SUNDRAY

安视交换机胖模式

用户手册

SUNDRAY
信锐技术

目录

声明 9

前言 10

本手册各章节内容如下： 10

本书约定 10

图形界面格式约定 10

各类标志 11

技术支持 11

致谢 12

第 1 章 安视交换机基本配置 1

1.1. 交换机登录 1

1.2. 配置管理地址 1

1.3. 配置接口 VLAN 3

第 2 章 功能说明 5

2.1. 系统状态 5

2.1.1. 运行状态 5

2.1.1.1. 系统信息 5

2.1.1.2. 设备信息 5

2.1.1.3. 端口状态 6

2.1.2. 地址表 6

2.1.2.1. MAC 地址表 6

2.1.2.2. ARP 地址表 7

2.1.2.3. 组播地址表 7

2.1.3. 路由状态 8

2.1.4. DHCP 状态 8

2.2. 对象定义 8

2.2.1. 时间计划 8

2.3. 端口管理 9

2.3.1. 端口列表 9

2.3.1.1. 编辑单个端口 10

2.3.1.2. 批量编辑端口 12

2.3.1.3. Mgmt 口配置 13

2.3.2. 端口镜像 13

2.4. 通信配置 14

2.4.1. VLAN 接口 14

2.4.2. DNS 地址 15

2.4.3. Loopback 地址 16

2.4.4. DHCP 服务 16

2.4.4.1. DHCP 策略 17

2.4.4.2. 地址池管理 17

2.4.5. ARP 地址表配置 18

2.5. 以太网管理 19

2.5.1. 链路聚合 19

2.5.2. 防环路配置 19

2.5.2.1. 生成树 20

2.5.2.2. 环路检测 20

2.5.3. Voice VLAN 21

2.5.4. MAC-VLAN 映射 22

2.5.5. MAC 地址表配置 23

2.6. 路由管理 24

2.6.1. 静态路由 24

2.6.2. 策略路由 25

2.6.3. RIP 配置 26

2.6.4. OSPF 配置 26

2.6.5. 路由优先级 27

2.7. 组播管理 28

2.7.1. IGMP Snooping 28

2.8. 流控与安全 29

2.8.1. ACL 策略 29

2.8.2. QoS 配置 30

2.8.2.1. 流量管理 30

2.8.2.2. 流量整形 31

2.8.2.3. 优先级映射 32

2.8.2.4. 拥塞管理 32

2.8.3. ARP 安全 33

2.8.3.1. ARP 泛洪防御 34

2.8.3.2. ARP 欺骗防御 35

2.8.4. DHCP 安全 37

2.8.4.1. DHCP 泛洪防御 37

2.8.4.2. DHCP 欺骗防御 39

2.8.5. 端口防护 39

2.8.5.1. 端口隔离 39

2.8.5.2. MAC 表项限制 40

2.9. 高可用性 41

2.9.1. 链路高可用 41

2.9.1.1. 备份链路 41

2.9.1.2. 上行链路监控 42

2.9.2. 堆叠 43

2.9.3. M-LAG 组 45

2.9.4. VRRP 策略 46

2.9.5. 链路检测 50

2.9.5.1. PING 检测 50

2.9.5.2. BFD 检测 51

2.10. 系统管理 53

2.10.1. 系统配置 53

2.10.1.1. 系统选项 5 3

2.10.1.2. 日期时间 5 4

2.10.2. 管理员账号 5 5

2.10.2.1. 管理员账号 5 5

2.10.2.2. 普通账号 5 5

2.10.3. SNMP 配置 5 6

2.10.3.1. SNMP 5 6

2.10.3.2. SNMP Traps 5 7

2.11. 系统管理 5 8

2.11.1. 系统日志 5 8

2.11.1.1. 操作日志 5 8

2.11.1.2. 安全日志 5 9

2.11.1.3. 远程日志 5 9

2.11.2. 端口诊断 6 0

2.11.3. 胖瘦切换 6 0

2.11.4. 固件升级 6 1

2.11.5. 调试选项 6 2

2.11.6. 重启设备 6 3

2.11.7. 备份恢复 6 3

2.11.8. 排障工具箱 6 4

2.11.8.1. 即时 Ping 检测 6 4

2.11.8.2. 持续 Ping 检测 6 5

2.11.9. webConsole 6 6

第 3 章 安视交换机常见问题排查 6 7

3.1. 端口镜像配置 6 7

3.2. Console 口命令查看相关配置 6 8

3.3. 使用 AP 诊断工具进行胖瘦切换 6 9

3.3.1. 下载 AP 诊断工具 6 9

3.3.2. 使用诊断工具扫描 6 9

3.4. Console 口进行胖瘦切换 7 2

3.5. Console 口恢复出厂设置 7 3

第 4 章 附录 7 4

4.1. SUNDRAY 设备升级系统的使用 7 4

声明

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系信锐网科技术有限公司客户服务部。

前言

本手册各章节内容如下：

第 1 部分 安视交换机的使用，如何登录配置界面等。

第 2 部分 安视交换机的功能说明及使用。

本手册以 SW3.3 版本的安视交换机为例进行配置。由于各型号产品硬件和软件规格存在一定差异，所有涉及产品规格的问题需要和信锐网科技术有限公司联系确认。

本书约定

图形界面格式约定

文字描述	代替符号	举例
按钮	边框+阴影+底纹	“确定”按钮可简化为确定
菜单项	『』or 【】	菜单项“系统设置”可简化为『系统设置』或【】

连续选择菜单项及子菜单项	→	选择【系统设置】→【接口配置】
下拉框、单选框、复选框选项	[ ]	复选框选项“启用用户”可简化为[启用用户]
窗口名	【】	如点击弹出【新增用户】窗口
提示信息	“”	提示框中显示“保存配置成功，配置已修改，需要重启 DLAN 服务才能生效，是否立即重启该服务?”

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：

 **小心、注意：**提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。

 **警告：**该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。

 **说明、提示、窍门：**对操作内容的描述进行必要的补充和说明。

技术支持

用户支持邮箱： support@sundray.com

技术支持热线电话： 400-878-3389（手机、固话均可拨打）

公司网址： www.sundray.com.cn

致谢

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢。

第 1 章 安视交换机基本配置

1.1. 交换机登录

胖模式的安视交换机，MGMT 管理口的默认 IP 地址为 192.168.0.1/24，非 MGMT 口的默认 IP 地址为 192.168.1.10/24，电脑连接 MGMT 管理口和非 MGMT 都可以登录智能交换机。注意：部分安视交换机没有 MGMT 管理口的，通过 192.168.1.10/24 地址登录。

1、如果电脑直连智能交换机的 MGMT 口，则配置 192.168.0.0/24 网段地址（不要配置 192.168.0.1），在浏览器中输入 https://192.168.0.1 即可访问到智能交换机 web 登录页面；

2、如果电脑直连智能交换机的非 MGMT 口，则配置 192.168.1.0/24 网段地址（不要配置 192.168.1.10），在浏览器中输入 https://192.168.1.10 即可访问到智能交换机登录页面。

智能交换机默认用户名和密码都为 admin。

1.2. 配置管理地址

【功能说明】

交换机默认的管理地址在 VLAN 1 上，为了方便日常运维，需要对管理地址进行配置和修改。

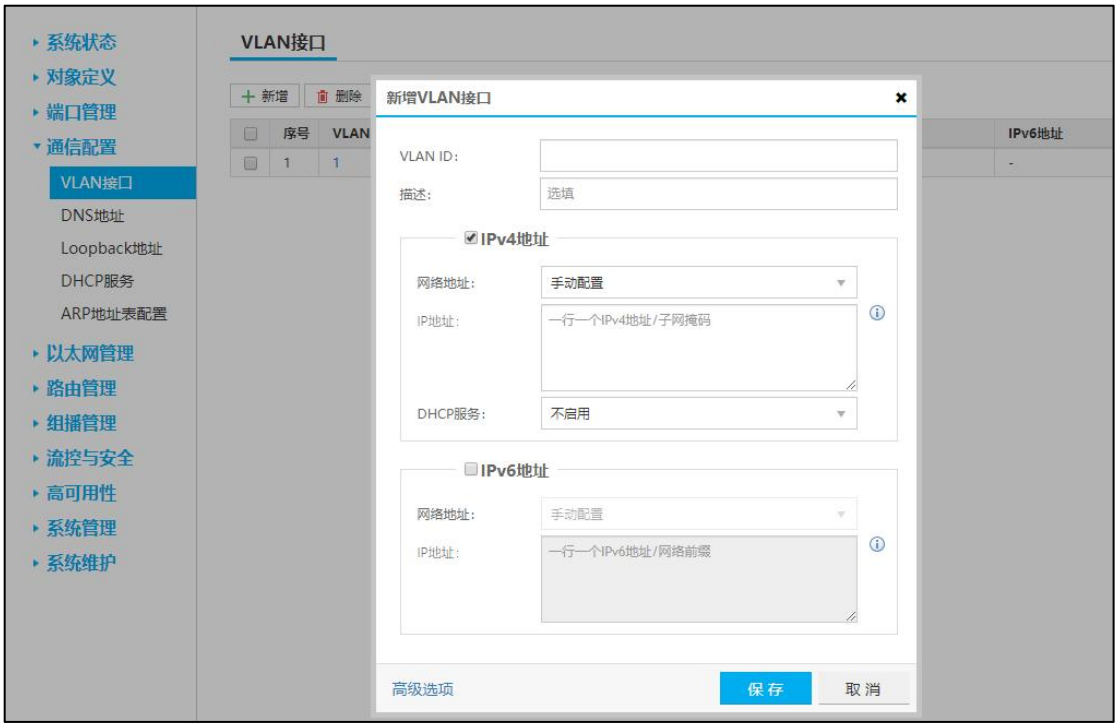
【注意事项】

所有场景都需要部署交换机管理网络以便于管理智能交换机。

【操作步骤】

进入『通信配置』→『VLAN 接口』页面，点击新增。

在弹出的窗口填入管理 VLAN，选择手动配置 IP 同时填入管理 IP，点击保存。



1.3. 配置接口 VLAN

【功能说明】

修改交换机接口 VLAN。

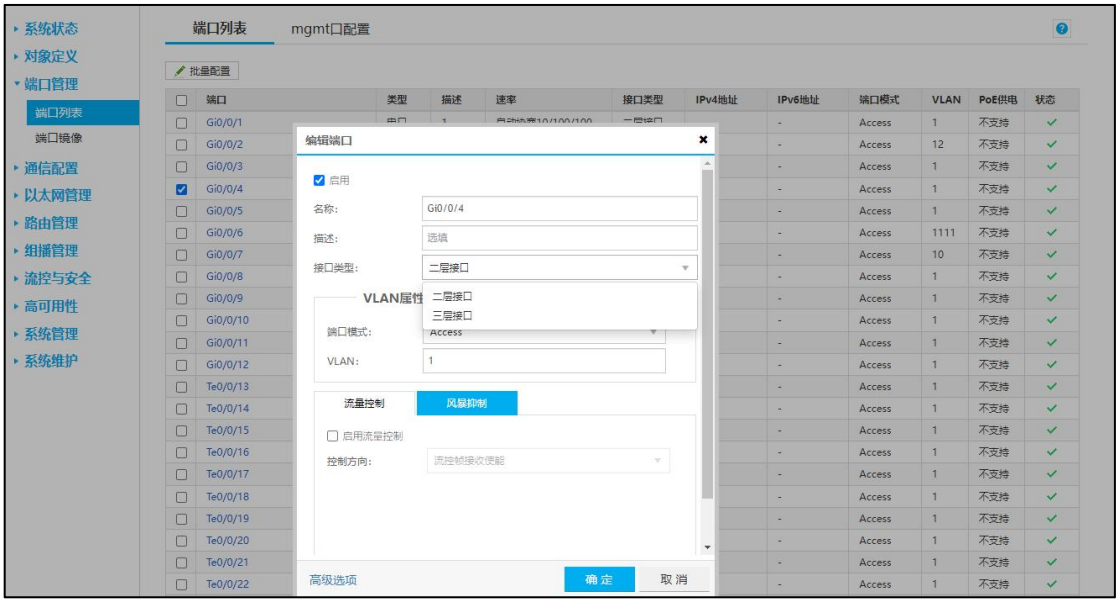
【注意事项】

无

【操作步骤】

进入『端口管理』→『端口列表』页面，点击端口名称。

在弹出的页签中可进行接口类型切换与 VLAN 修改。

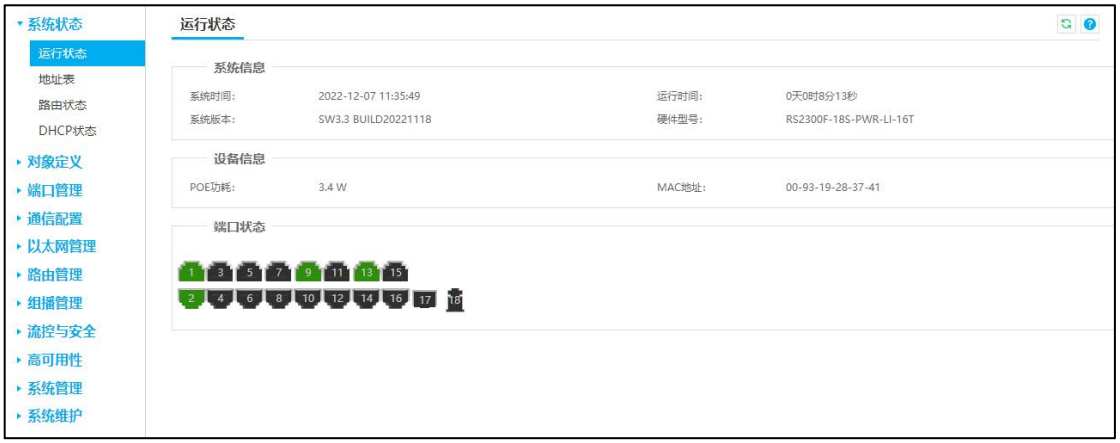


第 2 章 功能说明

2.1. 系统状态

2.1.1. 运行状态

『运行状态』可以查看设备运行的基本信息，包括系统信息、设备信息、端口状态等信息。



2.1.1.1. 系统信息

显示当前系统时间，已运行的时间、系统版本及硬件型号。

2.1.1.2. 设备信息

显示当前交换机的 MAC 地址及支持 PoE 的交换机的 PoE 功耗信息。

2.1.1.3. 端口状态

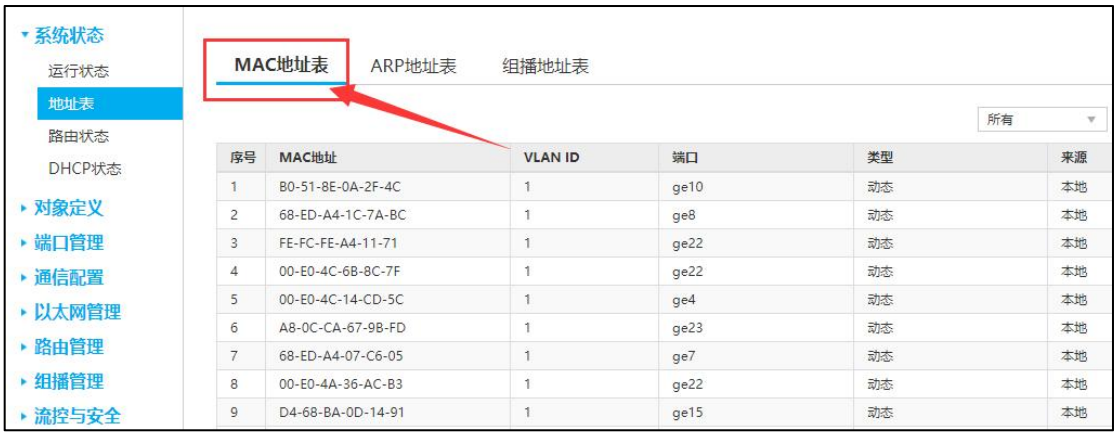
显示当前系统每个端口状态及端口信息。

2.1.2. 地址表

『地址表』可以查看 MAC 地址表、ARP 地址表、组播地址表、组播报文统计等信息。

2.1.2.1. MAC 地址表

交换机内有一张 MAC 地址表，用于指导单播报文的数据转发。MAC 地址表记录了 MAC 地址、所属 VLAN ID 和接口之间的对应关系。转发数据时，交换机根据单播数据的目的 MAC 地址查找地址表，如果在 MAC 地址表中查不到相应的条目，则把该单播数据广播，即向接收端口所在 VLAN 内的所有端口转发；如果查找到了对应的条目，交换机就把该单播数据向 MAC 地址表中对应的端口转发。



2.1.2.2. ARP 地址表

交换机内有一张 ARP 地址表，用于记录主机的 IP 地址与 MAC 地址的对应关系。主要负责根据主机的 IP 地址解析 MAC 地址。

2.1.2.3. 组播地址表

交换机内有一张组播地址表，用于指导组播数据转发。组播地址表记录了 MAC 地址、所属 VLAN ID 和接口之间的对应关系。转发数据时，交换机根据组播数据的目的组播地址查找组播地址表，如果在组播地址表中查不到相应的条目，则把该组播数据广播，即向接收端口所在 VLAN 内的所有端口转发；如果能查找到对应的条目，则目的地址应该是一组端口列表，于是交换机把这个组播数据复制成多份，每份转发到一个端口，从而完成组播数据的交换。

2.1.3. 路由状态

『路由状态』显示当前系统已运行的路由信息、OSPF 状态与 RIP 状态。

2.1.4. DHCP 状态

该页面可以观察到 NAC 作为 DHCP 服务器时，对外分配 IP 地址的分配情况：包括了 IP 地址、计算机名、MAC 地址、获取租约时间，租约过期时间：

2.2. 对象定义

2.2.1. 时间计划

缺省情况下，ACL 策略一旦被应用到业务模块后是一直生效的。通过定义生效时间段，

并将时间段与 ACL 规则关联，可以使 ACL 规则在某段时间计划范围内生效，从而达到使用基于时间的 ACL 策略来控制业务的目的。

默认的时间计划有全天，上班时间与下班时间，用户可以新增自定义单次时间计划和循环时间计划。

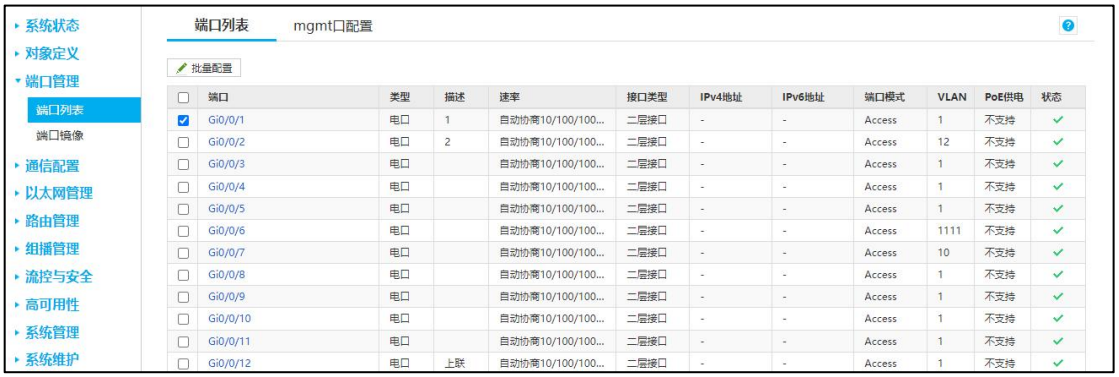
单次时间计划用于创建一次性的，无重复的时间计划，例如：元旦假期：2022 年 1 月 1 日 00:00 至 2022 年 1 月 3 日 23:30。

循环时间计划适用于以周为单位，重复性的时间计划，例如：上班时间：星期一至星期五 09:00-12:00；星期一至星期五 14:00-18:00。

2.3. 端口管理

2.3.1. 端口列表

配置交换机物理口的属性，包括接口名称，描述，协商速率以及 VLAN 属性。交换机支持 PoE 供电的话，还可以配置物理接口的 PoE 属性。



2.3.1.1. 编辑单个端口

点击单个端口名称，在弹出的页签中可进行接口类型切换与 VLAN 等配置的修改。

PoE 属性

用于开启或关闭该端口的 PoE 功能。

流量控制

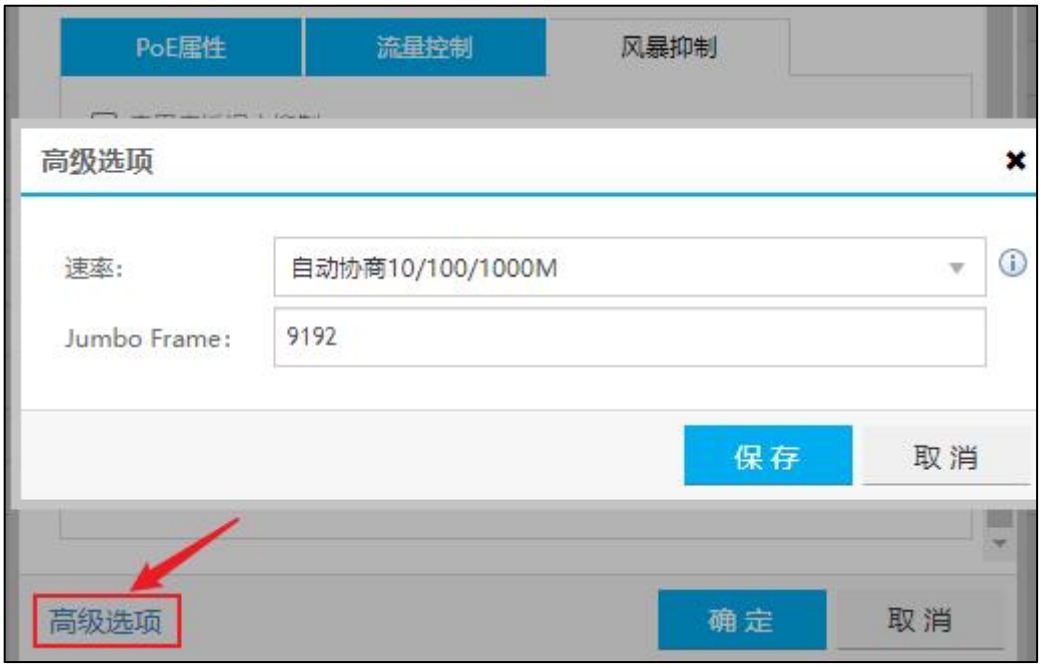
网络拥塞易引发丢包，流量控制是一种防止出现丢包现象的技术。配置流量控制功能后，如果本端设备发生拥塞，它将向对端设备发送消息，通知对端设备暂时停止发送报文。对端设备在接收到该消息后，无论其接口工作速率高低，都将暂时停止向本端发送报文，避免拥塞。

风暴抑制

为了限制进入接口的广播、未知组播或未知单播类型报文的速率，避免设备受到大的流量冲击，可以在该接口上配置对应报文类型的风暴控制功能。

高级选项

用于调整端口速率以及 Jumbo Frame（调整范围 1518-9192）。



2.3.1.2. 批量编辑端口

勾选需要批量修改的端口，然后点击批量编辑进行配置，即可对选中的端口进行批量处理，可编辑的配置同单个端口配置。

2.3.1.3. Mgmt 口配置

交换机的 MGMT 口配置，部分型号设备支持配置单独的网口以便于管理设备。

2.3.2. 端口镜像

端口镜像是指设备复制一份从镜像端口流经的报文，并将此报文传送到指定的观察端口进行分析和监控。

模式

常用的端口镜像模式包括入方向、出方向、出方向和入方向三种。入方向是指端口收到的报文，出方向是指端口发出的报文，入方向和出方向是指流经端口的所有报文。

源端口

源端口是镜像端口，即报文流经的端口。一条策略可以选择多个源端口。

目的端口

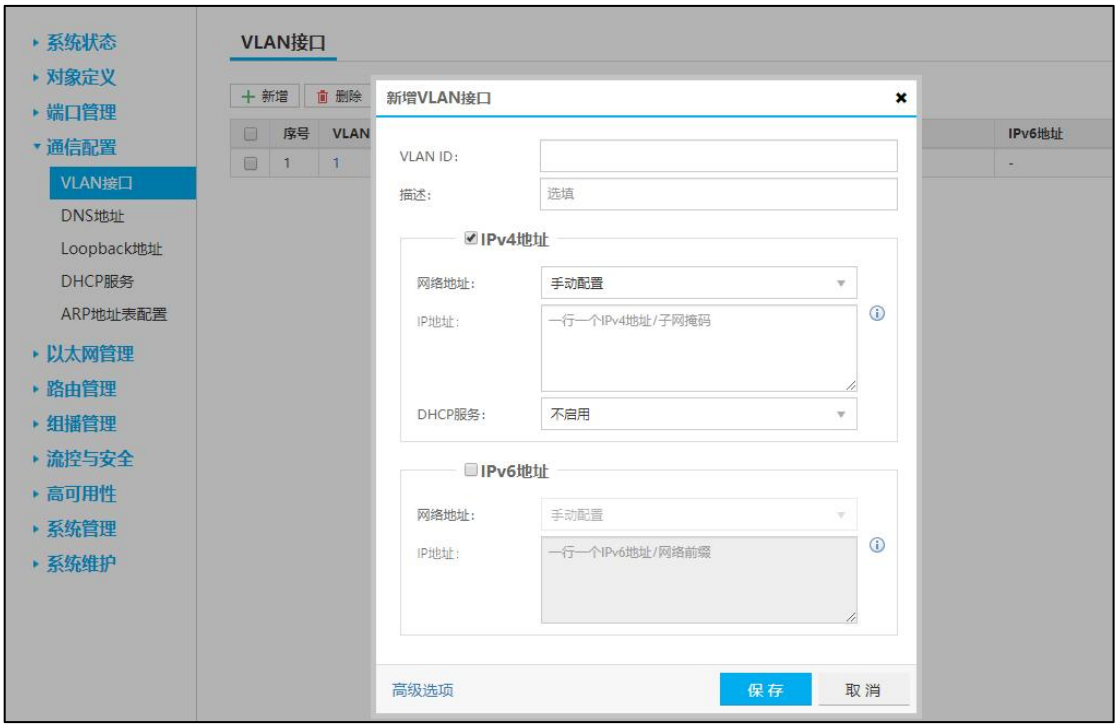
目的端口是观察端口，即报文重新发送至的指定端口。可以选择单个端口或者聚合口。目的端口仅能选择一个。

2.4. 通信配置

2.4.1. VLAN 接口

VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的 LAN 在逻辑上划分成多个广播域的通信技术。VLAN 内的主机间可以直接通信，而 VLAN 间不能直接互通，从而将广播报文限制在一个 VLAN 内。

通过配置 VLANIF 接口、子接口方式可以实现 VLAN 间的通信。



2.4.2. DNS 地址

域名系统 DNS（Domain Name System）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换服务。

域名系统解决了 IP 地址信息不便于记忆这一问题。用户进行访问网络主机操作时，可以直接使用便于记忆的、有意义的域名，由网络中的域名解析服务器将域名解析为正确的

IP 地址。

如果启用了 DNS 代理，客户端的 DNS 服务器可以指向交换机。交换机接收到 DNS 请求后，会转发到这里设置的外部 DNS 服务器解析。

2.4.3. Loopback 地址

Loopback 接口创建后除非手工关闭该接口，否则 Loopback 接口物理层状态和链路层协议永远处于 UP 状态，用户可通过配置 Loopback 接口达到提高网络可靠性的目的。

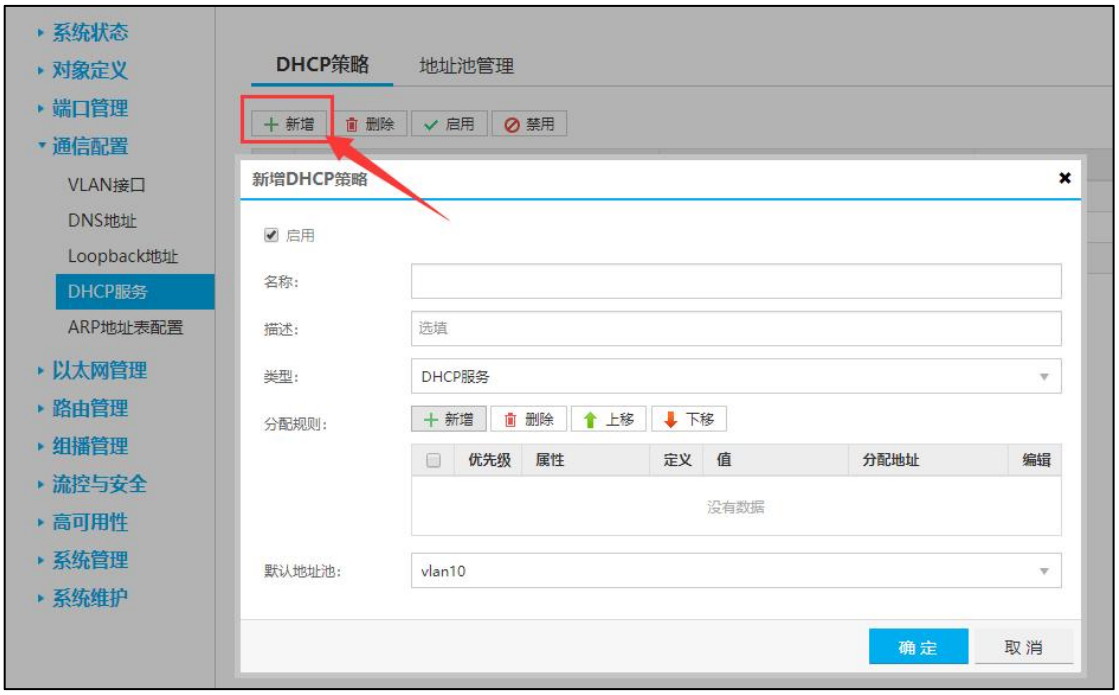
2.4.4. DHCP 服务

DHCP 服务可以为自动获取 IP 地址的终端分配 IP 地址，支持所有三层接口（物理口、

聚合口、vlan 接口、vrrp 接口）且支持在一个接口上分配不同网段 IP。三层接口通过引用 DHCP 策略可以生效 DHCP 服务。

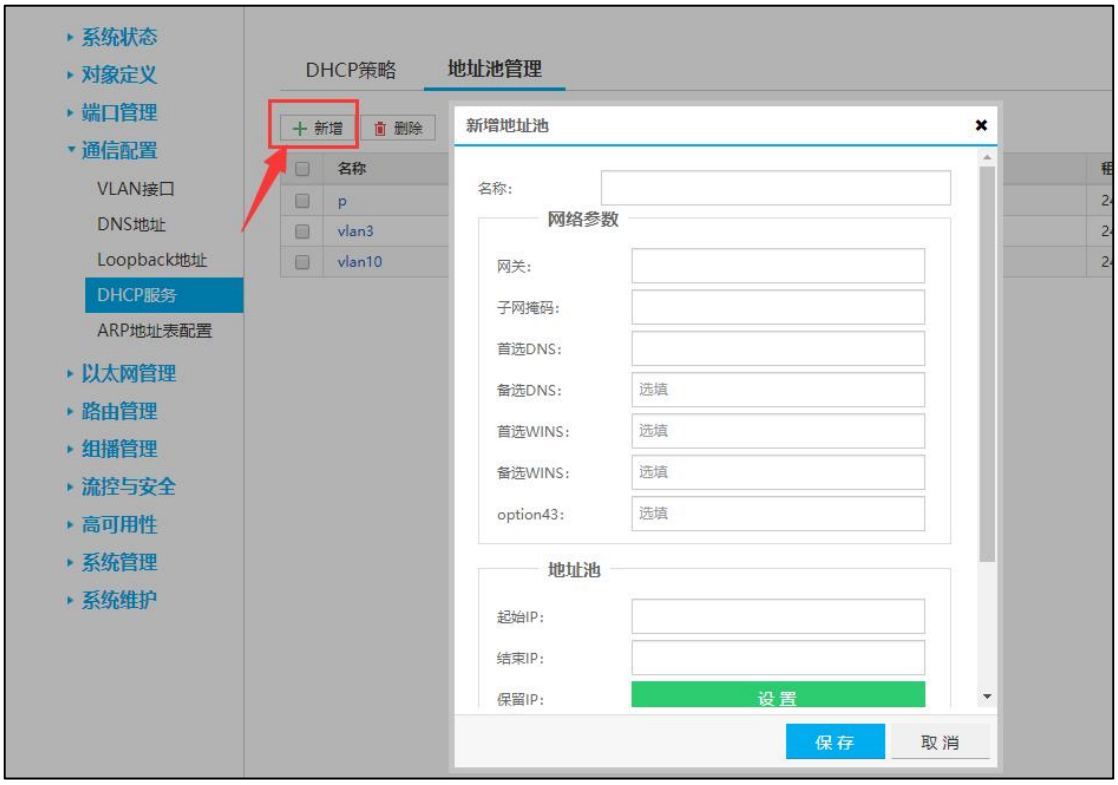
2.4.4.1. DHCP 策略

配置如何为终端分配 IP 地址的策略，支持根据 DHCP 终端的信息、用户属性、Option82 等为其分配不同网段的 IP，或将其 DHCP 请求转发至外部不同的 DHCP 服务器。



2.4.4.2. 地址池管理

配置 DHCP 地址池，多个地址池可以被同一个策略引用。



2.4.5. ARP 地址表配置

静态 ARP 表项不会被老化，不会被动态 ARP 表项覆盖，因此配置静态 ARP 表项可以增加通信的安全性。

当老化时间（默认 1200s）超时后，设备会清除动态 ARP 表项。此时如果设备转发 IP 报文匹配不到对应的 ARP 表项，则会重新生成动态 ARP 表项，如此循环重复。

用户可以通过手工方式或者自动扫描与绑定的方式配置静态 ARP 表项：当需要配置的静态 ARP 表项较少时，可以采用手工方式新增或删除；当需要配置的静态 ARP 表项较多，并且静态 ARP 表项中 IP 地址与 VLANIF 接口的 IP 地址在同一网段时，可以采用自动扫描与绑定方式批量配置。

2.5. 以太网管理

2.5.1. 链路聚合

链路聚合（Link Aggregation）是将多条物理链路捆绑在一起成为一条逻辑链路，从而增加链路带宽的技术。

根据是否启用链路聚合控制协议 LACP，链路聚合分为手工负载分担模式和 LACP 模式。

2.5.2. 防环路配置

『防环路配置』可进行生成树及环路检测的配置。端口上只能启用其中一种防环路配置。

2.5.2.1. 生成树

以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议 STP（Spanning Tree Protocol）。

在生成树协议中，MSTP 兼容 RSTP、STP，RSTP 兼容 STP。

2.5.2.2. 环路检测

环路检测机制可发现某个端口下的环路，并通知用户检查网络连接和配置情况，以避免对整个网络造成严重影响。

环路处理动作

环路处理动作是指发现二层网络中的环路以后所采取的处理方式，常用方式包括阻塞端口、关闭端口、退出环路 vlan。

环路检测间隔

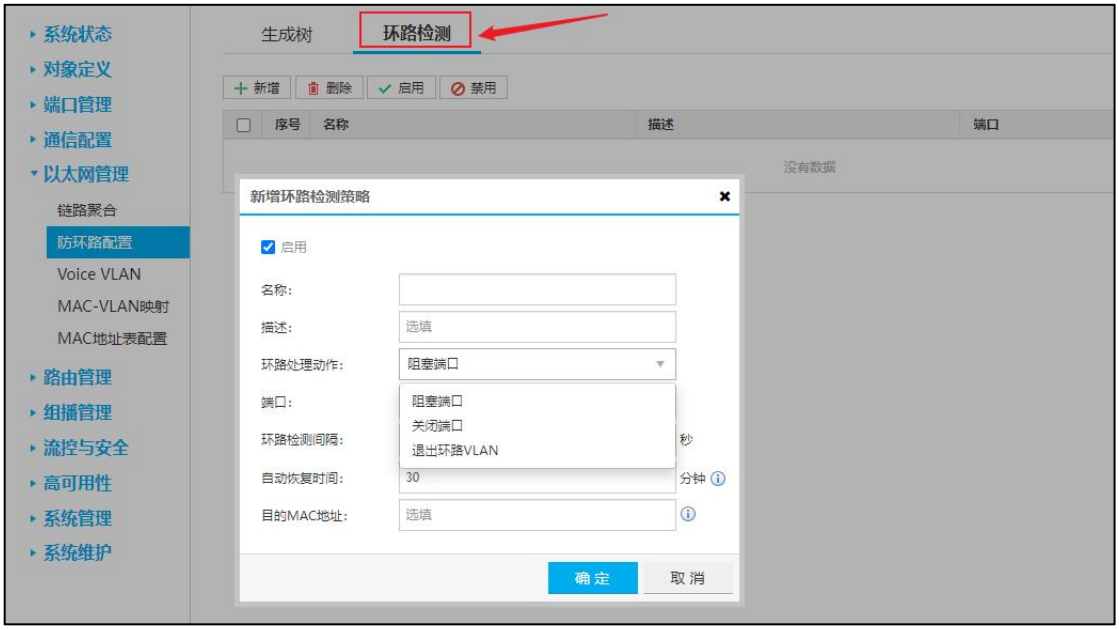
环路检测间隔是环路检测报文的发送时间间隔，通过环路检测报文来确定各端口是否出现环路、以及存在环路的端口上是否已消除环路等。

自动恢复时间

当设备检测到某端口出现环路后，若在一定环路检测时间间隔内仍未收到环路检测报文，就认为该端口上的环路已消除，自动将该端口恢复为正常转发状态。

目的 MAC 地址

环路检测报文的目的 MAC 地址默认为广播地址，用户可根据实际需要进行配置。

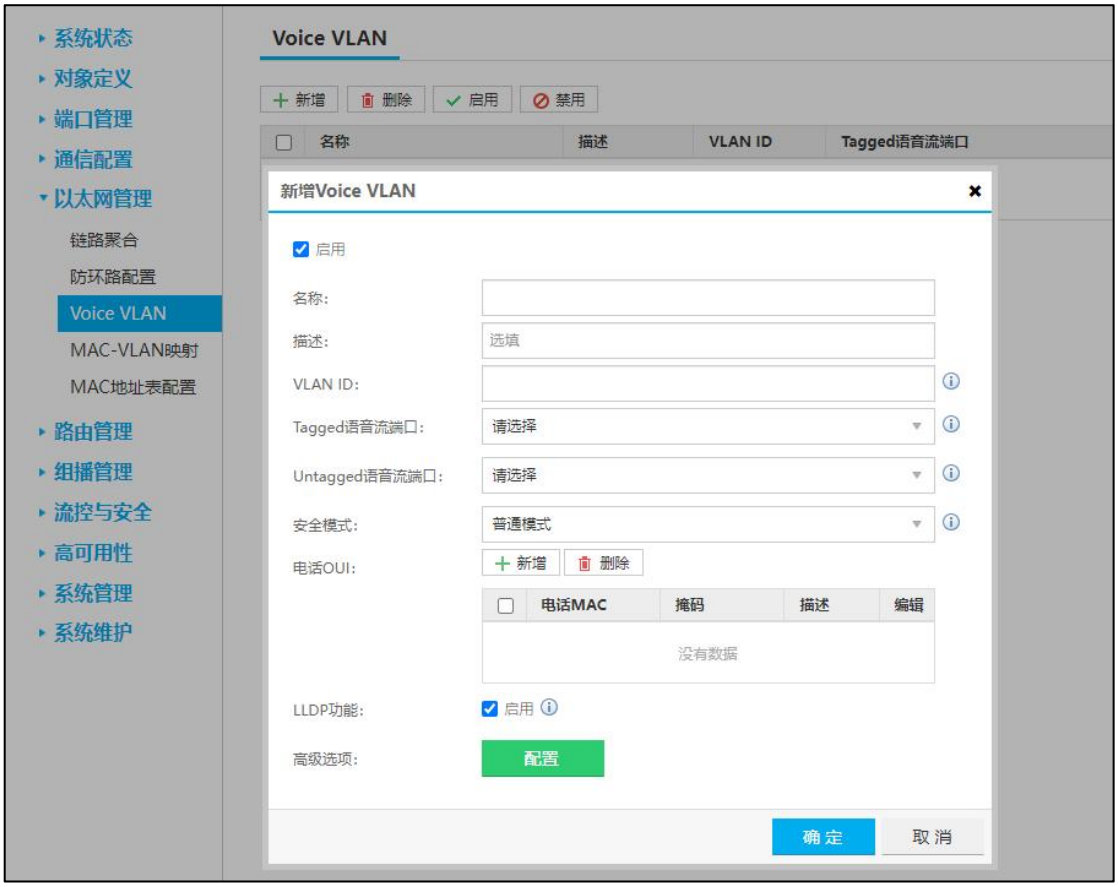


2.5.3. Voice VLAN

配置 Voice VLAN，交换机可识别语音流，对其进行有针对性的 QoS 保障，当网络发生拥塞时可以优先保证语音流的传输。

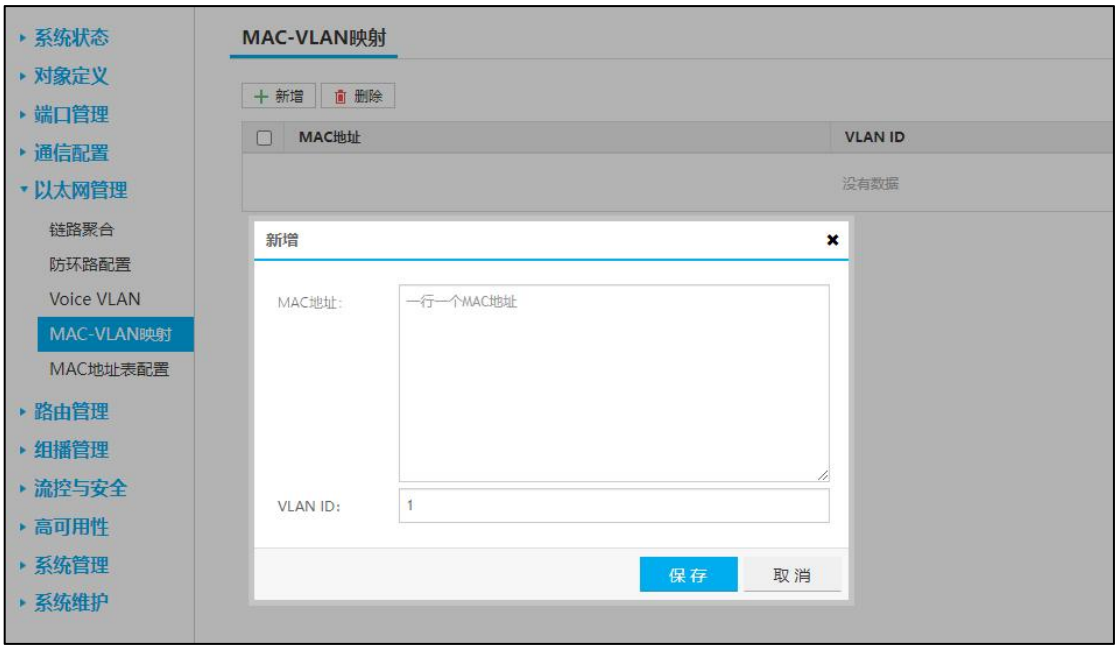
在电话通过 DHCP 获取 IP 的情况下，当电话开启 LLDP 功能接入时可以感知端口上 voice-vlan 变化，能够在 voice-vlan 发生变化时同步发起 DHCP 请求，获取新的 IP 地址；当

电话不开启 LLDP 功能接入时无法感知端口上 voice-vlan 变化，需要等待 IP 地址租期到期时才会发送续租请求，进而获取新的 IP 地址。



2.5.4. MAC-VLAN 映射

基于 MAC 地址划分 VLAN 不需要关注终端用户的物理位置，提高了终端用户的安全性和接入的灵活性。

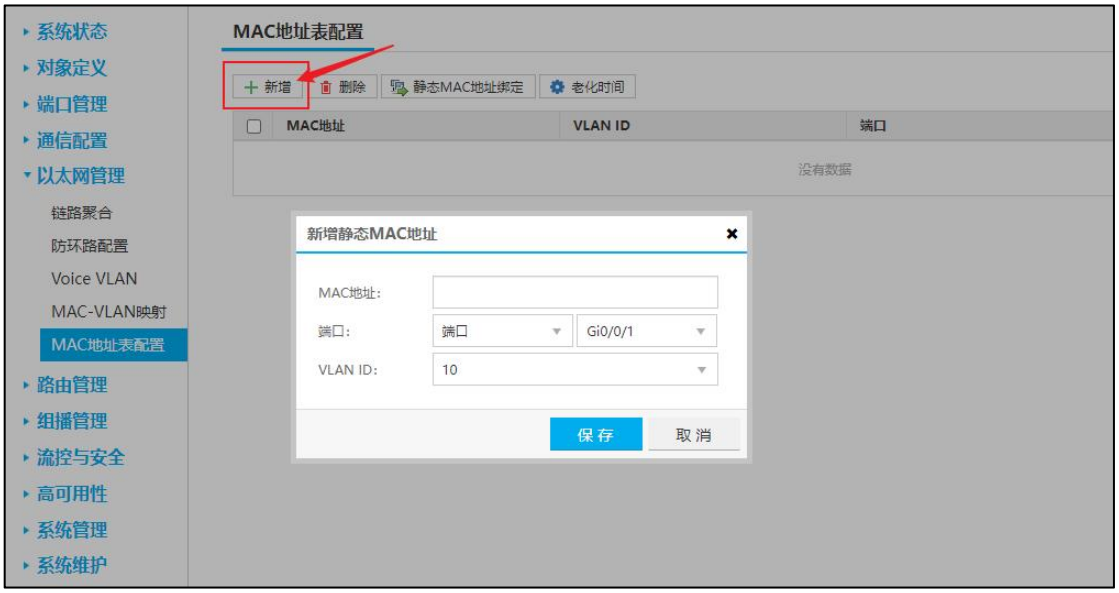


2.5.5. MAC 地址表配置

设备通过源 MAC 地址学习自动建立 MAC 地址表时，无法区分合法用户和非法用户的报文，带来了安全隐患。为了提高安全性，网络管理员可手工在 MAC 地址表中加入特定 MAC 地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。

为了避免 MAC 地址表项爆炸式增长，可以手工配置动态 MAC 表项的老化时间（默认为 300s）。老化时间越短，路由器对周边的网络变化越敏感，适合在网络拓扑变化比较频繁的环境；老化时间越长，路由器对周边的网络变化越不敏感，适合在网络拓扑比较稳定的环境。

当需要配置的静态 MAC 表项较多，并且静态 MAC 表项中 MAC 地址与端口在同一二层环境时，可以采用自动扫描与绑定方式批量配置。



2.6. 路由管理

2.6.1. 静态路由

静态路由是一种需要管理员手工配置的特殊路由。可支持配置 IPv4 和 IPv6 静态路由。

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

支持创建静态路由时，启用链路检测，包括 BFD 检测与 PING 检查，配置链路检测可见高可用性-链路检测。

在创建相同目的地址的多条静态路由时，支持创建静态路由时，启用链路检测并备份配置备份链路，实现路由备份。

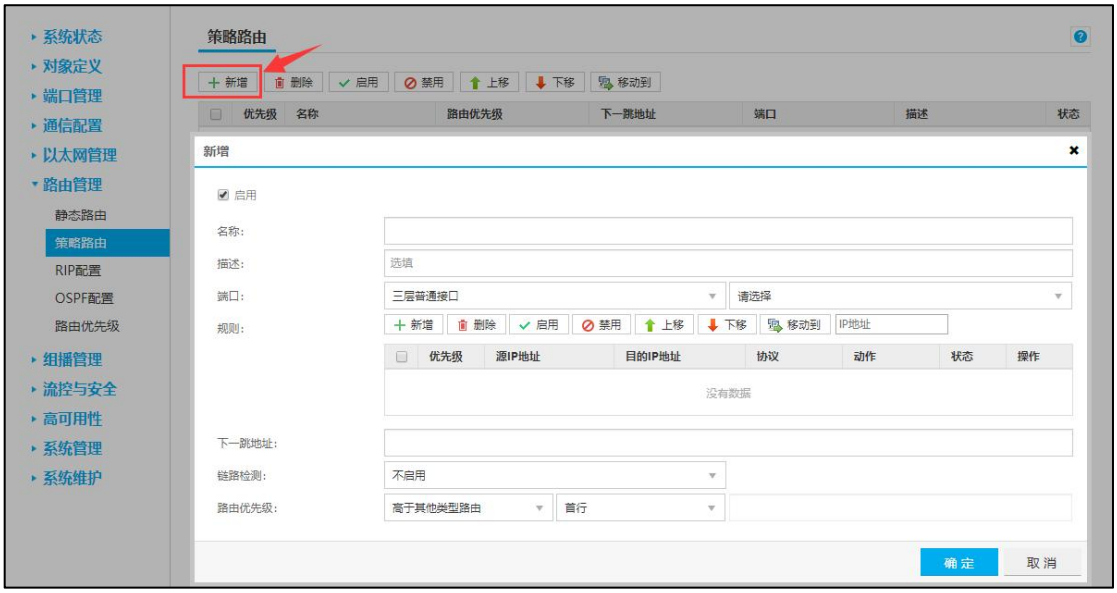
2.6.2. 策略路由

策略路由是一种依据用户制定的策略进行路由选择的机制。设备配置策略路由后，若接收的报文（包括二层报文）匹配策略路由的规则，则按照规则转发；若匹配失败，则根据目的地址按照正常转发流程转发。

支持使用 ACL 作为策略路由的分类规则，配置相应的 ACL 实现可以使不同的数据流通过不同的链路进行发送，提高链路的利用效率。

通过配置策略路由与链路检测联动可以为策略路由提供检测机制，配置完以后，当重定向下一跳对应的链路发生故障的时候，重定向下一跳会因为链路检测失败而立即失效，而不需要等待 ARP 表项老化。这样就可以达到缩短通信中断时间，提高服务质量的目的。

支持通过配置策略路由的优先级实现路由选择的优先顺序。



2.6.3. RIP 配置

RIP 主要应用于规模较小的网络中，例如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用 RIP 协议。支持 V1 和 V2 版本。

2.6.4. OSPF 配置

OSPF（Open Shortest Path First，开放最短路径优先）是 IETF（Internet Engineering Task Force，互联网工程任务组）组织开发的一个基于链路状态的内部网关协议。目前针对 IPv4 协议使用的是 OSPF Version 2。

2.6.5. 路由优先级

对于相同的目的地，不同的路由协议（包括静态路由）可能会发现不同的路由，但这些路由并不都是最优的。事实上，在某一时刻，到某一目的地的当前路由仅能由唯一的路由协议来决定。为了判断最优路由，各路由协议（包括静态路由）都被赋予了一个优先级，当存在多个路由信息源时，具有较高优先级（取值较小）的路由协议发现的路由将成为最优路由，并将最优路由放入本地路由表中。

支持手工为各路由协议配置的优先级，包含静态路由优先级、RIP 协议优先级和 OSPF 协议优先级。

2.7. 组播管理

2.7.1. IGMP Snooping

IGMP Snooping 即组播侦听功能，可以实现组播数据在数据链路层的转发和控制。当主机和上游三层设备之间传递的 IGMP 协议报文通过二层组播设备时，IGMP Snooping 分析报文携带的信息，根据这些信息建立和维护二层组播转发表，从而指导组播数据在数据链路层按需转发，减少二层网络中的广播报文，节约网络带宽，增强组播信息的安全性。

版本号

IGMPv1 主要基于查询和响应机制来完成对组播组成员的管理。与 IGMPv1 相比，IGMPv2 增加了查询器选举机制和离开组机制。IGMPv3 在兼容和继承 IGMPv1 和 IGMPv2 的基础上，进一步增强了主机的控制能力，并增强了查询和报告报文的功能。

查询间隔

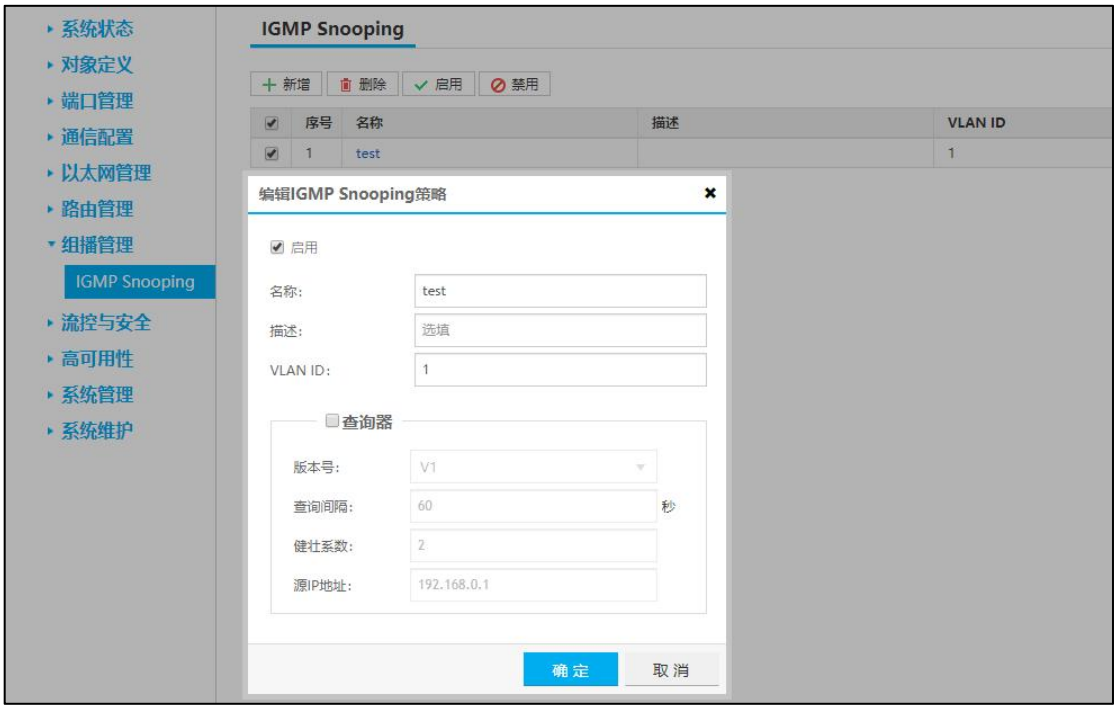
查询间隔是指查询者发送普遍组查询报文之间的时间间隔。普遍组查询报文用于向与其连接的所有子网进行轮询来发现是否有组员存在。

健壮系数

查询器的健壮系数是为了弥补可能发生的网络丢包而设置的报文重传次数。

源 IP 地址

用户可根据实际需要配置查询器的源 IP 地址，从而建立数据链路层组播转发表项，进行组播数据转发。



2.8. 流控与安全

2.8.1. ACL 策略

ACL（Access Control List）即访问控制列表，是一个有序的规则的集合，通过匹配报文中信息与规则中参数来对数据包进行分类，并执行规则对应的动作。

源/目的 IP 地址

支持使用以太网帧的源 IP 地址（地址段）或目的 IP 地址（地址段）来定义 ACL 规则。

源/目的 MAC 地址

支持使用以太网帧的源 MAC 地址或目的 MAC 地址来定义 ACL 规则。

VLAN ID

支持使用以太网帧的 VLAN ID 来定义 ACL 规则。

二层/三层协议

支持使用二层/三层网络协议来定义 ACL 规则，包括 ARP、RARP、ICMP、TCP、UDP、IGMP、IP、OSPF 等协议。

时间计划

时间计划是指 ACL 规则生效的时间段，表示仅在指定时间段内按该规则过滤。

2.8.2. QoS 配置

QoS（Quality of Service）即服务质量，是指网络通信过程中，允许用户业务在丢包率、延迟、抖动和带宽等方面获得可预期的服务水平。

2.8.2.1. 流量管理

流量管理功能包括重标记、流量监管、流镜像、重定向等。

重标记

通过设置报文的优先级或标志位，重新定义报文的优先级。

流量监管

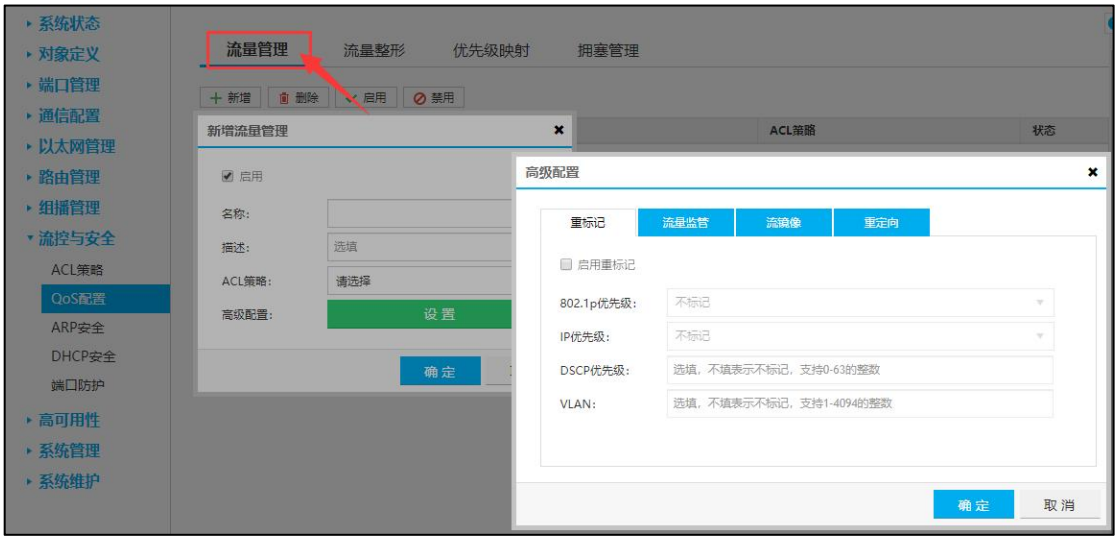
通过监控进入网络的流量速率，将输入流量限制在一个合理范围内。

流镜像

将镜像端口上特定业务流的报文复制到观察端口进行分析和监控。

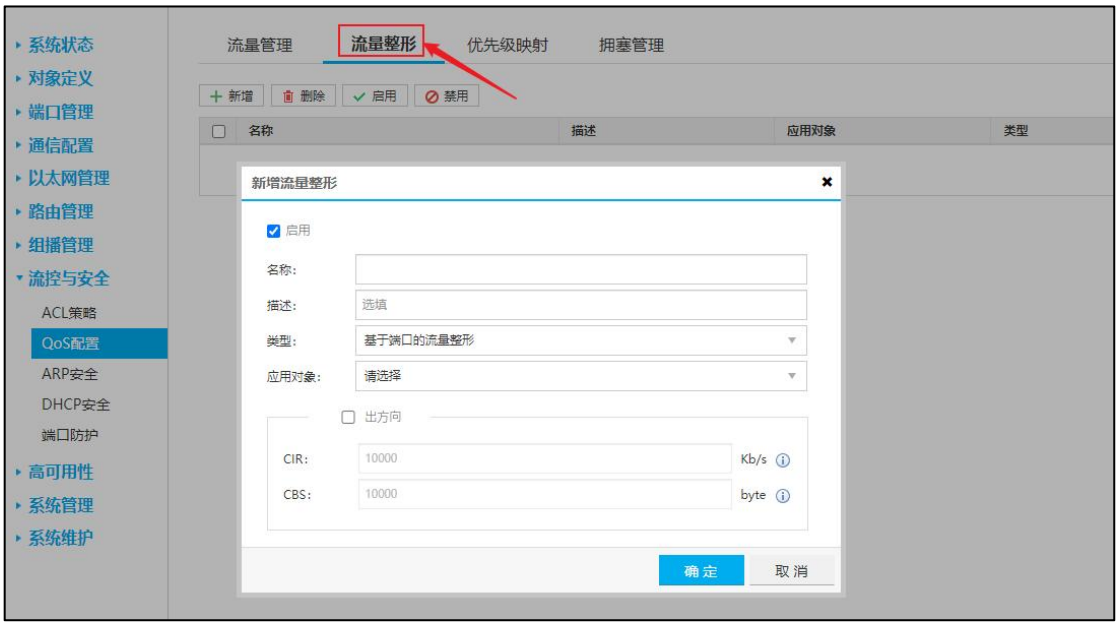
重定向

将符合流分类的报文流重定向到其他端口进行处理。



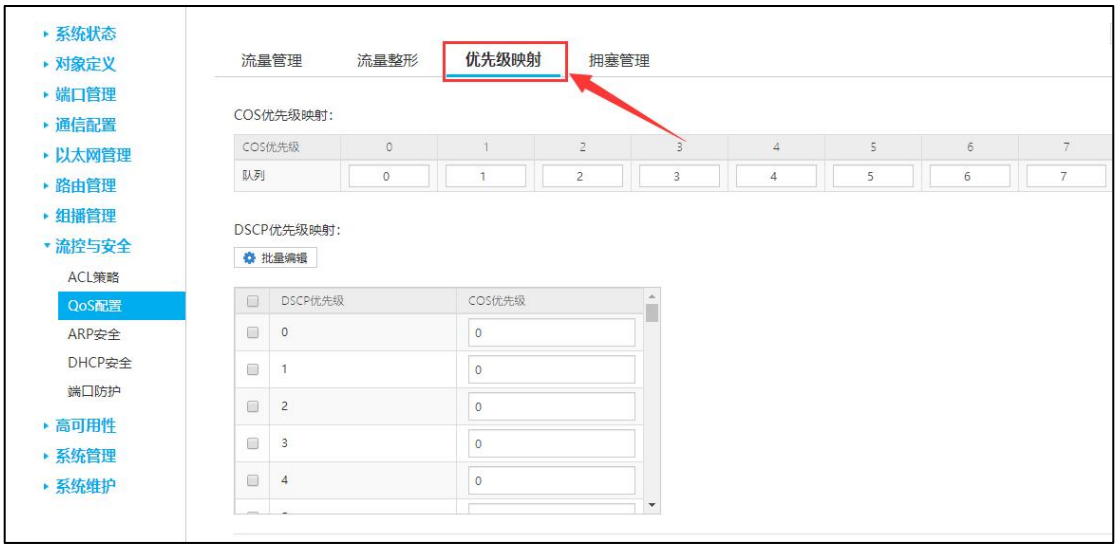
2.8.2.2. 流量整形

流量整形是一种主动调整流量输出速率的措施，对上游输入的不规整流量进行缓冲，使流量输出趋于平稳，从而解决下游设备的拥塞问题。



2.8.2.3. 优先级映射

优先级映射实现从 COS 优先级到 DSCP 优先级之间的映射，设备可根据优先级提供有差别的 QoS 服务。



2.8.2.4. 拥塞管理

当时延敏感业务要求得到比非时延敏感业务更高质量的 QoS 服务，且网络中间歇性的出现拥塞，此时需要进行拥塞管理。拥塞管理一般采用排队技术，使用不同的调度算法来发

送队列中的报文流。常用调度模式包括严格优先模式、轮询模式、加权轮询模式、严格优先+加权轮询模式和差分加权轮询模式。

常用优先级信任模式包括信任报文优先级和信任端口优先级。信任报文优先级是指直接根据报文携带的报文优先级来转发数据，信任端口优先级分两种情况：

1.当入口报文不带 802.1p 优先级，设备将使用端口优先级，根据此优先级查找 802.1p 优先级到内部优先级映射表，然后为报文标记内部优先级。

2.当入口报文携带 802.1p 优先级，此时按报文携带的 802.1p 优先级，查找 802.1p 优先级到内部优先级映射表，然后为报文标记内部优先级。

2.8.3. ARP 安全

ARP 安全是针对 ARP 攻击的一种安全特性，它通过一系列对 ARP 表项学习和 ARP 报文处理的限制、检查等措施来保证网络设备的安全性。ARP 安全特性不仅能够防范针对 ARP 协议的攻击，还可以防范网段扫描攻击等基于 ARP 协议的攻击。

2.8.3.1. ARP 泛洪防御

ARP 泛洪攻击也叫拒绝服务攻击 DoS（Denial of Service），主要存在这样两种场景：

1、设备处理 ARP 报文和维护 ARP 表项都需要消耗系统资源，同时为了满足 ARP 表项查询效率的要求，一般设备都会对 ARP 表项规模有规格限制。攻击者就利用这一点，通过伪造大量源 IP 地址变化的 ARP 报文，使得设备 ARP 表资源被无效的 ARP 条目耗尽，合法用户的 ARP 报文不能继续生成 ARP 条目，导致正常通信中断。

2、攻击者利用工具扫描本网段主机或者进行跨网段扫描时，会向设备发送大量目标 IP 地址不能解析的 IP 报文，导致设备触发大量 ARP Miss 消息，生成并下发大量临时 ARP 表项，并广播大量 ARP 请求报文以对目标 IP 地址进行解析，从而造成 CPU（Central Processing Unit）负荷过重。

报文限速

通过 ARP 报文限速功能，可以防止设备因处理大量 ARP 报文，导致 CPU 负荷过重而无法处理其他业务，分为基于单个交换机端口报文限速和基于源 MAC 地址报文限速。

仅学习本机的 ARP 请求应答

只有本设备主动发送的 ARP 请求报文的应答报文才能触发本设备学习 ARP，其他设备主动向本设备发送的 ARP 报文不能触发本设备学习 ARP。这可以防止设备收到大量 ARP 攻击报文时，ARP 表被无效的 ARP 条目占满。

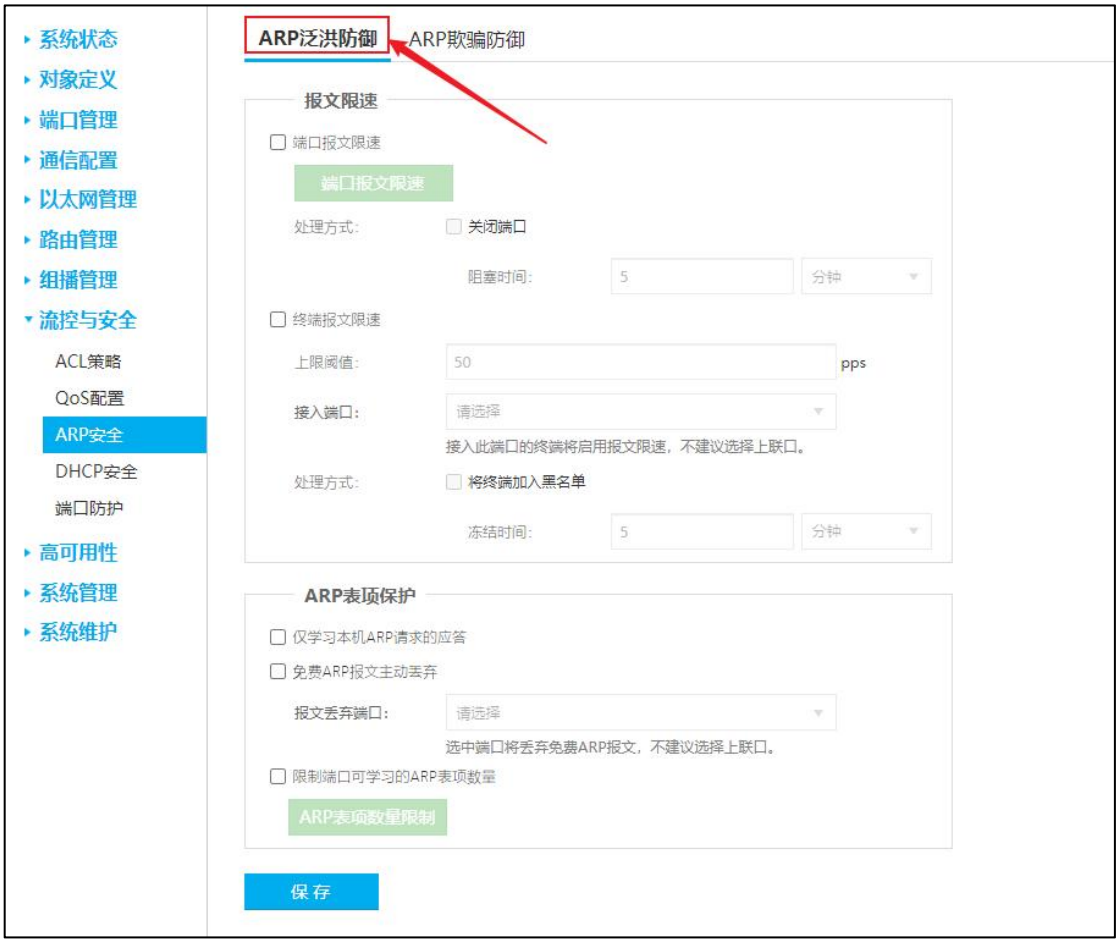
免费 ARP 报文主动丢弃

设备直接丢弃免费 ARP 报文，可以防止设备因处理大量免费 ARP 报文，导致 CPU 负荷过重而无法处理其他业务。

限制端口可学习的 ARP 表项数量

设备接口只能学习到设定的最大动态 ARP 表项数目。这可以防止当一个接口所接入的

某一台用户主机发起 ARP 攻击时整个设备的 ARP 表资源都被耗尽。



2.8.3.2. ARP 欺骗防御

ARP 欺骗攻击是指攻击者通过发送伪造的 ARP 报文，恶意修改设备或网络内其他用户主机的 ARP 表项，造成用户或网络的报文通信异常。ARP 攻击行为存在以下危害：

1、会造成网络连接不稳定，引发用户通信中断。

2、利用 ARP 欺骗截取用户报文，进而非法获取游戏、网银、文件服务等系统的账号和口令，造成被攻击者重大利益损失。

ARP 表项更新检查

设备在第一次学习到 ARP 之后，用户更新此 ARP 表项时通过发送 ARP 请求报文的方

式进行确认，以防止攻击者伪造 ARP 报文修改正常用户的 ARP 表项内容。

ARP 报文合法性校验

通过检查报文中的 IP 地址、MAC 地址，直接丢弃非法的 ARP 报文，避免非法用户伪造 ARP 报文，刻意的进行 ARP 攻击。

基于 DHCP 的 ARP 绑定关系检测（DAI）

当设备收到 ARP 报文时，将此 ARP 报文的源 IP、源 MAC（Media Access Control）、收到 ARP 报文的接口及 VLAN（Virtual Local Area Network）信息和绑定表的信息进行比较，如果信息匹配，则认为是合法用户，允许此用户的 ARP 报文通过，否则认为是攻击，丢弃该 ARP 报文。本功能仅适用于 DHCP Snooping（Dynamic Host Configuration Protocol Snooping）场景。

网关防欺骗

丢弃源 IP 地址为网关设备 IP 地址的 ARP 报文，防止攻击者仿冒网关，建议在网关设备上开启。

告警及处理方式

发生告警或欺骗时进行一些惩罚动作，并通过短信或 APP 通知管理员及时进行处理。

2.8.4. DHCP 安全

DHCP 安全是针对 DHCP 攻击的一种安全特性，它通过一系列对 DHCP 报文处理的限制、检查等措施来保证网络设备的安全性。

2.8.4.1. DHCP 泛洪防御

DHCP 泛洪攻击也叫拒绝服务攻击 DoS（Denial of Service），主要存在以下几种场景：

1、非法用户在短时间内发送大量 DHCP 报文，使 DHCP Server 无法正常处理报文，从而无法为客户端分配 IP 地址。

2、非法用户通过恶意申请 IP 地址，使 DHCP 服务器中的 IP 地址快速耗尽， 无法为合法用户再分配 IP 地址。

3、已获取到 IP 地址的合法用户通过向服务器发送 DHCP Request 报文用以续租 IP 地址。非法用户冒充合法用户不断向 DHCP Server 发送 DHCP Request 报文来续租 IP 地址，导致到期的 IP 地址无法正常回收，新的合法用户不能再获得 IP 地址。

4、已获取到 IP 地址的合法用户通过向服务器发送 DHCP Release 报文用以释放 IP 地址。

非法用户仿冒合法用户向 DHCP Server 发送 DHCP Release 报文，使合法用户异常下线。

报文限速

通过 DHCP 报文限速功能，可以防止设备因处理大量 DHCP 报文，导致 CPU 负荷过重而无法处理其他业务，分为基于单个交换机端口报文限速和基于源 MAC 地址报文限速。

限制端口可申请的 IP 地址数量

限制用户接入数。当用户数达到指定值时，任何用户将无法通过此接口申请到 IP 地址。

DHCP 续租报文合法性检查

在 DHCP Server 为客户端分配 IP 地址过程中，根据 DHCP 报文生成 DHCP Snooping 绑定表，该绑定表记录 MAC 地址、 IP 地址、租约时间、 VLAN ID、接口等信息，然后通过 DHCP 报文与绑定表的合法性检查，丢弃非法报文， 防止 DHCP 报文仿冒攻击。

2.8.4.2. DHCP 欺骗防御

DHCP 欺骗攻击，网络中如果存在私自架设的 DHCP Server 仿冒者，则可能导致 DHCP 客户端获取错误的 IP 地址和网络配置参数，无法正常通信。

DHCP Snooping 信任功能可以控制 DHCP 服务器应答报文的来源，以防止网络中可能存在的 DHCP Server 仿冒者为 DHCP 客户端分配 IP 地址及其他配置信息

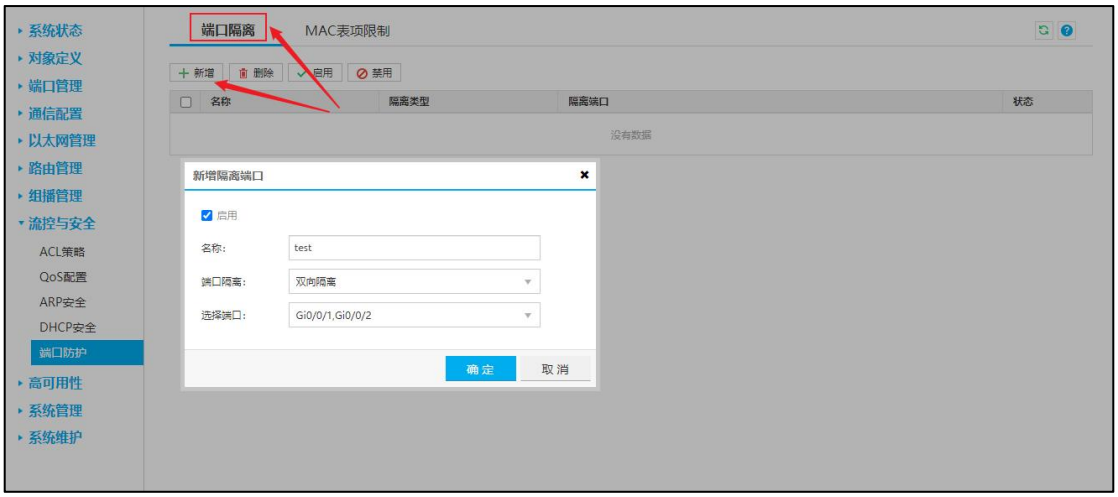
2.8.5. 端口防护

2.8.5.1. 端口隔离

采用端口隔离特性，可以实现报文之间的二、三层隔离，用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间的隔离，为用户提供了更安全、更灵活的组网方案。

单向隔离是指从“源端口”发送的报文不能到达“目的端口”，但从“目的端口”发送的报文可以到达“源端口”。

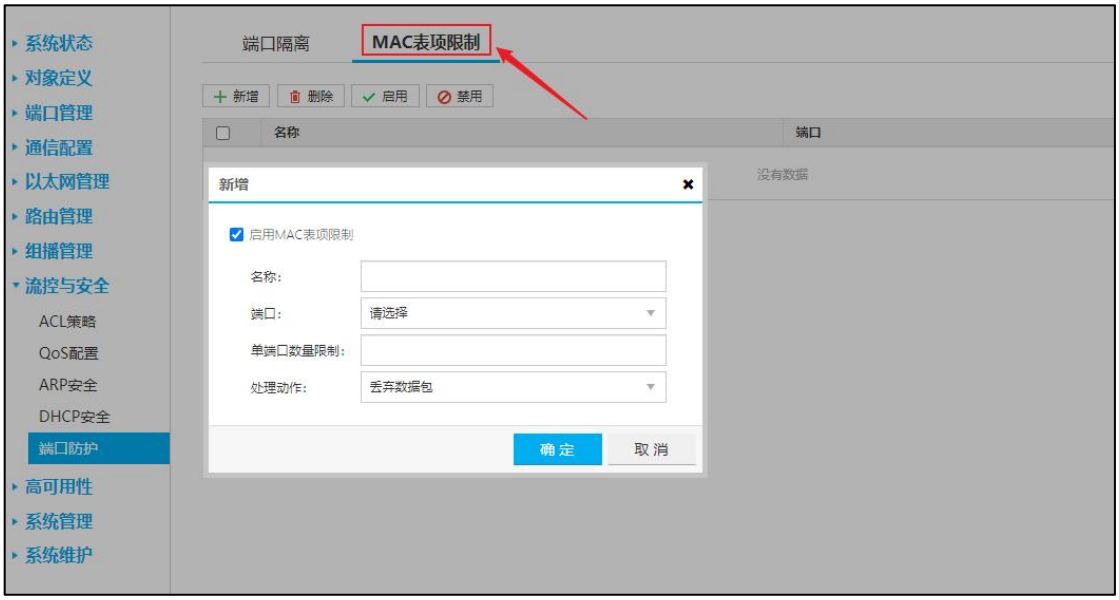
双向隔离是指隔离组内的任一端口发送的报文不能到达隔离组内的其他端口，但可以到达隔离组外的其他端口。



2.8.5.2. MAC 表项限制

一些安全性较差的网络容易受到黑客的 MAC 地址攻击，由于 MAC 地址表的容量是有限的，当黑客伪造大量源 MAC 地址不同的报文并发送给交换机后，交换机的 MAC 表项资源就可能被耗尽。当 MAC 表被填满后，即使它再收到正常的报文，也无法学习到报文中的源 MAC 地址。配置限制 MAC 地址学习数，当超过限制数时不再学习 MAC 地址，同时可以配置当 MAC 地址数达到限制后对报文采取的动作，从而防止 MAC 地址表资源耗尽，提高网络安全性。

处理动作为丢弃数据包时，如果端口上的 MAC 地址数量超过限制，交换机不再学习新的 MAC 地址并且不再转发处理新 MAC 的数据包；处理动作为转发数据报文时，如果端口上的 MAC 地址数量超过限制，交换机不再学习新的 MAC 地址，但还会转发处理新 MAC 的数据包。



2.9. 高可用性

2.9.1. 链路高可用

2.9.1.1. 备份链路

备份链路，又叫做灵活链路。一个备份链路由两个端口组成，其中一个端口作为另一个的备份。备份链路常用于双上行组网，提供可靠高效的备份和快速的切换机制。

备份链路组

灵活链路组，包括两条链路，其中一条进行转发，另一条链路阻塞，作冗余备份。

主用链路和备用链路

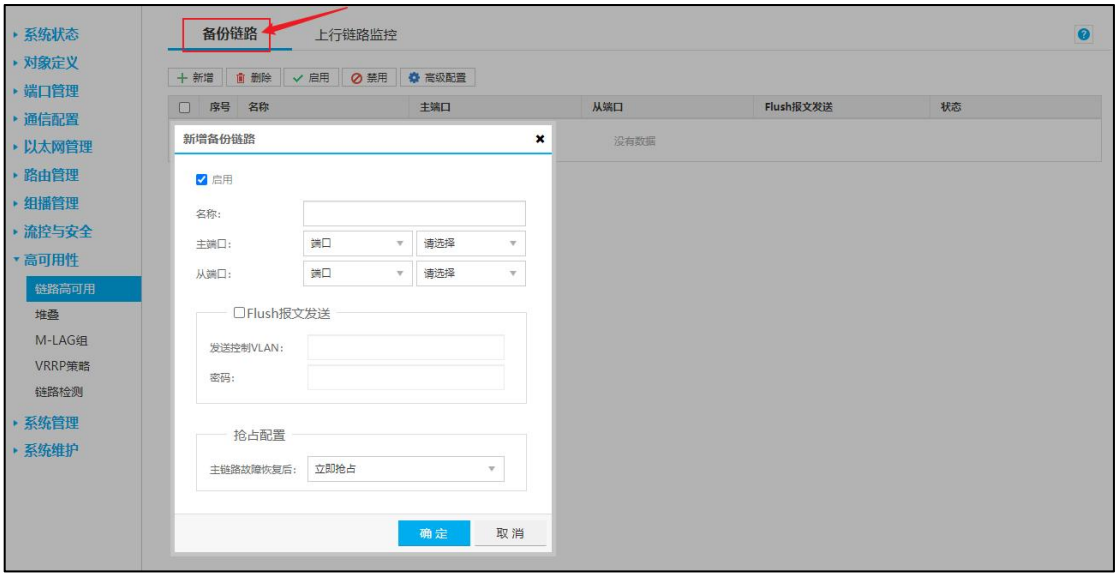
备份链路组中处于转发状态的链路称为主用链路，处于阻塞状态的链路称为备用链路。

主端口和从端口

备份链路组的主用和备用链路在特定的设备上体现为端口或者聚合组端口，此处统称为端口。为了区分备份链路组中的两个端口，将两个端口分别命名为主端口和从端口。

FLUSH 报文

端口切换之后，备份链路发送一个 FLUSH 报文通知其他设备进行地址刷新。但是，由于该技术为私有技术，目前只限于我司的交换机、华为、华三的设备能够识别该报文。对于不识别 FLUSH 报文的设备，只能通过流量触发 MAC 地址的更新。



2.9.1.2. 上行链路监控

上行链路监控是一种端口联动方案，它能通过监控设备的上行端口，根据其 UP/DOWN 状态的变化来触发下行端口 UP/DOWN 状态的变化，从而触发下游设备上的拓扑协议进行链路的切换。

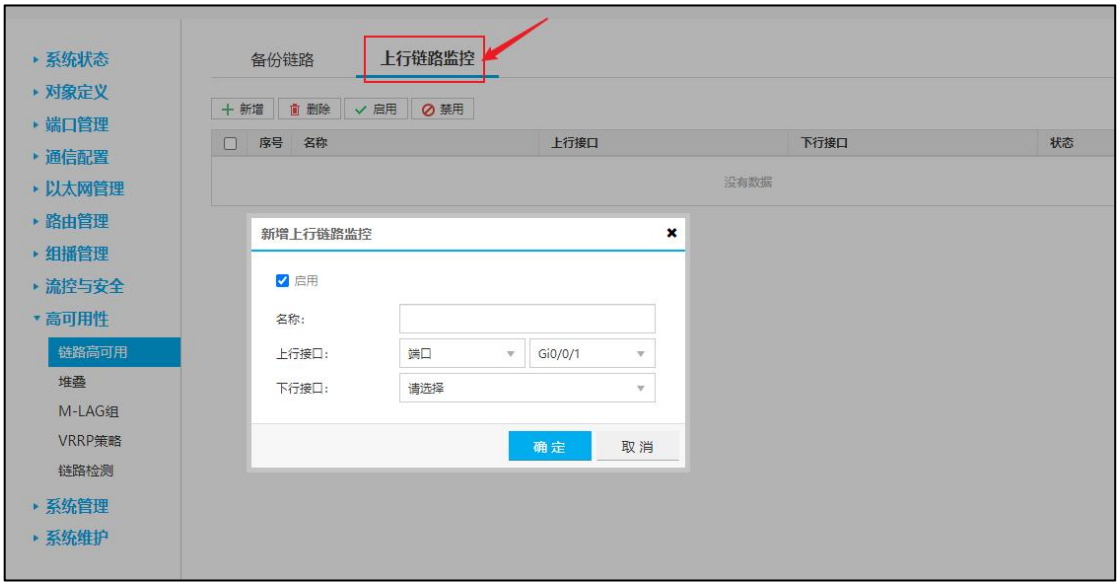
上行链路监控可用于扩展一些二层拓扑协议（例如：备份链路）的应用范围，通过监控上行链路对下行链路进行同步设置，达到上行链路故障迅速传达给下行设备，从而触发下游设备上的拓扑协议进行链路的切换，防止长时间因上行链路故障而出现流量丢失。

上行接口

上行接口是上行链路监控组中的监控对象，上行链路监控组的上行接口可以是以太网端口（电口或光口）、聚合口或备份链路组。

下行接口

下行接口是上行链路监控组中的监控者，上行链路监控组的下行接口可以是以太网端口（电口或光口）或聚合口。



2.9.2. 堆叠

堆叠就是将多台设备通过专用的堆叠口或业务口连接起来，形成一台虚拟的逻辑设备。用户对这台虚拟设备进行管理，来实现对堆叠中所有成员设备的管理。堆叠系统具有高可靠性及易管理等优点。

堆叠成员

组建堆叠的成员需要同样的软件版本，硬件型号满足组堆叠。最多支持两台交换机组堆叠。

堆叠口

堆叠系统通信链路两端的接口为堆叠口，仅支持光口做为堆叠口。堆叠口的连接可以由多条堆叠物理链路自动聚合而成，多条聚合链路之间可以对流量进行负载分担，有效地提高了带宽及堆叠可靠性。堆叠成员端口必须为统一类型端口，例如 10GE 与 40GE 端口不可以

组成堆叠聚合链路。普通口切换为堆叠口后，将不再支持切换速率与单双工，GE 口速率配置为 1000M 全双工，10GE 口速率配置为 10G 全双工，40GE 口速率配置为 40G 全双工，堆叠口再切换为普通口后，又会恢复原来的配置。

本地流量有线转发

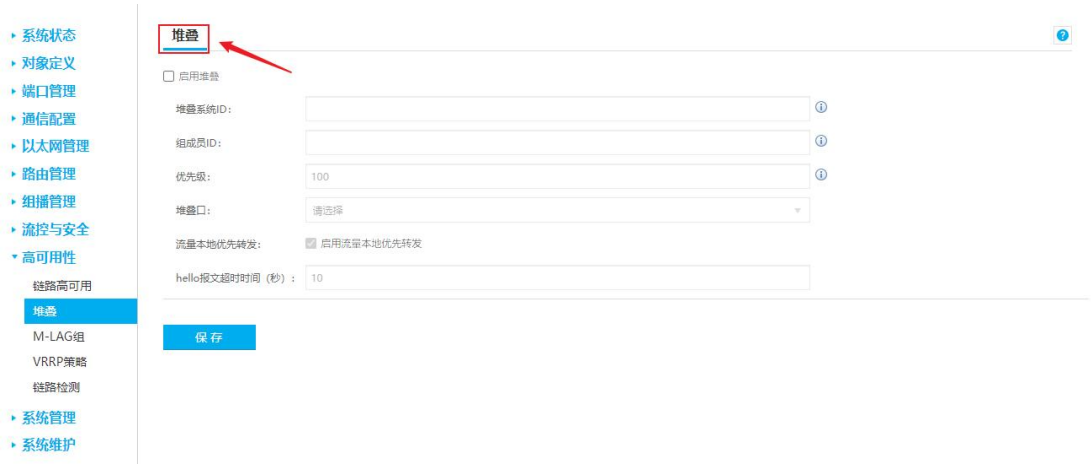
由于堆叠链路带宽有限，为了提高转发效率，减少跨堆叠成员的流量转发，支持 TRUNK 口的本地流量优先转发功能。即从本设备进入的流量，优先从本设备上相应的 TRUNK 成员口转发出去；如果本设备相应的接口故障或流量已经达到了接口线速，那么就从对端堆叠成员设备的接口转发出去。

Hello 报文超时时间

堆叠系统中备机超时时间内，未收到主机发送的保活报文，会自动升级为主机。

多主检测

为了减少堆叠分裂对业务的影响，建议用户在堆叠组建完成后进行双主检测的配置。堆叠链路断开或堆叠心跳超时出现多主时，MAD 检测机制会检测到网络中存在多个处于主机状态的堆叠系统。MAD 冲突检测机制会保持原主机继续工作，将其他的堆叠系统转入 recovery 状态，并且在 recovery 状态的堆叠系统的所有成员上，关闭除保留端口以外的其他所有物理端口，以保证该堆叠系统不再转发业务报文。堆叠多主检测支持不检测，直连检测与代理检测，且默认检测方式为直连检测。直连检测选择的检测端口需要覆盖所有的堆叠成员，每个成员只能选择一个端口。代理检测仅支持信锐的交换机的聚合口做代理检测。



2.9.3. M-LAG 组

M-LAG（Multichassis Link Aggregation Group）即跨设备链路聚合组，是一种实现跨设备链路聚合的机制，将一台设备与另外两台设备进行跨设备链路聚合，从而把链路可靠性从单板级提高到了设备级，组成双活系统。

M-LAG ID

设备的 M-LAG ID，MSTP 名称，修订级别和实例必须保持一致才能正常使用 MLAG 功能。

交换机优先级

Peer Link 链路组配对成功后，两端设备会确定出主从状态。先比较交换机优先级，值越小优先级越高，优先级高的为主设备。如果优先级相同，那么比较两台设备的 MAC 地址，MAC 地址较小的为主设备。

KeepAlive 口

KeepAlive 链路是一条三层互通链路，用于 M-LAG 主备设备间发送双主检测报文。

正常情况下，双主检测链路不会参与 M-LAG 的任何转发行为，只在故障场景下，用于检查是否出现双主的情况。用于检测对端的选举状态是否正常。

Peer Link 口

Peer Link 链路两端直连的接口均为 Peer Link 接口，支持配置光口，电口，聚合口。

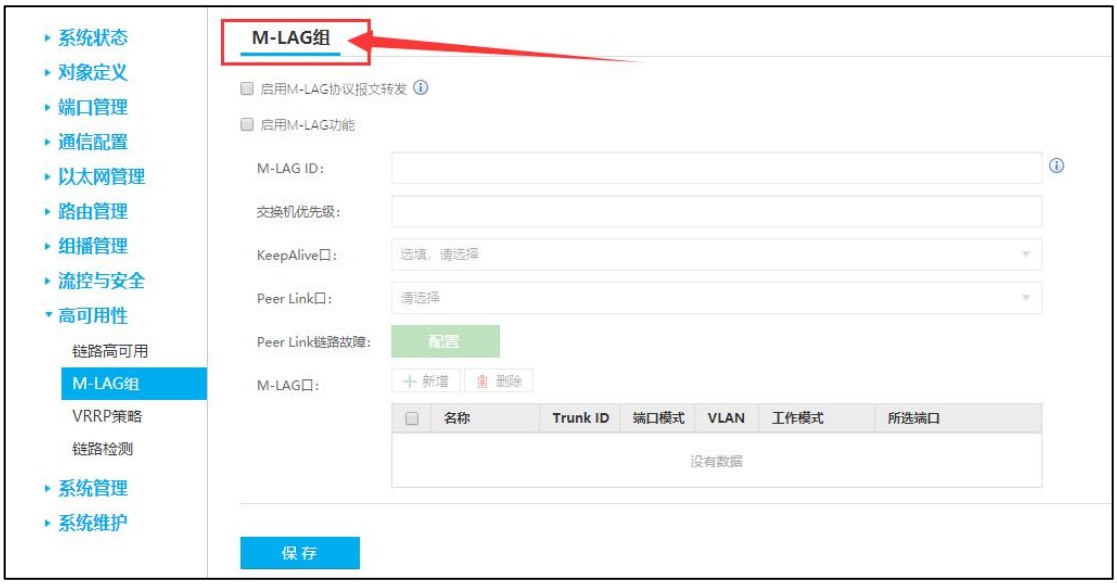
Peer Link 链路故障

Peer Link 链路是一条直连链路，用于交互协商报文及传输部分流量。

Peer Link 故障但心跳状态正常会导致备设备上除管理网口、peer-link 接口以及自定义的排除端口以外的物理接口处于 DOWN 状态，此时双归场景变为单归场景。一旦配置 Peer Link 链路故障恢复，处于 DOWN 状态的物理接口默认将在 120 秒时间自动恢复为 Up 状态。

M-LAG 口

M-LAG 口是 M-LAG 主备设备上连接上下行设备的 Eth-Trunk 接口。加入同一 M-LAG 口的接口，对外表现为同一个聚合接口。



2.9.4. VRRP 策略

VRRP（Virtual Router Redundancy Protocol）即虚拟冗余备份组协议,通过把几台路由设备联合组成一台虚拟的路由设备，使用一定的机制保证当主机的下一跳路由器发生故障时，

及时地将业务切换至备份路由器，从而保证业务的连续性和可靠性。

组 ID

虚拟路由器 ID，VRRP 备份组标识，同一个实例的 VRID 值必须一致才可以正常工作。

虚拟 IP 地址

VRRP 备份组的 IP 地址，一个虚拟路由器可以有一个或多个 IP 地址。

虚拟 MAC 地址

VRRP 备份组根据虚拟路由器 ID 自动生成的 MAC 地址。

通信方式

默认使用组播的通信方式，支持单播的通信方式。

优先级

VRRP 备份组中的设备优先级，备份组根据优先级选举出 Master 和 Backup 设备。

VRRP 绑定接口

VRRP 备份组中，虚拟 IP 地址所在的接口。

超时时间

VRRP 备份组中 Backup 设备因未收到 Master 设备报文，自动切换为 Master 所等待的时间。

接口监视

VRRP 备份组中，设备监控上联口或上联链路，当上联口或上联链路故障时，降低设备优先级，触发主备切换。

状态恢复延时时间

VRRP 备份组中，设备因故障进入 fault 状态后，在故障恢复正常时，设备从错误状态切换至 Backup 状态等待的时间。

DHCP 服务

VRRP 备份组支持提供 DHCP 服务，且 DHCP 服务仅对 Master 设备生效。

抢占功能

开启抢占功能后，Backup 设备的优先级高于 Master 设备优先级时，自动切换为 Master 设备。

VRRP 版本

默认采用 VRRPv2 版本，支持 VRRPv3 版本。

通告间隔

VRRP 备份组中，Master 设备主动发送保活报文的时间间隔。

免费 ARP 间隔

备份组虚拟 IP 地址不断发送免费 ARP 的时间间隔。

VRRP 报文认证方式

VRRP 备份组中，VRRPv2 版本支持不认证，简单认证和 MD5 认证方式，VRRPv3 版本不支持认证。

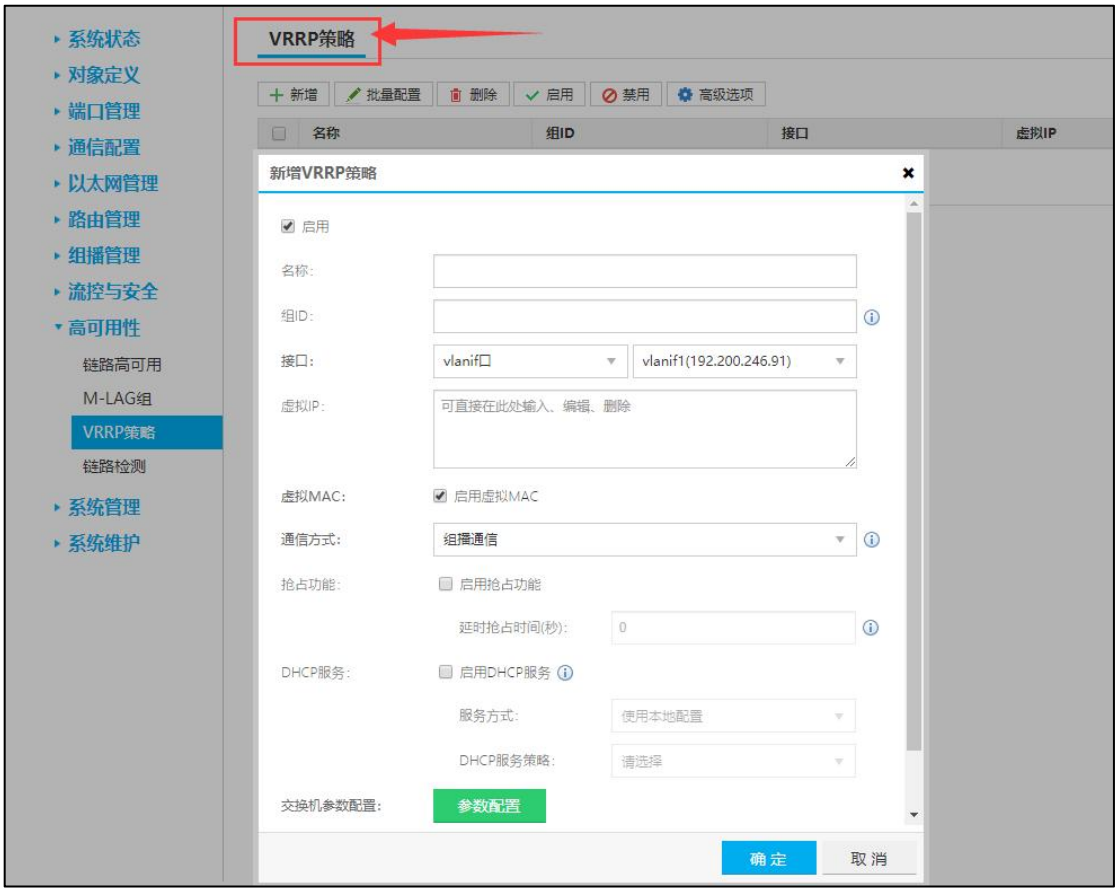
代管组

多个 VRRP 备份组实例加入同一个代管组中时，由备份组中当时 VRID 最小的 Master

设备代为发送 VRRP 报文，减少 VRRP 报文发送数量。

同步组

由同步源负责 VRRP 保活，成员设备不发送保活报文，实例状态与同步源状态保持一致，减少 VRRP 报文发送数量。

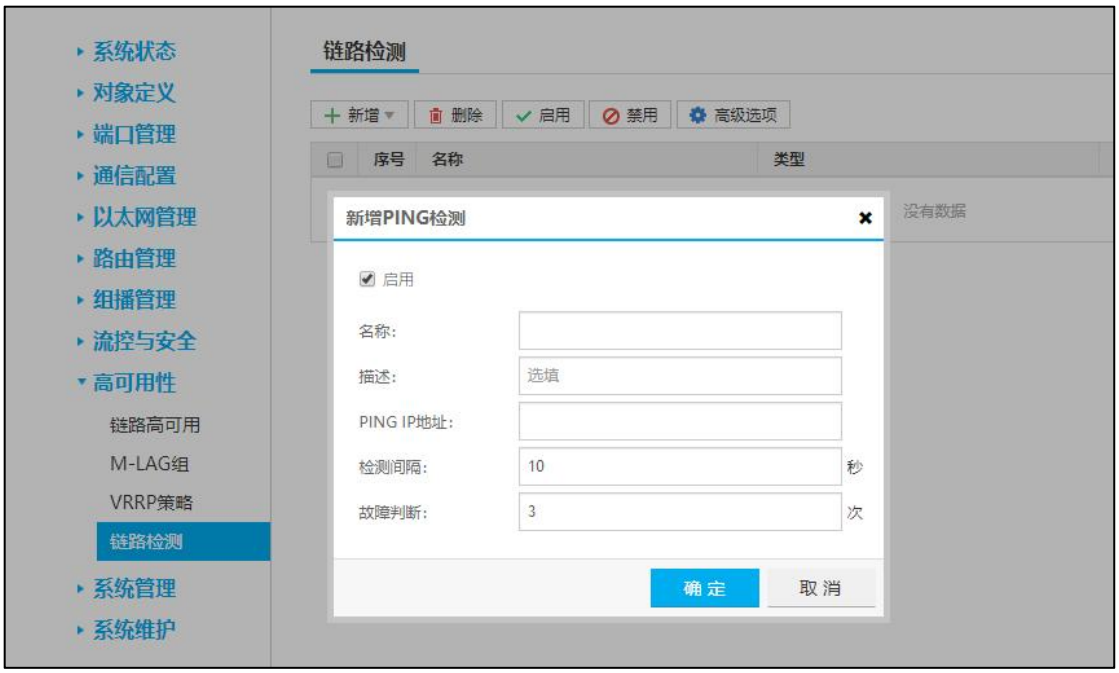


2.9.5. 链路检测

2.9.5.1. PING 检测

当设备出现故障时，可以使用 PING 检测测试网络连接是否正常工作。

PING 检测主要用于检查网络连接及主机是否可达。源主机向目的主机发送 ICMP 请求报文，目的主机向源主机发送 ICMP 回应报文。



2.9.5.2. BFD 检测

BFD 检测用于快速检测系统之间的通信故障，并在出现故障时通知上层应用。

BFD 提供了一个与介质和协议无关的快速故障检测机制。是网络设备间任意类型的双向转发路径提供快速、轻负荷的故障检测。

支持的检测类型有二层链路检测，三层链路检测和单臂回声功能。

二层链路检测

二层链路检测可以实现通过二层接口连通的设备间链路故障的快速检测。

三层链路检测

三层链路检测可以实现通过三层接口连通的设备间链路故障的快速检测。

单臂回声功能

在两台直接相连的设备中，其中一台设备支持 BFD 功能，另一台设备不支持 BFD 功能。为了能够快速的检测这两台设备之间的故障，可以在支持 BFD 功能的设备上创建单臂回声功能的 BFD 会话。支持 BFD 功能的设备主动发起回声请求功能，不支持 BFD 功能的设备接收到该报文后直接将其环回，从而实现转发链路的连通性检测功能。

标识符

静态建立 BFD 会话是指通过命令行手动配置 BFD 会话参数，包括配置本地标识符和远端标识符等，然后手工下发 BFD 会话建立请求。

如果对端设备采用动态 BFD，而本端设备既要与之互通，又要能够实现 BFD 检测静态路由，必须配置静态标识符自协商 BFD。

高级选项

报文优先级：支持将 BFD 报文设置为高优先级报文后，优先保证 BFD 报文的转发。

BFD 会话的检测时间由 BFD 会话的本端检测倍数、本端 BFD 报文的接收间隔、发送间隔决定，检测时间 = 检测倍数 × max（接收间隔，发送间隔）。

发送间隔（毫秒）：缺省情况下，BFD 报文的发送间隔是 1000 毫秒。

接收间隔（毫秒）：缺省情况下，BFD 报文的接收间隔是 1000 毫秒。

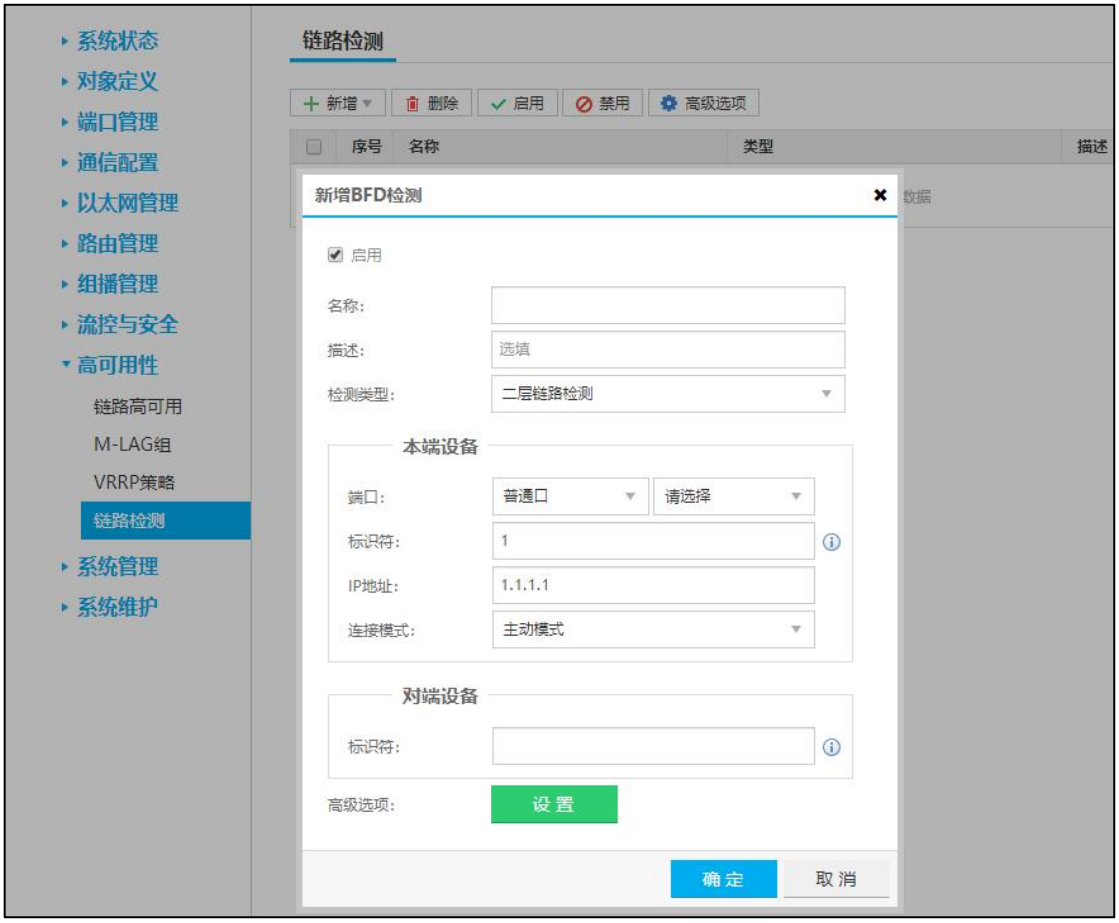
检测倍数：缺省情况下，本地检测倍数为 3。

报文生存时间：为使得使用不同版本的设备能够互通，并考虑后续版本升级以及和其他厂商的设备互通，此时可以配置报文生存时间。

DOWN 状态发包间隔（毫秒）：链路协议 Down 状态，在该状态下只可以处理 BFD 报文，支持配置 DOWN 状态发包间隔，从使是该接口也可以快速感知链路故障。

WTR 等待恢复时间（分钟）：如果 BFD 会话发生振荡，则与之关联的应用将会在主备之间频繁切换。

为避免这种情况的发生，可以配置 BFD 会话的等待恢复时间 WTR。当 BFD 会话从状态 Down 变为状态 Up 时，BFD 等待 WTR 超时后才将这个变化通知给上层应用。如果使用 WTR，用户需要手工在两端配置相同的 WTR。否则，当一端会话状态变化时，两端应用程序感知到的 BFD 会话状态将不一致。



2.10. 系统管理

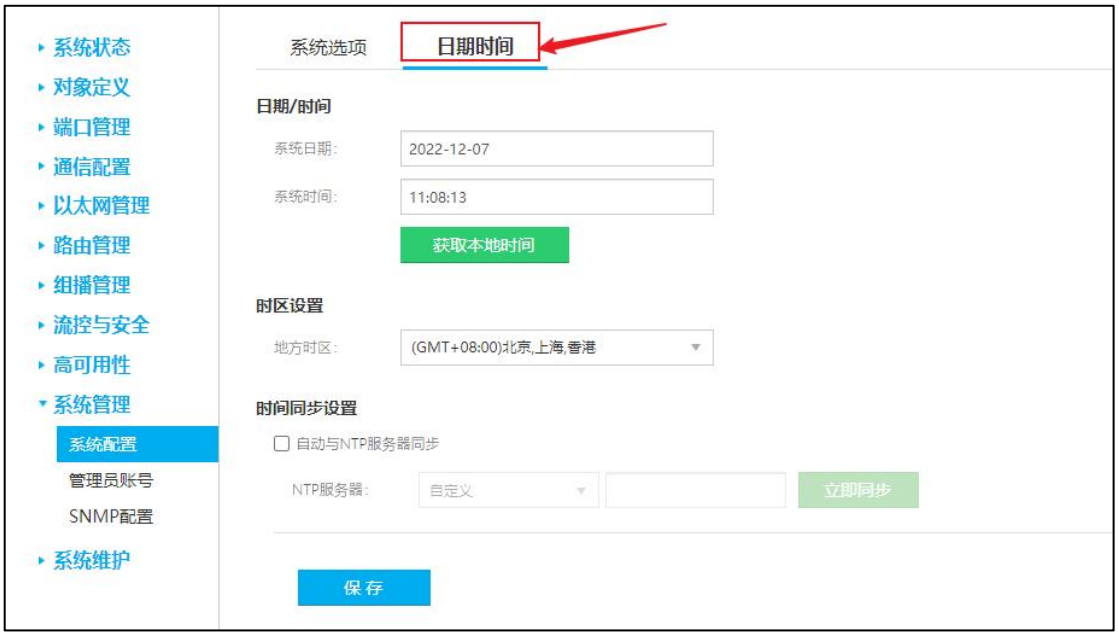
2.10.1. 系统配置

2.10.1.1. 系统选项

可进行 HTTPS 端口、设备名称、控制台超时、语言等配置修改

2.10.1.2. 日期时间

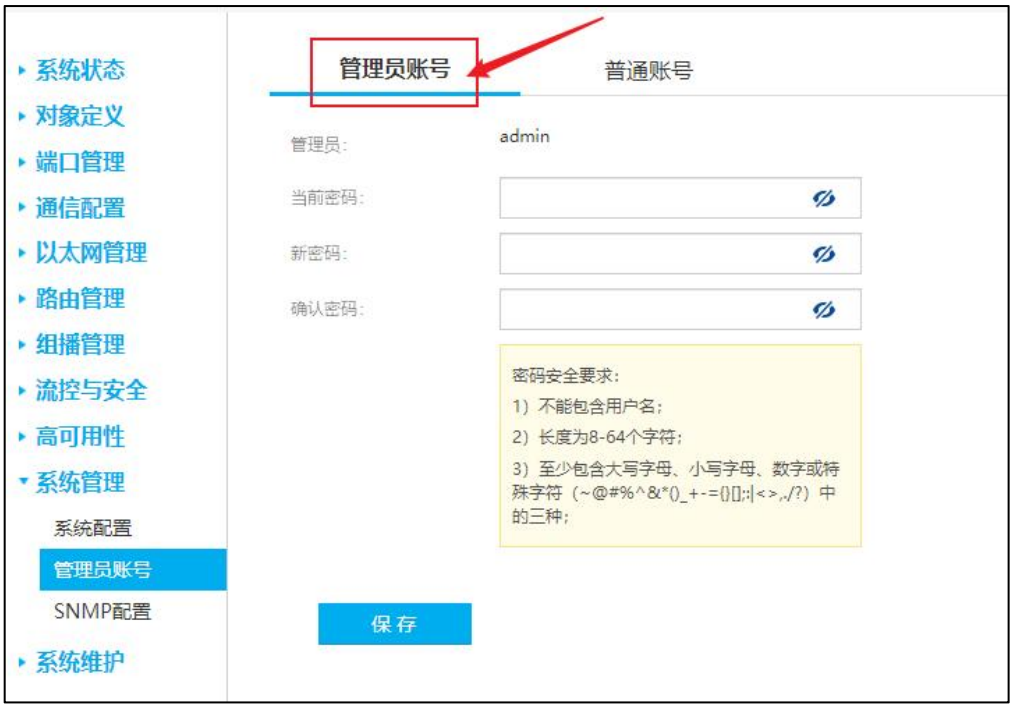
用于交换机的系统日期时间设定。可通过 NTP 服务器进行时间同步。



2.10.2. 管理员账号

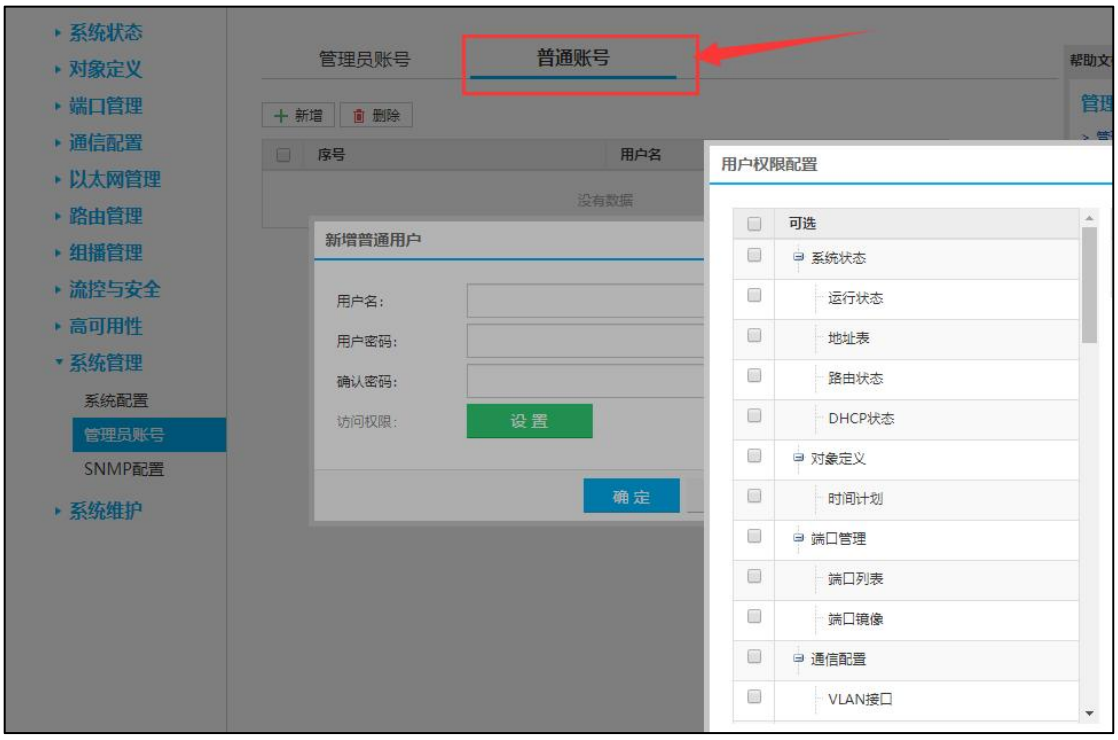
2.10.2.1. 管理员账号

系统内置的超级管理员，具备系统的所有管理权限。为了提高系统的安全性，避免未授权用户登陆管理系统，建议为超级管理员设置一个高强度的密码。



2.10.2.2. 普通账号

可为系统设置多个普通账号，并分别为每个普通账号设置权限。普通用户可通过此账号登录系统，在授权范围内进行操作。



2.10.3. SNMP 配置

SNMP(Simple Network Management Protocol,简单网络管理协议)，用于管理网络中上众多的软硬件平台。开启后可以通过 snmp 协议查询本设备系统信息，如设备型号，内存使用，硬盘使用率，cpu 消耗等。

2.10.3.1. SNMP

SNMP v1/v2

SNMP 的第一版本和第二版本。它们都是基于团体名进行报文认证。

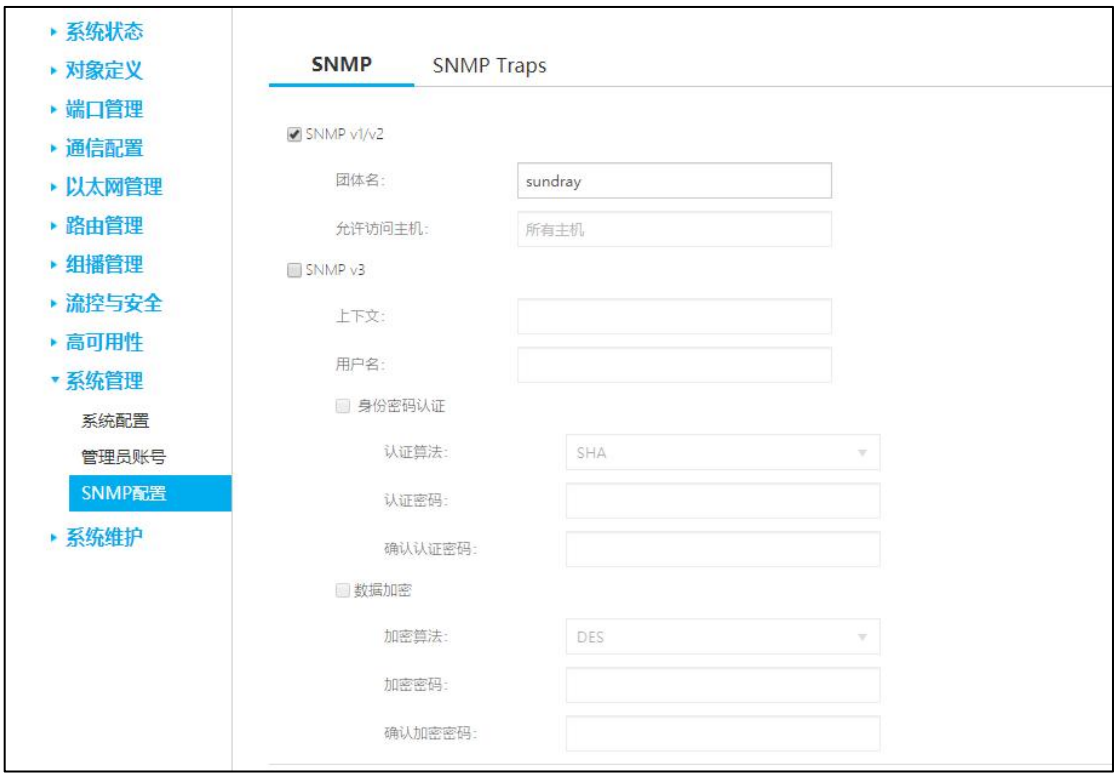
SNMP v3

SNMP 的第三版本。

此版本提供重要的安全性功能，其中就包括了认证和加密两项。

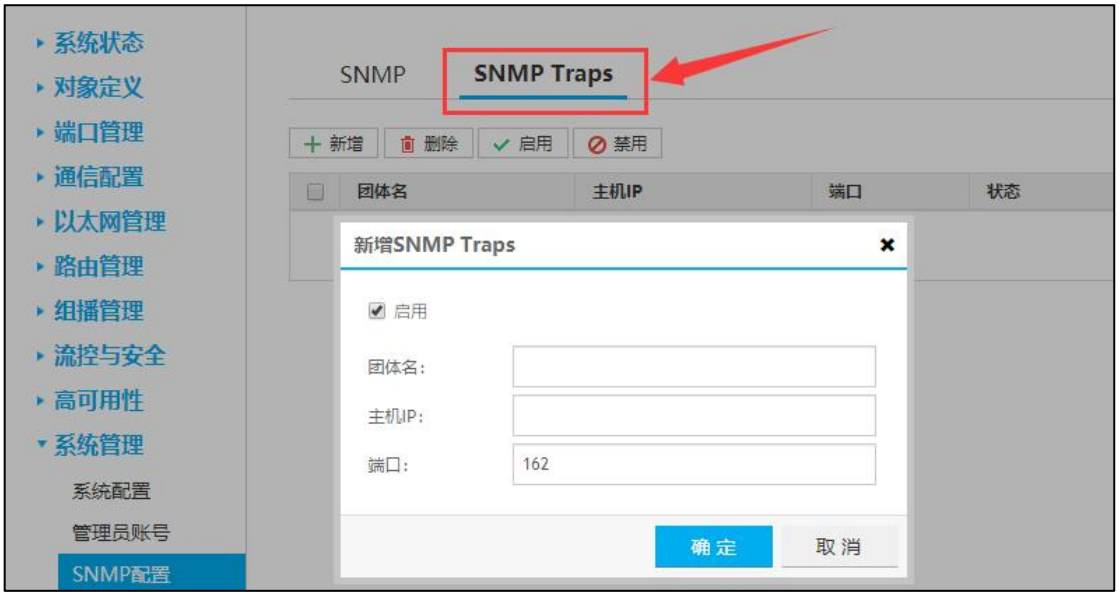
认证需要提供认证方式（MD5，SHA）和认证密码。

加密需要提供加密方式（DES）和加密密钥。



2.10.3.2. SNMP Traps

SNMP Trap 又称 SNMP 陷阱，启用后可以让本设备主动发送信息到管理端，而不需要等到的管理端轮询后再发送。需要配置管理端的 IP 地址和端口，以及团体名。支持向多个管理端发送信息。



2.11. 系统管理

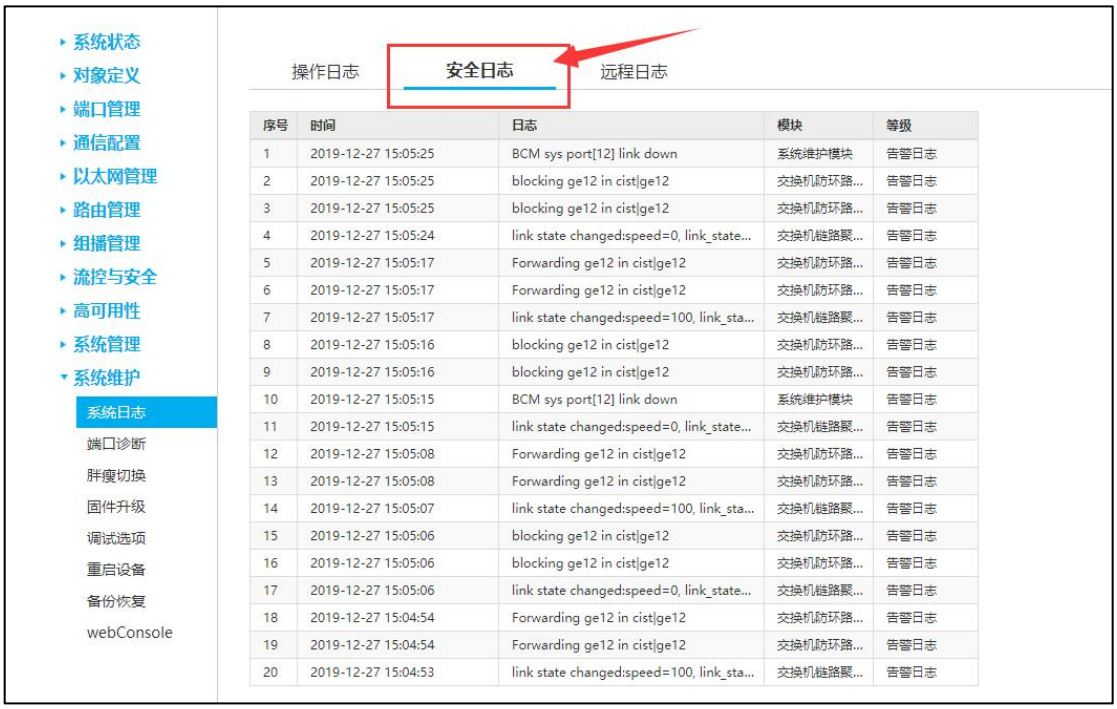
2.11.1. 系统日志

2.11.1.1. 操作日志

保存用户的操作记录，包括账号登陆及退出等。

2.11.1.2. 安全日志

记录所有的检测到的异常事件，并记录检测到的结果。



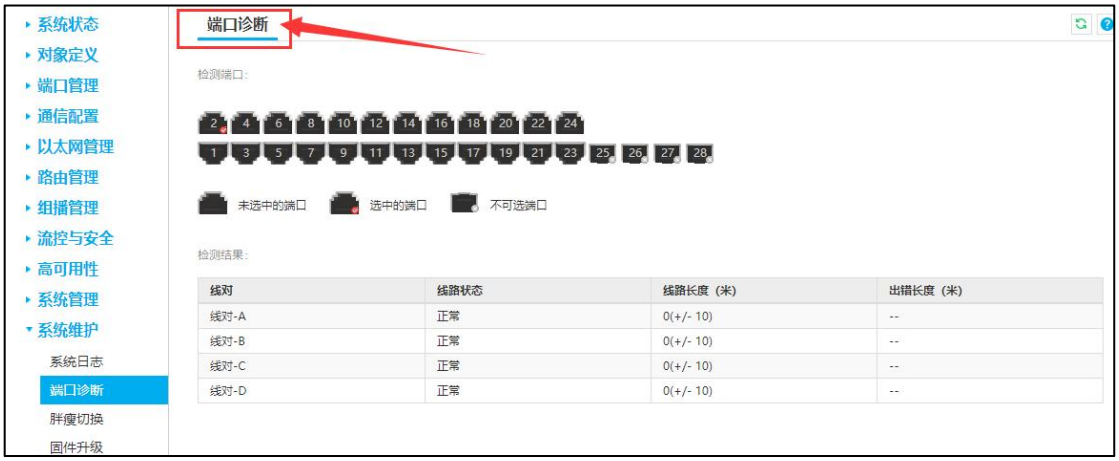
序号	时间	日志	模块	等级
1	2019-12-27 15:05:25	BCM sys port[12] link down	系统维护模块	告警日志
2	2019-12-27 15:05:25	blocking ge12 in cist|ge12	交换机防环路...	告警日志
3	2019-12-27 15:05:25	blocking ge12 in cist|ge12	交换机防环路...	告警日志
4	2019-12-27 15:05:24	link state changed:speed=0, link_state...	交换机链路聚...	告警日志
5	2019-12-27 15:05:17	Forwarding ge12 in cist|ge12	交换机防环路...	告警日志
6	2019-12-27 15:05:17	Forwarding ge12 in cist|ge12	交换机防环路...	告警日志
7	2019-12-27 15:05:17	link state changed:speed=100, link_sta...	交换机链路聚...	告警日志
8	2019-12-27 15:05:16	blocking ge12 in cist|ge12	交换机防环路...	告警日志
9	2019-12-27 15:05:16	blocking ge12 in cist|ge12	交换机防环路...	告警日志
10	2019-12-27 15:05:15	BCM sys port[12] link down	系统维护模块	告警日志
11	2019-12-27 15:05:15	link state changed:speed=0, link_state...	交换机链路聚...	告警日志
12	2019-12-27 15:05:08	Forwarding ge12 in cist|ge12	交换机防环路...	告警日志
13	2019-12-27 15:05:08	Forwarding ge12 in cist|ge12	交换机防环路...	告警日志
14	2019-12-27 15:05:07	link state changed:speed=100, link_sta...	交换机链路聚...	告警日志
15	2019-12-27 15:05:06	blocking ge12 in cist|ge12	交换机防环路...	告警日志
16	2019-12-27 15:05:06	blocking ge12 in cist|ge12	交换机防环路...	告警日志
17	2019-12-27 15:05:06	link state changed:speed=0, link_state...	交换机链路聚...	告警日志
18	2019-12-27 15:04:54	Forwarding ge12 in cist|ge12	交换机防环路...	告警日志
19	2019-12-27 15:04:54	Forwarding ge12 in cist|ge12	交换机防环路...	告警日志
20	2019-12-27 15:04:53	link state changed:speed=100, link_sta...	交换机链路聚...	告警日志

2.11.1.3. 远程日志

可开启远程日志功能，协助发现及排除故障。

2.11.2. 端口诊断

可选择检测端口，对线对、线路状态、线路长度、出错长度进行检测，查看检测结果。



2.11.3. 胖瘦切换

在当前页面填入控制器的地址与端口，要确保交换机地址能够与控制器连通。将接入点连接到控制器，确认后在控制器的接入点激活页面激活交换机，完成胖模式切换为瘦模式。需要注意的是，切换之后会清空已有配置。

2.11.4. 固件升级

支持.img 的包升级。

注意：当前不提供 img 包升级方式，需通过升级客户端加载 ssu 包升级。

2.11.5. 调试选项

允许用户通过 ssh、telnet 方式连接到本设备上进行调试。

2.11.6. 重启设备

可通过点击【重启设备】按钮重启交换机。

2.11.7. 备份恢复

系统中保存了大量的配置信息，包括各功能模块设置，用户账号等关键信息，因此定期对设备执行备份操作是一个良好的管理习惯。

在以下情况下，可以考虑从最近备份的配置中恢复系统，以尽快恢复您的网络，并减少损失：

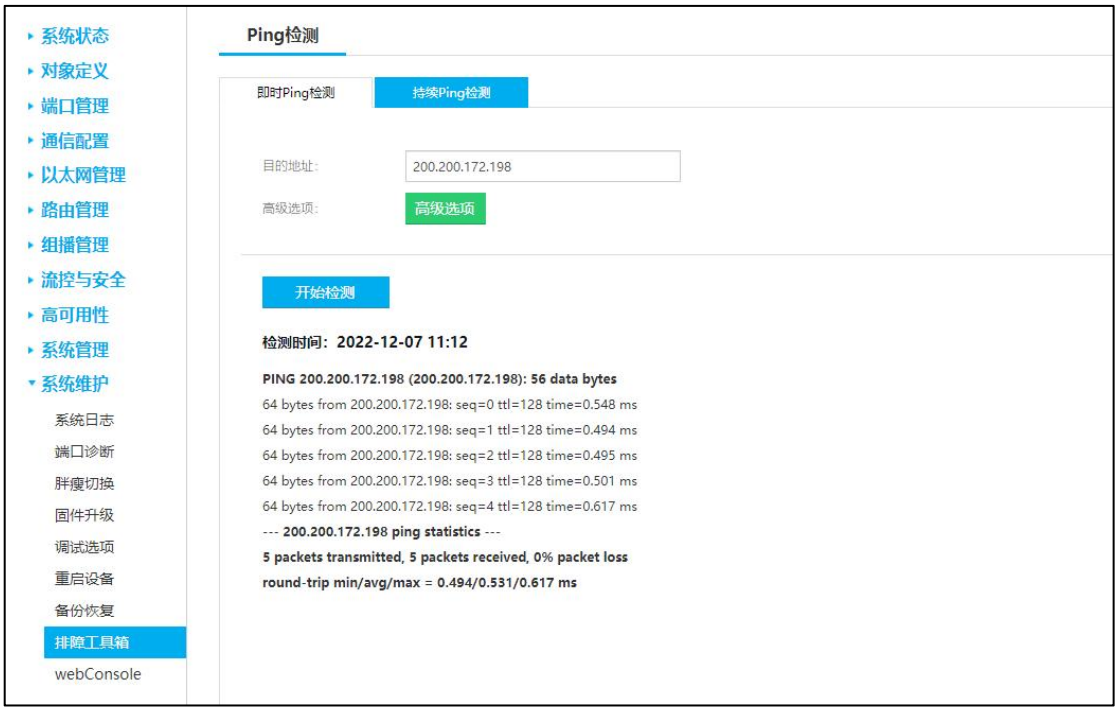
1、设备损坏或丢失，需要更换全新的硬件设备

2、设备误配置，例如误配置了某些基础功能

2.11.8. 排障工具箱

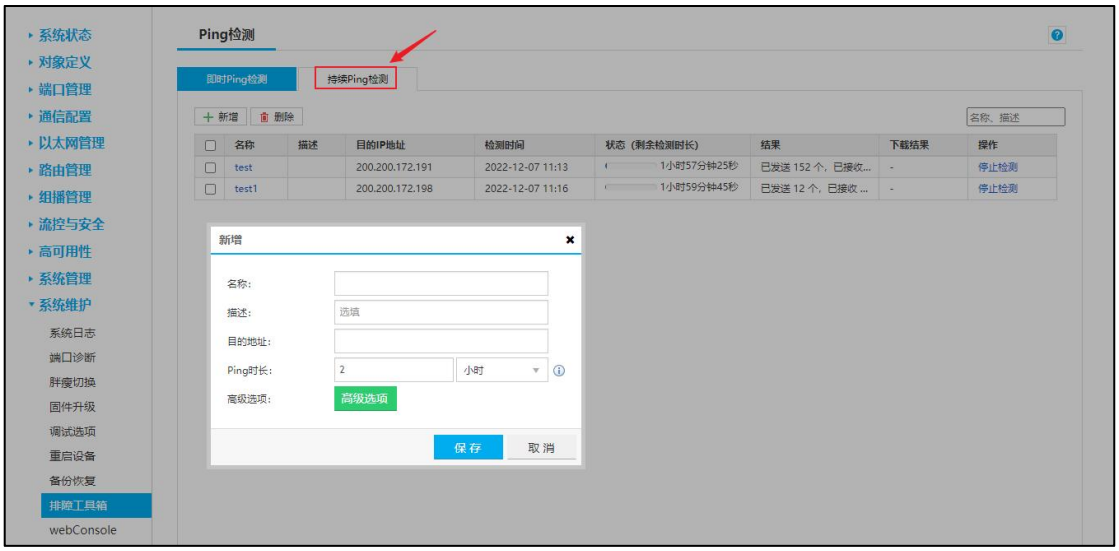
2.11.8.1. 即时 Ping 检测

交换机通过发送固定数量包到目的地址，统计丢包率与时延。



2.11.8.2. 持续 Ping 检测

可同时配置多条 Ping 检测任务，使交换机发送固定时长 ping 包到目的地址，持续统计丢包计数。测试结果支持下载。



2.11.9. webConsole

提供可直接操作 ap 设备的调试命令，用于排除问题。

支持命令：

cls[clear][ctrl+l]	清屏
term[ctrl+c]	结束当前执行程序
traceroute	跟踪数据包转发路径
ping	测试主机地址连通
tcpconnect	测试 TCP 端口连通性
udpconnect	测试 UDP 端口连通性

第 3 章 安视交换机常见问题排查

3.1. 端口镜像配置

在排查问题时，有时需要通过端口镜像抓包分析，如下拓扑，需要将服务器的流量镜像到电脑上抓包分析。

配置如下：

在【端口管理】->【端口镜像】，新增端口镜像策略，模式可以选择镜像源端口入方向、出方向或入方向和出方向的流量，根据以上拓扑源端口选择 ge1 口，目的端口选择 ge2 口，点击保存即可。

3.2. Console 口命令查看相关配置

1、list mac address-table 查看 mac 地址表：

```
Switch# list mac address-table
MAC Address           VLAN  TYPE        Port
====================  ====  ==========  ==========
9c:3a:9a:5f:dc:55     1     dynamic     ge0_0_9
00:0c:29:f3:5e:d5     1     dynamic     ge0_0_9
00:57:41:35:ee:dd     1     dynamic     ge0_0_9
e0:d5:5e:32:9d:4a     1     dynamic     ge0_0_9
b4:2e:99:93:e6:50     1     dynamic     ge0_0_9
00:0c:29:82:76:83     1     dynamic     ge0_0_9
3c:7c:3f:b9:b0:18     1     dynamic     ge0_0_9
```

2、list interface brief 查看所有接口的状态信息：

```
Switch# list interface  brief
Name            Speeds     Status          Duplex    Nego      Vlan_mode  Vlan_id
==============  =========  ==============  ========  ========  =========  =========
ge0_0_1         0          down            full      on        access     12
ge0_0_2         0          down            full      on        access     22
ge0_0_3         0          down            full      on        access     1
ge0_0_4         0          down            full      on        access     1
ge0_0_5         0          down            full      on        access     1
ge0_0_6         0          down            full      on        access     1
ge0_0_7         0          down            full      on        access     1
ge0_0_8         0          down            full      on        access     1
ge0_0_9         100        up              full      on        access     1
ge0_0_10        0          down            full      on        access     1
ge0_0_11        0          down            full      on        access     1
ge0_0_12        0          down            full      on        access     1
ge0_0_13        1000       up              full      on        access     1
ge0_0_14        0          down            full      on        access     1
ge0_0_15        0          down            full      on        access     1
ge0_0_16        0          down            full      on        access     1
ge0_0_17        0          down            full      on        access     1
ge0_0_18        0          down            full      on        access     1
vlan1           auto       up              full      on                   1
```

3、list mode 查看当前交换机的模式，是胖模式还是瘦模式：

```
Switch# list mode
FAT MODE
```

4、list vlan 查看所有 vlan 接口信息：

```
Switch# list vlan

--------------------------------------------------------------------------------
VLAN    Name            Status   Reason         Reserved       Interfaces
--------------------------------------------------------------------------------
1       DEFAULT_VLAN_1  up       ok                            ge0_0_3, ge0_0_4,
                                                               ge0_0_5, ge0_0_6,
                                                               ge0_0_7, ge0_0_8,
                                                               ge0_0_9, ge0_0_10,
                                                               ge0_0_11, ge0_0_12,
                                                               ge0_0_13, ge0_0_14,
                                                               ge0_0_15, ge0_0_16,
                                                               ge0_0_17, ge0_0_18
12      VLAN12          up       ok                            ge0_0_1
22      VLAN22          up       ok                            ge0_0_2
Switch#
```

3.3. 使用 AP 诊断工具进行胖瘦切换

3.3.1. 下载 AP 诊断工具

电脑访问 sundray.com.cn 找到【服务与支持】->【下载中心】->【软件更新】->【常用工具】找到 AP 诊断工具进行下载。

下载类型: 产品彩页 | 软件更新 | 方案彩页 | 使用指导

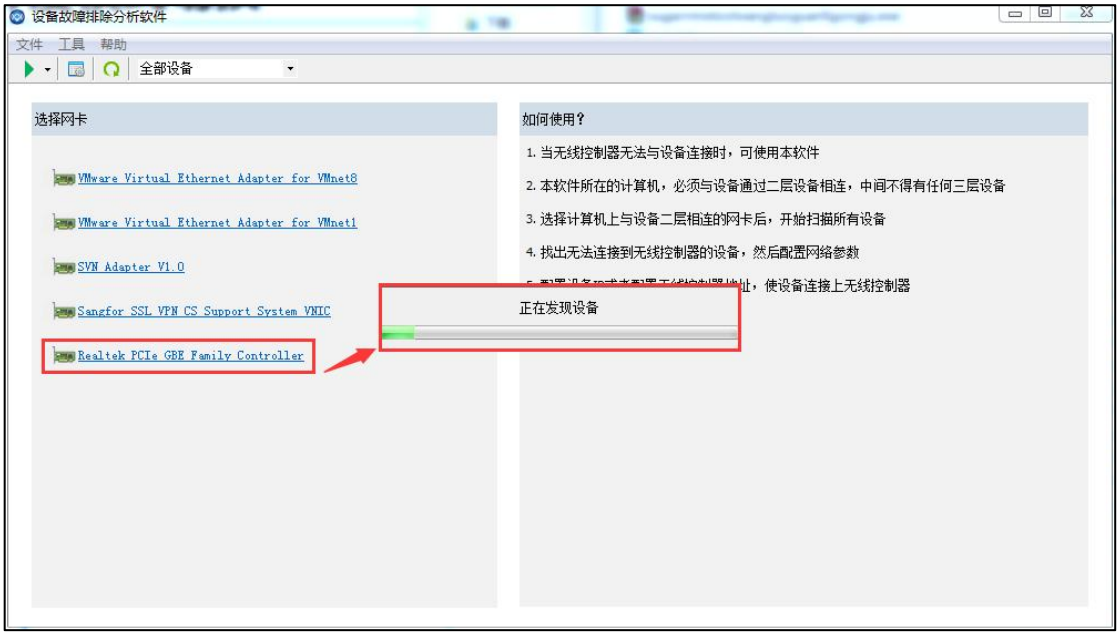
产品类型: · 全部 · 硬件控制平台 · 软件控制平台 · AP升级包 · 交换机 · 物联网平台 · 信锐锐灵系列 · 常用工具

名称	描述	大小	MD5	更新时间	下载
NAC母盘包	NAC母盘包，NAC3.4.2以上版本	158MB	点击查看	2019-08-19	
WDC2.4升级包	升级NAC 2.4前需升级此安装包	220.32M	点击查看	2015-01-26	
增强AC升级稳定性补丁包	支持在无线	691K	点击查看	2019-08-19	
SUNDRAY_Updater6.0	该工具支持SUNDRAY设备的升级	1.7M	点击查看	2019-07-06	
AP诊断工具troubleshoot	AP诊断工具troubleshoot最新版，	4.18 MB	点击查看	2021-09-09	
WinPcap官方软件	WinPcap官方软件	893KB	点击查看	2016-10-18	

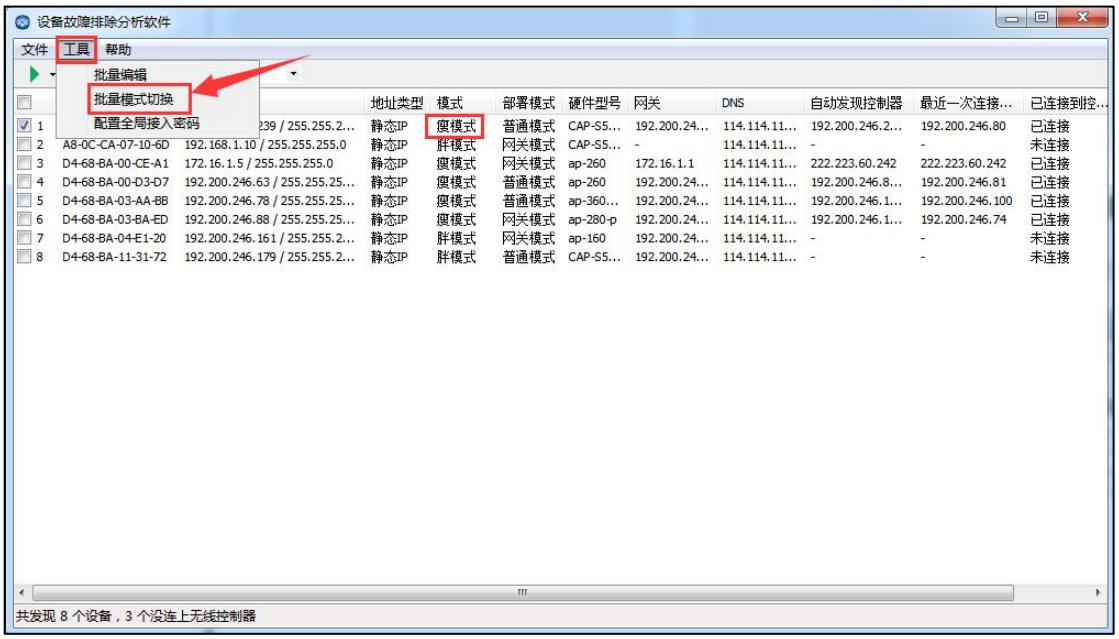
注意：下载时需要同时将 WinPcap 官方软件下载下来，此插件需要配合 AP 诊断工具使用，电脑如果没有安装 winpcap 插件时，AP 诊断工具是无法使用的，需要先安装 winpcap 官方软件后才可以运行。另外，不能使用 win10 系统自带的 winpcap 插件，需要卸载重新下载安装，否则可能出现无法扫描到设备的问题。

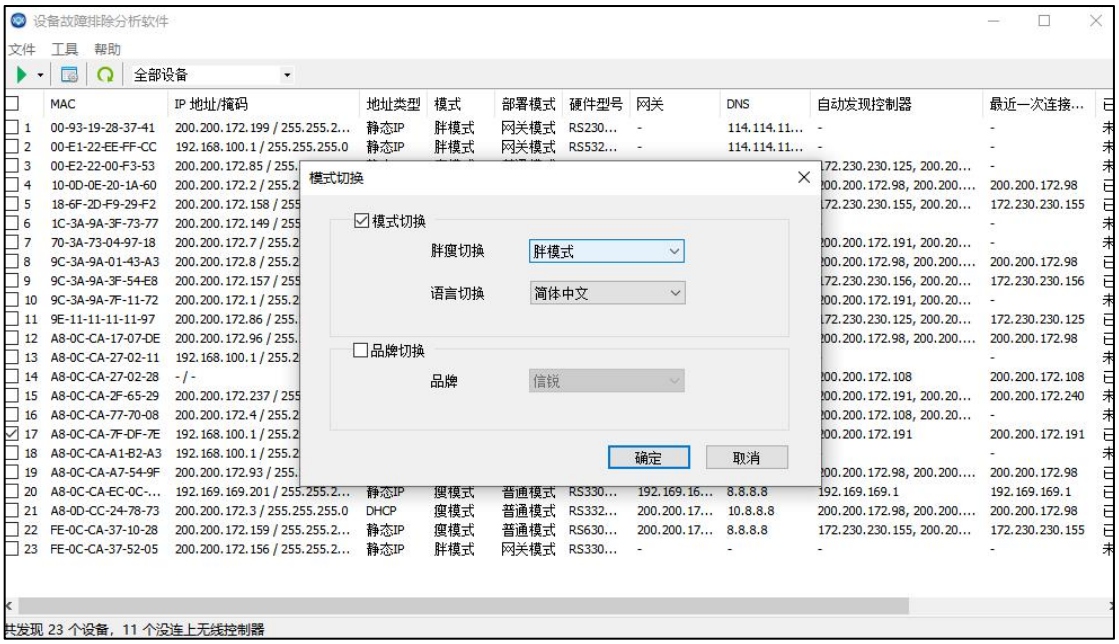
3.3.2. 使用诊断工具扫描

下载好工具后，电脑的有线口直连智能交换机除 MGMT 管理口外的任意电口，然后在 AP 诊断工具中选择电脑的有线网卡进行扫描。

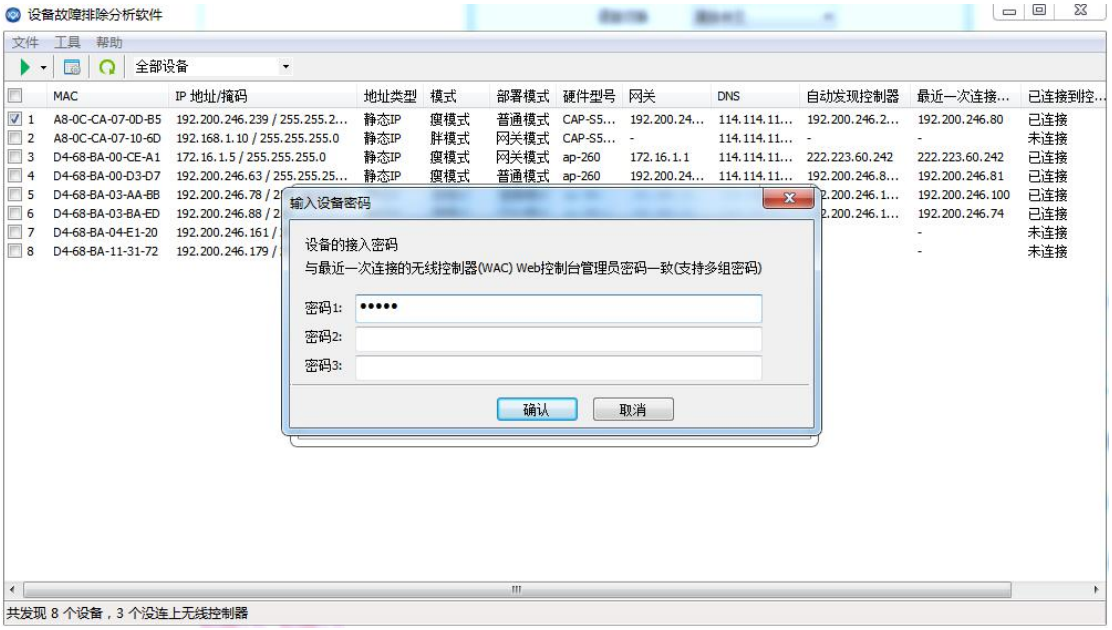


在扫描到智能交换机后，可以看出具体智能交换机的模式，如图为瘦模式，需要切换成胖模式，则选中该智能交换机，点击【工具】->【批量模式切换】进行胖瘦切换。





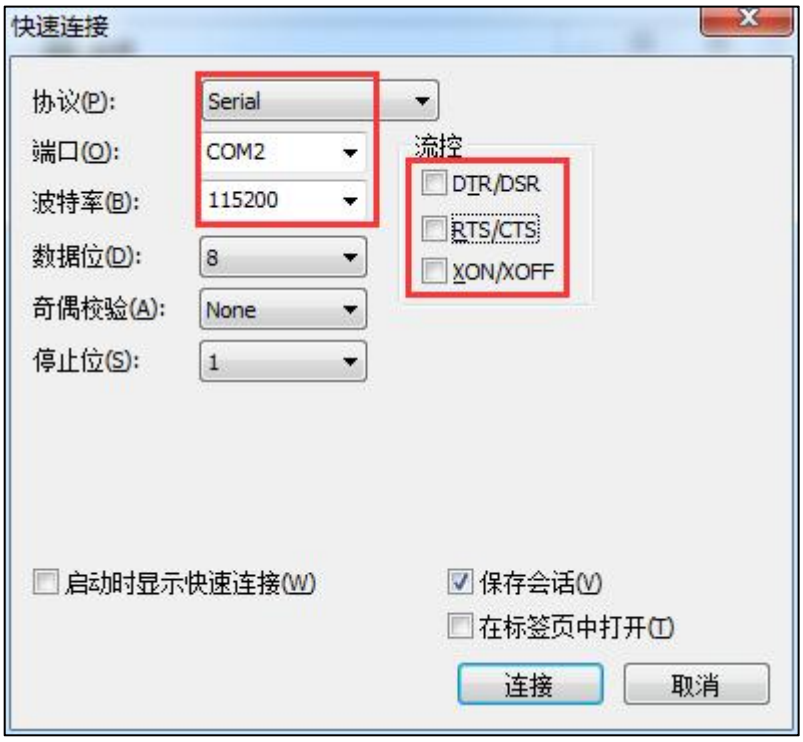
选择胖模式后点击确认，会提示输入密码，默认密码为 admin（若交换机为测试设备，且之前在无线控制器上激活过，那密码为无线控制器 admin 的登录密码，若不知道密码则使用 2.2 小节的方法操作），点击确认后，智能交换机就会自动重启，重启后就会切换到胖模式。



3.4. Console 口进行胖瘦切换

若智能交换机为全光交换机、通过诊断工具无法扫描到交换机，则可以连接 console 线的方法进行胖瘦切换。

以下使用 SecureCRT 进行演示，全系列智能交换机的波特率都为 115200，流控关闭，其他保持默认即可。



点击连接即可进入智能交换机的命令行后台。

```
**********************************************************************
                    Welcome to AnShi Switch
**********************************************************************
The AppVersion is:
SW3.3 BUILD20221118-125252

type 'list' print command list
Switch#
```

在 Switch#模式下进入 config 下使用 switch mode fat(胖)/fit(瘦)进行胖瘦切换。

```
Switch# configure  terminal
Password:
Switch(config)# switch  mode  fat
switch fatap success, but restore default config[y|Y/n|N]
y
```

在输入完 switch mode fat 后，智能交换机会提示交换机切换成功，但会恢复出厂设置，输入 y，智能交换机就会自动重启，重启好后就是胖模式。

3.5. Console 口恢复出厂设置

智能交换机之前在其他地方测试过但是忘记了登录密码或有其他原因需要恢复出厂设置，则按照以下步骤来恢复。

使用 console 线进交换机后台，在 switch#下输入 erase start-config，在提示 Reset switch confirm（y/n）后输入“y”回车，交换机自动重启完之后即恢复出厂设置，此时用户名密码重新恢复为 admin。

```
Switch# erase start-config
Reset switch confirm(y/n)?
y
sh: you need to specify whom to kill
sh: you need to specify whom to kill
/wns/shell/restore_default_config.sh: line 87: getopts: not found
sh: you need to specify whom to kill
find: /extdir/etc/config/ap_bak: No such file or directory
```

第 4 章 附录

4.1. SUNDRAY 设备升级系统的使用

SUNDRAY 设备升级系统可用于对设备进行内核版本升级和备份恢复设备配置。在设备出现致命错误时，也可通过 SUNDRAY 设备升级系统把设备恢复到出厂状态。同时，SUNDRAY 设备升级系统还可以启动技术支持工具来检查系统网口工作状态，路由等配置信息以及更改网口工作模式等。

SUNDRAY 设备升级系统为绿色版软件，解压后即可使用，解压文件里包含一个文件夹和一个主程序，界面如下：

双击打开主程序的主界面，界面如下：

『设备 IP 地址』：连接的 SUNDRAY 设备的 IP 地址，格式为 IP：端口，也可以直接输入 IP 地址进行访问，则默认连接的是该 IP 地址的 51111 端口。

『管理员密码』：默认密码为 admin。

『查找设备』：通过点击查找设备来搜索局域网内部的 SUNDRAY 设备。

输入 SUNDRAY 设备的 IP 地址以及管理员密码后，点击连接即可连接到设备进行系统升级、恢复默认配置等操作，界面如下：


SUNDRAY
当前设备信息
版本: AP3.3 BUILD20221118-125252
IP: 200.200.172.199
设备升级
在线升级
选择版本(S)...
从本地加载升级包
D:\downloads\RS2300F-18S-PWR-LI-16T_3.3_sign(20221118).ss
浏览(B)...
断开连接(D)
下一步(N)