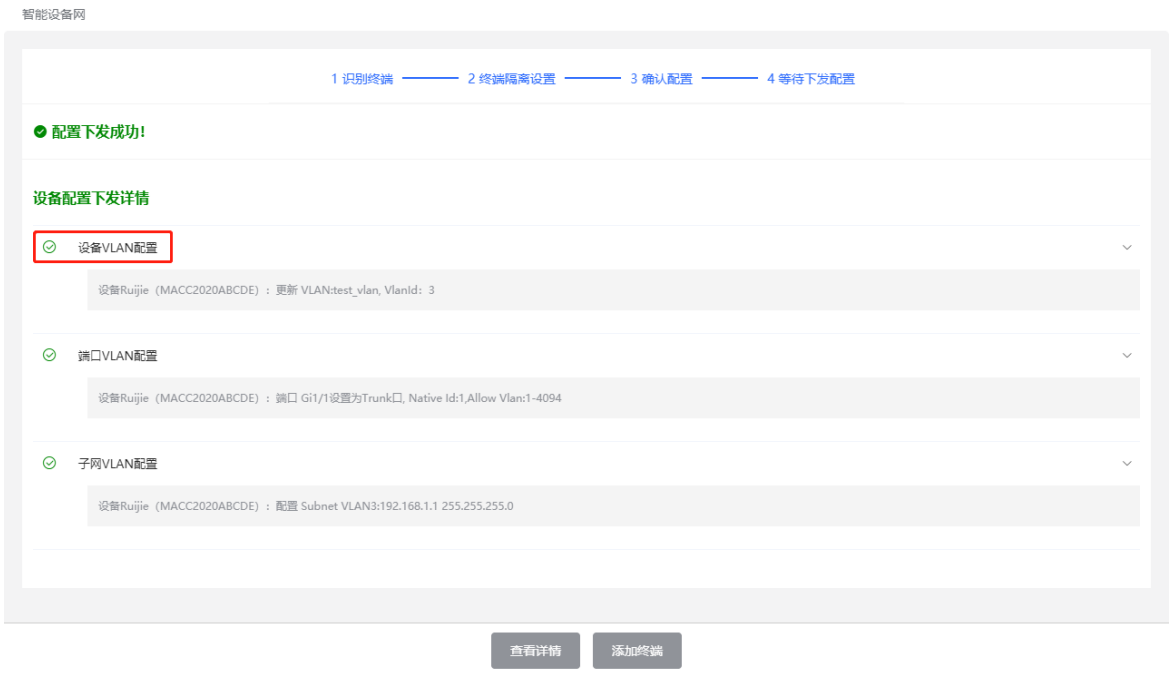


(4) 输入隔离终端的VLAN的名称、VLAN ID、网关地址和子网掩码。勾选需要配置的网段表项，点击<生成配置>。

(5) 确认需要下发的配置无误后，点击<下发配置>。如需修改，可点击<上一步>，回退至设置页面。



(6) 页面显示配置下发成功表示已完成设置。可点击配置项查看配置下发详情。完成配置下发后，点击<查看详情>将跳转至智能设备网监控信息页面；点击<添加终端>可继续设置终端网段。



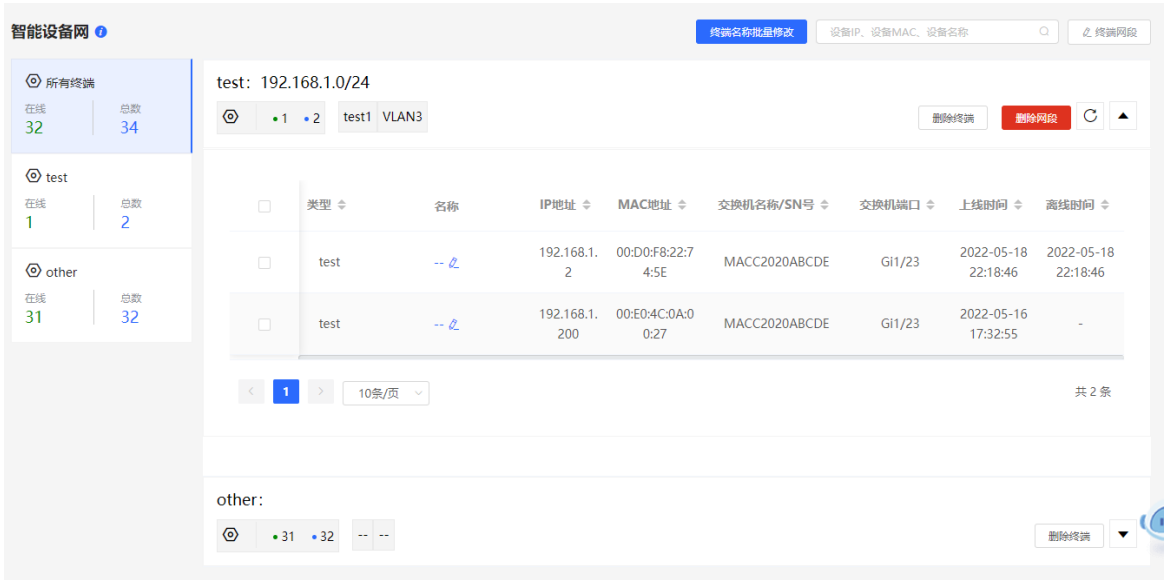
(7) 完成智能设备网设置后，可在页面查看终端的监控信息，包括终端在线状态、连接信息、设备信息和上下线时间等。

勾选终端表项后点击<删除终端>，可将指定终端从当前网络移除。

点击<终端名称批量修改>，可导入包含终端IP和终端名称的txt文件（每个终端一行，每行含有一个IP和一个名称，IP和名称之间用Tab键分隔），批量修改终端名称。

点击<终端网段>，可修改服务器和隔离VLAN信息，或添加新的终端网段。

点击<删除网段>，将删除对应智能设备网配置。



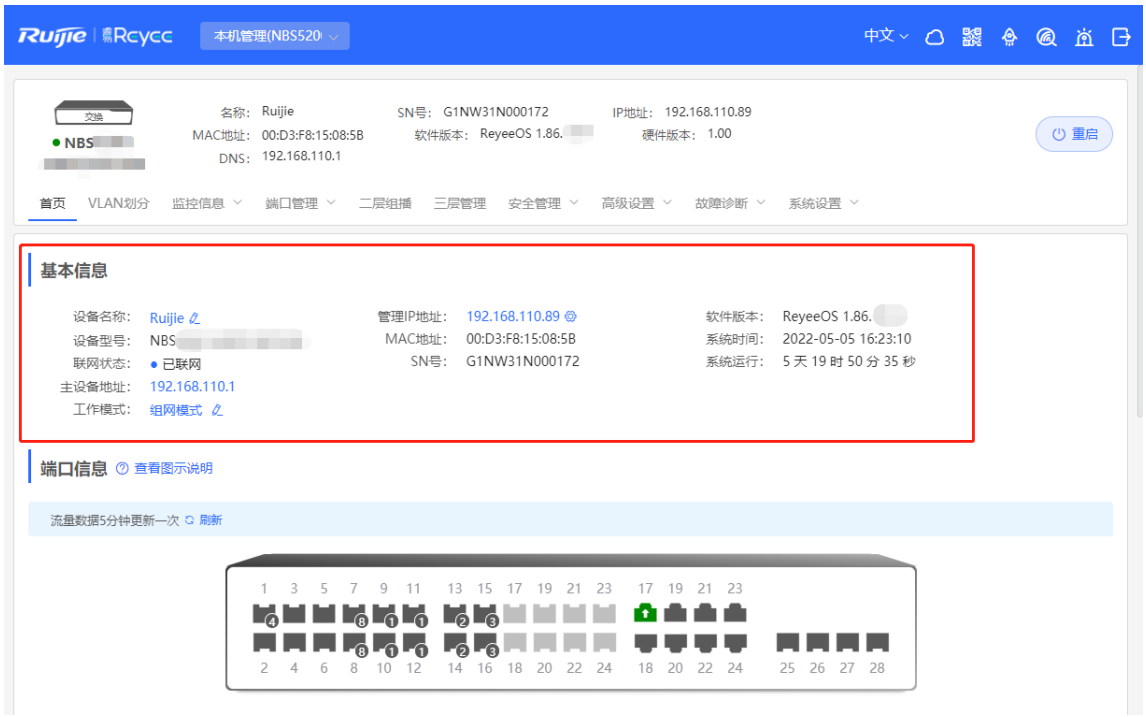
3 基础管理

3.1 交换机信息概览

3.1.1 设备基本信息

【本机管理-页面向导】首页>>基本信息

基本信息包含设备名称、设备型号、SN号、软件版本、管理IP、MAC地址、联网状态、系统时间和工作模式等信息。



1. 设置设备名称

点击设备名称，可对设备名称进行修改，以便于区分不同设备。

2. 切换工作模式

点击当前工作模式可进行修改。

3. 设置管理 IP

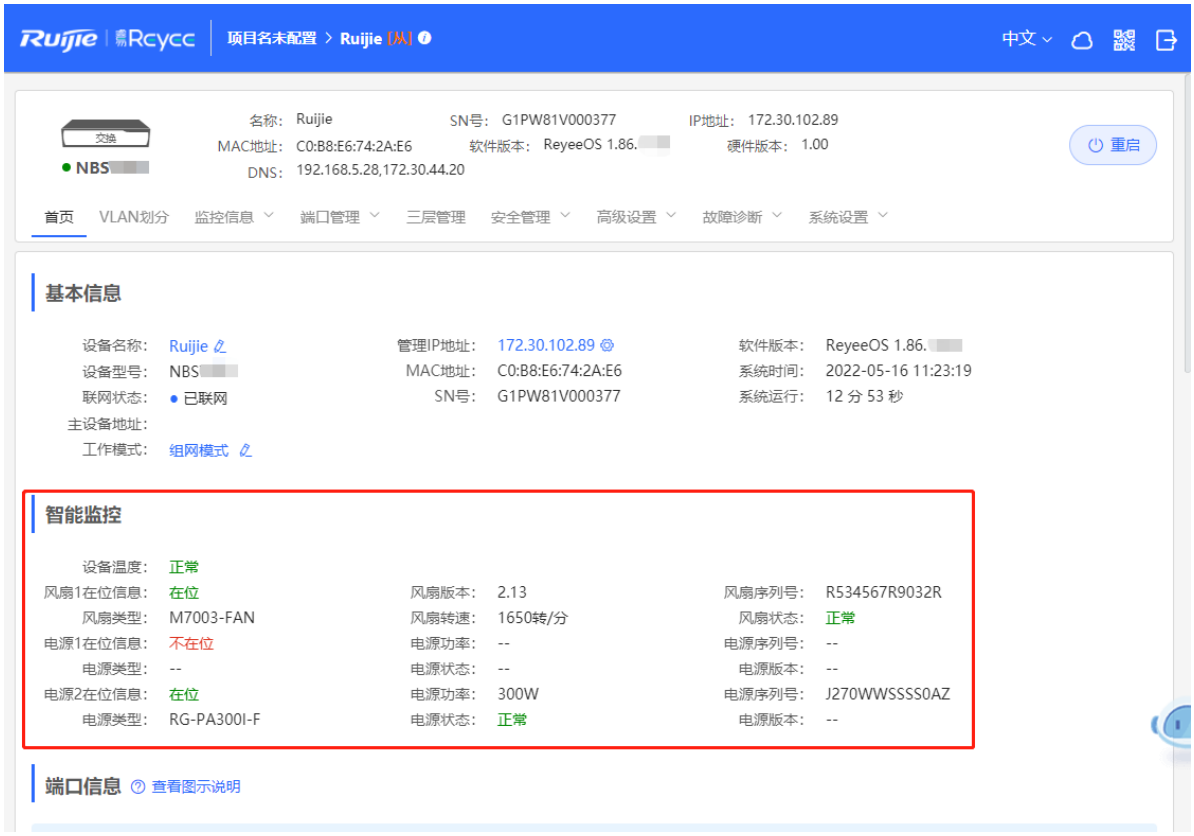
点击当前管理IP地址，将跳转至管理IP配置页面。详见4.6 设置管理IP。

3.1.2 硬件监控信息

> 注意
> 仅RG-NBS6002系列、RG-NBS7003系列和RG-NBS7006系列设备支持显示本类信息。

【本机管理-页面向导】首页>>智能监控

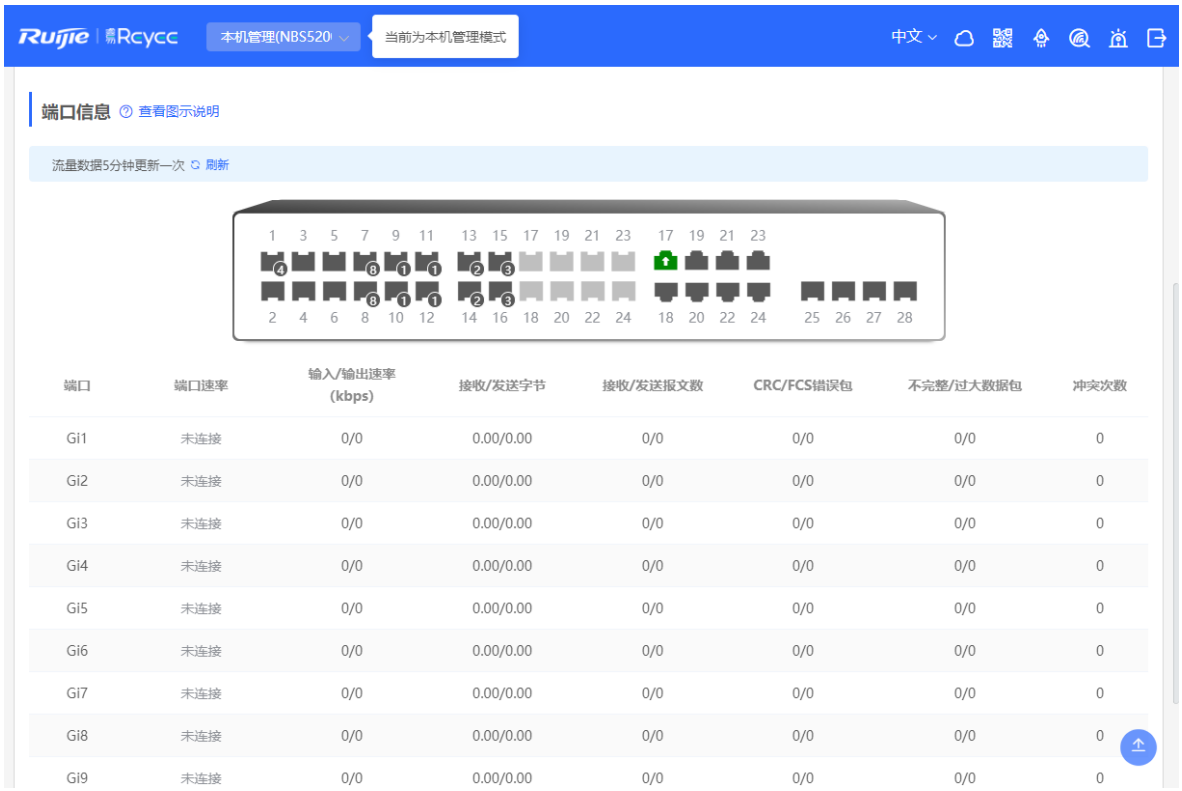
显示设备当前的硬件工作状态，如设备温度、电源状态等。



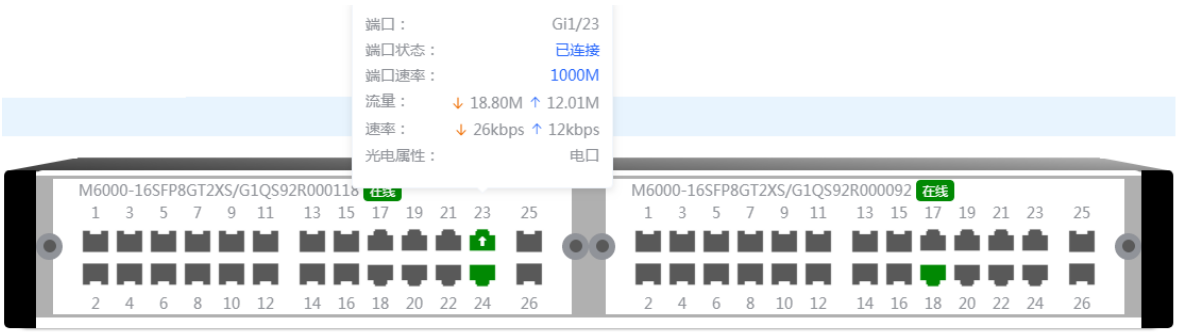
3.1.3 设备端口信息

【本机管理-页面向导】首页>>端口信息

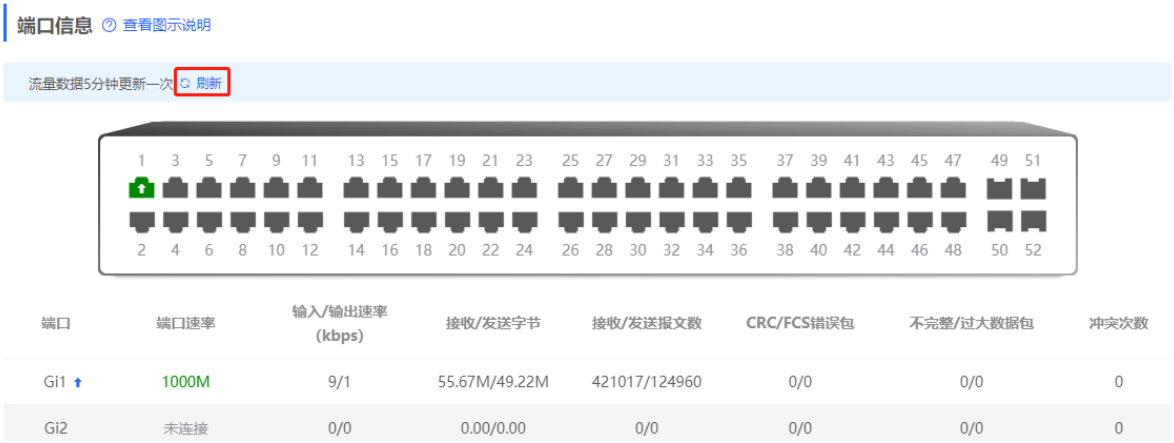
- 页面展示了交换机当前所有端口的详细信息。点击<查看图示说明>，可查看不同颜色或形状的端口图标所对应的端口角色与状态。



- 鼠标移至端口面板中的端口（如Gi1/23）图标上，将显示更多的端口信息，包括端口号、端口状态、端口速率、端口上下行流量和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”实时获取最新的端口流量及状态信息。



3.2 端口流量统计

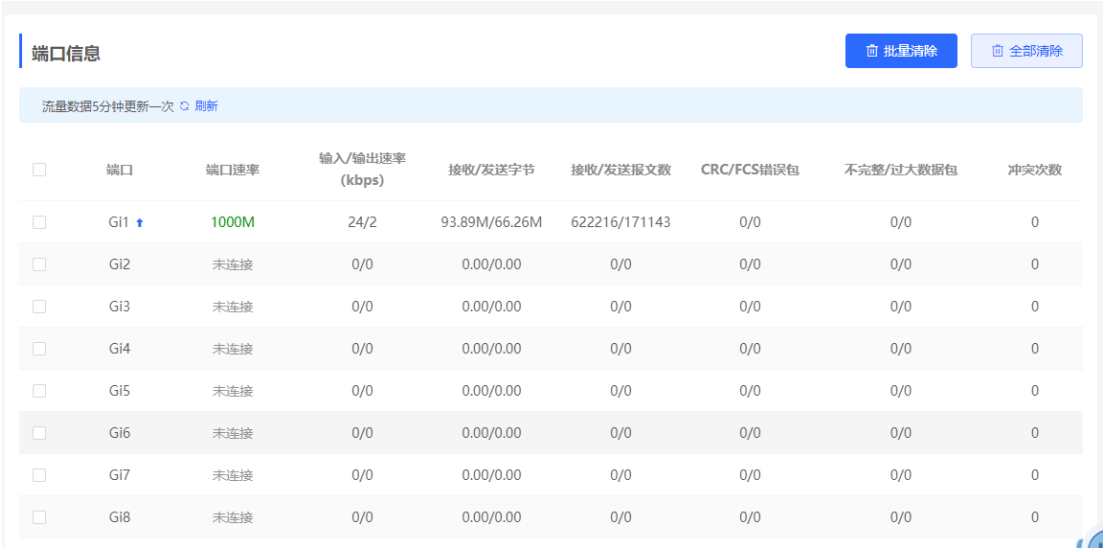
【本机管理-页面向导】监控信息>>端口流量

显示设备端口的速率、收发报文数、错包数等流量统计信息。端口速率每5秒更新一次数据，其他流量数据每5分钟更新一次。

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

端口包含聚合口，聚合口流量为成员口流量的总和。



3.3 MAC 地址管理

3.3.1 功能简介

MAC地址表中记录了MAC地址与端口及其所属VLAN的对应关系。

设备根据报文中的目的MAC地址查询MAC地址表，如果MAC地址表中存在与报文目的MAC相同的表项，则将报文从该条表项中记录的端口单播转发；如果MAC地址表中不存在与报文目的MAC相同的表项，设备将报文从接收端口以外的VLAN内所有其他端口广播转发。

MAC地址表项分为以下三种：

- 静态MAC地址表项：由用户手工配置，用于从正确端口转发目的MAC地址与表项中MAC地址匹配的报文，表项不老化。
- 动态MAC地址表项：由设备自动生成，用于从正确端口转发目的MAC地址与表项中MAC地址匹配的报文，表项存在老化时间。
- 过滤MAC地址表项：由用户手工配置，用于丢弃指定源或目的MAC地址的报文，表项不老化。

说明

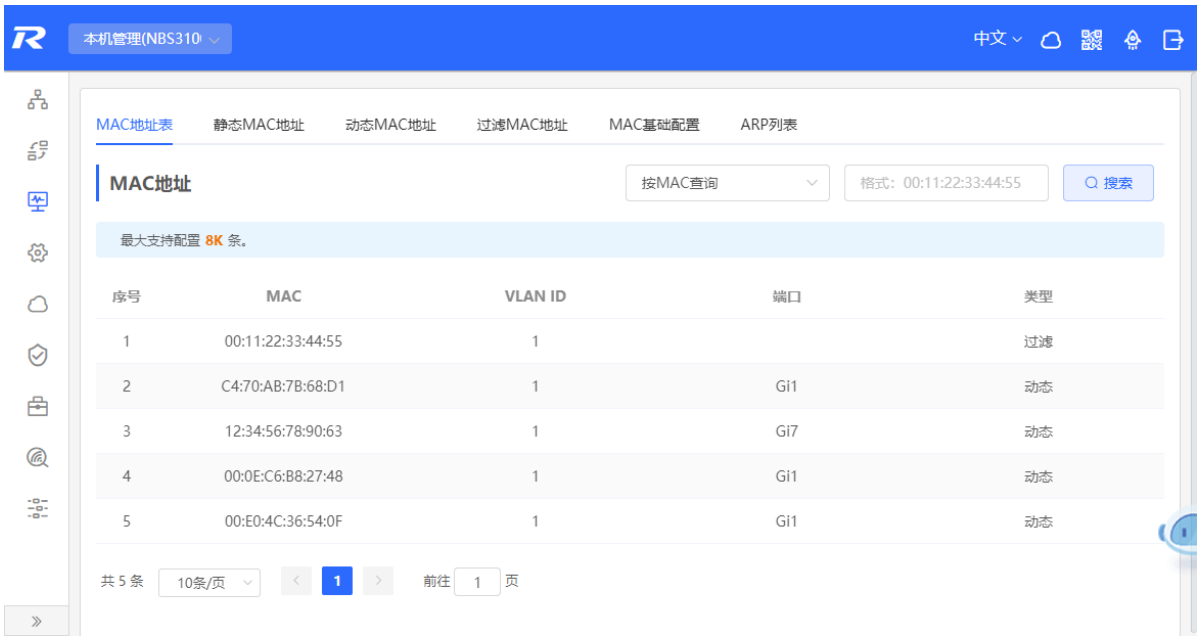
本章节只介绍动态、静态与过滤MAC地址表项的管理，不涉及组播MAC地址表项。

3.3.2 查看 MAC 地址表

【本机管理-页面向导】监控信息>>终端管理>>MAC地址表

显示设备的MAC地址信息，包含用户手动设置的静态MAC地址、过滤MAC地址以及设备自动学习到的动态MAC地址。

查询MAC地址表项：支持根据MAC地址、VLAN ID或端口查询MAC地址表项。选择搜索类型，输入搜索的字符串，点击<搜索>，列表将过滤出符合搜索条件的MAC表项。支持模糊搜索。



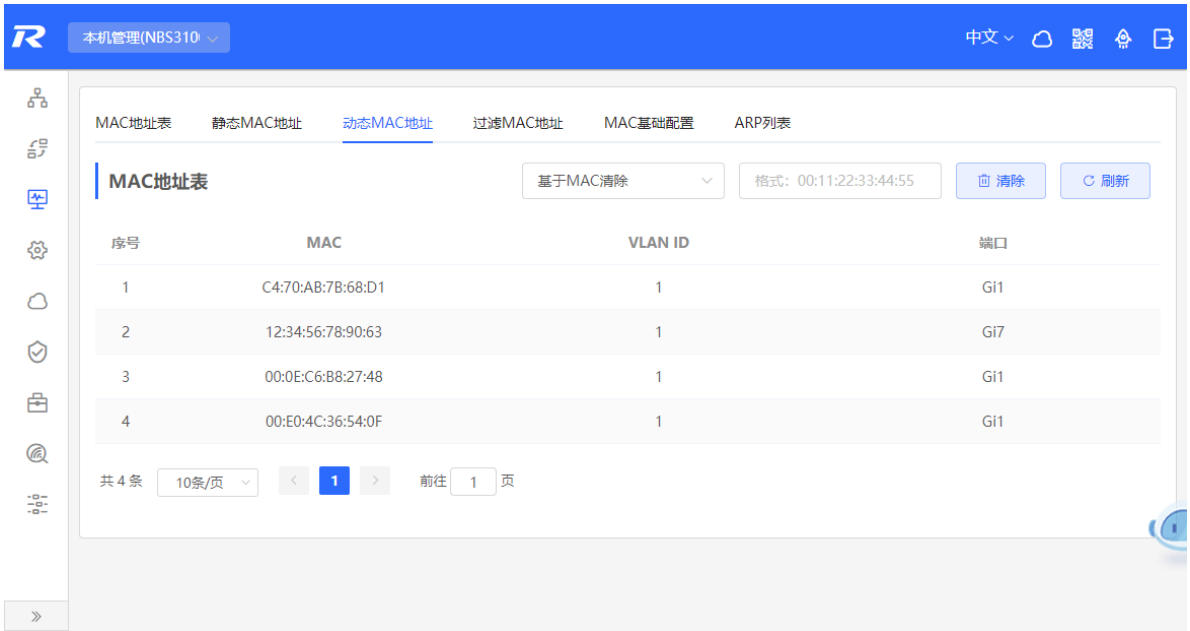
说明

MAC表容量在不同产品上存在差异，请以产品的实际情况为准。（例如示例图中设备MAC地址表容量为32K）。

3.3.3 查看动态 MAC 地址

【本机管理-页面向导】监控信息>>终端管理>>动态MAC地址

设备收到报文后会根据报文的源MAC自动生成动态MAC地址表项，当前页面显示设备学习到的动态MAC地址表项。点击<刷新>可重新获取最新的动态MAC地址表项。



清除动态MAC表项：选择清除类型（支持基于MAC、基于VLAN或基于端口清除），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。

3.3.4 设置静态 MAC 绑定

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地址表项，手工绑定设备下接的网络设备的MAC地址与端口。添加一个静态地址表项后，当在VLAN中接收到目的MAC地址为该地址的报文时，该报文将被转发到指定的端口中。例如，当端口开启了802.1x认证，可以通过设置静态MAC绑定实现免认证。

1. 添加静态 MAC 地址表项

【本机管理-页面向导】监控信息>>终端管理>>静态MAC地址

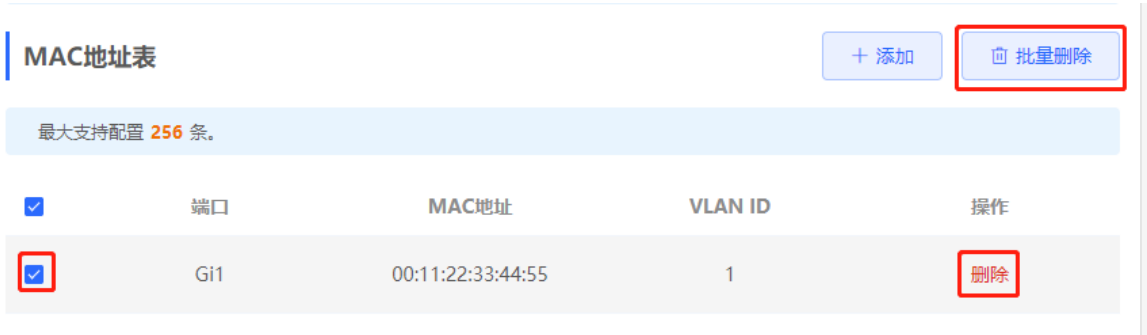
点击<添加>，输入MAC地址及所属VLAN ID，选择所要转发的出接口，点击<确定>。添加成功后MAC地址表将更新表项数据。

2. 删除静态 MAC 地址表项

【本机管理-页面向导】监控信息>>终端管理>>静态MAC地址

批量删除：在“MAC地址表”中勾选需要删除的MAC表项，点击<批量删除>，在提示信息框中点击<确定>。

删除单个表项：在“MAC地址表”找到需要删除的表项，点击最后一列操作栏下的<删除>，在提示信息框中点击<确定>。



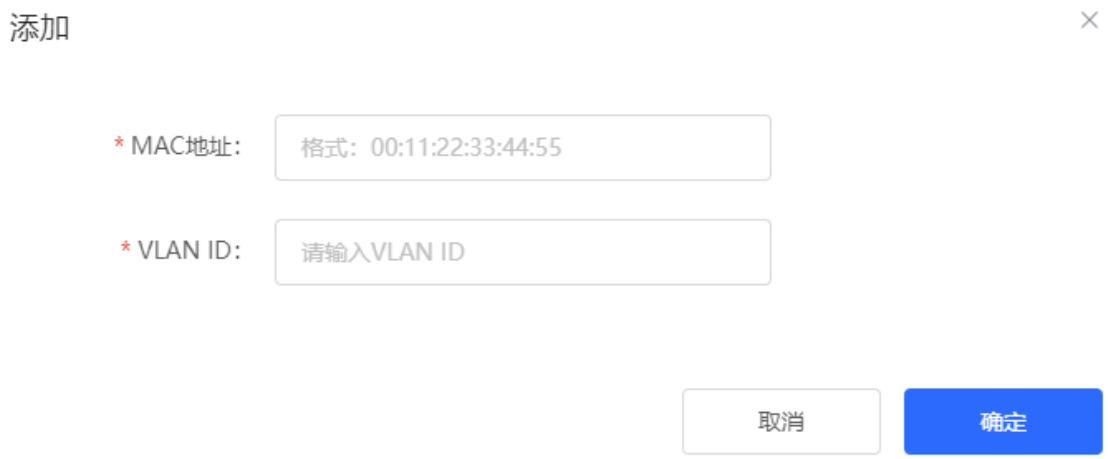
3.3.5 设置过滤 MAC 地址

在某些场景下，如果需要禁止部分用户发送或接收报文，可以将这部分用户的MAC地址配置为过滤MAC地址表项。配置本功能后，指定VLAN中收到源或目的MAC地址与过滤MAC地址表项匹配的报文后，将直接丢弃此报文。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。

1. 添加过滤 MAC 地址

【本机管理-页面向导】监控信息>>终端管理>>过滤MAC地址

点击<添加>，输入过滤的MAC地址及所属VLAN ID，点击<确定>。

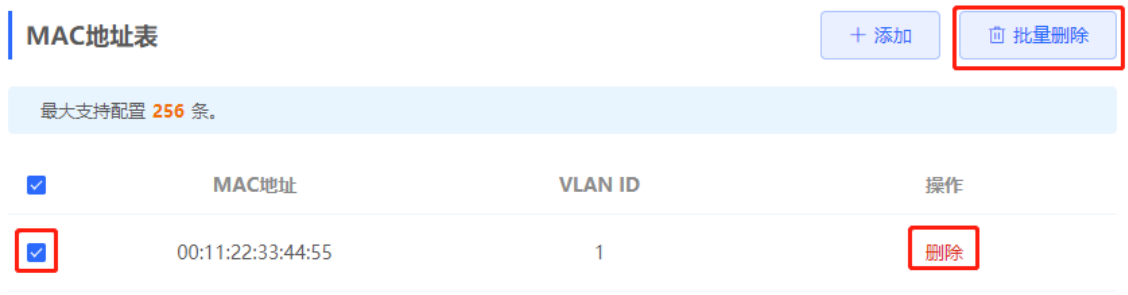


2. 删除过滤 MAC 地址

【本机管理-页面向导】监控信息>>终端管理>>过滤MAC地址

批量删除：在“MAC地址表”中勾选需要删除的MAC表项，点击<批量删除>，在提示信息框中点击<确定>。

删除单个表项：在“MAC地址表”找到需要删除的表项，点击最后一列操作栏下的<删除>，在提示信息框中点击<确定>。



3.3.6 设置 MAC 老化时间

用于设置设备学习到的动态MAC表项的老化时间，静态MAC地址表项与过滤MAC地址表项不会老化。

设备根据老化时间删除部分无用的动态MAC地址表项，以便节约设备上的表项资源。设备上配置的老化时间过长时，可能无法及时删除无用的表项；配置得过短时，可能删除部分有效表项，导致设备反复学习MAC地址，增加广播报文的发送。因此，请根据实际情况合理配置动态MAC地址表项的老化时间，保证在节省设备资源的同时不影响网络的稳定性。

【本机管理-页面向导】监控信息>>终端管理>> MAC基础配置

输入合法的老化时间，点击<保存>。老化时间的取值范围为10~630，单位为秒。0表示不老化。

3.4 查看 ARP 信息

【本机管理-页面向导】监控信息>>终端管理>>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。

设备学习连接在设备各端口上的网络设备的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。右上角搜索框支持根据IP或MAC地址来查找指定ARP表项。点击<刷新>，可重新获取最新的ARP表项。

说明

关于ARP表项的更多功能介绍，请参见6.4 设置ARP静态表项。

3.5 VLAN 划分

3.5.1 VLAN 简介

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端口实现三层通信。

VLAN划分包含创建VLAN和设置端口VLAN两部分功能。

3.5.2 创建 VLAN

【本机管理-页面向导】VLAN划分>>VLAN列表

VLAN列表包含当前已存在的所有VLAN信息，可对已有的VLAN进行修改或删除，或创建新的VLAN。

1. 添加 VLAN

批量创建VLAN：点击<批量添加>，在弹出框内输入VLAN ID范围（多个VLAN ID范围以英文逗号分割），点击<确定>，一次性创建多个VLAN。添加的VLAN将显示在“VLAN列表”中。

创建单个VLAN：点击<添加>，输入VLAN ID和VLAN的描述信息，点击<确定>。添加的VLAN将显示在“VLAN列表”中。

说明

- VLAN ID范围为1~4094。
- 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‘-’连接线分隔。
- 添加VLAN时，如果未设置描述信息，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。
- 若设备支持三层功能，VLAN将与路由口和L3AP（三层聚合）功能共享有限的硬件资源；若硬件资源不足，将提示“VLAN资源不足”。

2. 修改 VLAN 描述

点击“VLAN列表”最后一列操作栏下的<修改>，可修改指定VLAN的描述信息。

3. 删除 VLAN

批量删除VLAN：在“VLAN列表”中勾选需要删除的VLAN表项，再点击<批量删除>一次性删除多个VLAN。

删除单个VLAN：点击“VLAN列表”最后一列操作栏下的<删除>，删除指定VLAN。

说明

默认VLAN（VLAN 1）、管理VLAN、Native VLAN、SVI VLAN、MVR VLAN、Voice VLAN及Access VLAN不允许被删除，<删除>按钮为灰色的不可点击状态。

3.5.3 设置端口 VLAN

1. 功能简介

【本机管理-页面向导】VLAN划分>> 端口列表

端口列表显示了当前端口VLAN划分的情况。请先在VLAN列表中创建VLAN（参考3.5.2 创建VLAN），然后再进行基于VLAN的端口配置。

通过配置一个端口的端口模式和VLAN成员，可确定此端口允许通过的VLAN，以及此端口转发报文是否携带Tag。

表3-1 端口模式说明

端口模式	作用
Access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 Access VLAN同时具有Native VLAN和许可VLAN的属性 Access口发出的帧都不携带Tag，若Access口收到对端设备发送的Untagged帧，则判断该帧属于Access VLAN，并在内部强制加上Access VLAN ID
Trunk口	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，即该端口能够转发所有VLAN的帧。可以通过设置许可VLAN范围来限制允许转发的VLAN帧 注意，连接链路两端的Trunk口必须配置相同的Native VLAN
Hybrid口	一个Hybrid口可以有一个Native VLAN和若干个许可VLAN，许可VLAN分为Tag VLAN和Untag VLAN，Hybrid口转发Tag VLAN的帧携带Tag，转发Untag VLAN的帧不携带Tag，因为Hybrid口转发Native VLAN的帧不能携带Tag，所以Native VLAN只能属于Untag VLAN列表

说明

Hybrid模式的支持情况在不同产品版本上存在差异，请以产品的实际情况为准。

2. 配置步骤

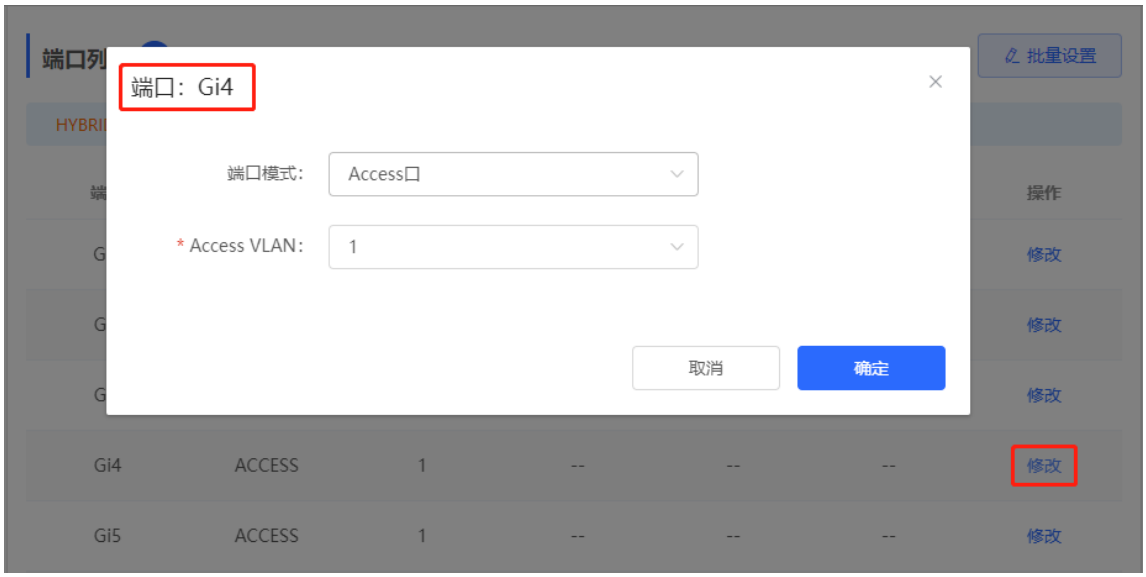
【本机管理-页面向导】VLAN划分>> 端口列表

批量设置端口VLAN：点击<批量设置>，在端口面板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，需要选择Access VLAN；若端口模式为Trunk口，需要选择Native VLAN并输入允许通过的VLAN ID范围；若端口模式为Hybrid口，需要选择Native VLAN并输入允许通过的VLAN范围和Untag VLAN范围。点击<确定>，完成批量设置。

说明

Hybrid模式下，允许通过的VLAN包含了Tag VLAN和Untag VLAN，Untag VLAN范围必须包含Native VLAN。

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



说明

- VLAN ID的取值范围为1~4094，其中VLAN 1是不可删除的默认VLAN。
- 当硬件资源不足的情况下，系统将提示创建VLAN失败。
- 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。

3.5.4 交换机批量设置

1. 功能简介

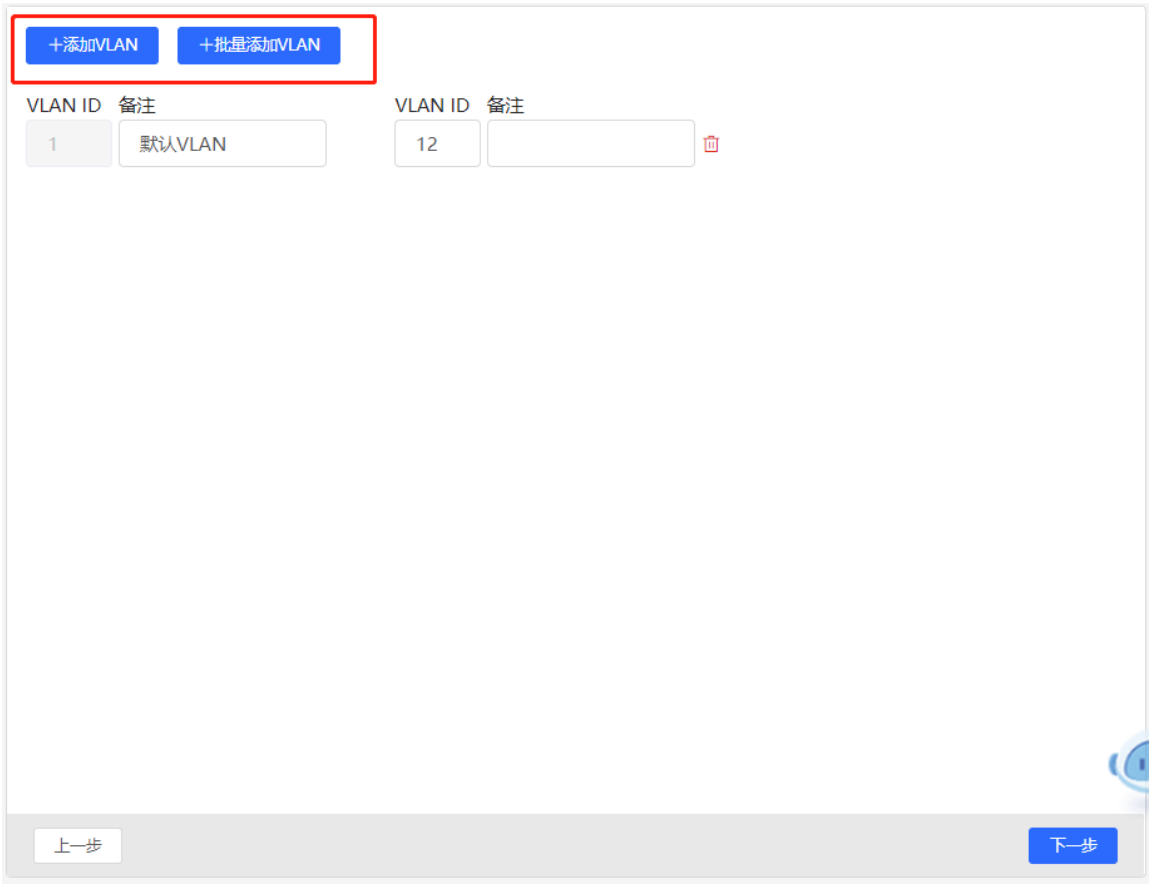
支持为组网中的交换机批量创建VLAN、设置端口属性以及划分端口VLAN。

2. 配置步骤

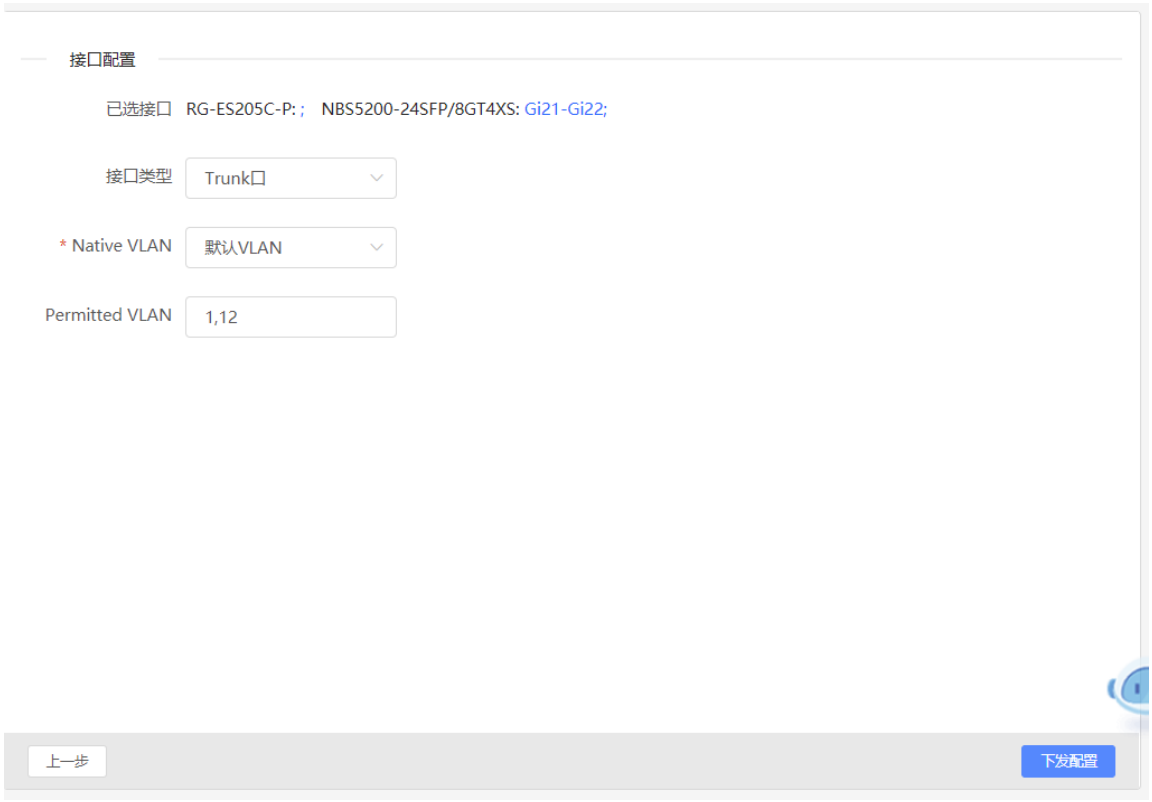
【整网管理-页面向导】整网管理>>交换机批量配置

(1) 页面将显示当前网络中所有的交换机，从中点击选择需要配置的设备，并在下方出现的设备端口视图中选择需要配置的端口。若当前网络中的设备较多，可在右上角下拉框中根据产品型号进行过滤。选择完毕后点击<下一步>。

(2) 点击<添加VLAN>即可为选中的设备批量创建VLAN。如需创建多个VLAN，点击<批量添加VLAN>并输入要创建的VLAN ID范围（如3-5,100）。完成VLAN设置后，点击<下一步>。

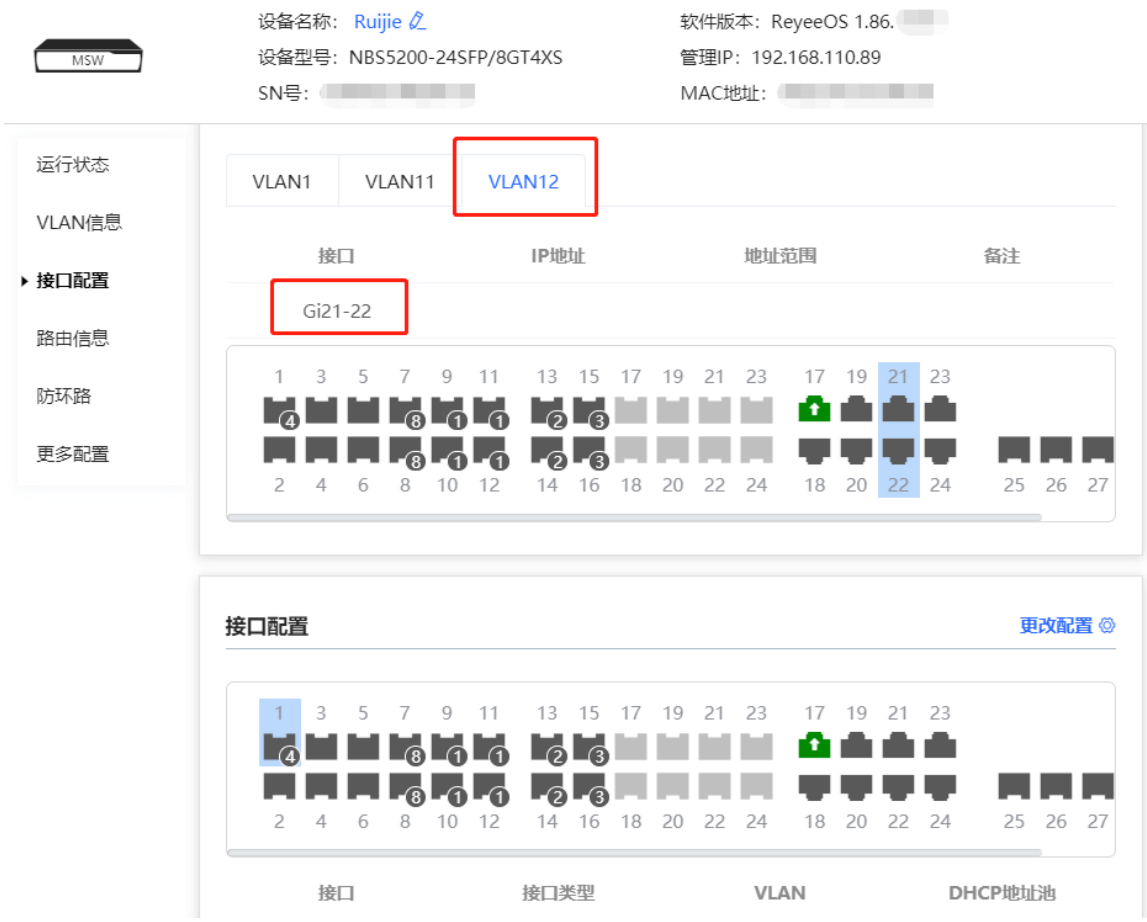


(3) 为第一步中选择的端口批量设置端口属性。选择端口类型，端口类型为“Access口”时需要设置端口的VLAN ID，端口类型为“Trunk口”时需要设置端口的Native VLAN和Permitted VLAN。完成端口属性设置后，点击<下发配置>，将批量配置下发至各设备。



3. 效果验证

查看交换机的VLAN和接口信息，能查看到批量下发的配置。


MSW
设备名称： Ruijie
设备型号：NBS5200-24SFP/8GT4XS
SN号：
软件版本：ReyeeOS 1.86.
管理IP：192.168.110.89
MAC地址：
运行状态
VLAN信息
接口配置
路由信息
防环路
更多配置
VLAN1
VLAN11
VLAN12
接口
IP地址
地址范围
备注
Gi21-22
1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 18 20 22 24 25 26 27
接口配置
更改配置
1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 18 20 22 24 25 26 27
接口
接口类型
VLAN
DHCP地址池

4 端口管理

4.1 功能简介

端口（也称接口）是网络设备能够实现数据交换功能的重要部件。端口管理功能支持对设备端口的基本属性进行设置，并支持设置端口聚合、端口镜像、端口限速和设备的管理IP等功能。

表4-1 端口类型说明

端口类型	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端口和与之相关的第二层协议。	本章介绍
二层聚合端口	聚合端口是指把多个物理成员端口捆绑在一起形成的逻辑链接。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，通过二层聚合端口的报文还将在二层聚合端口的成员端口上进行流量均衡，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口可以作为本机的管理接口，通过连接SVI口管理设备。也可以创建SVI口作为网关接口，相当于是对应VLAN的虚拟接口，可用于三层设备中跨VLAN之间的路由。	相关配置见6.1 设置三层端口
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。路由端口不具备二层交换功能，与VLAN无对应关系，只是作为访问接口。	相关配置见6.1 设置三层端口
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，通过三层聚合端口的报文同样能在三层聚合端口的成员端口上进行流量均衡，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。	相关配置见6.1 设置三层端口

4.2 端口设置

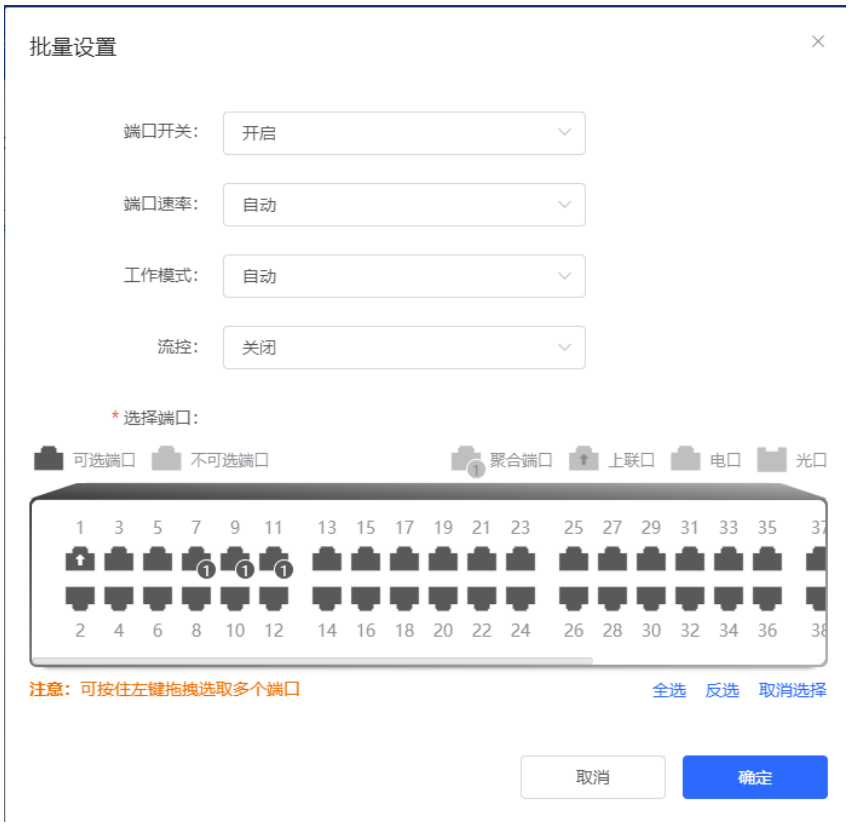
端口设置包含端口的基础配置与物理配置等通用属性。用户可以调整端口的速率，设置端口开关、双工模式、流控模式、节能管理开关、端口介质类型和MTU等。

4.2.1 基本配置

【本机管理-页面向导】端口管理>> 端口设置>>基本配置

支持设置是否启用端口、端口的速率和双工模式、流控模式，并显示当前各端口的实际状态。

批量设置：点击<批量设置>，在配置框中首先选中需要配置的端口，然后选择端口开关、速率、工作模式和流控模式，点击<确定>下发配置。批量配置时，配置的属性适用于所选范围内的所有端口，即只可配置所选端口共同支持的属性。



设置单端口：在端口列表中选择需要设置的端口表项，点击操作列中的<修改>，在配置框中选择端口启用状态、速率、工作模式和流控模式，点击<确定>。

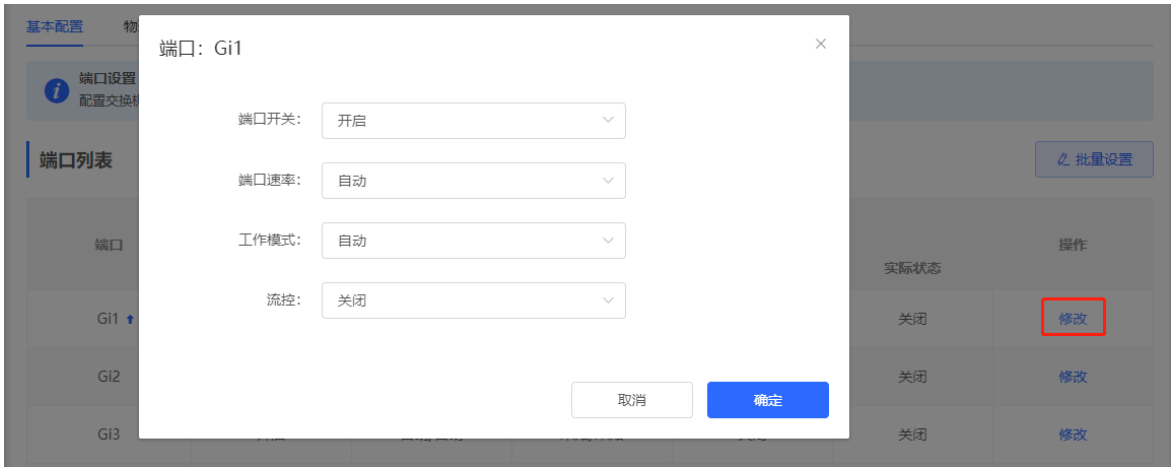


表4-2 端口基本配置参数说明

参数	说明	默认值
端口开关	如果关闭一个端口，则这个端口上将不会接收和发送任何帧，并丧失对应的数据处理功能，但端口的PoE供电功能不受影响	开启
端口速率	设置以太网物理接口工作的速率。设置为自动表示端口速率由本端和对端设备自协商决定。协商得到的速率可以是端口速率	自动

参数	说明	默认值
	能力范围内的任意一个速率	
工作模式	● 全双工：实现端口在发送数据包的同时可以接收数据包 ● 半双工：控制端口同一时刻只能发送数据包或接收数据包 ● 自动：端口的双工状态由本端口和对端端口自动协商而定	自动
流控	开启流控后，端口将会处理接收到的流控帧，并在端口出现拥塞时发送流控帧	关闭

说明

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。

4.2.2 物理配置

【本机管理-页面向导】端口管理>> 端口设置>>物理配置

支持开启端口的节能管理（EEE）功能，设置端口的介质类型和MTU。

批量设置：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、端口介质模式并输入端口描述，点击<确定>。

说明

批量配置时，不支持同时配置电口和光口。

设置单端口：点击端口表项操作列的<修改>，在配置信息框中选择EEE开关、端口模式，并输入端口描述，点击<确定>。

表4-3 端口物理配置参数说明

参数	说明	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。开启后EEE通过在以太网连接闲置时使端口进入LPI（Low Power Idle，低功耗节能）模式来达到节省能源的目的。 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	用户可以为端口添加描述，标注端口的作用	NA
MTU	MTU（Maximum Transmission Unit，最大传输单元）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。可以通过设置端口的MTU来控制该端口允许收发的最大帧长。	1500

说明

- 不同端口支持的属性及配置项有所不同。
- 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）。
- 光口不支持开启EEE。

4.3 聚合端口

4.3.1 聚合端口概述

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n根网线连接这两台设备，再将这些端口进行聚合绑定，这样这些端口就逻辑捆绑形成了1000M * n的最大流量。
- 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，而如果将多干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，那么在这些端口上承载的业务就不会断掉。

4.3.2 功能简介

1. 静态 AP

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模式下的聚合端口，称为静态聚合端口，对应的成员端口称为静态聚合端口的成员端口。静态AP实现简单，用户只要将指定的物理接口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。成员端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。

2. 动态聚合

动态聚合模式是针对RG-MR系列网关设备WAN口开发的特制化端口聚合功能。MR设备WAN口带宽最大能够支持2000M，但是内网端口与交换机连接后，单个端口最大只支持1000M的带宽。为了使下行带宽不被浪费，需要想办法增加MR设备与交换机之间的端口最大带宽，动态聚合功能应运而生。

将MR网关设备上固定的两个AG（聚合）成员口，与交换机上任意两个端口进行连接后，通过报文交互，能够将交换机上的两个端口自动聚合，从而实现带宽的倍增。交换机上通过这种方式自动生成的聚合端口，称为动态聚合口，对应的两个端口则为该聚合口的成员端口。

说明

动态聚合口不支持手工创建，由设备自动生成后可以被删除，但无法修改成员端口。

3. 流量均衡

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

4.3.3 设置聚合端口

【本机管理-页面向导】端口管理>> 聚合端口>>聚合口设置

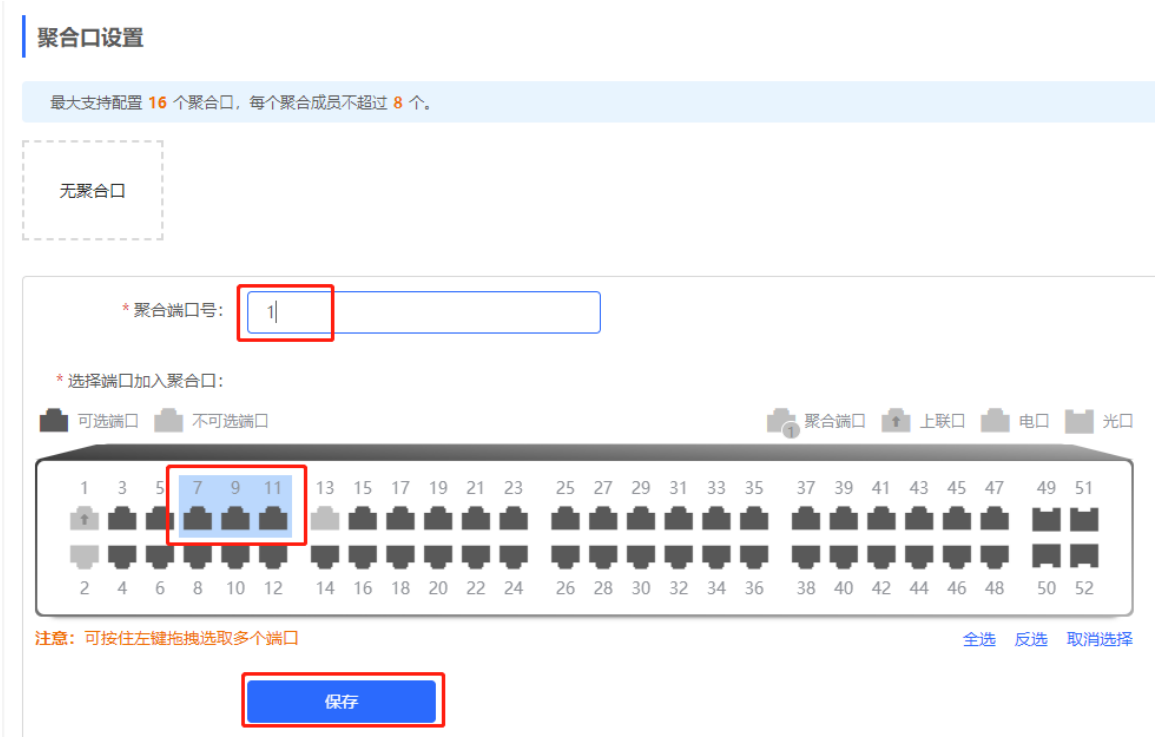
1. 添加静态聚合口

输入聚合端口号并选择成员端口（已经加入聚合口的端口不可选择），点击<保存>。添加成功后端口面板会显示添加的聚合口。

说明

- 单个聚合口的最大成员端口个数为8。

- 聚合端口属性必须一致，不能将电口和光口进行聚合。
- 动态聚合口不支持手动创建。

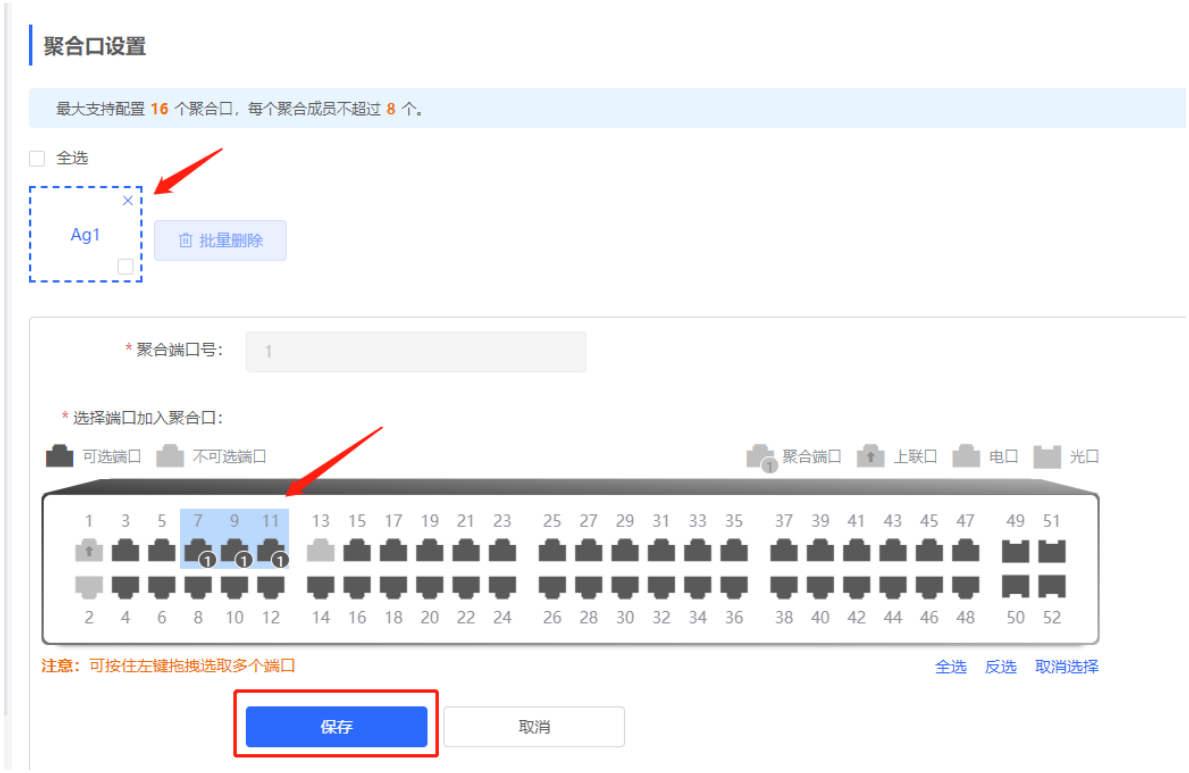


2. 修改静态聚合口的成员端口

点击已添加的静态聚合口，此时该聚合口的成员端口就会变成选中状态，点击端口可以取消选中；也可以继续选择其他端口加入当前聚合口。点击<保存>，即可以对聚合端口的成员端口进行修改。

说明

动态聚合口不支持修改成员口。



3. 删除聚合口

鼠标移至聚合口图标，点击右上角×图标，或勾选需要删除的聚合口，点击<批量删除>，即可删除指定聚合口。删除后面板中对应端口变为“可选端口”状态，可用于设置新的聚合口。

⚠ 注意

删除聚合口后，原聚合口中的成员口将会恢复至端口出厂属性，并且端口为关闭状态。

4.3.4 设置流量平衡模式

【本机管理-页面向导】端口管理>> 聚合端口>>全局配置

选择“流量平衡算法”，点击<保存>。设备会根据指定的流量平衡算法，对输入报文进行流量分配。同一报文流将固定通过同一条链路输出，不同报文流将平均分配到各个链路。

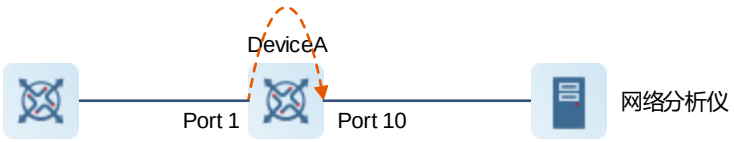
4.4 端口镜像

4.4.1 功能简介

镜像（SPAN）是将指定端口的报文复制到另一个连接有网络监测设备的端口的功能。设置端口镜像后，源端口上的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，从而实现对所有进入源端口和从源端口输出的报文的监控。

如图4-1所示，通过在DeviceA上配置了端口镜像，设备将Port 1上的报文复制一份到Port 10，连接在Port 10上的网络分析设备虽然未与Port1直接相连，但是可以接收通过Port1上的所有报文，从而实现了监控Port 1传输的数据流的目的。

图4-1 端口镜像工作原理图



镜像功能既实现了对可疑的网络节点或者设备端口进行数据流量分析，同时又不影响被监控设备的数据转发，主要应用于网络监控和故障排查场景中。

4.4.2 配置步骤

【本机管理-页面向导】端口管理>> 端口镜像

点击配置，选择镜像源端口、目的端口、监控报文类型以及是否接收非镜像源端口报文，点击<确定>。最多可配置4条镜像规则。

如需删除端口镜像配置，请点击对应操作列的<清空>。

注意

- 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。
- 镜像最多可以配置4条，已配置过的端口不可再次配置。


本机管理(NBS310
中文
端口镜像
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。
镜像列表
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


编辑
监控报文：
所有报文
是否接收非镜像源端口报文：
* 镜像源端口：
可选端口 不可选端口 聚合端口 上联口 电口 光口
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36
注意：可按住左键拖拽选取多个端口
全选 反选 取消选择
* 镜像目的端口：
可选端口 不可选端口 上联口 电口 光口
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36
取消选择
取消
确定

表4-4 端口镜像参数说明

参数	说明	默认值
镜像源端口	源端口也称为被监控口，源端口上的数据流会被复制一份到目的端口，用于网络分析或故障排除 支持选择多个源端口，将多个端口镜像到一个目的端口	NA
镜像目的端口	目的端口也称为监控口，即与监控设备相连接的端口，将接收到的源端口报文转发到监控设备	NA
监控报文	镜像源端口要监控的报文类型（数据流方向） ● 所有报文：经过端口的所有报文，包括输入和输出报文 ● 输入报文：源端口上接收到的所有报文都将被复制一份到目的端口 ● 输出报文：从源端口发送的报文都将被复制一份到目的端口	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：监控源端口报文的同时，对其他非镜像源端口的报文正常转发 ● 关闭：仅监控源端口报文	开启

4.5 端口限速

【本机管理-页面向导】端口管理>> 端口限速

配置端口的流量限制规则，包含端口出口方向和入口方向的速率限制。

1. 设置端口限速

点击<批量设置>，在弹出框中选择端口，并填写限制速率值，点击<确定>。入口速率和出口速率必至少填写一个。完成配置后会显示在端口限速规则列表中。

表4-5 端口限速参数说明

参数	说明	默认值
入口速率	报文从端口进入交换设备的最大速率值，单位为kbps	不限速
出口速率	报文从端口离开交换设备的最大速率值，单位为kbps	不限速

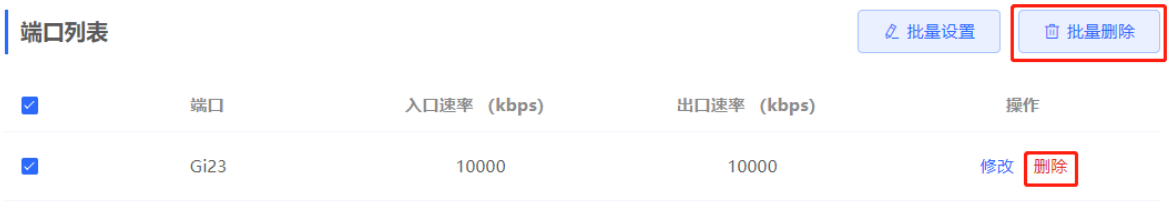
2. 修改单个端口的限速

在已经设置限速的端口列表中，点击对应端口表项的<修改>，在弹出框中填写入口速率和出口速率，点击<确定>。

3. 取消端口限速

批量设置：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>。

设置单端口：在“端口列表”中点击对应端口表项的<删除>，在确认框中点击<确定>。



说明

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

4.6 设置管理 IP

【本机管理-页面向导】端口管理>> 管理IP

配置设备的管理IP地址。用户可通过访问管理IP来配置和管理设备。

设备联网类型支持如下两种：

- 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：使用用户手工配置的固定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，需要手动输入管理VLAN、IP地址、子网掩码、默认网关IP及DNS服务器地址。点击<保存>生效。

说明

- 管理VLAN为空及不填时默认生效VLAN 1。
- 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3.5.2 创建VLAN）。
- 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。

4.7 设置机箱管理 IP

注意

仅RG-NBS6002系列、RG-NBS7003系列和RG-NBS7006系列设备支持本功能。

【本机管理-页面向导】端口管理>> 机箱管理IP

设置机箱的MGMT管理口IP，用于对设备多个槽位的模块进行集中管理。

说明

MGMT口默认未设置IP，目前仅支持静态配置IP，不支持动态方式获取。

4.8 PoE 配置

注意

仅PoE交换机（设备型号带有“-P”标识）支持本功能。

【本机管理-页面向导】端口管理>> PoE

设备支持通过端口为PoE受电设备供电。用户可以查看当前供电状态，并分别设置系统供电与端口供电的策略，实现灵活的功率分配。

4.8.1 PoE 全局设置

【本机管理-页面向导】端口管理>> PoE>>PoE全局设置

PoE供电模式是指设备为连接的PD（Powered Device，受电设备）分配功率的方式，支持自动模式（Auto mode）和节能模式（Energy-saving mode）。

自动模式下，系统根据检测出的端口PD的分级类型来分配功率。设备对Class 0~4级的PD设备按照固定值来分配功率：Class 0为15.4W，Class 1为4W，Class 2为7W，Class 3为15.4W，Class 4 Type 1为15.4W，Class 4 Type 2为30W。在该模式下，若端口连接一台分级为Class 3的设备，即使实际消耗的功率只有11W，PoE供电设备也会按照15.4W的功率为端口分配功率。

节能模式下，设备按照PD设备实际的消耗来动态的调整功率分配。该模式下，为了防止功率满载时由于PD实际消耗功率波动导致端口供电震荡，可设置保留功率，保留功率将不用于供电，以保证当前系统消耗的总功率不会超过PoE设备的极限。保留功率的大小通过占PoE总功率的百分比来表示，取值范围为0~50，单位为百分比。

4.8.2 端口供电设置

【本机管理-页面向导】端口管理>> PoE>>端口列表

点击端口表项的“修改”或点击<批量设置>，可对端口的PoE供电功能进行设置。

表4-6 端口供电设置参数说明

参数	说明	默认值
PoE功能	是否开启端口的供电功能	开启
非标模式	默认情况下，设备只为符合标准IEEE 802.3af和802.3at协议的PD供电。实际应用中可能存在不符合标准的PD，开启非标模式后，设备端口能够为部分非标准的PD设备供电。	关闭
优先级	端口的供电优先级，分为高、中、低三个等级 在自动模式和节能模式下，高优先级的端口优先得到供电。PoE设备整机功率不足时，低优先级的端口先掉电。 对于优先级等级相同的端口，优先级按照端口号顺序排列，端口号小的优先级高	低
限制功率	端口可输出的最大功率，取值范围为0~30，单位为瓦特（W）。为空表示不限制	不限制

4.8.3 查看全局 PoE 信息

【本机管理-页面向导】端口管理>> PoE>>PoE全局信息

显示PoE功能的全局供电信息，包括系统总功率、使用功率、保留功率、剩余可用功率、峰值最大功率以及当前供电的端口数量。

4.8.4 查看端口 PoE 信息

【本机管理-页面向导】端口管理>> PoE>>端口列表

端口列表显示各端口的PoE配置与状态信息，点击 › 可展开详细信息。

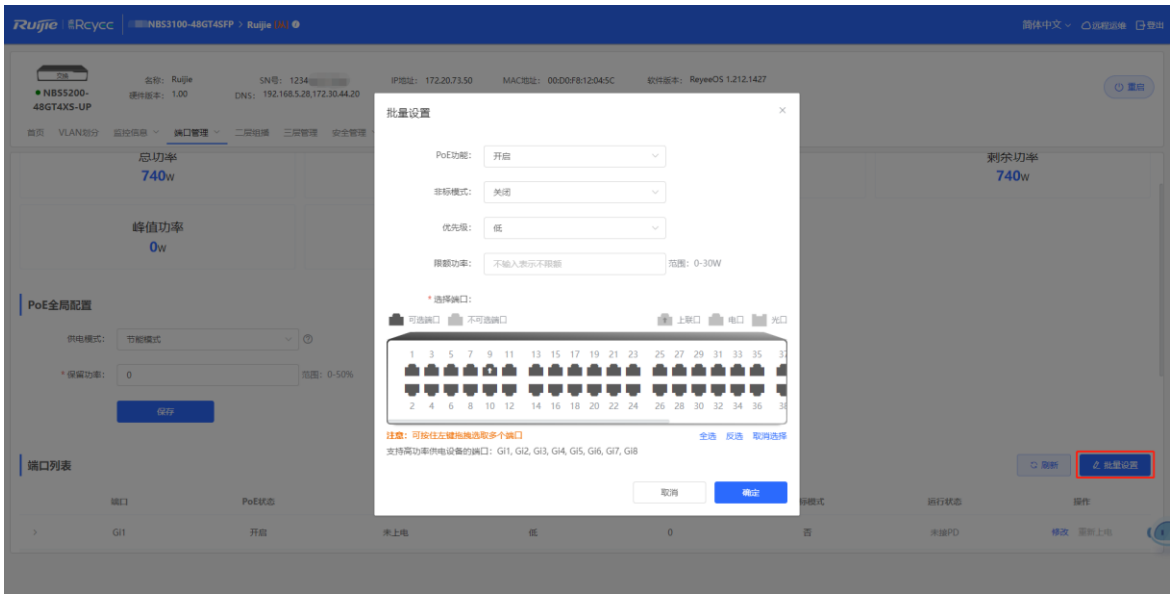
当端口所连PD设备需要重启，例如端口连接的AP出现异常时，可点击<重新上电>使端口短暂断电后重新上电，重启供电端口所连接的设备。

表4-7 端口供电信息说明

字段	说明
端口	设备端口编号
PoE状态	是否开启端口的PoE功能
是否上电	端口当前是否为PD供电
优先级	端口的供电优先级，分为高、中、低3个等级
当前功率	当前端口输出的功率，单位为瓦特（W）
非标模式	是否开启非标兼容模式
运行状态	PoE端口当前的工作状态
电流	端口的当前电流，单位为毫安（mA）
电压	端口的当前电流，单位为伏特（V）
平均功率	端口当前的平均功率，端口上电后端口消耗功率的采样平均值，单位为瓦特（W）
限额功率	端口的最大输出功率，单位为瓦特（W）
PD LLDP请求功率	PD向PSE（Power Sourcing Equipment，供电设备）请求的功率，单位为瓦特（W）
PSE LLDP分配功率	PSE分配给PD的功率，单位为瓦特（W）
PD type	通过LLDP分级获取的PD类型信息，分为Type 1和Type 2
PD等级	端口连接的PD的分级等级，按照IEEE 802.3af/802.3at标准分为Class 0~4

4.8.5 批量配置 PoE

点击批量配置，可以同时配置多个端口的PoE功能。可按住左键拖拽选取多个端口。




批量设置
PoE功能:
开启
非标模式:
关闭
优先级:
低
限额功率:
不输入表示不限额
范围：0-30W
* 选择端口:
可选端口
不可选端口
上联口
电口
光口
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36
注意：可按住左键拖拽选取多个端口
全选 反选 取消选择
支持高功率供电设备的端口：Gi1, Gi2, Gi3, Gi4, Gi5, Gi6, Gi7, Gi8
取消
确定

5 二层组播

5.1 组播概述

IP传输的三种方式包括单播、组播和广播。在IP组播中，IP报文从一个源发出，被转发到一组特定的接收者。与传统的单播和广播相比，IP组播可以节约带宽、减少网络负载，被广泛应用于网络电视、远程教育、在线直播和多媒体会议等实时性要求较高的网络业务中。

5.2 组播全局设置

【本机管理-页面向导】二层组播>> 全局配置

全局配置用于指定IGMP的协议版本、是否开启report报文抑制和设置对未知名组播报文的处理行为。

表5-1 组播全局配置参数说明

参数	说明	默认值
版本	IGMP（Internet Group Management Protocol，因特网组管理协议）是一个管理IPv4组播组成员的TCP/IP协议，运行在组播网络末梢的组播设备与用户主机上，用于用户主机和其直连的组播设备之间建立并维护组播组成员关系。目前IGMP演进出三个版本：IGMPv1、IGMPv2和IGMPv3。 该参数用于设置二层组播能处理的IGMP报文的最高版本，支持设置为IGMPv2或IGMPv3。	IGMPv2

参数	说明	默认值
report报文抑制	开启后，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，以减少网络中的报文数量，节约网络带宽并保障IGMP组播设备的性能。	关闭
未知名组播报文行为	全局和VLAN的组播功能都开启的情况下，接收到未知名组播报文的处理方式，可设置为丢弃或泛洪。	丢弃

5.3 IGMP Snooping

5.3.1 功能简介

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。

通常情况下，尤其是在一些局域网环境里面，组播报文需要经过二层交换设备。当二层交换设备没有运行IGMP Snooping时，IP组播报文在VLAN内被广播；当二层交换设备运行了IGMP Snooping后，二层设备可以侦听用户主机和上游PIM组播设备的IGMP协议报文，从而建立二层组播表项，控制IP组播报文只发给组成员接收者，防止组播数据在二层网络中的广播。

5.3.2 开启全局 IGMP Snooping

【本机管理-页面向导】二层组播>> IGMP Snooping

点击IGMP Snooping开关按钮，再点击<保存>。

5.3.3 设置协议报文处理参数

通过控制协议报文的处理，二层组播设备可以建立静态组播表项，也可以建立动态组播表项。其中通过调整各项参数还可以实现动态组播表项及IGMP Snooping成员关系快速刷新。

【本机管理-页面向导】二层组播>> IGMP Snooping

IGMP Snooping功能是基于VLAN进行的，因此每个VLAN都对应一个IGMP Snooping设置表项，设备有多少个VLAN，IGMP Snooping就有多少条表项。

点击VLAN表项的<修改>，在配置框中设置VLAN组播开关、动态学习功能开关、快速离开功能开关和静态路由连接口，并输入连接口老化时间、成员口老化时间等，点击<确定>。

表5-2 IGMP Snooping VLAN 配置参数说明

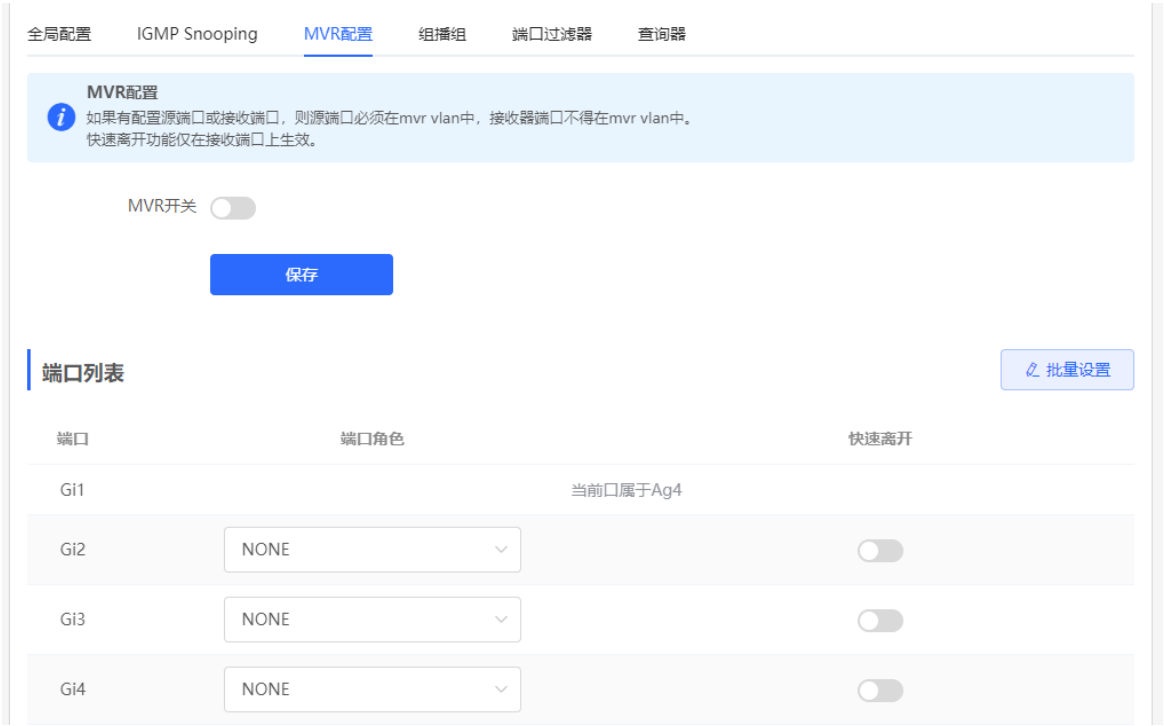
参数	说明	默认值
组播开关	VLAN的组播功能开关。只有全局IGMP Snooping功能和VLAN组播开关同时开启，VLAN的组播功能才能生效。	关闭
动态学习	运行IGMP Snooping的设备将VLAN内的端口标识为路由连接口或成员口，其中路由连接口为二层组播设备上连接三层组播设备的端口，成员口为二层组播设备上连接组成员主机的端口。 本参数表示路由器连接口的动态学习功能开关，开启后通过监听IGMP报文，二层组播设备可以自动发现并维护动态路由连接口。	开启
路由连接口	组播路由器连接口列表包含动态学习到的路由连接口（若开启动态学习功能）和静态配置的路由连接口。	NA

参数	说明	默认值
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；此后，当设备收到对应的特定组查询报文和组播数据报文时，设备不再向该端口转发。 该功能适用于设备一个端口下只连接一台主机的情况，一般在与终端直连的接入交换机上开启。	关闭
连接口老化时间	动态学习到的组播路由器连接口的老化时间，取值范围为30~3600，单位为秒	300秒
成员口老化时间	动态学习到的组播组成员口的老化时间，取值范围为30~65535，单位为秒	260秒
选择端口	在配置框中选取设置为静态路由连接口的端口。当端口配置为静态路由连接口，该端口不会老化	NA

5.4 MVR 配置

5.4.1 功能简介

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用户所属VLAN并转发出去。



5.4.2 设置全局 MVR 参数

【本机管理-页面向导】二层组播>> MVR配置

点击开启MVR开关后，选择MVR VLAN，并设置VLAN所支持的组播组，点击<保存>。可通过输入起始组播IP地址和结束组播IP地址来指定多个组播组。

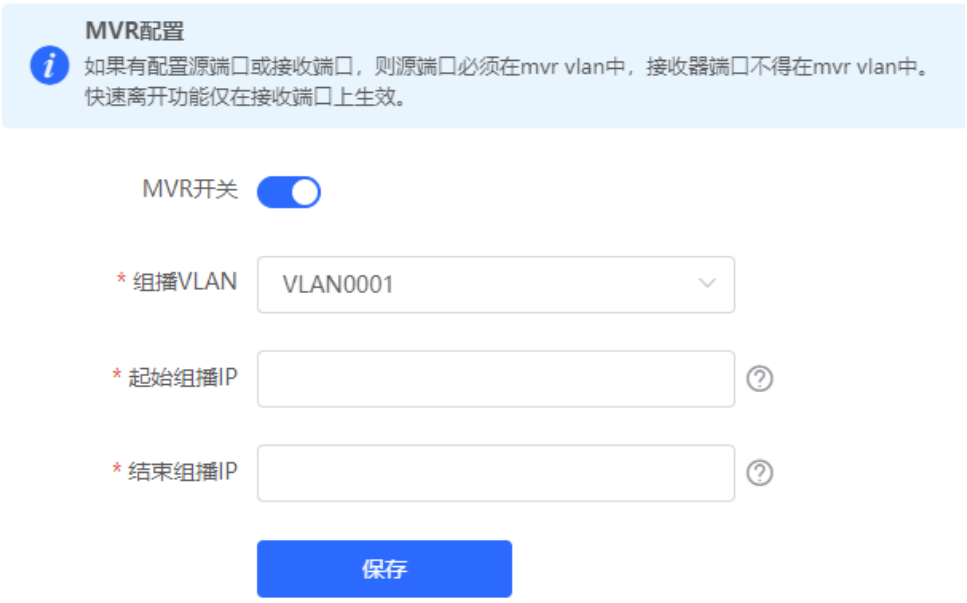


表5-3 全局 MVR 配置参数说明

参数	说明	默认值
MVR开关	全局MVR开关	关闭
组播VLAN	组播源所在的VLAN	1
起始组播IP	能够学习或者配置为MVR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MVR组播组的最大组播IP地址	NA

5.4.3 设置 MVR 端口

【本机管理-页面向导】二层组播>> MVR配置

批量设置：点击<批量设置>，选择端口角色、需要设置的端口以及是否在端口上开启快速离开功能，点击<确定>。

设置单端口：点击下拉框选择端口的MVR角色类型。点击“快速离开”列的开关可以设置端口是否开启快速离开功能。

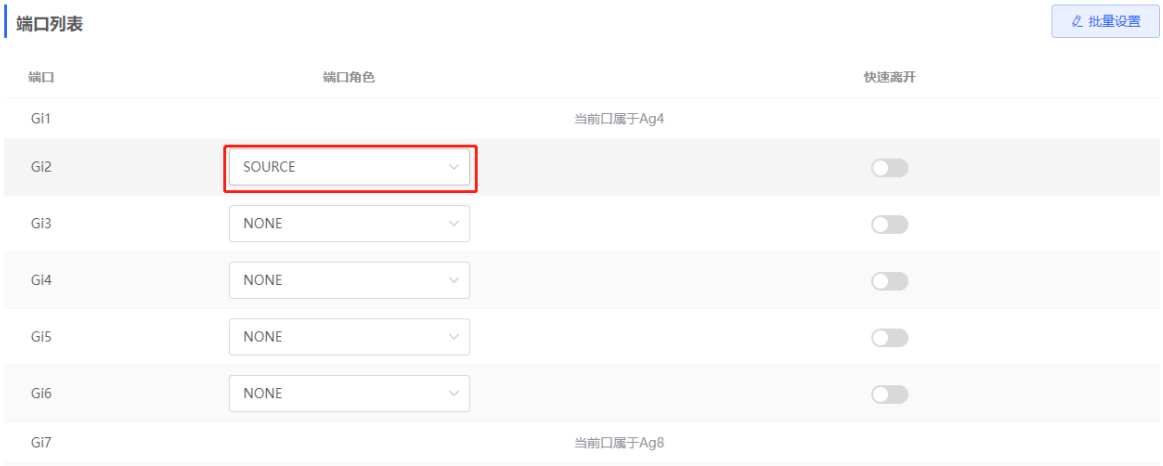


表5-4 端口 MVR 配置参数说明

参数	说明	默认值
端口角色	NONE：不开启MVR功能 SOURCE：源端口，接收组播数据流的端口 RECIEVER：接收器端口，与终端相连的端口	NONE
快速离开	设置端口的快速离开功能，开启后当设备端口收到离开报文，直接从对应组播组的成员口中删除该端口	关闭

说明

- 如果配置了源端口或接收端口，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。

5.5 设置组播组

【本机管理-页面向导】二层组播>> 组播组

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

可以在当前页面查看组播组列表。右上角搜索框支持根据VLAN ID或组播地址搜索组播组表项。

点击<添加>可创建组播组。

表5-5 组播组配置参数说明

参数	说明	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，分为静态配置和动态学习两种方式 正常情况下，端口下需要接收到某个组播组的IGMP加入报文后，才会把该端口加入到该组播组，即动态学习方式； 通过手动配置端口加入组，无需进行IGMP报文交互，即可直接将该端口静态加入该组播组，并与PIM路由器交换组播组信息	NA
转发端口	组播流量转发出去的端口列表	NA

说明

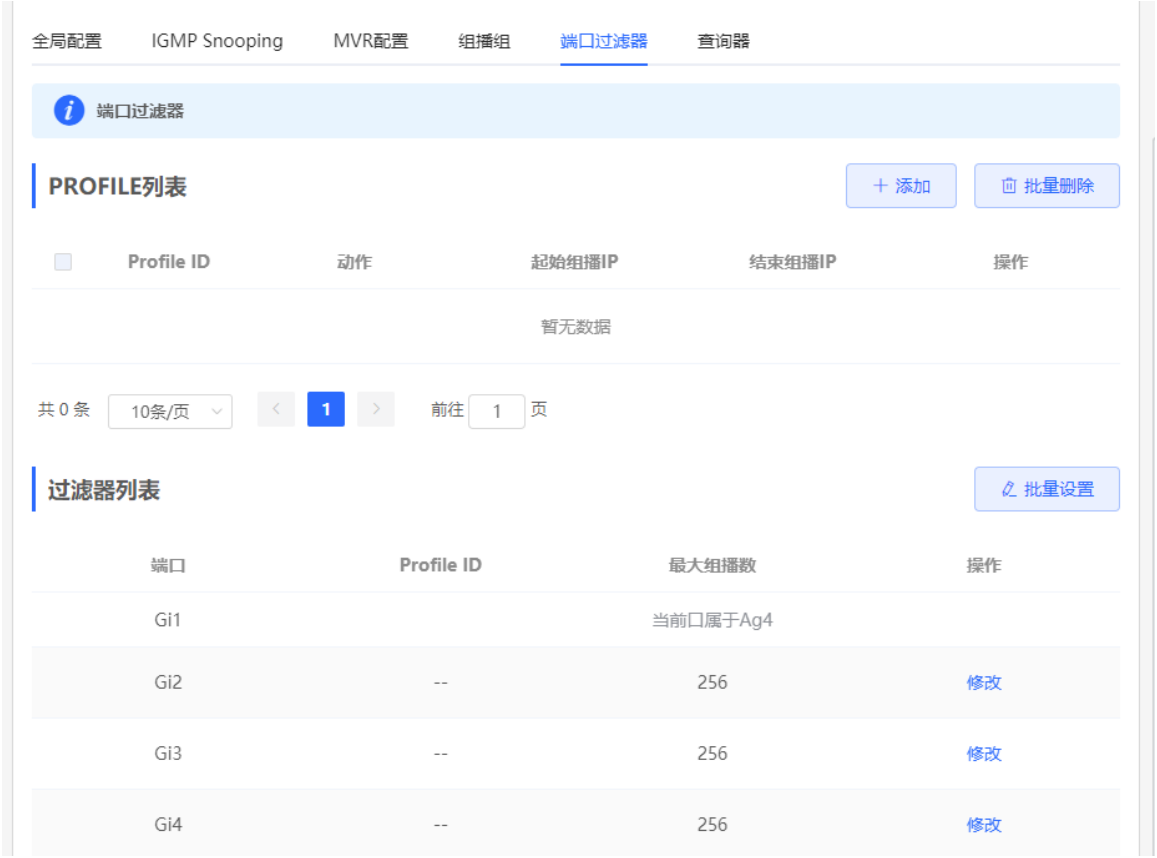
静态组播组不能学习其它动态转发端口。

5.6 设置端口过滤器

【本机管理-页面向导】二层组播>> 端口过滤器

一般情况下设备运行端口可以加入任意组。端口过滤器用于控制用户点播的组地址范围，可以为用户定制组播服务范围，保障运营商利益，防范非法组播流。

设置端口过滤器分为2个步骤：设置Profile和设置端口组地址范围限制。



5.6.1 设置 Profile

【本机管理-页面向导】二层组播>> 端口过滤器>> Profile列表

点击<添加>，创建Profile。Profile用于定义允许或禁止用户点播的组地址范围，供其他功能模块引用。

表5-6 Profile 配置参数说明

参数	说明	默认值
Profile ID	Profile标识	NA
动作	Deny：禁止点播指定范围内的组播IP Permit：只允许点播指定范围内的组播IP	NA
起始组播IP	组地址范围的起始组播IP地址	NA
结束组播IP	组地址范围的结束组播IP地址	NA

5.6.2 设置组地址范围限制

【本机管理-页面向导】二层组播>> 端口过滤器>> 过滤器列表

端口过滤器通过引用Profile来定义端口下允许/禁止用户点播的组地址范围。

点击<批量设置>，或点击单个端口表项的<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，点击<确定>。

表5-7 端口过滤器配置参数说明

参数	说明	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	允许转发端口包含该端口的组播组的最大数目。 如果用户同时点播的组播流过多，会对设备性能产生很大的压力，因此可通过限制端口下允许点播的组的最大个数来保障带宽	256

5.7 设置 IGMP 查询器

5.7.1 功能简介

在三层组播网络中，由三层组播设备充当查询器，运行IGMP协议维护组成员关系。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。但是在一个组播源和用户主机在同一个二层网络的场景中，由于二层设备不支持IGMP，因此无法实现查询器功能。为解决此问题，在二层设备上配置IGMP查询器功能，代替三层组播设备向用户主机发送IGMP Query报文，并对用户应答的IGMP Report报文进行侦听维护，建立二层组播的转发表项。

5.7.2 配置步骤

【本机管理-页面向导】二层组播>> 查询器

每个VLAN下都可设置一个查询器，查询器个数与设备VLAN数相同。

在查询器表项最后一列，点击<修改>，在配置框中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5-8 查询器配置参数说明

参数	说明	默认值
查询器开关	VLAN的查询器功能开关	关闭
查询器版本	查询器发送的查询报文的IGMP协议版本，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，取值范围为30~18000，单位为秒	60秒

说明

- 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。
- 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。

6 三层管理

> 注意
>
> 本章节仅适用于支持三层功能的NBS系列交换机。对于不支持三层功能的产品，如RG-NBS3100系列和RG-NBS3200系列交换机，则不支持本章节相关功能。

6.1 设置三层端口

【本机管理-页面向导】三层管理>> 三层口

端口列表下显示设备的各种类型的三层端口，包括SVI口、路由口以及三层聚合口。

点击<添加三层口>，可设置新的三层端口。

表6-1 三层口配置参数说明

参数	说明
端口类型	创建的三层口类型，包括SVI口、路由口和三层AP口。相关介绍见表4-1
联网方式	指定端口通过动态DHCP获取或静态配置方式获取端口IP
VLAN	SVI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。无法为端口下联终端分配IP地址； 本机分配：本设备作为DHCP服务器，为端口下联设备分配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；详见6.2 设置DHCP服务器 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地址分配给端口下联设备。需要设置端口IP地址和DHCP服务器的IP地址，其中端口IP地址应与DHCP服务器地址池处于同一网段
排除地址	当本设备作为DHCP服务器时，设置地址池中不用于分配的IP地址

说明

- VLAN1为设备的默认SVI口，不可更改、不可删除。
- 管理VLAN在三层口列表中显示但不能直接修改，如需修改请在[端口管理]>> [管理IP]页面中配置，详见4.6 设置管理IP。
- 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。
- 三层聚合的成员口必须为路由口类型。

6.2 设置 DHCP 服务器

三层口开启DHCP服务器功能后，能够为端口下联设备分配IP地址。

6.2.1 开启 DHCP 服务

【本机管理-页面向导】三层管理>> 三层口

点击指定端口的<修改>，或点击<添加三层口>添加一个三层口，选择DHCP模式为本机分配，并输入地址池的开始IP、分配IP数、排除IP地址范围以及地址租期。

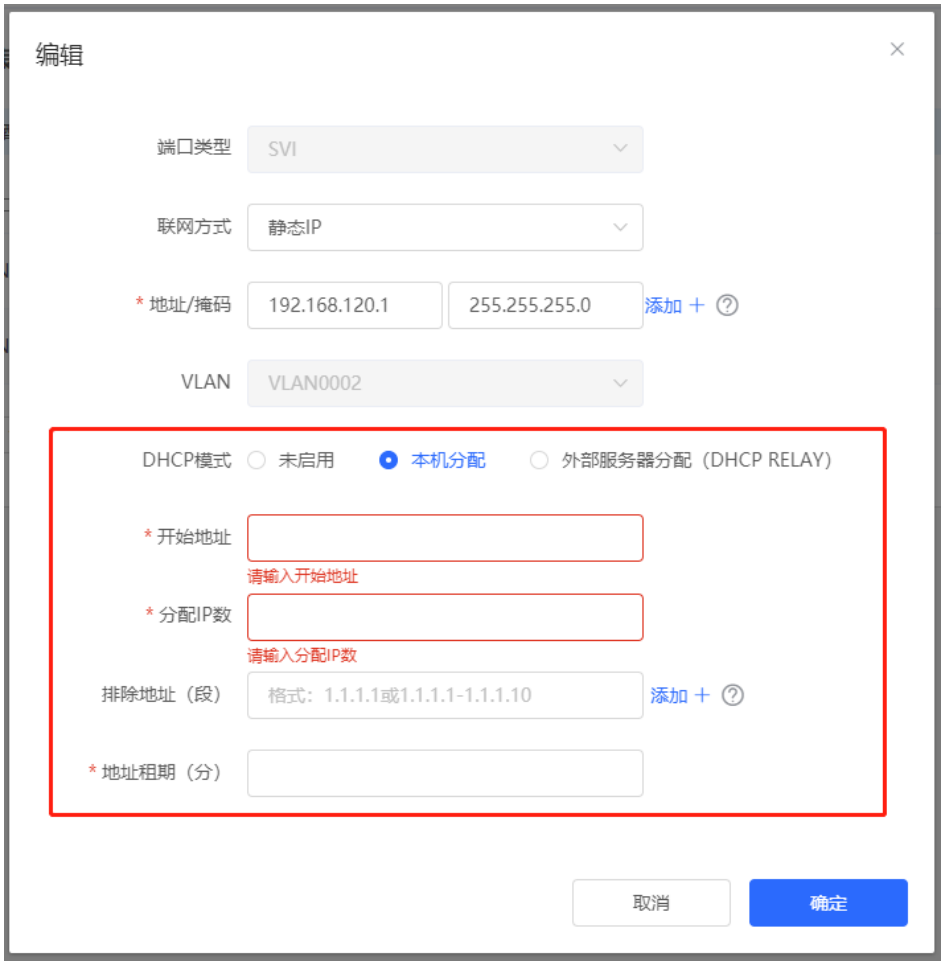


表6-2 DHCP 服务器配置参数说明

参数	说明
DHCP模式	选择本机分配
开始地址	DHCP服务器自动分配的IP的开始地址，即DHCP地址池的起始地址。客户端从地址池中获取IP地址，若地址池被用完，客户端将获取不到IP地址。

参数	说明
分配IP数	地址池中的IP地址数量
排除地址（段）	地址池中不用于分配的IP地址，支持输入单个IP地址或IP网段，最多可添加20个地址段
地址租期（分）	地址租约时间，单位为分钟。下联设备在连接状态时一般会自动续租保持IP地址不变；若因设备断开连接或网络不稳定等情况，没有续租，过了租期时间，将收回IP地址。此时下联设备恢复连接后需将重新请求地址

6.2.2 查看 DHCP 客户端

【本机管理-页面向导】三层管理>> 客户端列表

查看三层口启用DHCP服务后，为下联设备动态分配的地址信息。支持按MAC地址、按IP地址或按照主机名查找对应客户端信息。

点击状态栏中的<添加到静态地址>，或者勾选列表选择框后点击<批量转换>，将动态地址分配关系添加到静态地址分配列表中，使对应主机每次连接都将获取绑定的IP地址。静态地址分配列表的查看请参考6.2.3 配置静态地址分配。

6.2.3 配置静态地址分配

【本机管理-页面向导】三层管理>> 静态地址分配

显示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地址表项。右上角搜索框支持根据分配的IP地址或设备MAC地址查找对应表项。

点击<添加>，在弹出的静态IP地址绑定对话框中，填写要绑定的设备MAC地址和IP地址，点击<确定>。绑定静态IP后，对应下联设备每次连接都将获取绑定的IP地址。

如需删除静态地址，可在“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>；或点击对应表项最后一列操作栏下的<删除>。

6.2.4 设置 DHCP 服务器选项

【本机管理-页面向导】三层管理>> DHCP选项

设置设备三层口作为DHCP服务器时对下联设备下发的配置，均为可选配置，全局生效。

表6-3 DHCP 服务器选项配置参数说明

参数	说明
DNS服务器	运营商提供的DNS服务器地址。可输入多个地址，以空格分隔
Option 43	当AC（无线控制器）与AP不在同一局域网，AP通过DHCP服务器获取IP地址后，无法通过广播方式发现AC，因此需要在DHCP服务器上配置DHCP响应报文中携带的Option 43信息，通告AP使AP能够发现AC
Option 138	填入AC的IP地址。与Option 43类似，当AC与AP不在同一局域网时，可通过设置Option 138选项使AP获取AC的IPv4地址
Option 150	设置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。可输入多个地址，以空格分隔

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，一般无需配置。未指定DNS服务器地址时，下联口默认分配到的DNS为网关IP。

6.3 设置静态路由

【本机管理-页面向导】三层管理>> 静态路由

静态路由由用户手工配置。当数据报文与静态路由匹配成功时，将按照指定的转发方式进行转发。

注意

静态路由不能自动适应网络拓扑结构的变化，当网络拓扑结构发生变化，需要手工重新配置。

点击<添加>，输入目的地址、子网掩码、出接口和下一跳IP地址，创建静态路由。

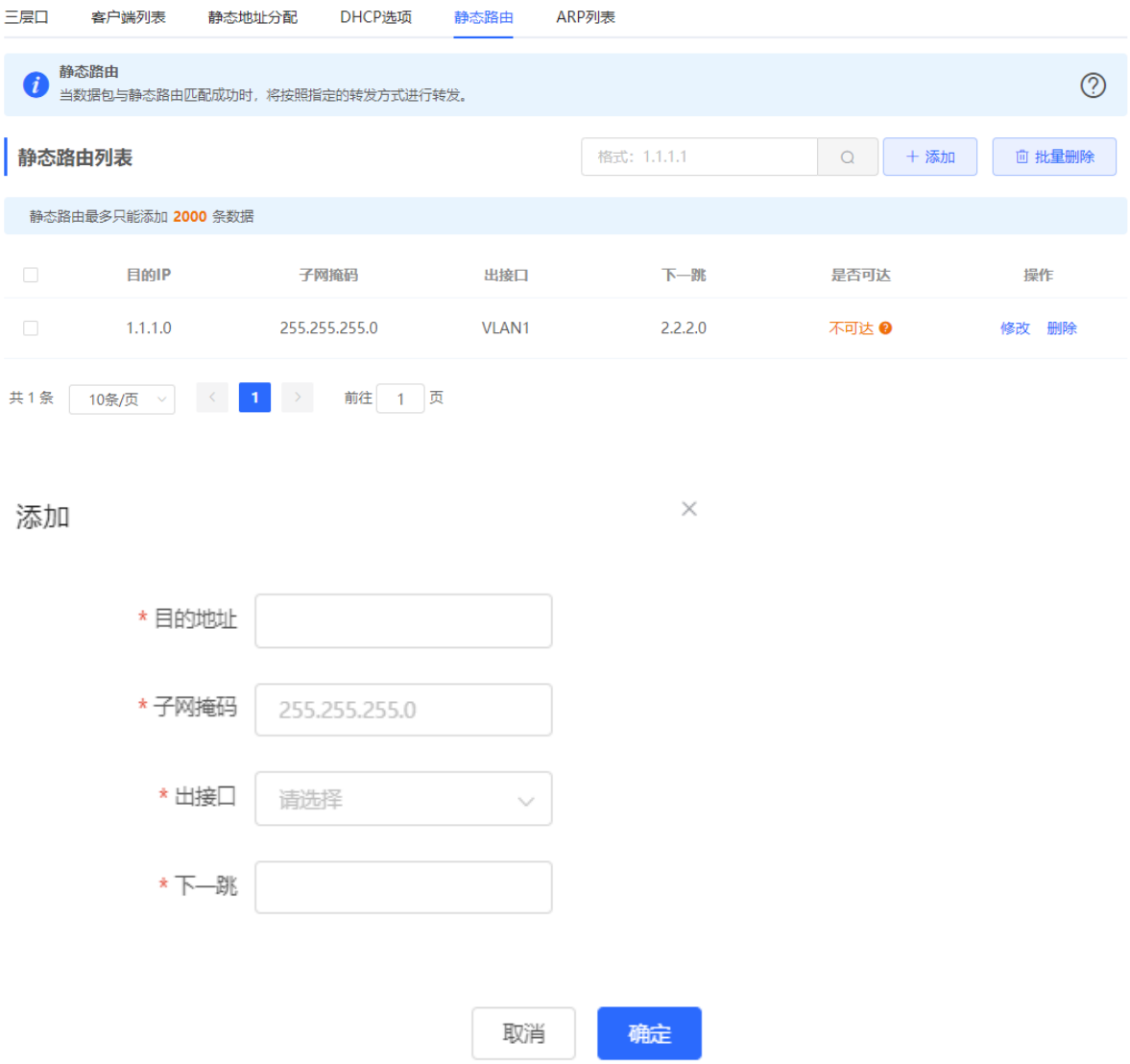


表6-4 静态路由配置参数说明

参数	说明
目的地址	数据包要到达的目的网络。根据目的地址与掩码匹配数据报文的目的IP
子网掩码	目的网络的子网掩码。根据目的地址与掩码匹配数据报文的目的IP
出接口	数据包进行转发的接口
下一跳	数据包将发往的下一个路由点的IP地址

创建静态路由后，可在页面的静态路由列表中查看到相关配置信息及路由是否可达。“是否可达”用来指示下一跳是否可达，以此判断路由是否能够正常生效。若显示“不可达”，请检查当前路由的出接口是否能Ping通下一跳地址。

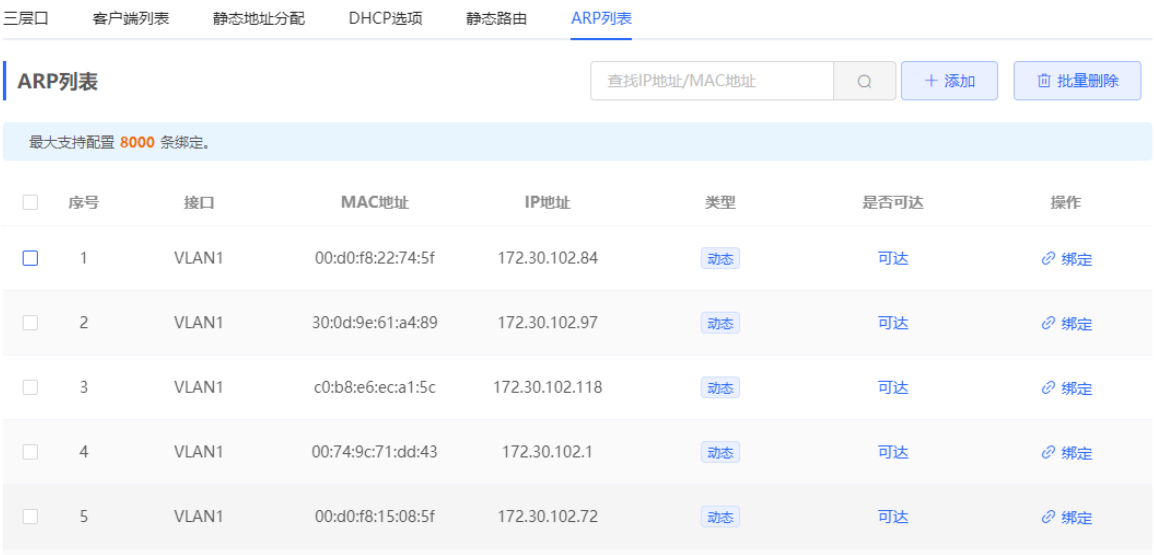
如需删除或修改静态路由，可在“静态路由列表”中点击最后一列操作栏下的<删除>或<修改>；或在“静态路由列表”中勾选需要删除的静态路由表项，点击<批量删除>，删除多条静态路由表项。

6.4 设置 ARP 静态表项

【本机管理-页面向导】三层管理>> ARP列表

设备学习连接在设备各端口上的网络设备的IP地址与MAC地址，生成对应ARP表项。支持绑定ARP映射或用户手动指定IP地址和MAC地址的映射来防止设备学到错误的ARP表项，提高网络安全性。

- 将动态ARP表项绑定为静态表项：选中ARP列表中动态获取到的ARP映射表项，单击<绑定>按钮即可完成绑定。
- 手动设置ARP静态表项：点击<添加>按钮，输入绑定的IP地址和MAC地址，点击<确定>。



若需要解除静态配置的IP地址和MAC地址绑定关系，点击操作栏中<删除>按钮。

7 安全管理

7.1 DHCP Snooping

7.1.1 功能简介

DHCP Snooping意为DHCP窥探，通过对客户端和服务器之间的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。

7.1.2 单机设置

【本机管理-页面向导】安全管理>> DHCP Snooping

点击开关开启DHCP Snooping功能，在端口面板上选择设置为信任口的端口，点击<保存>。开启DHCP Snooping后，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。

说明

一般将连接DHCP服务器的上联端口设置为信任口。

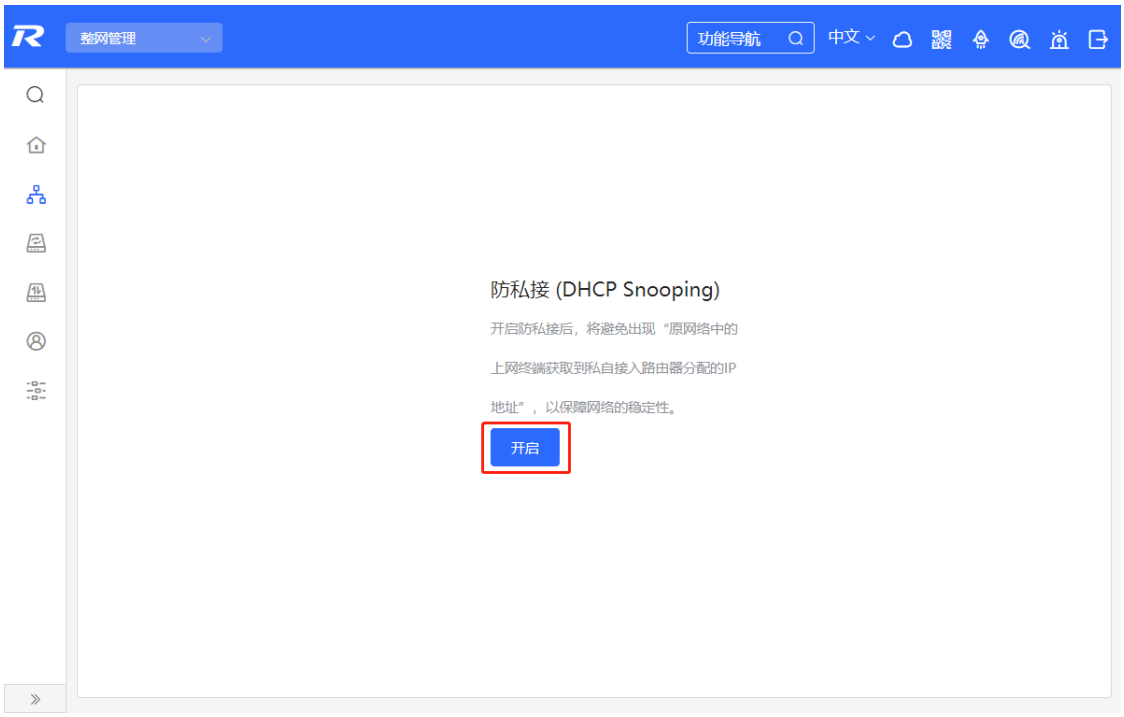
Option82选项是为了增强DHCP服务器的安全性，改善IP地址的分配策略而提出的一种DHCP选项。开启Option 82开关后，将在DHCP请求报文中携带Option 82信息。

7.1.3 批量设置整网交换机

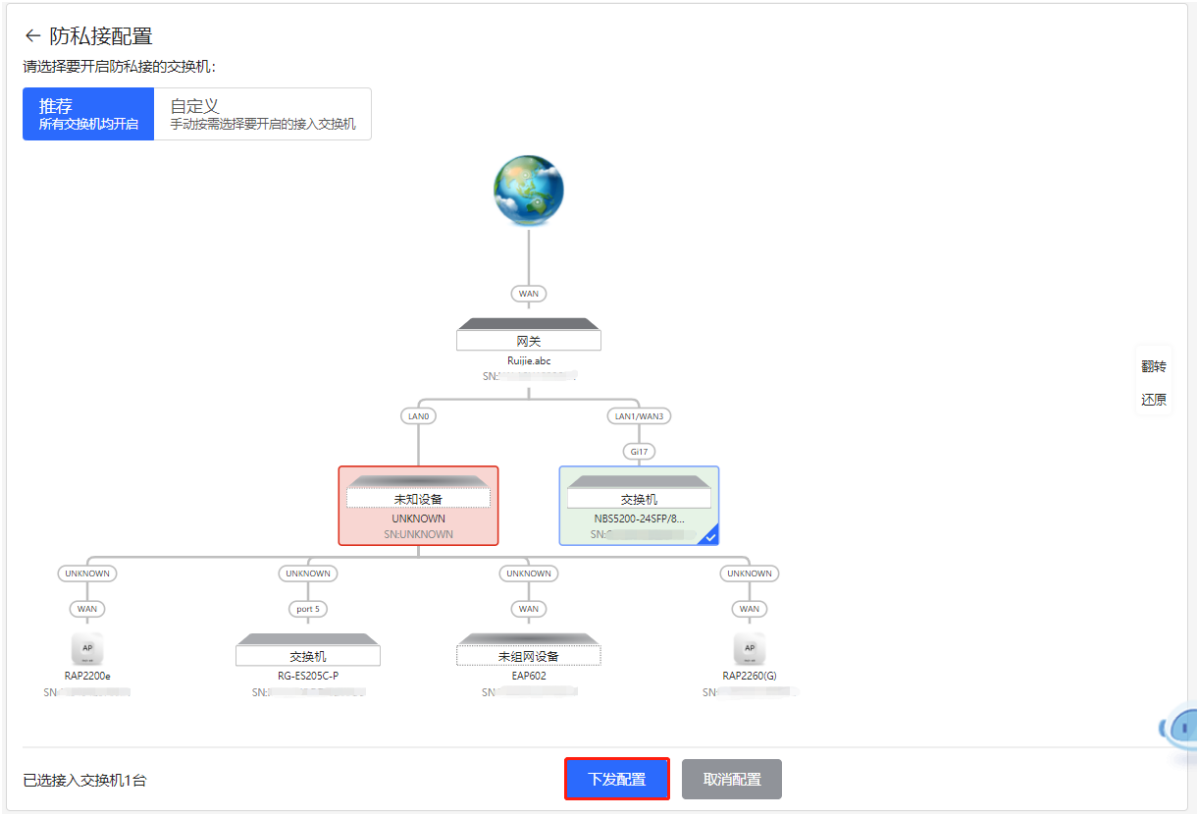
【整网管理-页面向导】整网管理>>防私接

在整网交换机上开启防私接功能（DHCP Snooping），能够保证用户只能从控制范围内的DHCP服务器获取网络配置参数，避免出现“原网络中的上网终端获取到私自接入的路由器所分配的IP地址”，以保障网络的稳定性。

(1) 点击<开启>，进入防私接配置页面。



(2) 在组网拓扑中选择需要开启防私接功能的接入交换机，分为推荐和自定义两种方式：选择推荐，将自动选中网络中的全部交换机；选择自定义，可手动选择要开启防私接功能的交换机。点击<下发配置>，将在选中的交换机上开启防私接功能。



(3) 完成配置下发后，如需修改防私接功能的生效范围，点击<前往配置>，可在拓扑中重新选择开启防私接的交换机。点击防私接开关，可一键关闭网络中所有交换机上的防接功能。

7.2 风暴控制

7.2.1 功能简介

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，加大报文传输超时机率。这种情况称之为局域网风暴。拓扑协议的执行错误或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设定范围时，设备将只允许设定范围内的数据流通过，超出设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。

7.2.2 配置步骤

【本机管理-页面向导】安全管理>>风暴控制

点击<批量设置>，在弹出框中选择风暴控制的限制类型、应用端口，并分别输入广播、未知名组播和未知名单播限制速率，点击<确定>。完成设置后如需修改或删除限速规则，可点击操作栏下的“修改”或“删除”。

配置类型分为两种：

- 基于每秒报文数的风暴控制：当设备端口接收到的数据流的速率超过所设定的每秒允许通过的报文数时，设备将只允许所设定每秒报文数的数据流通过，超出允许通过的每秒报文数部分的数据流将被丢弃，直到数据流恢复正常。
- 基于每秒千比特数的风暴控制：当设备端口接收到的数据流的速率超过所设定的每秒允许通过的千比特数时，设备将只允许所设定每秒千比特数的数据流通过，超出允许通过的每秒千比特数部分的数据流将被丢弃，直到数据流恢复正常。

7.3 ACL

7.3.1 功能简介

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端口上，对进出端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。

7.3.2 创建 ACL 规则

【本机管理-页面向导】安全管理>>ACL>>ACL列表

(1) 点击<添加>，选择ACL访问控制类型，并输入ACL名称，点击<确定>。

基于MAC地址控制：对端口上进出的二层报文进行控制，禁止或允许特定的二层报文进入网络

基于IP地址控制：对端口上进出的IPv4报文进行控制，禁止或允许特定的IPv4报文进入网络

(2) 点击ACL表项操作栏的<查看规则>，在弹出的侧栏中设置过滤规则后点击<添加规则>，为ACL添加规则。可添加多条规则。

规则包含“允许”或“禁止”两种动作，以及报文的匹配规则。ACL中规则的顺序决定了该规则在访问列表中的匹配优先级。网络设备在处理报文时，按规则的序号从小到大进行规则匹配。在规则列表点击<移动>，可调整匹配顺序。

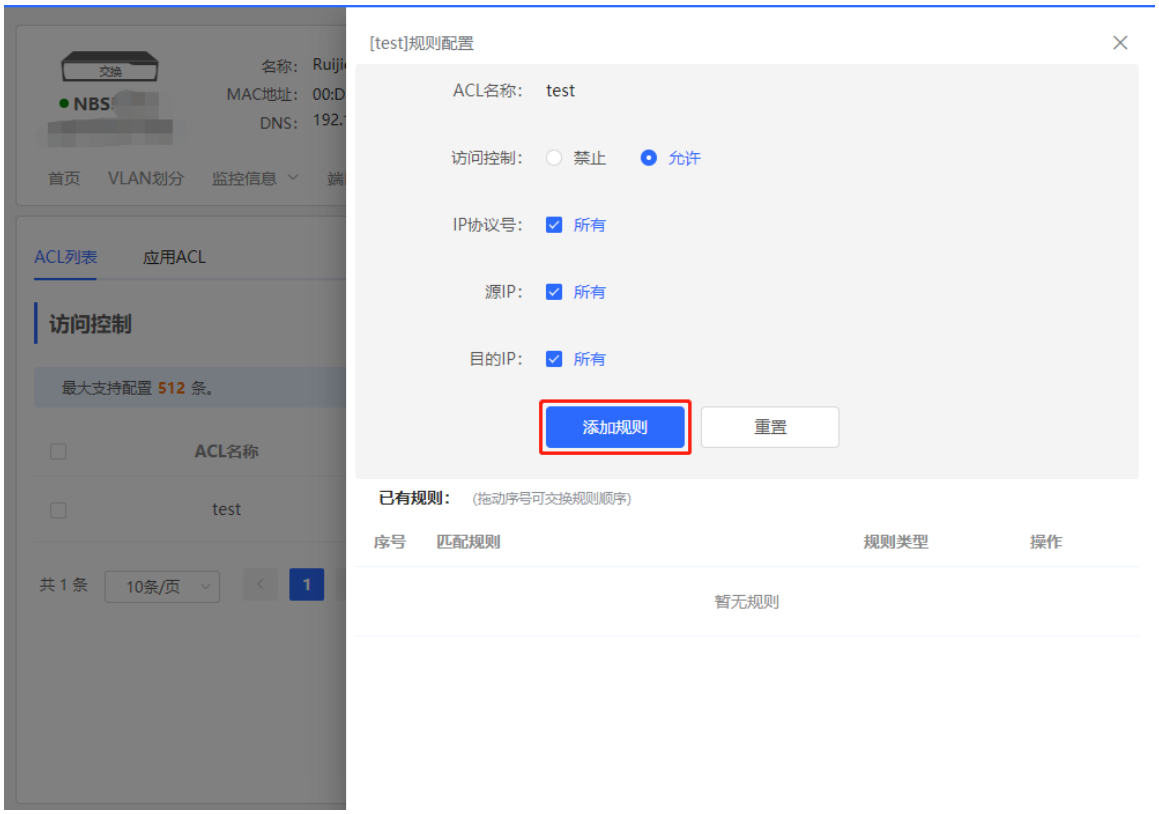


表7-1 ACL 规则配置参数说明

参数	说明
访问控制	配置ACL规则处理行为 禁止：如果匹配报文，则拒绝报文访问。 允许：如果匹配报文，则允许报文访问。
IP协议号	匹配IP协议编号。取值范围为0~255，勾选“所有”则匹配所有IP协议
源IP	匹配报文源IP地址，勾选“所有”则匹配所有源IP地址
目的IP	匹配报文目的IP地址，勾选“所有”则匹配所有目的IP地址
报文类型号	匹配以太网协议类型。取值范围为0x600~0xFFFF。勾选“所有”则匹配所有协议类型号
源MAC	匹配源主机的MAC地址，勾选“所有”则匹配所有源MAC地址
目的MAC	匹配目的主机的MAC地址，勾选“所有”则匹配所有目的MAC地址

说明

- ACL名称不可重复，ACL一旦创建只允许修改名称。
- 被端口应用的ACL不允许修改或删除，如需修改，请先解除ACL与端口的绑定。
- ACL规则中，隐藏最后一条默认规则，为禁止所有报文。

7.3.3 应用 ACL 规则

【本机管理-页面向导】安全管理>>ACL>>应用ACL

点击<批量添加>或操作列的<修改>，为端口选择应用的MAC ACL和IP ACL，点击<确定>。

说明

ACL目前只支持应用在端口的入口方向，即对接收到的报文进行过滤。

端口应用ACL后，可点击列表操作栏的<解除绑定>，或勾选端口表项并点击<批量删除>，解除端口与ACL的绑定。

7.4 端口保护

【本机管理-页面向导】安全管理>>端口保护

某些场景下，要求设备上的部分端口间不能互相通讯，可以通过将指定端口设置为保护口来实现。开启端口保护的端口（即保护口）之间互相无法通讯，不同端口下的用户二层隔离。而保护口与非保护口之间可以正常通讯。

各端口默认关闭端口保护功能，可点击 开启。如需批量开启多个端口的端口保护功能，可点击<批量设置>，开启端口保护功能开关并选择应用的端口，点击<确定>。

7.5 IP+MAC 端口绑定

7.5.1 功能简介

配置IP+MAC端口绑定功能后，将在指定端口上检查IP报文的源IP地址和源MAC地址是否符合所配置的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，以提高安全性。

7.5.2 配置步骤

【本机管理-页面向导】安全管理>>IP+MAC端口绑定

1. 添加 IP+MAC 端口绑定

点击<添加>，选择需要设置的端口并输入与端口绑定的IP地址和MAC地址，点击<确定>。IP地址和MAC地址至少需要输入一项。如需修改已创建的绑定关系，可直接点击操作列的“修改”。

注意

IP+MAC端口绑定配置将优先于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所配置的绑定关系，报文就会被允许通过。

2. 搜索绑定表项

右上角搜索框支持根据IP地址、MAC地址或端口查找绑定表项。在下拉框中选择搜索类型，输入搜索的字符串，点击<搜索>，列表将过滤出符合搜索条件的表项。

3. 取消 IP+MAC 端口绑定

批量设置：在IP+MAC端口绑定列表中勾选需要删除的表项，点击<批量删除>，在提示框中点击<确定>。

取消单条绑定关系：点击列表中表项最后一列操作栏下的<删除>，在提示框中点击<确定>。

7.6 IP Source Guard

7.6.1 功能简介

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

IP Source Gusrd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。设置DHCP Snooping功能请参考7.1 DHCP Snooping。

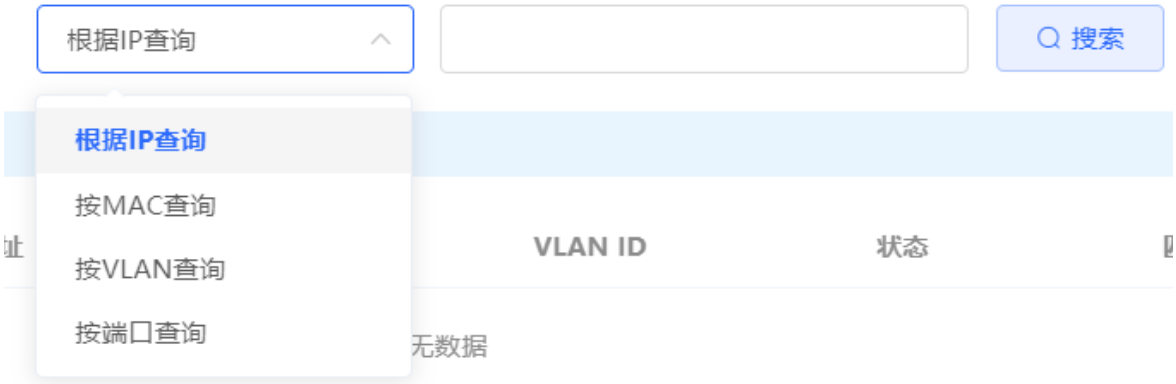
7.6.2 查看绑定列表

【本机管理-页面向导】安全管理>>IP Source Guard>>绑定列表

绑定列表是IP Source Guard安全控制的依据。目前，绑定列表中数据来自DHCP Snooping动态学习生成的绑定数据库。启动IP Source Guard功能后，DHCP Snooping数据库信息将同步到IP Source Guard的绑定列表中，这样IP Source Guard就可以在开启DHCP Snooping功能的设备上对客户端的IP报文进行严格过滤。

点击<刷新>可获取最新的绑定列表数据。

右上角搜索框支持根据IP地址、MAC地址、VLAN或端口在绑定列表中查找指定表项。点击下拉框选择搜索类型，输入搜索的字符串，点击<搜索>。



7.6.3 开启端口的 IP Source Guard 功能

【本机管理-页面向导】安全管理>>IP Source Guard>>端口设置

点击端口列表中操作列的“修改”，选择“开启”并选择匹配规则，点击<确定>。

匹配规则分为两种：

- IP地址：检查所有经过该端口的IP报文，仅对报文的源IP地址进行检测。只有报文的源IP字段符合绑定列表中的IP地址，才能通过端口。
- IP地址+MAC地址：检查所有经过该端口的IP报文的源IP和源MAC，只有报文的二层源MAC与三层源IP和绑定列表中的某条记录完全匹配上，才能通过端口。

注意

- DHCP Snooping信任口不支持开启IP Source Guard功能。
- 只支持在二层端口上开启IP Source Guard功能。

7.6.4 设置例外 VLAN

【本机管理-页面向导】安全管理>>IP Source Guard>>例外VLAN

默认情况下端口开启IP Source Guard后，会对该端口包含的所有VLAN生效。用户可以指定例外VLAN来实现不对该VLAN范围内的IP报文进行检查和过滤，即不受IP Source Guard的控制。

点击<添加>，输入例外VLAN ID和应用的端口，点击<确定>。

⚠ 注意

端口下必须先开启IP Source Guard才可以指定例外VLAN，端口下关闭IP Source Guard后会自动清除对应的例外VLAN。

7.7 防火墙管理

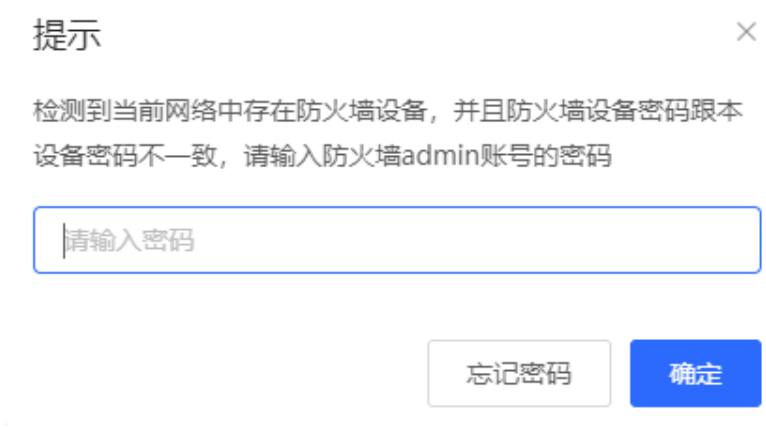
将防火墙设备添加到网络后，可以通过NBS设备的Web管理界面对防火墙设备进行管理、配置。

7.7.1 查看防火墙设备信息

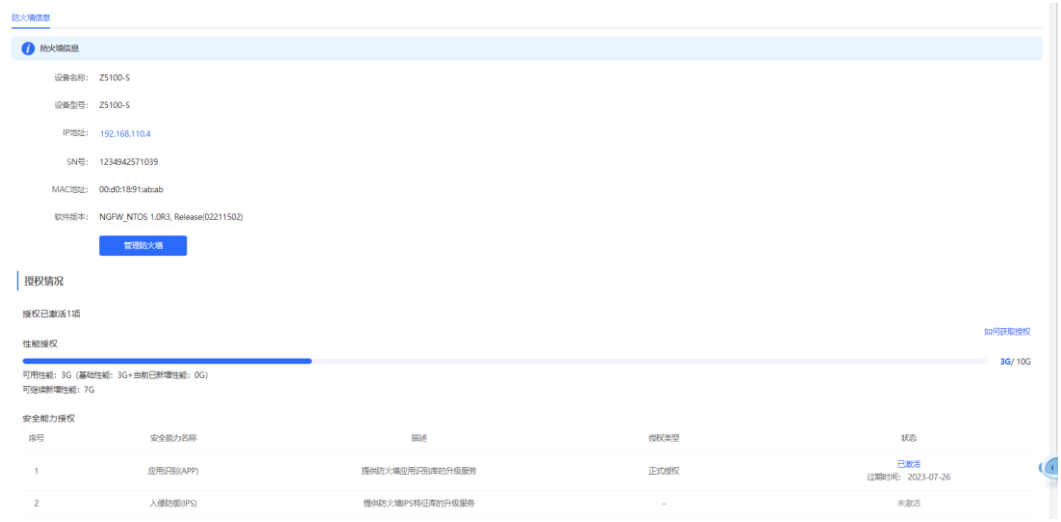
查看防火墙设备的基本信息、授权情况。

【整网管理-页面向导】整网管理>>防火墙管理

(1) 当防火墙设备的管理密码与NBS设备管理密码不同时，系统提示输入防火墙设备的管理密码，点击<确定>。



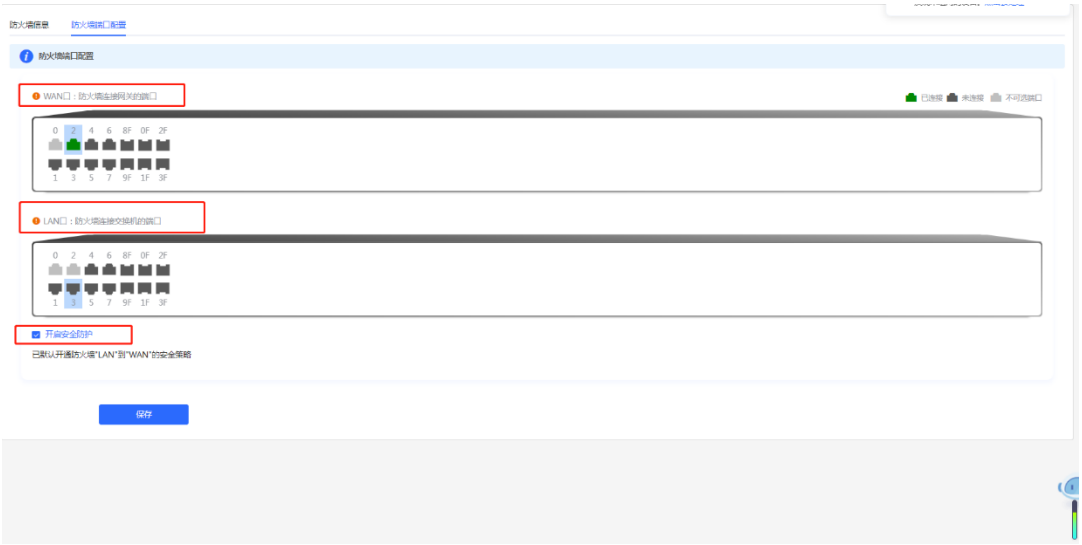
(2) 系统显示防火墙设备的基本信息、性能授权、安全能力授权等信息。



点击<管理防火墙>可跳转到防火墙设备的Web管理界面，配置防火墙安全策略、授权激活等操作。具体操作步骤，请参见对应防火墙设备的Web管理手册。

7.7.2 设置防火墙端口配置

当防火墙设置为透明模式接入网络时，系统会显示“防火墙端口配置”界面。可选择连接NBS设备的WAN口、连接交换设备LAN口，并开启安全防护功能。



7.8 防网关 ARP 欺骗

7.8.1 功能简介

防网关ARP欺骗在用户接入端口上检查ARP报文的源IP是否为配置的网关IP，如果是，则将该报文丢弃，防止用户收到错误的ARP响应报文；如果不是，则不对该报文进行处理。保证只有上联设备能够下发网关的ARP报文，其它终端发送的假冒网关ARP响应报文将被过滤，从而有效地预防针对网关的ARP欺骗。

7.8.2 配置步骤

【本机管理-页面向导】安全管理>>防网关ARP欺骗

1. 开启防网关 ARP 欺骗

点击<添加>，选择需要设置的端口并输入网关IP，点击<确定>。

说明

一般在设备的下联口开启防网关ARP欺骗功能。

2. 关闭防网关 ARP 欺骗

批量关闭：在列表中勾选需要删除的表项，点击<批量删除>。

关闭单个端口：点击对应表项最后一列操作栏下的<删除>。

8 高级设置

8.1 STP

STP（Spanning Tree Protocol，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。

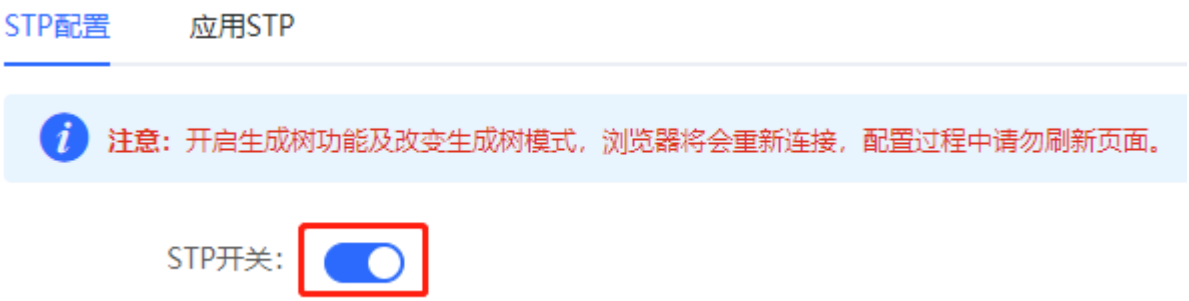
8.1.1 STP 全局设置

【本机管理-页面向导】高级设置>>STP>>STP配置

(1) 点击STP开关，在提示信息框中点击<确定>，开启设备的STP功能。默认情况下STP功能处于关闭状态。

注意

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) 设置STP全局参数，点击<保存>。

表8-1 STP 全局配置参数说明

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
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	BPDU消息生存的最长时间。当超出本时间，报文消息将被丢弃。若非根设备直至老化时间超时还没有收到根的BPDU信息，则认为根桥或通向根桥的链路发生了故障	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	发送两个相邻BPDU间的时间间隔	2秒
转发延时	端口状态改变的时间间隔，即端口从Listening转变向Learning，或者从Learning转向Forwarding状态的时间间隔	15秒
生成树模式	生成树协议版本，目前支持STP协议（Spanning Tree Protocol，生成树协议）和RSTP协议（Rapid Spanning Tree Protocol，快速生成树协议）	RSTP

8.1.2 端口应用 STP

【本机管理-页面向导】高级设置>>STP>>应用STP

设置端口的生成树属性。点击<批量设置>，选择端口并配置STP参数；或点击“端口列表”中操作列的<修改>，设置指定端口。

表8-2 端口的 STP 参数说明

参数	说明	默认值
端口角色	• root（根端口）：到根桥（Root Bridge）路径最短的端口 • alternate（替换端口）：根端口的备份端口。一旦根端口失效，替换端口立即转变为根端口 • designated（指定端口）：根桥或上游桥上连接下游设备的端口 • disable（阻塞端口）：生成树中不起作用的端口	NA

参数	说明	默认值
端口状态	● disable（禁用）：端口被手工关闭或由于故障导致关闭，不参与生成树也不转发数据，初始化或开启后可转为阻塞状态 ● blocking（阻塞）：处于该状态的端口不能够参与转发数据报文，能发送配置BPDU消息，也不能进行地址学习，但可以接收BPDU配置消息，并交给CPU处理 ● listening（监听）：如果某端口可成为根端口或指定端口，该端口将进入listening状态。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。 ● learning（学习）：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 ● forwarding（转发）：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	NA
优先级	端口的优先级，用于选举端口角色，优先选择高优先级的端口进入转发状态	128
连接类型 配置状态	设置链路类型，取值包括：共享、点对点和自动。自动模式下端口根据双工模式确定端口类型，端口为全双工模式时为点对点类型，端口为半双工模式时为共享类型	自动
连接类型 实际状态	实际的链路类型：共享、点对点	NA
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和终端相连的边缘端口，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Port Fast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。如果开启Port Fast的端口收到BPDU则Port Fast自动关闭，BPDU Filter特性也就自动失效 一般在连接终端的端口上开启本功能	关闭

说明

- 建议直连PC的端口开启Port Fast。
- 开启STP后需要等待30s以上端口才能变成转发状态，所以可能出现短暂断连，无法转发报文。

8.2 LLDP

8.2.1 功能简介

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并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、双工模式是否匹配等，管理员可以根据这些信息快速地定位及排查故障。

8.2.2 LLDP 全局设置

【本机管理-页面向导】高级设置>>LLDP>>LLDP配置

(1) 点击LLDP开关，在提示信息框中点击<确定>，开启设备的LLDP功能。设备默认开启LLDP功能，当LLDP开关处于  开启状态，可跳过本步骤。

(2) 配置全局LLDP参数，点击<保存>。

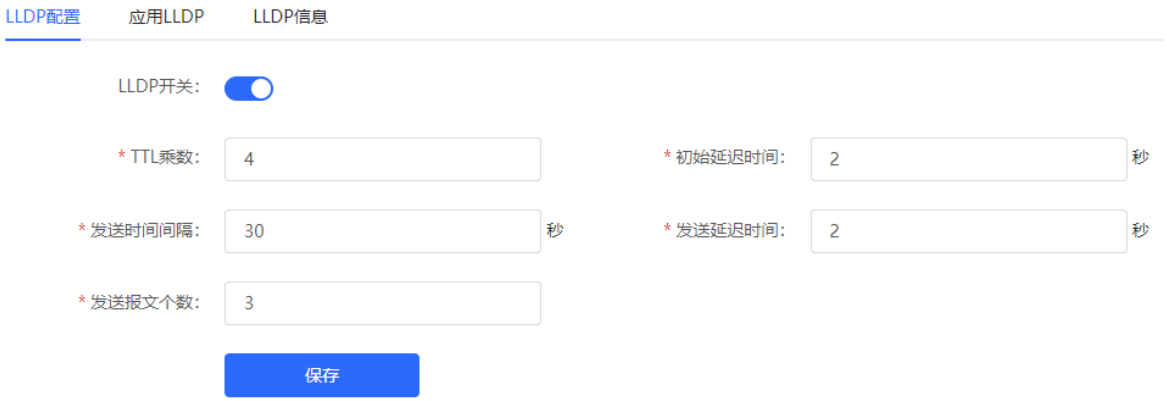


表8-3 LLDP 全局配置参数说明

参数	说明	默认值
LLDP开关	是否开启LLDP功能	开启
TTL乘数	LLDP的TTL乘数 在LLDP报文中，Time To Live TLV表示本设备的信息在邻居设备上的存活时间。Time To Live TLV=TTL乘数×报文发送时间间隔+1，通过配置TTL乘数和LLDP报文发送时间间隔，可以修改Time To Live TLV值	4
发送时间间隔	LLDP报文发送时间间隔，单位为秒 Time To Live TLV=TTL乘数×报文发送时间间隔+1，通过配置TTL乘数和LLDP报文发送时间间隔，可以修改Time To Live TLV值	30秒

参数	说明	默认值
发送报文个数	快速发送的报文个数 当发现新的邻居，或者LLDP工作模式发生变化时，为了让邻居设备尽快学习到本设备的信息，本设备将启动快速发送机制。快速发送机制将缩短LLDP报文的发送周期为1秒，并连续发送一定数量的LLDP报文，之后再恢复正常的发送周期。本功能用于配置快速发送机制下，LLDP报文发送的个数。	3
初始延迟时间	端口初始化的延迟时间，单位为秒。设置初始化延迟时间可以避免端口工作模式频繁变化引起状态机频繁的初始化	2秒
发送延迟时间	LLDP报文发送的延迟时间，单位为秒 当本地信息发生变化时会立即向邻居设备发送LLDP报文，为了避免本地信息频繁变化引起频繁发送LLDP报文，可以配置LLDP报文的发送延迟时间，限制LLDP报文的频繁发送。 若延迟时间配置过小，本地信息的变化将引起频繁发送LLDP报文；若延迟时间配置过大，本地信息的变化将不能及时发送LLDP报文。请根据实际情况配置合适的延时	2秒

8.2.3 端口应用 LLDP

【本机管理-页面向导】高级设置>>LLDP>>应用LLDP

点击“端口列表”操作栏的<修改>，或点击<批量设置>，选择需要设置的端口后，设置端口LLDP工作模式以及是否开启LLDP-MED功能，点击<确定>。

发送LLDPDU：开启后端口能够发送LLDPDU；

接收LLDPDU：开启后端口能够接收LLDPDU；

媒体终端发现MED：开启后，当对端为支持LLDP-MED（Link Layer Discovery Protocol-Media Endpoint Discovery，链路层发现协议-媒体端点发现）协议的终端时，可以发现邻居信息。

8.2.4 查看 LLDP 信息

【本机管理-页面向导】高级设置>>LLDP>>LLDP信息

查看LLDP信息，包括本地设备和各个端口的邻居设备的LLDP信息。点击端口名称可查看端口邻居的详细信息。

可以通过LLDP信息查看拓扑连接情况，或利用LLDP进行错误检测。例如当网络拓扑中有直连的两台交换机设备，当管理员进行VLAN、端口速率双工等配置时，若配置的信息与相连邻居设备的配置不匹配，系统将提示相应的错误。

8.3 RLDP

8.3.1 功能简介

RLDP（Rapid Link Detection Protocol，快速链路检测协议）是一种以太网链路故障检测协议，用于快速检测单向链路故障、双向链路故障以及下联环路故障。如果发现故障存在，RLDP会根据用户配置的故障处理方式自动关闭或通知用户手工关闭相关端口，以避免流量的错误转发或者防止以太网二层环路。

支持批量开启组网中接入交换机的RLDP功能，默认情况下发生环路后交换机端口将被自动关闭；也可以对单台交换机进行设置，分别配置各端口是否开启环路检测以及检测到链路故障后的处理方式。

8.3.2 单机设置

1. RLDP 全局设置

【本机管理-页面向导】高级设置>>RLDP>>RLDP配置

(1) 点击RLDP开关，在提示信息框中点击<确定>，开启设备的RLDP功能。默认情况下RLDP功能处于关闭状态。

(2) 配置全局RLDP参数，点击<保存>。

表8-4 RLDP 全局配置参数说明

参数	说明	默认值
RLDP开关	是否开启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	3秒
开启自动恢复功能	开启后，端口发生环路后能自动恢复到初始化状态	关闭
定时自动恢复时间	定时自动恢复所有故障端口到初始化状态并重新启动链路检测的时间间隔，单位为秒	30秒

2. 端口应用 RLDP

【本机管理-页面向导】高级设置>>RLDP>>应用RLDP

点击“端口列表”操作栏的<修改>，或点击<批量设置>，选择需要设置的端口后，设置端口是否开启环路检测和检测到故障后的处理方式，点击<确定>。

端口故障处理方式分为3种：

- 只告警（Warning）：只提示相关的信息说明当前的故障端口和故障类型；
- 告警且阻塞报文转发（Block）：在对故障作出告警提示的基础上，设置故障端口不对收到的报文进行转发
- 告警且关闭端口（Shutdown）：在对故障作出告警提示的基础上，将端口关闭

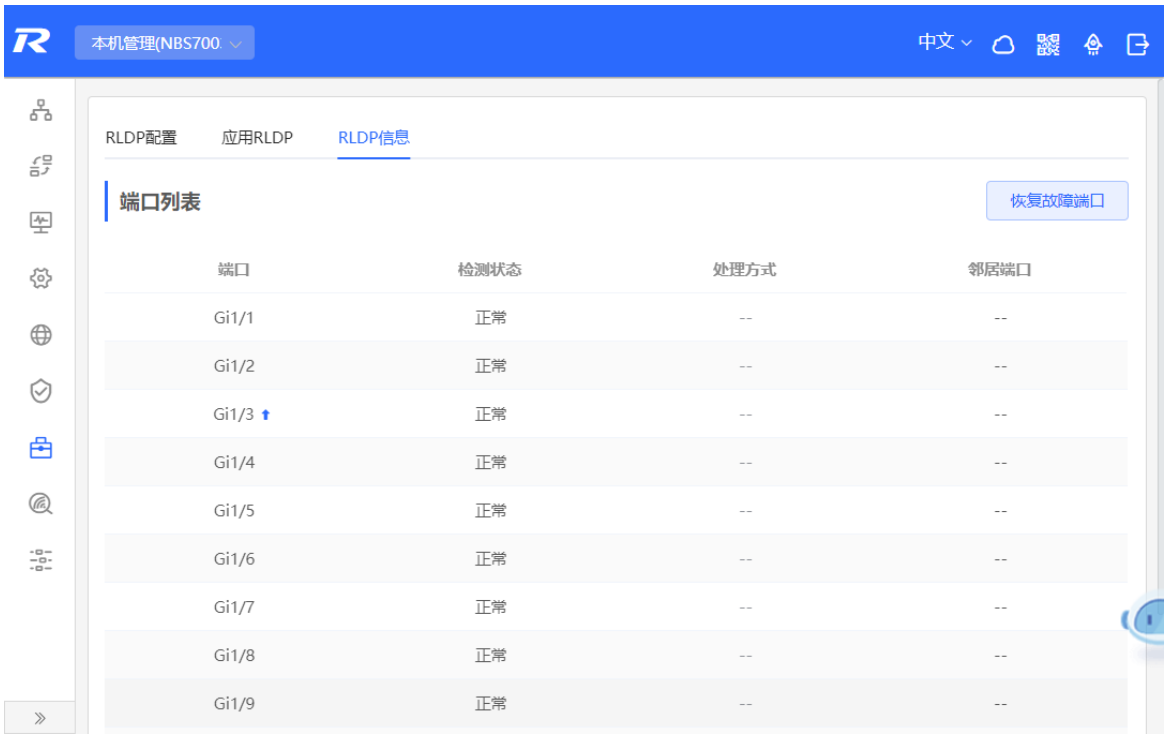
注意

- 在聚合端口上应用RLDP，“处理方式”只能配置为“告警且关闭端口（Shutdown）”。
- 在聚合口上进行RLDP检测时，若在同一设备上接收到检测报文，即使报文发送端口与接收端口的VLAN不同也会判断为环路故障。

3. 查看 RLDP 信息

【本机管理-页面向导】高级设置>>RLDP>>RLDP信息

可查看端口的检测状态、故障处理方式以及邻居设备与本端设备连接的端口。点击<恢复故障端口>可以把端口触发的RLDP故障状态恢复为正常状态。

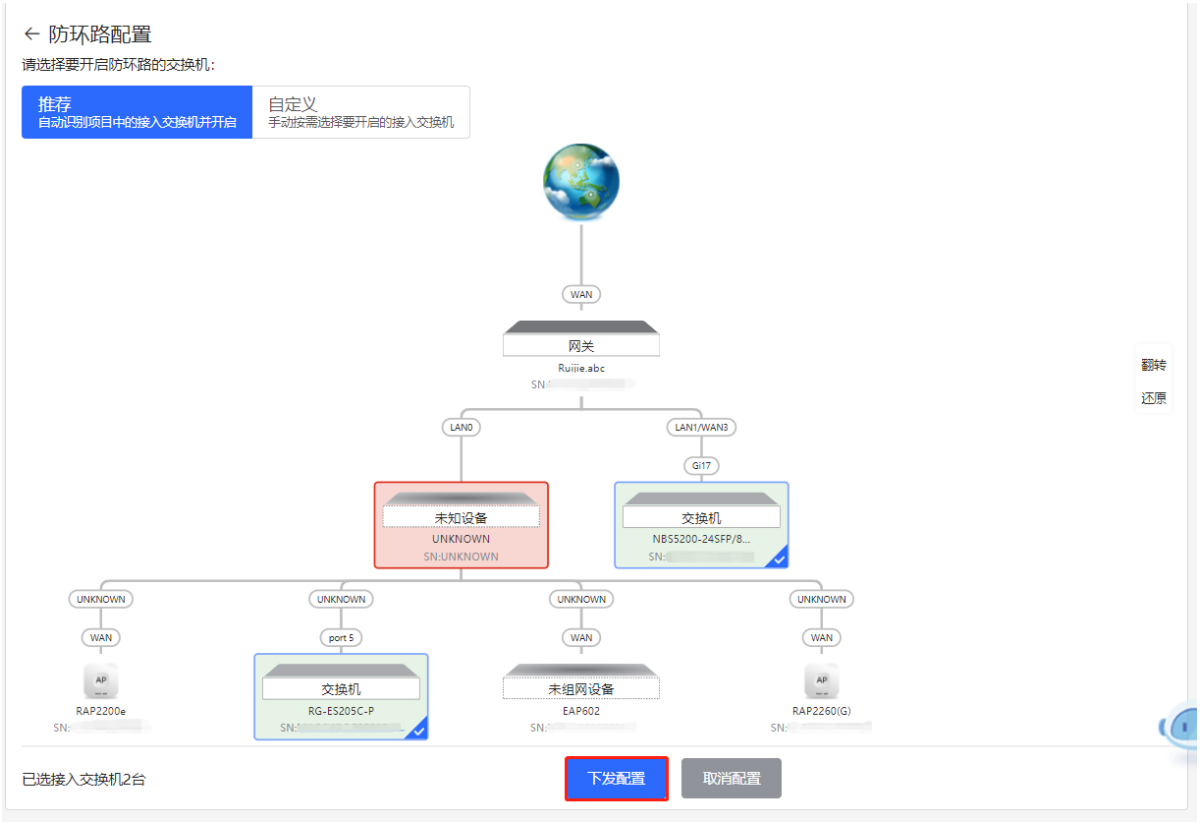


8.3.3 批量设置整网交换机

【整网管理-页面向导】整网管理>>防环路

(1) 点击<开启>，进入防环路配置页面。

(2) 在组网拓扑中选择需要开启防环路功能的接入交换机，分为推荐和自定义两种方式：选择推荐，将自动选中网络中的全部接入交换机；选择自定义，可手动选择要开启防环路功能的交换机。点击<下发配置>，将在选中的交换机上开启防环路功能。



(3) 完成配置下发后，如需修改防环路功能的生效范围，点击<前往配置>，可在拓扑中重新选择开启防环路的交换机。点击防环路开关，可一键关闭网络中所有交换机上的防环路功能。

8.4 设置本机 DNS

本机DNS服务器地址为可选配置，设备默认会从上联设备中获取DNS服务器地址。

【本机管理-页面向导】高级设置>>本机DNS

输入本机使用的DNS服务器地址，如果存在多个，中间使用空格隔开。点击<保存>。设置本机DNS后，优先使用管理IP的DNS进行解析，再使用该DNS地址。

8.5 Voice VLAN

注意

本功能的支持情况在不同产品间存在差异，目前支持本功能的NBS系列产品有：RG-NBS3100系列、RG-NBS3200系列、RG-NBS5100系列和RG-NBS5200系列交换机。

8.5.1 功能简介

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，并可为语音流下发有针对性的QoS（Quality of Service，服务质量）策略，提高语音流量的传输优先级，保证通话质量。

8.5.2 Voice VLAN 全局设置

【本机管理-页面向导】高级设置>>Voice VLAN>>全局配置

点击开启Voice VLAN开关并配置相关全局参数，点击<保存>。

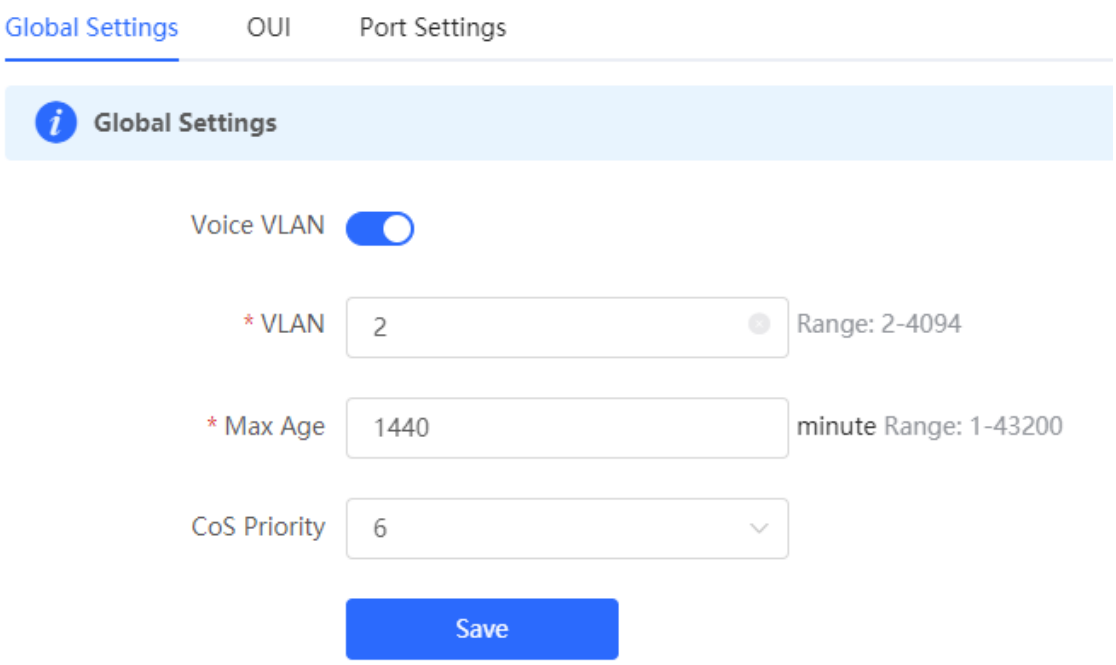


表8-5 Voice VLAN 全局配置参数说明

参数	说明	默认值
Voice VLAN开关	是否开启Voice VLAN功能	关闭
VLAN	作为Voice VLAN的VLAN ID	NA
老化时间	Voice VLAN老化时间，单位为分钟。在自动模式下，语音报文对应的MAC地址老化后，若经过一段老化时间设备仍未从输入端口接收到任何语音报文，则将该端口从Voice VLAN中删除	1440分钟
语音优先级	Voice VLAN语音流报文的二层优先级，取值范围为0~7，数值越大，优先级越高。 可以通过修改语音流的优先级来提高通话质量	6

8.5.3 设置 Voice VLAN 的 OUI 地址

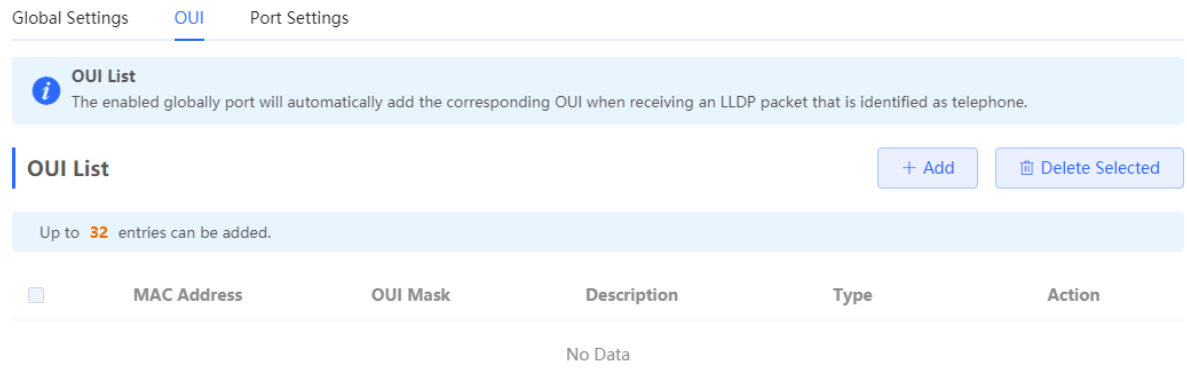
【本机管理-页面向导】高级设置>>Voice VLAN>>OUI

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。

说明

开启端口Voice VLAN功能后，当端口接收到IP电话发出的LLDP协议报文，可以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，并将协议报文中的源MAC提取出来作为语音设备MAC进行处理，从而实现自动添加对应的OUI。

点击<添加>，在弹出框中输入MAC地址，并选择OUI的掩码，点击<确定>。



8.5.4 设置端口 Voice VLAN 功能

【本机管理-页面向导】高级设置>>Voice VLAN>>端口配置

点击端口表项的<修改>或者页面右上角的<批量设置>，在弹出框中选择是否开启端口Voice VLAN功能、应用的Voice VLAN模式以及是否开启安全模式，点击<确定>。

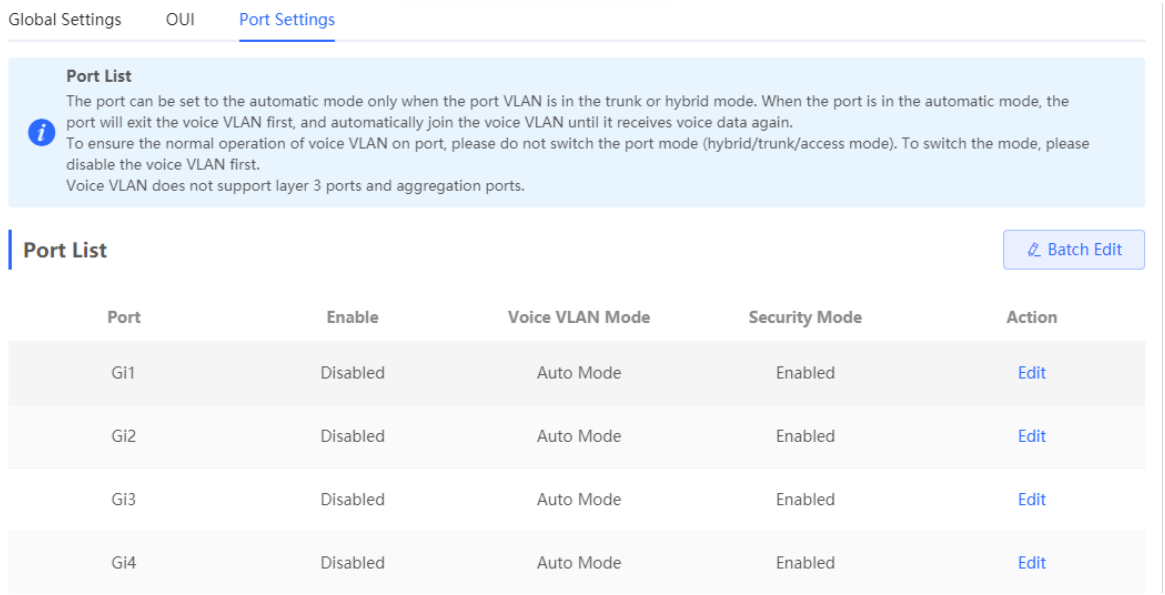


表8-6 Voice VLAN 端口配置参数说明

参数	说明	默认值
Voice VLAN模式	根据端口加入Voice VLAN的方式不同，分为自动模式和手动模式： ● 自动模式：端口开启Voice VLAN功能后检测端口的Permit VLAN是否包含Voice VLAN，如果包含，就会把Voice VLAN从端口的Permit 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Permit 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Permit VLAN中移除。 ● 手动模式：端口的Permit VLAN包含Voice VLAN时，语音报文就可以在Voice VLAN中传输。	自动模式
安全模式	安全模式开启时，Voice VLAN只允许传输语音流；设备会对报文源MAC地址逐一进行检查，当报文源MAC地址匹配Voice VLAN OUI地址时，允许该报文在Voice VLAN内传输，否则将其丢弃。 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。	开启

⚠ 注意

- 端口VLAN为Trunk模式时才能设置端口的Voice VLAN模式为自动模式。端口Voice VLAN模式为自动模式时，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。
- 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），如需切换，请先关闭端口的Voice VLAN功能
- 不建议在Voice VLAN中同时传输语音和业务数据。若的确有此需要，请关闭Voice VLAN安全模式。
- Voice VLAN不支持在三层端口和聚合端口上开启。

9 故障诊断

9.1 信息中心

【本机管理-页面向导】故障诊断>>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报文统计等状态和配置信息。

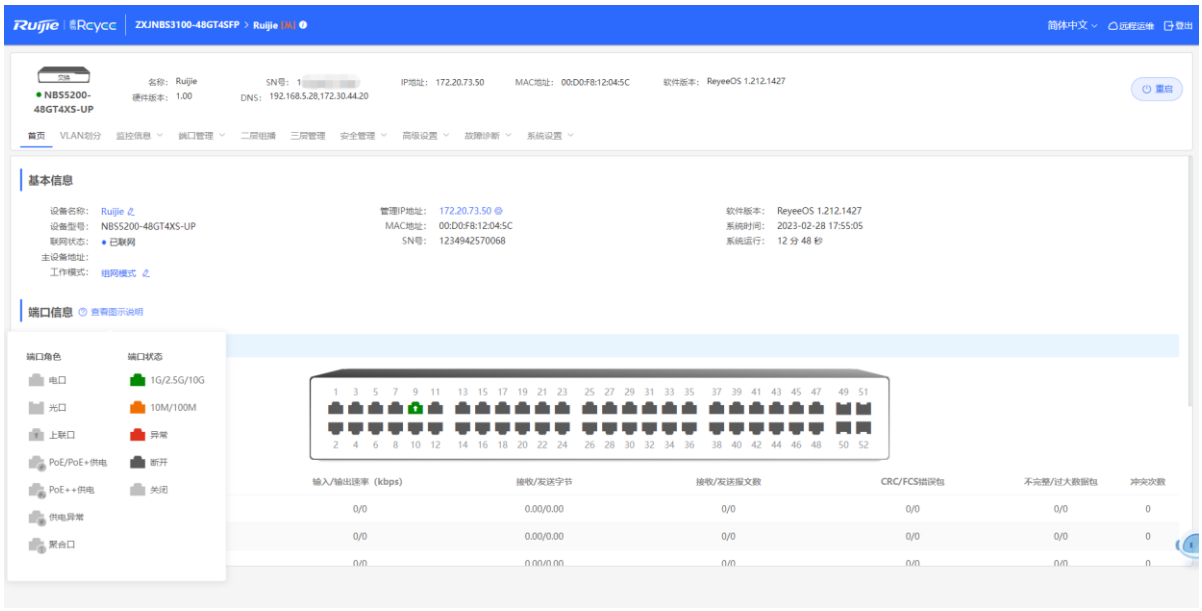
9.1.1 端口信息

【本机管理-页面向导】故障诊断>>信息中心>>端口信息

“端口信息”显示了设备的端口状态和配置信息。点击端口图标，可查看该端口的详细信息。

说明

- 如需设置端口的流控开关或设置光电复用口的光电属性，请参考4.2 端口设置章节。
- 如需设置端口二层模式以及所属VLAN，请参考3.5.3 设置端口VLAN章节。



9.1.2 VLAN 信息

【本机管理-页面向导】故障诊断>>信息中心>>VLAN信息

显示SVI口与路由口信息，包括VLAN包含的端口信息、端口IP地址、是否开启DHCP地址池等。

说明

- 如需设置VLAN，请参考3.5 VLAN划分章节。
- 如需设置SVI口和路由口，请参考6.1 设置三层端口章节。

9.1.3 路由信息

注意

若设备不支持三层功能（如RG-NBS3100系列和RG-NBS3200系列交换机），则不显示本类信息。

【本机管理-页面向导】故障诊断>>信息中心>>路由信息

显示设备上的路由信息。右上角搜索框支持根据IP地址查找路由表项。

说明

如需设置静态路由，请参考6.3 设置静态路由章节。

9.1.4 DHCP 客户端列表

注意

若设备不支持三层功能（如RG-NBS3100系列和RG-NBS3200系列交换机），则不显示本类信息。

【本机管理-页面向导】故障诊断>>信息中心>>客户端列表

显示设备作为DHCP服务器，为终端分配的IP地址信息。

说明

如需设置DHCP服务器相关功能，请参考6.2 设置DHCP服务器章节。

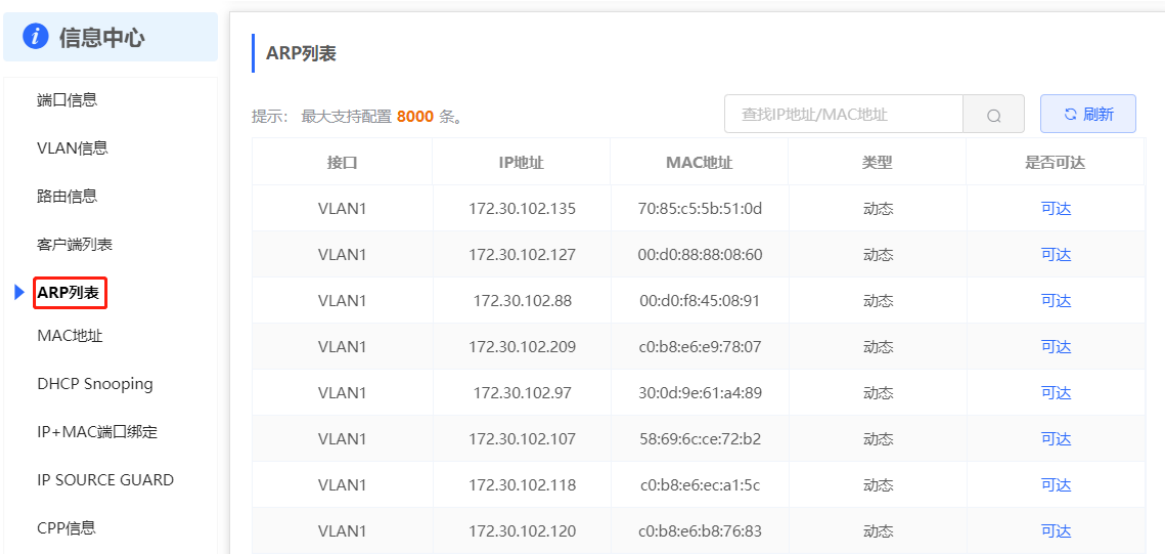
9.1.5 ARP 列表

【本机管理-页面向导】故障诊断>>信息中心>>ARP列表

查看设备上的ARP信息，包括动态学习到和静态配置的ARP映射表项。

说明

如需绑定动态ARP或手工设置静态ARP，请参考6.4 设置ARP静态表项章节。



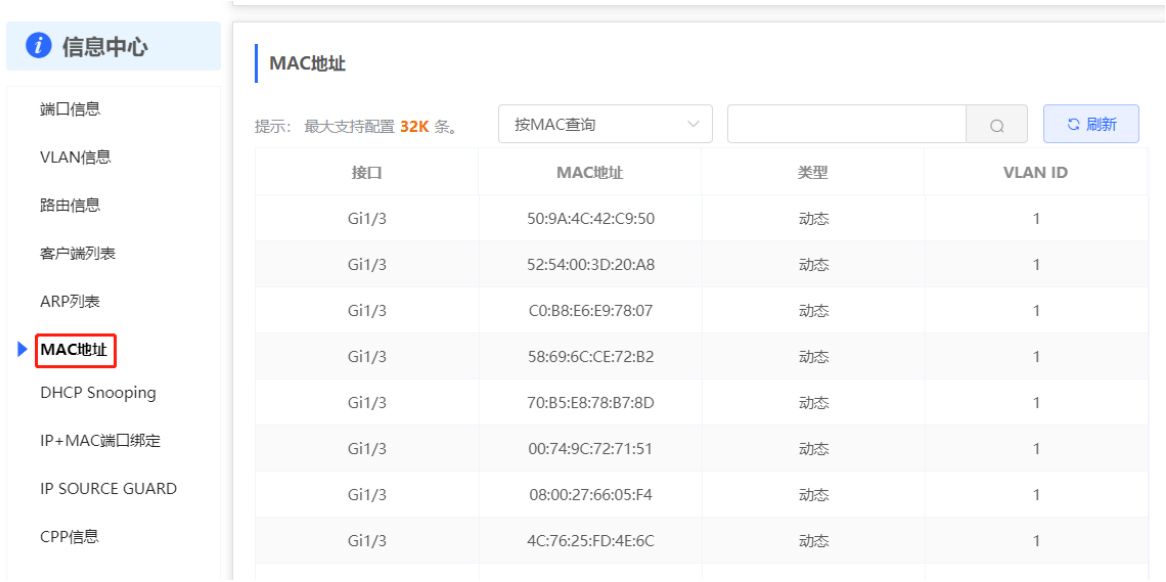
9.1.6 MAC 地址

【本机管理-页面向导】故障诊断>>信息中心>>MAC地址

显示设备的MAC地址信息，包含用户手动设置的静态MAC地址、过滤MAC地址以及设备自动学习到的动态MAC地址。

说明

如需对MAC地址进行配置与管理，请参考3.3 MAC地址管理章节。



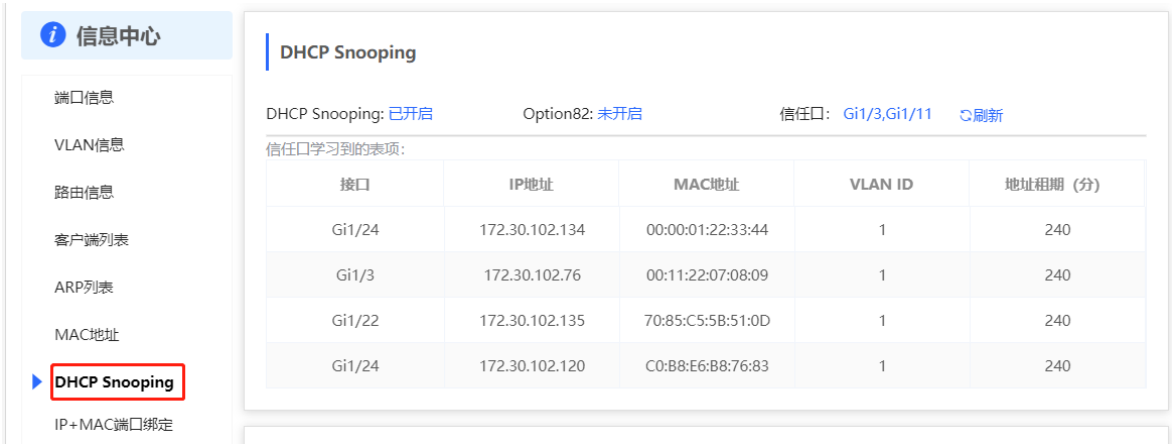
9.1.7 DHCP Snooping

【本机管理-页面向导】故障诊断>>信息中心>>DHCP Snooping

显示DHCP Snooping功能的当前配置以及信任口动态学习到的用户信息。

说明

如需修改DHCP Snooping相关配置，请参考7.1 DHCP Snooping章节。



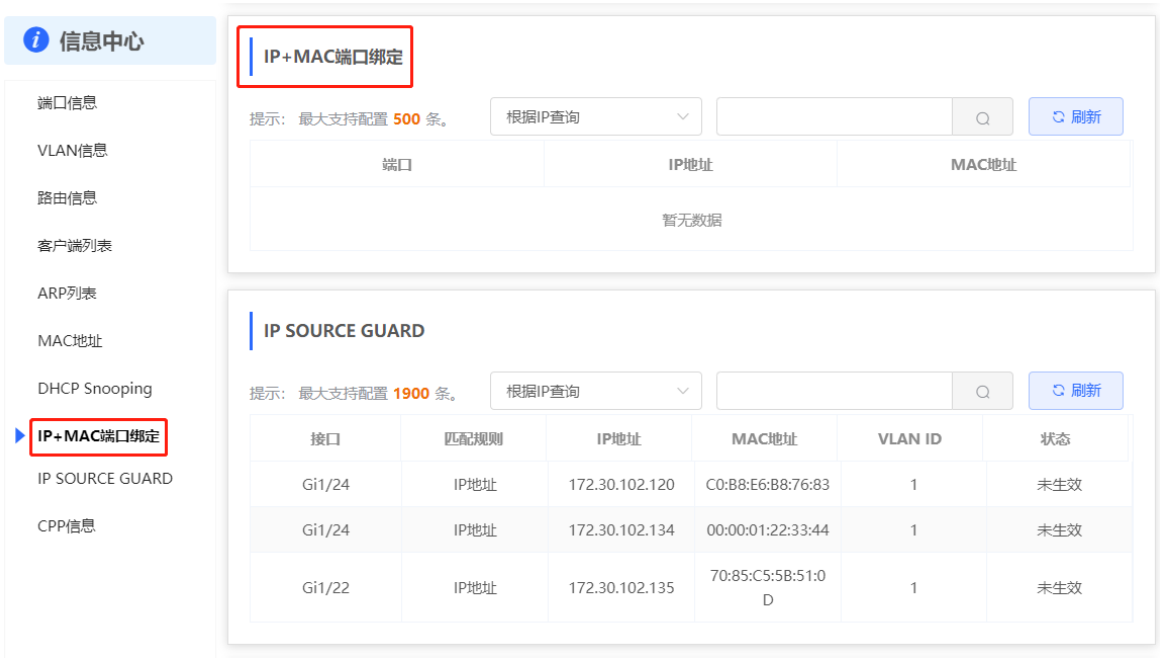
9.1.8 IP+MAC 端口绑定

【本机管理-页面向导】故障诊断>>信息中心>>IP+MAC端口绑定

显示配置的IP+MAC端口绑定表项。在指定端口上检查IP报文的源IP地址和源MAC地址是否符合所配置的IP地址和MAC地址，过滤不符合绑定关系的IP报文。

说明

如需添加或修改IP+MAC端口绑定关系，请参考7.5 IP+MAC端口绑定章节。



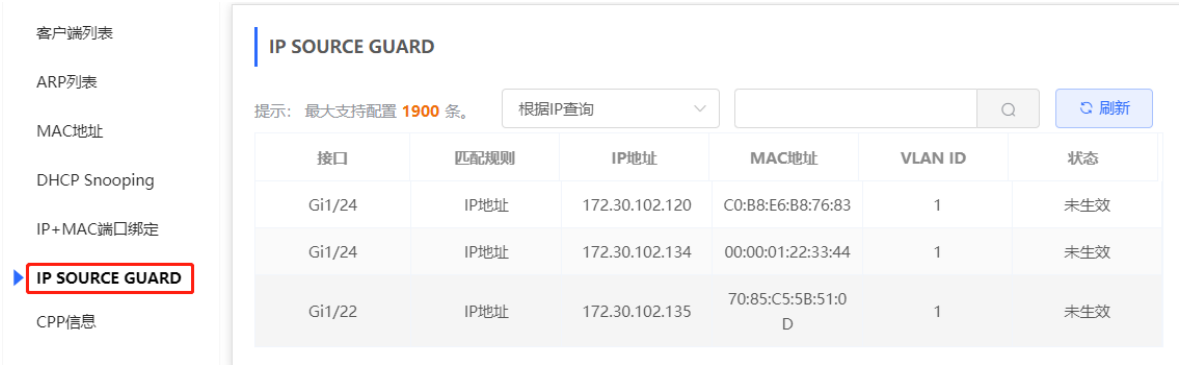
9.1.9 IP Source Guard

【本机管理-页面向导】故障诊断>>信息中心>>IP Source Guard

显示IP Source Guard功能的绑定列表，IP Source Guard功能将根据该列表检查来自非DHCP信任口的IP报文，过滤掉不在绑定列表中的IP报文。

说明

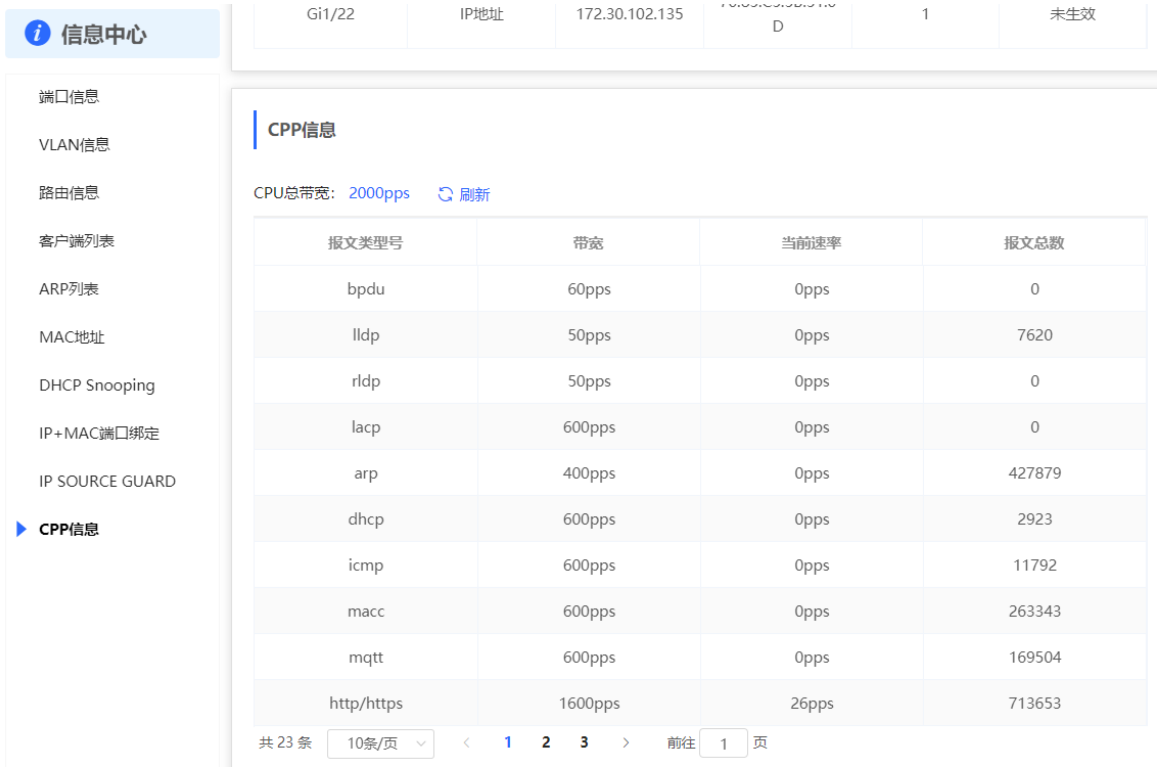
如需设置IP Source Guard功能，请参考7.5 IP+MAC端口绑定章节。



9.1.10 CPP 信息

【本机管理-页面向导】故障诊断>>信息中心>>CPP信息

显示当前CPU总带宽以及各报文类型的统计信息，包括带宽、当前速率和报文总数。



9.2 网络测试工具

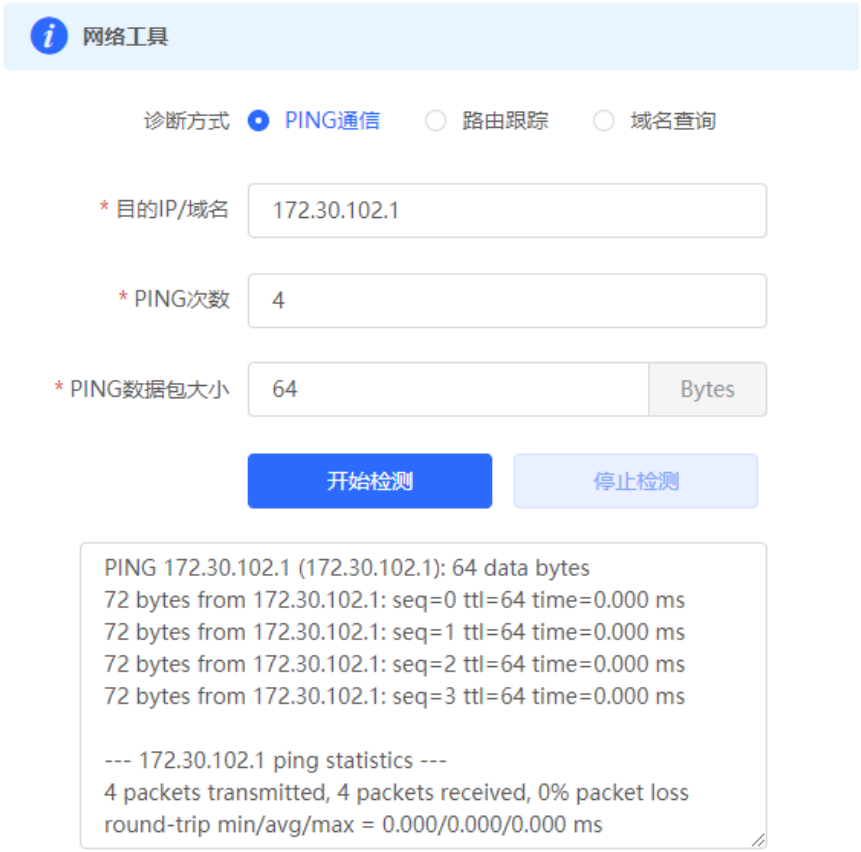
网络测试工具提供PING通信、路由跟踪和域名查询三种命令来检查网络状态。

9.2.1 PING 通信

【本机管理-页面向导】故障诊断>>网络工具

PING通信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。



9.2.2 路由跟踪

【本机管理-页面向导】故障诊断>>网络工具

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，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。

选择诊断方式为“路由跟踪”，输入目的 IP 地址或网址和路由跟踪所使用的最大 TTL 值，点击<开始检测>。

9.2.3 域名查询

【本机管理-页面向导】故障诊断>>网络工具

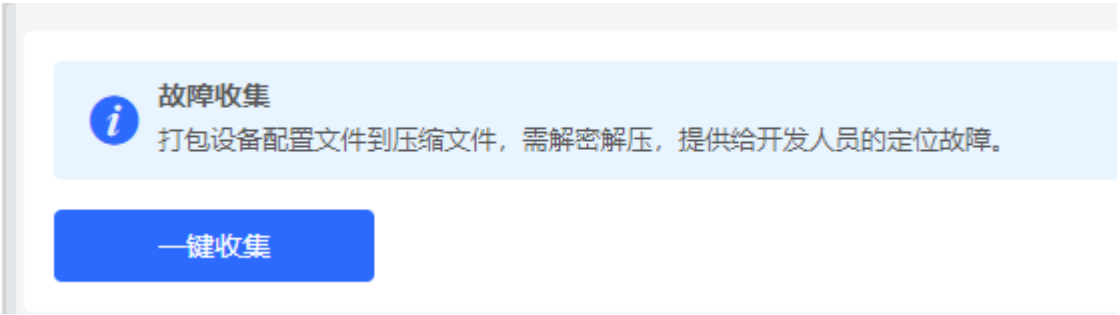
域名查询功能用来查询网络域名信息或诊断DNS服务器问题。若终端可以Ping通外网的IP地址但浏览器无法正常打开网页，可以尝试使用域名查询功能，检测域名解析是否正常。

选择诊断方式为“域名查询”，输入目的 IP 地址或网址，点击<开始检测>。

9.3 故障收集

【本机管理-页面向导】故障诊断>>故障收集

当设备出现未知原因的故障，可在本页面下一键收集故障信息。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。



9.4 线缆检测

【本机管理-页面向导】故障诊断>>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。

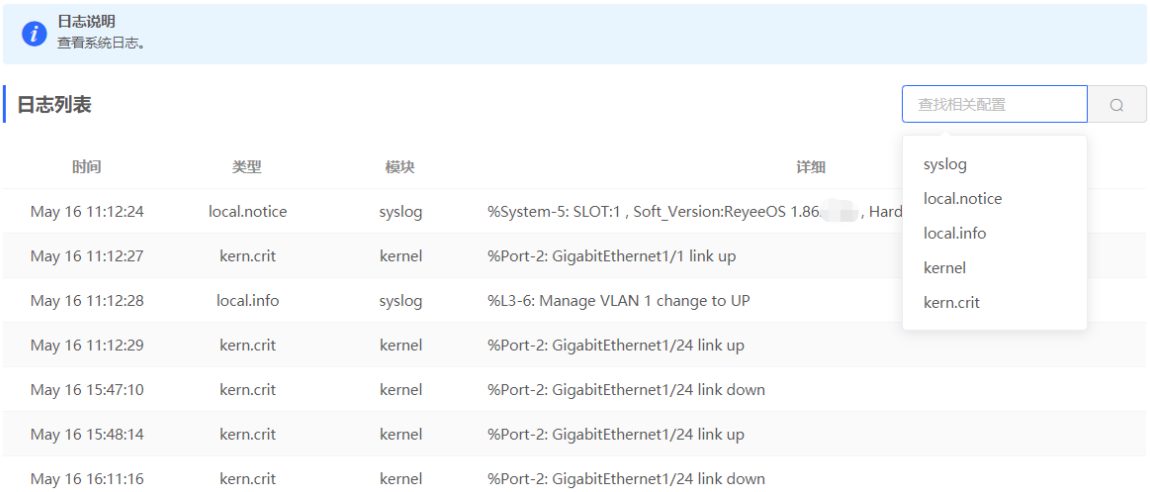
注意

- 光口不支持本功能。
- 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。

9.5 系统日志

【本机管理-页面向导】故障诊断>>系统日志

系统日志记录了设备在什么时间、什么模块发生了什么事件，主要用于管理员监控设备运行情况、分析网络情况和定位故障问题。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。



9.6 故障告警

【本机管理-页面向导】故障诊断>>故障告警

说明

对于组网中其他设备的告警信息，请在整网管理模式下的[整网管理]>>[故障告警]页面查看。

显示网络环境中可能存在的问题，以便于故障的预防与排查。可查看告警发生的时间、端口、告警影响以及处理建议，根据处理建议对设备故障进行修复。

默认关注所有类别的告警。点击告警项的<取消关注>按钮，可以取消关注该类告警，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。

注意

取消关注告警后，系统将不对该类故障进行告警提示，用户无法及时发现和处理故障，请谨慎操作。

表9-1 告警类型与产品支持情况

告警类型	说明	支持情况说明
DHCP地址池即将耗尽	设备作为DHCP Server，已分配的地址数即将达到地址池最大可分配地址数	仅适用于支持三层功能的设备 不支持三层功能的产品，如RG-NBS3100系列和RG-NBS3200系列交换机则不支持该类告警
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	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，有一台或一台以上设备的IP地址存在冲突	无
MAC地址表项满	二层的MAC地址表项即将达到产品的硬件容量上限	无
ARP表项满	网络中的ARP表项，超过设备的ARP表项容量	无
PoE进程未运行	设备PoE服务异常，无法供电	仅适用于支持PoE功能的NBS系列交换机 (设备型号带有“-P”标识)
PoE总功率过载	设备PoE总功率过载，无法为新接入的PD正	仅适用于支持PoE功能的NBS系列

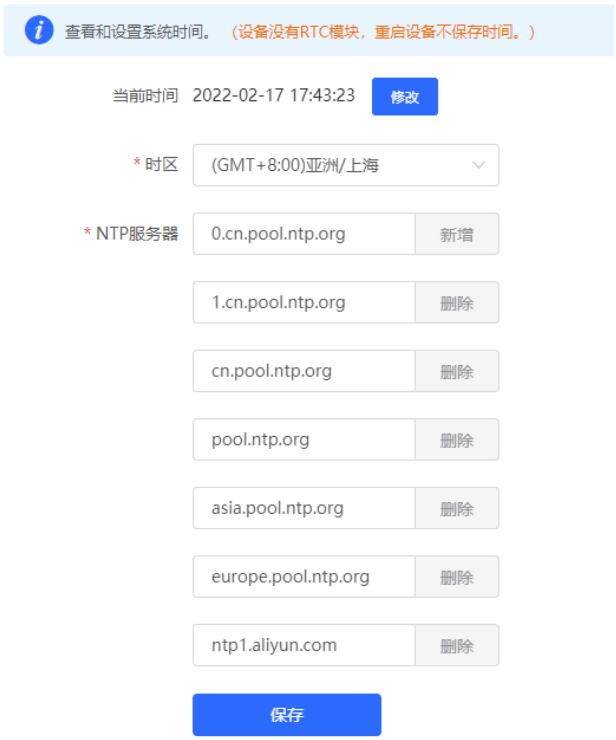
告警类型	说明	支持情况说明
	常供电	交换机 （设备型号带有“-P”标识)
设备有环路告警	局域网中的网络出现环路	无

10 系统设置

10.1 设置系统时间

【页面向导】系统管理/系统设置>> 系统时间

可查看当前系统时间，若时间错误，请检查并选择当地所在的时区。若时区正确时间仍有错误，可点击<修改>可手动设置。同时设备支持设置NTP服务器（Network Time Protocol，网络时间服务器），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。



修改时间时点击“当前时间”，将自动填入当前登录设备的系统时间。

10.2 设置 Web 登录密码

【页面向导】系统管理/系统设置>>（登录管理>>）登录密码

输入旧密码和新密码，保存后需使用新密码重新登录。

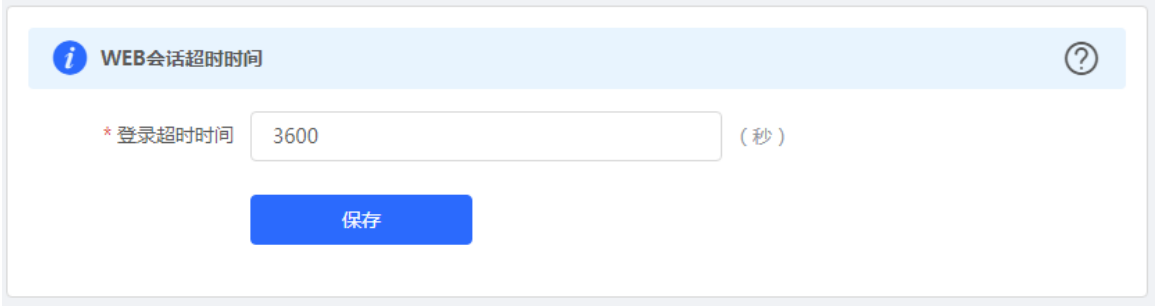
注意

当自组网发现处于开启状态，将同步修改网络中的所有设备的登录密码。

10.3 设置页面超时时间

【本机管理-页面向导】系统设置>> 登录管理>>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。



10.4 配置备份与导入

【页面向导】系统管理/系统设置>> 配置管理>> 备份与导入

配置备份：点击<备份>，将生成备份配置并下载导出的配置文件到本地。

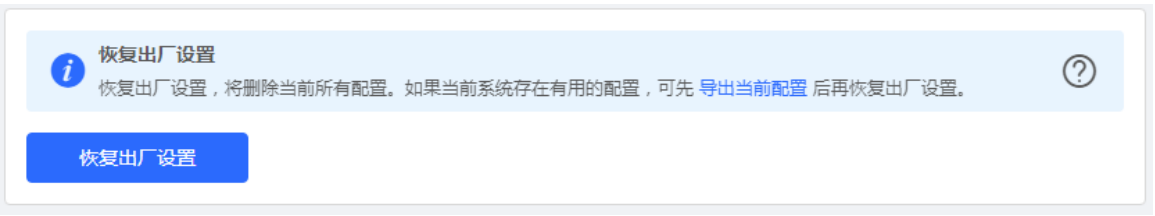
配置导入：点击<浏览>，在本地选择之前备份的配置文件，再点击<导入>，将文件所指定的配置应用到设备上。导入配置后设备将重启。

10.5 恢复出厂设置

10.5.1 本设备恢复出厂

【本机管理-页面向导】系统设置>> 配置管理>> 恢复出厂设置

点击<恢复出厂设置>按钮后确认，将恢复出厂的默认配置。



⚠ 注意

该操作将清空现有设定，并重启设备。如果当前系统存在有用的配置，可先导出当前配置（请参考10.4 配置备份与导入）后再恢复出厂设置。请谨慎操作。

10.5.2 整网设备恢复出厂

【整网管理-页面向导】系统管理>> 配置管理>> 恢复出厂设置

选择<整网设备>，并选择是否“解除用户帐号绑定”，点击<整网恢复出厂设置>，当前网络的所有设备都将恢复出厂设置。

注意

该操作将清空整网中所有设备的现有设定，并重启设备。请谨慎操作。

10.6 重启设备

10.6.1 重启本设备

【组网模式-整网管理-页面向导】系统管理>> 设备重启>> 系统重启

【独立模式-页面向导】系统设置>> 设备重启

选择<本设备>，点击<重启系统>，设备将重新启动。重启过程中，请勿刷新或关闭页面，当设备重启成功并且Web服务可用后，将自动跳转到登录页。

10.6.2 重启整网设备

【整网管理-页面向导】系统管理>> 设备重启>> 系统重启

选择<整网设备>，点击<整网重启系统>，重启当前网络中的所有设备。

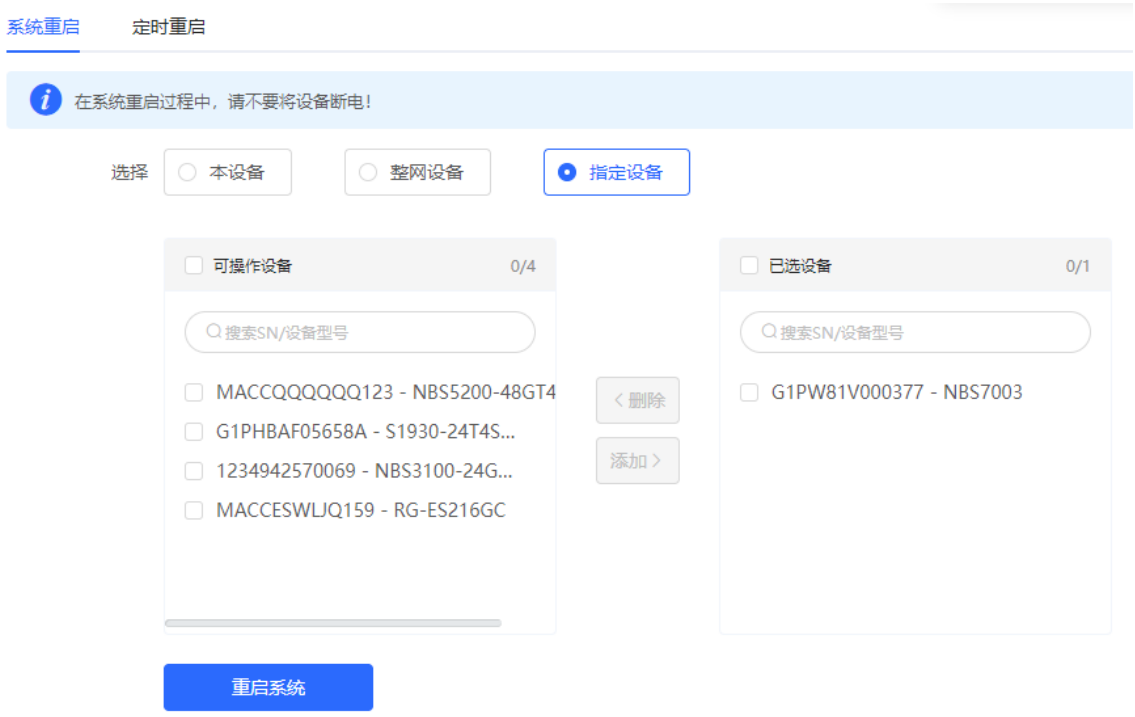
注意

整网重启需花费一定时间，请耐心等待。整网操作将对整个网络造成影响，请谨慎操作。

10.6.3 重启网络中的指定设备

【整网管理-页面向导】系统管理>> 设备重启>> 系统重启

选择<指定设备>，从“可操作设备”列表中选择要操作的设备，点击<添加>到右侧“已选设备”列表。点击<重启系统>，将重启“已选设备”列表中所指定的设备。



10.7 设置定时重启

请确认系统时间准确，关于系统时间的配置介绍请参考10.1 设置系统时间。防止在错误的时间重启导致断网。

【组网模式-整网管理-页面向导】系统管理>> 设备重启>> 定时重启

【独立模式-页面向导】系统设置>> 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。

注意

在整网管理模式下开启定时重启，当系统时间匹配到定时时间，整网设备都将重启，请谨慎设置。

10.8 系统升级

注意

- 建议在进行软件升级前进行配置备份。
- 版本更新将重启设备，升级过程中请不要刷新或关闭浏览器。

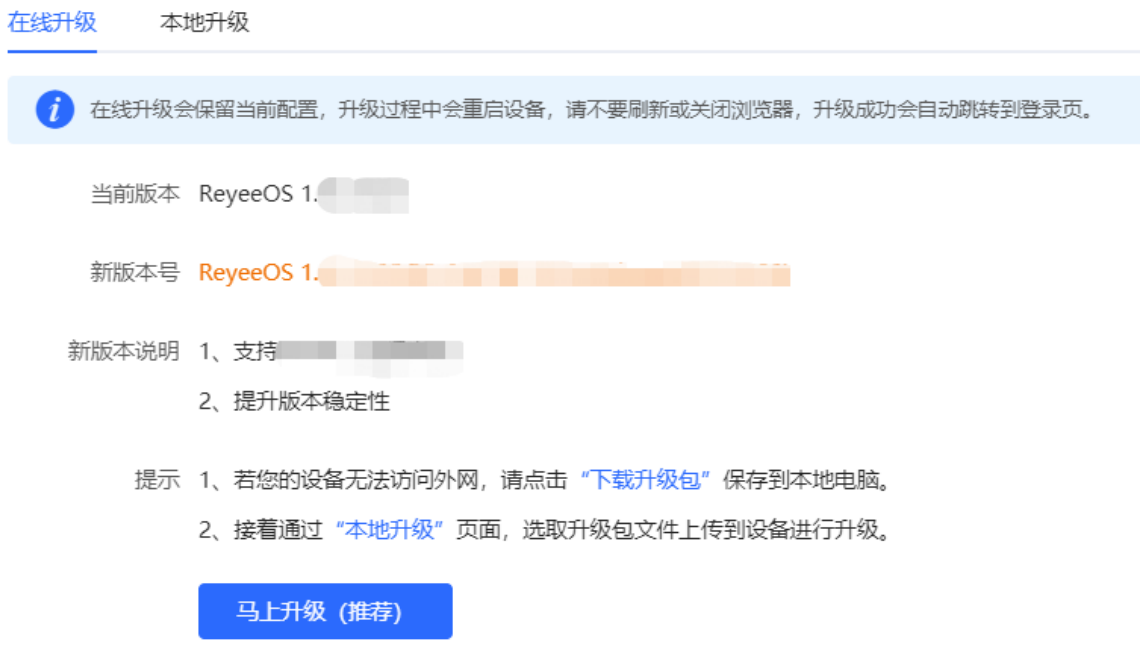
10.8.1 在线升级

【本机管理-页面向导】系统设置>>系统升级>>在线升级

显示当前系统版本并检测是否存在可更新版本。如果检测到版本更新可以点击<马上升级>按钮进行在线更新。若不具备在线升级的网络环境，可先点击“下载升级包”将升级安装包保存至本地，再进行本地升级。

说明

- 在线升级会保留当前配置。
- 请不要在升级过程中刷新页面或关闭浏览器，升级成功后将自动跳转到登录页。



10.8.2 本地升级

【本机管理-页面向导】系统设置>>系统升级>>本地升级

显示设备型号及当前软件版本。可以选择是否保留配置升级。点击<浏览>选择本地软件安装包，点击<上传>上传安装包并进行升级。

10.9 指示灯开关

【整网管理-页面向导】整网管理>> LED灯设置

点击开关按钮，控制下联AP的LED灯是否开启。点击<保存>使配置下发生效。

10.10 切换语言

【页面向导】Web页面右上角 中文

在下拉框中点击选择语言，将切换系统界面的语言。

11 整网无线设置

说明

- 若要对组网中的其他设备进行管理，需开启自组网发现功能（见3.1.1 2. 切换工作模式）。无线设置默认将同步到网络中所有无线设备上，可通过设置分组来限定配置的设备范围，详见11.1 设置AP分组。
- 设备本身不支持发射无线Wi-Fi信号，无线设置需同步至网络中的无线设备才能实际生效。

11.1 设置 AP 分组

11.1.1 功能介绍

开启自组网发现，用户可从整网视角对网络中的AP以分组为单位进行配置和管理。在设置AP前，先对AP进行分组。

说明

在设置无线网络时指定分组，则对应配置将在指定分组中的无线设备上生效。

11.1.2 配置步骤

【整网管理-页面向导】设备管理>> AP

(1) 查看当前网络中所有的AP设备的信息，包括基本信息、射频信息和型号信息。点击序列号可对单台设备进行设置。

(2) 点击<展开分组>，列表左侧会出现当前所有分组的信息。点击 创建新分组，最多支持添加8个分组。对于已创建的分组，可以点击 修改分组名称，点击 删除分组。默认组不可修改名称与删除。

(3) 点击左侧分组名称，将显示该分组下的所有AP。一台AP只能属于一个分组。默认所有AP都属于默认组。勾选列表中的表项，点击<迁移分组>，可将选中设备迁至指定分组。迁移分组后，设备将应用该分组下的配置。点击<删除离线设备>可将不在线的设备从列表中移除。

11.2 设置 Wi-Fi

【整网管理-页面向导】整网管理>> 无线设置>> 无线网络

输入Wi-Fi名称和Wi-Fi密码，选择Wi-Fi信号的使用频段，点击<保存>。

点击展开高级设置，可设置更多Wi-Fi特性。

注意

修改配置会重启无线配置，可能导致当前连接的终端掉线。请谨慎操作。

表11-1 无线网络配置信息描述表

参数	说明
Wi-Fi名称	无线终端搜索无线网络时显示的名称
应用频段	设置Wi-Fi信号的使用频段，支持2.4GHz和5GHz频段。5GHz频段相较于2.4GHz频段网络传输速率更快，受干扰更小，不过在信号覆盖范围和穿墙方面通常不如2.4GHz频段，可根据实际需求选择信号频段。默认Wi-Fi频段为2.4GHz+5GHz，同时在2.4GHz和5GHz频段放出Wi-Fi信号
加密类型	无线网络连接时的加密方式，有三种加密方式可选： 不加密：无需密码即可连接上Wi-Fi WPA-PSK/WPA2-PSK：使用WPA/WPA2加密方式 WPA_WPA2-PSK（推荐）：使用WPA2-PSK/WPA-PSK加密方式
Wi-Fi密码	连接无线网络的密码，由8~16个字符组成
选择时段	Wi-Fi开启的时段，设置后，其他时段用户无法接入Wi-Fi上网

参数	说明
VLAN	设置Wi-Fi信号所属VLAN，可在当前已有VLAN中选择，或选择“去添加新VLAN”，跳转至[LAN设置]页面添加VLAN
隐藏Wi-Fi	开启隐藏Wi-Fi功能能够防止Wi-Fi被非法用户接入，增强安全性。但手机或电脑将搜索不到Wi-Fi名称，必须手动输入正确的名称和密码进行连接。开启前需记录当前的Wi-Fi名称，防止隐藏后无法连接
用户隔离	开启后，接入该Wi-Fi的终端之间相互隔离，终端用户不能与同一AP下的其他用户（同一个网段）相互访问，以增强安全性
5G优先	开启后支持5G的终端设备优先选择5G Wi-Fi。Wi-Fi开启双频合一（即应用频段为“2.4G+5G”）才能开启本功能
竞速模式	开启后优先发送游戏报文，为游戏提供更稳定的无线网络
三层漫游	开启后终端在同一个Wi-Fi下IP保持不变，提升用户跨VLAN场景下的漫游体验
Wi-Fi6	开启后无线用户能够体验更快的上网速度，优化上网体验。 本配置只对支持802.11ax协议的AP和路由器生效。同时接入终端也需支持802.11ax协议，才能体验Wi-Fi 6带来的高速上网体验。若终端不支持Wi-Fi 6特性，可关闭本功能

11.3 设置访客 Wi-Fi

【整网管理-页面向导】整网管理>> 无线设置>> 访客Wi-Fi

访客Wi-Fi是为访客提供的无线网络，默认关闭。访客Wi-Fi默认开启“用户隔离”且不可关闭，即接入的用户之间相互隔离，只能连接Wi-Fi上网，无法互访，以此提高安全性。访客网络支持配置生效时段，时间到后，访客网络会变为关闭状态。

点击开启“访客Wi-Fi”开关，设置访客Wi-Fi的名称和密码。点击展开高级设置，可配置访客Wi-Fi的生效时段与更多Wi-Fi属性（配置项详情请参考11.2 设置Wi-Fi）。保存设置后，访客可通过Wi-Fi名称和密码连接无线网络上网。

11.4 添加 Wi-Fi

【整网管理-页面向导】整网管理>> 无线设置>> Wi-Fi列表

点击<添加>，输入Wi-Fi名称和密码，点击<确定>创建Wi-Fi。点击展开高级设置，可以配置更多Wi-Fi属性。可参考11.2 进行设置。添加Wi-Fi后，终端设备可以搜索到新建的Wi-Fi，Wi-Fi列表显示添加的Wi-Fi信息。

11.5 健康模式

【整网管理-页面向导】整网管理>> 无线设置>> 健康模式

点击开启健康模式，支持选择生效时段。

开启健康模式后，无线设备将在生效时段里降低无线发射功率，Wi-Fi覆盖面积减小。可能导致信号弱，网络卡顿问题。建议保持关闭或将生效时段设置为无人使用网络的时间段。

11.6 射频设置

【整网管理-页面向导】整网管理>> 射频设置

无线设备在开机时能够检测周围无线环境并选择合适的配置。但无法避免无线环境变化而引起的网络卡顿。用户可以分析AP和路由器周围的无线环境，手动选择合适的参数。

注意

修改配置会重启无线配置，可能导致当前连接的终端掉线。请谨慎操作。

表11-2 射频配置信息描述表

参数	说明
国家码	各国规定的Wi-Fi信道有可能不同。为防止终端搜索不到Wi-Fi，请选择实际所在的国家或地区

参数	说明
2.4G/5G频宽	频宽小网络较稳定，频宽大易受干扰。若干扰较严重，选择较低的频宽能够一定程度上避免网络卡顿。2.4GHz频段支持20MHz和40MHz的频宽，5GHz频段支持20MHz、40MHz和80MHz的频宽。 默认为“自动”，表示自动根据环境选择频宽
最大用户数	大量用户接入AP或路由器上，可能导致无线网络性能下降，影响用户上网体验。设置最大用户数后，当接入用户达到阈值，将禁止新用户接入。若接入终端带宽需求较高，可调低最大用户数。无特殊情况建议保持默认
踢下线阈值	在存在多个Wi-Fi信号的情况下，设置踢下线阈值可一定程度上改善无线信号质量。当终端距离无线设备较远，终端用户的无线信号强度低于踢下线阈值时，将断开Wi-Fi连接，迫使终端重新选择距离较近的无线信号。 但踢下线阈值越高，终端越容易被踢下线，为避免影响正常终端上网，建议保持关闭或小于-75dBm

说明

- 可选无线信道与国家码有关，请正确选择所在的国家或地区的国家码。
- 信道、功率和漫游灵敏度不支持全局设置，需要在对应设备上进行单独设置。

11.7 设置无线黑名单或白名单

11.7.1 功能简介

支持设置基于所有Wi-Fi的全局黑白名单或者基于SSID的无线黑白名单。黑白名单支持匹配终端设备的MAC地址前缀（OUI）。

无线黑名单：名单中的设备将被禁止上网，未加入名单的设备不限制。

无线白名单：只有名单中的设备能够上网，未加入名单的设备都禁止。

注意

白名单列表为空时，无线白名单不生效，即所有MAC均可接入。

11.7.2 全局黑白名单

【整网管理-页面向导】终端管理>>黑白名单>>全局黑白名单

选择黑/白名单模式，点击<添加>设置黑/白名单列表。在弹出的对话框中输入想要拉黑或加入白名单的设备的MAC地址和备注，点击<确定>保存。MAC地址输入框将弹出已连接的终端信息，点击可自动填入。黑名单模式下，将断开并禁止该终端设备的连接。全局黑白名单将在网络中所有设备的所有Wi-Fi上生效。

黑名单模式下点击<删除>，对应终端设备即可重新连接Wi-Fi；白名单模式下点击<删除>，且删除后白名单列表不为空，则会断开并禁止对应终端设备连接Wi-Fi。

11.7.3 基于 SSID 黑白名单

【整网管理-页面向导】终端管理>>黑白名单>>基于SSID黑白名单

在左侧列表选择设置的Wi-Fi，并选择黑/白名单模式，点击<添加>设置黑/白名单列表。基于SSID的黑白名单将限制指定Wi-Fi下的接入用户。

11.8 一键优化无线网络

【整网管理-页面向导】整网管理>>无线优化

在“无线优化”页签，勾选“我已阅读以上注意事项”，点击<无线优化>，将在组网环境下对无线网络进行自动优化。支持设置定时网优，在指定时间对网络进行优化。建议定时网优时间设置为凌晨或无人使用网络的时间段。

注意

优化期间可能造成终端掉线，且优化开始后无法回退配置至优化前，请谨慎操作。

优化开始后，请耐心等待优化完成。优化完成后，点击<取消优化>可以将优化的射频参数恢复为默认值。点击<查看详情>或点击<优化记录>页签，可查看最近一次的优化记录详情。

11.9 开启易联功能

【整网管理-页面向导】整网管理>> 易联设置

开启易联功能后，支持易联的设备可以通过配对组成Mesh网络。设备间可以通过Mesh按键自动搜索周围的新路由器并自动配对，或登录路由器管理页面搜索选择新路由器进行配对。默认开启。

11.10 设置 AP 有线口

注意

本配置仅对带有线LAN口的AP生效。

【整网管理-页面向导】整网管理>> AP有线口

输入VLAN ID，点击<保存>设置AP有线口所属的VLAN。VLAN ID为空表示有线口与WAN口同VLAN。

组网模式下，AP有线口配置将应用于当前网络中所有带有线LAN口的AP。其中，优先生效“AP有线口配置列表”中应用到AP的配置，点击<添加>可新增AP有线口配置；“AP有线口配置列表”中未应用到的AP，将生效AP有线口默认配置。

12 常见问题

12.1 无法登录 Web 管理系统

(1) 确认网线已正常连接到了设备端口，对应的指示灯闪烁或者常亮。

(2) 访问Web管理系统前，建议将PC设置为使用静态IP地址，并设置计算机的IP与设备IP在一网段（设备默认IP为10.44.77.200，子网掩码为255。255.255.0），例如设置计算机的IP地址为10.44.77.100，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) 若完成上述步骤后仍无法登录到设备管理界面，请将设备恢复为出厂配置。

12.2 忘记密码和恢复出厂配置

若忘记登录密码，可在设备接通电源的情况下，长按面板上的Reset键5秒以上，待系统指示灯出现闪烁后松开Reset键，设备将还原为出厂设置。设备重新启动可使用默认管理IP（10.44.77.200）登录设备Web，并根据提示信息选择是否恢复备份配置。

选择<恢复备份>：配置将恢复至备份状态，仅登录密码恢复至默认密码；

选择<删除备份>：恢复出厂配置，即密码和配置都会被清除。